DrayTek

Vigor2915 Series

Dual-WAN Security Router

USER'S GUIDE

V1.2

Vigor2915 Series
Dual-WAN Security Router

User's Guide

Version: 1.2

Firmware Version: V4.3.3.2

(For future update, please visit DrayTek web site)

Date: September 16, 2022

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.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

- Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

  https://www.DrayTek.com

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.

Table of Contents

Part I Installation i

I-1 Introduction 1

I-1-1 Indicators and Connectors 2

I-1-1-1 For Vigor2915 2
I-1-1-2 For Vigor2915F 4
I-1-1-3 For Vigor2915ac 6
I-1-1-4 For Vigor2915Fac 8

I-2 Hardware Installation 10

I-2-1 Installing Vigor Router 10

I-2-2 Wall-Mounted Installation 11

I-2-3 Installing USB Printer to Vigor Router 12

I-3 Accessing Web Page 19

I-4 Changing Password 21

I-5 Dashboard 22

I-5-1 Virtual Panel 23

I-5-2 Name with a Link 23

I-5-3 Quick Access for Common Used Menu 23

I-5-4 GUI Map 25

I-5-5 Web Console 25

I-5-6 Config Backup 26

I-5-7 Manual Download 26

I-5-8 Logout 27

I-5-9 Online Status 27

I-5-9-1 Physical Connection 27
I-5-9-2 Virtual WAN 29

I-6 Quick Start Wizard 30

I-6-1 For WAN1/WAN2 31

I-7 Service Activation Wizard 40

I-8 Registering Vigor Router 42

Part II Connectivity 45

II-1 WAN 46

Web User Interface 48

II-1-1 General Setup 48

II-1-1-1 WAN1 (Fiber) 50
II-1-1-2 WAN1/ WAN2 (Ethernet) 51
II-1-1-3 WAN2 (Wireless LAN 2.4G / 5G) 53
II-1-1-4 WAN2 (USB) 54

II-1-2 Internet Access 55

II-1-2-1 Details Page for PPPoE in WAN1/ WAN2 (Physical Mode: Ethernet) 57
II-1-2-2 Details Page for Static or Dynamic IP in WAN1/ WAN2 (Physical Mode: Ethernet) 60
II-1-2-3 Details Page for PPTP/ L2TP in WAN1/ WAN2 (Physical Mode: Ethernet) 63

II-1-2-4 Details Page for 3G/4G USB Modem (PPP mode) in WAN2 65
II-1-2-5 Details Page for 3G/4G USB Modem (DHCP mode) in WAN2 67
II-1-2-6 Details Page for IPv6 – Offline in WAN1/WAN2 69
II-1-2-7 Details Page for IPv6 – PPP in WAN1/WAN2 70
II-1-2-8 Details Page for IPv6 – TSPC in WAN1/WAN2 71
II-1-2-9 Details Page for IPv6 – AICCU in WAN1/WAN2 73
II-1-2-10 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2 75
II-1-2-11 Details Page for IPv6 – Static IPv6 in WAN1/WAN2 76
II-1-2-12 Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2 78
II-1-2-13 Details Page for IPv6 – 6rd in WAN1/WAN2 79
II-1-3 Multi-VLAN 81
II-1-4 WAN Budget 86
II-1-4-1 General Setup 86
II-1-4-2 Status 89
II-2 LAN 90
Web User Interface 92
II-2-1 General Setup 92
II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup 94
II-2-1-2 Details Page for LAN2 ~ LAN4 97
II-2-1-3 Details Page for IP Routed Subnet 99
II-2-1-4 Details Page for LAN IPv6 Setup 100
II-2-1-5 Advanced DHCP Options 104
Application Notes 106
A-1 Multi-subnet Application - How to utilize Vigor router with non-NAT? 106
II-2-2 VLAN 109
II-2-3 Bind IP to MAC 113
II-2-4 LAN Port Mirror 116
II-3 Hardware Acceleration 117
II-3-1 Setup 117
II-4 NAT 119
Web User Interface 120
II-4-1 Port Redirection 120
II-4-2 DMZ Host 124
II-4-3 Open Ports 127
II-4-4 Port Triggering 129
II-4-5 ALG 131
II-5 Applications 132
Web User Interface 134
II-5-1 Dynamic DNS 134
II-5-2 LAN DNS / DNS Forwarding 140
II-5-3 DNS Security 143
II-5-3-1 General Setup 143
II-5-3-2 Domain Diagnose 144
II-5-4 Schedule 145
II-5-5 RADIUS 148
II-5-6 Active Directory/LDAP 150

II-5-6-1 General Setup *150*
II-5-6-2 Active Directory / LDAP Profiles *151*
II-5-7 UPnP 152
II-5-8 IGMP 153
II-5-8-1 General Setting *153*
II-5-8-2 Working Status *154*
II-5-9 Wake on LAN 155
II-5-10 SMS / Mail Alert Service 156
II-5-10-1 SMS Alert *156*
II-5-10-2 Mail Alert *157*
II-5-11 Bonjour 158
Application Notes 161
A-1 How to Configure Customized DDNS? *161*
II-6 Routing 165
Web User Interface 166
II-6-1 Static Route 166
II-6-2 Load-Balance /Route Policy 172
II-6-2-1 General Setup *172*
II-6-2-2 Diagnose *177*
Application Notes 179
A-1 How to use destination domain name in a route policy? *179*
A-2 How to use a Public IP on LAN *181*
A-3 Introduction to Load Balance/ Route Policy *186*
Part III Wireless LAN 189
III-1 Wireless LAN (2.4GHz/5GHz) 190
Web User Interface 193
III-1-1 Wireless Wizard 193
III-1-2 General Setup 197
III-1-3 Security 199
III-1-4 Access Control 202
III-1-5 WPS 203
III-1-6 WDS (for 5GHz only) 206
III-1-7 Advanced Setting 209
III-1-8 Station Control 212
III-1-9 Bandwidth Management 213
III-1-10 AP Discovery 214
III-1-11 Airtime Fairness 215
III-1-12 Band Steering (for 2.4GHz only) 217
III-1-13 Roaming 221
III-1-14 Station List 222
Part IV VPN 223
IV-1 VPN and Remote Access 224

Web User Interface 225
IV-1-1 VPN Client Wizard 225
IV-1-2 VPN Server Wizard 232
IV-1-3 Remote Access Control 237
IV-1-4 PPP General Setup 238
IV-1-5 SSL General Setup 240
IV-1-6 IPsec General Setup 241
IV-1-7 IPsec Peer Identity 243
IV-1-8 VPN Matcher Setup 245
IV-1-9 OpenVPN 247
IV-1-9-1 OpenVPN Server Setup 247
IV-1-9-2 Client Config 248
IV-1-9-3 Import Certificate 250
IV-1-10 Remote Dial-in User 252
IV-1-11 LAN to LAN 255
IV-1-12 VPN Trunk Management 264
IV-1-13 Connection Management 272
Application Notes 273
A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode ... 273
A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2 278
IV-2 Certificate Management 280
Web User Interface 281
IV-2-1 Local Certificate 281
IV-2-2 Trusted CA Certificate 285
IV-2-3 Certificate Backup 287
IV-2-4 Self-Signed Certificate 287

Part V Security 289

V-1 Firewall 290
Web User Interface 292
V-1-1 General Setup 292
V-1-2 Filter Setup 297
V-1-3 Defense Setup 306
V-1-3-1 DoS Defense 306
V-1-3-2 Spoofing Defense 309
V-2 Central Security Management (CSM) 310
Web User Interface 311
V-2-1 APP Enforcement Profile 311
V-2-2 URL Content Filter Profile 313
V-2-3 Web Content Filter Profile 317
V-2-4 DNS Filter Profile 321
Application Notes 323
A-1 How to Create an Account for MyVigor 323

A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter 327

Part VI Management 333

VI-1 System Maintenance 334

Web User Interface 335

VI-1-1 System Status 336

VI-1-2 TR-069 338

VI-1-2-1 ACS and CPE Settings 338
VI-1-2-2 Reporting Configuration 340
VI-1-2-3 Export Parameters 340

VI-1-3 Administrator Password 341

VI-1-4 User Password 345

VI-1-5 Login Page Greeting 348

VI-1-6 Configuration Backup 350

VI-1-7 Syslog/Mail Alert 354

VI-1-8 Time and Date 357

VI-1-9 SNMP 358

VI-1-10 Management 360

VI-1-11 Panel Control 365

VI-1-12 Self-Signed Certificate 368

VI-1-13 Reboot System 370

VI-1-14 Firmware Upgrade 371

VI-1-15 Dashboard Control 372

VI-2 Bandwidth Management 373

Web User Interface 375

VI-2-1 Sessions Limit 375

VI-2-2 Bandwidth Limit 377

VI-2-3 Quality of Service 379

VI-2-4 APP QoS 385

VI-3 Hotspot Web Portal 387

Web User Interface 387

VI-3-1 Profile Setup 387

VI-3-1-1 Login Method 388
VI-3-1-2 Steps for Configuring a Web Portal Profile 388

VI-3-2 User Information 405

VI-3-2-1 User Info 405
VI-3-2-2 Database Setup 406

VI-3-3 Quota Management 408

VI-3-4 PIN Generator 411

VI-3-4-1 PIN Status 411
VI-3-4-2 PIN Generator 412
VI-3-4-3 PIN Voucher 413

VI-4 User Management 415

Web User Interface 416
VI-4-1 General Setup 416
VI-4-2 User Profile 418
VI-4-3 User Group 423
VI-4-4 User Online Status 424
Application Notes 426
A-1 How to authenticate clients via User Management 426
A-2 How to use Landing Page Feature 435
VI-5 Central Management (External Devices) 439
VI-5-1 All Devices 439

Part VII Others 441

VII-1 Objects Settings 442
Web User Interface 443
VII-1-1 IP Object 443
VII-1-2 IP Group 446
VII-1-3 IPv6 Object 448
VII-1-4 IPv6 Group 450
VII-1-5 Service Type Object 452
VII-1-6 Service Type Group 454
VII-1-7 Keyword Object 456
VII-1-8 Keyword Group 458
VII-1-9 File Extension Object 459
VII-1-10 SMS/Mail Service Object 461
VII-1-11 Notification Object 466
VII-1-12 String Object 468
VII-1-13 Objects Backup/Restore 469
Application Notes 471
A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection 471
VII-2 USB Application 475
Web User Interface 476
VII-2-1 USB General Settings 476
VII-2-2 USB User Management 477
VII-2-3 File Explorer 479
VII-2-4 USB Device Status 480
VII-2-5 Temperature Sensor 481
VII-2-6 Modem Support List 483
VII-2-7 SMB Client Support List 484
Application Notes 485
A-1 How can I get the files from USB storage device connecting to Vigor router? ... 485

Part VIII Troubleshooting 489

VIII-1 Diagnostics 490
Web User Interface 491
VIII-1-1 Dial-out Triggering 491
VIII-1-2 Routing Table 492
VIII-1-3 ARP Cache Table 493
VIII-1-4 IPv6 Neighbour Table 494
VIII-1-5 DHCP Table 495
VIII-1-6 NAT Sessions Table 496
VIII-1-7 DNS Cache Table 497
VIII-1-8 Ping Diagnosis 498
VIII-1-9 Data Flow Monitor 499
VIII-1-10 Traffic Graph 502
VIII-1-11 Trace Route 503
VIII-1-12 Syslog Explorer 504
VIII-1-13 IPv6 TSPC Status 506
VIII-1-14 DoS Flood Table 507
VIII-1-15 Route Policy Diagnosis 508
VIII-2 Checking If the Hardware Status Is OK or Not 510
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not 511
VIII-4 Pinging the Router from Your Computer 514
VIII-5 Checking If the ISP Settings are OK or Not 515
VIII-6 Problems for 3G/4G Network Connection 516
VIII-7 Backing to Factory Default Setting If Necessary 517

Part IX Telnet Commands 519

Accessing Telnet of Vigor2915 520

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.

Vigor2915 series integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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

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

User Management implemented on your router firmware can allow you to prevent any computer from accessing your Internet connection without a username or password. You can also allocate time budgets to your employees within office network.

With the 6-port Gigabit switch on the LAN side provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. The tagged VLANs (IEEE802.1Q) 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 (Multiple-Private LAN Subnets).

On the Wireless-equipped models (Vigor2915ac/n-plus/Vn/Vn-plus/ac/Vac) each of the wireless SSIDs can also be grouped within one of the VLANs.

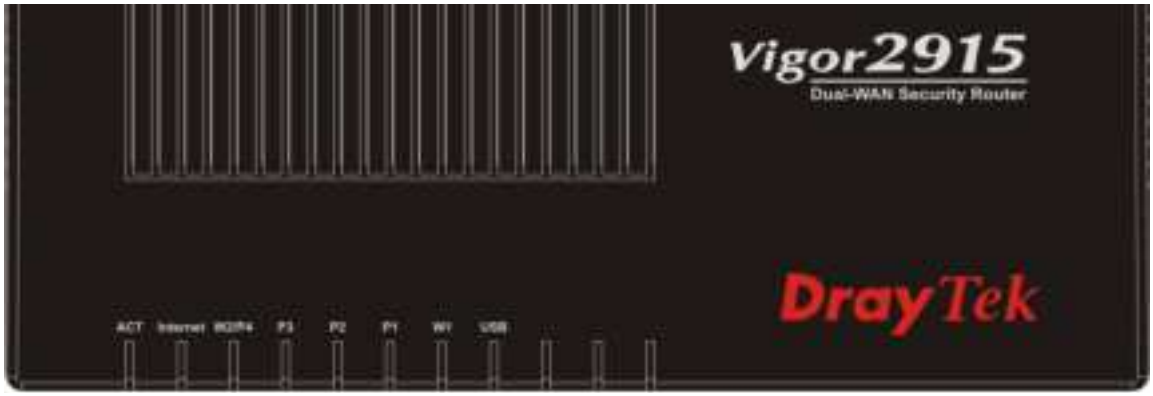
In addition, Vigor2915 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2915 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

I-1-1 Indicators and Connectors

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

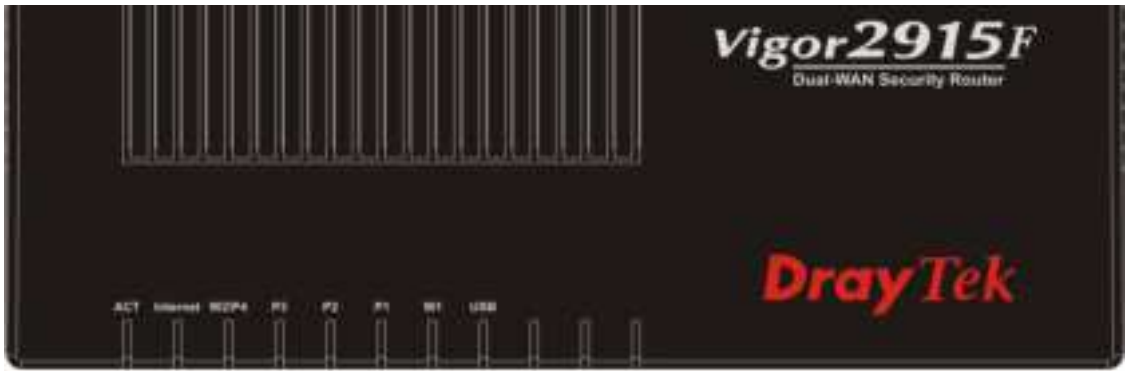
I-1-1-1 For Vigor2915



LED	Status	Explanation
ACT	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
Internet	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
W2/P4	On	The WAN/LAN port is connected.
	Off	The WAN/LAN port is disconnected.
	Blinking	The data is transmitting.
P3~P1	On	The LAN port is connected.
	Off	The LAN port is disconnected.
	Blinking	The data is transmitting.
W1	On	The WAN port is connected.
	Off	The WAN port is disconnected.
	Blinking	The data is transmitting.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.

Interface	Description
PWR	Connector for a power cord.
ON/OFF	Power Switch.
USB	Connector for a USB device (for 3G/4G USB Modem or printer or Environmental Thermometer).
W1	Connecter for local network devices or modem for accessing Internet.
P1~P3	Connecters for local network devices.
W2/P4	The function of this connector is adjustable and controlled by web user interface. It can perform the job as a WAN port (for accessing Internet) or as a LAN port (for local network devices).
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

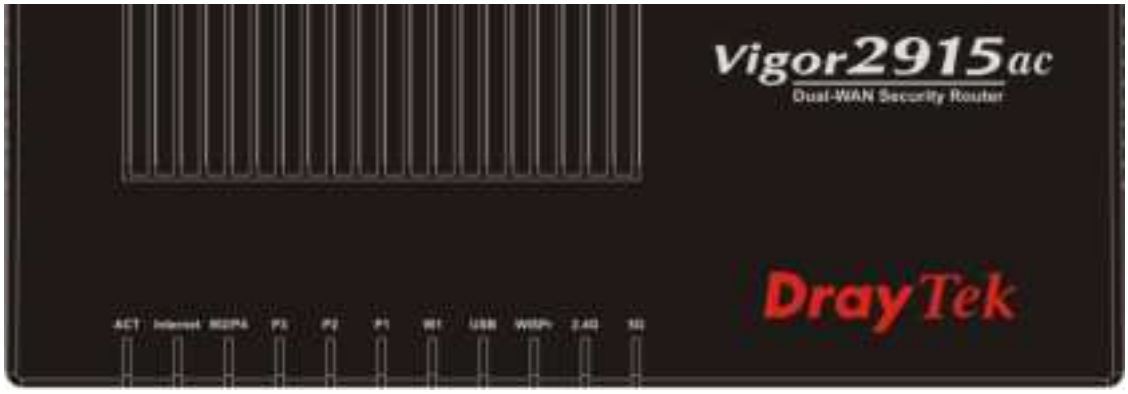
I-1-1-2 For Vigor2915F



LED	Status	Explanation
ACT	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
Internet	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
W2/ P4	On	The WAN/ LAN port is connected.
	Off	The WAN/ LAN port is disconnected.
	Blinking	The data is transmitting.
P3~P1	On	The LAN port is connected.
	Off	The LAN port is disconnected.
	Blinking	The data is transmitting.
W1	On	SFP module is plugged and the fiber link is up.
	Off	SFP module is unplugged or the fiber link is down.
	Blinking	The data is transmitting.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.

Interface	Description
PWR	Connector for a power cord.
ON/OFF	Power Switch.
USB	Connector for a USB device (for 3G/4G USB Modem or printer or Environmental Thermometer).
W1	Fiber connection (1G) for accessing the Internet.
P1~P3	Connecters for local network devices.
W2/P4	The function of this connector is adjustable and controlled by web user interface. It can perform the job as a WAN port (for accessing Internet) or as a LAN port (for local network devices).
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

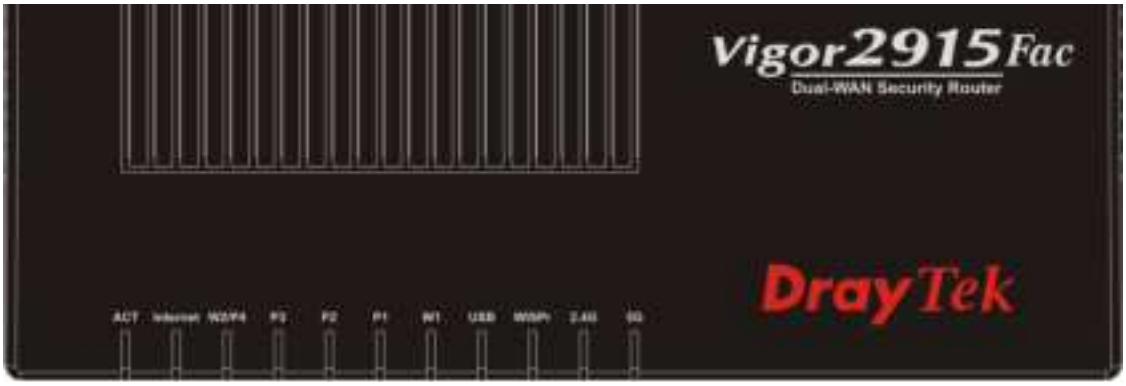
I-1-1-3 For Vigor2915ac



LED	Status	Explanation
ACT	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
Internet	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
W2/ P4	On	The WAN/ LAN port is connected.
	Off	The WAN/ LAN port is disconnected.
	Blinking	The data is transmitting.
P3~P1	On	The LAN port is connected.
	Off	The LAN port is disconnected.
	Blinking	The data is transmitting.
W1	On	The WAN port is connected.
	Off	The WAN port is disconnected.
	Blinking	The data is transmitting.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
WISPr	On	Wi-Fi WAN connected.
	Off	Wi-Fi WAN disconnected.
	Blinking	The data is transmitting.
2.4G/ 5G	On	Wireless access point with bandwidth of 2.4GHz/ 5GHz is ready.
	Blinking	It will blink slowly while wireless traffic goes through. ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)

Interface	Description
PWR	Connector for a power cord.
ON/OFF	Power Switch.
USB	Connector for a USB device (for 3G/4G USB Modem or printer or Environmental Thermometer).
W1	Connecter for local network devices or modem for accessing Internet.
P1~P3	Connecters for local network devices.
W2/P4	The function of this connector is adjustable and controlled by web user interface. It can perform the job as a WAN port (for accessing Internet) or as a LAN port (for local network devices).
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

I-1-1-4 For Vigor2915Fac



LED	Status	Explanation
ACT	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
Internet	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
W2/P4	On	The WAN/LAN port is connected.
	Off	The WAN/LAN port is disconnected.
	Blinking	The data is transmitting.
P3~P1	On	The LAN port is connected.
	Off	The LAN port is disconnected.
	Blinking	The data is transmitting.
W1	On	SFP module is plugged and the fiber link is up.
	Off	SFP module is unplugged or the fiber link is down.
	Blinking	The data is transmitting.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
WISPr	On	Wi-Fi WAN connected.
	Off	Wi-Fi WAN disconnected.
	Blinking	The data is transmitting.
2.4G/5G	On	Wireless access point with bandwidth of 2.4GHz/5GHz is ready.
	Blinking	It will blink slowly while wireless traffic goes through. ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)

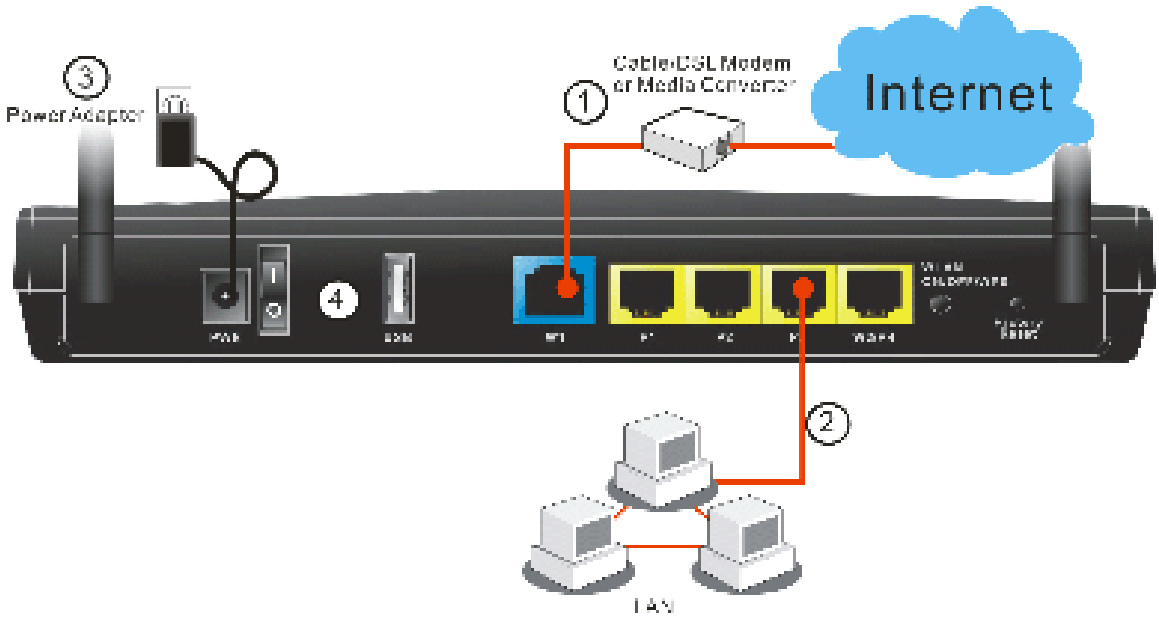
Interface	Description
PWR	Connector for a power cord.
ON/ OFF	Power Switch.
USB	Connector for a USB device (for 3G/ 4G USB Modem or printer or Environmental Thermometer).
W1	Fiber connection (1G) for accessing the Internet.
P1~P3	Connecters for local network devices.
W2/ P4	The function of this connector is adjustable and controlled by web user interface. It can perform the job as a WAN port (for accessing Internet) or as a LAN port (for local network devices).
Wireless LAN ON/ OFF/ WPS	Press "Wireless LAN ON/ OFF/ WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/ OFF/ WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

I-2 Hardware Installation

I-2-1 Installing Vigor Router

Before starting to configure the router, you have to connect your devices correctly. In this section, Vigor2915ac is taken as an example.

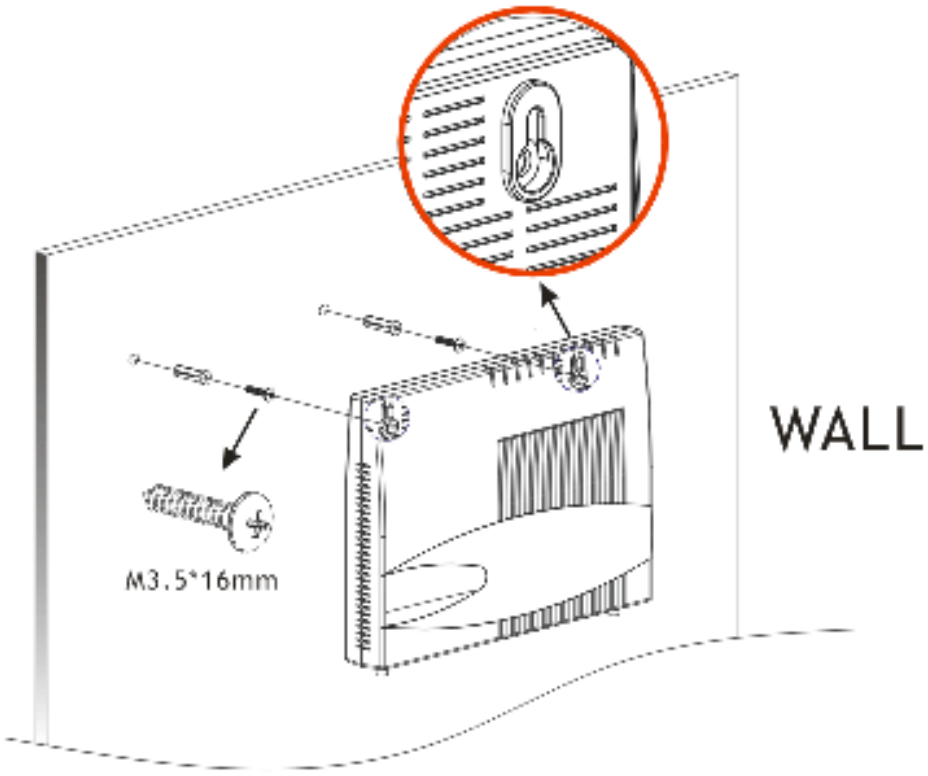
1. Connect the cable Modem/ DSL Modem/ Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports (P1~P4) of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
4. Power on the device by pressing down the power switch on the rear panel.
5. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.



I-2-2 Wall-Mounted Installation

Vigor router has keyhole type mounting slots on the underside.

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

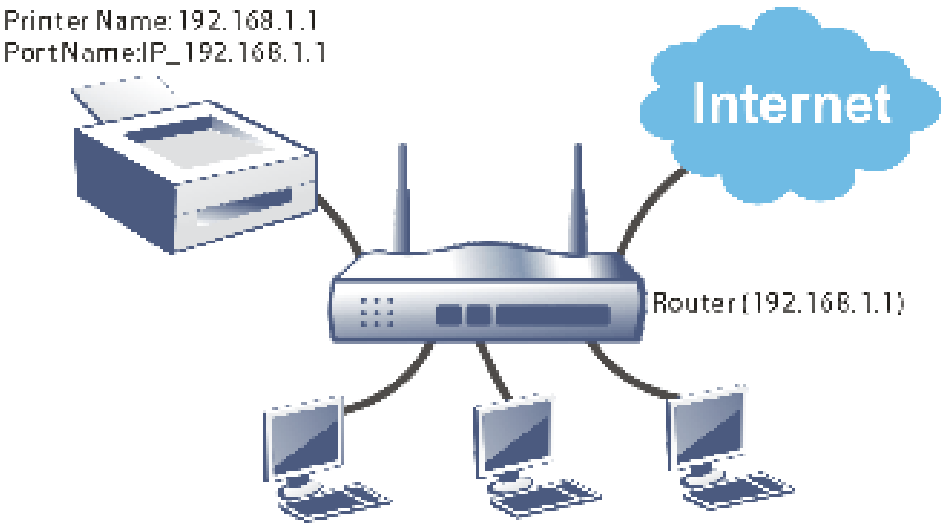


Note The recommended drill diameter shall be 6.5mm (1/4").

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

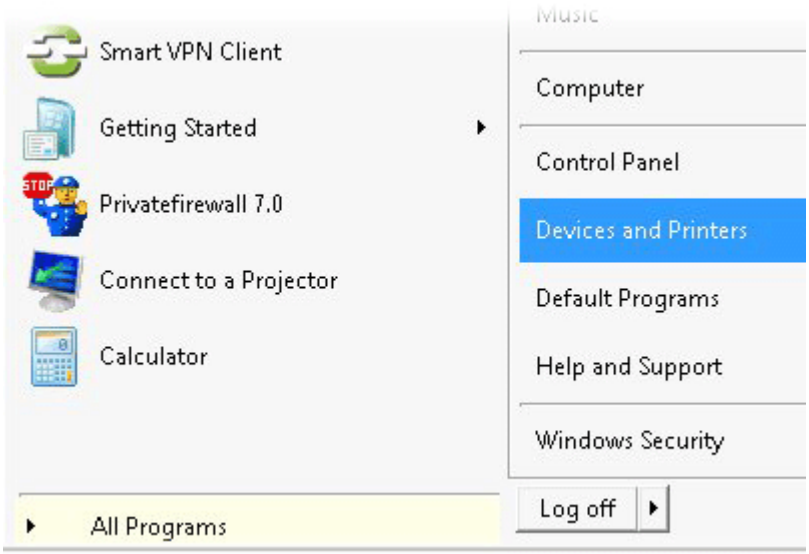
I-2-3 Installing USB Printer to Vigor Router

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows 7. For other Windows system, please visit **www.DrayTek.com**.

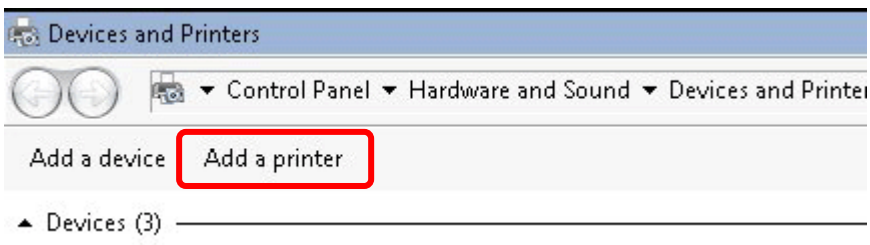


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

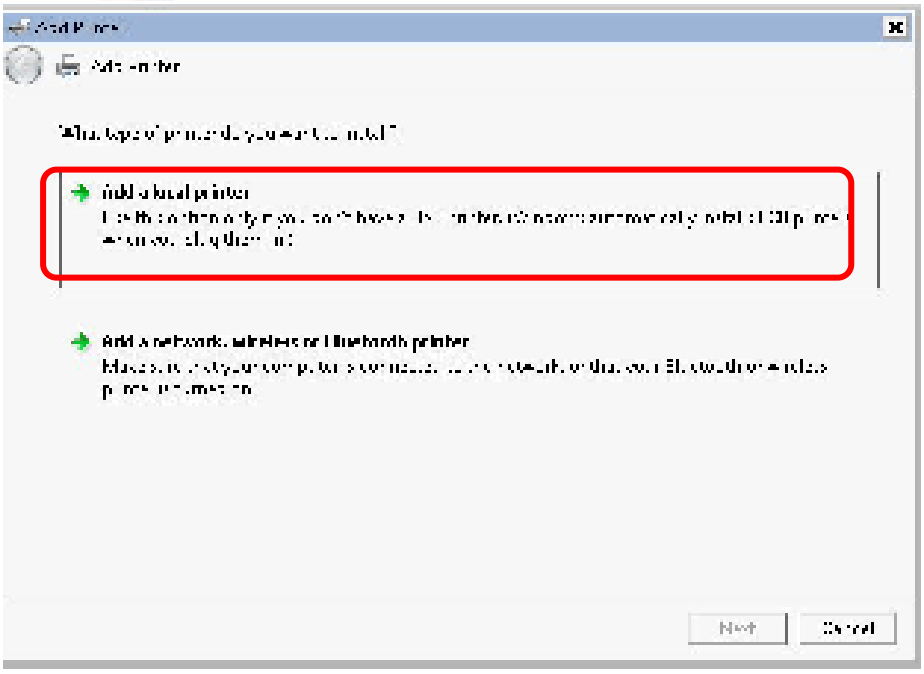
1. Connect the printer with the router through USB/ parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



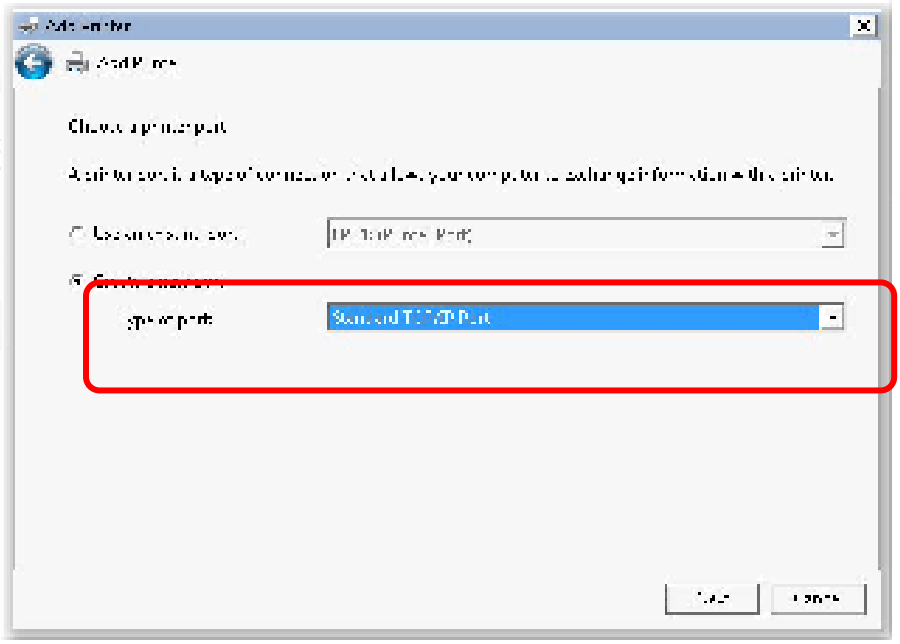
3. Click **Add a printer**.



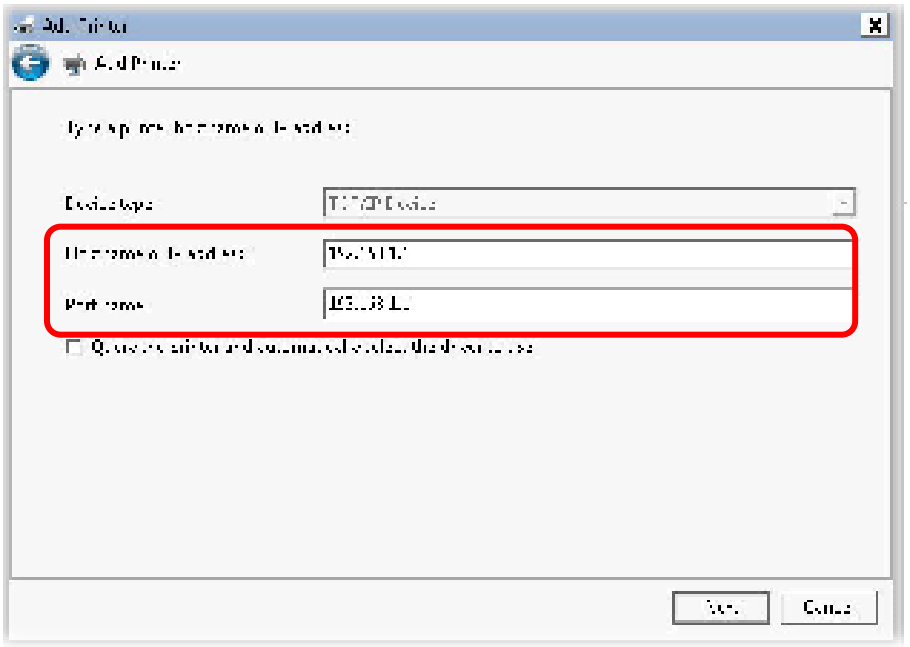
4. A dialog will appear. Click **Add a local printer** and click **Next**.



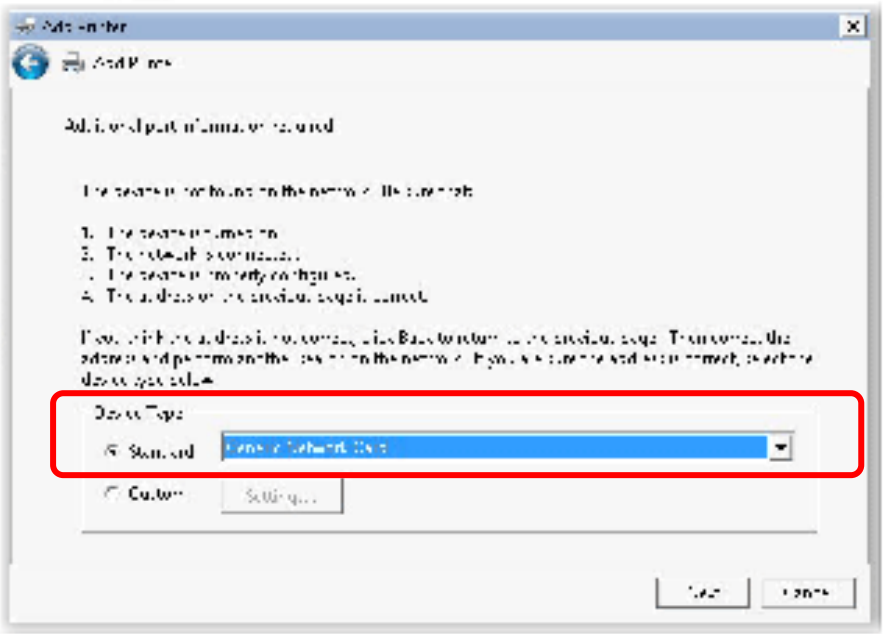
5. In this dialog, choose **Create a new port.** In the field of **Type of port,** use the drop down list to select **Standard TCP/IP Port**. Then, click **Next**.



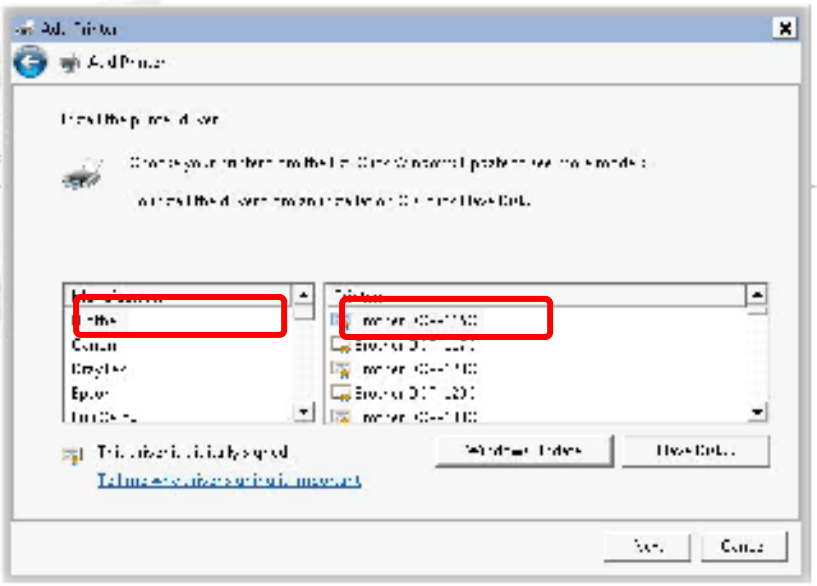
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.



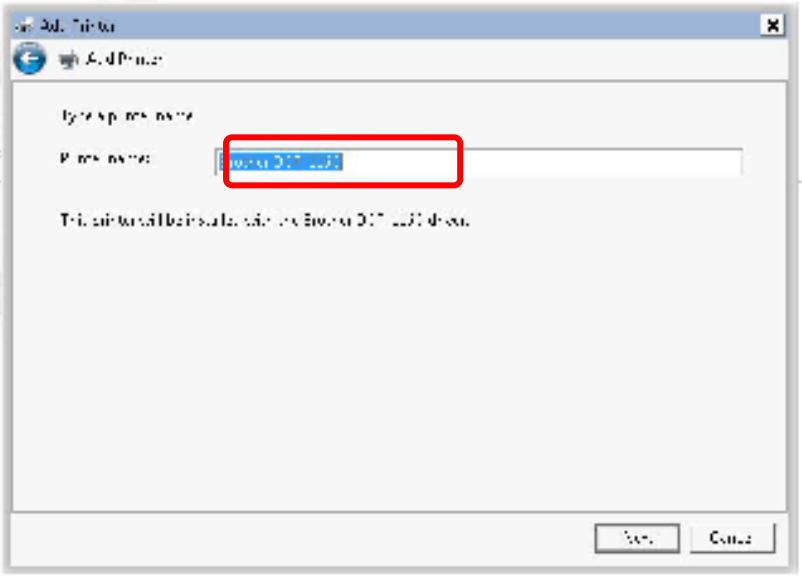
7. Click **Standard** and choose **Generic Network Card**.



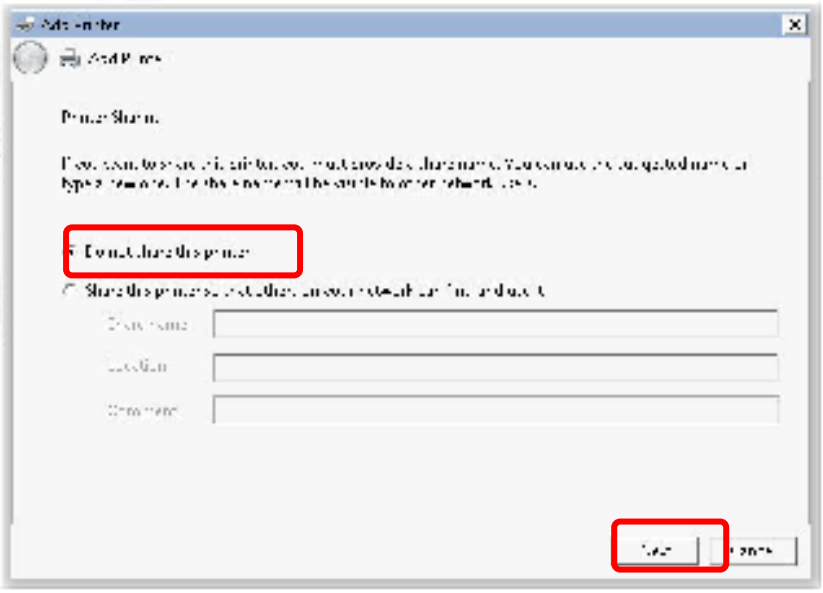
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



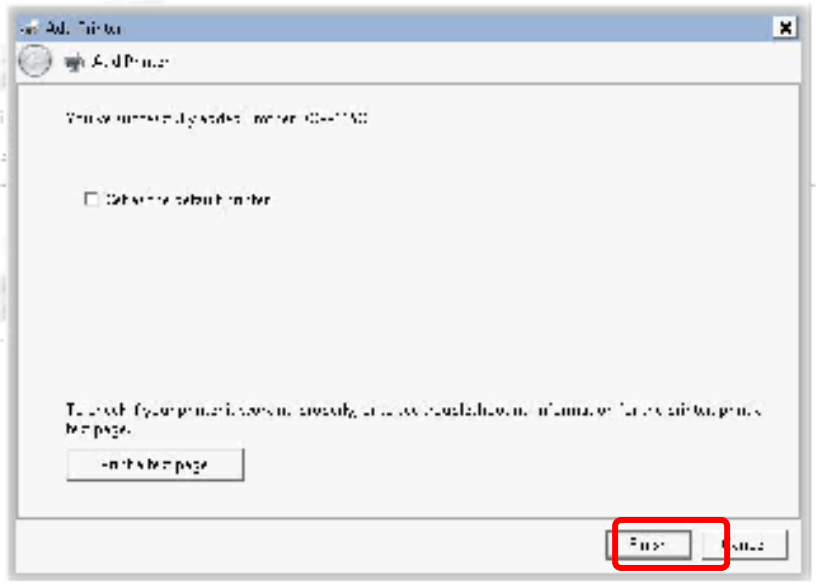
9. Type a name for the chosen printer. Click **Next.**



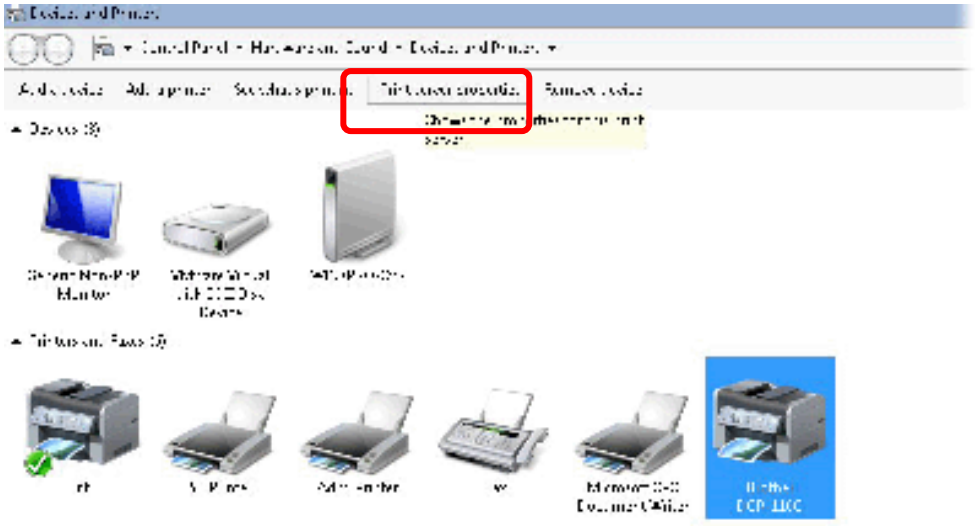
10. Choose **Do not share this printe**r and click **Next**.



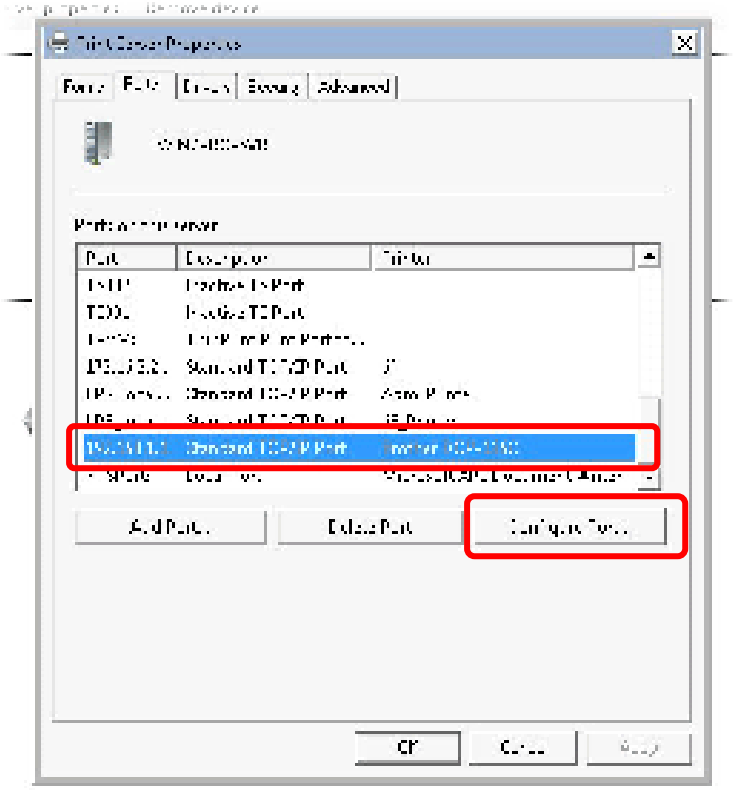
11. Then, in the following dialog, click **Finish**.



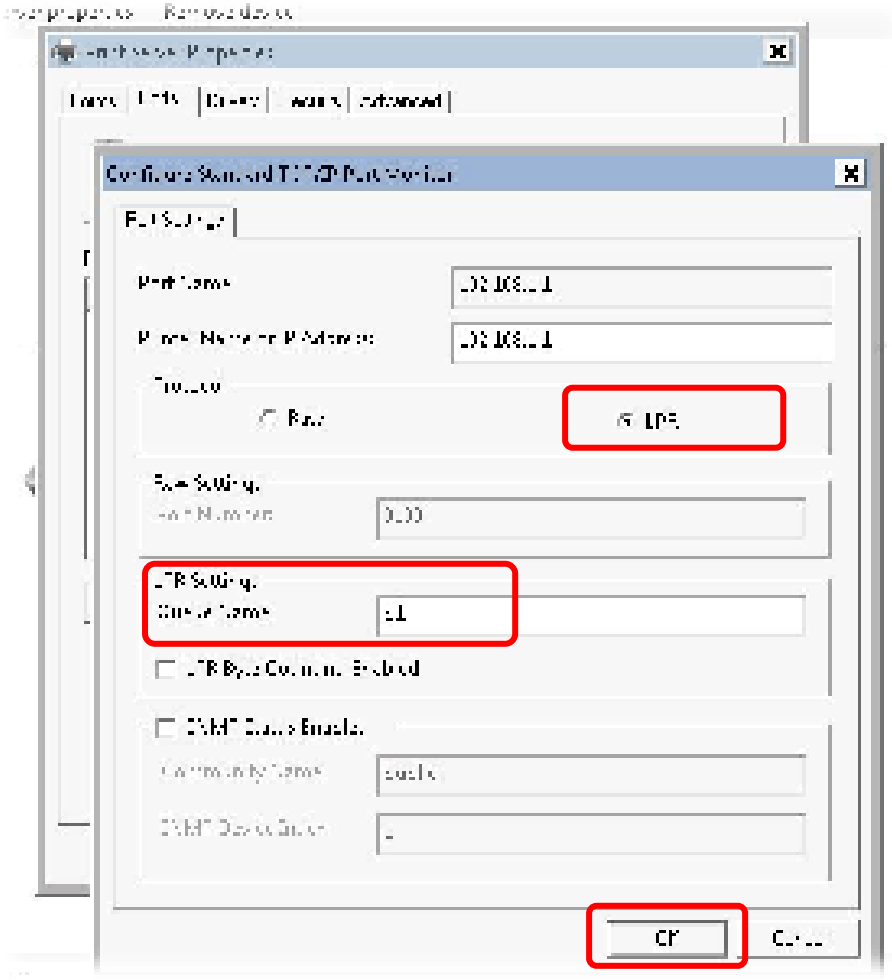
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



13. Edit the property of the new printer you have added by clicking **Configure Port**.



14. Select "**LPR**" on Protocol, type **p1** (number 1) as **Queue Name**. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.



The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Info	Some printers with the fax/scanning or other additional functions are not supported. Vigor router supports printing request from computers via LAN ports but not WAN port.

I-3 Accessing Web Page

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

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

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

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

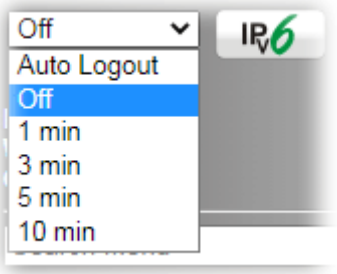
Info	If you fail to access to the web configuration, please go to "Trouble Shooting" for detecting and solving your problem.

4. Now, the **Main Screen** will appear. Take Vigor2915ac as as example.

Info

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

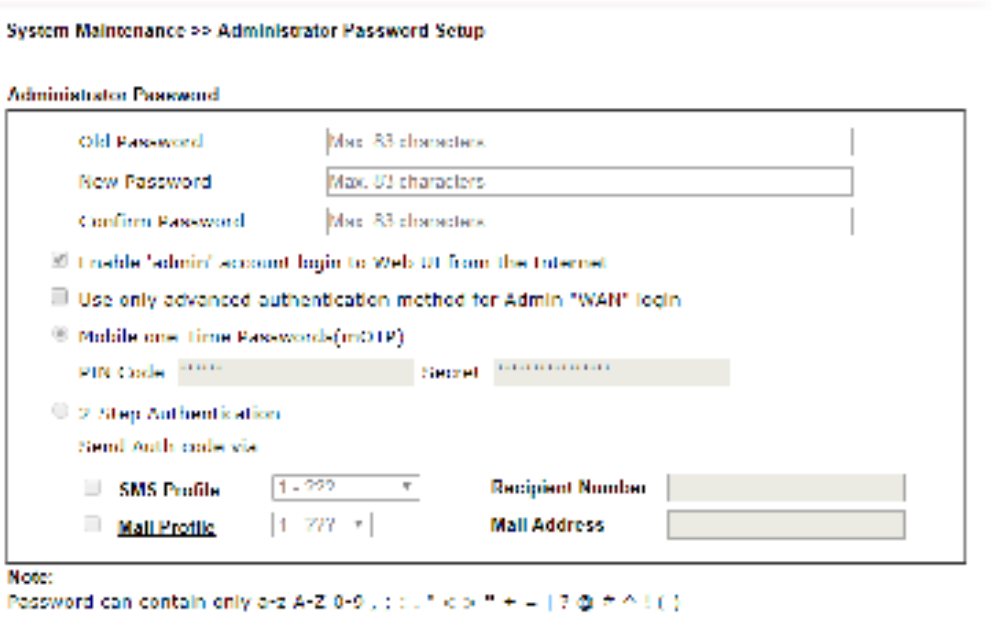
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



I-4 Changing Password

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

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



4. Enter the login password (the default is "admin") on the field of **Old Password**. Enter **New Password** and **Confirm Password**. Then click **OK** to continue.
5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.

Info

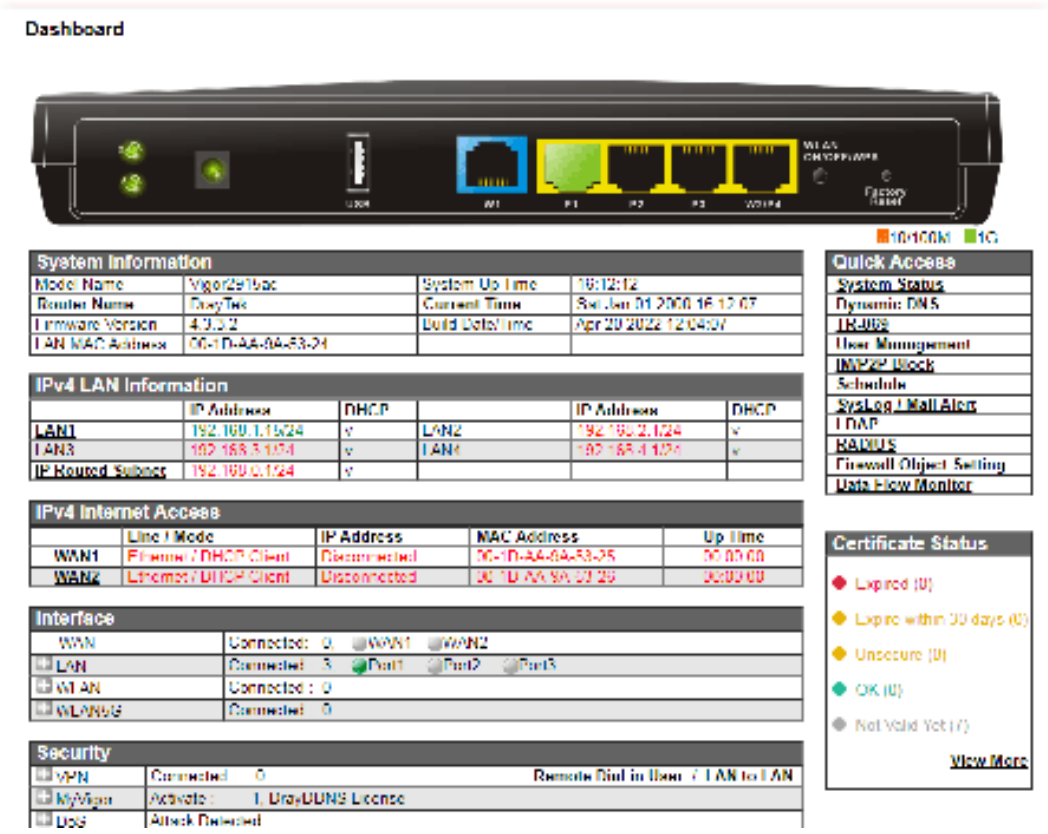
Even the password is changed, the Username for logging onto the web user interface is still "admin".

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

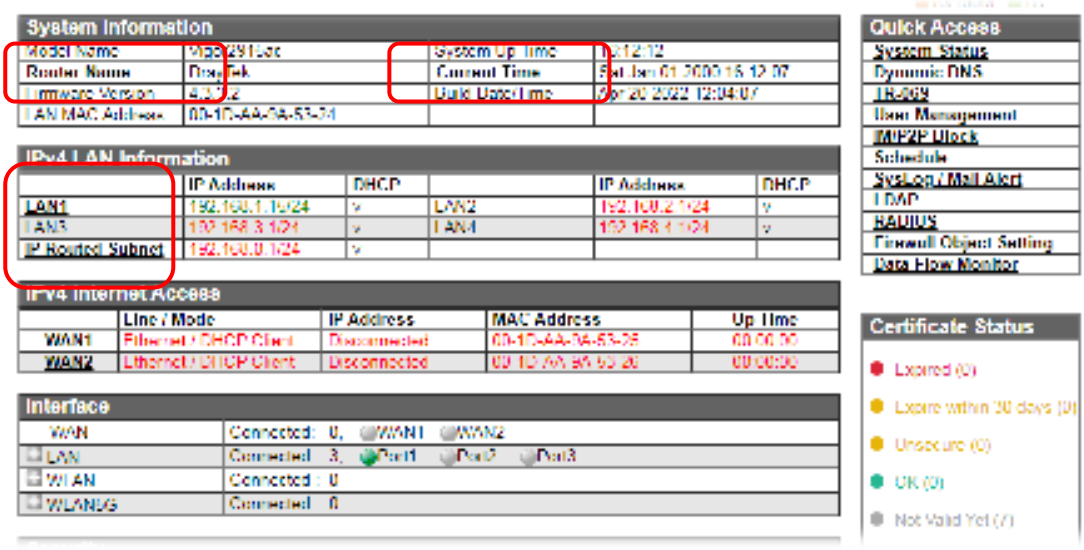
On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on WAN or LAN, related web setting page will be open for you to configure if required.

Port	Color	Description
Ethernet Port (WAN/ LAN)	Black	It means such port is disconnected.
	Green	It means such port is connected (with Giga transmission rate, 1Gbps) physically.
	Orange	It means such port is connected (with 10/ 100 Mbps) physically.

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

I-5-2 Name with a Link

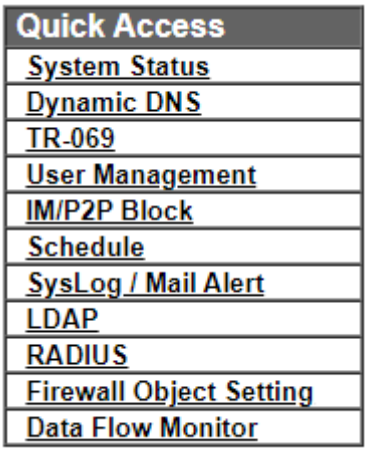
A name with a link (e.g., Router Name, Current Time, WAN1~3 and etc.) below means you can click it to open the configuration page for modification.



I-5-3 Quick Access for Common Used Menu

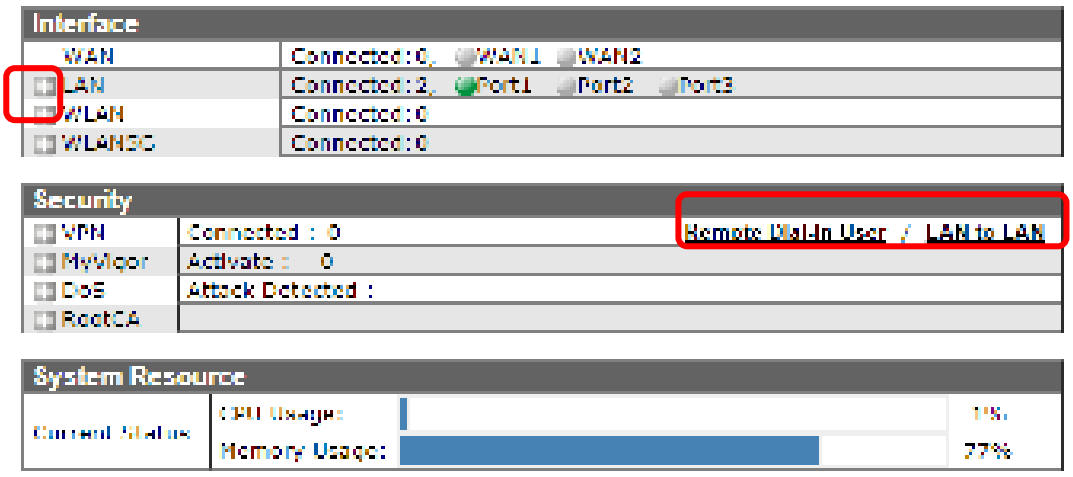
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

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

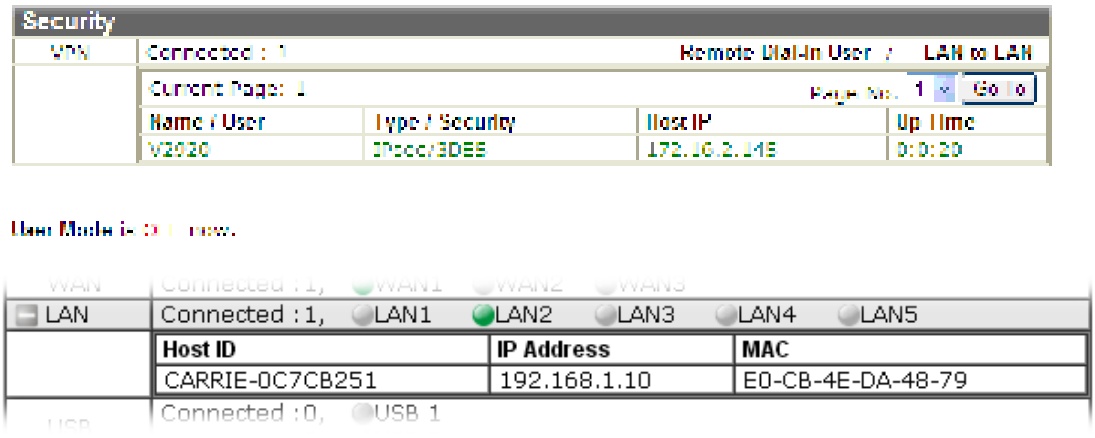


The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, LDAP, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be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

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



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

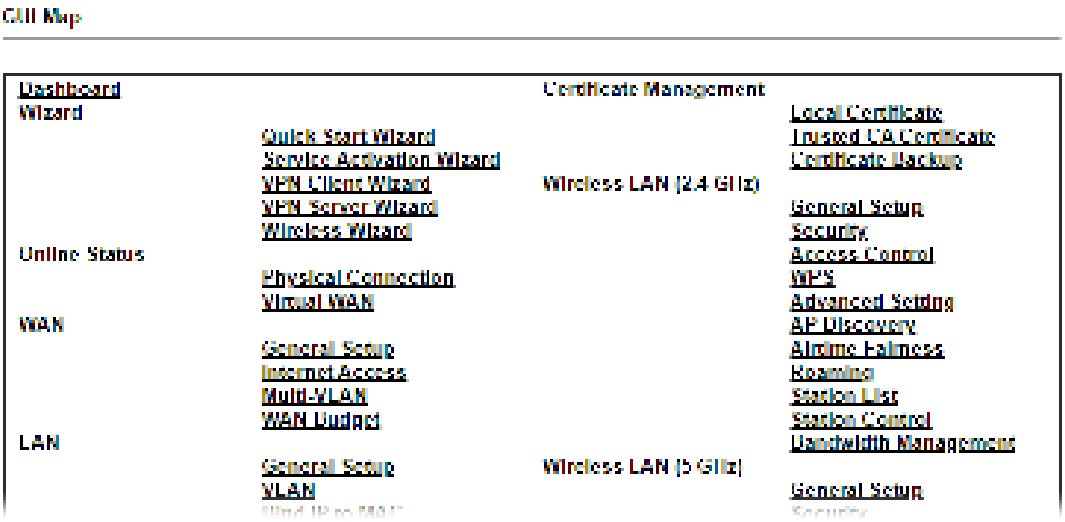


Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

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

I-5-4 GUI Map

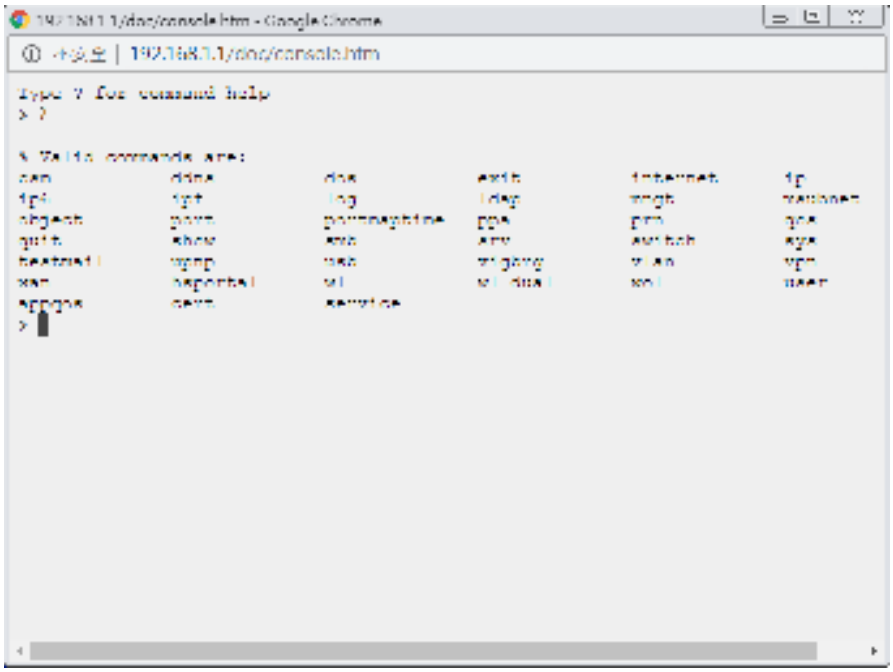
All the functions the router supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.



I-5-5 Web Console

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

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

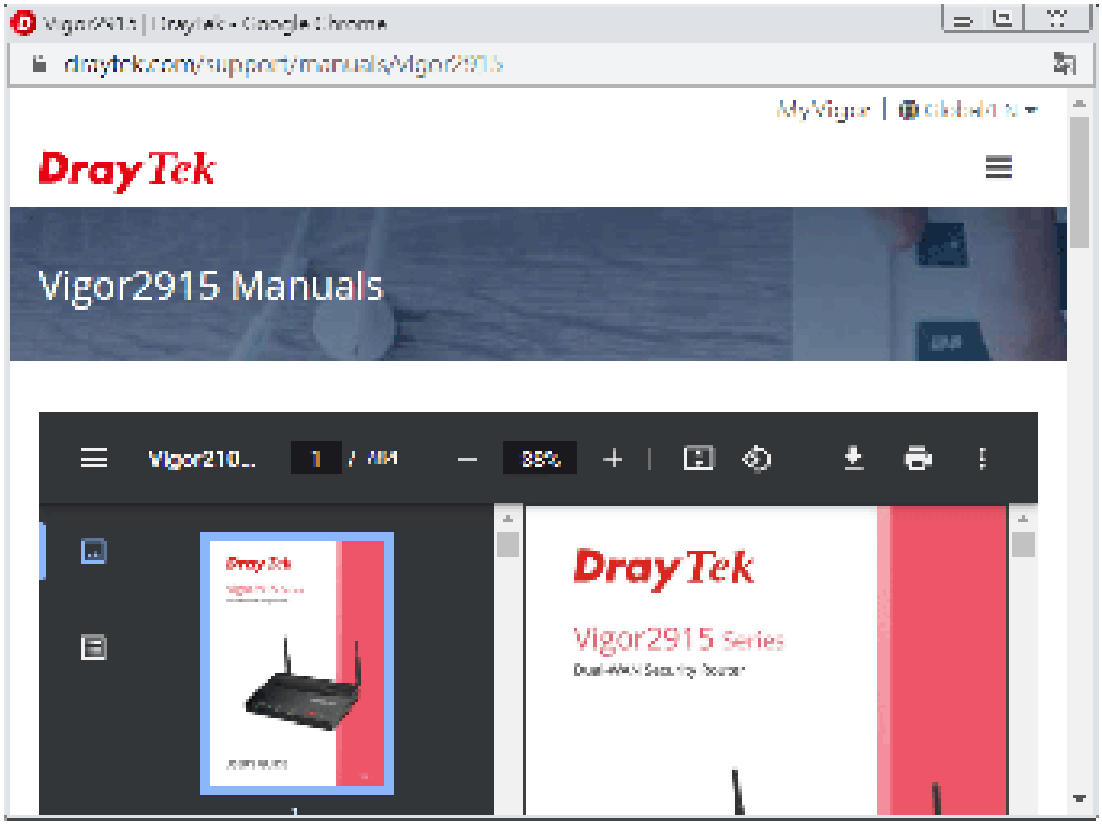


I-5-6 Config Backup

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

I-5-7 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-5-8 Logout

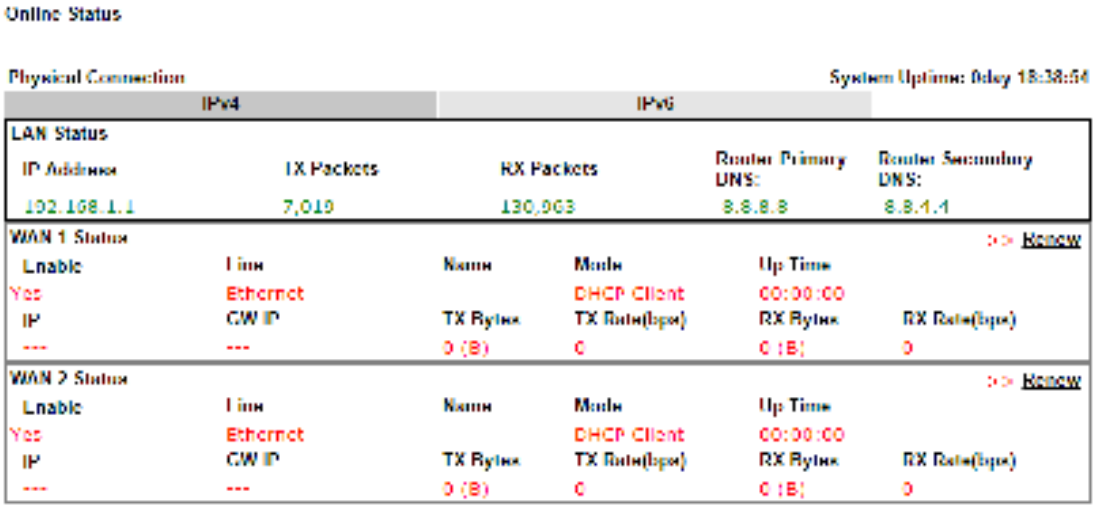
Click this icon to exit the web user interface.

I-5-9 Online Status

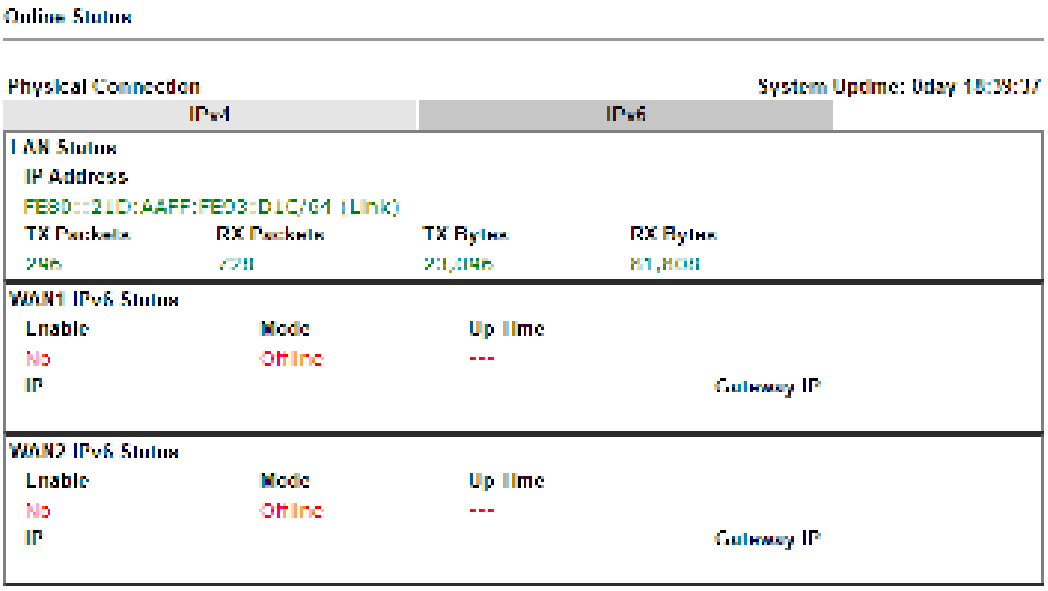
I-5-9-1 Physical Connection

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



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/WAN2 Status	**Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled.

Item	Description
	Line – Displays the physical connection (Ethernet, or USB) of this interface. **Name** – Display the name of the router. **Mode** - Displays the type of WAN connection (e.g., PPPoE). **Up Time** - Displays the total uptime of the interface. **IP** - Displays the IP address of the WAN interface. **GW IP** - Displays the IP address of the default gateway. **TX Packets** - Displays the total transmitted packets at the WAN interface. **TX Rate** - Displays the speed of transmitted octets at the WAN interface. **RX Packets** - Displays the total number of received packets at the WAN interface. **RX Rate** - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

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

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

I-5-9-2 Virtual WAN

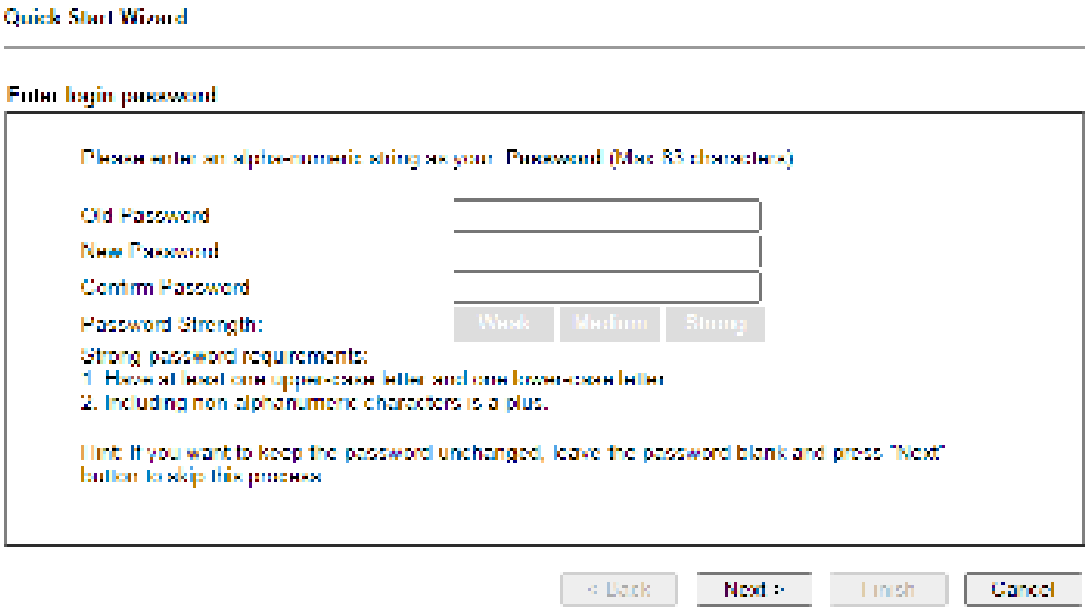
Such page displays the virtual WAN connection information.

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

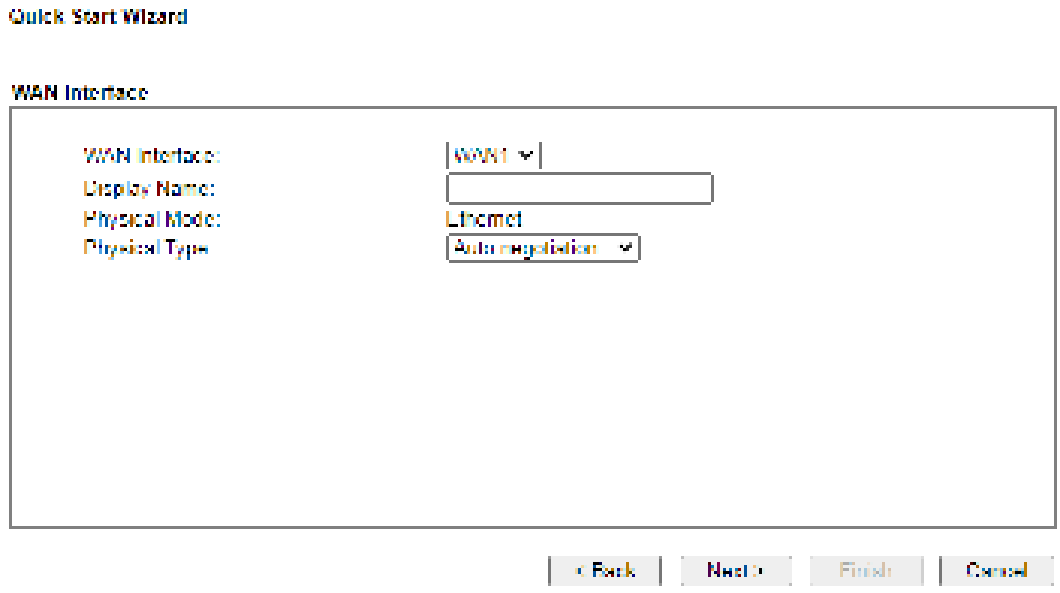
The field of Application will list the purpose of such WAN connection.

I-6 Quick Start Wizard

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



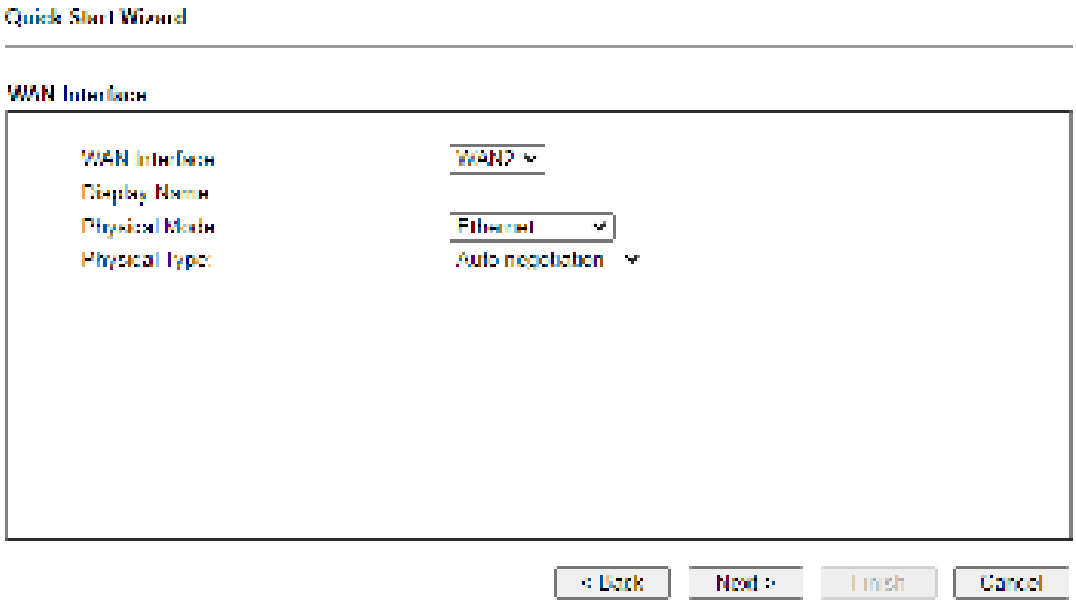
On the next page as shown below, please select the WAN interface that you use. If fiber is used, please choose WAN1; if Ethernet is used, please choose WAN1/WAN2. Then click **Next** for next step.



WAN1 and WAN2 will bring up different configuration page. Refer to the following for detailed information.

I-6-1 For WAN1/WAN2

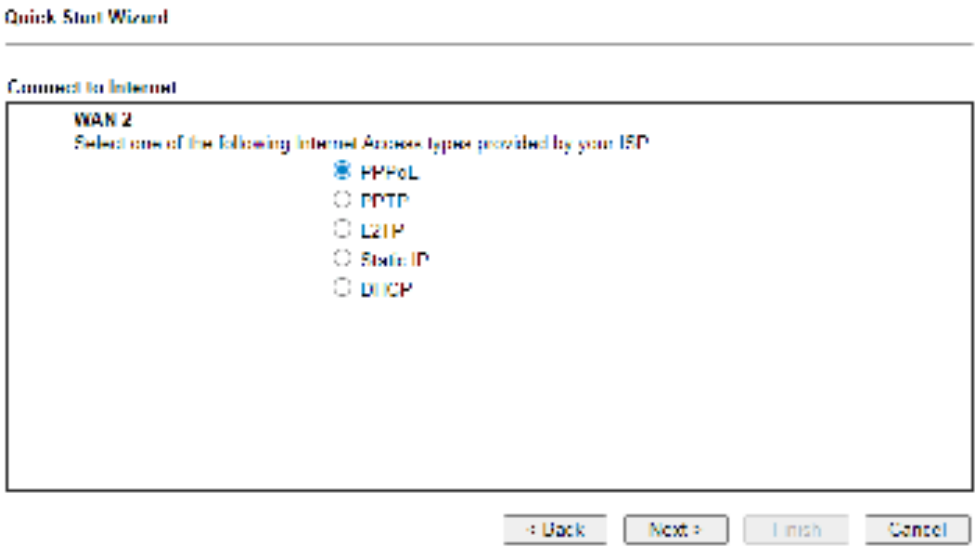
If you choose WAN2, you can specify physical type to fit your request. Then, click **Next**.



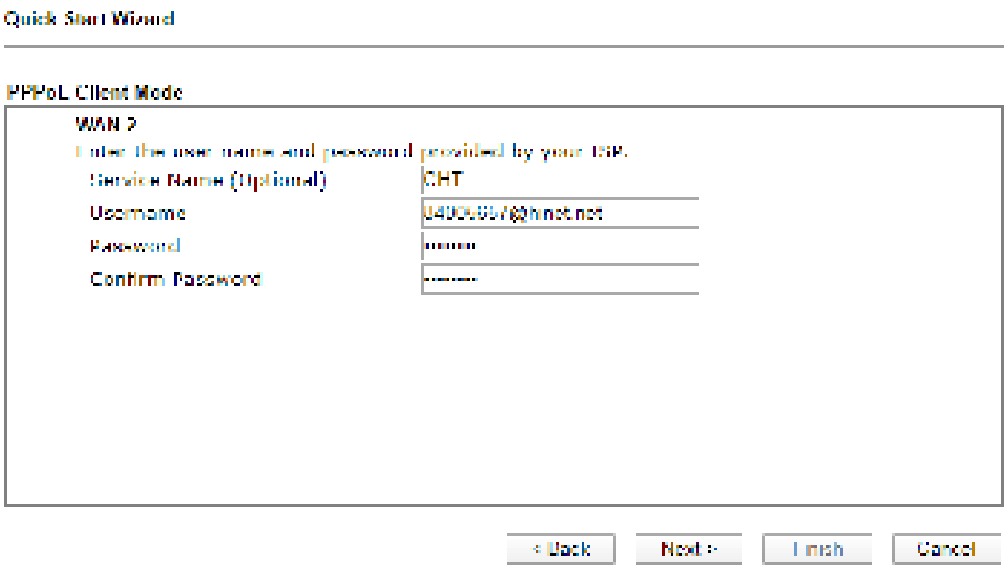
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

PPPoE

1. Choose **WAN1**/**WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **PPPoE** as the Internet Access Type. Then click **Next** to continue.

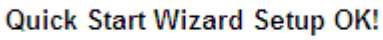


Available settings are explained as follows:

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

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

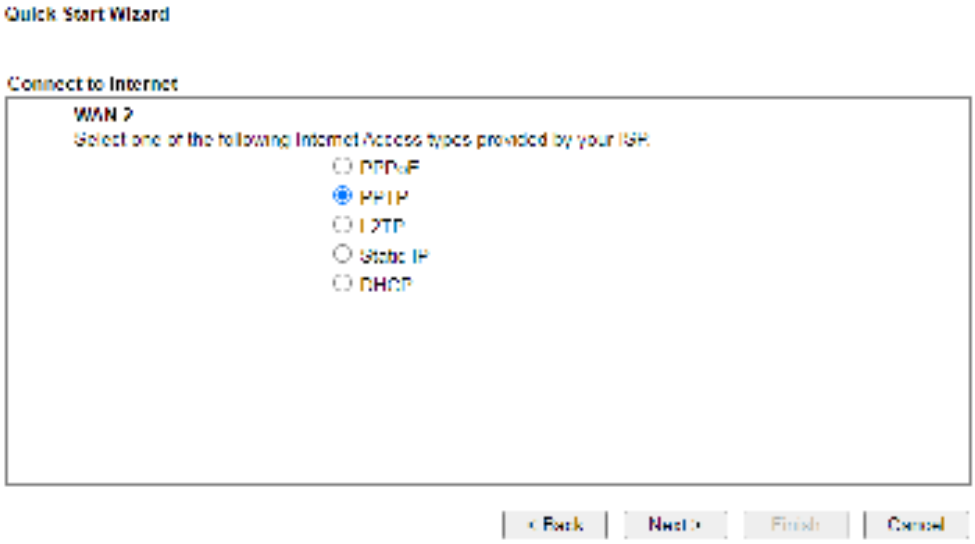
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



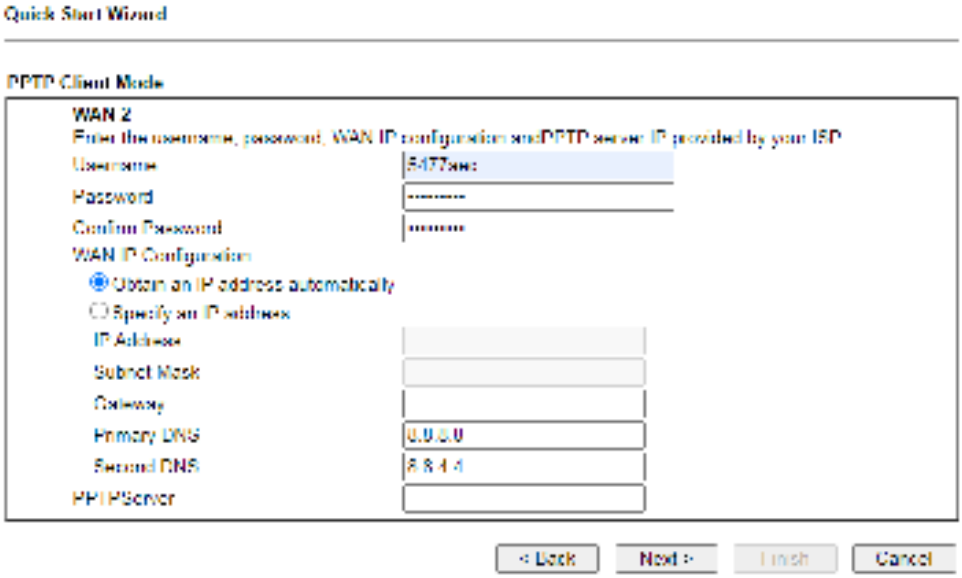
5. Now, you can enjoy surfing on the Internet.

PPTP/L2TP

1. Choose **WAN1**/**WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.



2. Click **PPTP**/**L2TP** as the Internet Access Type. Then click **Next** to continue.

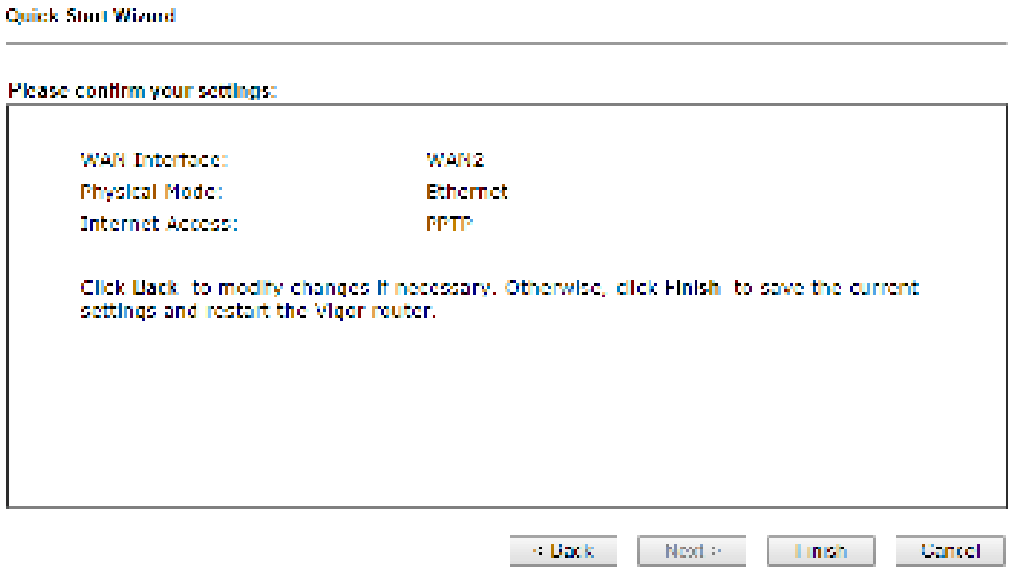


Available settings are explained as follows:

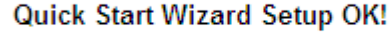
Item	Description
Username	Assign a specific valid user name provided by the ISP. **Note:** The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. **Note:** The maximum length of the password you can set is 62 characters.
Confirm Password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

	manually. **IP Address** - Enter the IP address. **Subnet Mask** –Enter the subnet mask. **Gateway** – Enter the IP address of the gateway. **Primary DNS** / **Second DNS** – Enter the IP address of the DNS server.
PPTP Server / **L2TP Server**	Enter the IP address of the server.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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



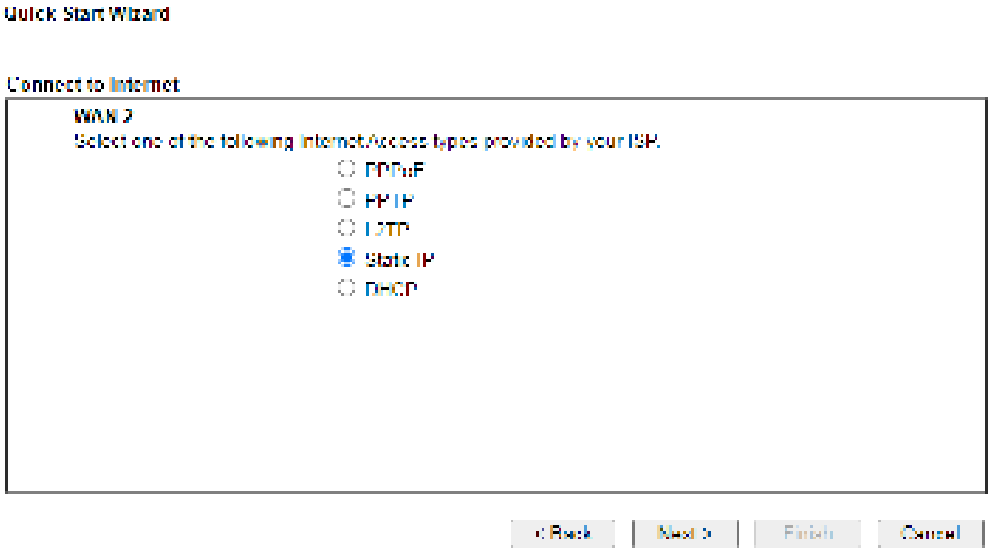
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



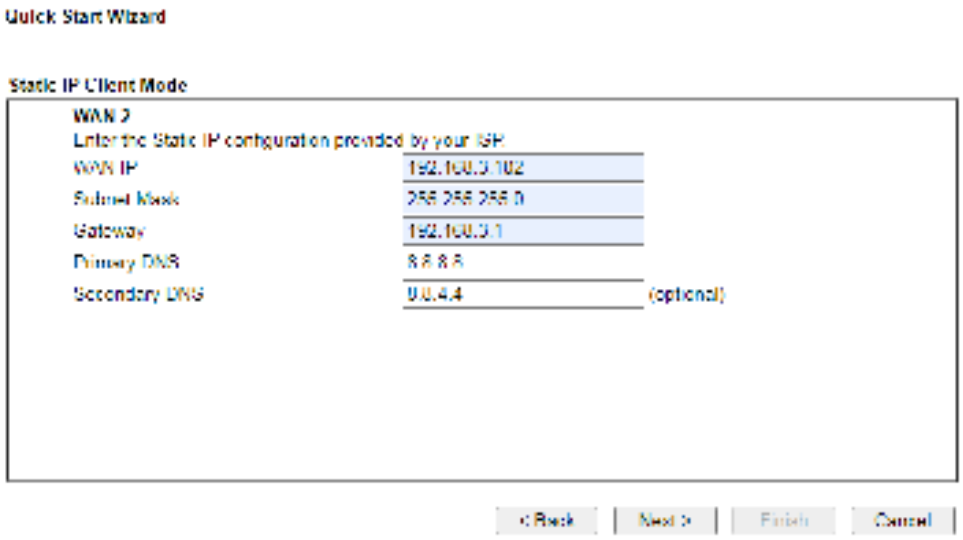
5. Now, you can enjoy surfing on the Internet.

Static IP

1. Choose **WAN1**/**WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.



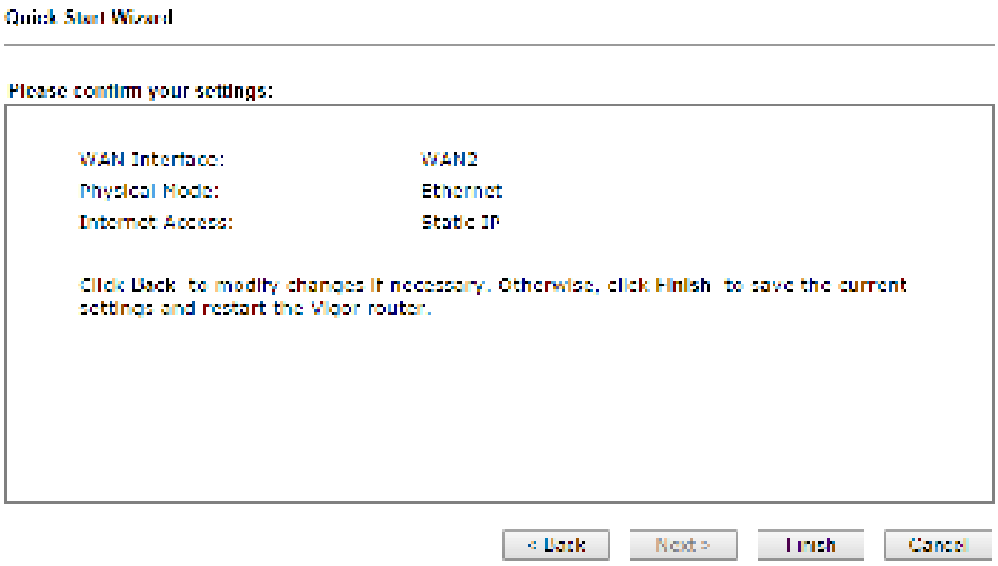
2. Click **Static IP** as the Internet Access type. Simply click **Next** to continue.



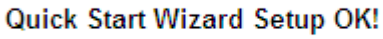
Available settings are explained as follows:

Item	Description
WAN IP	Enter the IP address.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in 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 type in the IP address information originally provided by your ISP. Then click **Next** for next step.



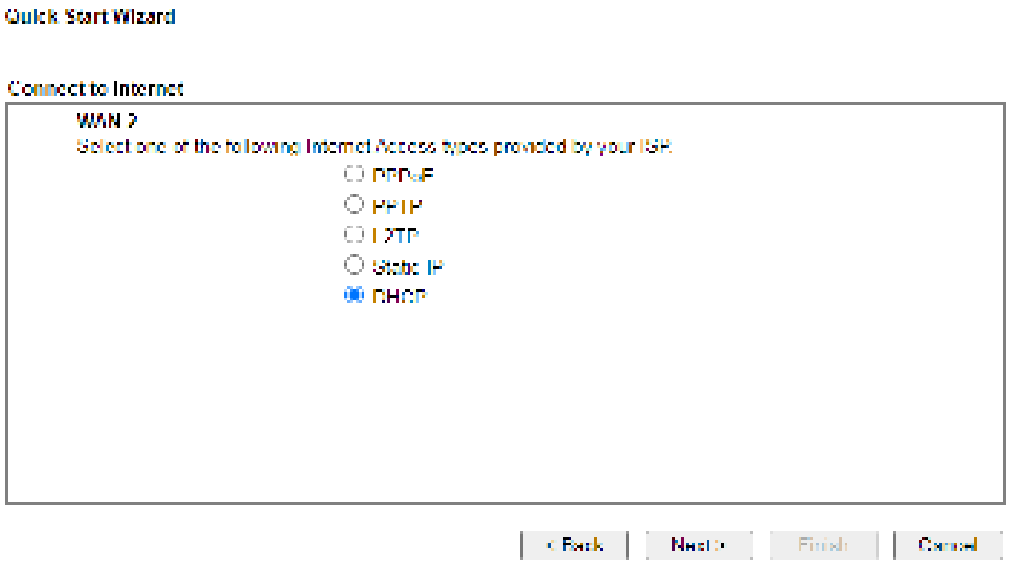
4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



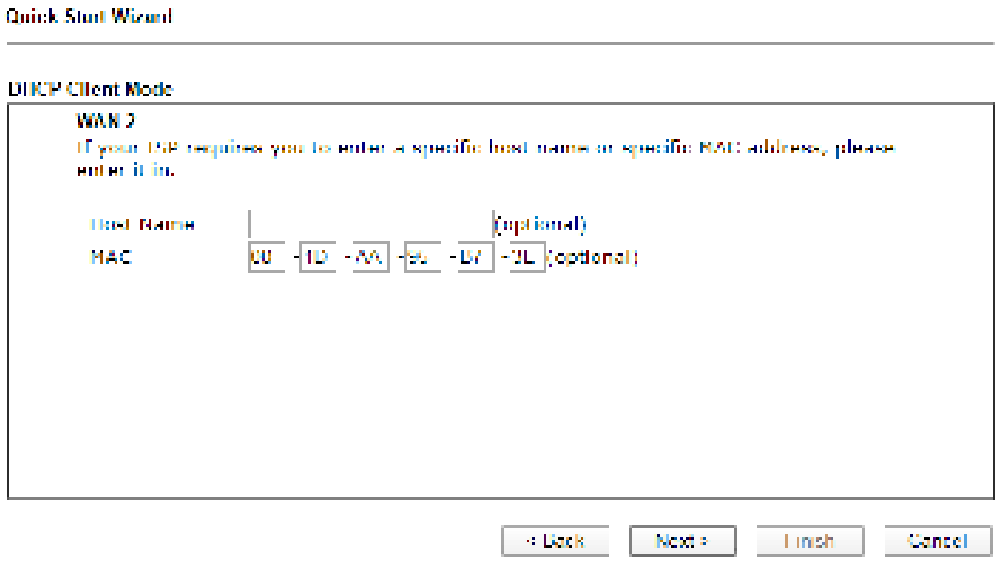
5. Now, you can enjoy surfing on the Internet.

DHCP

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



2. Click **DHCP** as the Internet Access type. Simply click **Next** to continue.

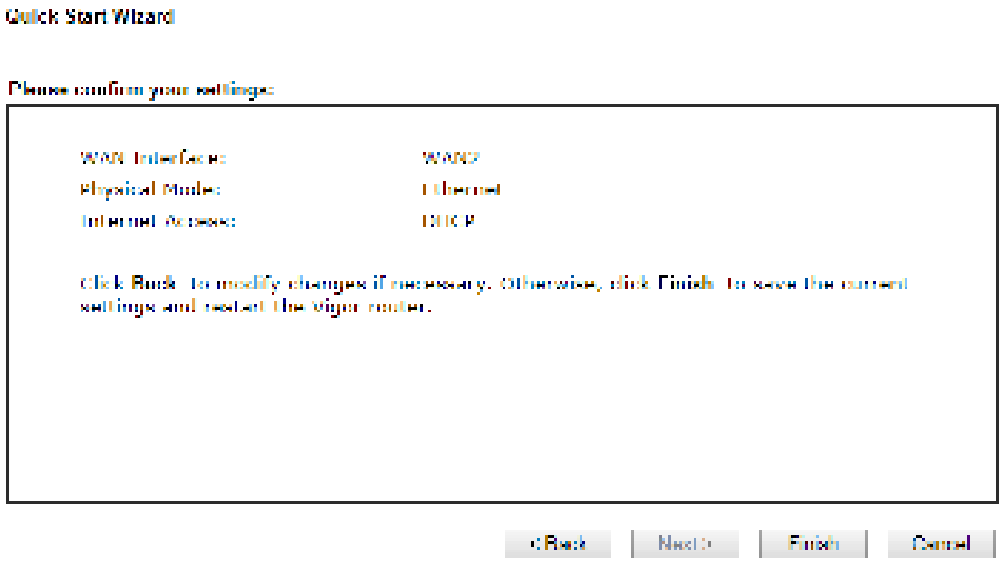


Available settings are explained as follows:

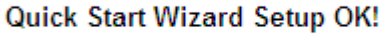
Item	Description
Host Name	Enter the name of the host. **Note:** The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous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

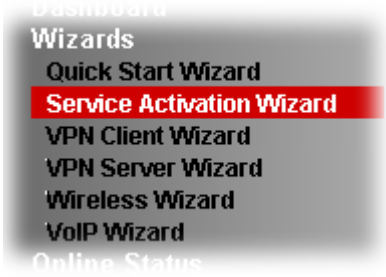
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.**

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.

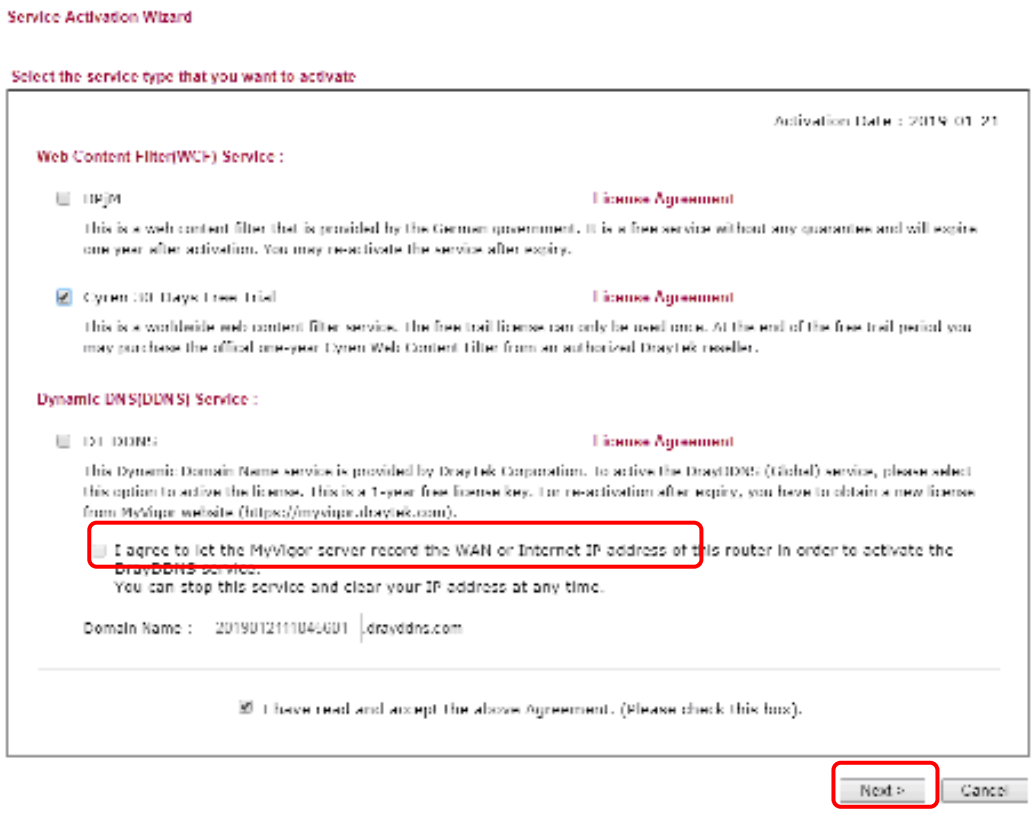
Now, follow the steps listed below to activate WCF feature for your router.

Info	Such function is available only for Admin Mode.

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



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



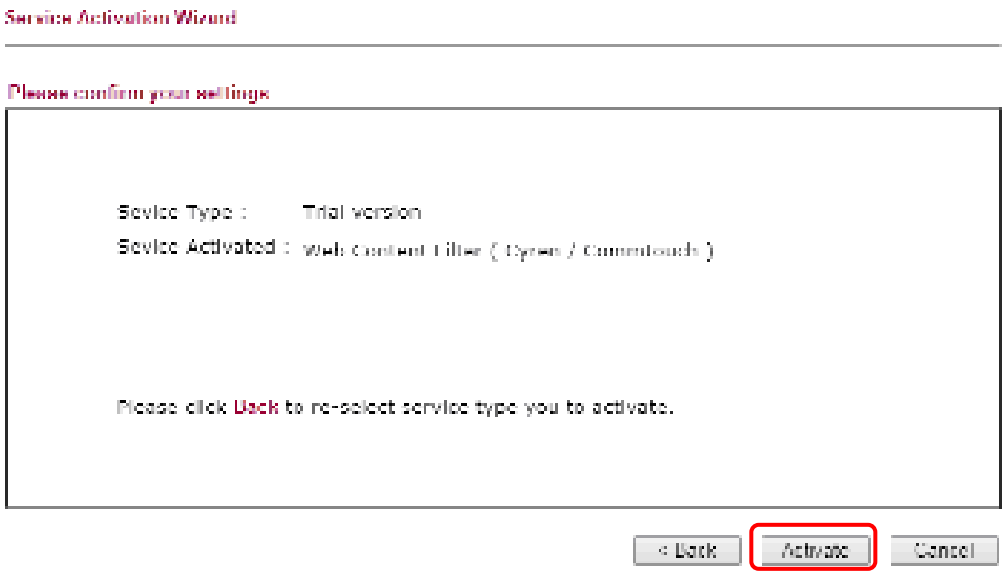
Info

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

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

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

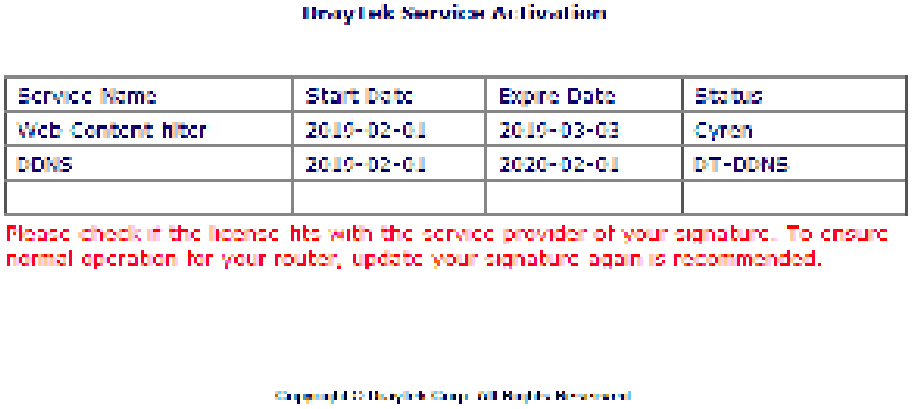
3. Setting confirmation page will be displayed as follows, please click **Activate**.



Info

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

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



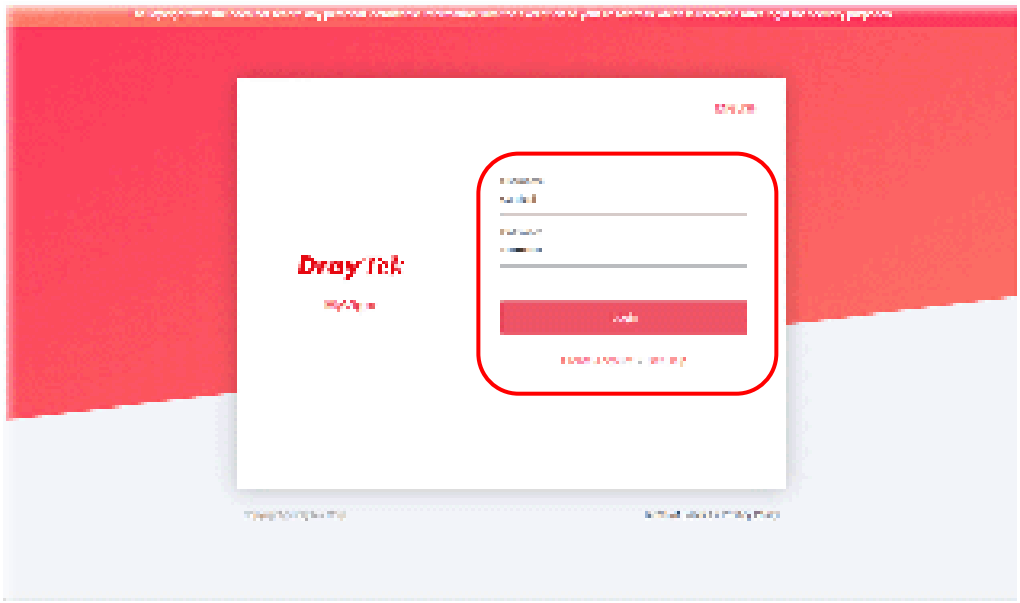
I-8 Registering Vigor Router

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

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

2 Click **MyVigor Services>>Production Registration** from the home page.

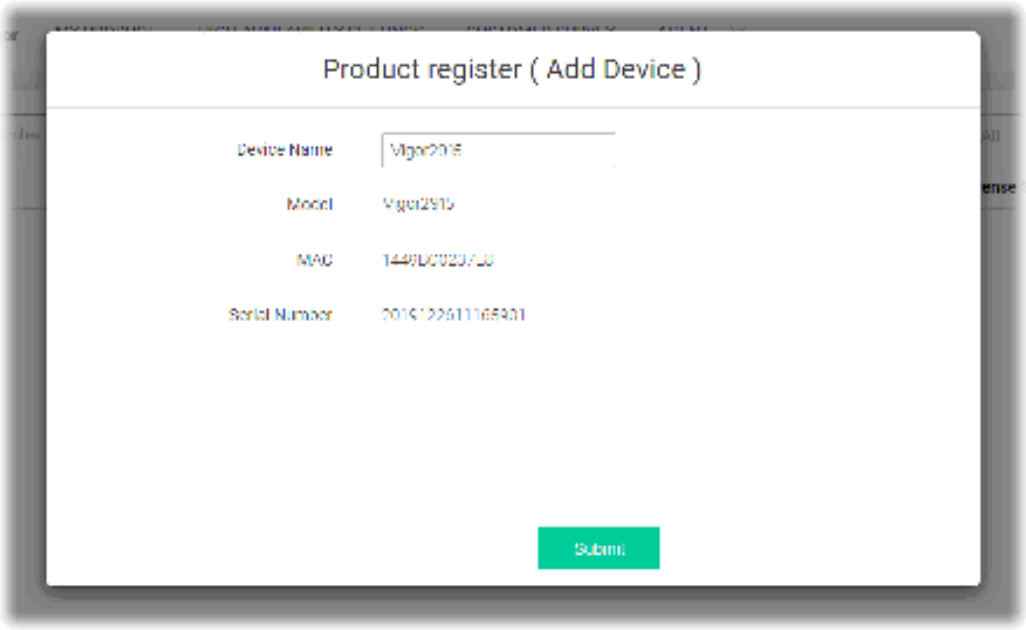
3 A **Login** page will be shown on the screen. Please Enter the account and password that you created previously. And click **Login**.



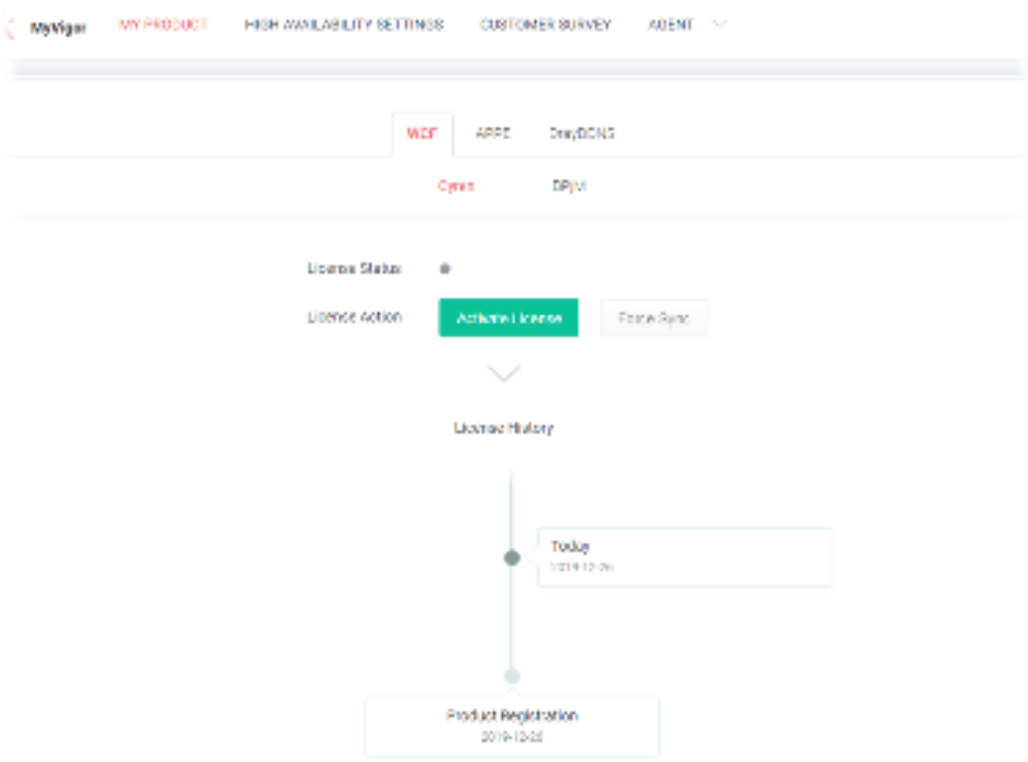
Info If you haven't an accessing account, please refer to section Creating an

Account for MyVigor to create your own one. Please read the articles on the Agreement regarding user rights carefully while creating a user account.

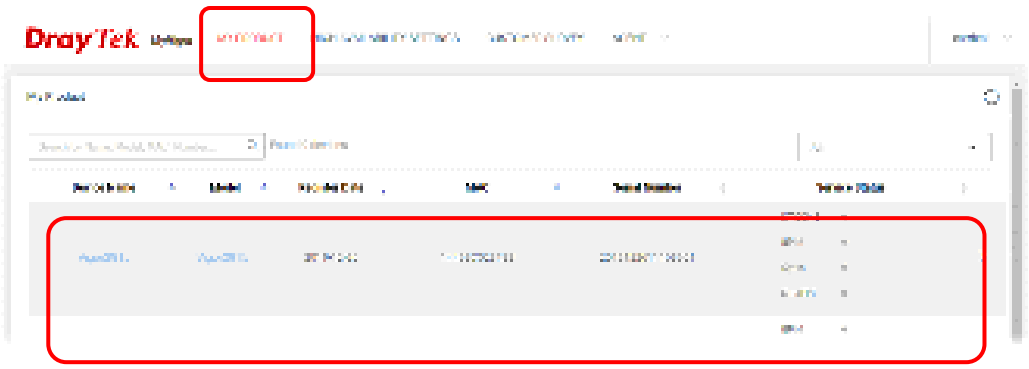
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Submit**.



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



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



Part II Connectivity

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

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

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

DDNS, LAN DNS, DNS Forwarding, DNS Security, Schedule, IGMP, LDAP, UPnP, WOL, RADIUS, SMS, Bonjour

Static Route, Load-Balance/Route Policy

II-1 WAN

It allows users to access Internet.

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2915 adds the function of 3G/4G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2915, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2915ac with 3G/4G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2915ac, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2915ac series.

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

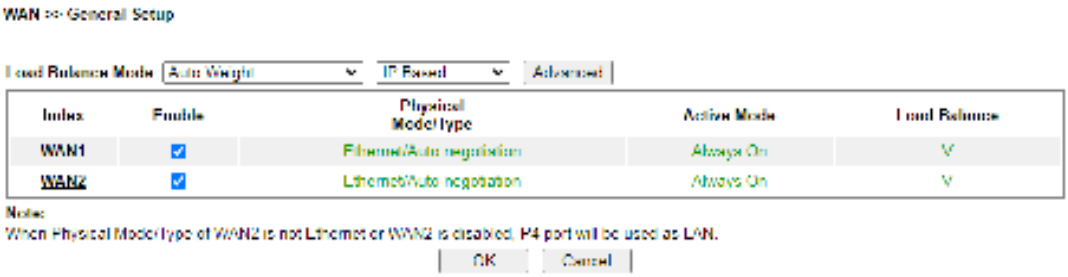
Web User Interface

II-1-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 in details.

This router supports dual-WAN function. It allows users to access Internet and combine the bandwidth of the 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.

This webpage allows you to set general setup for WAN interface.



Available settings are explained as follows:

Item	Description
Load Balance Mode	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 Weight** to let the router reach the best load balance.
IP Based / Sesseion Based	**IP Based** -The same source / destination IP pair will select the same WAN interface as policy. It is the default setting. If you have no strong demand about speed test result, keep default settings as IP based. **Sesseion 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.
Advanced	Click it to open the following dialog for configuring settings of protocol, port and comment.

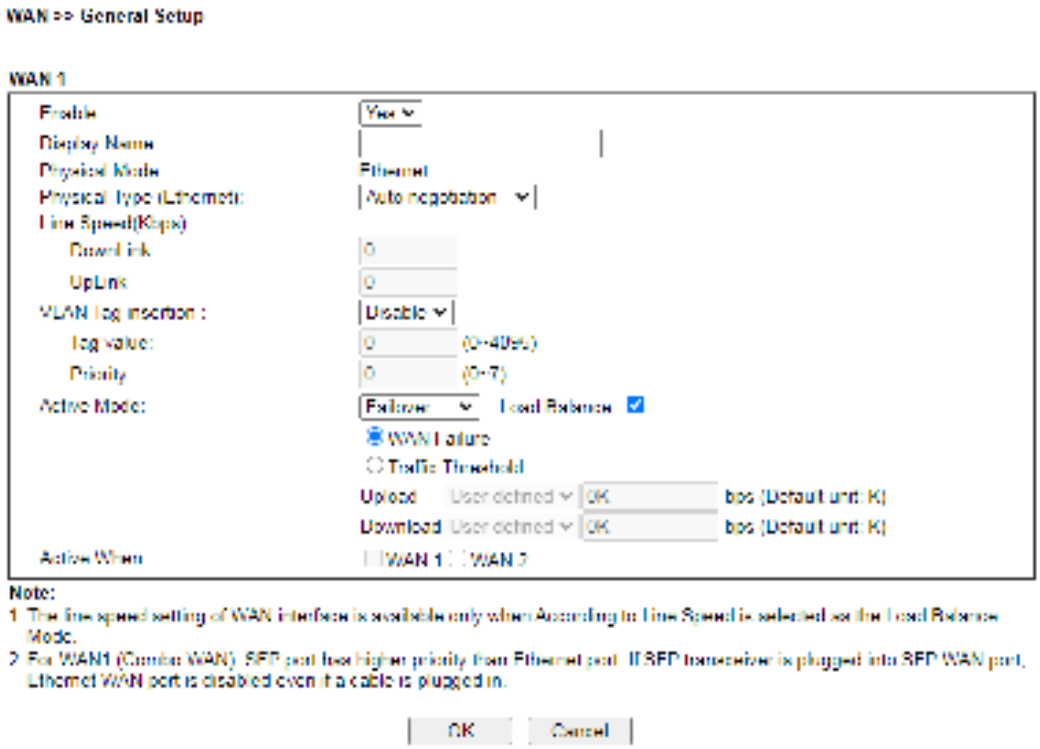
Index	Click the WAN interface link under Index to access into the WAN configuration page.
Enable	**V** means such WAN interface is enabled and ready to be used.
Physical Mode / Type	Display the physical mode (Fiber, Ethernet, Wireless 2.4G, Wireless 5G or USB) and physical type of the WAN interface.
Line Speed(Kbps) DownLink/UpLink	Display the downstream and upstream rate of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Load Balance	**V** means the function of load balance for such WAN interface is enabled.

Info	In default, each WAN port is enabled.

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

II-1-1-1 WAN1 (Fiber)

When fiber is used for network connection, click WAN1 to get the following page.



Available settings are explained as follows:

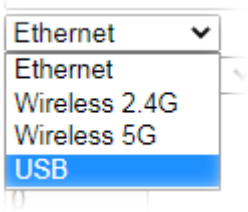
Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical Type	You can change the physical type or choose **Auto negotiation** for determined by the system.
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please enter the line speed for downloading and uploading for such WAN interface. The unit is kbps.
VLAN Tag insertion	**Enable** – Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by WAN1. **Disable** – Disable the function of VLAN with tag. **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.
Active Mode	Choose **Always On** to make the WAN connection be activated always. **Load Balance**: Check this box to enable **auto** load balance function for such WAN interface.

	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status. **Failover** – Choose it to make the WAN connection as a backup connection. ● **WAN Failure** – When the active WAN failed, such WAN will be activated as the main network connection. ● **Traffic Threshold** – When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	If you choose **Failover** as the **Active Mode**, **Active When** will appear. Please specify which WAN will be the Backup interface.

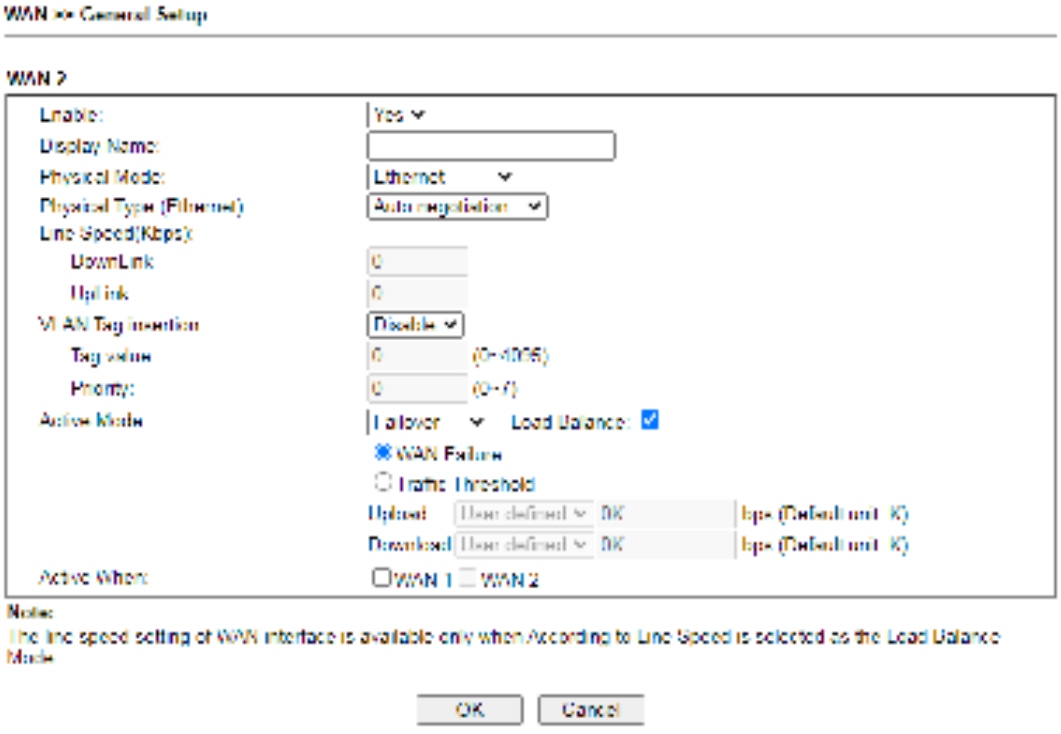
After finished the above settings, click **OK** to save the settings.

II-1-1-2 WAN1/WAN2 (Ethernet)

The WAN2 interface can be specified as Ethernet, Wireless 2.4G, Wireless 5G, or USB.



When Ethernet is used for network connection, click WAN1. Or click WAN2 and select Ethernet as the Physical Mode to get the following page.



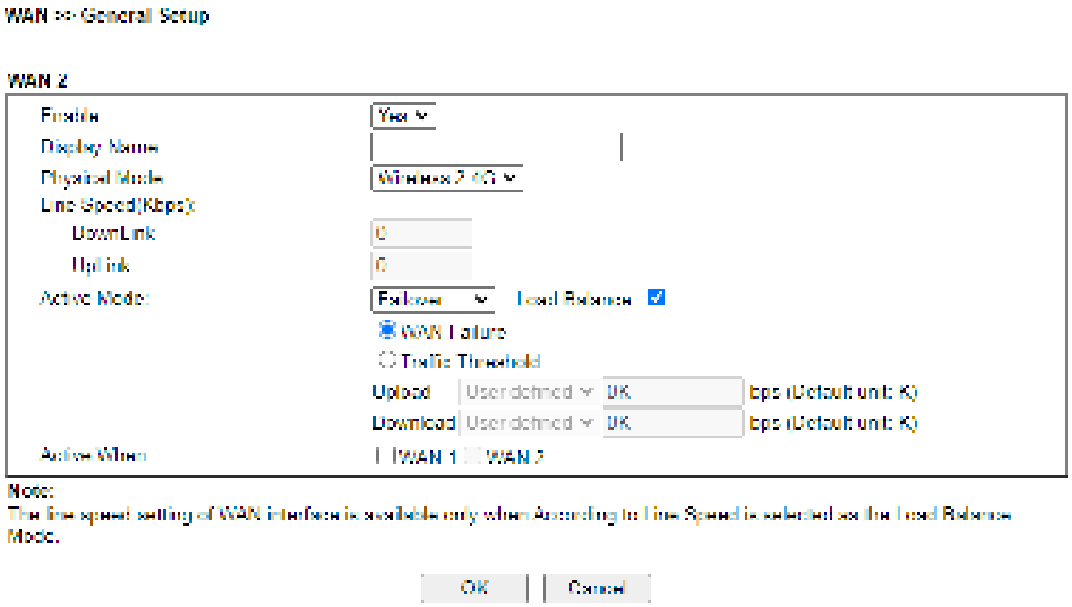
Available settings are explained as follows:

Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Choose Ethernet for such WAN interface.
Physical Type	You can change the physical type or choose **Auto negotiation** for determined by the system.
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please Enter the line speed for downloading and uploading for such WAN interface. The unit is kbps.
VLAN Tag insertion	**Enable** – Enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the WAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by WAN1. **Disable** – Disable the function of VLAN with tag. **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.
Active Mode	Choose **Always On** to make the WAN connection be activated always. **Load Balance**: Check this box to enable **auto** load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status. **Failover** – Choose it to make the WAN connection as a backup connection. ● **WAN Failure** – When the active WAN failed, such WAN will be activated as the main network connection. ● **Traffic Threshold** – When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	If you choose **Failover** as the **Active Mode**, **Active When** will appear. Please specify which WAN will be the Backup interface.

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

II-1-1-3 WAN2 (Wireless LAN 2.4G / 5G)

To use WLAN WAN connection, please configure WAN2 interface and choose Wirelss 2.4G or Wireless 5G as the Physical Mode.



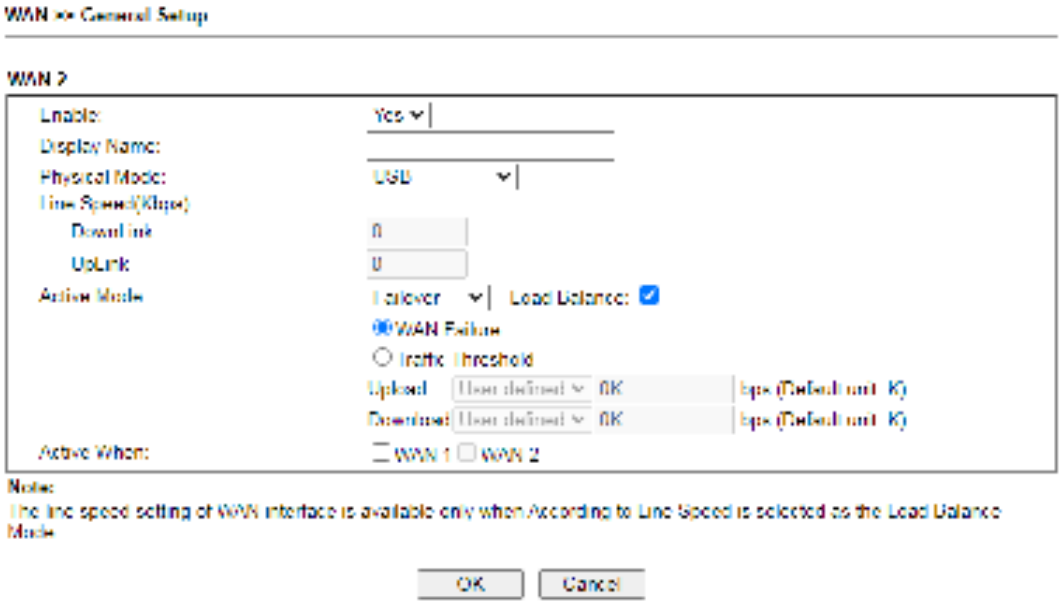
Available settings are explained as follows:

Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Choose Ethernet for such WAN interface.
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please Enter the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	Choose **Always On** to make the WAN connection be activated always. **Load Balance**: Check this box to enable **auto** load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status. **Failover** –Choose it to make the WAN connection as a backup connection. ● **WAN Failure** –When the active WAN failed, such WAN will be activated as the main network connection. ● **Traffic Threshold** –When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	If you choose **Failover** as the **Active Mode**, **Active When** will appear. Please specify which WAN will be the Backup interface.

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

II-1-1-4 WAN2 (USB)

To use 3G/ 4G network connection through 3G/ 4G USB Modem, please configure WAN2 interface and choose USB as the Physical Mode.



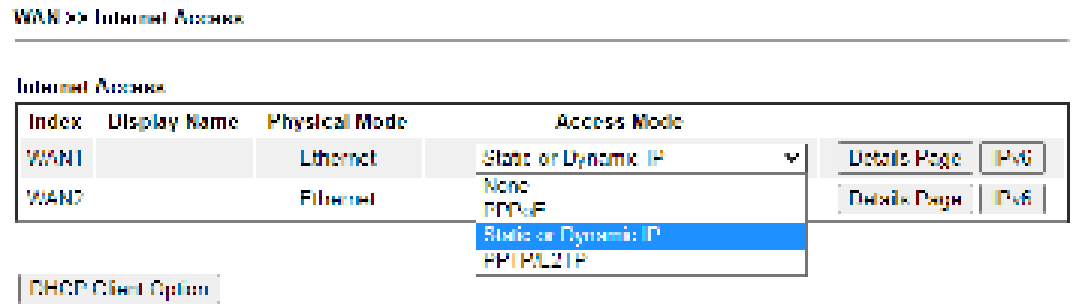
Available settings are explained as follows:

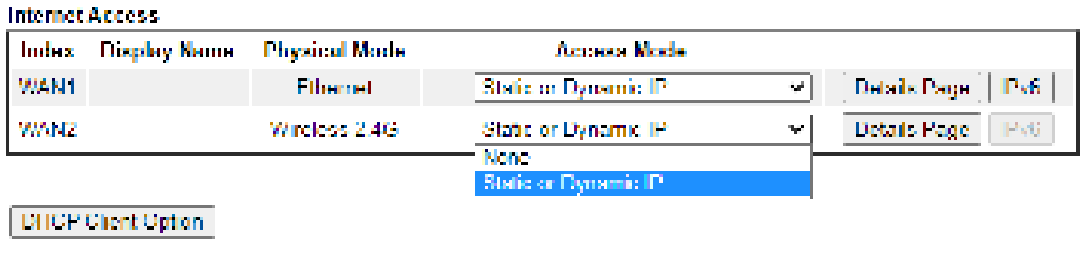
Item	Description
Enable	Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.
Display Name	Enter the description for such WAN interface.
Physical Mode	Choose USB.
Line Speed	If your choose **According to Line Speed** as the **Load Balance Mode**, please Enter the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	Choose **Always On** to make the WAN connection be activated always. **Load Balance**: Check this box to enable **auto** load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status. **Failover** –Choose it to make the WAN connection as a backup connection. ● **WAN Failure** –When the active WAN failed, such WAN will be activated as the main network connection. ● **Traffic Threshold** –When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic.
Active When	If you choose **Failover** as the **Active Mode**, **Active When** will appear. Please specify which WAN will be the Backup interface.

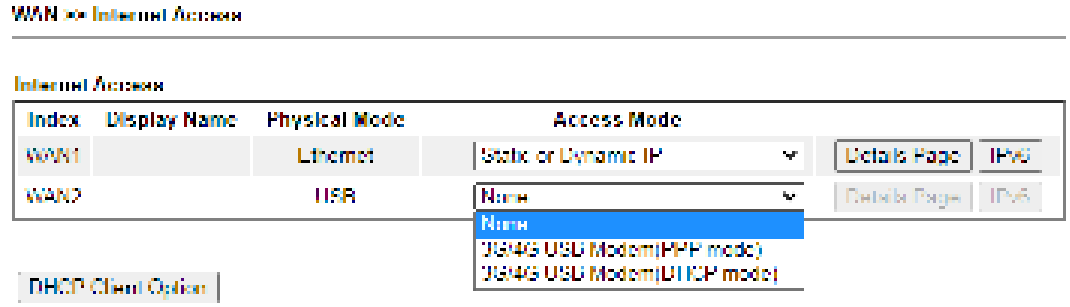
After finished the above settings, click **OK** to save the settings.

II-1-2 Internet Access

For the router supports dual-WAN function, the users can set different WAN settings (for WAN1/ WAN2) for Internet Access. Due to different Physical Mode for WAN interface, the Access Mode for these connections also varies. Refer to the following figures for examples.







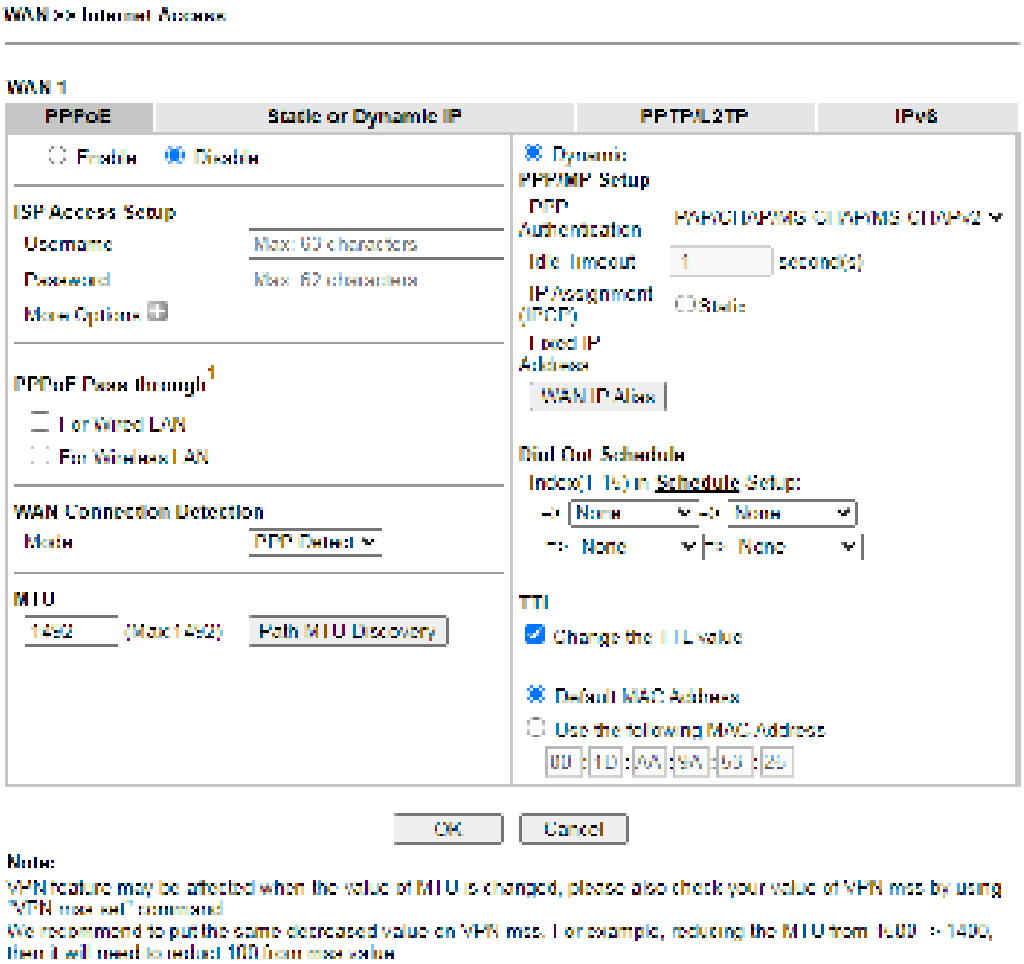
Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN interface that entered in general setup.
Physical Mode	It shows the physical connection for WAN interface according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click **Details Page** for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface.
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN

	interface. If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.
DHCP Client Option	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured. **Enable/Disable** – Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets. **Interface** – Specify the WAN interface(s) that will be overwritten by such function. **Option Number** – Type a number for such function. **Note:** If you choose to configure option 61 here, the detailed settings in **WAN>>Interface Access** will be overwritten. **DataType** – Choose the type (ASCII or Hex) for the data to be stored. **Data** – Enter the content of the data to be processed by the function of DHCP option.

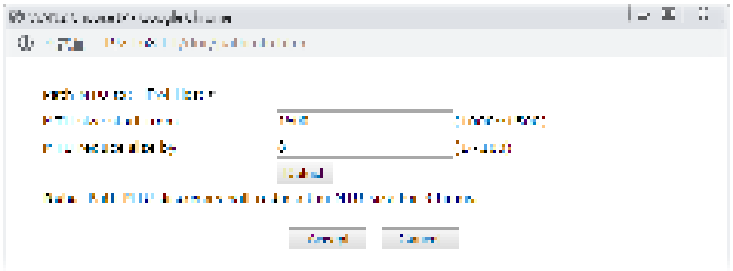
II-1-2-1 Details Page for PPPoE in WAN1/WAN2 (Physical Mode: Ethernet)

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



Available settings are explained as follows:

Item	Description
Enable/Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **Username** –Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. **Password** –Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. **More Options** – It shows optional settings for configuration. ● **Service Name (Optional)** - Enter the description of the specific network service.
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you

	also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. **For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. **For Wireless LAN** – It is available for *n* model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet. **Note:** To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through PPP Detect or Ping Detect. **Mode** – Choose **PPP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● **TTL (Time to Live)** – Set TTL value of PING operation. ● **Ping Interval** – Enter the interval for the system to execute the PING operation. ● **Ping Retry** – Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.  ● **Path MTU to** – Enter the IP address as the specific transmit path. ● **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500,

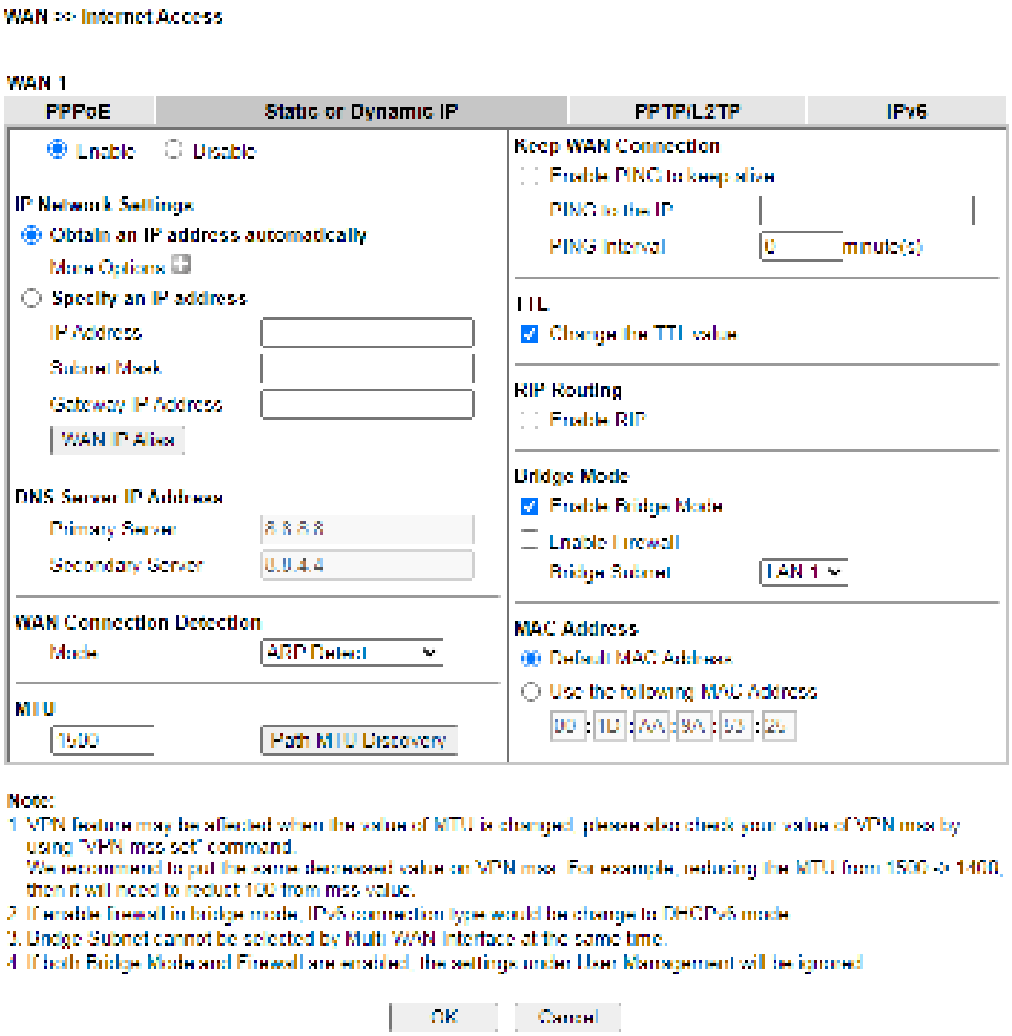
	1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
PPP/MP Setup	**PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. **IP Assignment (IPCP) -** Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. **Fixed IP Address** – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. Enter the additional WAN IP address and check the Enable box. Then click **OK** to exit the dialog.
Dial-Out Schedule	**Index (1-15) in Schedule Setup -** 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.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. ● **If enabled** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0". ● **If disabled** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP. **Default MAC Address** – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router. **Specify a MAC Address –** Enter the MAC address for the router manually.

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

II-1-2-2 Details Page for Static or Dynamic IP in WAN1/WAN2 (Physical Mode: Ethernet)

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

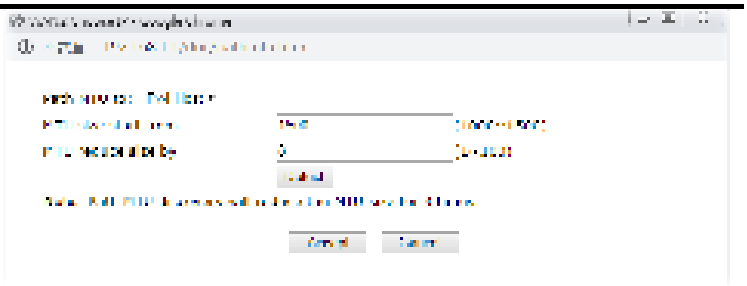
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Enable / Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. **Obtain an IP address automatically** – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode. **More Options** - It shows optional settings for configuration.

	• **Router Name**: Type in the router name provided by ISP. • **Domain Name**: Type in the domain name that you have assigned. • **Enable DHCP Client Identifier:** Check the box to specify username and password as the DHCP client identifier for some ISP. • **Username:** Type a name as username. The maximum length of the user name you can set is 63 characters. • **Password:** Type a password. The maximum length of the password you can set is 62 characters. **Specify an IP address** – Click this radio button to specify some data if you want to use **Static IP** mode. • **IP Address**: Enter the IP address. • **Subnet Mask**: Enter the subnet mask. • **Gateway IP Address**: Enter the gateway IP address. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using.
DNS Server IP Address	Type in the **primary IP** address for the router if you want to use **Static IP** mode. If necessary, type in **secondary IP** address for necessity in the future.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect, Ping Detect** or **Always On** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. • **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. • **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. • **TTL (Time to Live)** – Set TTL value of PING operation. • **Ping Interval** – Enter the interval for the system to execute the PING operation. • **Ping Retry** – Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.

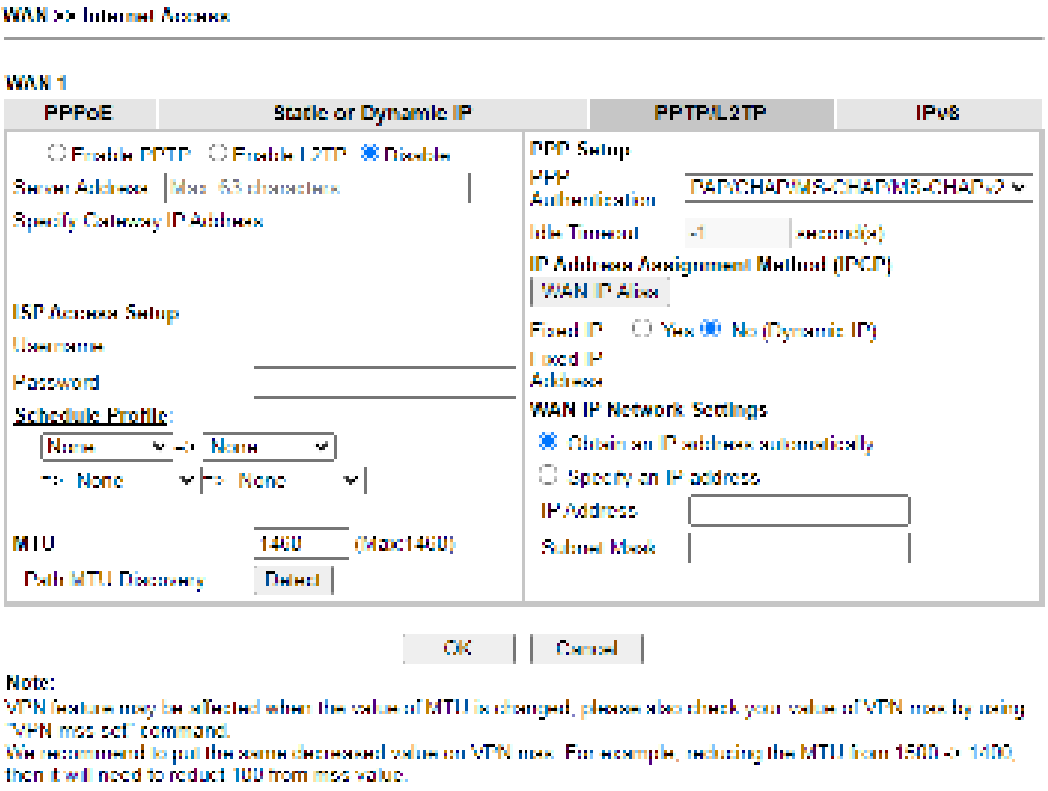
	 • **Path MTU to** – Enter the IP address as the specific transmit path. • **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. • **Detect** – Click it to detect a suitable MTU value • **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. • **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. • **PING Interval** - Enter the interval for the system to execute the PING operation.
TTL	**Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router. • **If enabled** - TTL value will be reduced (-1) when it passess through Vigor router. It will cause the client, accessing Internet through Vigor router, be blocked by certain ISP when TTL value becomes "0". • **If disabled** – TTL value will not be reduced. Then, when a packet passes through Vigor router, it will not be cancelled. That is, the client who sends out the packet will not be blocked by ISP.
RIP Routing	Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
Bridge Mode	**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem. **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. **Bridge Subnet** – Make a bridge between the selected LAN subnet and such WAN interface.
MAC Address	**Default MAC Address**: Click this radio button to use default MAC address for the router. **Specify a MAC Address**: Some Cable service providers specify a specific MAC address for access authentication. In

	such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

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

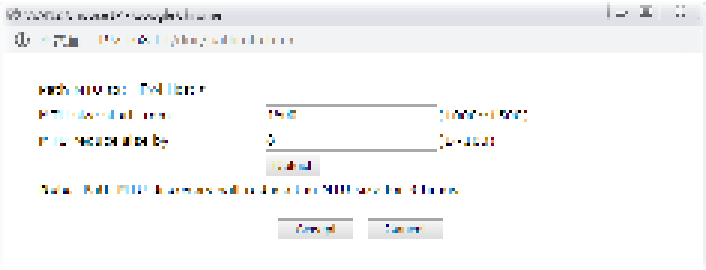
II-1-2-3 Details Page for PPTP/L2TP in WAN1/WAN2 (Physical Mode: Ethernet)

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



Available settings are explained as follows:

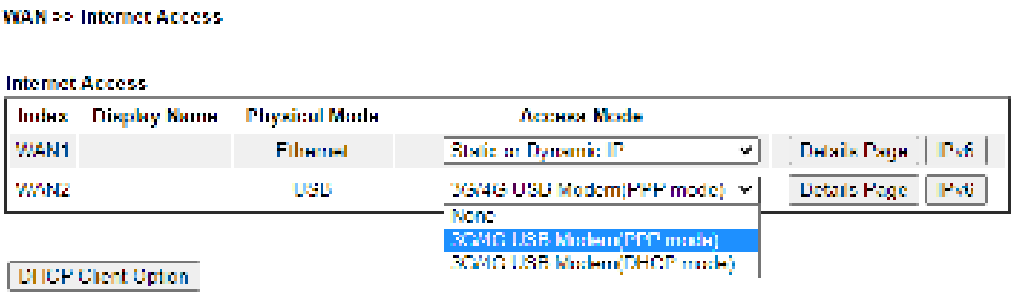
Item	Description
PPTP/L2TP	**Enable PPTP-** Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface. **Enable L2TP** - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface. **Disable** – Click this radio button to close the connection through PPTP or L2TP. **Server Address** - Specify the IP address of the PPTP/ L2TP server if you enable PPTP/ L2TP client mode. **Specify Gateway IP Address** – Specify the gateway IP address for DHCP server.
ISP Access Setup	**Username** -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters. **Password** -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters. **Schedule Profile -** 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.
Schedule Profile	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Detect** to open the following dialog.  ● **Path MTU to** – Enter the IP address as the specific transmit path. ● **MTU reduce size by**– It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
PPP Setup	**PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 32 public IP addresses other than the current one you are using. **Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box. **Fixed IP Address -**Type a fixed IP address.
WAN IP Network Settings	**Obtain an IP address automatically** – Click this button to obtain the IP address automatically. **Specify an IP address** – Click this radio button to specify some data. ● **IP Address** – Enter the IP address. ● **Subnet Mask** – Enter the subnet mask.

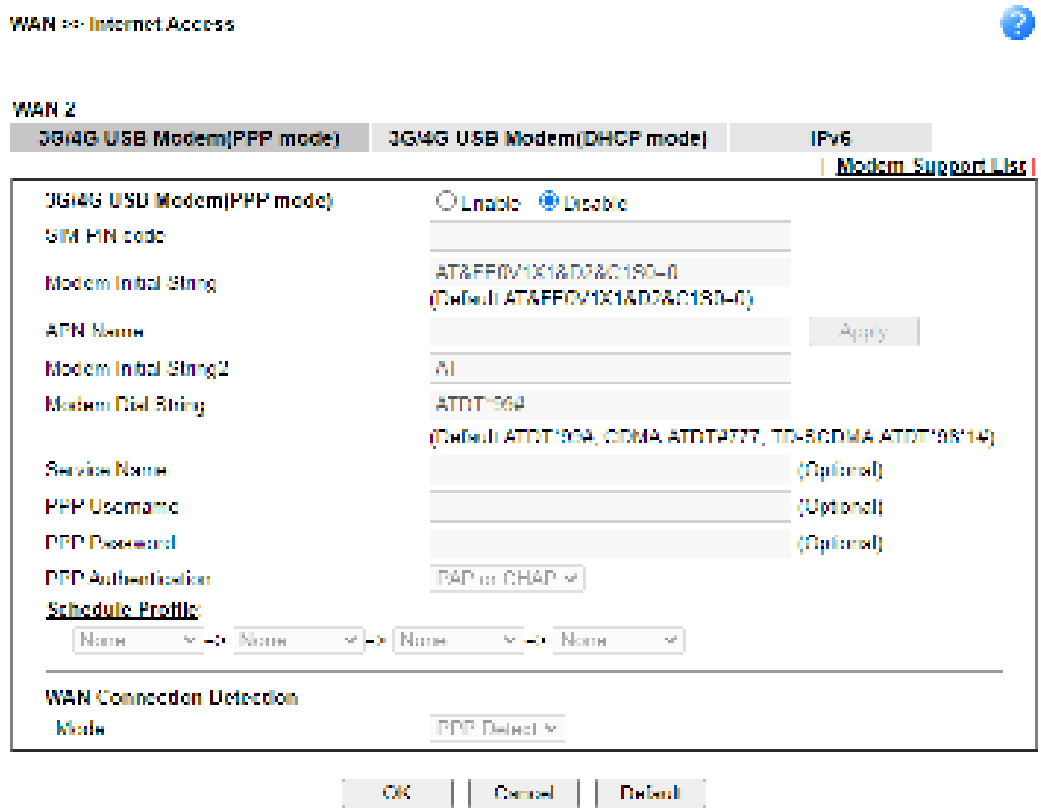
After finishing all the settings here, please click **OK** to activate them.

II-1-2-4 Details Page for 3G/4G USB Modem (PPP mode) in WAN2

To use **3G/4G USB Modem (PPP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu.



Then, select **3G/4G USB Modem (PPP mode)** for WAN2. The following web page will be shown.



Available settings are explained as follows:

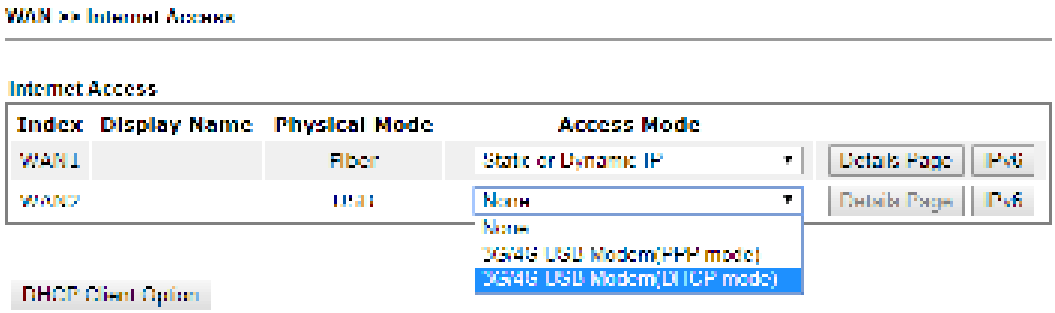
Item	Description
Modem Support List	It lists all of the modems supported by such router.
3G /4G USB Modem (PPP mode)	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.

Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Enter the name and click **Apply**. The maximum length of the name you can set is 43 characters.
Modem Initial String2	The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. The maximum length of the string you can set is 47 characters.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 31 characters.
Service Name	Enter the description of the specific network service.
PPP Username	Enter the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Enter the PPP password (optional). The maximum length of the password you can set is 62 characters.
PPP Authentication	Select **PAP only** or **PAP or CHAP** for PPP.
Schedule Profile	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
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through PPP Detect or Ping Detect. **Mode** – Choose **PPP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● **TTL (Time to Live)** – Set TTL value of PING operation. ● **Ping Interval** – Enter the interval for the system to execute the PING operation. ● **Ping Retry** – Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.

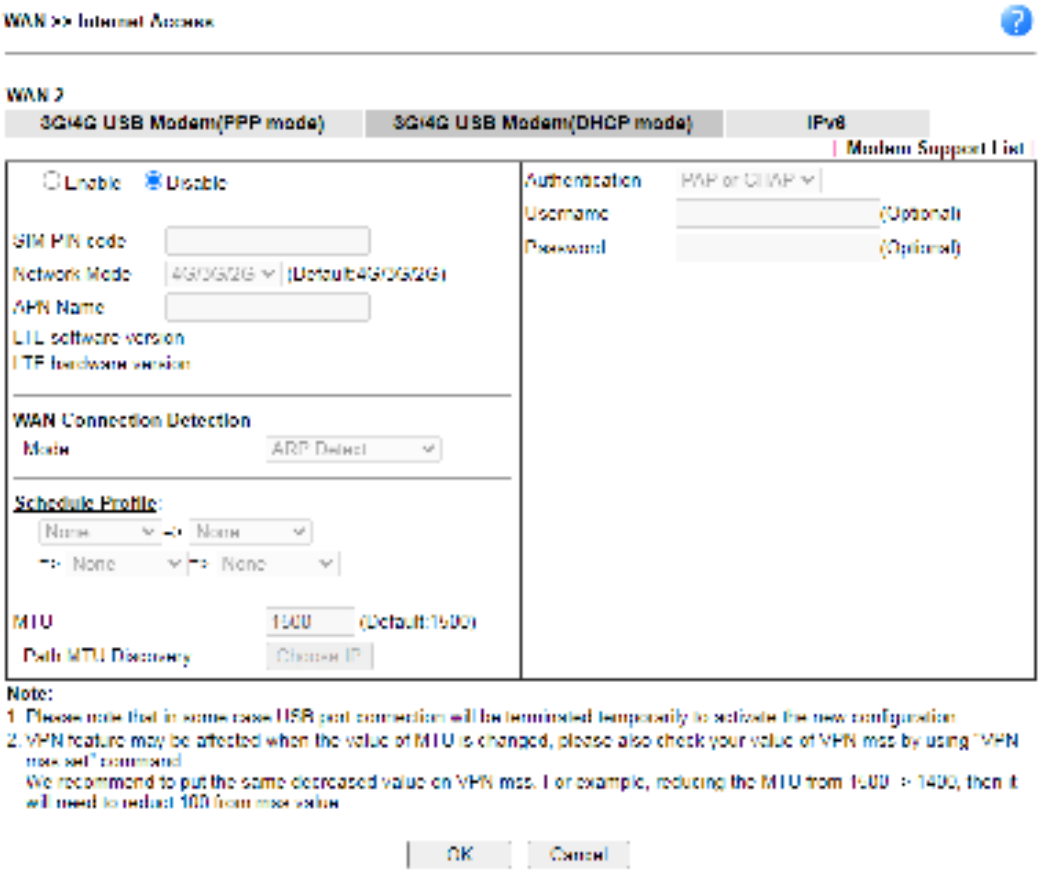
After finishing all the settings here, please click **OK** to activate them.

II-1-2-5 Details Page for 3G/4G USB Modem (DHCP mode) in WAN2

To use **3G/4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu.

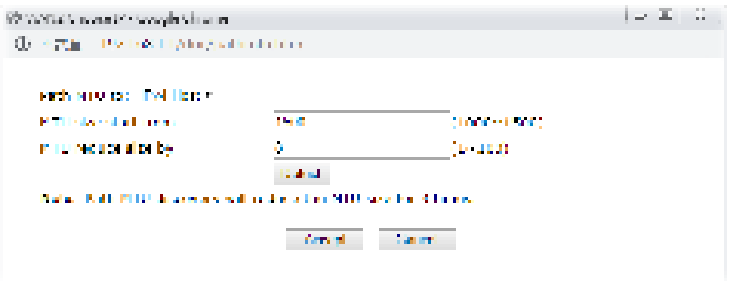


Then, select **3G/4G USB Modem (DHCP mode)** for WAN2. The following web page will be shown.



Available settings are explained as follows:

Item	Description
Modem Support List	It lists all of the modems supported by such router.
Enable / Disable	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19

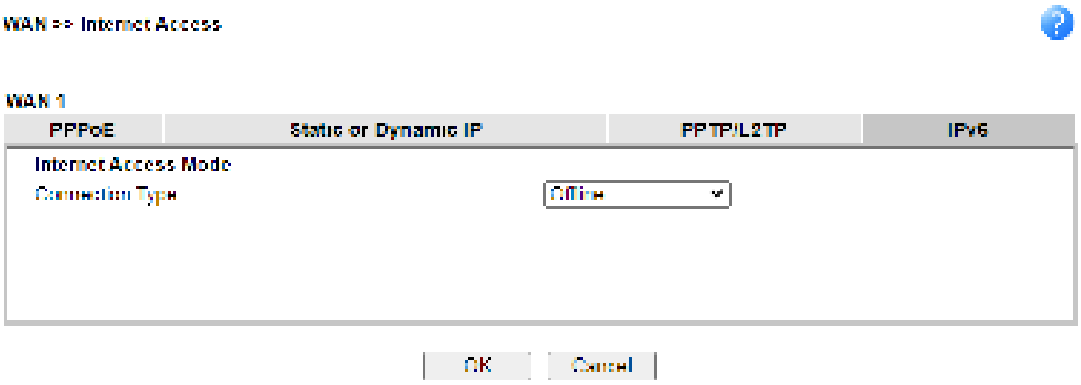
	characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Enter the name and click **Apply.** The maximum length of the name you can set is 47 characters.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items. ● **Primary/Secondary Ping IP** – If you choose **Ping Detect** as detection mode, you have to type Primary or Secondary IP address in this field for pinging. ● **Ping Gateway IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging. ● With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. ● **TTL (Time to Live)** – Set TTL value of PING operation. ● **Ping Interval** – Enter the interval for the system to execute the PING operation. ● **Ping Retry** – Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.
Schedule Profile	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
MTU	It means Max Transmit Unit for packet. **Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path. Click **Choose IP** to open the following dialog.  ● **Path MTU to** – Enter the IP address as the specific transmit path. ● **MTU reduce size by**– It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500,

	1492, 1484 and etc., automatically. ● **Detect** – Click it to detect a suitable MTU value ● **Accept** – After clicking it, the detected value will be displayed in the field of MTU.
Authentication	Select **PAP only** or **PAP or CHAP** for PPP authentication. **Username** – Enter the username for authentication (optional). **Password** – Enter the password for authentication (optional).

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

II-1-2-6 Details Page for IPv6 – Offline in WAN1/WAN2

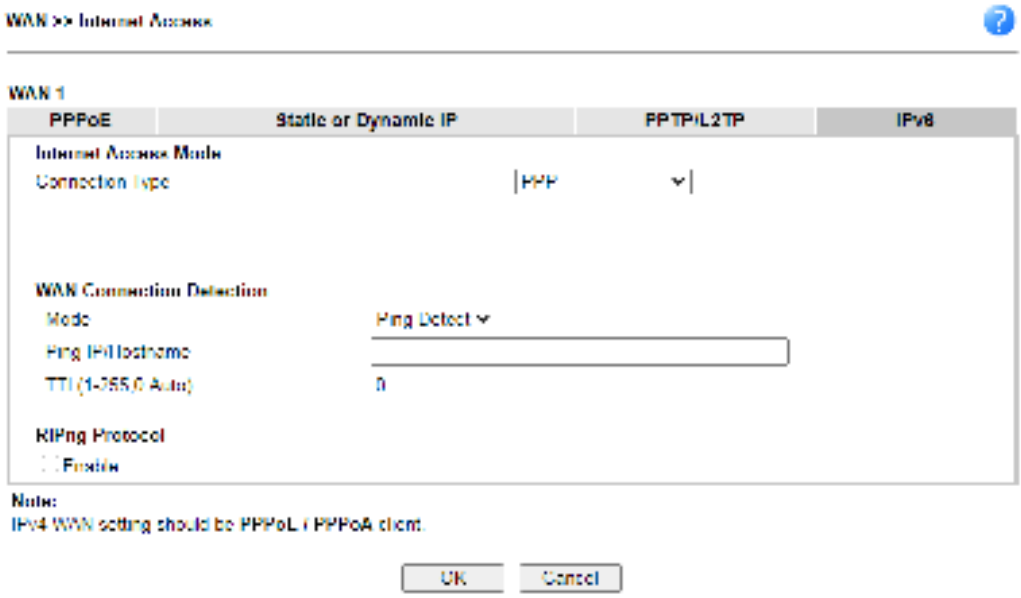
When Offline is selected, the IPv6 connection will be disabled.



II-1-2-7 Details Page for IPv6 – PPP in WAN1/WAN2

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

No need to type any other information for PPP mode.



Available settings are explained as follows:

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

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

Info

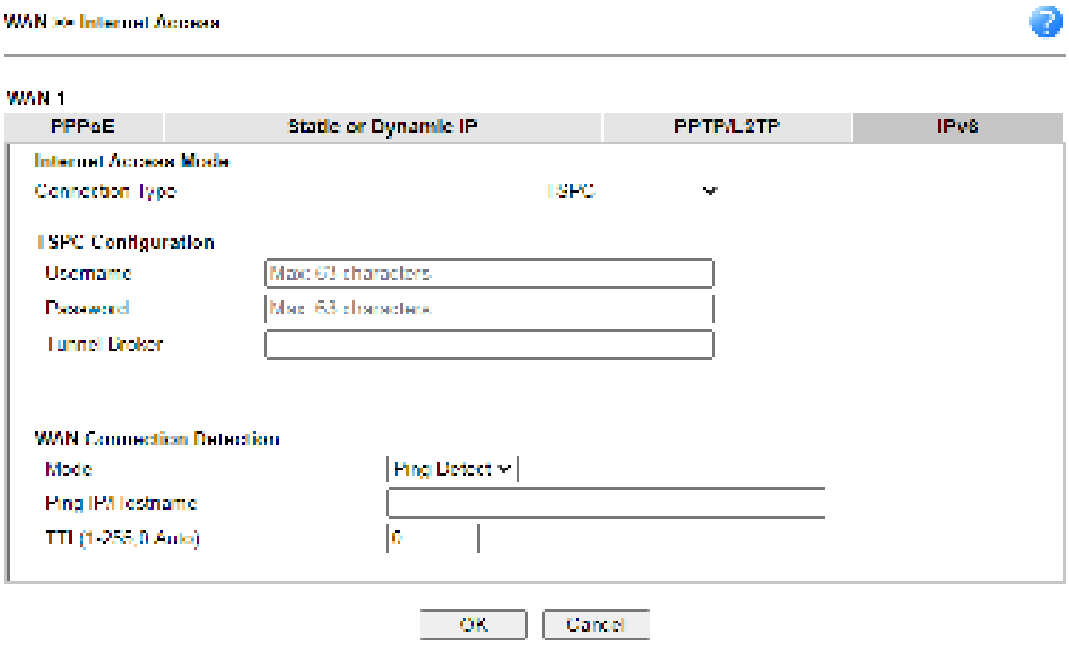
At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

II-1-2-8 Details Page for IPv6 – TSPC in WAN1/WAN2

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

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

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

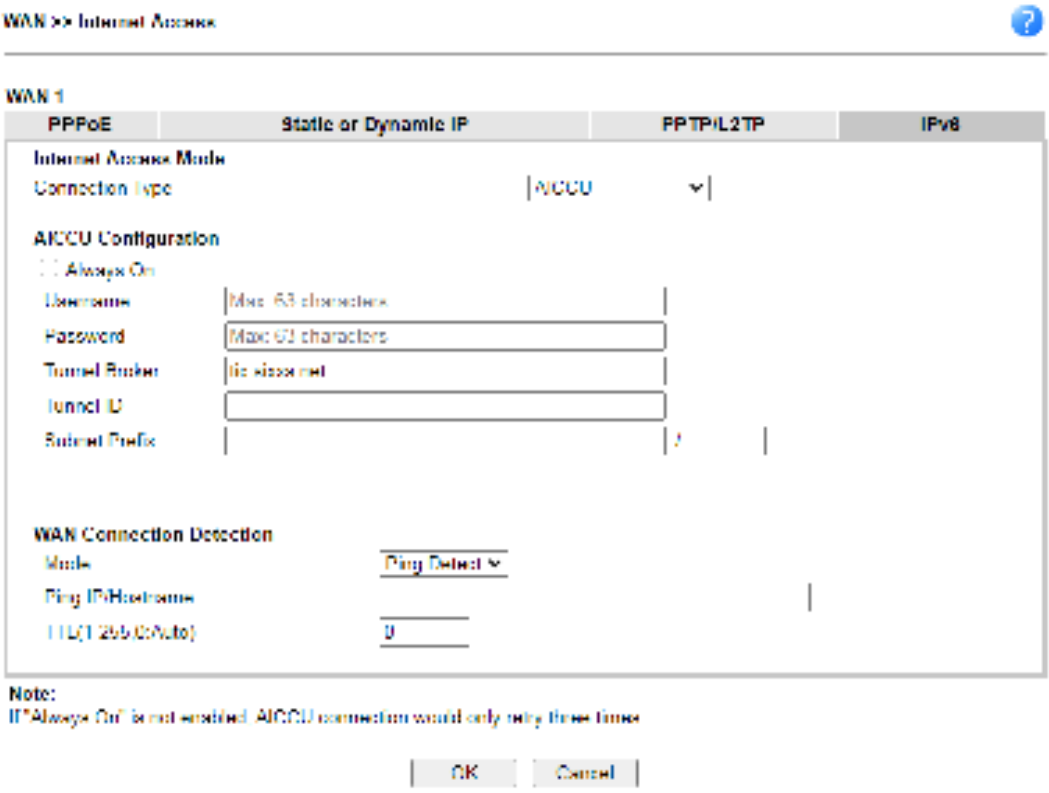


Available settings are explained as follows:

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

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

II-1-2-9 Details Page for IPv6 – AICCU in WAN1/WAN2



Available settings are explained as follows:

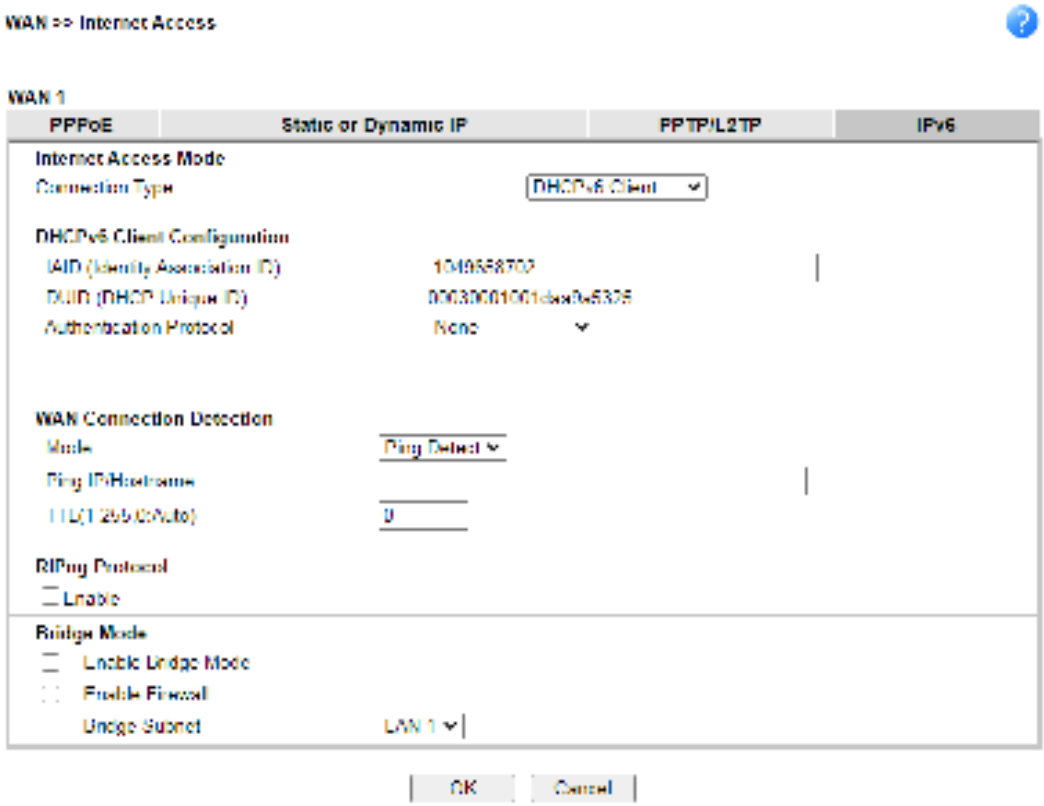
Item	Description
Always On	Check this box to keep the network connection always.
Username	Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password. The maximum length of the name you can set is 19 characters.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

	execute for WAN detection. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

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

II-1-2-10 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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



Available settings are explained as follows:

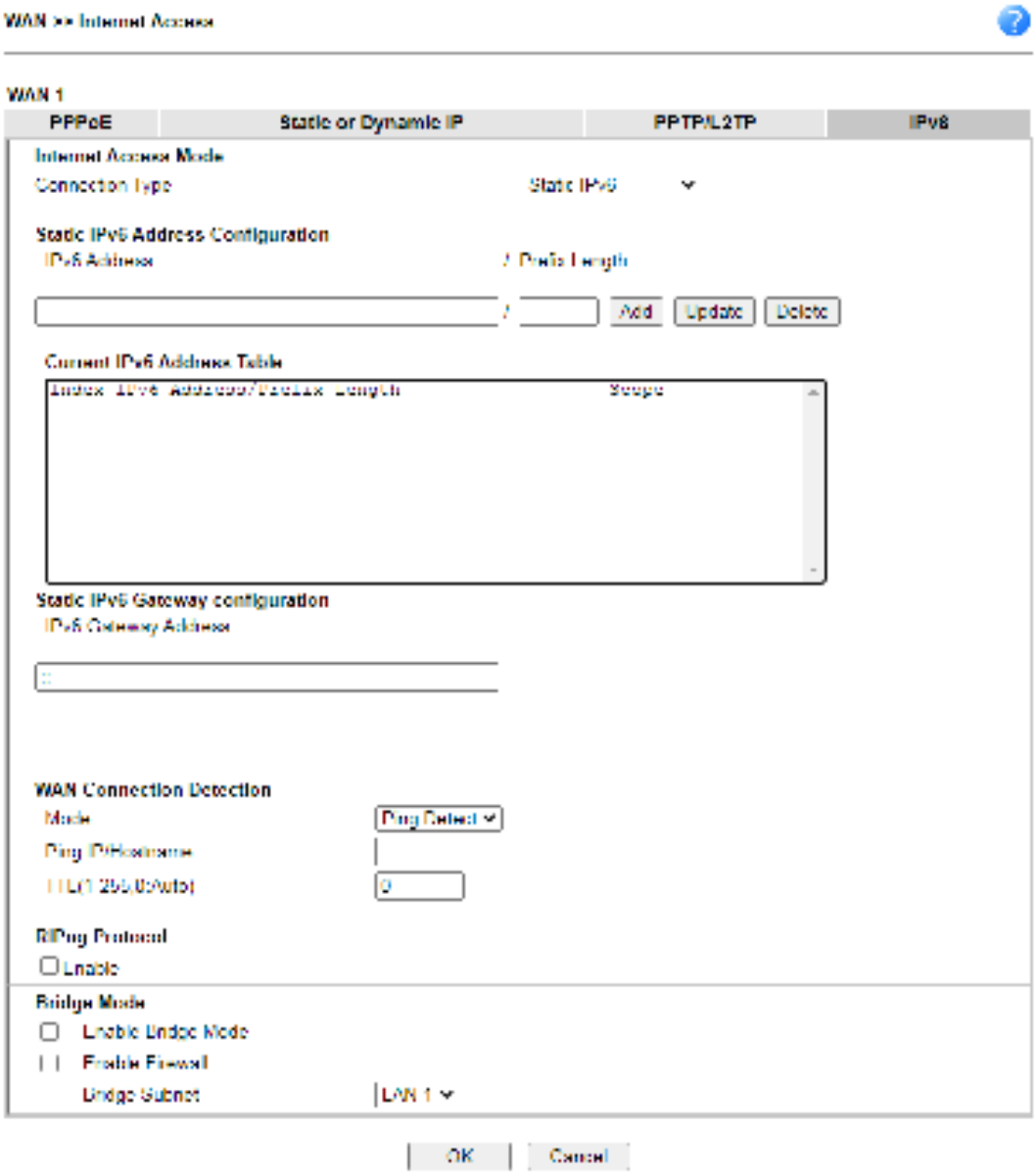
Item	Description
IAID	Type a number as IAID.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect. **Mode** – Choose **Always On**, **Ping Detect** or **NS Detect** for the system to execute for WAN detection. With **NS Detect** mode, the system will check if network connection is established or not, like IPv4 ARP Detect. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.
RIPng Protocol	RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.
Bridge Mode	**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem. **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.

	Bridge Subnet – Make a bridge between the selected LAN subnet and such WAN interface.

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

II-1-2-11 Details Page for IPv6 – Static IPv6 in WAN1/WAN2

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



Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	**IPv6 Address** – Enter the IPv6 Static IP Address. **Prefix Length** – Enter the fixed value for prefix length. **Add** – Click it to add a new entry. **Update** – Click it to modify an existed entry. **Delete** – Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.

Static IPv6 Gateway Configuration	**IPv6 Gateway Address -** Type your IPv6 gateway address here.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.
RIPng Protocol	Check the Enable box to make RIPng (RIP next generation) offer the same functions and benefits as IPv4 RIP v2.
Bridge Mode	**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem. **Enable Firewall** – It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated. **Bridge Subnet** – Make a bridge between the selected LAN subnet and such WAN interface.

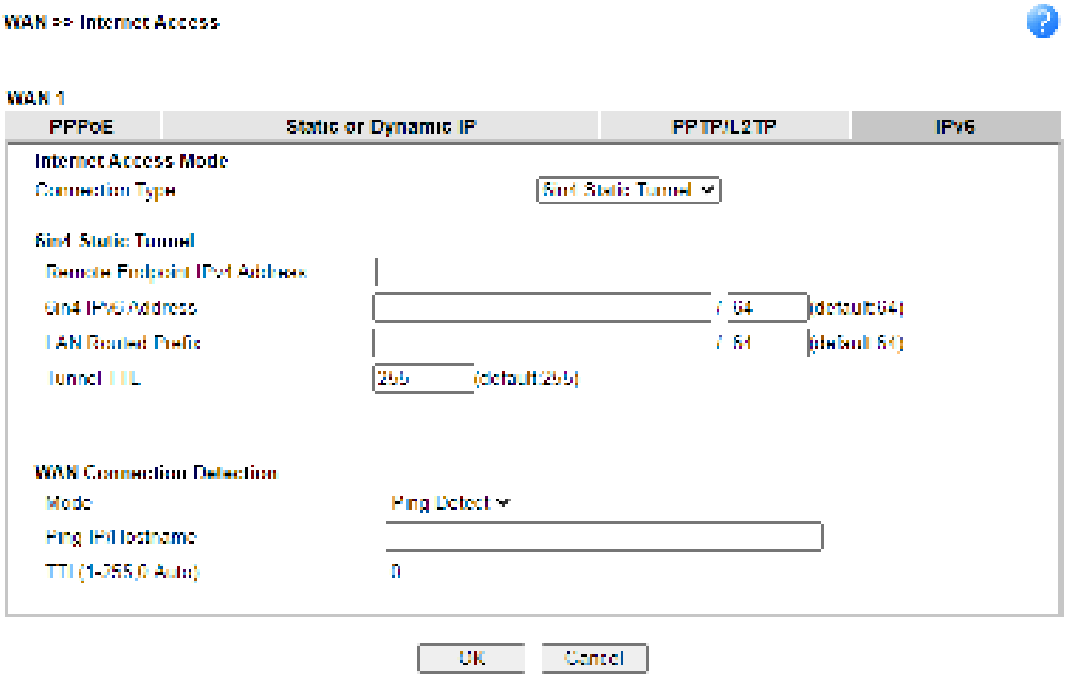
After finished the above settings, click **OK** to save the settings.

II-1-2-12 Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2

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

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

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

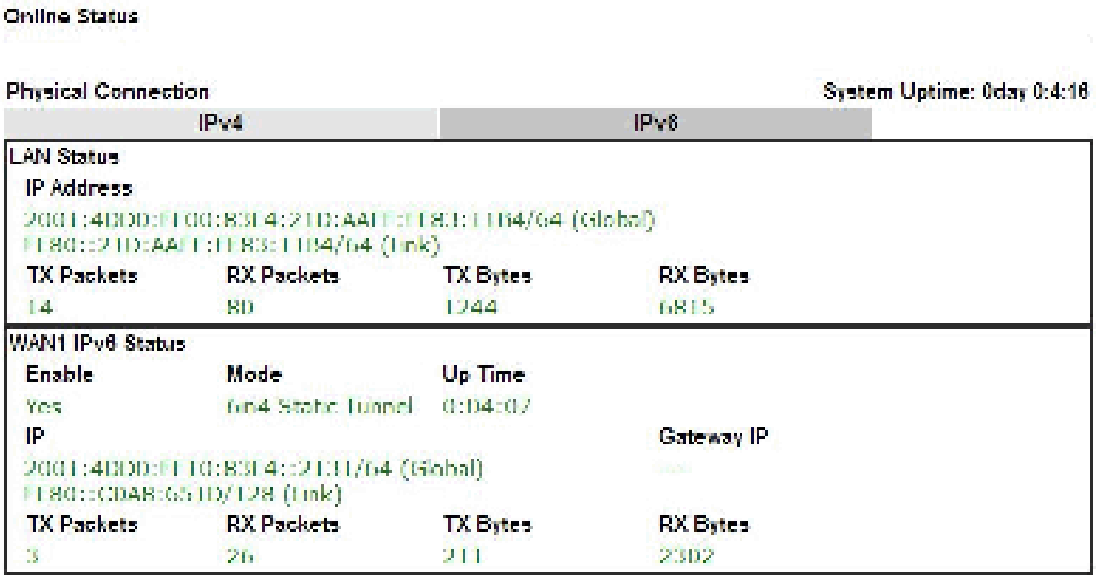


Available settings are explained as follows:

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

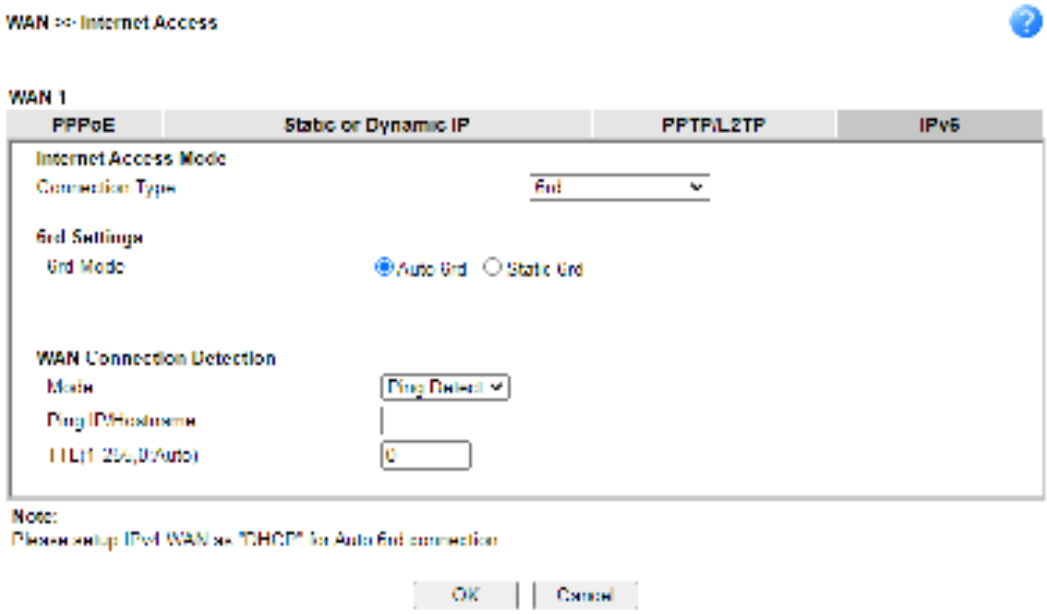
After finished the above settings, click **OK** to save the settings.

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



II-1-2-13 Details Page for IPv6 – 6rd in WAN1/WAN2

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



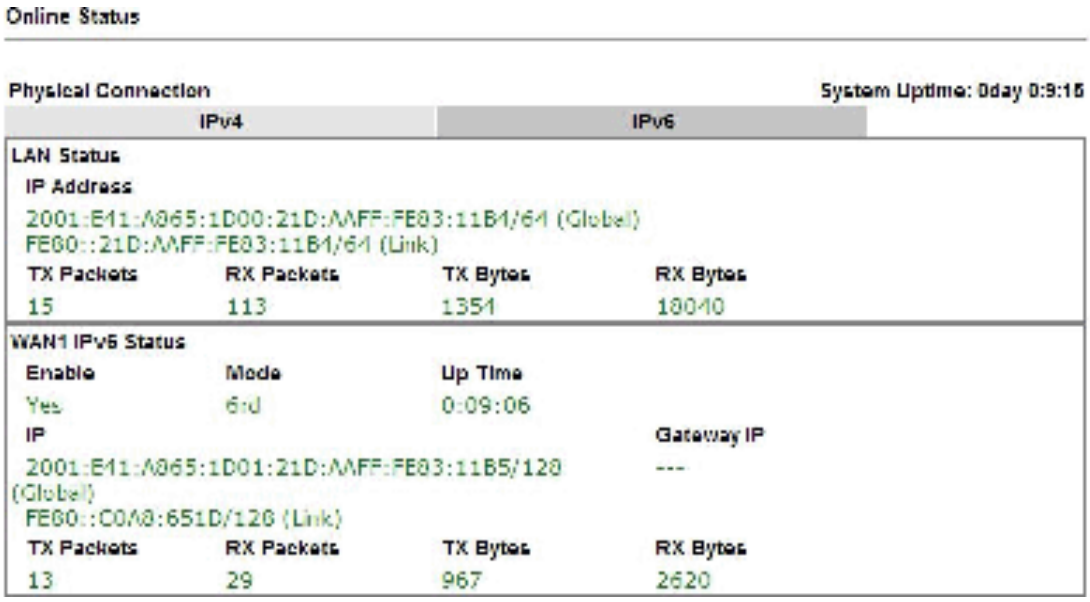
Available settings are explained as follows:

Item	Description
6rd Mode	**Auto 6rd** – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". **Static 6rd -** Set 6rd options manually.
IPv4 Border Relay	Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Enter the 6rd IPv6 address.

6rd Prefix Length	Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through Ping Detect. **Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always. ● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value.

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

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



II-1-3 Multi-VLAN

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

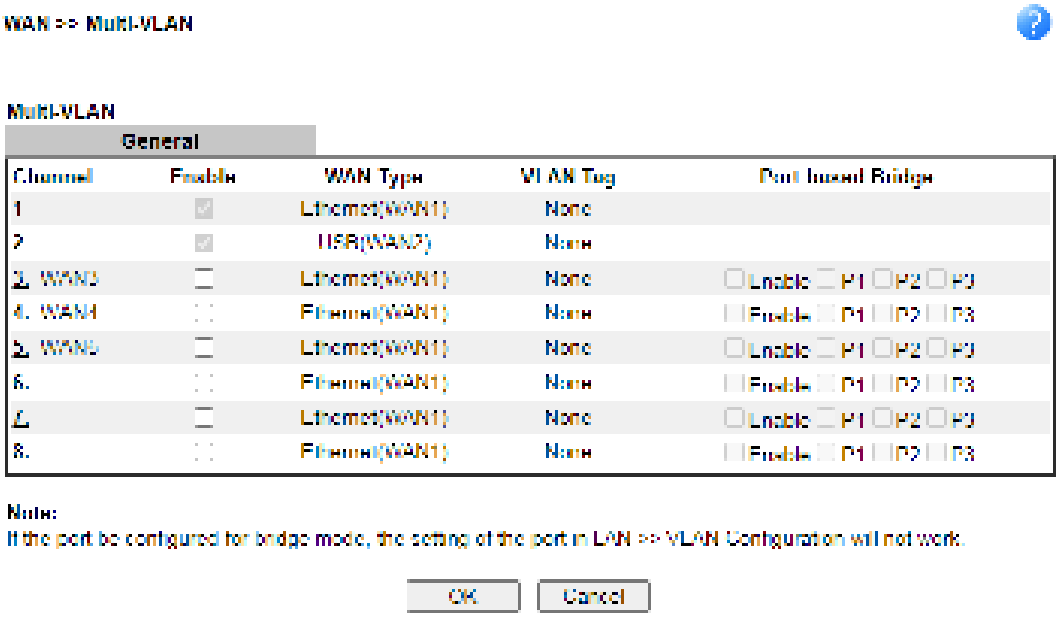
Channel 1 to 2 have the following fixed assignments and cannot be altered.

- Channel 1: Ethernet / Fiber on WAN1.
- Channel 2: Ethernet / USB on WAN2 (based on the model)

Channels 3 through **8** can be bridged to one or more of the 3 LAN ports P2 through P4. In addition, **Channels 3** through 5 can be configured as virtual WANs (WAN3 through WAN5).

General

This page shows the basic configurations used by every channel.



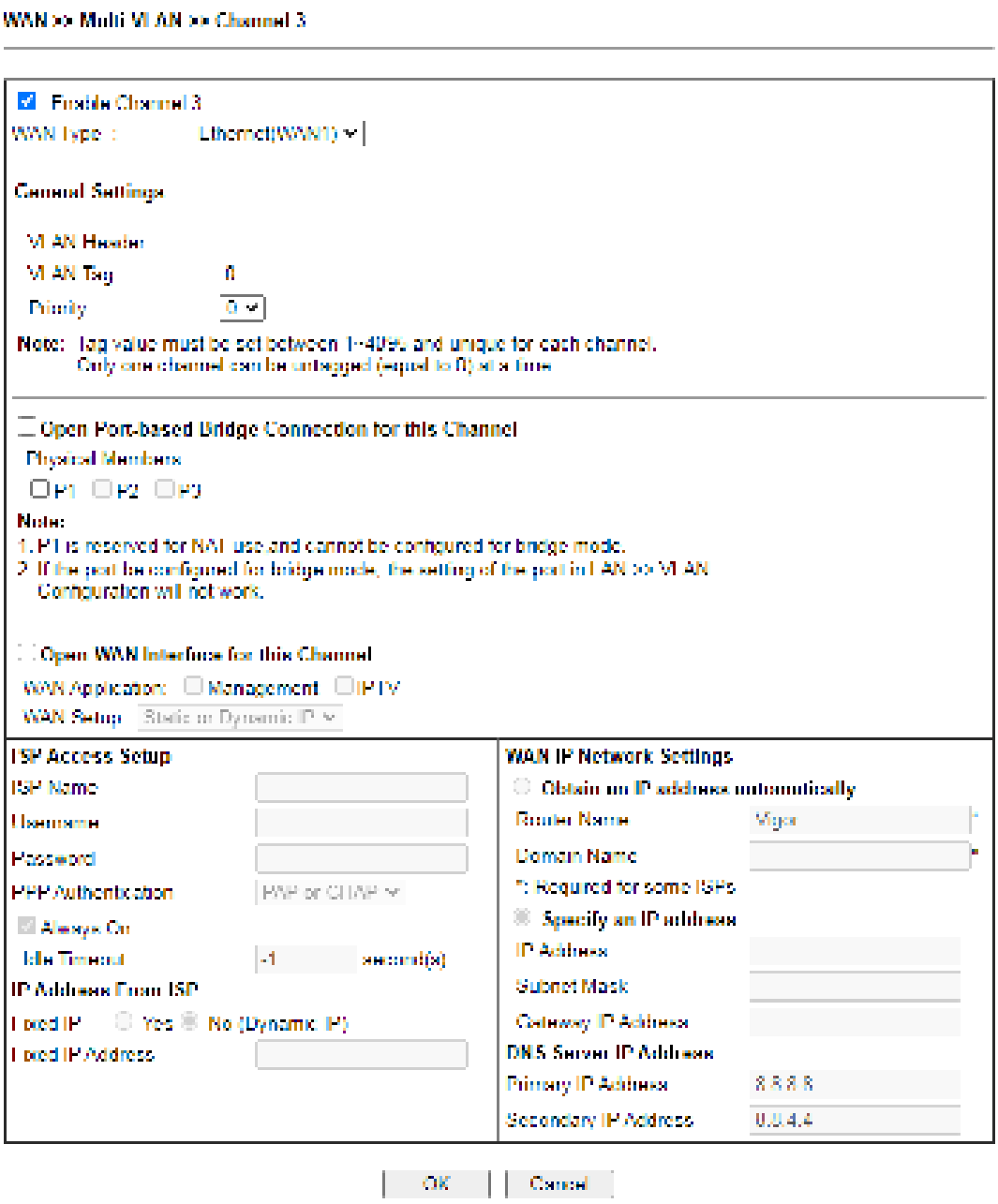
Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here. Channels 3 ~ 8 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.

Port-based Bridge	The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Enable** - Check this box to enable the port-based bridge function on this channel. **P1** ~ **P3** – Check the box(es) to build bridge connection on LAN.

To configure a PVC channel, click its channel number.

WAN links for Channel 3, 4 and 5 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3, 4 or 5 to configure your router.



Available settings are explained as follows:

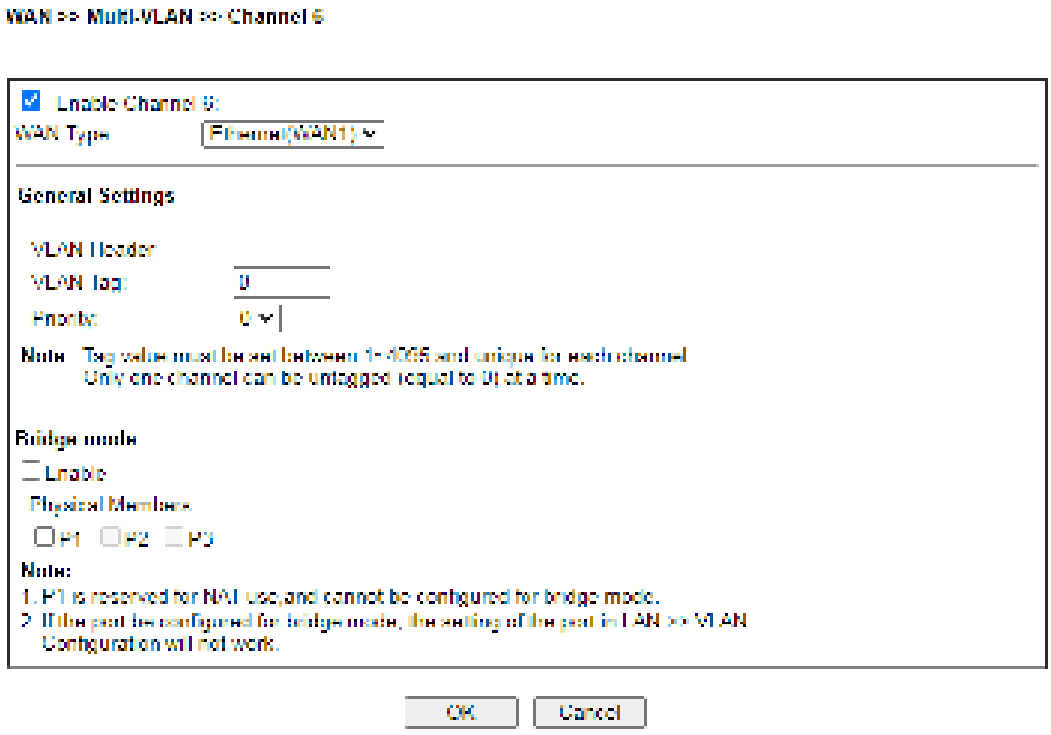
Item	Description

Enable Channel 3/4/5	Check it to enable this channel.
WAN Type	Specify a WAN type of the VLAN.
General Settings	**VLAN Tag –** Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Priority –** Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7. **Service Tag Value** – Such value varies depending on the setting configured in **WAN>>General Setup**. If required, click **Modify** to open **WAN>>General Setup.** Then, enable **VLAN Tag insertion** for service (outer tag) and specify the value as the VLAN ID number. Or, disable it.
Open Port-based Bridge Connection for this Channel	The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured. **Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection. **Note:** LAN port P1 is reserved for NAT use and cannot be selected for bridging.
Open WAN Interface for this Channel	Check the box to enable relating function. **WAN Application - Management** can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069. **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers. **WAN Setup** – Choose **PPPoE/PPPoA** or **Static or Dynamic IP** to determine what WAN settings must be configured.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. **ISP Name** – PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank. **Username** – Name provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. **Password** – Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters. **PPP Authentication** –The protocol used for PPP authentication. ● **PAP only**- Only PAP (Password Authentication Protocol) is used. ● **PAP or CHAP**- Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. **Always On** – If selected, the router will maintain the PPPoE/PPPoA connection. **Idle Timeout** – Maximum length of time, in seconds, of idling

	allowed (no traffic) before the connection is dropped. **IP Address From ISP** - Specifies how the WAN IP address of the channel configured. ● **Fixed IP** **Yes** - IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN. **No** - Virtual WAN IP address will be assigned by the ISP's PPPoE/ PPPoA server.
WAN IP Network Settings	**Obtain an IP address automatically** – Select this option if the router is to receive IP configuration information from a DHCP server. ● **Router Name** – Sets the value of DHCP Option 12, which is used by some ISPs. ● **Domain Name** – Sets the value of DHCP Option 15, which is used by some ISPs. **Specify an IP address** – Select this option to manually enter the IP address. ● **IP Address** – Type in the IP address. ● **Subnet Mask** – Type in the subnet mask. ● **Gateway IP Address** – Type in gateway IP address. **DNS Server IP Address -** Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

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

Click any index (6, 7 and 8) to get the following web page:



Available settings are explained as follows:

Item	Description
Enable Channel 6/7/8	Click it to enable the configuration of this channel.

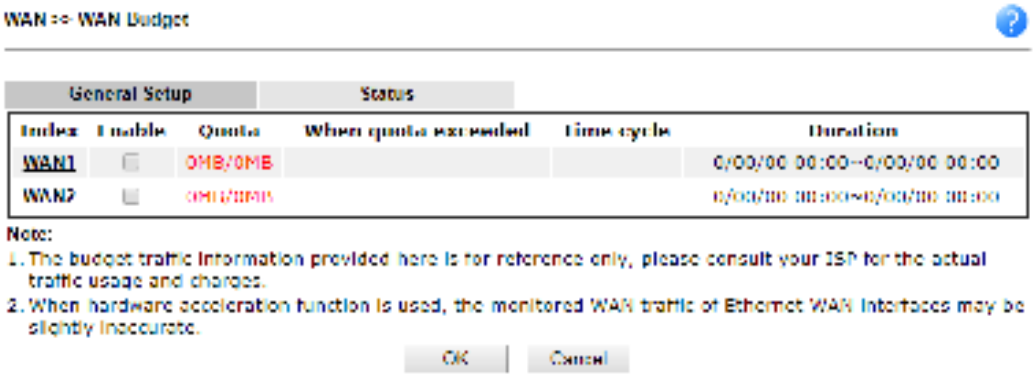
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
General Settings	**VLAN Tag –** Enter the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value. **Priority –** Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
Bridge mode	**Enable –** Click it to enable Bridge mode for such channel. **Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the bridge connection. **Note:** LAN port P1 is reserved for NAT use and cannot be selected for bridging.

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

II-1-4 WAN Budget

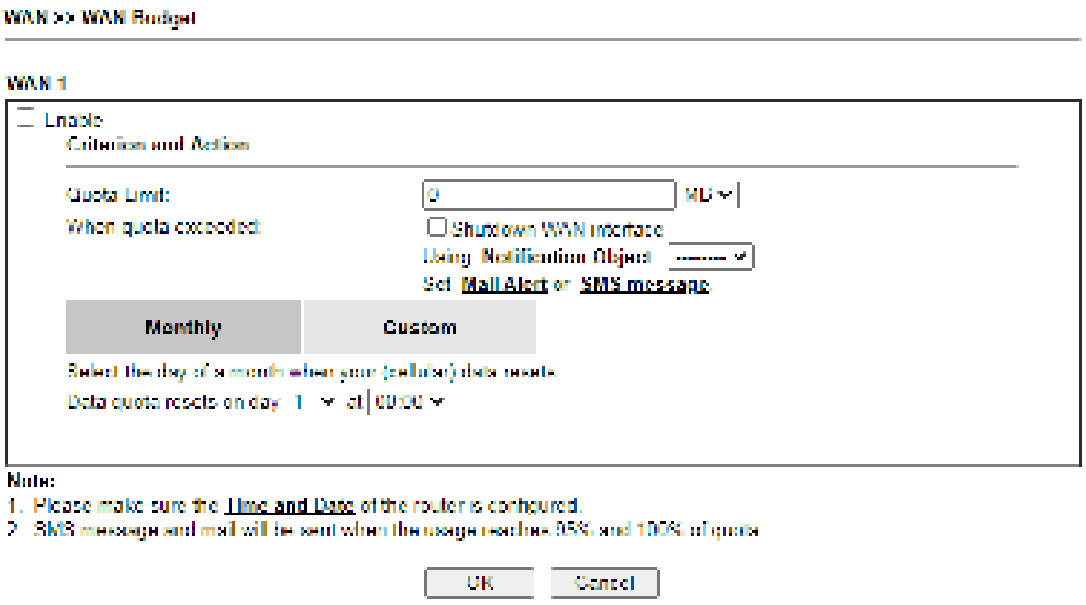
This function is used to determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP. Please note that the Quota Limit and Billing cycle day of month settings will need to be configured correctly first in order for some period calculations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

II-1-4-1 General Setup



Item	Description
Index	The WAN port. Click to configure WAN Budget for a particular WAN.
Enable	Check to enable WAN Budget 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/ WAN2 link to open the following web page.

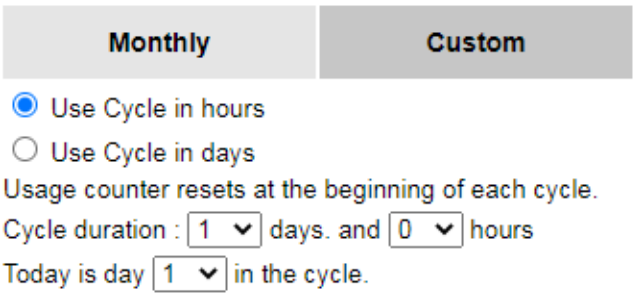


Available settings are explained as follows:

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

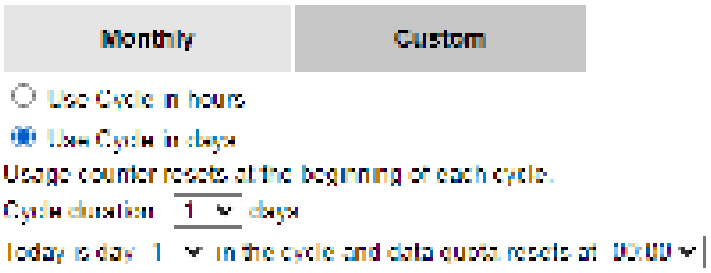
required, use **Custom**. The period of cycle duration is between 1 day and 60 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.

Use Cycle in hours –



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

Use Cycle in days -

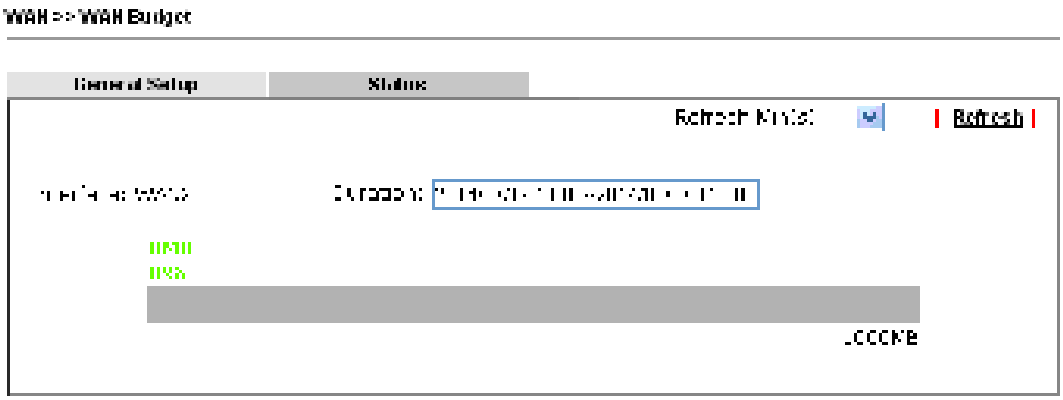


- **Cycle duration**: Specify the days to reset the traffic record. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the router will reset the traffic record automatically.
- **Today is day** – Specify the day and time for data quota rest in the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

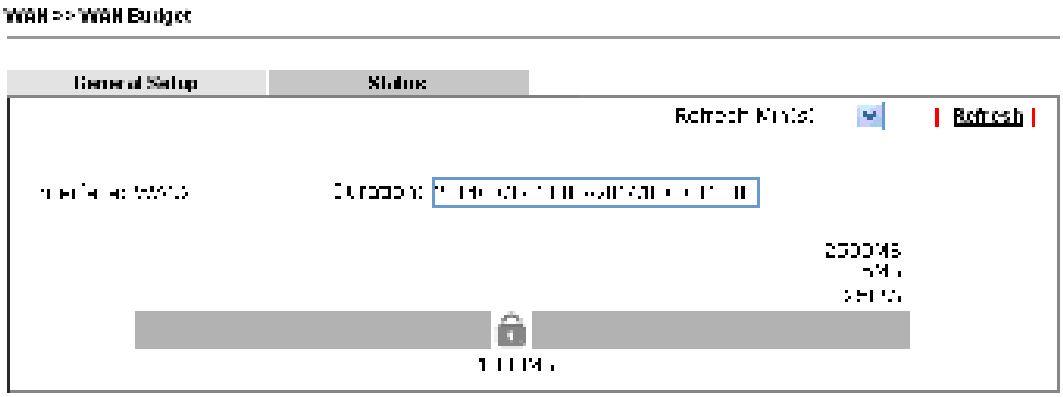
After finished the above settings, click **OK** to save the settings.

II-1-4-2 Status

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



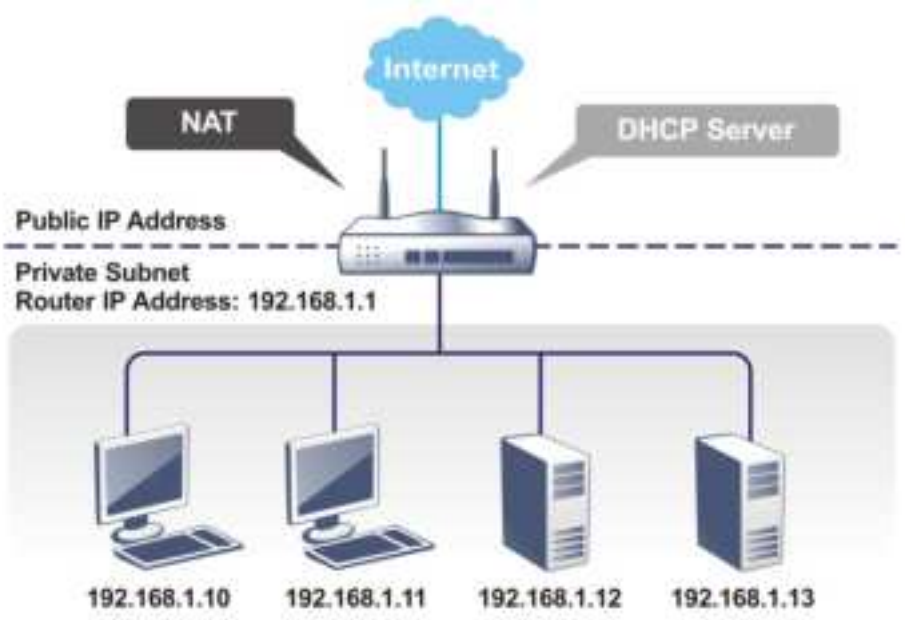
If the WAN budget is exhausted, a lock will be displayed on the page if **Shutdown WAN interface** is selected. Which means no data transmission will be carried out. Moreover, the system will send out a warning message to the administrator if **Mail Alert** is selected**.** Or, the system will send out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



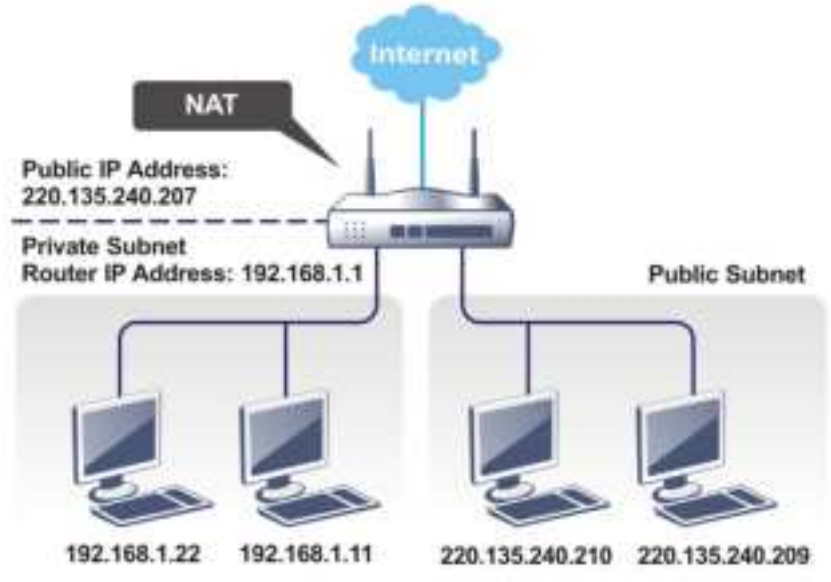
II-2 LAN

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

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



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



What is Routing Information Protocol (RIP)

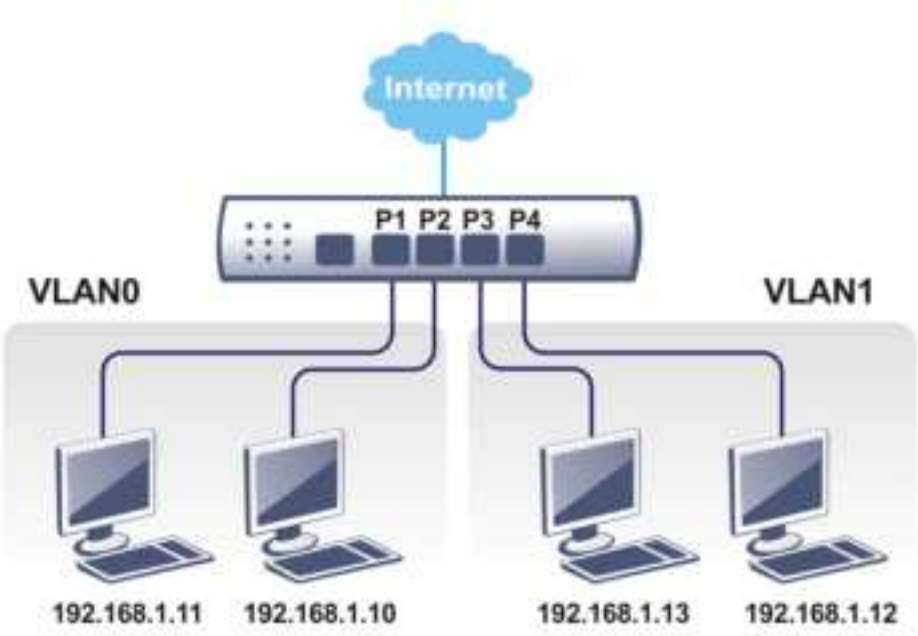
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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

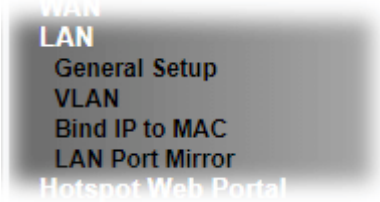


Web User Interface

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

LAN clients within the same LAN are normally able to communicate with one another directly, as they are peers to one another, unless measures, such as firewalls or VLANs, have been put in place to restrict such access. Nowadays the most common LAN firewalls are implemented on the LAN client itself. For example, Microsoft Windows since Windows XP and Apple OS X have built-in firewalls that can be configured to restrict traffic coming in and going out of the computer. VLANs, on the other hand, are usually set up using network switches or routers, such as the Vigor2915.

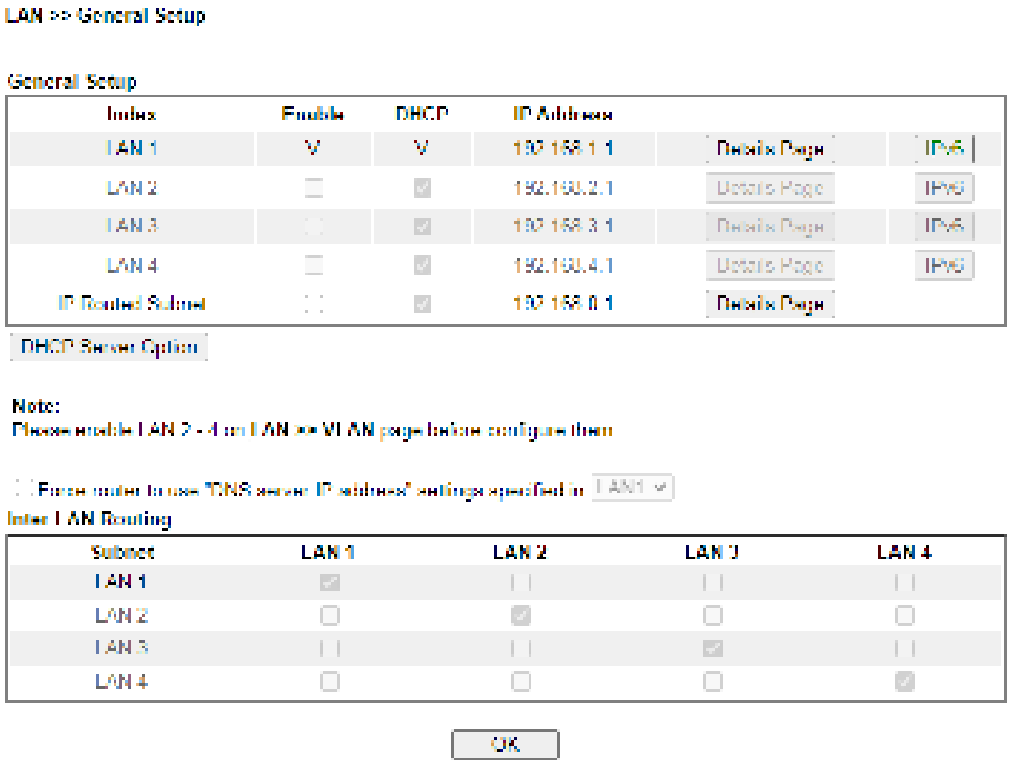
To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router (such as the Vigor 2915) that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach their intended destinations.



II-2-1 General Setup

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

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



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. **Status-** Basically, LAN1 status is enabled in default. LAN2 –LAN5 and IP Routed Subnet can be observed by checking the box of **Status**. **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 Option	DHCP packets can be processed by adding option number and data information when such function is enabled. For detailed information, refer to later section.
Force router to use "DNS server IP address ...."	Force Vigor router to use DNS servers configured in LAN1/ LAN2/ LAN3/ LAN4 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN). Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. Refer to section II-2-2 VLAN on how to set up VLANs. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each

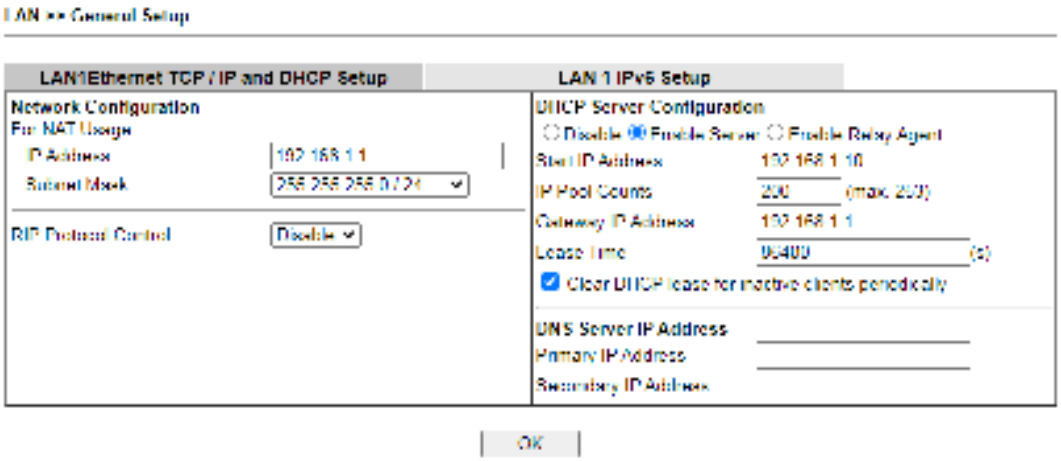
	other.

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

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

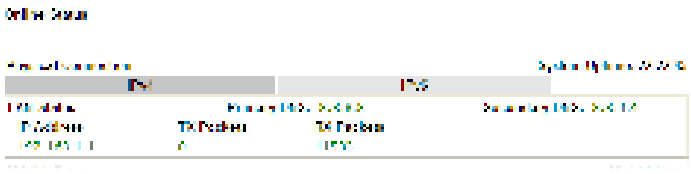
II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

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



Available settings are explained as follows:

Item	Description
Network Configuration	**For NAT Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **RIP Protocol Control,** **Enable** – When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **Disable Server** – Let you manually assign IP address to every host in the LAN. **Enable Server -** Let the router assign IP address to every host

	in the LAN. ● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients. ● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 200. Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above. ● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. ● **Clear DHCP lease for inactive clients periodically -** If selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. **Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following: - Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30. - Clear DHCP lease when the client is not responding ARP replies. **Enable Relay Agent –** When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. ● **DHCP Server IP Address –** It is available when **Enable Relay Agent** is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. **Primary IP Address -** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. **Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. The default DNS Server IP address can be found via Online Status:  If both the Primary IP and Secondary IP Address fields are left

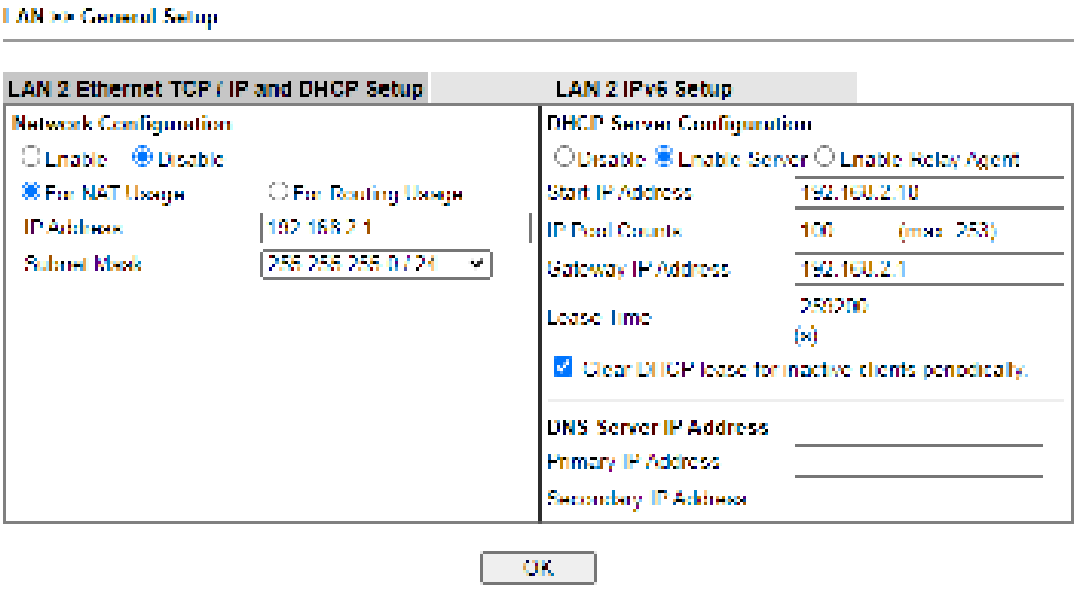
	empty, the router will assign DNS servers obtained from WAN interface to local users as a DNS proxy server and maintain a DNS cache. If there is no DNS servers available, router will use its own IP address instead. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/ Cable) connection.

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

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

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

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



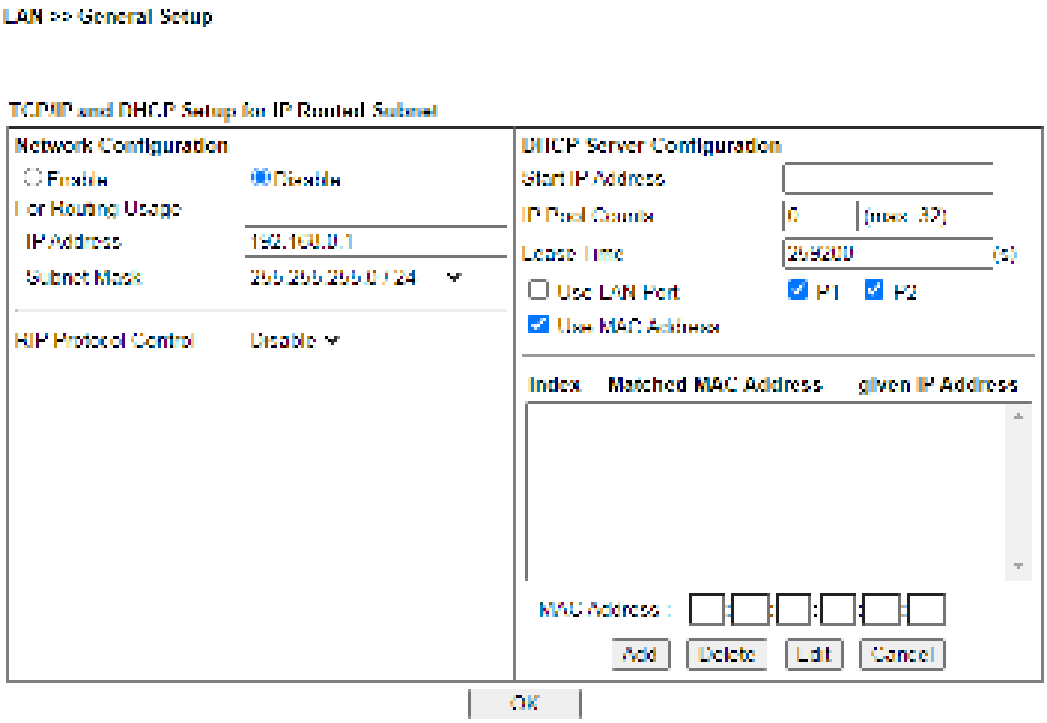
Available settings are explained as follows:

Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For NAT Usage -** Click this radio button to invoke NAT function. **For Routing Usage -** Click this radio button to invoke this function. **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24).
DHCP Server Configuration	**Disable Server –** Let you manually assign IP address to every host in the LAN. **Enable Server -** Let the router assign IP address to every host in the LAN. ● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients. ● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253. The actual number of IP addresses available for assignment is the IP Pool Counts, or 253 minus the last octet of the Start IP Address, whichever is smaller. ● **Gateway IP Address -** The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router, and therefore the Gateway IP Address should be identical to the IP Address in the **Network Configuration** section above. ● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed. ● **Clear DHCP lease for inactive clients periodically -** If

	selected, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. **Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following: ■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30 ■ Clear DHCP lease when the client is not responding ARP replies. **Enable Relay Agent** – When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. ● **DHCP Server IP Address** – It is available when **Enable Relay Agent** is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. **Primary IP Address -** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. **Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. The default DNS Server IP address can be found via Online Status: If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/ Cable) connection.

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

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



Available settings are explained as follows:

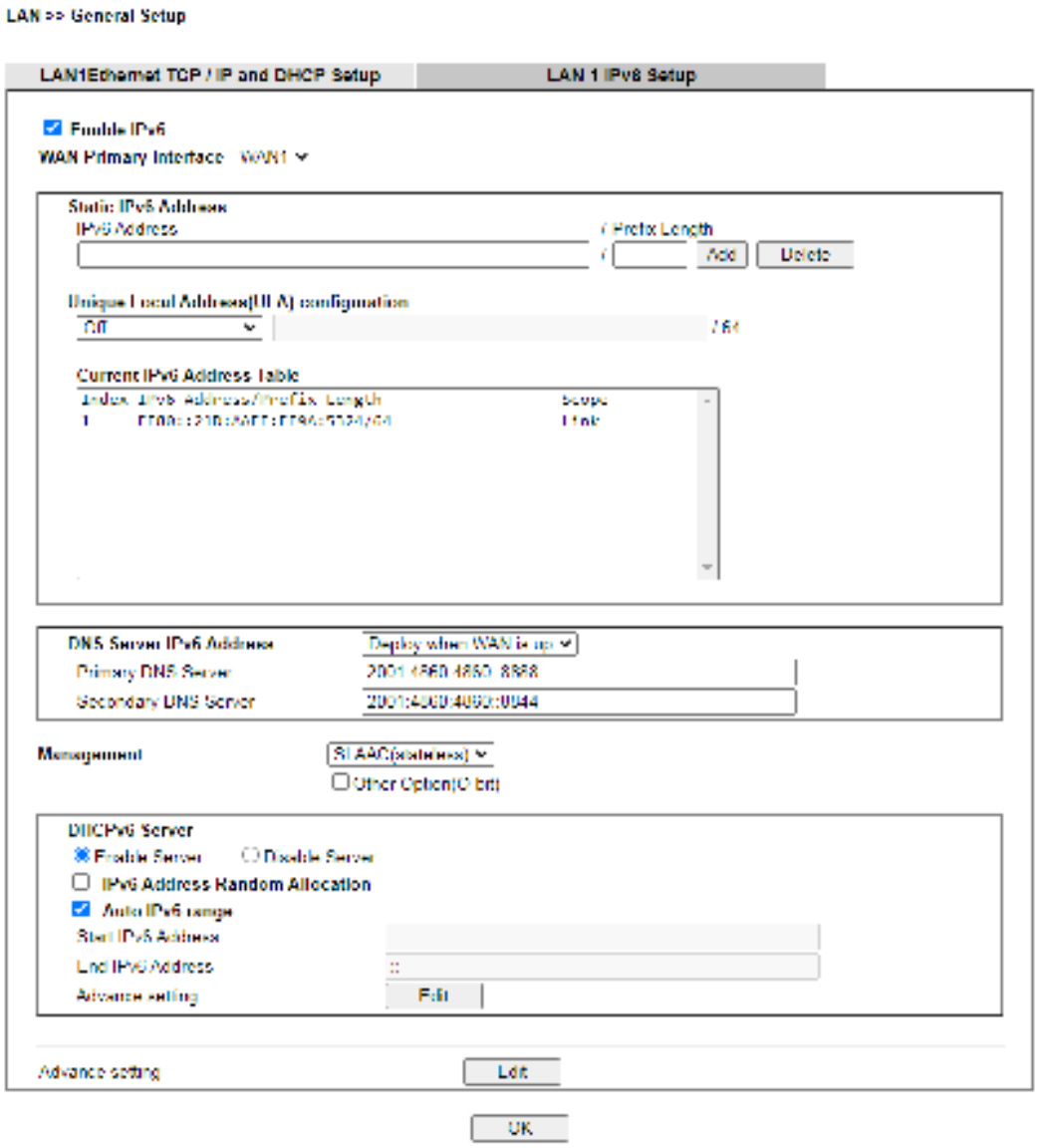
Item	Description
Network Configuration	**Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration. **For Routing Usage,** **IP Address** - This is the IP address of the router. (Default: 192.168.1.1). **Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). **RIP Protocol Control,** **Enable** – When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **Start IP Address -** 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 0 and the maximum is 32. **Lease Time** - Enter the time to determine how long the IP address assigned by DHCP server can be used. **Use LAN Port** – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2. **Use MAC Address -** Check such box to specify MAC address. ● **MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts which can be assigned, deleted or edited from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet. **Add** – Enter the MAC address in the boxes and click this button to add. **Delete** – Click it to delete the selected MAC address. **Edit** – Click it to edit the selected MAC address. **Cancel** – Click it to cancel the job of adding, deleting and editing.

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

II-2-1-4 Details Page for LAN IPv6 Setup

There are two configuration pages for LAN1/LAN2/LAN3/LAN4, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

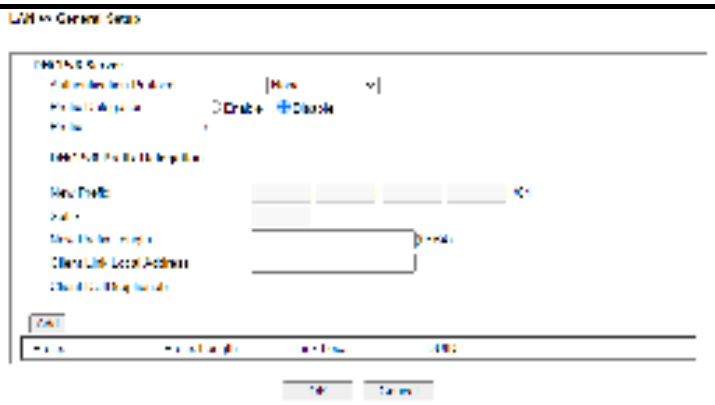
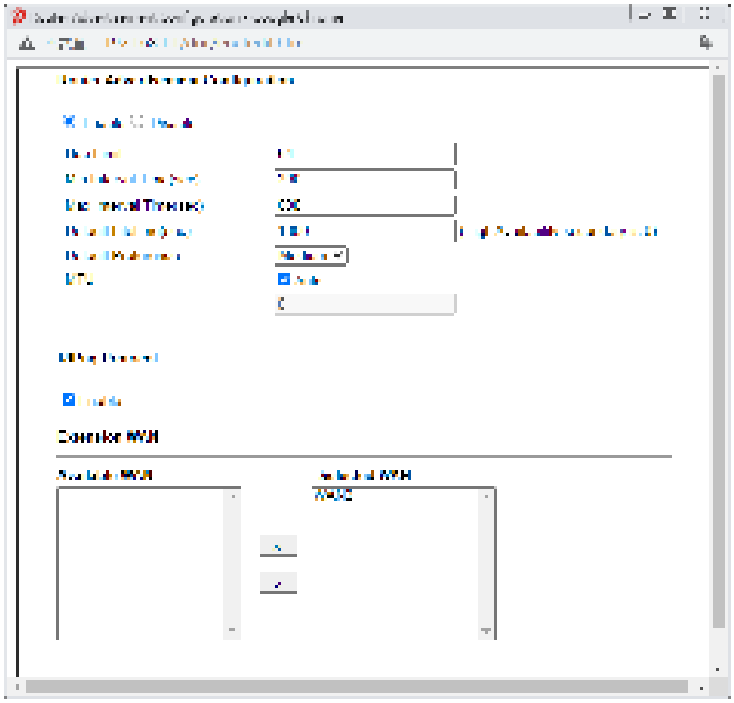


It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6** (Stateful) server.

Available settings are explained as follows:

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

	automatically-determined prefix.
Current IPv6 Address Table	Display current used IPv6 addresses.
DNS Server IPv6 Address	**Deploy when WAN is up** – The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up. **Enable** – The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not. ● **Primary DNS Sever** – Enter the IPv6 address for Primary DNS server. ● **Secondary DNS Server** –Type another IPv6 address for DNS server if required. **Disable** – DNS server will not be used.
Management	Configures the Managed Address Configuration flag (M-bit) in Route Advertisements. ● **Off** - No configuration information is sent using Route Advertisements. ● **SLAAC(stateless) -** M-bit is unset. ● **DHCPv6(stateful**) - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor router, or a separate DHCPv6 server. **Other Option (O-bit)** - Check this box to enable the O-bit for obtaining additional information (e.g., DNS) from DHCPv6. 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** – After check the box, Vigor router will assign the IPv6 range automatically. **Start IPv6 Address** / **End IPv6 Address** –Enter the start and end address for IPv6 server. **Advance setting** – Click the Edit button to configure advanced IPv6 settings for DHCPv6 server.

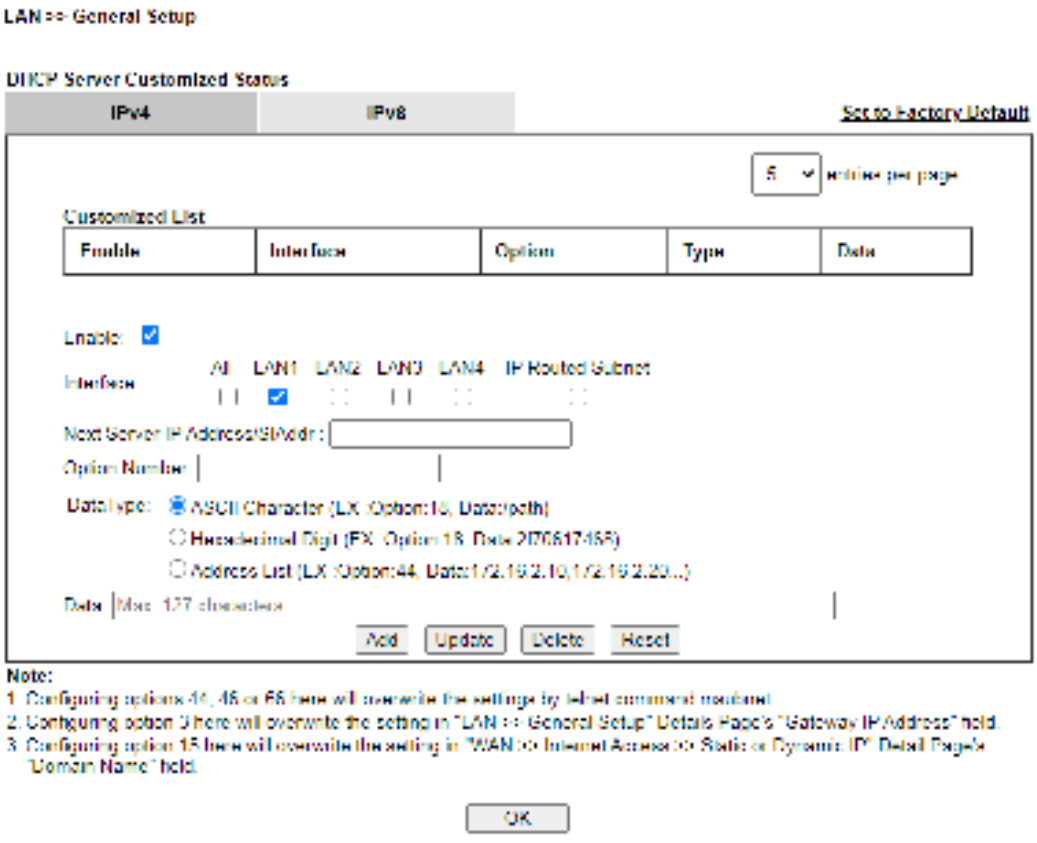
	
Advance setting	The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic.  **Router Advertisement Configuration** – Click **Enable** to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration. ● **Disable** – Click it to disable router advertisement server. ● **Hop Limit** – The value is required for the device behind the router when IPv6 is in use. ● **Min/Max Interval Time (sec)** – It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets. ● **Default Lifetime (sec)** –Within such period of time, Vigor2915 can be treated as the default gateway. ● **Default Preference** – It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted. ● **MTU** – It means Max Transmit Unit for packet. If **Auto** is

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

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

II-2-1-5 Advanced DHCP Options

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



Available settings are explained as follows:

Item	Description
Customized List	Shows all the DHCP options that have been configured in the system.
Enable	If selected, DHCP option entry is enabled. If unselected, DHCP option entry is disabled.
Interface	LAN interface(s) to which this entry is applicable.

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

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

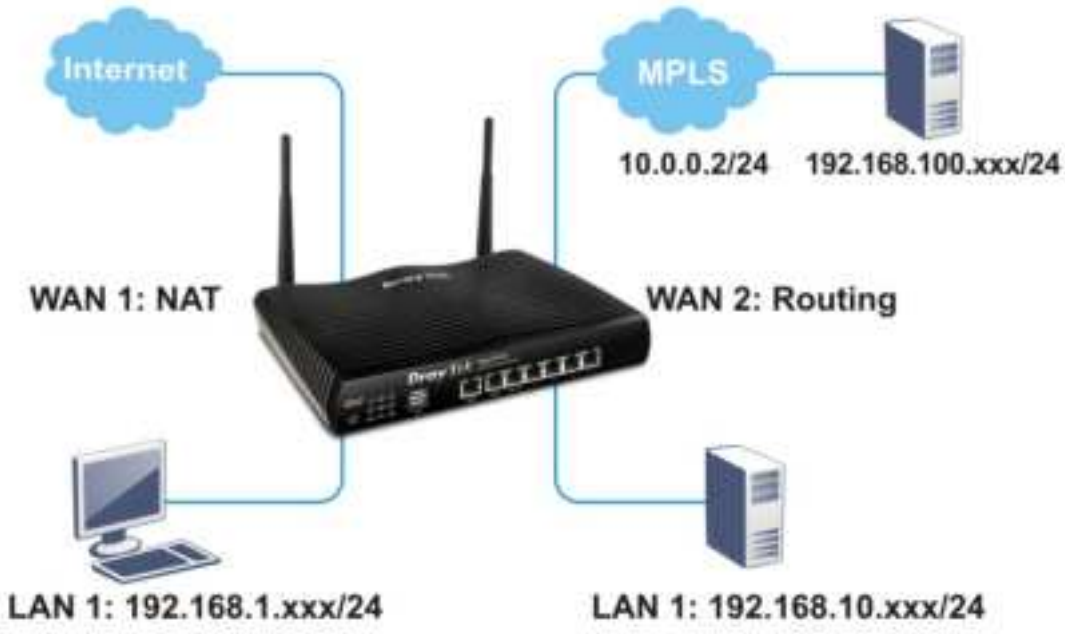
To add a DHCP option entry modeled after an existing entry, click the model entry in **Customized List**. The data entry fields will be populated with values from the model entry. After making all necessary changes for the new entry, click **Add** to create it.

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

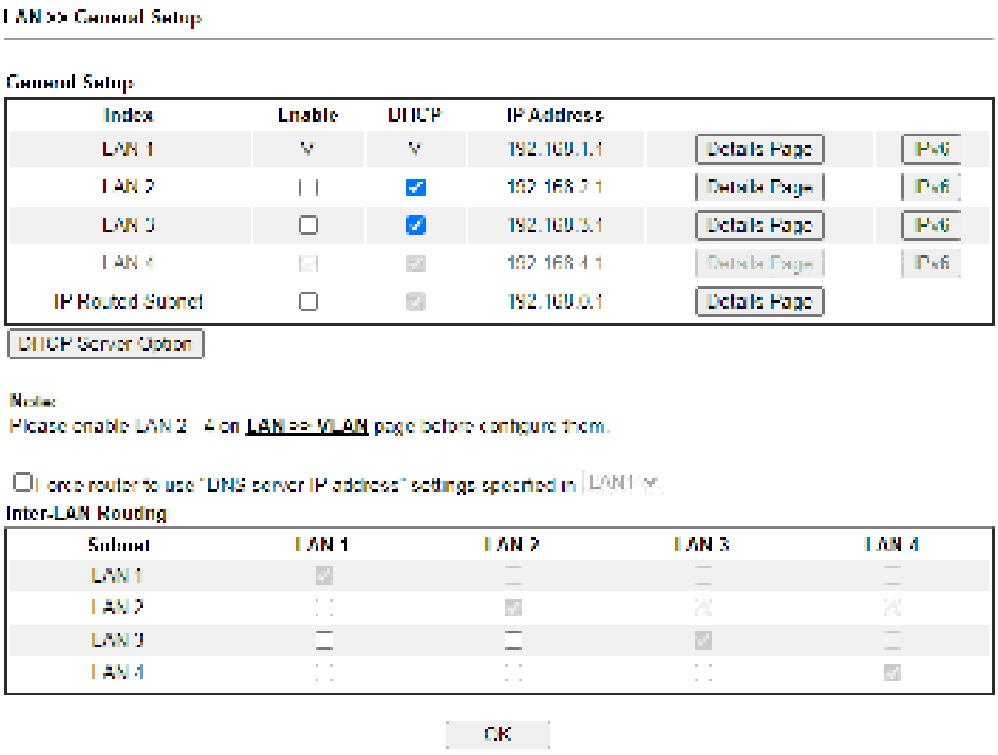
To delete a DHCP option entry, click on it in **Customized List**, and then click **Delete**.

Application Notes

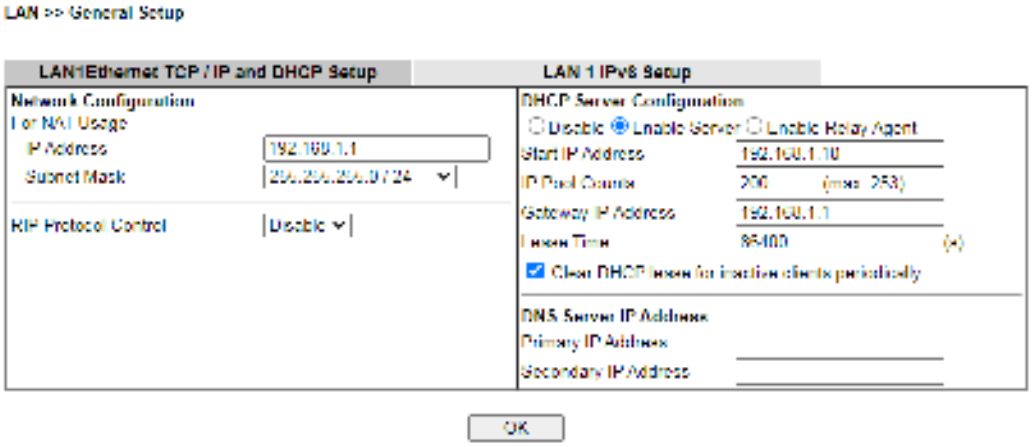
A-1 Multi-subnet Application - How to utilize Vigor router with non-NAT?



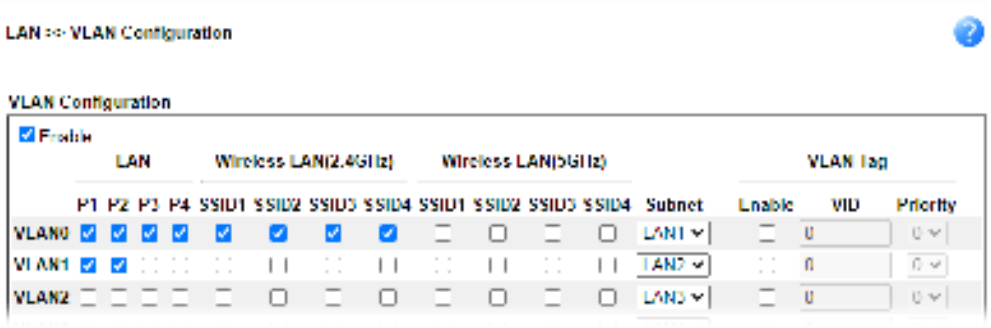
1. Open **LAN>>General Setup**. Click the **Details Page** button of LAN1.



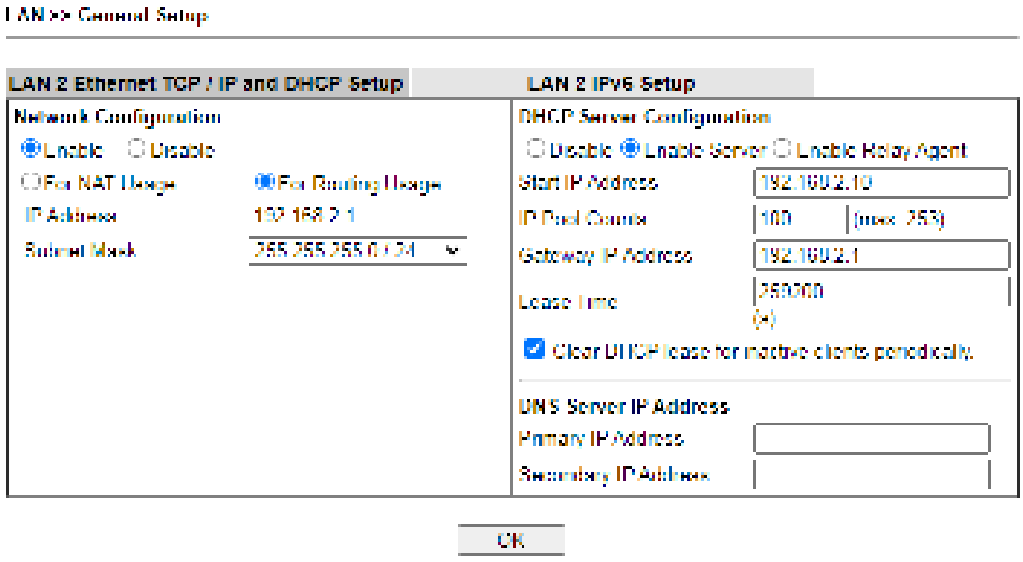
2. In the setting page, Enter the settings as follows and click **OK** to save the settings. Note that LAN1 is always for NAT usage.



3. In the setting page, Enter the settings as follows and click **OK** to save the settings. Note that LAN1 is always for NAT usage.

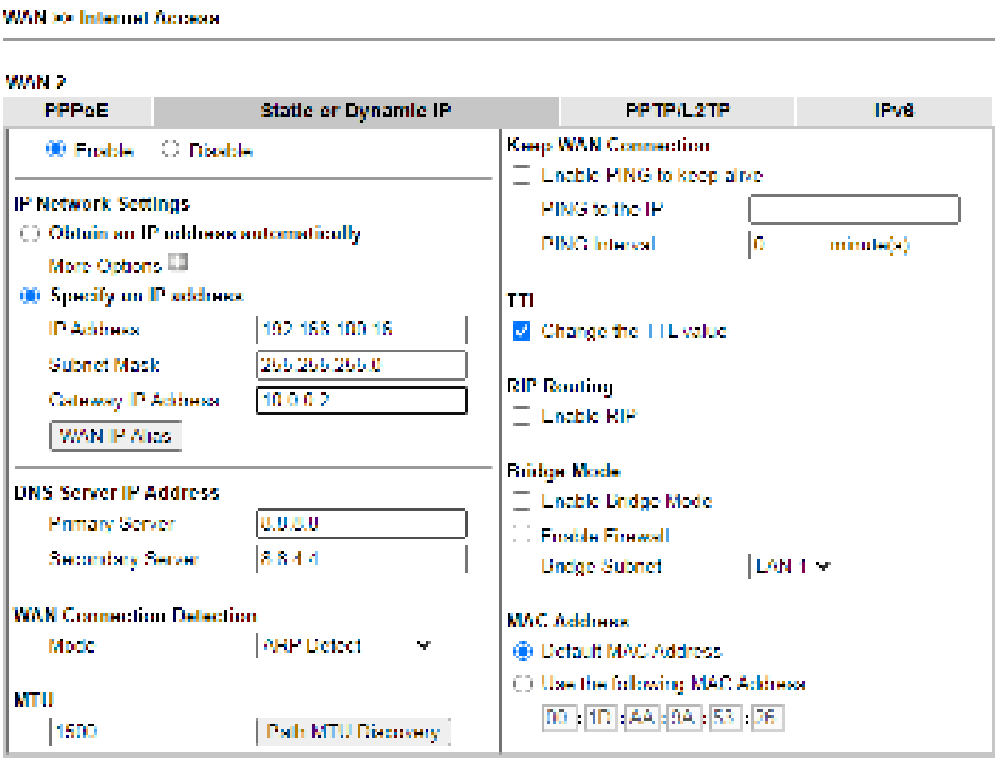


4. Return to **LAN>>General Setup**. Now, LAN2 is available for configuration. Click the **Details Page** button of LAN2. Choose **For Routing Usage**. Enter the settings as follows and click **OK** to save the settings.



5. Open **WAN>>Internet Access**. Choose **Static or Dynamic IP** as **Access Mode**. Then click **Details Page**.

6. In the configuration web page, Enter the settings as follows and click **OK** to save the settings.



7. Now, a network connection via MPLS (Multiprotocol Label Switching) between LAN2 user and the Branch user is established successfully. Internet is not required for them.

II-2-2 VLAN

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

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

Tagged VLAN

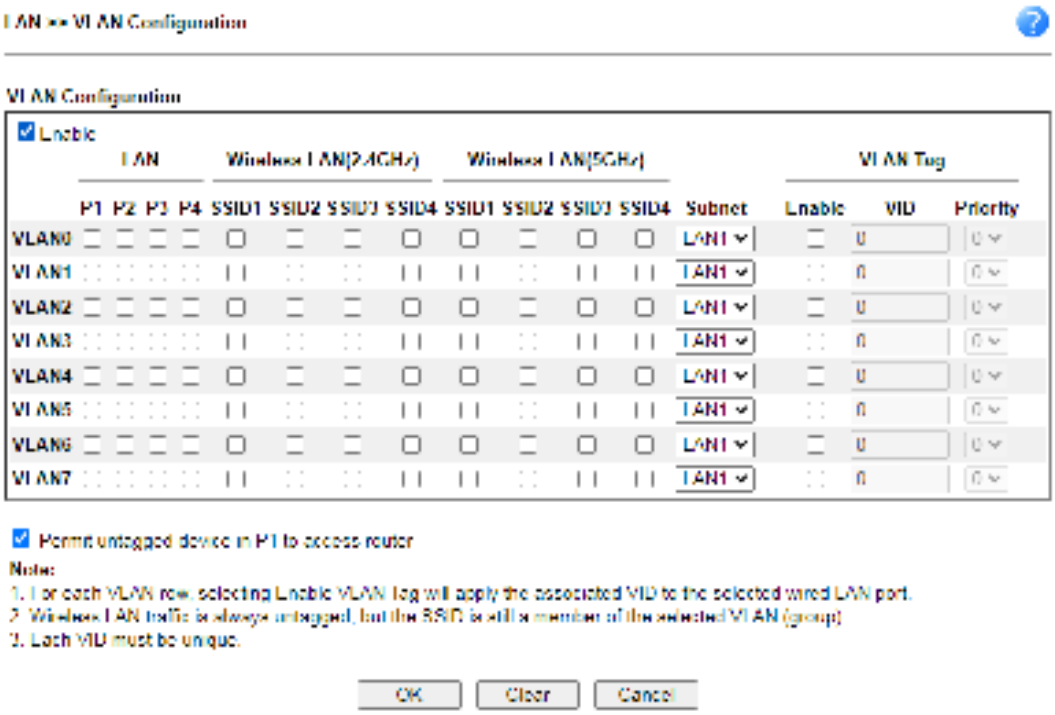
The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each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

Port-Based VLAN

Relative to tag-based VLAN which groups clients with an identifier, port-based VLAN uses physical ports (P1 ~ P4) to separate the clients into different VLAN group.

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

For Vigor router with 2.4GHz and 5GHz features, the web page will be shown as follow:



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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	**P1 – P4**– Check the LAN port(s) to group them under the selected VLAN.
Wireless LAN (2.4GHz)	**SSID1 – SSID4** – Check the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	**SSID1 – SSID4** – Check the SSID boxes to group them under the selected VLAN. This option is only available for Vigor2915ac / Vigor2915Vac / Vigor2915Lac.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
VLAN Tag	**Enable** – Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out. Please Enter the tag value and specify the priority for the packets sending by LAN. **VID** – Enter the value as the VLAN ID number. The range is

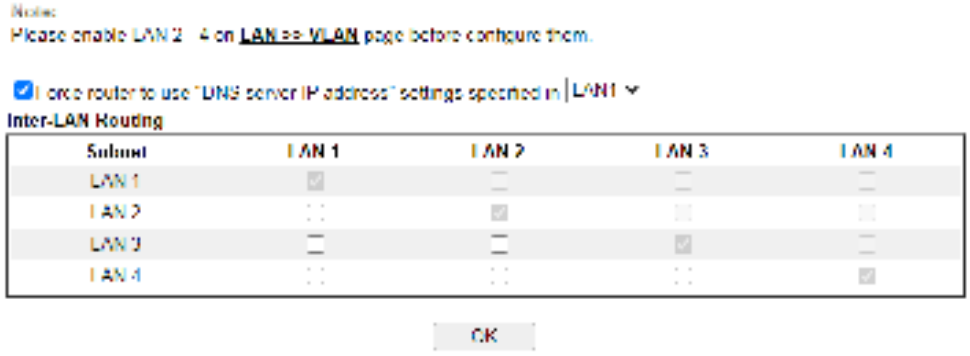
	form 0 to 4095. VIDs must be unique. **Priority** – Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority.
Permit untagged device in P1 to access router	Select to allow untagged hosts connected to LAN port P1 to access the router. In case you have incorrectly configured VLAN functionality, you will still be able to access the router via the Web UI, and telnet and SSH shells to adjust the configuration.

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

Inter-LAN Routing

The Vigor router supports up to 16 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).



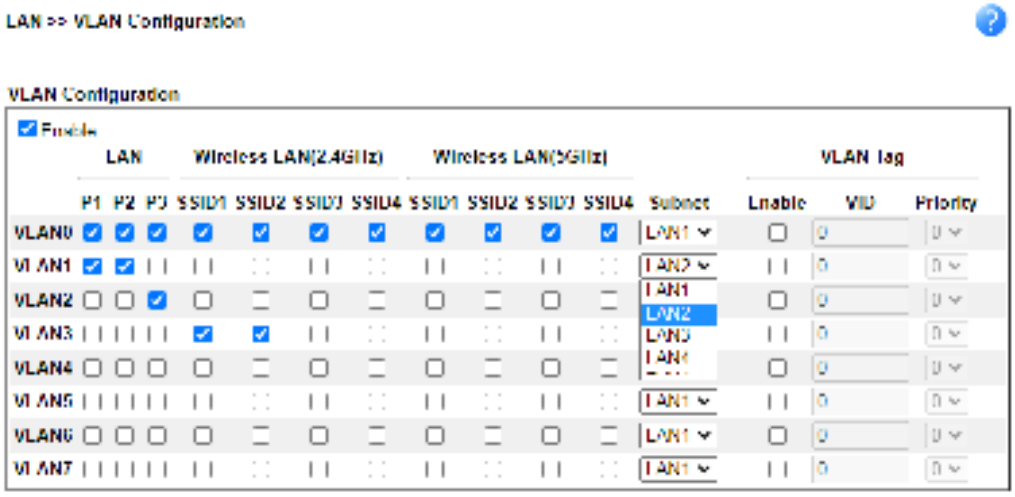
Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

Vigor2915 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

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

1. All the wire network clients are categorized to group VLAN0 in subnet 192.168.1.0/24 (LAN1).
2. All the wireless network clients are categorized to group VLAN1 in subnet 192.168.2.0/24 (LAN2).

3. Open **LAN>>VLAN Configuration**. Check the boxes according to the statement in step 1 and Step 2.



4. Click **OK**.

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

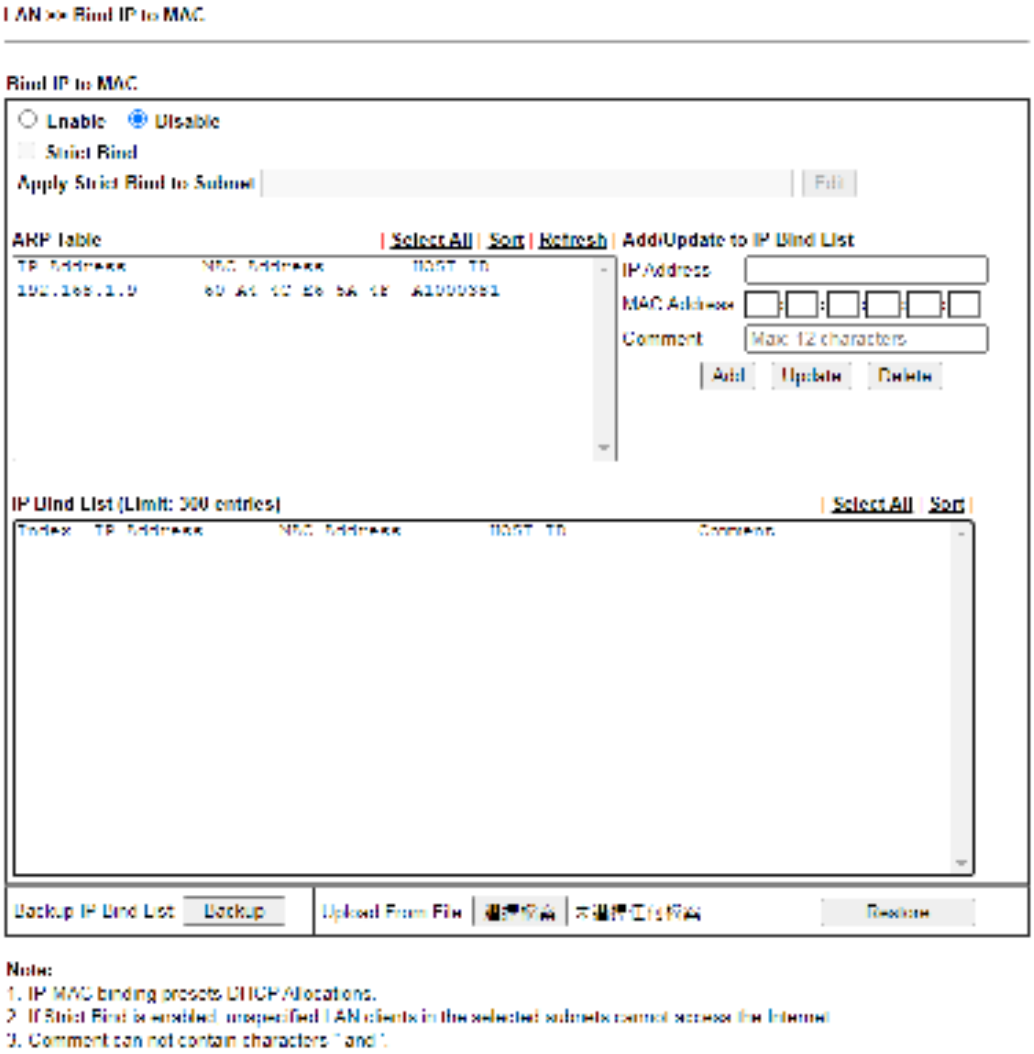
Vigor router supports up to six private IP subnets on LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

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

II-2-3 Bind IP to MAC

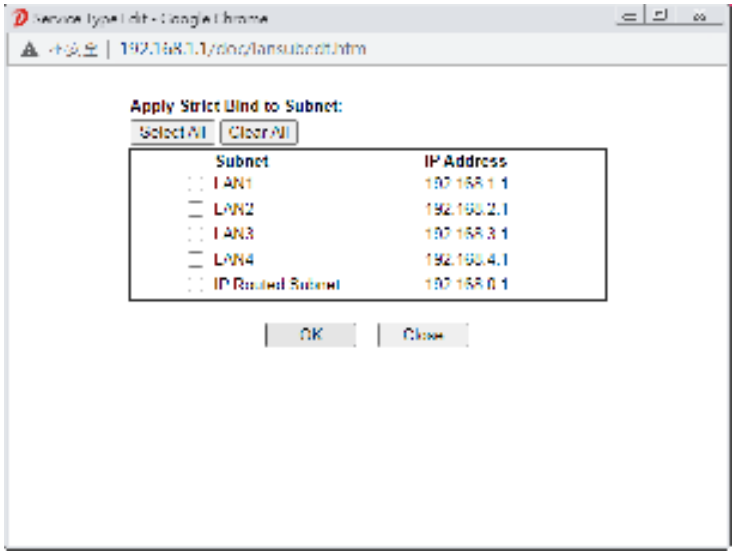
This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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



Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Check the box to block the connection of the IP/MAC which is not listed in IP Bind List. LAN clients will be assigned IP addresses according to the MAC-to-IP address associations on this page. LAN client whose MAC address has not been bound to an IP address will be denied network access.

	Note: Before selecting **Strict Bind**, make sure at least one valid MAC address has been bound to an IP address. Otherwise no LAN clients will have network access, and it will not be possible to connect to the router to make changes to its configuration. **Apply Strict Bind to Subnet** – Choose the subnet(s) for applying the rules of Bind IP to MAC. 
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Select All	Select all entries in the ARP Table for manipulation.
Sort	Reorder the entry based on the IP address.
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add/Update to IP Bind List	**IP Address** – Enter the IP address to be associated with a MAC address. **Mac Address** – Enter the MAC address of the LAN client's network interface. **Comment** – Type a brief description for the entry.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.
Update	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.
IP Bind List	It displays a list for the IP bind to MAC information.
Backup IP Bind List	Click **Backup** and enter a filename to back up IP Bind List to a file.
Upload From File	Click **Browse…** to select an IP Bind List backup file. Click **Restore** to restore the backup and overwrite the existing list.

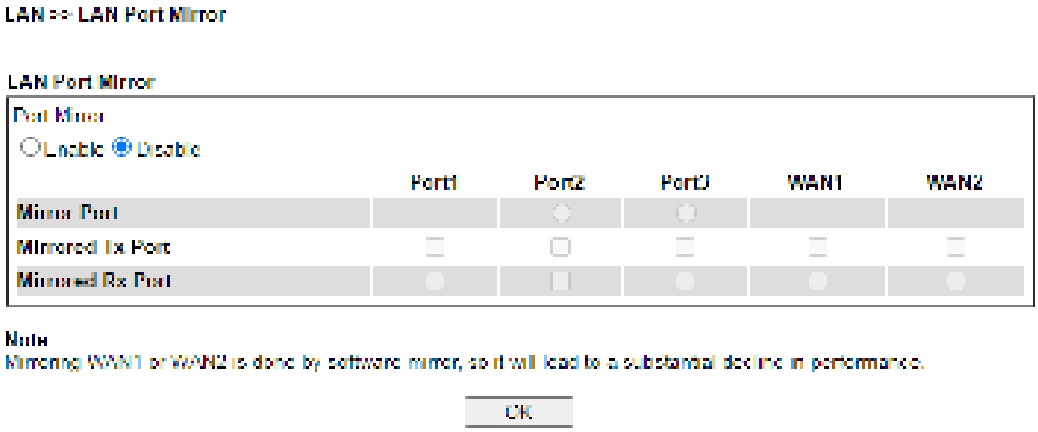
Info	Before you select Strict Bind, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

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

II-2-4 LAN Port Mirror

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

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



Available settings are explained as follows:

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

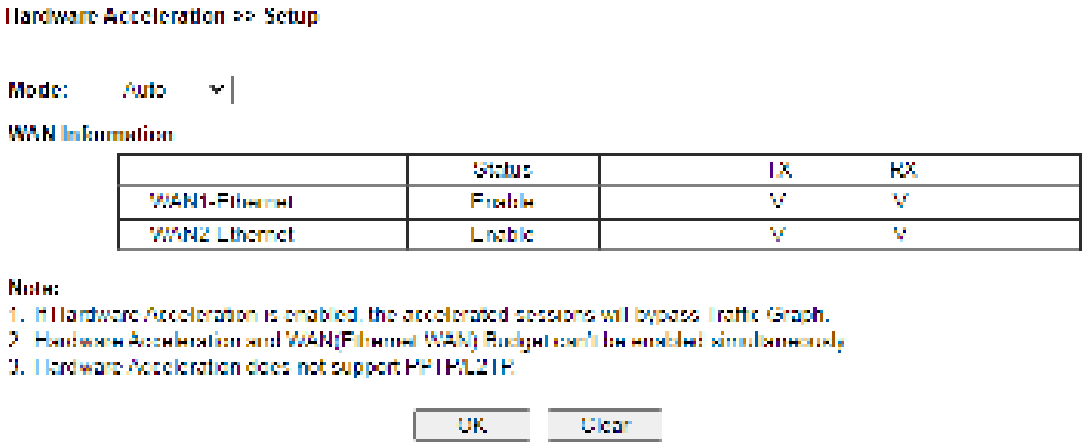
After finishing all the settings here, please click **OK** to save the configuration.

II-3 Hardware Acceleration

Hardware Acceleration is also called **PPA** in DrayTek for it is based on **Protocol Processing Engine (PPE)** of Infineon. It can only support 128 sessions for network traffic (IN & OUT) with implementing three kinds of modes - Disable, Auto and Manual.

II-3-1 Setup

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself. Open **Hardware Acceleration** to access into the following page:

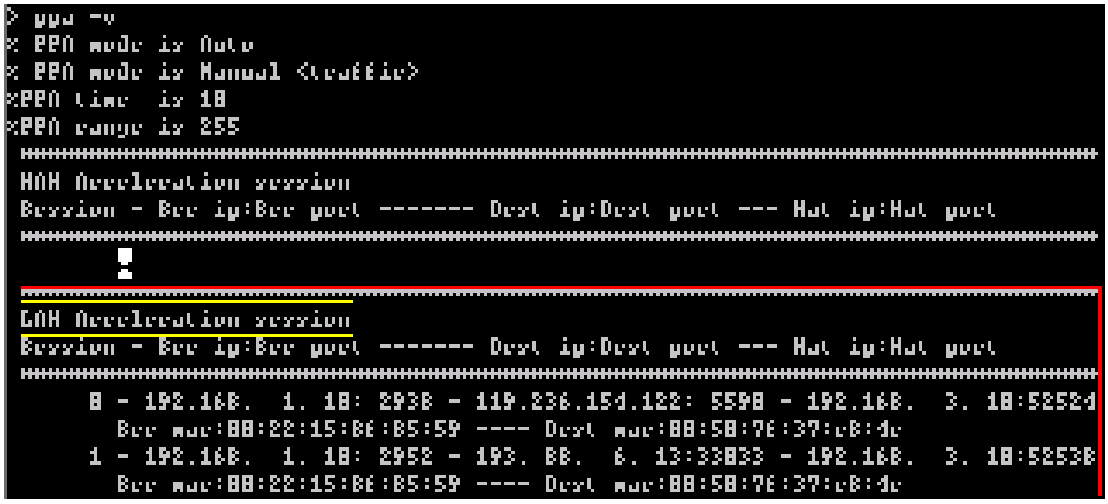


Available settings are explained as follows:

Item	Description
Mode	**Disable –** The default setting. **Auto -** When the hardware acceleration is configured with the **Auto** mode, the sessions with the heaviest loading and the lower latency traffic will be added into PPA. However, the Auto mode does not support UDP protocol by designed.

Checking the PPA status

For checking whether the rule of PPA is working or not, a user can login to Vigor2915 series by using telnet. User can view how many sessions are transferring in each direction of PPA table after entering "**`ppa -v`**".


> ppa -v
% PPA mode is Auto
% PPA mode is Manual <traffic>
%PPA time is 10
%PPA range is 255
NAT Acceleration session
Session - Ser ip:Ser port ------- Dest ip:Dest port --- Nat ip:Nat port
LAN Acceleration session
Session - Ser ip:Ser port ------- Dest ip:Dest port --- Nat ip:Nat port
0 - 192.168. 1. 10: 2938 - 119.236.151.122: 5598 - 192.168. 3. 10:52524
Ser mac:00:22:15:BE:B5:59 ---- Dest mac:00:50:7F:37:C8:4C
1 - 192.168. 1. 10: 2952 - 193. 88. 6. 13:33833 - 192.168. 3. 10:52538
Ser mac:00:22:15:BE:B5:59 ---- Dest mac:00:50:7F:37:C8:4C

II-4 NAT

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

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

The benefit of the NAT includes:

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

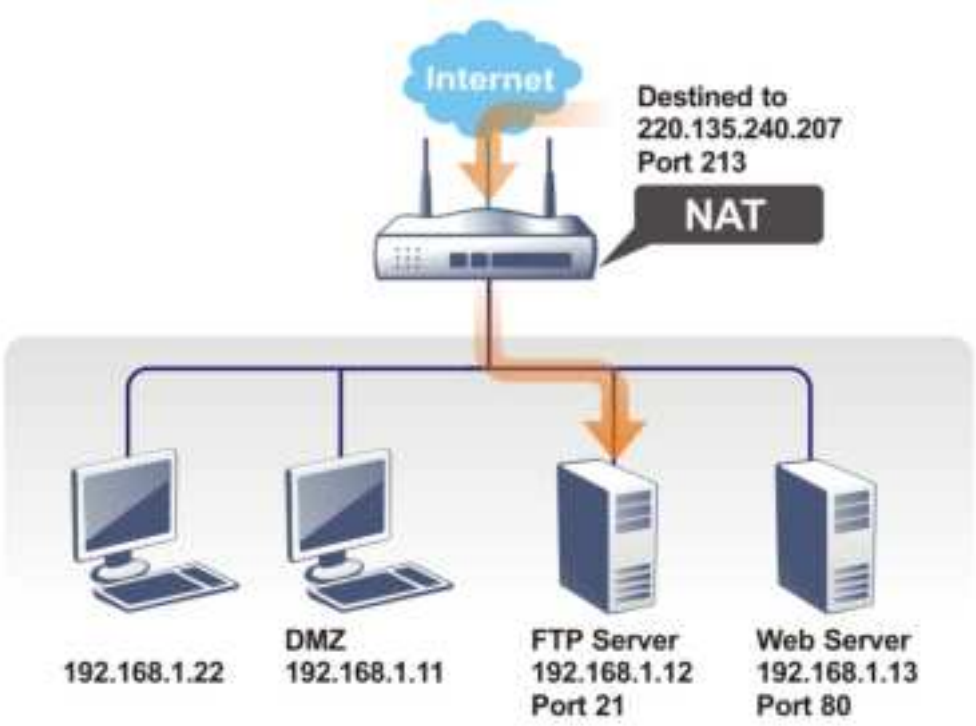
Info

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

Web User Interface

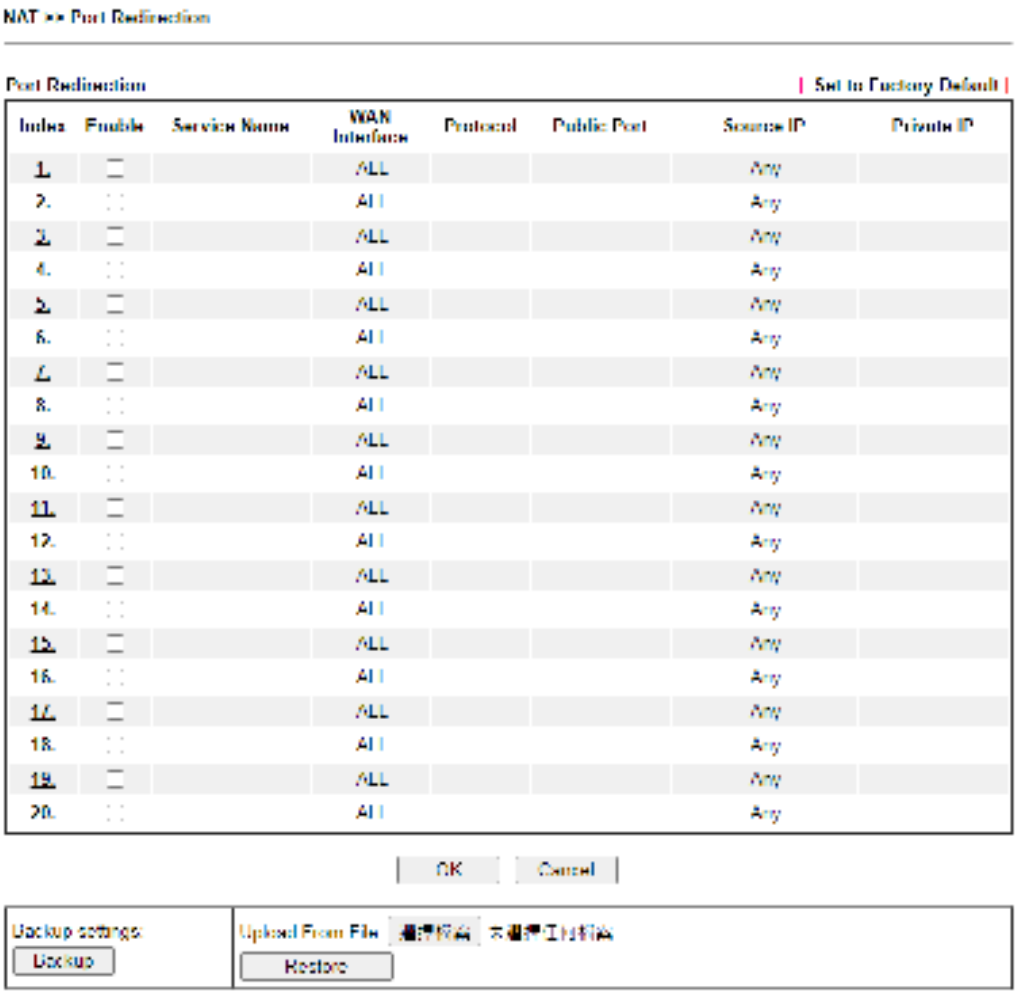
II-4-1 Port Redirection

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



The port redirection can only apply to incoming traffic.

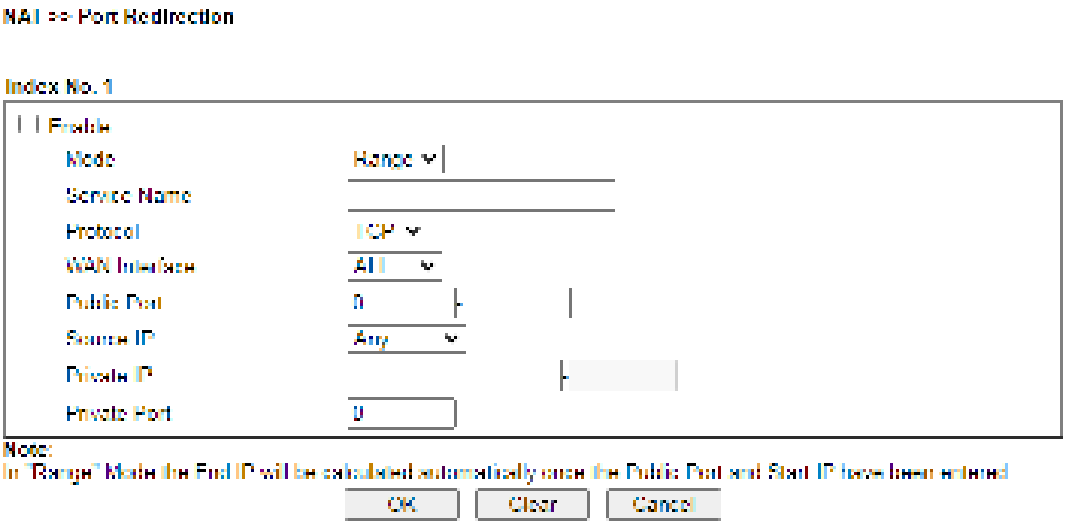
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 40 port-mapping entries for the internal hosts.



Each item is explained as follows:

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

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



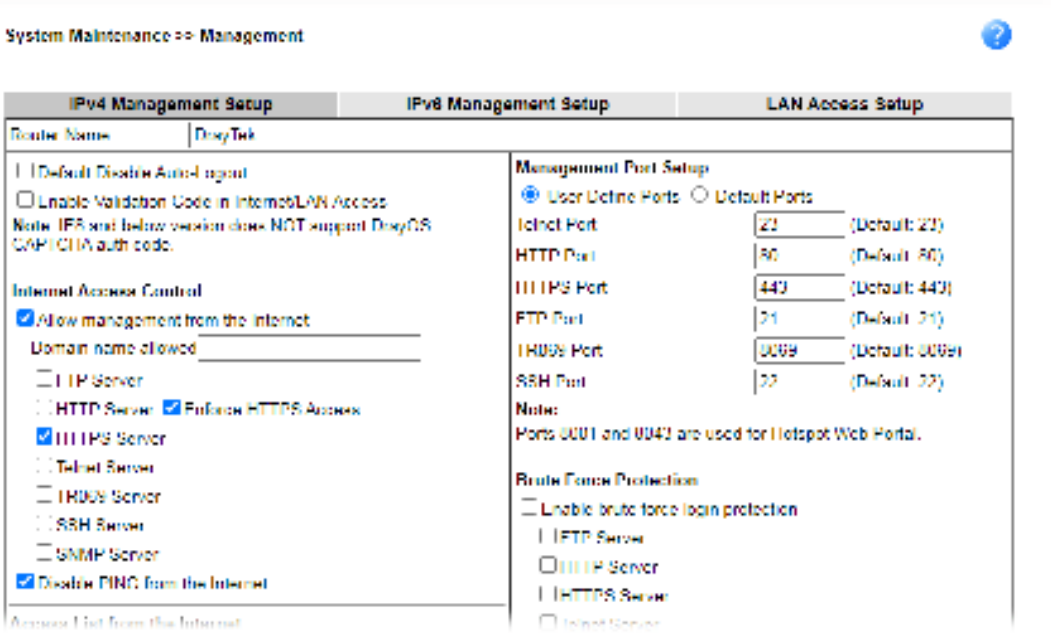
Available settings are explained as follows:

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

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

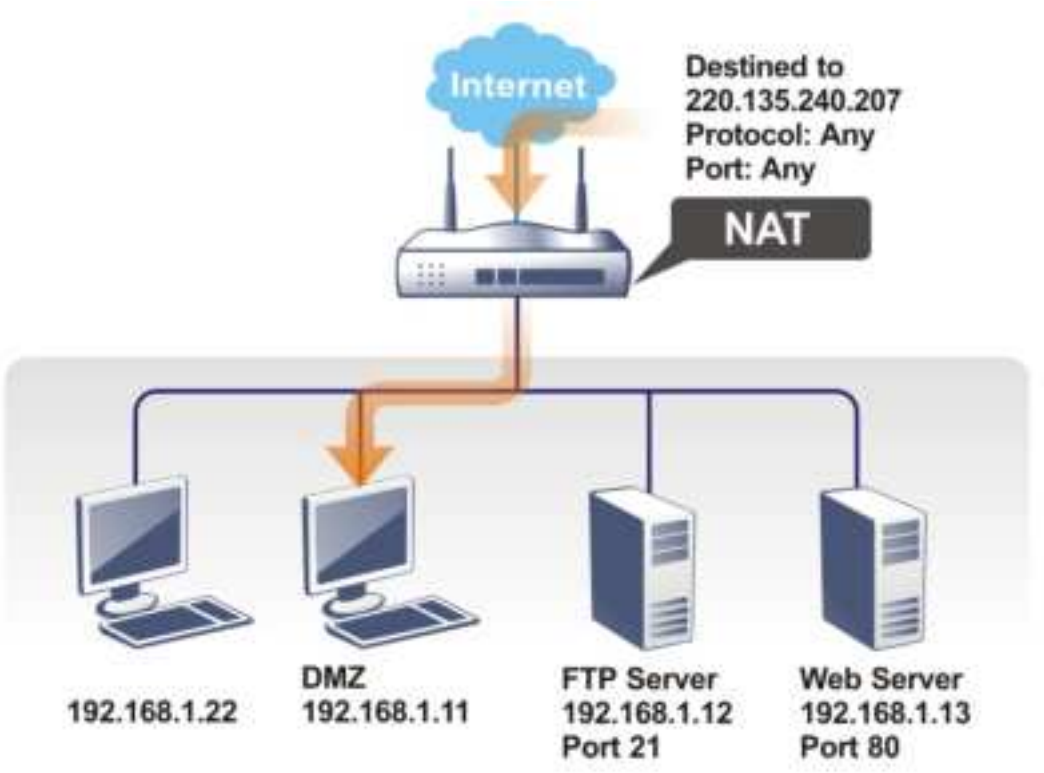
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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



II-4-2 DMZ Host

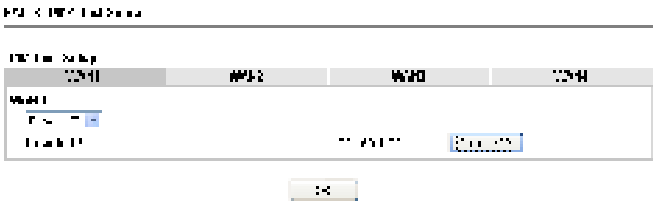
As mentioned above, **Port Redirection** can redirect incoming TCP/ UDP or other traffic on particular ports to the specific private IP address/ port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility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



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

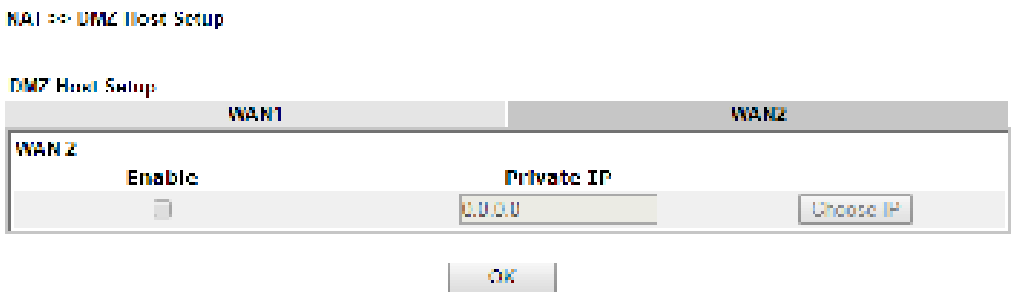
Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.

Available settings are explained as follows:

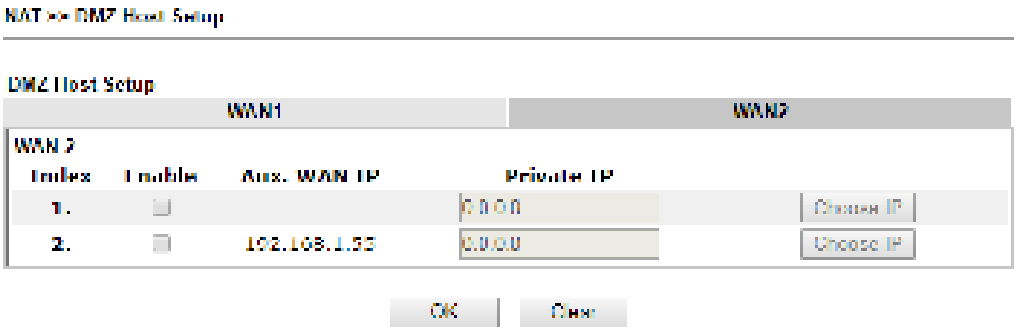
Item	Description
WAN1	Choose **Private IP** or **None** first.
Private IP	Enter the private IP address of the DMZ host, or click Choose IP to select one.
Choose IP	Click this button and then a window will automatically pop up. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting. 

DMZ Host for WAN2 is slightly different with WAN1.

See the following figure.



If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2 interface, you will find them in **Aux. WAN IP** for your selection.



Available settings are explained as follows:

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

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

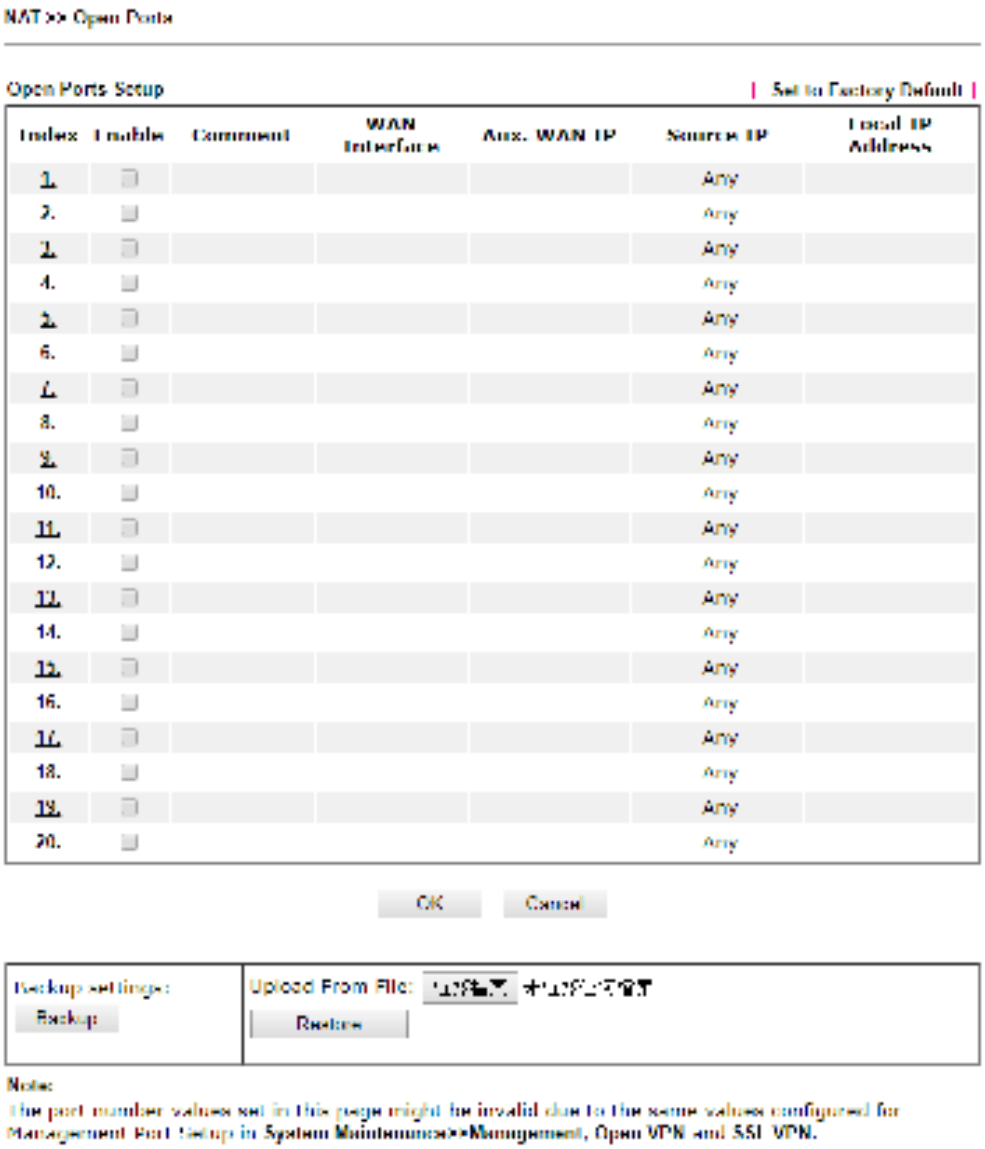
After finishing all the settings here, please click **OK** to save the configuration.

II-4-3 Open Ports

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

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

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

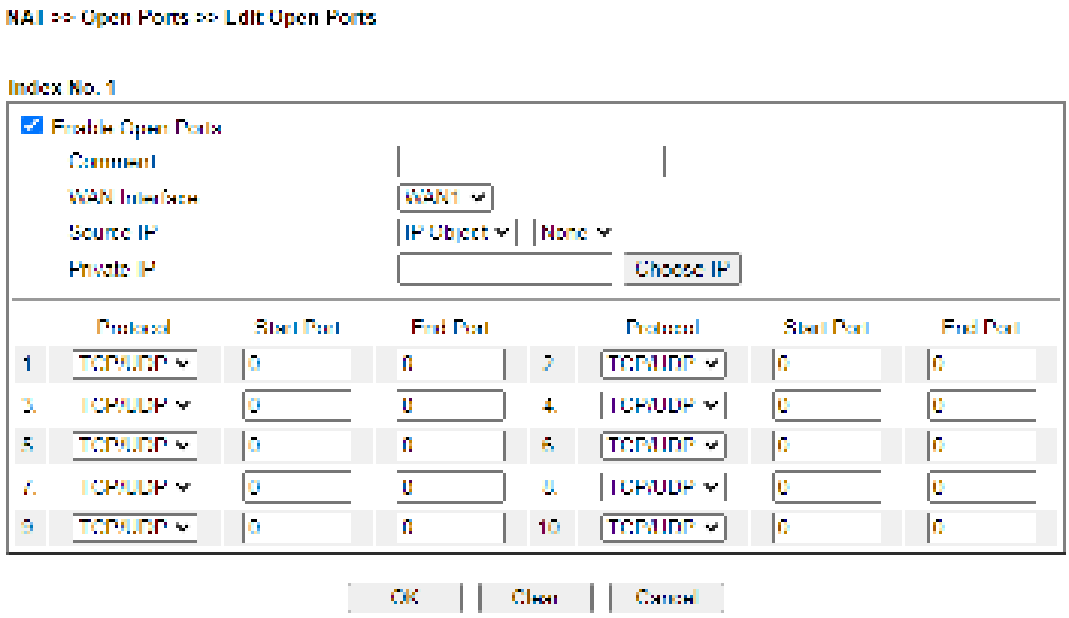


Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Enable	Check the box to enable the open port profile.
Comment	Specify the name for the defined network service.

WAN Interface	Display the WAN interface used by such index.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
Source IP	Display the IP object of the source IP.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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



Available settings are explained as follows:

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

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

II-4-4 Port Triggering

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.

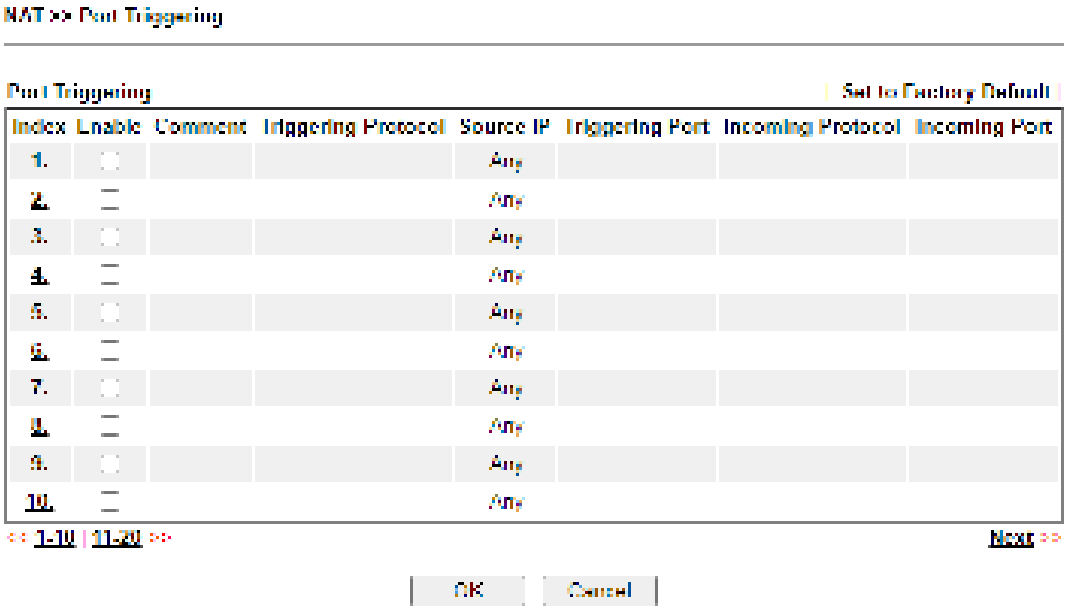
  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

  TCP SYN: 60 sec.

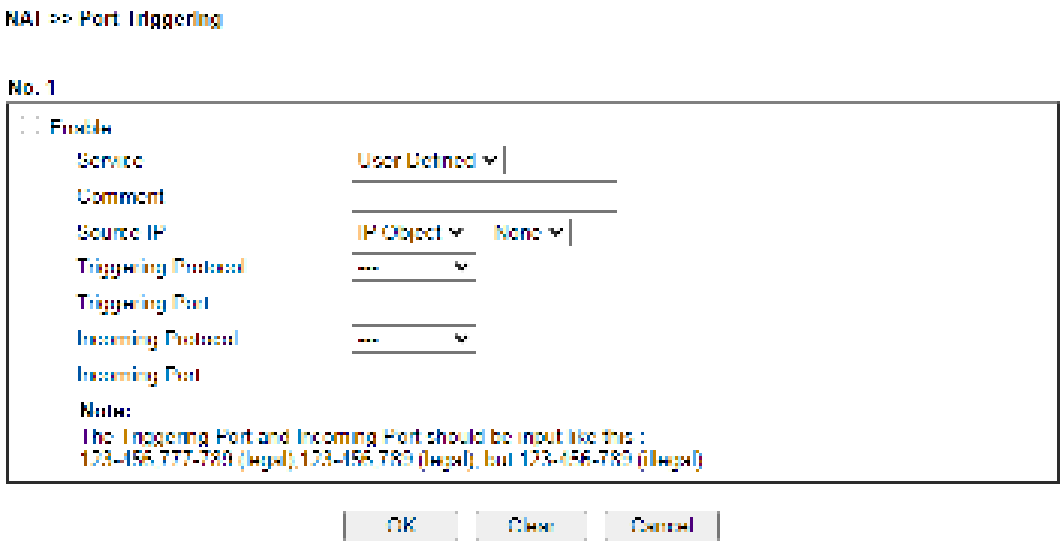


Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the port triggering profile. You should click the appropriate index number to edit or clear the corresponding entry.
Enable	Check the box to enable the Port Triggering profile.
Comment	Display the text which memorizes the application of this rule.
Triggering Protocol	Display the protocol of the triggering packets.
Triggering Port	Display the port of the triggering packets.
Source IP	Display the name of the IP object.

Incoming Protocol	Display the protocol for the incoming data of such triggering profile.
Incoming Port	Display the port for the incoming data of such triggering profile.

Click the index number link to open the configuration page.



Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the **predefined** service to apply for such trigger profile.
Comment	Enter the text to memorize the application of this rule.
Source IP	Use the drop down list to specify an IP object. Or click IP Object link to create a new one for applying.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.
Triggering Port	Enter the port or port range for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.
Incoming Port	Enter the port or port range for the incoming packets.

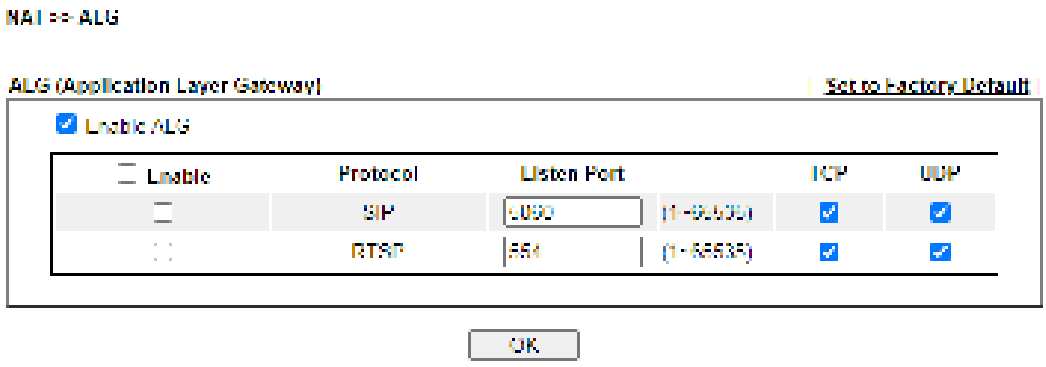
After finishing all the settings here, please click **OK** to save the configuration.

II-4-5 ALG

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

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

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



Available settings are explained as follows:

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

II-5 Applications

Dynamic DNS

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

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

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 Vigor2915 series will respond the specified private IP address.

Schedule

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

RADIUS

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

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

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

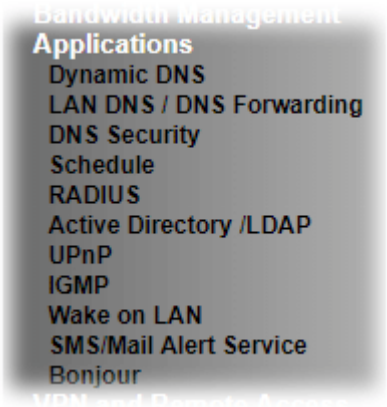
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on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

Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** (WOL) of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.

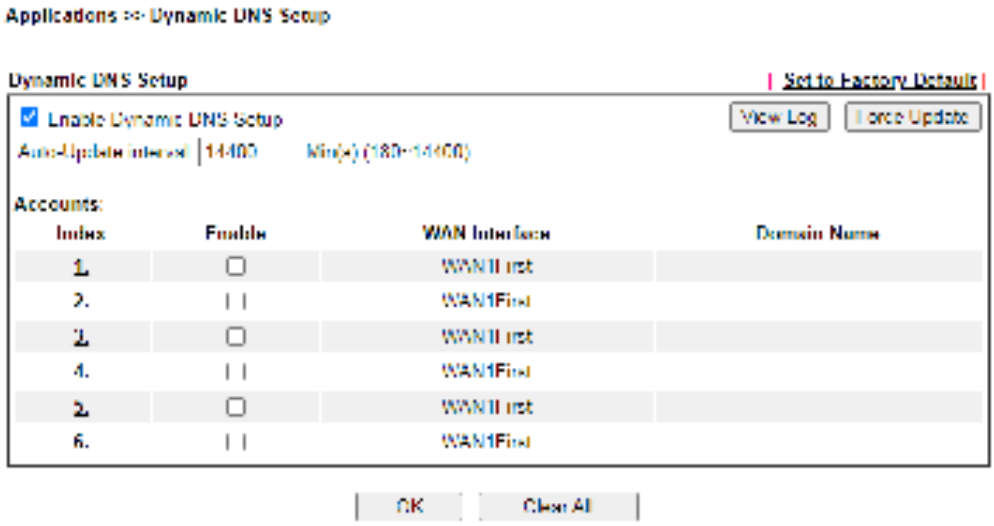
Web User Interface



II-5-1 Dynamic DNS

Enable the Function and Add a Dynamic DNS Account

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

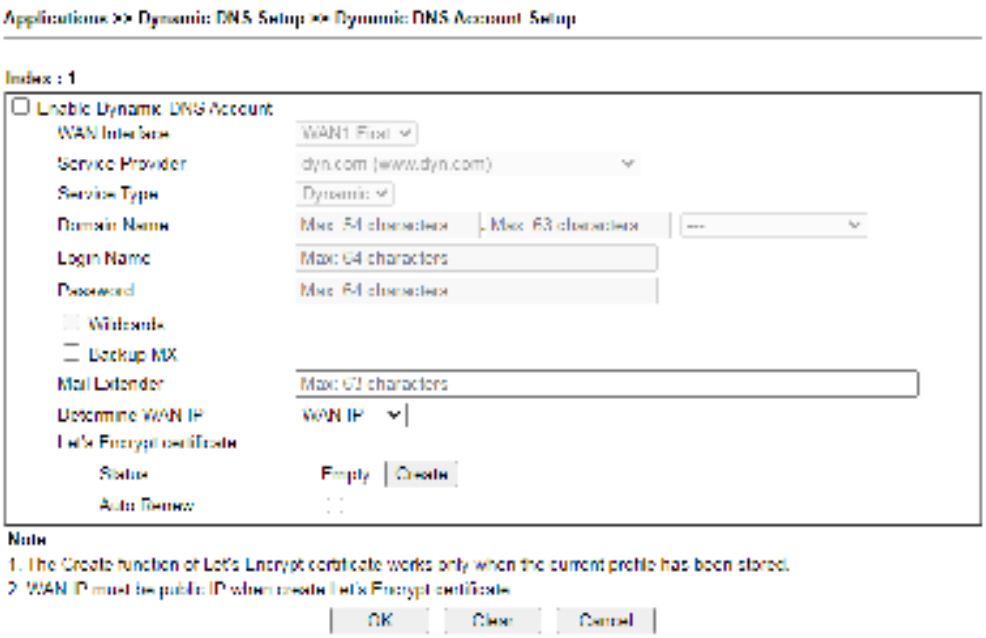


Available settings are explained as follows:

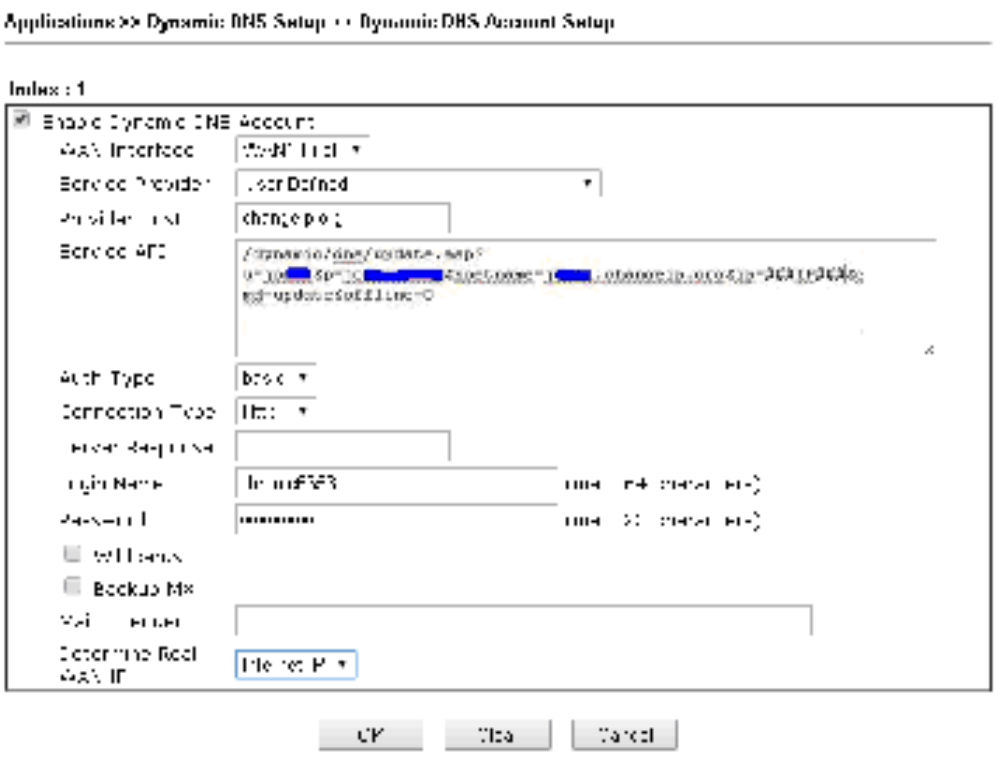
Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Enable	Check the box to enable such account.
WAN Interface	Display the WAN interface used.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

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



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



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	**WAN1/WAN2 First** - While connecting, the router will use WAN1/WAN2 as the first channel for such account. If WAN1/WAN2 fails, the router will use another WAN interface instead. **WAN1/WAN2 Only** - While connecting, the router will use WAN1/WAN2 as the only channel for such account.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. Note that such option is not available when User-Defined is selected as Service Provider.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain. Note that such option is not available when User-Defined is selected as Service Provider.
Provider Host	Enter the IP address or the domain name of the host which provides related service. Note that such option is available when User-Defined is selected as Service Provider.
Service API	Enter the API information obtained from DDNS server. Note that such option is available when User-Defined is selected as Service Provider. (e.g:

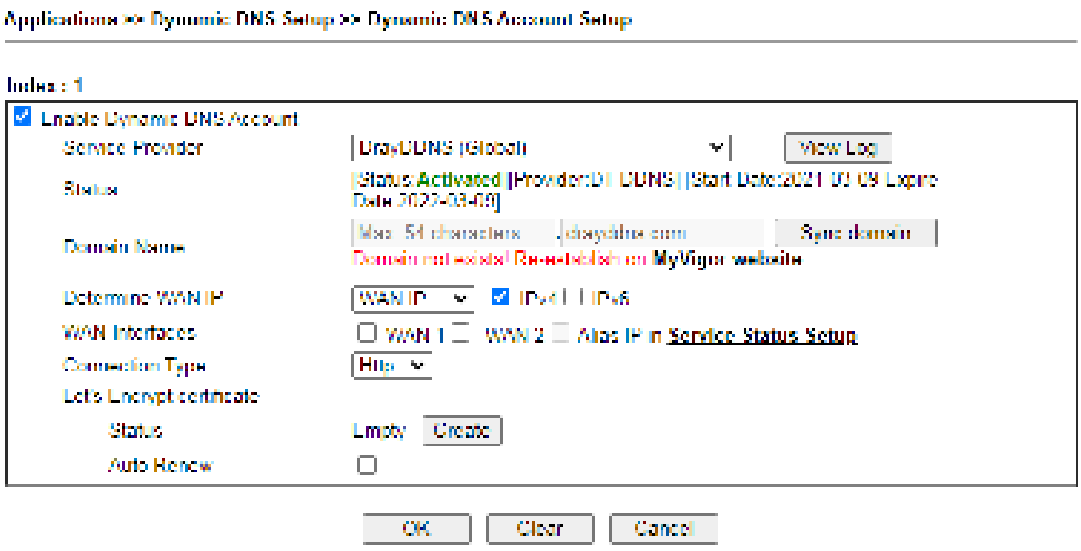
	/dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j*****.changeip.org&ip=###IP### &cmd=update&offline=0)
Auth Type	Two types can be used for authentication. **Basic** – Username and password defined later can be shown from the packets captured. **URL** - Username and password defined later can be 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 User-Defined 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 User-Defined is selected as Service Provider.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
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** - 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.
Let's Encrypt certificate	**Create** – Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account. **Auto Update** – Check the box to make the system update the certificate automatically.

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

DrayDDNS Settings

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

Choose **DrayTek Global** as the service provider, the web page will be displayed as follows:



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Choose **DrayTek Global** as the service provider. **Wizard** – This button is available when DrayTek Global is selected as Service Provider. To activate the DrayTek's DDNS service, click it to enable license issued by DrayTek through **Wizards>>Service Activation Wizard**. Refer to secion **A-1 How to use DrayDDNS?** for detailed information.
Status	Display if the license is actvtaed or not.
Determine WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: ● **WAN IP** - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. ● **Internet IP** – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.
WAN Interfaces	**WAN1**/**WAN2** - While connecting, the router will use WAN1/ WAN2 as the channel for such account.
Connection Type	Choose **Http** or **Https**.
Let's Encrypt certificate	**Status** – Click the link to display the certificate information. **Auto Renew** – Check the box to make the system update the certificate automatically.

Disable the Function and Clear all Dynamic DNS Accounts

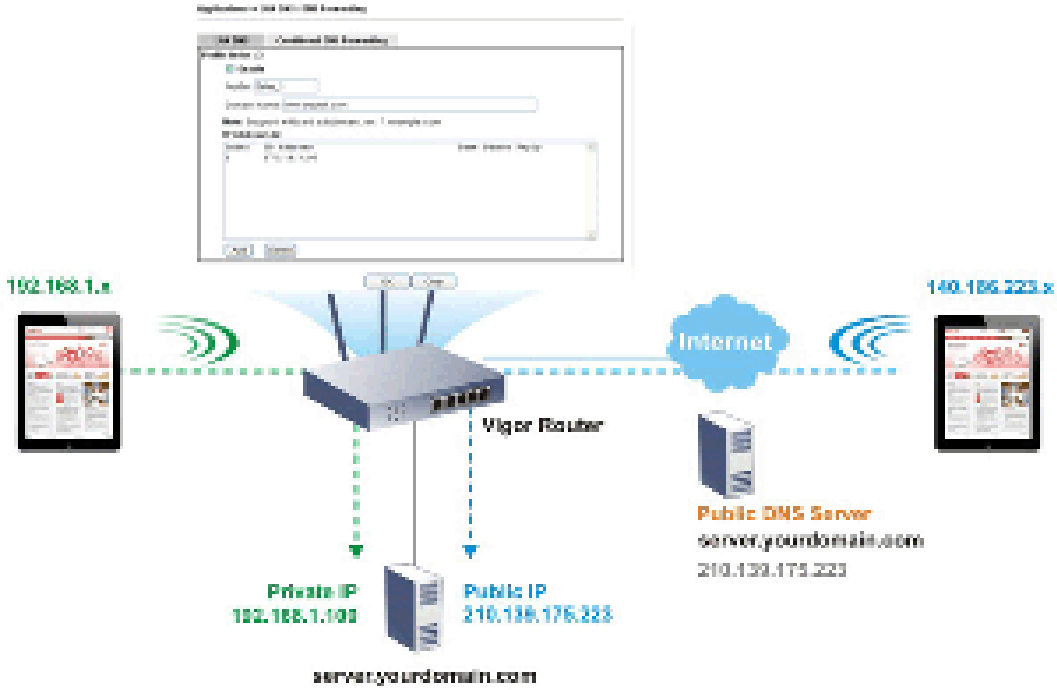
Uncheck **Enable Dynamic DNS Setup**, and click **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

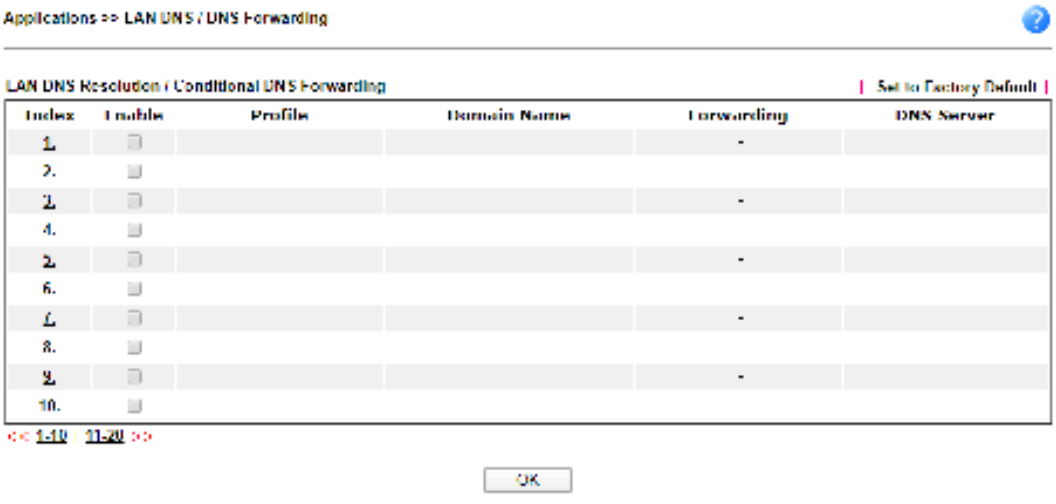
Click the **Index** number you want to delete and then click **Clear All** button to delete the account.

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 Vigor2915 series will respond the specified private IP address.



Simply click **Application>>LAN DNS / DNS Forwarding** to open the following page.

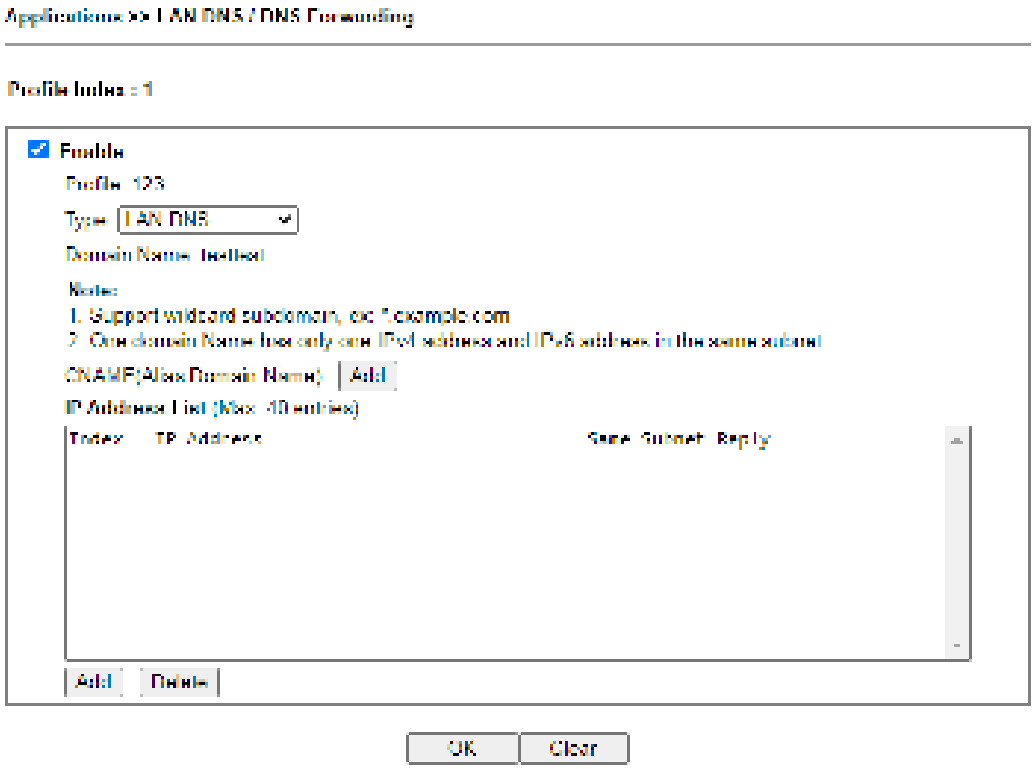


Each item is explained as follows:

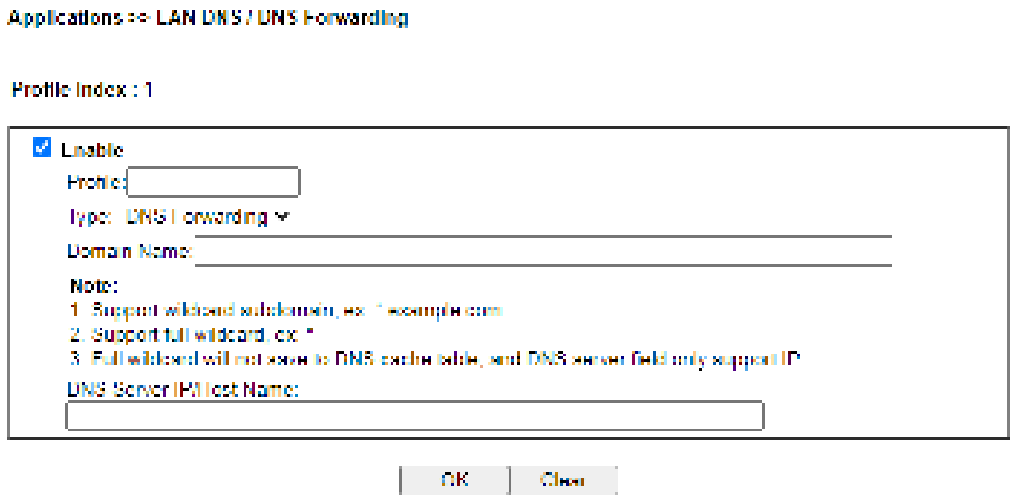
Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page.
Enable	Check the box to enable the selected profile.

Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.
Forwarding	Display that such profile is conditional DNS forwarding or not.
DNS Server	Display the IP addres of the DNS Server.

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

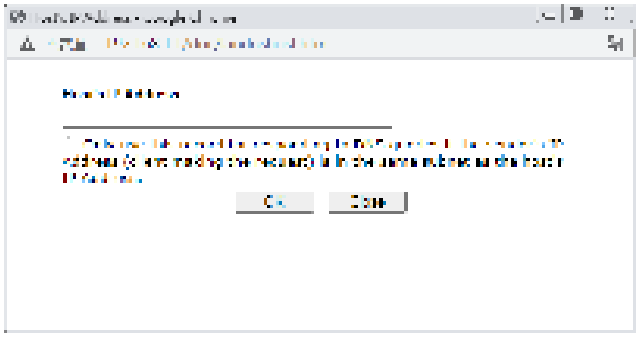


Or,



Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.

Profile	Type a name for such profile. **Note:** If you type a name here for LAN DNS and click **OK** to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Type	Select LAN DNS or DNS 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 responds to the DNS...** – 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 / Host Name -** Enter the IP address of the DNS server or the host name 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

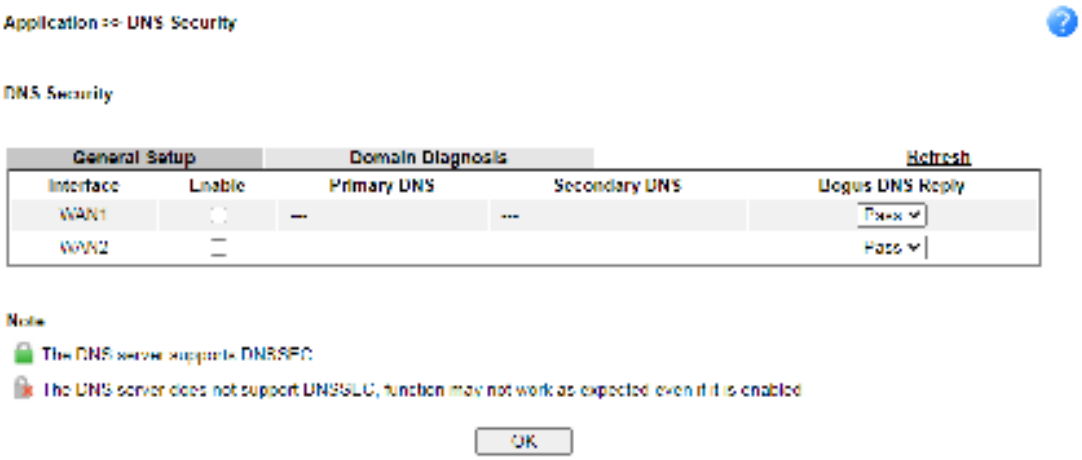
Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

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.

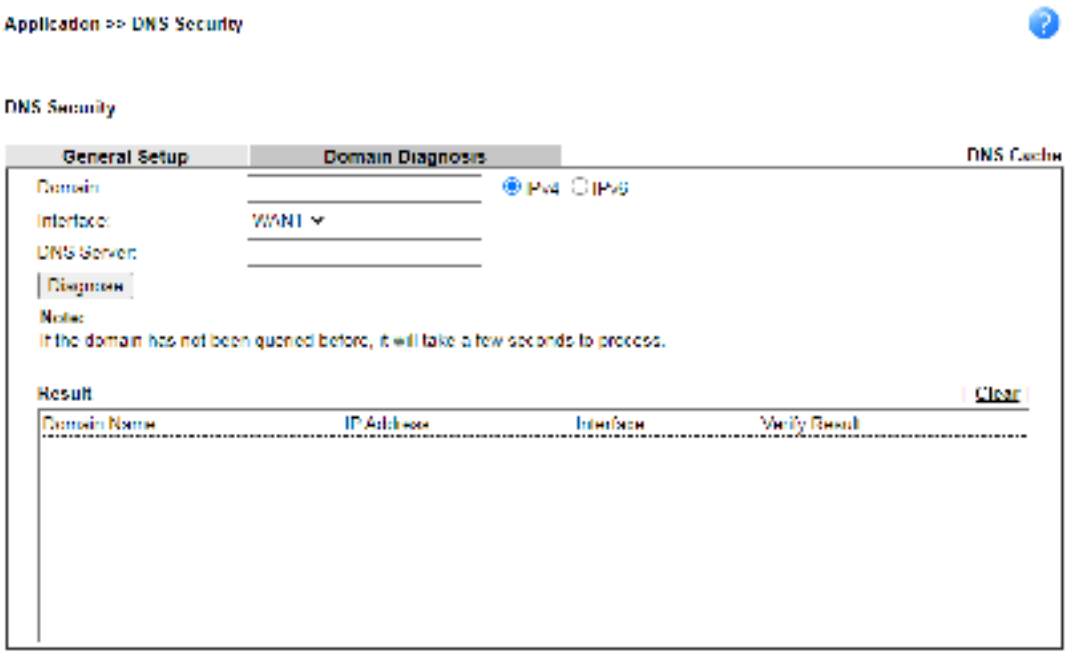


Available settings are explained as follows:

Item	Description
Interface	There are four WAN interfaces allowed to be set with DNS security enabled.
Enable	Check the box to enable the DNS security management.
Primary DNS	Display the IP address of primary DNS obtained from DHCP server or specified by Static WAN.
Secondary DNS	Display the IP address of secondary DNS obtained from DHCP server or specified by Static WAN.
Bogus DNS Reply	Sometime, Vigor router might encounter packets from bogus DNS inquiry. There are two ways to reply such DNS inquiry. **Drop** – Discard the packets. **Pass** – Accept the packets and let them pass through Vigor router.

II-5-3-2 Domain Diagnose

This page is used to configure settings for manually detecting if the domain is secure not.



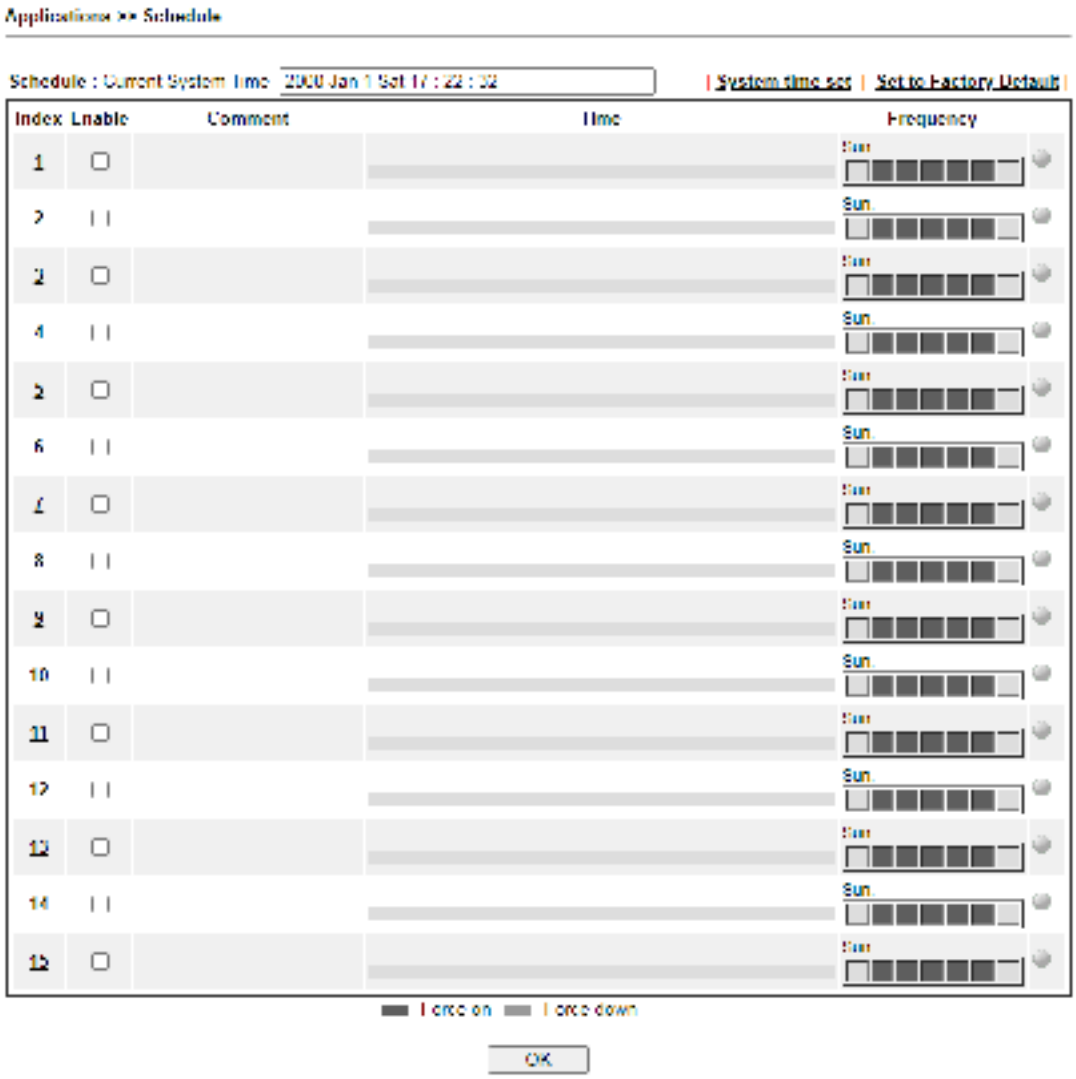
Available settings are explained as follows:

Item	Description
Domain	Enter the domain name or IP address (IPv4/ IPv6) that you want to query.
Interface	Specify the interface required for executing diagnose.
DNS Server	Enter the IP address of the DNS Server which will diagnose the domain specified above.
Diagnose	Click it to perform the diagnosis for the domain.
Result	The diagnosed information will be displayed on such field.

II-5-4 Schedule

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

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



Available settings are explained as follows:

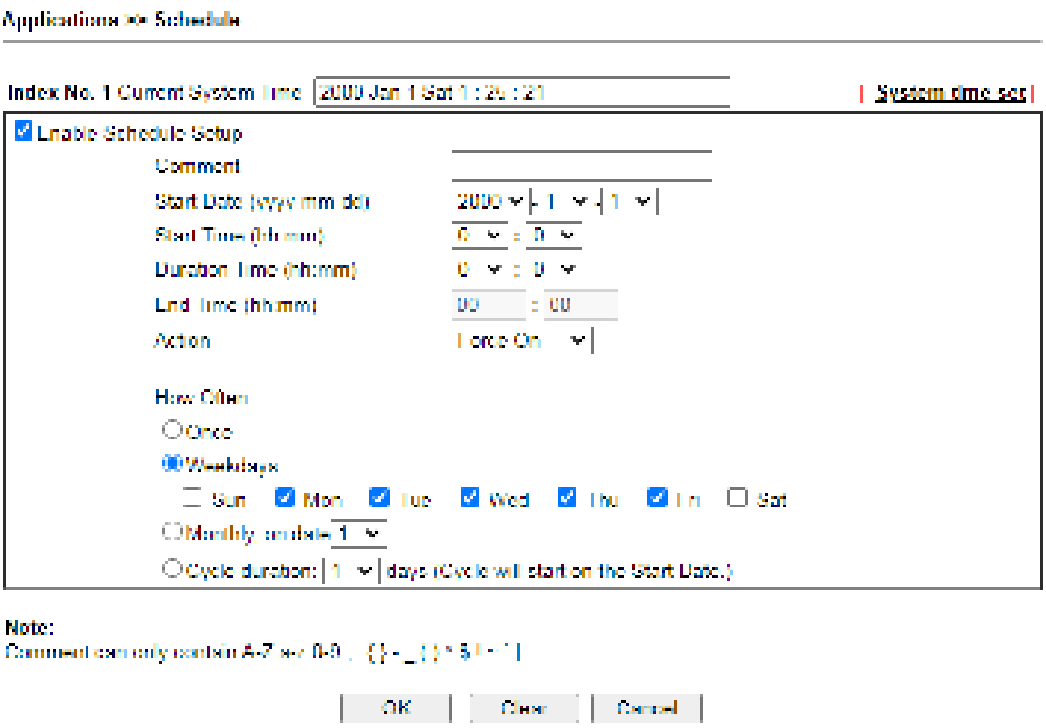
Item	Description
Current System Time	Display the time Vigor router used.
System time set	Click it to acess into the time setup page (System Maintenance>>Time and Date).
Set to Factory Default	Clear all profiles and recover to factory settings.

Index	Click the index number link to access into the setting page of schedule.
Enable	Click the box to enable such schedule profile.
Comment	Display the name of the time schedule.
Time	Display the valid time period by time bar.
Frequency	Display which day(s) will be always on and which day(s) will be always off of the schedule profile by color boxes. - If it lights in green, it means such schedule is active.

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

To add a schedule:

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



Available settings are explained as follows:

Item	Description
Enable Schedule Setup	Check to enable the schedule.
Comment	Type a short description for such schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
End Time (hh:mm)	It will be calculated automatically when Start Time and Duration Time are configured well.

Action	Specify which action should be applied during the period of the schedule. **Force On -**Force the connection to be always on. **Force Down -**Force the connection to be always down.
How Often	Specify how often the schedule will be applied. ● **Once -**The schedule will be applied just once ● **Weekdays -**Specify which days in one week should perform the schedule. ● **Monthly, on date –** The router will only execute the action applied such schedule on the date (1 to 28) of a month. ● **Cycle duration –** Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date.

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

Example

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

Office Hour:

(Force On)

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

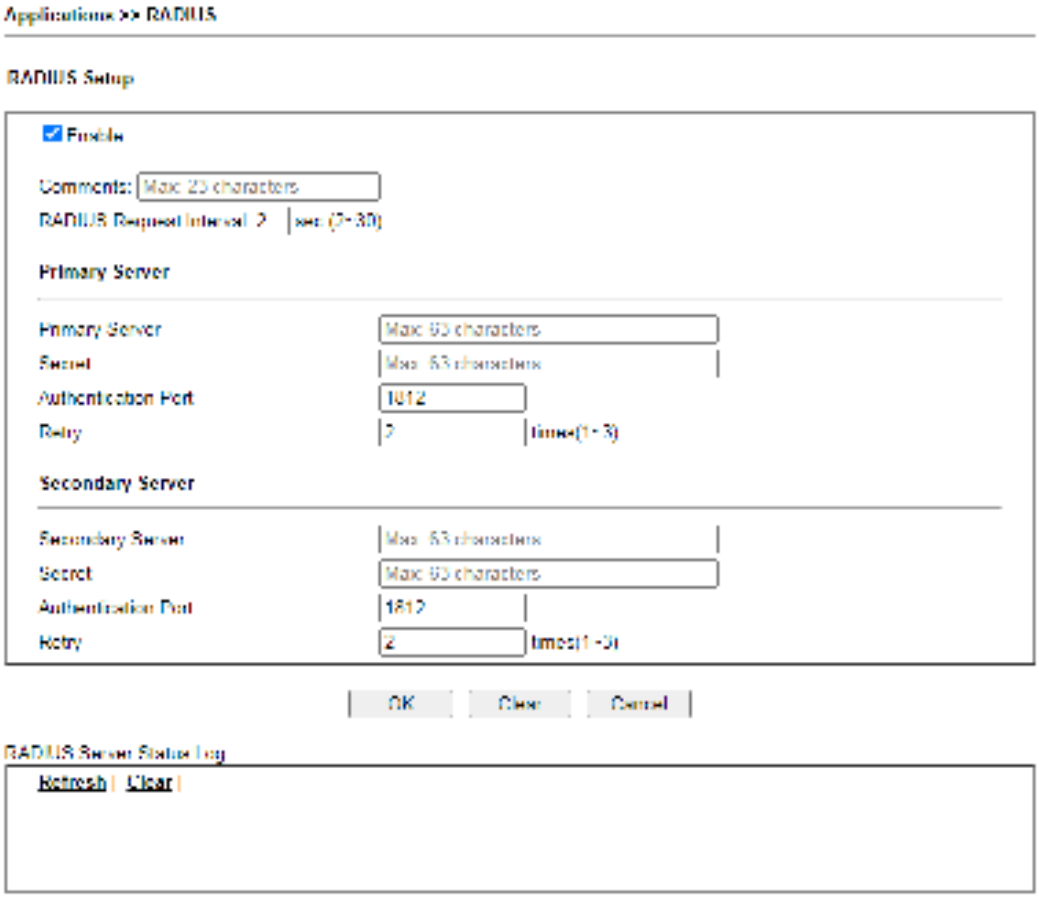
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet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

II-5-5 RADIUS

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

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

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



Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature.
Comments	Enter a brief description.
RADIUS Request Interval	Set a timeout value for the router waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again.
Primary Server	**Primary Server** - Enter the IP address of 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** - Enter a times number for sending the access request to the RADIUS server. When reaching the threshold of retry number, Vigor system will switch and send the request to the other RADIUS server (e.g., 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** - Enter a times number for sending the access request to the RADIUS server. When reaching the threshold of retry number, Vigor system will switch and send the request to the primary RADIUS server.
RADIUS Server Status Log	Display the record of current status of RADIUS server.

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

II-5-6 Active Directory/LDAP

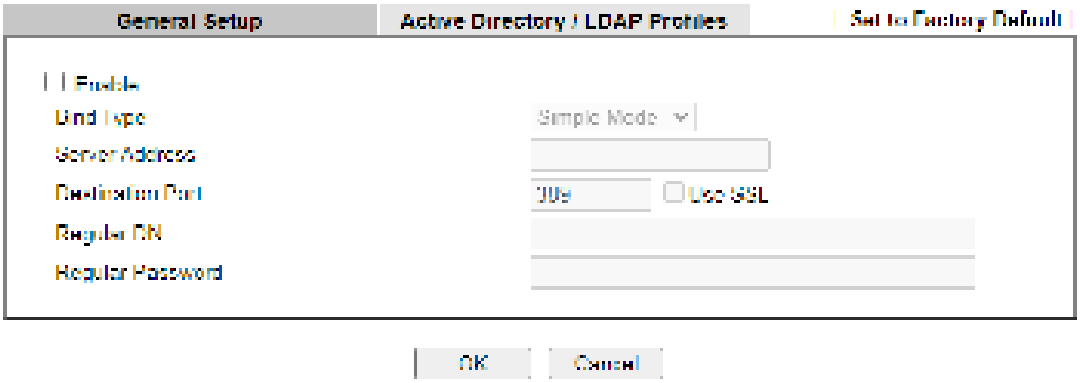
Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/ IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team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

II-5-6-1 General Setup

This page allows you to enable the function and specify general settings for LDAP server.

Applications >> Active Directory / LDAP



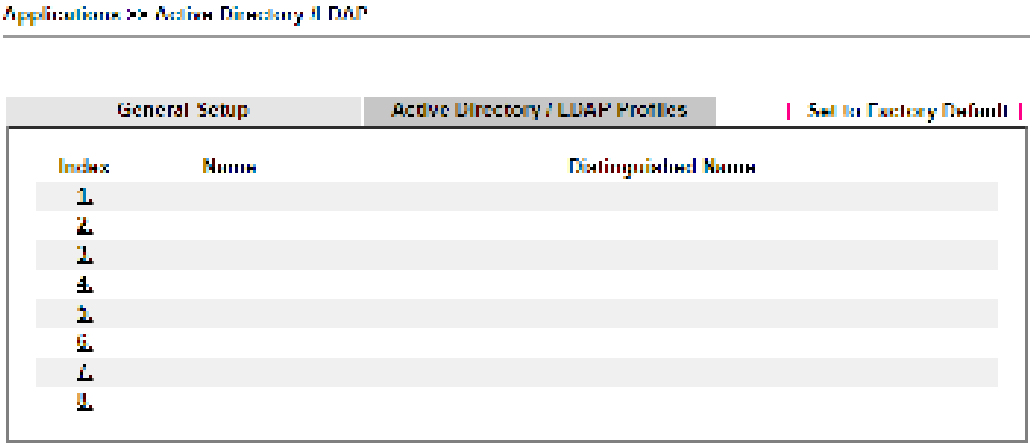
Available settings are explained as follows:

Item	Description
Enable	Check to enable such function.
Bind Type	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**.
Server Address	Enter the IP address of LDAP server.
Destination Port	Type a port number as the destination port for LDAP server.
Regular DN	Type this setting if **Regular Mode** is selected as **Bind Type.**
Regular Password	Specify a password if **Regular Mode** is selected as **Bind Type.**

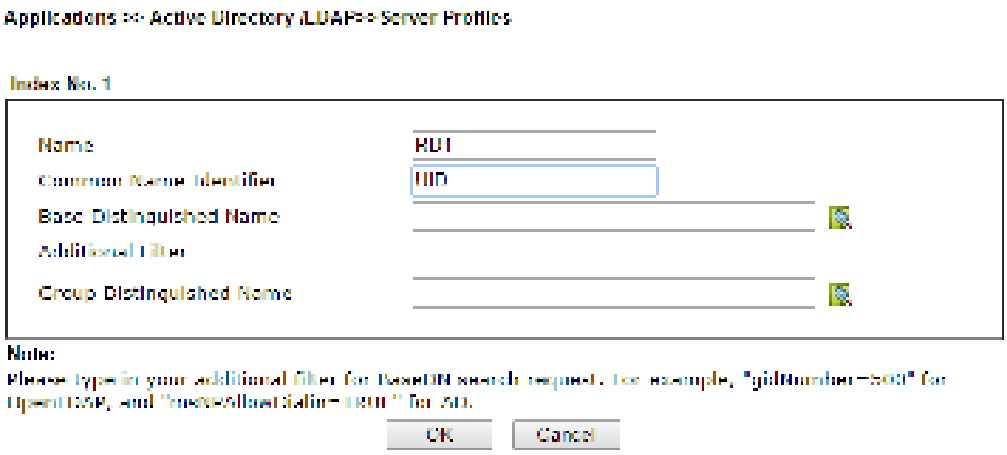
After finished the above settings, click **OK** button to save the settings.

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

You can configure eight AD/ LDAP profiles. These profiles would be used with User Management for different purposes in management.



Click any index number link to open the following page.



Available settings are explained as follows:

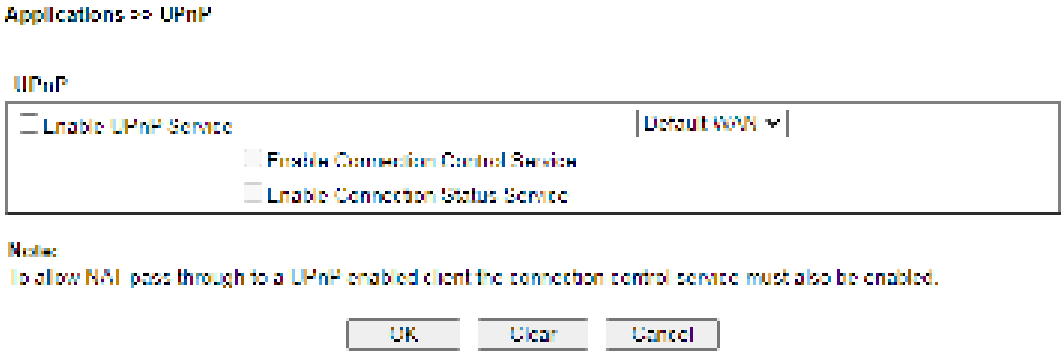
Item	Description
Name	Type a name for such profile. The length of the user name is limited to 19 characters.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is “cn”.
Additional Filter	Enter the condition for additional filter.
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it’s too long. Then you may click the button to list all the account information on the AD/ LDAP Server to assist you finish the setup.

After finished the above settings, click **OK** to save and exit this page. A new profile has been created.

II-5-7 UPnP

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

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



Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.
Default WAN	It is used to specify the WAN interface for applying such function.

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

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

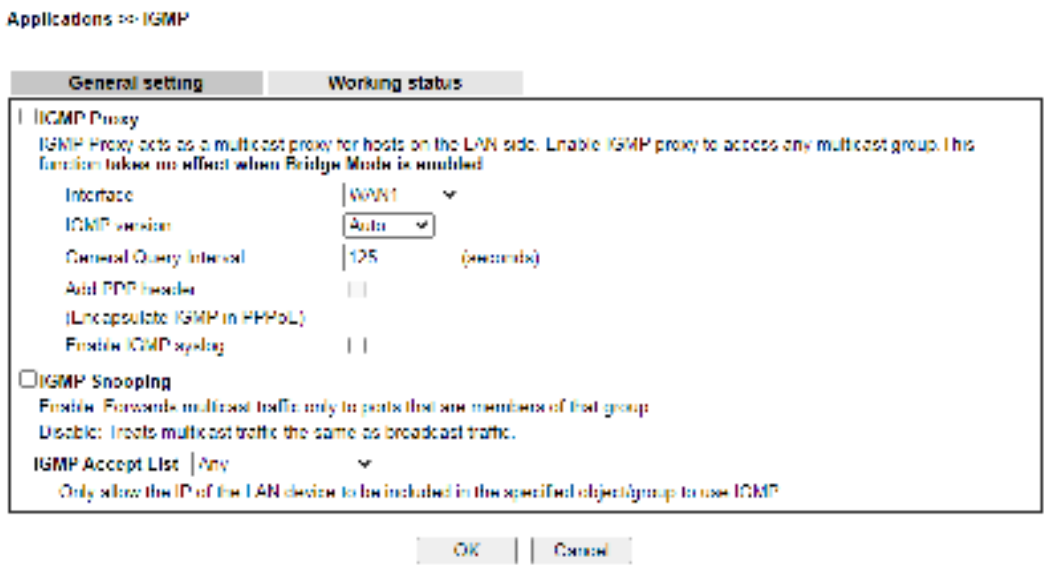
- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

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

II-5-8 IGMP

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

II-5-8-1 General Setting



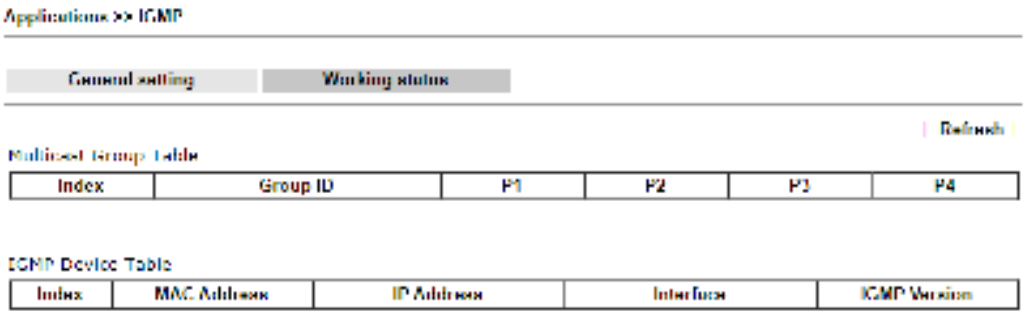
Available settings are explained as follows:

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 send the record related to the IGMP server to Syslog.
IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.

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.

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

II-5-8-2 Working Status



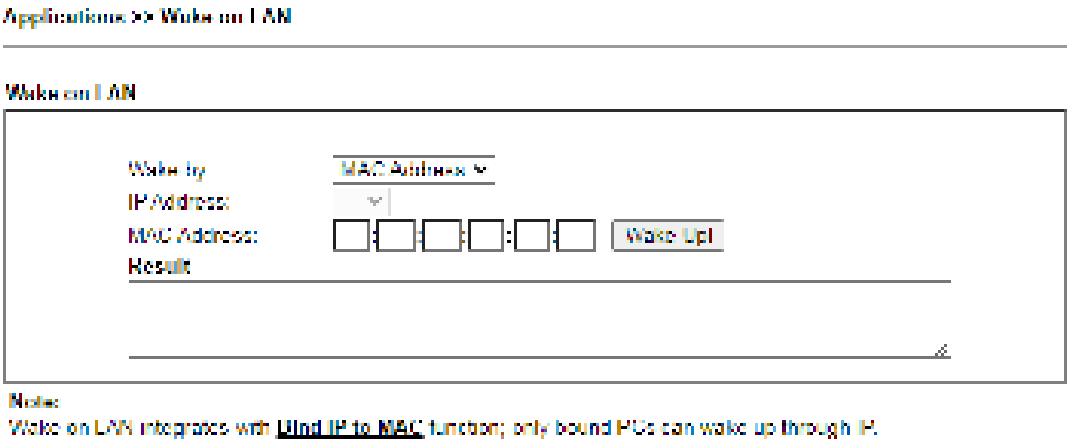
Available settings are explained as follows:

Item	Description
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

II-5-9 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** (WOL) of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.



Available settings are explained as follows:

Item	Description
Wake by	Two types provide for you to wake up the binded IP. ● 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. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the bound PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

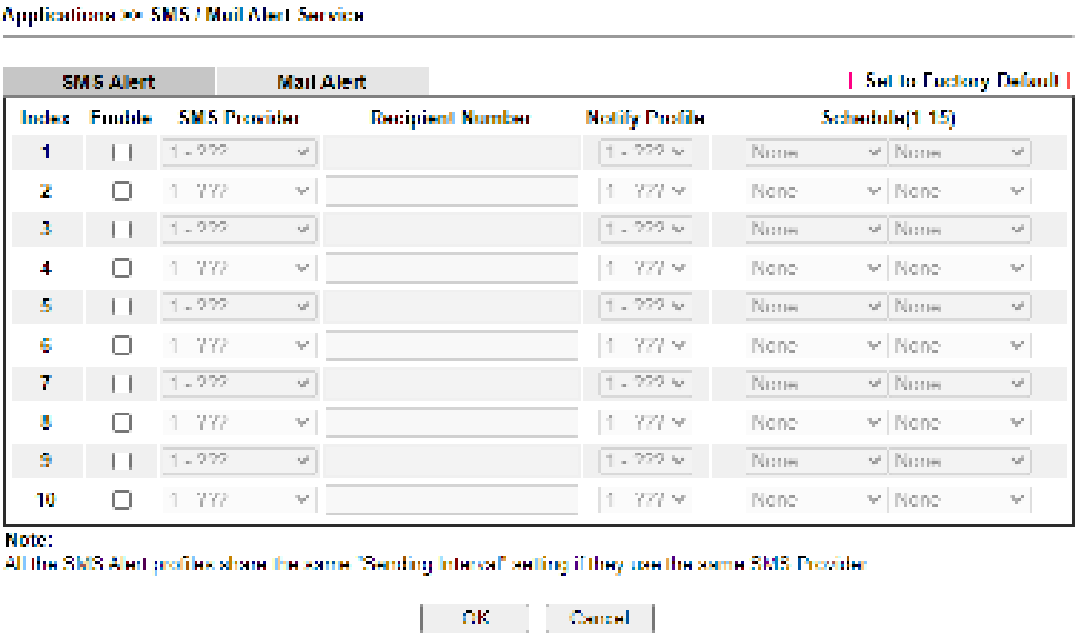
II-5-10 SMS / Mail Alert Service

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

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

II-5-10-1 SMS Alert

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



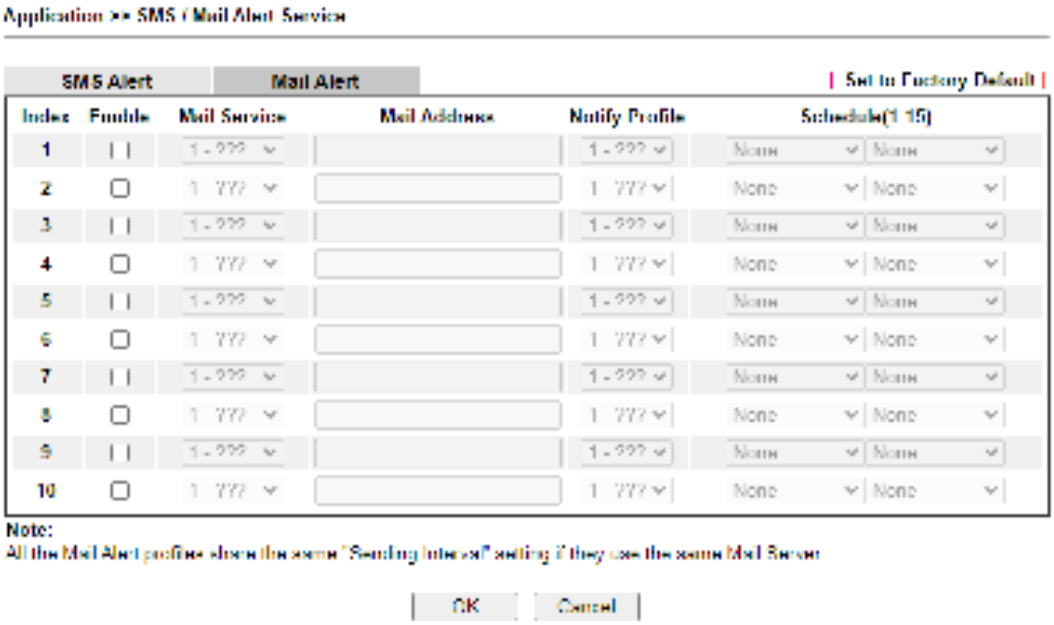
Available settings are explained as follows:

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

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

II-5-10-2 Mail Alert

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.



Available settings are explained as follows:

Item	Description
Enable	Check the box to enable such profile.
Mail Service	Use the drop down list to choose mail service object. All of the available objects are created in **Object Settings>>SMS/Mail Service Object**. If there is no object listed, click **Mail Service** link to define a new one with specified service provider.
Mail Address	Enter the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the **Notify Profile** link to define the content of the mail message.
Schedule (1-15)	Enter the schedule number that the notification will be sent out. You can click the **Schedule(1-15)** link to define the schedule.

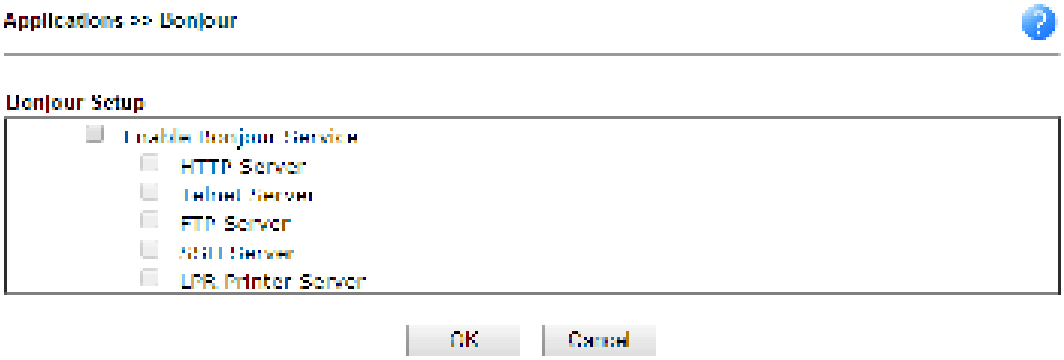
After finishing all the settings here, please click **OK** to save the configuration.

II-5-11 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.

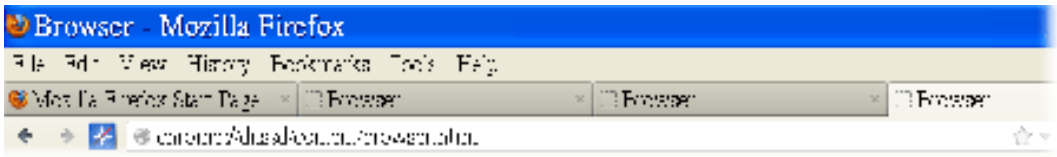
Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer have the plug-in bonjour driver install, they can utilize the service offered by the router by clicking the router name icon. In short, what the Clients/ users need to know is the name of the router only.

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.

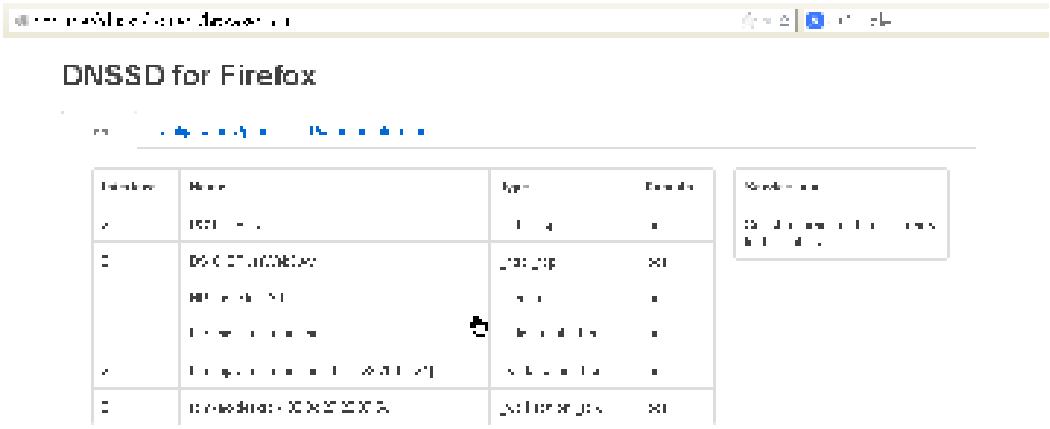


Below shows an example for applying the bonjour feature that Vigor router can be used as the FTP server.

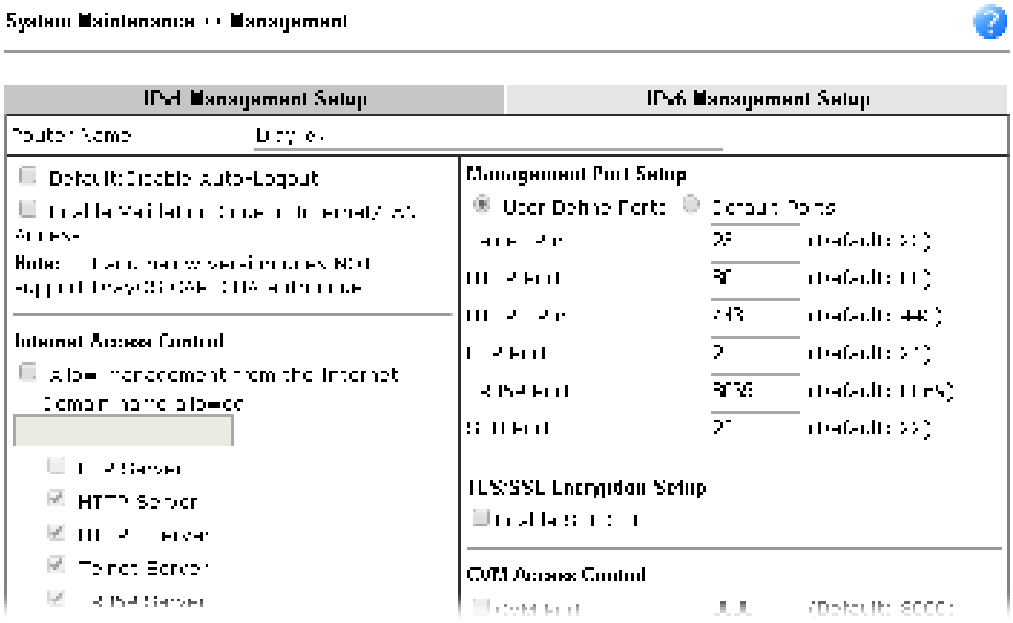
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



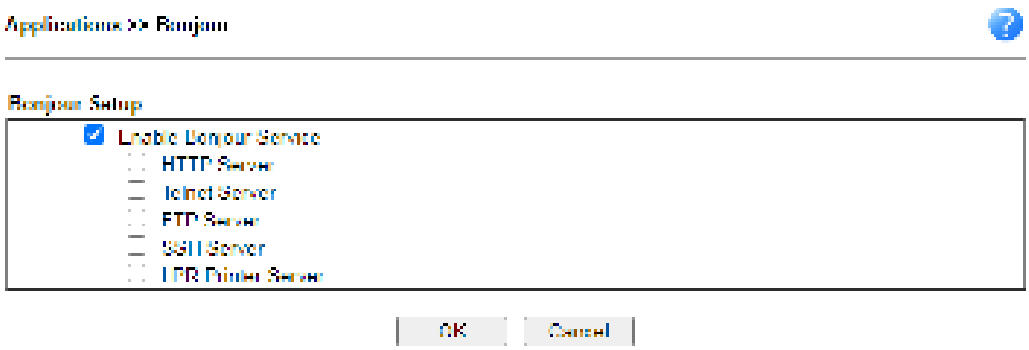
2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



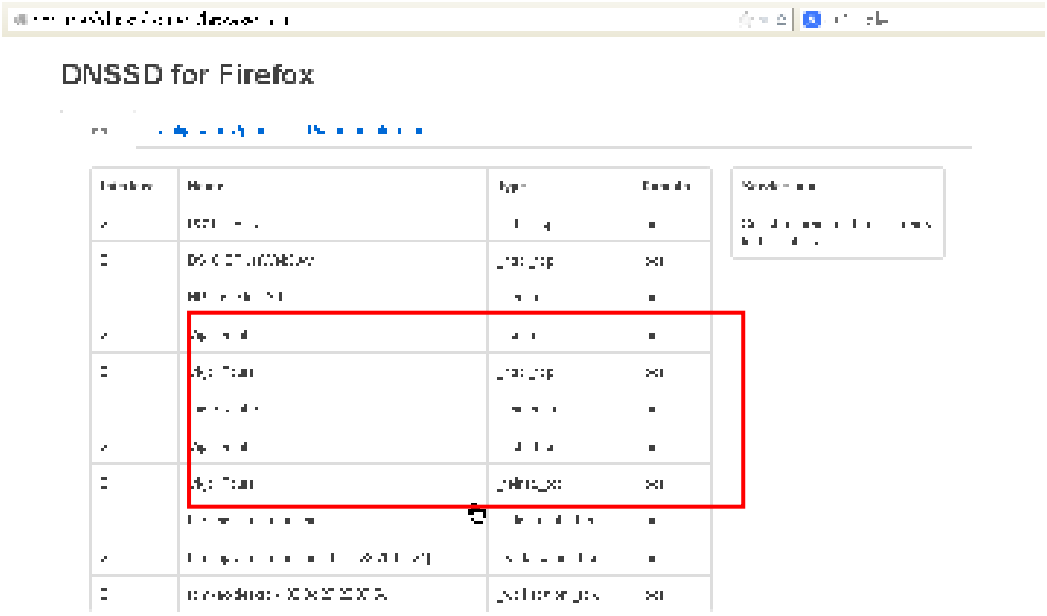
3. Open **System Maintenance>>Management**. Type a name as the Router Name and click **OK**.



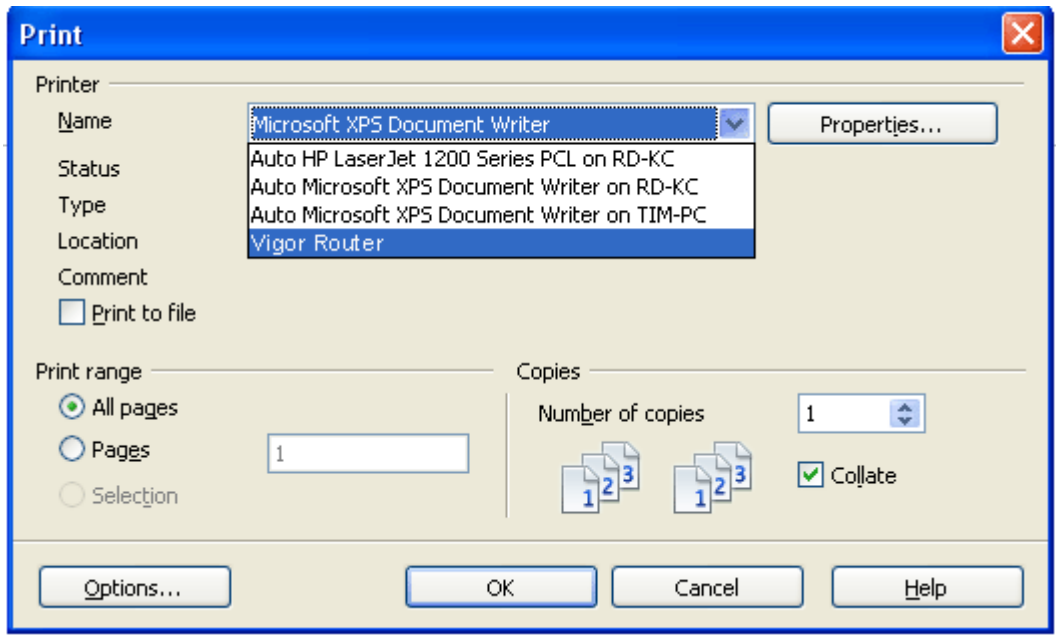
4. Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.



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



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

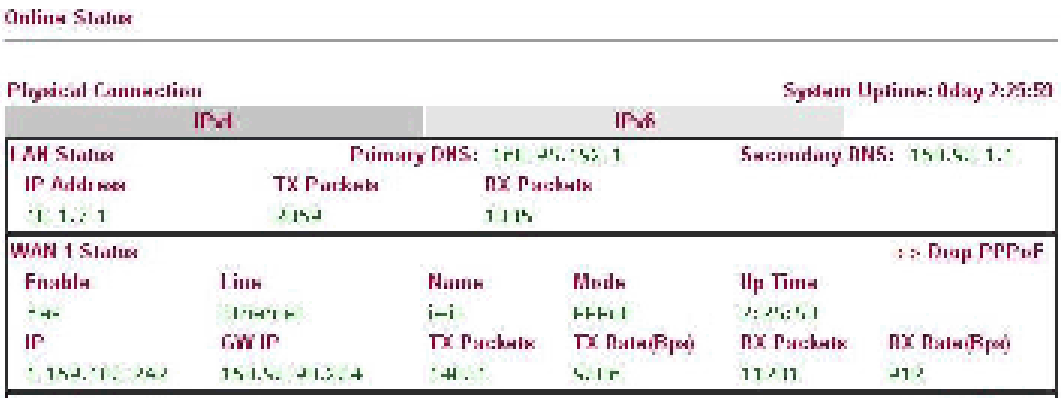


Application Notes

A-1 How to Configure Customized DDNS?

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

Part A : Changeip.org



Note that,

Username: jo***

Password: jo********

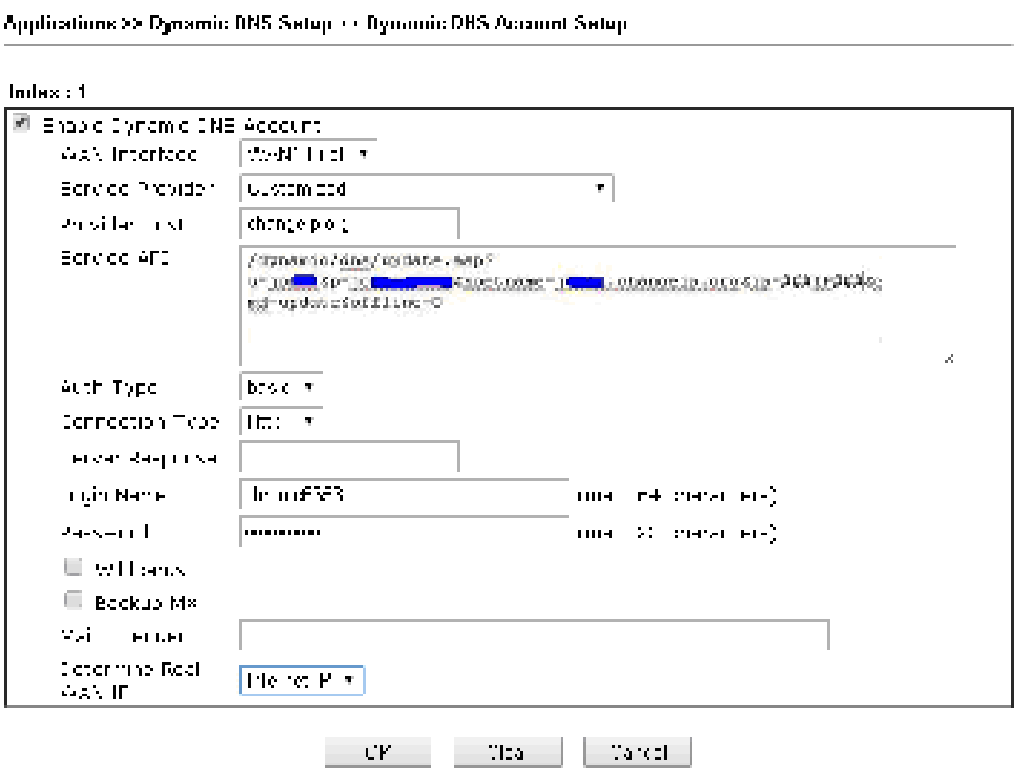
Host name: j*****.changeip.org

WAN IP address: 1.169.185.242

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

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

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



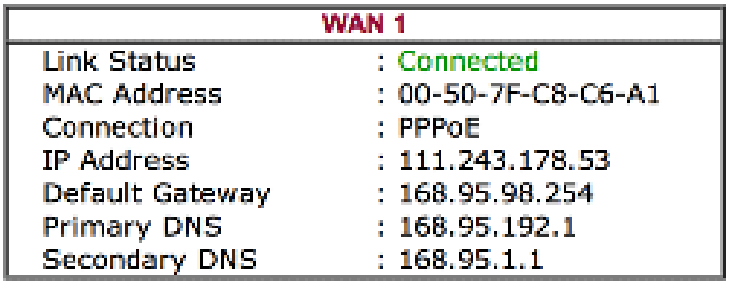
2. Set the Service Provider as **Customized**.

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

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

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

Part B : 3322.net



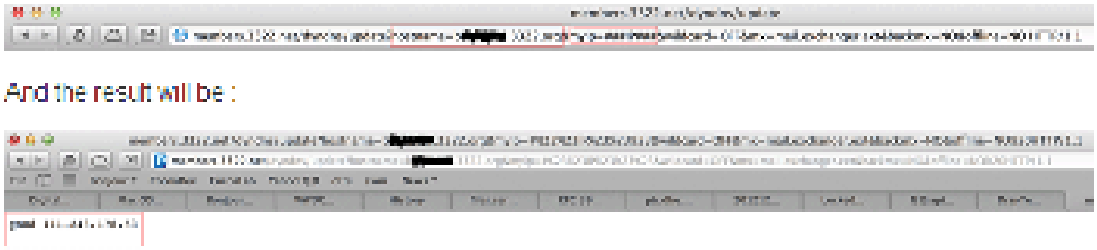
Username: bi*******

Password: 88********

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

WAN IP address: 111.243.178.53

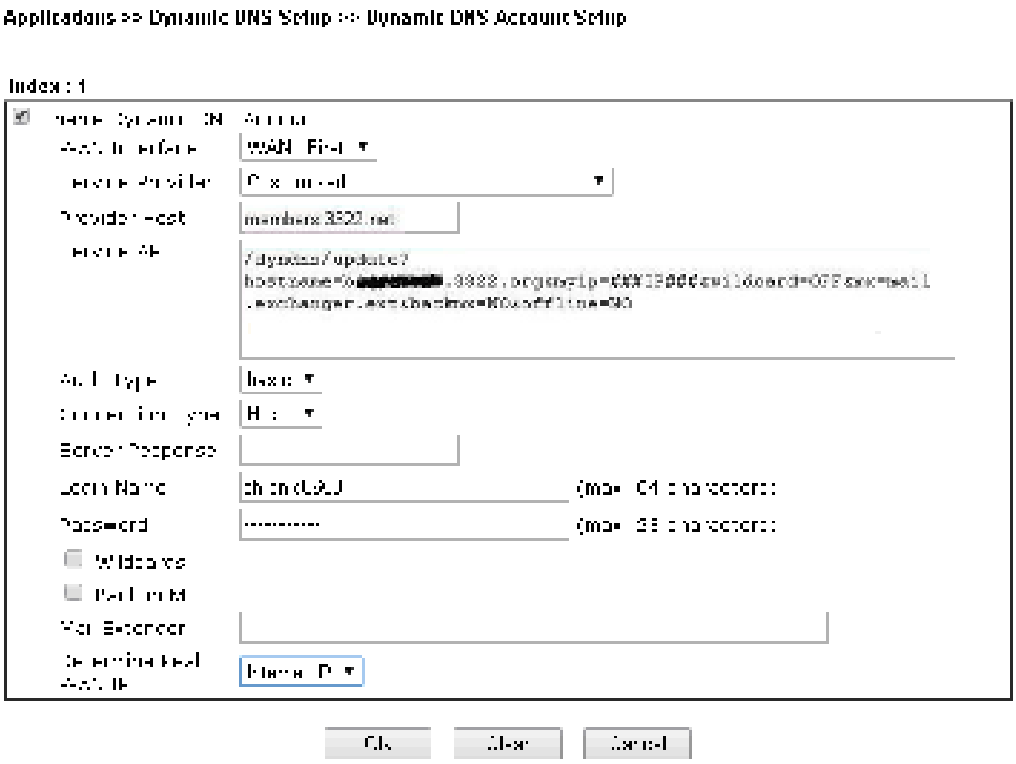
To update the IP to the DDNS server via editing the HTML script, we can Enter the following script on the browser:



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

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

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



2. Set the Service Provider as **Customized**.

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

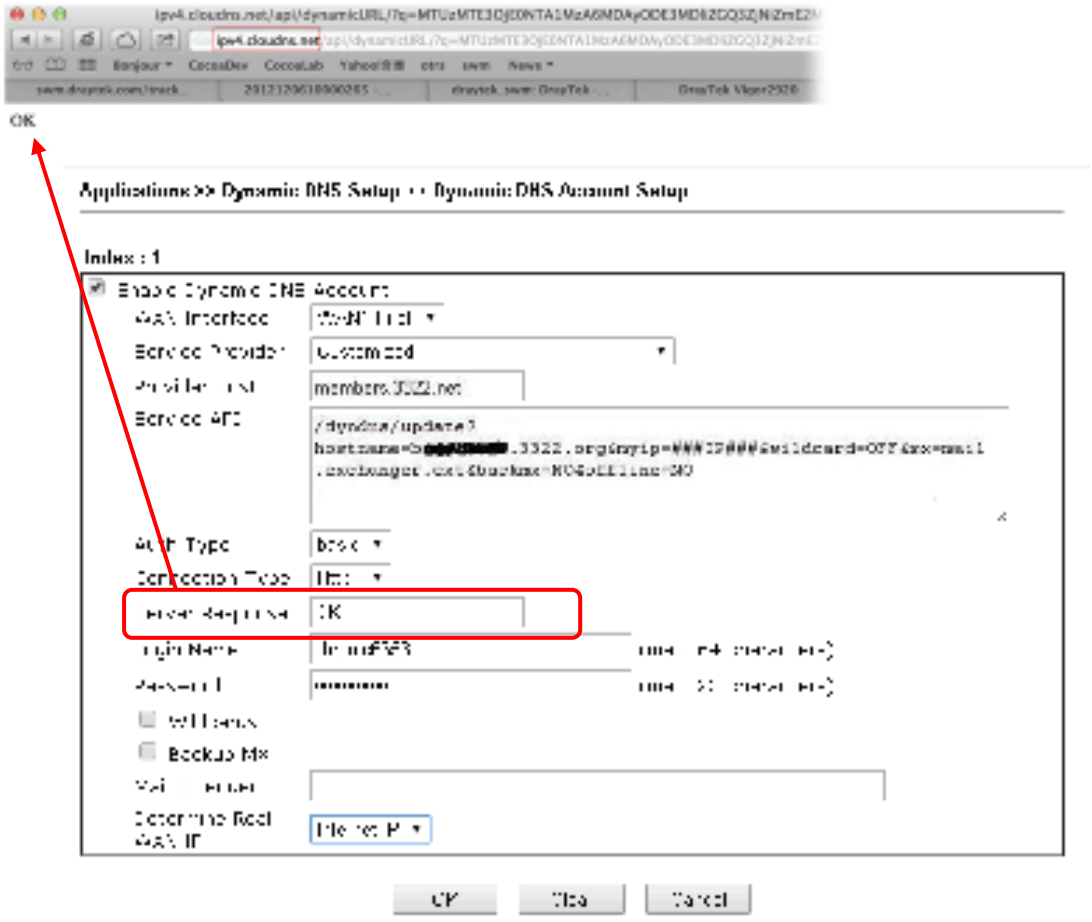
4. Set the Service API as:
/dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail.exchanger.ext&backmx=NO&offline=NO

5. Enter your account and password.

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

Part C : Extend Note

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



II-6 Routing

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

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

Load Balance

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

Specify Interface

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

Address Mapping

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

Priority

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

Failover to/Failback

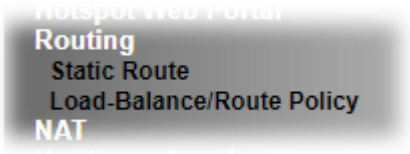
Packets will be sent through another Interface or follow another Policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.

Other routing

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

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

Web User Interface

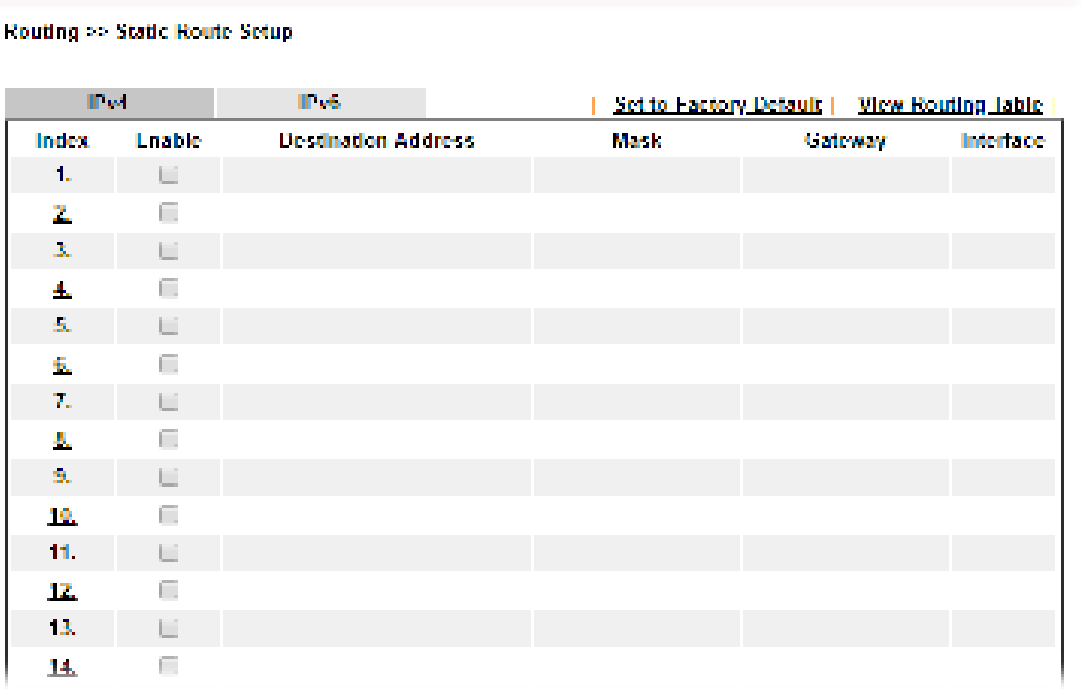


II-6-1 Static Route

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

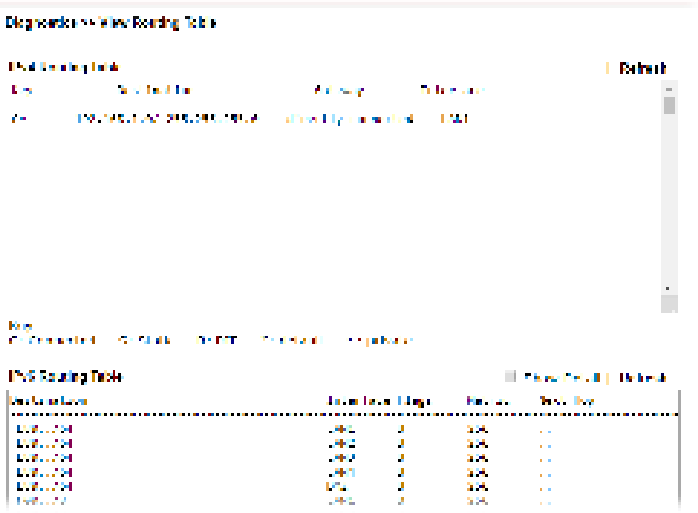
Go to **Routing** >> **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4



Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Enable	Check the box to enable the static route profile.
Destination Address	Displays the destination address of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.

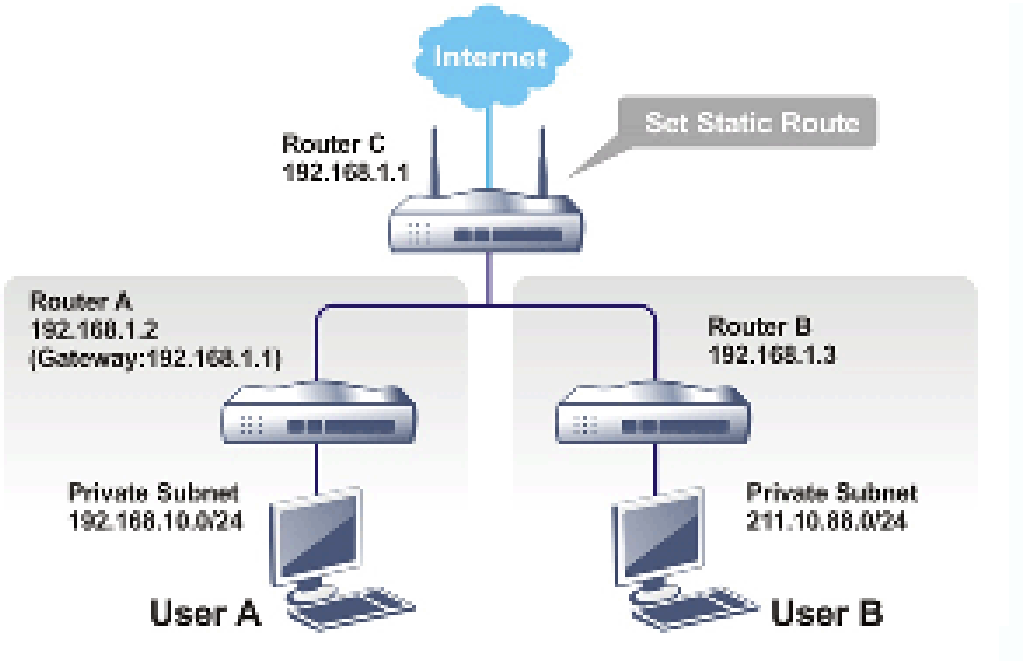
Viewing Routing Table	Displays the routing table for your reference. 
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

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.

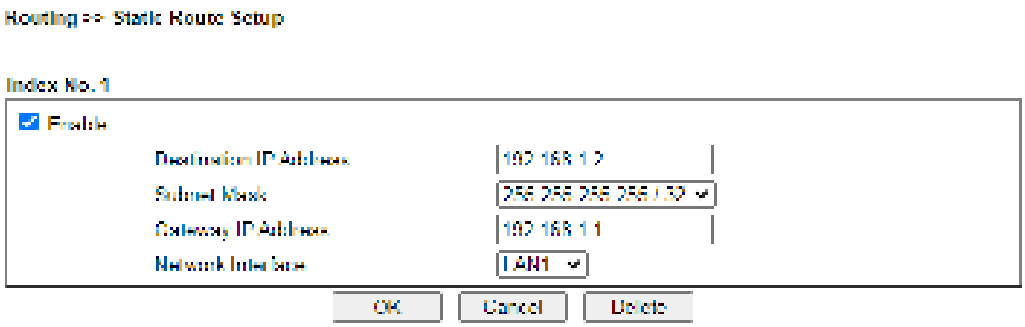


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

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.

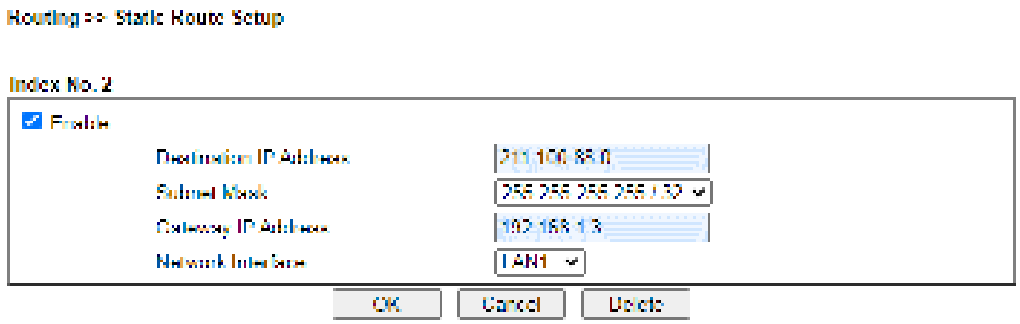
2. Click the **Routing >> Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



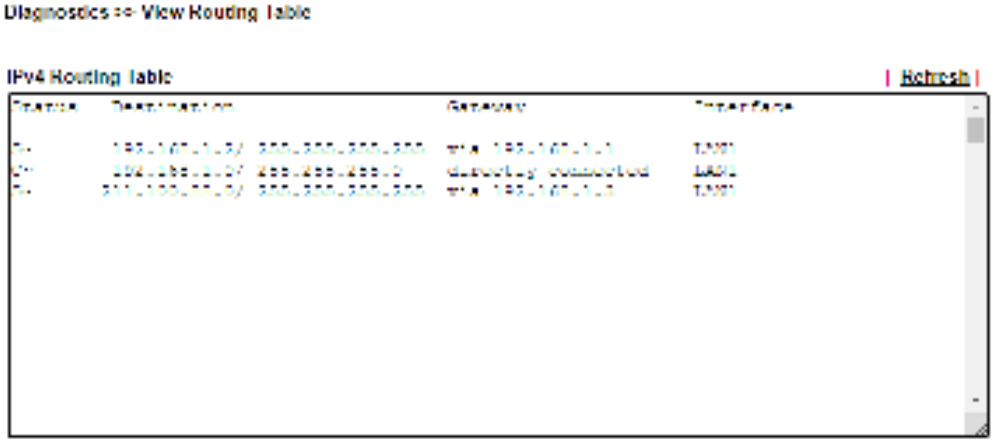
Available settings are explained as follows:

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

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

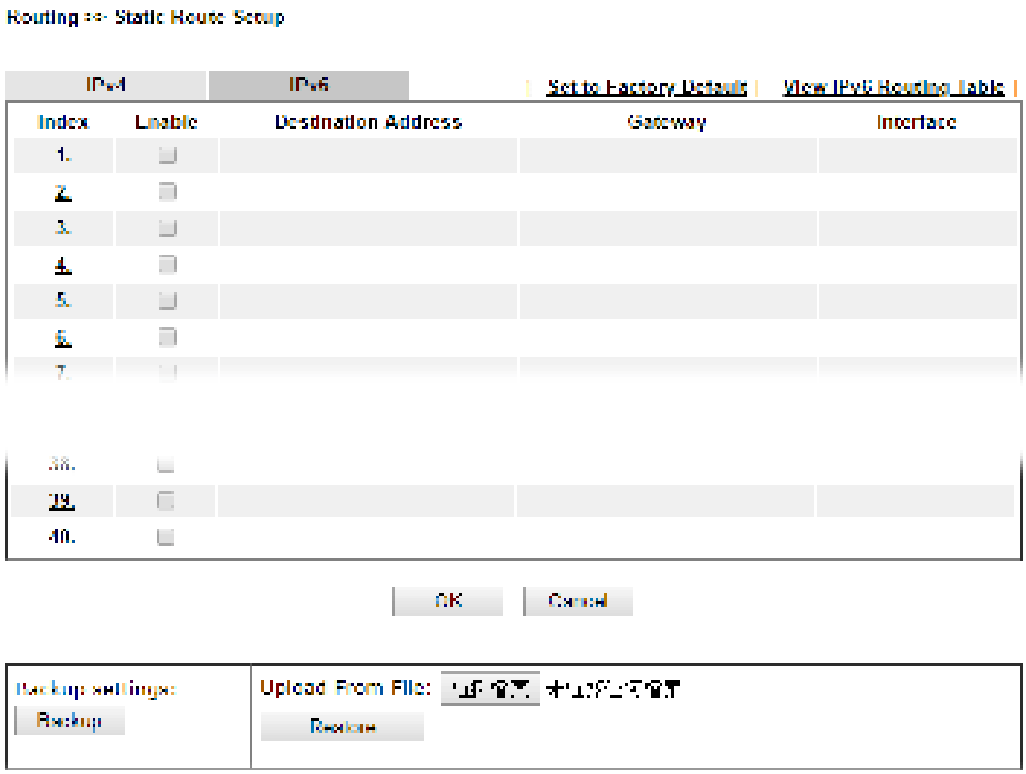


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



Static Route for IPv6

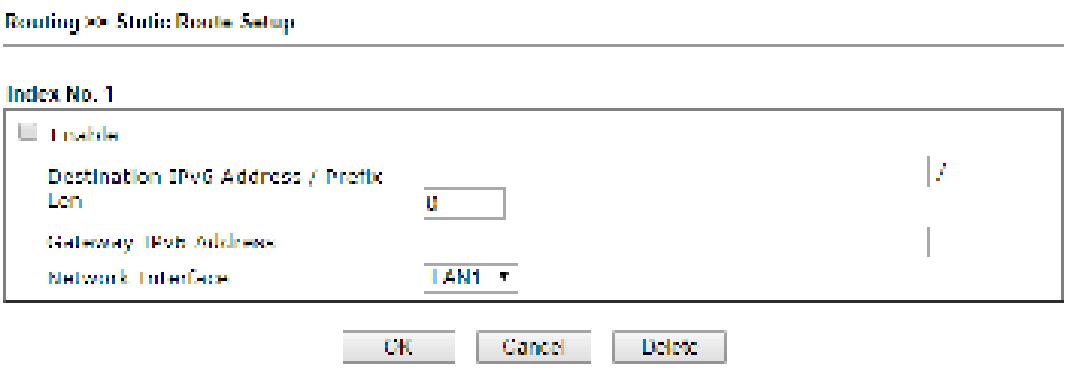
You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:



Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.
Backup	Click it to backup the configuration of static route settings.
Restore	Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router.

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



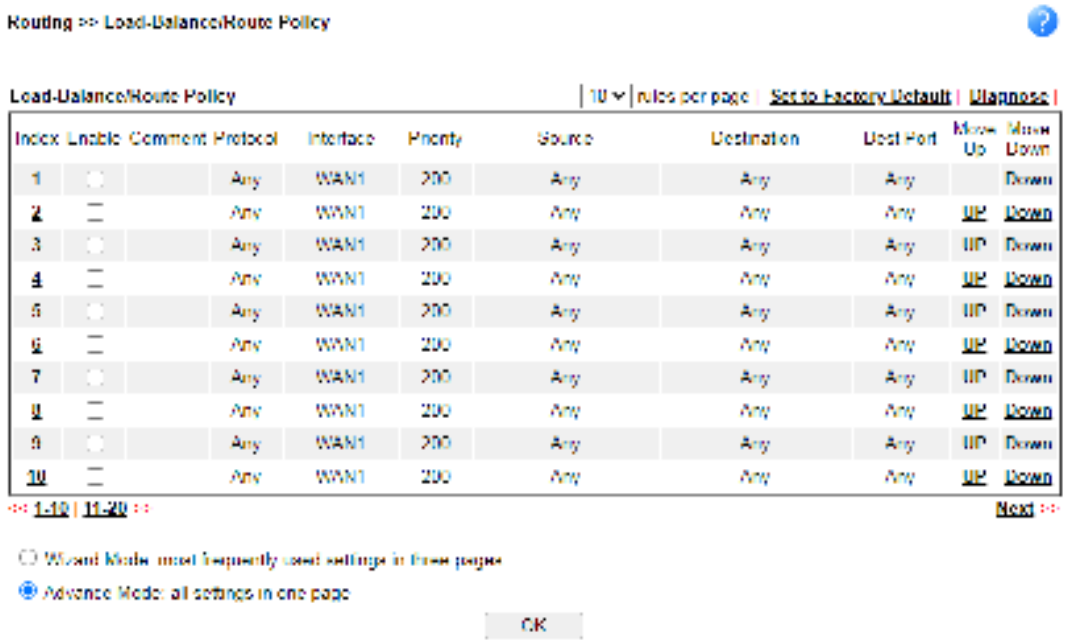
Available settings are explained as follows:

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

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

II-6-2 Load-Balance /Route Policy

II-6-2-1 General Setup

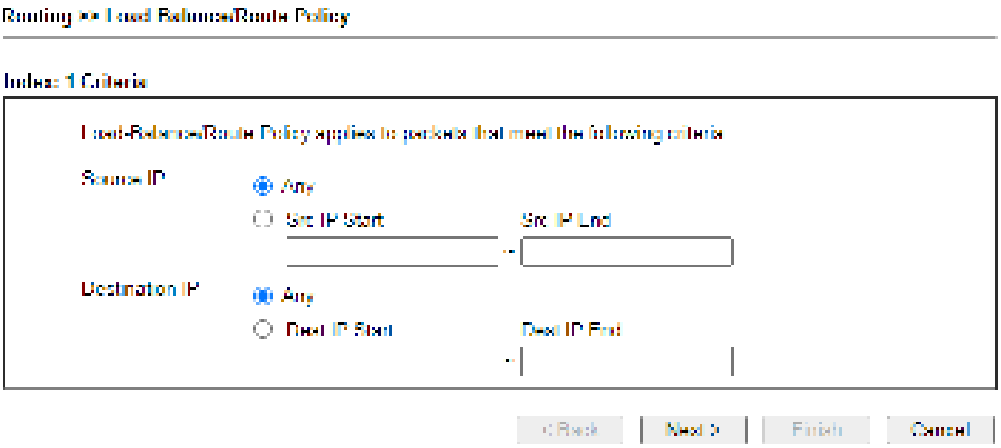


Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.
Enable	Check this box to enable this policy.
Protocol	Display the protocol used for this policy.
Interface	Display the interface to send packets to once the policy is matched.
Priority	Display the priority value for such route policy profile.
Src IP Start	Display the IP address for the start of the source IP.
Src IP End	Display the IP address for the end of the source IP.
Dest IP Start	Display the IP address for the start of the destination IP.
Dest IP End	Display the IP address for the end of the destination IP.
Dest Port Start	Display the IP address for the start of the destination port.
Dest Port End	Display the IP address for the end of the destination port.
Move UP/Move Down	Use **Up** or **Down** link to move the order of the policy.
Wizard Mode	Allow to configure frequently used settings of route policy via three setting pages
Advance Mode	Allow to configure detailed settings of route policy.

To use Wizard Mode, simple do the following steps:

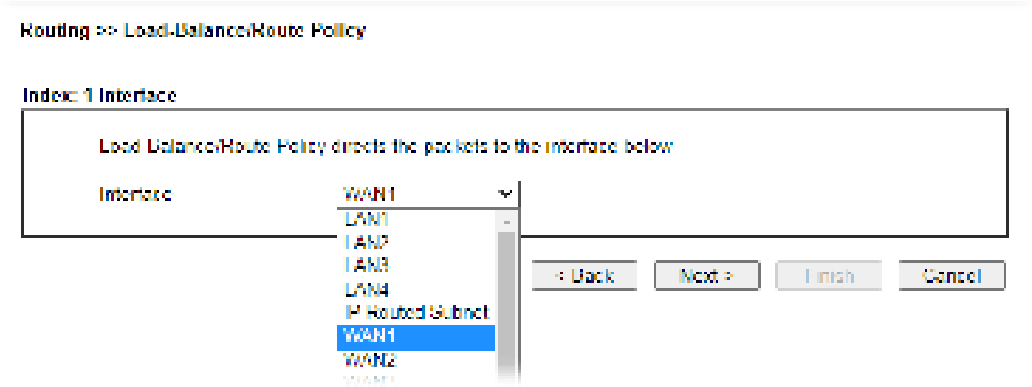
1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:



Available settings are explained as follows:

Item	Description
Source IP	**Any** – Any IP can be treated as the source IP. **Src IP Start -** Enter the source IP start for the specified WAN interface. **Src IP End -** Enter the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Destination IP	**Any** – Any IP can be treated as the destination IP. **Dest IP Start-** Enter the destination IP start for the specified WAN interface. **Dest IP End -** Enter the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

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

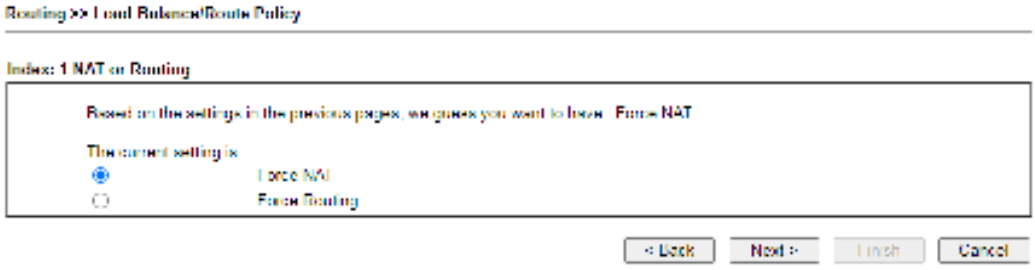


Available settings are explained as follows:

Item	Description

Interface	Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.

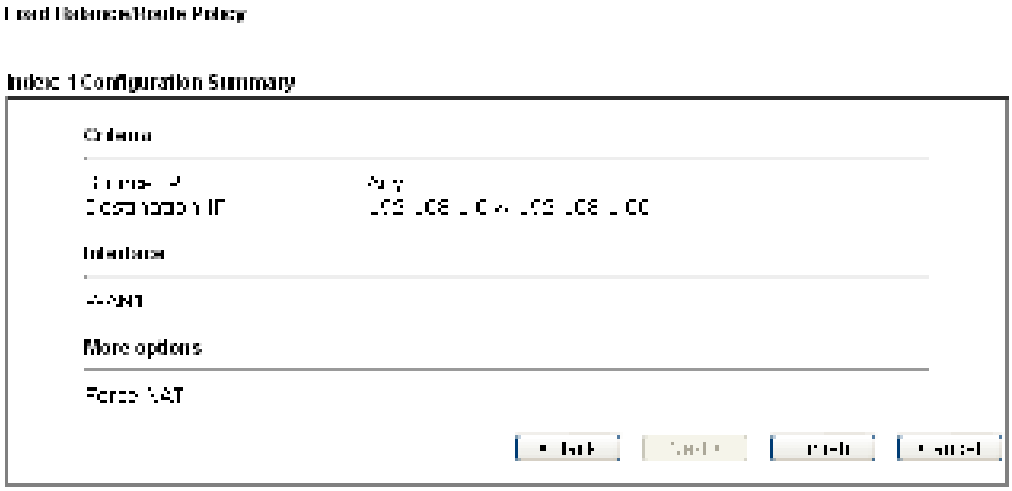
4. After specifying the interface, click **Next** to get the following page.



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.

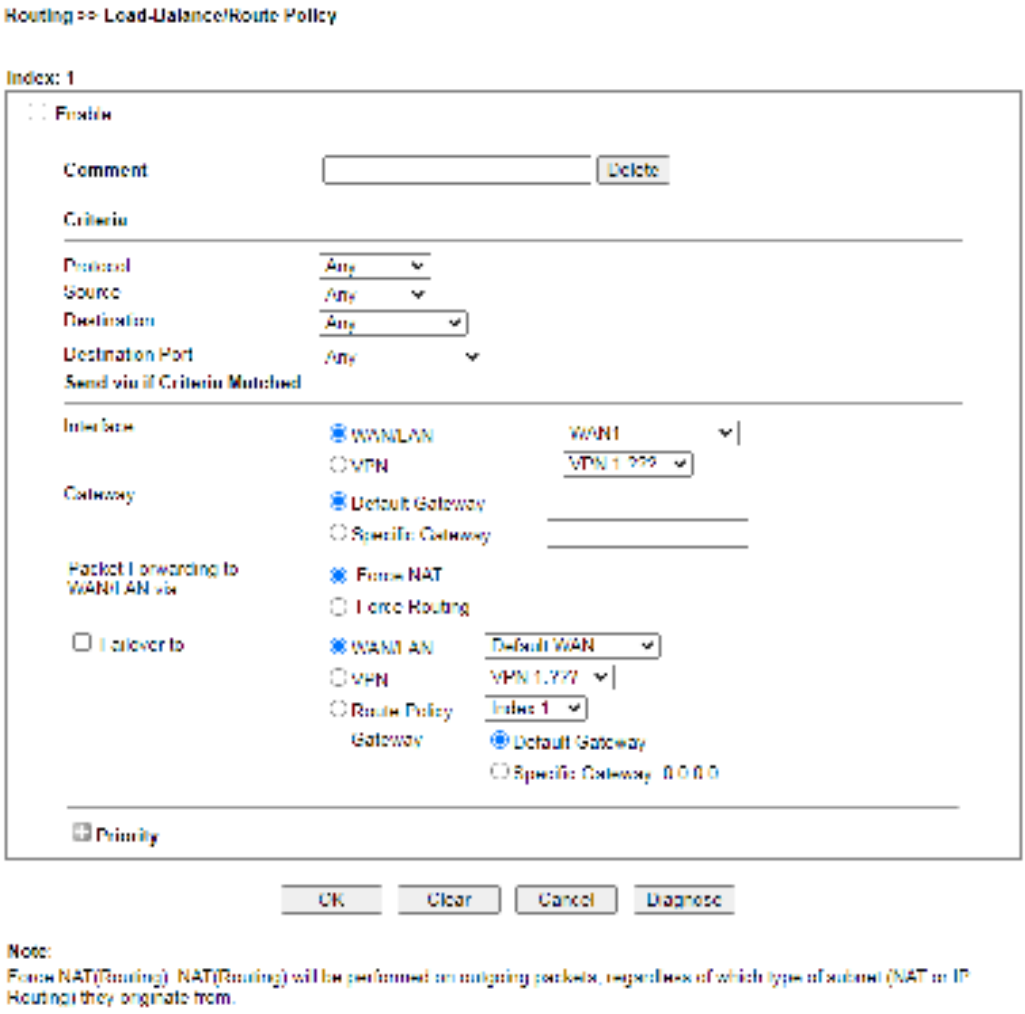
5. After choosing the mechanism, click **Next** to get the summary page for reference.



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

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

1. Click the **Advance Mode** radio button.
2. Click any **Index** number link (e.g., 1 in this case) to access into the following page.



Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.
Comment	Type a brief explanation for such profile.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source	**Any** – Any IP can be treated as the source IP. **IP Range** – Define a range of IP address as source IP addresses. ● **Start -** Type an address as the starting IP for such profile. ● **End -** Type an address as the ending IP for such profile. **IP Subnet** – Define a subnet containing IP address and mask address.

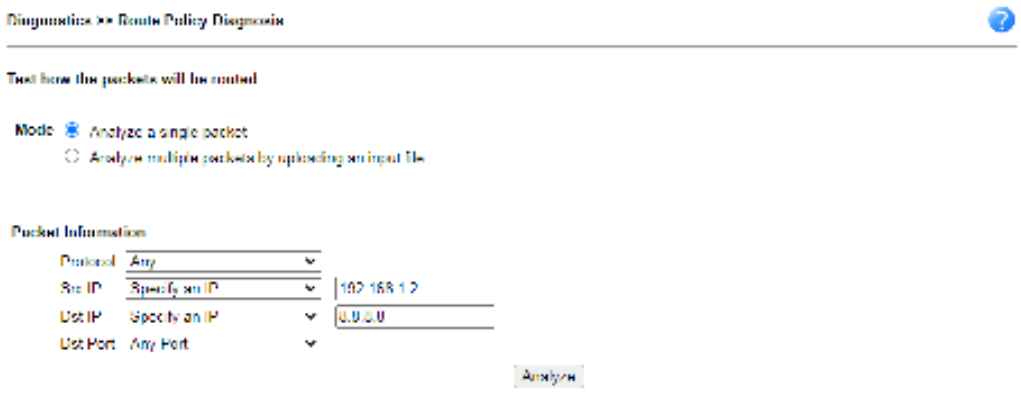
	• **Network** – Type an IP address here. • **Mask** – Use the drop down list to choose a suitable mask for the network. **IP Object** / **IP Group**– Use the drop down list to choose a preconfigured IP object/group.
Destination	**Any** – Any IP can be treated as the destination IP. **IP Range** – Define a range of IP address as destination IP addresses. • **Start -** Type an address as the starting IP for such profile. • **End -** Type an address as the ending IP for such profile. **IP Subnet** – Define a subnet containing IP address and mask address. • **Network** – Type an IP address here. • **Mask** – Use the drop down list to choose a suitable mask for the network. **Domain Name** – Specify a domain name as the destination. • **Select** – Click it to choose an existing domain name defined in Objects Setting>>String Object. • **Delete** – Remove current used domain name. • **Add** – Create a new domain name as the destination. **IP Object** / **IP Group**– Use the drop down list to choose a preconfigured IP object/group.
Destination Port	**Any** – Any port number can be treated as the destination port. **Dest Port Range –** • **Start -** Enter the destination port start for the destination IP. • **End -** Enter the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if Criteria Matched	**Interface** – Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here. **Gateway IP** – **Specific gateway** is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default. **Packet Forwarding to WAN/LAN via** – When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose **Force NAT** or **Force Routing**. **Failover to** – Check this button to lead the data passing through specific interface (WAN/ LAN/ VPN/ Route Policy) automatically when the selected interface (defined in **Send via if criteria matched**) is down. • **WAN/LAN –** Use the drop down list to choose an interface as an auto failover interface. • **VPN –** Use the drop down list to choose a VPN tunnel as a failover tunnel. • **Route Policy –** Use the drop down list to choose an existed route policy profile.

	● **Gateway IP** – **Specific gateway** is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.
Priority	Packets will be transmitted based on all routes or Route Policy. Vigor router will determine which rule will be adopted for transmitting the packet according to the priority of Static Route and Route Policy. The greater the value is, the lower the priority is. Default value for route policy is "200" which means it has higher priority than the default route.

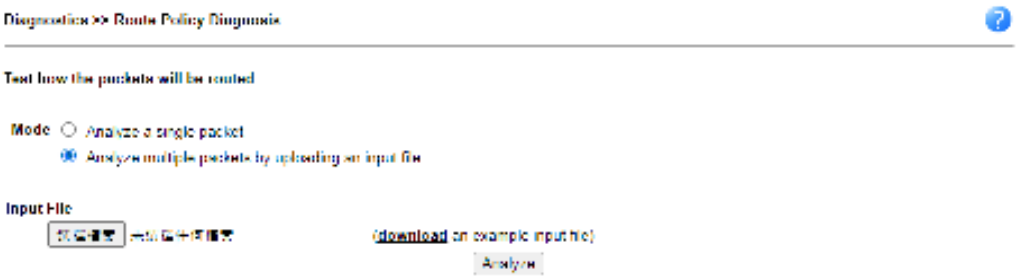
3. When you finish the configuration, please click **OK** to save and exit this page.

II-6-2-2 Diagnose

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.

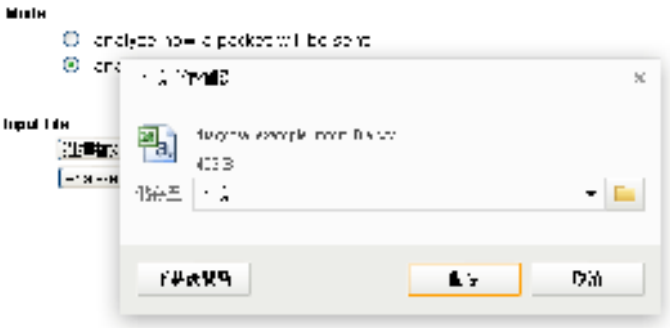


or



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. **Prococol -** Specify a protocol(**ICMP**/**UDP**/**TCP**/**ANY**) for diagnosis. **Src IP** – Type an IP address as the source IP. **Dst IP** – Type an IP address as the destination IP.

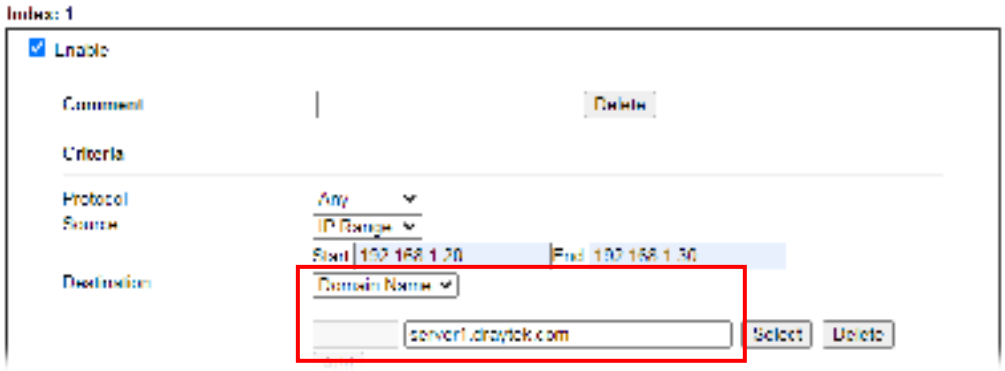
	Dst Port – Use the drop down list to specify the destination port. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page.
Input File	It is available when "Analyze mulitple packets.." is selected as the Mode. **Select** – Click the download link to get a 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. 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.

Application Notes

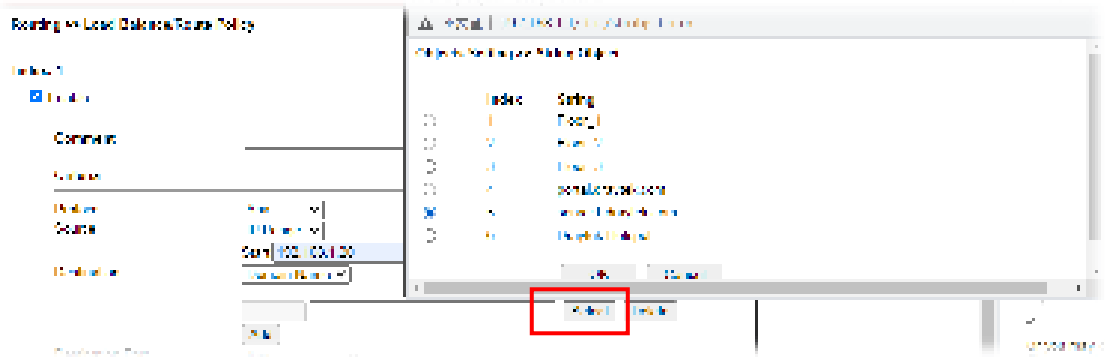
A-1 How to use destination domain name in a route policy?

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

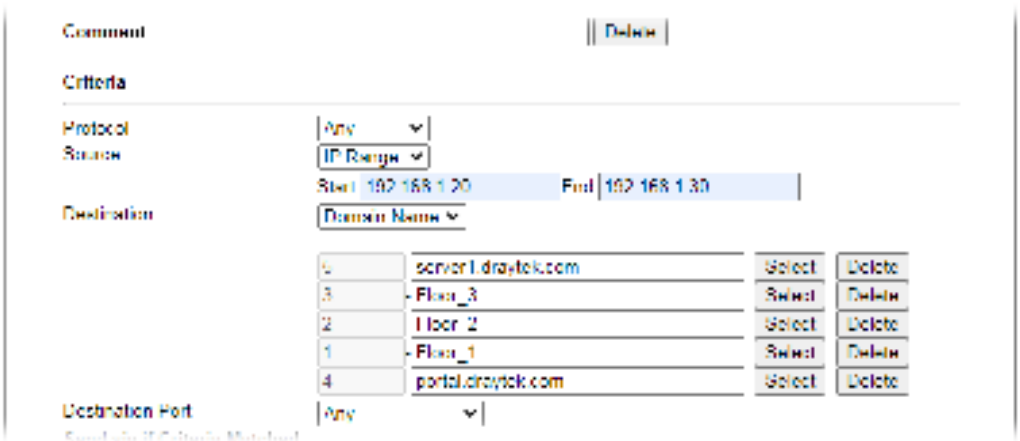
To use a destination domain name as criteria, just select **Domain Name** as **Destination** in Criteria, and enter the domain name in the empty field.



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

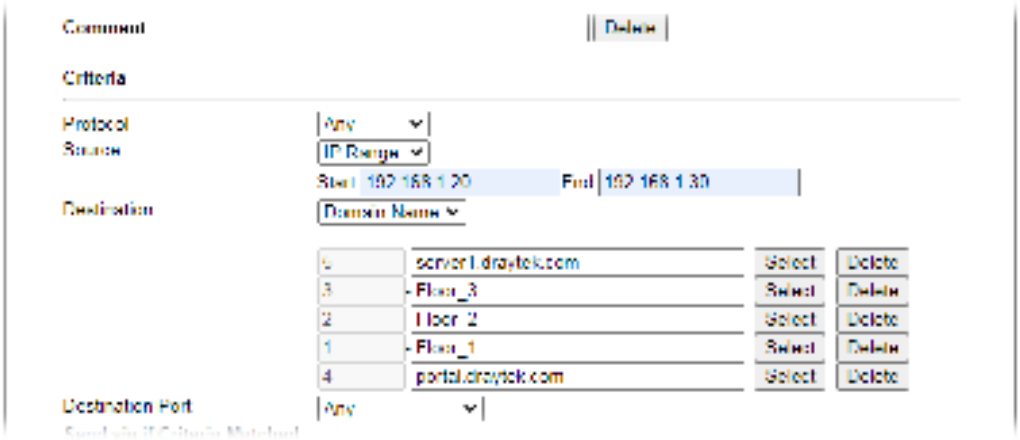


Click **Add** too add more domain names, we can set up to 5 domain names in one route policy.

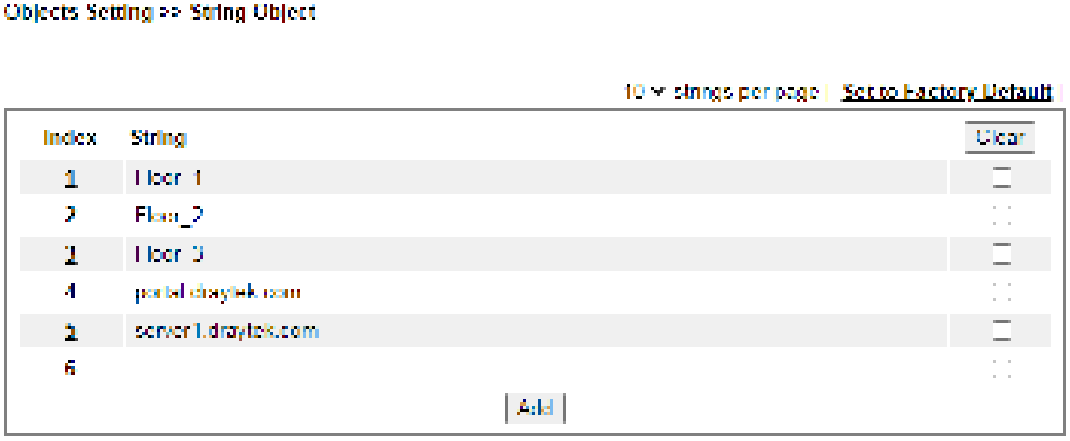


Auto-create String Objects

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

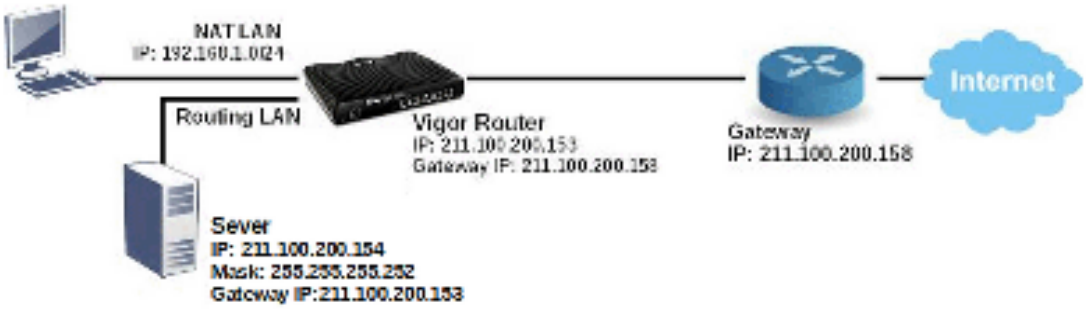


That means the router has automatically created string objects for those domain names, so that they can be used in other route policies or other functions.



A-2 How to use a Public IP on LAN

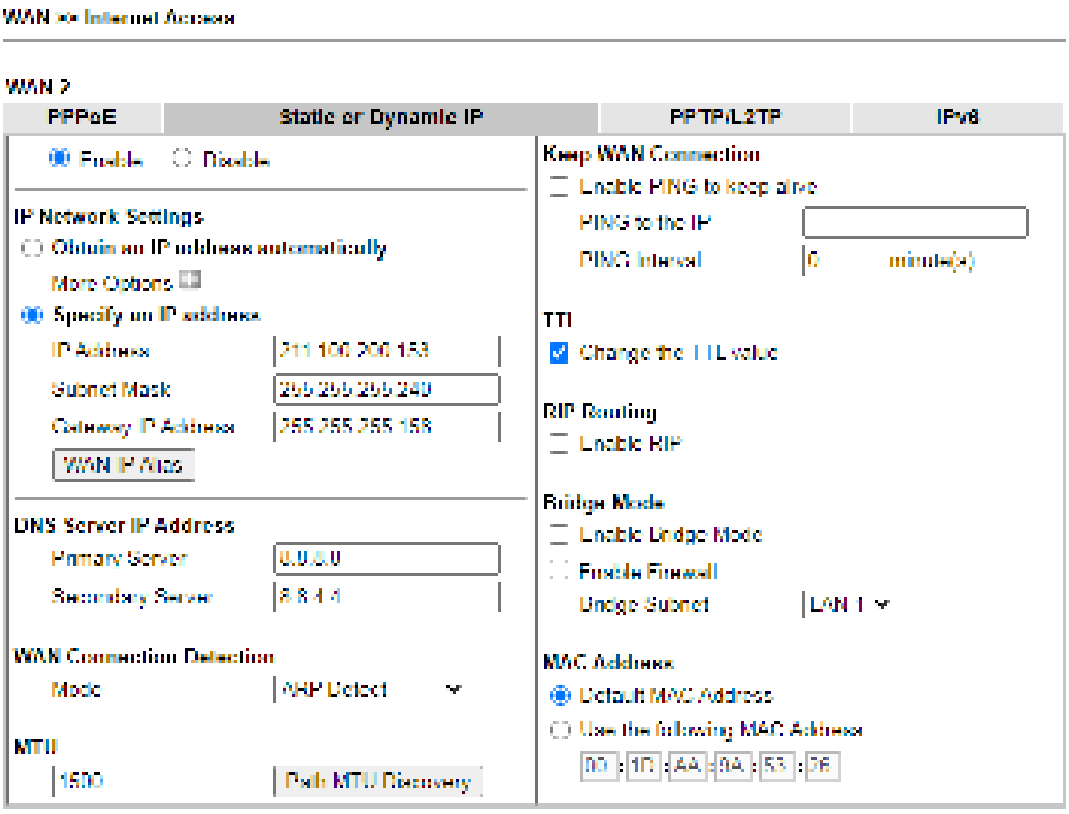
We cannot disable NAT on Vigor Router, but still, we may use a public IP address on a host behind Vigor Router. If our ISP allocates a block public IP addresses for us, then we may use the public IP address with IP Routed Subnet or Routing Usage LAN.



Suppose ISP provides a public IP subnet 211.100.200.152/ 255.255.255.248 for us, and the gateway IP is 211.100.200.158. The public IP addresses we can use are between 211.100.200.153 to 211.100.200.157. The following shows how to set up a non-NAT subnet so that the server behind Vigor Router can use the public IP address 211.100.200.154.

WAN Setup

Go to **WAN >> Internet Access** and configure the WAN connection according to what ISP provides. (Note: If it is necessary to specify an IP address manually, remember that subnet mask for WAN interface should be larger than that of LAN interface.)

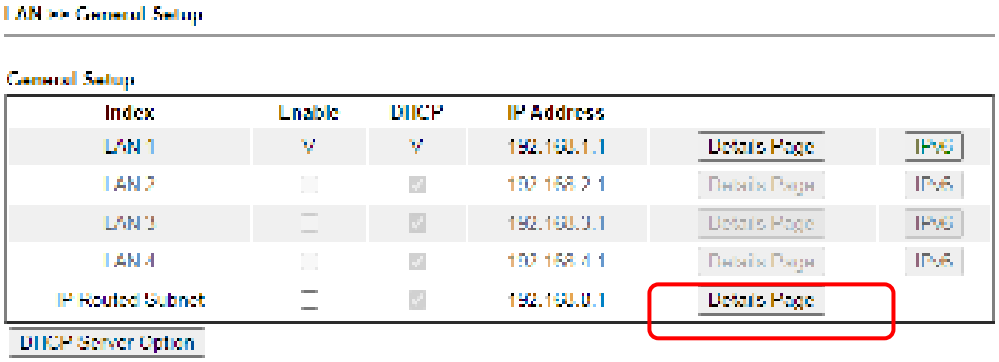


Now we have two methods to configure it

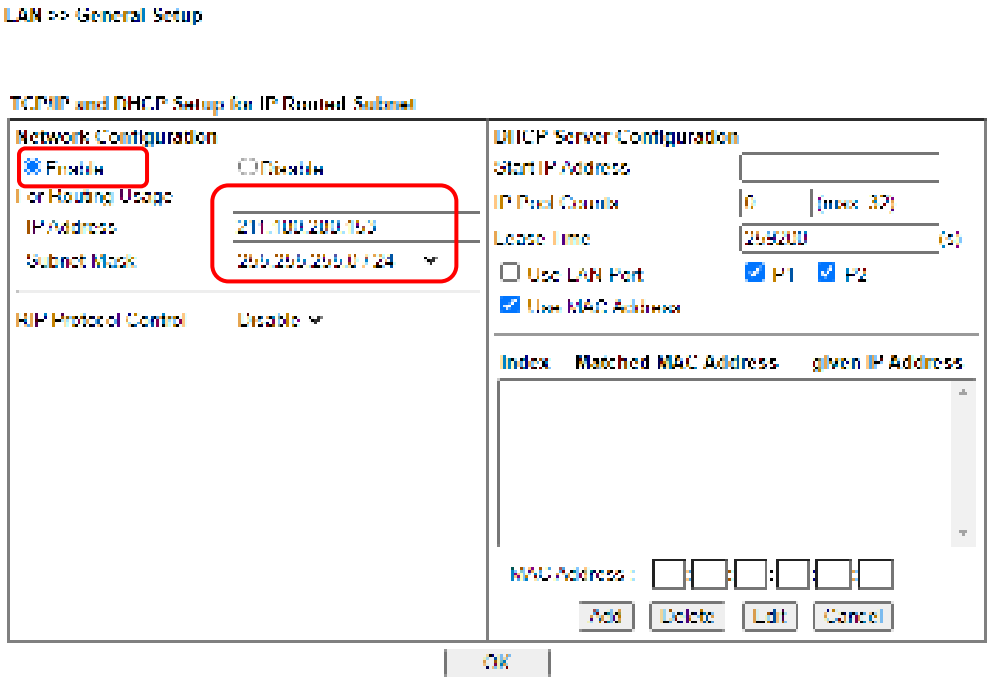
- IP Routed LAN
- Routing Usage LAN

IP Routed LAN Setup

1. Go to **LAN >> General Setup**, click on **Details Page** for IP Routed Subnet.



2. Set up TCP/IP details for IP Routed Subnet.



   a. Enable IP Routed Subnet.

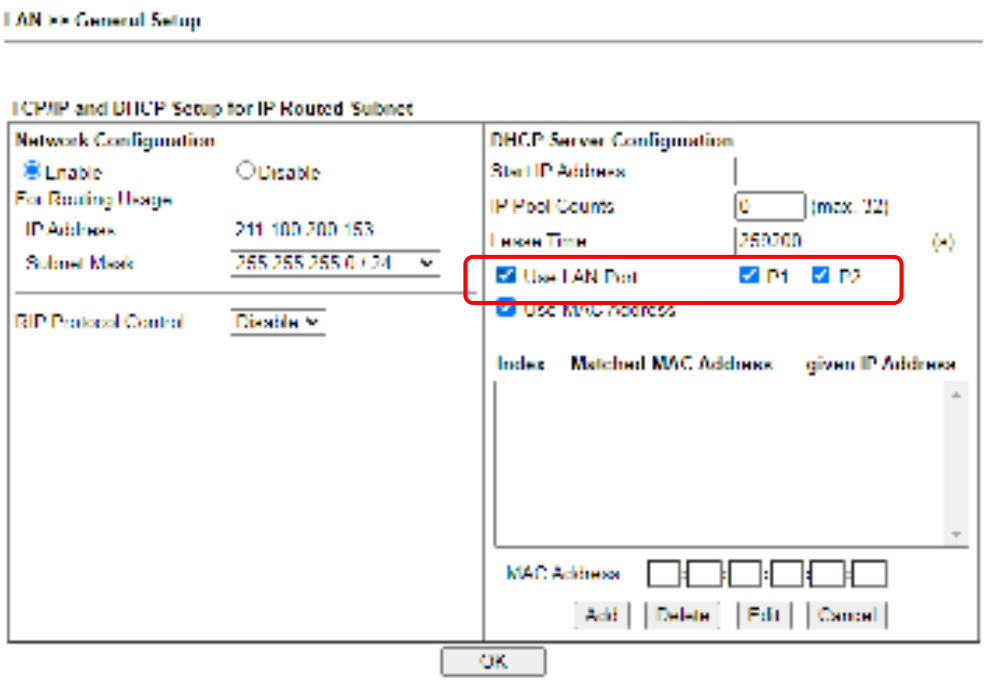
   b. Enter the IP Address for the router. Note that this could be the same as router's WAN IP.

   c. Enter the Subnet Mask according to ISP.

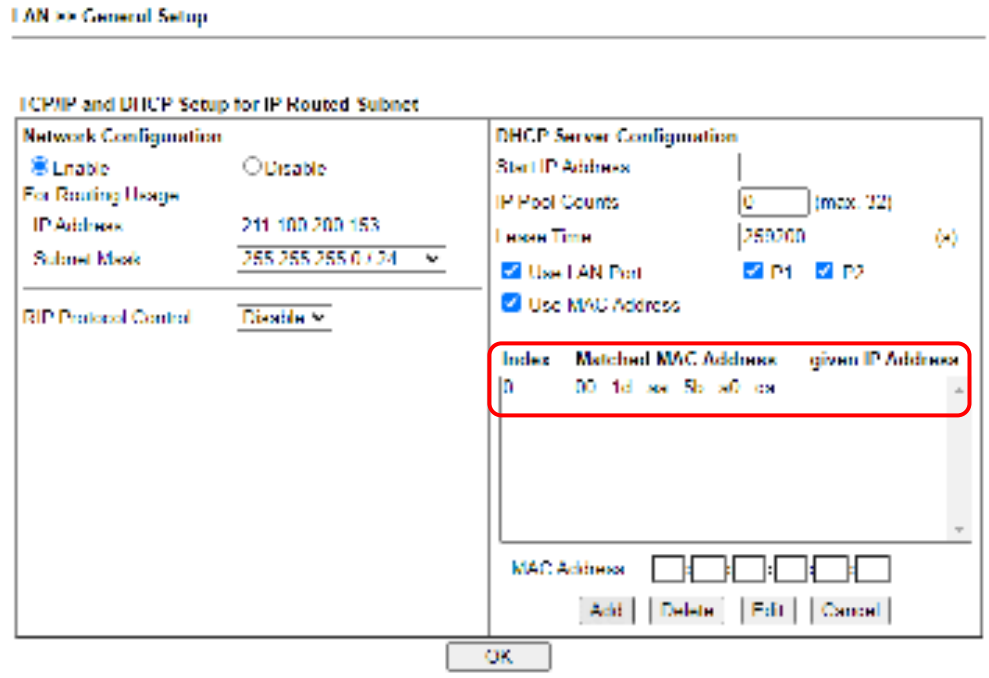
3. For the host behind Vigor Router to obtain the public IP address, we may:

   a. Configure a fixed IP/Subnet Mask on the host

   b. Set up DHCP IP Pool, enable Use LAN Port, and connect the host to the router on the specified LAN port (which is port 1 and 2 in this example)



c. Set up DHCP IP pool, enable Use MAC Address, add the host's MAC address to the table, and connect the host to the router from any of the LAN ports.

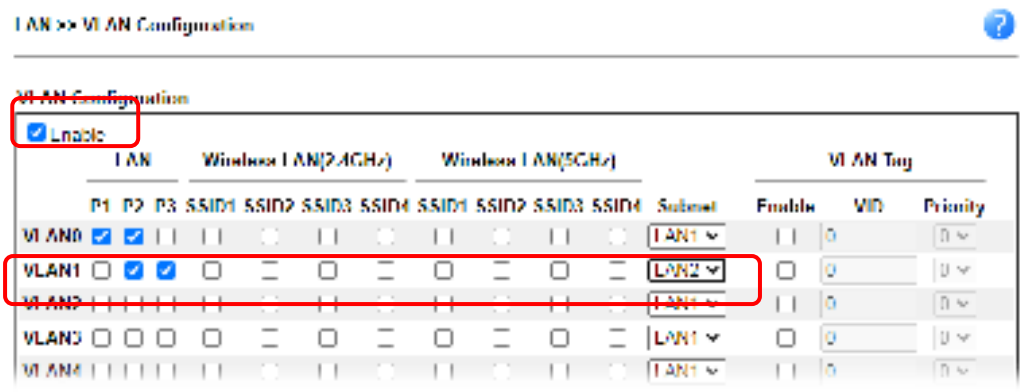


After finishing above configurations, host with a public IP 211.100.200.154/ mask 255.255.255.248/ Gateway IP 211.100.200.153 will be able to access Internet through Vigor Router.

Routing Usage LAN

We may also create a LAN subnet for routing usage. Here we take LAN 2 for example.

1. Go to **LAN >> VLAN**,

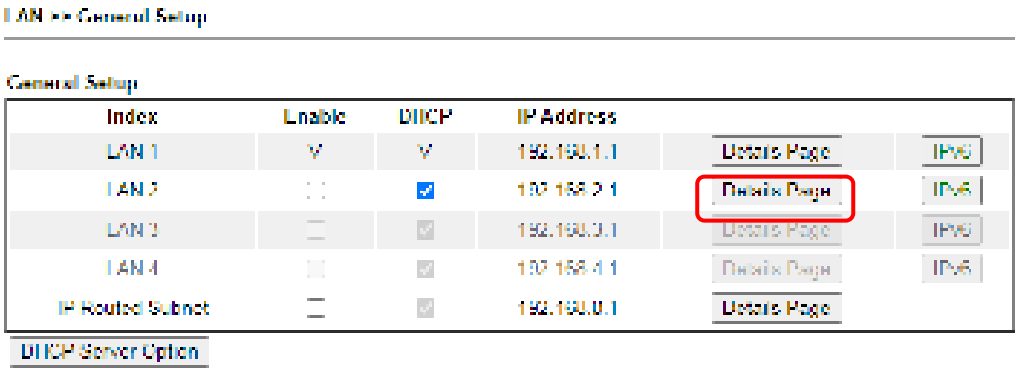


a. Enable VLAN Configuration.

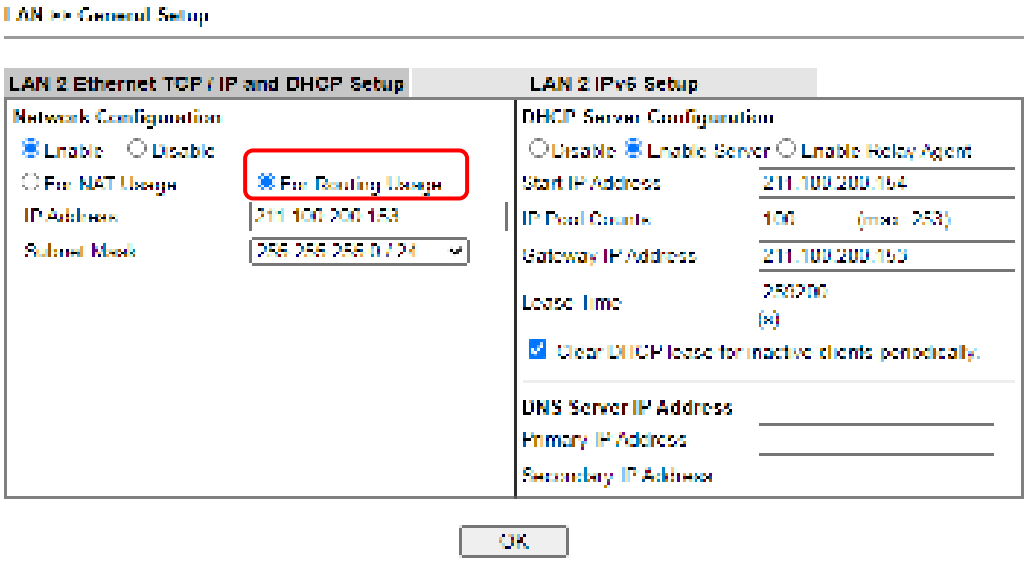
b. Set up a VLAN for LAN2 Subnet.

c. Specify the LAN ports that belongs to LAN2 subnet (which is port 5 and 6 in this example), note that these are the ports to which the host should connect.

2. Go to **LAN >> General Setup**, click on Details Page for LAN 2.



3. Set up TCP/ IP details for LAN 2,



a. Enable LAN2.

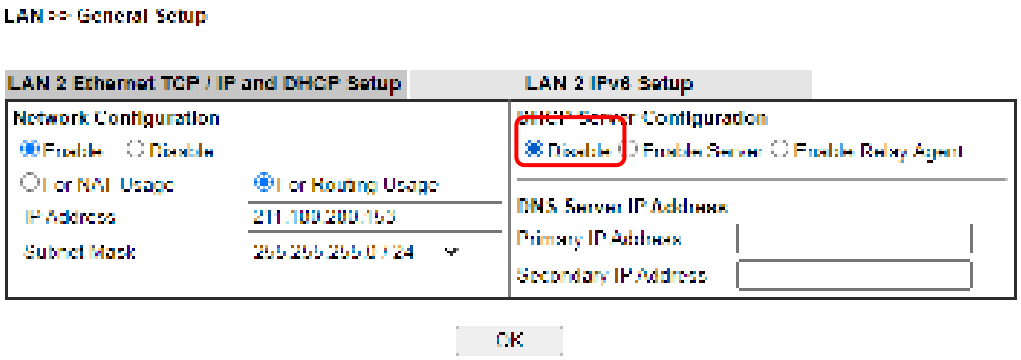
b. Select For Routing Usage.

c. Enter the IP Address for the router. Note that this could be the same as router's WAN IP.

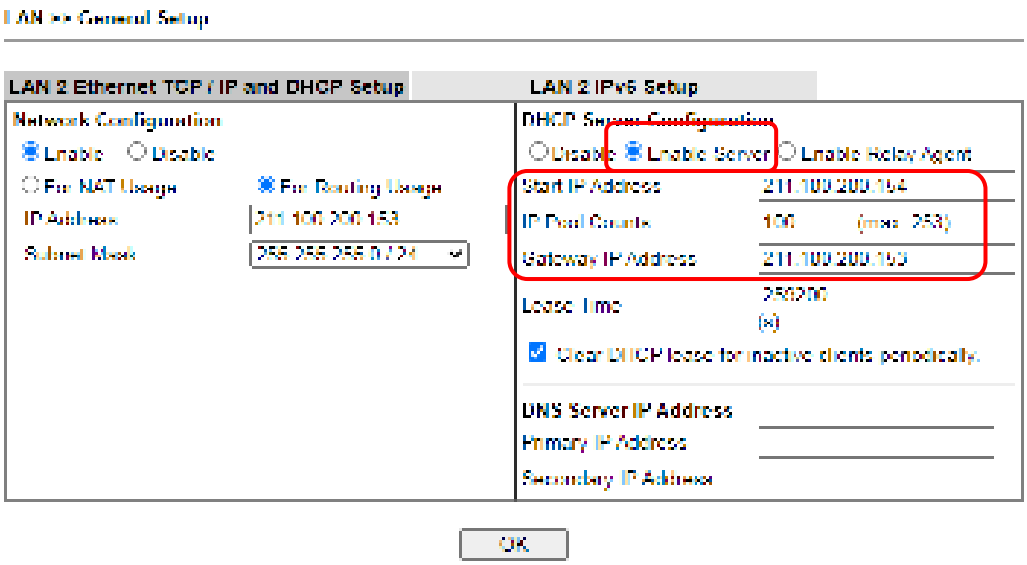
d. Enter the Subnet Mask according to ISP.

4. For DHCP Server Configuration, we may either:

- Disable DHCP Server, and manually set a fixed IP/ Subnet Mask on the host.



- Enable DHCP Server, and set up the DHCP IP pool according to IP range which the ISP provides.



After finishing the above configurations, PC or Server that connects to Port 5 or Port 6 with IP settings as IP 211.100.200.154/ mask 255.255.255.252/ Gateway IP 211.100.200.153 will be able to access Internet through Vigor Router.

Trouble-shooting

If PC with public IP address setting cannot access Internet after above configuration, please check:

- If the public IP address has been used by another device.
- If the router's WAN Access Mode is "Static or Dynamic IP", make sure the subnet mask of WAN interface is larger than that of LAN interface.

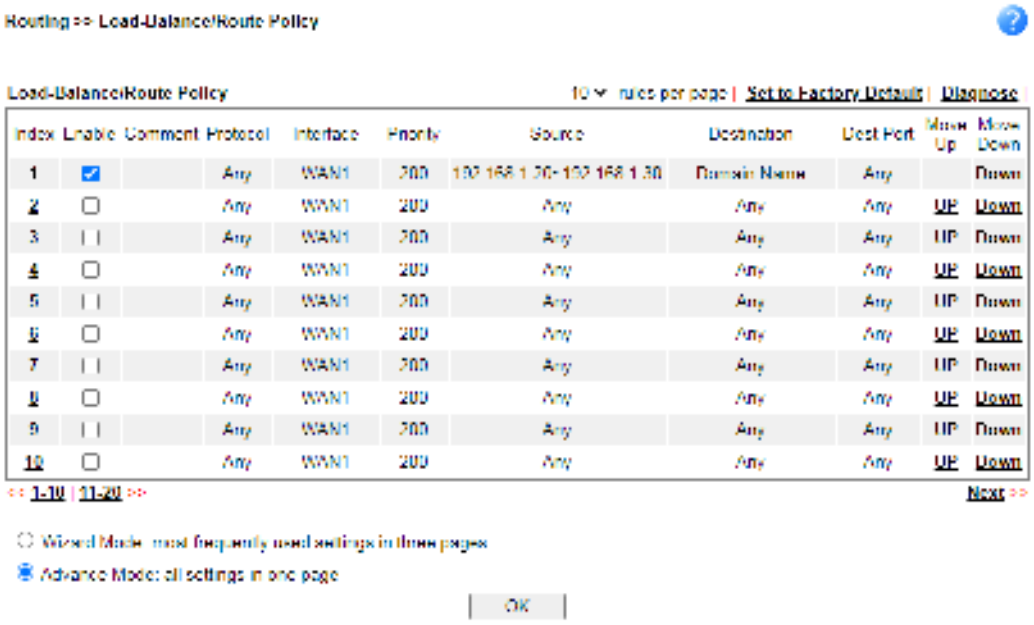
If none of the above helps, please change the host's Gateway IP from Vigor Router's IP (211.100.200.153) to the IP Gateway IP (211.100.200.158), and connect the PC to the ISP Modem directly and see if it can work.

A-3 Introduction to Load Balance/Route Policy

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

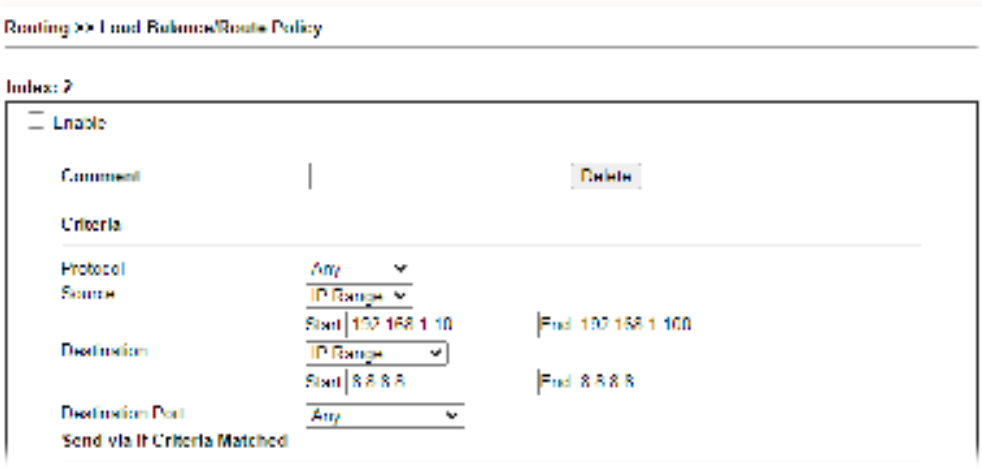
The Policy set in Load-Balance/ Route Policy always has higher priority than Default Route and Auto Load Balance set in **WAN >> General Setup**, and always has lower priority than the Firewall Rules. Administrator may also define a priority to this policy.

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



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

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



a. Select a Protocol.

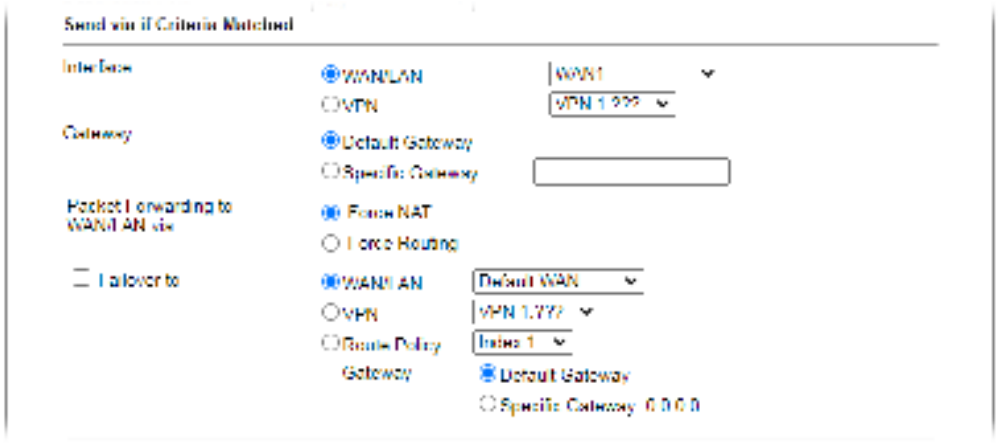
b. Enter the Source IP address range, the Source IP could be a single address if the Start and End are the same.

c. Enter the Destination IP address range.

d. Select the Destination Port.

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

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

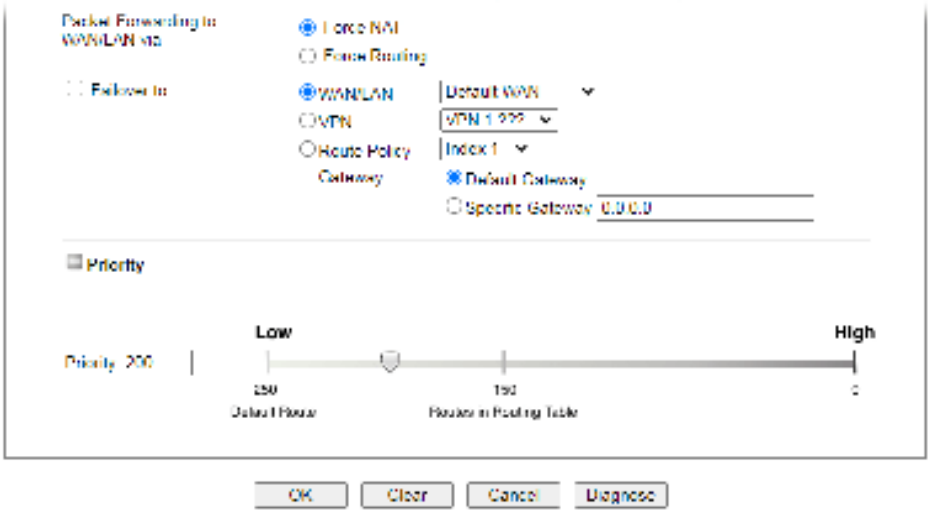


a. Select an Interface.

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

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

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



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

This page is left blank.

Part III Wireless LAN

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

III-1 Wireless LAN (2.4GHz/5GHz)

This function is used for "n" and "ac" models only.

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor2915 wireless series router (with "n", "n-plus" or "ac" in model name) is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

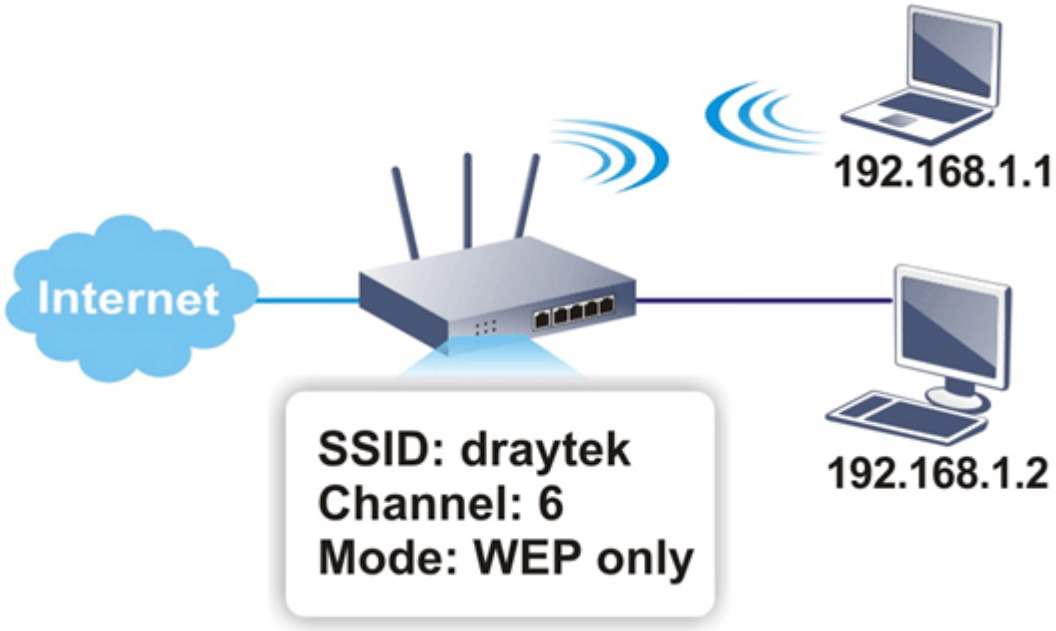
The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy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

Vigor2915 wireless router is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. Vigor2915 "ac" series router can support data rates up to 1.3 Gbps in 802.11ac 80 MHz channels. Vigor2915 "n" series router supports 802.11n up to 300 Mbps for 40 MHz channel operations.

Info

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

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



Multiple SSIDs

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

Real-time Hardware Encryption

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

Complete Security Standard Selection

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

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

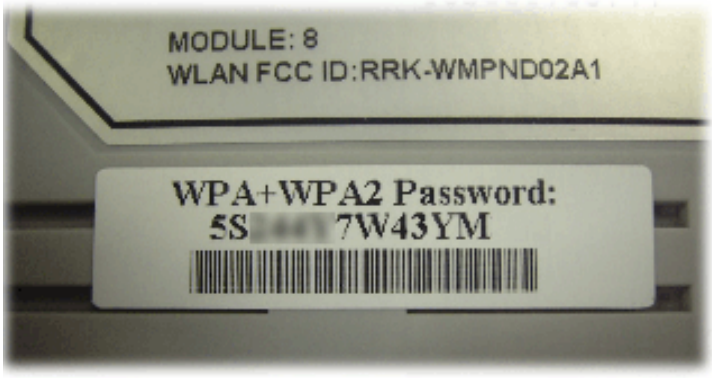
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

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

Info

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



Separate the Wireless and the Wired LAN- WLAN Isolation

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

Manage Wireless Stations - Station List

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

DFS Restrictions

Some of 5GHz channels are DFS channels which are governed radars. Without passing DFS certificate test, we can not open those DFS channels in Vigor router. We are working on DFS certification in Europe and open those channels by releasing new firmware once we receive DFS certification. According to DFS certificate in Europe, we will open channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, and 136.

At present, we will not open DFS channels in the USA because we do not have plan for DFS certification in the USA. Channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, and 136 will be restricted in the USA.

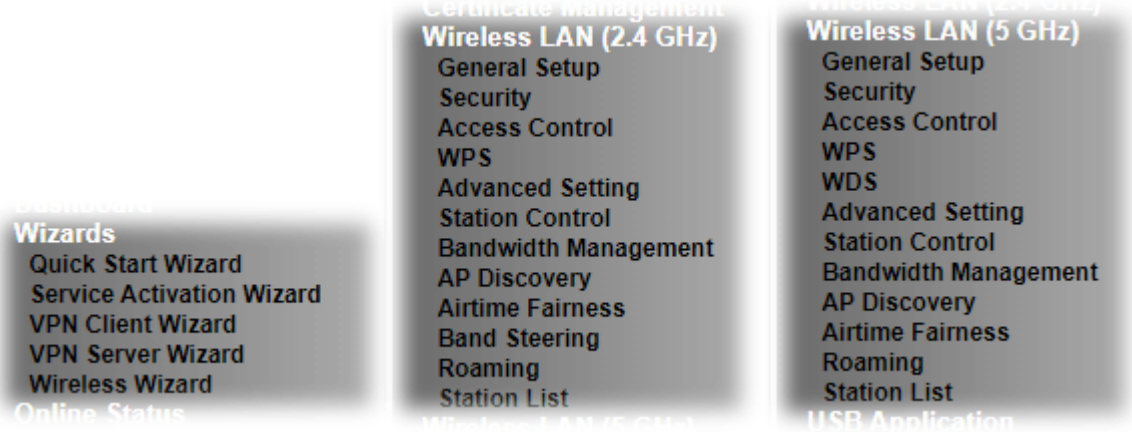
In some countries, there are restrictions on DFS channels as well. We will implement country code to restrict uncertified channels.

Below shows the menu items for Wireless LAN (2.4Ghz) and Wireless LAN(5GHz).

WPS

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

Web User Interface

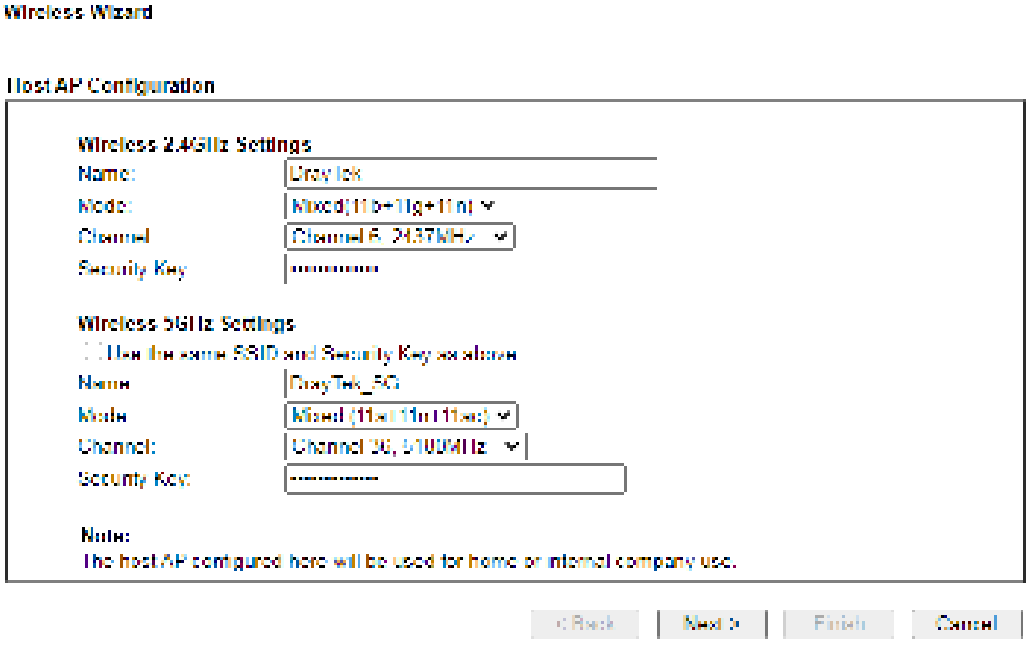


III-1-1 Wireless Wizard

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

Follow the steps listed below:

1. Open **Wizards>>Wireless Wizard**.
2. The screen of wireless wizard will be shown as follows. This page will be used for internal users in a company or your home. Besides, the settings will change based on different model of Vigor2915 series. In this case, Vigor2915ac is used as an example.

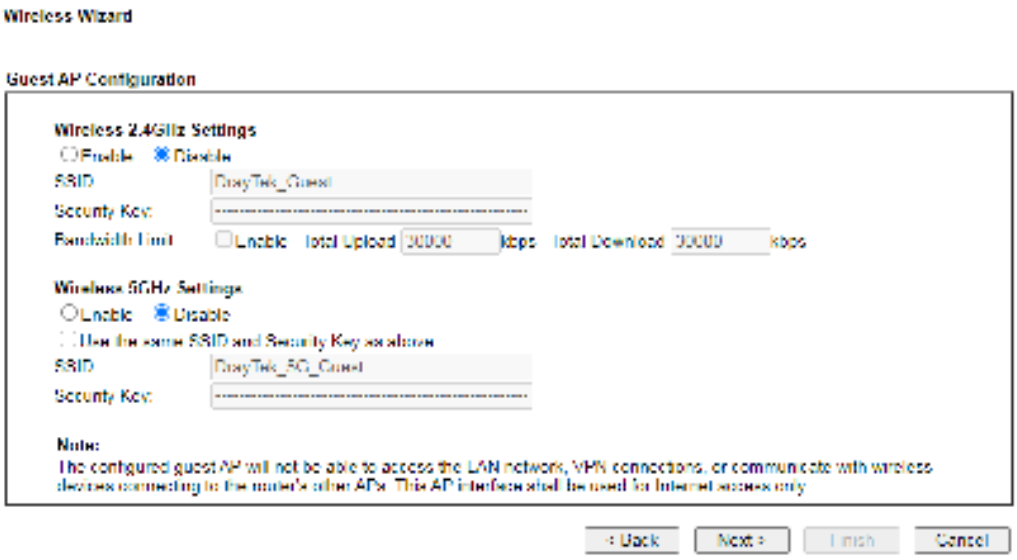


Available settings are explained as follows:

Item	Description

Wireless 2.4GHz Settings	
Name	Enter the SSID name of this router for wireless 2.4GHz. The default name is defined with DrayTek. Change the name if required.
Mode	At present, the router can connect to 11n Only, 11g Only, Mixed (11b+11g), Mixed (11a+11n), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Wireless 5GHz Settings – Such part is available when your Vigor router supports wireless 5GHz.	
Use the same SSID and Security Key as above	Check the box to use the same settings configured above.
Name	Enter the SSID name of this router for wireless 5GHz.
Mode	At present, the router can connect to 11a Only, 11n Only (5GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 36. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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



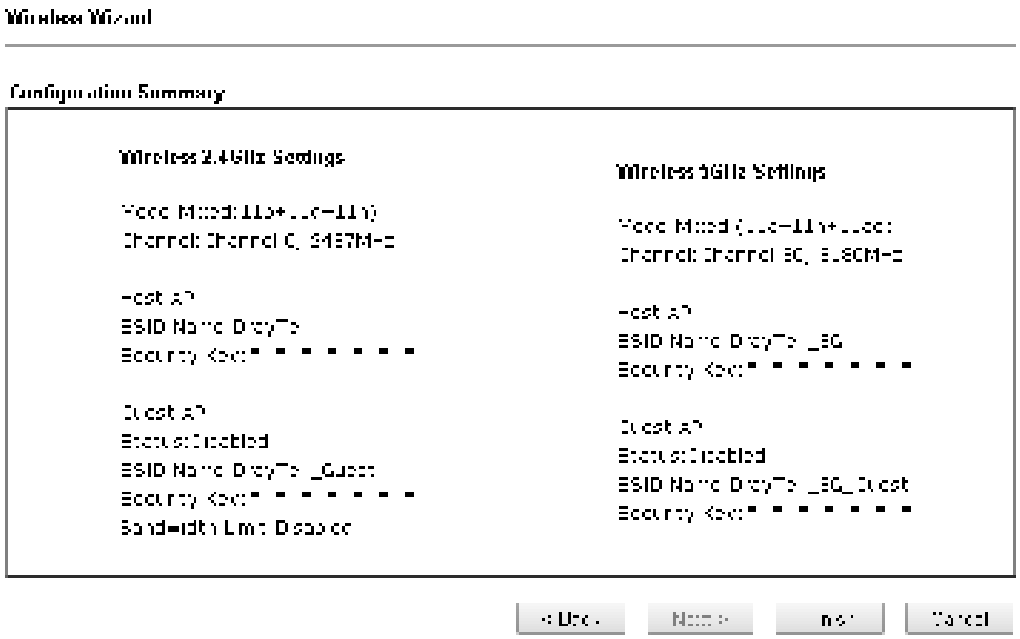
Available settings are explained as follows:

Item	Description
Wireless 2.4GHz Settings	
Enable/Disable	Click it to enable or disable settings in this page.
SSID	Enter the SSID name of this router. (SSID1)
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Bandwidth Limit	**Enable** – Check the box to set the bandwidth limit for data transmission in upload and download. It controls the data transmission rate through wireless connection. **Total Upload** – Check Enable and Enter the transmitting rate for data upload. Default value is 30,000 kbps. **Total Download** – Enter the transmitting rate for data download. Default value is 30,000 kbps.
Wireless 5GHz Settings	
Enable/Disable	Click it to enable or disable settings in this page.
Use the same SSID and Security Key as above	Check the box to use the same settings configured above.
SSID	Enter the SSID name of this router. (SSID2)
Security Key	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64

	Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

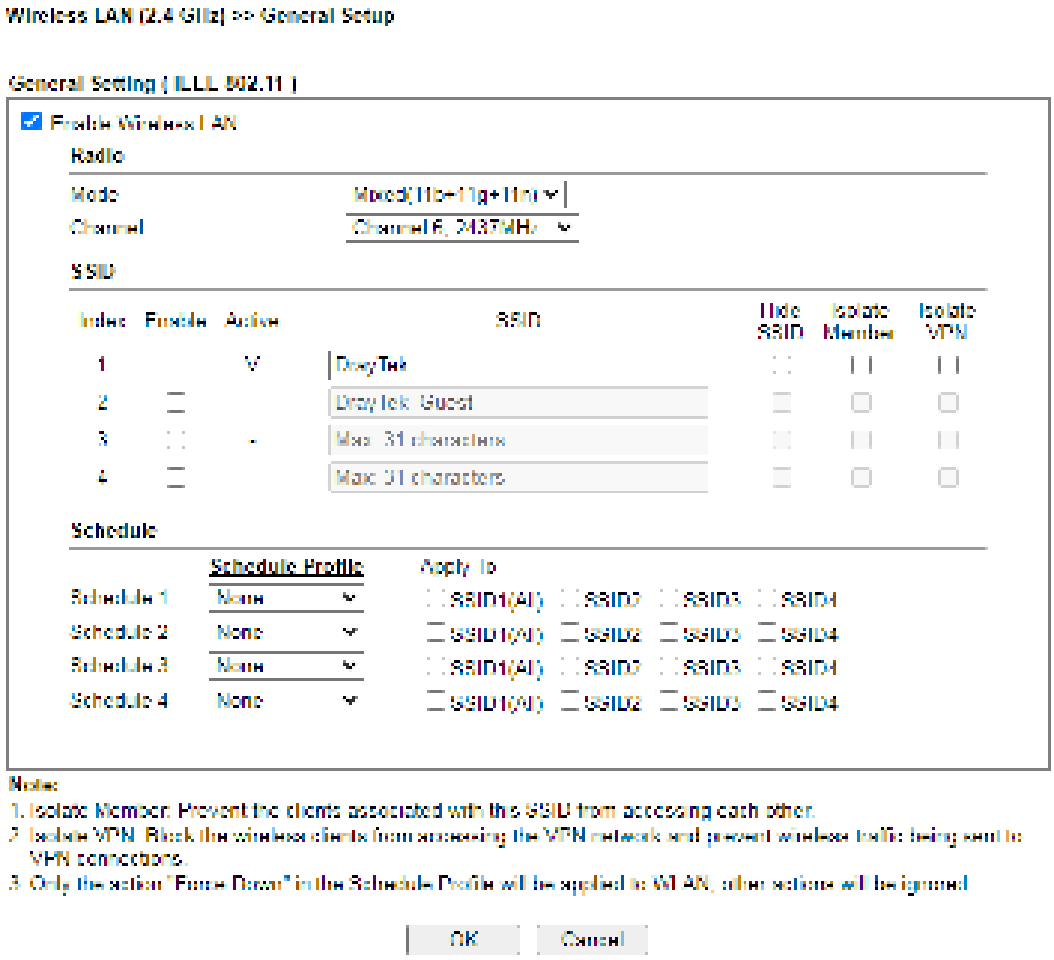
5. The following page will display the configuration summary for wireless setting.



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

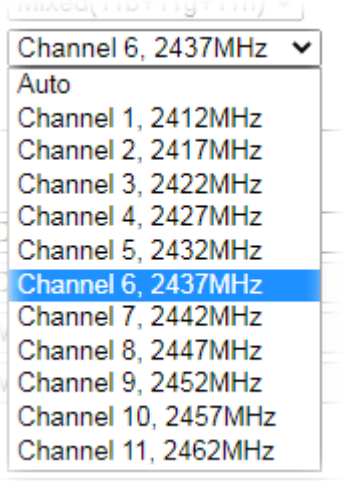
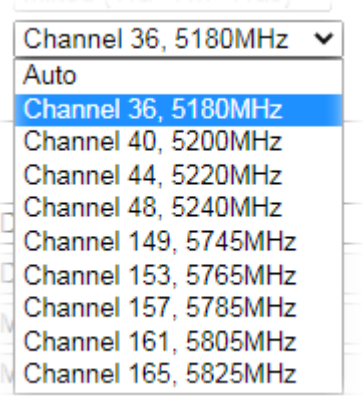
III-1-2 General Setup

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



Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	**2.4GHz in "n" and "ac" model**: At present, the router can connect to 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode. **5 GHz in "n" model:** At present, the router can connect to 11a Only, 11n Only (5 GHz), Mixed (11a+11n) stations simultaneously. Simply choose Mixed (11a+11n) mode. **5 GHz in "ac" model:** At present, the router can connect to 11a Only, 11n Only (5 GHz), Mixed (11a+11n) and Mixed (11a+11n+11ac) stations simultaneously. Simply choose Mixed (11a+11n+11ac) mode. **Note**: 802.11b/ g operates on 2.4G band, 802.11a operates

	on 5G band, 802.11n operates on either 2.4G or 5G band, and 802.11ac operates on 5G band only.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. **2.4GHz**:  **5 GHz**:  **Note:** For the restricted channels on DFS, please refer to 4.18.1 Basic Concepts for more detailed information.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
Isolate	**Member** –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. **VPN** – Check this box to make the wireless clients (stations)

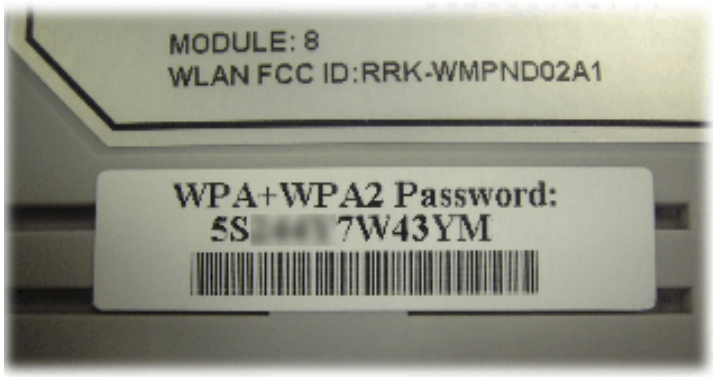
	with different VPN not accessing for each other.
Schedule Profiles	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
Apply To	Selected SSID (2 / 3 / 4) will be forced up / down based on the schedule profile used. Check SSIDx(All) to select all of the SSID items.

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

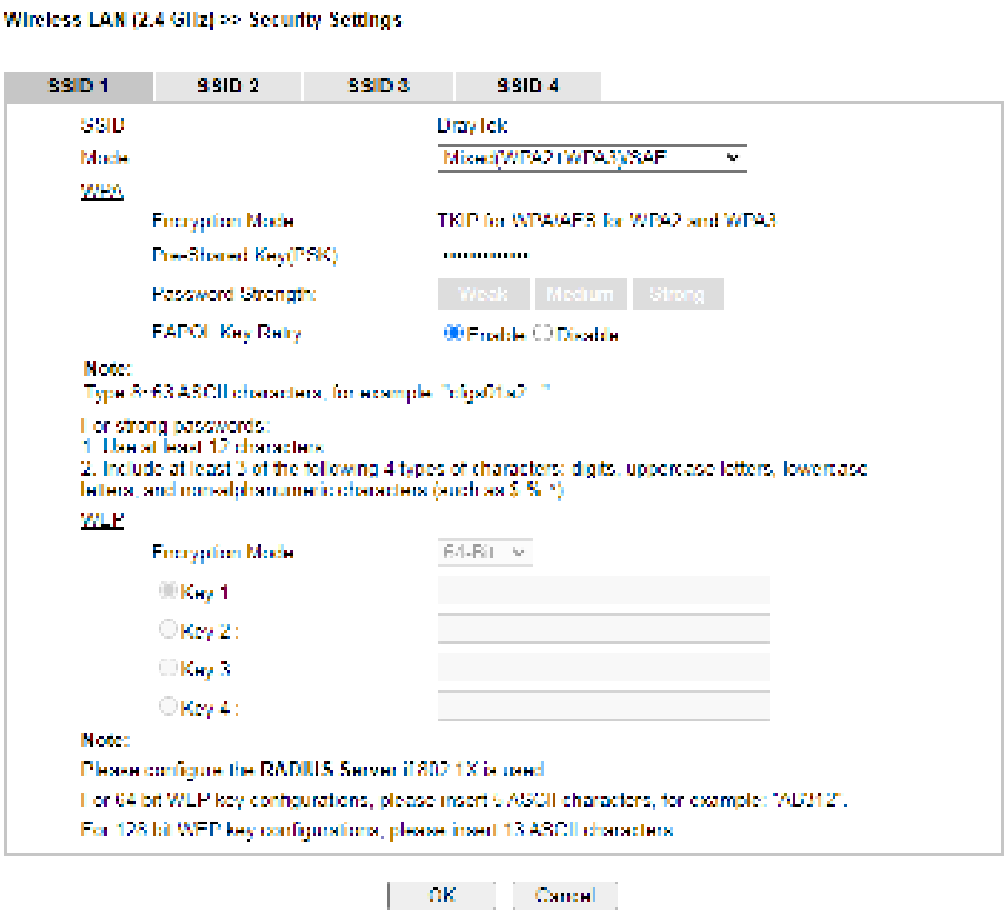
III-1-3 Security

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

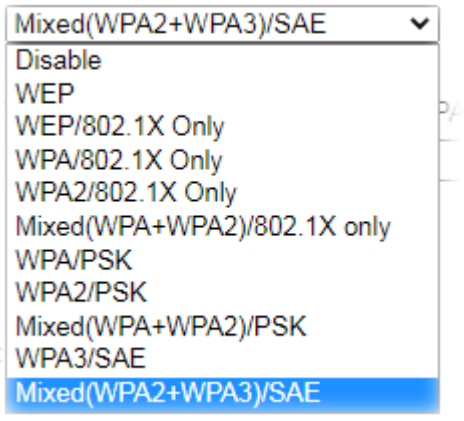
The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



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



Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.  **Info** — You should also set **Wireless LAN(2.4GHz) 802.1X Setting** simultaneously if 802.1x mode is selected. **Disable** - Turn off the encryption mechanism. **WEP-**Accepts only WEP clients and the encryption key should be entered in WEP Key. **WEP/802.1x Only -** Accepts only WEP clients and the

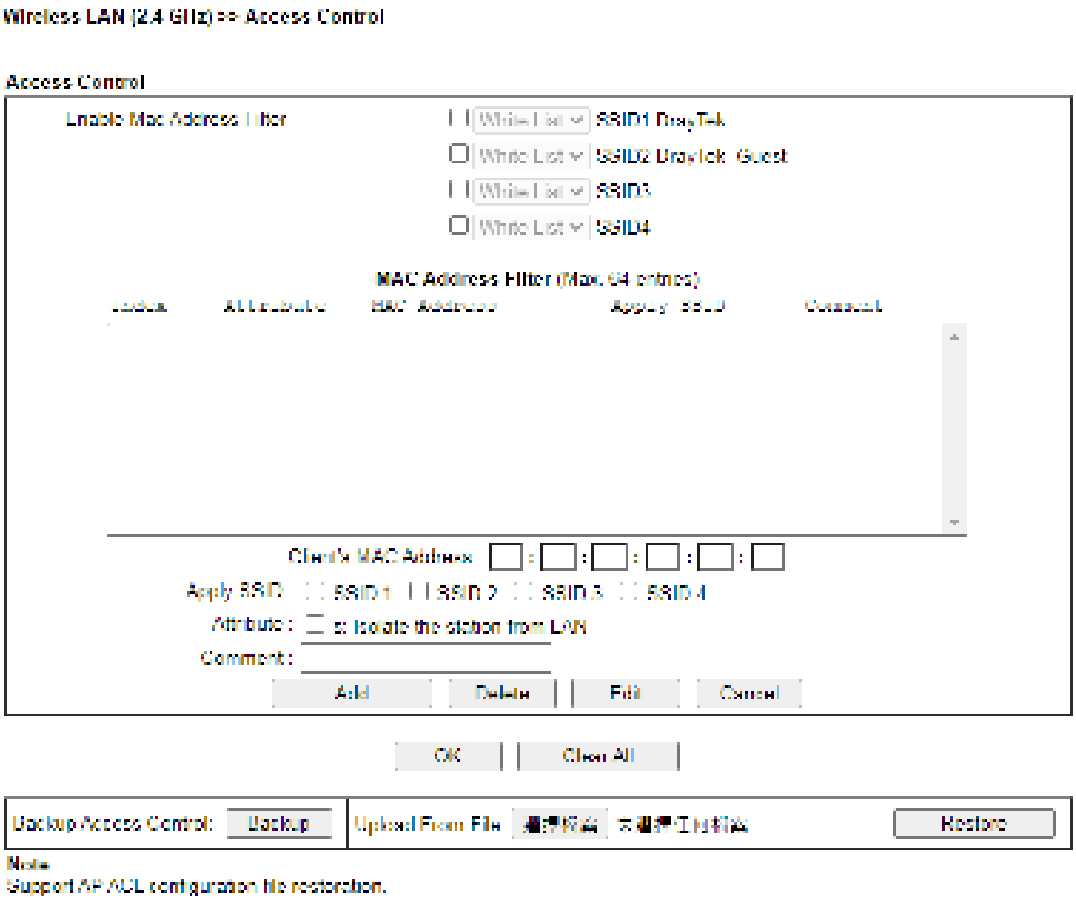
	encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA/802.1x Only-** Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA2/802.1x Only-** Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **Mixed (WPA+WPA2/802.1x only) -** Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. **WPA/PSK-**Accepts only WPA clients and the encryption key should be entered in PSK. **WPA2/PSK-**Accepts only WPA2 clients and the encryption key should be entered in PSK. **Mixed (WPA+ WPA2)/PSK -** Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). **Password Strength** – The system will display the password strength (represented with the word of weak, medium or strong) of the PSK specified above. **EAPOL Key Retry** - The default setting is "Enable". It can make sure that the key will be installed and used once in order to prevent key reinstallation attack.
WEP	**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) **128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D). All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

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

III-1-4 Access Control

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

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



Available settings are explained as follows:

Item	Description
Enable Mac Address Filter	Select the SSIDs that you would like to have MAC Address filter enabled. Select **White List** or **Black List** in the combo box next to each enabled SSIDs. **White List** - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list. **Black List** - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access

	control list.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Comment	Type a brief description for the specified client's MAC address.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.
Backup Access Control	Settings on this web page can be saved as a file which can be restored in the future by this device or other device.
Upload From File	Restore wireless access control settings and applied onto this device.

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

III-1-5 WPS

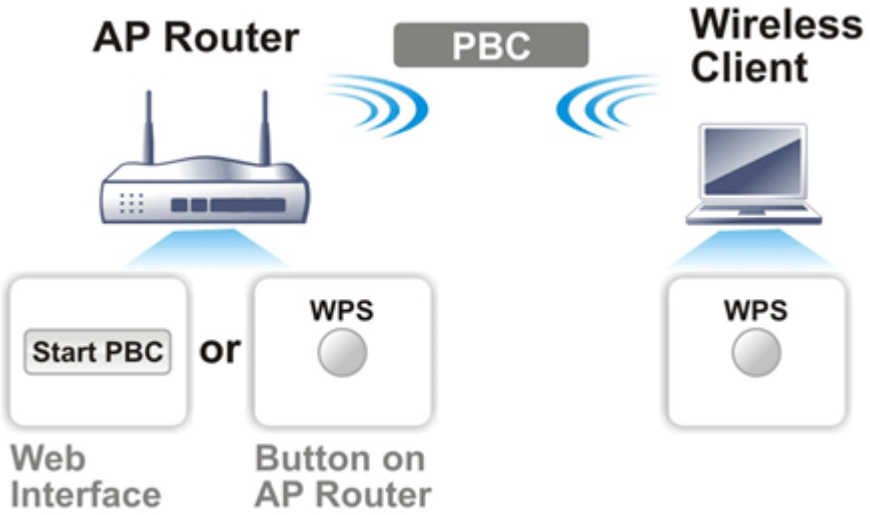
WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

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

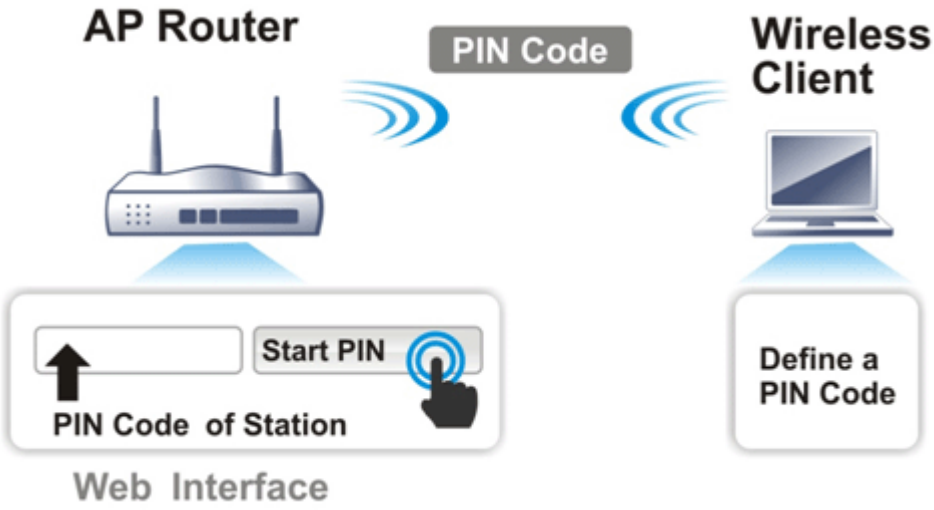
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

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

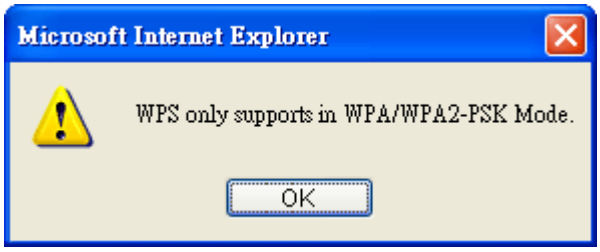
- On the side of Vigor2915 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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

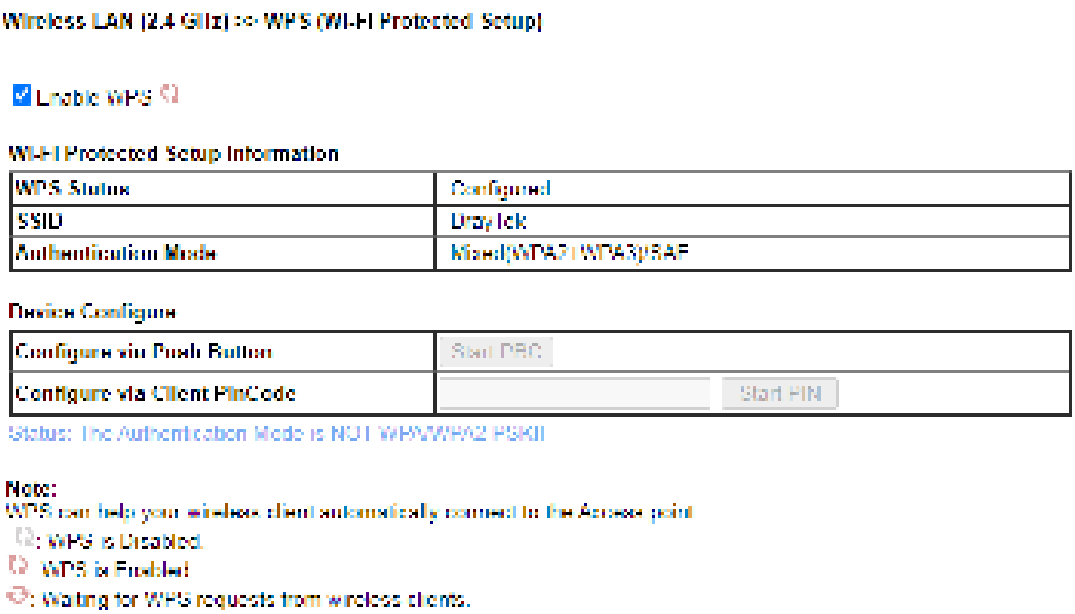


- For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



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

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



Available settings are explained as follows:

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

III-1-6 WDS (for 5GHz only)

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

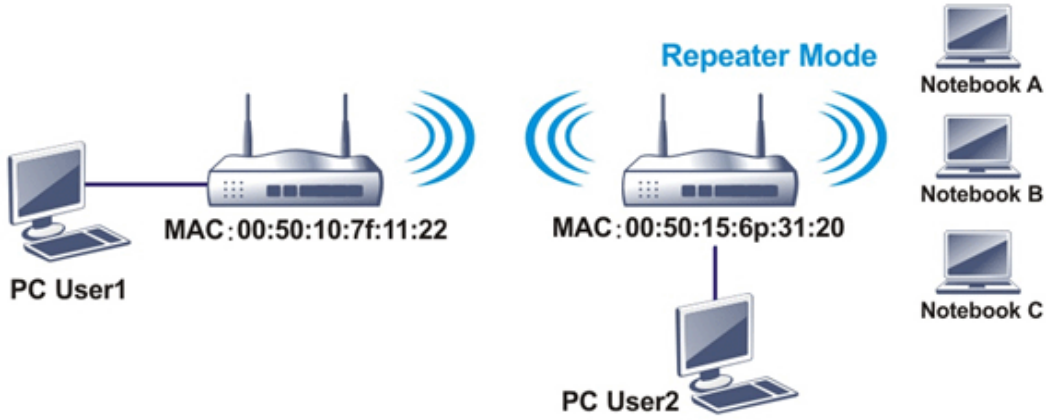
- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

Refer to the following table:

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

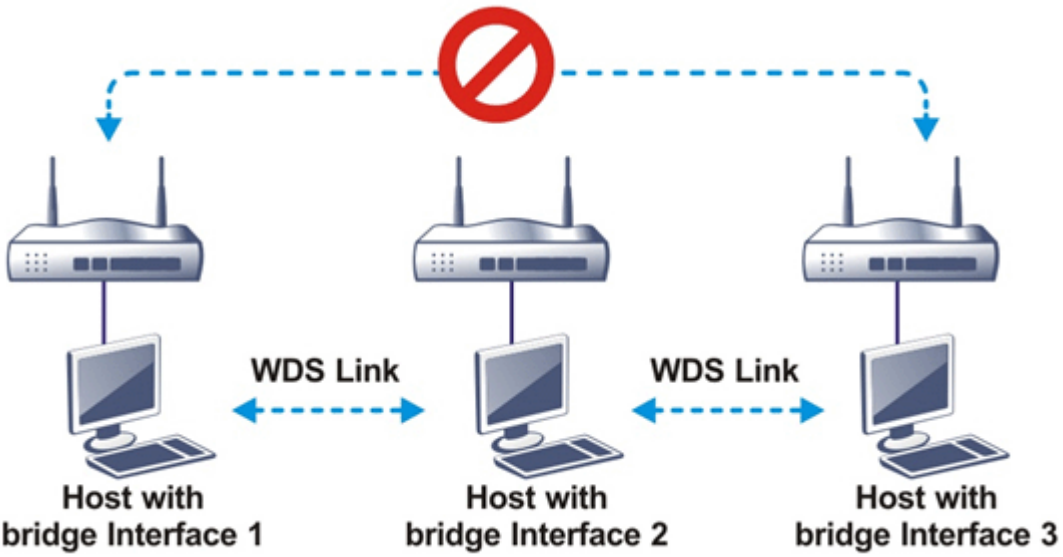
To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

The application for the WDS-Repeater mode is depicted as below:

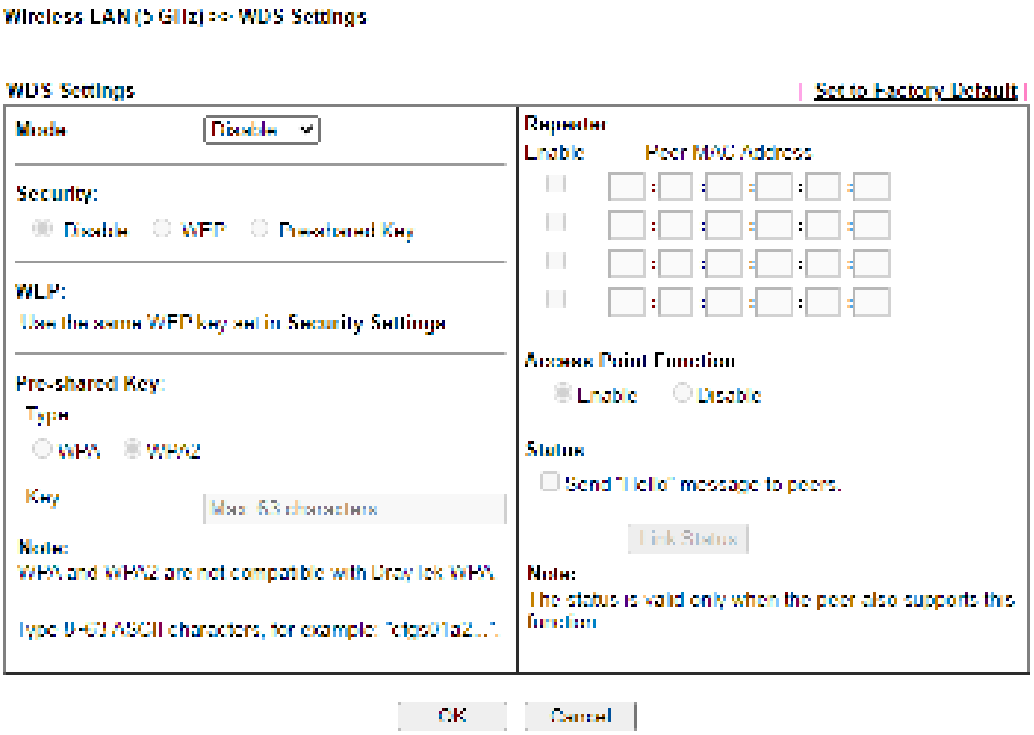


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words,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

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



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



Available settings are explained as follows:

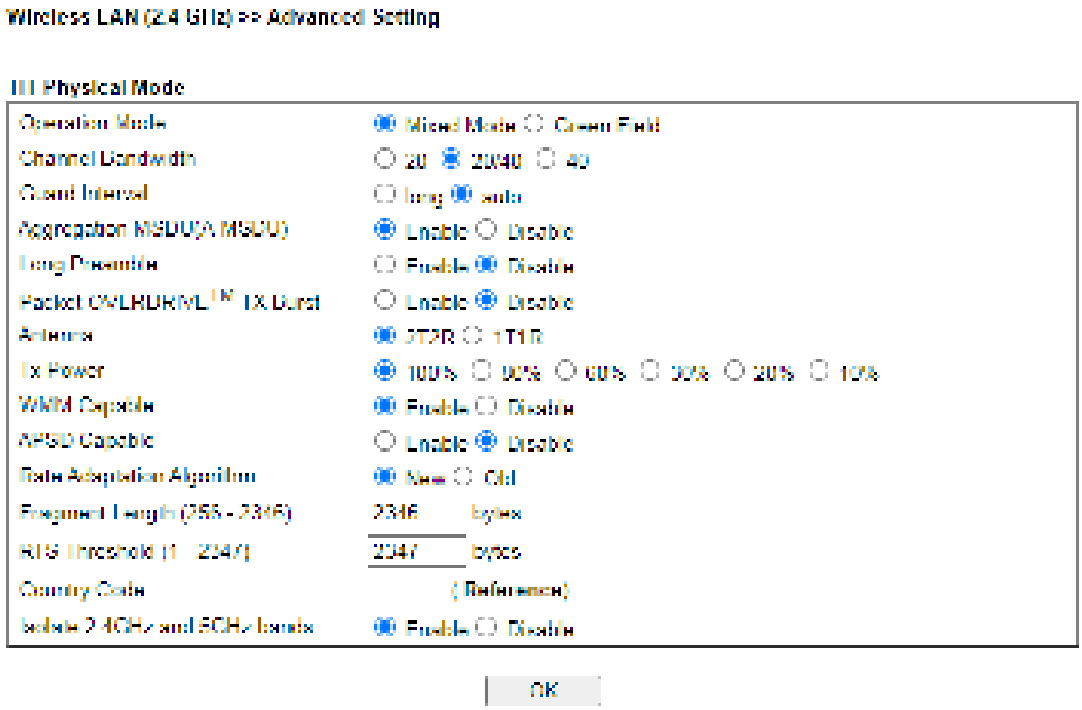
Item	Description
Mode	Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Repeater** mode is for the second one.
Security	There are three types for security, **Disable** and **Pre-shared key**. The setting you choose here will make the following Pre-shared key field be valid or not. Choose one of the types for the router.
Pre-shared Key	When **Pre-Shared Key** is selected as Security above, configure the following settings if required. **Type** – There are some types for you to choose. **WPA** and **WPA2** are used for WDS devices (e.g.2925n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. **Key** – Set the encryption key in this field. Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by "0x".
Repeater	If you choose **Repeater** as the connecting mode, please type in the peer MAC address (of VigorAP/ Vigor router required to make connection with such Vigor router and used to extend the wireless signal) in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.
Access Point Function	Click **Enable** to make this router serve as an access point. When **Repeater** is set as WDS Mode, click **Enable** to use such function. Click **Disable** if **Bridge** is set as WDS Mode.

Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

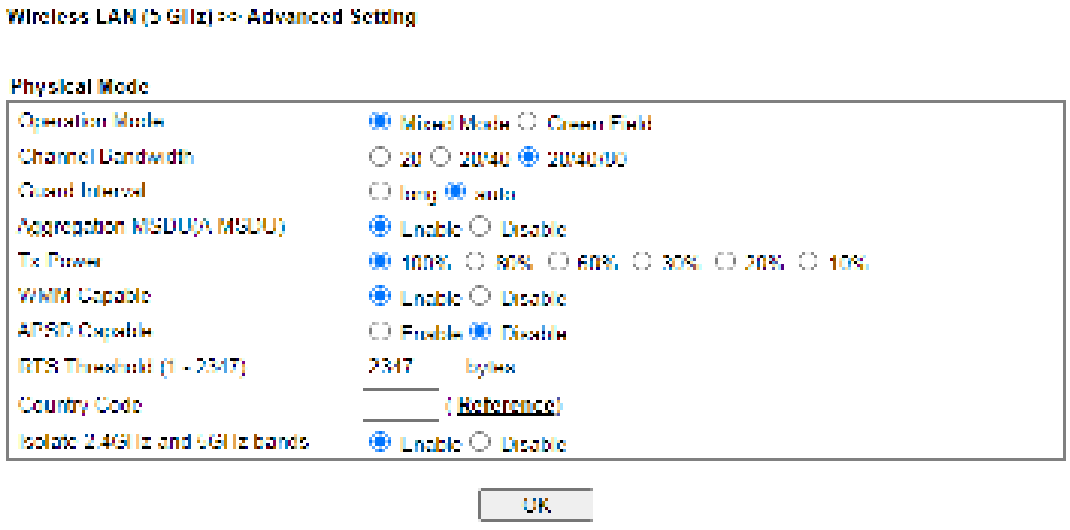
After finishing all the settings here, please click **OK** to save the configuration.

III-1-7 Advanced Setting

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

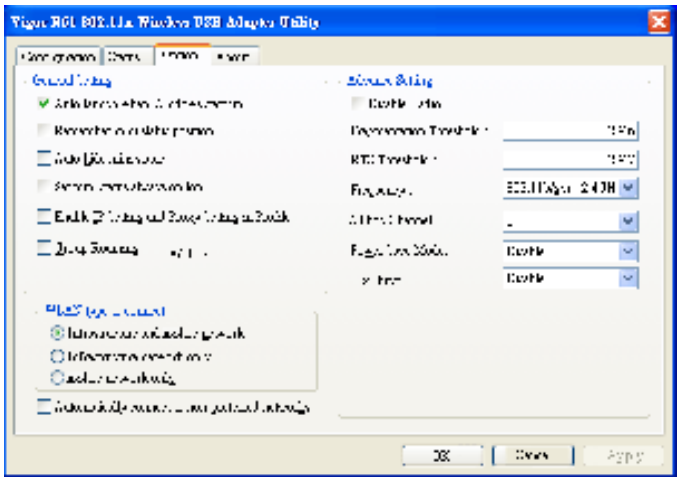


or,



Available settings are explained as follows:

Item	Description
Operation Mode	**Mixed Mode** –the router can transmit data with the ways supported in both 802.11a/ b/ g and 802.11n standards.

	However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected. **Green Field** –to get the highest throughput, please choose such mode. Such mode can make the data transmission happen between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/ b/ g.
Channel Bandwidth	**20-** the router will use 20Mhz for data transmission and receiving between the AP and the stations. **40-** the router will use 40Mhz for data transmission and receiving between the AP and the stations. **20/40** –Vigor Router will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose **auto** as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is **Enable.**
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click **Enable** to use **Long Preamble** if needed to communicate with this kind of devices.
Packet-OVERDRIVE (for 2.4GHz only)	This feature can enhance the performance in data transmission about 40%* (by checking **Tx Burst**). It is active only when both the Access Point and Station (in wireless client) support and invoke this function at the same time. **Note:** Vigor N61 wireless adapter supports this function. Therefore, you can install it on your PC to take advantage of Packet-OVERDRIVE (Refer to the following picture of Vigor N61 wireless utility window: choose Enable for TxBURST on the **Option** tab). 

	 Info * Real transmission rate depends on the environment of the network.
Antenna **(for 2.4GHz only)**	Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R.
TX Power	Set the power percentage for transmission signal of access point. The greater the value is, the higher intensity of the signal will be.
WMM Capable	WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM. To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. The default setting is **Disable**.
Rate Adaptation Algorithm	Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old". Sets the way the Wireless transmission rate is adjusted dynamically. In most cases, selecting "New" will result in better performance than "Old".
Fragment Length **(256 – 2346)**	Set the Fragment threshold. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold (1 – 2347)	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.
Country Code	Vigor router broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: ● No matter such function is enabled or disabled, clients

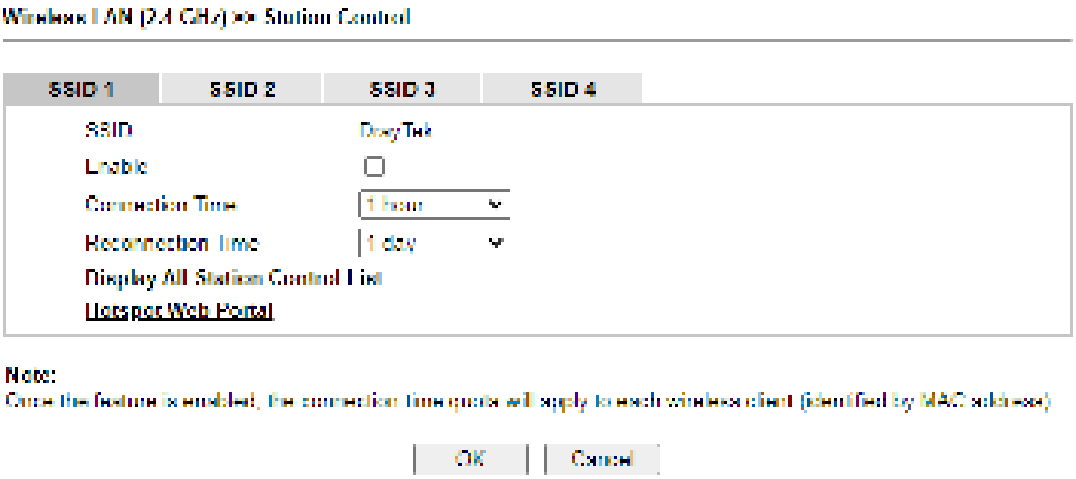
	using WLAN 2.4GHz and 5GHz can communicate for each other if **Isolate Member** (in **Wireless LAN>>General Setup**) is NOT enabled for such SSID. ● Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.

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

III-1-8 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect Vigor router. If such function is not enabled, the wireless client can connect Vigor router until the router shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as "1 hour" and reconnection time can be set as "1 day". Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.



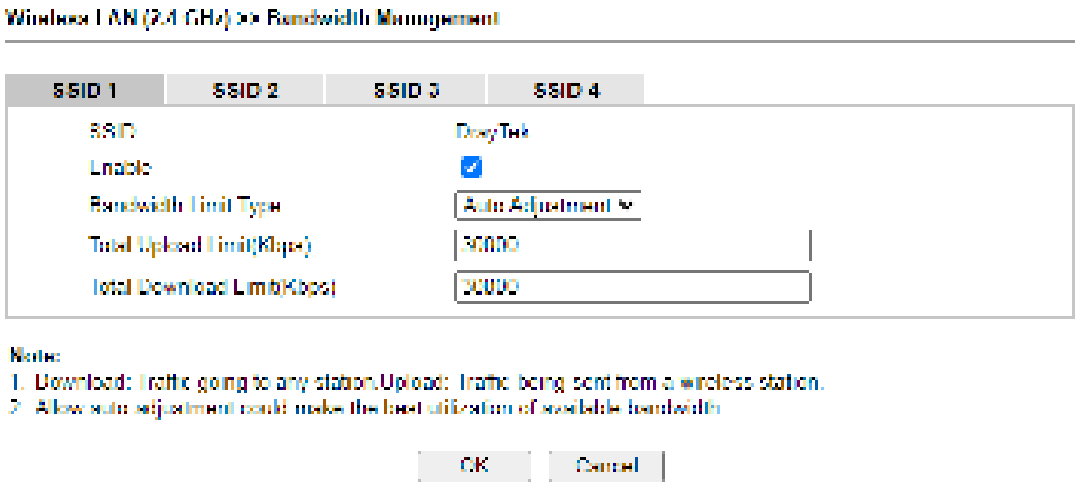
Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting / reconnecting to Vigor router. Or, Enter the duration manually when you choose **User defined**.
Display All Station Control List	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.
Hotspot Web Portal	Click it to access in to **Hotspot Web Portal** page for modifying the settings if required.

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

III-1-9 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Available settings are explained as follows:

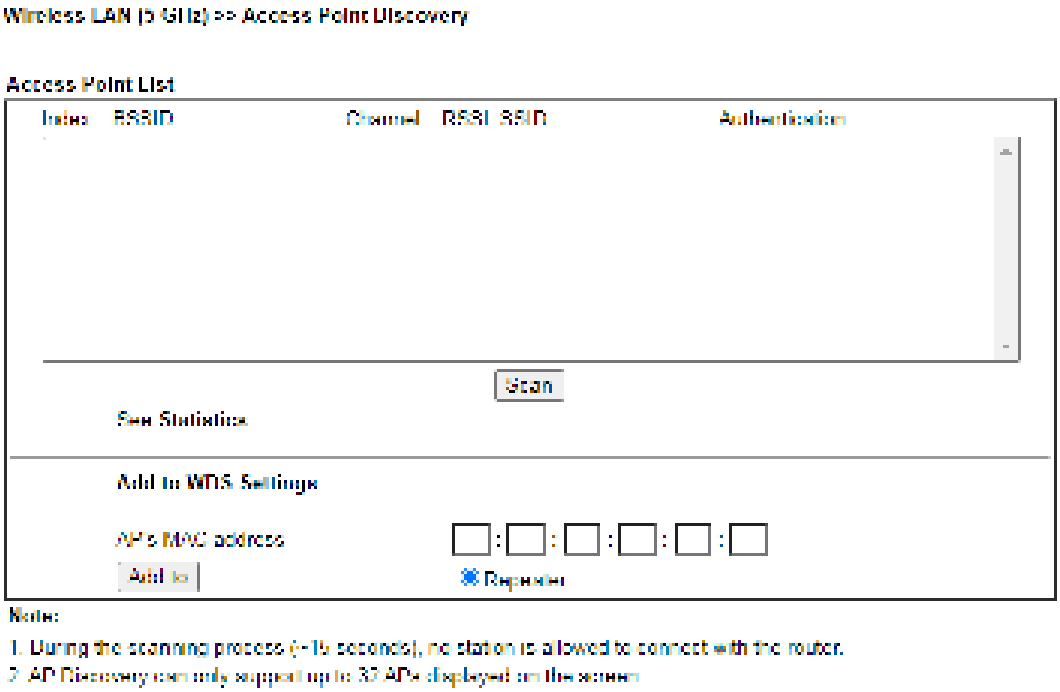
Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Bandwidth Limit Type	**Auto Adjustment -** Bandwidth limit is determined by the system automatically. **Per Station Limit** –Bandwidth limit is determined according to the limitation of the wireless client.
Total Upload Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to Vigor2915.
Total Download Limit	It is available when Auto Adjustment is selected. Type a value to define the maximum data clientstations connecting to Vigor2915.
Upload Limit	It is available when Per Station Limit is selected. Type a value to define the maximum data traffic (uploading) for each wireless client connecting to Vigor2915.
Download Limit	It is available when Per Station Limit is selected Type a value to define the maximum data traffic (downloading) for each wireless client connecting to Vigor2915.

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

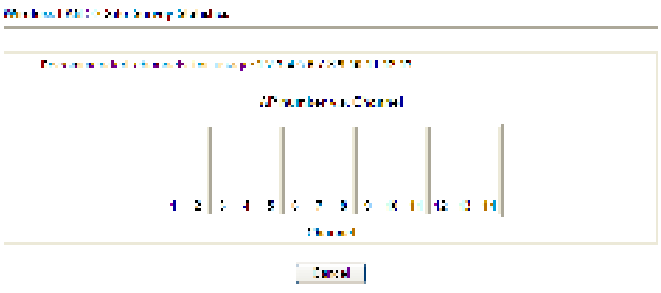
III-1-10 AP Discovery

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

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



Available settings are explained as follows:

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

III-1-11 Airtime Fairness

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

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

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

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

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

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

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through Vigor router. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).

To improve this problem, Airtime Fairness is added for Vigor router. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).

It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime

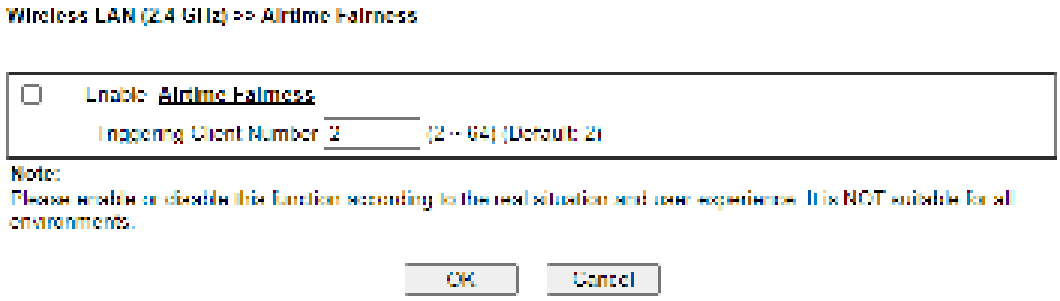
Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

(1) Many wireless stations.

(2) All stations mainly use download traffic.

(3) The performance bottleneck is wireless connection.



Available settings are explained as follows:

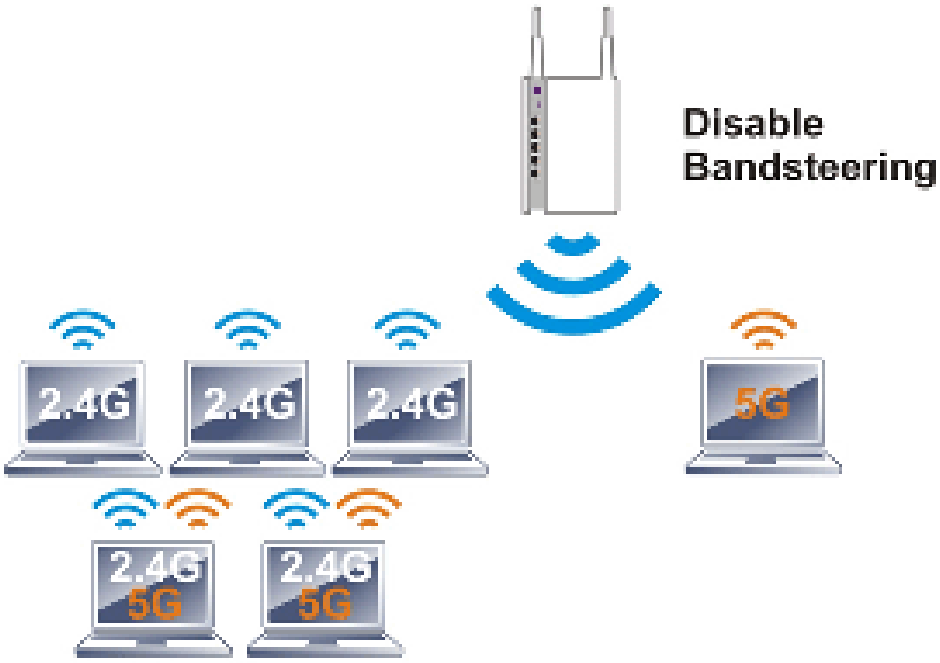
Item	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. **Airtime Fairness** – Click the link to display the following screen of airtime fairness note. **Triggering Client Number** – Airtime Fairness function is applied only when active station number achieves this number.

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

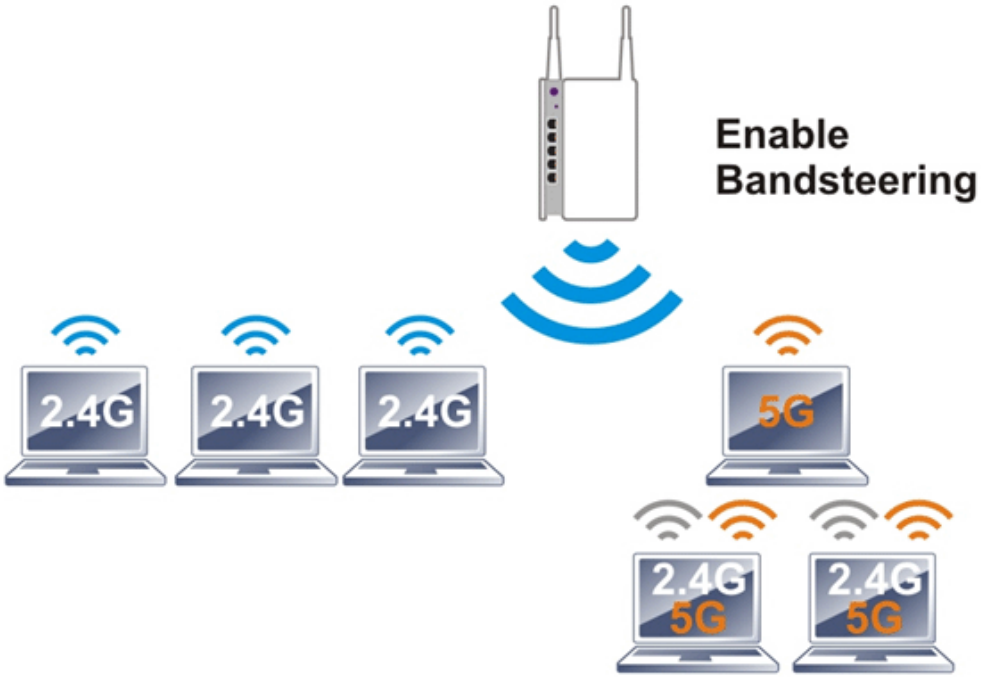
Info	Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

III-1-12 Band Steering (for 2.4GHz only)

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



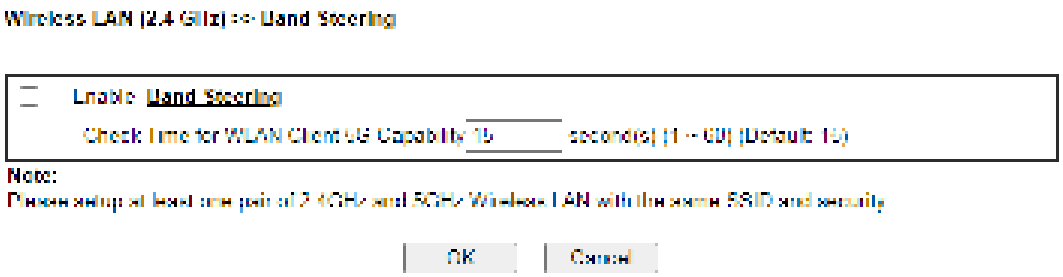
If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



Info

To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

Open **Wireless LAN (2.4GHz)>>Band Steering** to get the following web page:

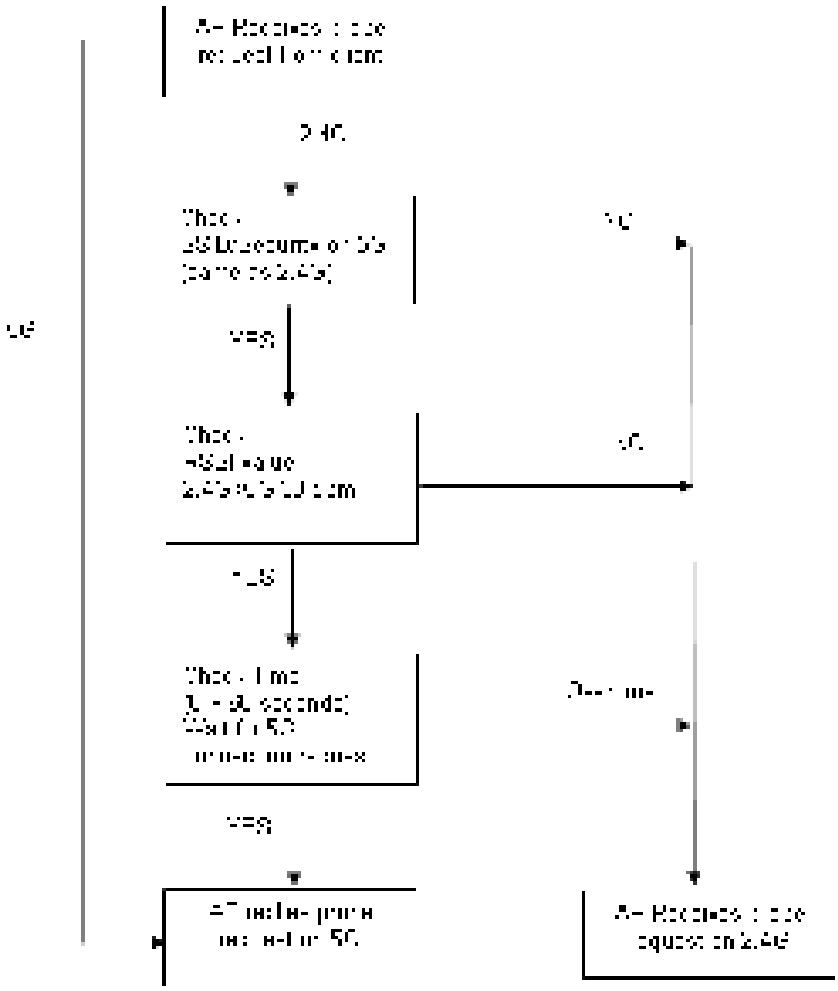


Available settings are explained as follows:

Item	Description
Enable Band Steering	If it is enabled, Vigor router will detect if the wireless client is capable of dual-band or not within the time limit. **Check Time**... –If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client.

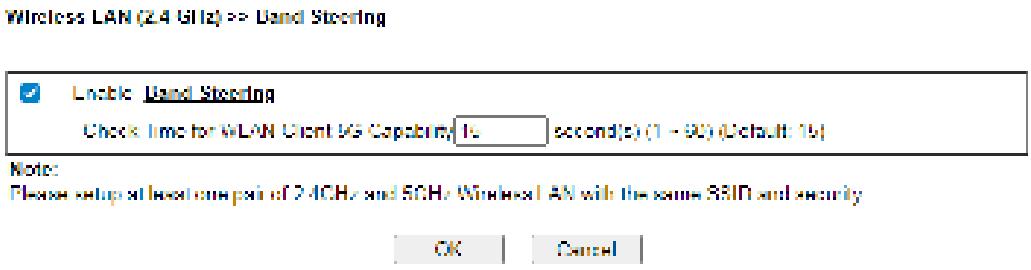
After finishing this web page configuration, please click **OK** to save the settings.

Below shows how Band Steering works.



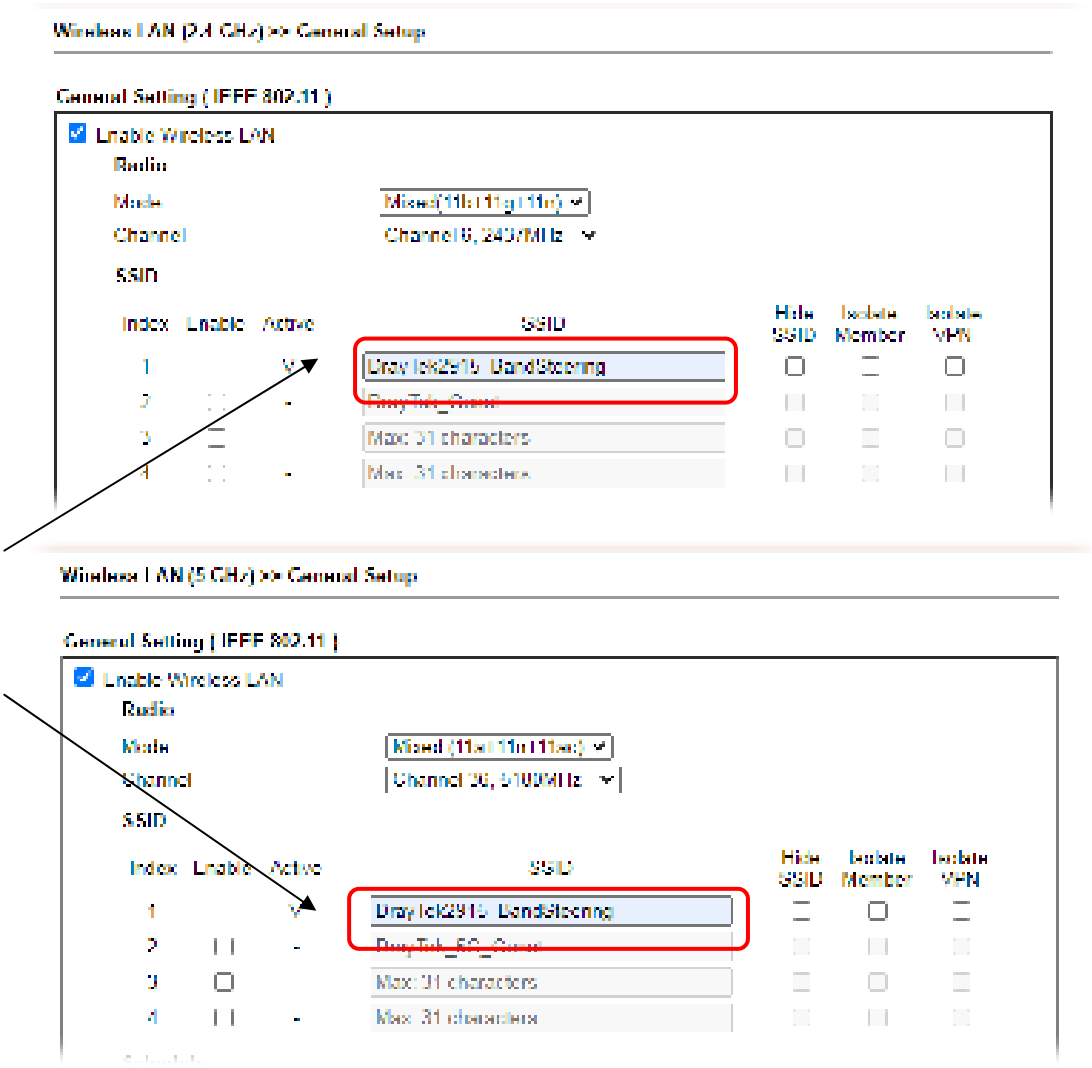
How to Use Band Steering?

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

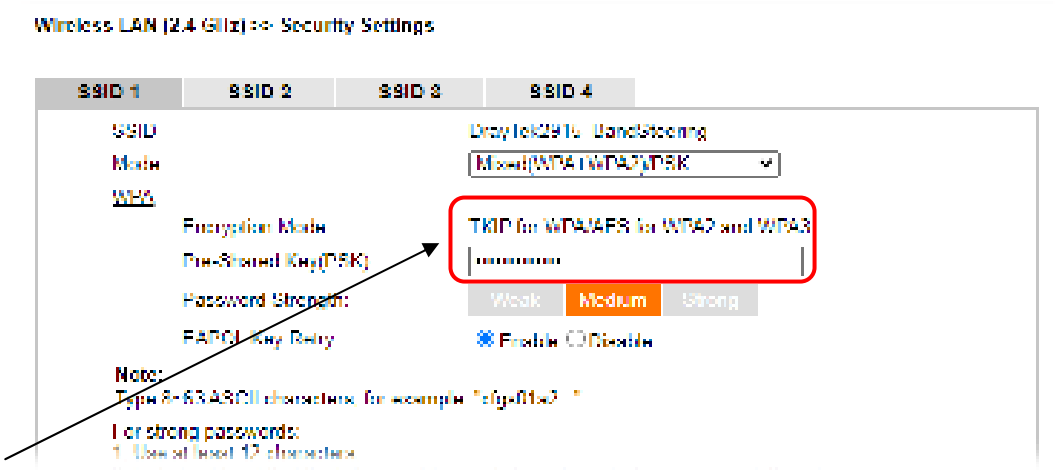


3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *DrayTek2915_BandSteering* for both pages. Click **OK** to save the settings.

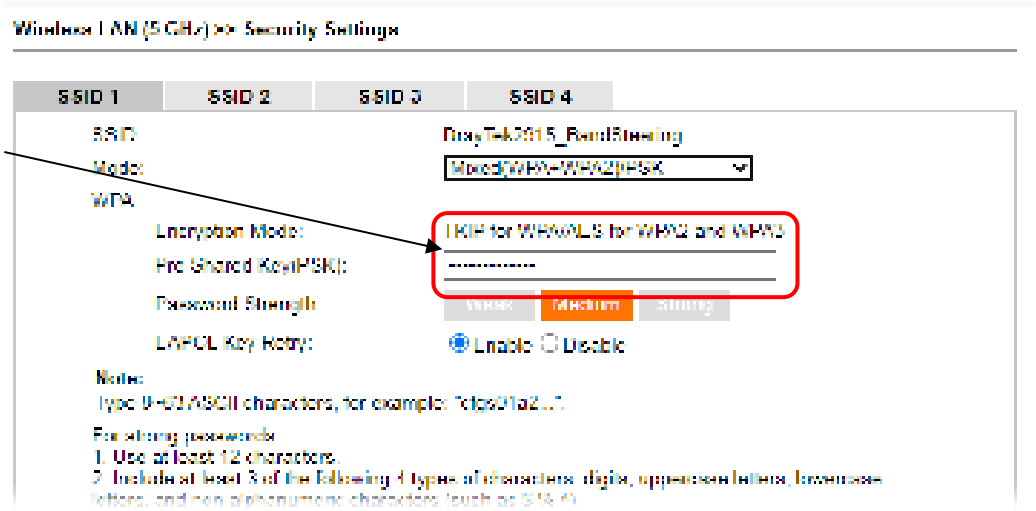
Same value for 2.4GHz and 5GHz



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



Same value for 2.4GHz and 5GHz

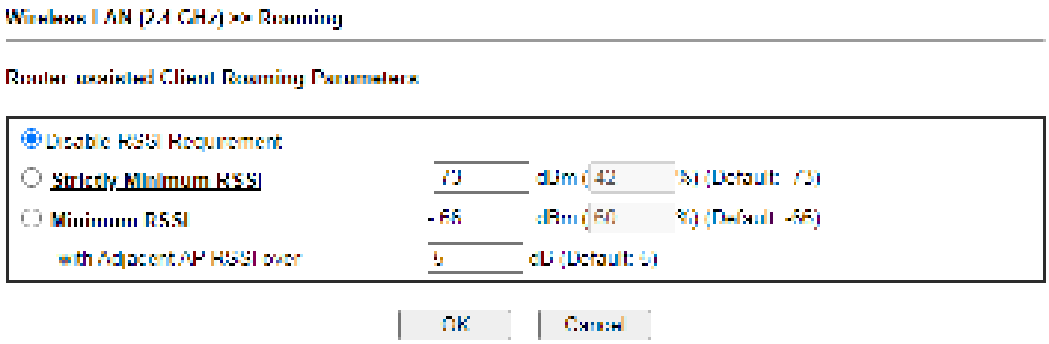


6. Now, Vigor router will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

III-1-13 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



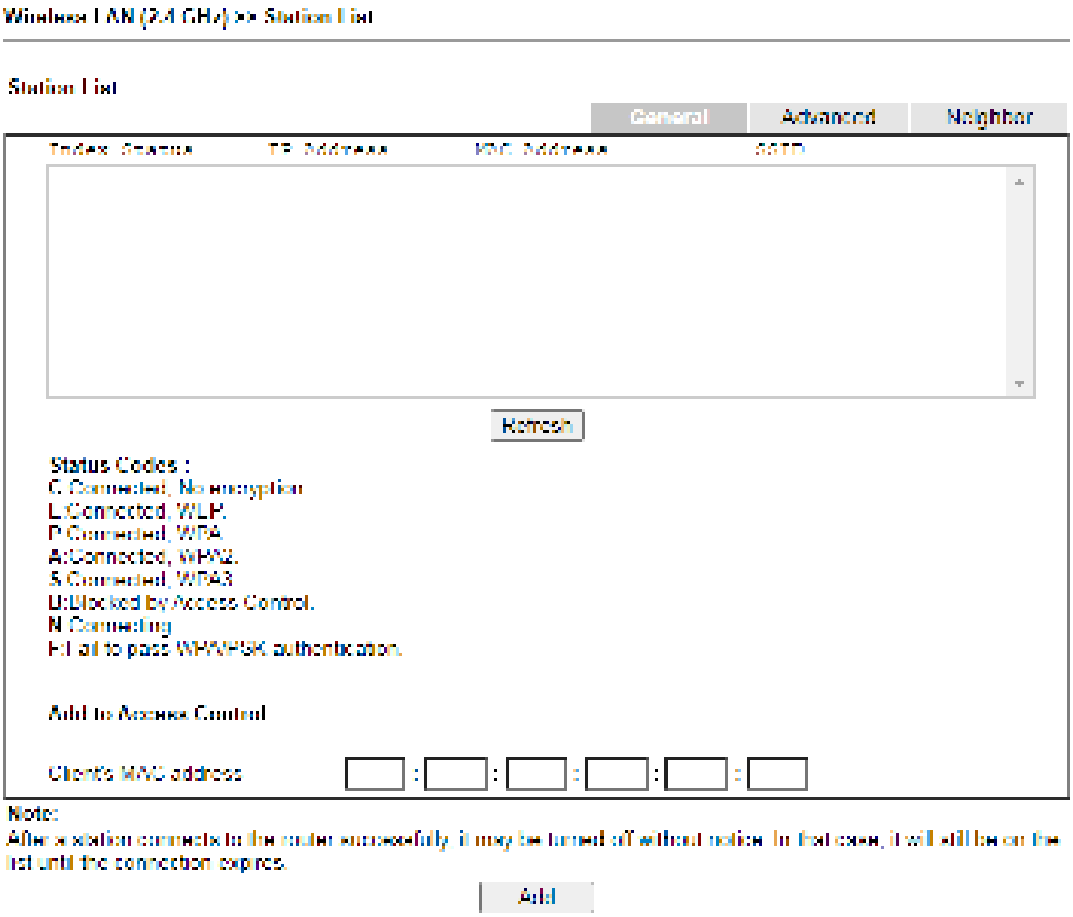
Available settings are explained as follows:

Item	Description
Disable RSSI Requirement	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, Vigor router will automatically detect (based on the link rate and RSSI requirement) and cut off the network connection for that wireless station to assist it to connect another Wireless AP to get better signal. This option is to disable the roaming mechanism.
Strictly Minimum RSSI	Vigor router uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (**dBm**) set here, Vigor router will terminate the network connection for that wireless station.
Minimum RSSI	**Minimum RSSI -** When the signal strength of the wireless station is below the value (**dBm**) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of **With Adjacent AP RSSI over**) is detected by Vigor router, Vigor router will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). ● **With Adjacent AP RSSI over** – Specify a value as a threshold.

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

III-1-14 Station List

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



Available settings are explained as follows:

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

Part IV VPN

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

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

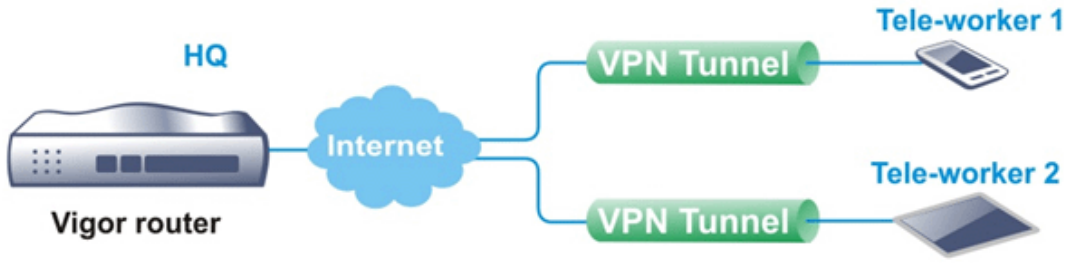
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

IV-1 VPN and Remote Access

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

The VPN built is suitable for:

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

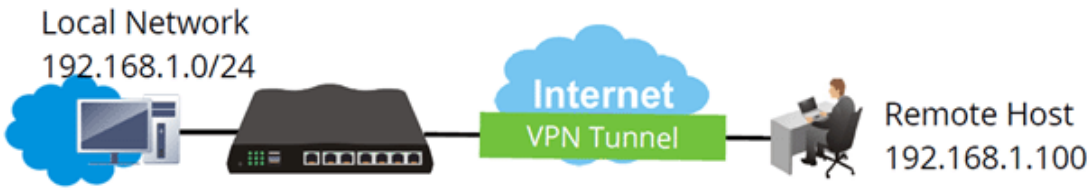


Site-to-Site (LAN-to-LAN)

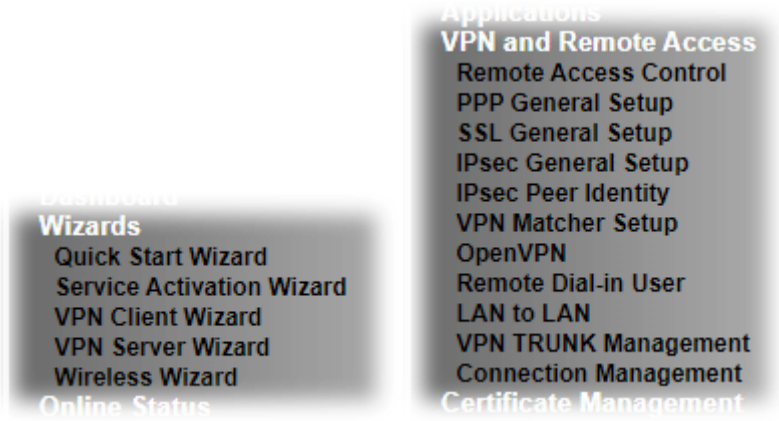
- A connection between two router's LAN networks.
- Allows employees in branch offices and head office to share the same network resources.

Remote Access (Remote Dial-in)

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



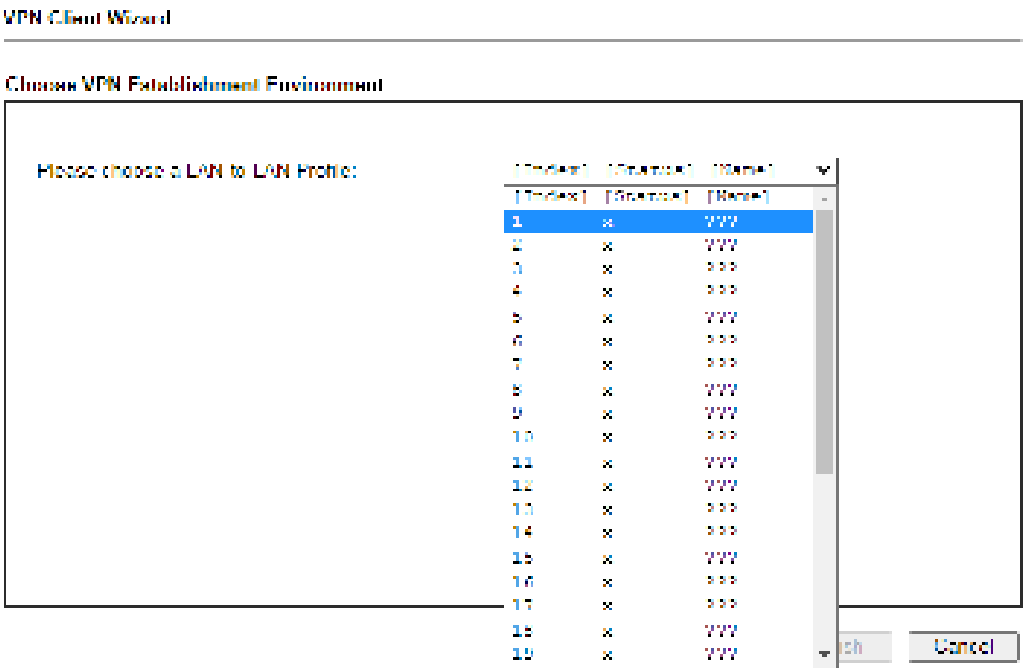
Web User Interface



IV-1-1 VPN Client Wizard

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

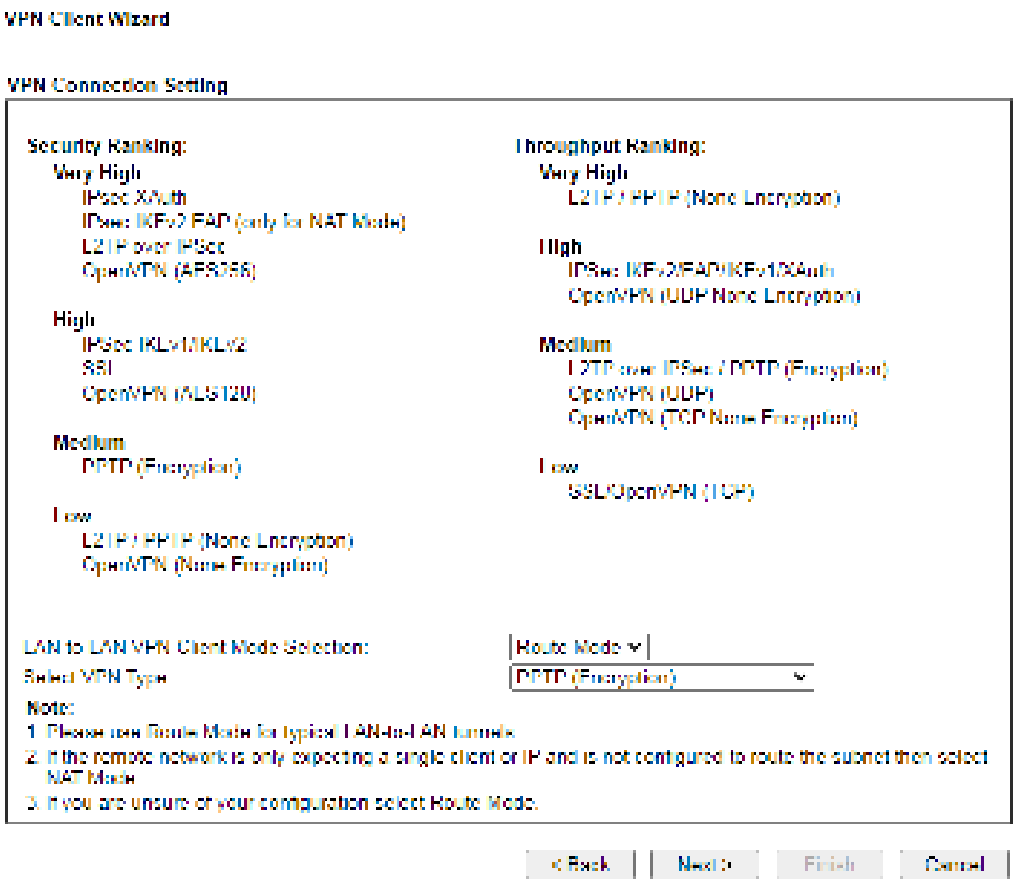
1. Open **Wizards>>VPN Client Wizard**. The following page will appear.



Available settings are explained as follows:

Item	Description
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

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

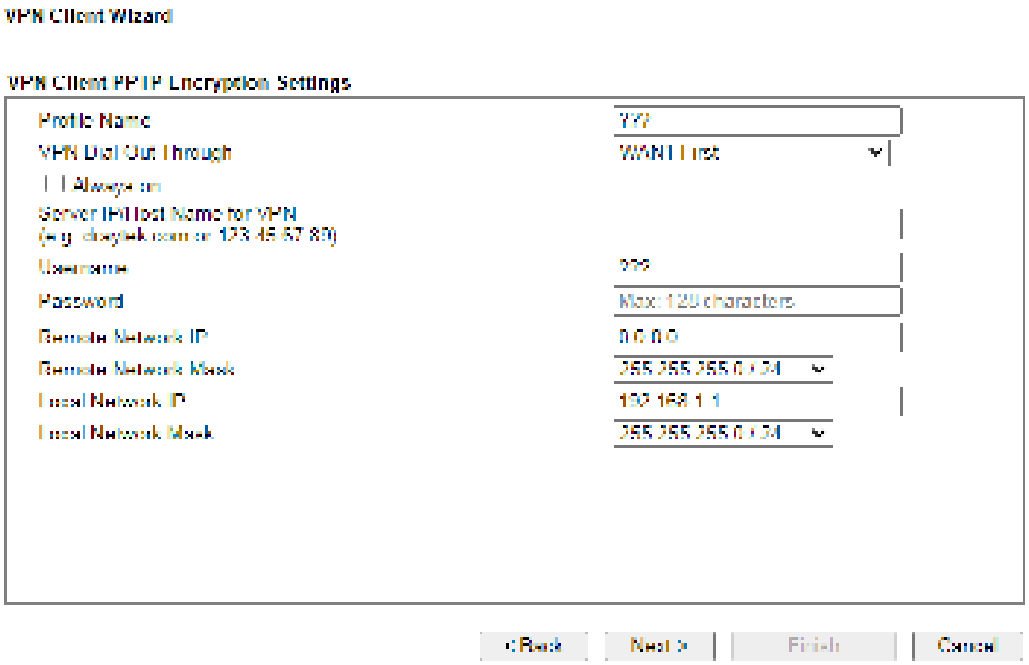


Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. **Route Mode/NAT Mode** – If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise please choose Route Mode.
Select VPN Type	Select suitable VPN type for the VPN client profile. There are several types provided here. Different type will lead to different configuration page.

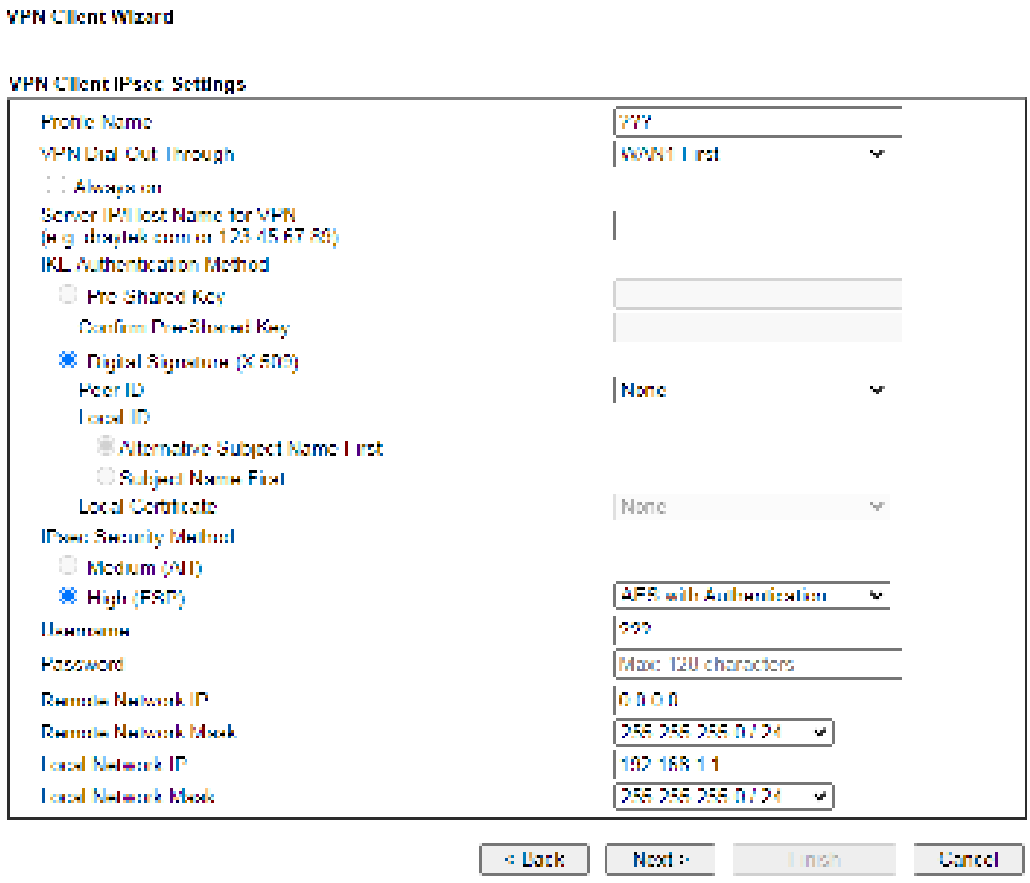
After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

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

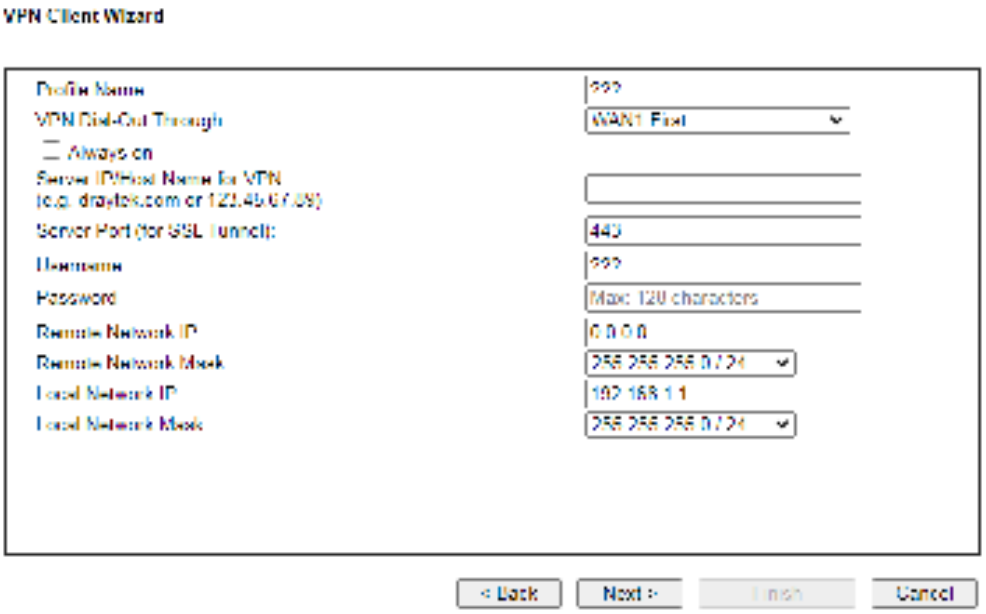
When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:



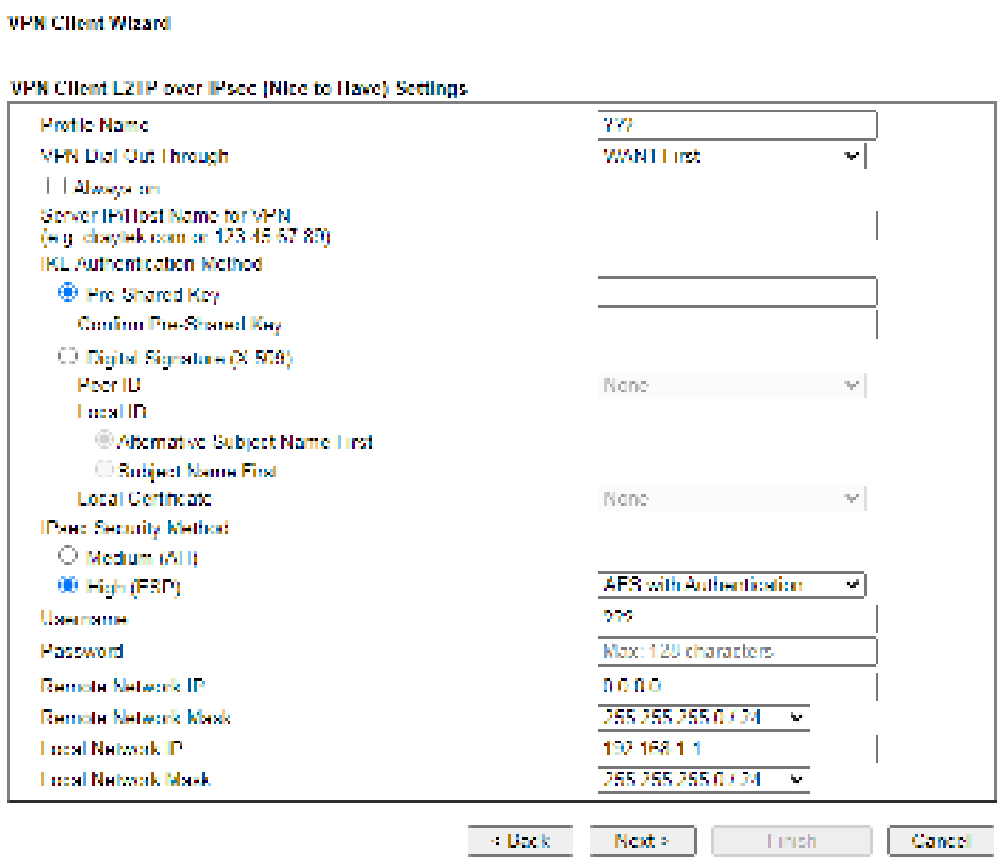
When you choose **IPsec**, you will see the following graphic:



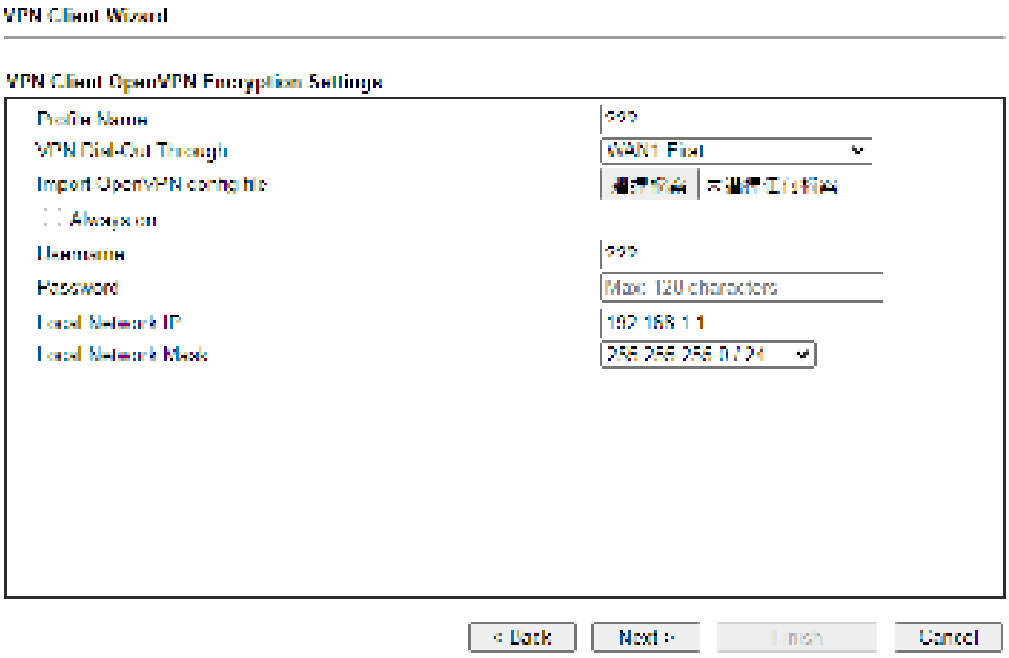
When you choose **SSL**, you will see the following graphic:



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



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

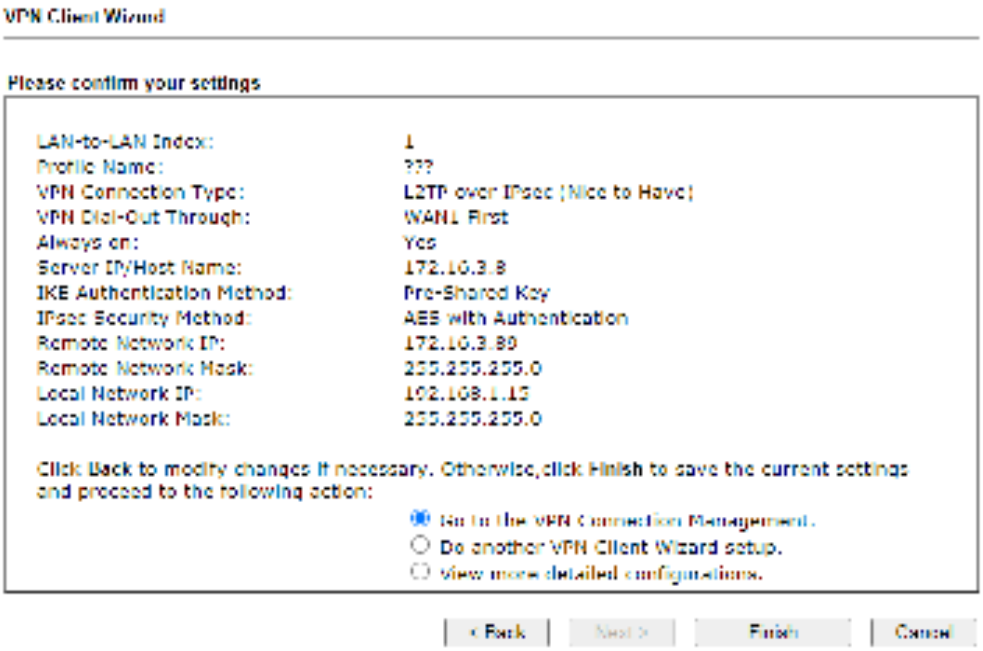


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
VPN Dial-Out Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. **WAN1 First**/ **WAN2 First** - While connecting, the router will use WAN1/ WAN2/ WAN3 as the first channel for VPN connection. If WAN1/ WAN2/ WAN3 fails, the router will use another WAN interface instead. **WAN1 Only** /**WAN2 Only** - While connecting, the router will use WAN1/ WAN2/ WAN3 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	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Enter the IP address of the server or Enter the host name for such VPN profile.
IKE Authentication Method	IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. **Pre-Shared Key-** Specify a key for IKE authentication. **Confirm Pre-Shared Key-**Confirm the pre-shared key.
Digital Signature (X.509)	Click **Digital Signature** to invoke this function. **Peer ID** – Choose the peer ID selection from the drop down list.

	Local ID – Choose **Alternative Subject Name First** or **Subject Name First**. **Local Certificate** – Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in **Certificate Management >> Local Certificate.** Otherwise, the setting you choose here will not be effective.
IPsec Security Method	**Medium** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High** - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
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 type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please Enter the network mask (according to the real location of the remote host) for building VPN connection.
Local Network IP	Enter the local network IP for TCP / IP configuration.
Local Network Mask	Enter the local network mask for TCP / IP configuration.

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



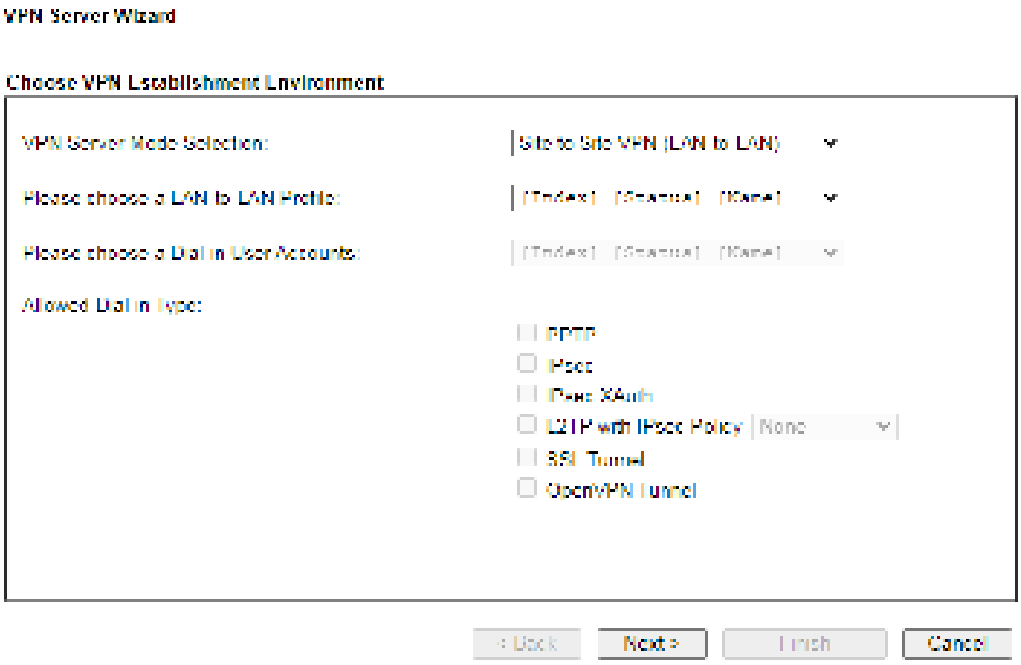
Available settings are explained as follows:

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

IV-1-2 VPN Server Wizard

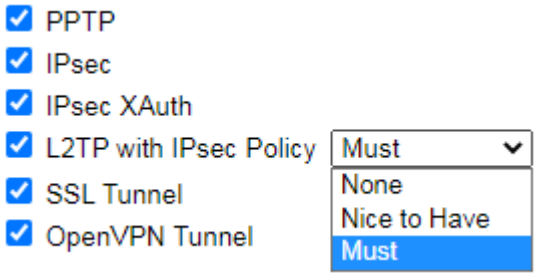
Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

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



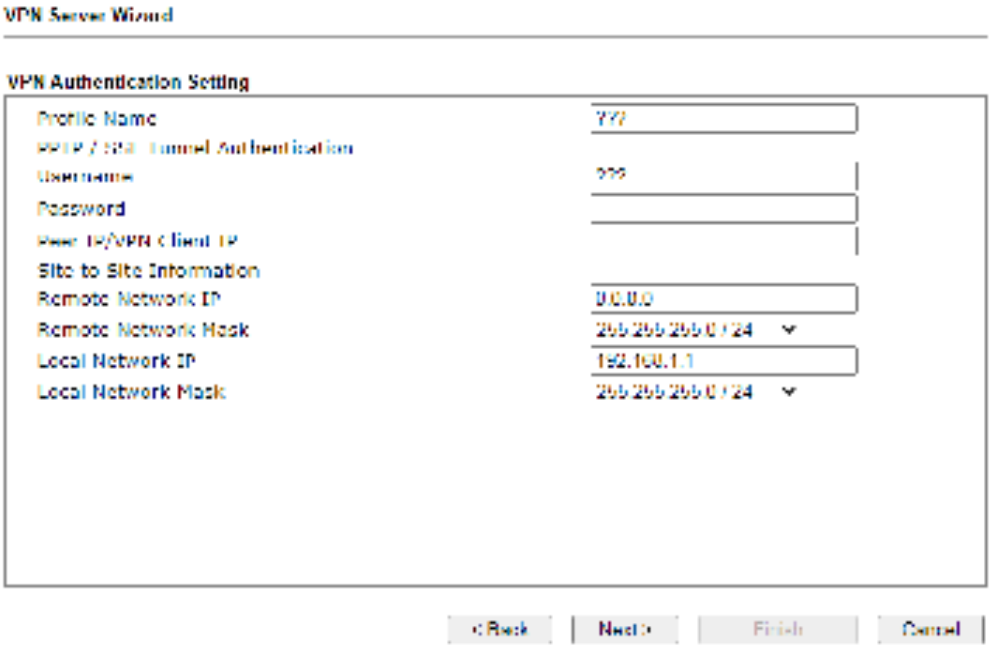
Available settings are explained as follows:

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

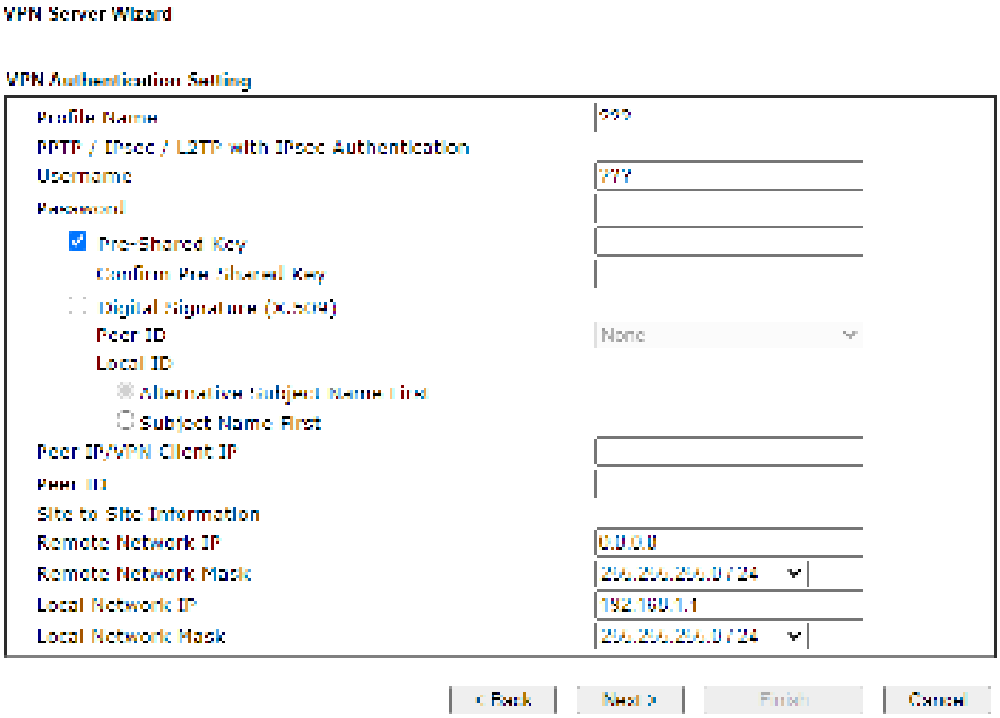
	 Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected.

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

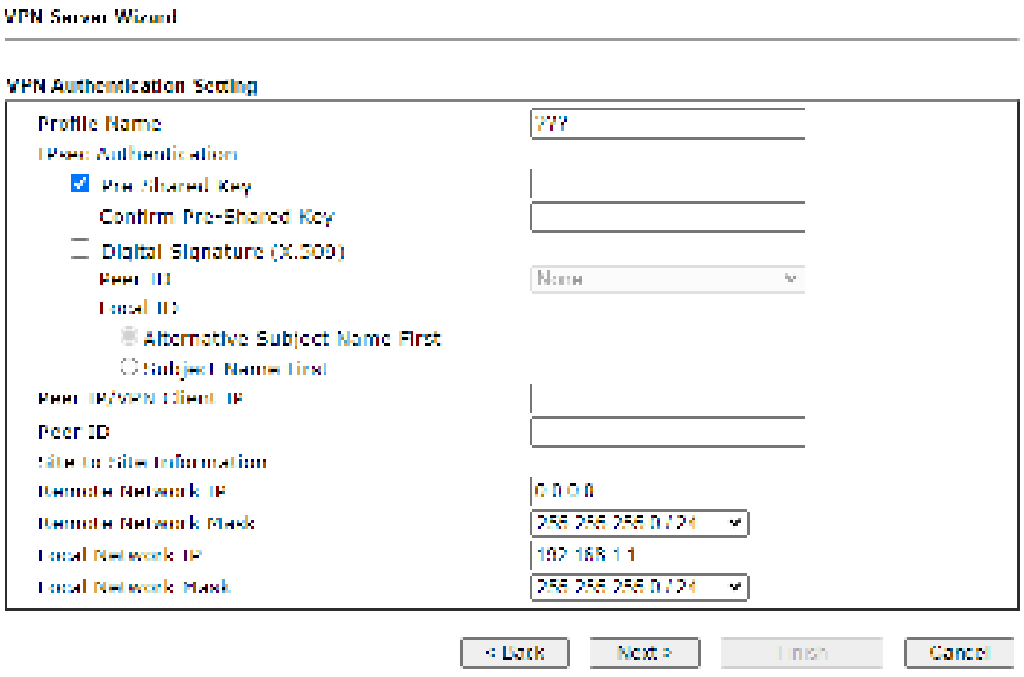
When you check **PPTP**/**SSL**, you will see the following graphic:



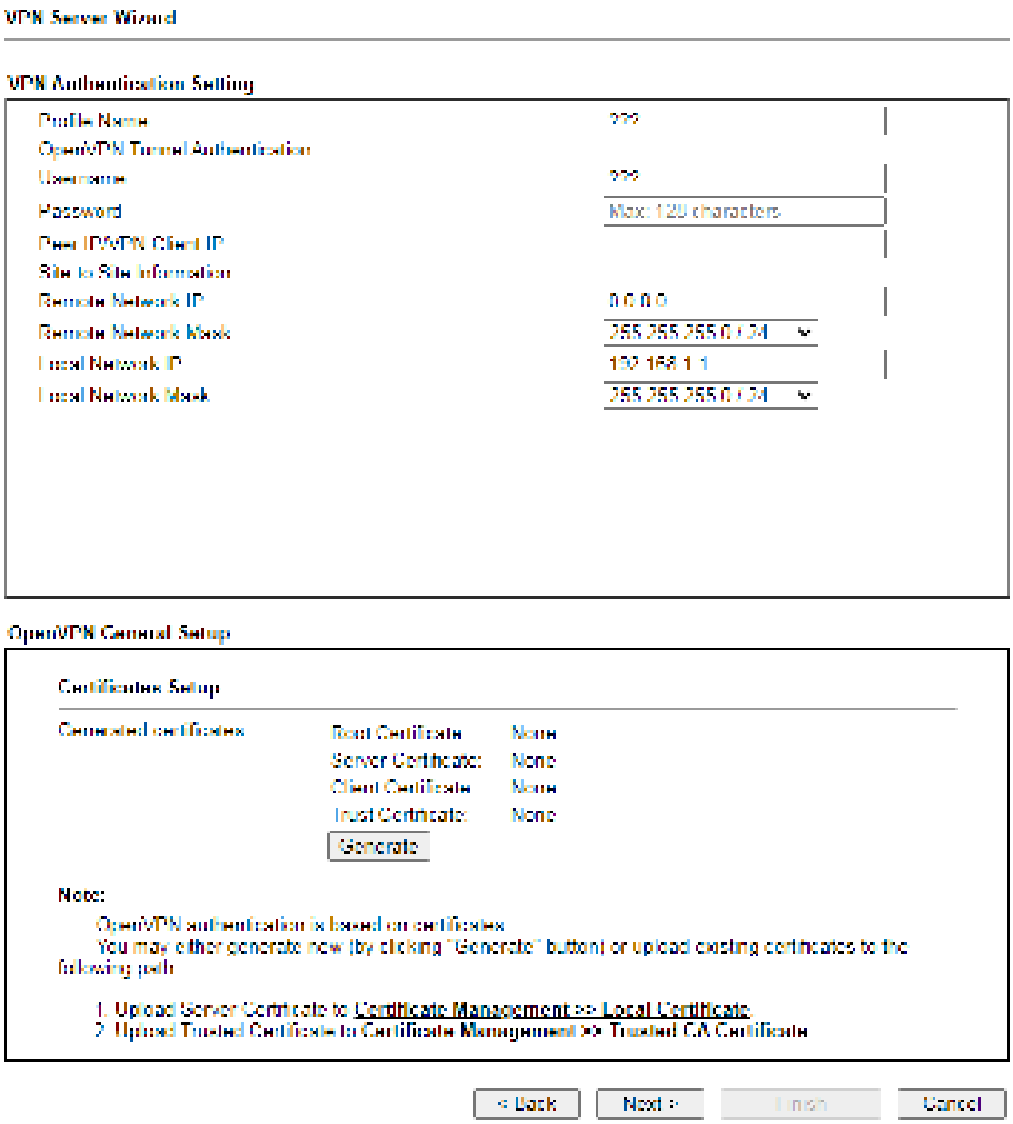
When you check **PPTP & IPsec & L2TP** (three types) or **PPTP & IPsec** (two types) or **L2TP with Policy (Nice to Have**/**Must)**, you will see the following graphic:



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



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

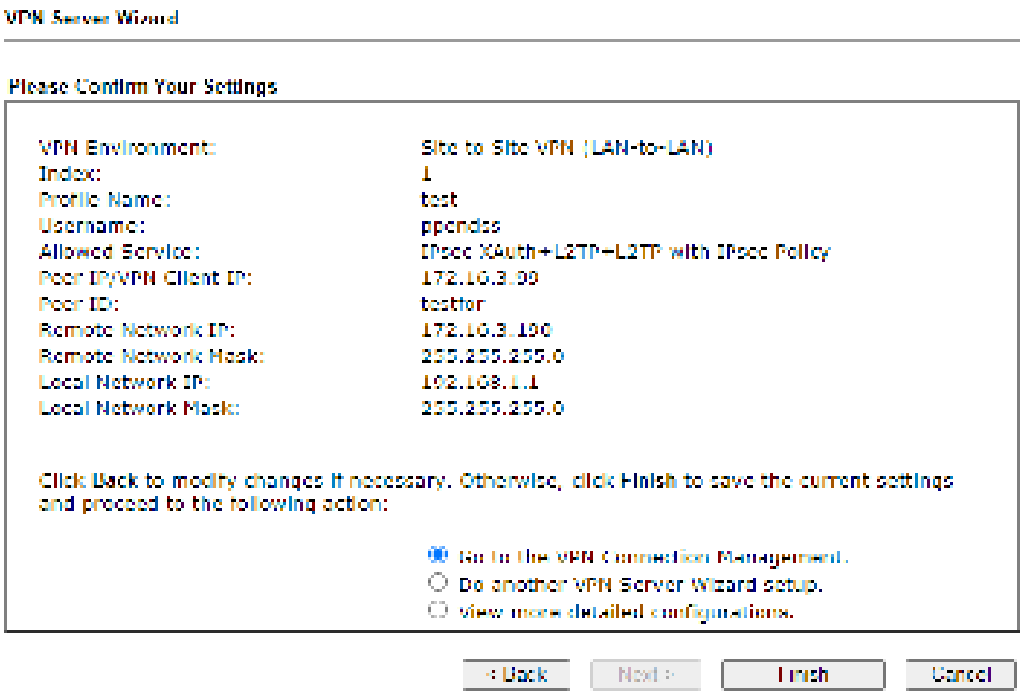


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/ L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Enter the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. **Peer ID** – Choose the peer ID selection from the drop down

	list. **Local ID** – Choose **Alternative Subject Name First** or **Subject Name First**.
Peer IP/VPN Client IP	Enter the WAN IP address or VPN client IP address for the remote client.
Peer ID	Enter the ID name for the remote client. The length of the name is limited to 47 characters.
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.

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



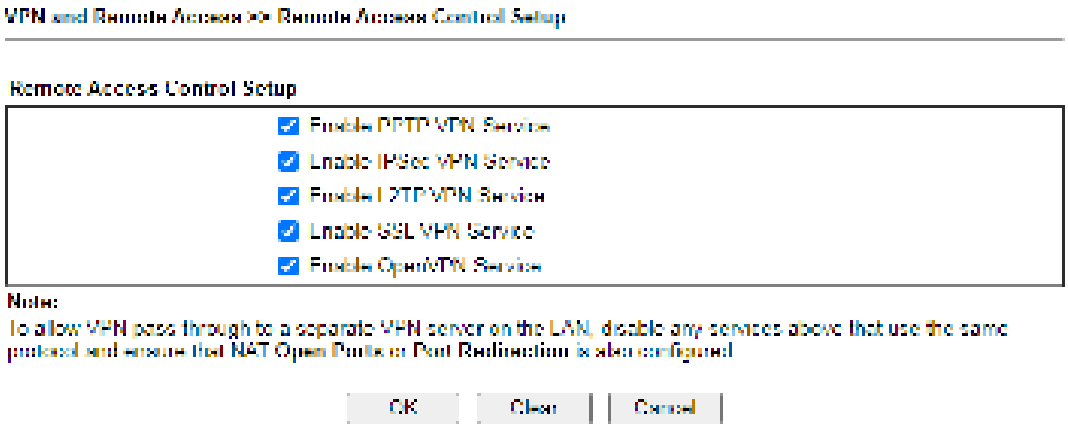
Available settings are explained as follows:

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

IV-1-3 Remote Access Control

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

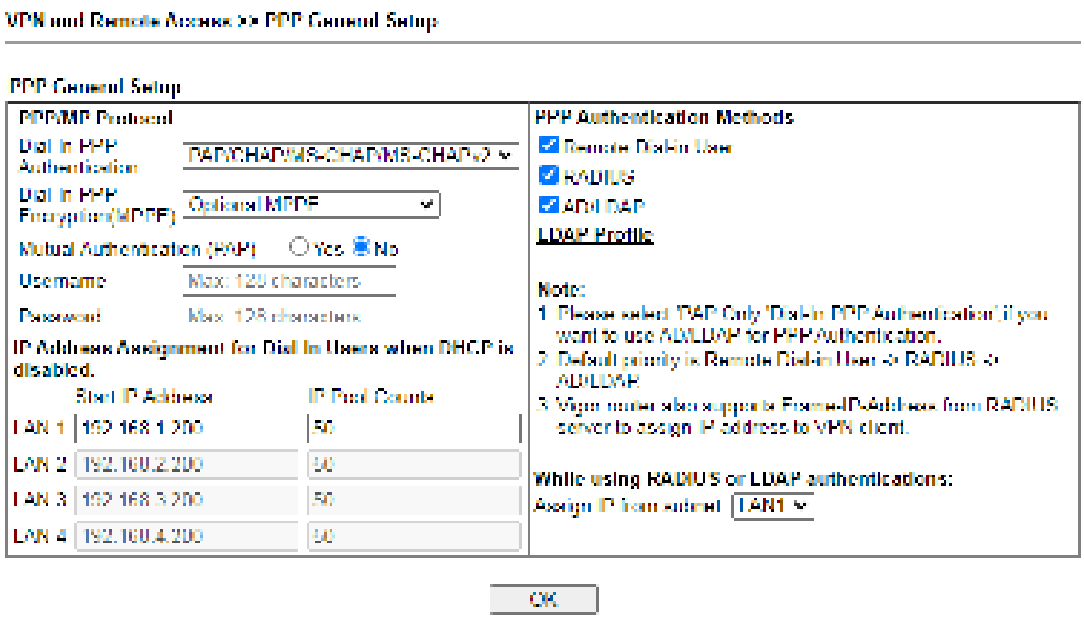
Open **VPN and Remote Access>>Remote Access Control**.



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

IV-1-4 PPP General Setup

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



Available settings are explained as follows:

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

	authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.
IP Address Assignment for Dial-In Users when DHCP is disabled	Enter a start IP address for the dial-in PPP connection for LAN1. LAN2 ~ LAN4 will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface.
PPP Authentication Methods	Select the method(s) to be used for authentication in PPP connection.
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.
While using Radius or LDAP Authentication	If PPP connection will be authenticated via RADIUS server or LDAP profiles, it is necessary to specify the LAN profile for the dial-in user to get IP from.

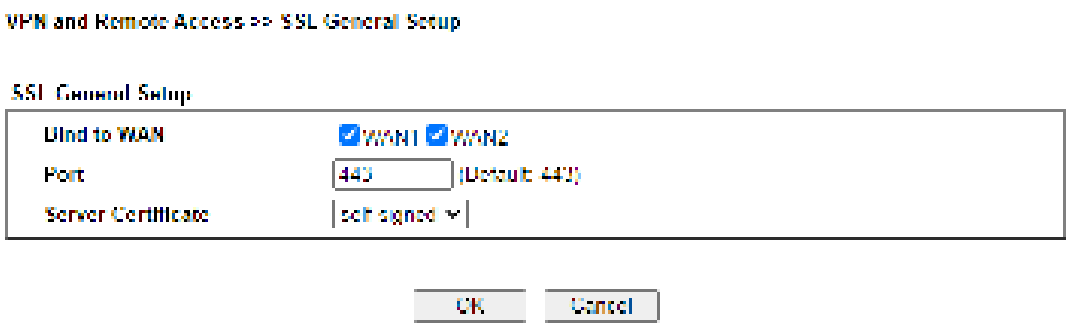
IV-1-5 SSL General Setup

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

In short,

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

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



Available settings are explained as follows:

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

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

IV-1-6 IPsec General Setup

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

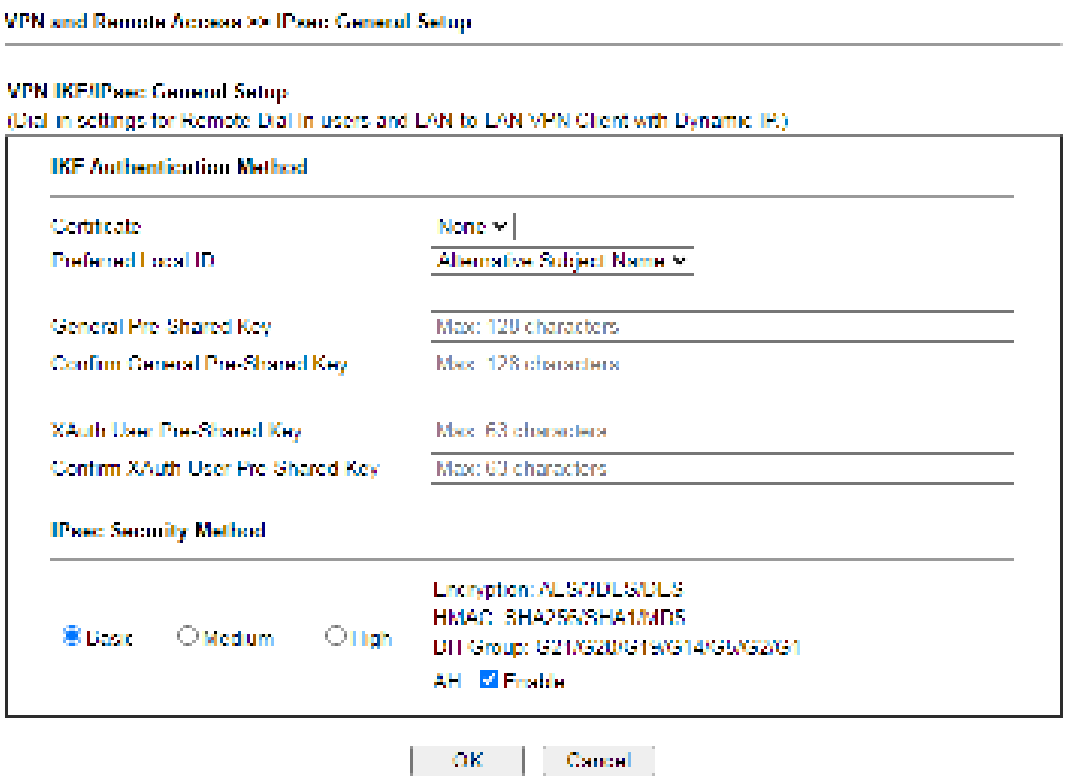
There are two phases of IPsec.

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

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

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

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



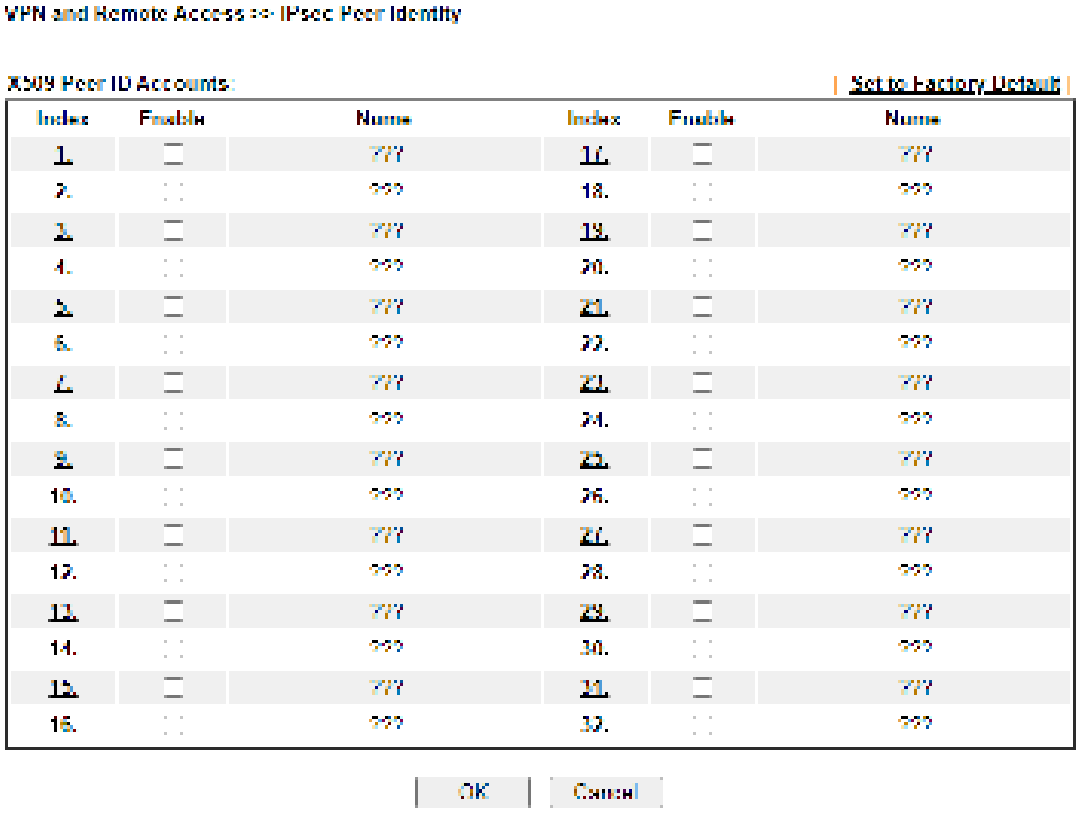
Available settings are explained as follows:

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

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

IV-1-7 IPsec Peer Identity

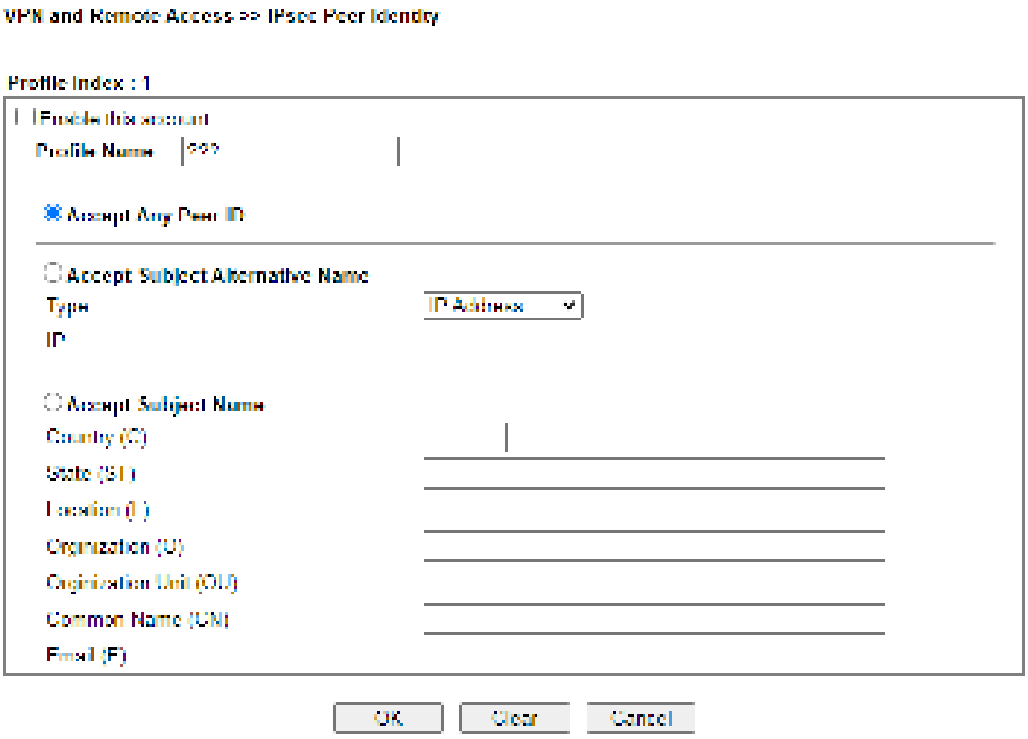
To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for peer dial-in users.



Available settings are explained as follows:

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

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



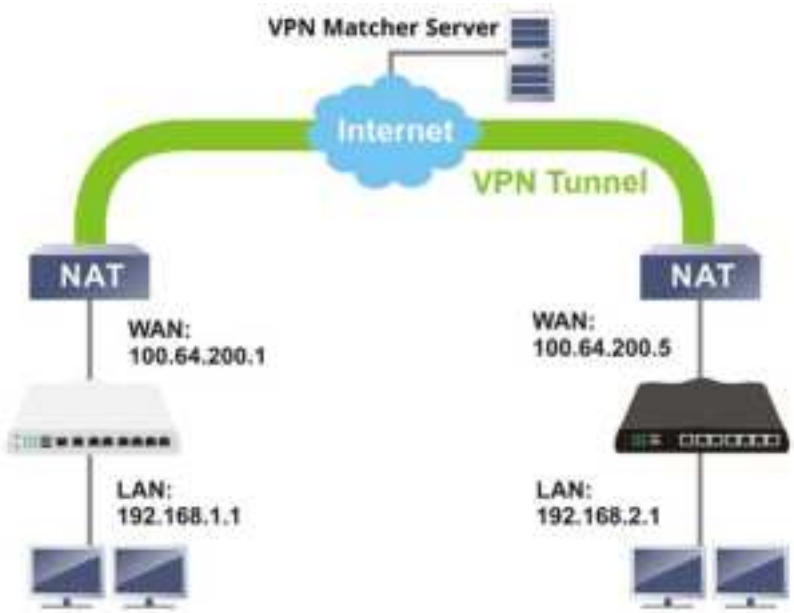
Available settings are explained as follows:

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

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

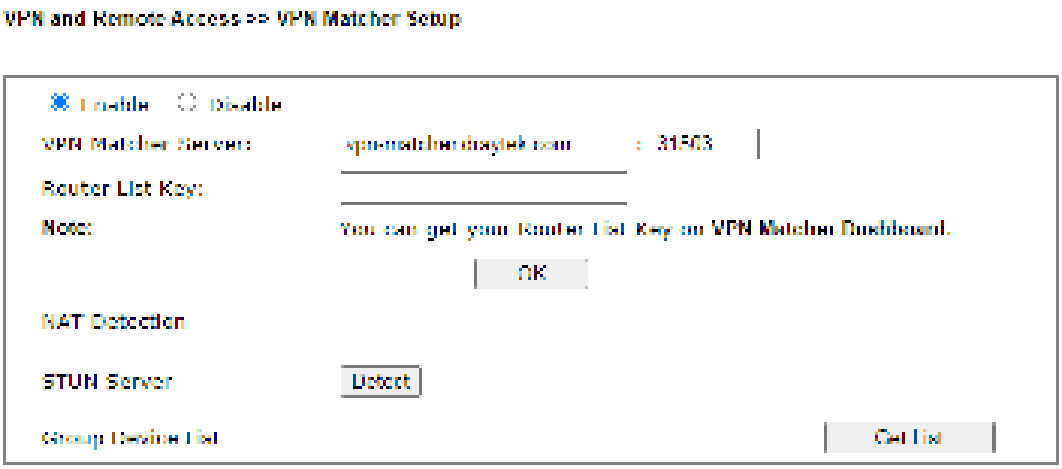
IV-1-8 VPN Matcher Setup

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 number "31503".
Router List Key	Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via

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

IV-1-9 OpenVPN

OpenVPN offers a convenient way for users to build VPN between local end and remote end.

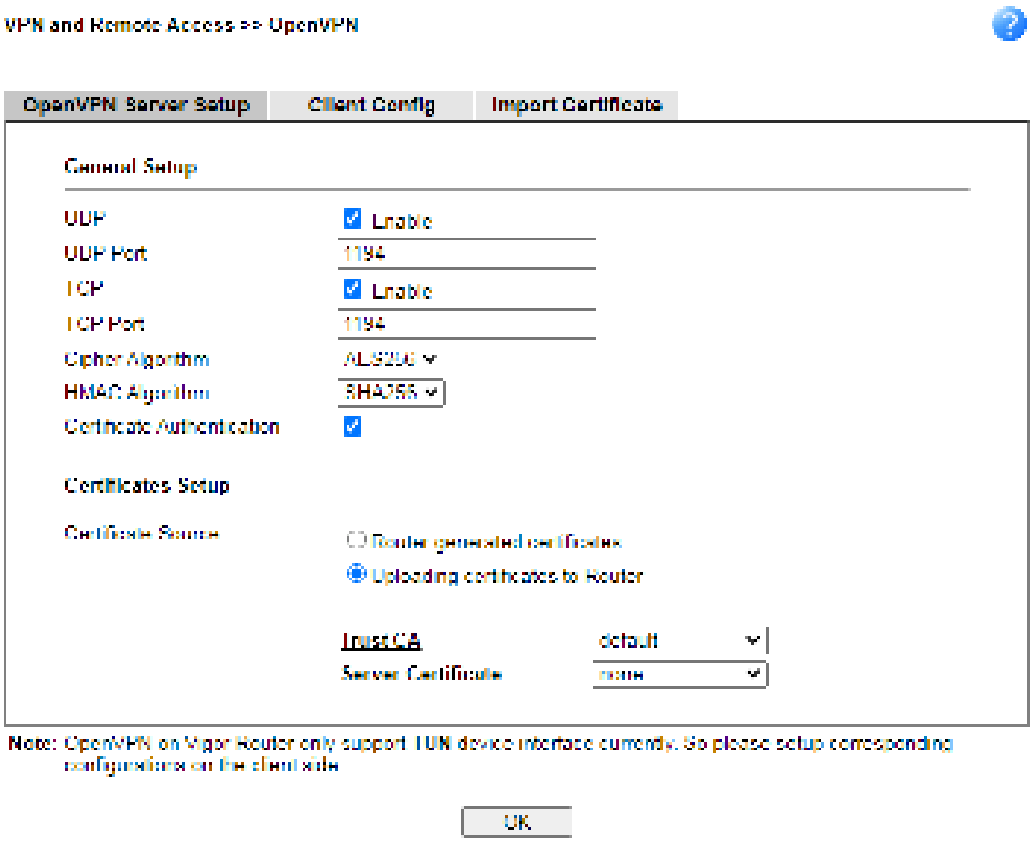
With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

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.

IV-1-9-1 OpenVPN Server Setup

Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.



Available settings are explained as follows:

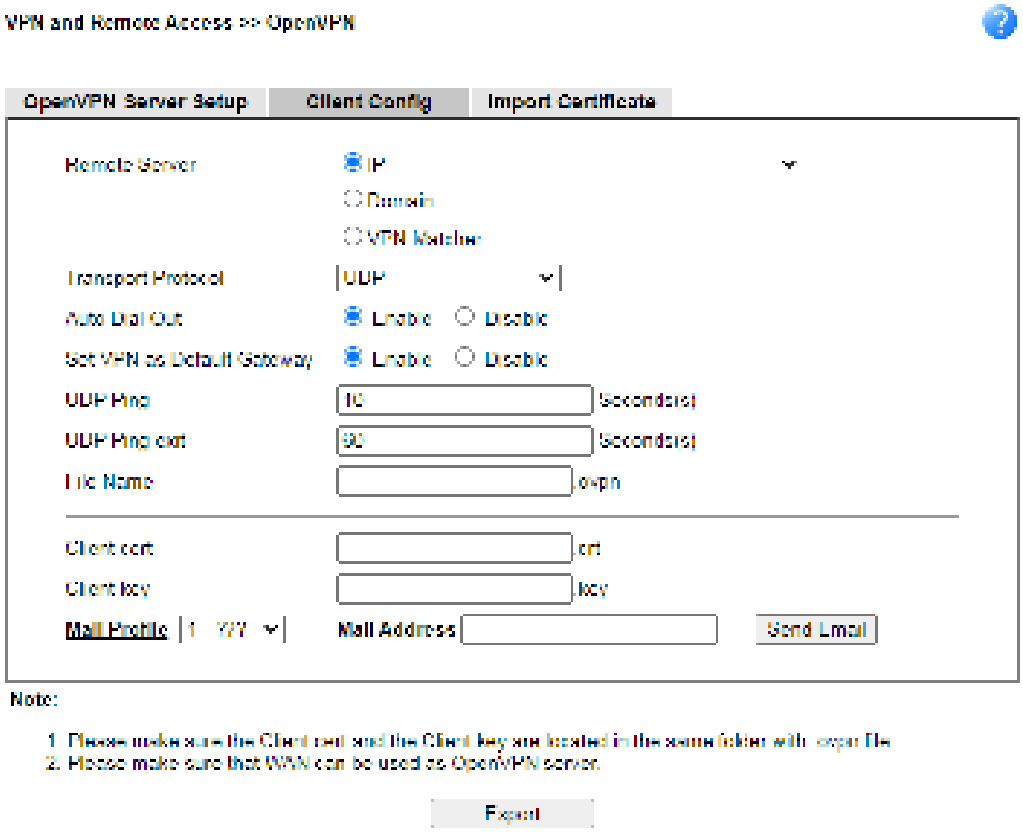
Item	Description
Enable UDP	Check the box to enable UDP port setting for OpenVPN. **UDP Port** – Enter a number.
Enable TCP	Check the box to enable TCP port setting for OpenVPN. **TCP Port** – Enter a number.
Cipher Algorithm	Two encryptions are supported, AES128 and AES256.

HMAC Algorithm	The HMAC algorithm only supports SHA1/SHA256.
Certificate Authentication	If certificate authentication is required for OpenVPN, simply check the box to apply the trusted CA certificate and local certificate for OpenVPN tunnel. Certificate authentication can offer more secure VPN tunnel between the client and the router.
Certificate Source	Select a source for the certificate to be used for OpenVPN. **Router generated certificates** - Router-generated certificates that will be used for OpenVPN. ● **GENERATE** - Click to generate a certificate. ● **Delete all certificate** - Click to remove all certificates generated by the router. **Uploading certificates to Router** - Third-party certificates will be used for OpenVPN. ● **Trust CA** - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the **Certificate Management >> Trusted CA Certificate** page to perform the operation. ● **Server Certificate** - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the **Certificate Management >> Local Certificate** page to perform the operation.

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

IV-1-9-2 Client Config

The settings on this page can be downloaded as a file. Later, such file can be imported and applied to remote end's CPE (as VPN client). Then, a private connection via OpenVPN tunnel between the server and the client can be connected successfully.



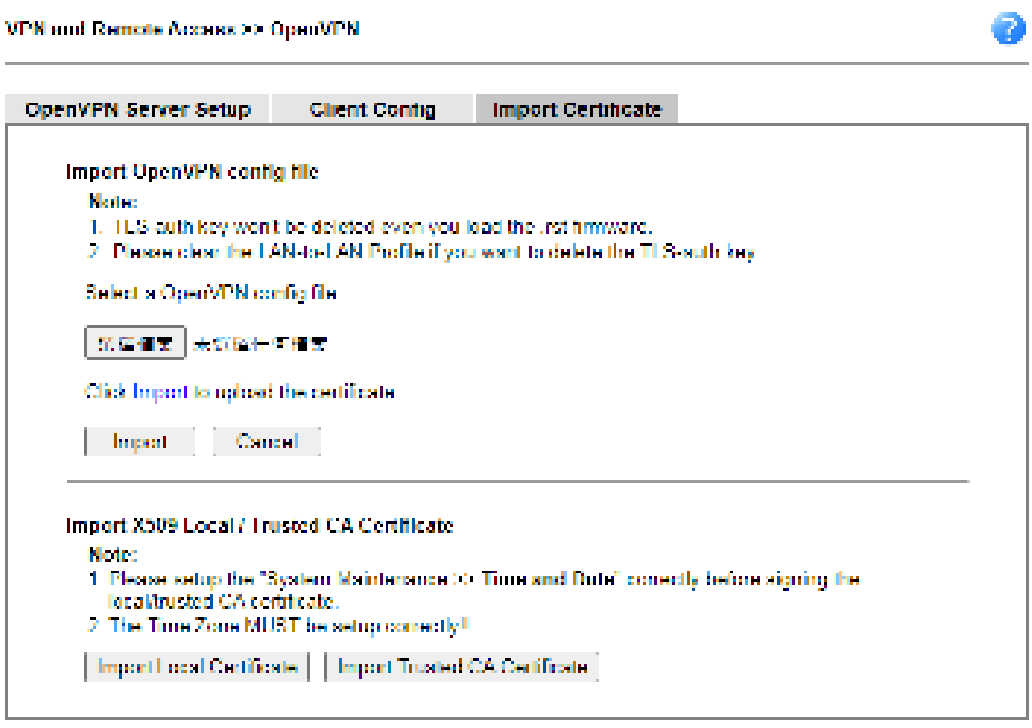
Available settings are explained as follows:

Item	Description
Remote Server	The OpenVPN client will use the IP address or domain name to connect to the router. Select either IP or Domain. **IP** – The OpenVPN configuration file will use the numeric IP address as the server address. **Domain** – The OpenVPN configuration file will use the domain as the server address. You need to ensure that the domain resolves to the IP address of a router WAN port. **VPN matcher** - The OpenVPN configuration file will use the VPN matcher as the server address.
Transport Protocol	Simply choose UDP or TCP as protocol for building OpenVPN connection between the server and the remote client.
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	Each client in an OpenVPN connection must have its certificate and private key. Enter the certificate file name obtained from 3rd party provider
Client key	Enter the private key file name obtained from 3rd party provider
Mail Profile	The system administrator can send an email containing the OpenVPN client configuration to someone who needs it. Later, the recipient can use the configuration to connect to the company's Intranet. It is useful and convenient for Smart VPN Client user or employee on a business trip. **Mail Address** - Enter the IP address of the recipient. **Send Email** - After clicking this button, the recipient will receive an email with the content of OpenVPN client configuration.
Export	The settings in this page can be saved as a file after clicking such button. Later, the downloaded file can be imported to the VPN client for building OpenVPN connection.

IV-1-9-3 Import Certificate

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



Available settings are explained as follows:

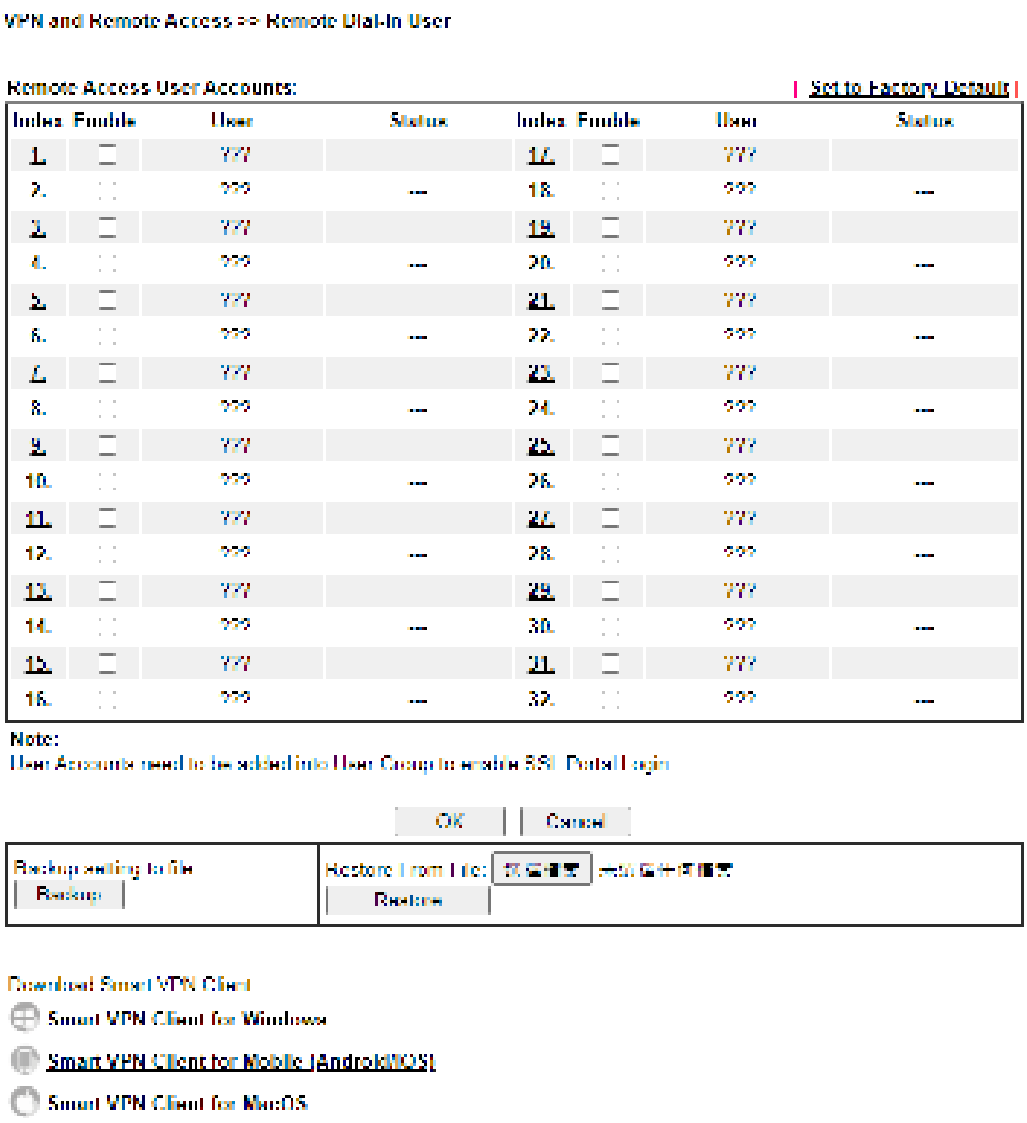
Item	Description
Select an OpenVPN config file	**Browse** - Click to select a file. **Import** - Click to import a configuration file.

Import Local Certificate	Click to access into Local Certificate page for importing a certificate.
Import Trusted CA Certificate	Click to access into Trusted CA Certificate page for importing a certificate.

IV-1-10 Remote Dial-in User

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

The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

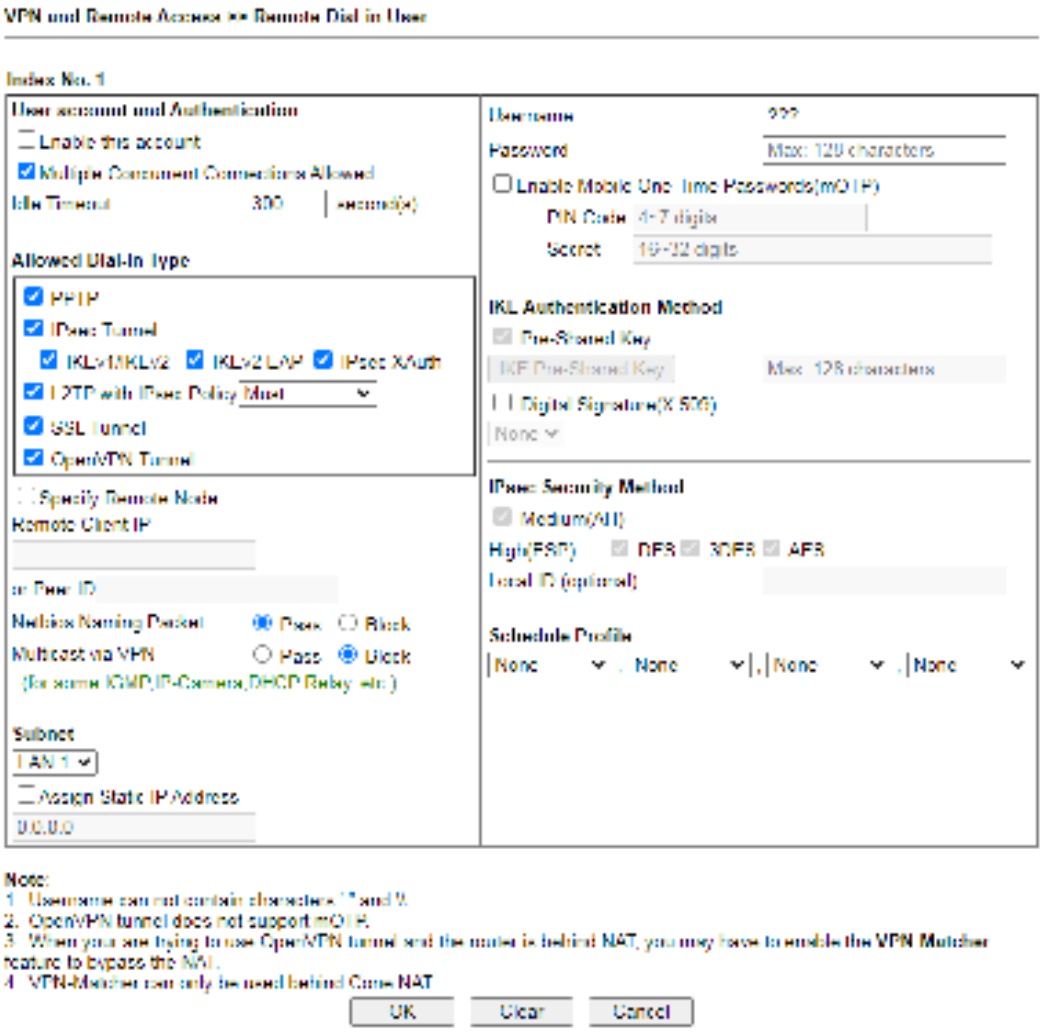


Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
Enable	Check it to enable such account profile.
User	Display the username for the specific dial-in user of the

	LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.
Backup setting to file	Click the button to backup the remote dial-in user settings on this page as a file.
Restore From File	Click the button to restore the remote dial-in user settings from the selected configuration file.

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



Available settings are explained as follows:

Item	Description
User account and Authentication	**Enable this account** - Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
Allowed Dial-In Type	**PPTP** - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User

	Name and Password of remote dial-in user below. **IPsec Tunnel** - Allow the remote dial-in user to make an IPsec VPN connection through Internet. **L2TP with IPsec Policy** - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: ● **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● **Nice to Have -** Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● **Must -**Specify the IPsec policy to be definitely applied on the L2TP connection. **SSL Tunnel** – Allow the remote dial-in user to make an SSL VPN connection through Internet. **OpenVPN Tunnel** – Allow the remote dial-in user to set a VPN connection through OpenVPN. **Specify Remote Node -**You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the **general settings**. **Netbios Naming Packet -** ● **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. ● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN** - Some programs might send multicast packets via VPN connection. ● **Pass** – Click this button to let multicast packets pass through the router. ● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. **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 23 characters. **Password** - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters. **Enable Mobile One-Time Passwords (mOTP) -** Check this box to make the authentication with mOTP function. **PIN Code** – Enter the code for authentication (e.g, 1234). **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Subnet	Chose one of the subnet selections for such VPN profile. **Assign Static IP Address** – Please type a static IP address for the subnet you specified.
IKE Authentication	This group of fields is applicable for IPsec Tunnels and L2TP

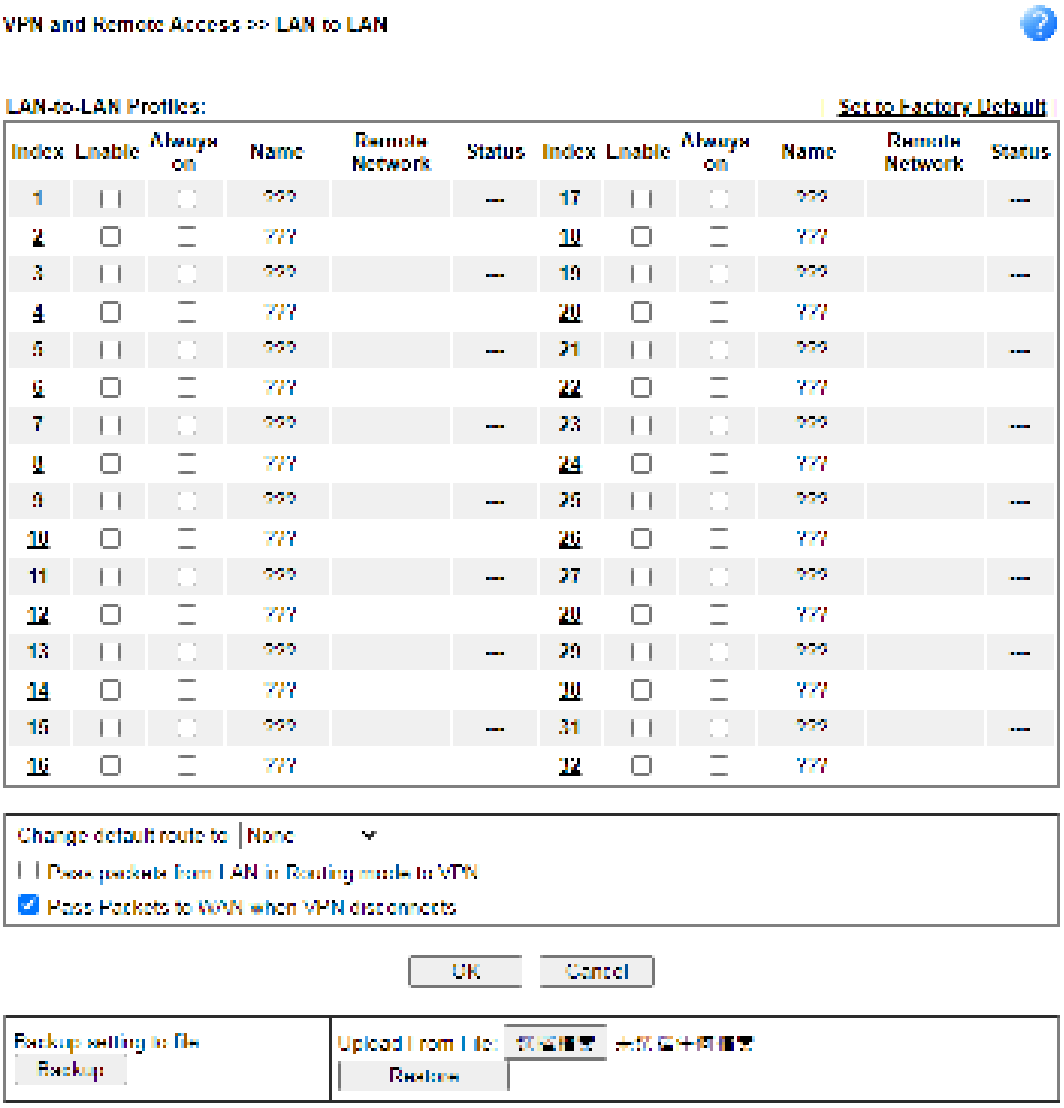
Method	with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specifying the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity.**
IPsec Security Method	This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. **High-Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. **Local ID (Optional)-** Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
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.

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

IV-1-11 LAN to LAN

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

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



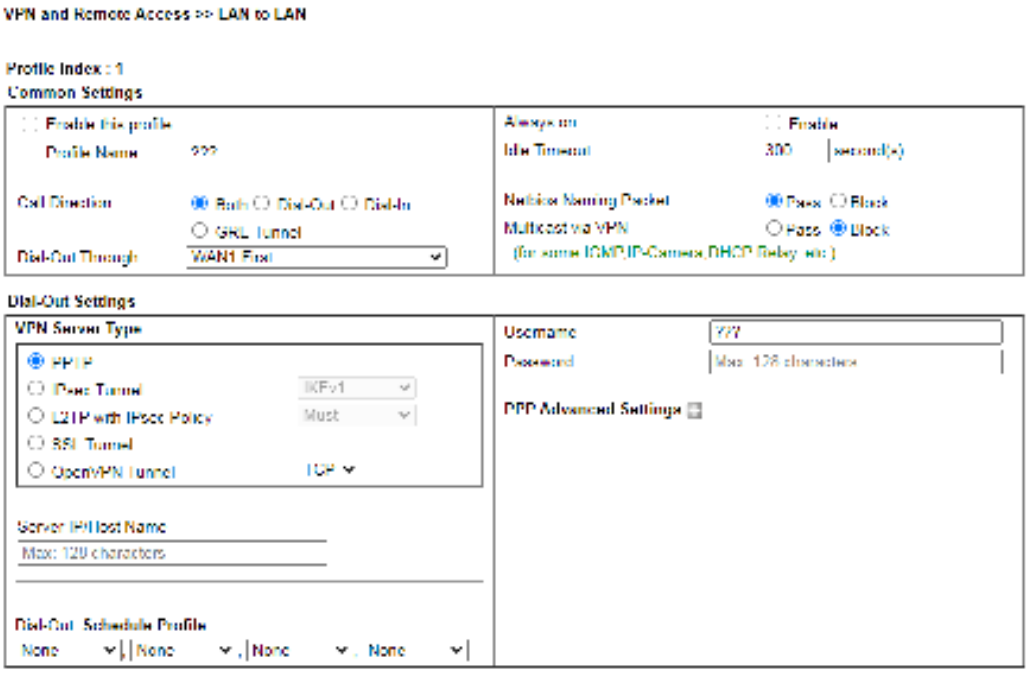
Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of LAN to LAN profile.
Enable	Check this box to enable this profile.
Always On	Check to enable router always keep VPN connection.
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Remote Network	Display the IP address/ subnet mask of the remote network.
Status	Online – means such LAN to LAN profile is in use. Offline – means such LAN to LAN profile isn't in use even if the profile has been enabled.
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 NAT when	If enabled, the packets can pass through via NAT when the

VPN disconnects	VPN disconnects.
Backup	Click **Backup** to save the configuration.
Restore	Click **Select** to choose a configuration file. Then click **Restore** to apply the file.

To edit each profile:

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

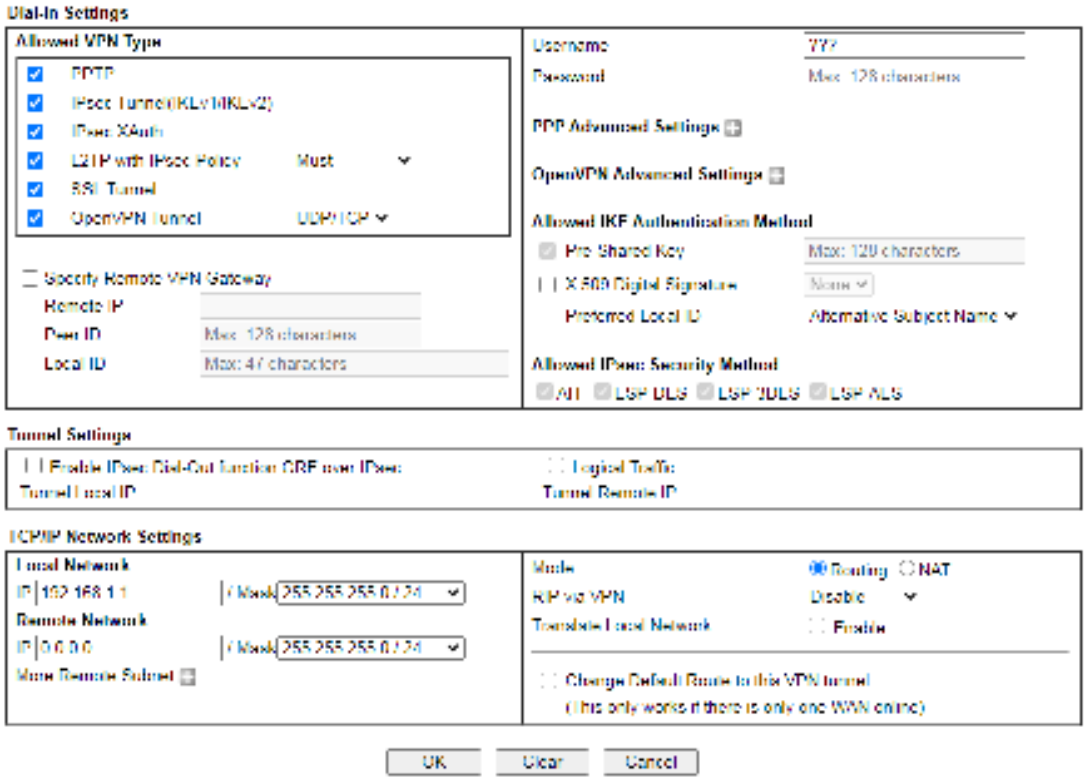


Available settings are explained as follows:

Item	Description
Common Settings	**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. ● **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. ● **WAN1 First**/ **WAN2 First**- While connecting, the router will use WAN1/ WAN2 as the first channel for VPN connection. If WAN1/ WAN2 fails, the router will use another WAN interface instead.

	• **WAN1 Only /WAN2 Only** - While connecting, the router will use WAN1/ WAN2 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-**Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection. **Netbios Naming Packet** • **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. • **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. **Multicast via VPN -** Some programs might send multicast packets via VPN connection. • **Pass** – Click this button to let multicast packets pass through the router. • **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
Dial-Out Settings	**VPN Server** • **PPTP** - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server. • **IPsec Tunnel** - Build an IPsec VPN connection to the server through Internet. • **L2TP with IPsec Policy -** Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: - **None:** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. - **Nice to Have:** Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. - **Must:** Specify the IPsec policy to be definitely applied on the L2TP connection. • **SSL Tunnel** - Build an SSL VPN connection to the server through Internet. • **OpenVPN Tunnel** - Build an OpenVPN connection via TCP or UDP. **Server IP / Host Name -** Enter the IP address of the server or the host name. **Dial-Out Schedule Profile -** Set the wireless LAN to work at

	certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work. **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 49 characters. **Password -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters. **PPP Advanced Settings** - Click it to configure advanced settings. ● **PPP Authentication -** This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/ CHAP/ MS-CHAP/ MS-CHAPv2 is the most common selection due to compatibility. ● **VJ compression -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/ IP protocol header compression. Normally set to **On** to improve bandwidth utilization. ● **Request IP Address** - Enter an IP address.

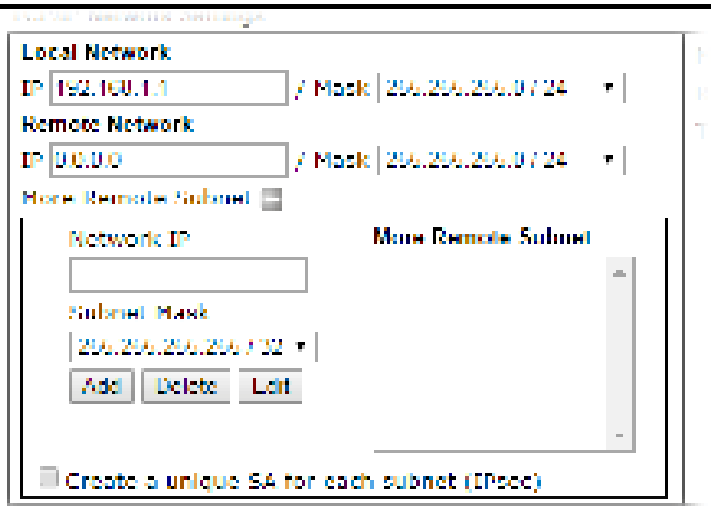


Available settings are explained as follows:

Item	Description
Dial-In Settings	**Allowed VPN Type -** Determine the dial-in connection with different types. ● **PPTP -** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user

	below. ● **IPsec Tunnel-** Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● **IPsec XAuth** - Allow the remote dial-in user to make an IPsec VPN connection after authenticated with the sever. ● **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** - Allow the remote dial-in user to trigger an OpenVPN connection through Internet. **Specify Remote VPN Gateway -** You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings. **Username -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters. **Password -** This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters. **PPP Advanced Settings** - Click it to configure advanced settings. ● **VJ Compression -** VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above. ● **Assign Peer IP Address** - Enter the IP address of the peer. **Allowed IKE Authentication Method -** This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node. ● **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. ● **X.509 Digital Signature –** Check the box of Digital

	Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPsec Peer Identity**. **Preferred Local ID** – Specify which one will be inspected first. - **Alternative Subject Name First** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first. - **Subject Name First** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first. **Allowed IPsec Security Method -** This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node. ● **AH/ESP-DES/ESP-3DES/ESP-AES -** Authentication Header (AH) means data will be authenticated, but not be encrypted. 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 IP / Mask -** Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required. **Remote Network 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 -** Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Masks through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



Mode - If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

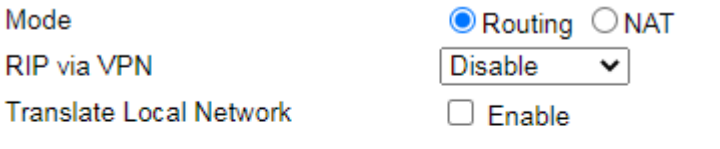
For NAT,

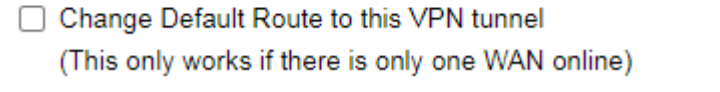
- **Change default route to this VPN tunnel -** Check this box to change the default route with this VPN tunnel.
- **RIP via VPN -** The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/ disable one of direction here. Herein, we provide four options: TX/ RX Both, TX Only, RX Only, and Disable.

For Routing,

- **RIP via VPN -** The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/ disable one of direction here. Herein, we provide four options: TX/ RX Both, TX Only, RX Only, and Disable.
- **Translate Local Network** - This function is enabled in default.

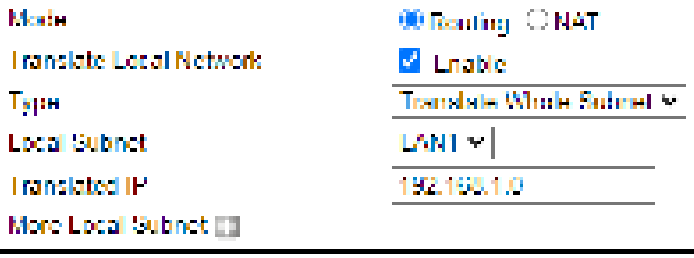
  When it is disabled, you can enable or disable **Change Default route to this VPN tunnel.**





Change default route to this VPN tunnel - Check this box to change the default route with this VPN tunnel.

When it is enabled, you have to specify type, local subnet, translated IP and more local subnet.



	Type – There are two types for you to choose, **Translate Whole Subnet** and **Translate Specific IP.** **Local Subnet -** Select the LAN whose IP addresses are to be translated. **Translate 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:

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

IV-1-12 VPN Trunk Management

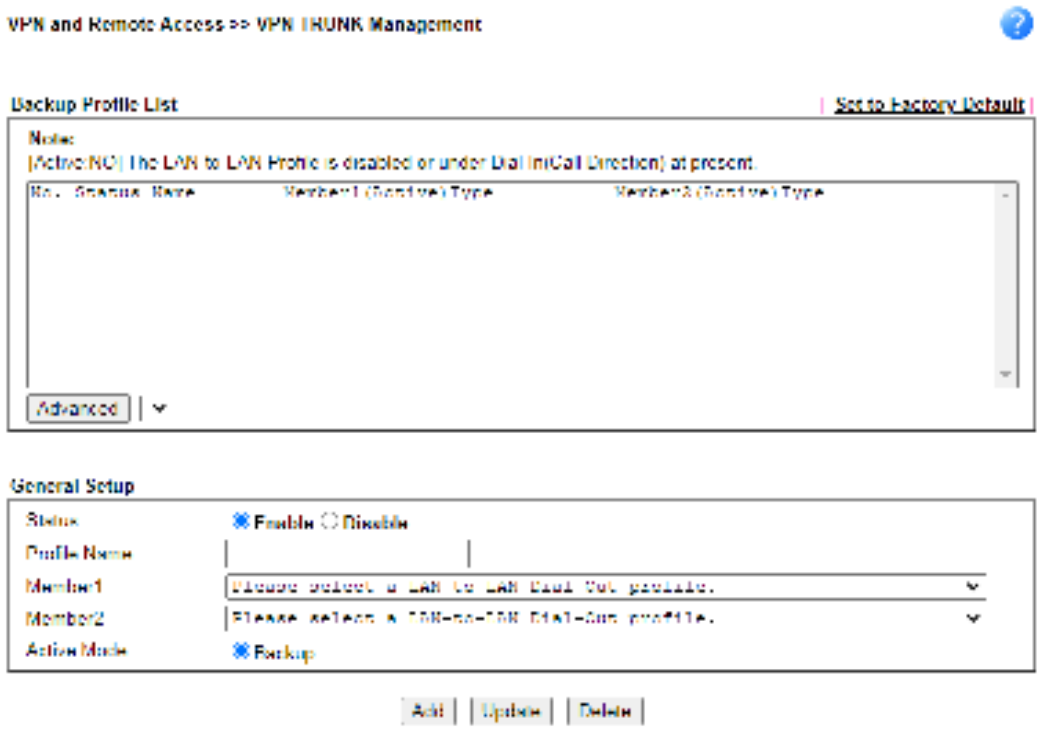
VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

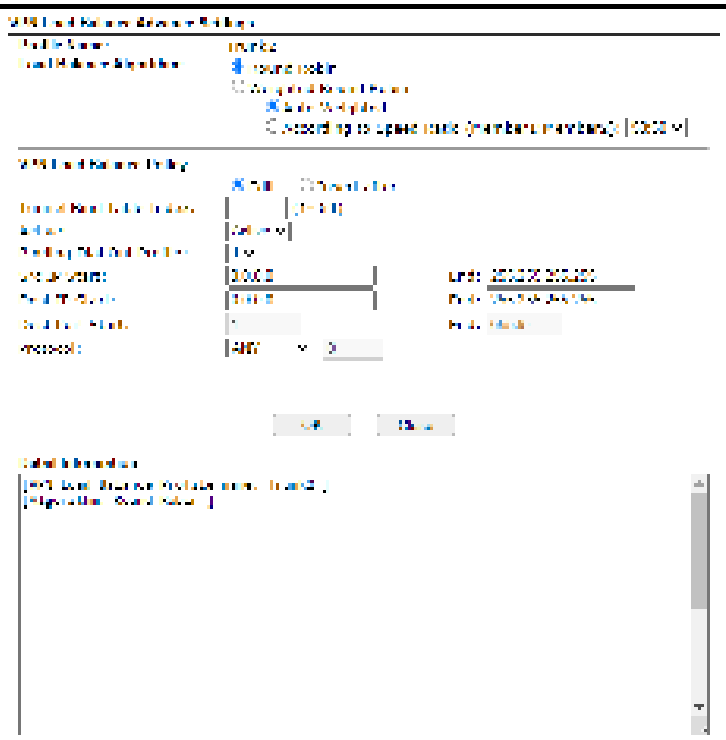
- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/ multi)
- Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and ISDN (depends on hardware specification)
- The web page is simple to understand and easy to configure
- Fully compliant with VPN Server LAN Site Single/ Multi Network
- Mail Alert support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Syslog support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.



Available settings are explained as follows:

Item	Description
Backup Profile List	**Set to Factory Default -** Click to clear all VPN TRUNK-VPN Backup mechanism profile. **No –** The order of VPN TRUNK-VPN Backup mechanism profile. **Status** - "v" means such profile is enabled; "x" means such profile is disabled. **Name -** Display the name of VPN TRUNK-VPN Backup mechanism profile. **Member1 -** Display the dial-out profile selected from the Member1 drop down list below. **Active -** "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN. **Type -** Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on. **Member2 -** Display the dial-out profile selected from the Member2 drop down list below. **Advanced** – This button is available only when LAN to LAN profile (or more) is created. Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.
Load Balance Profile List	**Set to Factory Default -** Click to clear all VPN TRUNK-VPN Load Balance mechanism profile. **No. -** The order of VPN TRUNK-VPN Load Balance mechanism profile. **Status** - "v" means such profile is enabled; "x" means such profile is disabled. **Name -** Display the name of VPN TRUNK-VPN Load Balance mechanism profile. **Member1 -** Display the dial-out profile selected from the Member1 drop down list below. **Active -** "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN. **Type -** Display the connection type for that profile, such as IPsec, PPTP, L2TP, L2TP over IPsec (NICE), L2TP over IPsec(MUST) and so on. **Member2 -** Display the dial-out profile selected from the Member2 drop down list below. **Advanced** – This button is only available when there is one or more profiles created in this page.

	 Detailed information for this dialog, see later section - **Advanced Load Balance and Backup**.
General Setup	**Status**- After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/ Load Balance mechanism profile will not have any effect for VPN tunnel. **Profile Name**- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields. The length of the name is limited to 11 characters. **Member 1**/**Member2** - Display the selection for LAN-to-LAN dial-out profiles (configured in **VPN and Remote Access >> LAN-to-LAN**) for you to choose for grouping under certain VPN TRUNK-VPN Backup/ Load Balance mechanism profile. ● **No** - Index number of LAN-to-LAN dial-out profile. ● **Name** - Profile name of LAN-to-LAN dial-out profile. ● **Connection Type** - Connection type of LAN-to-LAN dial-out profile. ● **VPN ServerIP (Private Network)** - VPN Server IP of LAN-to-LAN dial-out profiles. **Active Mode** - Display available mode for you to choose. **Add -** Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in red. VPN TRUNK – VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in blue. **Update -** Click this button to save the changes to the **Status** (Enable or Disable), profile name, member1 or member2. **Delete -** Click this button 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.

Time for activating VPN TRUNK – VPN Backup mechanism profile

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

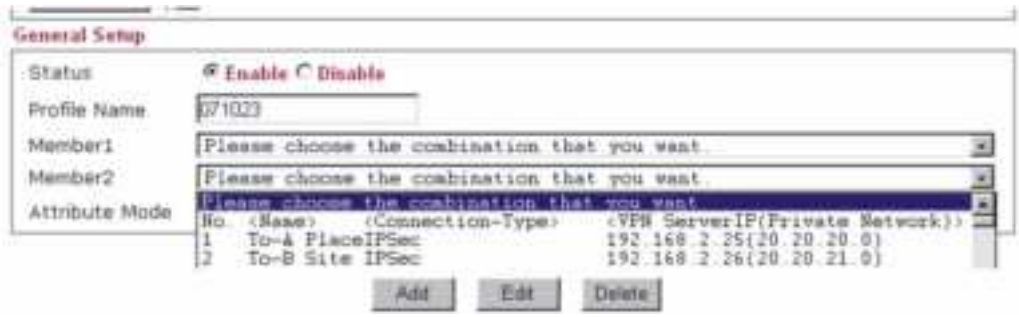
Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

1. First of all, go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup / Load Balance mechanism profile management well.
2. Access into **VPN and Remote Access>>VPN TRUNK Management**.
3. Set one group of VPN TRUNK – VPN Backup/ Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.

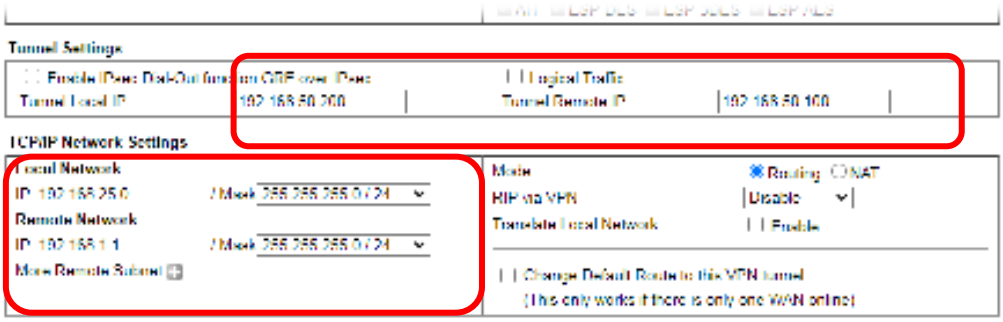


4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup/ Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

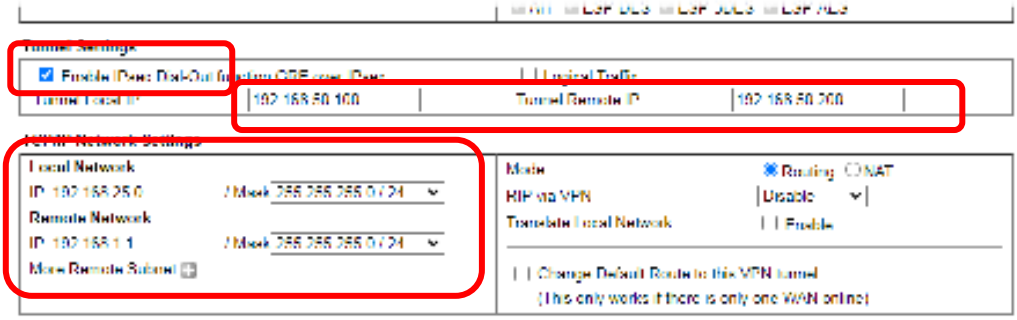
Index	Name	Active	Status
1.	To-A Place	V	offline
2.	To-B Site	V	offline
3.	To-C Place	V	offline
4.	To-D Site	V	offline
5.	222	X	---

How can you set a GRE over IPsec profile?

1. Please go to LAN to LAN to set a profile with IPsec.
2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.



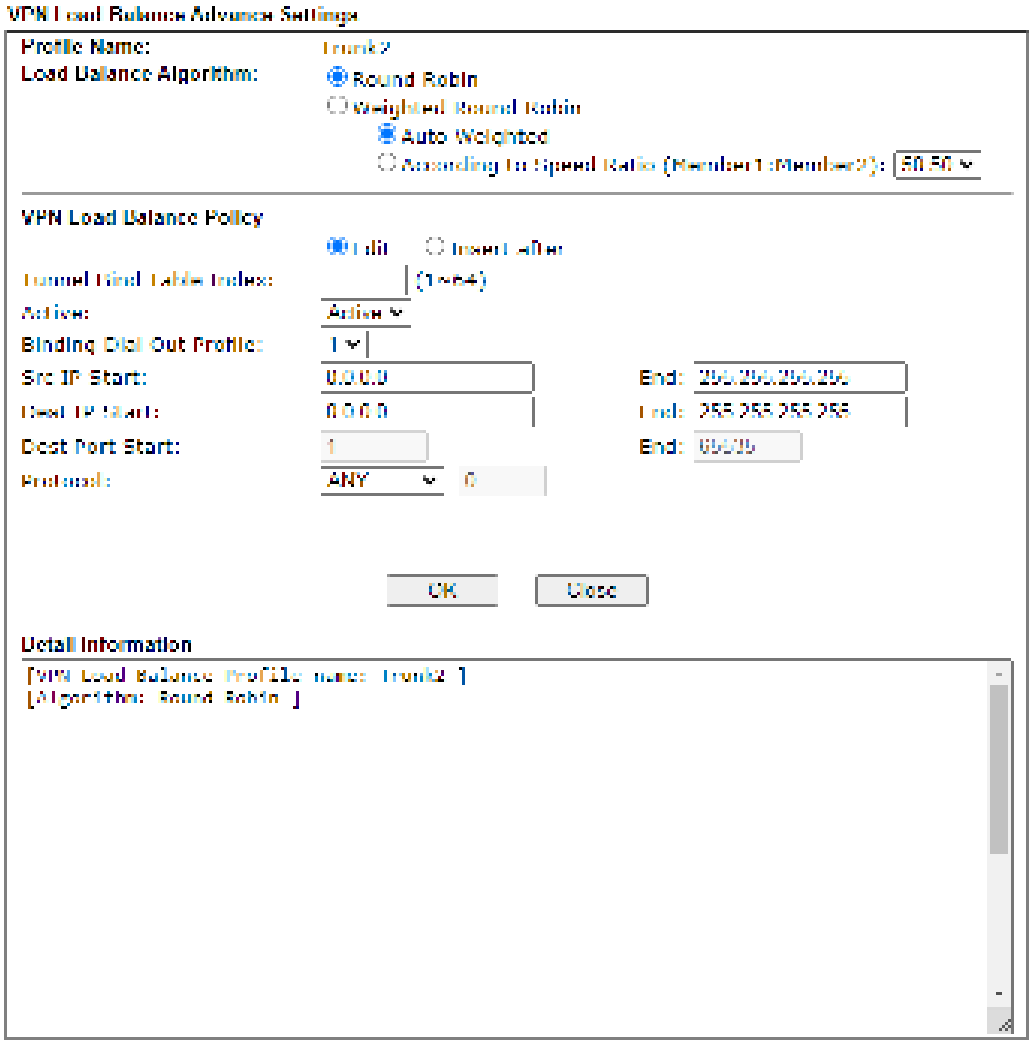
3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.



Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

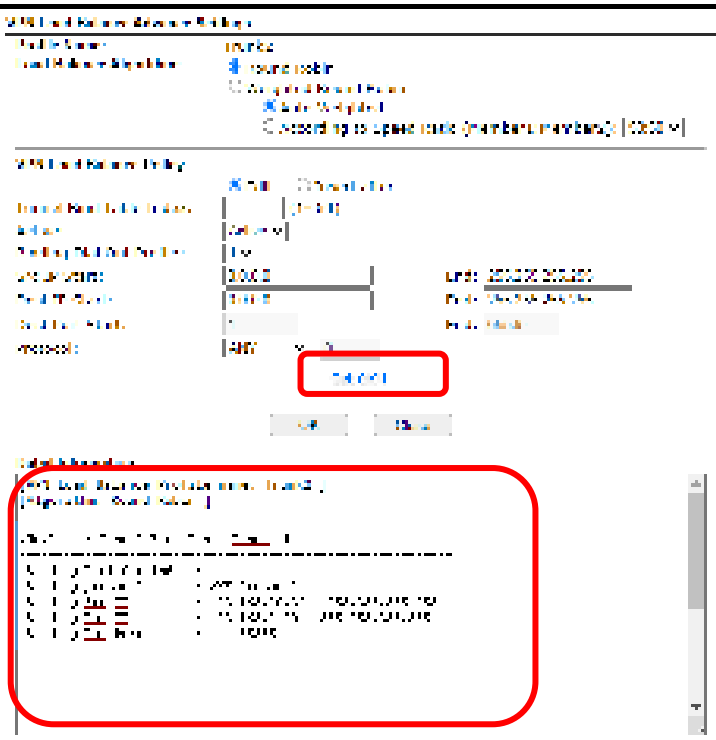
Advanced Load Balance



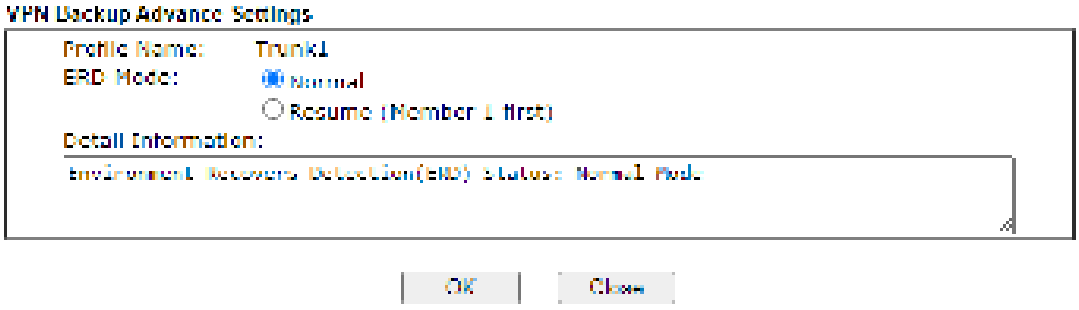
Available settings are explained as follows:

Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	**Round Robin** – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate. **Weighted Round Robin** –Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. **Auto Weighted** can detect the device speed (10Mbps/ 100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. **According to Speed Ratio** allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).
VPN Load Balance Policy	Below shows the algorithm for Load Balance. **Edit** – Click this radio button for assign a blank table for configuring Binding Tunnel. **Insert after** – Click this radio button to adding a new binding

	tunnel table. **Tunnel Bind Table Index**- 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile. **Active** – In-active/ Delete can delete this binding tunnel table. Active can activate this binding tunnel table. **Binding Dial Out Index** – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table. **Scr IP Start** /**End**– Specify source IP addresses as starting point and ending point. **Dest IP Start**/**End** – Specify destination IP addresses as starting point and ending point. **Dest Port Start** /**End**– Specify destination service port as starting point and ending point. **Protocol** – **Any** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/ UDP Service Port/ ICMP/ IGMP specified here. **TCP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. **UDP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. **TCP**/**UPD** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/ UDP Service Port also fits the number here, such binding tunnel table can be established. **ICMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. **Other** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/ UDP Service Port/ ICMP/ IGMP, such binding tunnel table can be established.
Detail Information	This field will display detailed information for Binding Tunnel Policy. Below shows a successful binding tunnel policy for load balance:

	 **To configure a successful binding tunnel, you have to:** Type Binding Src IP range (Start and End) and Binding Des IP range (Start and End). Choose TCP/ UDP, IGMP/ ICMP or Other as Binding Protocol.

Advanced Backup

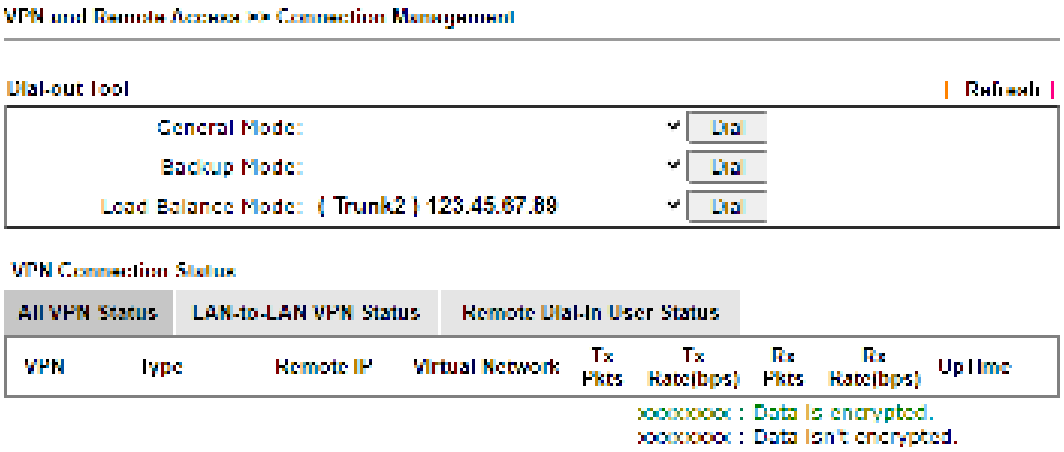


Available settings are explained as follows:

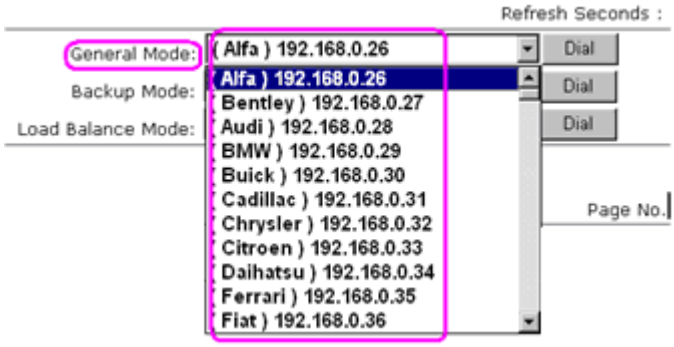
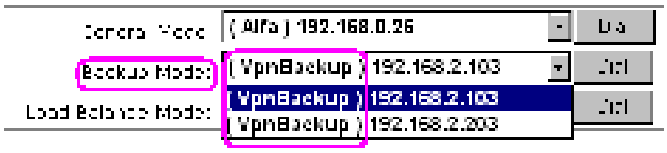
Item	Description
Profile Name	List the backup profile name.
ERD Mode	ERD means “Environment Recovers Detection”. **Normal** – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively. **Resume** – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.
Detail Information	This field will display detailed information for Environment Recovers Detection.

IV-1-13 Connection Management

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



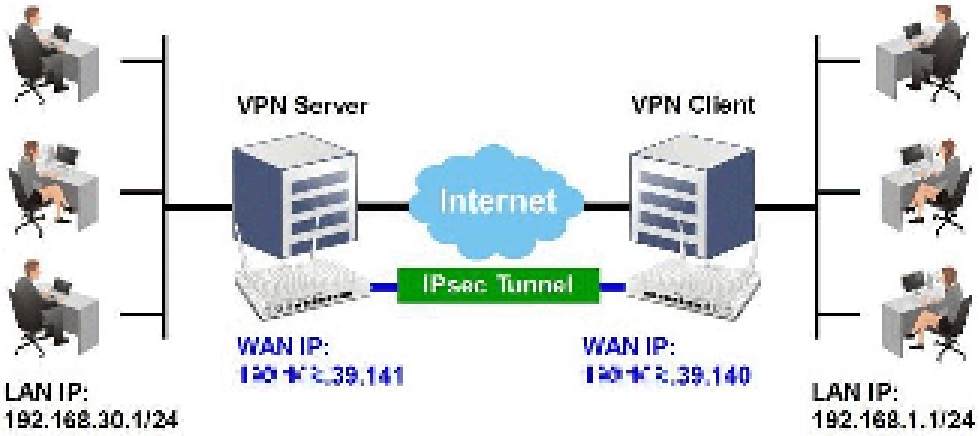
Available settings are explained as follows:

Item	Description
Dial-out Tool	**General Mode -** This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.  **Backup Mode -** This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.  **Dial -** Click this button to execute dial out function. **Refresh Seconds -** Choose the time for refresh the dial information among 5, 10, and 30. **Refresh -** Click this button to refresh the whole connection status.

Application Notes

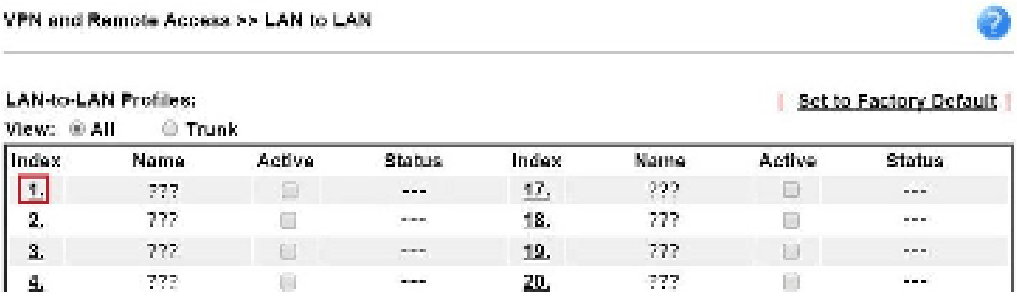
A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode

This document introduces how to set up Main mode IPsec Tunnel between two Vigor Routers. IPsec VPN with Main mode use the IP address of VPN client as identifier, and the IP address must be set on VPN server; therefore, if the VPN client doesn't have a static IP, please use Aggressive mode instead.

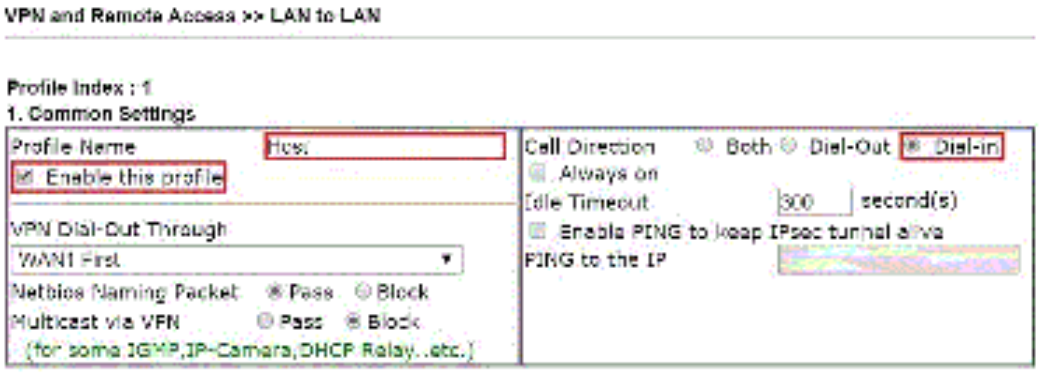


VPN Server (Dial-In Site) Setup

1. Create a Dial-In profile for VPN user, go to **VPN and Remote Access >> LAN to LAN**, click on an available index to add a new profile.



2. Set up the dial-in profile.



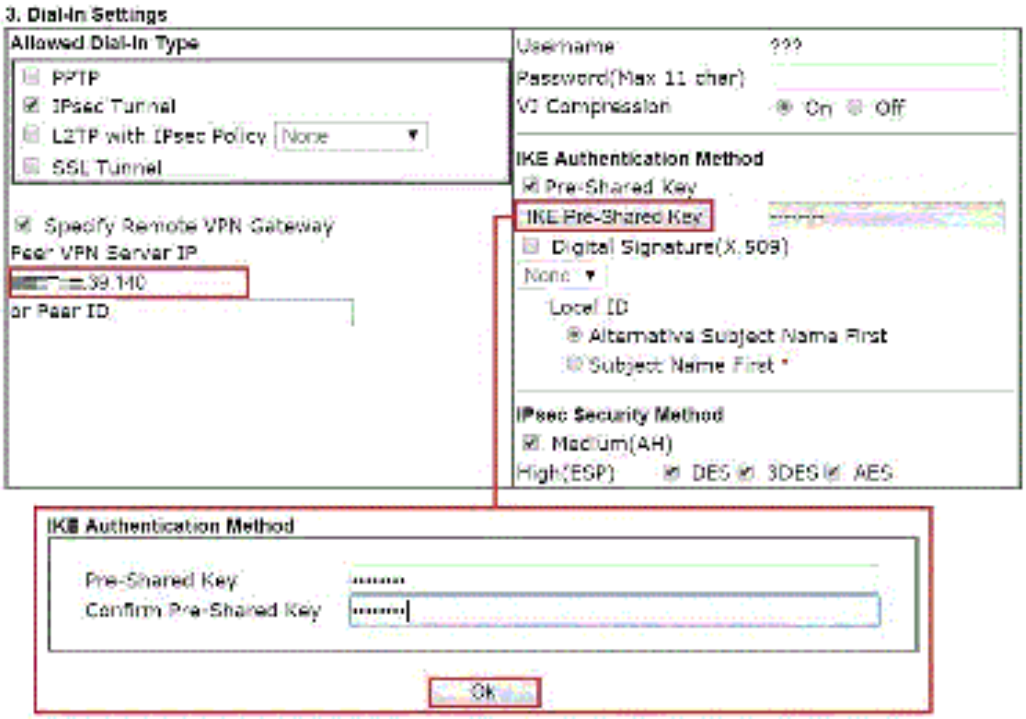
In Common Settings,

(a) Enter the **Profile Name**.

(b) Enable this profile.

(c) Set **Call Direction** to **Dial-in**.

In Dial-In Setting,



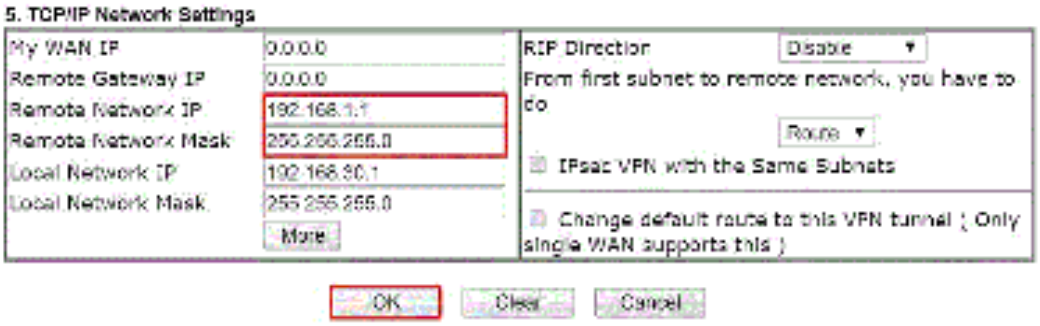
(d) Make sure Allowed Dial-in Type has **IPsec Tunnel** enabled.

(e) Enable **Specify Remote VPN Gateway** and enter **Peer VPN Server IP** as the public IP of VPN client router.

(f) Click on **IKE Pre-Shared Key** and enter the Pre-shared Key.

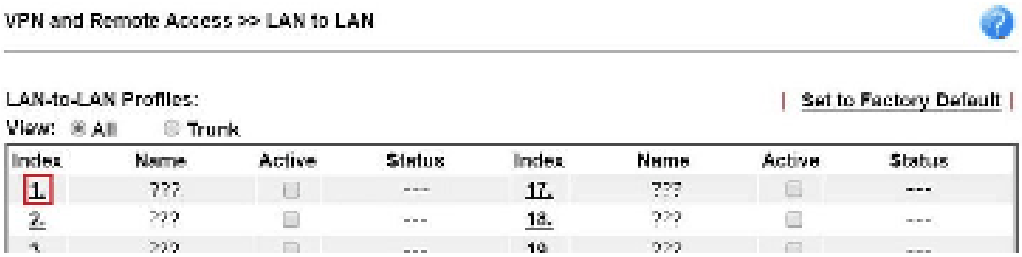
(g) Select the **IPsec Security Method** that are allowed to use.

3. In TCP/IP Network Settings, enter VPN Client's LAN network in **Remote Network IP** and **Remote Network Mask**. Click **OK** to save the profile.



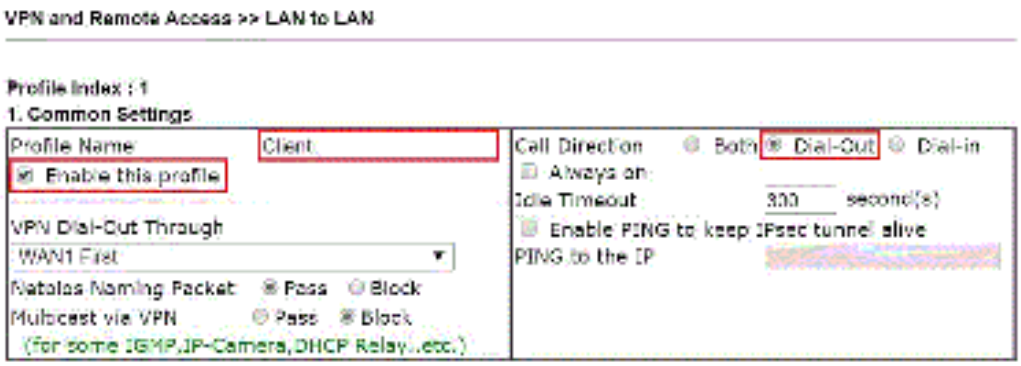
VPN Client (Dial-out Site) Setup

1. Create a Dial-out profile to VPN server: Go to VPN and Remote Access >> LAN to LAN, click on an available index to add a new profile.



2. Setup the dial-out profile.

In Common Settings,

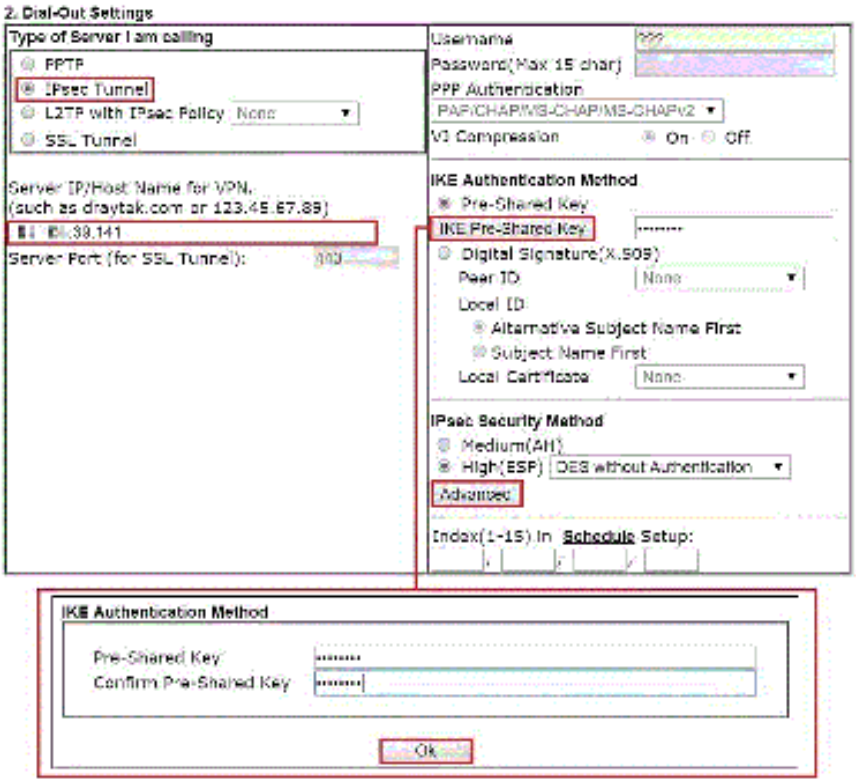


(a) Enter a **Profile Name**.

(b) Enable this profile.

(c) Set **Call Direction** to **Dial-Out**.

In Dial-out Setting,



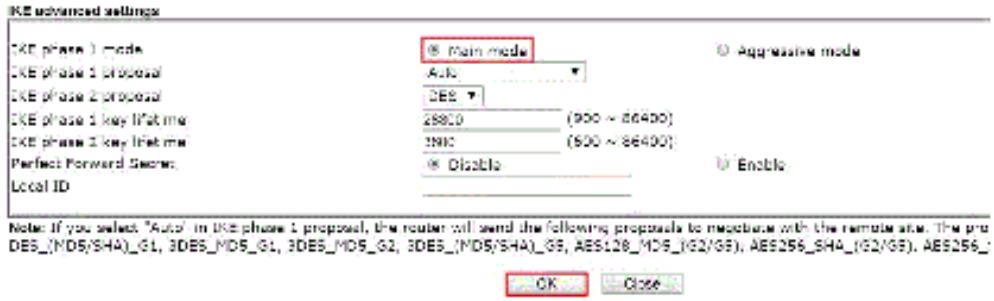
(d) Select **IPsec Tunnel** for **Type of Sever I am Calling**.

(e) Enter VPN Server's WAN IP or domain name in **Sever IP/Host Name for VPN**.

(f) Click **IKE Pre-Shared Key** and enter the same Pre-Shared key as VPN Server.

(g) Click on **Advanced** in IPsec Security Method.

In IKE advanced settings,

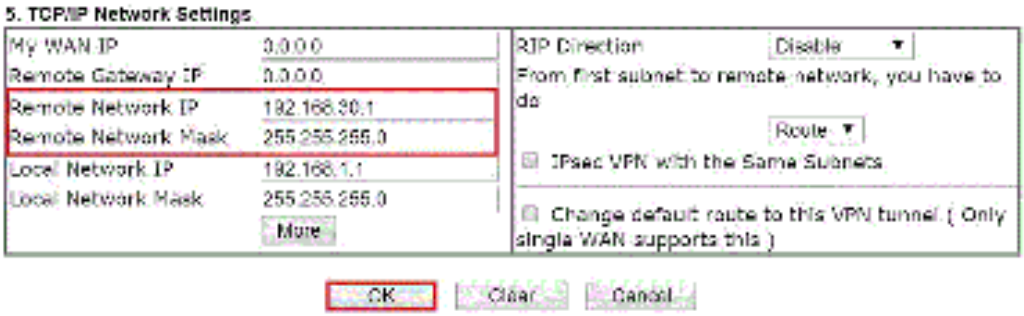


(h) Select **Main Mode** for IKE phase 1 mode.

(i) Make sure phase 1 and phase 2 proposal are using the security methods which are accepted by VPN server.

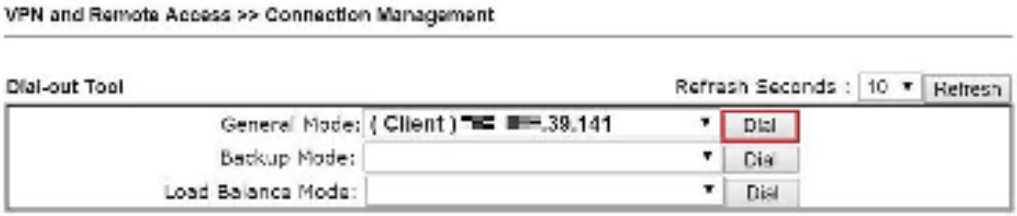
(j) Click **OK** to save.

3. In TCP/IP Network Settings, enter VPN Server's LAN Network in **Remote Network IP** and **Remote Network Mask**. Click **OK** to save the profile.



VPN Tunnel Establishment

To initiate the VPN connection, go to **VPN and Remote Access >> Connection Management** on VPN Client. Select the profile to VPN Sever and click **Dial**.

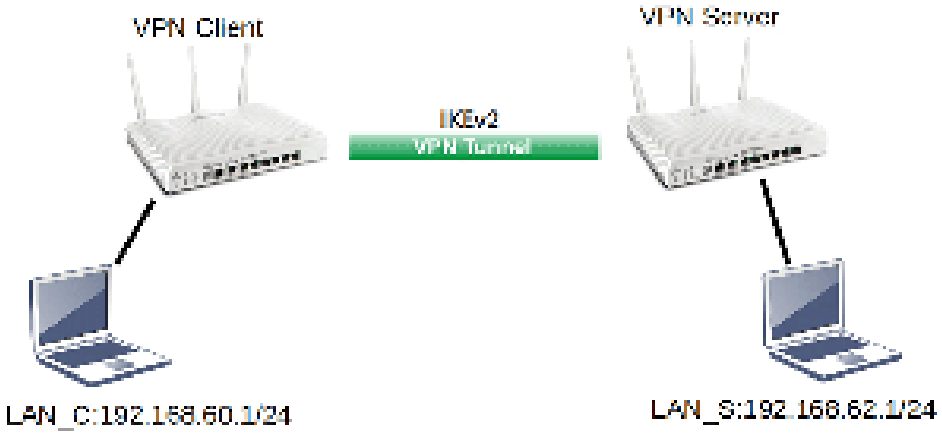


If all the settings are matched, the VPN will be established, and the statistics will be displayed on the same page.

A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2

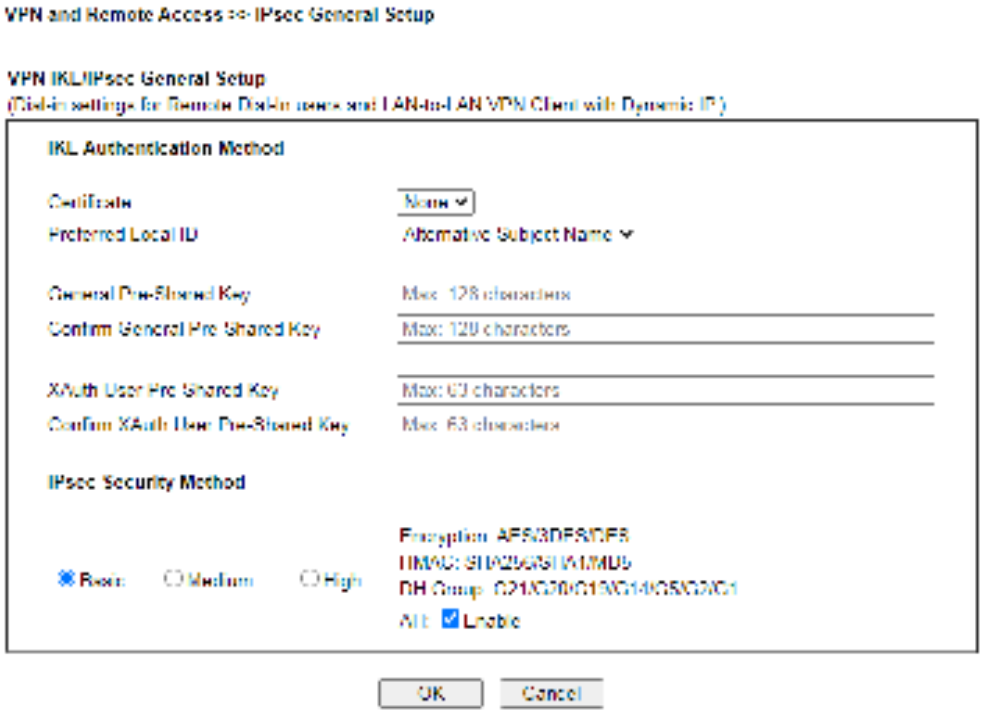
Modified from the previous version IKEv1, IKEv2 is a new VPN protocol and has lots of improvements then the former. It is more stable, more secure and faster connection establishing speed. Support newer and more complicated secure ciphers to make the connection more secure. Using new connection progress and discard the PPP, IKEv2 provides the faster establishing speed.

This application note demonstrates how to establish IKEv2 VPN connection between two Vigor Routers by the following topology.



VPN Server Settings

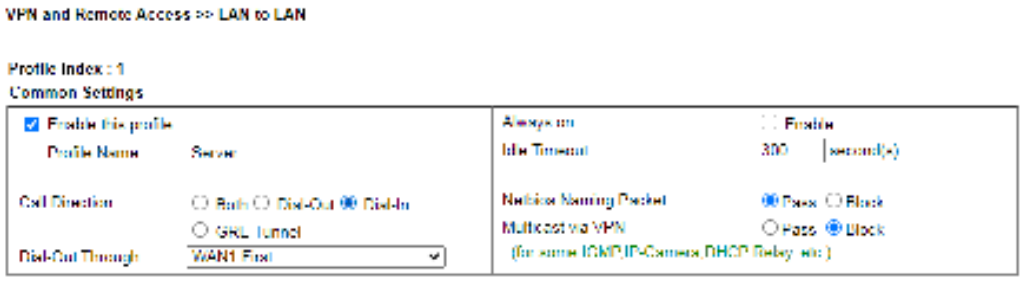
1. Go to **VPN and Remote Access >> IPsec General Setup**.



(a) Input **Pre-shared Key** and **Confirm Pre-Shared Key**.

(b) Click **OK**.

2. Go to **VPN and Remote Access >> LAN to LAN** and click an available index.



(a) Check **Enable this profile**.

(b) Select **Dial-in** as **Call Direction**.

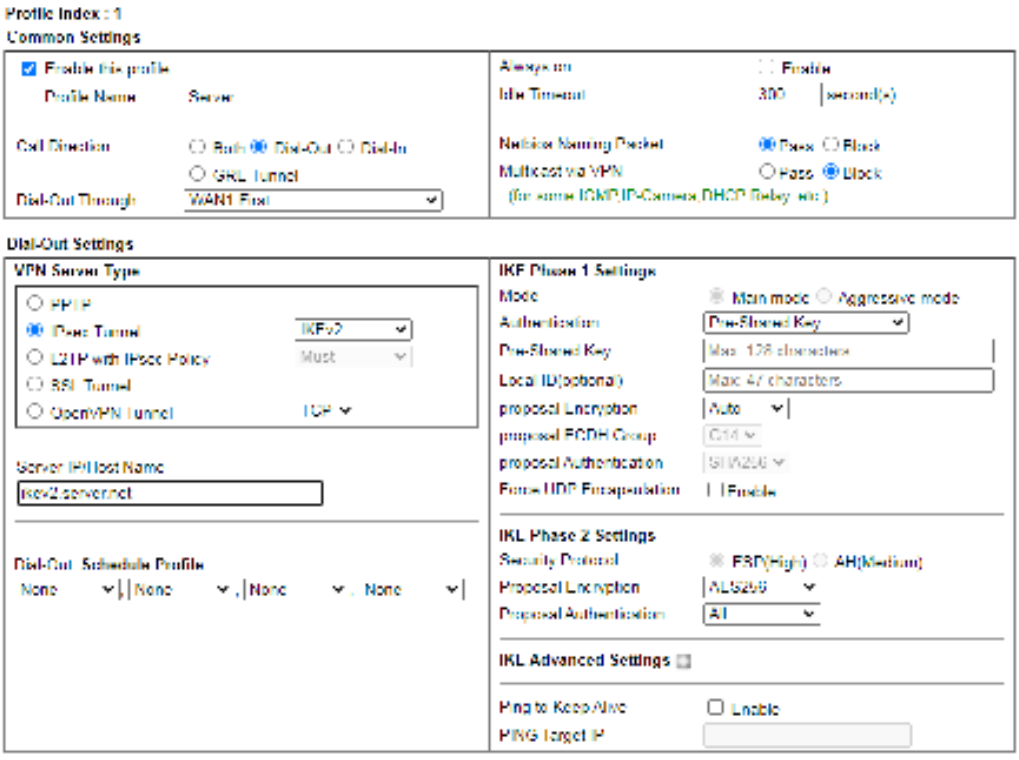
(c) Allow **IPsec Tunnel** in Dial-In Settings.

(d) Input the IP address of LAN_C as **Remote Network IP** and **Remote Network Mask**.

(e) Click **OK**.

VPN Client Settings

1. Go to **VPN and Remote Access >> LAN to LAN** and click an available index.



(a) Give a Profile Name.

(b) Check **Enable this profile**.

(c) Select **Dial-Out** as **Call Direction**.

(d) Select **IPsec Tunnel** with **IKEv2** in Dial-Out Settings.

(e) Input VPN server's WAN IP or domain name at **Server IP/Host Name for VPN**.

(f) Input **Pre-Shard Key** of VPN server.

2. In TCP/ IP Network Settings, input the IP address of LAN_S as Remote Network IP and Remote Network Mask. Click **OK** to save the profile.

IV-2 Certificate Management

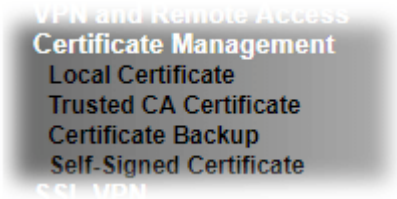
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

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

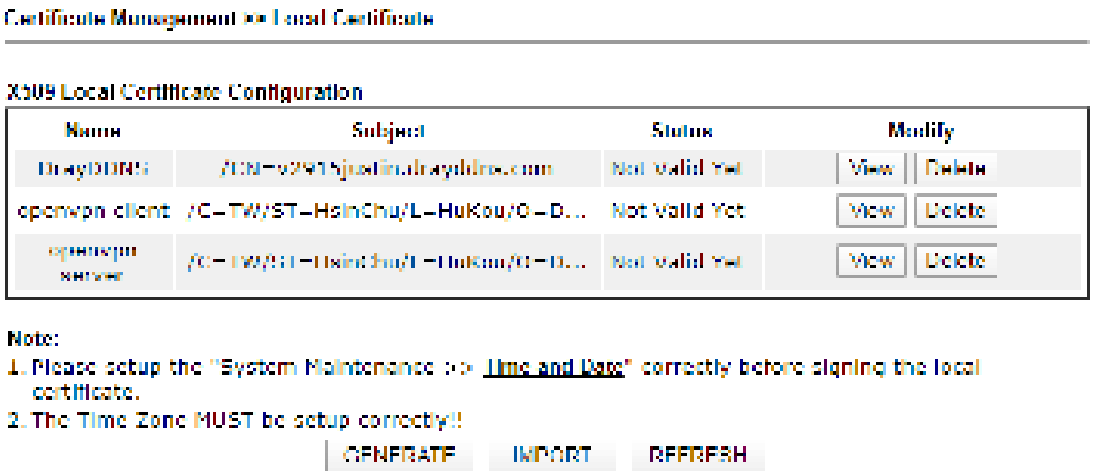
Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

Web User Interface



IV-2-1 Local Certificate

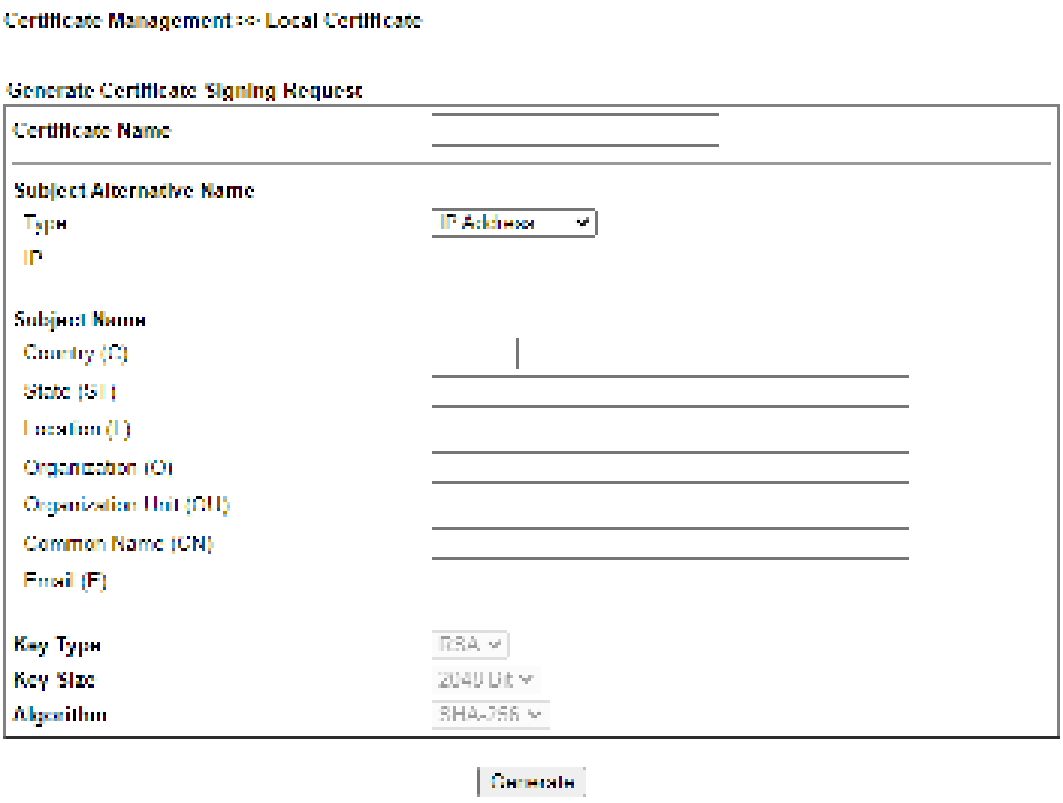


Available settings are explained as follows:

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

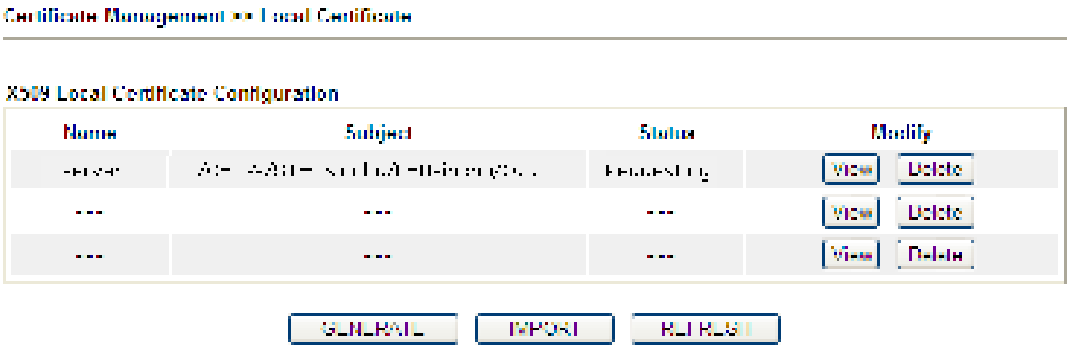
GENERATE

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



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

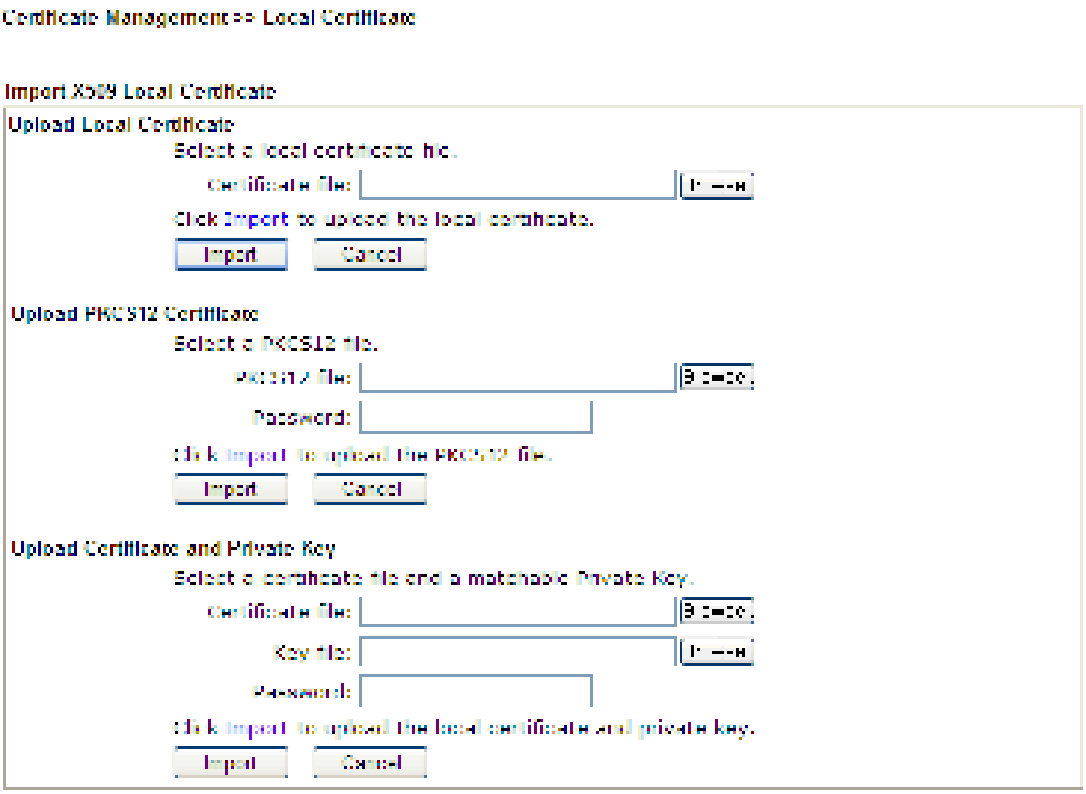
After clicking **GENERATE**, the generated information will be displayed on the window below:



IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

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



Available settings are explained as follows:

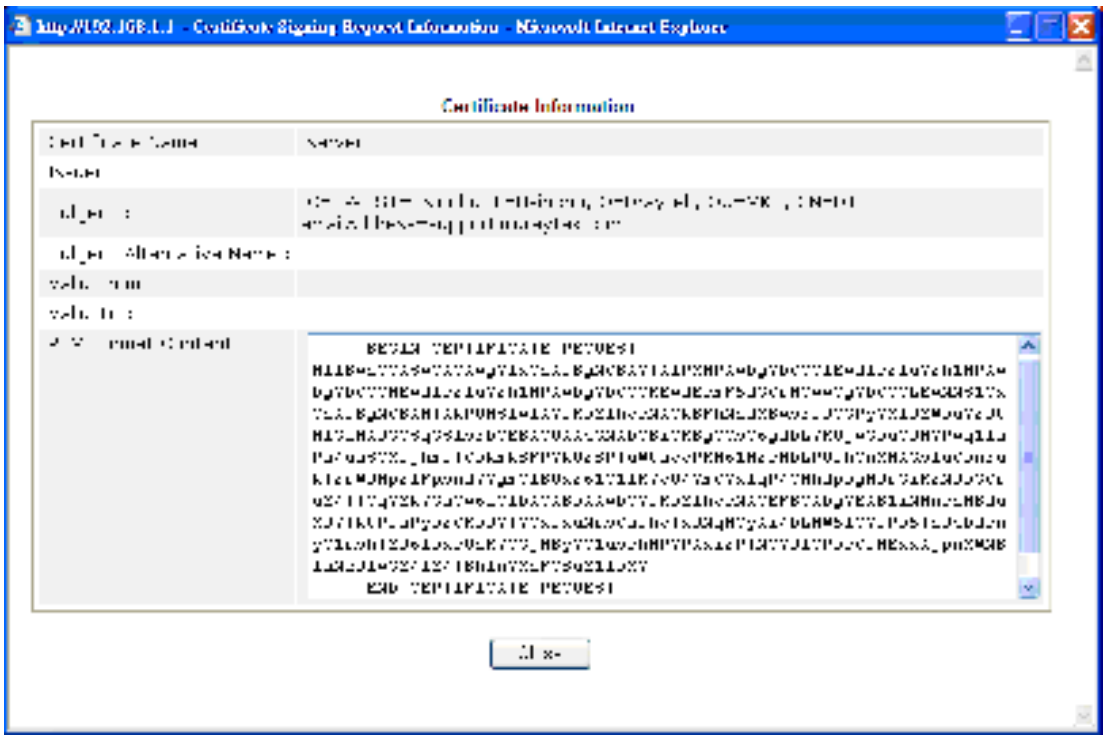
Item	Description
Upload Local Certificate	It allows users to import the certificate which is generated by Vigor router and signed by CA server. If you have done well in certificate generation, the Status of the certificate will be shown as "**OK**".
Upload PKCS12 Certificate	It allows users to import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

REFRESH

Click this button to refresh the information listed below.

View

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



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

Delete

Click this button to remove the selected certificate.

IV-2-2 Trusted CA Certificate

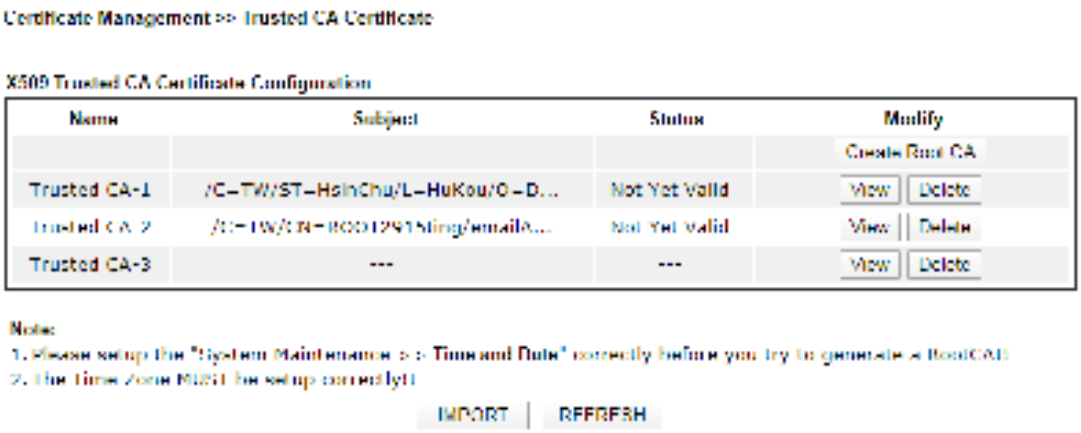
Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

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.

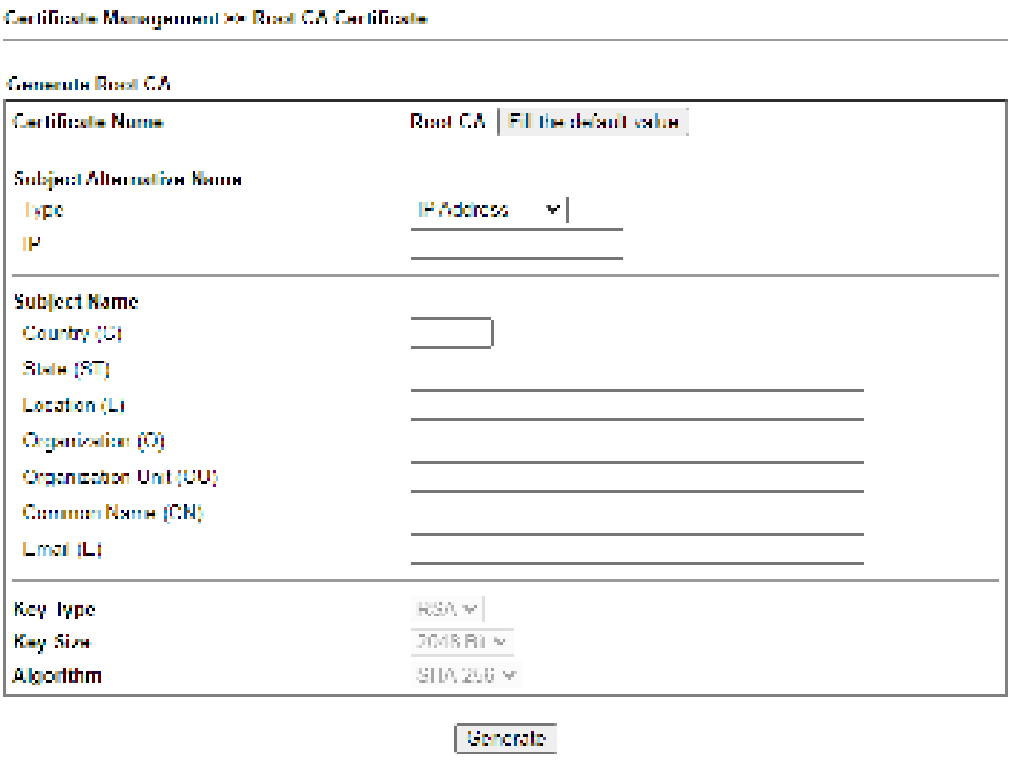
Info

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.



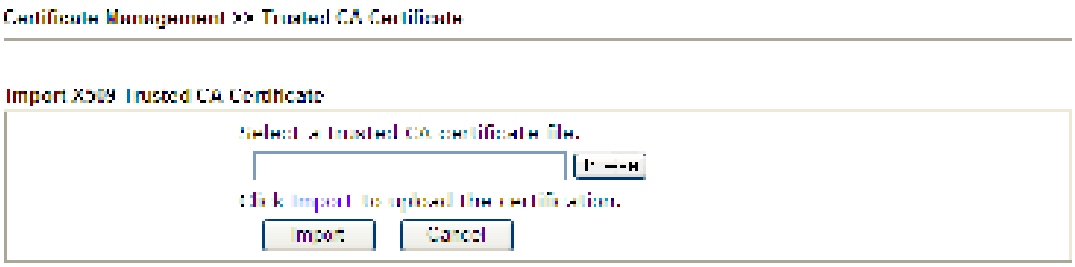
Creating a Root CA

Click **Create** to open the following page. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **Generate** again. Click the **Fill the debault value** button to enter related values automatically.

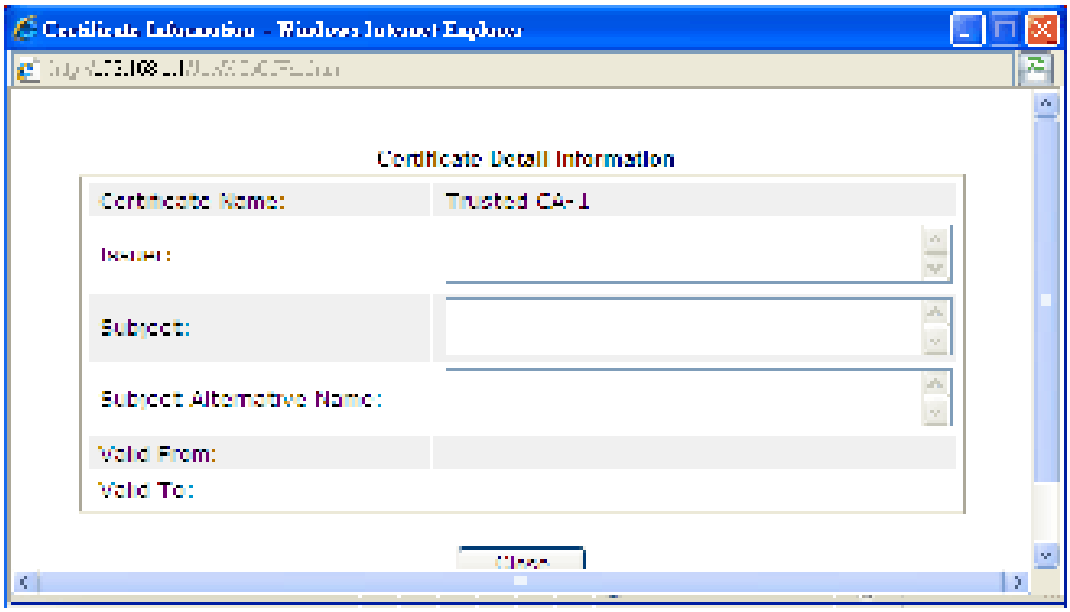


Importing a Trusted CA

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



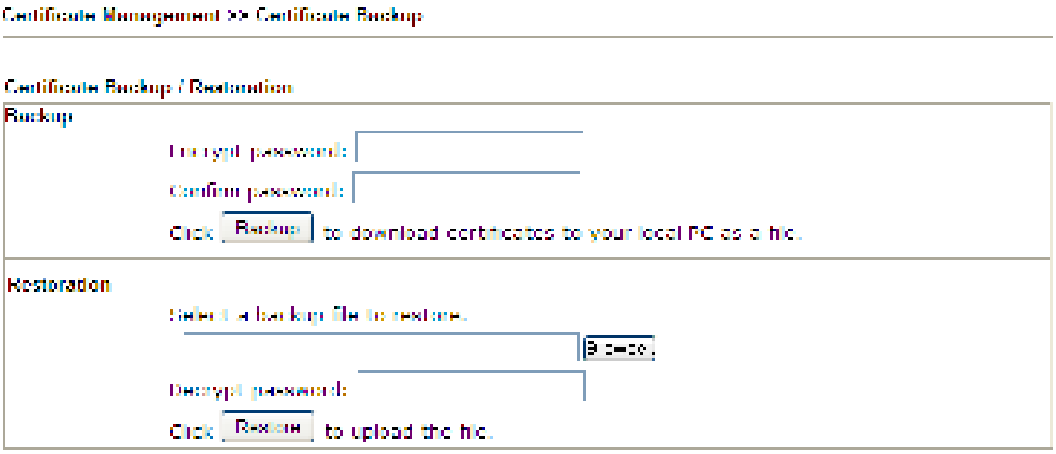
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



IV-2-3 Certificate Backup

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

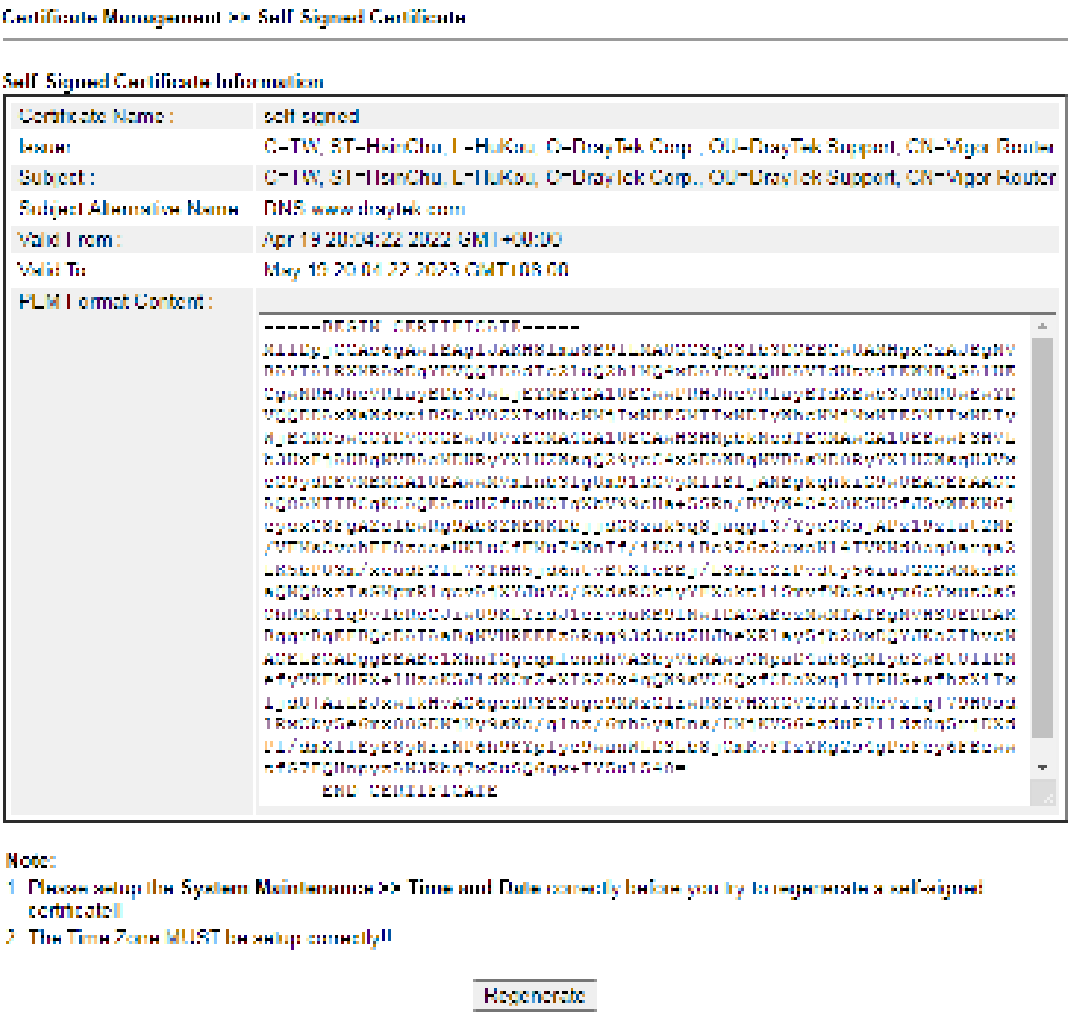
Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



IV-2-4 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.



Click **Regenerate** to open **Regenerate Self-Signed Certificate** window. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

Part V Security

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.

V-1 Firewall

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

Firewall Facilities

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

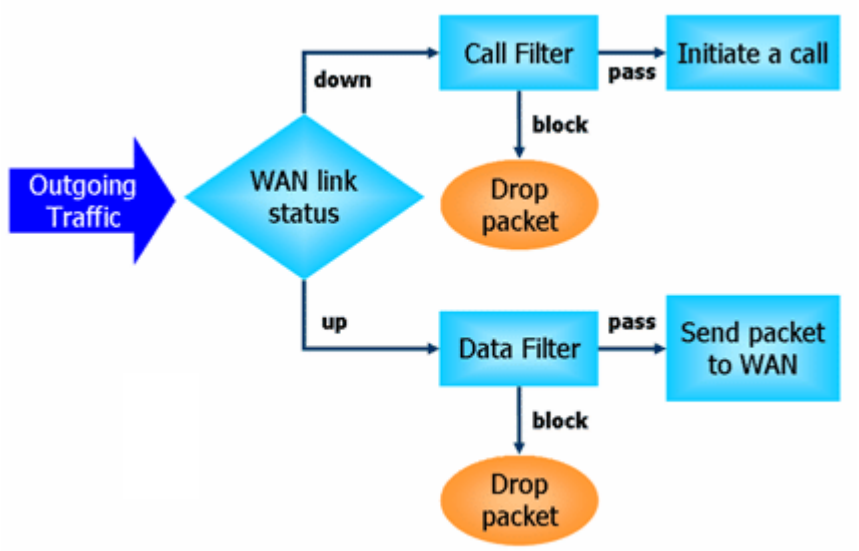
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) / Distributed DoS (DDoS) attacks protection

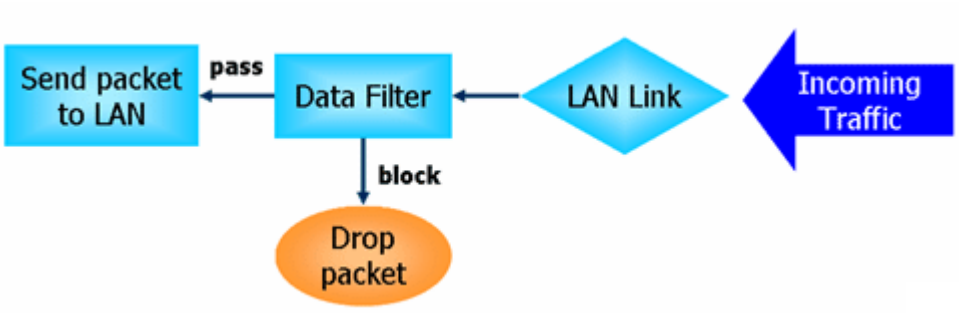
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

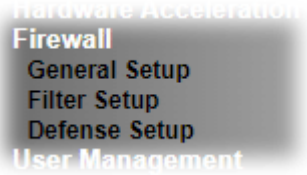
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

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

Web User Interface

Below shows the menu items for Firewall.



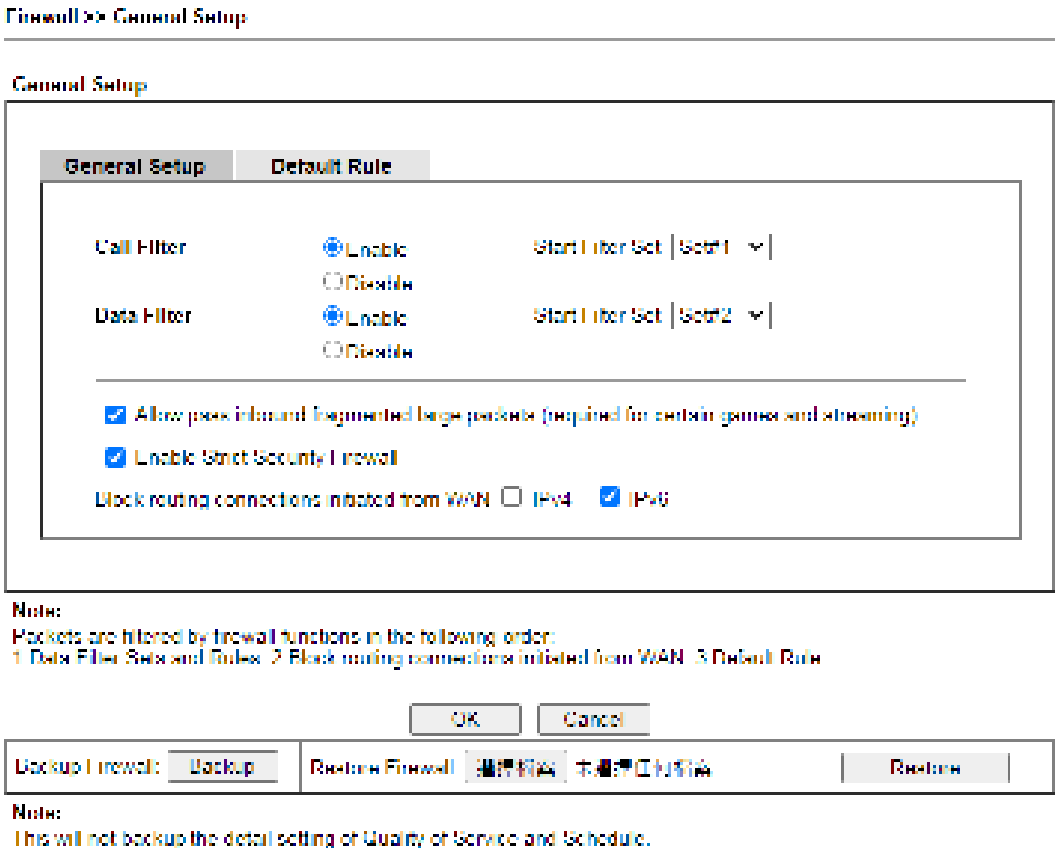
V-1-1 General Setup

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

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

General Setup Page

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

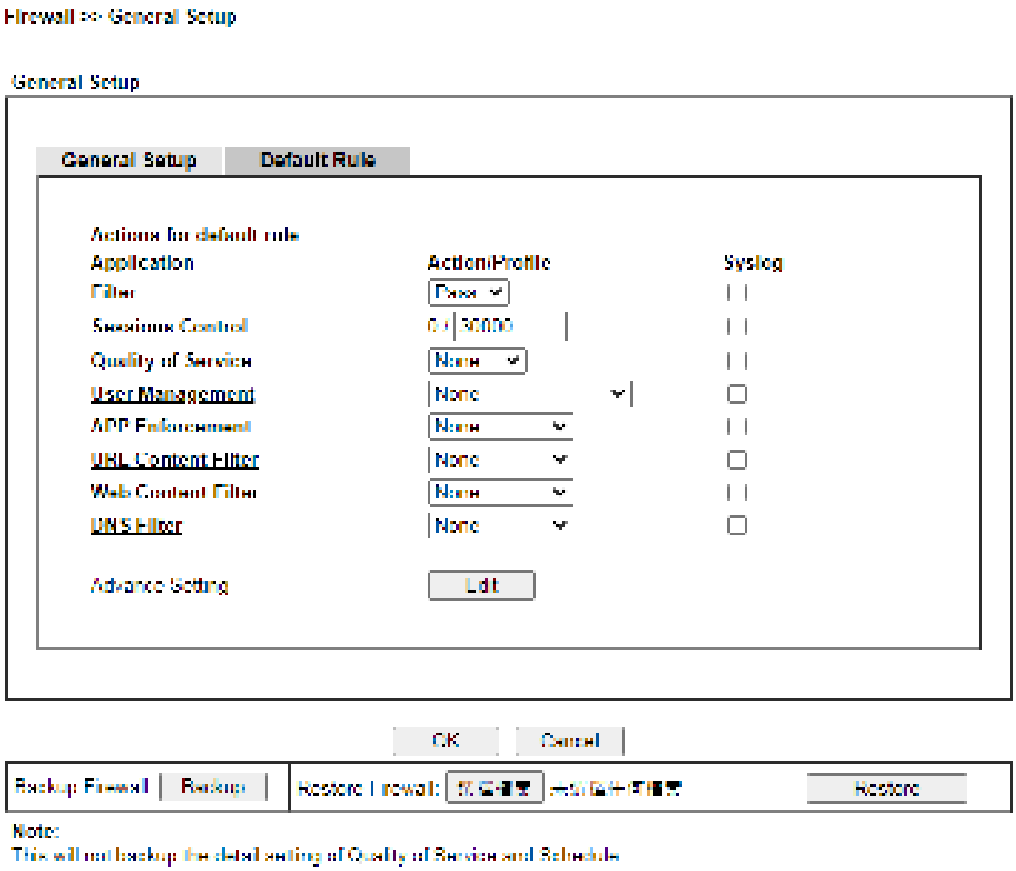


Available settings are explained as follows:

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

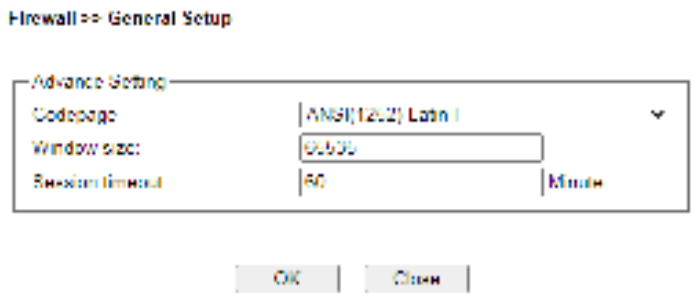
Default Rule Page

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



Available settings are explained as follows:

Item	Description
Filter	Select **Pass** or **Block** for the packets that do not match with the filter rules.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 50000.
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	Such item is available only when **Rule-Based** is selected in **User Management>>General Setup**. The general firewall rule will be applied to the user/ user group/ all users specified here. When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.
APP Enforcement	Select an **APP Enforcement** profile for global IM/ P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile

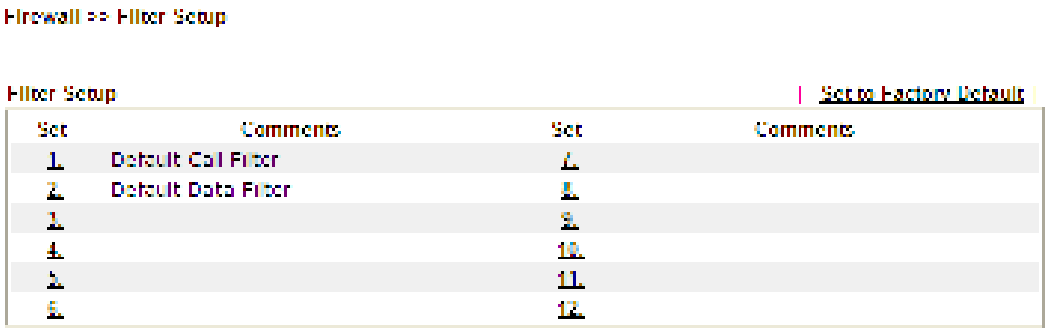
	selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link in this page to create a new profile.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtain correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

	 Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper. **Session timeout** – Setting timeout for sessions can make the best utilization of network resources.

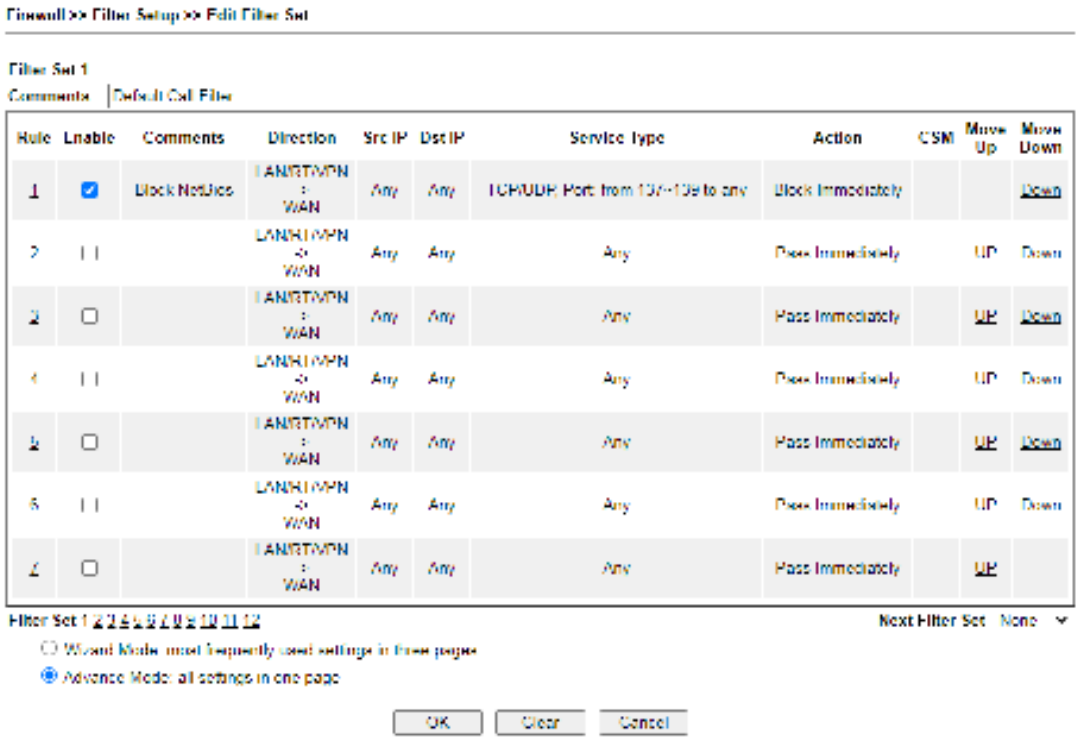
After finishing all the settings here, please click **OK** to save the configuration.

V-1-2 Filter Setup

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



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



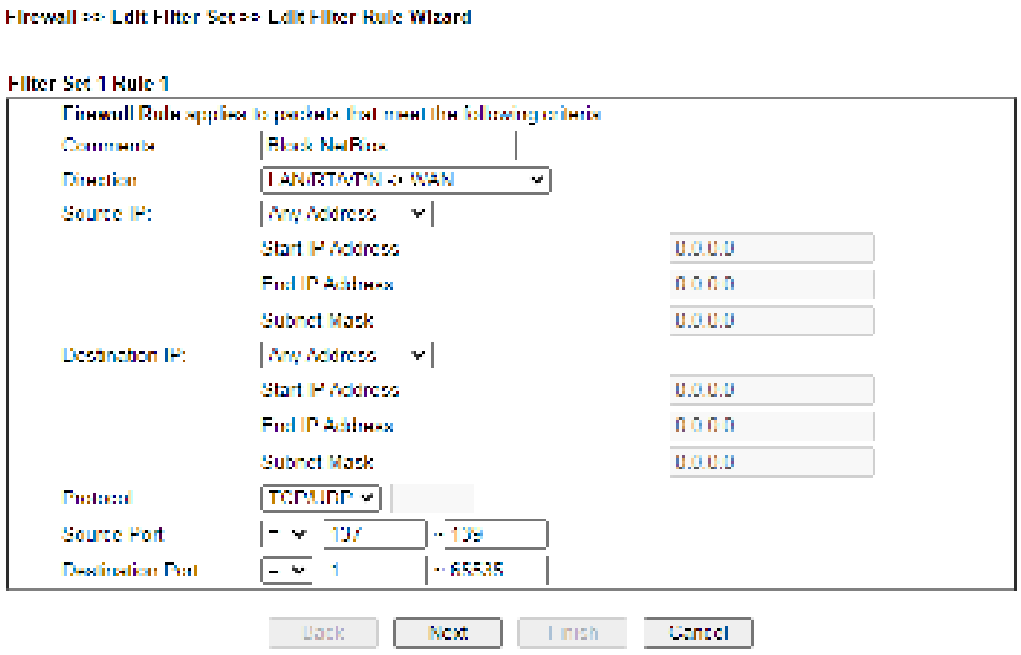
Available settings are explained as follows:

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

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

To use Wizard Mode, simple do the following steps:

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

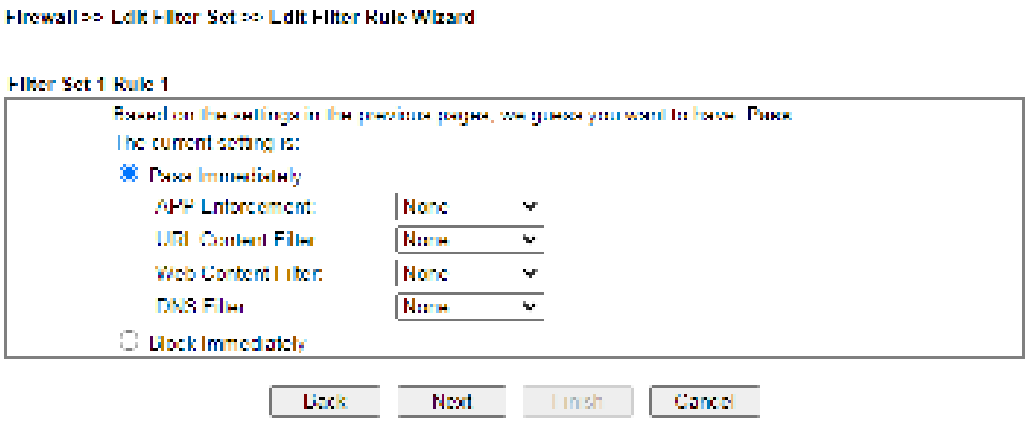


Available settings are explained as follows:

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

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

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

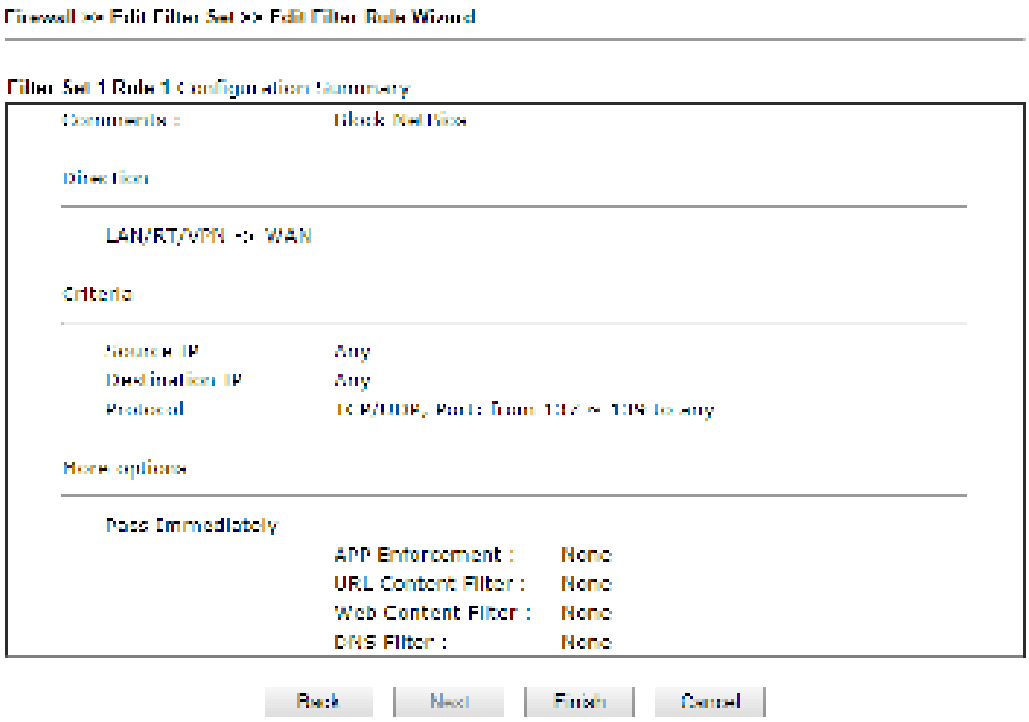


Available settings are explained as follows:

Item	Description
Pass Immediately	Packets matching the rule will be passed immediately. **APP Enforcement -** Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information. **URL Content Filter -** Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information. **Web Content Filter -** Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed

	information. **DNS Filter -** Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.
Block Immediately	Packets matching the rule will be dropped immediately.

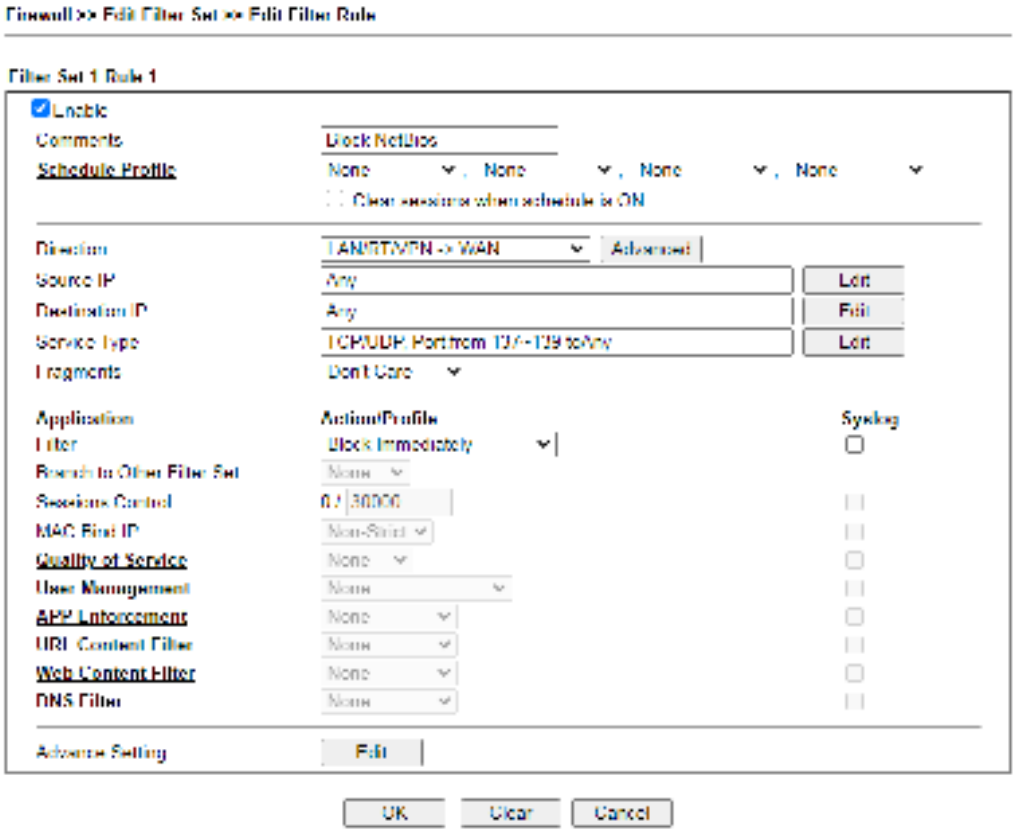
4. After choosing the mechanism, click **Next** to get the summary page for reference.



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

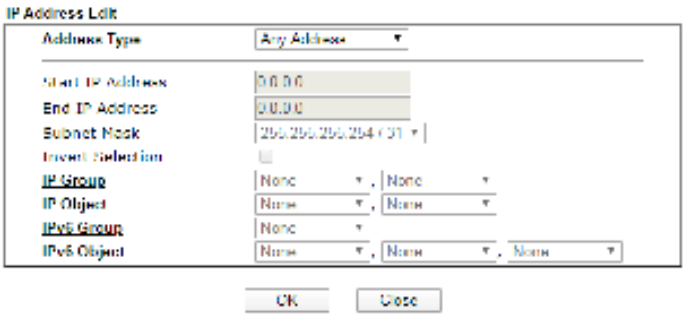
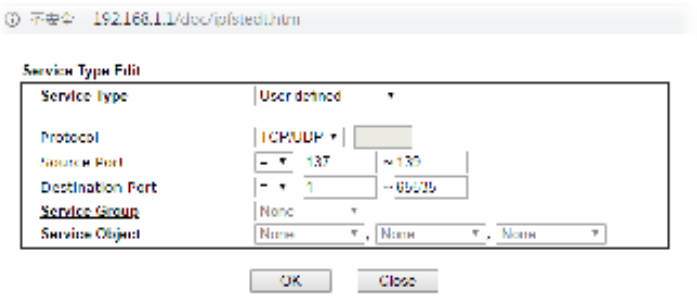
To use **Advance** Mode, do the following steps:

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

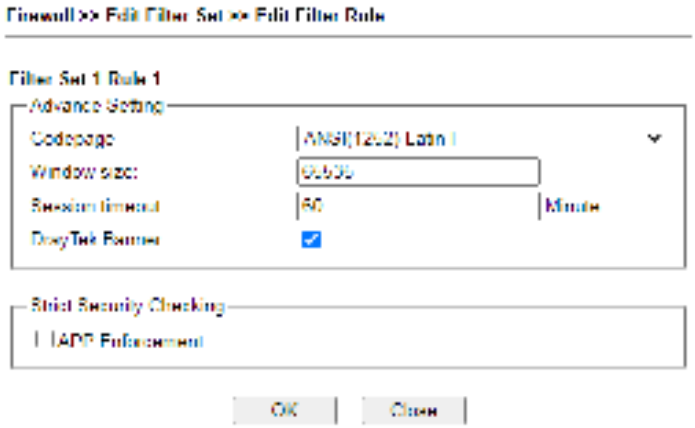


Available settings are explained as follows:

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

	 To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and Enter them in this dialog. In addition, if you want to use the IP range from defined groups or objects or any IP in a country, please choose **Group and Objects** as the Address Type. From the **IP Group/IPv6 Group** drop down list, choose the one that you want to apply. Or use the **IP Object** / **IPv6 Group** drop down list to choose the object that you want.
Service Type	Click **Edit** to access into the following dialog to choose a suitable service type.  To set the service type manually, please choose **User defined** as the Service Type and Enter them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type. **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port –** ***(=)*** –when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. ***(!=)*** –when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** –the port number greater than this value is available. ***(<)*** –the port number less than this value is available for this profile. **Service Group/Object** - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only.

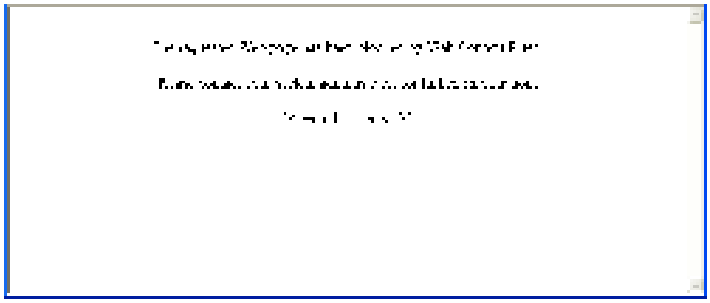
	Don't care -No action will be taken towards fragmented packets. ***Unfragmented -***Apply the rule to unfragmented packets. ***Fragmented -*** Apply the rule to fragmented packets. ***Too Short -*** Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately -** Packets matching the rule will be dropped immediately. **Pass Immediately -** Packets matching the rule will be passed immediately. **Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	**Strict** – Make the MAC address and IP address settings configured in **IP Object** for **Source IP** and **Destination IP** are bound for applying such filter rule. **No-Strict -** no limitation.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.
User Management	Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall rule will be applied to the user/ user group/ all users specified here. **Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.
APP Enforcement	Select an **APP Enforcement** profile for global IM/ P2P application blocking. If there is no profile for you to select, please choose **[Create New]** from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/ P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create

	a new profile. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
Web Content Filter	Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
DNS Filter	Select one of the DNS Filter profile settings (created in CSM>>DNS Filter) for applying with this router. Please set at least one profile in **CSM>> Web Content Filter** web page first. Or click the DNS Filter link from the drop down list in this page to create a new profile.
Advance Setting	Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.  **Codepage** - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.



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

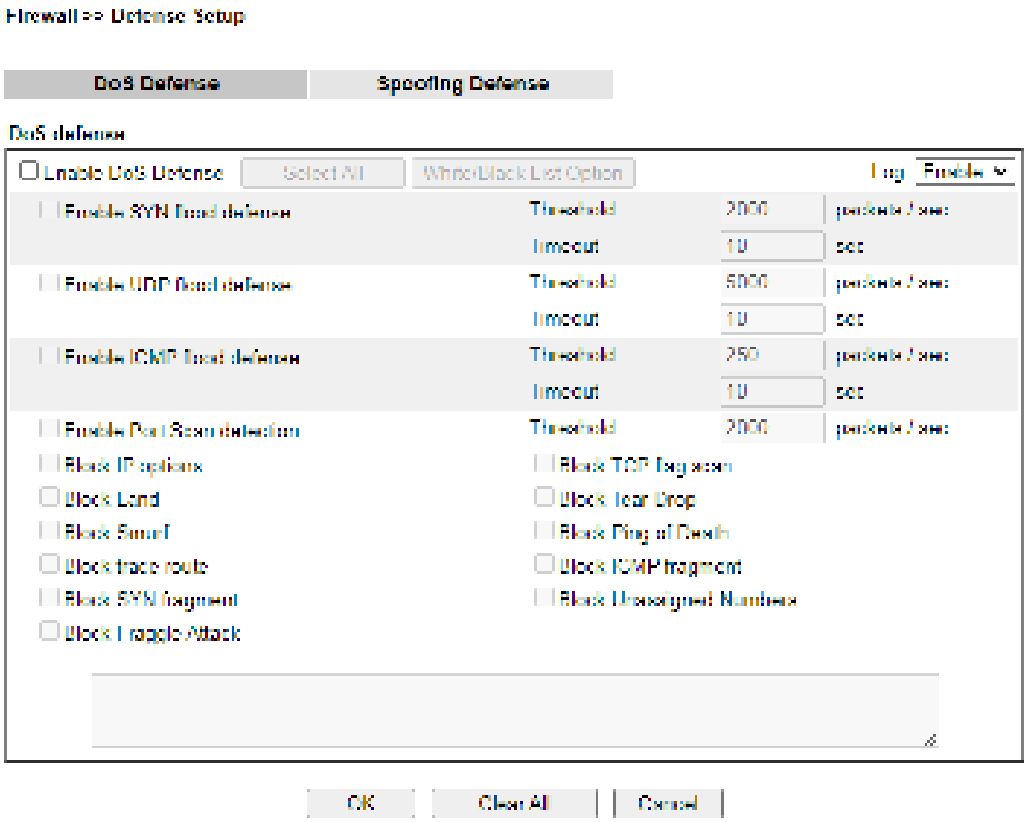
3. When you finish the configuration, please click **OK** to save and exit this page.

V-1-3 Defense Setup

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

V-1-3-1 DoS Defense

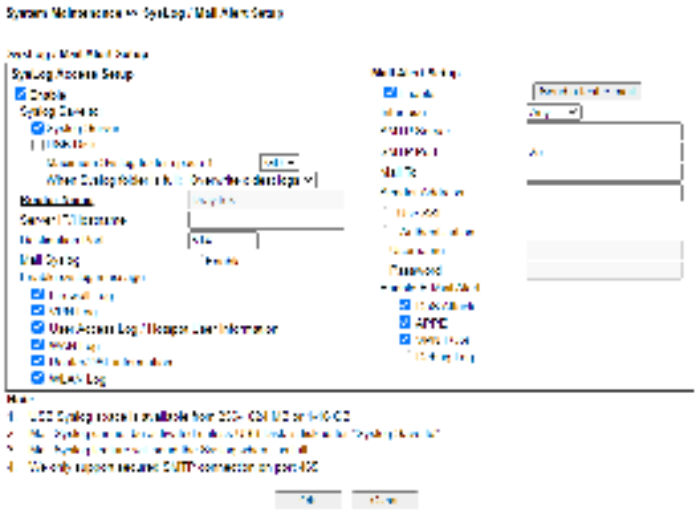
Click **Firewall** and click **DoS Defense** to open the setup page.

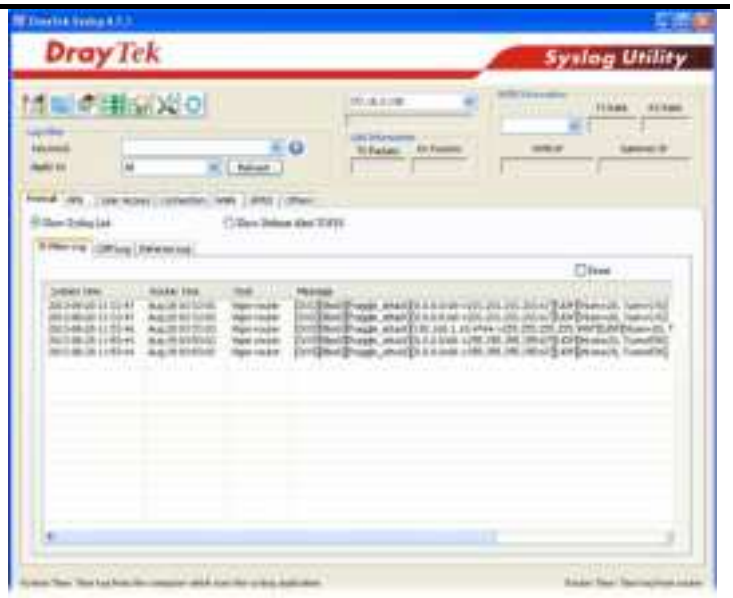


Available settings are explained as follows:

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

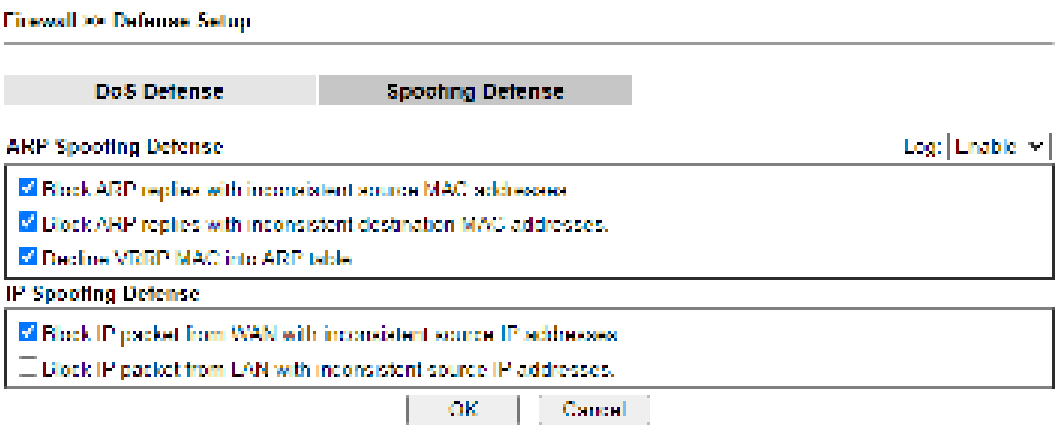
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 5000 packets per second and 10 seconds, respectively. That means, when 5000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable Port Scan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace route	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.

	Activating the DoS/ DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected. 



V-1-3-2 Spoofing Defense

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



V-2 Central Security Management (CSM)

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

APP Enforcement Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserved attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

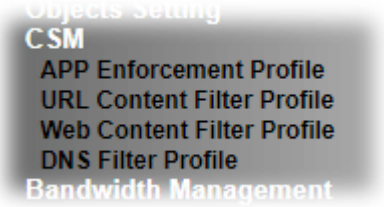
Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

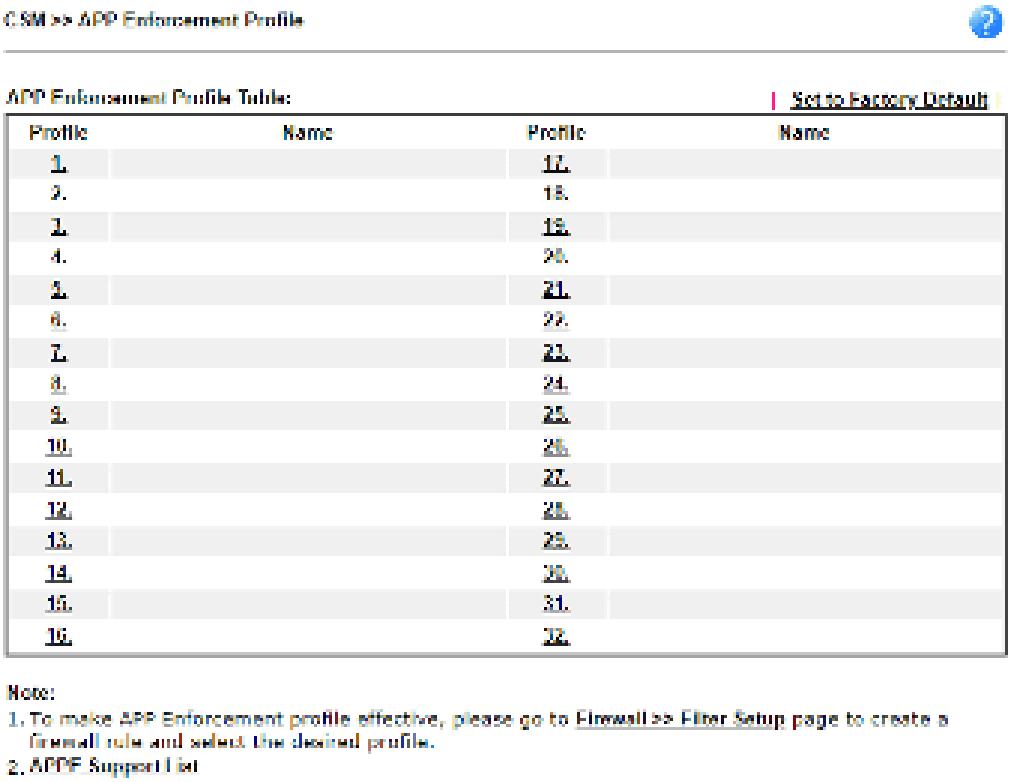
Info	The priority of URL Content Filter is higher than Web Content Filter.

Web User Interface



V-2-1 APP Enforcement Profile

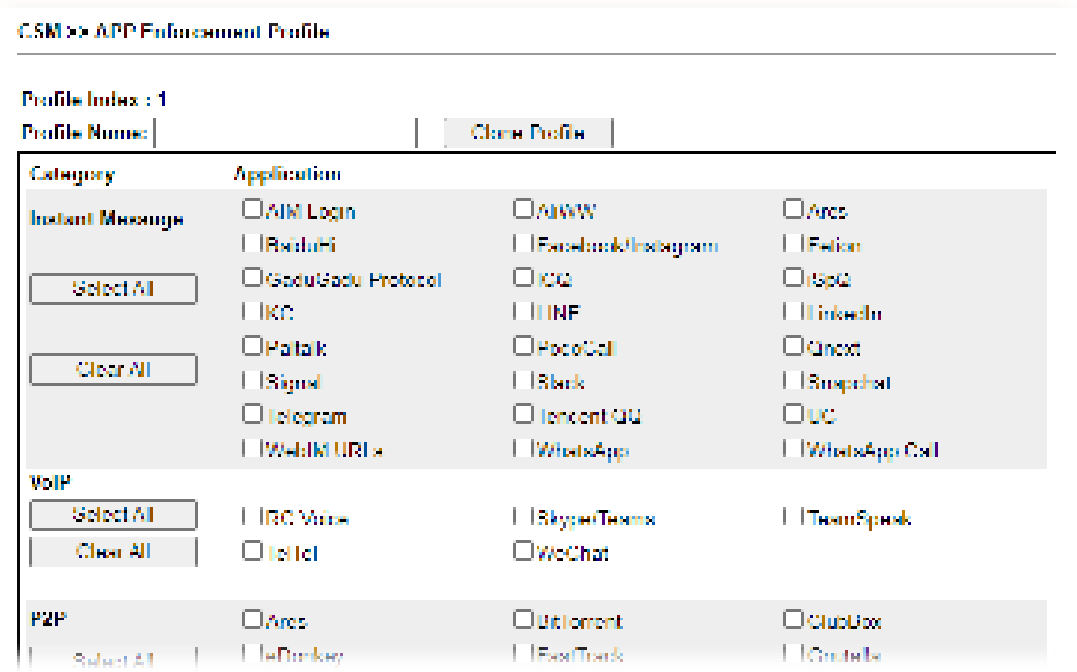
You can define policy profiles for IM (Instant Messenger)/ P2P (Peer to Peer)/ Protocol/ Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.



Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Enable	Check the box to select the APP to be blocked by Vigor router.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

V-2-2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

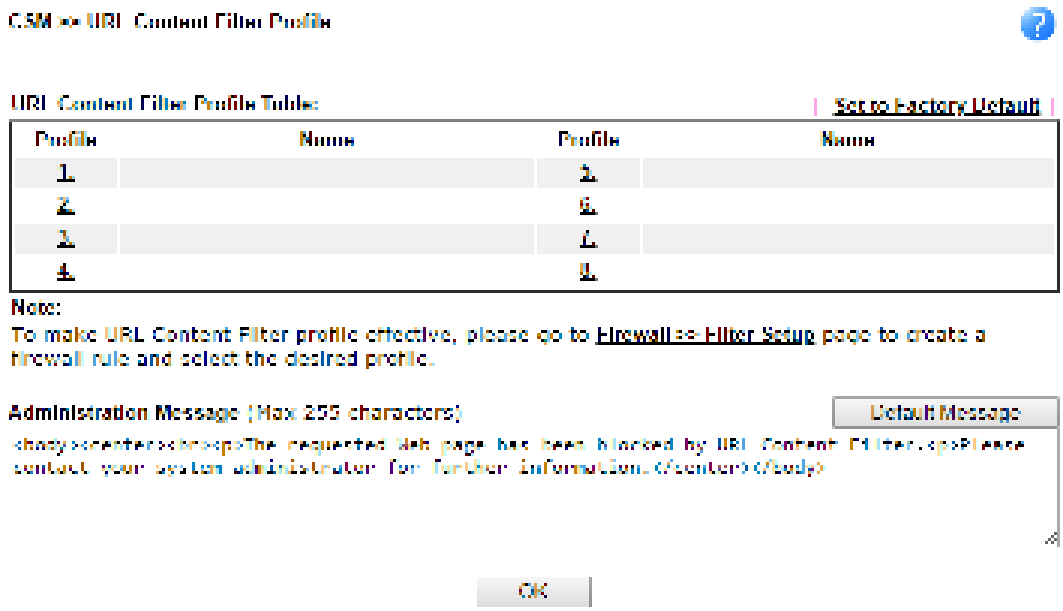
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click **CSM** and click **URL Content Filter Profile** to open the profile setting page.

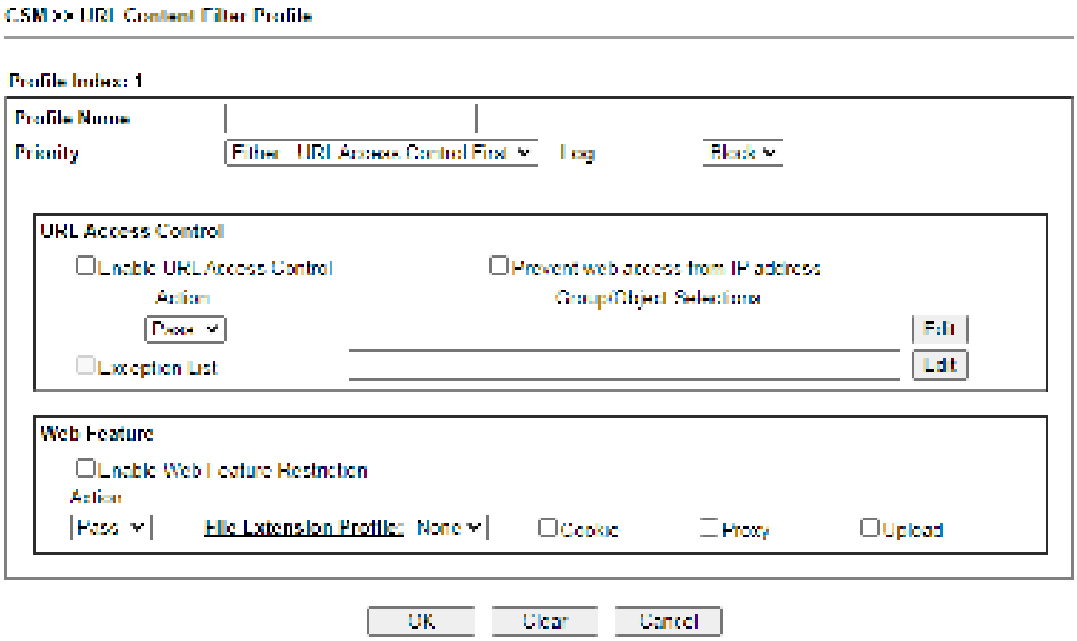


Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.

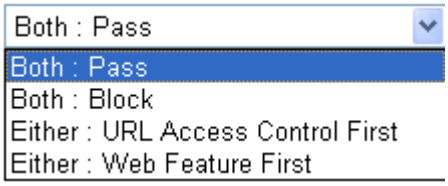
Administration Message	You can Enter the message manually for your necessity. **Default Message** - You can Enter the message manually for your necessity or click this button to get the default message which will be displayed on the field of **Administration Message**.

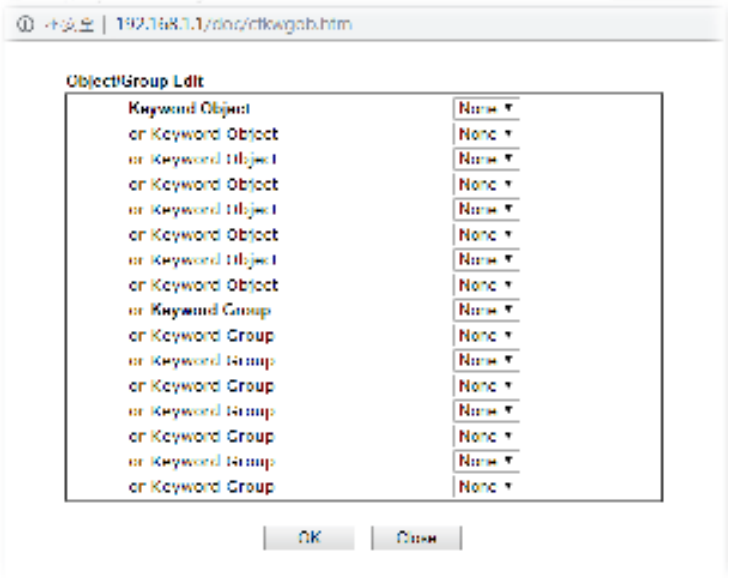
You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	It determines the action that this router will apply. **Both: Pass** – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Both:Block** –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. **Either: URL Access Control First** – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second. **Either: Web Feature First** –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

	
Log	**Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog.
URL Access Control	**Enable URL Access Control** - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature. **Prevent web access from IP address** - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before. **Action** – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ● ***Pass*** - Allow accessing into the corresponding webpage with the keywords listed on the box below. ● ***Block*** **-** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. **Exception List** – Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above. **Group/Object Selections** – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.

	
Web Feature	**Enable Web Feature Restriction -** Check this box to make the keyword being blocked or passed. **Action -** This setting is available only when **Either: URL Access Control First** or **Either: Web Feature First** is selected. ● ***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below. ● ***Block* -** Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. **File Extension Profile –** Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading. **Cookie** - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. **Proxy** - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. **Upload** – Check the box to block the file upload by way of web page.

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

V-2-3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

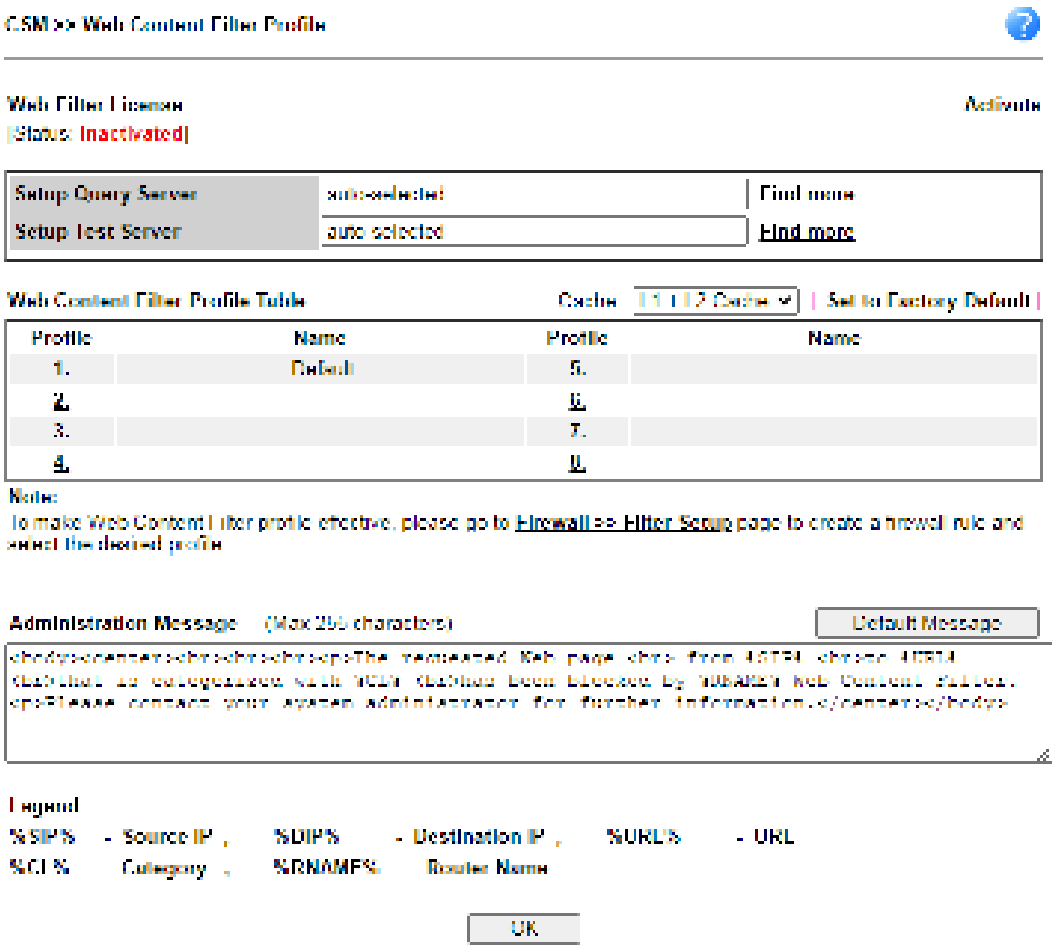
Service Activation Wizard allows you to use trial version of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (***MyVigor***) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server / Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

Info 1	Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
Info 2	Commtouch is merged by Cyren, and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

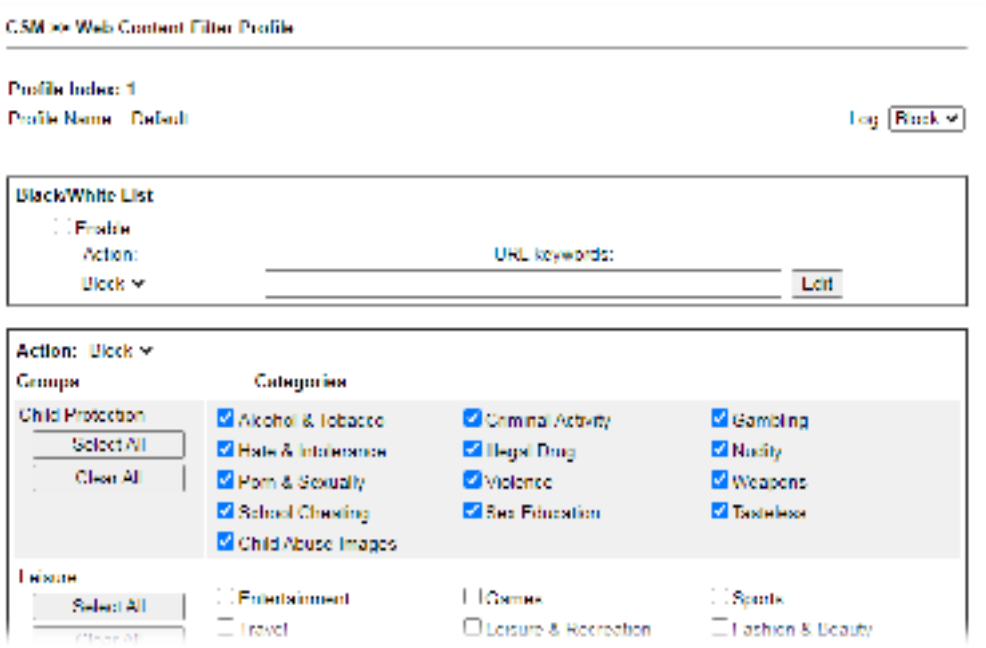


Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Cache	**None** –the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching. **L1** –the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate. **L2** –the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will

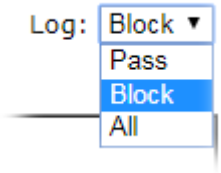
	check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate. **L1+L2 Cache** – the router will check the URL with fast processing rate combining the feature of L1 and L2.
Set to Factory Default	Click this link to retrieve the factory settings.
Administration Message	You can Enter the message manually for your necessity or click **Default Message** button to get the default text displayed on the field of **Administration Message**.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.



Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	**Enable** – Activate white/black list function for such profile. **Pass** - **allow** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **Block** - **restrict** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **URL Keywords** – Click **Edit** to choose the group or object profile as the content of white/black list.

Action	**Pass** - allow accessing into the corresponding webpage with the categories listed on the box below. **Block** - restrict accessing into the corresponding webpage with the categories listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action.
Log	**Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog. 

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

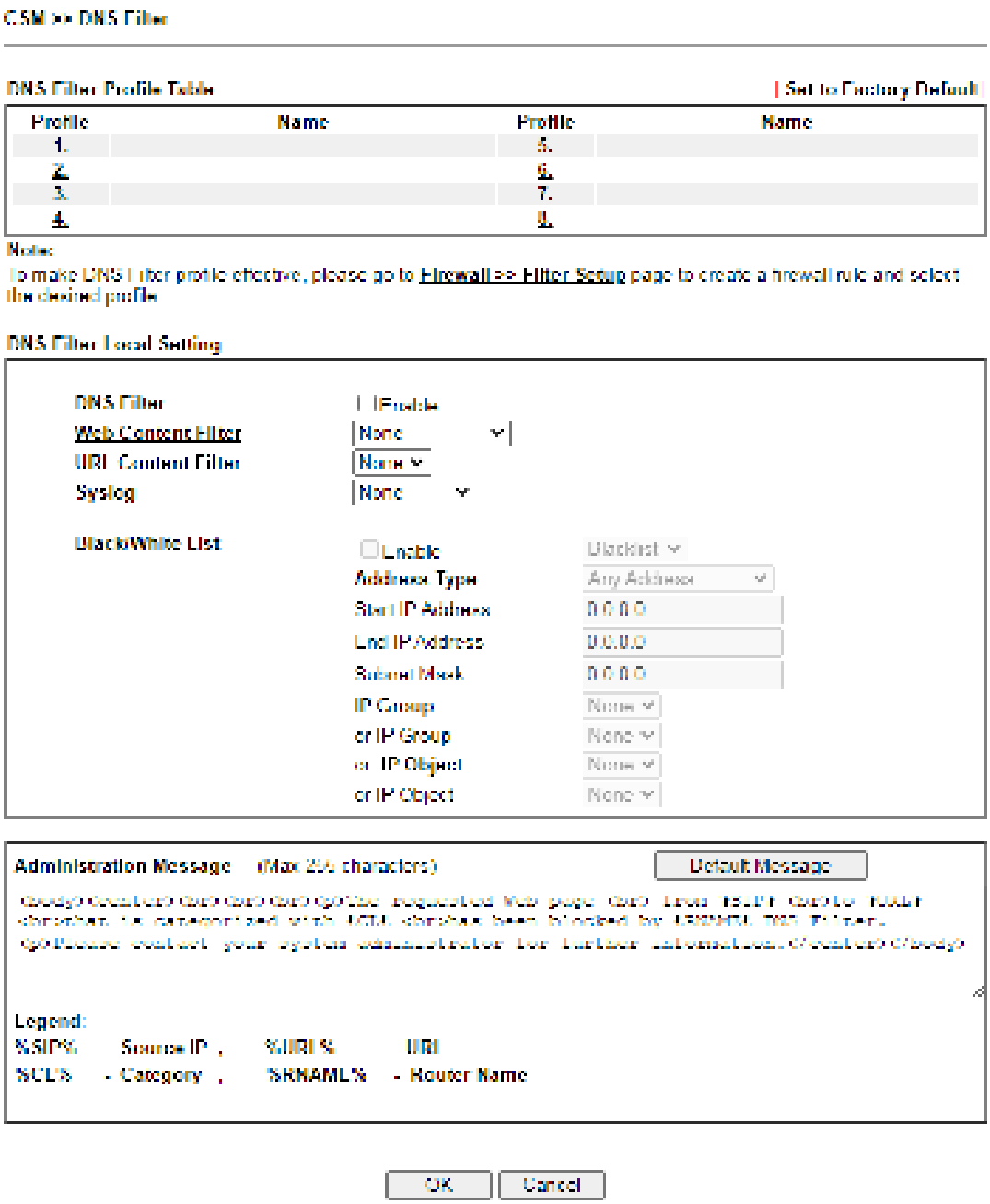
V-2-4 DNS Filter Profile

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

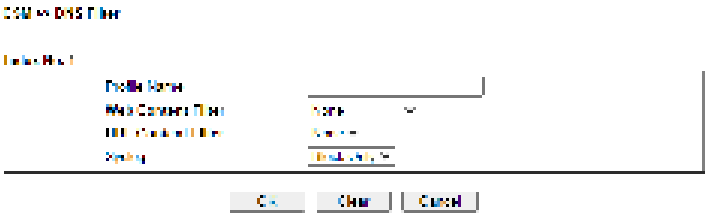
DNS can be specified in **LAN>>General Setup** by using the server (e.g., 168.95.1.1) on router or external DNS server (e.g., 8.8.8.8). If the router server is used, **DNS Filter General Setting** will be applied to DNS query from clients on LAN. However, if the external DNS server is used, **DNS Filter Profile** will be applied to DNS query coming from clients on LAN.

Info

For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.



Available settings are explained as follows:

Item	Description
DNS Filter Profile Table	It displays a list of different DNS filter profiles (with specified WCF and UCF). Click the profile link to open the following page. Then, Enter the name of the profile and specify Web Content Filter/URL Content Filter based on your requirement. 
DNS Filter Local Setting	DNS Filter Local Setting will be applied to DNS query from clients on LAN when router's DNS server is used. **DNS Filter -** Check **Enable** to enable such feature. **Web Content Filter-** Set the filtering conditions. **URL Content Filter** - Set the filtering conditions. **Syslog -** The filtering result can be recorded according to the setting selected for Syslog. ● **None** – There is no log file will be recorded for this profile. ● **Pass Only** – Only the log about Pass will be recorded in Syslog. ● **Block Only**– Only the log about Block will be recorded in Syslog. ● **Both** – All the actions (Pass and Block) 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	Enter the words or sentences which will be displayed when a web page is blocked by Vigor router. You can Enter the message manually for your necessity or click **Default Message** button to get the default text displayed on the field of **Administration Message**.

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

Application Notes

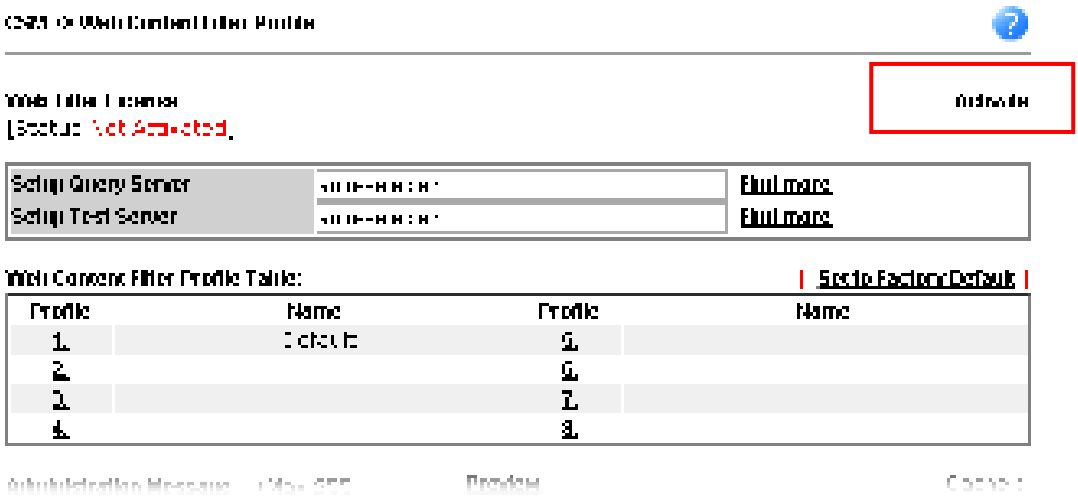
A-1 How to Create an Account for MyVigor

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.

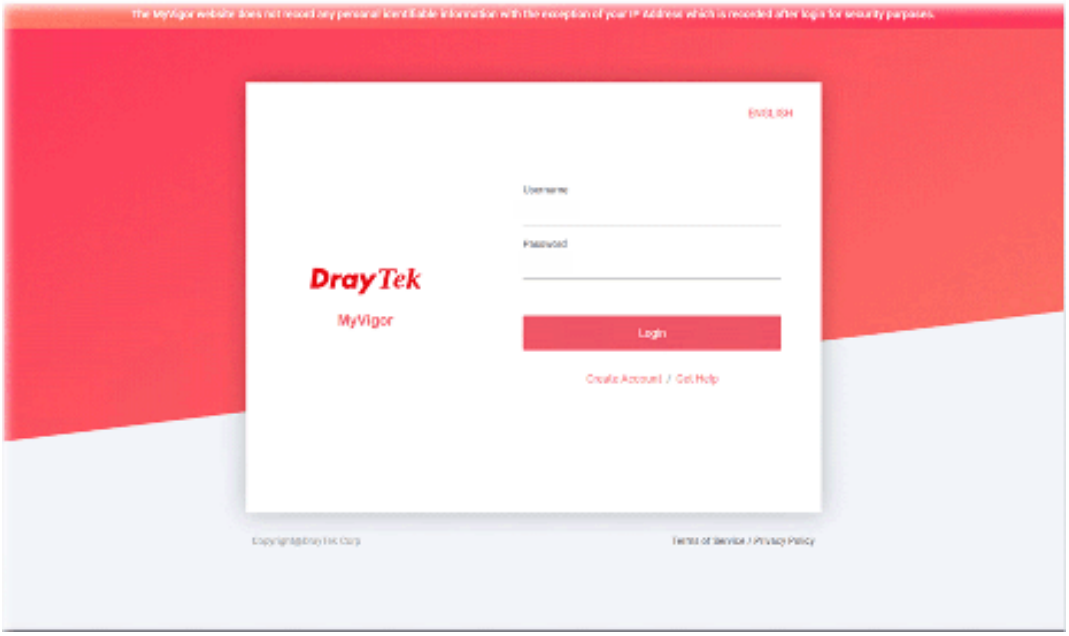
To access into MyVigor for getting more information, please create an account for MyVigor.

Create an Account via Vigor Router

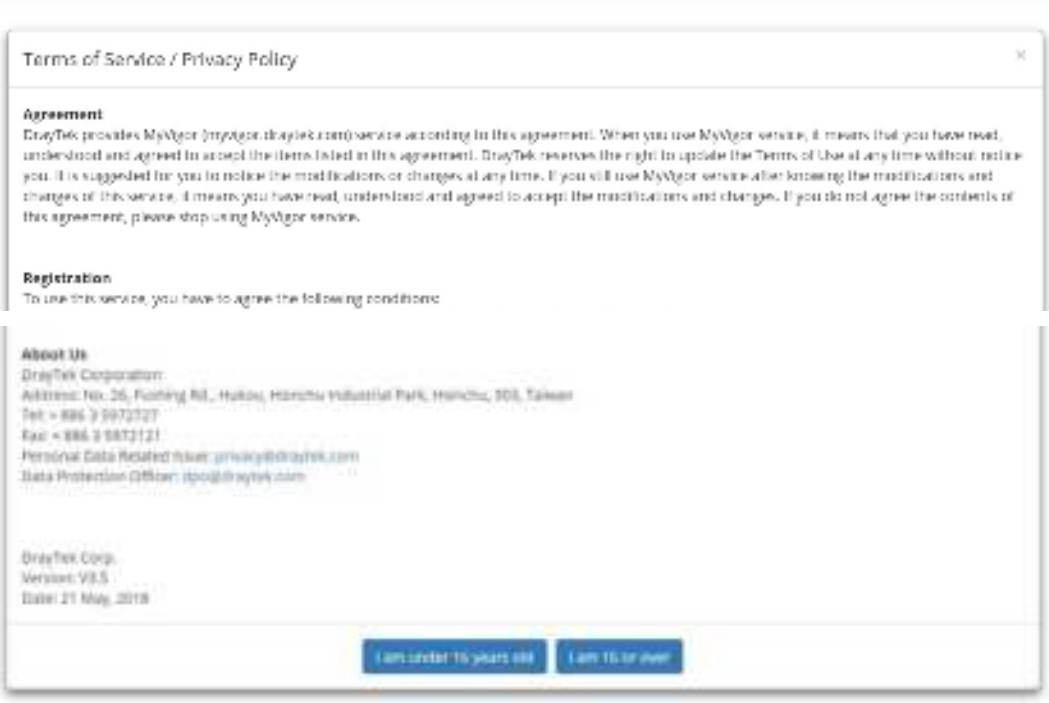
1. Click **CSM>> Web Content Filter Profile**. The following page will appear.



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



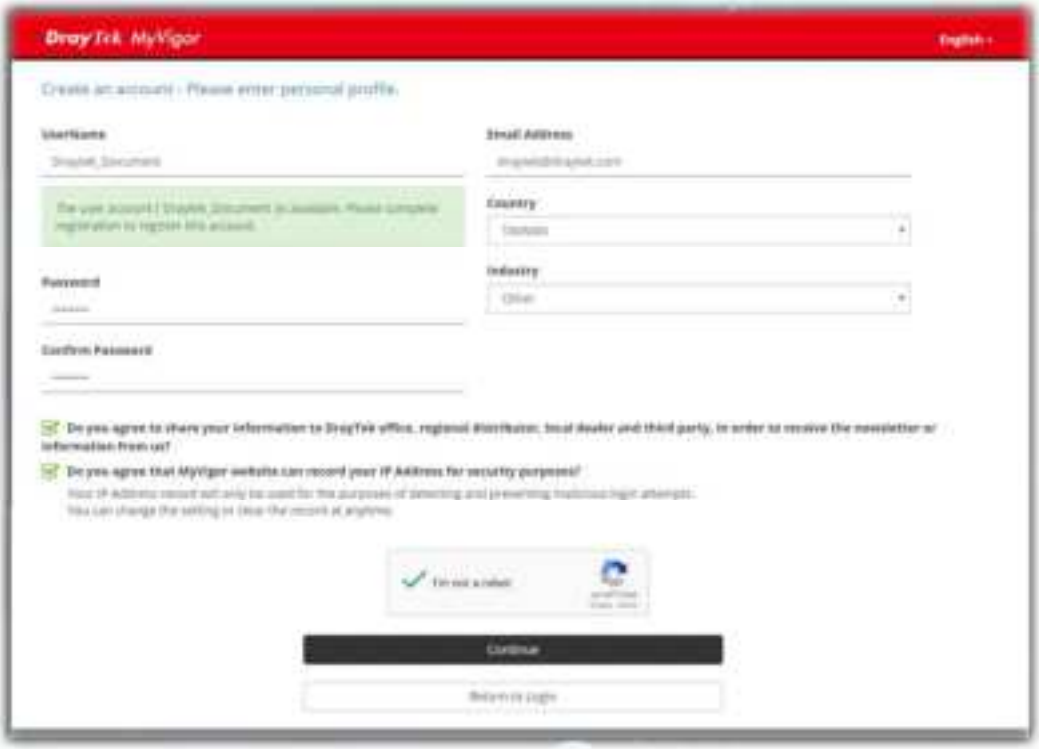
3. Click the link of **Create Account**.
4. The system will ask if you are 16 years old or over.
   - If yes, click **I am 16 or over**.



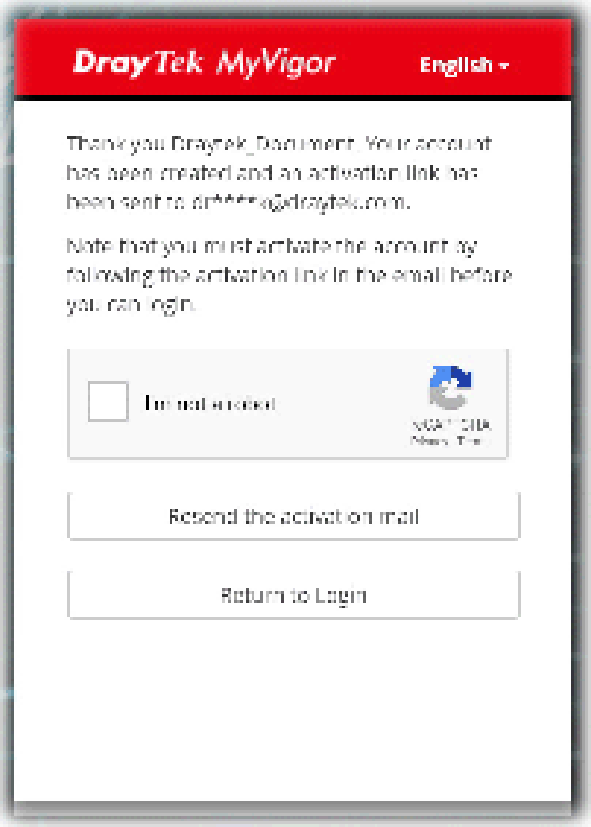
- If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.

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

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



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



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

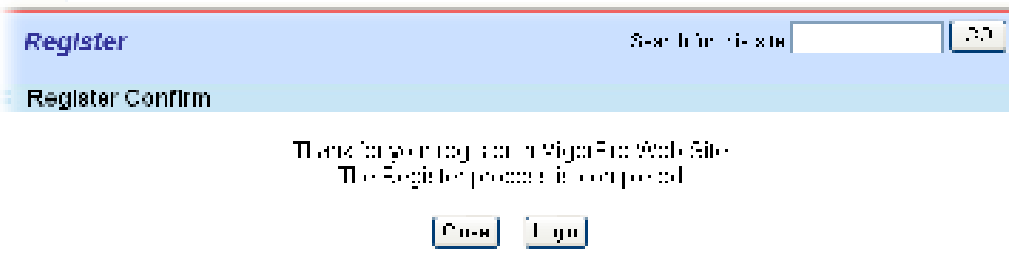
****** This is an automated message from myvigor.draytek.com.******

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

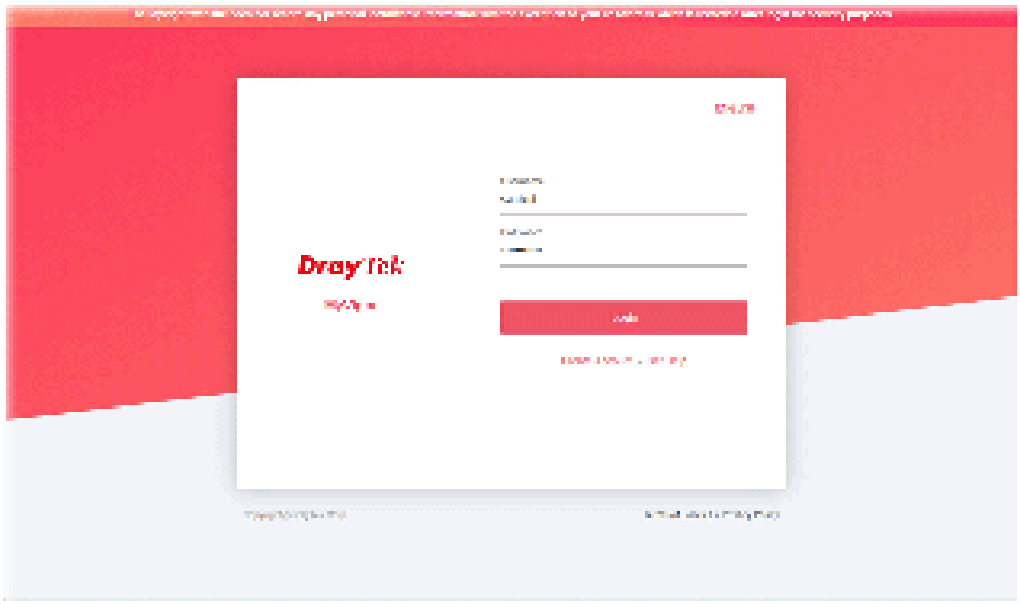
Please click on the activation link below to activate your account

Link : Activate my Account

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



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



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

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

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

Web Content Filter,

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

Note: License is required.

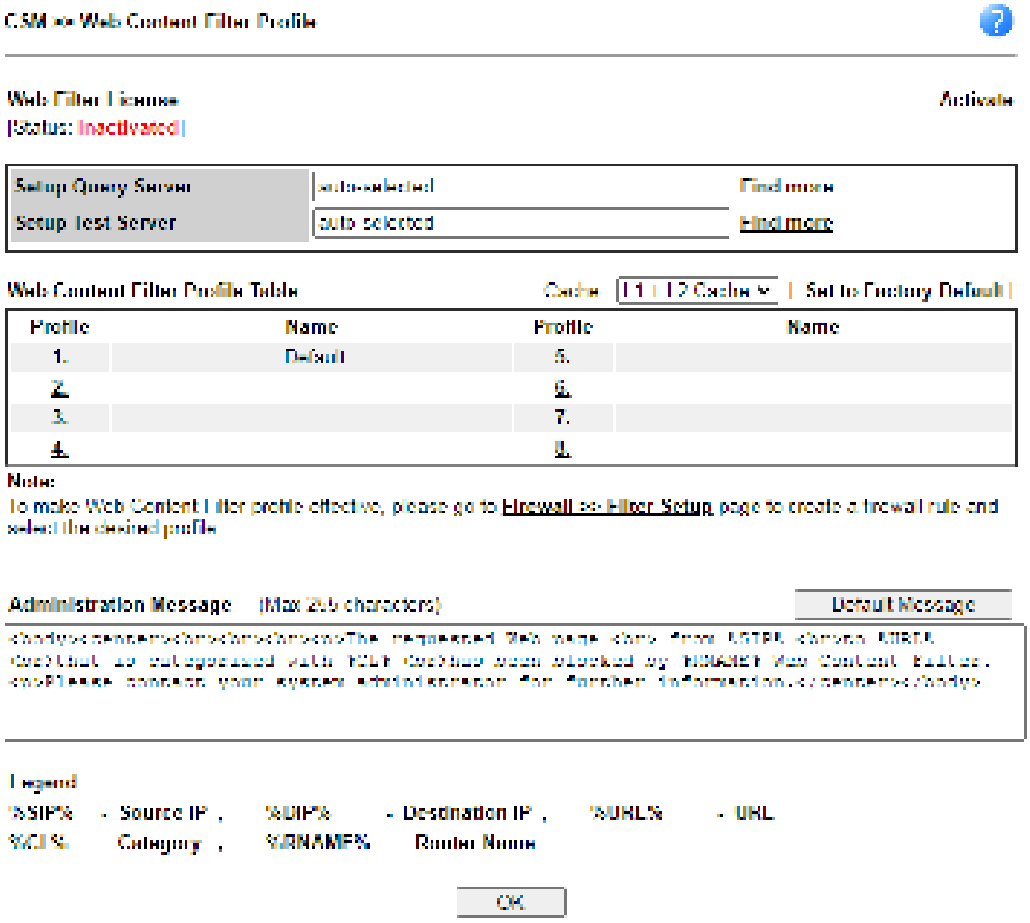
URL Content Filter,

Benefits: Free, flexible for customize webpage.

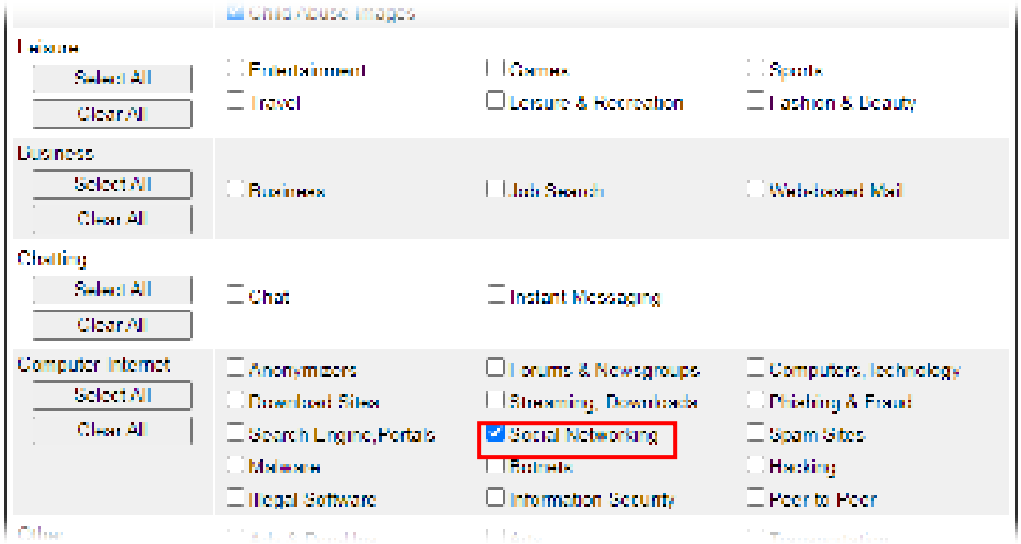
Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

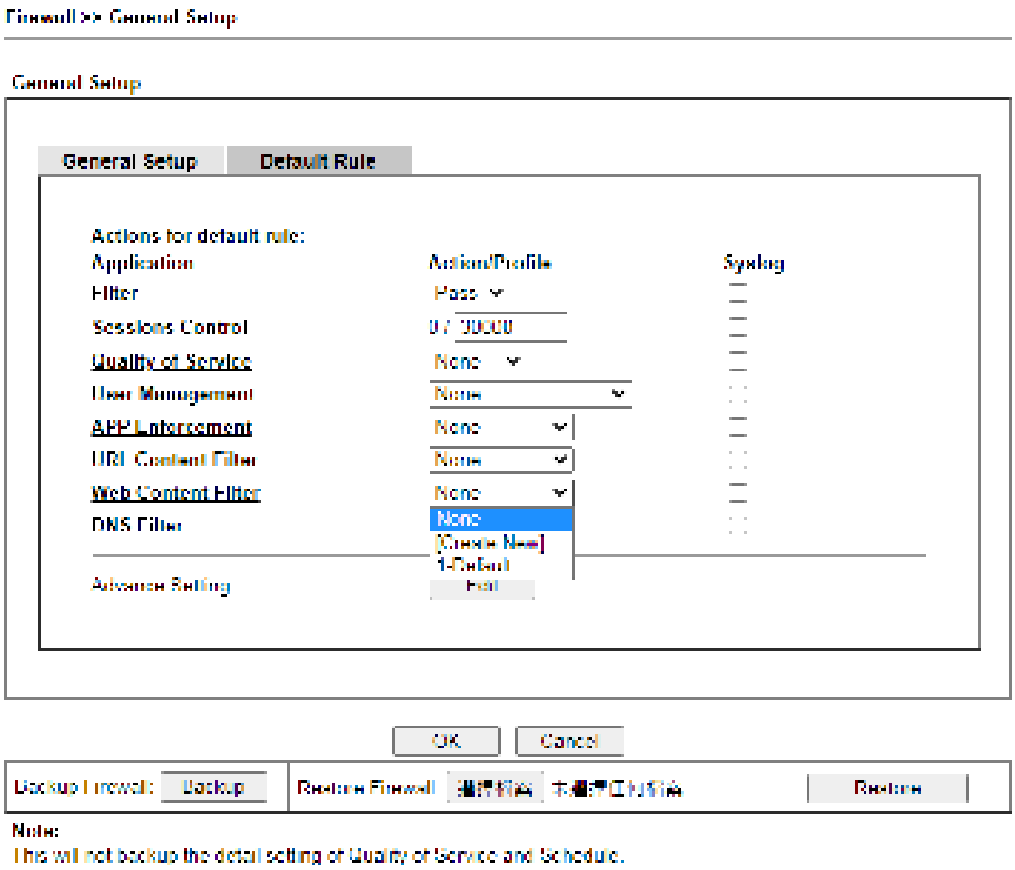
1. Make sure the Web Content Filter (powered by Commtouch) license is valid.



2. Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action**, Block**.



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

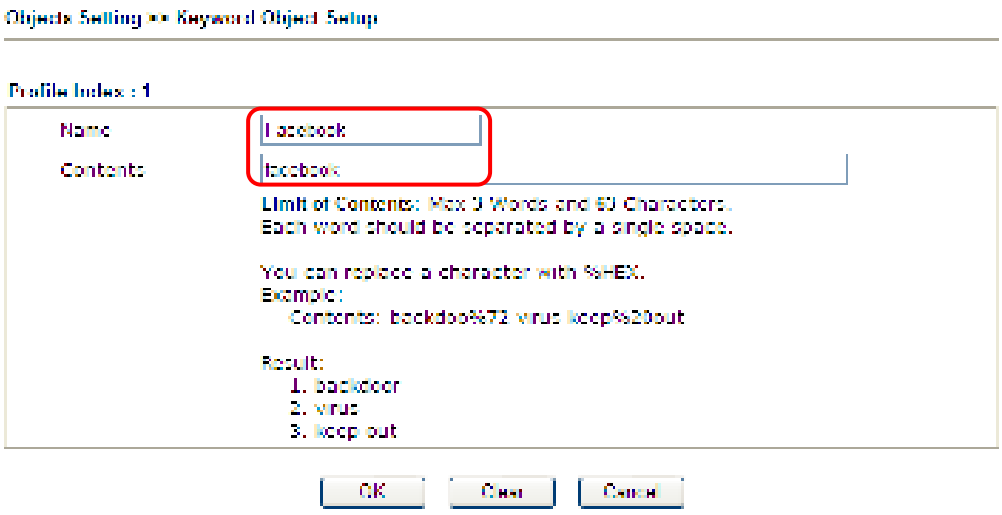


4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

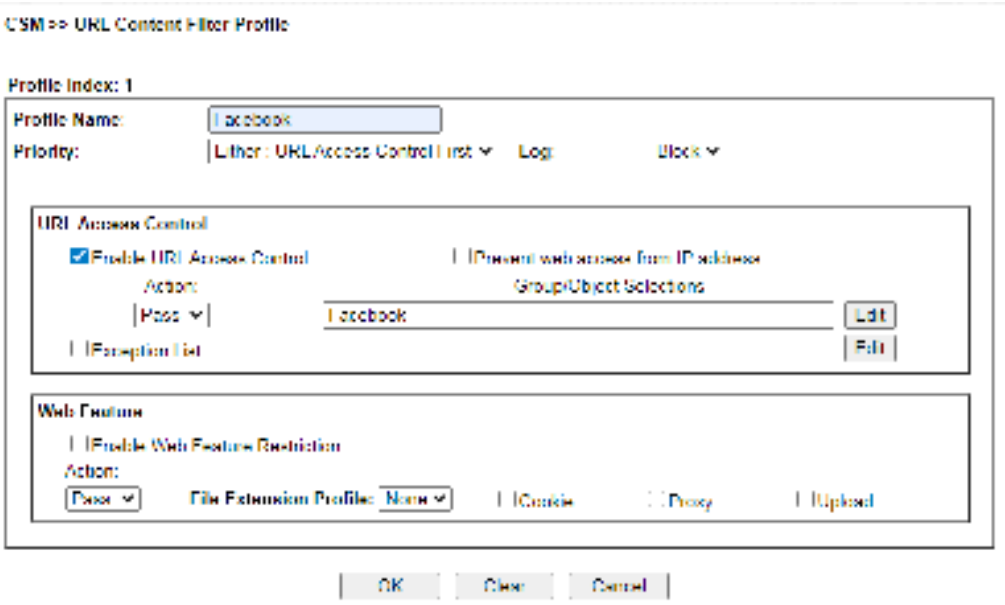
II. Via URL Content Filter

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

1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
2. In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.

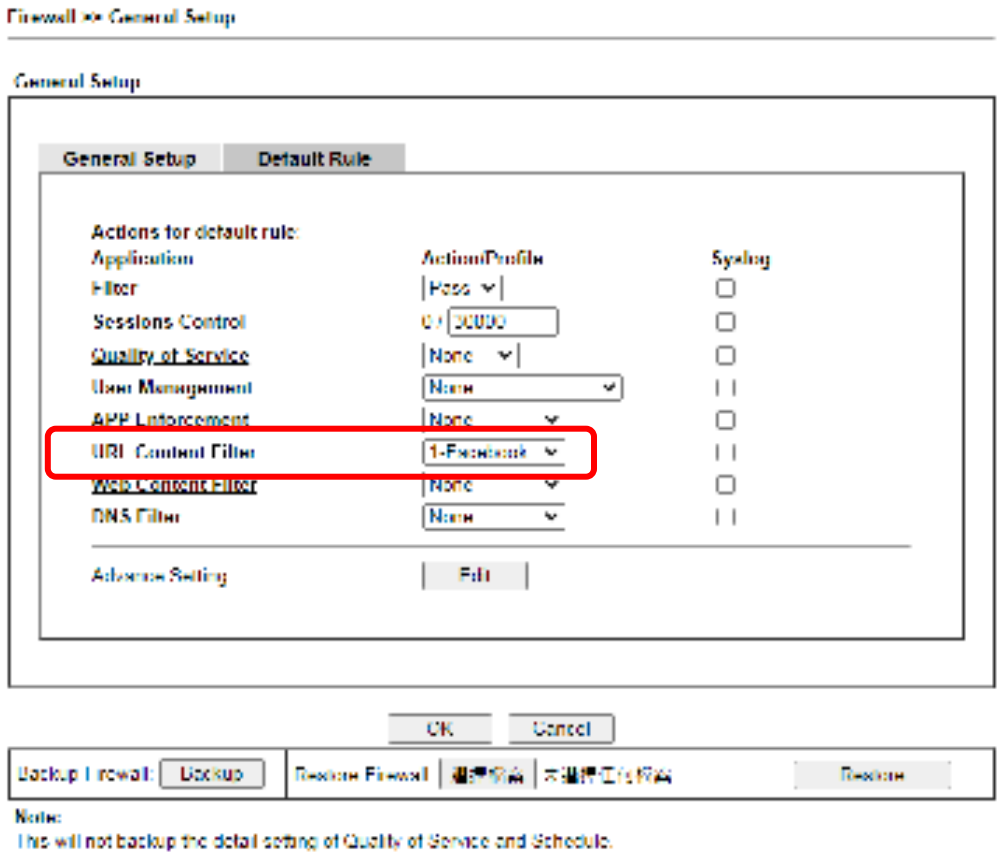


3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
4. Configure the settings as the following figure.



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

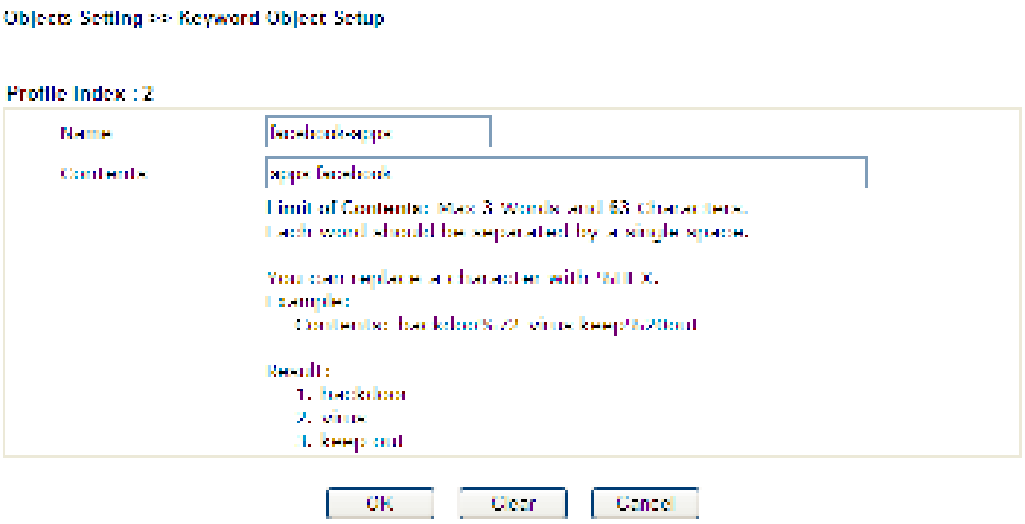
6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.



B. Disallow users to play games on Facebook

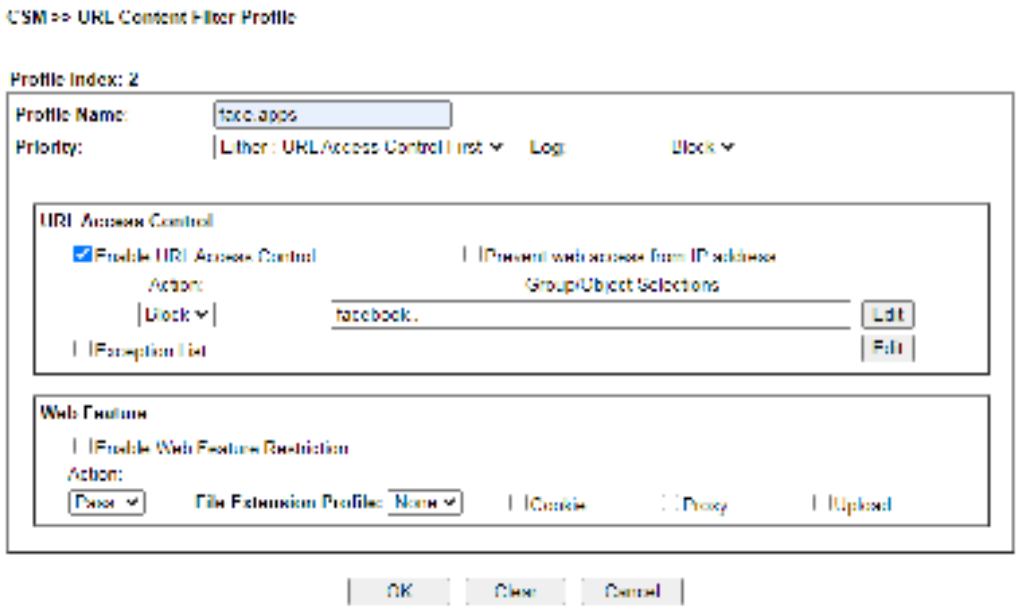
1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.

2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.



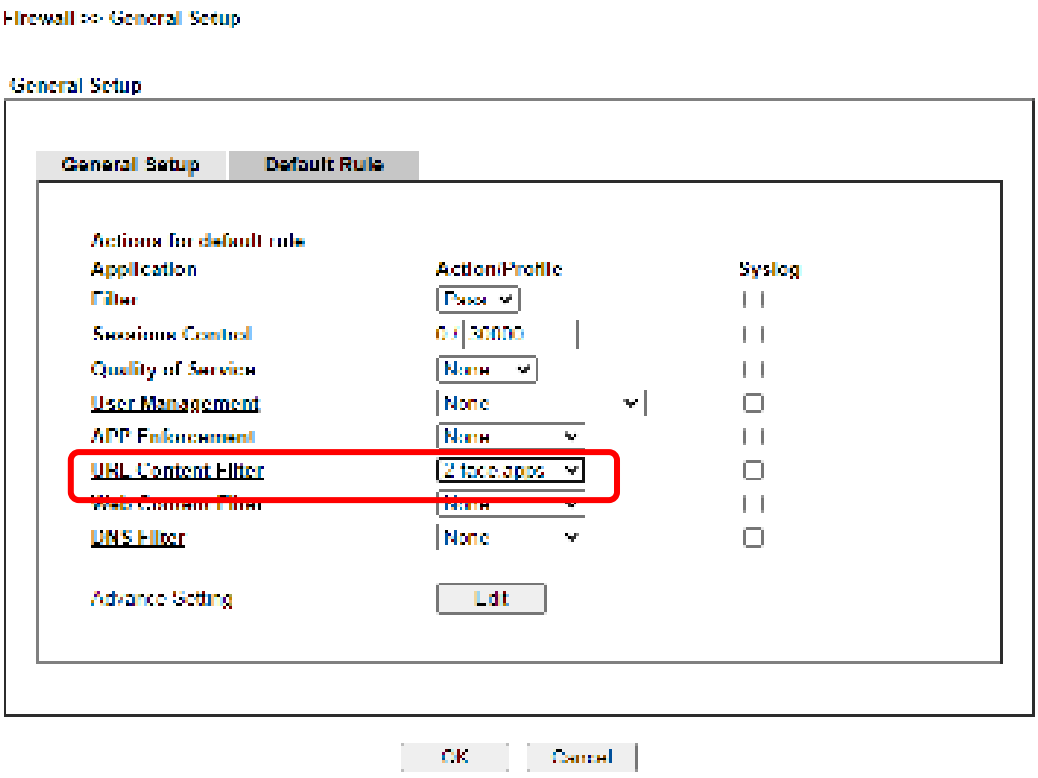
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.



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

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


Firewall >> General Setup
General Setup
General Setup
Default Rule
Actions for default rule
Application
Action/Profile
Syslog
Filter
Session Control
Quality of Service
User Management
None
APP Enforcement
URL Content Filter
Web Content Filter
DNS Filter
Advance Setting
Edit
OK
Cancel

Part VI Management

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog / Mail Alert, Time and Date, Management, Panel Control, Self-Signed Certificate, Reboot System, Firmware Upgrade, Activation and Dashboard Control.

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

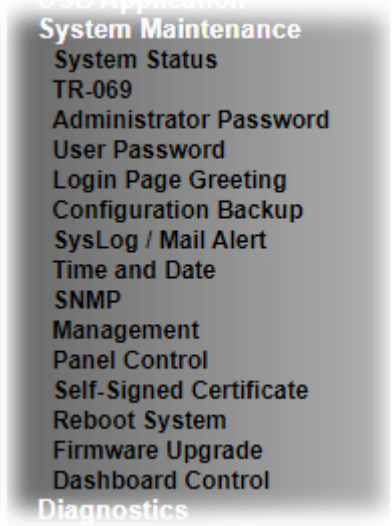
It is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password.

VI-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog / Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Dashboard Control.

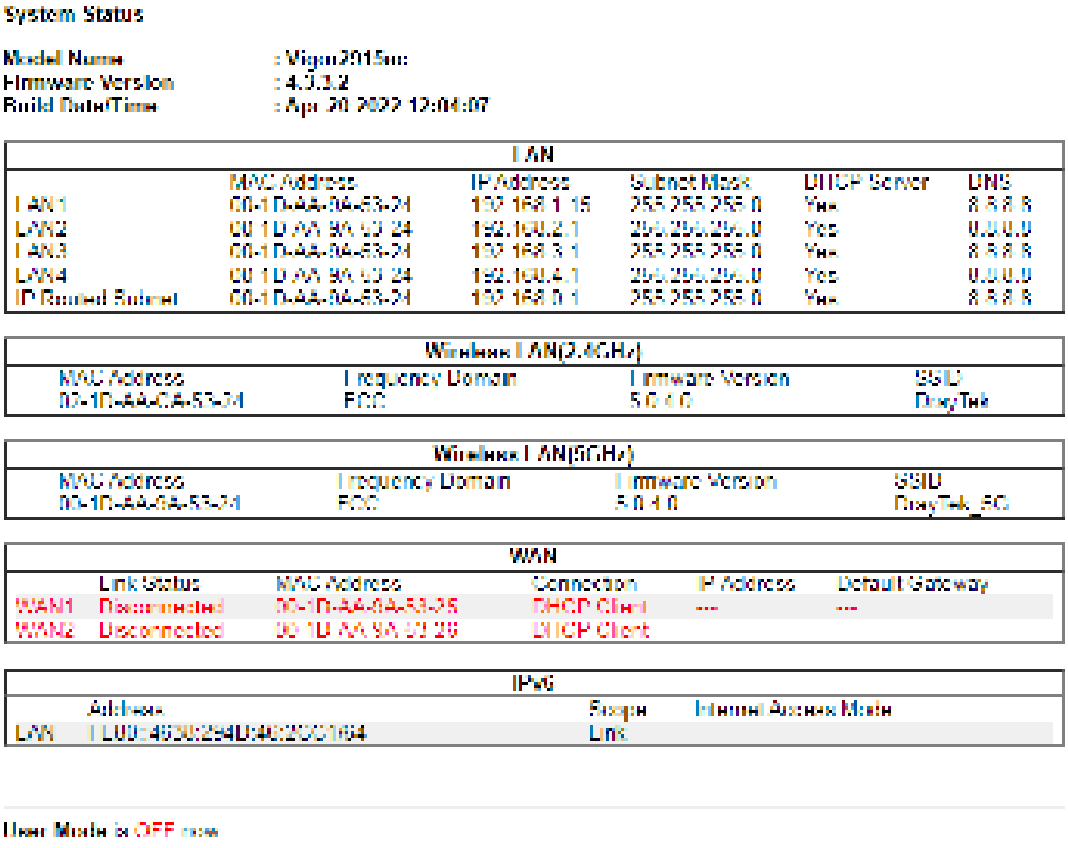
Web User Interface

Below shows the menu items for System Maintenance.



VI-1-1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.



Available settings are explained as follows:

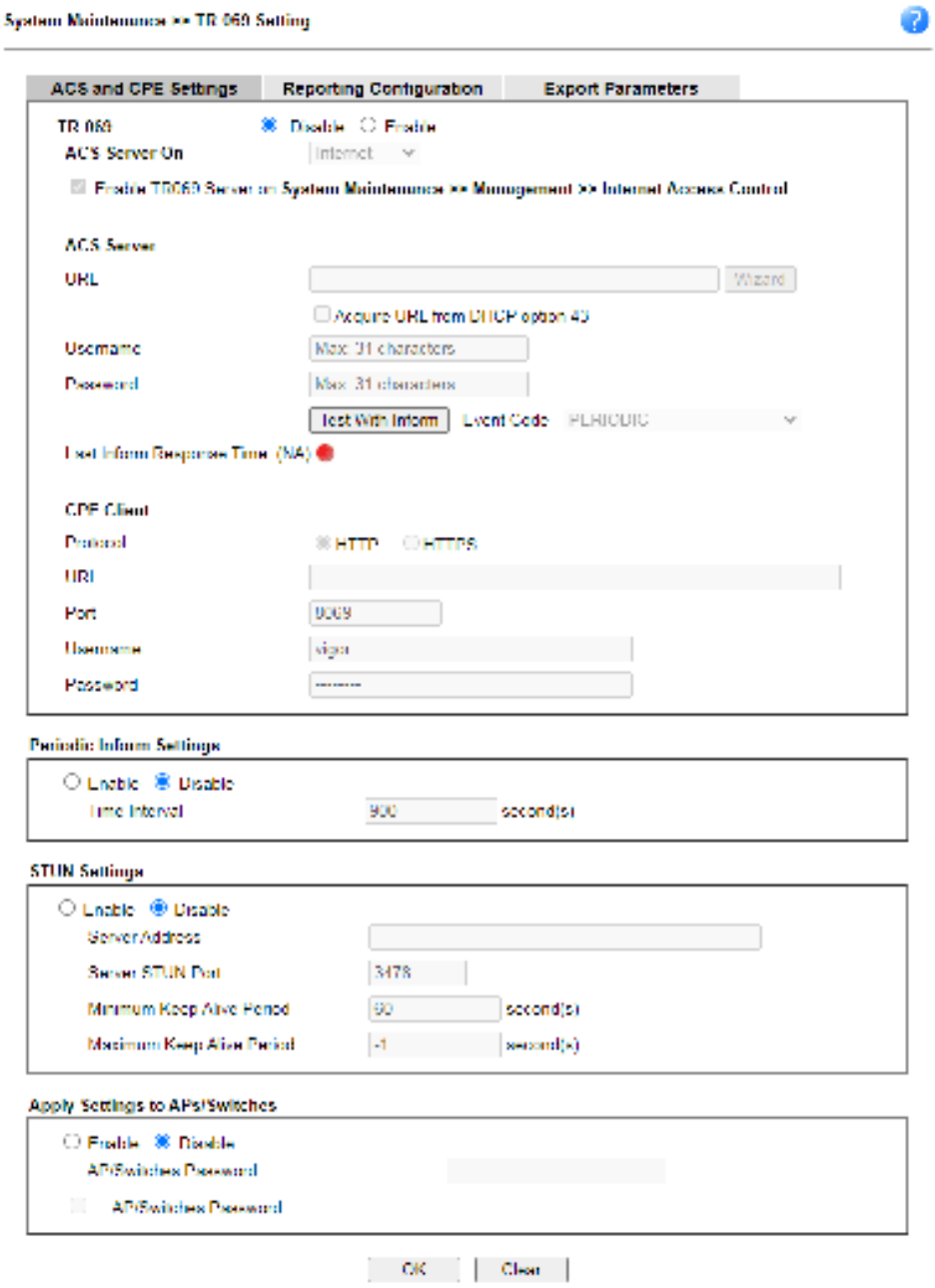
Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	**MAC Address** - Display the MAC address of the LAN Interface. **IP Address** - Display the IP address of the LAN interface. **Subnet Mask** - Display the subnet mask address of the LAN interface. **DHCP Server** - Display the current status of DHCP server of the LAN interface **DNS** - Display the assigned IP address of the primary DNS.
WAN	**Link Status** - Display current connection status.

	MAC Address **-** Display the MAC address of the WAN Interface. **Connection** **-** Display the connection type. **IP Address** **-** Display the IP address of the WAN interface. **Default Gateway** **-** Display the assigned IP address of the default gateway.
IPv6	**Address -** Display the IPv6 address for LAN. **Scope -** Display the scope of IPv6 address. For example, IPv6 **Link Local** could only be used for direct IPv6 link. It can't be used for IPv6 internet. **Internet Access Mode –** Display the connection mode chosen for accessing into Internet.

VI-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

VI-1-2-1 ACS and CPE Settings



Available settings are explained as follows:

Item	Description
TR-069	Click **Enable** to activate the settings on this page. **ACS Server On -** Choose the interface for the router connecting to ACS server. **Enable TR069 Server on....-** If enabld, a user will be

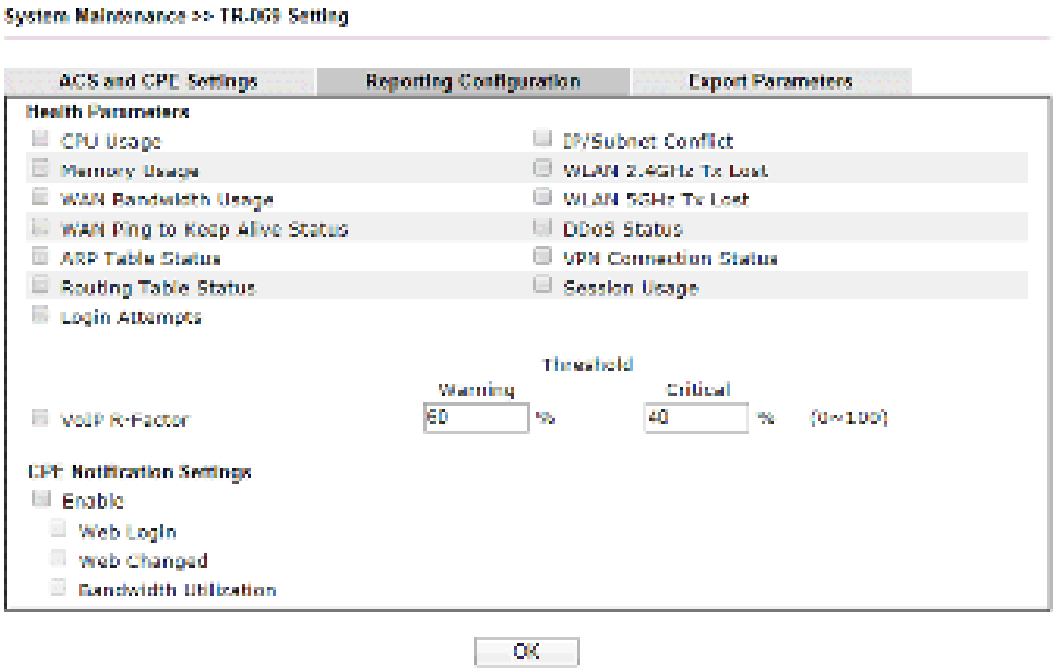
	allowed to access into TR-069 from WAN. If the TR-069 Server not enabled, VigorACS can not manage the Vigor rotuer remotely.
ACS Server	**URL** – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. ● **Wizard** – Click it to enter the IP address of VigorACS server, port number and the handler. ● **Acquire URL form DHCP option 43** – Check the box to get the URL from DHCP option 43. **Username**/**Password** – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. ● **Test With Inform** – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server. ● **Event Code** – Use the drop down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Client	Such information is useful for Auto Configuration Server. **Protocol** - Select Https if the connection is encrypted; otherwise select Http. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username** and **Password** – Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	**Enable** – It is the default setting. ● **Time Interval** - Please set interval time or schedule time for the router to send notification to CPE. **Disable** - Click it to close the mechanism of notification.
STUN Settings	**Disable** - The default is **Disable**. **Enable** - Please Enter the relational settings listed below: ● **Server Address** – Enter the IP address of the STUN server. ● **Server Port** – Enter the port number of the STUN server. ● **Minimum Keep Alive Period** – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". ● **Maximum Keep Alive Period** – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply Settings to APs/Switches	This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2862 at the same time. **Disable** – Related settings will not be applied to VigorAP. **Enable** – Above STUN settings will be applied to VigorAP after clicking **OK**. If such feature is enabled, you have to Enter the password for accessing VigorAP.

	AP/Switches Password – Enter the password of the VigorAP that you want to apply Vigor2915's TR-069 settings.

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

VI-1-2-2 Reporting Configuration

Information related to the router's health are divided into several categories and listed in this field. After checking the item(s), Vigor router will arrange and send corresponding data to VigorACS as a reference for the system administrator.



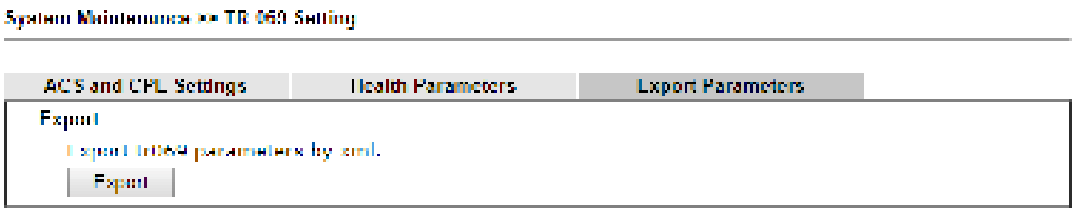
Available settings are explained as follows:

Item	Description
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.

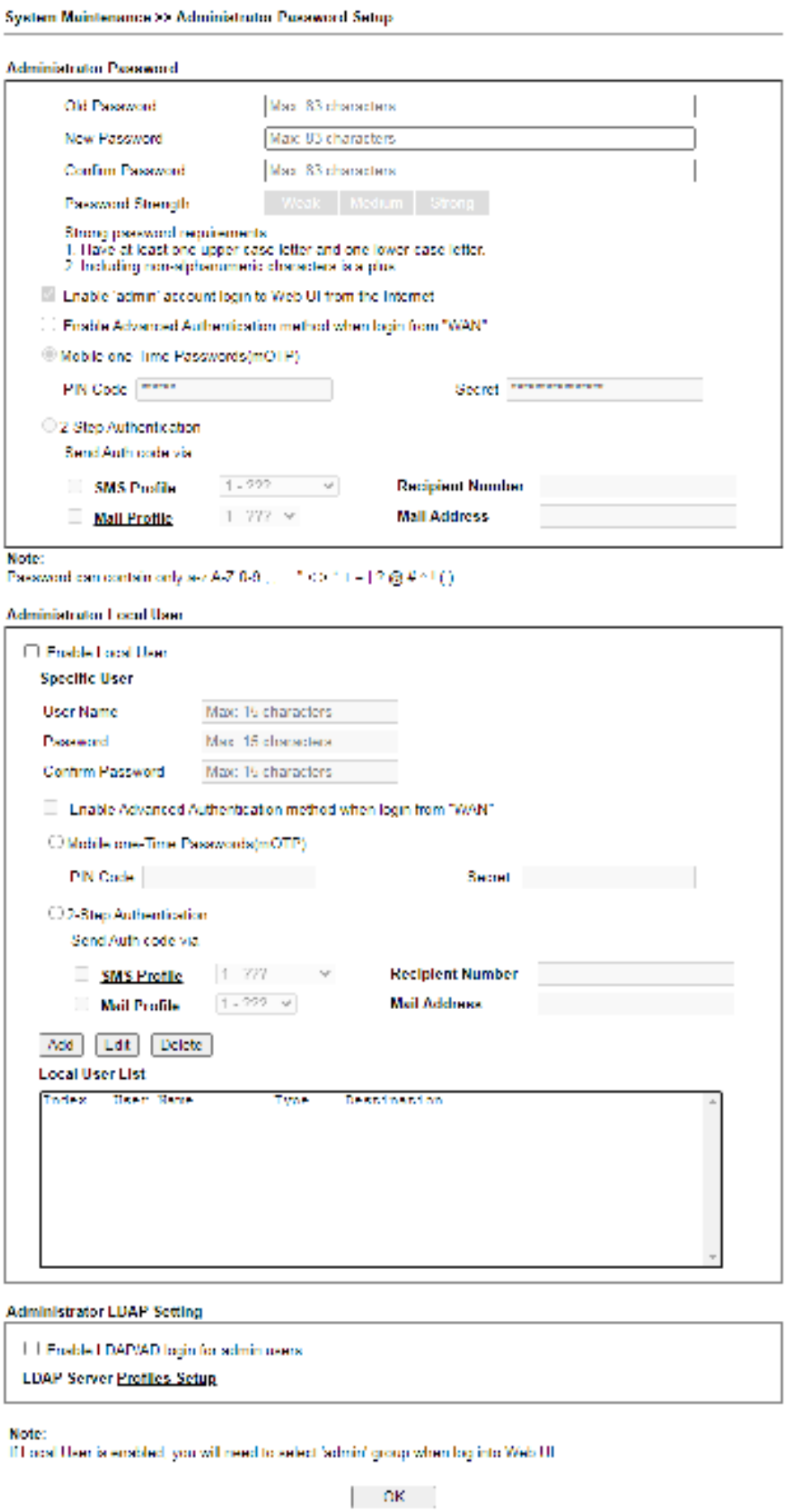
VI-1-2-3 Export Parameters

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



VI-1-3 Administrator Password

This page allows you to set new password.


System Maintenance >> Administrator Password Setup
Administrator Password
Old Password
New Password
Confirm Password
Password Strength
Weak
Medium
Strong
Enable 'admin' account login to Web UI from the Internet
Mobile one-time Passwords(mOTP)
PIN Code
Secret
2-Step Authentication
SMS Profile
Recipient Number
Mail Profile
Mail Address
Note:
Administrator Local User
Enable Local User
Specific User
User Name
Password
Confirm Password
Enable Advanced Authentication method when login from "WAN"
Mobile one-Time Passwords(mOTP)
PIN Code
Secret
2-Step Authentication
Send Auth code via
SMS Profile
Recipient Number
Mail Profile
Mail Address
Add
Edit
Delete
Local User List
Index
User Name
Type
Description
Administrator LDAP Setting
Enable LDAP/AD login for admin users
LDAP Server Profiles Setup
Note:
OK

Available settings are explained as follows:

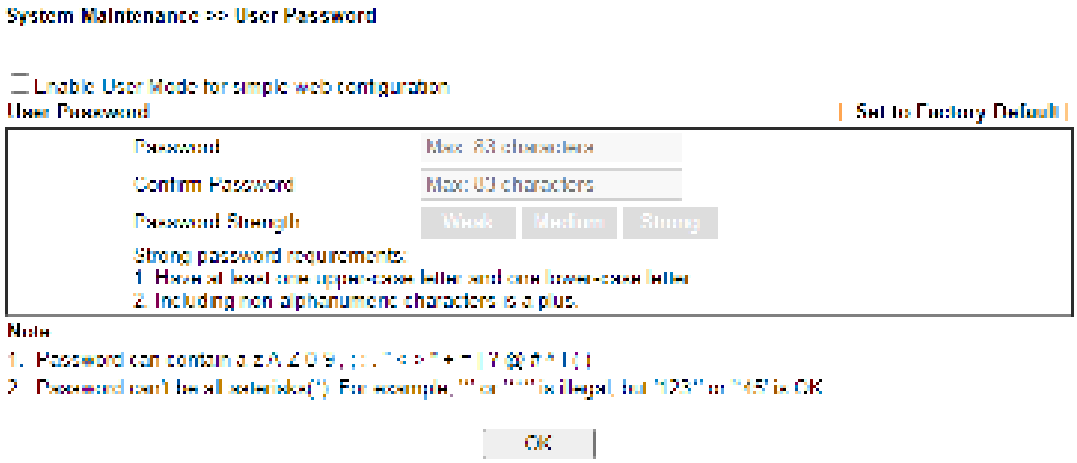
Item	Description
Administrator Password	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. **Old Password** - Type in the old password. The factory default setting for password is **"admin"**. **New Password** – Define the basic password. The length of the password is limited to 23 characters. **Confirm Password** – Enter the basic 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** – It is configurable only when Administrator Local User is enabled. The default setting is enabled. It can ensure that any user is able to successfully accesses into web user interface of Vigor router through **Internet** by username/password of "admin/admin". However, if you want to prevent the admin account from password attacks by hackers, disable this function and let local user account access into the WUI instead. **Enable Advanced Authentication method when login from "WAN"** – Advanced authentication method can offer a **more secure** network connection. In general, the above basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings. • **Mobile one-Time Password (mOTP)** – Click it to use mOTP as the advanced authentication method. Enter the PIN code and secret settings for one-time usage. • **2-Step Auth code via SMS Profile and/or Mail Profile** – Click it to use authentication code as the advanced authentication method. The authentication code will be sent out based on the selected SMS profile and Mail profile.
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 is used to **define other users in LAN** who can access into the web user interface with the same privilege 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. **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. **Mobile one-Time Password (mOTP)** – Click it to use mOTP as the advanced authentication method. Enter the PIN code and secret settings for one-time usage. **2-Step Authentication via SMS Profile and/or Mail Profile** – Click it to use authentication code as the advanced authentication method. The authentication code will be sent out based on the selected SMS profile and Mail profile. ● **Add** – After typing the user name and password above, simply click it to create a new local user. The new one will be shown on the Local User List immediately. ● **Edit** – If the username listed on the box above is not satisfied, simply click the username and modify it on the field of User Name. Later, click **Edit** to update the information. ● **Delete** – If the local user listed on the box above is not satisfied, simply click the username and click **Delete** 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** – If it is enabled, any user can access into the web user interface of Vigor router through the LDAP server authentication. Available profiles will be displayed here under the link of LDAP Profile Setup. To create a new profile, simply click the link of **LDAP Profiles Setup**.

After finishing all the settings here, please click **OK** to save the configuration. After logging out the webuser interface, please use the new password to access into the web user interface again.

VI-1-4 User Password

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



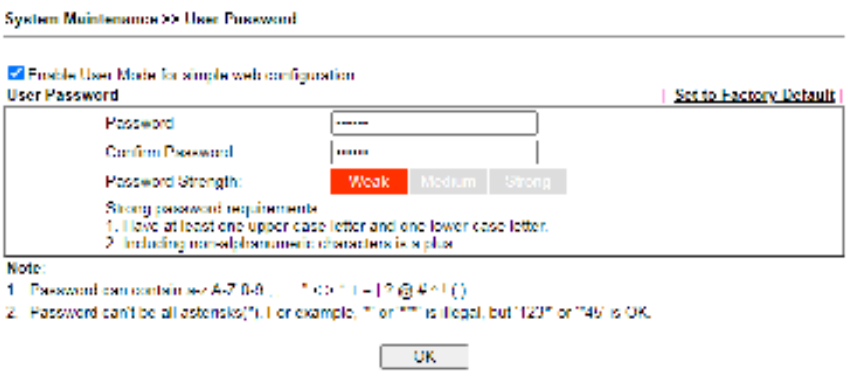
Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.
Password Strength	Display the security strength of the password specified above.
Set to Factory Default	Click to return to the factory default setting.

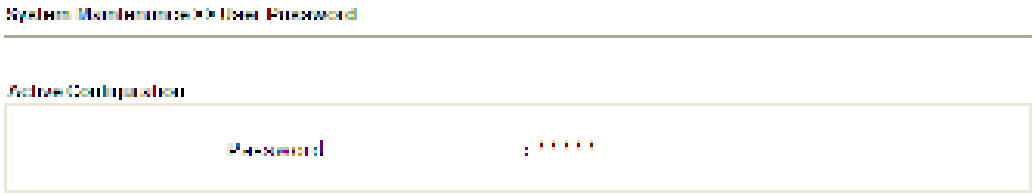
When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again. Below shows an example for accessing into User Operation with User Password.

1. Open **System Maintenance>>User Password**.

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



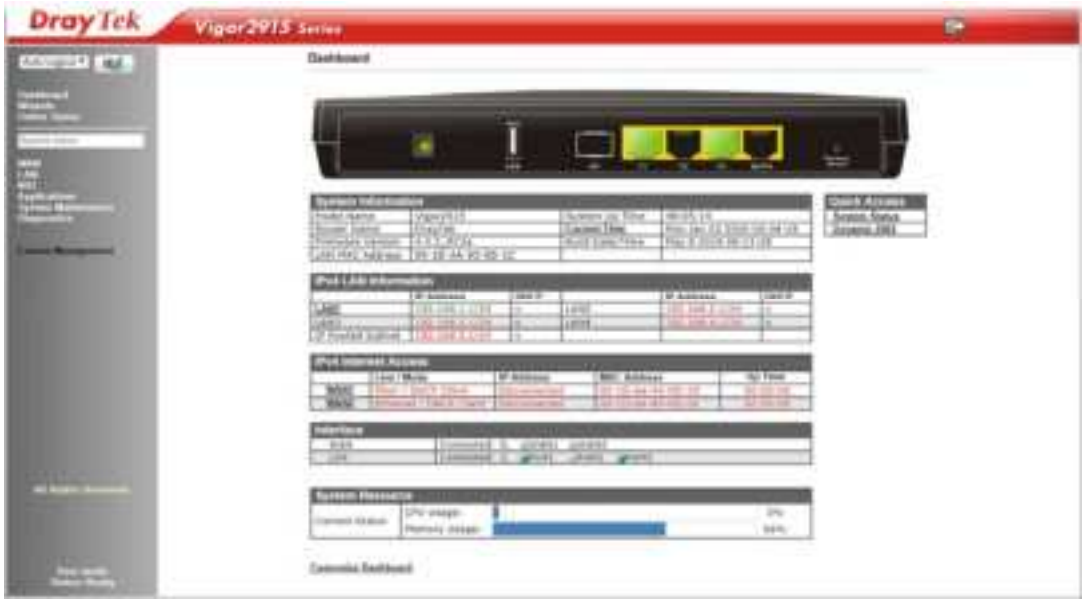
3. The following screen will appear. Simply click **OK**.



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

5. The following window will be open to ask for username and password. Enter the new user password in the filed of **Password** and click **Login**.

6. The main screen with User Mode will be shown as follows.

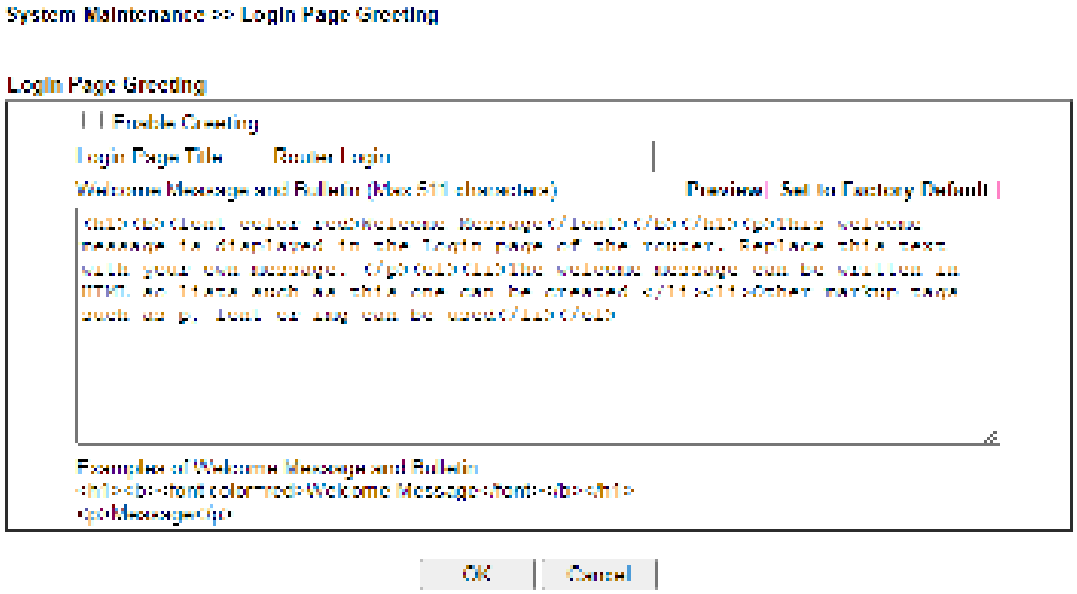


Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

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

VI-1-5 Login Page Greeting

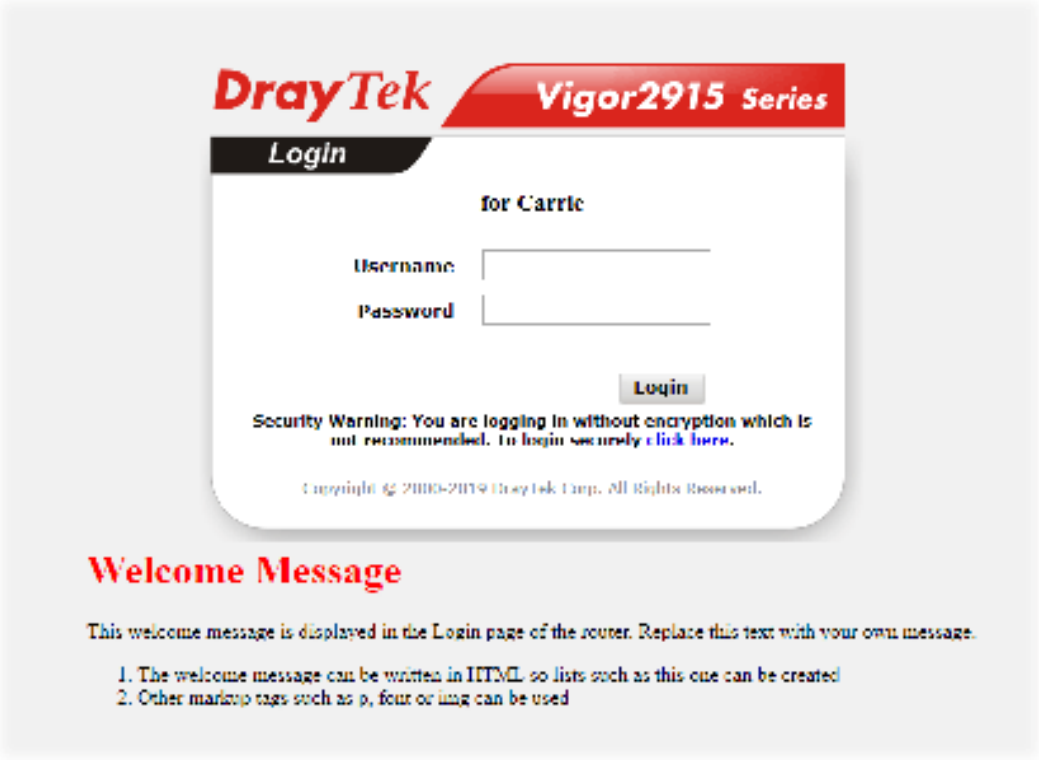
When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.



Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type 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 type URL redirect link here.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.


DrayTek
Vigor2915 Series
Login
for Carrie
Username
Password
Login
Security Warning: You are logging in without encryption which is
not recommended. To login securely click here.
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

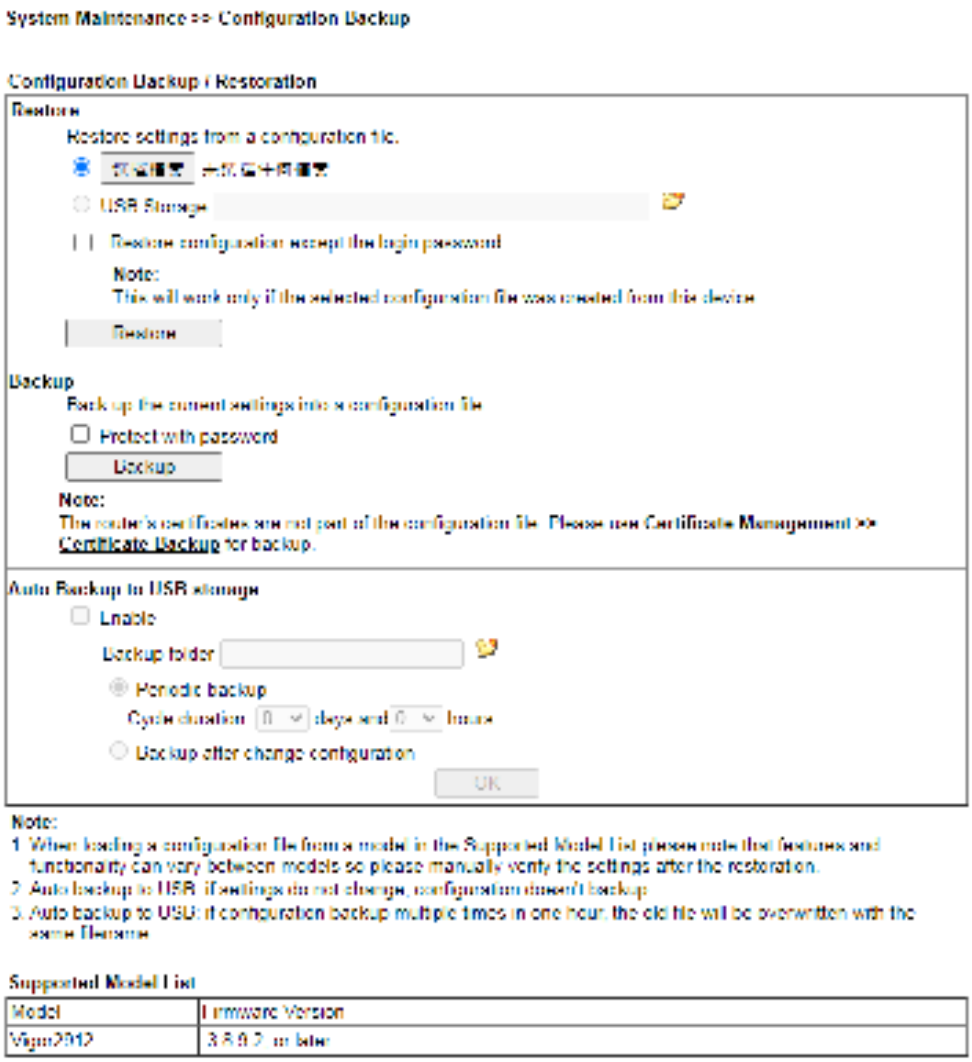
VI-1-6 Configuration Backup

Such function can be used to apply the router settings configured by Vigor2925 to Vigor2915.

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following page will be popped-up, as shown below.

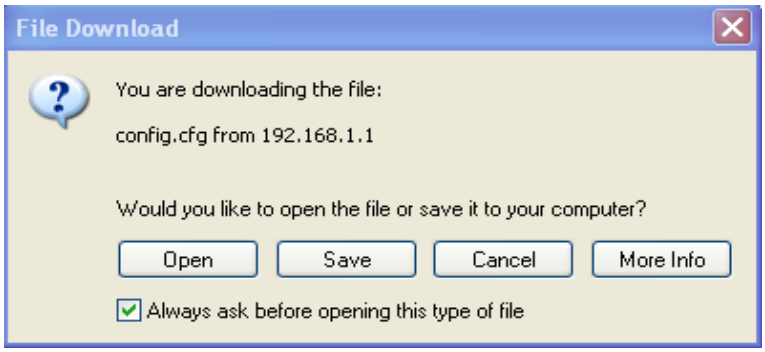


Available settings are explained as follows:

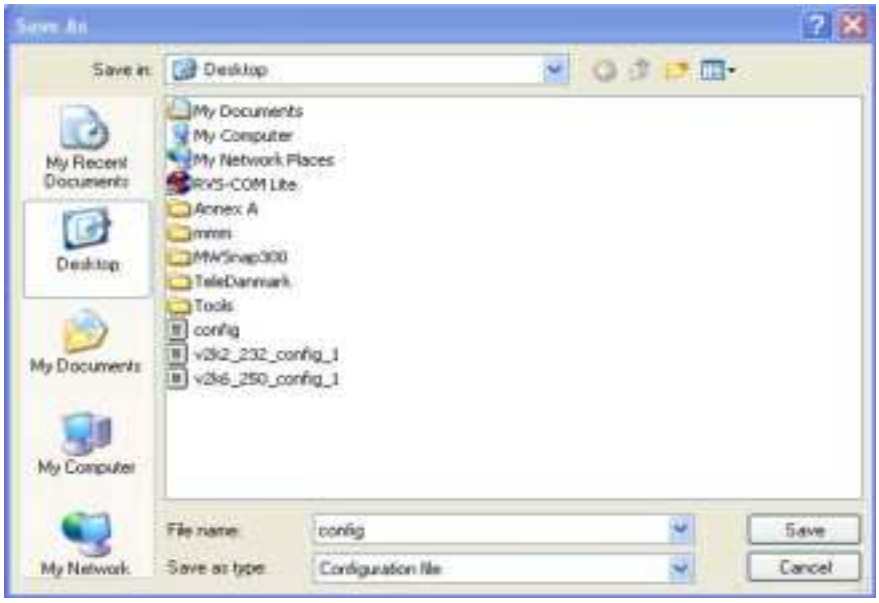
Item	Description
Restore	**Restore settings from a configuration file** – Click the **Select File** button to specify a file to be restored or click **USB Storage** (if a USB storage disk connected) to choose the configuration file. **Restore configuration except the login password** – Check the box to restore the configuration file except the login password. **Restore** - Click **Restore** to restore the configuration. If the file is encrypted, the system will ask you to Enter the password to decrypt the configuration file.

Backup	Click it to perform the configuration backup of this router. **Protect with password-** For the sake of security, the configuration file for the router can be encrypted. ● **Password** – Type several characters as the password for encrypting the configuration file. ● **Confirm Password** – Enter the password again for confirmation.
Auto Backup to USB storage	The configuration can be stored to a USB connecting to Vigor router as a backup. **Backup folder** – Set the path for downloading. **Periodicity backup** – Set the circle duration for backup. **Backup after change configuration** – Backup will be executed whenever the configuration is changed.
Support Model List	Web configuration file from *other* Vigor router can be applied to Vigor2915 series. At present, only the configuration file of Vigor2912 is accepted for Vigor2915. This field displays model name(s) and firmware which web configuration file saved can be used by such router.

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



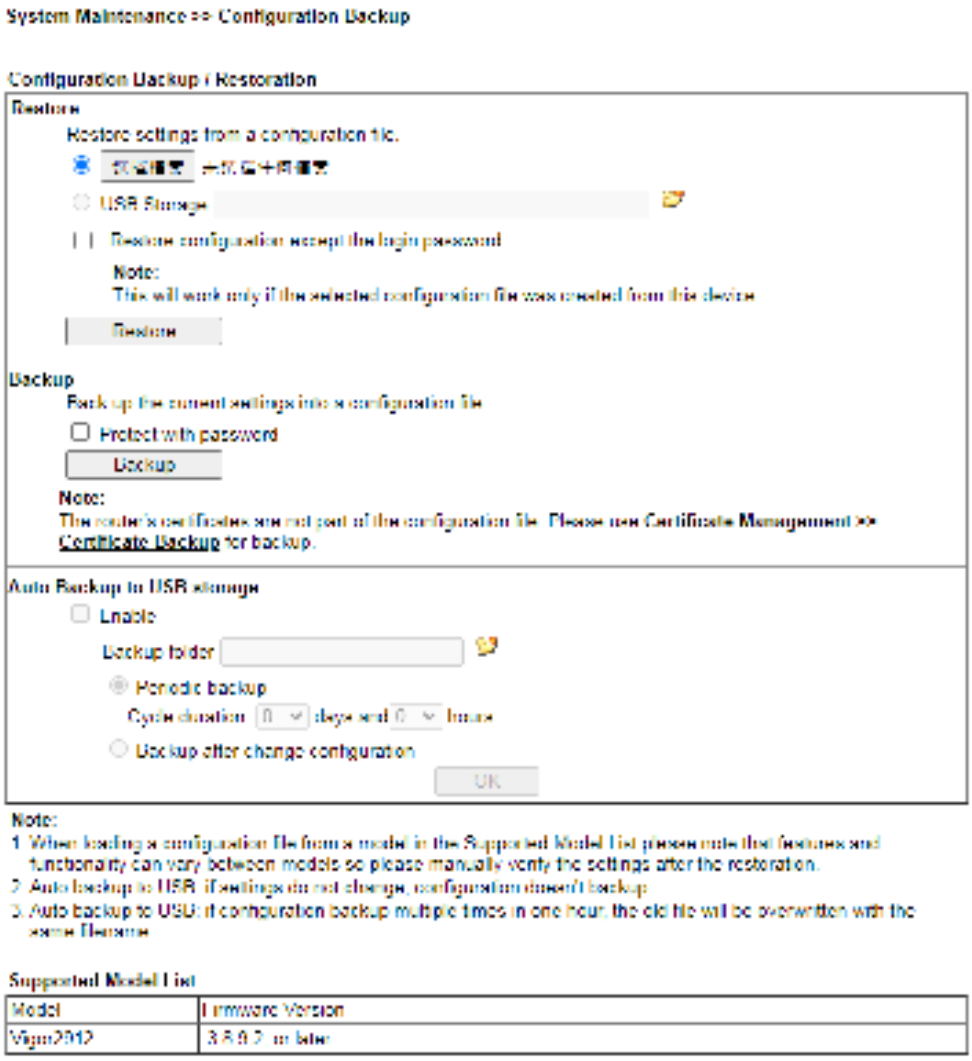
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Info	Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

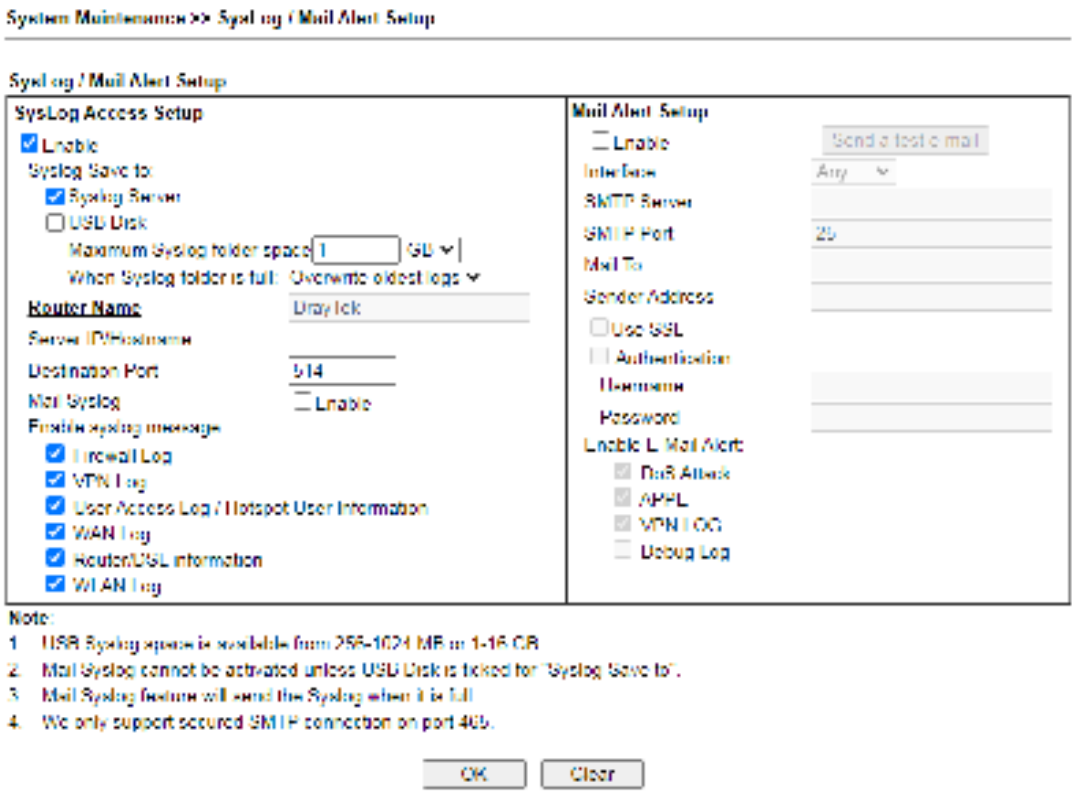


2. Click **Choose File** button to choose the correct configuration file for uploading to the router.

3. Click **Restore** button and wait for few seconds.

VI-1-7 Syslog/Mail Alert

SysLog function is provided for users to monitor router.



Available settings are explained as follows:

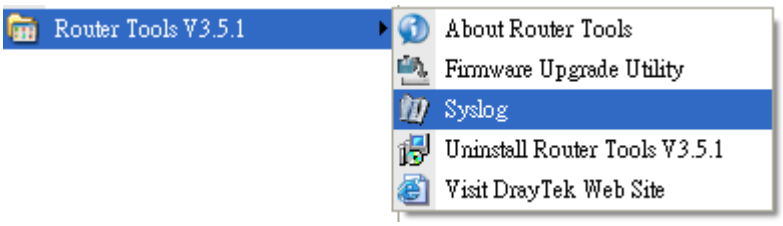
Item	Description
SysLog Access Setup	**Enable** - Select to enable the Syslog function. **Syslog Save to** – Check Syslog Server and / or USB Disk. ● **Syslog Server** – Events will be sent to a Syslog server. ● **USB Disk** – Events will be saved to a USB storage device connected to the router. ● **Maximum Syslog folder space** - Set a space (unit GB/ MB) to store event logs. ● **When Syslog folder is full** - Specify the action (overwrite the olderest logs or stop logging) to be executed.
Router Name	Display the name for such router configured in **System Maintenance>>Management.** If there is no name here, simply lick the link to access into **System Maintenance>>Management** to set the router name. **Server IP Address / Hostname -**The IP address of the Syslog server. **Destination Port -** Assign a port for the Syslog protocol.

	Mail Syslog – Check the box to recode the mail event on Syslog. **Enable syslog message -** Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Mail Alert Setup	Check **Enable** to activate function of mail alert. **Send a test e-mail -** Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not. **SMTP Server/SMTP Port -** The IP address/ Port number of the SMTP server. **Mail To -** Assign a mail address for sending mails out. **Sender Address -** Assign a path for receiving the mail from outside. **Use SSL -** Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method. **Authentication -** Check this box to activate this function while using e-mail application. ● **Username -** Enter the user name for authentication. ● **Password -** Enter the password for authentication. **Enable E-mail Alert -** Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

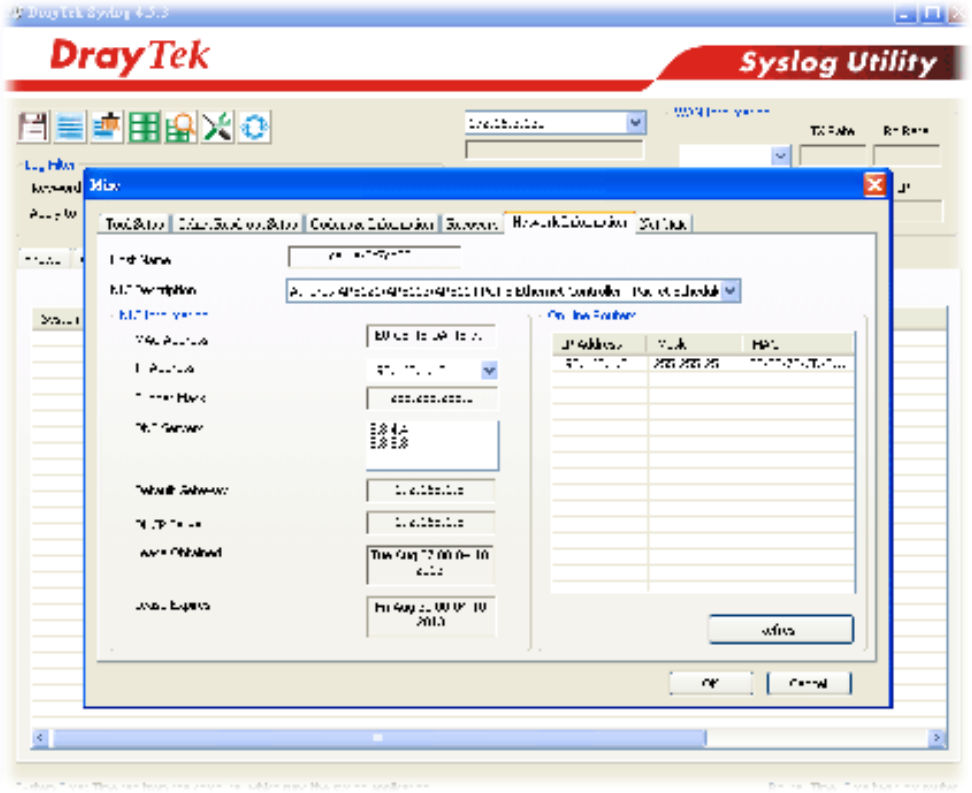
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

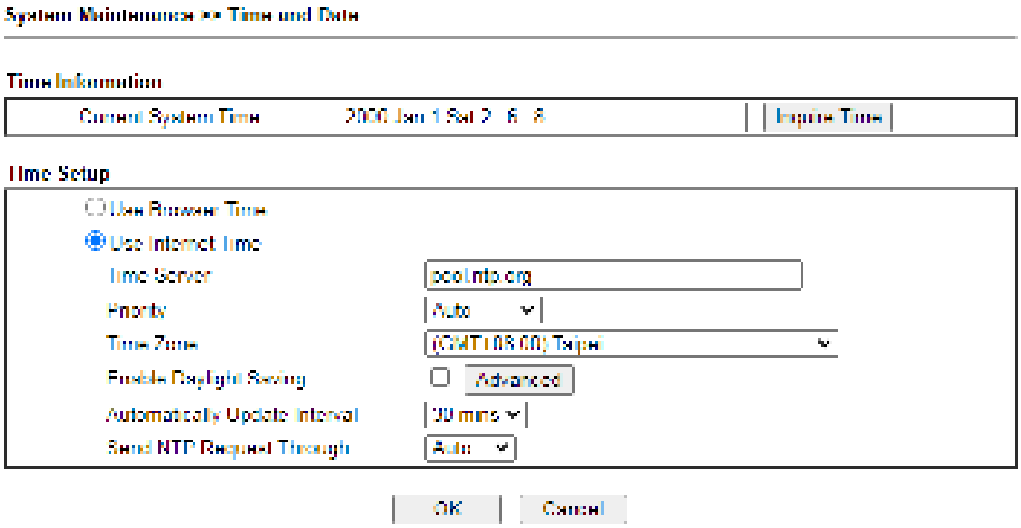


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

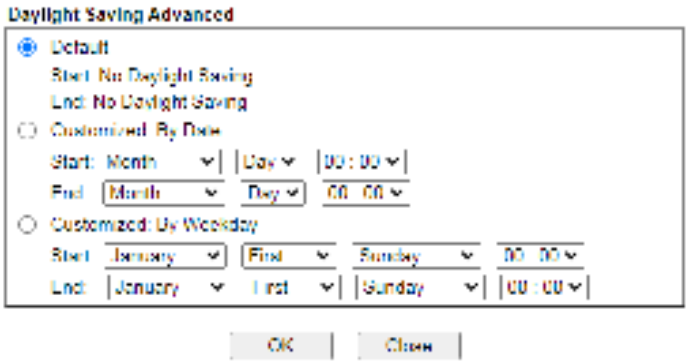


VI-1-8 Time and Date

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



Available settings are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Enter the web site of the time server.
Priority	Choose **Auto** or **IPv6 First** as the priority.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area. **Advanced** – Click it to open a pop up dialog.  Use the default time setting or set user defined time for your requirement.
Automatically Update Interval	Select a time interval for updating from the NTP server.

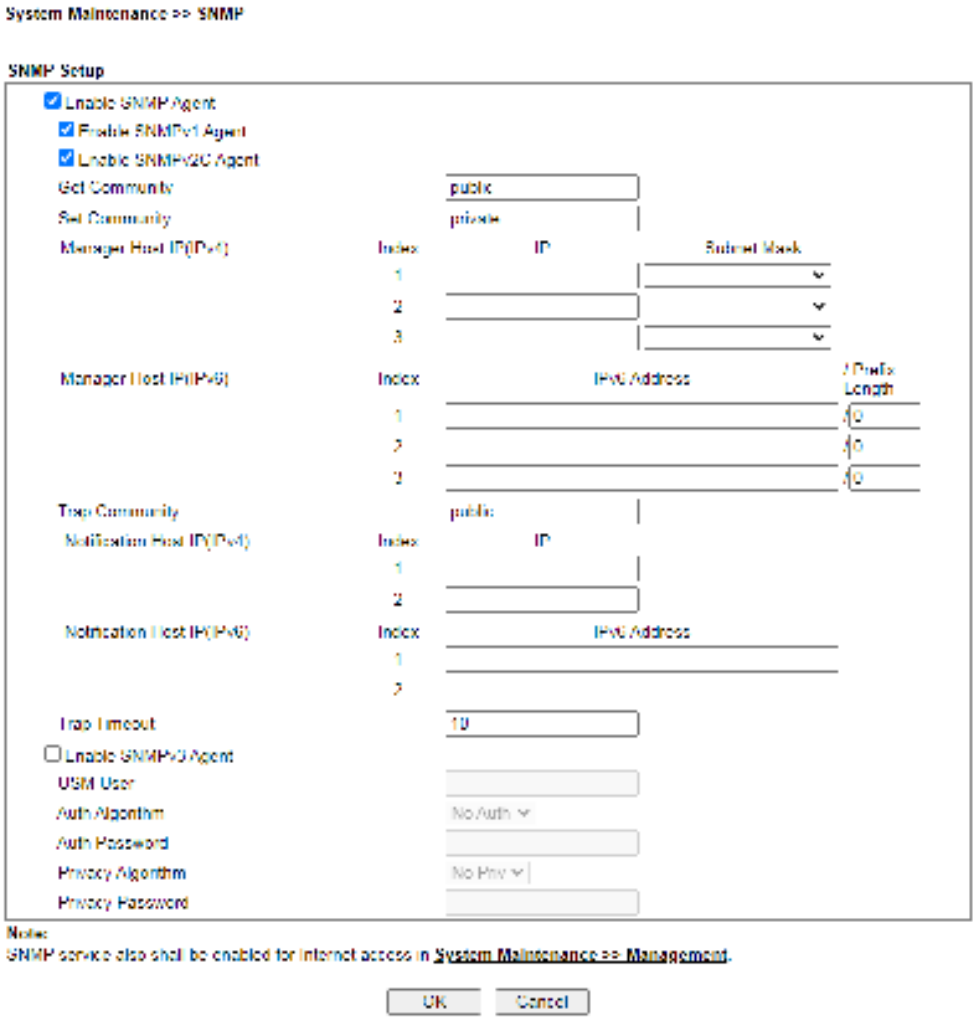
Send NTP Request Through	Specify a WAN interface to send NTP request for time synchronization.

Click **OK** to save these settings.

VI-1-9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.



Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function. Then, enable SNMPV1 agent/ SNMPV2C agent.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is **private.** The maximum length of the text is limited to 23 characters.

Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is **public.** The maximum length of the text is limited to 23 characters.
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.
Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm.
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm.
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

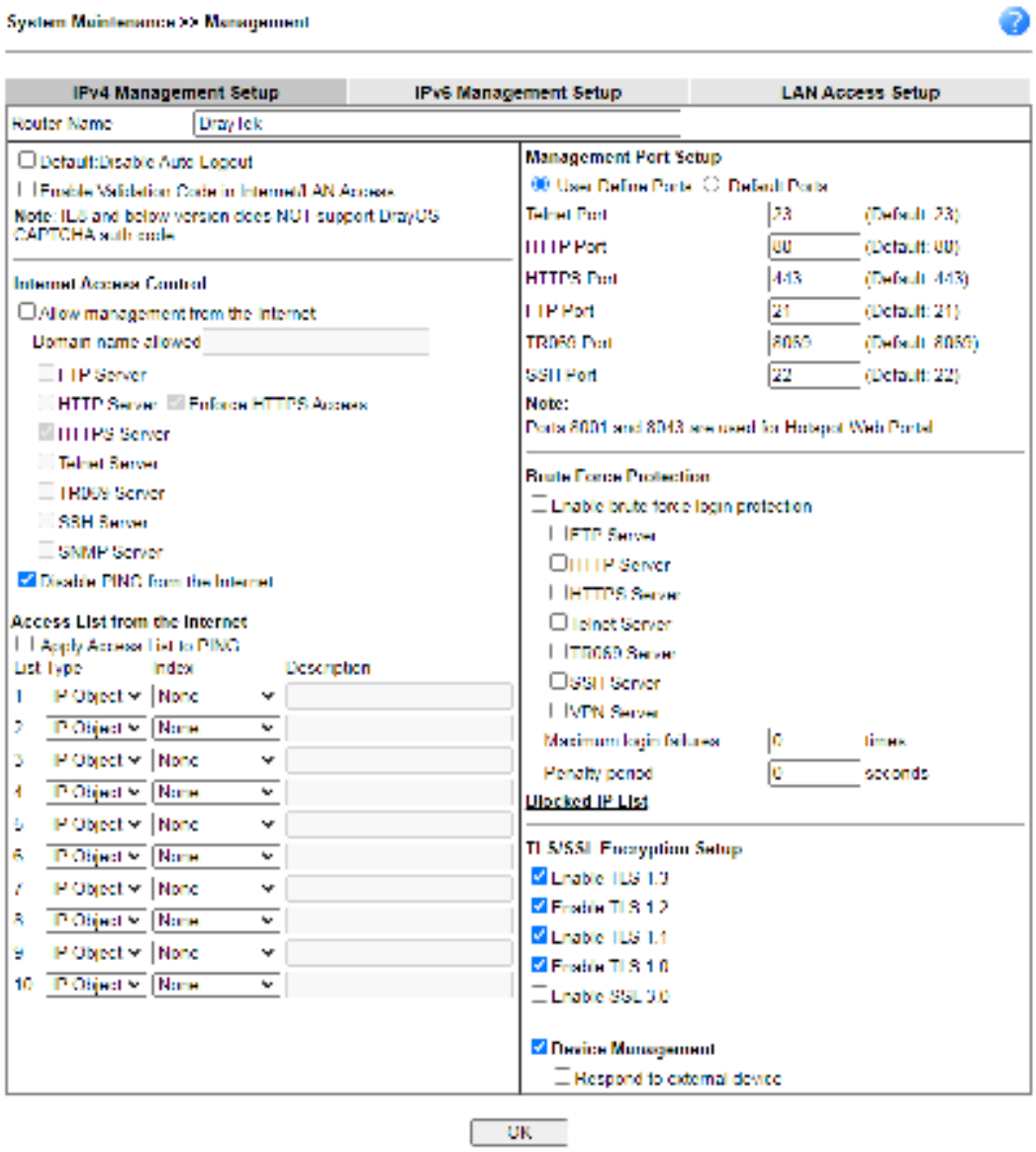
Click **OK** to save these settings.

VI-1-10 Management

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

The management pages for IPv4 and IPv6 protocols are different.

For IPv4



Available settings are explained as follows:

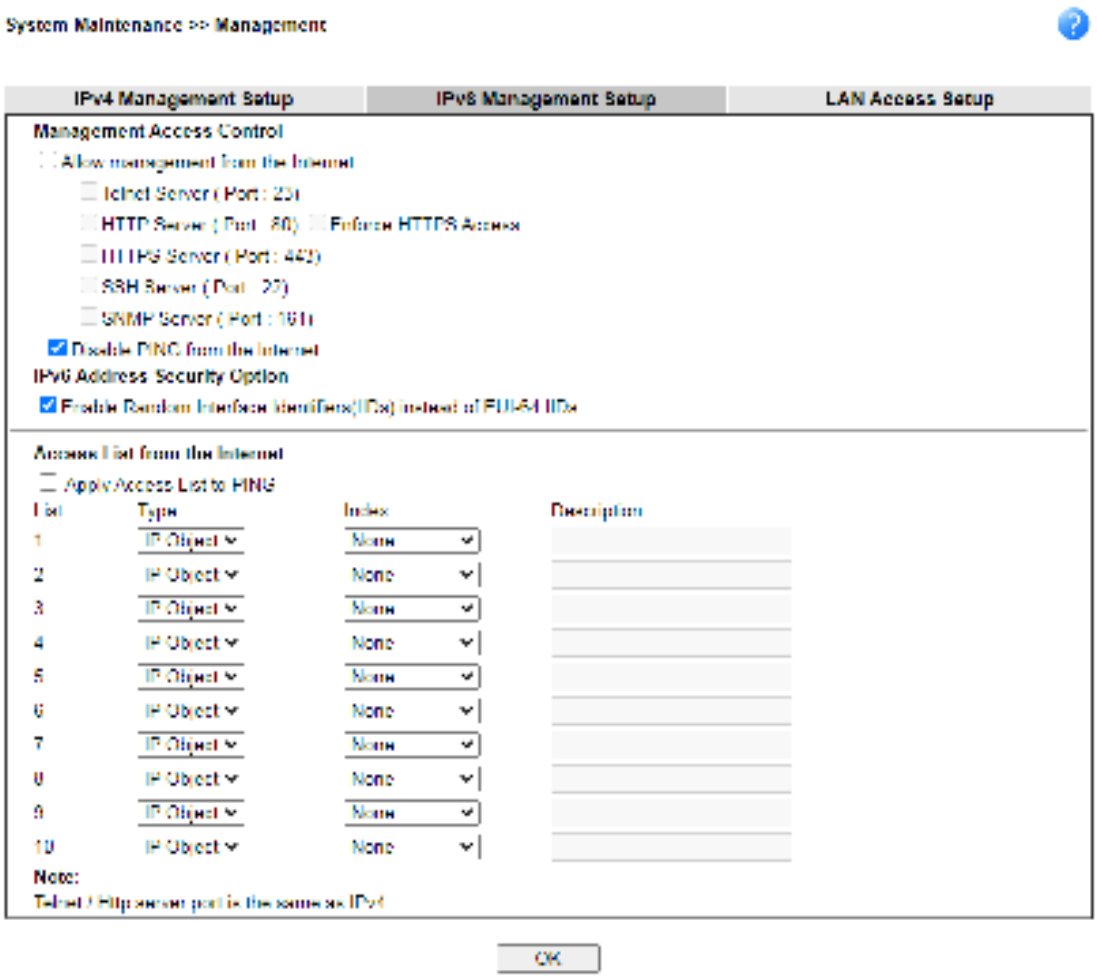
Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.

	 The web user interface will be open until you click the Logout icon manually.
Enable Validation Code in Internet/LAN Access	If it is enabled, the mechanism of validation code will be offered by Vigor router. That is, the client must type validation code while accessing into Internet or web user interface of Vigor router.
Internet Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify. **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 -** Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List from the Internet	The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks. **Apply Access List to PING** – When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, which blocks all pings from the Internet. **Type** - Select **IP Object** 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** – Enable the protection mechanism. **Maximum login failure** – Specify the maximum number of wrong password that client can try for logging to Vigor router. **Penalty period** – Set a period of time to block the IP address which is used (by user or hacker) for passing through the user authentication again and again but failed always. When the time is up, Vigor system will unblock that IP and allow it to access into Vigor router again. **Blocked IP List** – Open another web page which displays current blocked IPs.
TLS/SSL Encryption Setup	**Enable TLS 1.0/1.1/1.2 & SSL 3.0** – Check the box to enable the function of TLS 1.0/ 1.1/ 1.2 / SSL 3.0 if required. Due to security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol.
Device Management	Check the box to enable the device management function for Vigor2915. **Respond to external device** – If it is enabled, Vigor2915 will be regarded as slave device. When the external device (master device) sends request packet to Vigor2915, Vigor2915 would send back information to respond the request coming from the external device which is able to manage Vigor2915.

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

For IPv6



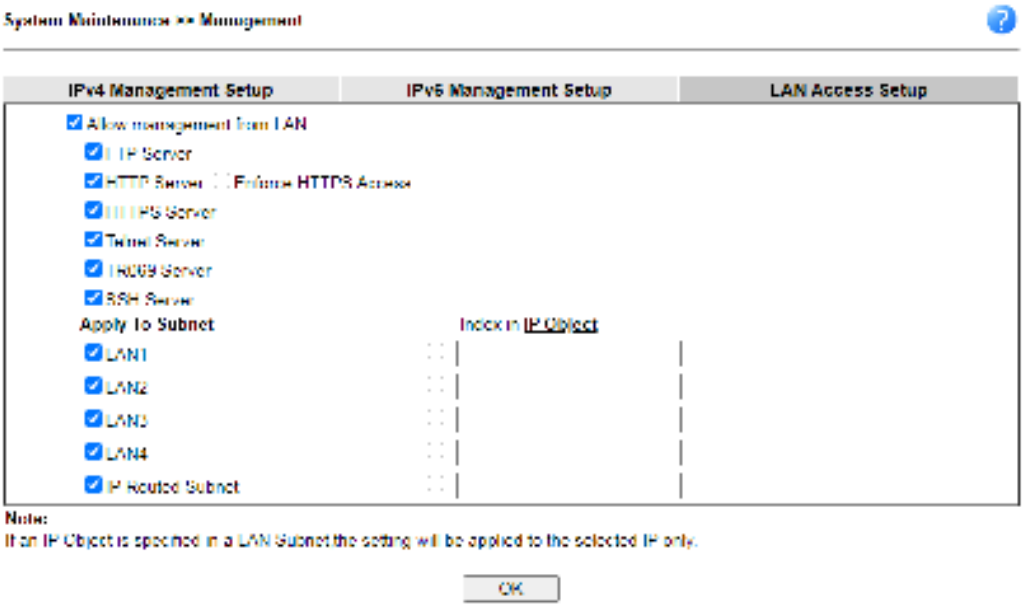
Available settings are explained as follows:

Item	Description
Management Access Control	**Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify. **Disable PING from the Internet** - Check the checkbox to disable all PING packets from the Internet. For security issue, this function is enabled by default.
IPv6 Address Security Option	**Enable Random Interface Identifiers (IIDs)... -** The IPv6 address will be generated randomly but not using LAN/ WAN MAC to prevent the attack from the hacker.
Access List from the Inernet	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/ subnet masks is allowed. **Apply Access List to PING** – When this option is checked and **Disable PING from the Internet** is unchecked, pings originating from the Internet will be accepted only if they are from one of the IP addresses and/ or subnet masks specified below. This option has no effect if **Disable PING from the Internet** is checked, which blocks all pings from the Internet. **Type** - Select **IP Object** or **Hostname**.

	Index - Select the index number of a configured IPv6 object.

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

For LAN



Available settings are explained as follows:

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

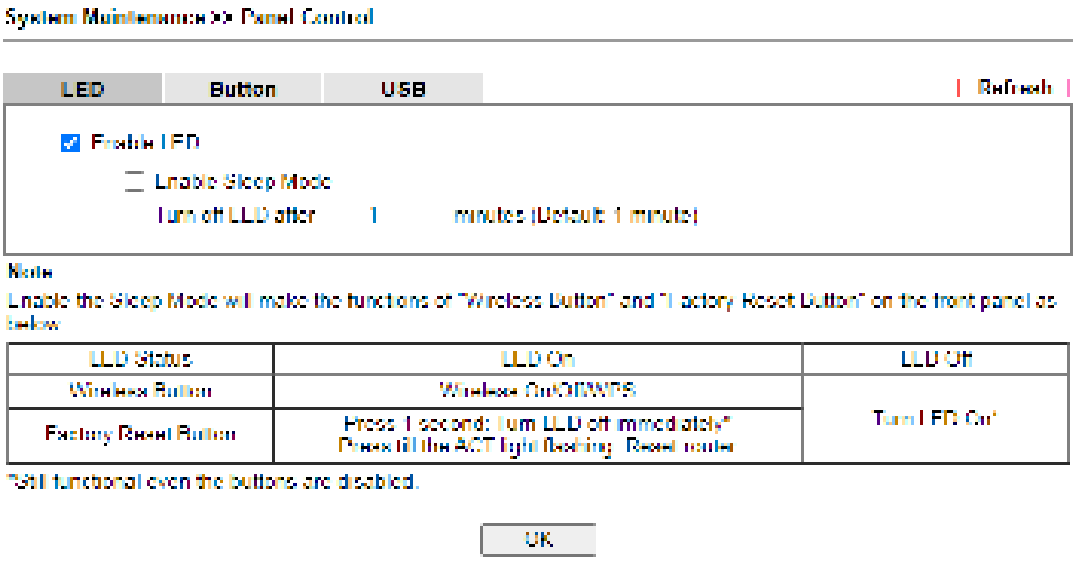
After finished the above settings, click **OK** to save the configuration.

VI-1-11 Panel Control

The behavior of the LEDs, buttons, USB ports and LAN ports on the front panel of the Vigor router can be customized as desired.

For LED

By default, the LEDs are enabled, and will illuminate or blink continuously to show the status of the various functions in the router. However, they can be configured to remain off at all times, or remain off until a button is pressed to wake them up.



Available settings are explained as follows:

Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable LED	Select to enable front panel LEDs. ● **Enable Sleep Mode/Turn off LED after _ minutes** – Available when **Enable LED** is selected. Select this option to turn off the LEDs after the specified number of minutes. ● When sleep mode is enabled, LEDs can be woken up by pressing either the **Wireless LAN ON/OFF/WPS** button or the **Factory Reset** button on the front panel, or by clicking the **Wake up LED** button on this page. When LEDs are lit, they can be put to sleep by briefly pressing the **Factory Reset** button, or by clicking the **LED sleep immediately** button on this page.
Status	Shows the status of the LEDs: **Status :** Sleep [Wake up LED] – LEDs are in sleep mode. To wake them up, do one of the following: ● press the **Wake up LED** button on this page ● press the **Wireless On/Off/WPS** button on the front panel ● press the **Factory Reset** button on the front panel.

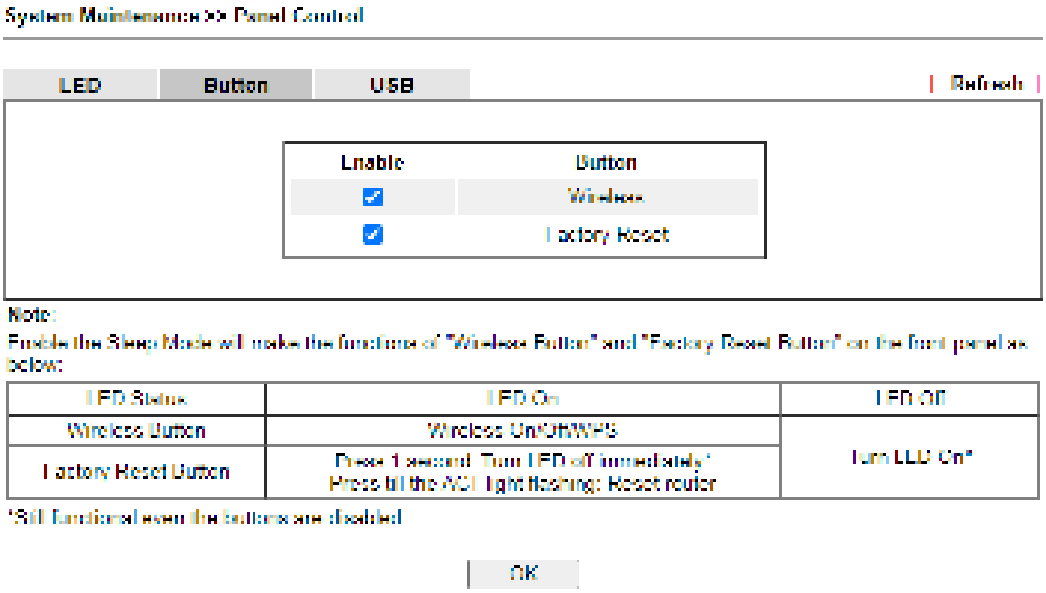
	Status : Awake, sleep after 1 minutes [LED sleep immediately] – LEDs are awake. To put them to sleep immediately ● press the **LED sleep immediately** button on this page ● press the Factory Reset button on the front panel for 1 second.

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

For Button

The **Factory Reset** and **Wireless ON/OFF/WPS** buttons on the front panel are enabled by default and can be enabled or disabled if required. Disabling the Factory Reset button will prevent tampering by unauthorized parties, or to avoid accidental triggering of a router reset when being used wake up LEDs. Disabling the wireless button will prevent changing the wireless setting when LED Sleep Mode is enabled, and the buttons are primarily used to turn the LEDs on and off.

Click the **Button** tab to get the following page.



Available settings are explained as follows:

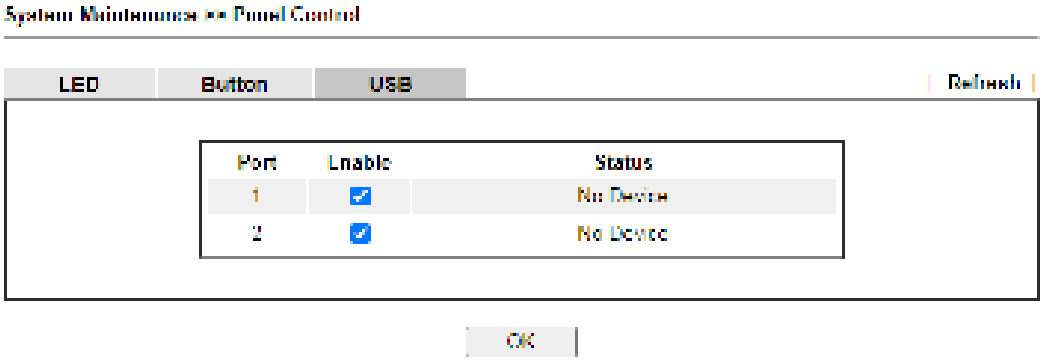
Item	Description
Refresh	Click to refresh the page to display the latest information.
Enable Wireless Button	It is available for wireless model. The default value is **Enabled**. Deselect to disable the ability of the Wireless button to control WLAN and WPS functions. Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled.
Enable Factory Reset Button	The default value is **Enabled**. Deselect to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings. It

	can still be used to wake up the LEDs when LED sleep mode is enabled.

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

For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.



Available settings are explained as follows:

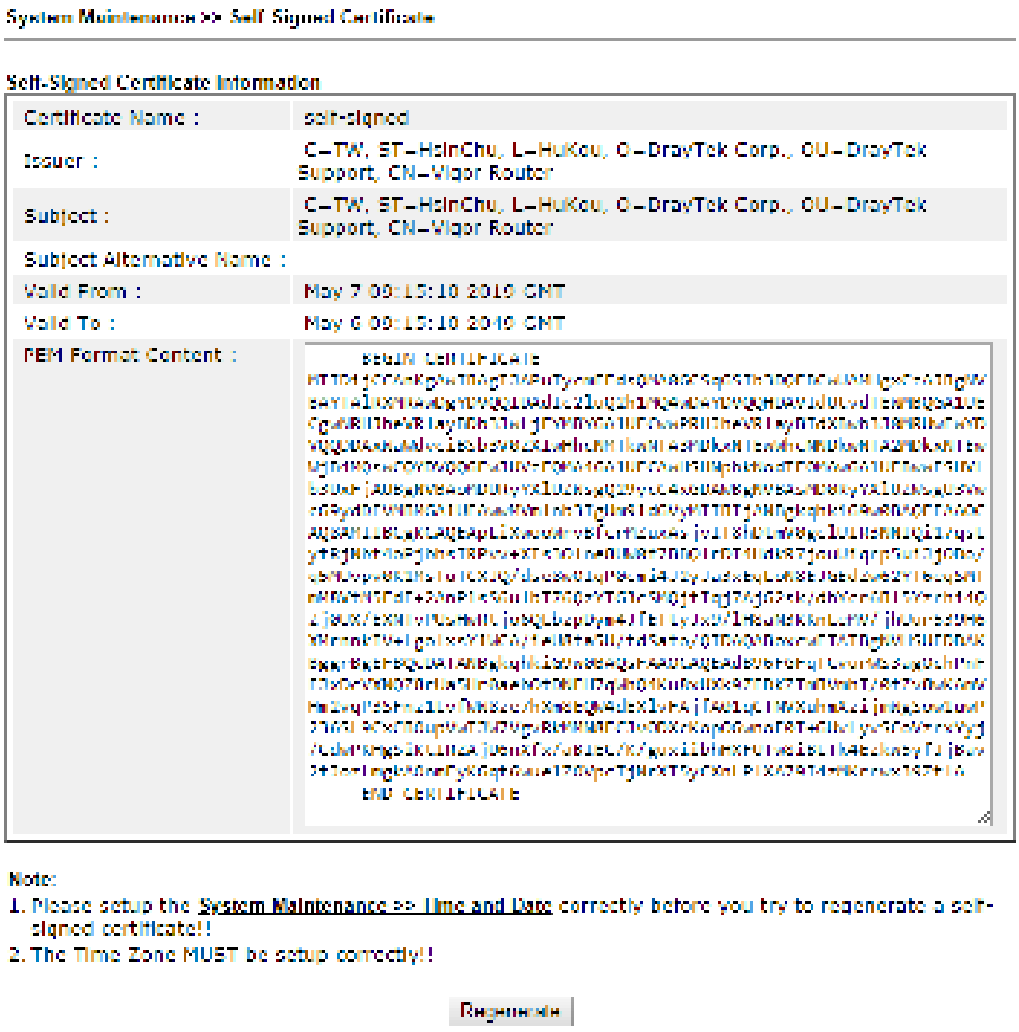
Item	Description
Refresh	Click to refresh the page to display the latest information**.**
Port	The number corresponds to the USB port number shown on the front panel.
Enable	Deselect to disable the USB port. The default value is enabled.
Status	Shows the status of the USB port. **No device** –no USB device is connected to the port. **Connected** –a USB device is connected to the port. **---** –the USB port is disabled.

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

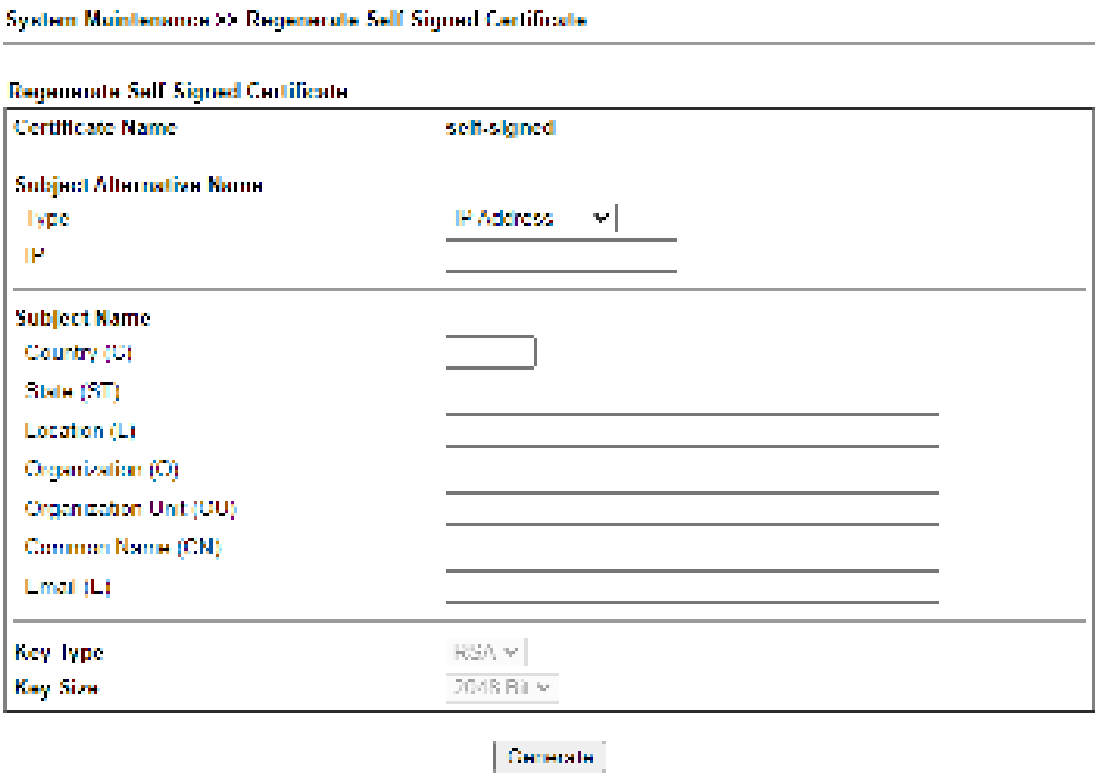
VI-1-12 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.

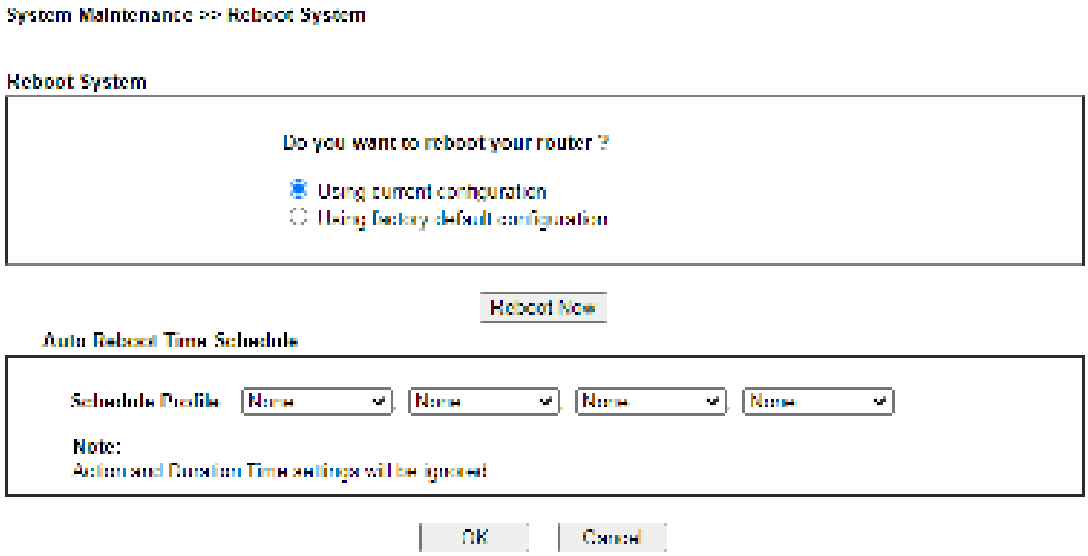


Click **Regeneration** to open **Regenerate Self-Signed Certificate** window. Type in all the information that the window request such as certifcate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE**.


System Maintenance >> Regenerate Self Signed Certificate
Regenerate Self Signed Certificate
Certificate Name
self-signed
Subject Alternative Name
Type
IP Address
IP
Subject Name
Country (C)
State (ST)
Location (L)
Organization (O)
Organization Unit (OU)
Common Name (CN)
Email (E)
Key Type
RSA
Key Size
2048 Bit
Generate

VI-1-13 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.



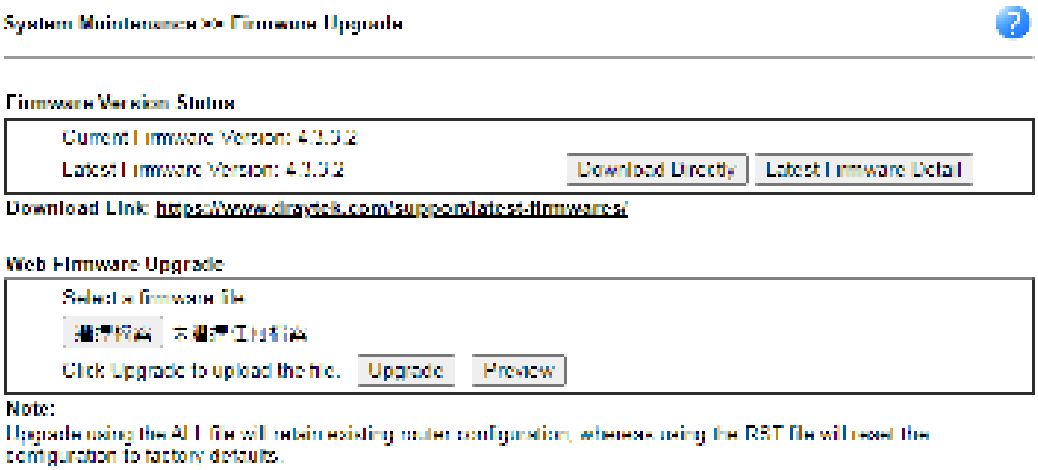
Schedule Profile - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.

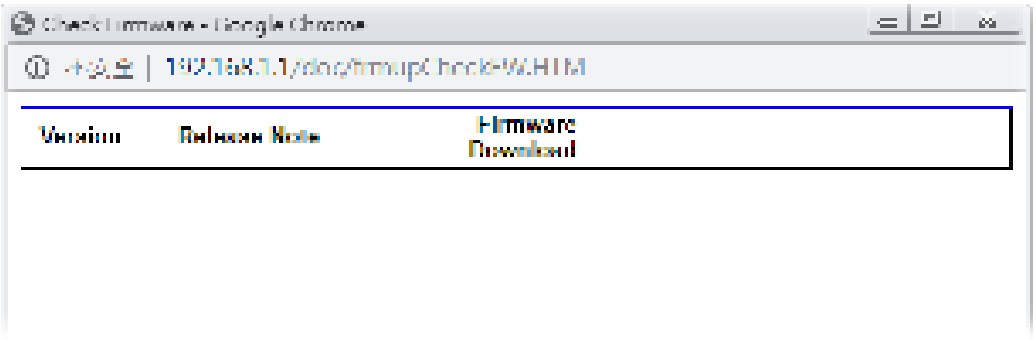
Info	When the system pops up Reboot System web page after you configure web settings, please click Reboot Now to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

VI-1-14 Firmware Upgrade

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



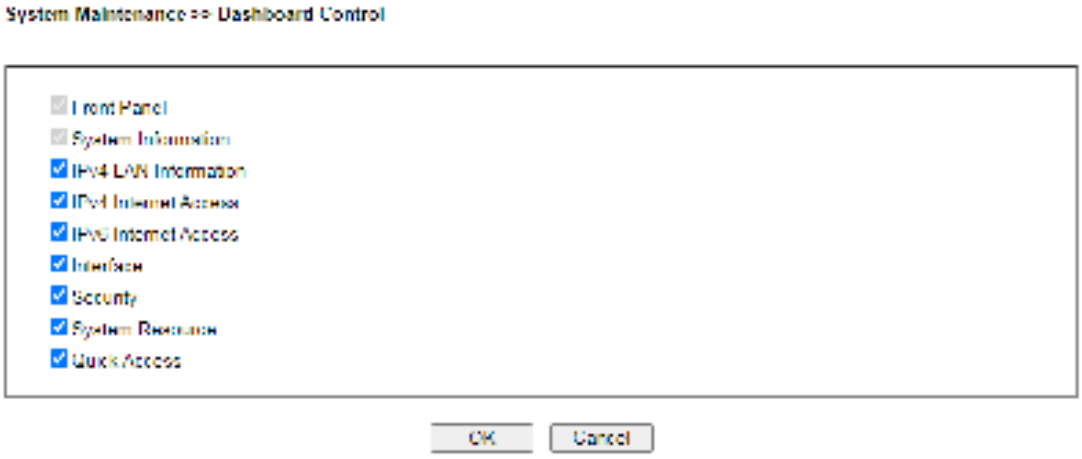
Click the button of **Check The Latest Firmware** to open a pop up window displaying the newest firmware version released for such Vigor router.



Choose the one you need and click **Download**. After that, click **Select** to specify the one you just download. Then, click **Upgrade**. The system will upgrade the firmware of the router automatically.

VI-1-15 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/ user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.



VI-2 Bandwidth Management

Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

Quality of Service (QoS)

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.

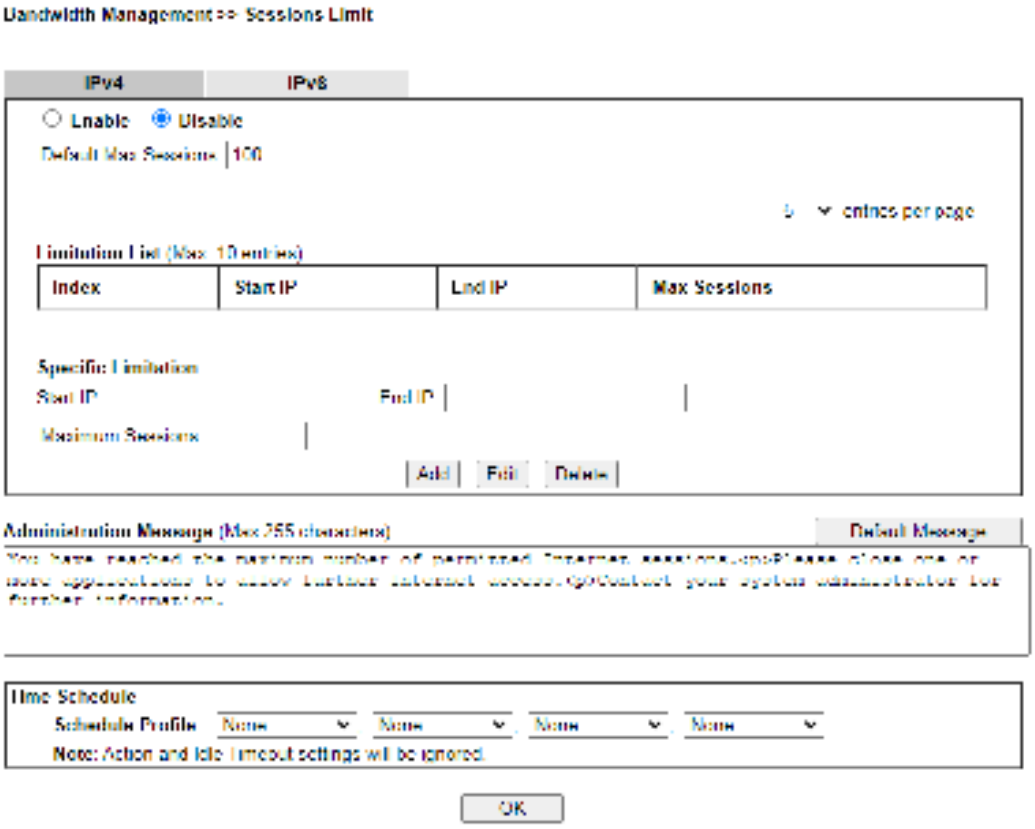
However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

Web User Interface

Below shows the menu items for Bandwidth Management.

VI-2-1 Sessions Limit

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



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

Available settings are explained as follows:

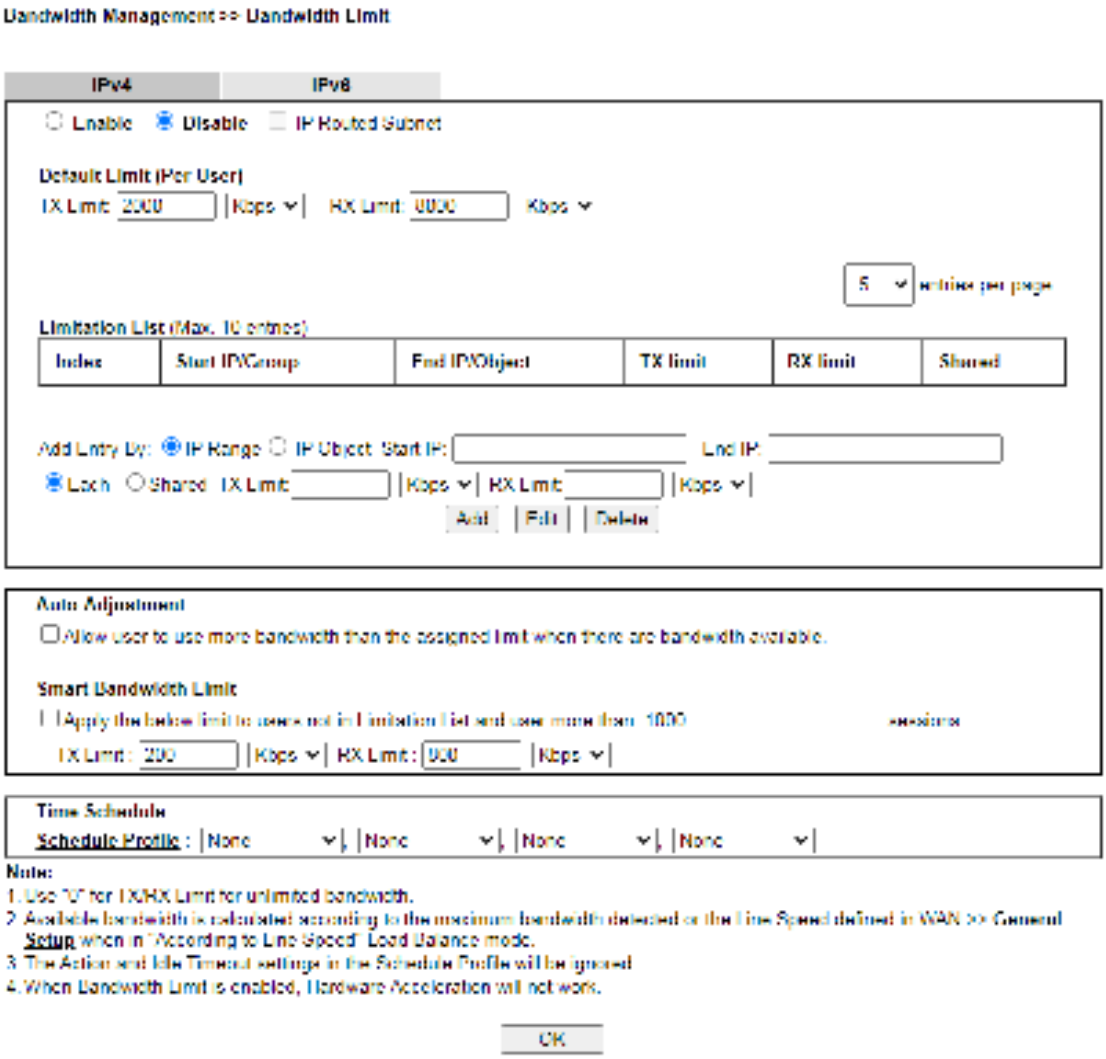
Item	Description
Session Limit	**Enable -** Click this button to activate the function of limit session. **Disable** - Click this button to close the function of limit session. **Default Max Session -** Defines the default maximum session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web

	page.
Specific Limitation	**Start IP-** Defines the start IP address for limit session. **End IP -** Defines the end IP address for limit session. **Maximum Sessions -** Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index. **Add -** Adds the specific session limitation onto the list above. **Edit -** Allows you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.
Administration Message	Enter the words which will be displayed when reaches the maximum number of Internet sessions permitted. **Default Message -** Click this button to apply the default message offered by the router.
Time Schedule	**Schedule Profile** - You can 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.

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

VI-2-2 Bandwidth Limit

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



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

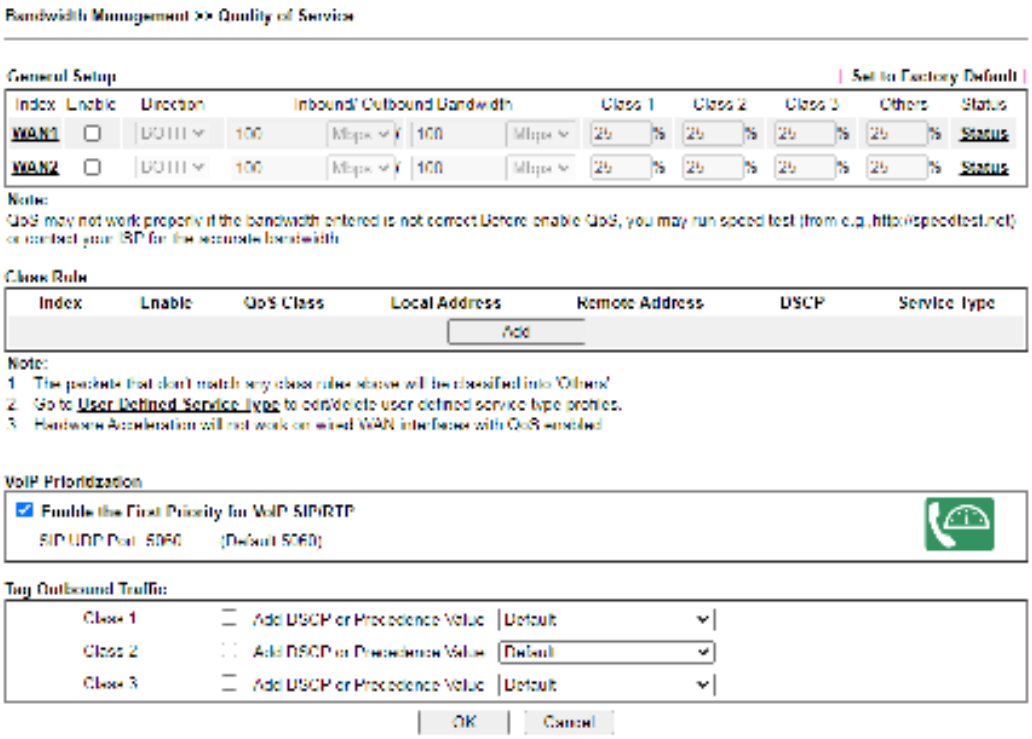
Available settings are explained as follows:

Item	Description
Enable	Click this button to activate the function of limit bandwidth. **IP Routed Subnet** – Check this box to apply the bandwidth limit to the second subnet specified in **LAN>>General Setup**. It is available for IPv4 settings only. **Default limit (Per User)** ● **TX LImit -** Define the default speed of the upstream for each computer in LAN. ● **RX limit -** Define the default speed of the downstream for each computer in LAN.
Disable	Click this button to close the function of limit bandwidth.
Limitation List	Display a list of specific limitations that you set on this web page.

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 -** Define the start IP address for limit bandwidth. ● **End IP -** Define the end IP address for limit bandwidth. **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** / **Shared -** Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields. ● **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. ● **RX limit -** Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. **Add -** Add the specific speed limitation onto the list above. **Edit -** Allow you to edit the settings for the selected limitation. **Delete -** Remove the selected settings existing on the limitation list.
Auto-Adjustment	**Allow user to use more bandwidth ···-** Check this box to make the best utilization of available bandwidth.
Smart Bandwidth Limit	**Apply the below limit to ...** - Check this box to have the bandwidth limit determined by the system automatically. ● **TX limit -** Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. ● **RX limit -** Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Time Schedule	**Schedule Profile -** You can 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.

VI-2-3 Quality of Service

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page. This page displays the QoS settings result of the WAN interface.



Available settings are explained as follows:

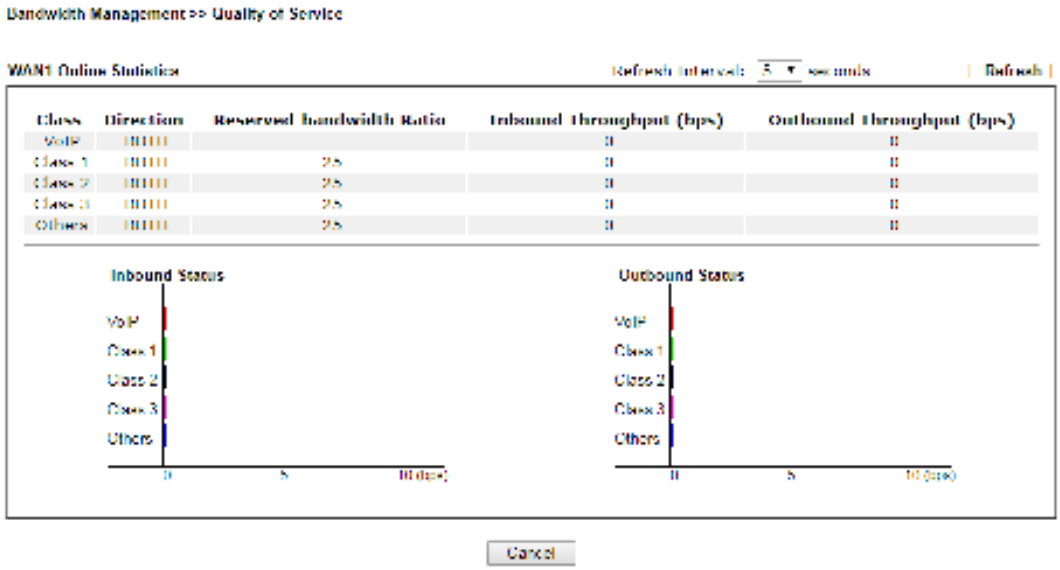
Item	Description
General Setup	**Index** – Display the WAN/LTE interface number link that you can edit. **Enable** – Check the box to enable the QoS function for WAN/LTE interface. If it is enabled, you can configure general QoS setting for each WAN/LTE interface. ● **Direction** – Define which traffic the QoS Control settings will apply to. ■ **IN-** apply to incoming traffic only. ■ **OUT-**apply to outgoing traffic only. ■ **BOTH-** apply to both incoming and outgoing traffic. ● **Inbound/Outbound Bandwidth** – Set the connecting rate of data input/output for other WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps. ● **Class 1 ~ 3 / Others** – Define the ratio of bandwidth to upstream speed and bandwidth to downstream speed. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. In which, the "Others" field is used for the packets which are not suitable for the three class rules. **Status** – Display the online statistics of WAN interface.

Item	Description
Class Rule	Set detailed settings for the selected Class. **Index** – Display the class number that you can edit. **Enable** - Display the status of this class rule. **QoS Class** - Display the QoS class level. **Local Address** - Display the local IP address for the rule. **Remote Address** - Display the remote IP address for the rule. **DSCP** - Display the levels of the data for processing with QoS control. **Service Type** – Display 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** - When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority. **SIP UDP Port** – Set a port number used for SIP.
Tag Outbound Traffic	**Add DSCP or Precedence Value for Class 1 to Class 3 -** Check the box to add DSCP or Precedence value to Class 1 to Class 3.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request. Click the link (WAN1 to WAN2) under Index to access into next page for the general setup of WAN interface. As to class rule, simply click the **Add** link to access into next page for configuration.

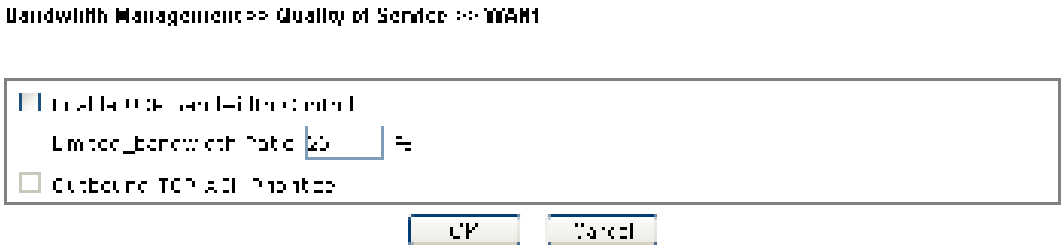
Online Statistics

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.



General Setup for WAN Interface

Click WAN interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.



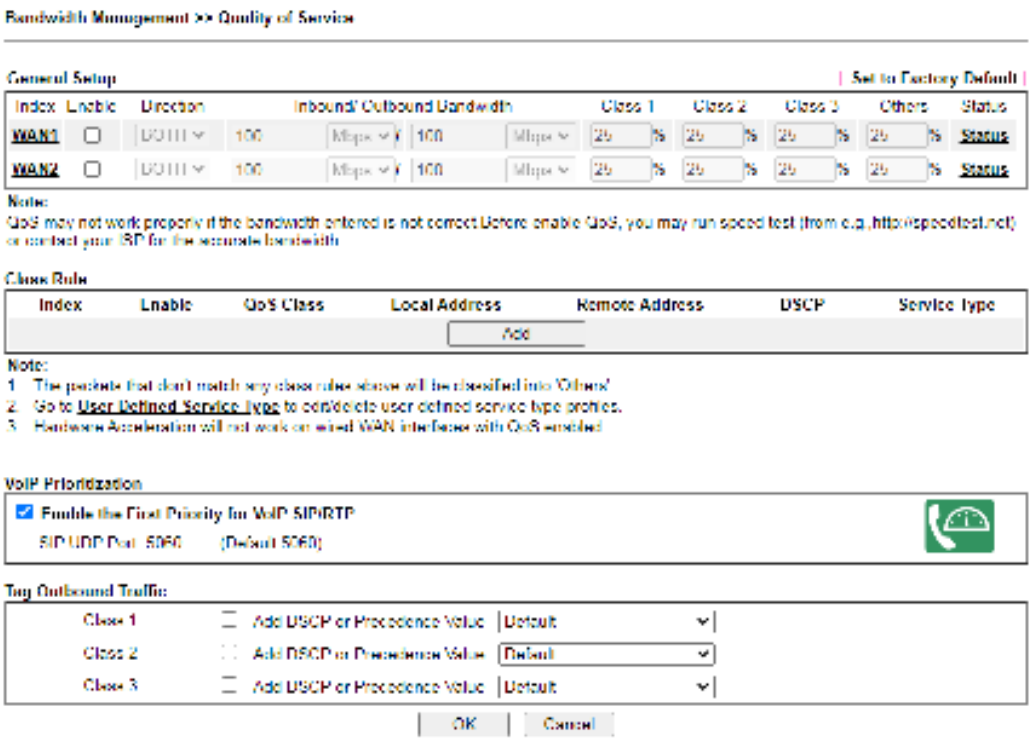
Available settings are explained as follows:

Item	Description
Enable UDP Bandwidth Control	Set the limited bandwidth ratio. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth. **Limited_bandwidth Ratio -** The ratio typed here is reserved for limited bandwidth of UDP application.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

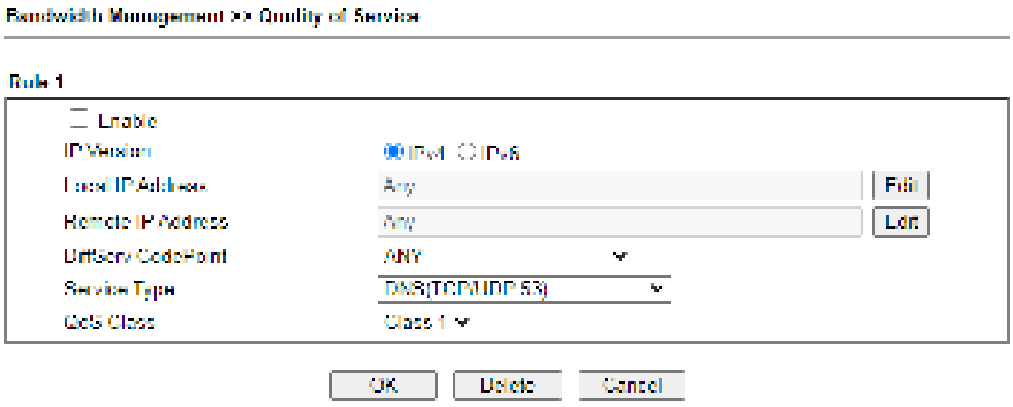
Info	The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80%- 85%of physical network speed provided by ISP to maximize the QoS performance.

Add a Class Rule for QoS

1. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Add** / **Edit** button of that one.

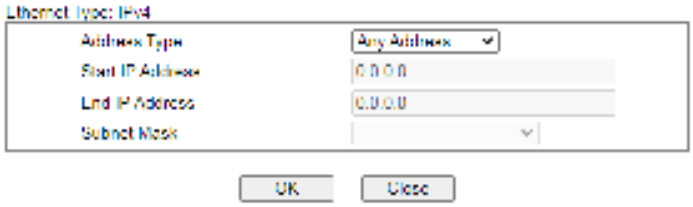


2. For adding a new rule, click **Add** to open the following page.

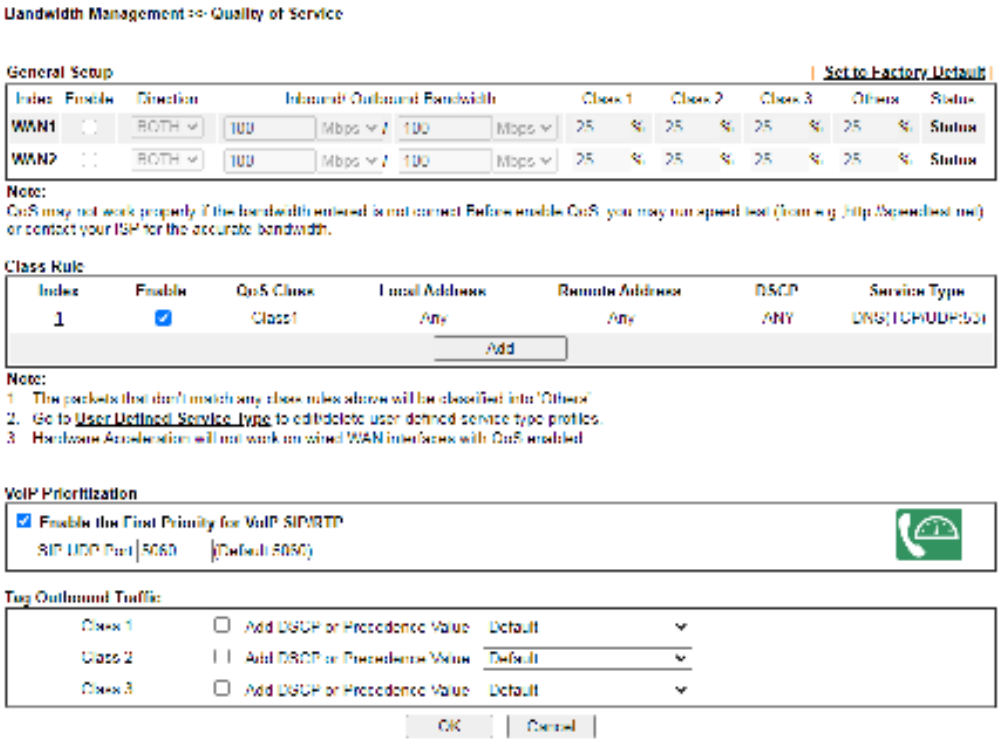


Available settings are explained as follows:

Item	Description
Enable	Check this box to invoke these settings.
Hardware Acceleration	Check this box to enable the hardware acceleration when such rule is applied.
IP Version	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the **Edit** button to set the local IP address (on LAN) for the rule.

Remote Address	Click the **Edit** button to set the remote IP address (on LAN/ WAN) for the rule.  **Address Type** – Determine the address type for the source address. For **Single Address**, you have to fill in Start IP address. For **Range Address**, you have to fill in Start IP address and End IP address. For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.
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.

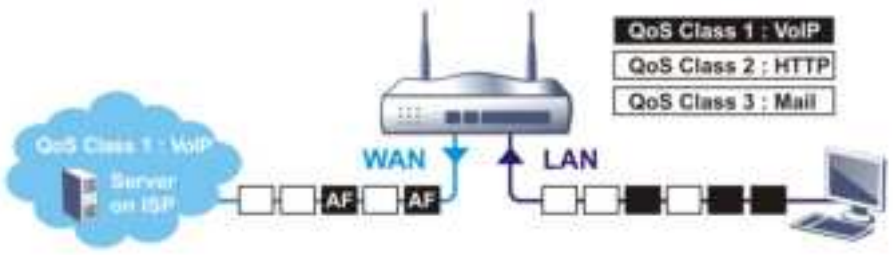


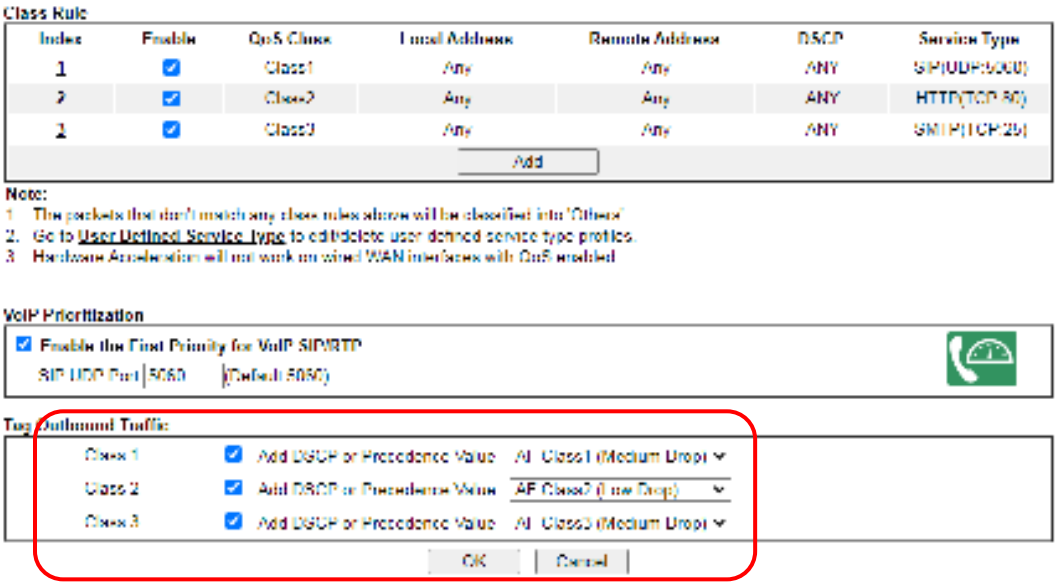
By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Retag the Packets for Identification

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



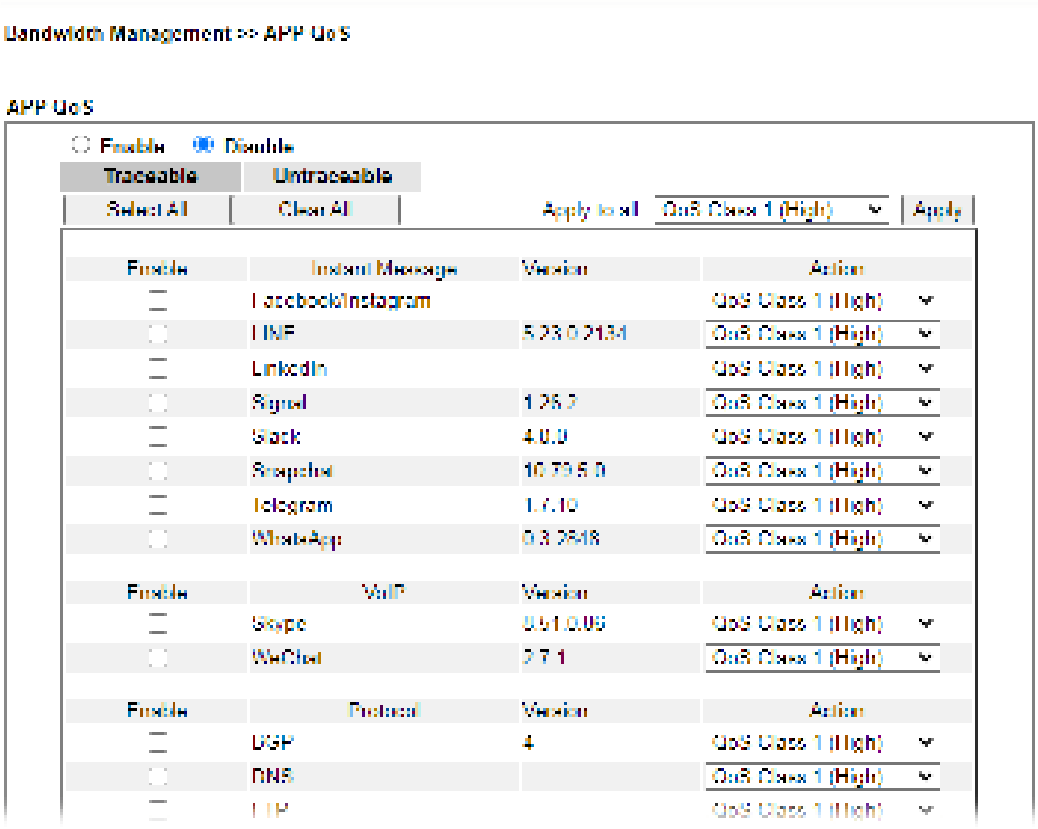


VI-2-4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as VNC or PPTV without fixed IP or port number.

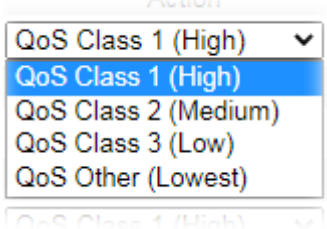
APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbond bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click **Bandwidth Management>>APP QoS** to open the following page.



Available settings are explained as follows:

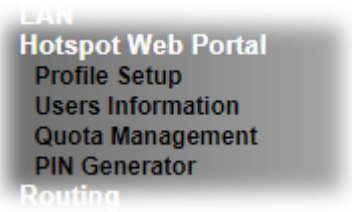
Item	Description
Enable/Disable	Click **Enable** to activate APP QoS function. Click **Disable** to deactivate APP QoS function.
Traceable	The protocol listed below is traceable by Vigor router. Each tab offers different types of protocols to fit your request.
Untraceable	The protocol listed below is not easy to be traced by Vigor router. Each tab offers different types of protocols to fit your request.
Select All	Click it to select all of the protocols.
Clear All	Click it to de-select all of the protocols.
Apply to all	Choose one of the actions from the drop down list. It is

	prepared for applying to all protocols. **Apply** – Click it to make the selected action be applied all of the selected protocols immediately.
Action	There are many protocols which can be specified with different QoS Class. 

VI-3 Hotspot Web Portal

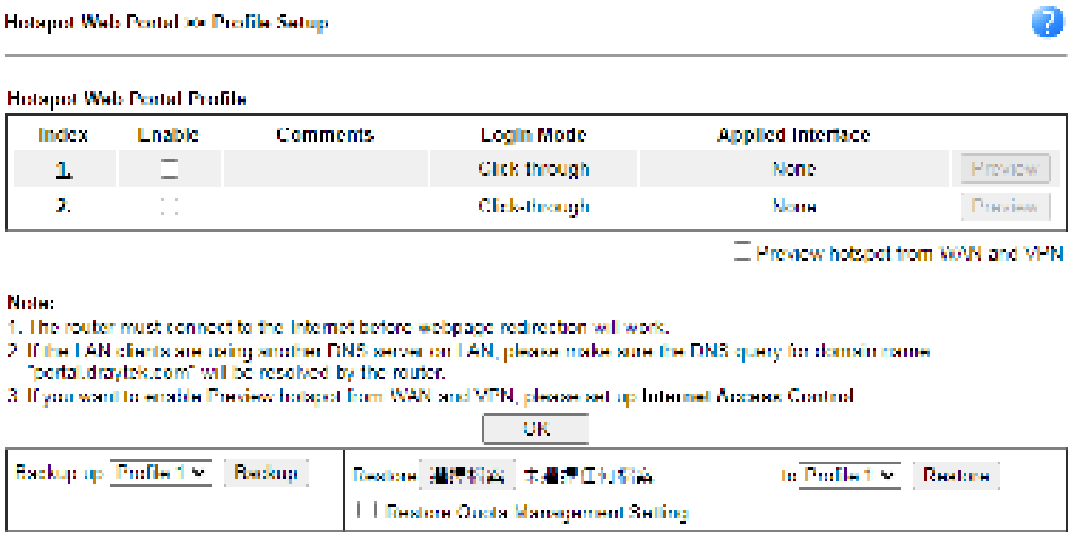
The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Web User Interface



VI-3-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.



Available settings are explained as follows:

Item	Description
Index	Click the index number link to view or update the profile settings.
Enable	Check the box to enable the profile.
Comments	Shows the description of the profile.
Login Mode	Shows the login mode used by the profile. See the section

	Login Mode for details.
Applied Interface	Shows the interfaces to which this profile applies.
Preview	Click this button to preview the Hotspot Web Portal page that will be displayed to users.
Backup	Select Profile 1 (index 1) or Profile 2 (index 2) and click the Backup button to save the configuration settings as a backup file.
Restore	Specify an existed backup file first and select Profile 1 (index 1) or Profile 2 (index 2) to apply the backup file to. Click the Restore button to perform the job. **Resotore Quota Management Setting** - After checking the box, those settings related to bandwidth/session limit will be restored at the same time.

VI-3-1-1 Login Method

There are four login methods to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

(A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

(B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

(C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

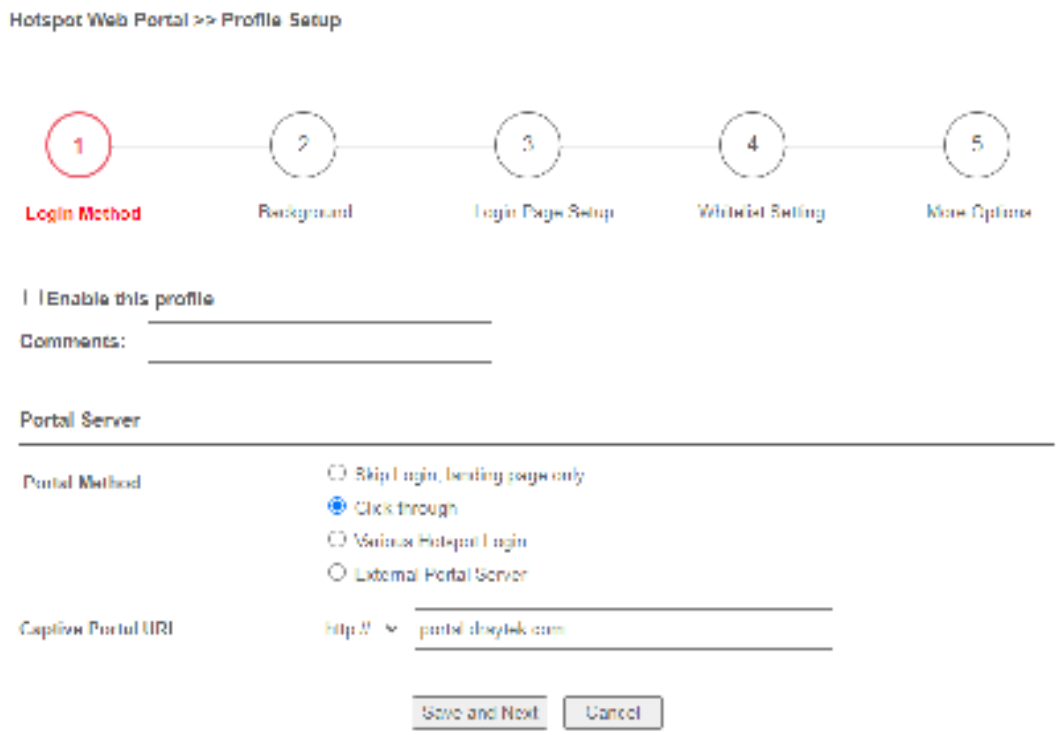
(D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

VI-3-1-2 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. 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 ● Leave Info Login
Facebook (Login with	This setting is available when **Various Hotspot Login** is selected as the portal method. Select one or more desired login methods:

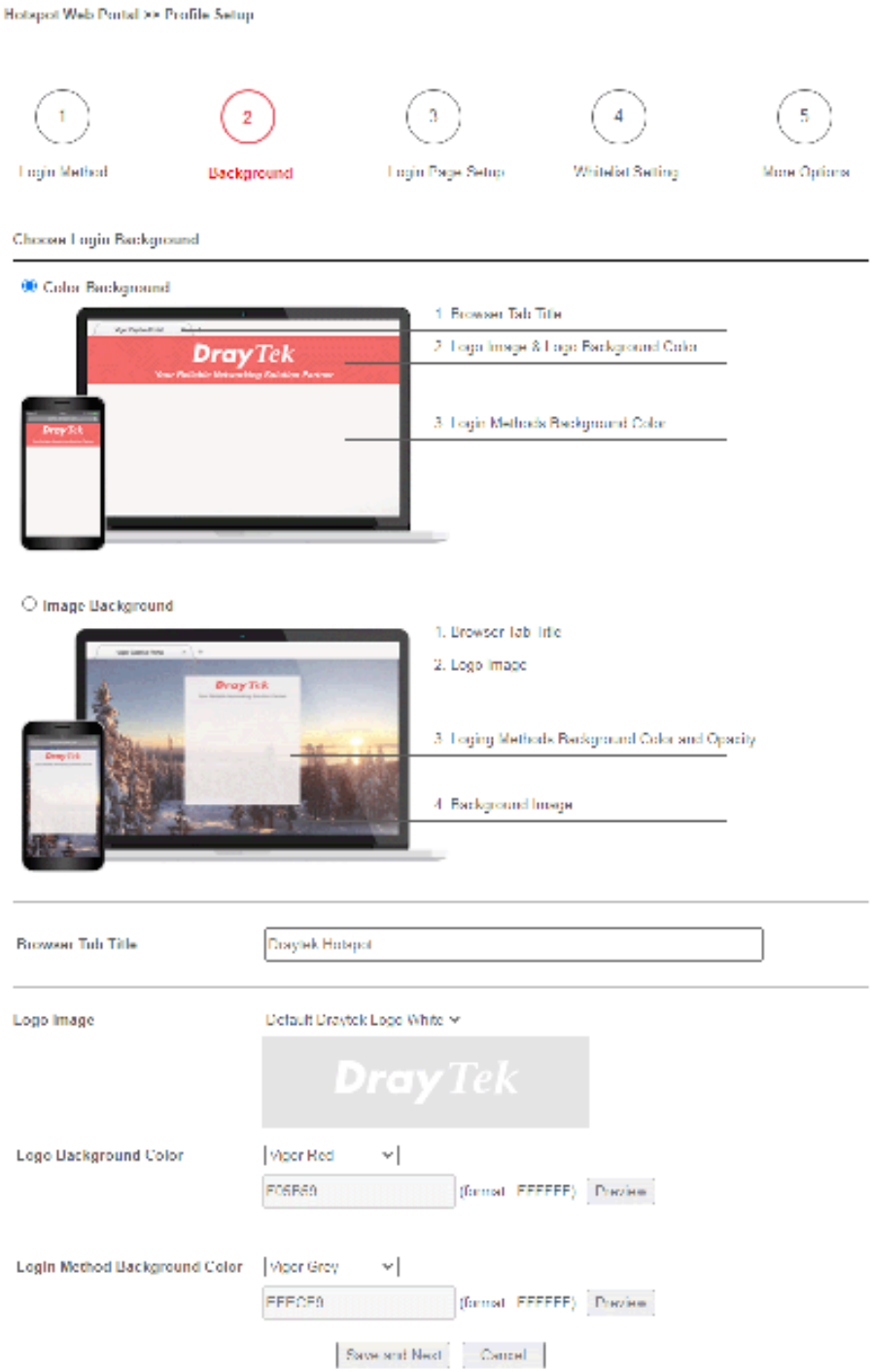
Facebook)	**Facebook APP ID** - Enter a valid Facebook developer app ID. If you do not already have an app ID, refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for instructions on obtaining an APP ID. **Facebook APP Secret** - Enter the secret configured for the APP 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 **Various Hotspot Login** is selected as the portal method. Select one or more desired login methods: **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.
*When **External Portal Server** is selected as Portal Method*	
Redirection URL	Enter the URL to which the client will be redirected.
RADIUS Server	**Authentication Method** - To configure the RADIUS server, click the External RADIUS Server link and you will be presented with the configuration page. **RADIUS MAC Authentication** - If the RADIUS server supports authentication by MAC address, enable **RADIUS MAC Authentication** and select the MAC address format that is used by the RADIUS server. **MAC Address Format** - Select the MAC address format.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to save the configuration on this page and proceed to the next page.

If you have chosen **Skip Login, landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

2 Background

If you have selected a Login Mode that requires authentication, select a background for the login page.



Available settings are explained as follows:

Item	Description
Choose Login Background	Select either **Color Background** or **Image Background** as the login page background scheme.
Browser Tab Title	Enter the text to be shown as the webpage title in the browser.

Logo Image	The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo.
Login Method Background Color	Select the background color of the login panel from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Opacity (10 ~ 100)	Available when **Image Background** is selected. Set the opacity of the background image.
Background Image	Available when Image Background is selected. Click **Browse...** to select an image file (.JPG or .PNG format), then click **Upload** to upload it to the router.
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

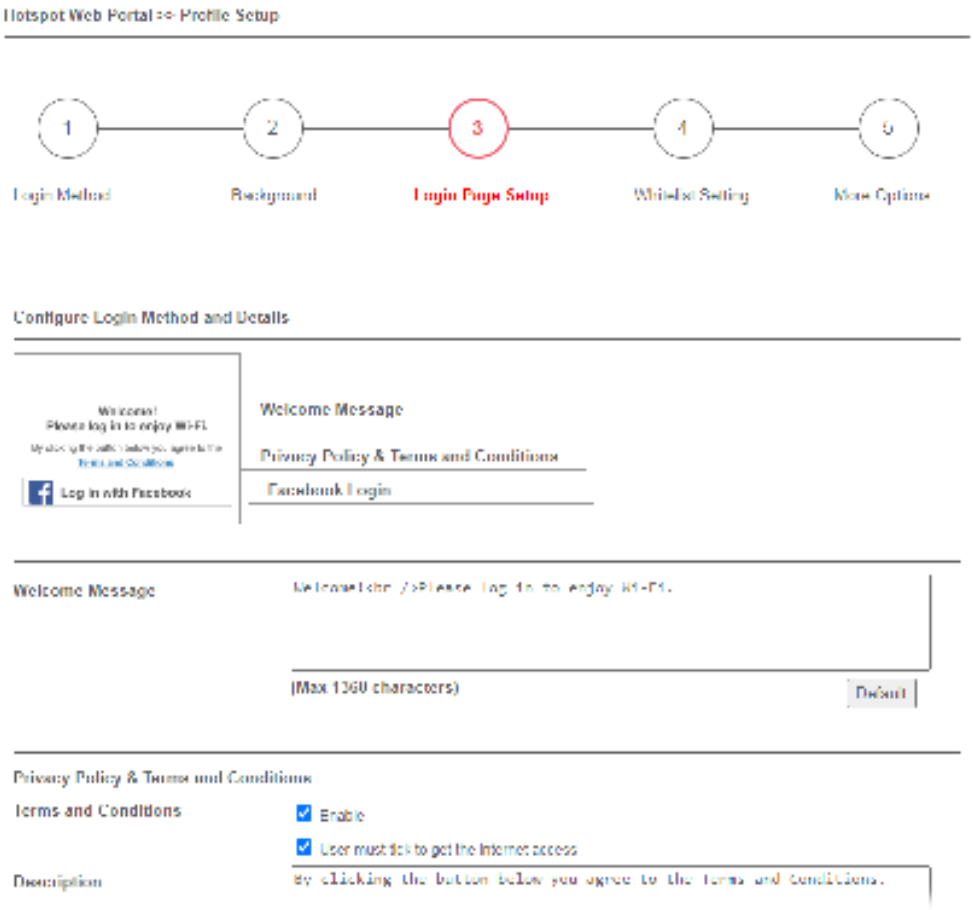
If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup*.

3 Login Page Setup

In this step you can configure settings for the login page.

Click Through

This section describes the Login Page setup if you have selected **Click Through** as the Login Method.



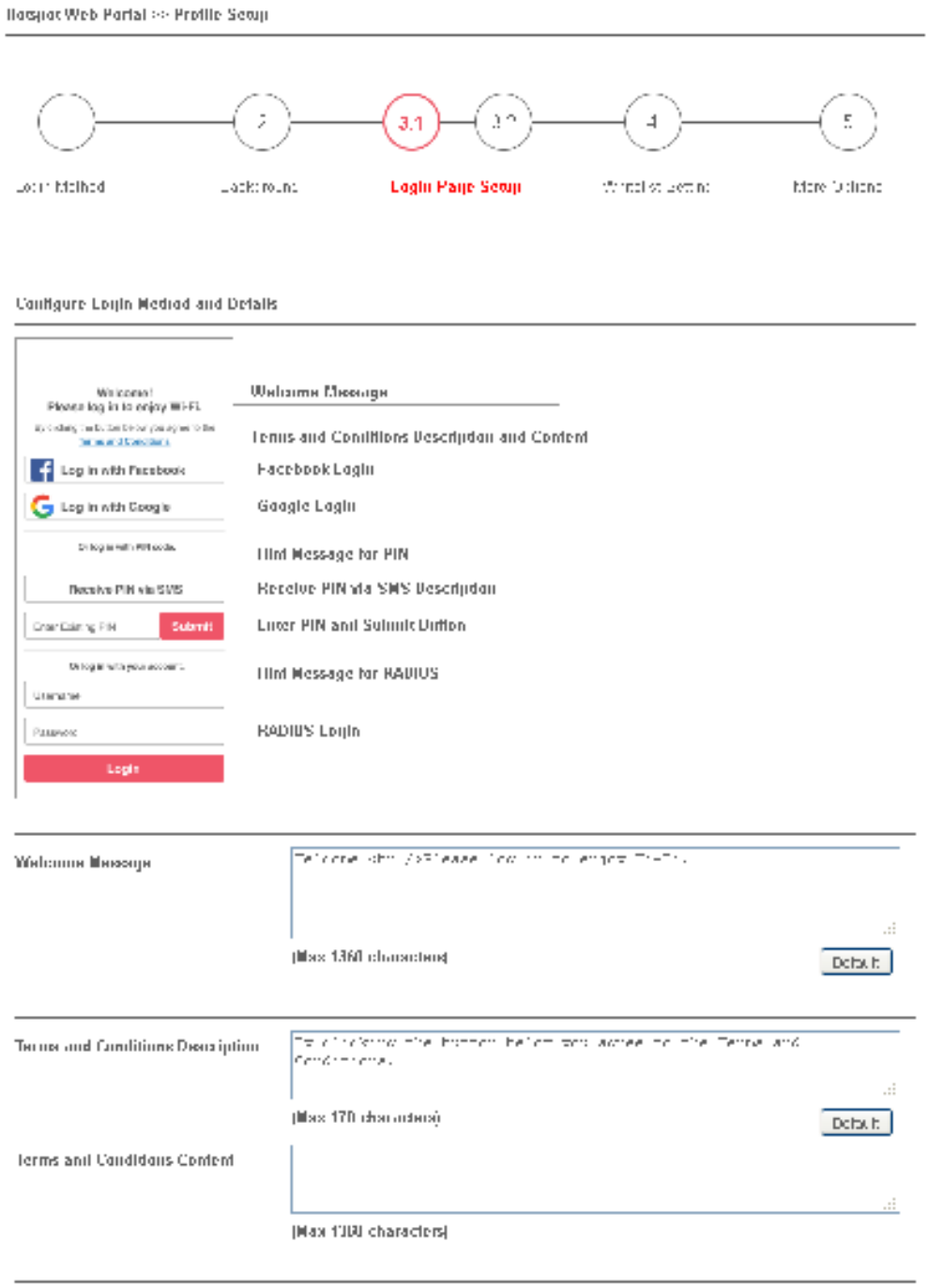
Available settings are explained as follows:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.
Accept Button Description	Enter the text to be displayed on the accept button
Accept Button Color	Select the color of the accept button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.
Save and Next	Click to save the configuration on this page and proceed to the next page.

Cancel	Click to abort the configuration process and return to the profile summary page.

Various Hotspot Login

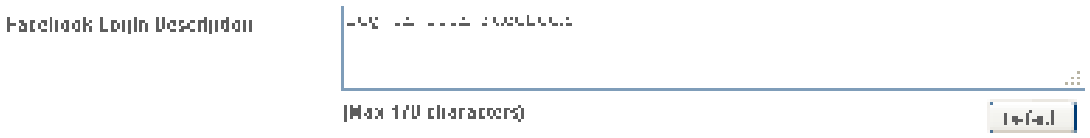
This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).



Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

Item	Description
Welcome Message	Enter the text to be displayed as the welcome message.
Terms and Conditions Description	Enter the text to be displayed as the Terms and Conditions hyperlink text.
Terms and Conditions Content	Enter the text to be displayed in the Terms and Conditions pop-up window.

If you have selected Facebook login, the setting will appear:



Item	Description
Facebook Login Description	Enter the text to be displayed on the Facebook login button.

If you have selected Google login, the setting will appear:

Item	Description
Google Login Description	Enter the text to be displayed on the Google login button.

If you have selected PIN login, these settings will appear:

Item	Description
Hint Message for PIN	Enter the text used to suggest users to choose SMS authentication.
Receiving PIN via SMS Description	Enter the text to be displayed on the button that the user clicks to receive an SMS PIN.
Receiving PIN via SMS Content	Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message.
Enter PIN Description	Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN.
Submit Button Description	Enter the text to be displayed on the submit PIN button
Submit Button Color	Select the color of the submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

If you have selected RADIUS account login, these settings will appear:

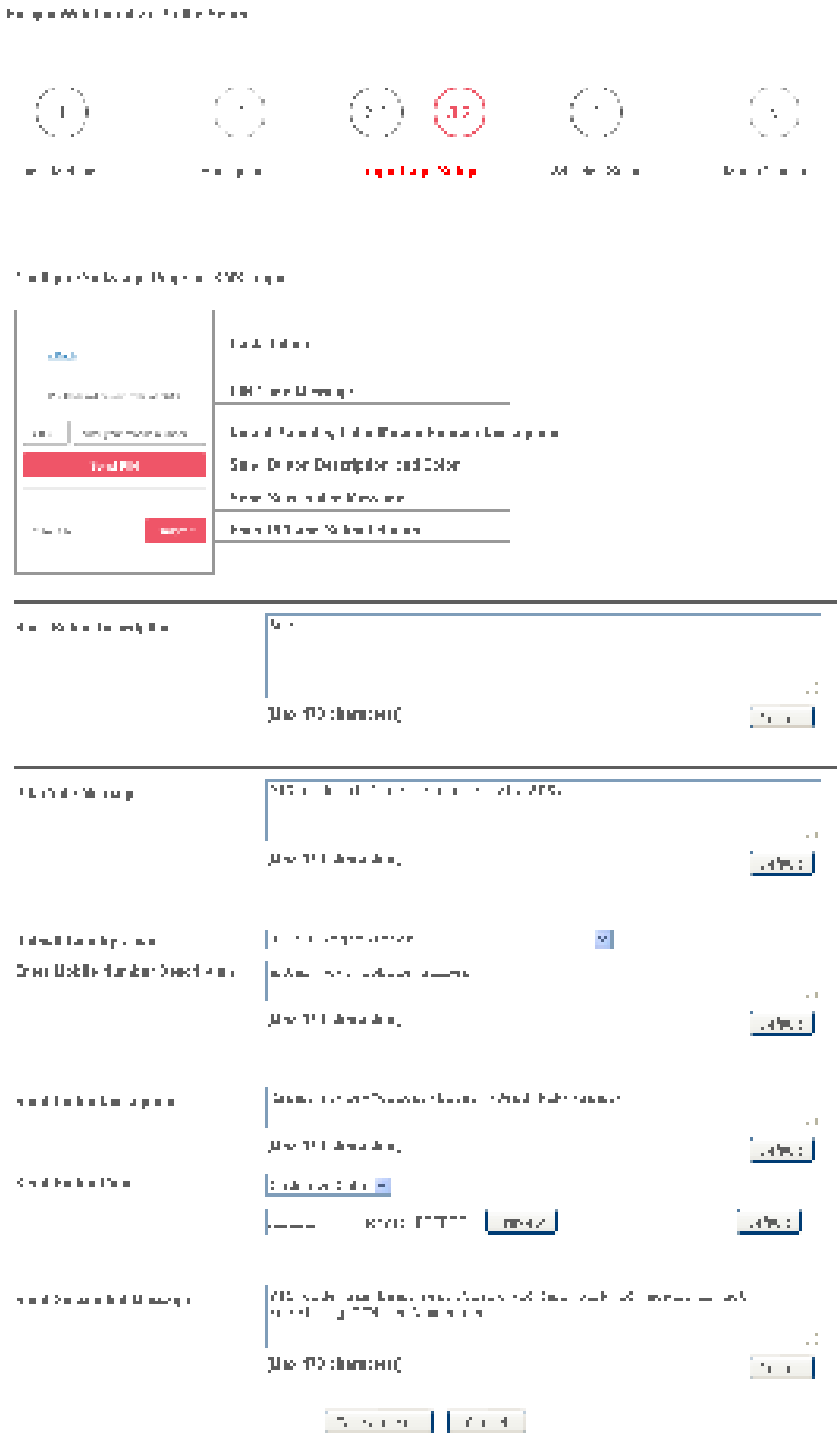
Item	Description
Hint Message for RADIUS	Enter the text used to prompt the user to login.
RADIUS Account Description	Enter the text to prompt the user to enter the username.
RADIUS Password Description	Enter the text to prompt the user to enter the password.
Login Button Description	Enter the text to be displayed on the login button.
Login Button Color	Select the color of the login button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color.

And finally, the save and cancel buttons are always displayed.

Item	Description
Save and Next	Click to save the configuration on this page and proceed to the next page.
Cancel	Click to abort the configuration process and return to the profile summary page.

2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login method, you will also need to configure the page that is displayed to users when they request a PIN.



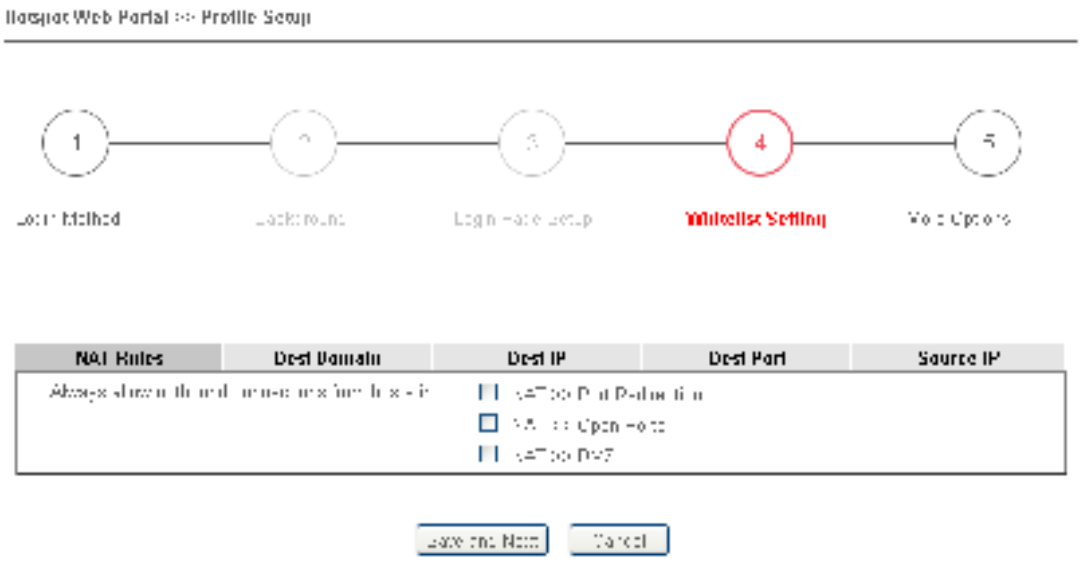
Available settings are explained as follows:

Item	Description
Back Button Description	Enter text for the label of the hyperlink to return to the previous page.
PIN Code Message	Enter text to be displayed as the body text on the page.
Default Country	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.

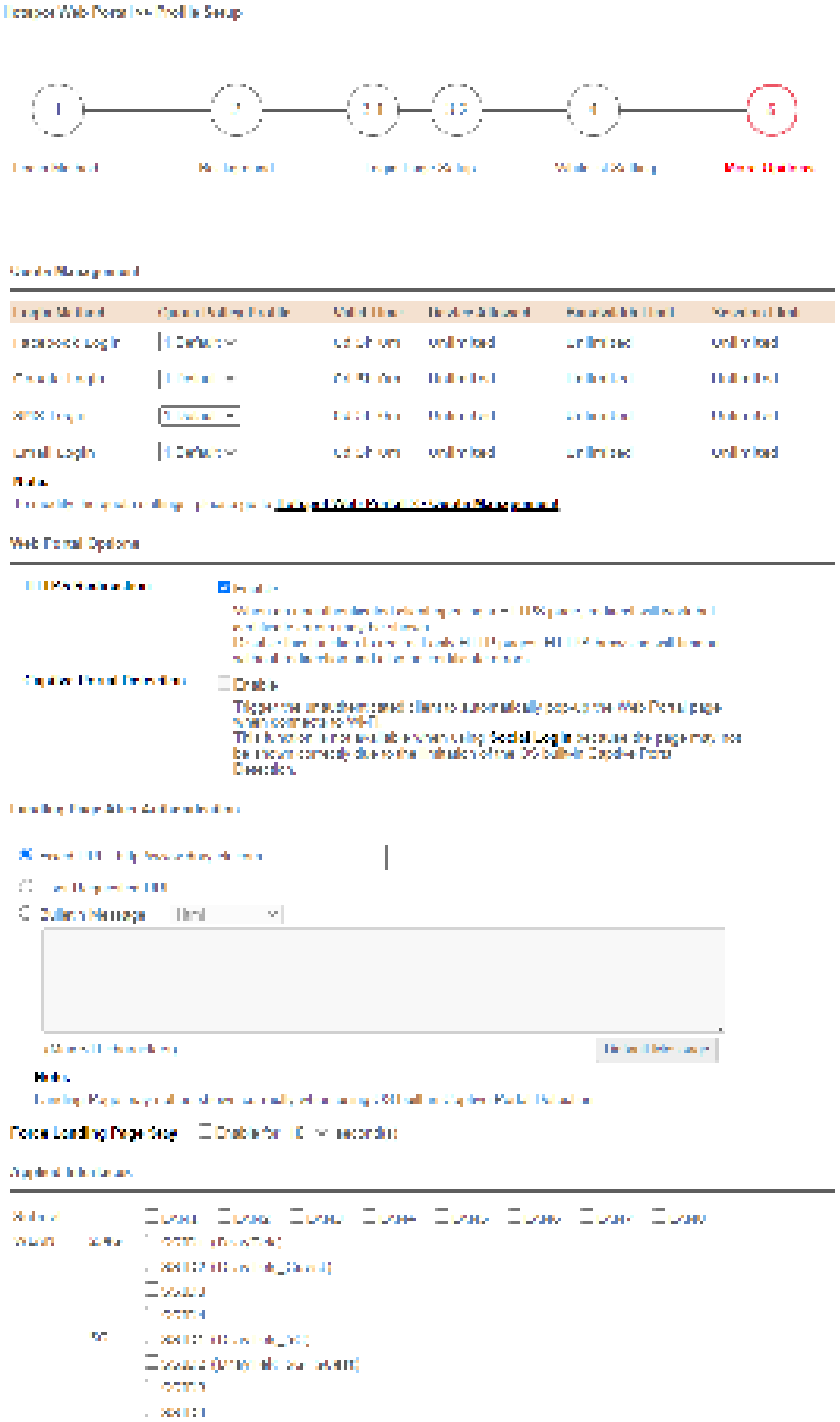


Available settings are explained as follows:

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	
Expired Time After Activation	Enter the time duration that users are allowed to have Internet access after logging in.

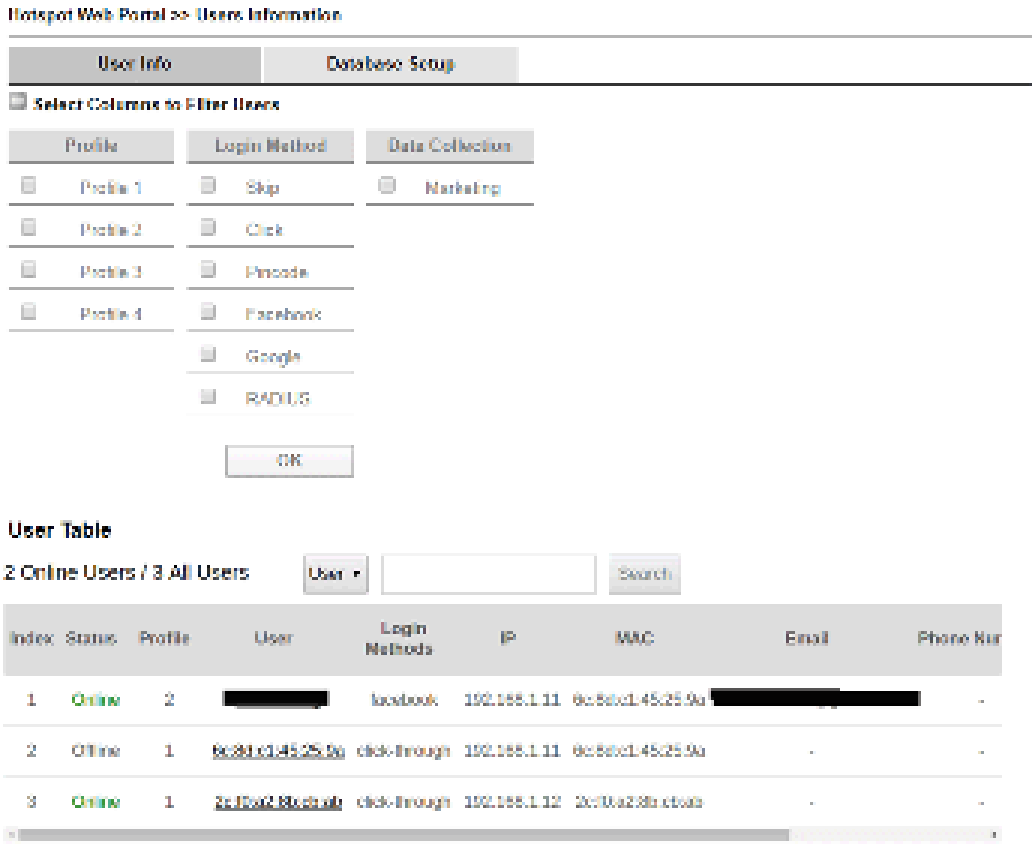
Quota Policy Profile	Choose a policy profile to apply to web portal clients.
Web Portal Options	
HTTPS Redirection	If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option 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.
Landing Page After Authentication	
Fixed URL	Specifies the webpage that will be displayed after the user has successfully authenticated. The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.
User Requested URL	The user will be redirected to the URL they initially requested.
Bulletin Message	The message configured here will be briefly shown for a few seconds to the user. **Default Message** – This button is enabled when **Bulletin Message** is selected. Click to load the default text into the bulletin message textbox.
Applied Interfaces	
Subnet	The current Hotspot Web Portal profile will be in effect for the selected subnets.
WLAN	The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs.
Finish	Click to complete the configuration.
Cancel	Click to abort the configuration process and return to the profile summary page.

VI-3-2 User Information

This page displays information of users accessing the Internet through the web portal. Clicking on a user link will open a new window that shows detailed information about that user.

VI-3-2-1 User Info

You may choose to limit the displayed user information by adding profile or login method filters.



Available settings are explained as follows:

Item	Description
Select Columns to Filter Users	Select the profiles and the login methods to filter the displayed users. This is useful when there are a lot of users and you want to manage only a subset of users based on their profiles and/or login methods.
User Table	Details of users accessing the Internet via Hotspot Web Portal will be displayed in this section.

Click the MAC address (or pincode, facebook/google name, RADIUS account) link for a particular user and detailed information on the selected device will be shown in the following page.

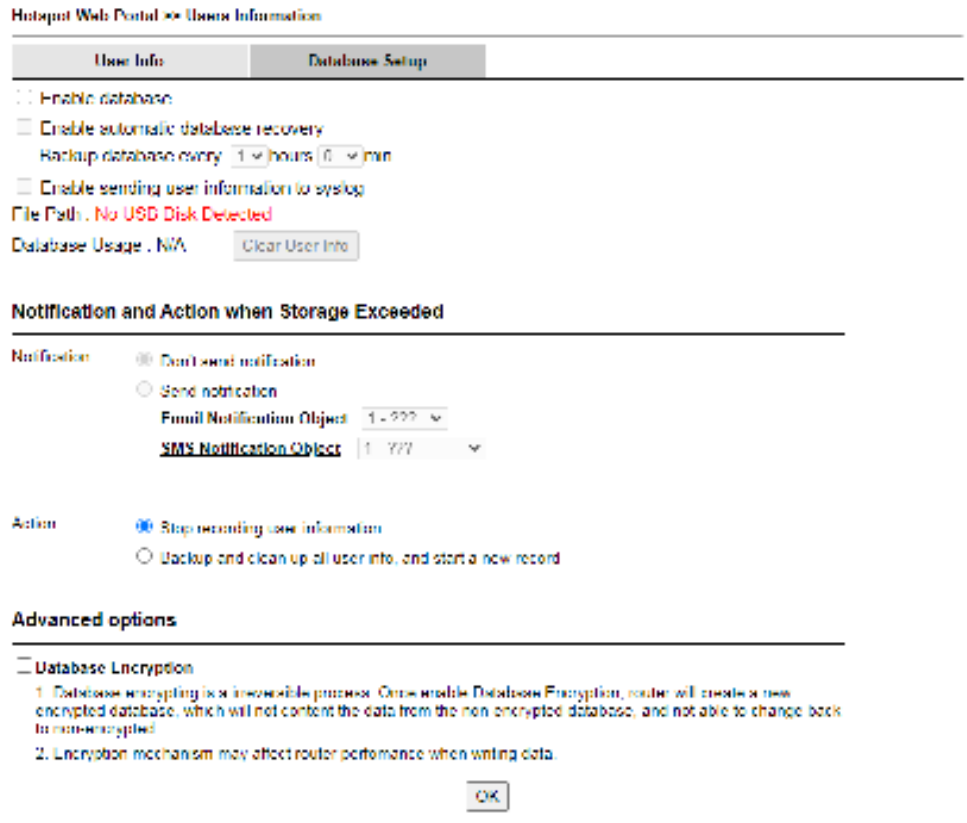
Information about the user is shown under the Login Info section.

Devices used by the user are shown under the Devices section. To forcibly log out a device, select the checkbox in front of the device and click the Log Out Device button.

The Login History section shows the 10 most recent login sessions of the user.

VI-3-2-2 Database Setup

This page allows the user to configure settings for database on USB disk.



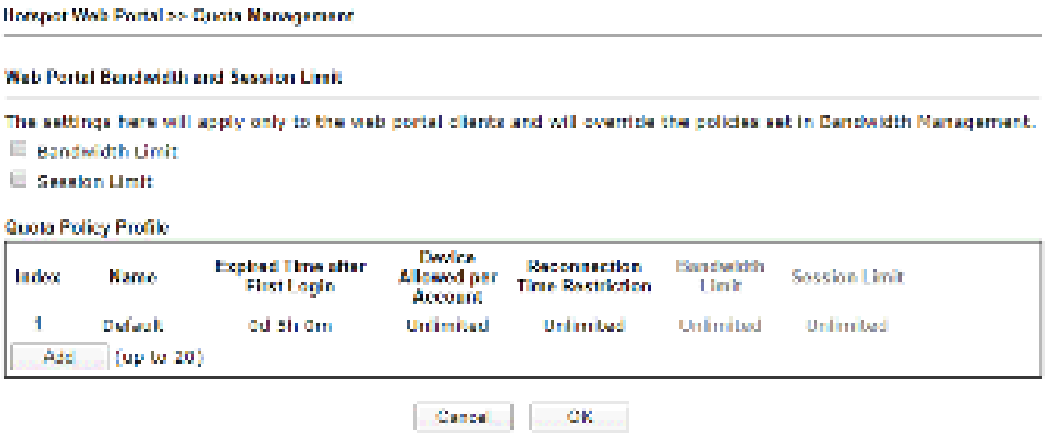
Available settings are explained as follows:

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 automatic database recovery	Check the box to enable the functionality of the database recovery on the USB disk. **Backup database every**... - Set the interval to backup the database.
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 not 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.

VI-3-3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

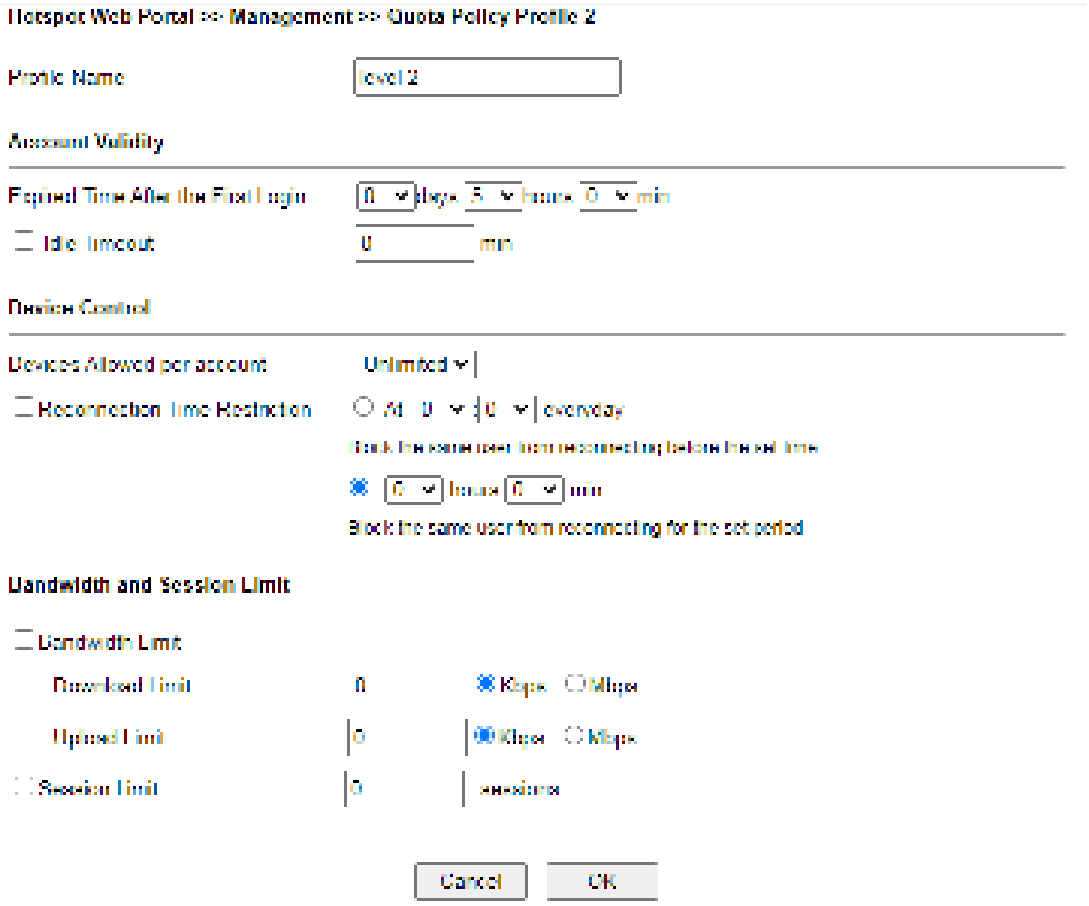
Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.



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.

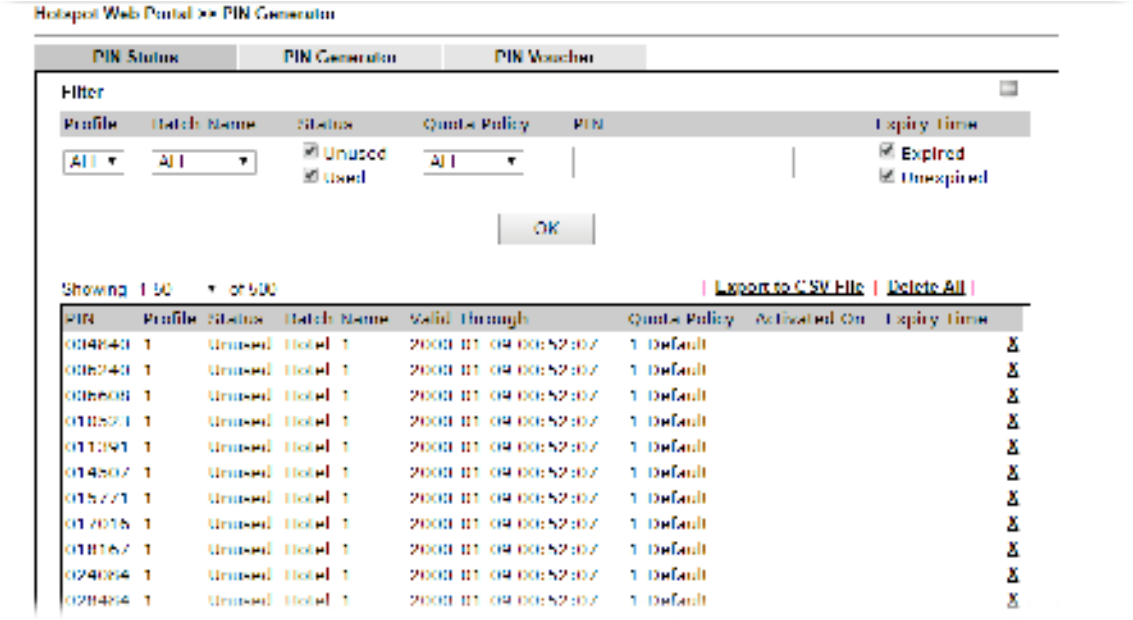
After finishing all the settings here, please click **OK** to save the configuration.

VI-3-4 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.

VI-3-4-1 PIN Status

This page displays the PIN codes generated by PIN Generator.

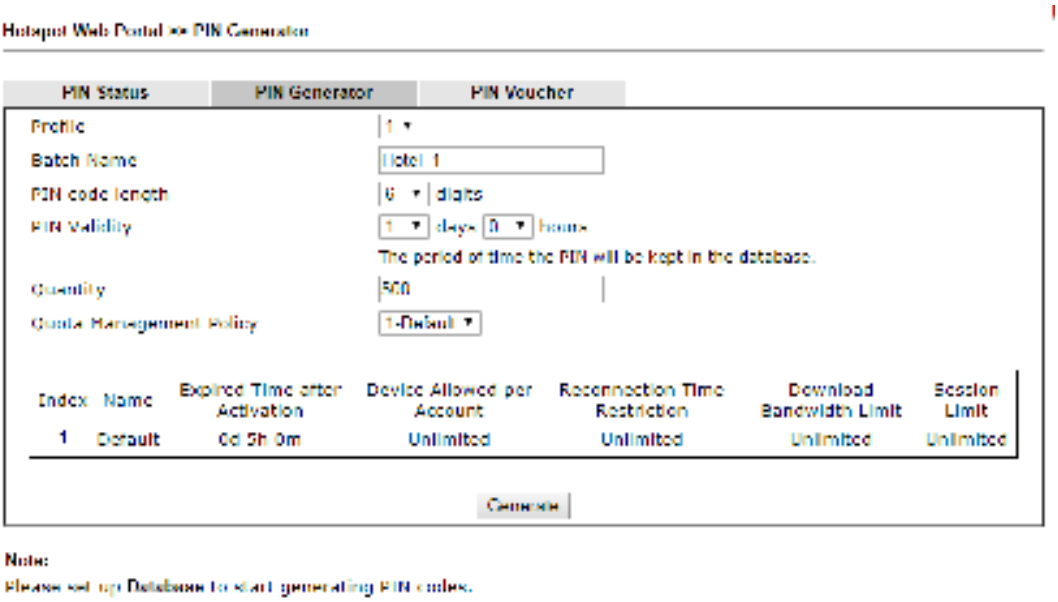


Available settings are explained as follows:

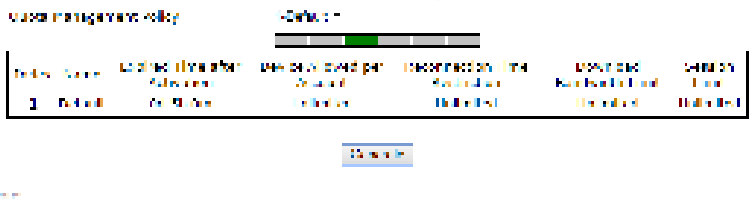
Item	Description
Profile	Use the drop down menu to choose an index number (1 to 4) for PIN generator profile.
Batch Name	Use the drop down menu to choose an existed PIN profile or choose ALL to display the PIN status.
Status	**Unused** - After checking the box, only the unused PIN codes will be shown 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.

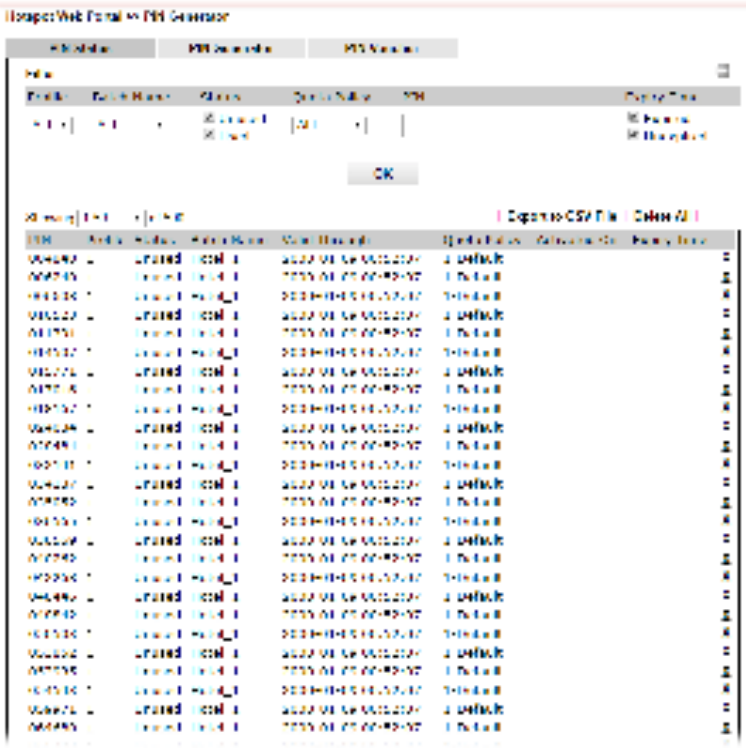
VI-3-4-2 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.



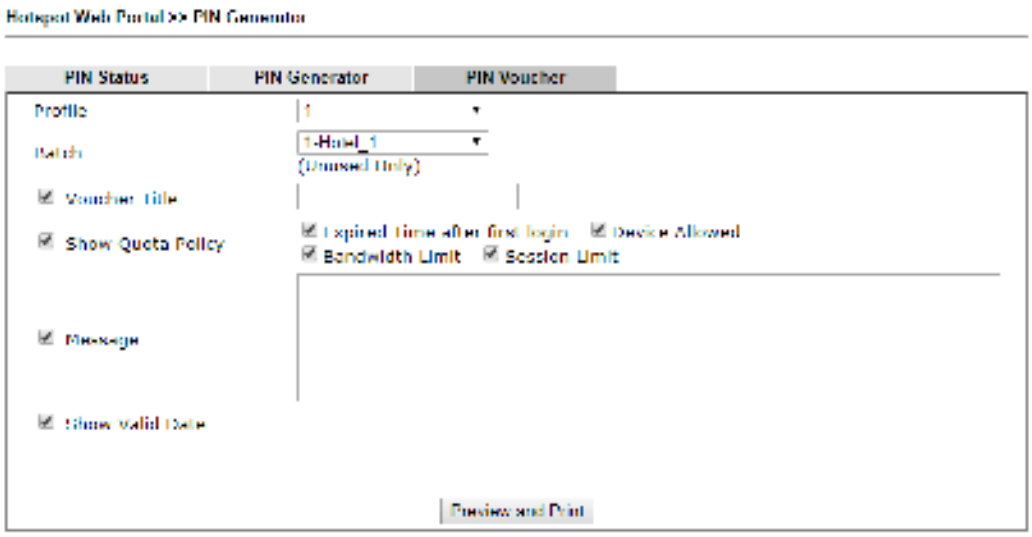
Available settings are explained as follows:

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.

VI-3-4-3 PIN Voucher

This page allows to print out the PIN code list.



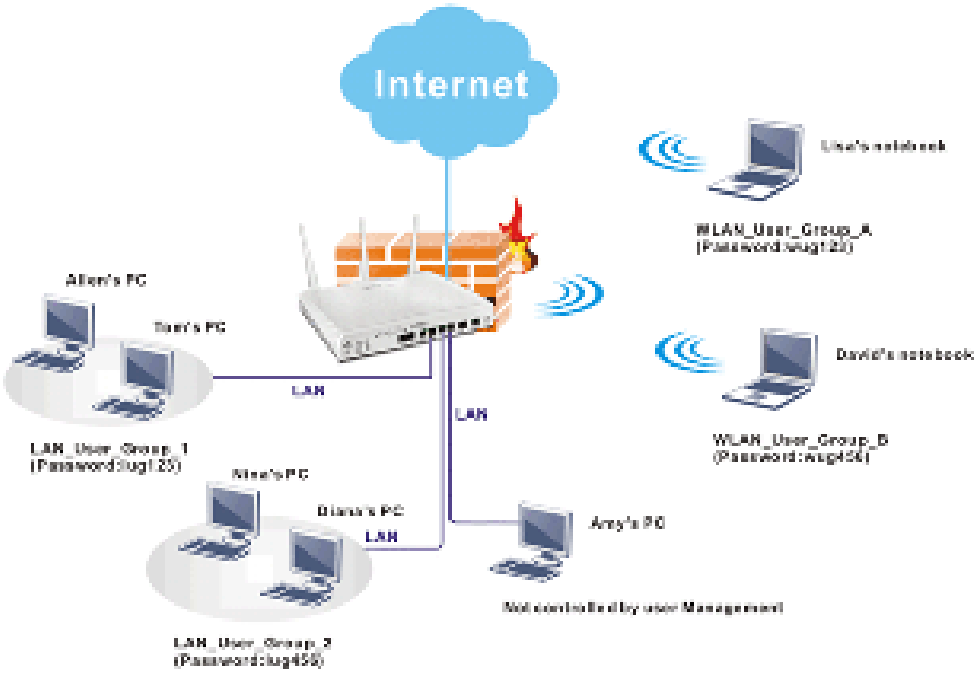
Available settings are explained as follows:

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	Choose 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.
Preview and Print	Click it to display the PIN code list. This list can be printed out if required.

VI-4 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.



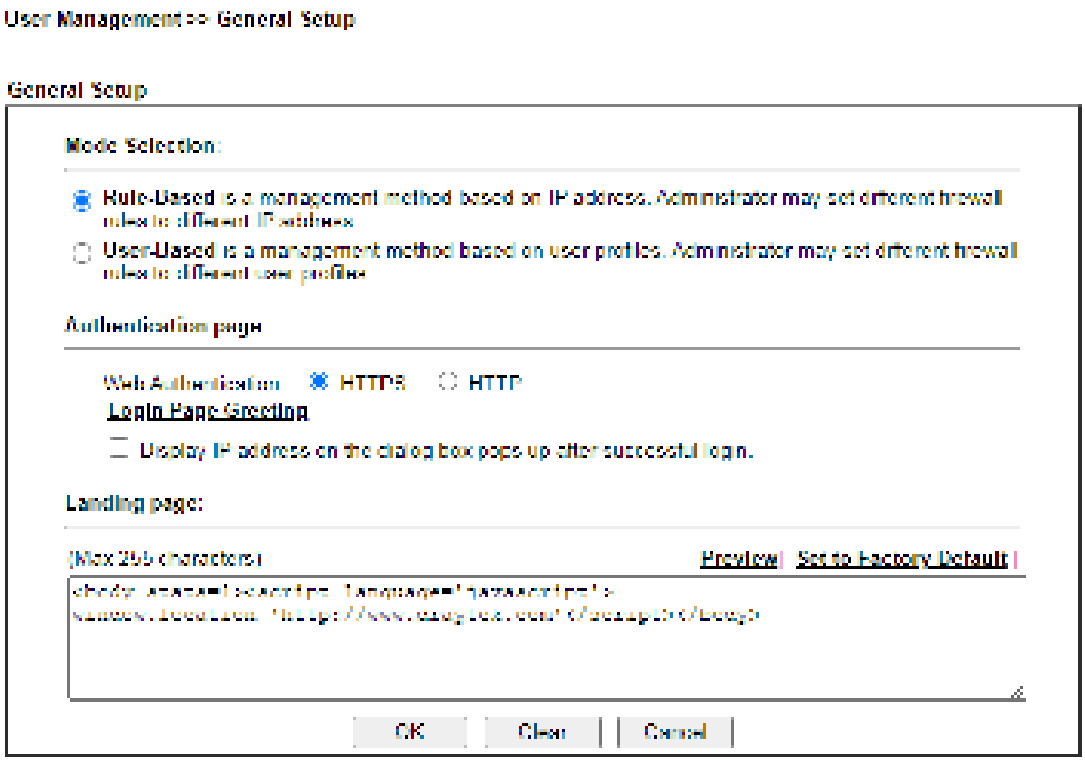
Info

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

VI-4-1 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:

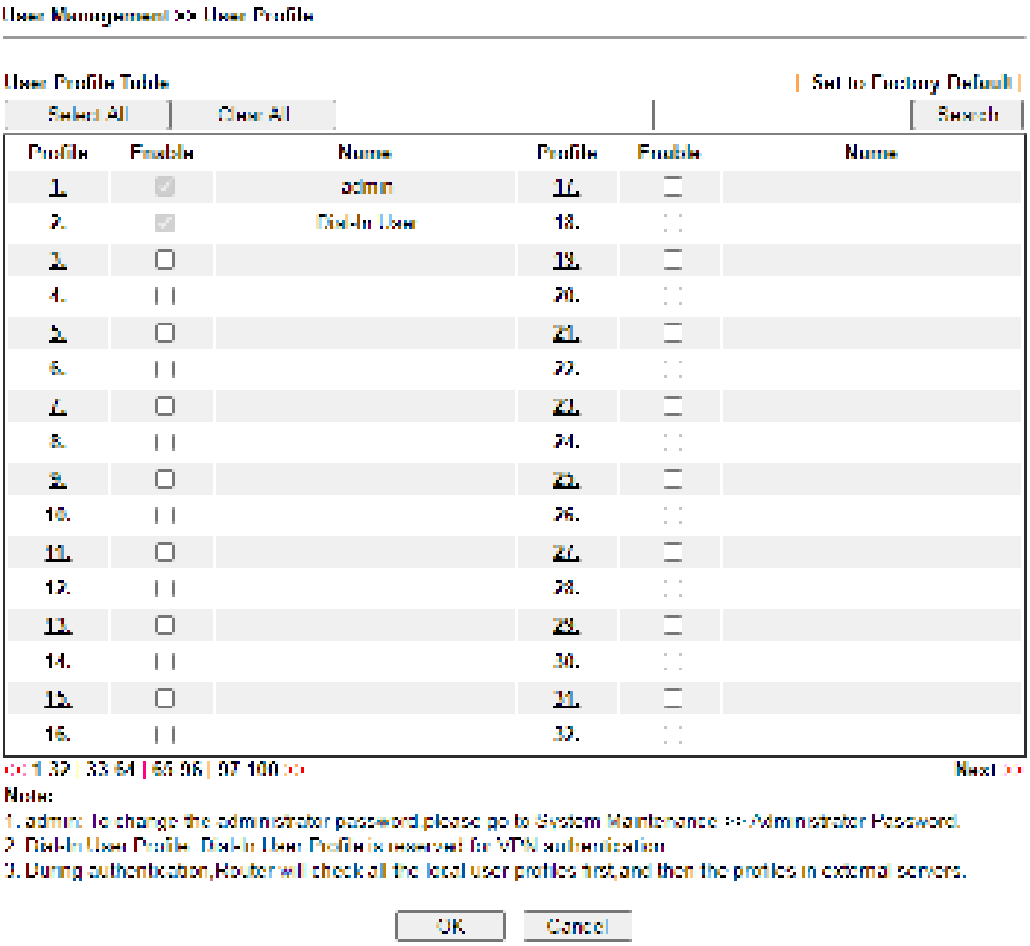
Item	Description
Mode Selection	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved. **User-Based** - If you choose such mode, the router will apply the filter rules configured in **User Management>>User Profile** to the users. **Rule-Based** –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	Enter the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

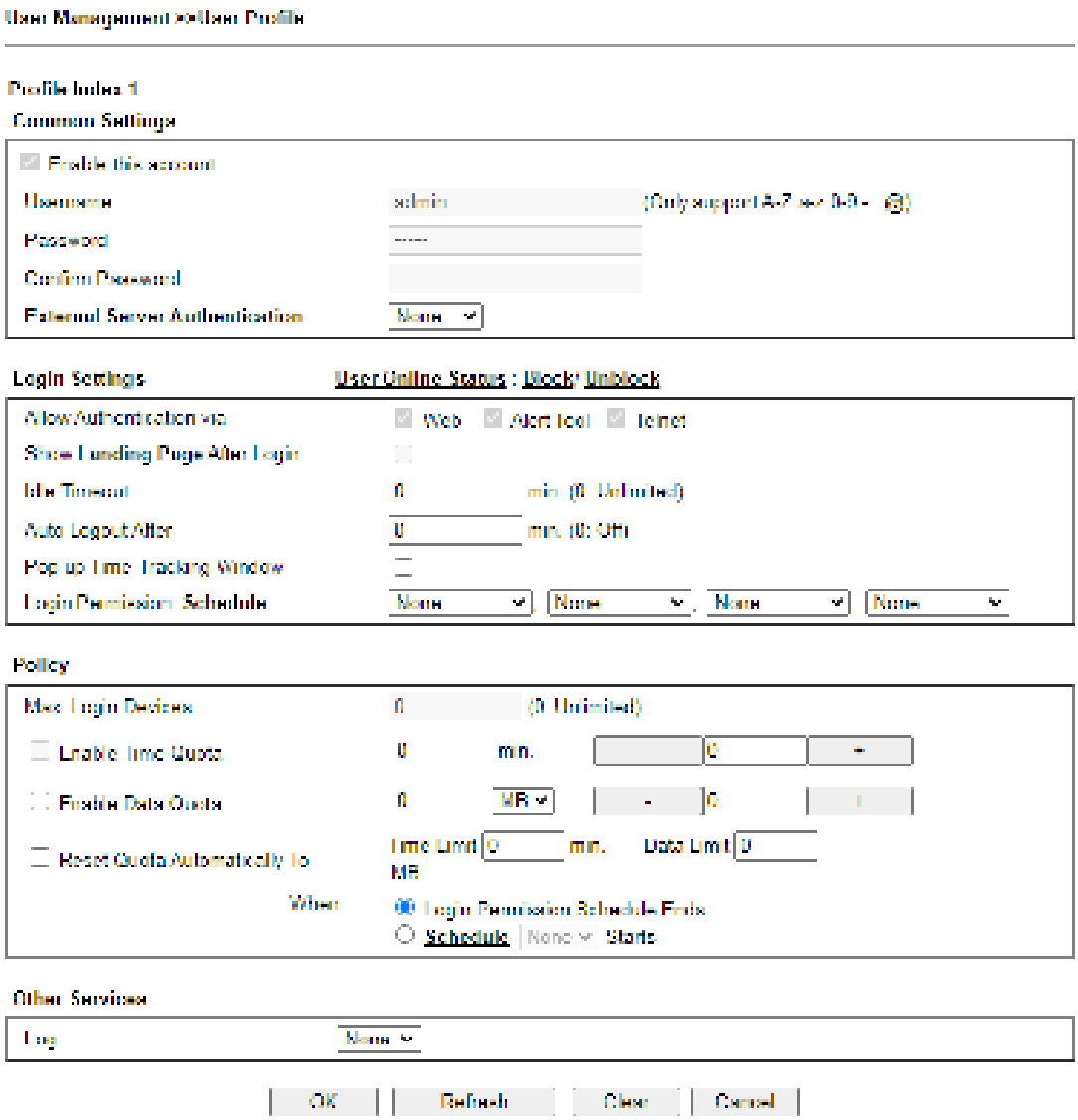
After finishing all the settings here, please click **OK** to save the configuration.

VI-4-2 User Profile

This page allows you to set customized profiles (up to 100) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile**.



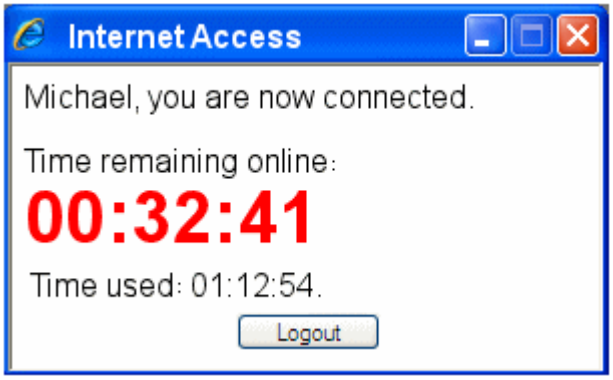
To set the user profile, please click any index number link to open the following page. Notice that profile 1 (**admin**) and profile 2 **(Dial-In User)** are factory default settings. Profile 2 is reserved for future use.

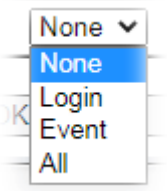


Available settings are explained as follows:

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 Enter 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 Enter 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	Enter 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 Enter the URL of the router from any browser. Then, a login window will be popped up and ask the user to Enter 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 Enter 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 Enter four sets of time schedule for your request. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.
Policy	
Max. Login Devices	Such profile can be used by many users. You can set the

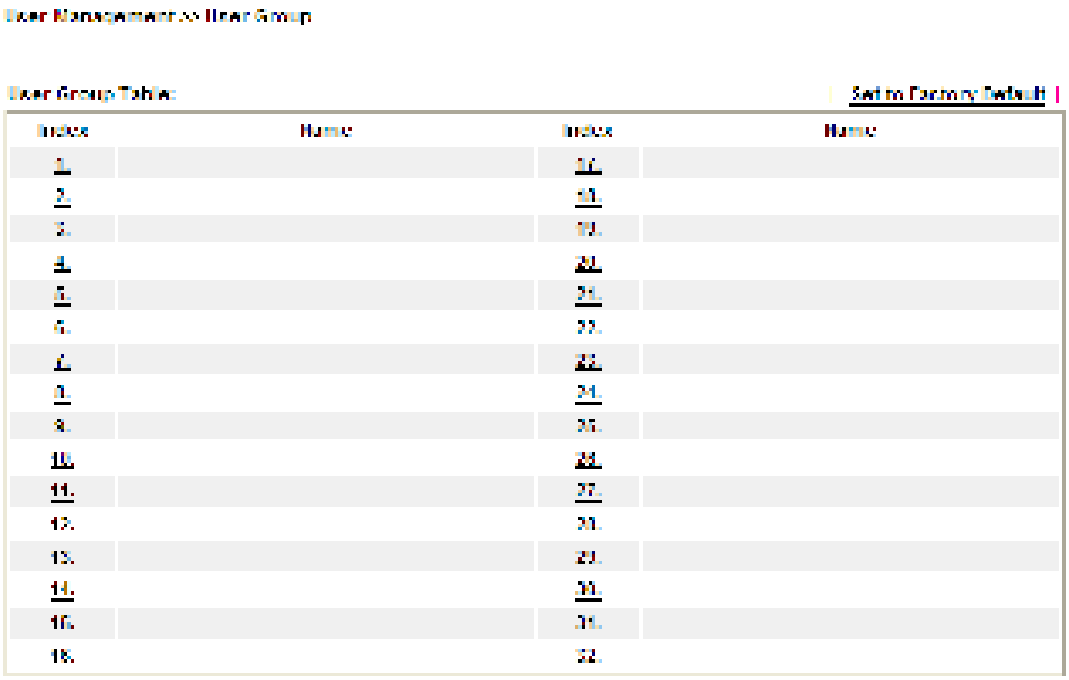
	limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
Enable Time Quota	Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to Enter 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 Automatically	Check the box to set default time quota and data quota for such profile. Vigor router will reset the quota automatically according to the factory quota settings. **Time Limit** –Enter the value for the time manually. **Data Limit** –Enter 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.
Other Services	
Log	Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the

	log items to take down relational records for the user(s). 

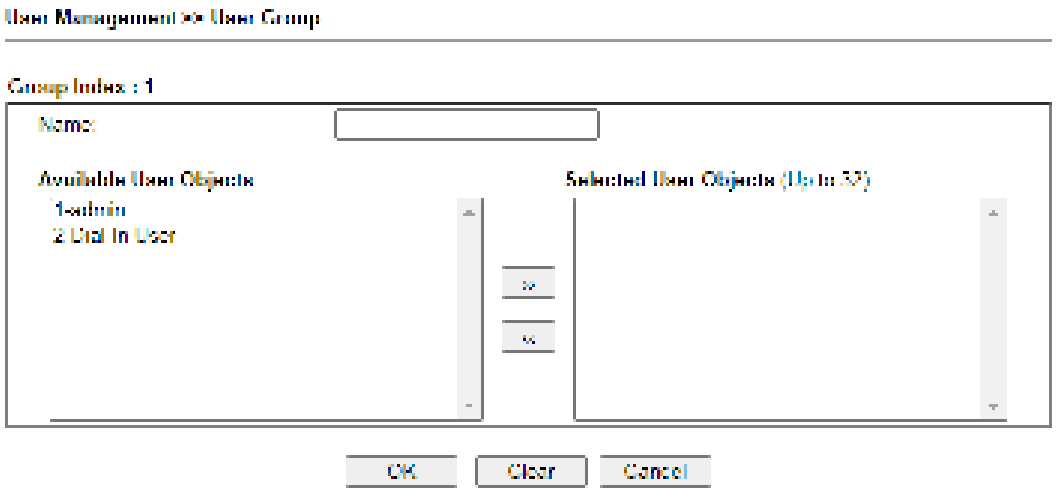
After finishing all the settings here, please click **OK** to save the configuration.

VI-4-3 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:

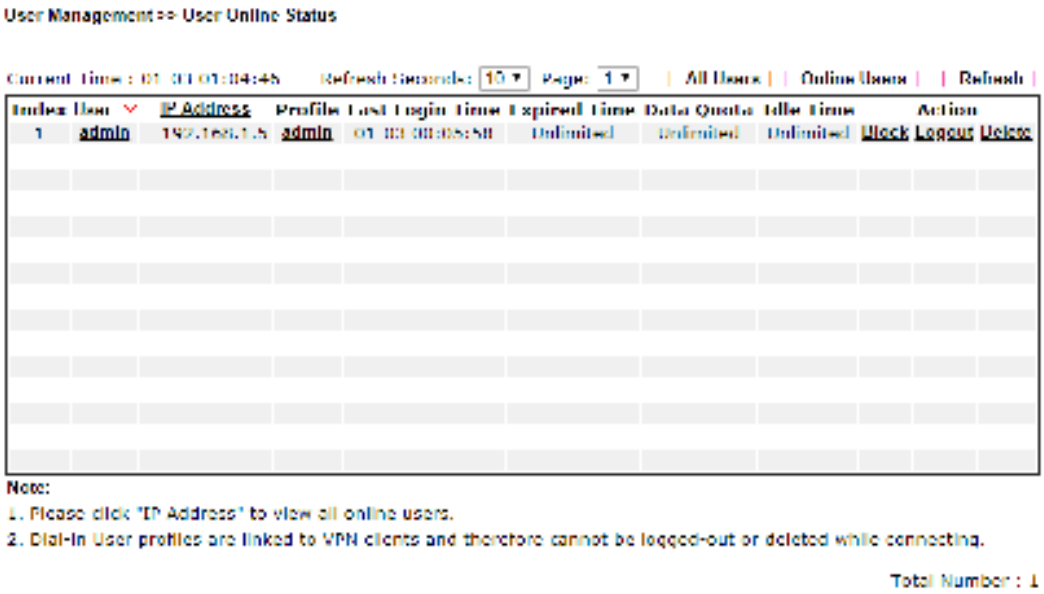
Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from **User Profile** page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory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

VI-4-4 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:

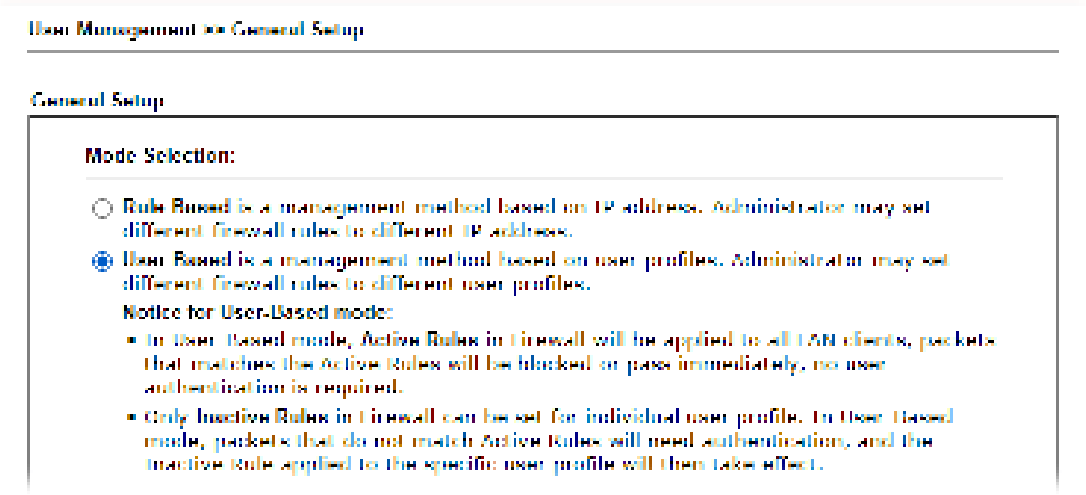
Item	Description
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
User	Display the users which connect to Vigor router 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. **Delete** – Removes the user entry from the User Online Status page.

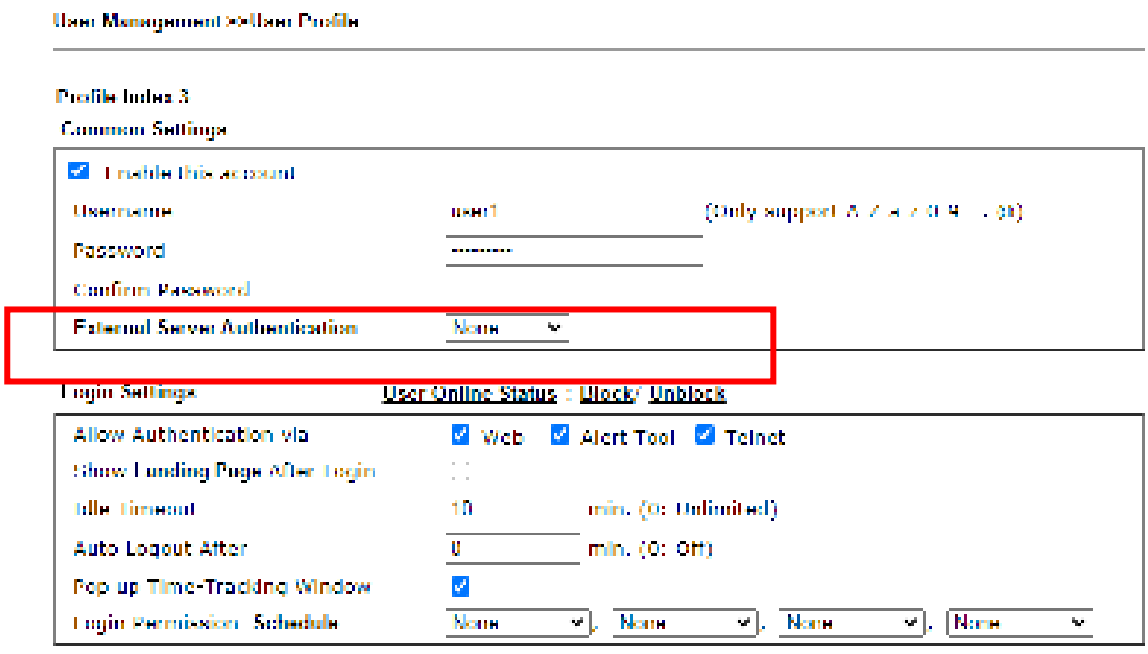
Application Notes

A-1 How to authenticate clients via User Management

Before using the function of User Management, please make sure **User-Based** has been selected as the **Mode** in the **User Management>>General Setup** page.



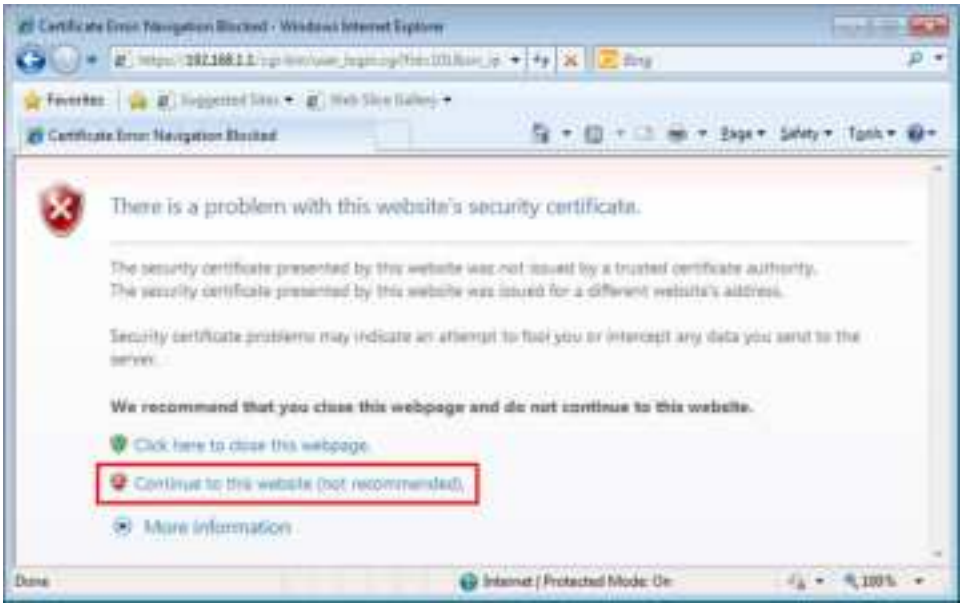
With **User Management** authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: **Web**, **Telnet** and **Alert Tool**.



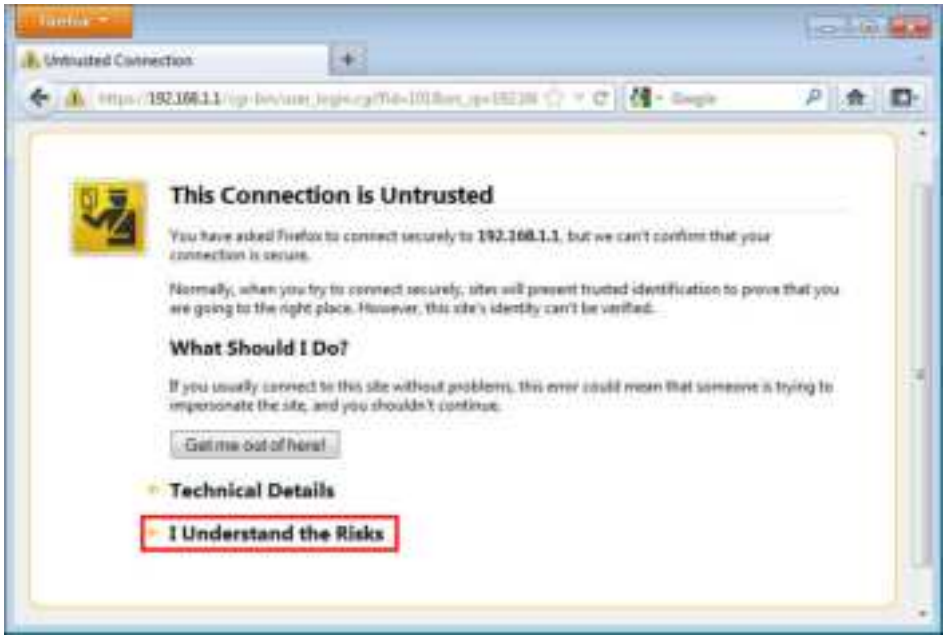
Authentication via Web

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

- With Microsoft Internet Explorer, you may get the following warning message. Please press **Continue to this website (not recommended)**.

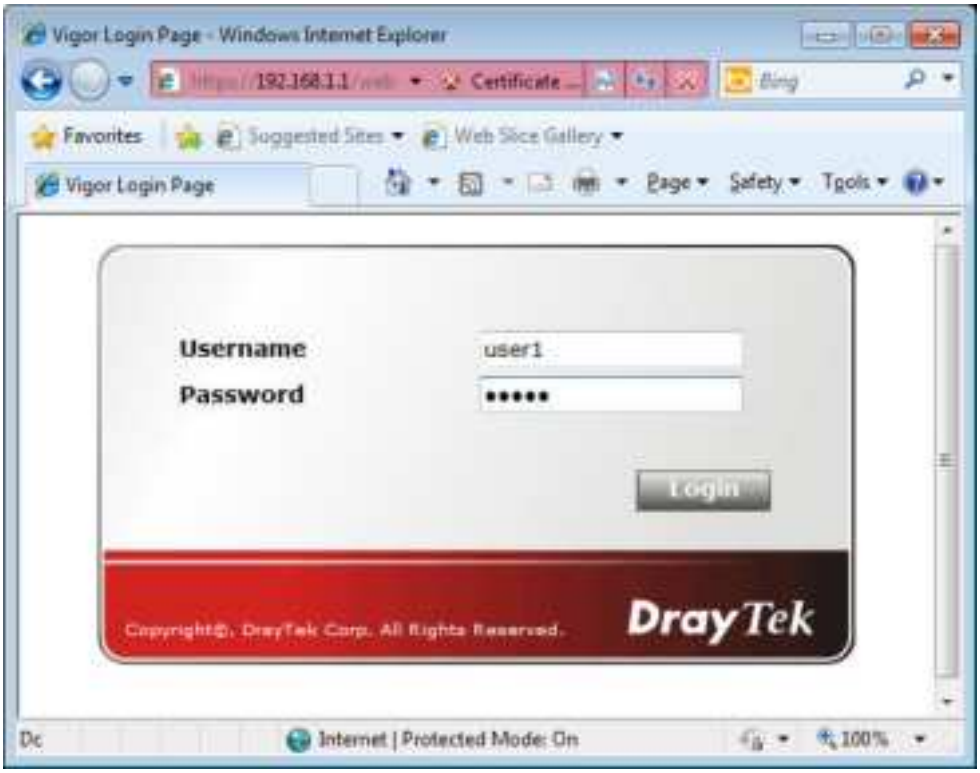


- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.

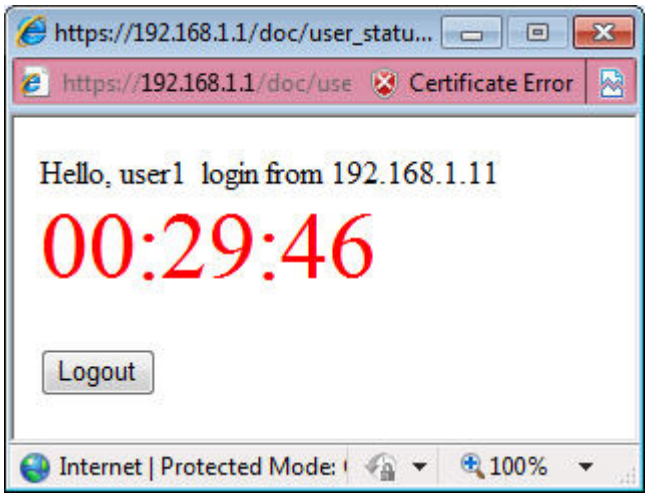


- With Chrome browser, you may get the following warning. Click **Proceed anyway**.

After that, the web authentication window will appear. Input the user name and the password for your account (defined in **User Management**) and click **Login**.

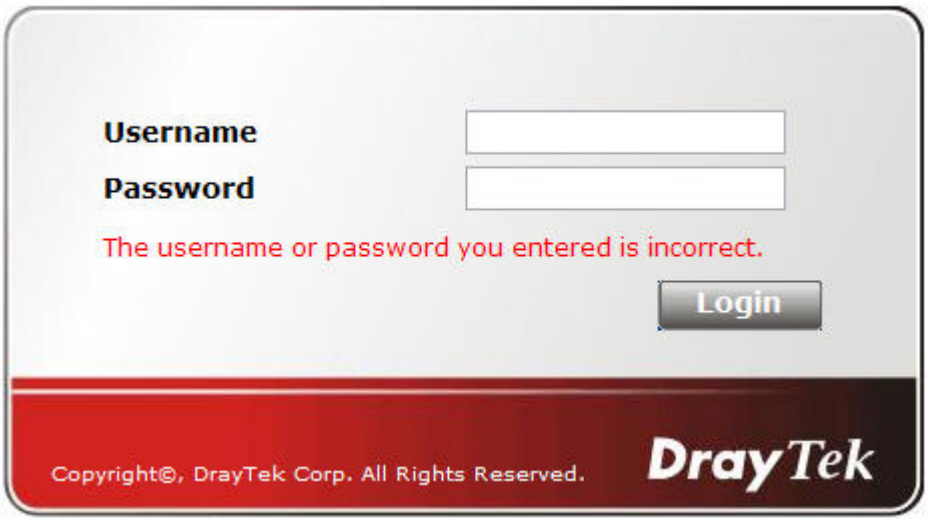


If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



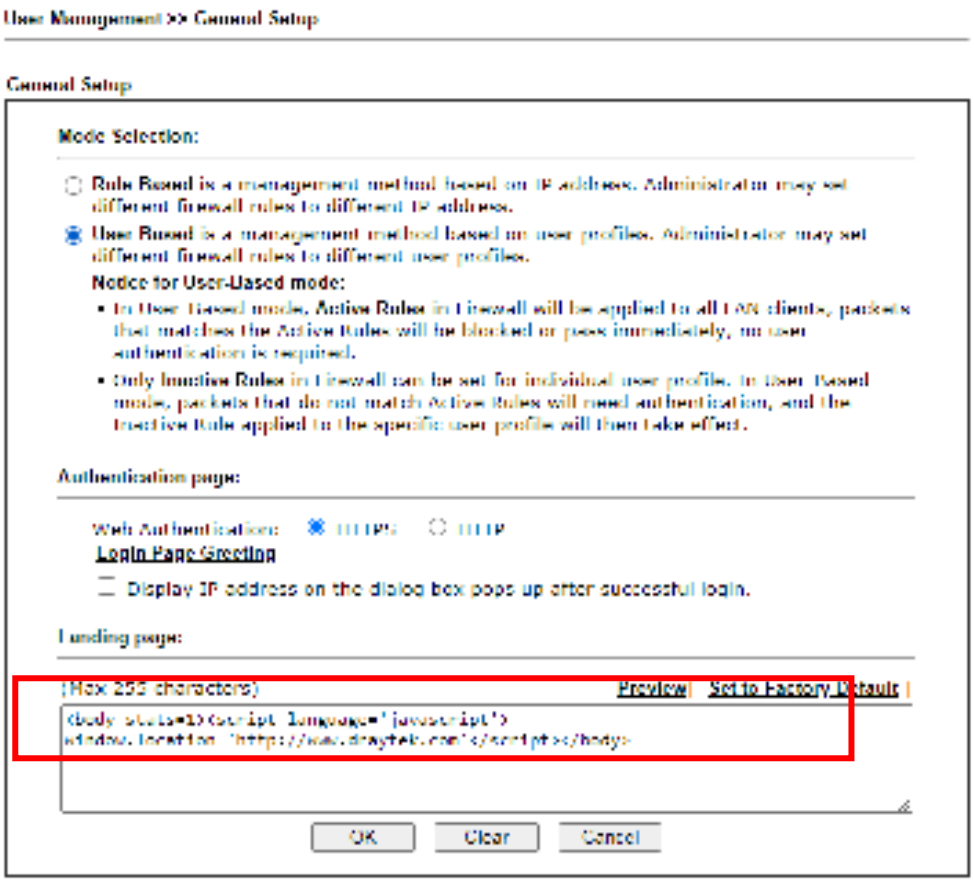
Note, if you block the web browser to pop up any window, you will not see such window.

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

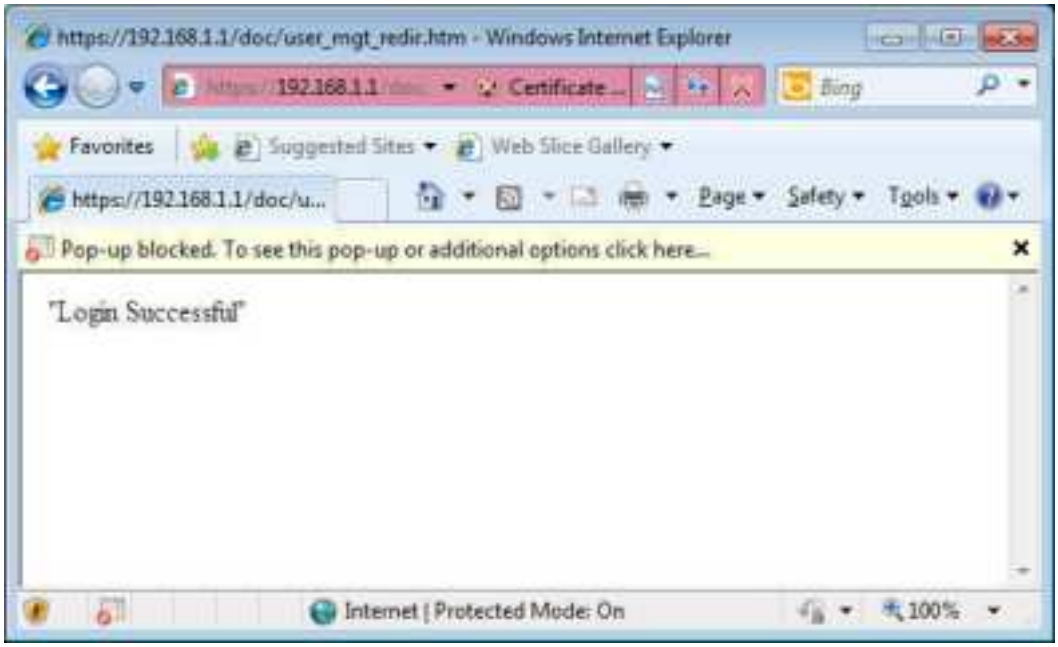


- In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address,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

  If the authentication is successful, you will get the **Welcome Message** that is set in the **User Management >> General Setup** page.



With the default setup **<body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body>,** you will be redirected to http://www.draytek.com . You may change it if you want. For example, you will get the following welcome message if you enter **Login Successful** in the **Welcome Message** table.

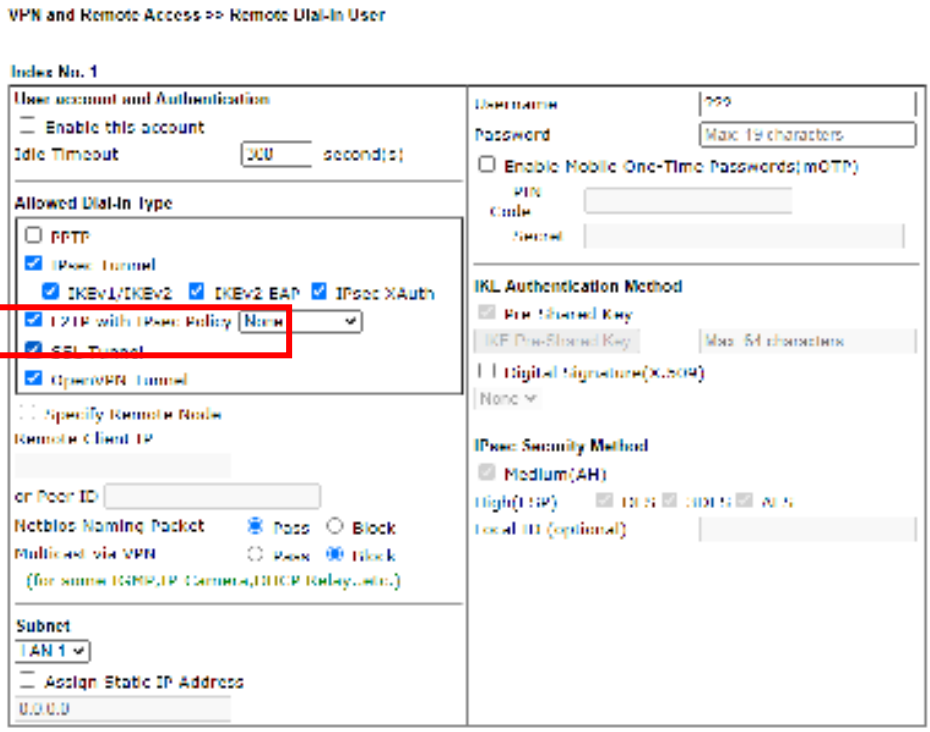


Also you will get a **Tracking Window** if you don't block the pop-up window.

- Don't setup a user profile in **User Management** and a VPN Remote Dial-in user profile with the same Username. Otherwise, you may get unexpected result. It is because the VPN Remote Dial-in User profiles can be extended to the User profiles in User Management for authentication.

There are two different behaviors when a User Management account and a VPN profile share the same Username:

- If **SSL Tunnel** or **SSL Web Proxy** is enabled in the VPN profile, the user profile in User Management will always be invalid for Web authentication. For example, if you create a user profile in User Management with **chaochen**/**test** as username/password, while a VPN Remote Dial-in user profile with the same username "chaochen" but a different password "1234", you will always get error message **The username or password you entered is incorrect** when you use **chaochen**/**test** via Web to do authentication.



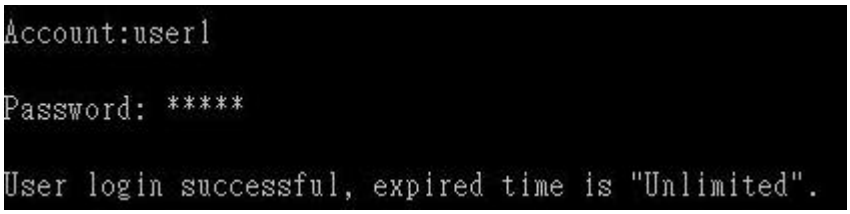
- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

Authentication via Telnet

The LAN clients can also authenticate their accounts via telnet.

1. Telnet to the router's LAN IP address and input the account name for the authentication:

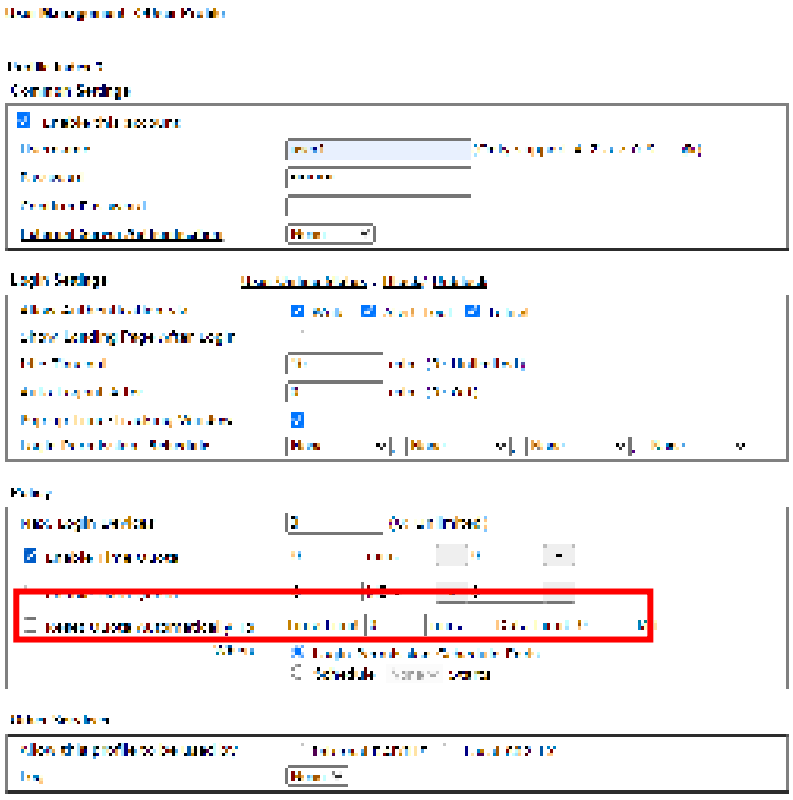
2. Enter the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).



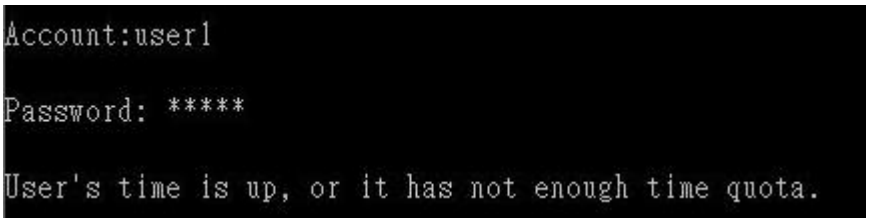
Info

Here expired time is "Unlimited" means the Time Quota function is not enabled for this account. After login, this account will not be expired until it is logout.

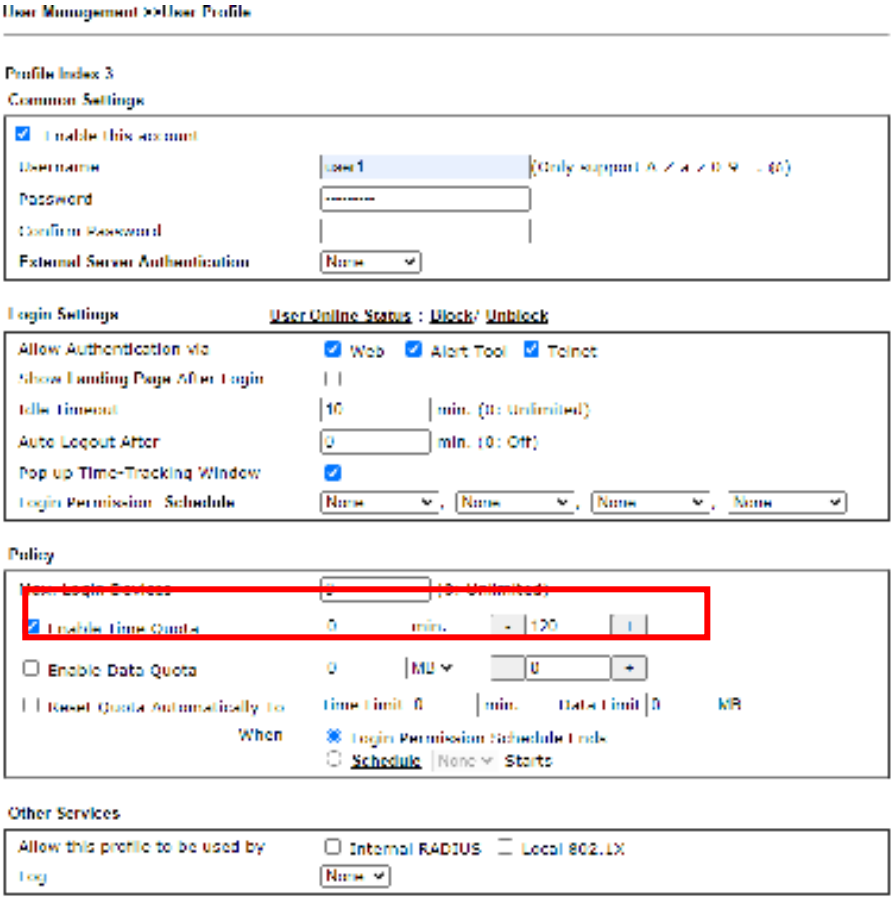
3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.



4. If the Time Quota is set with "0" minute, you will get the following message which means this account has no time quota.



If the **Time Quota** is enabled and time is not 0 minute,



You will get the following message. The expired time is shown after you login.

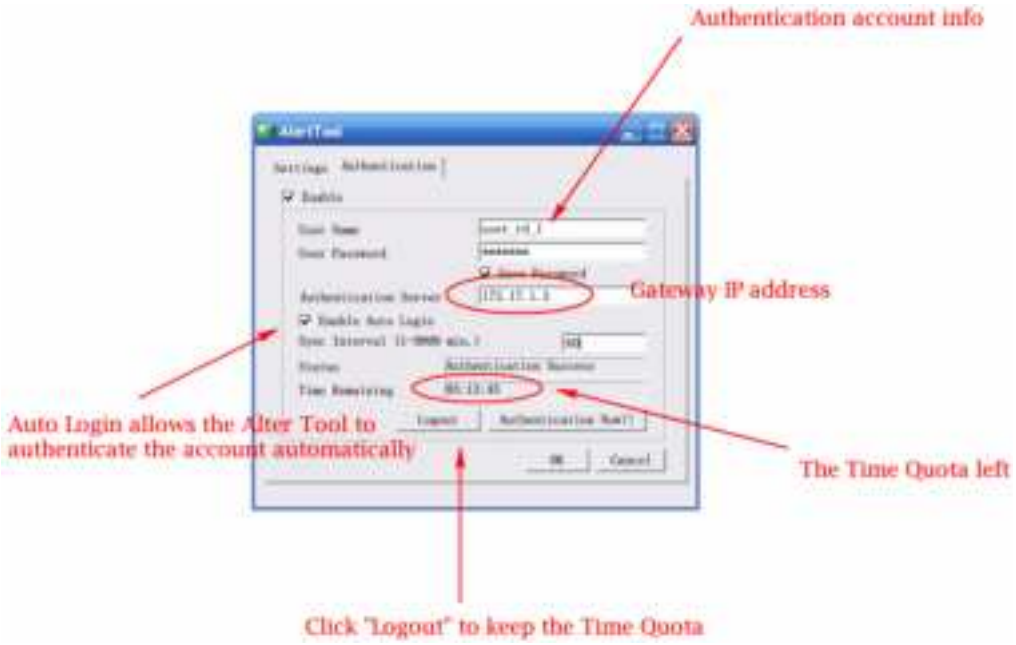
After you run out the available time, you can't use this account any more until the administrator manually adds additional time for you.

Authentication via VigorPro Alert Notice Tool

Authentication via Web or Telnet is convenient for users; however, it has some limitations. The most advantage with VigorPro Alert Notice Tool to operate the authentication is the ability to do **auto login**. If the timeout value set on the router for the user account has been reached, the router will stop the client computer from accessing the Internet until it does an authentication again. Authentication via VigorPro Alert Notice Tool allows user to setup the re-authentication interval so that the utility will send authentication requests periodically. This will keep the client hosts from having to manually authenticate again and again.

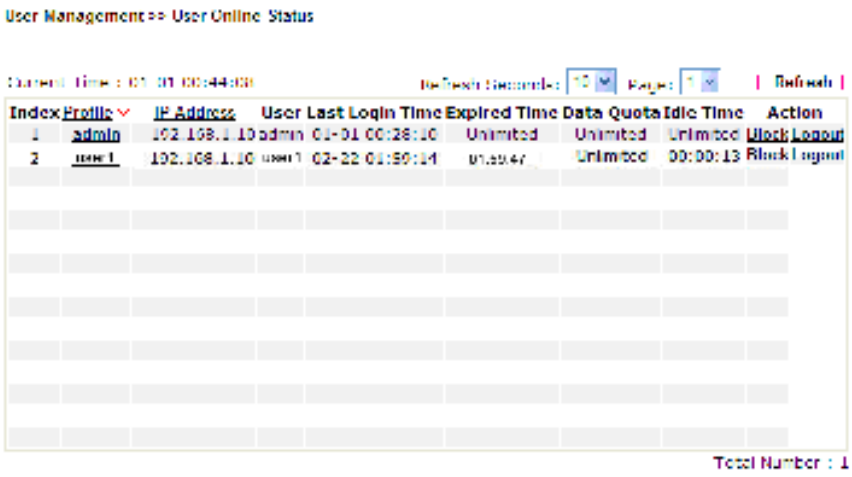
The configuration of the VigorPro Alert Notice Tool is as follows:

1. Click **Authenticate Now!!** to start the authentication immediately.



2. You may get the **VigorPro Alert Notice Tool** from the following link: http://www.draytek.com/user/SupportDLUtility.php

Info 1	Any modification to the Firewall policy will break down the connections of all current users. They all have to authenticate again for Internet access.
Info 2	The administrator may check the current users from **User Online Status** page.

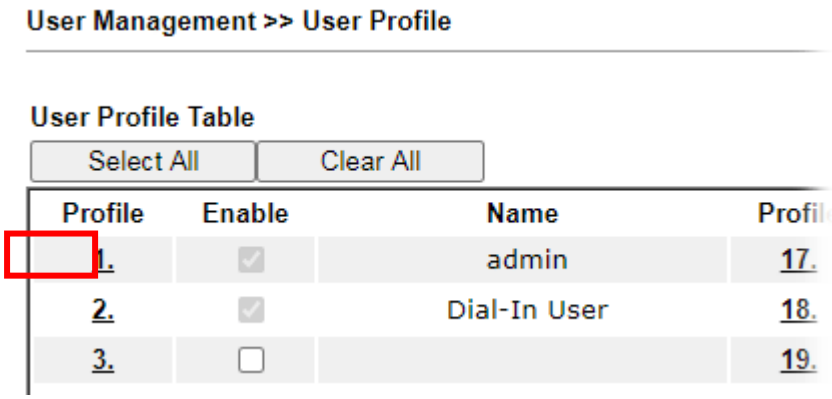


A-2 How to use Landing Page Feature

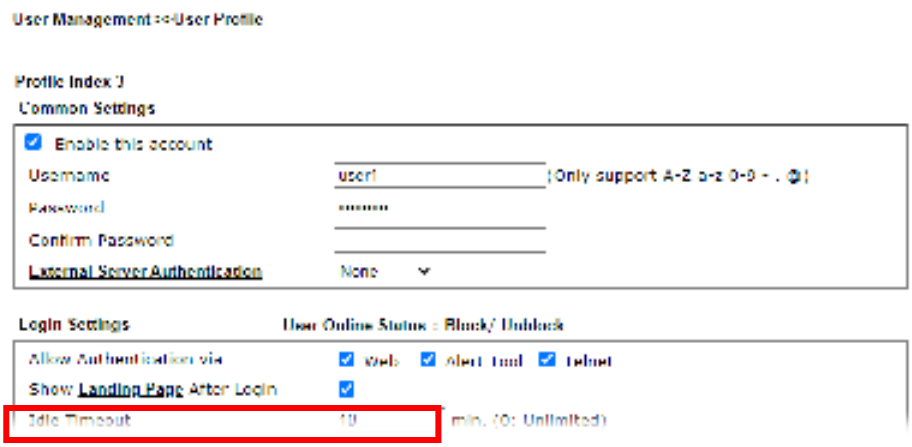
Landing Page is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor2915 series router as an example.

Example 1 : Users can see the message for landing page after logging into Internet successfully

1. Open the web user interface of Vigor2915.
2. Open **User Management -> General Setup** to get the following page. In the field of **Landing Page**, please Enter the words of "**Login Success**". Please note that the maximum number of characters to be typed here is 255.
3. Now you can enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



4. In the following page, check the box of **Landing page** and click **OK** to save the settings.



5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.

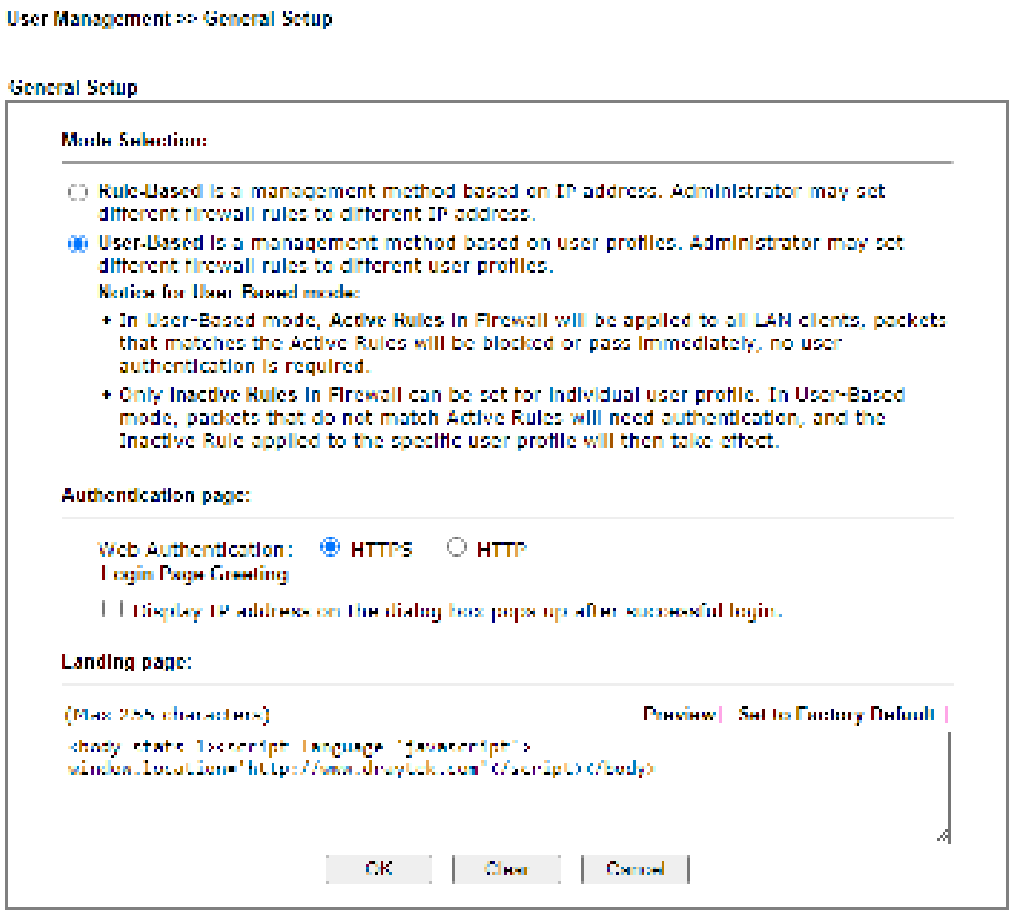
6. Click **Login**. If the logging is successful, you will see the message of Login Success from the browser you use.

Example 2：The system will connect to http://www.draytek.com automatically after logging into Internet successfully

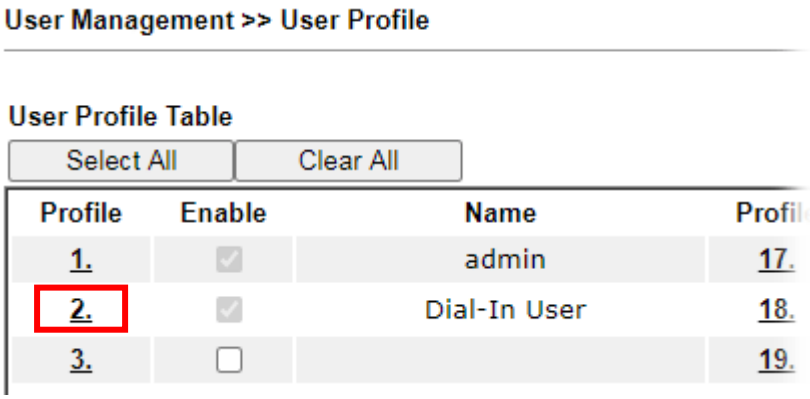
1. In the field of **Landing Page**, please Enter the words as below:

   “ <body stats=1><script language='javascript'>

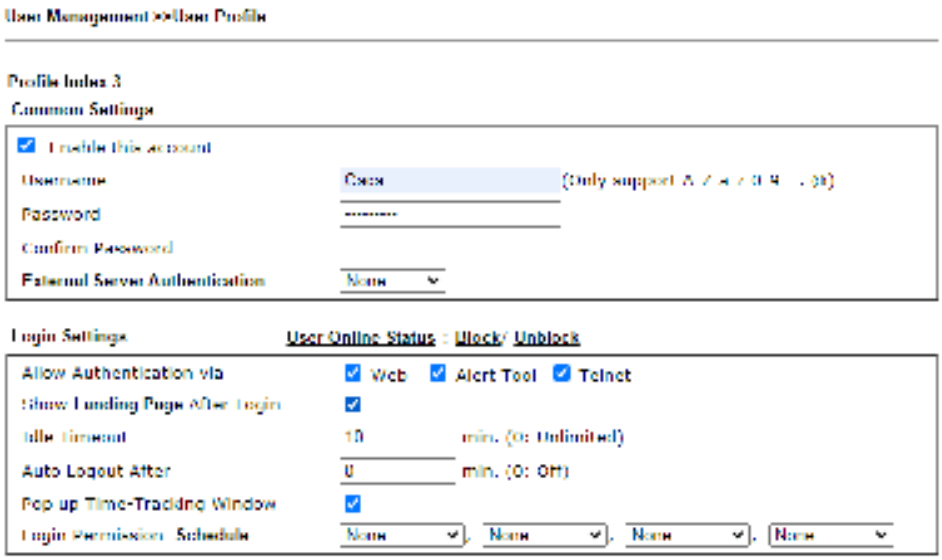
   window.location='http://www.draytek.com'</script></body>”



2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



3. In the following page, check the box of **Landing page** and click **OK** to save the settings.



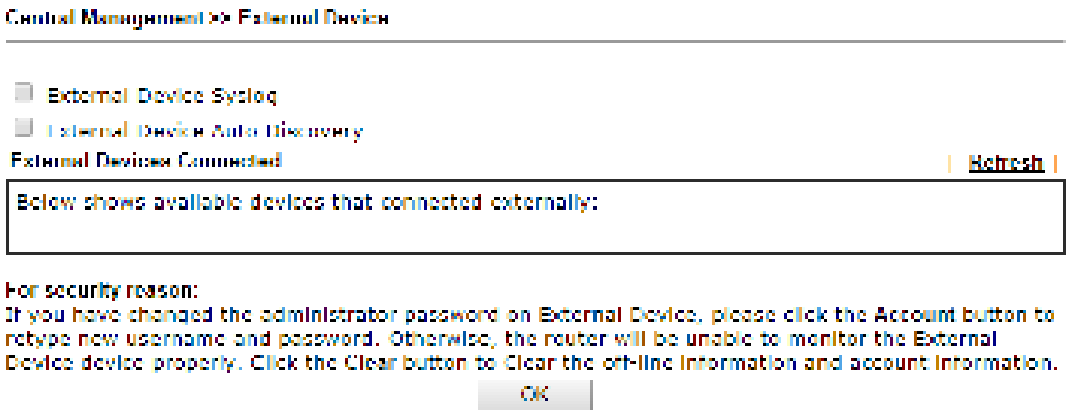
4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.

5. Click **Login**. If the logging is successful, you will be directed into the website of www.draytek.com.

VI-5 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.

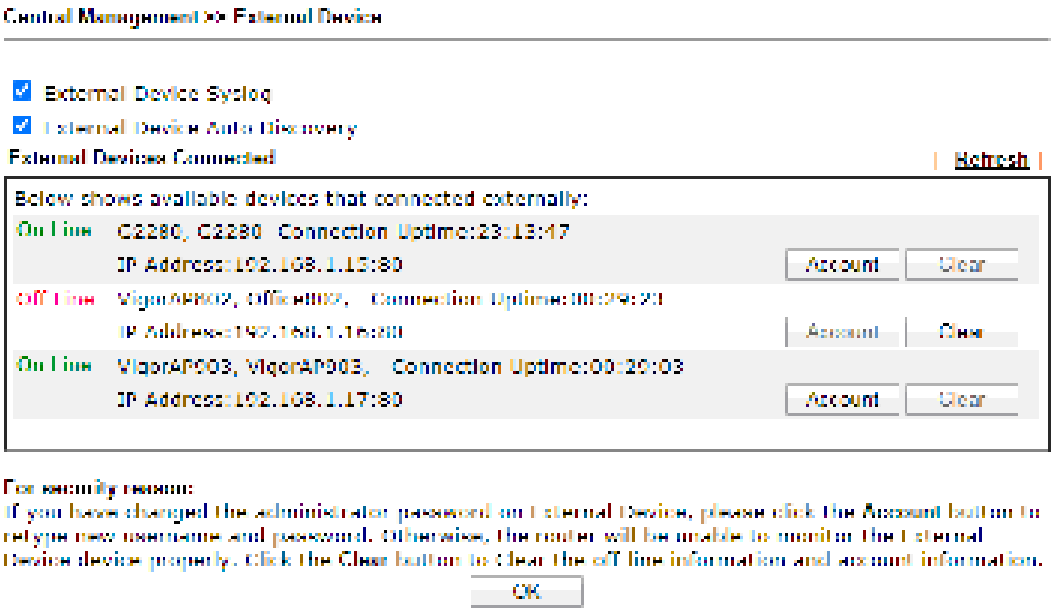
VI-5-1 All Devices



Available settings are explained as follows:

Item	Description
External Device Syslog	Check this box to display information of the detected device on Syslog.
External Device Auto Discovery	Check this box to detect the external device automatically and display on this page.

From this web page, check the box of **External Device Auto Discovery**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.



When you finished the configuration, click **OK** to save it.

Info	Only DrayTek products can be detected by this function.

Part VII Others

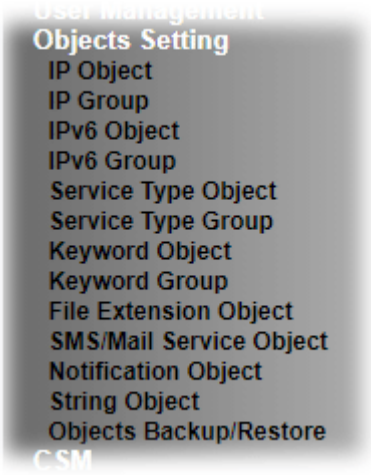
Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

VII-1 Objects Settings

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.

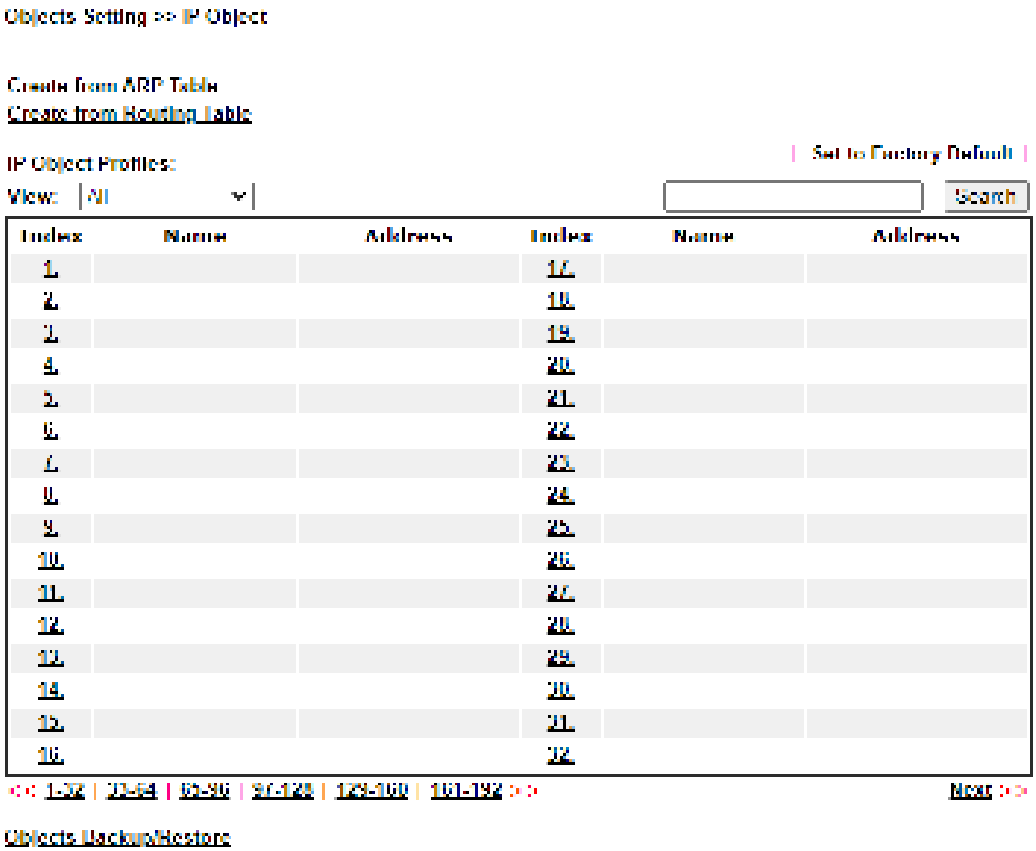
Web User Interface



VII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with ***objects*** and bind them with ***groups*** for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

You can set up to 192 sets of IP Objects with different conditions.

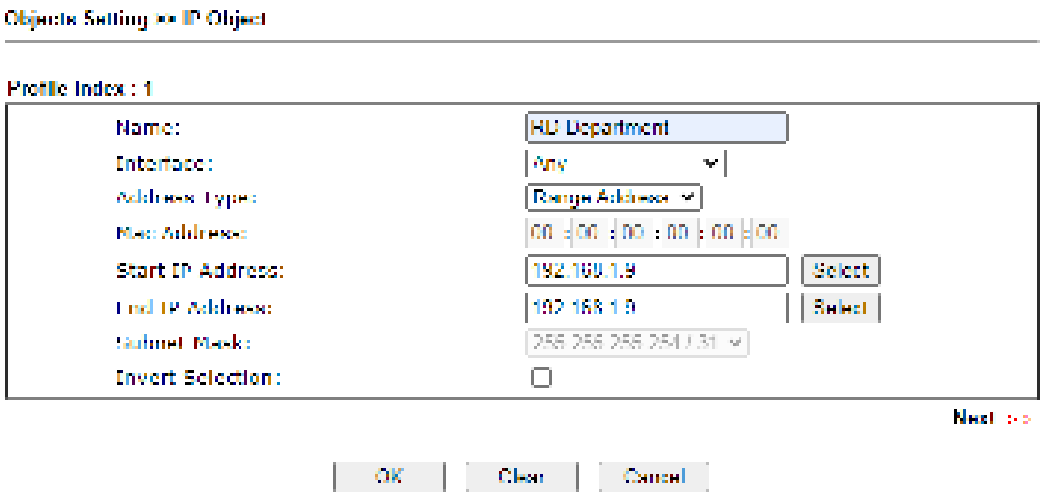


Available settings are explained as follows:

Item	Description
View	Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page.
Set to Factory Default	Clear all profiles.
Search	Type a string of the IP object that you want to search.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Address	Display the IP address configured for the object profile.
Objects Backup/Restore	Click it to backup or restore the IP object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

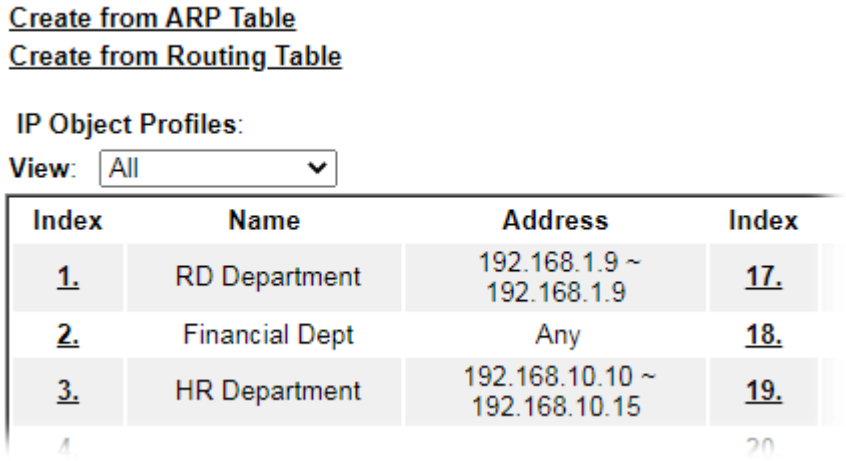


Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface. For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN/ RT/ VPN or any IP address. If you choose LAN/ RT/ VPN as the **Interface** here, and choose LAN/ RT/ VPN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN/ RT/ VPN interface will be opened for you to choose in **Edit Filter Rule** page.
Address Type	Determine the address type for the IP address. Select **Single Address** if this object contains one IP address only. Select **Range Address** if this object contains several IPs within a range. Select **Subnet Address** if this object contains one subnet for IP address. Select **Any Address** if this object contains any IP address.

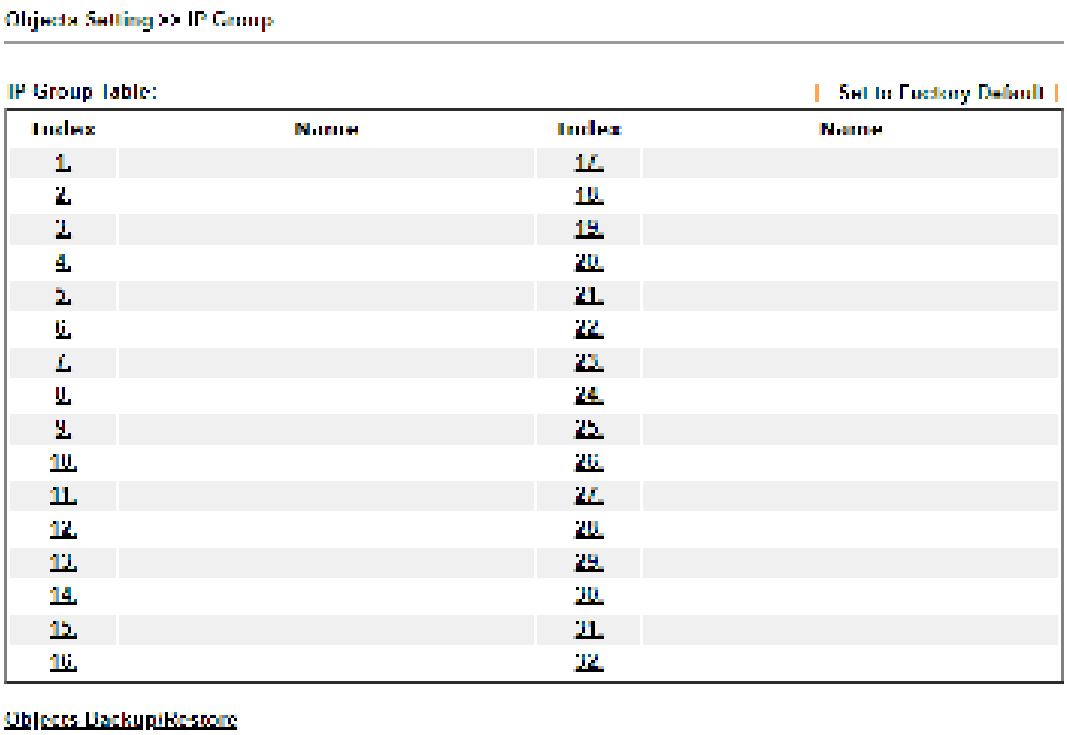
	Select **Mac Address** if this object contains Mac address.
MAC Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Enter the start IP address for Single Address type.
End IP Address	Enter the end IP address if the Range Address type is selected.
Subnet Mask	Enter the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

4. After finishing all the settings here, please click **OK** to save the configuration. Below is an example of IP objects settings.



VII-1-2 IP Group

This page allows you to bind several IP objects into one IP group.



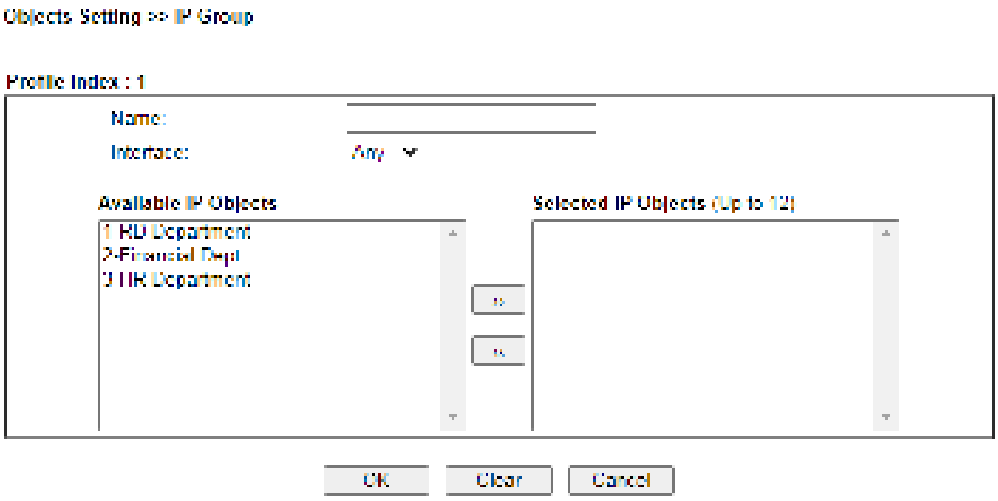
Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.
Objects Backup/Restore	Click it to backup or restore the IP group object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

2. The configuration page will be shown as follows:



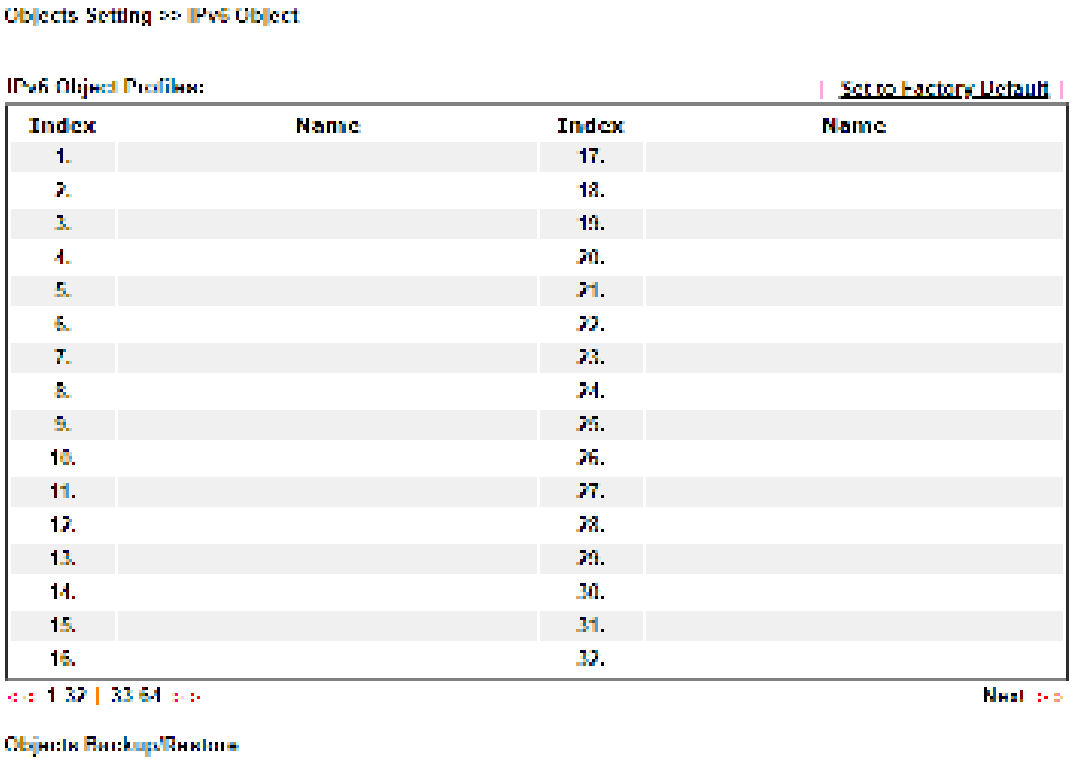
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click **>>** button to add the selected IP objects in this box.

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

VII-1-3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.



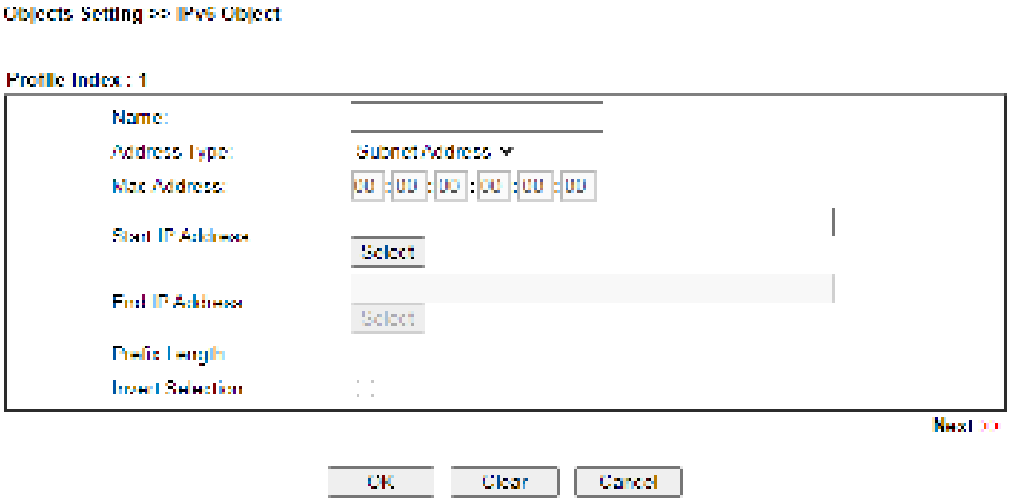
Objects Backup/Restore

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



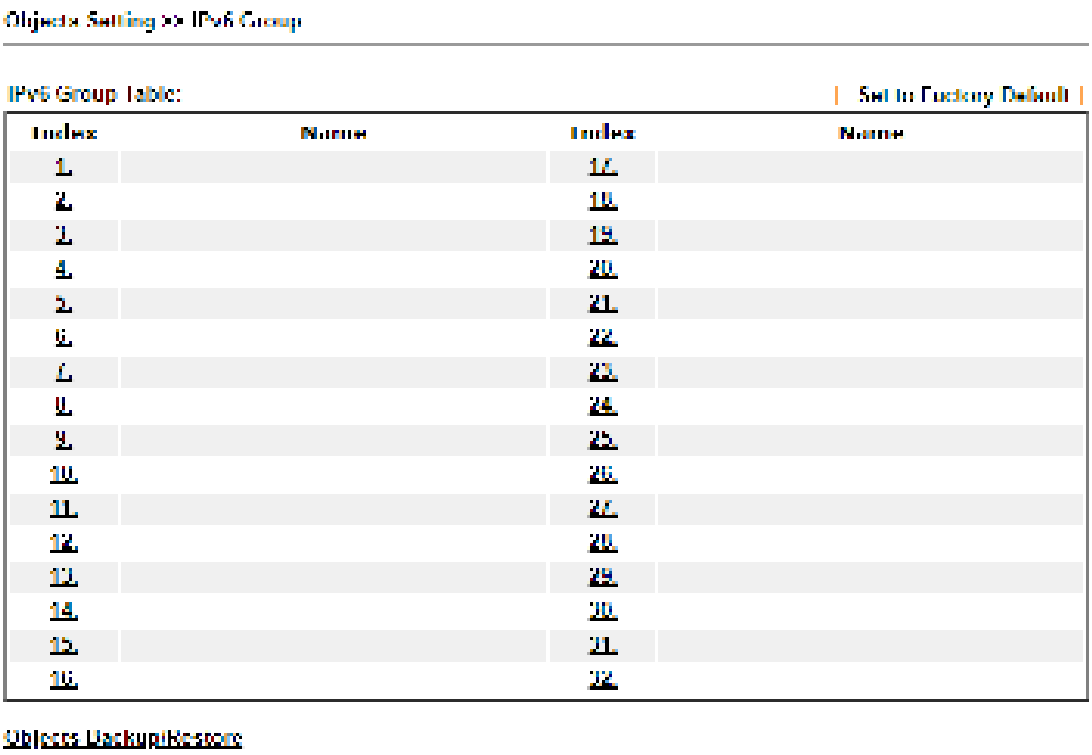
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select **Single Address** if this object contains one IPv6 address only. Select **Range Address** if this object contains several IPv6s within a range. Select **Subnet Address** if this object contains one subnet for IPv6 address. Select **Any Address** if this object contains any IPv6 address. Select **Mac Address** if this object contains Mac address.
Mac Address	Enter the MAC address of the network card which will be controlled.
Start IP Address	Enter the start IP address for Single Address type. Or, click **Select** to specify an IP address.
End IP Address	Enter the end IP address if the Range Address type is selected. Or, click **Select** to specify an IP address.
Prefix Length	Enter the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

VII-1-4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

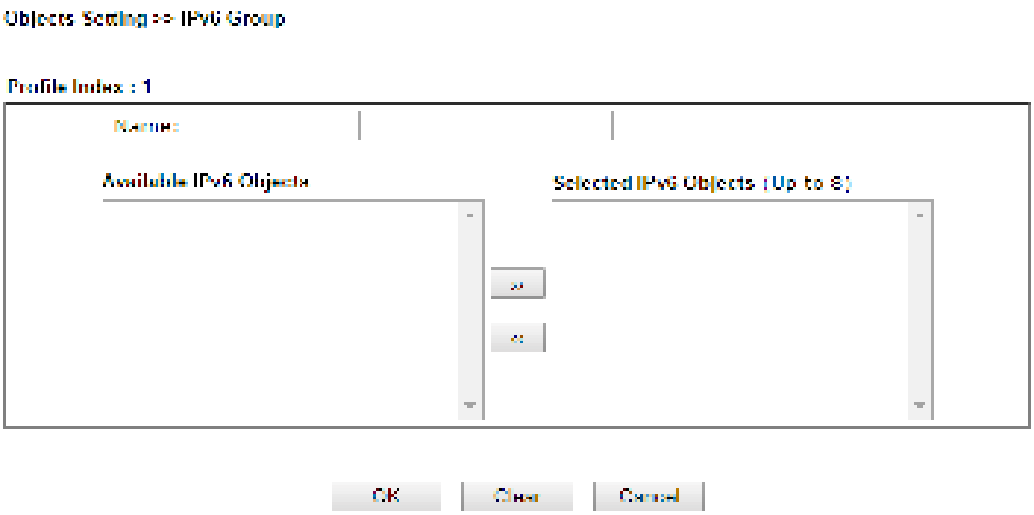


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.
Objects Backup/Restore	Click it to backup or restore the IPv6 object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



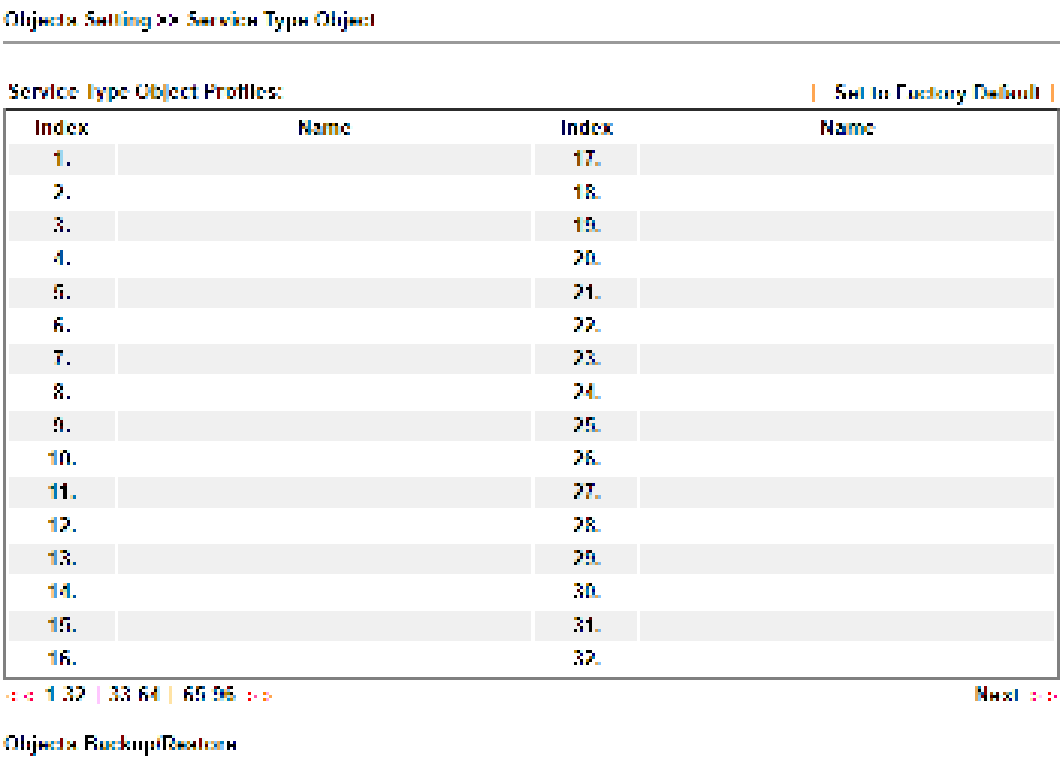
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click **>>** button to add the selected IPv6 objects in this box.

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

VII-1-5 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

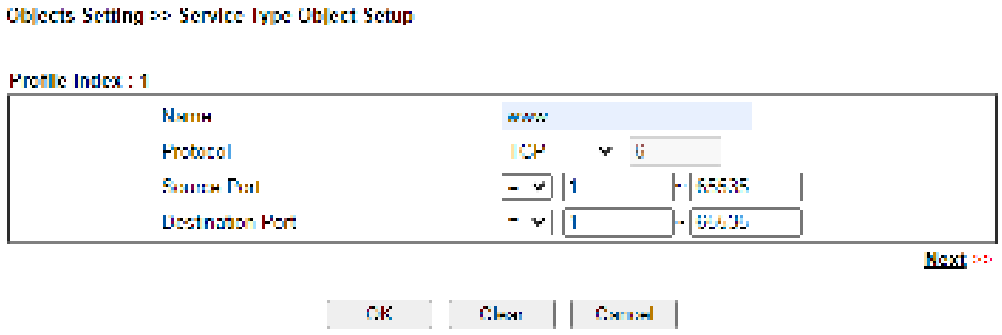


Available settings are explained as follows:

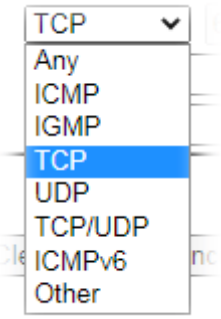
Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Objects Backup/Restore	Click it to backup or restore the service type object.

To set a new profile, please do the steps listed below:

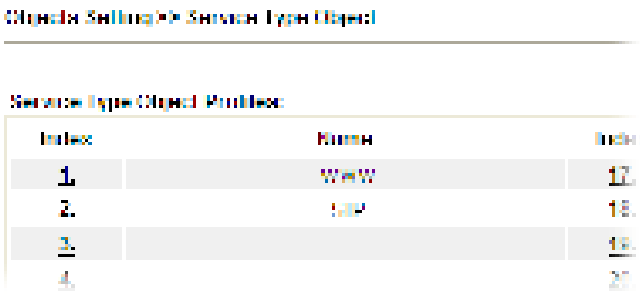
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

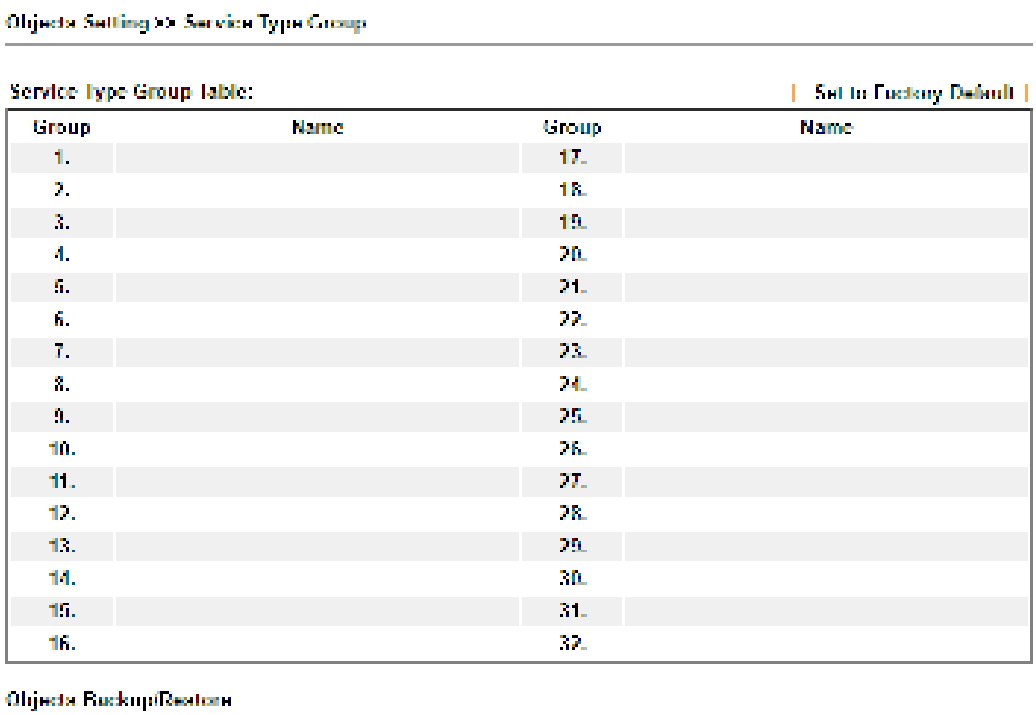
Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	**Source Port** and the **Destination Port** columns are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. ***(=)*** –when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile. ***(!=)*** –when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** –the port number greater than this value is available. ***(<)*** –the port number less than this value is available for this profile.

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



VII-1-6 Service Type Group

This page allows you to bind several service types into one group.

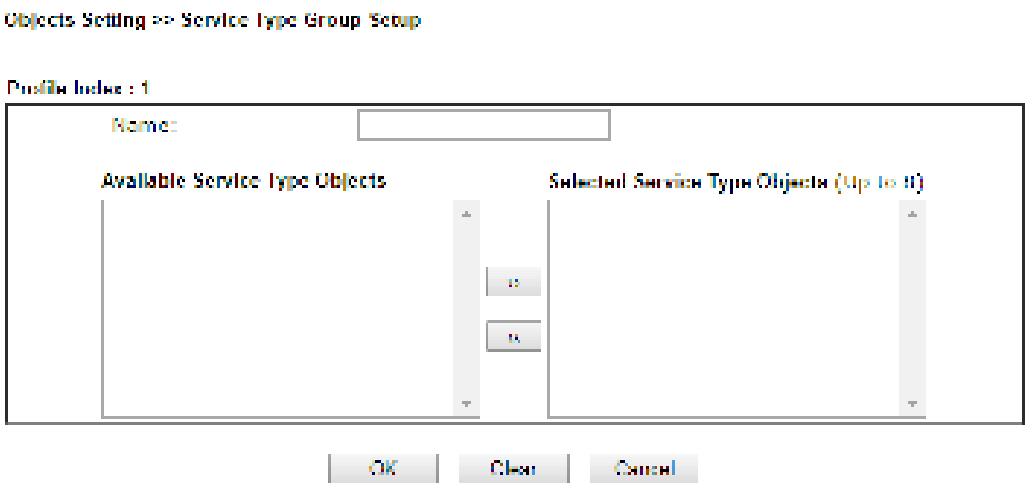


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.
Objects Backup/Restore	Click it to backup or restore the service type group object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Group column for configuration in details.
2. The configuration page will be shown as follows:



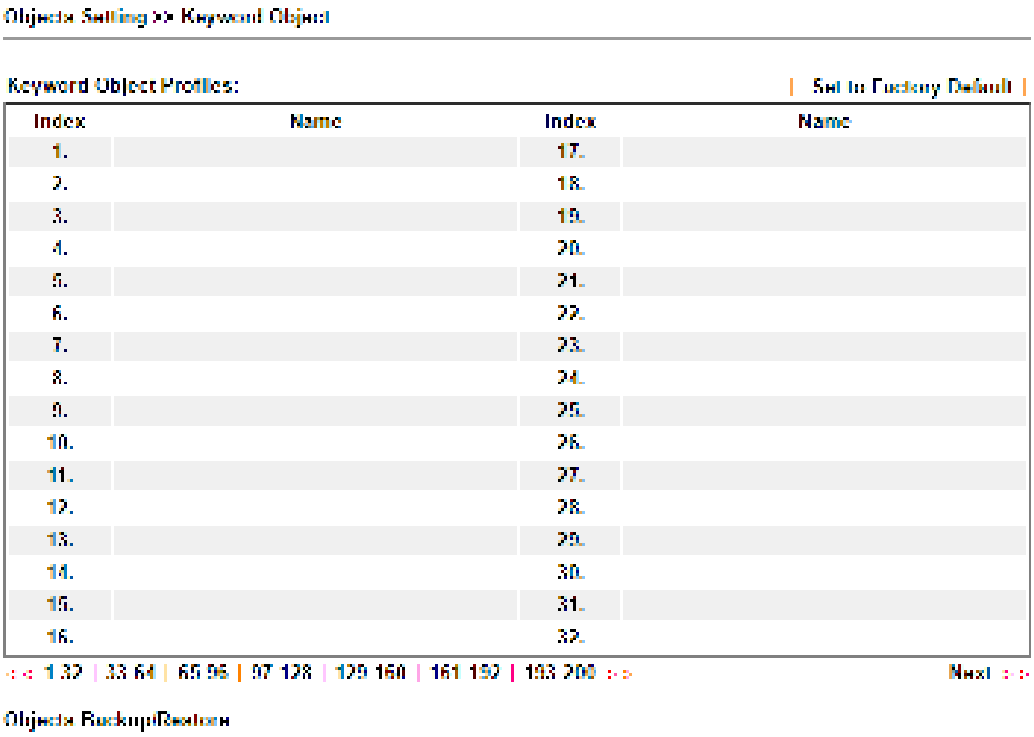
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on **Objects Setting>>Service Type Object** will be shown in this box.
Selected Service Type Objects	Click **>>** button to add the selected IP objects in this box.

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

VII-1-7 Keyword Object

You can set 200 keyword object profiles for choosing as black / white list in **CSM >>URL Web Content Filter Profile.**

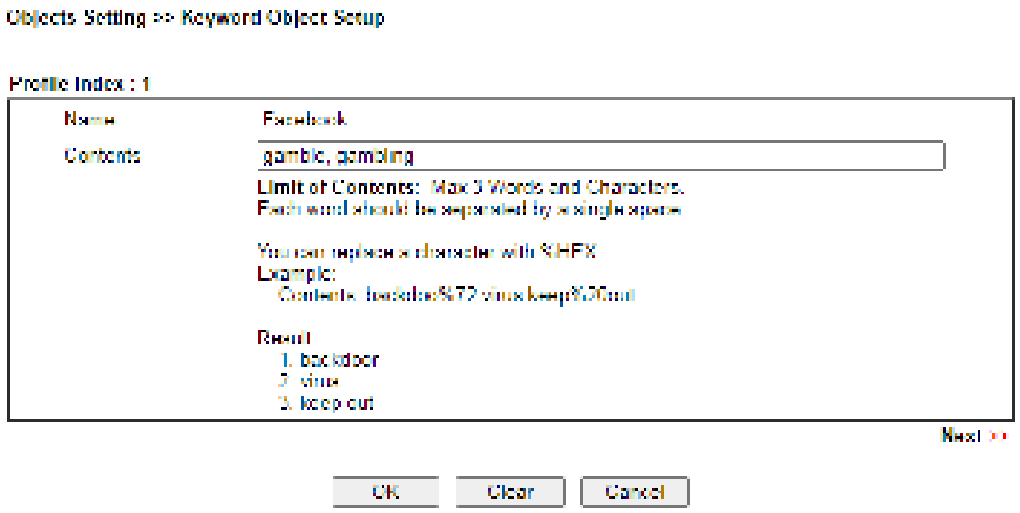


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Objects Backup/Restore	Click it to backup or restore the keyword object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



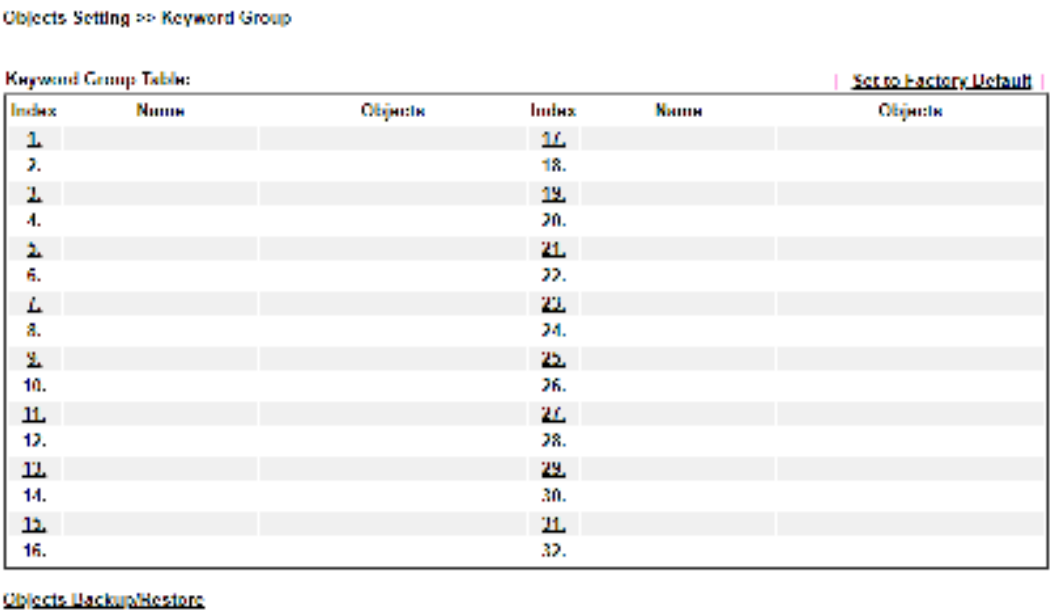
Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.
Contents	Enter the content for such profile based on the selected type. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/ blocked based on the configuration on Firewall settings.

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

VII-1-8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black / white list in **CSM >>URL /Web Content Filter Profile**.

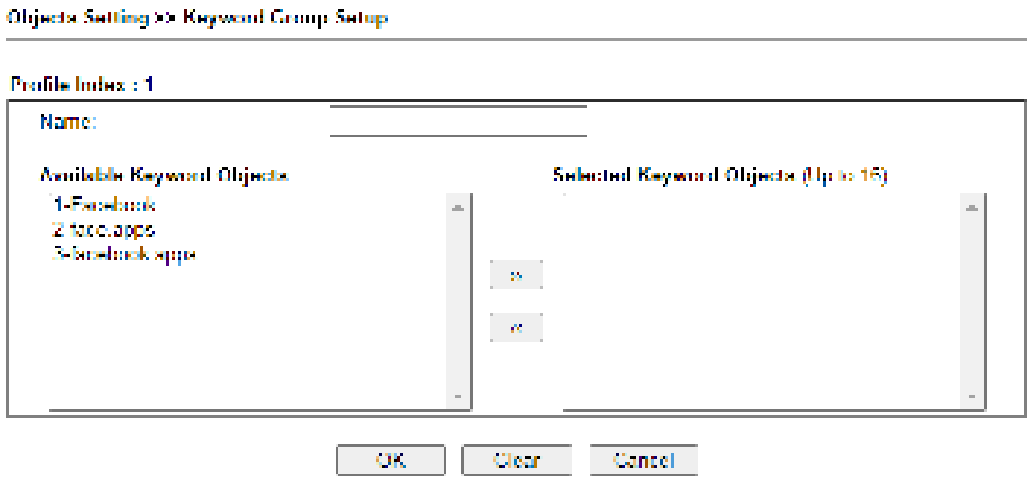


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.
Objects Backup/Restore	Click it to backup or restore the keyword group object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:



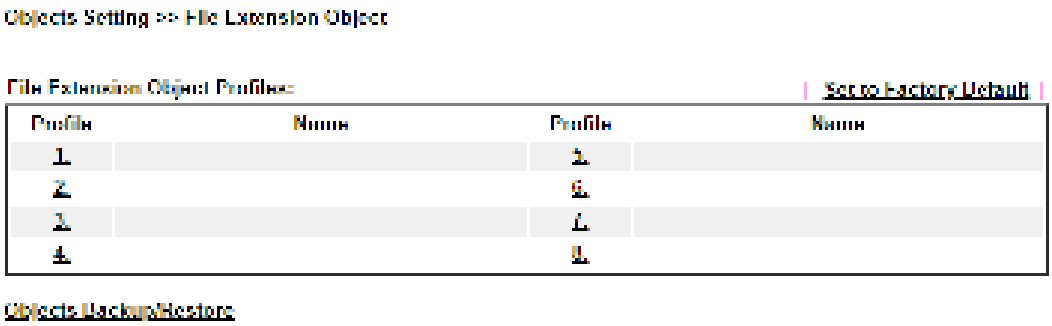
Available settings are explained as follows:

Item	Description
Name	Type a name for this group. Maximum 15 characters are allowed.
Available Keyword Objects	You can gather keyword objects from **Keyword Object** page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click » button to add the selected Keyword objects in this box.

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

VII-1-9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

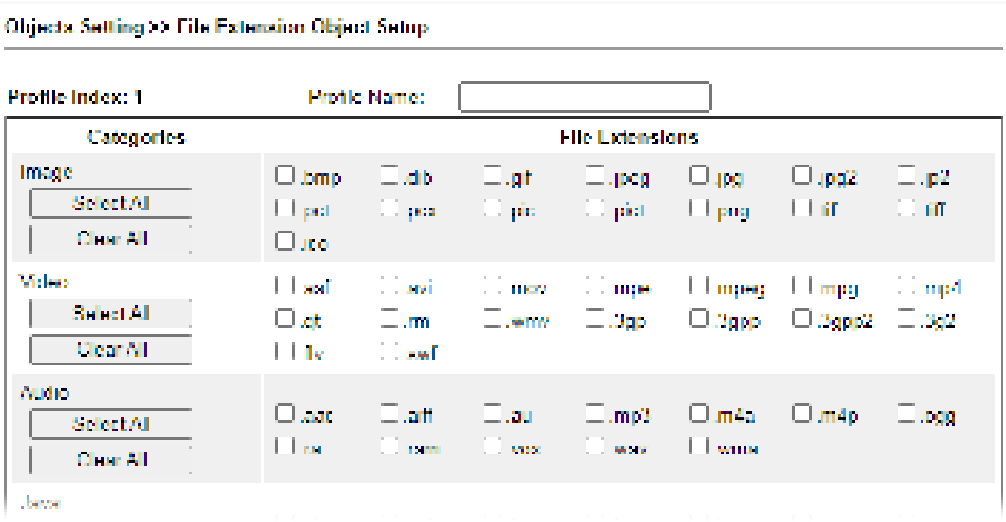


Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.
Objects Backup/Restore	Click it to backup or restore the file extension object.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Profile column for configuration in details.
2. The configuration page will be shown as follows:



Available settings are explained as follows:

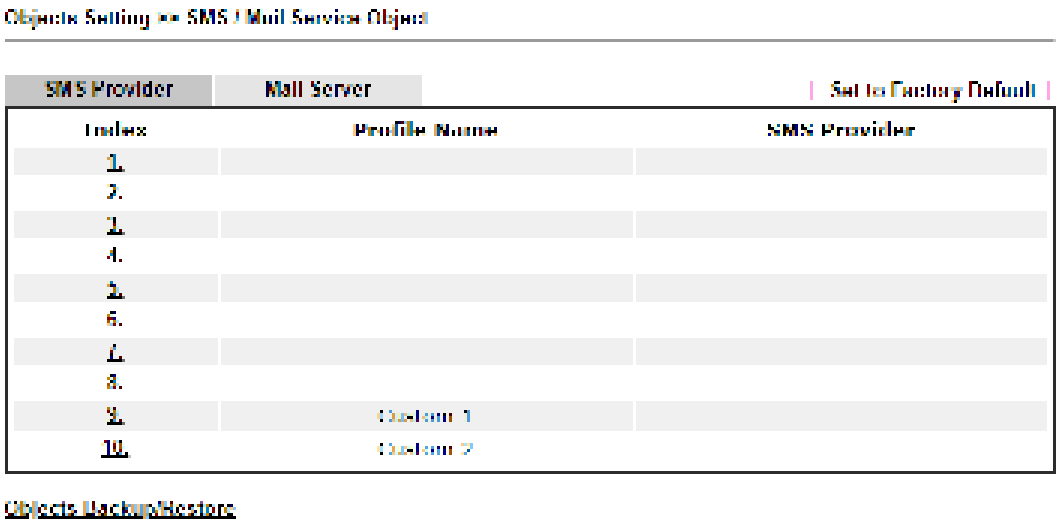
Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

VII-1-10 SMS/Mail Service Object

SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

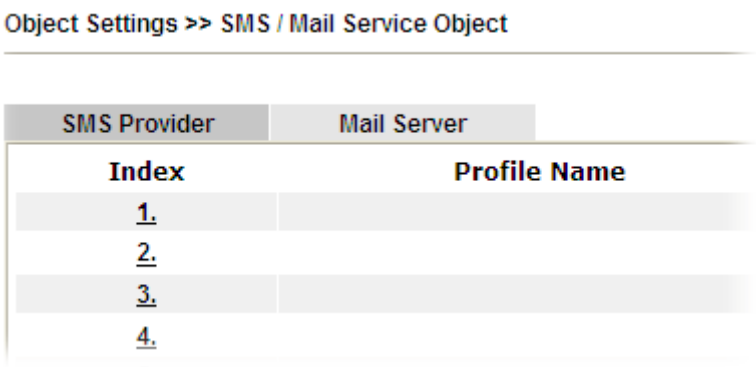


Each item is explained as follows:

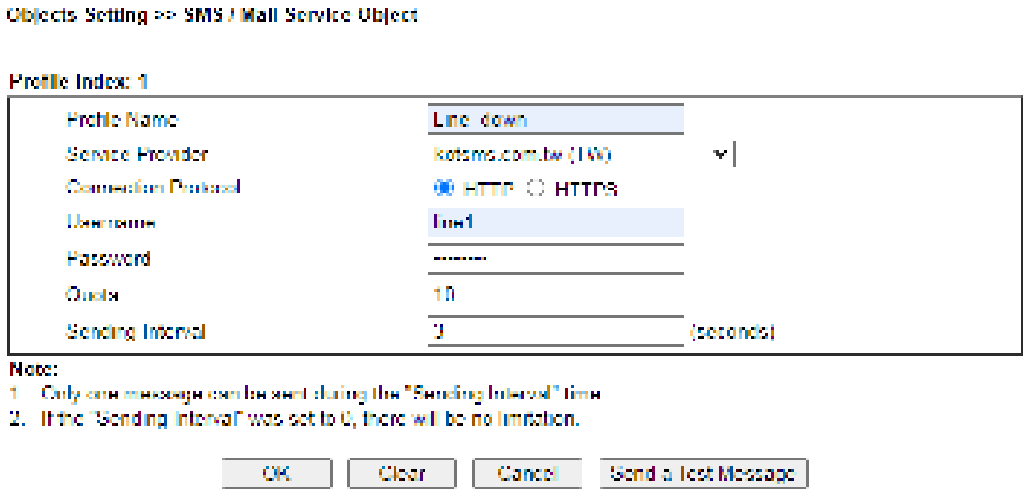
Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.
Objects Backup/Restore	Click it to backup or restore the SMS service object.

To set a new profile, please do the steps listed below:

1. Click the **SMS Provider** tab, and click the number (e.g., #1) under Index column for configuration in details.



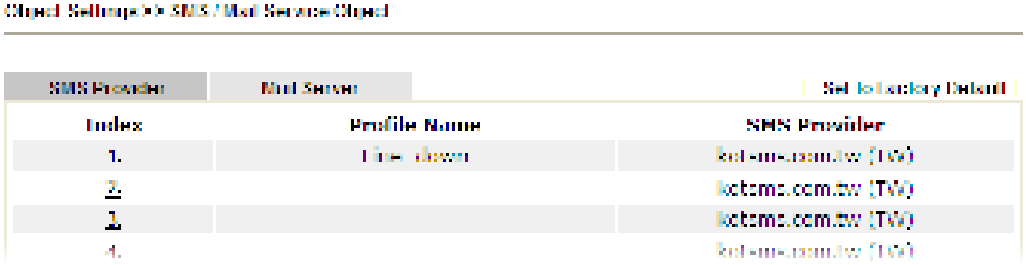
2. The configuration page will be shown as follows:



Available settings are explained as follows:

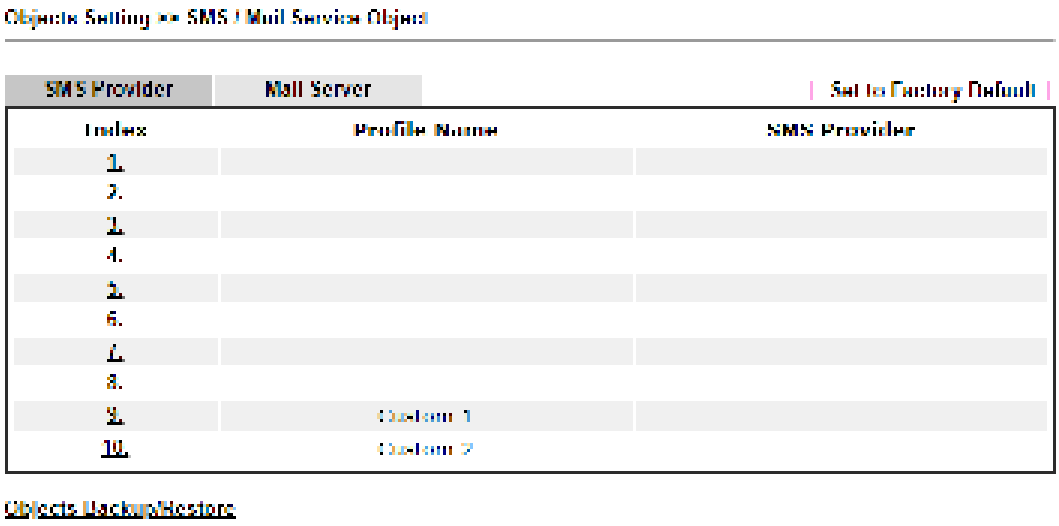
Item	Description
Profile Name	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Connection Protocol	Specify HTTP or HTTPS.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

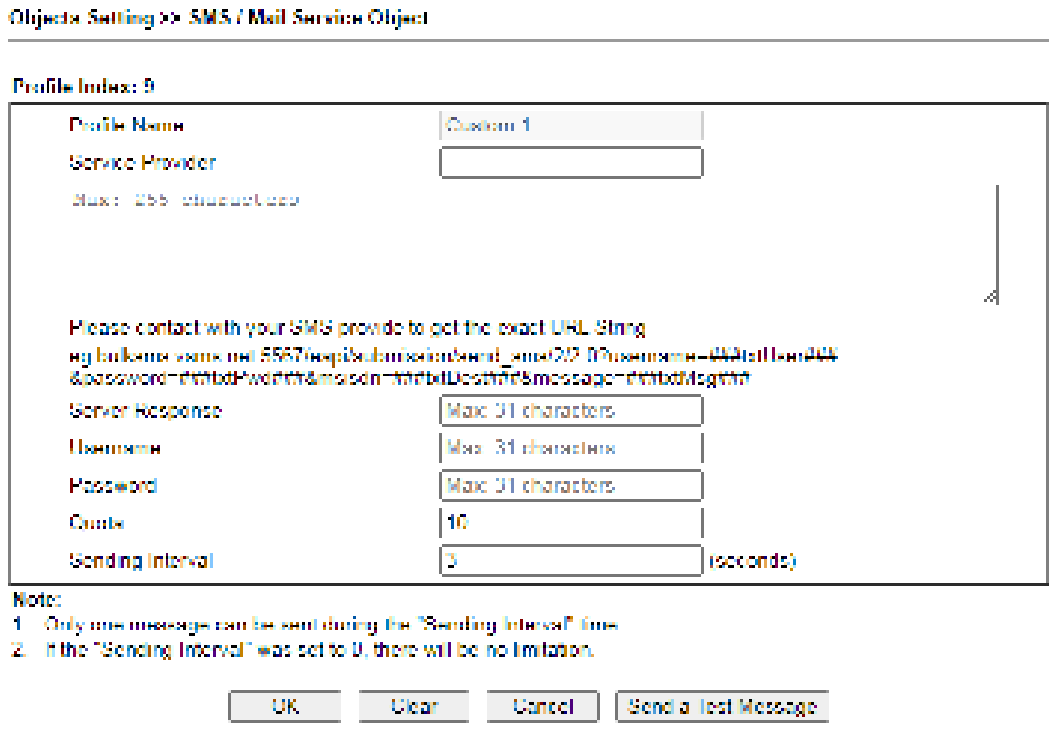


Customized SMS Service

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.



You can click the number (e.g., #9) under Index column for configuration in details.



Available settings are explained as follows:

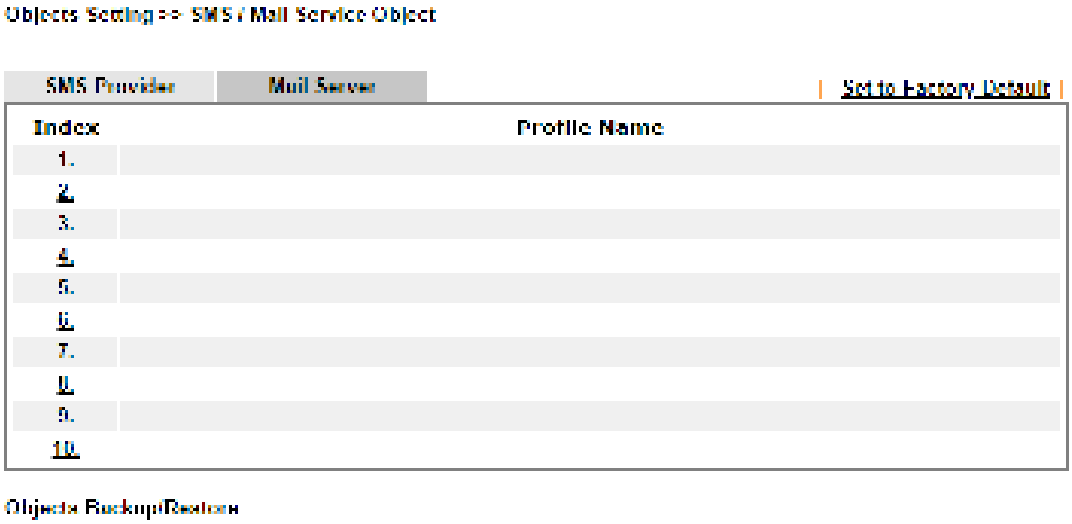
Item	Description
Profile Name	Display the name of this profile. It cannot be modified.
Service Provider	Enter the website of the service provider. Enter the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.

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	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Enter the total number of the messages that the router will send out.
Sending Interval	Enter the shortest time interval for the system to send SMS.

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

Mail Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

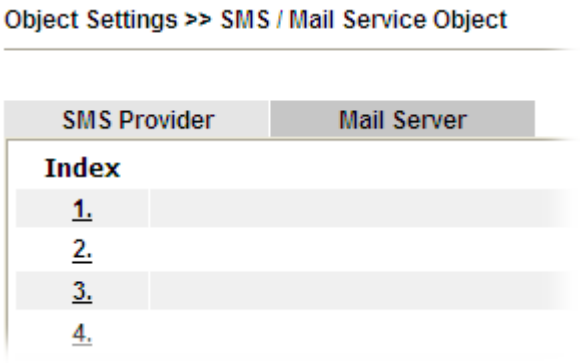


Each item is explained as follows:

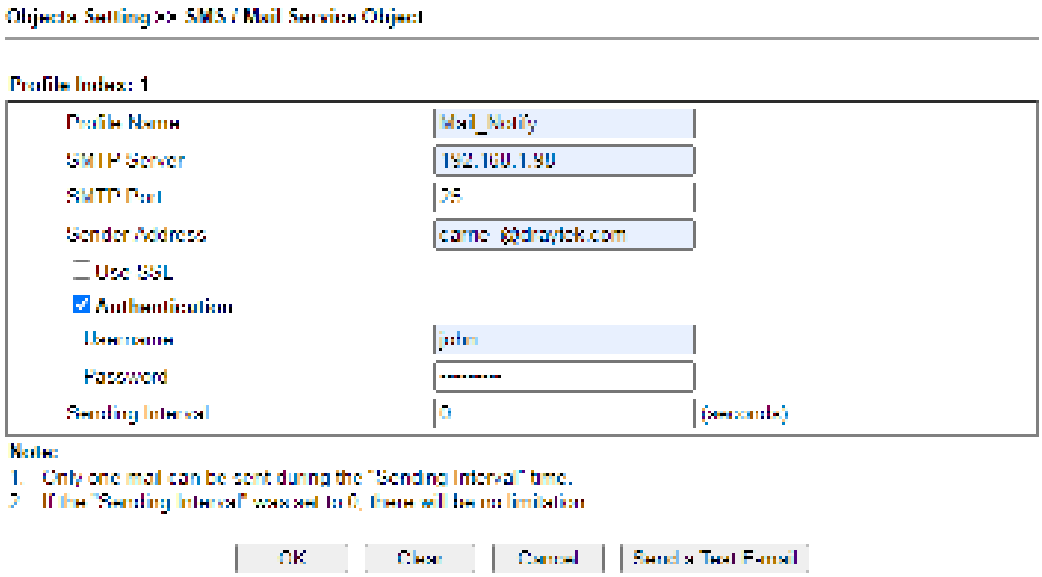
Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.
Objects Backup/Restore	Click it to backup or restore the mail service object.

To set a new profile, please do the steps listed below:

1. Click the **Mail Server** tab, and click the number (e.g., #1) under Index column for configuration in details.



2. The configuration page will be shown as follows:

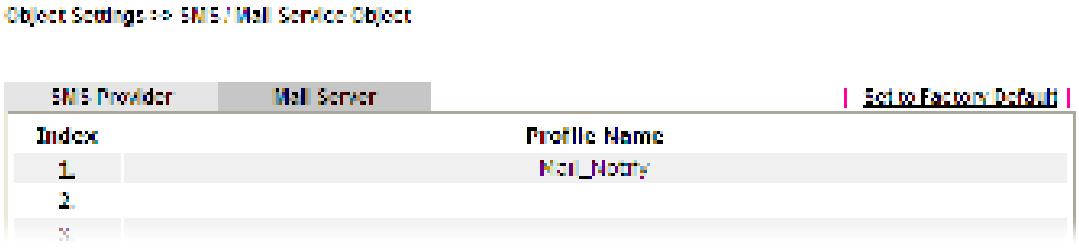


Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Enter the IP address of the mail server.
SMTP Port	Enter the port number for SMTP server.
Sender Address	Enter the e-mail address of the sender.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function. **Username** –Type a name for authentication. The maximum length of the name you can set is 31 characters. **Password** –Type a password for authentication. The maximum length of the password you can set is 31 characters.

Sending Interval	Define the interval for the system to send the SMS out.

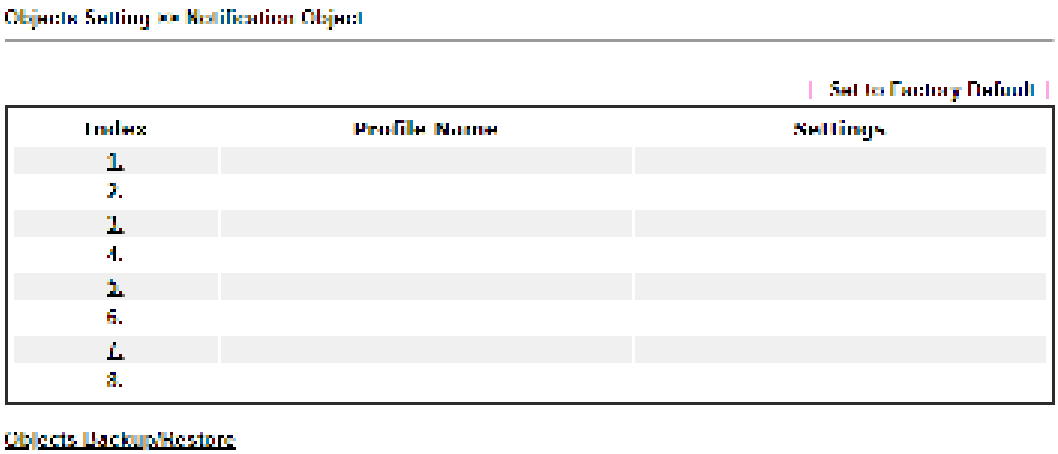
3. After finishing all the settings here, please click **OK** to save the configuration.



VII-1-11 Notification Object

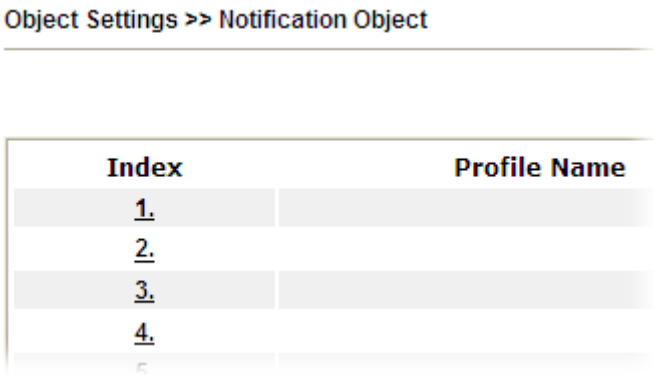
This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

You can set an object with different monitoring situation.

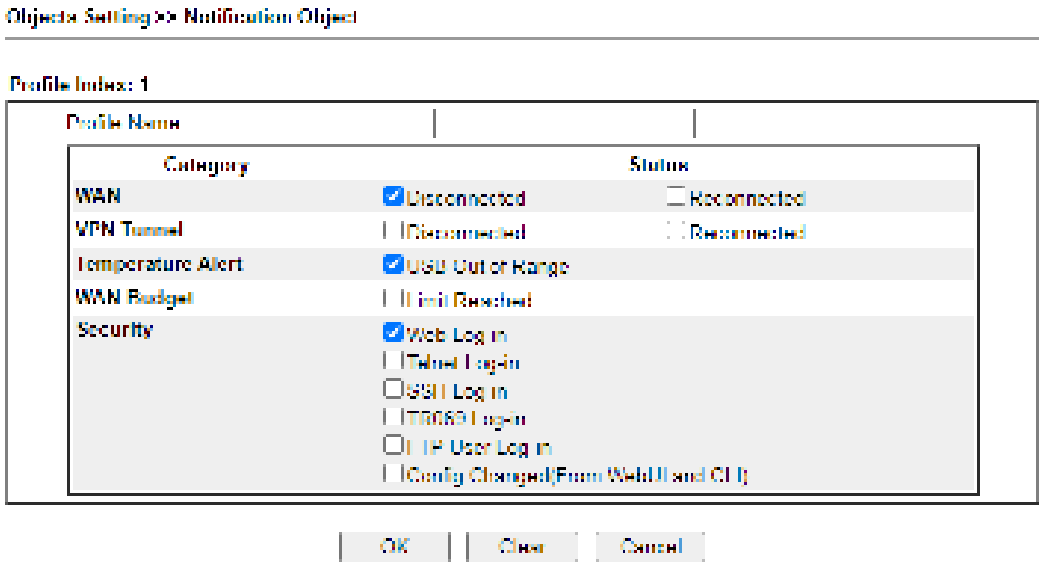


To set a new profile, please do the steps listed below:

1. Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.



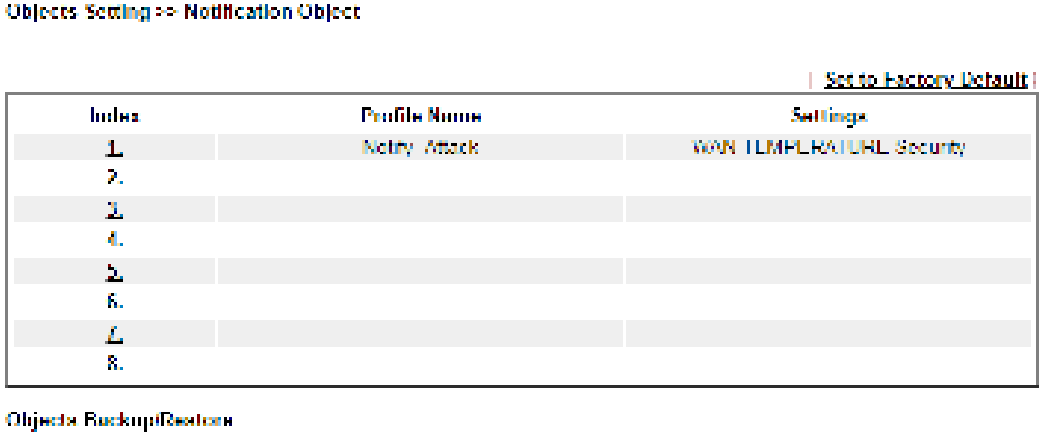
2. The configuration page will be shown as follows:



Available settings are explained as follows:

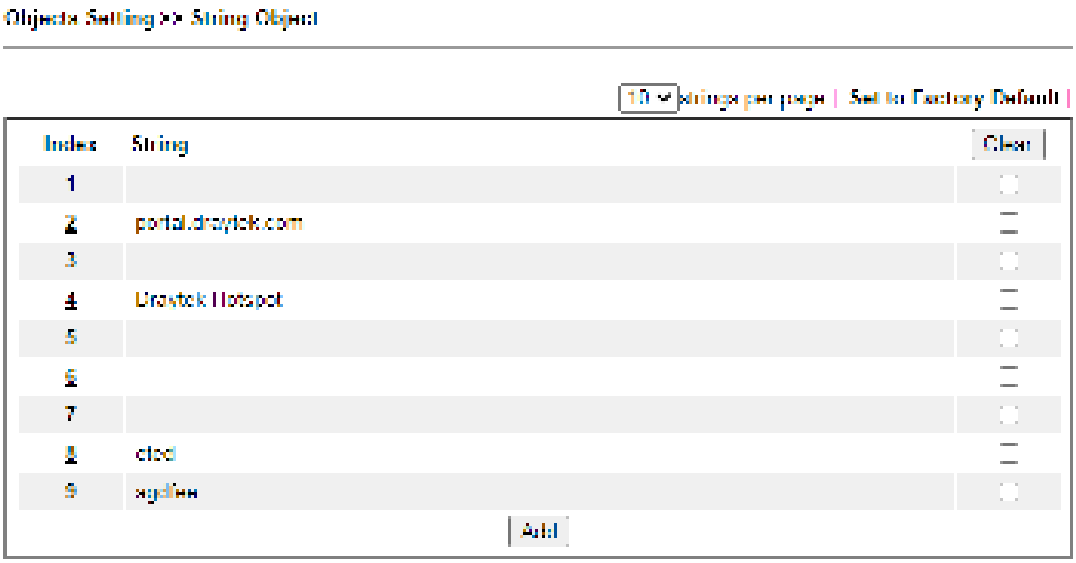
Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box to be monitored.

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

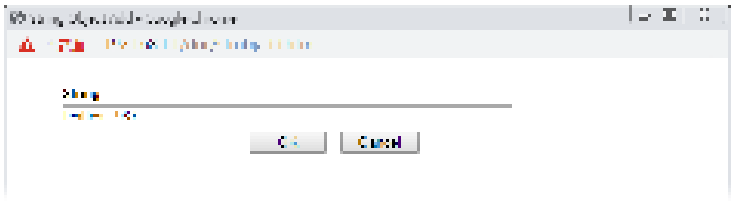


VII-1-12 String Object

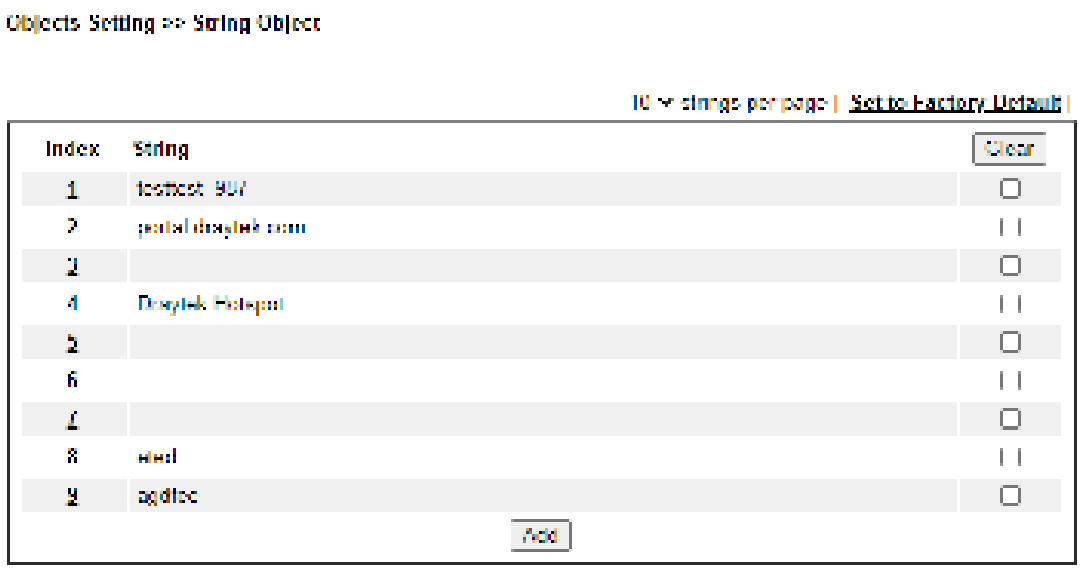
This page allows you to set string profiles which will be applied in route policy (domain name selection for destination), hotspot web portal and etc.

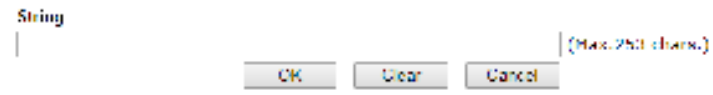


Available settings are explained as follows:

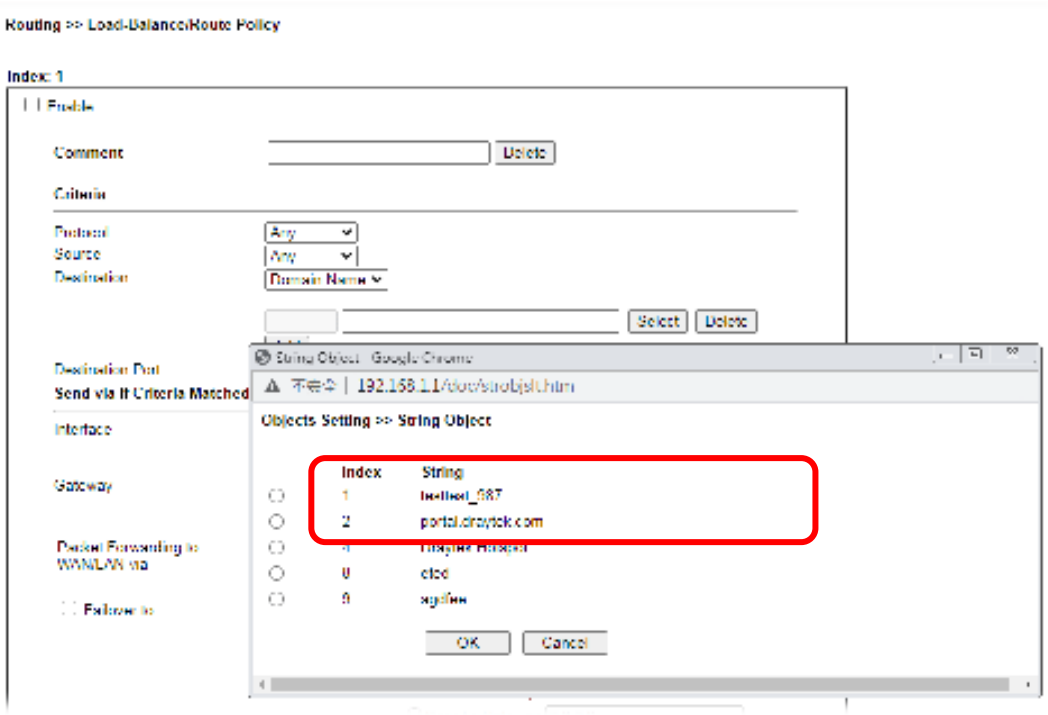
Item	Description
Set to Factory Default	Click it to clear all of the settings in this page.
Add	Click it to create a new string object profile. 
Objects Backup/Restore	Click it to backup or restore the string object.

After creating a new string profile, the new added profile will be shown as follows:



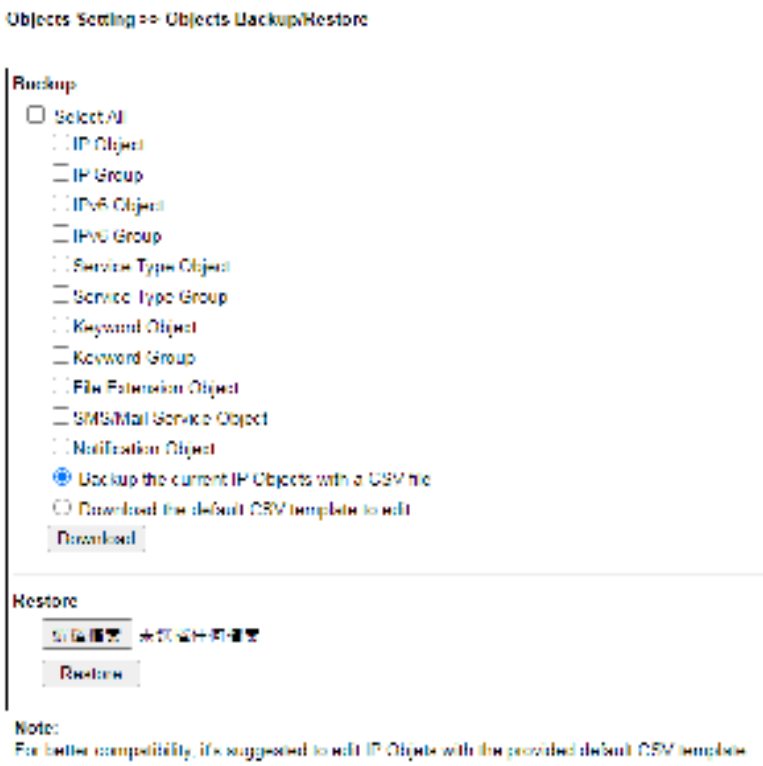
Item	Description
Index	Click it to open the following page for modifying an existed string object. 
String	Display the name of a string profile.
Clear	Choose the string that you want to remove. Then check the box and click Clear to delete the selected string profile.
Add	Click it to create a new string object profile.

Below shows an example to apply string object (in Route Policy):



VII-1-13 Objects Backup/Restore

The objects settings can be backup as a file. The backup file can be imported to the device to restore the configuration in the future if required.



Available settings are explained as follows:

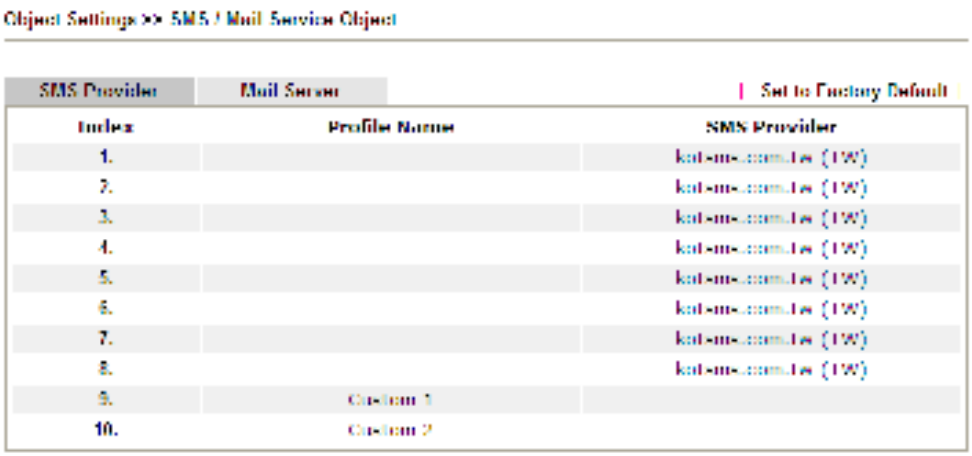
Item	Description
Backup	Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file. All of the IP objects (or the template) can be exported as a file by clicking Download. Then the user can open the CSV file through Microsoft Excel and modify all the IP objects at the same time. **Backup the current IP Objects with a CSV file** – Click it to backup current IP objecsts as a CSV file. Such file can be restored for future use. **Download the default CSV template to edit** – After clicking it, press Download to store the default CSM template (a table without any input data) to your hard disk. **Download** – Download the CSV file from Vigor router and store in your hard disk.
Restore	**Select** – Click it to specify a predefined CSV file. **Restore** – Import the selected CSV file onto Vigor router.

Application Notes

A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

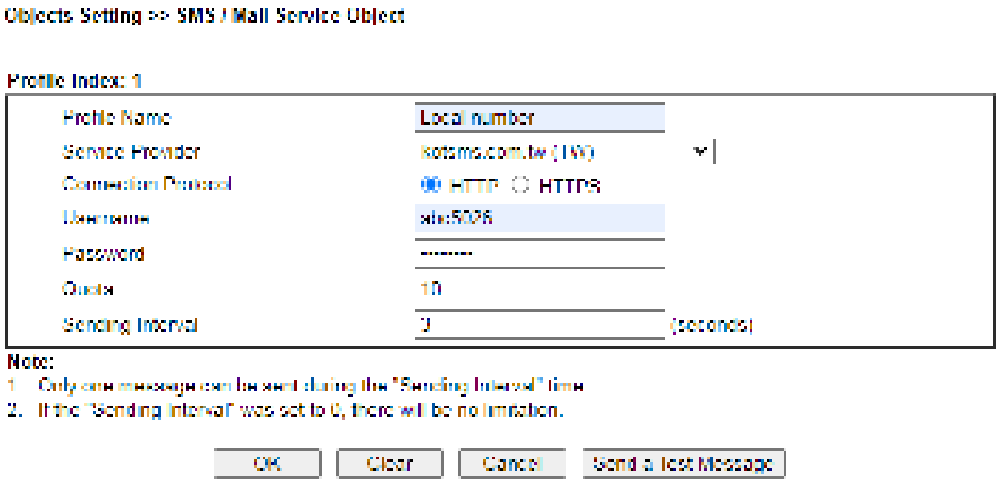
Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

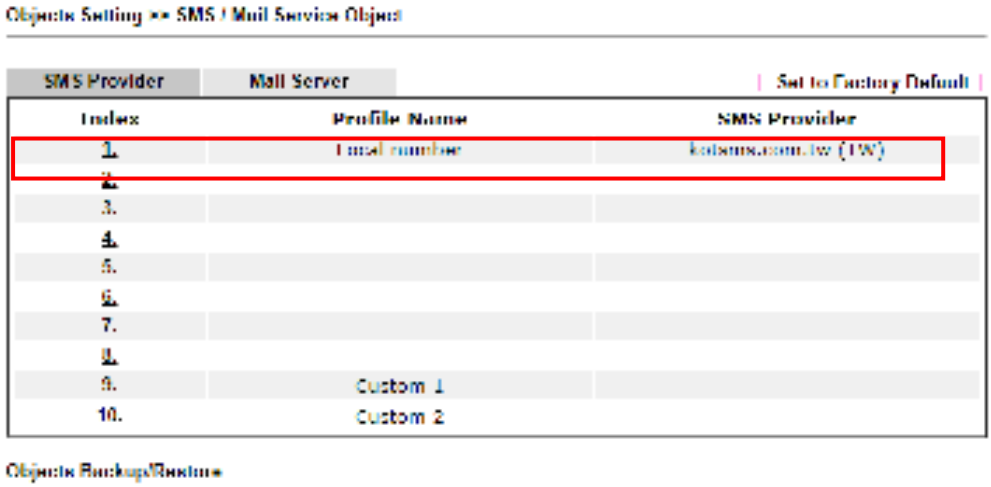


Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

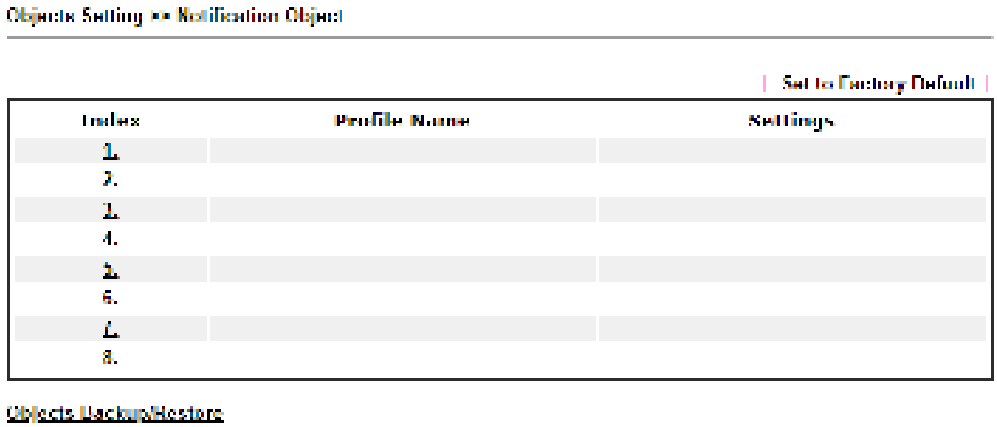
3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, Enter the username and password and set the quota that the router can send the message out.



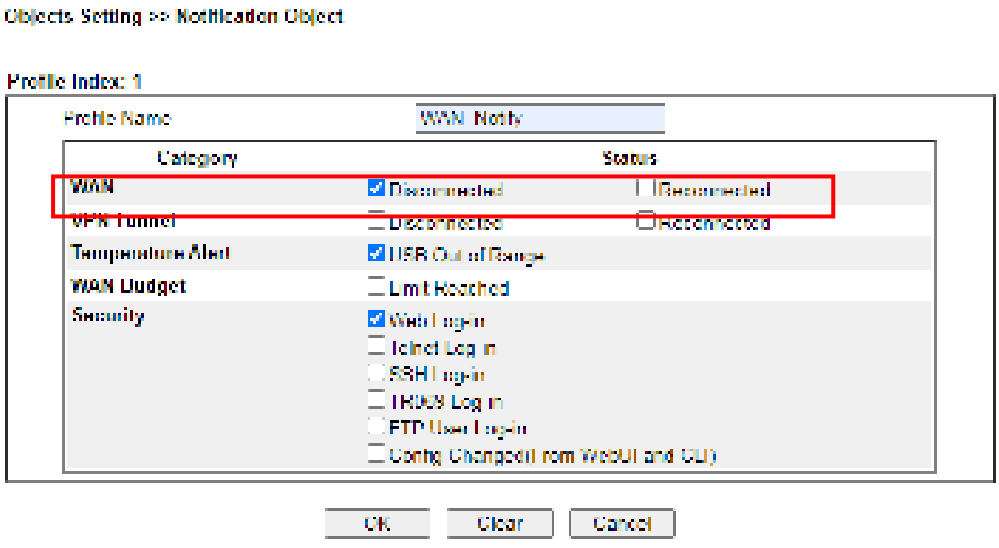
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.



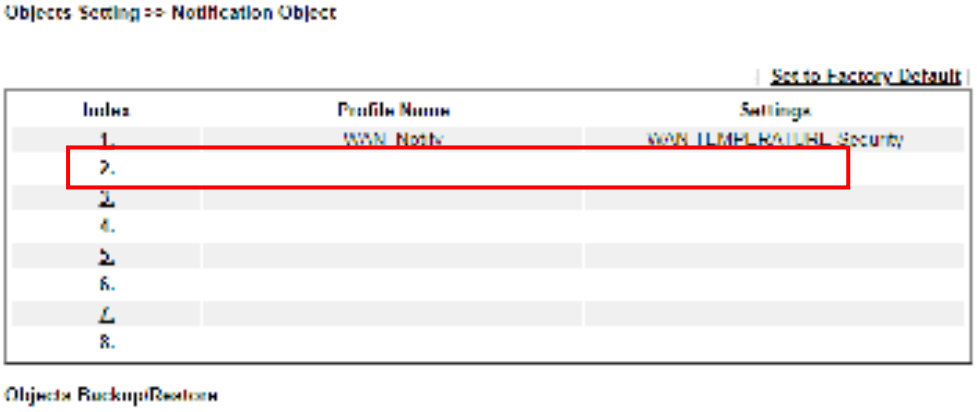
5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.



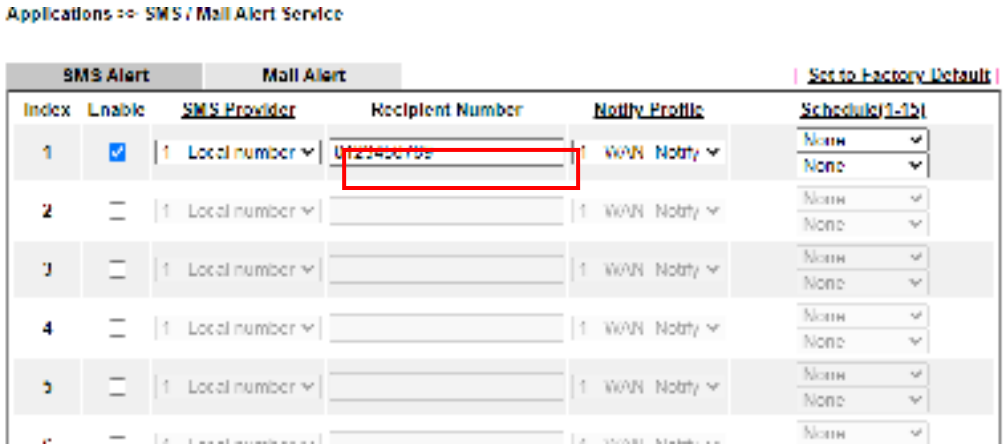
6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, Enter the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.



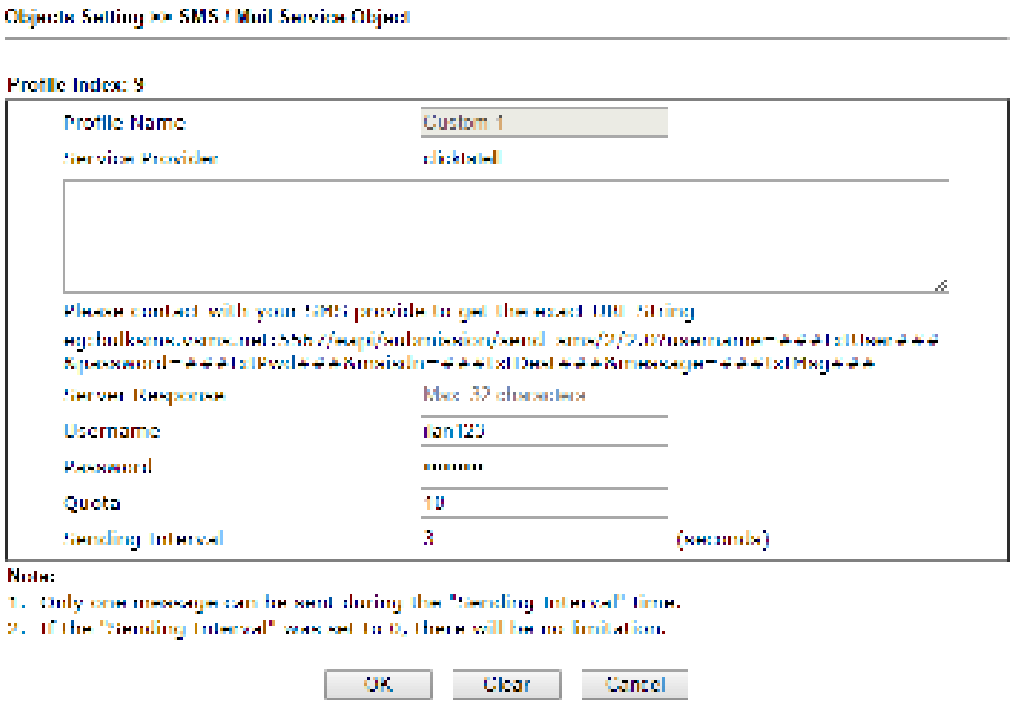
8. Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, Enter the phone number in the field of Recipient (the one who will receive the SMS).



9. Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, Enter the URL string of the SMS provider and Enter the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.



VII-2 USB Application

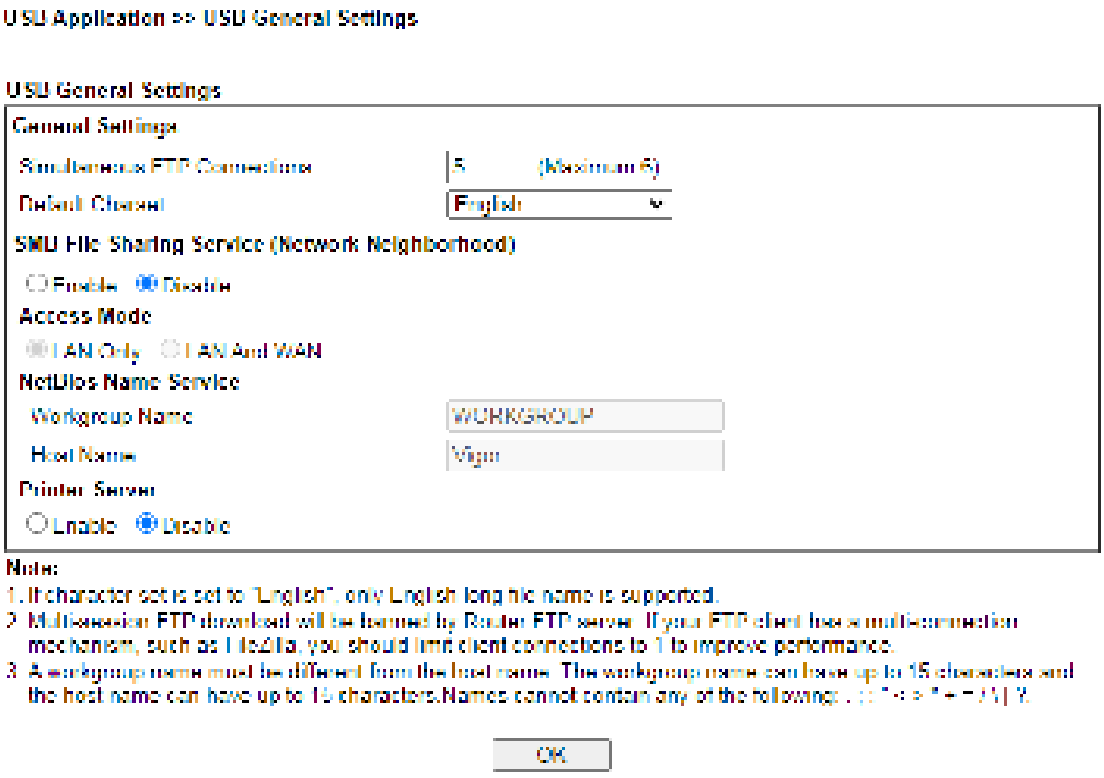
USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can Enter the IP address of the Vigor router and username/ password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the SMB service through Vigor router.

Info	USB ports on Vigor router are allowed to connect to USB modem. Models of the modems supported by Vigor router can be seen from **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>Internet Access** and **WAN>>General Setup** for detailed information.

Web User Interface

VII-2-1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable SMB service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).



Available settings are explained as follows:

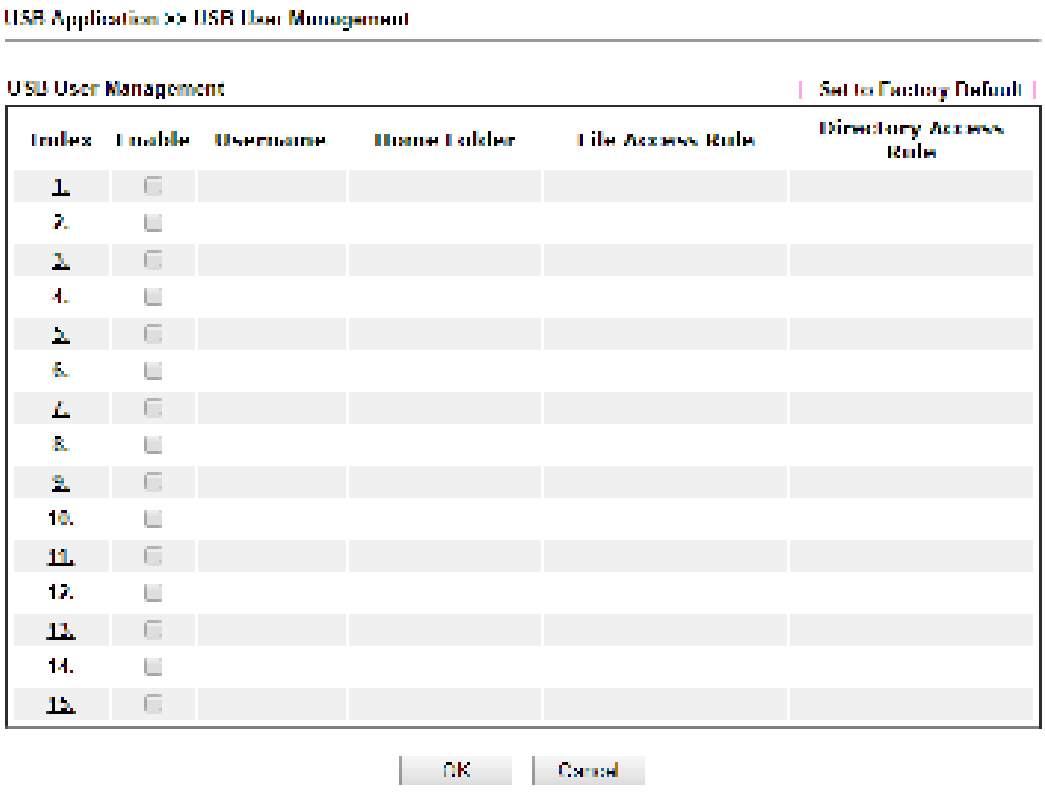
Item	Description
General Settings	**Simultaneous FTP Connections -** This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time. **Default Charset -** At present, Vigor router supports four

	types of character sets. Default Charset is for English based file name.
SMB File Sharing Service	Click **Enable** to invoke SMB service (file sharing) via the router.
Access Mode	**LAN Only** –Users coming from internet cannot connect to the SMB server of the router. **LAN And WAN** - Both LAN and WAN users can access SMB server of the router.
NetBios Name Service	For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ | ?. **Workgroup Name –** Type a name for the workgroup. **Host Name –** Enter the host name for the router.
Printer Server	**Enable** –Click it to make Vigor router act as a printer server (with USB printer attached).

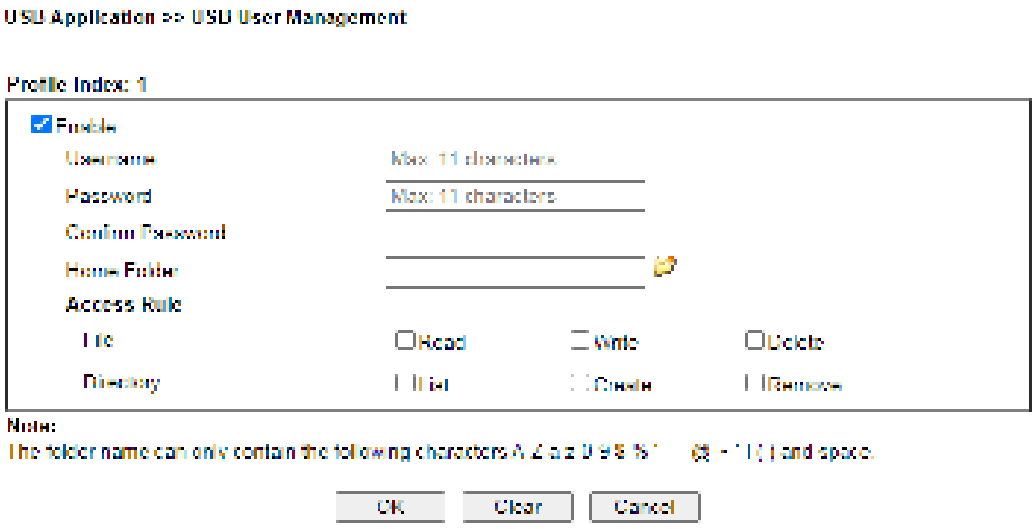
After finishing all the settings here, please click **OK** to save the configuration.

VII-2-2 USB User Management

This page allows you to set profiles for FTP/SMB users. Any user who wants to access into the USB storage disk must Enter the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.



Click index number to access into configuration page.



Available settings are explained as follows:

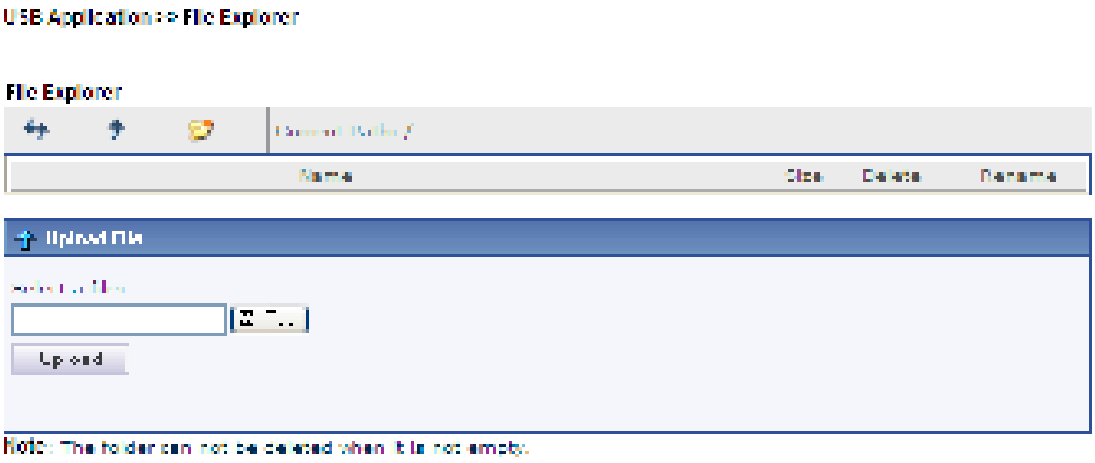
Item	Description
Enable	Check it to activate this profile (account) for FTP service or SMB file sharing service. Later, the user can use the username specified in this page to login into FTP server.
Username	Enter the username for FTP/ SMB users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and Enter the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters. **Note:** "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage. **Note:** FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.
Password	Enter the password for FTP/ SMB users for accessing FTP server. Later, you can open FTP client software and Enter the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.
Confirm Password	Enter the password again to make confirmation.
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/ new folder in the USB storage disk. In addition, if the user types "/" here, he/ she can access into all of the disk folders and files in USB storage disk. **Note:** When write protect status for the USB storage disk is **ON**, you cannot type any new folder name in this field. Only "/" can be used in such case. You can click to open the following dialog to add any new folder which can be specified 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.

Before you click **OK**, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

VII-2-3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.



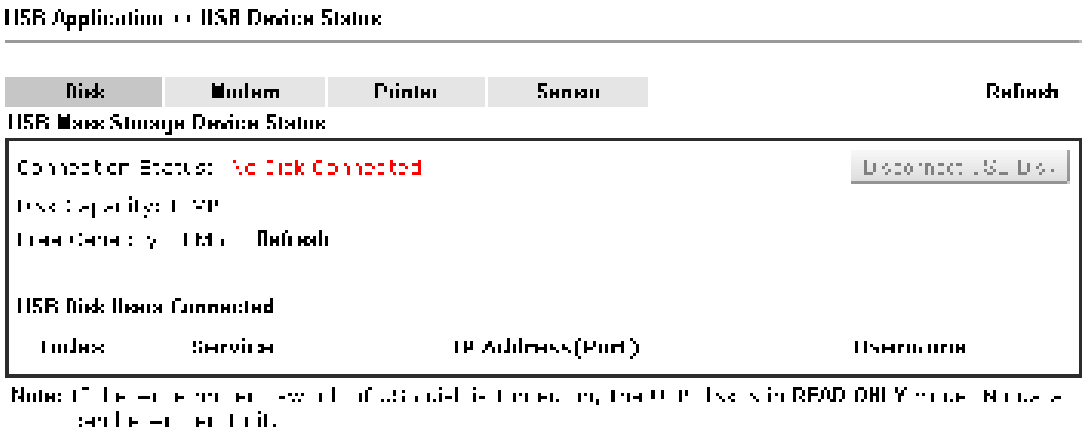
Available settings are explained as follows:

Item	Description
Refresh	Click this icon to refresh files list.
Back	Click this icon to return to the upper directory.
Create	Click this icon to add a new folder.
Current Path	Display current folder.

Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

VII-2-4 USB Device Status

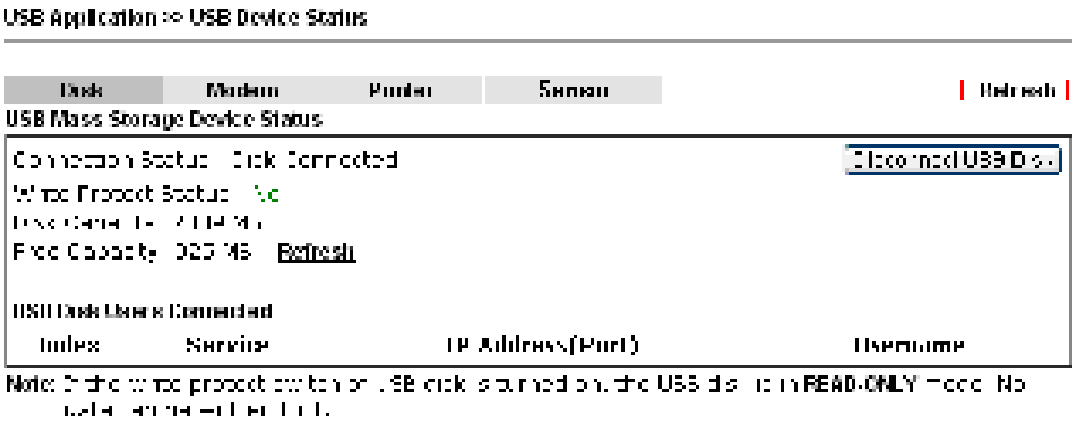
This page is to monitor the status for USB device connecting to Vigor router. . In addition, the status of the USB modem or USB printer or USB sensor connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB device later.



Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB device connected to Vigor router, "**No Disk Connected**" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click **Refresh** at any time to get new status for free capacity.
Index	It displays the number of the client which connects to FTP server.
IP Address	It displays the IP address of the user's host which connects to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB device into the Vigor router, the system will start to find out such device within several seconds.



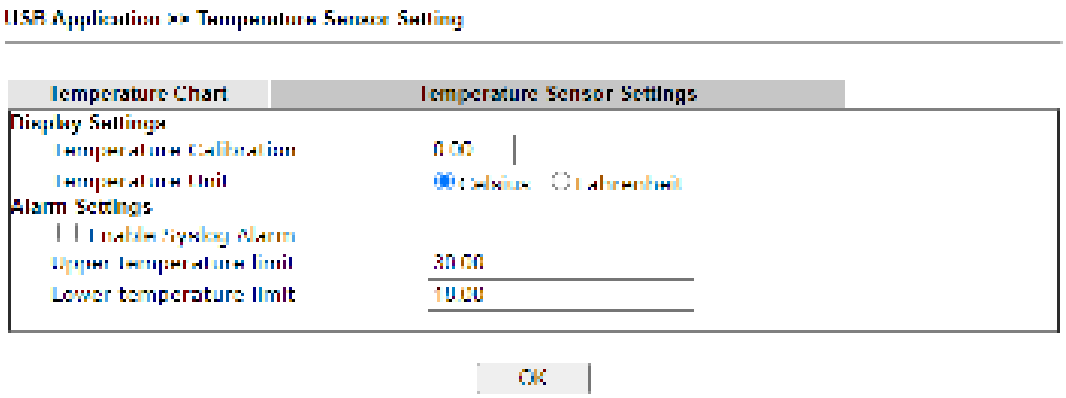
VII-2-5 Temperature Sensor

A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

Temperature Sensor Settings



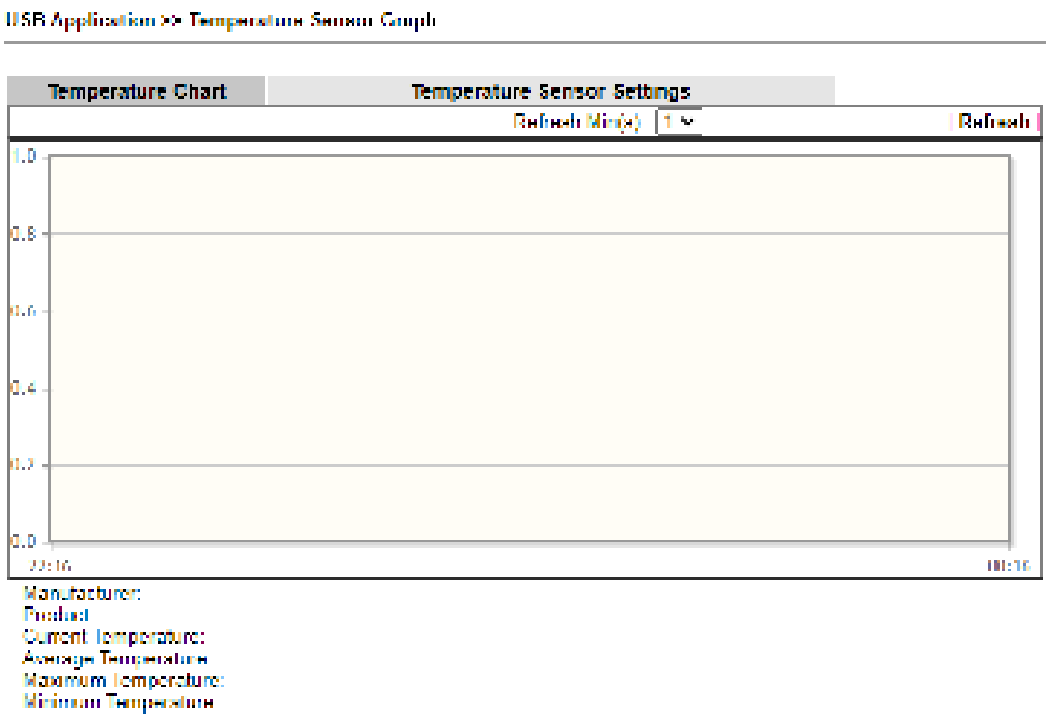
Available settings are explained as follows:

Item	Description

Display Settings	**Temperature Calibration** - Type a value used for correcting the temperature error. **Temperature Unit -** Choose the display unit of the temperature. There are two types for you to choose.
Alarm Settings	**Enable Syslog Alarm** - The temperature log will be recorded on Syslog if it is enabled. **Upper temperature limit/Lower temperature limit** - Enter the upper limit and lower limit for the system to send out temperature alert.

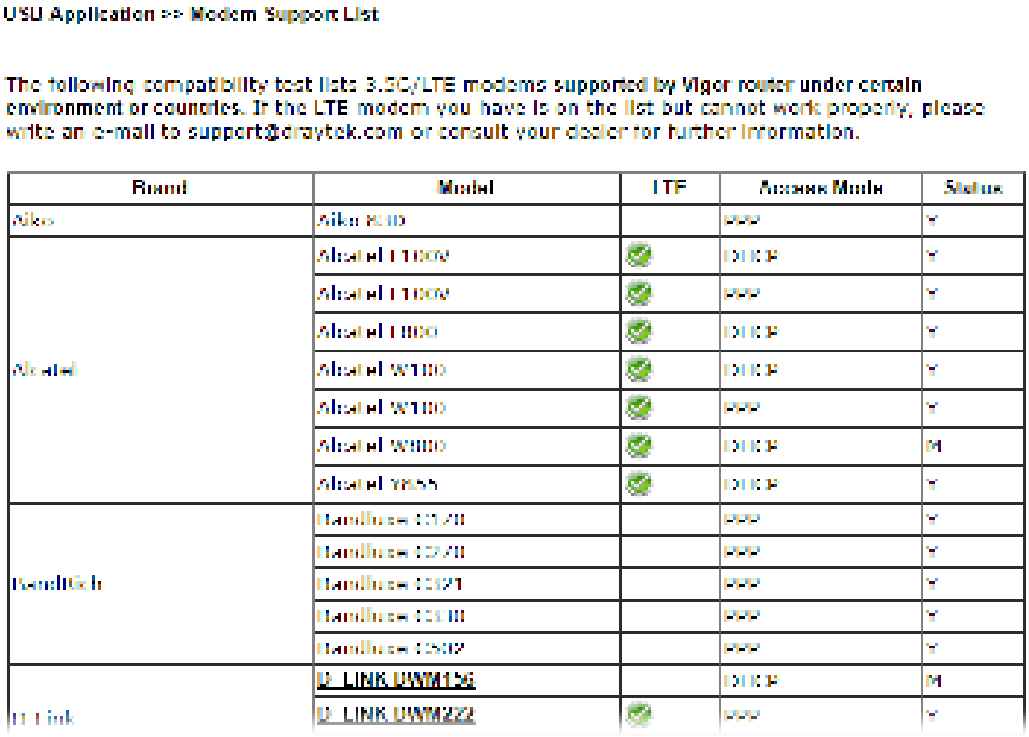
Temperature Chart

Below shows an example of temperature graph:



VII-2-6 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.



USB Application >> Modem Support List

The following compatibility test lists 3.3G/LTE modems supported by Vigor router under certain environment or countries. If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

Brand	Model	ITF	Access Mode	Status
Aiko	Aiko [illegible]		[illegible]	V
Alcatel	Alcatel [illegible]	✓	[illegible]	V
	Alcatel [illegible]	✓	[illegible]	V
	Alcatel [illegible]	✓	[illegible]	V
	Alcatel [illegible]	✓	[illegible]	V
	Alcatel [illegible]	✓	[illegible]	V
	Alcatel [illegible]	✓	[illegible]	M
	Alcatel [illegible]	✓	[illegible]	V
BandLuxe	BandLuxe [illegible]		[illegible]	V
	BandLuxe [illegible]		[illegible]	V
	BandLuxe [illegible]		[illegible]	V
	BandLuxe [illegible]		[illegible]	V
	BandLuxe [illegible]		[illegible]	V
D-Link	D-LINK DWM156		[illegible]	M
	D-LINK DWM222	✓	[illegible]	V

VII-2-7 SMB Client Support List

SMB Client Support List provides the test status information for applications with file sharing operated under different platforms.

USB Application >> SMB Client Support List

The following compatibility test lists suggested SMB clients supported by Vigor router.

Platform	Application	Status
Microsoft Windows XP	Built-in	I
Microsoft Windows Vista™	Built-in	Y
Microsoft Windows 7	Built-in	Y
Microsoft Windows 8	Built-in	M
Microsoft Windows 8.1	Built-in	Y
[illegible]	Built-in	Y
[illegible]	Built-in	Y
[illegible]	Built-in	Y
Android™	Total MP	Y
Apple™	ES File Explorer	Y
Android™	[illegible]	Y
Apple™	File Manager	Y
Android™	[illegible]	Y
Apple™	SharesFinder	Y
iOS	[illegible]	Y
iOS	[illegible]	Y

Y: Tested and it supported.
I: Supported but has some issue.
M: Has not been tested but might be supported.

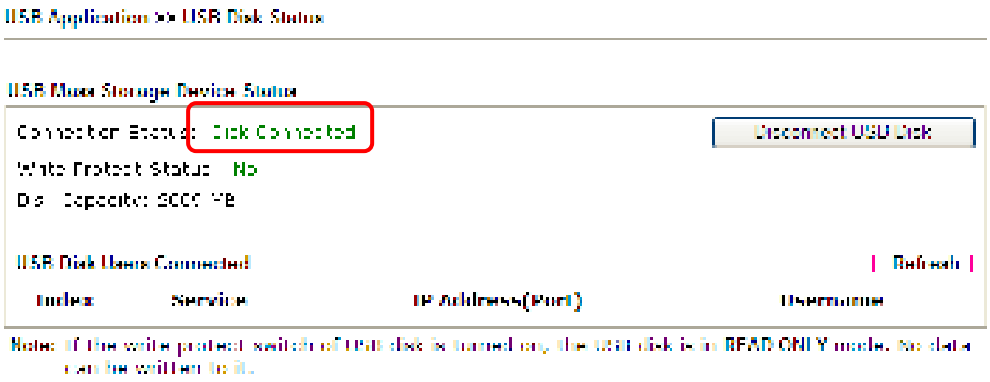
Application Notes

A-1 How can I get the files from USB storage device connecting to Vigor router?

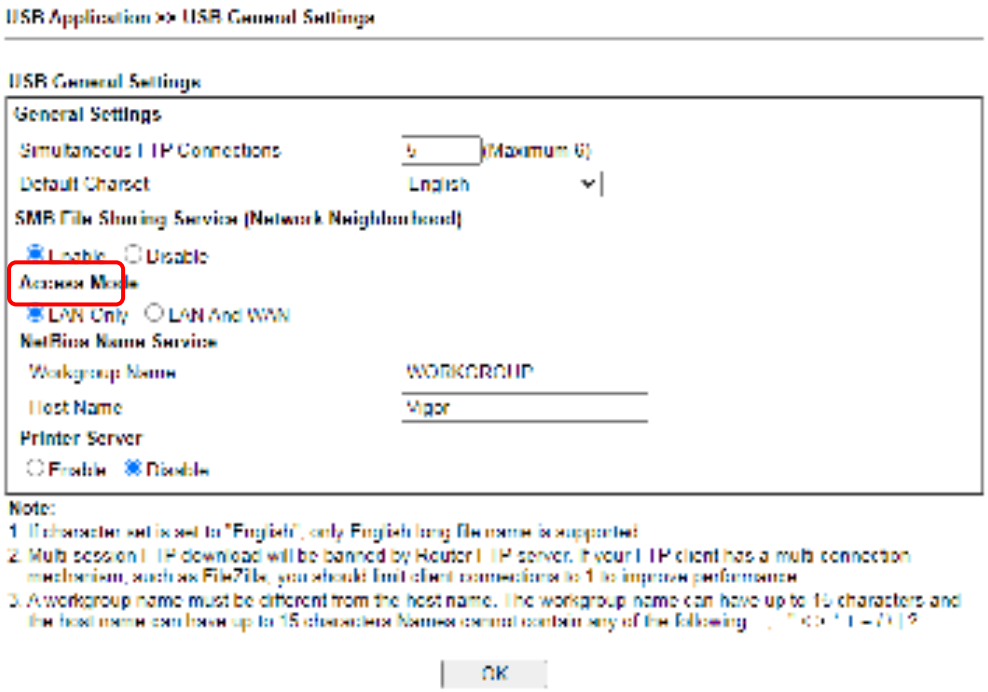
Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SMB server or FTP server.

SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

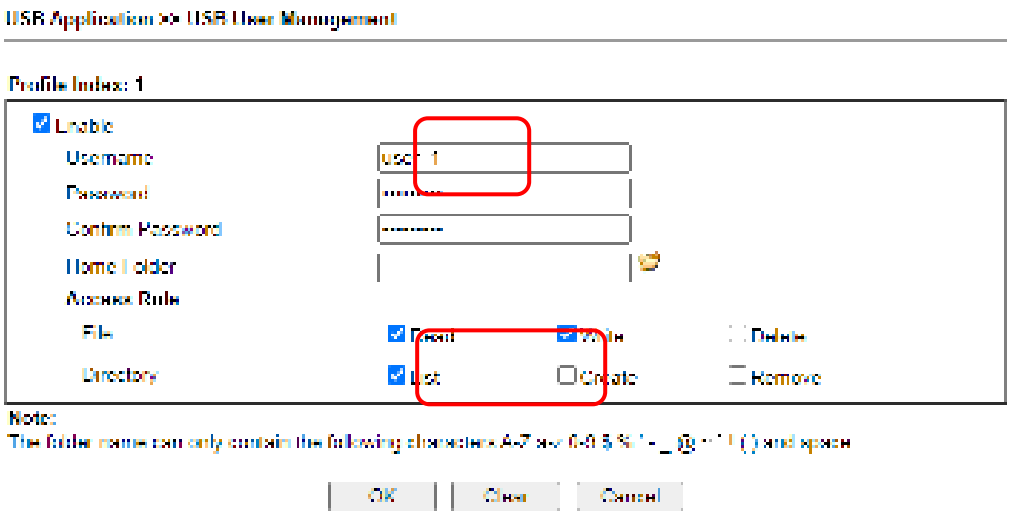
1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:



2. Then, please open **USB Application >> USB General Settings** to enable SMB service.

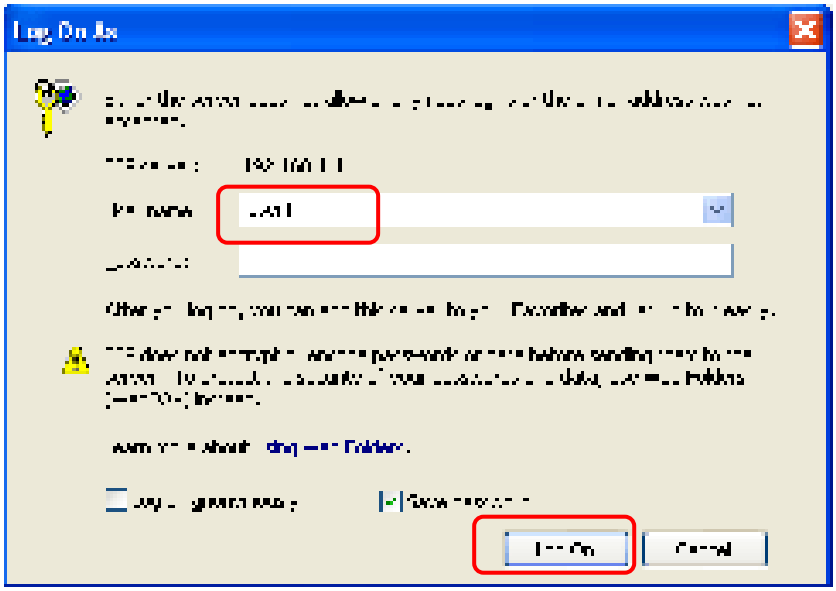


3. Setup a user account for the FTP service by using **USB Application >>USB User Management.** Click **Enable**. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

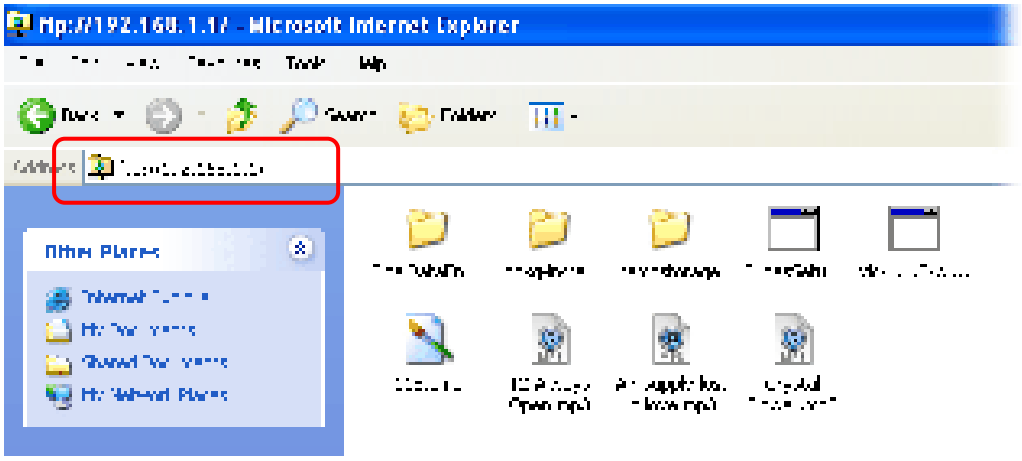


4. Click **OK** to save the configuration.

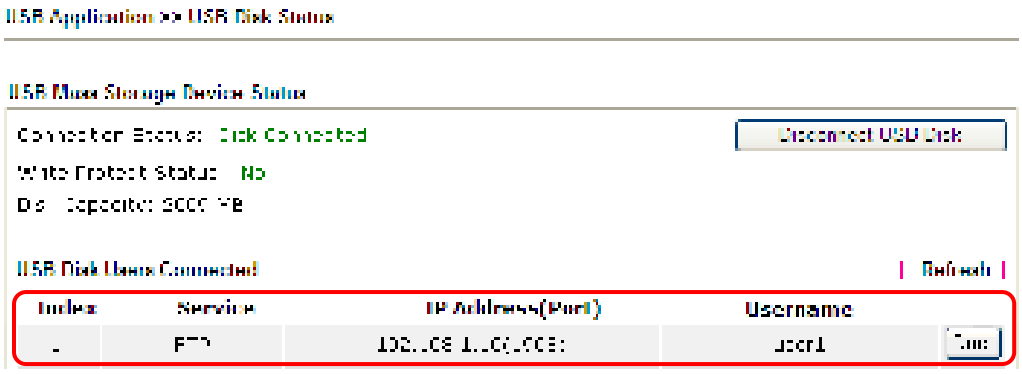
5. Make sure the FTP service is running properly. Please open a browser and type *ftp://192.168.1.1.* Use the account "**user1**" to login.



6. When the following screen appears, it means the FTP service is running properly.



7. Return to **USB Application >> USB Disk Status**. The information for FTP server will be shown as below.



Now, users in LAN of Vigor2915 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

This page is left blank.

Part VIII Troubleshooting

This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

VIII-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

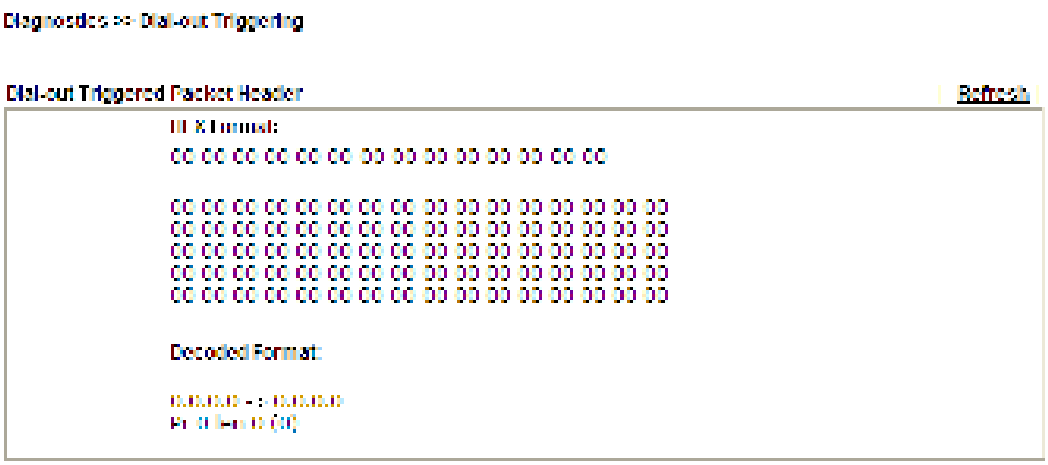
If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Web User Interface

Fisrt, take a look at the menu items under Diagnostics. Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

VIII-1-1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

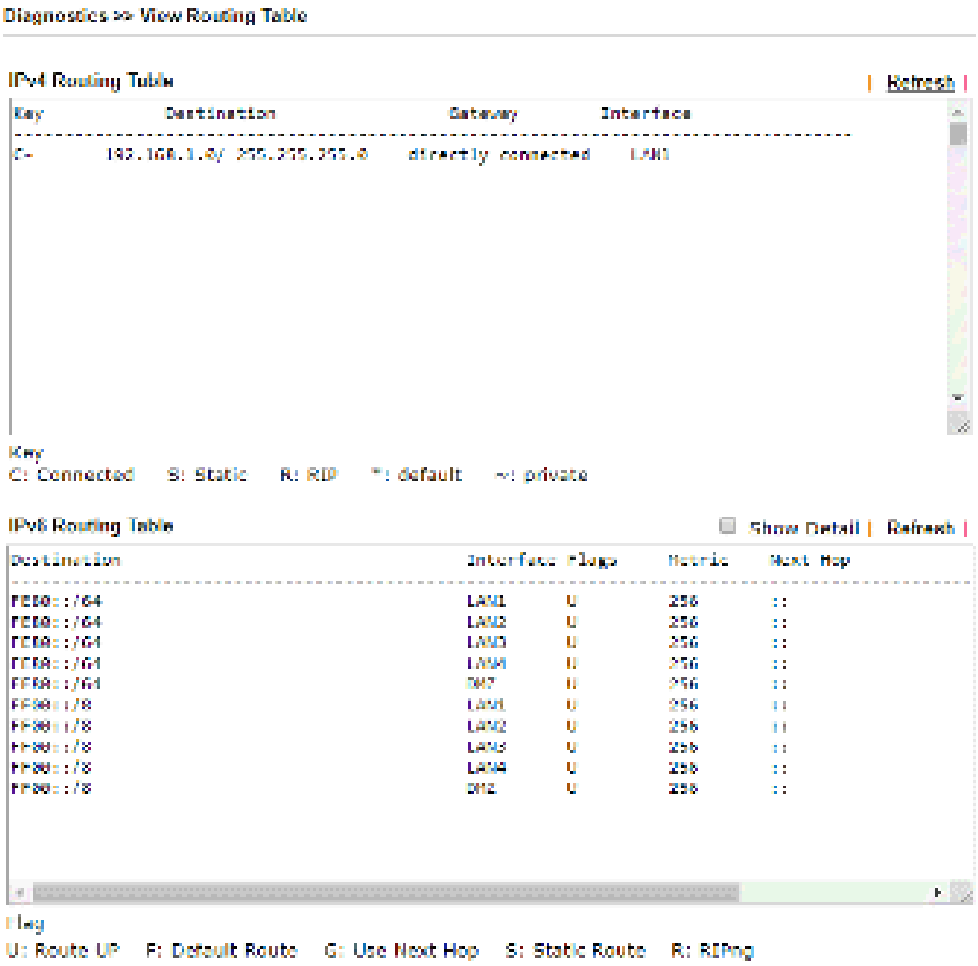


Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

VIII-1-2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

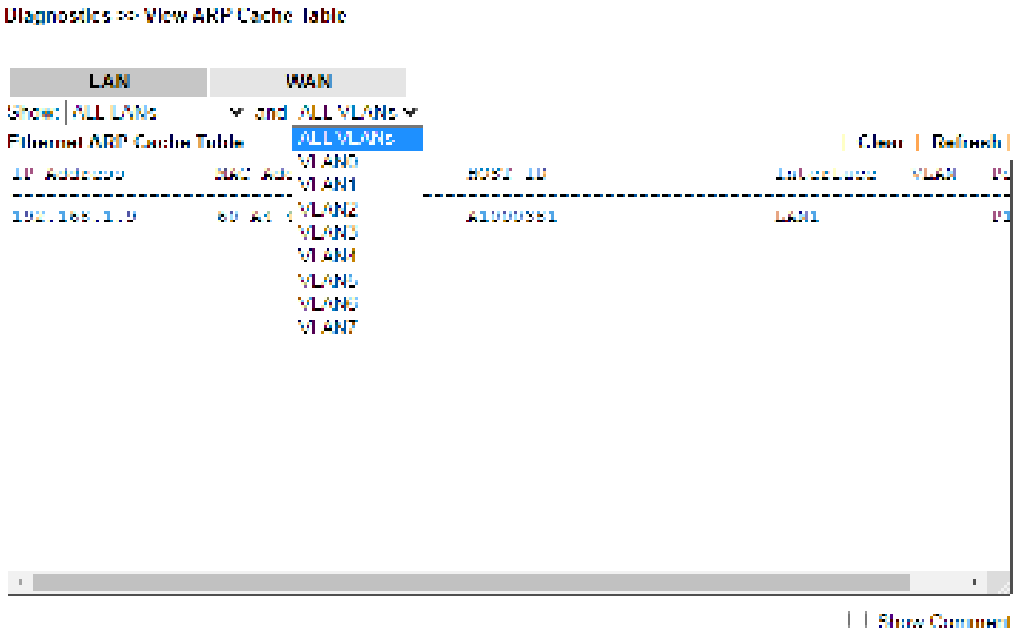


Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.



Available settings are explained as follows:

Item	Description
Show	Specify LAN and VLAN to display related information. In default, this page will display all of the information about LAN and VLAN.
Refresh	Click it to reload the page.

VIII-1-4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

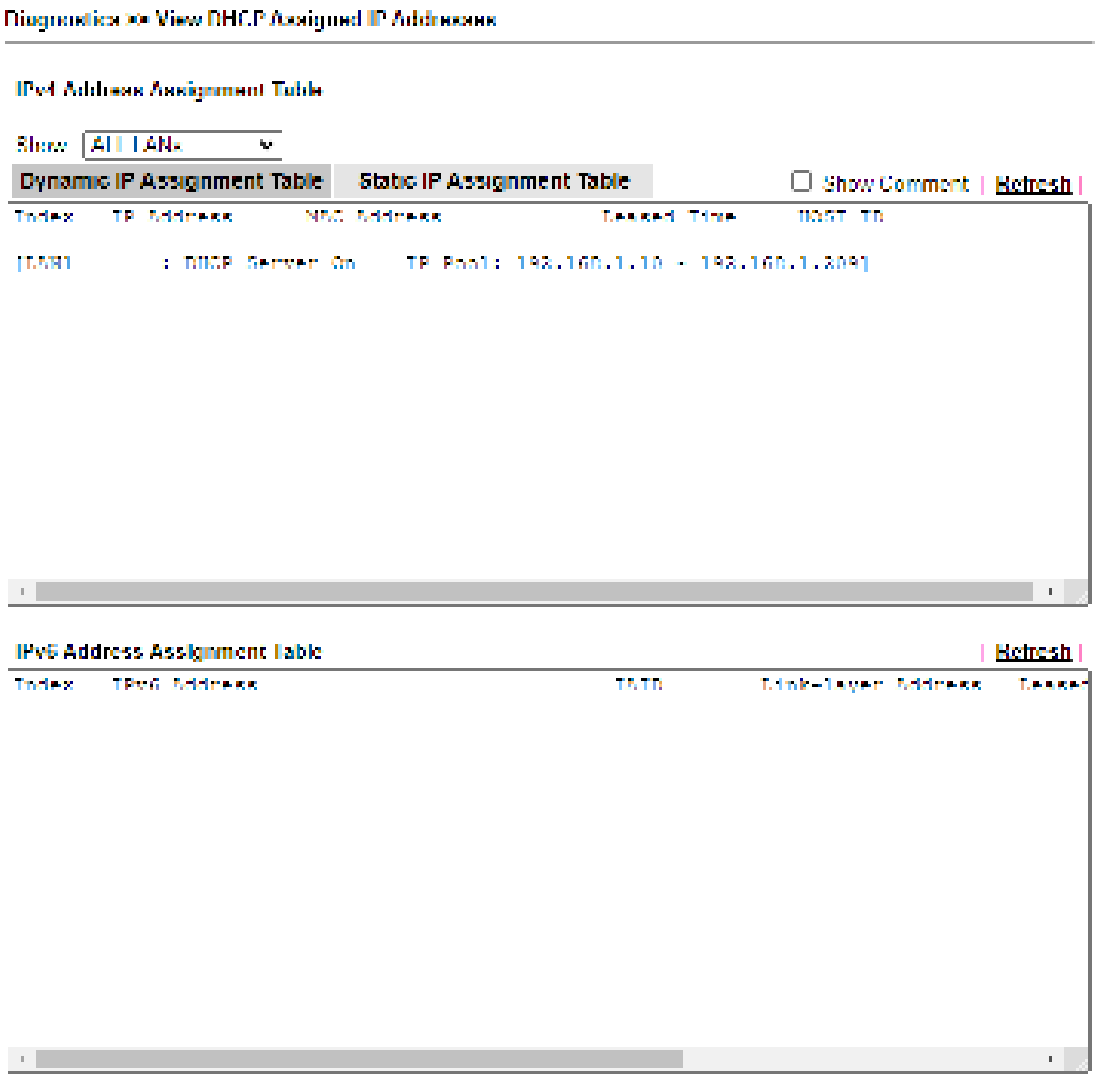
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

VIII-1-5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

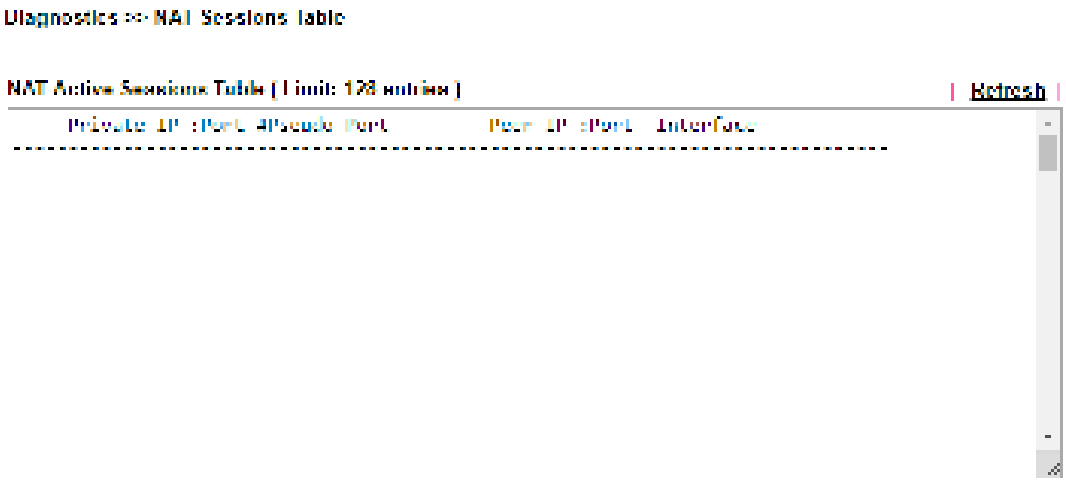


Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

VIII-1-6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.



Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

VIII-1-7 DNS Cache Table

Click **Diagnostics** and click **DNS Cache Table** to open the web page.

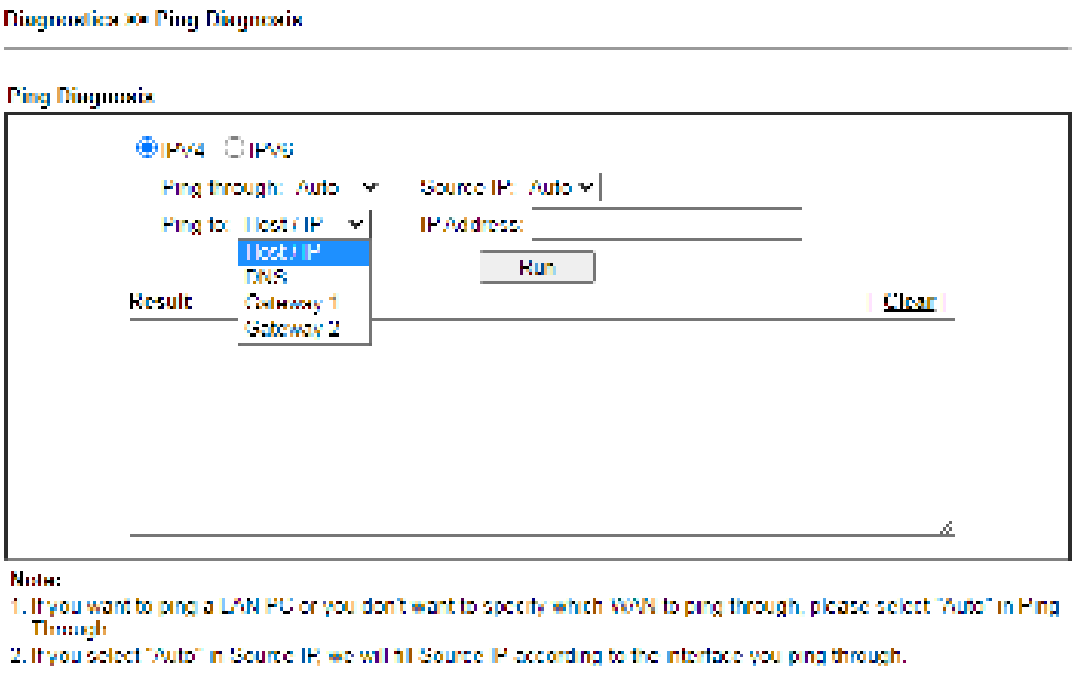
The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Available settings are explained as follows:

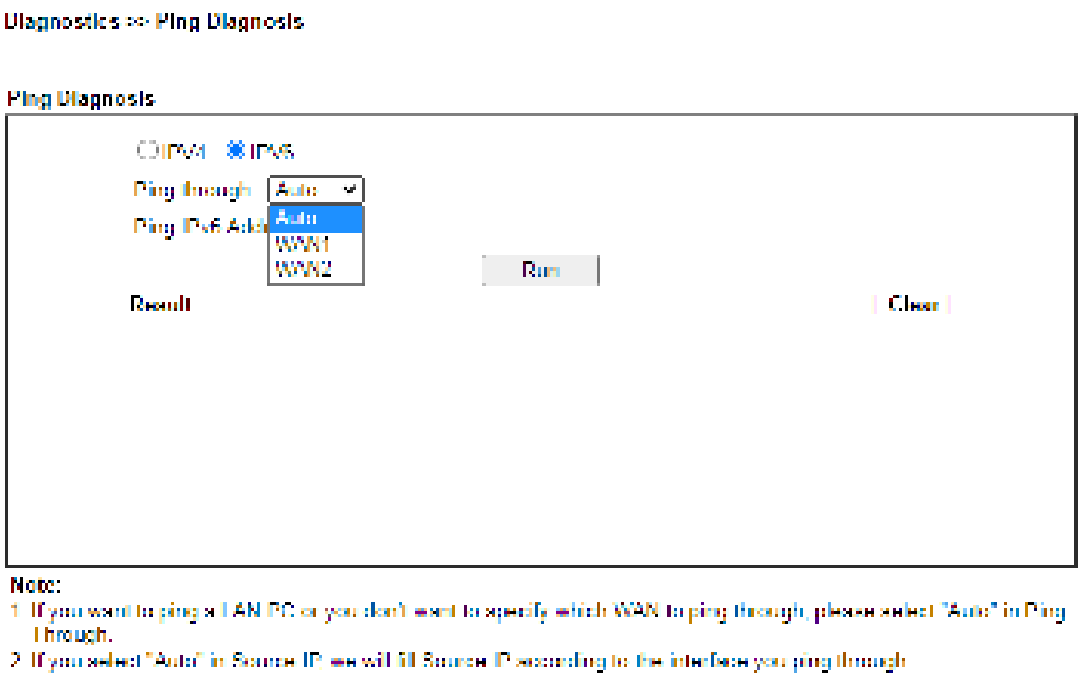
Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than...	Check the box the Enter the value of TTL (time to live) for each entry. Click **OK** to enable such function. It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

VIII-1-8 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to open the web page.



or



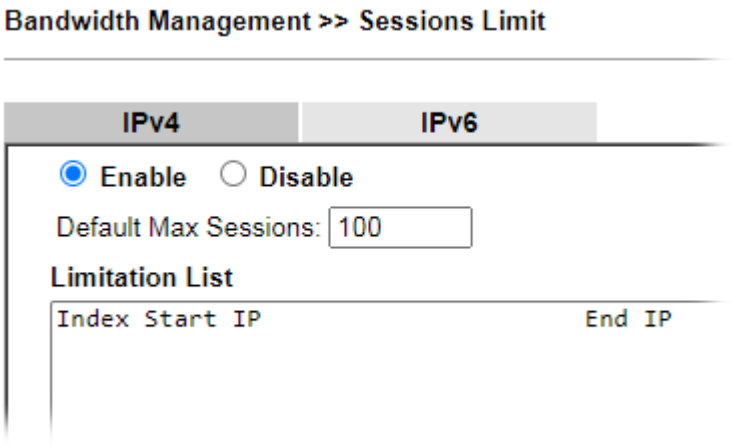
Available settings are explained as follows:

Item	Description
IPV4 / IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN/ LTE interface that you want to ping through or choose **Auto** to be determined by the router automatically.

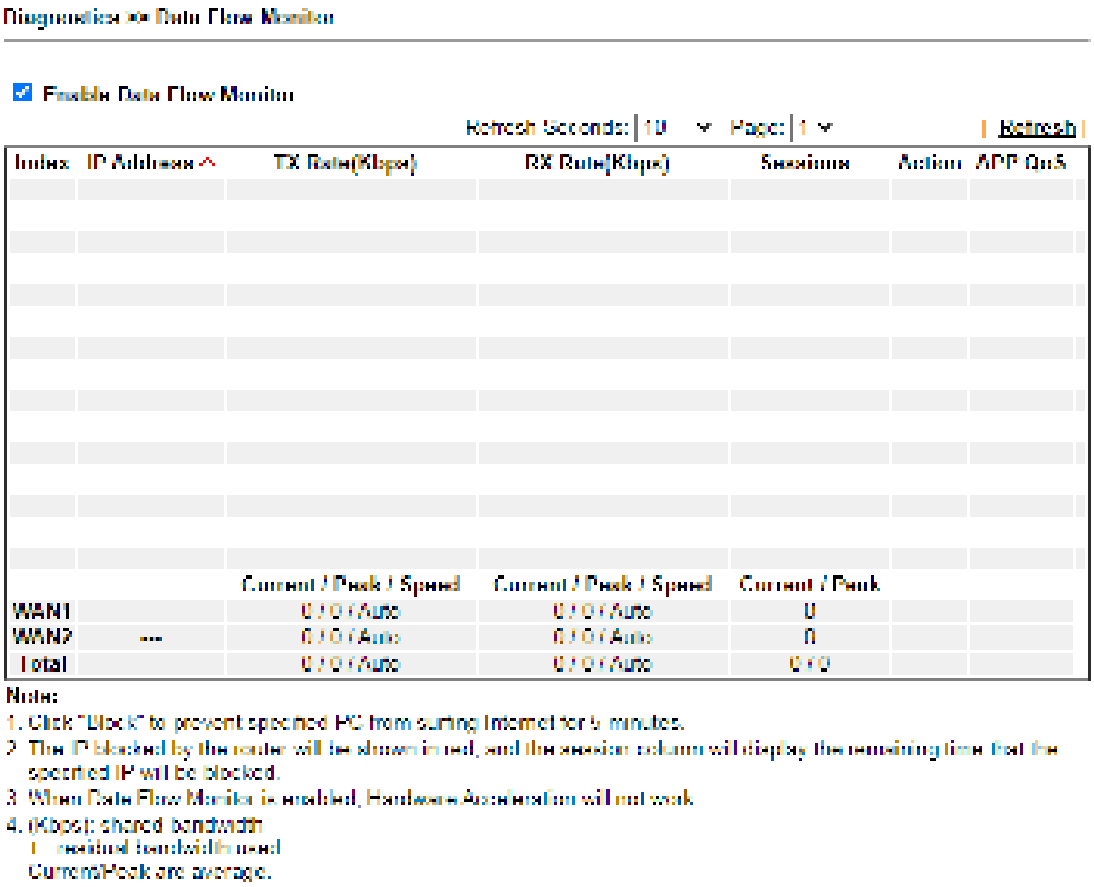
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Enter the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Enter the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

VIII-1-9 Data Flow Monitor

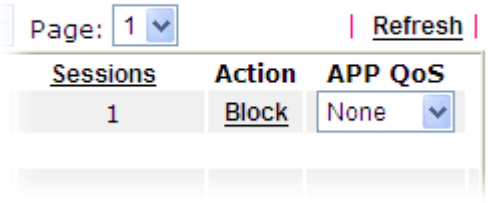
This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoking Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

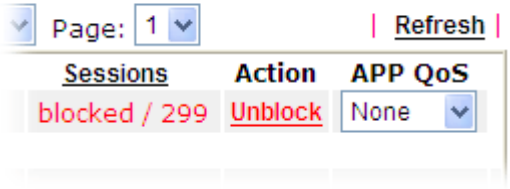
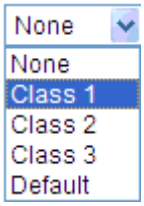


Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.



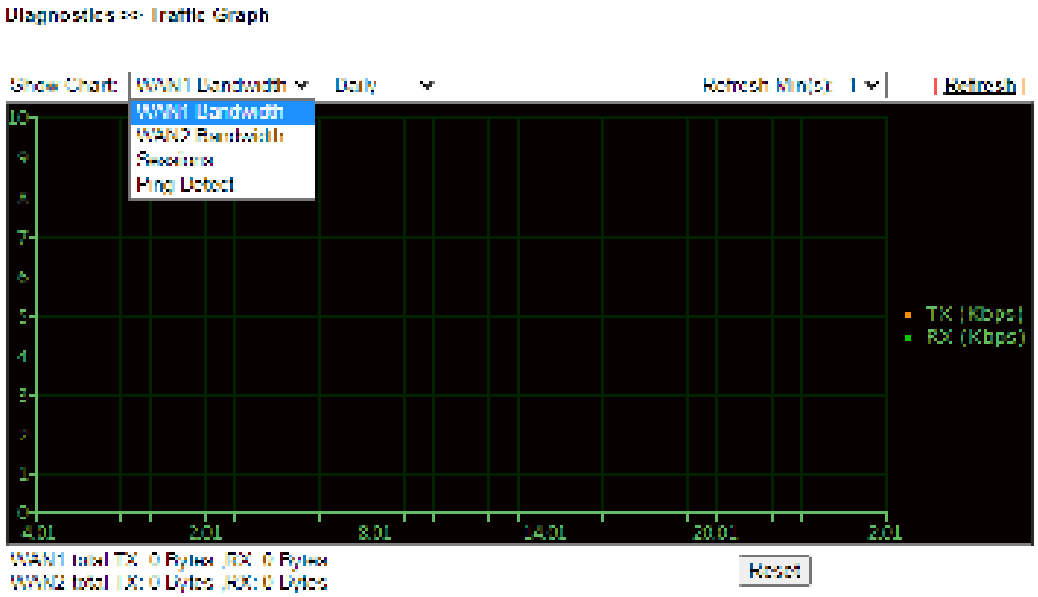
Available settings are explained as follows:

Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.  **Unblock** –The device with the IP address will be blocked for

	five minutes. The remaining time will be shown on the session column. Click it to cancel the IP address blocking. 
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host). 
Current /Peak/Speed	**Current** means current transmission rate and receiving rate for WAN interface. **Peak** means the highest peak value detected by the router in data transmission. **Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

VIII-1-10 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2 Bandwidth, Sessions, Ping Detect, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.

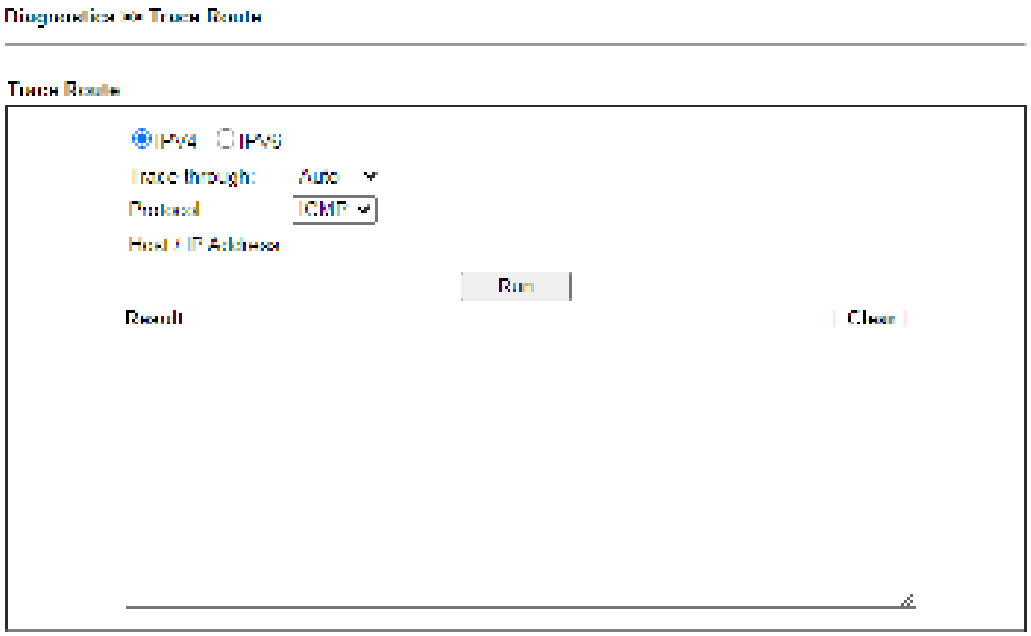


The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

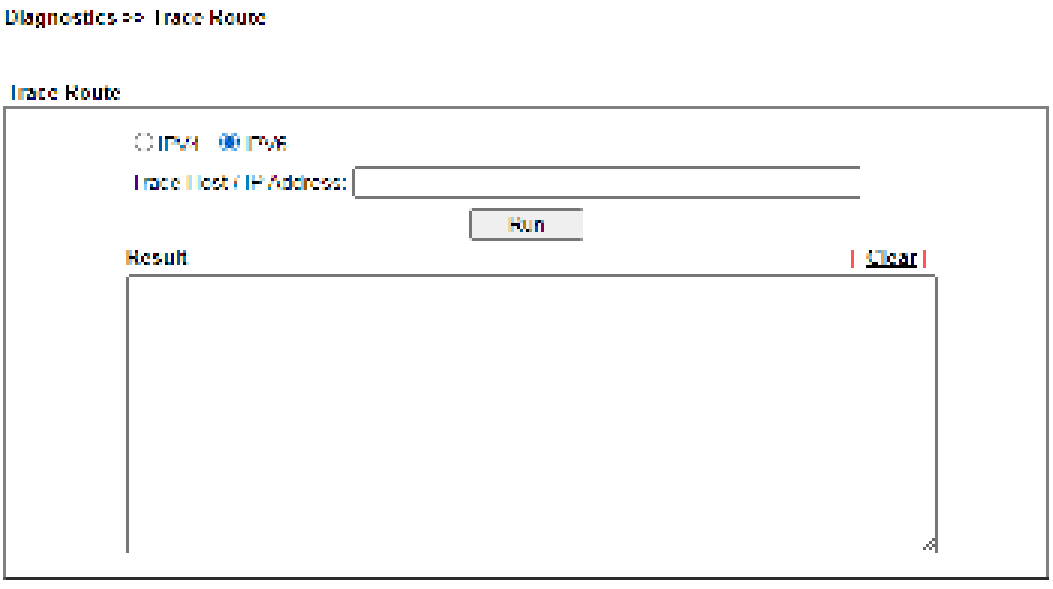
For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

VIII-1-11 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply Enter the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



or



Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Trace through	Use the drop down list to choose the interface that you want to ping through.

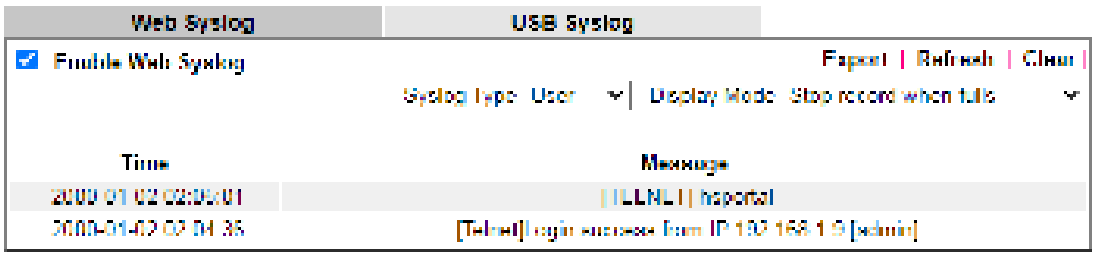
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

VIII-1-12 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

For Web Syslog

This page displays the time and message for User/ Firewall/ call/ WAN/ VPN settings. You can check **Enable Web Syslog,** specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

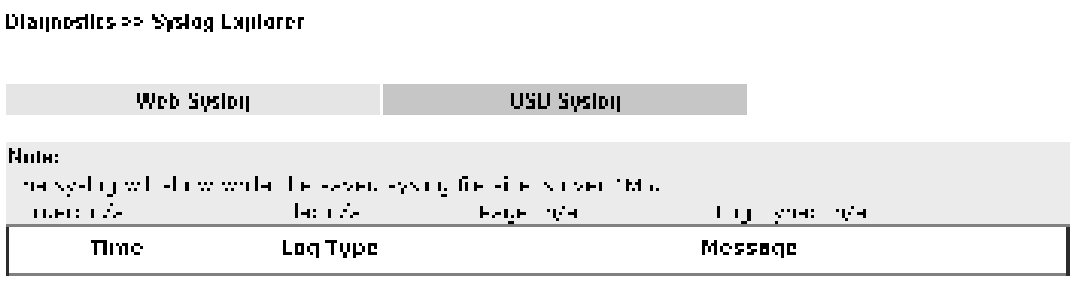


Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed.
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose. **Stop record when fulls** – when the capacity of syslog is full, the system will stop recording. **Always record the new event** – only the newest events will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.



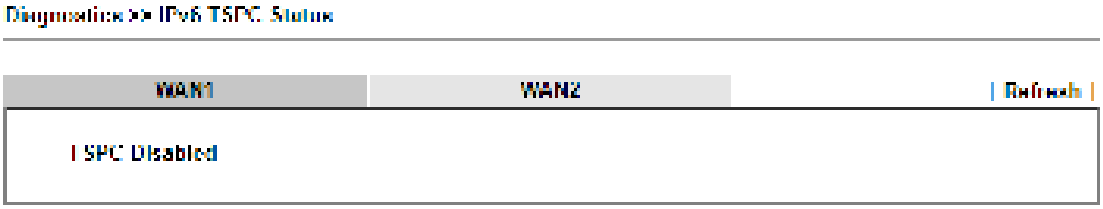
Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

VIII-1-13 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.



Available settings are explained as follows:

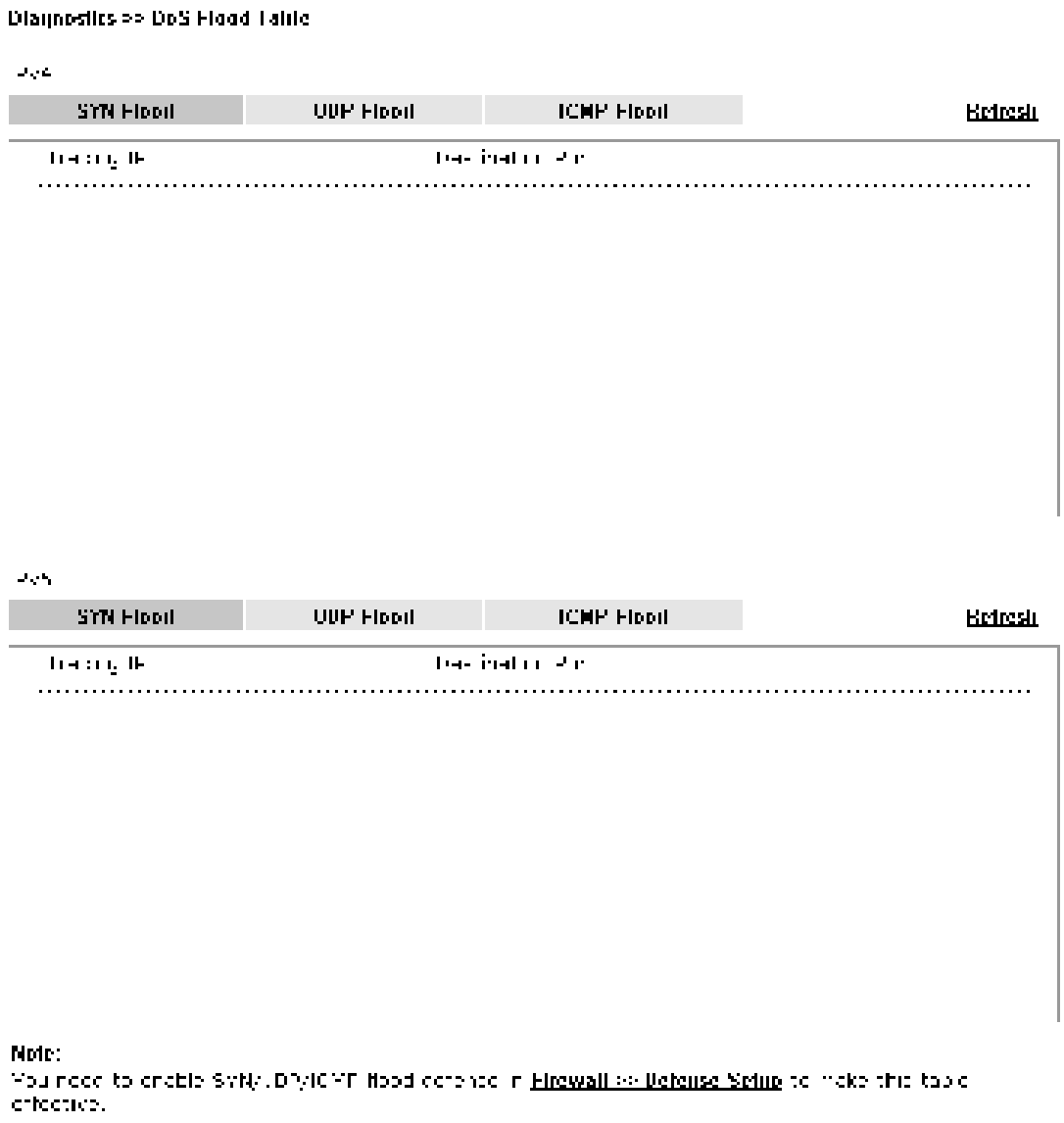
Item	Description
Refresh	Click this link to refresh this page manually.

VIII-1-14 DoS Flood Table

This page can display content of IP connection detected by DoS Flooding Defense mechanism. It is useful and convenient for network engineers (e.g., MIS engineer) to inspect the network environment to find out if there is any abnormal connection.

Information of IP traced and destination port used for SYN Flood, UDP Flood and ICMP Flood attacks will be detected and shown respectively on different pages.

Moreover, IP address detected and suspected to attack the network system can be blocked shortly by clicking the **Block** button shown on pages of SYN Flood, UDP Flood and ICMP Flood.

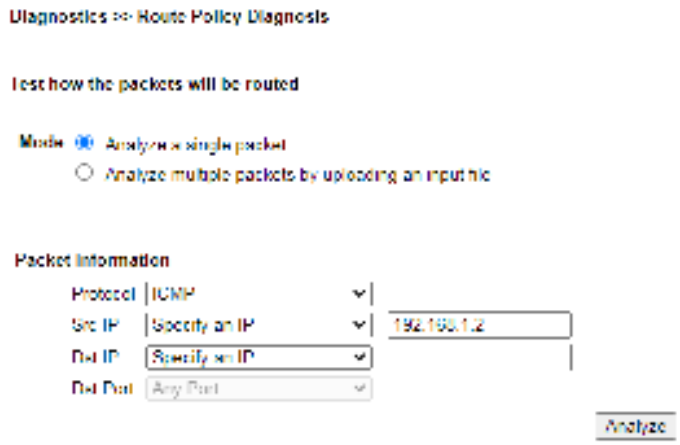


Info

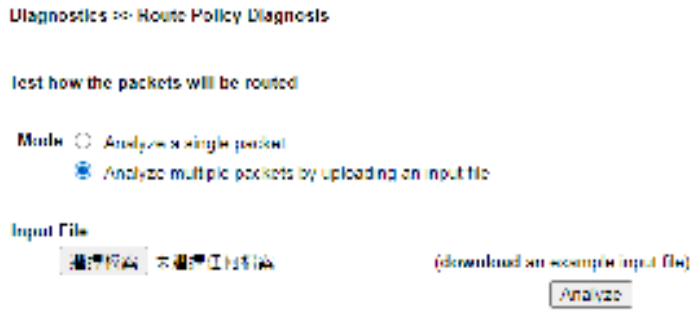
The icon - ( ) - means there is something wrong (e.g., attacking the system) with that IP address.

VIII-1-15 Route Policy Diagnosis

With the analysis done by such page, possible path (static route, routing table or policy route) of the packets sent out of the router can be traced.



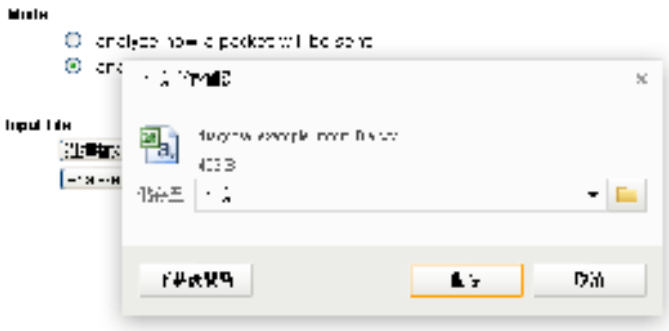
or



Available settings are explained as follows:

Item	Description
Mode	**Analyze a single packet** – Choose such mode to make Vigor router analyze how a single packet will be sent by a route policy. **Analyze multiple packets**...- Choose such mode to make Vigor router analyze how multiple packets in a specified file will be sent by a route policy.
Packet Information	Specify the nature of the packets to be analyzed by Vigor router. **ICMP/UDP/TCP/ANY-** Specify a protocol for diagnosis. **Src IP** – Type an IP address as the source IP. **Dst IP** – Type an IP address as the destination IP. **Dst Port** – Use the drop down list to specify the destination port. **Analyze** – Click it to perform the job of analyzing. The analyzed result will be shown on the page..
Input File	It is available when Analyze multiple packets.. is selected as **Mode.** **Select** – Click the download link to get a blank example file.

Then, click such button to select that blank ".csv" file for saving the result of analysis.



Analyze – Click it to perform the job of analyzing. The analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file.

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

VIII-2 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/ LAN cable connections.
   Refer to "**I-2 Hardware Installation**" for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.

3. If not, it means that there is something wrong with the hardware status. Simply back to "**I-2 Hardware Installation**" to execute the hardware installation again. And then, try again.

VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not

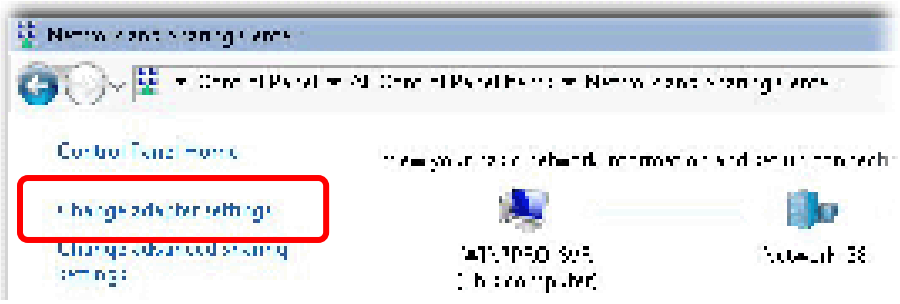
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

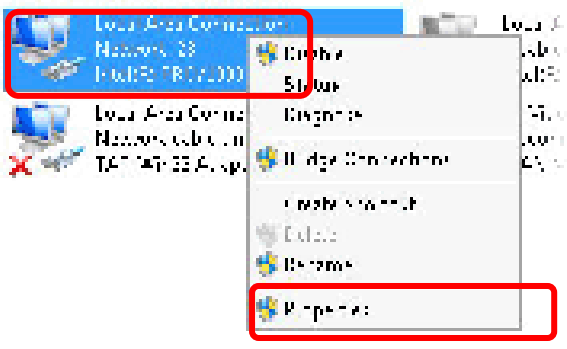
Info	The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

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

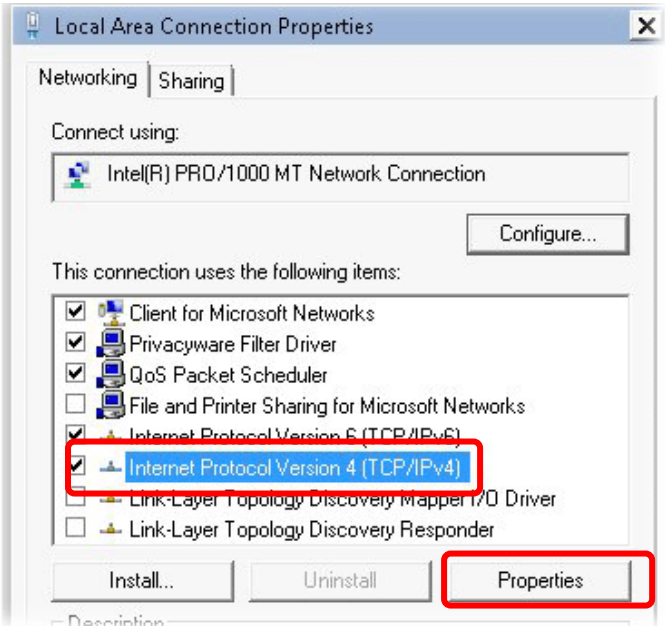
2. In the following window, click **Change adapter settings**.



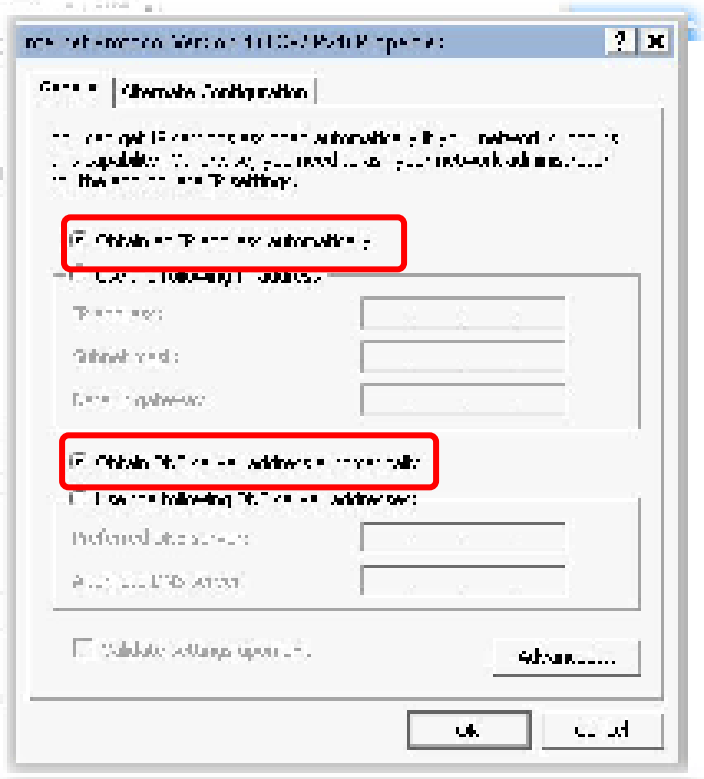
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

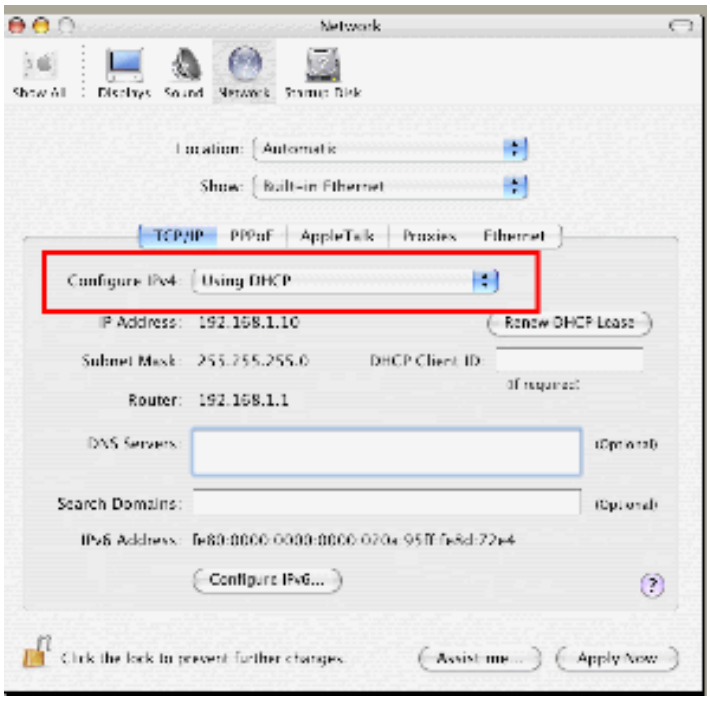


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

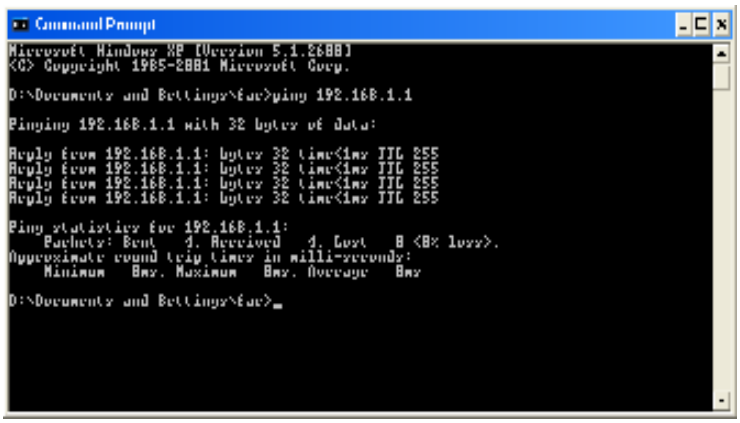


VIII-4 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the previous section IX-3) Please follow the steps below to ping the router correctly.

For Windows

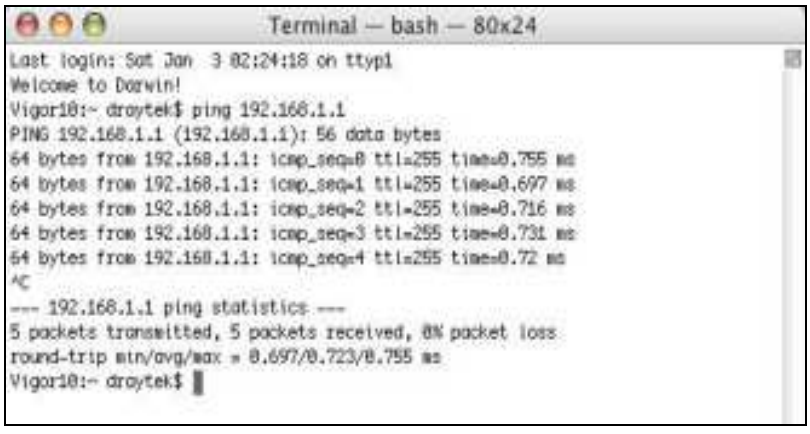
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/ 98/ ME) or **cmd** (for Windows NT/ 2000/ XP/ Vista/ 7). The DOS command dialog will appear.



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.



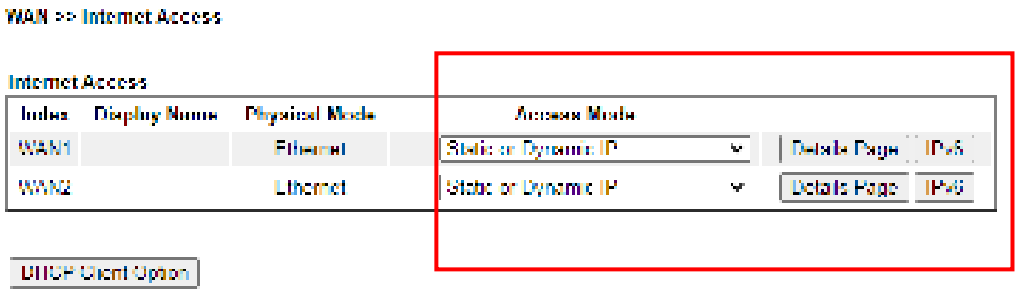
VIII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section 1.2) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, 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~WAN4 to review the settings that you configured previously.



VIII-6 Problems for 3G/4G Network Connection

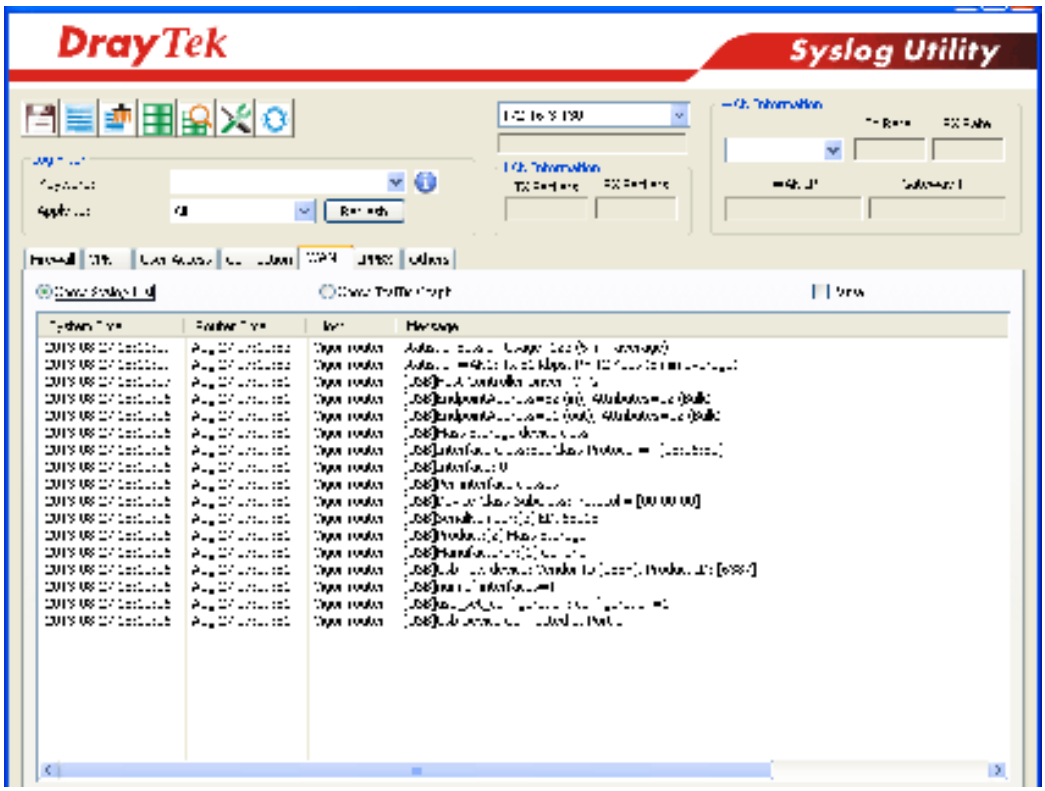
When you have trouble in using 3G/4G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2915. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2915.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G/4G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G/4G USB Modem to test the connection speed to verify if the problem is caused by Vigor2915. In addition, please refer to the manual of 3G/4G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

VIII-7 Backing to Factory Default Setting If Necessary

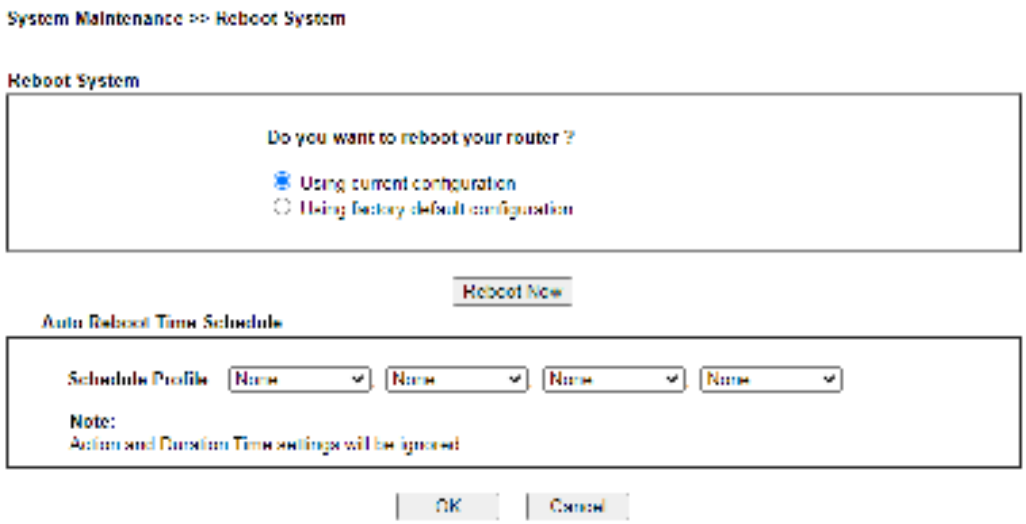
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

Info	After pressing factory default setting, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

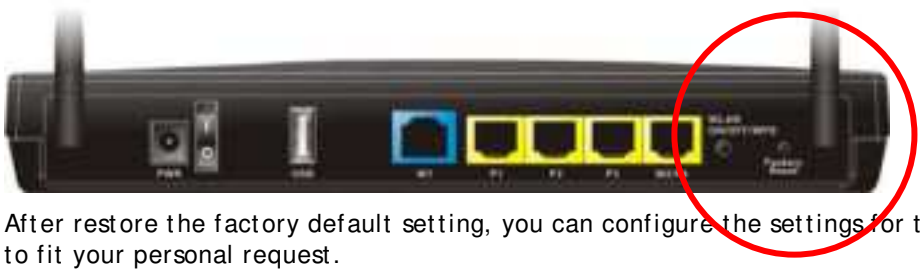
You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

This page is left blank.

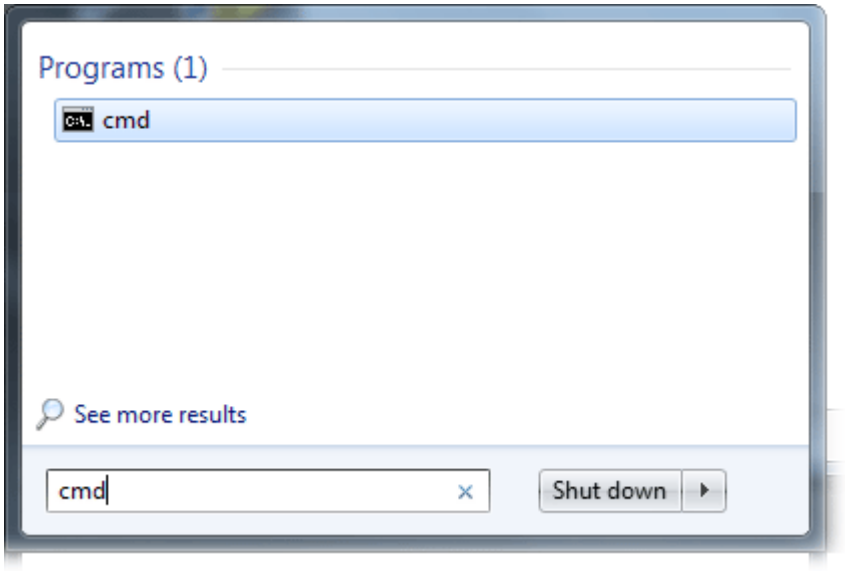
Part IX Telnet Commands

Accessing Telnet of Vigor2915

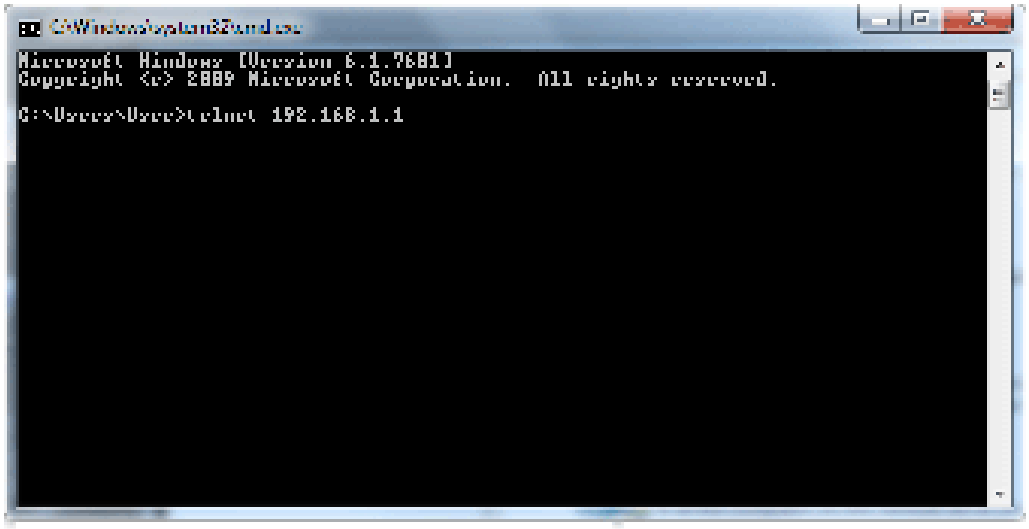
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

Info	For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under **Control Panel>>Programs**.

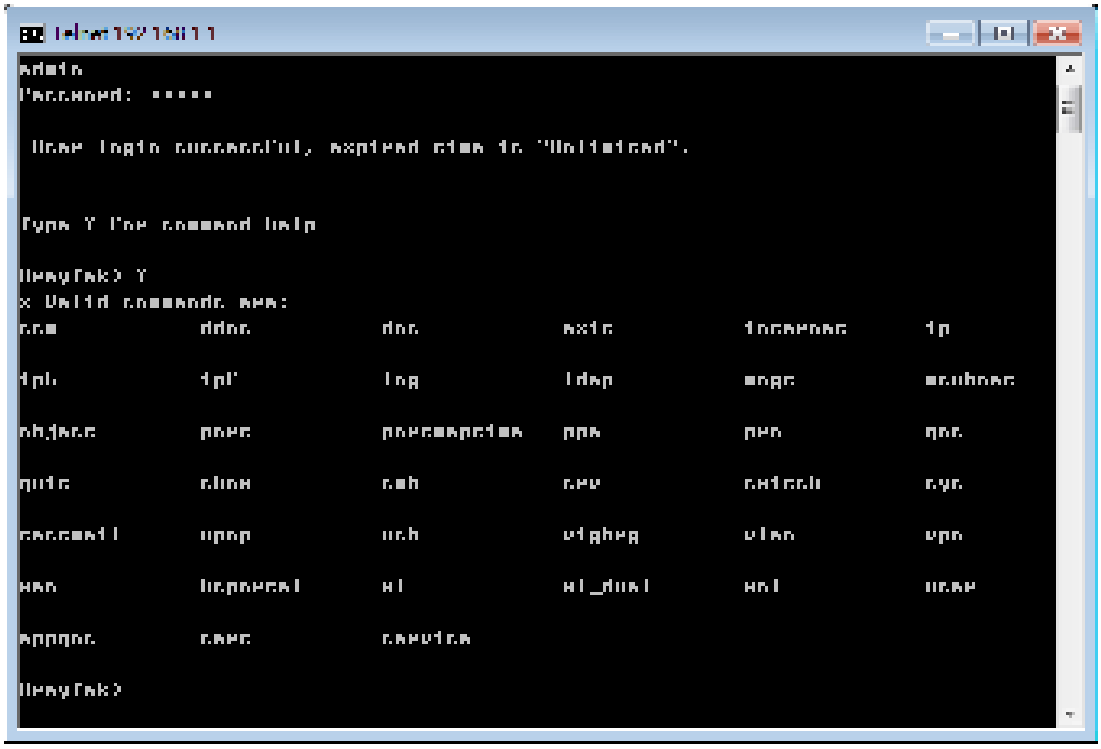
Type **cmd** and press Enter. The Telnet terminal will be open later.



In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, type admin/ admin for Account/ Password. Then, type **?**. You will see a list of valid/ common commands depending on the router that your use.


admin
Password: *****
Type Y for command help
x Valid commands are:

Telnet Command: csm appe prof

Commands under CSM allow you to set CSM profile to define policy profiles for different policy of IM (Instant Messenger)/ P2P (Peer to Peer) application.

"csm appe prof " is used to configure the APP Enforcement Profile name. Such profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

Syntax

csm appe prof -i *INDEX [-v | -n NAME| setdefault]*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 32.
- v	It means to view the configuration of the CSM profile.
- n	It means to set a name for the CSM profile.
NAME	It means to specify a name for the CSM profile, less then 15 characters.
setdefault	Reset to default settings.

Example

```
> csm appe prof –i 1 –n games
The name of APPE Profile 1 was setted.
```

Telnet Command: csm appe set

It is used to configure group settings for IM/ P2P/ Protocol and Others in APP Enforcement Profile.

csm appe set *-i INDEX [-v GROUP| -e AP_IDX | -d AP_IDX]*

Syntax Description

Parameter	Description
INDEX	Specify the index number of CSM profile, from 1 to 32.
- v	View the IM/ P2P/ Protocol and Others configuration of the CSM profile.
-e	Enable to block specific application.
-d	Disable to block specific application.
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

```
> Vigor> csm appe set –i 1 –e 1
Profile 1 – : AIM is enabled.
```

Telnet Command: csm appe show

It is used to display group (IM/ P2P/ Protocol and Others) information APP Enforcement Profile.

csm appe show *[-a| -i| -p| -t| -m]*

Syntax Description

Parameter	Description
-a	View the configuration status for All groups.
-i	View the configuration status of IM group.
-p	View the configuration status of P2P group.
-t	View the configuration status of protocol group.
-m	View the configuration status of Others group.

Example

```
>csm appe show -t

          Type    Index                 Name        Version   Advance
 Advanced Option: (M)essage, (F)ile Transfer, (G)ame, (C)onference, and (O)ther
Activities
-------------------------------------------------------------
      PROTOCOL       52                  DB2
      PROTOCOL       53                  DNS
      PROTOCOL       54                  FTP
      PROTOCOL       55                 HTTP            1.1
      PROTOCOL       56                 IMAP            4.1
      PROTOCOL       57          IMAP STARTTLS           4.1
      PROTOCOL       58                  IRC          2.4.0            ……
```

Telnet Command: csm appe config

It is used to display the configuration status (enabled or disabled) for IM/ P2P/ Protocol/ Other applications.

csm appe config -v *INDEX [-i| -p| -t| -m]*

Syntax Description

Parameter	Description
INDEX	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.

csm appe interface *[AUTO/ WAN#]*

Syntax Description

Parameter	Description
AUTO	Vigor router specifies WAN interface automatically.
WAN	Specify the WAN interface for signature downloading.

Example

```
> csm appe interface wan1
Download interface is set as "WAN1" now.
> csm appe interface auto
Download interface is set as "auto-selected" now.
```

Telnet Command: csm appe email

It is used to set notification e-mail for APPE signature based on the settings configured in **System Maintenance>>SysLog/Mail Alert Setup (**in which, the box of **APPE Signature** is checkd under **Enable E-Mail Alert**).

csm appe email <*-e*/ *-d*/ *-s*>

Syntax Description

Parameter	Description
-e	Enable notification e-mail mechanism.
-d	Disable notification e-mail mechanism.
-s	Send an example e-mail.

Example

```
> csm appe email -e
Enable APPE email.
```

Telnet Command: csm ucf

It is used to configure settings for URL control filter profile.

Syntax

csm ucf show

csm ucf setdefault

csm ucf msg *MSG*

csm ucf obj *INDEX <-n PROFILE_NAME | -l [P| B| A| N] | uac | wf >*

csm ucf obj *INDEX -n PROFILE_NAME*

csm ucf obj *INDEX -p VALUE*

csm ucf obj *INDEX -l P| B| A| N*

csm ucf obj *INDEX uac*

csm ucf obj *INDEX wf*

Syntax Description

Parameter	Description
show	It means to display all of the profiles.
setdefault	It means to return to default settings for all of the profile.
msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
obj	It means to specify the object for the profile.
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
-n	It means to set the profile name.
PROFILE_NAME	It means to 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	It means to specify the Administration Message, less then 255 characters
uac	It means to set URL Access Control part.
wf	It means to set Web Feature part.

Example

```
> csm ucf obj 1 -n game -l B
Profile Index: 1
```

```
Profile Name:[game]
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	It means to specify the index number of CSM profile, from 1 to 8.
- v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the function of URL Access Control.
-d	It means to disable the function of URL Access Control.
-a	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
```

```
Log:[block]
Priority Select : [Either : Url Access Control First]
------------------------------------------------
URL Access Control
[ ]Enable URL Access Control    Action:[pass]
[v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ----------------------------------

  No  Grp NO.    Group Name
 --- -------- ----------------------------------

> csm ucf obj 1 uac -a B
Log:[block]
Priority Select : [Either : Url Access Control First]
------------------------------------------------
URL Access Control
[ ]Enable URL Access Control    Action:[block]
[v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ----------------------------------

  No  Grp NO.    Group Name
 --- -------- ----------------------------------
```

Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

Syntax

csm ucf obj *INDEX wf -v*

csm ucf obj *INDEX wf -e*

csm ucf obj *INDEX wf -d*

csm ucf obj *INDEX wf -a P|B*

csm ucf obj *INDEX wf -s WEB_FEATURE*

csm ucf obj *INDEX wf -u WEB_FEATURE*

csm ucf obj *INDEX wf -f File_Extension_Object_index*

Syntax Description

Parameter	Description
INDEX	It means to specify the index number of CSM profile, from 1 to 8.
- v	It means to view the protocol configuration of the CSM profile.
-e	It means to enable the restriction of web feature.
-d	It means to disable the restriction of web feature.
-a	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	It means to enable the the Web Feature configuration. Features available for configuration are:

	c: Cookie p: Proxy u: Upload
-u	It means to cancel the web feature configuration.
-f	It means to set the file extension object index number.
File_Extension_Object_index	Enter the index number (1 to 8) for the file extension object.

Example

```
> csm ucf obj 1 wf -s c
-----------------------------------------------
Web Feature
[ ]Enable Restrict Web Feature   Action:[pass]

File Extension Object Index : [0] Profile Name : []

[V] Cookie [ ] Proxy [ ] Upload

>
```

Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

Syntax

csm wcf show

csm wcf look

csm wcf cache

csm wcf server WCF_SERVER

csm wcf msg MSG

csm wcf setdefault

csm wcf obj *INDEX -v*

csm wcf obj *INDEX -a P| B*

csm wcf obj *INDEX -n PROFILE_NAME*

csm wcf obj *INDEX -l N| P| B| A*

csm wcf obj *INDEX -o KEY_WORD Object Index*

csm wcf obj *INDEX -g KEY_WORD Group Index*

csm wcf obj *INDEX -w E| D| P| B*

csm wcf obj *INDEX -s CATEGORY| WEB_GROUP*

csm wcf obj *INDEX -u CATEGORY| WEB_GROUP*

Syntax Description

Parameter	Description
show	It means to display the web content filter profiles.
Look	It means to display the license information of WCF.
Cache	It means to set the cache level for the profile.
Server WCF_SERVER	It means to set web content filter server.

Msg MSG	It means de set the administration message. MSG means the content (less than 255 characters) of the message itself.
setdefault	It means to return to default settings for all of the profile.
obj	It means to specify the object profile.
INDEX	It means to specify the index number of web content filter profile, from 1 to 8.
- v	It means to 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	It means to set the profile name.
PROFILE_NAME	It means to 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	It means to 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: "Advertisement & Pop-Ups", "Alcohol & Tobacco", "Anonymizers", "Arts", "Business", "Transportation", "Chat", "Forums & Newsgroups", "Compromised", "Computers & Technology", "Criminal & Activity", "Dating & Personals", "Down sites", "Education", "Entertainment", "Finance", "Gambling", "Games", "Government", "Hate & Intolerance", "Health & Medicine", "Illegal Drug", "Job Search", "Streaming Media & Downloads", "News", "Non-profits & NGOs", "Nudity", "Persional Sites", "Phishing & Fraud", "Politics", "Pornography & Sexually explicit", "Real Estate", "Religion", "Restaurants & Dining", "Search engines & Portals", "Shopping", "Social Networking", "Spam sites", "Sports", "Malware", "Translators", "Travel", "Violence", "Weapons", "Web-Based Email", "General", "Leisure & Recreation", "Botnets", "Cults", "Fashion & Beauty", "Greeting Cards", "Hacking", "Illegal Softwares", "Image Sharing", "Information Security", "Instant Messaging", "Network Errors", "Parked Domains", "Peer-to-Peer", "Private IP Address", "School Cheating", "Sex Education", "Tasteless", "Child Abuse Images", "Uncategorised Sites"

Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.    Object Name
 --- -------- ---------------------------------
  No  Grp NO.    Group Name
 --- -------- ---------------------------------
Action:[block]
Log:[block]
-------------------------------------------------------------------------------
-----
child Protection Group:
  [v]Alcohol & Tobacco     [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug          [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence             [v]Weapons

  [v]School Cheating       [v]Sex Education         [v]Tasteless
  [v]Child Abuse Images
-------------------------------------------------------------------------------
-----
leisure Group:
  [ ]Entertainment         [ ]Games                 [ ]Sports
  [ ]Travel               [ ]Leisure & Recreation  [ ]Fashion & Beauty
.
.
>
```

Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

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 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. OFF is no cache ; AUTO is using TTL from pkt.
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: Enter 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: Enter the index number of the WCF profile.
-u UCF_PROFILE	UCF_PROFILE: Enter the index number of the UCF profile.
-c CACHE_TIME	-c means to set the cache time for DNS filter. CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter.
profile_setdefault	Reset to factory default setting.
local_bw e/d/p/b/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_edit 1
Profile Index: 1
Profile Name:[]

Log:[block]

WCF Profile Index: 0

UCF Profile Index: 0
> csm dnsf profile_setdefault
setdefault!!!
> 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]*

ddns set *-i <account index> -S <service provider> -T <service type> -D <hostname> -L <username> -P <password>*

Syntax Description

Parameter	Description
-i <value>	It means index number of Dynamic DNS Account. value: 1-6
-E <value>	It means to enable / disable Dynamic DNS Account. value: 0: Disable, 1:Enable
-W <value>	It means to specify WAN Interface. [value]: Must be between 1-8 1: WAN1 First 2: WAN1 Only 3: WAN2 First 4: WAN2 Only example: To set WAN Interface: WAN1 First
-L <value>	It means to type Login Name. [value]: limit up to 64 characters
-P <value>	It means to type Password. [value]: limit up to 24 characters
-C <value>	It means to enable / disable Wildcards. [value]: 0: Disable, 1:Enable
-B <value>	It means to enable / disable Backup MX. [value]: 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: WAN IP, 1: Internet IP
-S <value>	It means to specify Servive Provider. If user want to set User-Defined page, value must select 1. [value]: value must be between 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]: value must be between 1-3. 1: Dynamic 2: Custom 3: Static
-D <Host Name> <sub Domain Name>	It means to type Domain Name. i.e: Account index 1 setting Domain Name for Dynamic Service Type >> ddns set -i 1 -T 1 -D "host ddns.com.cn" i.e: Account index 2 setting Domain Name for Custom Service Type >> ddns set -i 2 -T 2 -D "domain name" i.e: Account index 3 setting Domain Name for Static Service Type >> ddns set -i 3 -T 3 -D "domain name"
-H <value>	It means to type User-Defined Provider Host. [value]: limit up to 64 characters
-A <value>	It means to type User-Defined Service API. [value]: limit up to 256 characters
-a <value>	It means to type User-Defined Auth Type. [value]: 0: basic 1: URL
-N <value>	It means to type User-Defined Connection Type. [value]: 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
> ddns log2017-09-04 04:43:46.5 >>>>>  DDNS is updating.  <<<<<2017-09-04
 04:43:05.6 >>>>>  DDNS is updating.  <<<<<
```

Telnet Command: ddns time

Sets and displays the DDNS time.

Syntax

ddns time *<update in minutes>*

Syntax Description

Parameter	Description
Update in minutes	Enter the value as DDNS time. The range is from 1 to 14400.

Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

Telnet Command: ddns forceupdate

This command will update DDNS automatically.

Example

```
> ddns forceupdate
 Now updating DDNS ...
 Please check result by using command "ddns log"
```

Telnet Command: ddns setdefault

This command will return DDS with factory default settings.

Example

```
>ddns setdefault
>Set to Factory Default.
```

Telnet Command: ddns show

This command allows users to check the content of selected DDNS account.

Syntax

ddns show -i *<value>*

Syntax Description

Parameter	Description
-I <value>	Display the content of selected DDNS account. [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

>
```

Telnet Command: dos

This command allows users to configure the settings for DoS defense system.

Syntax

dos *-V / D / A*

dos *-s ATTACK_F <THRESHOLD>< TIMEOUT>*

dos *-a / e <ATTACK_F><ATTACK_0> / d <ATTACK_F><ATTACK_0>*

dos *-o <LOG_TYPE>/ p <LOG_TYPE> / l <LOG_TYPE>*

dos *-P <add4/ remove4> <type> <value> / <add6/ remove6> <type> <value> / <show> / remove4 all / remove6 all>*

dos *-B <add4/ remove4> <type> <value> / <add6/ remove6> <type> <value> / <show> / remove4 all / remove6 all>*

Syntax Description

Parameter	Description
-V	It means to view the configuration of DoS defense system.
-D	It means to deactivate the DoS defense system.
-A	It means to activate the DoS defense system.
-s	It means to enable the defense function for a specific attack and set its parameter(s).
ATTACK_F	It means to 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	It means to enable the defense function for all attacks listed in ATTACK_0.
-e	It means to enable defense function for a specific attack(s).
ATTACK_0	It means to specify a name of the following attacks: ip_option, tcp_flag, land, teardrop, smurf, pingofdeath, traceroute, icmp_frag, syn_frag, unknow_proto, fraggle.
-d	It means to 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.
dos -o <LOG_TYPE>	Enable/Disable dos defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
dos -p <LOG_TYPE>	Enable/Disable spoofing defense log. <LOG_TYPE>: Enter 0 or 1. 0: Disable 1: Enable
dos -l <LOG_TYPE>	Enable/Disable dos defense black/white list log. <LOG_TYPE>: Enter 0 to 3. 0: None 1: White list 2: Black List 3: All
dos -f <0/1/show>	Set the priority of the whitelist/blacklist. 0: white list 1: black list
dos -i <1/2/3/4/show>	Set the sending time interval for whitelist/blacklist 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 select WAN interface. n: 1: WAN1 ,2: WAN2, ... x: WANx. Default is WAN1.
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 7, A, B) 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 n=A: 3G/4G USB Modem(PPP mode) n=B: 3G/4G USB Modem(DHCP mode)
<command><parameter>|..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-S <isp name>	It means to set ISP Name (max. 23 characters).
-P <on/off>	It means to enable PPPoE Service.
-u <username>	It means to set username (max. 49 characters) for Internet accessing.
-p <password>	It means to set password (max. 49 characters) for Internet accessing.
-a n	It means to set PPP Authentication Type and n means different types (represented by 0-1). n=0: PAP/CHAP (this is default setting) n=1: PAP Only
-t n	It means to set connection duration and n means different conditions. n=-1: Always-on n=1 ~ 999: Idle time for offline (default 180 seconds)
-i <ip address>	It means that *PPPoE server* will assign an IP address specified here for CPE (PPPoE client). If you type 0.0.0.0 as the <ip address>, ISP will assign suitable IP address for you. However, if you type an IP address here, the router will use that one as a fixed IP.

-w <ip address>	It means to assign WAN IP address for such connection. Please type an IP address here for WAN port.
-n <netmask>	It means to assign netmask for WAN connection. You have to type 255.255.255.xxx (x is changeable) as the netmask for WAN port.
-g <gateway>	It means to assign gateway IP for such WAN connection.
-s <server ip>	It means to set PPTP/L2TP Server IP. <server ip>= ppp.qqq.rrr.sss: PPTP/L2TP server IP
-A <idx>	Set to Always On mode, and <idx> as backup WAN#.
-B <mode>	Set to Backup mode. <mode> 0: When any WAN disconnect; 1: When all WAN disconnect.
-V	It means to view Internet Access profile.
-C <sim pin code>	Set (PPP mode) SIM PIN code (max. 15 characters) for 3G/4G USB Modem.
-O <init string>	Set (PPP mode) Modem Initial String (max. 47 characters) for 3G/4G USB Modem.
-T <init string2>	Set (PPP mode) Modem Initial String2 (max. 47 characters) for 3G/4G USB Modem.
-D <dial string>	Set (PPP mode) Modem Dial String (max. 31 characters) for 3G/4G USB Modem.
-v <service name>	Set (PPP mode) Service Name (max. 23 characters) for 3G/4G USB Modem.
-m <ppp username>	Set (PPP mode) PPP Username (max. 63 characters) for 3G/4G USB Modem.
-o <ppp password>	Set (PPP mode) PPP Password (max. 62 characters) for 3G/4G USB Modem.
-e n	Set (PPP mode) PPP Authentication Type for 3G/4G USB Modem. 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.
-R n	Set (PPP mode) WAN Connection Detection Echo Interval secondes. n= 3 to 60.
-E <sim pin code>	Set (DHCP mode) SIM PIN code (max. 19 characters).
-G <mode>	Set (DHCP mode) Network Mode. <mode> 0: 4G/3G/2G; 1: 4G Only; 2: 3G Only; 3: 2G Only

-N <apn name>	Set (DHCP mode) APN Name (max. 47 characters)
-U n	(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 -M 1 -u link1 -p link1 -a 0
 WAN1 Internet Mode set to PPPoE/PPPoA
 WAN1 Username set to link1
 WAN1 Password set successful
 WAN1 PPP Authentication Type set to PAP/CHAP
```

Telnet Command: ip pubsubnet

This command allows users to enable or disable the public subnet for your router.

Syntax

ip pubsubnet *<Enable/ Disable>*

Syntax Description

Parameter	Description
Enable	Enable the function.
Disable	Disable the function.

Example

```
> ip pubsubnet enable
public subnet enabled!
```

Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

Syntax

ip pubaddr *?*

ip pubaddr *<public subnet IP address>*

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet IP address.
public subnet IP address	Specify an IP address. The system will set the one that you specified as the public subnet IP address.

Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

Syntax

ip pubmask *?*

ip pubmask *<public subnet mask>*

Syntax Description

Parameter	Description
?	Display an IP address which allows users set as the public subnet mask.
public subnet IP address	Specify a subnet mask. The system will set the one that you specified as the public subnet mask.

Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

Telnet Command: ip addr

This command allows users to set/add a specified LAN IP your router.

Syntax

ip addr *<IP address>*

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.

Example

```
>ip addr 192.168.50.1
% Set IP address OK !!!
```

Info

When the LAN IP address is changed, the start IP address of DHCP server are still the same. To make the IP assignment of the DHCP server being consistent with this new IP address (they should be in the same network segment), the IP address of the PC must be fixed with the same LAN IP address (network segment) set by this command for accessing into the web user interface of the router. Later, modify the start addresses for the DHCP server.

Telnet Command: ip nmask

This command allows users to set/add a specified netmask for your router.

Syntax

ip nmask *<IP netmask>*

Syntax Description

Parameter	Description
IP netmask	It means the netmask of LAN IP.

Example

```
> ip nmask 255.255.0.0
% Set IP netmask OK !!!
```

Telnet Command: ip arp

ARP displays the matching condition for IP and MAC address.

Syntax

ip arp add *<IP address> <MAC address> <LAN or WAN>*

ip arp del *<IP address> <LAN or WAN>*

ip arp flush

ip arp status

ip arp accept *<0/1/2/3/4/5/status>*

ip arp setCacheLife *<time>*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source / destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

Syntax Description

Parameter	Description
IP address	It means the LAN IP address.
MAC address	It means the MAC address of your router.
LAN or WAN	It indicates the direction for the arp function.
0/1/2/3/4/5	0: disable to accept illegal source mac address 1: enable to accept illegal source mac address 2: disable to accept illegal dest mac address 3: enable to accept illegal dest mac address 4: Decline VRRP mac into arp table 5: Accept VRRP mac into arp table status: display the setting status.
Time	Available settings will be 10, 20, 30,....2550 seconds.

Example

```
> ip arp accept status
Accept illegal source mac arp: disable

Accept illegal dest mac arp: disable

Accept VRRP mac into arp table: disable
> ip arp status
[ARP Table]
 Index IP Address        MAC Address        Netbios Name
   1   192.168.1.113     00-05-5D-E4-D8-EE    A1000351
```

Telnet Command: ip dhcpc

This command is available for WAN DHCP.

Syntax

ip dhcpc *option*
ip dhcpc *option -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 -u <idx unmber>*
ip dhcpc *release <wan number>*
ip dhcpc *renew <wan number>*
ip dhcpc *status*

Syntax Description

Parameter	Description
option	It is an optional setting for DHCP server. -h: display usage -l: list all custom set DHCP options -d: delete custom dhcp client option by index number -e: enable/ disable option feature, 1:enable, 0:disable -w: set WAN number (e.g., 1=WAN1) -c: set option number: 0~255 -v: set option value by string -x: set option value by raw byte (hex) -u: update by index number
release	It means to release current WAN IP address.
renew	It means to renew the WAN IP address and obtain another new one.
status	It displays current status of DHCP client.

Example

```
> ip dhcpc option -e 1 -w1 -c 100 -v string
> ip dhcpc status
=====================================
WAN1:

DHCP Client Status: None active DHCP client!

=====================================
WAN2:

DHCP Client Status: None active DHCP client!

=====================================
...
```

Telnet Command: ip ping

This command allows users to ping IP address of WAN1/ WAN2/ PVC3/ PVC4/ PVC5 for verifying if the WAN connection is OK or not.

Syntax

ip ping *<IP address> <AUTO/ WAN1/ WAN2 > <Source IP address>*

Syntax Description

Parameter	Description
IP address	It means the WAN IP address.
AUTO/ WAN1/ WAN2	It means the WAN port / PVC that the above IP address passes through.
Source IP address	It means the source IP address.

Example

```
> ip ping 192.168.1.1 AUTO
Pinging 192.168.1.1 with 64 bytes of Data through LAN
Receive reply from 192.168.1.1, time=0.0ms
Receive reply from 192.168.1.1, time=0.0ms
Receive reply from 192.168.1.1, time=0.0ms
Receive reply from 192.168.1.1, time=0.0ms
```

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> <Udp/ Icmp>*

Syntax Description

Parameter	Description
IP address	It means the target IP address.
WAN1/ WAN2	It means the WAN port that the above IP address passes through.
Udp/ Icmp	It means the UDP or ICMP.

Example

```
>ip tracert 22.128.2.62 WAN1
Traceroute to 22.128.2.62, 30 hops max
1    172.16.3.7    10ms
2    172.16.1.2    10ms
3    Request Time out.
4    168.95.90.66  50ms
5    211.22.38.134 50ms
6    220.128.2.62  50ms
Trace complete
```

Telnet Command: ip telnet

This command allows users to access specified device by telnet.

Syntax

ip telnet <*IP address*><*Port*>

Syntax Description

Parameter	Description
IP address	Enter the WAN or LAN IP address of the remote device.
Port	Type a port number (e.g., 23). Available settings: 0 ~65535.

Example

```
> ip telnet 172.17.3.252 23
>
```

Telnet Command: ip rip

This command allows users to set the RIP (routing information protocol) of IP.

Syntax

ip rip <*0/1/2*>

Syntax Description

Parameter	Description
0/1/2	0 means disable; 1 means first subnet and 2 means second subnet.

Example

```
> ip rip 1
%% Set RIP 1st subnet.
```

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
 WAN[6] Rip Protocol enable
 WAN[7] Rip Protocol enable
 WAN[8] Rip Protocol enable
> 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
 WAN[6] Rip Protocol enable
 WAN[7] Rip Protocol enable
 WAN[8] Rip Protocol enable
```

Telnet Command: ip route

This command allows users to set static route.

Syntax

ip route *add <dst><netmask><gateway><ifno><rtype>*
ip route *del <dst><netmask><rtype>*
ip route *status*
ip route *cnc*
ip route *default <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 5=WAN3, 6=WAN4, 7=WAN5 However, WAN3, WAN4, WAN5 are router-borne WANs
rtype	It means the type of the route. default : default route; static: static route.
cnc	It means current IP range for CNC 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~       192.168.1.0/   255.255.255.0 is directly connected, LAN1
S         172.16.2.0/   255.255.255.0 via 172.16.2.4, WAN1
```

Telnet Command: ip igmp_proxy

This command allows users to enable/disable igmp proxy server.

Syntax

ip igmp_proxy *set*
ip igmp_proxy *reset*
ip igmp_proxy *wan*
ip igmp_proxy *t_home <on/off/show/help>*
ip igmp_proxy *query*
ip igmp_proxy *ppp <0/1>*
ip igmp_proxy *status*
ip igmp_proxy *version <v2/v3/auto/show>*
ip igmp_proxy *syslog <0/1>*

Syntax Description

Parameter	Description
set	It means to enable proxy server.
reset	It means to disable proxy server.
wan	It means to specify WAN interface for IGMP service.
t_home	It means to specify t_home proxy server for using.
On/off/show/help	It means to turn on/off/display or get more information of the T_home service.
query	It means to set IGMP general query interval. The default value is 125000 ms.
ppp	0 – No need to set IGMP with PPP header. 1 – Set IGMP with PPP header.
status	It means to display current status for proxy server.
version <v2/v3/auto/show>	It means to set IGMP version fixed on v2 or v3.
syslog <0/1>	It means to set IGMP syslog. 0: disable 1: enable

Example

```
> ip igmp_proxy query 130000
 This command is for setting IGMP General Query Interval
 The default value is 125000 ms
 Current Setting is:130000 ms
>
```

Telnet Command: ip igmp_snoop

This command allows users to enable or disable IGMP snoop function.

Syntax

ip igmp_snoop enable

ip igmp_snoop disable

ip igmp_snoop status

ip igmp_snoop 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>*

ip igmp_snoop acceptlist *<type><index>*

Syntax Description

Parameter	Description
enable	It means to enable igmp snoop function
disable	It means to disable igmp snoop function.
status	It means to display current igmp configuration.
table	It means to display current configuration of igmp.
txquery <on/off> <v2/v3>	It means to send out IGMP QUERY to LAN periodically. On: enable Off: disable v2: version v2 v3: version v3
mode <hw/sw>	It means to set software or hardware mode for snooping working on.
chkleave <on/off>	It means to check the leave status. On: enable the IGMP snoop leave checking function. Off: it will drop LEAVE if still clients on the same group.
separate <on/off>	It means to set IGMP packets being separated by NAT/Bridge. On: The packets will be separated. Off: The packets will not be separated by NAT/Bridge.
portchk <on/off>	It means to perform LAN port checking for IGMP packets. On: Perform the LAN port checking. Off: No perform the LAN port checking.
acceptlist <type><index>	Type: Enter 0 (disable), 1 (ip object) or 2 (ip group). Index: Enter 0 to 192 (for ip object); enter 0 to 32 (for ip group).

Example

```
> ip igmp_snoop enable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Enabled.
> ip igmp_snoop disable
%% ip igmp snooping [enable|disable|status], IGMP Snooping is Disabled.
```

```
> ip igmp_snoop mode hw
 igmp snooping works on SW mode now.
> ip igmp_snoop mode ?
% ip igmp mode [hw/sw]
 igmp snooping works on HW mode now.
> ip igmp_snoop separate ?
% ip igmp separate [on/off]
 igmp snoop seprate is ON now.
 igmp packets will be separated by  NAT/Bridge.
```

Telnet Command: ip dmz

Specify MAC address of certain device as the DMZ host.

Syntax

ip dmz *<mac>*

Syntax Description

Parameter	Description
mac	It means the MAC address of the device that you want to specify

Example

```
>ip dmz ?
% ip dmz <mac>,  now : 00-00-00-00-00-00
> ip dmz 11-22-33-44-55-66
> ip dmz ?
% ip dmz <mac>,  now : 11-22-33-44-55-66
>
```

Telnet Command: ip dmzswitch

This command allows users to set DMZ mode.

ip dmzswitch *off*

ip dmzswitch *private*

ip dmzswitch *active_trueip*

Syntax Description

Parameter	Description
off	It means to turn off DMZ function.
private	It means to set DMZ with private IP.
active_trueip	It means to set the DMZ with active true IP.

Example

```
> ip dmzswitch off
%% ip dmzswitch [off|private|trueip|active_trueip], DMZ is OFF
>
```

Telnet Command: ip session

This command allows users to set maximum session limit number for the specified IP; set message for exceeding session limit and set how many seconds the IP session block works.

Syntax

ip session *on*

ip session *off*

ip session *default <num>*

ip session *defaultp2p <num>*

ip session *status*

ip session *show*

ip session *timer <num>*

ip session *<block/unblock> <IP>*

ip session *<add/del> <IP1-IP2> <num> <p2pnum>*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default [num]	It means to set the default number of session num limit.
Defaultp2p [num]	It means to set the default number of session num limit for p2p.
status	It means to display the current settings.
show	It means to display all session limit settings in the IP range.
timer [num]	It means to set when the IP session block works. The unit is second.
[block/unblock][IP]	It means to block/unblock the specified IP address. Block: The IP cannot access Internet through the router. Unblock: The specified IP can access Internet through the router.
add	It means to add the session limits in an IP range.
del	It means to 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 *routing <on/off>*
ip bandwidth *schedule <s1> <s2> <s3> <s4>*
ip bandwidth *show*
ip bandwidth *<add/del><IP1-IP2><tx][rx><shared>*

Syntax Description

Parameter	Description
on	It means to turn on the IP bandwidth limit.
off	It means to turn off the IP bandwidth limit.
default <tx_rate><rx_rate>	It means to set default tx and rx rate of bandwidth limit. The range is from 0 – 65535 Kpbs.
status	It means to display the current settings.
routing <on/off>	It means to apply to IP Routed Subnet. On: apply to Off: not apply to
schedule <s1> <s2> <s3> <s4>	It means to set schedule profile (1 to 4). S1 ~ S4: Up to four profile can be set. Available schedule profiles from 0 to 16.
show	It means to display all the bandwidth limits settings within the IP range.
add	It means to add the bandwidth within the IP range.
del	It means to delete the bandwidth within the IP range.
IP1-IP2	It means the range of IP address specified for this command.
tx	It means to set transmission rate for bandwidth limit.
rx	It means to set receiving rate for bandwidth limit.
shared	It means that the bandwidth will be shared for the IP range.

Example

```
> ip bandwidth default 200 800
> ip bandwidth add 192.168.1.50-192.168.1.100 10 60
> ip bandwidth status

  IP range:
    192.168.1.50 - 192.168.1.100 : Tx:10K Rx:60K

  Current ip Bandwidth limit is turn off


  Auto adjustment is off
```

Telnet Command: ip dataflowmonitor.

This command allows users to set data flow monitor.

Syntax

ip dataflowmonitor *on*
ip dataflowmonitor *off*
ip dataflowmonitor *status*

Syntax Description

Parameter	Description
on	It means to enable the Data Flow Monitor function.
off	It means to disable the Data Flow Monitor function.
show	It means to display current status of Data Flow Monitor function.

Example

```
> ip dataflowmonitor status
Data Flow Monitor: 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 *subnet <all/set LAN_Index/unset LAN_Index/clear/show>*
ip bindmac *add <IP><MAC><comment>*
ip bindmac *del <IP/all>*
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 the IP bindmac policy.
subnet <all/set LAN_Index/unset LAN_Index/clear/show>	It means to set LAN subnet to bind strict mode.
show	It means to display the IP address and MAC address of the pair of binded one.
add	It means to add one ip bindmac.
del	It means to delete one ip bindmac.

IP	It means to Enter the IP address for binding with specified MAC address.
MAC	It means to Enter the MAC address for binding with the IP address specified.
Comment	It means to type words as a brief description.
All	It means to delete all the IP bindmac settings.

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 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 type in 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> | ...]*

Parameter	Description
-a <IP Address>	It is used to configure IP address mapping (IPv4/ IPv6 Address or multiple subnet addresses). *IP Address:* Enter the IP address (e.g., 192.168.1.56).
-d <address mapping index number>	It means to delete index number with address mapping configured. *address mapping index number :* Enter 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 :* Enter the index number which represents the profile with domain name configured.
-l	It means to list detailed information of profile configuration. > ip lanDNSRes -l % %Idx: 7 %State: Enable %Profile: DrayTekFTP %Domain Name: ftp.draytek.com %-------- Address Mapping Table -------- %Idx ReplyOnlySameSubnet IP Address %1 Yes 172.16.2.10 %2 Yes 172.16.3.10 %3 Yes 172.16.4.10
-n<domain name>	It means to specify a domain name to be accessed.
-p<profile name>	It means to set name of the LAN DNS profile.
-r	It means to clear specified domain name profile and the address mapping setting.
-R	It means to set to factory default setting.
-s<0/ 1>	It means to determine all subnet packets or only the packets with the same subnet will be replied for address mapping profile. *0:* reply all subnet packets. *1*: reply only same subnet packet.
-z	It means to update LAN DNS configuration to DNS cache.

Example

```
> ip lanDNSRes -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip lanDNSRes -i 1 -n ftp.drayTek.com
> ip lanDNSRes -i 1 -a 172.16.2.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.3.10 -s 1
> ip lanDNSRes -i 1 -a 172.16.4.10 -s 1
> ip lanDNSRes -l
%
```

```
% Idx: 7
% State: Enable
% Profile: DrayTekFTP
% Domain Name: ftp.draytek.com
% -------- Address Mapping Table --------
% Idx ReplyOnlySameSubnet IP Address
% 1   Yes                 172.16.2.10
% 2   Yes                 172.16.3.10
% 3   Yes                 172.16.4.10
```

Telnet Command: ip dnsforward

This command is used to set LAN DNS profile for conditional DNS forwarding.

ip dnsforward *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-a <IP Address/ Domain Name>	Set forwarded DNS server IP Address or domain name. <IP Address/ Domain Name>: Enter an IP address or the domain name.
-d <DNS server mapping index number>	Delete the selected LAN DNS profile. <DNS server mapping index number>: Enter the index number.
-e <0/ 1>	0: disable this function. 1: enable this function.
-i <profile setting index number>	Type the index number of the profile. <profile setting index number>: Enter the index number.
-l	List the content of LAN DNS profile (including domain name, IP address and message).
-n <domain name>	Set domain name.
-p <profile name>	Set profile name for LAN DNS.
-r	Reset the settings for selected profile.
-R	Set to factory default setting.

Example

```
> ip dnsforward -i 1 -n ftp.drayTek.com
% Configure Set1's DomainName:ftp.drayTek.com
> ip dnsforward -i 1 -a 172.16.1.1
% Configure Set1's IP:172.16.1.1
> ip dnsforward -i 1 -l
% Idx: 1
% State: Disable
% Profile: test
% Domain Name: ftp.drayTek.com
% DNS Server IP: 172.16.1.1
>
```

Telnet Command: ip spoofdef

This command is used to enable/disable the IP Spoofing Defense.

Syntax

ip spoofdef *<WAN/LAN><0/1>*

Syntax Description

Parameter	Description
<WAN/LAN>	It means to block IP packet from WAN/LAN with inconsistent source IP address.
<0/1>	0: Disable the function. 1: Enable the funciton.

Example

```
> ip spoofdef WAN 1
Setting saved:
>
```

Telnet Command: ip6 addr

This command allows users to set the IPv6 address for your router.

Syntax

ip6 addr -s *<prefix> <prefix-length> <LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>*

ip6 addr -d *<prefix> <prefix-length> <LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>*

ip6 addr -a*<LAN1/..LAN4 / WAN1/WAN2/ VPN1/..VPN32> -u*

ip6 addr -v*<LAN1/..LAN4 / WAN1/WAN2 >*

ip6 addr -t *<old-prefix><old-prefix-length><new-prefix> <new-prefix-length> < LAN1/..LAN4/WAN1/WAN2>*

ip6 addr -o *<1/2/3>*

ip6 addr -o 3 *<prefix> <prefix-length> <WAN1/WAN2/USB1/USB2>*

ip6 addr -l *<prefix> <prefix-length> <LAN1/..LAN4>*

ip6 addr <-*p/-b> <prefix> <prefix-length> <WAN1/WAN2 >*

ip6 addr -x *<LAN1/..LAN4>*

ip6 addr -c *<LAN1/..LAN4>*

ip6 addr -e *<type> < LAN1/..LAN4>*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> < LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>	It means to add a static ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. < LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>: It means to specify LAN/WAN/ VPN interface for such address.
-d <prefix> <prefix-length> < LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32>	It means to delete an ipv6 address. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the

	prefix. < LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>: It means to specify LAN/WAN/ VPN interface for such address.
-a < LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32> -u	It means to show current address(es) status. < LAN1/..LAN4/ WAN1/WAN2/ VPN1/..VPN32>: It means to specify LAN/WAN/ VPN interface. <-u>: It means to show unicast address only.
-v <LAN1/..LAN4/ WAN1/WAN2 >	It means to show prefix list status.
-t <old-prefix><old-prefix-length><new-prefix> <new-prefix-length> <LAN1/..LAN4 / WAN1/WAN2 >	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/..LAN4/WAN1/WAN2 >: 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/WAN2>	<3>: It means to set old prefix. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <WAN1/WAN2 >: It means to specify a WAN interface for such address.
-l <prefix> <prefix-length> < LAN1/..LAN4>	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/..LAN4>: It means to specify a LAN interface for such address.
-p/-b <prefix> <prefix-length> <WAN1/WAN2>	It means to add/delete an prefix to/from prefix list. p: Add a prefix to a prefix list. b: Delete a prefix from a prefix list. <prefix>: It means to enter the prefix number of IPv6 address. <prefix-length>: It means to enter a fixed value as the length of the prefix. <WAN1/WAN2 >: It means to specify a WAN interface for such address.
-x <LAN1/..LAN4>	It means to generate a ULA automatically. <LAN1/..LAN4>: It means to specify a LAN interface.
-c <LAN1/..LAN4>	It means to delete a ULA . <LAN1/..LAN4>: It means to specify a LAN interface.
-e <type> <LAN1/..LAN4>	It means to set ULA type. <type>: 0, disable; 1, static; 2, auto <LAN1/..LAN4>: It means to specify a LAN interface.

Example

```
> ip6 addr -a
LAN
Unicast Address:
```

```
 FE80::250:7FFF:FE00:0/64 (Link)
Multicast Address:
 FF02::2
 FF02::1:FF00:0
 FF02::1
...
...
```

Telnet Command: ip6 dhcp req_opt

This command is used to configure option-request settings for DHCPv6 client.

Syntax

ip6 dhcp *req_opt <LAN1| LAN2| ...| LAN4| WAN1| WAN2>-<command> <parameter>| ...*]

Syntax Description

Parameter	Description
req_opt	It means option-request.
*LAN1| LAN2| ...| LAN4| WAN1	WAN2*	It means to specify LAN or WAN interface for such address.
[<command> <parameter>| ..]	The available commands with parameters are listed below. *[..]* means that you can 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| WAN2> [-<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.
-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.
-i <parameter>	It means to send information request to server.
-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 -d
 Client DUID = 000300011449bc0a6241
```

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 type in 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 LAN1 pdadd 11:22:33 64 fe80::e202:1bff:fe65:4084
000100011d2ce39a00e06f25c839
%      Add to PD list success!
%% PD status : invalid, no prefix available.
>
```

Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

Syntax

ip6 internet *-W n -M n [-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>| ..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-W n	**W** means to set WAN interface and **n** means different selections. Default is WAN1. n=1: WAN1 n=2: WAN2 n=3: WAN3 . . n=X: WANx
-M n	M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5) n= 0: Offline, n=1: PPP, n=2: TSPC, n=3: AICCU, n=4: DHCPv6, n=5: Static n=6:6in4-Static n=7:6rd
6rd	

-C <n>	It means to set 6rd connection mode. n=0: Auto n=1: Static
-s <server>	It means to set 6rd IPv4 Border Relay. <server>: Enter a string.
-m <n>	It means to set 6rd IPv4 address mask length. <n>: Enter a number.
-p <prefix>	It means to set IPv6 prefix for 6rd connection. <prefix>: Enter a prefix number of IPv6 address.
-l <n>	It means to set the prefix length for 6rd connection. <n>: It means to enter a fixed value as the length of the prefix.
6in4	
-s <server>	It means to set 6in4 remote endpoint IPv4 address.
-l <IPv6 Addr>	It means to set the IPv6 address for 6in4 connection.
-P <n>	It means to set IPv6 WAN prefix length for 6in4 connection.
-p <prefix>	It means to set 6in4 LAN Routed Prefix.
-l <n>	It means to set 6in4 LAN Routed Prefix length.
-T <n>	It means to set 6in4 Tunnel TTL.
TSPC/AICCU	
-u <username>	It means to set username (max. 63 characters). <username>: Enter a string.
-P <password>	It means to set Password (max. 63 characters). <password>: Enter a password.
-s <server>	It means to set Tunnel Server IP. <server>: Enter an IPv4 Address or URL (max. 63 characters)
AICCU	
-p <prefix>	It means to set Subnet Prefix (AICCU). <prefix>: Enter a prefix number of IPv6 address.
-l <n>	It means to set Subnet Prefix length (AICCU). <n>: Enter a number.
-o <1/0>	It means to set AICCU always on. 1: on 0: off
-f	It means to set AICCU tunnel ID.
Static	
-w <addr>	It means to set Default Gateway. <addr>: Enter an IPv6 address.
Others	
-d <server>	It means to set 1st DNS Server IP. <server>: Enter an IPv6 address.
-D <server>	It means to set 2nd DNS Server IP. <server>: Enter an IPv6 address.
-t <dhcp/ra/none>	It means to set ipv6 PPP WAN test mode for DHCP or RA. <dhcp/ra/none> : Enter dhcp, ra or none.
-V	It means to view IPv6 Internet Access Profile.
-k	It means to dial the Tunnel on the WAN.
-j	It means to drop the Tunnel on the WAN.
-r n	It means to set Prefix State Machine RA timeout.
-c n	It means to set Prefix State Machine DHCPv6 Client timeout.
-q <0/1/2>	It means to set WAN detection mode. 0:NS Detect 1:Ping Detect 2:Always On
-z <value>	It means to set Ping Detect TTL (0-255). <value>: Enter 0~255.
-x <hostname/ IPv6 addr>	It means to set Ping Detect Host (hostname or IPv6 address). <hostname/ipv6 addr> : Enter a hostname or an IPv6 address.
-i <value>	It means to set ipv6 connection interval. <value>: Enter a number (1500-60000 (unit:10ms)).
-b <0/1>	It means to enable DNSv6 based on DHCPv6. 1 = on 0 = off
-R <0/1>	It means to Enable RIPng. 1 = on 0 = off

Example

```
> ip6 internet -W 2 -M 2 -u 88886666 -p draytek123456 -s amsterdam.freenet6.net
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
> system reboot
```

Telnet Command: ip6 neigh

This command allows you to display IPv6 neighbour table.

Syntax

ip6 neigh *-s <inet6_addr> <eth_addr> <LAN1/..LAN4/ WAN1/ WAN2>*

ip6 neigh *-d <inet6_addr> <LAN1/..LAN4/ WAN1/ WAN2>*

ip6 neigh *-a <inet6_addr> <-N LAN1/..LAN4/ WAN1/ WAN2>*

Syntax Description

Parameter	Description
-s <inet6_addr> <eth_addr> < LAN1/..LAN4/ WAN1 / WAN2>	It means to add a neighbour. <inet6_addr>: Enter an IPv6 address. <eth_addr>: Enter a submask address. <LAN1/..LAN4/ WAN1/ WAN2>: Specify an interface for the neighbor.
-d <inet6_addr> < LAN1/..LAN4 / WAN1 / WAN2>	It means to delete a neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ WAN2>: Specify an interface for the neighbor.
-a <inet6_addr> <-N LAN1/..LAN4 / WAN1 / WAN2>	It means to show neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ WAN2>: 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
-------------------------------------------------------------------------
LAN FF02::1                                33-33-00-00-00-01    CONNECTED
WAN2 2001:5C0:1400:B::10B8                 00-00-00-00-00-00    CONNECTED
WAN2 2001:2222:3333::1111                  00-00-00-00-00-00    CONNECTED
WAN2 2001:2222:6666::1111                  00-00-00-00-00-00    CONNECTED
WAN2 ::                                    00-00-00-00-00-00    CONNECTED
LAN  ::                                                         NONE
>
```

Telnet Command: ip6 pneigh

This command allows you to add a proxy neighbour.

Syntax

ip6 pneigh *-s <inet6_addr> <LAN1/..LAN4/ WAN1/ WAN2>*

ip6 pneigh *-d <inet6_addr> <LAN1/..LAN4/ WAN1/ WAN2>*

ip6 pneigh *-a <inet6_addr> <LAN1/..LAN4/ WAN1/ WAN2>*

Syntax Description

Parameter	Description
-s <inet6_addr> < LAN1/..LAN4/ WAN1/ WAN2>	It means to add a proxy neighbour. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ WAN2>: Specify an interface for the proxy neighbor.
-d <inet6_addr> < LAN1/..LAN4/ WAN1/ WAN2>	It means to delete a proxy neighbour. <inet6_addr>: Enter an IPv6 address. < LAN1/..LAN4/ WAN1/ WAN2>: Specify an interface for the proxy neighbor.
-a <inet6_addr> < LAN1/..LAN4/ WAN1/ WAN2>	It means to show proxy neighbour status. <inet6_addr>: Enter an IPv6 address. <LAN1/..LAN4/ WAN1/ WAN2>: Specify an interface for the proxy neighbor.

Example

```
> ip6 neigh –s FE80::250:7FFF:FE12:300 LAN1
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

Telnet Command: ip6 route

This command allows you to

Syntax

ip6 route *-s <prefix> <prefix-length> <gateway> <LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32> <-D>*

ip6 route -*d <prefix> <prefix-length>*

ip6 route -*a <LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32>*

ip6 route -*l*

Syntax Description

Parameter	Description
-s <prefix> <prefix-length> <gateway> < LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32> <-D>	It means to add a route. <prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix. <gateway>: It means to enter the gateway of the router. < LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32>**:** It means to specify LAN or WAN or VPN interface for such address. <-D>: It means that such route will be treated as the default route.
-d <prefix> <prefix-length>	It means to delete a route. <prefix>: It means to enter the prefix number of IPv6 address. <prefix length>: It means to enter a fixed value as the length of the prefix.

-a < LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32>	It means to show the route status. <LAN1/..LAN4/ WAN1/ WAN2/ VPN1/..VPN32>**:** It means to specify LAN or WAN or VPN interface for such address.
-l	It means to clear the routing table.

Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN1
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN1

 PREFIX/PREFIX-LEN                  I/F METRIC FLAG NEXT-HOP
-------------------------------------------------------------------------
 ::0.0.0.1/128                      LAN1    0 U ::
 FE80::/128                         LAN1    0 U ::
 FE80::21D:AAFF:FE9A:5324/128       LAN1    0 U ::
 FE80::/64                          LAN1  256 U ::
 FE80::/16                          LAN1 1024 UGS FE80::250:7FFF:FE12:100
 FF02::1/128                        LAN1    0 U FF02::1
 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/..LAN4/ WAN1/ WAN2> <send count> <data_size>*

Syntax Description

Parameter	Description
IPV6 address/ Host	It means to specify the IPv6 address or host for ping.
LAN1/..LAN4/ WAN1/ WAN2	It means to specify an interface for such address.
data_size	Ranges from 1 to 1452.

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*><*LAN1/ ..LAN4/ WAN1/ WAN2*>

Syntax Description

Parameter	Description
IPV6 address/ Host	It means to specify the IPv6 address or host for ping.
< *LAN1/ ..LAN4 / WAN1 / WAN2*>	It means to specify an interface for such address.

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/..LAN4> <-<command> <parameter>/ ... >*

Syntax Description

Parameter	Description
<<command> <parameter>/..>	The available commands with parameters are listed below. <..> means that you can Enter several commands in one line.
-s <0/1>	It means to enable or disable the default lifetime of the RADVD server. 1: Enable the RADVD server. 0: Disable the RADVD server.
-D <0/1/2>	It means to set RDNSS Disable/Enable/Deploy (0/1/2) when WAN is up.
-d <lifetme>	It means to set RA default lifetime.
-i <lifetme>	It means to set RA min interval time(sec).
-I <lifetme>	It means to set RA MAX interval time(sec).
-h <hoplimit>	It means to set RA hop limit.
-m <mtu/auto>	It means to set RA MTU, 1280-1500. mtu: auto - auto select MTU from WAN,
-e <time>	It means to set reachable time.
-a <time/infinity>	It means to set retransmit timer / infinity.
-p <0/1/2>	It means to set radvd default preference Low/Medium/High. 0-low 1-medium 2-high
-v	It means to view radvd configuration.
-V	It means to view setting in RA.
-L <time/infinity>	It means to set prefix valid lifetime.
-P <time/infinity>	It means to set prefix preferred lifetime.
-r <num>	It means to to set RA test for item. <num>: 0, 121, 124 0: default, 121: logo 121, 124: logo 124..
-R	It means to reload Config and send RA for subnets.
-u	It means to view MTU on all interfaces.

Example

```
> ip6 radvd LAN1 -s 1
% [LAN1] setting !
%   Enable LAN1 radvd OK!
```

```
> ip6 radvd LAN1 -d 1800
% [LAN1] setting !
%   Set default lifetime ok: 1800 !
> ip6 radvd LAN1 -V
% [LAN1] setting !
%  Default Lifetime   : 0 seconds
%  min interval time  : 200 seconds
%  MAX interval time  : 600 seconds
%  Hop limit          : 64
%  MTU                : 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 <NO.>| flush>	It means to add an IPv6 address which can be used to execute management through Internet. <Index>: 1 to 10. Ten profiles can be set for IPv6 access list. <IPv6 Object Index>: It means the index number of IP object (1 to 64) or keyword object (1 to 64) . remove <Index>: It means to remove (delete) the specified IP/Keyword object.
flush	It means to clear the IPv6 access table.
status	It means to show the status of IPv6 remote management.
internet/ http/telnet/ping/https/ssh /enforce_https	These protocols are used for accessing Internet.
on/off	It means to enable (on) or disable (off) the Internet accessing through http/telnet/ping.

Example

```
> ip6 mngt list add 1 62
%% Set OK.
```

Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN / WAN.

Syntax

ip6 *online <WAN1| WAN2>*

Syntax Description

Parameter	Description
WAN1| WAN2	It means the connection interface. 1=WAN1 2=WAN2

Example

```
> ip6 online WAN1
 % WAN1 online status :
 % IPv6 WAN1 Disabled
 % Default Gateway : ::
 % Interface : DOWN
 % UpTime : 00:00:00
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
  % MTU Onlink: 1280 , Config MTU : 0
```

Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

Syntax

ip6 aiccu -i *<ifno>* **-r**

ip6 aiccu -i *<ifno>* **-s**

Syntax Description

Parameter	Description
<Ifno>	It means the connection interface. 1=WAN1 2=WAN2
-r	It means to remove (delete) the specified index number with IPv6 settings.
-s	It means to display the AICCU status.

Example

```
> ip6 aiccu -i 1 -s
Status: Idle
>
```

Telnet Command: ip6 ntp

This command allows you to set IPv6 settings for NTP (Network Time Protocols) server.

Syntax

ip6 ntp –h

ip6 ntp –v

ip6 ntp –p <0/1>

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-v	It is used to show the NTP state.
-p <0/1>	It is used to specify NTP server for IPv6. 0 – Auto 1 – First Query IPv6 NTP Server.

Example

```
> ip6 ntp –p 1
% Set NTP Priority: IPv6 First
```

Telnet Command: ip6 lan

This command allows you to set IPv6 settings for LAN interface.

Syntax

ip6 lan -l n *[-<l:w:d:D:m:o:s> <parameter> | ...]*

Syntax Description

Parameter	Description
–h	It is used to display the usage of such command.
-l n	It means to selete LAN interface to be set. n= 1: LAN1 n= 2: LAN2, ... x: LANx. Default is LAN1
-w n	It means to selete WAN interface to be primary interface. n= 0: None, n=1: WAN1 , n=2: WAN2, ... x: WANx.
-d <server>	It means to set 1st DNS Server IP. <server>= IPv6 Address
-D <server>	It means to set 2nd DNS Server IP. <server>= 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:

	bit 0: WAN1 bit 1: WAN2, ... bit n: WAN(n+1).
-f n	It means to disable IPv6. n= 1: Disable IPv6, n=0: Enable IPv6.
-R n	It means to enable / disable RIPng. n=1: Enable RIPng, n=0: Disable RIPng.
-s n	It means to show IPv6 LAN setting. n=0:show all. Default is show all. n=1: LAN1 n=2: LAN2, ... 4: LAN4, n=9: DMZ.

Example

```
> ip6 lan -l 1 -w 1 -d 2001:4860:4860::8888 -o 1 -f 0 -s 2
%   Set LAN1!

%   Set primary WAN1!

%  Set 1st DNS server 2001:4860:4860::8888

%   Set Other Option Enable!

%   [LAN1] support ipv6!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

% [LAN2] setting:
%  Primary WAN    : WAN1
%  Management     : SLAAC
%  Other Option   : Disable
%  WAN Exten      : None
%  Subnet ID      : 2
%  Static IP(0)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(1)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(2)   : ::/0
%                 [ifno: 0, enable: 0]
%  Static IP(3)   : ::/0
%                 [ifno: 0, enable: 0]
%  DNS1           : 2001:4860:4860::8888
%  DNS2           : 2001:4860:4860::8844
%  ULA Type       : OFF
%  RIPng          : Enable
```

Telnet Command: ip6 session

This command allows you to set sessions limit for IPv6 address.

Syntax

ip6 session *on*
ip6 session *off*
ip6 session *default <num>*
ip6 session *status*
ip6 session *show*
ip6 session *add <P1-IP2> <num> <p2pnum>*
ip6 session *del <P1-IP2> <num><p2pnum>*

Syntax Description

Parameter	Description
on	It means to turn on session limit for each IP.
off	It means to turn off session limit for each IP.
default <num>	It means to set the default number of session num limit.
status	It means to display the current settings.
show	It means to display all IP range session limit settings.
add <IP1-IP2><num> <p2pnum>	<add>*:* It means to add the session limit for an IPv6 range. <IP1-IP2> : Specify a range for IPv6 addresses. <num>: Enter a number.
del<IP1-IP2><num> <p2pnum>	<del>*:* It means to delete the session limit for an IPv6 range. <IP1-IP2> : Specify a range for IPv6 addresses. <num>: Enter a number.

Example

```
> ip6 session on
> ip6 session add 2100:ABCD::2-2100:ABCD::10 100
> ip6 session status

  IPv6 range:
    2100:ABCD::2 - 2100:ABCD::10 : 100

  Current ip6 session limit is turn on

  Current default session number is 100
```

Telnet Command: ip6 bandwidth

This command allows you to set IPv6 settings

Syntax

ip6 bandwidth *on*

ip6 bandwidth *off*

ip6 bandwidth *default <tx_rate> <rx_rate>*

ip6 bandwidth *status*

ip6 bandwidth *show*

ip6 bandwidth *add <IP1-IP2> <tx><rx><shared>*

ip6 bandwidth *del <IP1-IP2> <tx><rx><shared>*

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. <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> <tx><rx><shared>	<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.

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
ipf: IP Filter: v3.3.1 (1848)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x0 = none set
Default: pass all, Logging: available
```

Telnet Command: ipf set

This command is used to set general rule, filter set and filter rule for firewall.

Syntax

ipf set <*Options*>

ipf set <*SET_NO*><*Options*>

ipf set <*SET_NO*> ***rule*** <*RULE_NO*><*Options*>

Syntax Description

Parameter	Description
ipf set <*Options*>	It means to set the firewall general setup and default rule.
ipf set <SET_NO><Options>	It means to set the firewall fiter set including comments and next fiter set.
ipf set <SET_NO> rule <RULE_NO> <Options>	It means to set the firewall rule in 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.
-c <p1>	It means to setup Call Filter. <p1>: Specify the index number (1 to 12) of the set profile. To disable the setting, enter "0".

-d <p1>	It means to setup Data Filter. <p1>: Specify the index number (1 to 12) of the set profile. To disable the setting, enter "0".
- p <p1><p2>	It means to setup actions for packet not matching any rule and whether record syslog. <p1>: Type " 0" to let packets not matching any rule pass; Type " 1" to block the packets not matching any rule. <p2>: "0" means the log related to rule matching will not be recorded on Syslog; "1" means the log related to rule matching will be recorded on Syslog. For example, to set pass for packet not matching any rule and enable syslog, ***-p 0 1***.
-R <v4/ v6> <Enable/ Disable>	It means to accept routing packet from WAN. <v4/ v6>: IPv4 or IPv6. <Enable/ Disable>: Enter 0 (enable) or 1 (disable). Set Accept routing packet from WAN by IPv4, please enter ***-R v4 0***.
-L <p1>	It means to enable or disable the Strict Security Firewall function. <p1>: Enter 1(enable) or 0 (disable).
-C <p1>	It means to setup Code Page. <p1>: Enter a code page number (0 to 20). For example, ipf set -C 20. 0. None 1. ANSI(1250)-Central Europe 2. ANSI(1251)-Cyrillic 3. ANSI(1252)-Latin I 4. ANSI(1253)-Greek 5. ANSI(1254)-Turkish 6. ANSI(1255)-Hebrew 7. ANSI(1256)-Arabic 8. ANSI(1257)-Baltic 9. ANSI(1258)-Viet Nam 10. OEM(437)-United States 11. OEM(850)-Multilingual Latin I 12. OEM(860)-Portuguese 13. OEM(861)-Icelandic 14. OEM(863)-Canadian French 15. OEM(865)-Nordic 16. ANSI/ OEM(874)-Thai 17. ANSI/ OEM(932)-Japanese Shift-JIS 18. ANSI/ OEM(936)-Simplified Chinese GBK 19. ANSI/ OEM(949)-Korean 20. ANSI/ OEM(950)-Traditional Chinese Big5
-M <p1><p2>	It means to setup APP Enforcement and Syslog. <p1>: Enter a number (0 to 32). In which, 0 means none; 1 to 32 mens the index number of the profile. <p2>: "0" means the log related to APP Enforcement will not be recorded on Syslog; "1" means the log related to APP Enforcement will be recorded on Syslog.
-U <p1><p2>	It means to setup URL Content Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to URL Content Filter will not be

	recorded on Syslog; "1" means the log related to URL Content Filter will be recorded on Syslog.
-W <p1><p2>	It means to setup Web Content Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to Web Content Filter will not be recorded on Syslog; "1" means the log related to Web Content Filter will be recorded on Syslog.
-D <p1><p2>	It means to setup DNS Filter for packets not matching any rule. <p1>: Enter a number (0 to 8). In which, 0 means none; 1 to 8 mens the index number of the profile. <p2>: "0" means the log related to DNS Filter will not be recorded on Syslog; "1" means the log related to DNS Filter will be recorded on Syslog.
-a <p1>	It means to configure the advanced settings.
-f <p1>	It means to accept large incoming fragmented UDP or ICMP packets. <p1>: Enter 1(enable) or 0 (disable).
-t <p1>	It means to enable or disable the Transparent Mode. <p1>: Enter 1(enable) or 0 (disable).
-E <p1><p2>	It means to set the maximum count for session limitation. <p1>: Enter a number (0 to 50000) <p2>: "0" means the log related to session control will not be recorded on Syslog; "1" means the log related to session control will be recorded on Syslog.
-Q <p1><p2>	It means to set the QoS Class. <p1>: Enter a number (0 to 4). 0: None 1: Class 1 2: Class 2 3: Class 3 4: Default Class <p2>: "0" means the log related to QoS Class will not be recorded on Syslog; "1" means the log related to QoS Class will be recorded on Syslog.
-Y <p1><p2>	It means to set the User Management. <p1>: Enter a number (-1 to 2). -1: None 0: All 1: user object 2: user group <p2>: 1 to 200 (if p1 is set with 1, user object) or 1 to 32 (if p1 is set with 2, user group)
-y <p1>	It means the log related to User Management will be or be not recorded on Syslog. <p1>: Enter 1(enable) or 0 (disable).
-w <p1>	It means to set the window size of TCP protocol. <p1>: Enter a value (0 to 65535).
-A <p1>	It means to enable or disable the function of packet capture. <p1>: Enter 1(enable) or 0 (disable).
About ipf set [SET_NO] [Options]	
-m [Comments]	It means to set comment for a filter set.

	[Comments]: Enter a description for the filter set.
-v	It means to view the comment and the next filter set.
-n [NEXT_SET_NO]	It means to specify the next filter set of current filter set. [NEXT_SET_NO]: Enter a number (1 to 12). For example, ipf set 1 -n 2.

Example

```
> ipf set -R "v4 1"
Setting saved.
DrayTek> ipf set -R "v6 1"
Setting saved.
> ipf set -v

Call Filter: Enable (Start Filter Set = 1)
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   : 30000
  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
  ------------------------------------------------------------------------
  CodePage             : ANSI(1252)-Latin I
  Window size          : 65535
  Session timeout      : 60
  DrayTek Banner       : Enable
  ------------------------------------------------------------------------
  Accept large incoming fragmented UDP or ICMP packets: Enable
  Transparent Mode     : Disable
  ------------------------------------------------------------------------
  Block routing packet from WAN:
    [v] IPv4
    [v] IPv6
  ------------------------------------------------------------------------
  [v] Enable Strict Security Firewall

>
```

Telnet Command: ipf rule

This command is used to set filter rule for firewall.

Syntax

ipf rule *s r* *[-<command> <parameter> | ...*

ipf rule s r -v

Syntax Description

Parameter	Description
s	It means the Filter Set. s: Enter a value (1 to 12).
r	It means Filter Rule r: Enter a value (1~7).
[<command> <parameter>|...]	The available commands with parameters are listed below. *[...]* means that you can type in several commands in one line.
-e <0/1>	It means to enable or disable the rule setting. 0- disable 1- enable
-v	It is used to show current filter rule settings.
-D <value>	It means to set the direction of packet flow. It is for **Data Filter** only. 0: LAN/RT/VPN -> WAN 1: WAN -> LAN/ RT/VPN 2: LAN/ RT/VPN -> LAN/ RT/VPN
-I "<e/d><para1, para2,...>"	It means to set incoming interface. e: Enable the function. d: Disable the function. Para1, para2,...: Available values include all, LAN1, LAN2,...LAN4, RT, VPN, WAN1, WAN2,...WAN5 (RT means IP Routed Subnet) 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,...LAN4, RT, VPN, WAN1, WAN2,...WAN5 (RT means IP Routed Subnet) 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"
-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 30000) 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 2 1 -v

Filter Set 2 Rule 1:

Status  : Enable
```

```
Comments: xNetBios -> DNS
Index(1-15) in Schedule Setup: <null>, <null>, <null>, <null>

Direction         : LAN -> WAN
Source IP         : Group1,
Destination IP    : Group2,
Service Type      : TCP/UDPGroup1,
Fragments         : Don't Care

Pass or Block              : Block Immediately
Branch to Other Filter Set : None
Max Sessions Limit         : 32000
Current Sessions           : 0
Mac Bind IP                : Non-Strict
Qos Class                  : None
APP Enforcement            : None
URL Content Filter         : None
Load-Balance policy        : Auto-select
Log                        : Disable
-----------------------------------------------------------------
CodePage                   : ANSI(1252)-Latin I
Window size                : 65535
Session timeout            : 1440
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 *[-re]*

ipf flowtrack view *[-f]*

ipf flowtrack *[-i][-p][-t]*

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 -r
Refresh the flowstate ok
> ipf flowtrack view -f
Start to show the flowtrack sessions state:

ORIGIN>>  192.168.1.11:59939 ->       8.8.8.8:  53 ,ifno=0
REPLY >>      8.8.8.8:  53 ->   192.168.1.11:59939 ,ifno=3
      proto=17, age=93023180(3920), flag=203
ORIGIN>>  192.168.1.11:15073 ->       8.8.8.8:  53 ,ifno=0
REPLY >>      8.8.8.8:  53 ->   192.168.1.11:15073 ,ifno=3
      proto=17, age=93025100(2000), flag=203
ORIGIN>>  192.168.1.11: 7247 ->       8.8.8.8:  53 ,ifno=0
REPLY >>      8.8.8.8:  53 ->   192.168.1.11: 7247 ,ifno=3
      proto=17, age=93020100(7000), flag=203
End to show the flowtrack sessions state
> ipf flowtrack set -e
Current flow_enable=0
> ipf flowtrack set -e
Curretn flow_enable=1
```

Telnet Command: Log

This command allows users to view log for WAN interface such as call log, IP filter log, flush log buffer, etc.

Syntax

log *[-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 <0-2>	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: mngt ftpport

This command allows users to set FTP port for management.

Syntax

mngt ftpport *<FTP port>*

Syntax Description

Parameter	Description
FTP port	It means to Enter the number for FTP port. The default setting is 21.

Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

Syntax

mngt httpport *<Http port>*

Syntax Description

Parameter	Description
Http port	It means to enter the number for HTTP port. The default setting is 80.

Example

```
> mngt httpport 80
% Set web server port to 80 done.
```

Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

Syntax

mngt httpsport *<Https port>*

Syntax Description

Parameter	Description
Https port	It means to Enter the number for HTTPS port. The default setting is 443.

Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

Telnet Command: mngt sslvpnport

This command allows users to set SSL VPN port for management.

Syntax

mngt sslvpnport *<SSL VPN port>*

Syntax Description

Parameter	Description
SSL VPN port	It means to type the number for SSL VPN port. The default setting is 443.

Example

```
> mngt sslvpnport 1010
% Set SSL VPN port to 1010 done.
```

Telnet Command: mngt telnetport

This command allows users to set telnet port for management.

Syntax

mngt telnetport *<Telnet port>*

Syntax Description

Parameter	Description
Telnet port	It means to Enter the number for telnet port. The default setting is 23.

Example

```
> mngt telnetport 23
% Set Telnet server port to 23 done.
```

Telnet Command: mngt sshport

This command allows users to set SSH port for management.

Syntax

mngt sshport *<ssh port>*

Syntax Description

Parameter	Description
ssh port	It means to Enter the number for SSH port. The default setting is 22.

Example

```
> mngt sshport 23
% Set ssh port to 23 done.
```

Telnet Command: mngt noping

This command is used to pass or block Ping from LAN PC to the internet.

Syntax

mngt noping *on*
mngt noping *off*
mngt noping *viewlog*
mngt noping *clearlog*

Syntax Description

Parameter	Description
on	All PING packets will be forwarded from LAN PC to Internet.
off	All PING packets will be blocked from LAN PC to Internet.
viewlog	It means to display a log of ping action, including source MAC and source IP.
clearlog	It means to clear the log of ping action.

Example

```
> mngt noping off
No Ping Packet Out is OFF!!
```

Telnet Command: mngt defenseworm

This command can block specified port for passing through the router.

Syntax

mngt defenseworm *on*
mngt defenseworm *off*
mngt defenseworm *<add port>*
mngt defenseworm *<del port>*
mngt defenseworm *<viewlog>*
mngt defenseworm *<clearlog>*

Syntax Description

Parameter	Description
on	It means to activate the function of defense worm packet out.
off	It means to inactivate the function of defense worm packet out.
add port	It means to add a new TCP port for block.
del port	It means to delete a TCP port for block.
viewlog	It means to display a log of defense worm packet, including source MAC and source IP.
clearlog	It means to remove the log of defense worm packet.

Example

```
> mngt defenseworm add 21
Add TCP port 21
Block TCP port list: 135, 137, 138, 139, 445, 21
> mngt defenseworm del 21
Delete TCP port 21
Block TCP port list: 135, 137, 138, 139, 445
```

Telnet Command: mngt rmtcfg

This command can allow the system administrators to login from the Internet. By default, it is not allowed.

Syntax

mngt rmtcfg *<status>*

mngt rmtcfg *<enable>*

mngt rmtcfg *<disable>*

mngt rmtcfg *<http/https/ftp/telnet/ssh/tr069/ enforce_https> <on/off>*

Syntax Description

Parameter	Description
status	It means to display current setting for your reference.
enable	It means to allow the system administrators to login from the Internet.
disable	It means to deny the system administrators to login from the Internet.
http/https/ftp/telnet/ssh/tr069/ enforce_https	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>*

mngt lanaccess *–l <value>*

mngt lanaccess *–E <value>*

mngt lanaccess *–f*

mngt lanaccess *–d*

mngt lanaccess *–v*

mngt lanaccess *–h*

Syntax Description

Parameter	Description
-e <0/1>	It means to enable/disable the function. 0-disable the function. 1-enable the function.
-s <value>	It means to specify service offered. Available values include: FTP, HTTP, HTTPS, TELNET, SSH, None, All
-i <value>	It means the interface which is allowed to access. Available values include: LAN2~LAN6, DMZ, IP Routed Subnet, None, All **Note**: LAN1 is always allowed for accessing into the router.
-l <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
> mngt lanaccess –s FTP,TELNET
> mngt lanaccess –i LAN3
> mngt lanaccess –v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
   - FTP:Yes
```

```
   - HTTP:No
   - HTTPS:No
   - TELNET:Yes
   - SSH:No
   - TR069:No
   - Enforce HTTPS:No
* Subnet:
   - LAN 1: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 2: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 3: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 4: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 5: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 6: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 7: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - LAN 8: enabled
     - Specific IP(type:IP Object)(index:0) is disabled
   - IP Routed Subnet: enabled
     - 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 three IPs/ subnet masks is allowed.

Syntax

mngt accesslist *list*

mngt accesslist *add <Index><IP Object Index>*

mngt accesslist *remove <Index>*

mngt accesslist *flush*

Syntax Description

Parameter	Description
list	It can display current setting for your reference.
add	It means adding a new entry.
<Index><IP Object Index>	It means to specify the IP object. Available settings: <index> - Enter the index number of the accesslist profile. <IP Object Index> - Enter the index number of the IP object.
index	It means the index number (1 to 192) of the IP objects preconfigured.
remove	It means to delete the selected item.
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 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 180 (seconds).

Example

```
> mngt sshtimeout 200
% SSH timeout : 200s
>
```

Telnet Command: msubnet switch

This command is used to configure multi-subnet.

Syntax

msubnet switch *<2/3/4> <On/Off>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
On/Off	On means turning on the subnet for the specified LAN interface. Off means turning off the subnet.

Example

```
> msubnet switch 2 On
% LAN2       Subnet On!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet addr

This command is used to configure IP address for the specified LAN interface.

Syntax

msubnet addr *<2/3/4> <IP address>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP address	Enter the private IP address for the specified LAN interface.

Example

```
> msubnet addr 2 192.168.5.1
% Set LAN2 subnet IP address done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nmask

This command is used to configure net mask address for the specified LAN interface.

Syntax

msubnet nmask *<2/3/4> <IP address>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP address	Enter the subnet mask address for the specified LAN interface.

Example

```
> msubnet nmask 2 255.255.0.0
% Set LAN2 subnet mask done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet status

This command is used to display current status of subnet.

Syntax

msubnet status *<2/3/4>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4

Example

```
> msubnet status 2
% LAN2       Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

Syntax

msubnet dhcps *<2/3/4> <On/Off>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
On/Off	On means enabling the DHCP server for the specified LAN interface. Off means disabling the DHCP server.

Example

```
> msubnet dhcps 3 off
% LAN3       Subnet DHCP Server disabled!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

Syntax

msubnet nat *<2/3/4> <On/Off>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
On/Off	On – It means the subnet will be configured for NAT usage. Off - It means the subnet will be configured for Routing usage.

Example

```
> > msubnet nat 2 off
% LAN2 Subnet is for Routing usage!
%Note: If you have multiple WAN connections, please be reminded to setup a
Load-Balance policy so that packets from this subnet will be forwarded to the
right WAN interface!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet gateway

This command is used to configure an IP address as the gateway used for subnet.

Syntax

msubnet gateway *<2/3/4> <Gateway IP>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Gateway IP	Specify an IP address as the gateway IP.

Example

```
> msubnet gateway 2 192.168.1.13
% Set LAN2 Dhcp Gateway IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet ipcnt

This command is used to defined the total number allowed for each LAN interface.

Syntax

msubnet ipcnt *<2/3/4> <IP counts>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
IP counts	Specify a total number of IP address allowed for each LAN interface. The available range is from 0 to 220.

Example

```
> msubnet ipcnt 2 15
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

Syntax

msubnet talk *<1/2/3/4> <1/2/3/4> <On/Off>*

Syntax Description

Parameter	Description
1/2/3/4	It means LAN interface. 1=LAN1 2=LAN2 3=LAN3 4=LAN4
On/Off	On – It means Off - It means

Example

```
> msubnet talk 1 2 on
% Enable routing between LAN1       and LAN2      !

 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> <1/2/3/4/5> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4
% Now:
%            LAN1   LAN2   LAN3   LAN4
% LAN1         V
```

```
% LAN2              V
% LAN3                    V
% LAN4                          V
>
```

Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

Syntax

msubnet startip *<2/3/4> <Gateway IP>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Gateway IP	Type an IP address as the starting IP address for a subnet.

Example

```
> msubnet startip 2 192.168.2.90
% Set LAN2 Dhcp Start IP done !!!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet startip ?
% msubnet startip <2/3/4> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10
```

Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

Syntax

msubnet pppip *<2/3/4> <Start IP>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
Start IP	Type an IP address as the starting IP address for PPP connection.

Example

```
> msubnet pppip 2 192.168.2.250
% Set LAN2 PPP(IPCP) Start IP done !!!
```

```
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.

> msubnet pppip ?
% msubnet pppip <2/3/4> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200
```

Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

Syntax

msubnet nodetype *<2/3/4> <count>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
count	Choose the following number for specifying different node type. 1= B-node 2= P-node 4= M-node 8= H-node 0= Not specify any type for node.

Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 0; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node

>  msubnet nodetype 2 1
% Set LAN2 Dhcp Node Type done !!!

> msubnet nodetype ?
% msubnet nodetype <2/3/4> <count>
% Now: LAN2 1; LAN3 0; LAN4 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

Syntax

msubnet primWINS *<2/3/4> <WINS IP>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
WINS IP	Enter the IP address as the WINS IP.

Example

```
> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

Syntax

msubnet secWINS *<2/3/4> <WINS IP>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
WINS IP	Enter the IP address as the WINS IP.

Example

```
> msubnet secWINS 2 192.168.3.89
% Set LAN2 Dhcp Secondary WINS IP done !!!

> msubnet secWINS ?
% % msubnet secWINS <2/3/4> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0
```

Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

Syntax

msubnet tftp *<2/3/4> <TFTP server name>*

Syntax Description

Parameter	Description
2/3/4	It means LAN interface. 2=LAN2 3=LAN3 4=LAN4
TFTP server name	Type a name to indicate the TFTP server.

Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2
       LAN3
       LAN4

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp ?
% msubnet tftp <2/3/4> <TFTP server name>
% Now: LAN2 publish
       LAN3
       LAN4
```

Telnet Command: msubnet mtu

This command allows you to configure MTU value for LAN/ DMZ/ IP Routed Subnet.

Syntax

msubnet mtu *<interface> <value>*

Syntax Description

Parameter	Description
interface	Available settings include LAN1~LAN4, IP_Routed_Subnet.
value	1000 ~ 1500 (Bytes), default: 1500 (Bytes)

Example

```
> msubnet mtu ?
Usage:

  >msubnet mtu <interface> <value>
```

```
  <interface>: LAN1~LAN4,IP_Routed_Subnet,  <value>:    1000 ~ 1500 (Bytes),
default: 1500 (Bytes)
  e.x: >msubnet mtu LAN1 1492

Current Settings:

   LAN1 MTU:               1500 (Bytes)
   LAN2 MTU:               1500 (Bytes)
   LAN3 MTU:               1500 (Bytes)
   LAN4 MTU:               1500 (Bytes)
   IP Routed Subnet MTU:   1500 (Bytes)
```

Telnet Command: msubnet leasetime

This command allows you to set leasetime for DHCP server. It is helpful to manage the IP address(es) assigned by DHCP server.

Syntax

msubnet leasetime *<1/2/3/4> <Lease Time (sec.)>*

Syntax Description

Parameter	Description
1/2/3/4	1 – 4 represent LAN1 to LAN6.
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

```
> msubnet leasetime 1 80800
Set LAN1 lease time: 80800

> msubnet leasetime 1
% Set LAN1 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 Rang Example: *object ip obj 3 -a 2*
[START_IP]	When the TYPE is set with 2, you have to type an IP address as a starting point and another IP address as end point. Type an IP address.
[END/MASK_IP]	Type an IP address (different with START_IP) as the end IP address.

Example

```
> object ip obj 1 -n marketing
> object ip obj 1 -a 1 192.168.1.45
> 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]
 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]

> object ip grp 2 -i 1
> 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]
```

Telnet Command: object ipv6 obj

This comman is used to create an IP object profile.

Syntax

object ip obj setdefault

object ip obj *INDEX -v*

object ip obj *INDEX -n NAME*

object ip obj *INDEX -i INTERFACE*

object ip obj *INDEX -s INVERT*

obj ipv6 obj *INDEX -e MATCH_TYPE*

object ip 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 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*
-e [0/1]	It means to set the match type of the IPv6 object profile. 0: means 128 Bits 1: means suffix 64 bits interface ID.
-a TYPE	It means to set the address type and IP for the IP object profile. TYPE=0, means Mask TYPE=1, means Single TYPE=2, means Any TYPE=3, means Rang

	Example: *object ip obj 3 -a 2*
<START_IP><END_IP>	When the TYPE is set with 0, 1,3, you have to type an IP address as a starting point and another IP address as end point. Type the IP address(es) based on the selection of TYPE.
<Prefix Length>	When the TYPE is set with 0, 1 or 3, you have to enter a number as prefix length for the IPv6 address.

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 IP objects under an IP group profile.

Syntax

object ip grp setdefault

object ip grp *INDEX -v*

object ip grp *INDEX -n NAME*

object ip grp *INDEX -i INTERFACE*

object ip grp *INDEX -a IP_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object ip grp 1 -v*
-n NAME	It means to define a name for the IP group. NAME: Type a name with less than 15 characters. Example: *object ip grp 8 -n bruce*
-i INTERFACE	It means to define an interface for the IP group. INTERFACE=0, means any INTERFACE=1, means LAN INTERFACE=2, means WAN Example: *object ip grp 3 -i 0*
-a IP_OBJ_INDEX	It means to specify IP object profiles for the group profile. Example: *:object ip grp 3 -a 1 2 3 4 5* The IP object profiles with index number 1,2,3,4 and 5 will be group

	under such profile.

Example

```
> object ipv6 grp 1 -n marketingtest
 IP 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]

> 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]
```

Telnet Command: object service obj

This command is used to create service object profile.

Syntax

object service obj setdefault

object service obj *INDEX -v*

object service obj *INDEX -n NAME*

object service obj *INDEX -p PROTOCOL*

object service obj *INDEX -s CHK <START_P><END_P>*

object service obj *INDEX -d CHK <START_P><END_P>*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified service object profile.
-v	It means to view the information of the specified service object profile. Example: *object service obj 1 -v*
-n NAME	It means to define a name for the IP object. NAME: Type a name with less than 15 characters. Example: *object service obj 9 -n bruce*

-i PROTOCOL	It means to define a PROTOCOL for the service object profile. PROTOCOL =0, means any PROTOCOL =1, means ICMP PROTOCOL =2, means IGMP PROTOCOL =6, means TCP PROTOCOL =17, means UDP PROTOCOL =255, means TCP/ UDP Other values mean other protocols. Example: *object service obj 8 -i 0*
CHK	It means the check action for the port setting. 0=equal**(=)**, when the starting port and ending port values are the same, it indicates one port; when the starting port and ending port values are different, it indicates a range for the port and available for this service type. 1=not equal**(!=)**, when the starting port and ending port values are the same, it indicates all the ports except the port defined here; when the starting port and ending port values are different, it indicates that all the ports except the range defined here are available for this service type. 2=larger**(>)**, the port number greater than this value is available.. 3=less**(<)**, the port number less than this value is available for this profile.
-s CHK <START_P><END_P>	It means to set souce port check and configure port range (1~65565) for TCP/ UDP. END_P, type a port number to indicate 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. END_P, type a port number to indicate 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:[255]
 Source port check action:[!=]
 Source port range:[120~240]
 Destination port check action:[!=]
 Destination port range:[200~220]
```

Telnet Command: object service grp

This command is used to integrate several service objects under a service group profile.

Syntax

object service grp setdefault

object service grp *INDEX -v*

object service grp *INDEX -n NAME*

object service grp *INDEX -a SER_OBJ_INDEX*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
INDEX	It means the index number of the specified group profile.
-v	It means to view the information of the specified group profile. Example: *object service grp 1 –v*
-n NAME	It means to define a name for the service group. NAME: Type a name with less than 15 characters. Example: *object service grp 8 –n bruce*
-a SER_OBJ_INDEX	It means to specify service object profiles for the group profile. Example: *:object service grp 3 –a 1 2 3 4 5* The service object profiles with index number 1,2,3,4 and 5 will be group under such profile.

Example

```
>object service grp 1 –n Grope_1
 Service Group Profile 1
 Name   :[Grope_1]
 Included service object index:
 [0:][0]
 [1:][0]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]

> object service grp 1 –a 1 2
 Service Group Profile 1
 Name   :[Grope_1]
 Included service object index:
 [0:][1]
 [1:][2]
 [2:][0]
 [3:][0]
 [4:][0]
 [5:][0]
 [6:][0]
 [7:][0]
```

Telnet Command: object kw

This command is used to create keyword profile.

Syntax

object kw obj setdefault

object kw obj show PAGE

object kw obj *INDEX -v*

object kw obj *INDEX -n NAME*

object kw obj *INDEX -a CONTENTS*

Syntax Description

Parameter	Description
setdefault	It means to return to default settings for all profiles.
show PAGE	It means to show the contents of the specified profile. PAGE: Enter the page number.
show	It means to show the contents for all of the profiles.
INDEX	It means the index number of the specified keyword profile.
-v	It means to view the information of the specified keyword profile.
-n NAME	It means to define a name for the keyword profile. NAME: Type a name with less than 15 characters.
-a CONTENTS	It means to set the contents for the keyword profile. Example: *object kw obj 40 –a test*

Example

```
> object kw obj 1 –n children
 Profile 1
 Name   :[children]
 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, P2P, Document Example: *object fe obj 1 –e Image* FILE_EXTENSION: ".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".ico", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".flv", ".swf", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr", ".torrent", ".doc", ".docx", ".odp", ".ods", ".odt", ".pdf", ".ppt", ".pptx", ".xls", ".xlsx" Example: *object fe obj 1 –e .bmp*

Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]

-------------------------------------------------------------------------
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff  [ ].ico
-------------------------------------------------------------------------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [ ].mp4   [ ].qt
 [ ].rm    [ ].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2   [ ].flv   [ ].swf
-------------------------------------------------------------------------
```

```
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
------------------------------------------------------------------------
Execution category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
------------------------------------------------------------------------
P2P category:
 [ ].torrent
------------------------------------------------------------------------
Document category:
 [ ].doc   [ ].docx  [ ].odp   [ ].ods   [ ].odt   [ ].pdf   [ ].ppt   [ ].pptx
 [ ].xls   [ ].xlsx
DrayTek>
```

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 <Use SSL>*
object mail obj *INDEX -m <SMTP Port>*
object mail obj *INDEX -a <Sender Address>*
object mail obj *INDEX -t <Authentication>*
object mail obj *INDEX -u <Username>*
object mail obj *INDEX -p <Password>*
object mail obj *INDEX -i <Sending Interval>*

Syntax Description

Parameter	Description
show	It means to show the contents for all of the profiles.
setdefault	It means to return to default settings for all profiles.

<INDEX>	It means the index number (from 1 to 10) of the specified mail object profile.
-v	It means to view the information of the specified mail object profile.
-n <Profile Name>	It means to define a name for the mail object profile. *Profile Name*: Type a name with less than 15 characters.
-s <SMTP Server>	It means to set the IP address of the mail server.
-l <Use SSL>	It means to use port 465 for SMTP server for some e-mail server uses https as the transmission method. 0 – disable 1 – enable to use the port number.
-m <SMTP Port>	It means to set the port number for SMTP server.
-a <Sender Address>	It means to set the e-mail address (e.g., johnwash@abc.com.tw) of the sender.
-t <Authentication>	The mail server must be authenticated with the correct username and password to have the right of sending message out. 0 – disable 1 – enable to use the port number.
-u <Username>	Type a name for authentication. The maximum length of the name you can set is 31 characters.
-p <Password>	Type a password for authentication. The maximum length of the password you can set is 31 characters.
-i <Sending Interval>	Define the interval for the system to send the SMS out. The unit is second.

Example

```
> object mail obj 1 -n buyer
> object mail obj 1 -n buyer
> object mail obj 1 -s 192.168.1.98
> object mail obj 1 -m 25
> object mail obj 1 -t 1
> object mail obj 1 -u john
> object mail obj 1 -p happy123456
> object mail obj 1 -i 25
> object mail obj 1 -v
Profile Index: 1
Profile Name:[buyer]
SMTP Server:[192.168.1.98]
SMTP Port:[25]
Sender Address:[]
Use SSL:[disable]
Authentication:[enable]
Username:[john]
Password:[******]
Sending Interval:[25(seconds)]
```

Telnet Command: object noti

This command is used to create notification object profile.

Syntax

object noti show
object noti setdefault
object noti obj *INDEX -v*
object noti obj *INDEX -n <Profile Name>*
object noti obj *INDEX –e <Category> <status>*
object noti 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; 9: Security
<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 Security – 1: 1 : Web Log-in event occurs. 2 : Telnet Log-in event occurs. 3 : SSH Log-in event occurs. 4 : TR069 Log-in event occurs. 5 : FTP User Log-in event occurs. 6 : Config-Changed event occurs.

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 -e 9 1
> object noti obj 1 -v

Profile Index: 1
Profile Name:[markbei]
    Category                  Status
  WAN                 [v]Disconnected     [ ]Reconnected
  VPN Tunnel          [v]Disconnected     [ ]Reconnected
  Temperature Alert   [ ]USB Temperature Out of Range
  WAN Budget Alert    [ ]Limit Reached
  Security            [v]Web Log-in event occurs
                      [ ]Telnet Log-in event occurs
                      [ ]SSH Log-in event occurs
                      [ ]TR069 Log-in event occurs
                      [ ]FTP User Log-in event occurs
```

```
                    [ ]Config-Changed event occurs

DrayTek>
```

Telnet Command: object schedule

This command is used to create schedule object profile.

Syntax

object schedule set *INDEX option*
object schedule view
object schedule setdefault

Syntax Description

Parameter	Description
set	It means to set the schedule profile.
<INDEX>	It means the index number (from 1 to 15) of the specified object profile.
option	Available options for schedule.
-e <value>	It means to enable the schedule setup. 0 – disable 1 – enable
-c <comment>	It means to set brief description for the specified profile. The length range of the comment: 0 ~ 32 characters.
-D <year><month><day>	It means to set the starting date of the profile. [year] – Must be between 2000-2049. [month] - Must be between 1-12. [day] - Must be between 1-31. For example: To set Start Date 2015/10/6, type *> object schedule set 1 -D "2015 10 6"*
-T <hour><minute>	It means to set the starting time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Start Time 10:20, type *> object schedule set 1 -T "10 20"*
-d <hour><minute>	It means to set the duration time of the profile. [hour] - Must be between 0-23. [minute] - Must be between 0-59. For example: To set Duration Time 3:30, type *> object schedule set 1 -d "3 30"*
-a <value>	It means to set the action used for the profile. [value] – 0:Force On, 1:Force Down, 2:Enable Dial-On-Demand, 3:Disable Dial-On-Demand
-I <value>	It means to set idle time. [value] – Must be between 0-255(minute). The default is 0.
-h <option><day>	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, all> <AN, 100F, 100H, 10F, 10H, status>*

port *<wan2> <AN, 1000F, 100F, 100H, 10F, 10H, status>*

port wan1 fiber

port wan1 ethernet *<AN, 100F, 100H, 10F, 10H, status>*

port status

port sniff *<on,off,port,txrx,restart,status>*

port jumbo *<on/off> / <value>*

port wanfc

Syntax Description

Parameter	Description
1, 2, 3, all	It means the number of LAN port and WAN port.
AN...10H	It means the physical type for the specific port. AN: auto-negotiate. 1000F: 1000M Full Duplex. 100F: 100M Full Duplex. 100H: 100M Half Duplex. 10F: 10M Full Duplex. 10H: 10M Half Duplex.

status	It means to view the Ethernet port status.
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
jumbo <on/off>	It means to enable (on) or disable (off) the Jumbo frame function.
jumbo size <value>	If jumbo is enabled, set a jumbo size. <value>: 1537 to 9022. Set a number.
wanfc <INDEX> <on/off/status>	It means to set WAN flow control. <INDEX>: Enter the index number (1 to 2) of the WAN interface. <on/off/status>: Enter "on" to enable the function; enter "off" to disable the function; enter "status" to view current settings.

Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

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: ppa

This command allows you to configure PPA mode.

ppa *[-<command> <parameter> | ...]*

ppa n *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-m <mode>	Specify a mode. 1=auto 2=manual(traffic) 3=manual(qos) 4=manual(specific hosts) 0=disable
-p <proto>	Specify a protocol. proto - 1-TCP; 2-UDP; 3-Both.
-b 1/0	Enable/disable TWO-way hardware acceleration.
-M enable/disable	Enable/disable the multicast hardware acceleration.
-v	Show PPA_WAN_Table and PPA_LAN_Table for reference.
-c	Clean all settings.
ppa n – used in QoS or specific host	
-l <rule>	Specify an index number of rule profile for QoS mode.
-h <host>	Type an IP address for Specific Host mode.
-s <start port>	Specify a starting port number for Specific Host mode.
-e <end port>	Specify an ending port number for Specific Host mode

Example

```
> ppa -m 1 -p 1 -b 0
 Set ok! The PPA mode is Auto

% You need to set the Manual mode first !

%TWO way accleration is disable

> ppa -v
%PPA is enabled
%PPA NAT is enabled
% PPA mode is Auto
```

```
%PPA Protocol TCP 1, UDP 0
%PPA range is 4096
%PPA total entries 0
%PPA statistics interval: 5 sec
>
```

Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

Syntax

prn status

prn enable <0/1>

Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

>
```

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 <1~2>	It means to select an interface. <1~2>: 1 is WAN1; 2 is WAN2 and etc. The default is WAN1.
-m <mode>	It means to define which traffic the QoS control settings will apply to and eable QoS control. 0: disable. 1: in, apply to incoming traffic only. 2: out, apply to outgoing traffic only. 3: both, apply to both incoming and outgoing traffic. Default is enable (for outgoing traffic).
-i <bandwidth>	It means to set inbound bandwidth in kbps (Ethernet WAN only) The available setting is from 1 to 100000.
-o <bandwidth>	It means to set outbound bandwidth in kbps (Ethernet WAN only). The available setting is from 1 to 100000.
-r <index:ratio>	It means to set ratio for class index, in %.
-u <mode>	It means to enable bandwidth control for UDP. 0: disable 1: enable Default is disable.

-p <ratio>	It means to enable bandwidth limit ratio for UDP.
-t <mode>	It means to enable/ disable Outbound TCP ACK Prioritize. 0: disable 1: enable
-V	Show all the settings.
-I <bandwidth>	It means the minimum available non-VoIP Inbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN inbound bandwidth.
-O <bandwidth>	It means the minimum available non-VoIP Outbound Bandwidth when VoIP is detected (Kbps). <bandwidth>: Enter a value. Default value: half of WAN outbound bandwidth.
-v <0/ 1>	It means to adjust to minimum In/ Out bandwidth setting (or half QoS bandwidth). 0: Auto bandwidth adjustment. 1: When VoIP detected, QoS In/ Out bandwidth will be adjusted to minimum values.
-D	Set all to factory default (for all WANs).

Example

```
> qos setup -W 2 -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1

 Setup WAN2 !!!!
 WAN2 QOS mode is both
 inbound bandwidth set to 9500
 outbound bandwidth set to 8500
 WAN2 class 3 ratio set to 20
 WAN2 udp bandwidth control set to enable
 WAN2 udp bandwidth limit ratio set to 50
 WAN2 Outbound TCP ACK Prioritizel set to enable
QoS WAN2 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>: Enter the index number for the rule.
-d <no>	It means to delete specified rule. <no>: Enter the index number for the rule.
-m <mode>	It means to enable or disable the specified rule. 0: disable, 1: enable
-I <addr>	Set the local address. *Addr1* – It means Single address. Please specify the IP address directly, for example, "*-I 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50.*" *addr1:subnet* – It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "*-I 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-I*" to specify any address for this command.
-r <addr>	Set the remote address. *addr1* – It means Single address. Please specify the IP address directly, for example, "*-I 172.16.3.9*". *addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50.*" *addr1:subnet* – It means the subnet address with start IP address. Please Enter the subnet and the IP address, for example, "*-I 172.16.3.9:255.255.0.0".0* *any* – It means Any address. Simple type "*-I*" to specify any address for this command.
-p <DSCP id>	Specify the ID.
-s <Service type>	Specify the predefined service type by typing the number. The available types are listed as below: 1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP 11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP 16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP 21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS 26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP
-u <Service type>	Specify the user defined service type by typing the number (1 to 40).
-S <d/s>	Show the content for specified DSCP ID/ Service type.
-V <1/2/3>	Show the rule in the specified class.

Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

 Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 2 rule is 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:
         ip             mask       dhcp  star_ip          pool   gateway
-------------------------------------------------------------------------
[V]LAN1  192.168.1.1    255.255.255.0   V   192.168.1.10    200
192.168.1.1
[X]LAN2  192.168.2.1    255.255.255.0   V   192.168.2.90    100
192.168.2.1
[X]LAN3  192.168.3.1    255.255.255.0   V   192.168.3.10    100
192.168.3.1
[X]LAN4  192.168.4.1    255.255.255.0   V   192.168.4.10    100
192.168.4.1
[X]Route 192.168.0.1    255.255.255.0   V    0.0.0.0        0    192.168.0.1
```

Telnet Command: show dmz

This command displays current status of DMZ host.

Example

```
> 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
```

Telnet Command: show dns

This command displays current status of DNS setting

Example

```
> show dns
%%     Domain name server settings:
%  LAN1  Primary DNS: [Not set]
%  LAN1  Secondary DNS: [Not set]

%  LAN2  Primary DNS: [Not set]
%  LAN2  Secondary DNS: [Not set]

%  LAN3  Primary DNS: [Not set]
%  LAN3  Secondary DNS: [Not set]
```

```
%  LAN4  Primary DNS: [Not set]
%  LAN4  Secondary DNS: [Not set]

%  LAN5  Primary DNS: [Not set]
%  LAN5  Secondary DNS: [Not set]

%  LAN6  Primary DNS: [Not set]
%  LAN6  Secondary DNS: [Not set]

%  LAN7  Primary DNS: [Not set]
%  LAN7  Secondary DNS: [Not set]

%  LAN8  Primary DNS: [Not set]
%  LAN8  Secondary DNS: [Not set]
```

Telnet Command: show openport

This command displays current status of open port setting.

Example

```
> show openport
%%     Openport settings:
Index   Status  Comment        Local IP Address
********************************************************
                 No data entry.
```

Telnet Command: show nat

This command displays current status of NAT.

Example

```
> show nat
 Port Redirection Running Table:

Index  Protocol  Public Port   Private IP       Private Port
 1          0          0   0.0.0.0                  0
 2          0          0   0.0.0.0                  0
 3          0          0   0.0.0.0                  0
 4          0          0   0.0.0.0                  0
 5          0          0   0.0.0.0                  0
 6          0          0   0.0.0.0                  0
 7          0          0   0.0.0.0                  0
 8          0          0   0.0.0.0                  0
 9          0          0   0.0.0.0                  0
10          0          0   0.0.0.0                  0
11          0          0   0.0.0.0                  0
12          0          0   0.0.0.0                  0
13          0          0   0.0.0.0                  0
14          0          0   0.0.0.0                  0
15          0          0   0.0.0.0                  0
16          0          0   0.0.0.0                  0
17          0          0   0.0.0.0                  0
18          0          0   0.0.0.0                  0
19          0          0   0.0.0.0                  0
20          0          0   0.0.0.0                  0
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page]
```

Telnet Command: show portmap

This command displays the table of NAT Active Sessions.

Example

```
> show portmap
-------------------------------------------------------------------------
  Private_IP:Port Pseudo_IP:Port Peer_IP:Port [Timeout/Protocol/Flag]
-------------------------------------------------------------------------
```

Telnet Command: show pmtime

This command displays the reuse time of NAT session.

Level0: It is the default setting.

Level1: It will be applied when the NAT sessions are smaller than 25%of the default setting.

Level2: It will be applied when the NAT sessions are smaller than the eighth of the default setting.

Example

```
> show pmtime
  Level0 TCP=86400001 UDP=300001 ICMP=10001
  Level1 TCP=600000 UDP=90000 ICMP=7000
  Level2 TCP=60000 UDP=30000 ICMP=5000
```

Telnet Command: show session

This command displays current status of current session.

Example

```
> show session
% Maximum Session Number: 30000
% Maximum Session Usage: 0
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
% WAN2 Current Session Usage: 0
>
```

Telnet Command: show status

This command displays current status of LAN and WAN connections.

Example

```
> show status
System Uptime:50:58:27
LAN Status
Primary DNS:8.8.8.8          Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:270353    Rx Rate:91170

WAN 1 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
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

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
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
>
```

Telnet Command: show traffic

This comman can display traffic graph for WAN1, WAN2, transmitted bytes, receivied bytes and sessions.

Syntax

show traffic *<wan1/wan2><tx/rx><weekly>*

show traffic session *<weekly>*

show traffic *<ipaddr><tx/rx>*

Example

```
> show traffic session weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,2 ,1 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,1 ,3 ,0 ,0 ,0 ,0 ,0 ,2 ,15 ,5 ,4 ,1 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 0 ,0 ,0 ,0
> show traffic wan1 tx weekly0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
 0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
```

Telnet Command: show clienttraffic

This command displays packet information for specified external device.

Syntax

show clienttraffic *<device index><wan# or lan#><tx/rx><weekly>*

Syntax Description

Parameter	Description
<device index>	Enter the device index (01 – 30) in double-digit (ex: 01, 02) for external device. Use "switch list" to check which VigorSwitch connects to this router. Then, Enter the index number of this VigorSwitch in this field.
<wan# or lan#>	wan# - Specify WAN interface (WAN1 to WAN2) for Vigor router. lan#- Specify LAN interface (LANA / LANB) for VigorAP.
<tx/rx>	Tx – Inidcate transmitted data. Rx – Indicate receivied data.
<weekly>	Display the transmitted data or receivied data collected weekly.

Example

```
> show clienttraffic 01 lana tx weekly
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,
0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0
```

Telnet Command: show statistic

This command displays statistics for WAN interface.

Syntax

show statistic

show statistic reset *<interface>*

Syntax Description

Parameter	Description
reset	It means to reset the transmitted/received bytes to Zero.
interface	It means to specify WAN1 ~WAN5 (including multi-PVC) interface for displaying related statistics.

Example

```
> show statistic
 WAN1 total TX: 0 Bytes ,RX: 0 Bytes
 WAN2 total TX: 0 Bytes ,RX: 0 Bytes
 WAN3 total TX: 0 Bytes ,RX: 0 Bytes
 WAN4 total TX: 0 Bytes ,RX: 0 Bytes
 WAN5 total TX: 0 Bytes ,RX: 0 Bytes
 >
```

Telnet Command: smb setting

This command is used to configure file sharing settings for SMB server.

Syntax

smb setting *<enable/disable>*

smb setting *show status*

smb setting *set workgroup <Workgroup name>*

smb setting *set host <host name>*

smb setting *set access <LAN / LANWAN>*

smb setting *set version <v1v2/v2>*

Syntax Description

Parameter	Description
<enable/disable>	Enable or disable the SMB service.
show status	Display current status of SMB service.
Set workgroup <Workgroup name>	Set a name of workgroup for SMB service.
set host <host name>	Set a name of the host for SMB service.
set access <LAN / LANWAN>	Allow to access into SMB server by LAN or borth LAN and WAN.
set version <v1v2/v2>	It means to set SMB server version.

Example

```
> smb setting enable
SMB service is enabled.
```

```
> smb setting set access LAN
Allow SMB access from LAN only.
> smb setting set version v1v2
SMB version: v1 and v2.
```

Telnet Command: srv dhcp dhcp2

This command is used to enable DCHP2 server.

Syntax

srv dhcp dhcp2 *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
[<command> <parameter>|..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-l <enable>	It menas to enable the LAN port to public DHCP. 0: Disenable 1: Enable
-m <enable>	It menas to enable MAC address to public DHCP. 0: Disenable 1: Enable
-e <id>	It menas to turn on the flag of LAN port 3/4.
-d <id>	It menas to turn off the flag of LAN port 3/4.
-v	It menas to view current status.

Example

```
> srv dhcp dhcp2 -l 1 -e 1
> srv dhcp dhcp2 -v
 2nd DHCP server flag status --
   Server works on specified MAC address: ON
   Server works on specified LAN port: ON
   Port 1 flag: ON
   Port 2 flag: ON
   Port 3 flag: OFF
   Port 4 flag: OFF
```

Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

Syntax

srv dhcp public *start <IP address>*
srv dhcp public *cnt <IP counts>*
srv dhcp public *status*
srv dhcp public *add <MAC Addr XX-XX-XX-XX-XX-XX>*
srv dhcp public *del <MAC Addr XX-XX-XX-XX-XX-XX/ all/ ALL>*

Syntax Description

Parameter	Description
start <IP address>	It means the starting point of the IP address pool for the DHCP

	server. *<IP address>:* Specify an IP address as the starting point in the IP address pool.
cnt <IP counts>	It means the IP count number. *<IP counts>:* Specify the number of IP addresses in the pool. The maximum is 10.
status	It means the execution result of this command.
add <MAC Addr XX-XX-XX-XX-XX-XX>	It means creating a list of hosts to be assigned. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host.
del <MAC Addr XX-XX-XX-XX-XX-XX/all/ALL>	It means removing the selected MAC address. <MAC Addr XX-XX-XX-XX-XX-XX>: Specify MAC Address of the host. all/ALL: It means all of the MAC addresses.

Example

```
> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
> srv dhcp public status
Index   MAC Address
```

Telnet Command: srv dhcp dns1

This command allows users to set Primary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns1 *<lan1/lan2/lan3/lan4> <DNS IP address>*

Syntax Description

Parameter	Description
<lan1/lan2/lan3/lan4>	It means to sepcify the LAN interface for setting the DNS server.
DNS IP address	It means the IP address that you want to use as DNS1. **Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns1 lan1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1>
```

Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

Syntax

srv dhcp dns2 *<lan1/lan2/lan3/lan4> <DNS IP address>*

Syntax Description

Parameter	Description
<lan1/lan2/lan3/lan4>	It means to sepcify the LAN interface for setting the DNS server.
DNS IP address	It means the IP address that you want to use as DNS2.

	Note: The IP Routed Subnet DNS must be the same as NAT Subnet DNS).

Example

```
> srv dhcp dns2 lan1 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
>
```

Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

Syntax

srv dhcp frcdnsmanl <*on/off*>

Syntax Description

Parameter	Description
?	It means to display the current status.
on	It means to use manual setting for DNS setting.
Off	It means to use auto settings acquired from ISP.

Example

```
> srv dhcp frcdnsmanl on
% Domain name server now is using manual settings!
> srv dhcp frcdnsmanl off
% Domain name server now is using auto settings!
```

Telnet Command: srv dhcp gateway

This command allows users to specify gateway address for DHCP server.

Syntax

srv dhcp gateway *[Gateway IP]*

Syntax Description

Parameter	Description
Gateway IP	It means to specify a gateway address used for DHCP server.

Example

```
> srv dhcp gateway 192.168.2.1
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp ipcnt

This command allows users to specify IP counts for DHCP server.

Syntax

srv dhcp ipcnt *<IP counts>*

Syntax Description

Parameter	Description
IP counts	It means the number that you have to specify for the DHCP server.

Example

```
> srv dhcp ipcnt ?
% srv dhcp ipcnt <IP counts>
% Now: 150
```

Telnet Command: srv dhcp off

This function allows users to turn off DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp on

This function allows users to turn on DHCP server. It needs rebooting router, please type "sys reboot" command to reboot router.

Telnet Command: srv dhcp relay

This command allows users to set DHCP relay setting.

Syntax

srv dhcp relay servip *<server ip>*

srv dhcp relay 2nd_servip *<server ip>*

srv dhcp relay subnet *<index>*

Syntax Description

Parameter	Description
server ip	It means the IP address that you want to used as DHCP server.
Index	It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here.

Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
>srv dhcp relay servip 192.168.1.46
>srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
% Now: 192.168.1.46
```

Telnet Command: srv dhcp startip

Syntax

srv dhcp startip *<IP address>*

Syntax Description

Parameter	Description
IP address	It means the IP address that you can specify for the DHCP server as the starting point.

Example

```
> srv dhcp startip 192.168.1.53
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: srv dhcp status

This command can display general information for the DHCP server, such as IP address, MAC address, leased time, host ID and so on.

Syntax

srv dhcp status *<LAN1/2/3/4/ip_routed_subnet>*

Syntax Description

Parameter	Description
< LAN1/2/3/4/ ip_routed_subnet >	It means to display current status for the selected interface.

Example

```
> srv dhcp status
LAN1      : DHCP Server On    IP Pool: 192.168.1.10 ~ 192.168.1.209
            Default Gateway: 192.168.1.1
IP Routed  : DHCP Server Off
-------------------------------------------------------------------------
------
Index   IP Address     MAC Address           Leased Time     HOST ID
-------------------------------------------------------------------------
------
LAN1
1       192.168.1.10    00-1D-AA-0F-2E-68       17:24:58
 2       192.168.1.11    00-1D-AA-4F-E2-98       17:54:14
```

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

```
> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

Syntax

srv dhcp tftp *<TFTP server name>*

Syntax Description

Parameter	Description
TFTP server name	It means to Enter the name of TFTP server.

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
```

Telnet Command: srv dhcp tftpdel

This command can remove the name defined for the TFTP server.

Syntax

srv dhcp tftpdel

Example

```
> srv dhcp tftp TF123
> srv dhcp tftp ?
%% srv dhcp tftp <TFTP server name>
% Now: TF123
> srv dhcp tftpdel
% The TFTP Server Name had been deleted !!!
```

Telnet Command: srv dhcp option

This command can set the custom option for the DHCP server.

Syntax

srv dhcp option *-h*

srv dhcp option *-l*

srv dhcp option *-d <idx>*

srv dhcp option *-e <1 or 0> -i <lan number> -s <Next Server IP Address>*

srv dhcp option *-e <1 or 0> -i <lan number> -c <option number> -v <option value>*

srv dhcp option *-e <1 or 0> -i <lan number> -c <option number> -x <option value>*

srv dhcp option *-e <1 or 0> -i <lan number> -c <option number> -a <option value>*

srv dhcp option *-u <idx number>*

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.
-i <lan number>	<lan number> *:* It means to specify the LAN interface. 1: lan1 a: all LAN r: routed subnet d: DMZ
-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 ~ 32 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 <IP address>	It means to specify the private IP address of the DMZ host. IP address: Enter an IP address.
-r	It means to remove DMZ host setting.
-v	It means to display current status.

Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> 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
```

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 Enter the description (less than 23 characters) for the defined network service.
-I <source ip idx>	It means to set source IP object. 1 to 192: for IP object 1 to 32: for IP group 0: Any For example: srv nat openport 1 1 -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 by entering the index number of WAN interface. 1: WAN1 Default, 2: WAN1 Alias 1, ..and so on. ipidx: Specify the index number of an alias IP (1 to 32).
-p <protocol>	Specify the transport layer protocol. Available values are TCP, UDP and ALL.
-s <start port>	It means to specify the starting port number of the service offered by the local host. The range is from 0 to 65535.
-e <end port>	It means to specify the ending port number of the service offered by the local host. The range is from 0 to 65535.
-v	It means to display current settings.
-r <remove>	It means to delete the specified open port setting. remove: Enter the index number of the profile.
-f <flush>	It means to return to factory settings for all the open ports profiles.

Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.55 -w 1 1 -p TCP -s 56 -e
83
 Set WAN Port ok!!

DrayTek> 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             83
>
```

Telnet Command: srv nat portmap

This command allows users to set port redirection table for NAT server.

Syntax

srv nat portmap *add <idx> <serv name> <proto> <pub port> <src ip type> <src ip idx> <pri ip> <pri port> <wan idx> <alias IP>*

srv nat portmap *del <idx>*

srv nat portmap *disable <idx>*

srv nat portmap *enable <idx><proto>*

srv nat portmap *flush*

srv nat portmap *table*

srv nat portmap *view*

Syntax Description

Parameter	Description
add <idx>	It means to add a new port redirection table with an index number. Available index number is from 1 to 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 (1 to 65535) of the service offered by the internal host.
<wan idx>	It means to specify WAN interface for the port redirection. Idx: wan1 to wan2, 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     game             6          80   192.168.1.11        100     -1
 2                      0          0                    0     -2
 3                      0          0                    0     -2
 4                      0          0                    0     -2
 5                      0          0                    0     -2
 6                      0          0                    0     -2
 7                      0          0                    0     -2
 8                      0          0                    0     -2
 9                      0          0                    0     -2
10                      0          0                    0     -2
11                      0          0                    0     -2
12                      0          0                    0     -2
13                      0          0                    0     -2
14                      0          0                    0     -2
15                      0          0                    0     -2
16                      0          0                    0     -2
17                      0          0                    0     -2
18                      0          0                    0     -2

19                      0          0                    0     -2
```

```
20                    0          0                    0      -2


Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

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     0.0.0.0:80               192.168.1.11:100          Y

O01     TCP     0.0.0.0:23~83             192.168.1.100:23~83       Y

R:Port Redirection, O:Open Ports, D:DMZ
```

Telnet Command: srv nat pseudoctl

This command allows users to check the pseudo port number to prevent from port conflict.

Syntax

srv nat pseudoctl *session <value>*

srv nat pseudoctl *function <0-3>*

Syntax Description

Parameter	Description
session <value>	Set the threshold of the session. <value>: o to 2147483647.
function <0-3>	0: It means "Auto". Check the created pseudo port number automatically when the session number is over the threshold. 1: It means "Not". Create a pseudo port number based on subnet setting. No verification. 2: It means "Must". Check the created pseudo port number if it is used by other client. 3: Create a pseudo port number. No verification.

Example

```
> srv nat pseudoctl function 2
 pesudo port: get hash pseudo port + subnet.
 pseudo port search: check pseudo port(Must).

> srv nat pseudoctl function 3
 pesudo port: get hash pseudo port.

> srv nat pseudoctl function 0
 pesudo port: get hash pseudo port + subnet.
 pseudo port search: check pseudo port(Auto).
```

Telnet Command: srv nat RSTTimeout

This command is used for forwarding RST out via TCP after a period of time.

Syntax

srv nat RSTTimeout *<value>*

Syntax Description

Parameter	Description
<value>	Set the timeout value. <value>: 0 to 10 (one unit is 10msec).

Example

```
>  srv nat RSTTimeout 2
Set timeout 2 unit

> srv 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 status for external devices.

Example

```
> switch status
External Device auto discovery status : Disable

No Respond to External Device : 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   Model_Name
-------------------------------------------------------------------------
--
[1]  00-50-7f-cd-07-48  192.168.1.3    On-Line   00:01:01   Vigor2920
Series
```

Telnet Command: switch clear

This command is used to reset the switch table and reboot the router.

Syntax

switch clear *<idx>*

Syntax Description

Parameter	Description
idx	It means the index number of each item shown on the table. The range is from 1 to 8.
-f	It means to clear all of the data.

Example

```
> switch clear 1
Switch Data clear successful

> switch clear -f
Switch Data clear successful
```

Telnet Command: switch query

This command is used to enable or disable the switch query.

Example

```
> switch query on
Extern Device status query is Enable
> switch query off
Extern Device status query is Disable
```

Telnet Command: switch syslog

This command is used to enable or disable the external device syslog.

Example

```
> switch syslog on
Extern Device status is Enable
> switch syslog off
Extern Device status is Disable
```

Telnet Command: sys admin

This command is used for RD engineer to access into test mode of Vigor router.

Telnet Command: sys adminuser

This command is used to create user account and specify LDAP server. The server will authenticate the local user who wants to access into the web user interface of Vigor router.

Syntax

sys adminuser *<option>*

sys adminuser edit *<index> username password*

Syntax Description

Parameter	Description
option	Available options includes: Local <0-1> LDAP <0-1> Edit <index> delete <index> view <index>
Local <0-1>	0 – Disable the local user. 1 – Enable the local user.
LDAP <0-1>	0 – Disable the LDAP. 1 – Enable the LDAP.
edit <index> username password	Edit an existed user account or create a new local user account. <index> – 1 ~8. There are eight profiles to be added / edited. Username – Type a new name for local user. Password – Type a password for local user.
delete <index>	Delete a local user account.
view <index>	Show the user account/password detail information.

Example

```
> sys adminuser Local 1
Local User has enabled!
> sys adminuser LDAP 1
LDAP has enabled!
>> sys adminuser edit 1 carrie test123
Updated!
>> sys adminuser view 1

Index:1
User Name:carrie
User Password:test123
```

Telnet Command: sys board

This command is used to turn on or turn off the function of physical factory reset button, WLAN button, LEDs, and / or the USB ports on Vigor router.

Syntax

sys board button def *<on/off>*

sys board button wlan *<on/off>*

sys board led control *<on/off>*

sys board led sleepMode *<on/off>*

sys board led sleepMode time *<minute>*

sys board usb p1/p2 *<on/off>*

Syntax Description

Parameter	Description
button def <on/off>	The default reset button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
Button wlan <on/off>	The wireless button will be invalid if turn it off. On - The button is valid. Off - The button is invalid.
led control <on/off>	All LEDs on the front panel will be invalid if turn it off. On - The LEDs are valid. Off - The LEDs are invalid.
led sleepMode <on/off>	All LEDs on the front panel will be set in sleep mode. On - The sleep mode is on. Off - The sleep mode is off. If the sleep mode is on, push the "wireless button" and the "factory reset button" to turn the LED on (even the buttons are disabled).
led sleepMode time [minutes]	After enableing the sleep mode for all LEDs, they will sleep after the minutes configured here. Minutes: Enter the number of the time.
usb <p1/p2> <on/off>	The USB port will be invalid if turn it off. On - The port is valid. Off - The port is invalid.

Example

```
> sys board led sleepMode on
 LEDs Sleep Mode is on now.

> sys board led sleepMode time 10
 Sleep Countdown Time set as 10 minute(s).
 Reset the led sleep timer success..
```

Telnet Command: sys bonjour

This command is used to disable/enable and configure the Bonjour service.

Syntax

sys bonjour *[-<command> <parameter> | ...]*

Syntax Description

Parameter	Description
-e <enable>	It is used to disable/enable bonjour service (0: disable, 1: enable).
-h <enable>	It is used to disable/enable http (web) service (0: disable, 1: enable).
-t <enable>	It is used to disable/enable telnet service (0: disable, 1: enable).
-f <enable>	It is used to disable/enable FTP service (0: disable, 1: enable).

-s <enable>	It is used to disable/ enable SSH service (0: disable, 1: enable).
-p <enable>	It is used to disable/ enable printer service (0: disable, 1: enable).
-6 <enable>	It is used to disable/ enable IPv6 (0: disable, 1: enable).

Example

```
> sys bonjour -s 1
>
```

Telnet Command: sys cfg

This command reset the router with factory default settings. When a user types this command, all the configuration will be reset to default setting.

Syntax

sys cfg default

sys cfg status

Syntax Description

Parameter	Description
default	It means to reset current settings with default values.
status	It means to display current profile version and status.

Example

```
> sys cfg status
Profile version: 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 ?
    [2] sys cmdlog >
    [3] sys cmdlog ?
    [4] sys cmdlog
>
```

Telnet Command: sys ftpd

This command displays current status of FTP server.

Syntax

sys ftpd *on*

sys ftpd *off*

Syntax Description

Parameter	Description
on	It means to turn on the FTP server of the system.
off	It means to turn off the FTP server of the system.

Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

Syntax

sys domainname *<wan1/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 39.
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	Enter the old password.
new password	Enter a string as the new password for administrator. The maximum character that you can set is 83.

Example

```
> sys passwd admin admin123
Password change successful !!!
>
```

Telnet Command: sys reboot

This command allows users to restart the router immediately.

Example

```
> sys reboot
>
```

Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

Syntax

sys autoreboot *<on/off/hour(s)>*

Syntax Description

Parameter	Description
on/off	On – It means to enable the function of auto-reboot. Off – It means to disable the function of auto-reboot.
hours	It means to set the time schedule for router reboot. For example, if you type "2" in this field, the router will reboot with an **interval** of two hours.

Example

```
> sys autoreboot on
 autoreboot is ON
> sys autoreboot 2
 autoreboot is ON
 autoreboot time is 2 hour(s)
```

Telnet Command: sys commit

This command allows users to save current settings to FLASH. Usually, current settings will be saved in SRAM. Yet, this command will save the file to FLASH.

Example

```
> sys commit
>
```

Telnet Command: sys tftpd

This command can turn on TFTP server for upgrading the firmware.

Example

```
> sys tftpd
% TFTP server enabled !!!
```

Telnet Command: sys cc

This command can display current country code and wireless region of this device.

Example

```
> sys cc
Country Code       : 0x 0 [International]
Wireless Region Code: 0x30
>
```

Telnet Command: sys version

This command can display current version for the system.

Example

```
> sys version
Router Model: Vigor2915ac    Version: 4.3.0 English
Profile version: 4.0.0    Status: 1 (0xbde1fea3)
Router IP: 192.168.1.1    Netmask: 255.255.255.0
Firmware Build Date/Time: Dec  4 2020 10:21:46
Router Name: DrayTek
Revision: 2998_945_49d80f8 HEAD
>
```

Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff  ( 200B), used#: 1647, cached#:   30
Buf KMC4088  (4088B), used#:    0, cached#:    8
Buf KMC2552  (2552B), used#: 1641, cached#:   42
Buf KMC1016  (1016B), used#:    7, cached#:    1
Buf KMC504   ( 504B), used#:    8, cached#:    8
Buf KMC248   ( 248B), used#:   26, cached#:   22
Buf KMC120   ( 120B), used#:   67, cached#:   61
Buf KMC56    (  56B), used#:   20, cached#:   44
Buf KMC24    (  24B), used#:   58, cached#:   70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the router.

Syntax

sys pollbuf *<on/off>*

Syntax Description

Parameter	Description
on	It means to turn on pulling buffer.
off	It means to turn off pulling buffer.

Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
% Buffer polling is off!
```

Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

Syntax

sys tr069 get *<parm> <option>*
sys tr069 set *<parm> <value>*
sys tr069 getnoti *<parm>*
sys tr069 setnoti *<parm> <value>*
sys tr069 log
sys tr069 debug *<on/off>*
sys tr069 save
sys tr069 inform *<event code>*
sys tr069 port *<port num>*
sys tr069 cert_auth*<on/off>*
sys tr069 only_standard_parm *<on/off>*
sys tr069 notify -S
sys tr069 notify -n *<on/off>*
sys tr069 notify -l *<on/off>*
sys tr069 notify -c *<on/off>*
sys tr069 notify -b *<on/off>*
sys tr069 notify -B *"<WAN number> <Medium threthold> <High threthold> <TX Speed>Mb <RX Speed>Mb"*

Syntax Description

Parameter	Description
get <parm> <option>	It means to get parameters for tr-069. option=<nextlevel>: only gets nextlevel for GetParameterNames.
set <parm> <value>	It means to set parameters for tr-069.
getnoti <parm>	It means to get parameter notification value.
setnoti <parm> <value>	It means to set parameter notification value.
log	It means to display the TR-069 log.
debug <on/off>	on: turn on the function of sending debug message to syslog. off: turn off the function of sending debug message to syslog.
save	It means to save the parameters to the flash memory of the router.
Inform <event code>	It means to inform parameters for tr069 with different event codes. [event code] includes: 0-"0 BOOTSTRAP", 1-"1 BOOT", 2-"2 PERIODIC", 3-"3 SCHEDULED", 4-"4 VALUE CHANGE", 5-"5 KICKED",

	6-"6 CONNECTION REQUEST", 7-"7 TRANSFER COMPLETE", 8-"8 DIAGNOSTICS COMPLETE", 9-"M Reboot"
port <port num>	It means to change tr069 listen port number.
cert_auth <on/off>	on: turn on certificate-based authentication. off: turn off certificate-based authentication.
only_standard_parm <on/off>	It means to turn on or off to exclude all the Vendor-Specific ("X_") parameters, and only send out standard parameters.
notify -n <on/off>	It means to set CPE notification settings. It means to / not to record the CPE notify log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -l <on/off>	It means to / not to record the web login log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -c <on/off>	It means to / not to record the web changed log on the Syslog. on: Record on the Syslog. off: Not record on the Syslog.
notify -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

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
```

```
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
..
> sys tr069 notify -B "1 30 60 100 100"
Please enable the CPE notify log.
> sys tr069 notify -n on
> sys tr069 notify -b on
set OK
> sys tr069 notify -B "1 30 60 100 100"
> sys tr069 notify -S
CPE Notify Settings:
 CPE Notify           Enable
 -Web Login           Disable
 -Web Changed         Disable
 -Bandwidth Utilization Enable

      Threshold(%)     Speed(Mb)
  WAN1 Med: 30 High: 60 TX:  100 RX:  100
  WAN2 Med:  0 High:  0 TX:    0 RX:    0
>
```

Telnet Command: sys alg

This command can enable or disable ALG (Application Layer Gateway) master switch.

Syntax

sys alg *<1/0>*

Syntax Description

Parameter	Description
1	It means to enable ALG master switch.
0	It means to disable ALG master switch.

Example

```
> sys alg -e 1
 Enable ALG

> sys alg
Usage: sys alg <command> <parameter>
 -e: enable ALG (0:disable, 1:enable)

Current ALG status
 -ALG Master Switch: Enabled
```

Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

Syntax

sys sip_alg *<command> <parameter>| ...*

Syntax Description

Parameter	Description
[<command> <parameter>| ..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-e <0/1>	0: Disable the function of SIP ALG. 1: Enable the function of SIP ALG.
-p <parameter>	It means to set the listening port for SIP ALG. <parameter> : Ranges from 1 to 65535.
-u <0/1>	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t <0/1>	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable

Example

```
> sys sip_alg -e 1
 Auto enable ALG Master Switch

 Enable SIP ALG

> sys sip_alg -p 65535
 Current listening port: 65535

> sys sip_alg ?
Usage: sys sip_alg <command> <parameter>
 -e: enable SIP ALG (0:disable, 1:enable)
 -p: set your listening port for SIP ALG
 -u: enable listen along UDP path (0:disable, 1:enable)
 -t: enable listen along TCP path (0:disable, 1:enable)

Current SIP ALG status
 -ALG Master Switch: Enabled
 -SIP ALG: Enabled
 -Listen along UDP path: Yes
 -Listen along TCP path: Yes
 -Listening Port: 65535
 -Max sipalg session num: 256
 -Remain sipalg session num: 256
```

Telnet Command: sys rtsp_alg

This command is used to configure settings (e.g., listen port) for ALG with the protocol of RTSP.

Syntax

sys rtsp_alg *[<command> <parameter>]*

Syntax Description

Parameter	Description
[<command> <parameter>|..]	The available commands with parameters are listed below. *[..]* means that you can type in several commands in one line.
-e <0/1>	0: Disable the function of RTSP ALG. 1: Enable the function of RTSP ALG.
-p <parameter>	It means to set the listening port for RTSP ALG. <parameter> : Ranges from 1 to 65535.
-u <0/1>	It means to enable or disable the listen along UDP path setting. 0: Disable 1: Enable
-t <0/1>	It means to enable or disable the listen along TCP path setting. 0: Disable 1: Enable
-v	It displays RTP and RTCP portmap information of RTSP ALG.

Example

```
> sys rtsp_alg -e 1
  Enable RTSP ALG

> sys rtsp_alg -p 375
 Current listening RTSP Port: 375

> 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*

Syntax Description

Parameter	Description
reset_regser	It means the license register server setting or register service in portal.
licera	It means to erase license setting.

licifno <AUTO/WAN#>	It means license and signature download interface setting.
licalias <index>	It means to specify an IP alias by entering the index number of the IP alias profile.
lic_trigger	It means to trigger the license.
licelog	It means to show the authentication log.
dev_chg	It means to change the device key.
dev_key	It means to show device key.

Example

```
> sys license licifno wan3
Download interface is set as "WAN3" 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 diag_log

This command is used for RD debug.

Syntax

sys diag_log *[status| enable| disable| flush| lineno [w] | level [x] | feature [on|off] [y]| log]*

Syntax Description

Parameter	Description
status	It means to show the status of diagnostic log.
enable	It means to enable the function of diag_log.
disable	It means to disenable the function of diag_log.
flush	It means the flush log buffer.
lineno [w]	It means the total lines for displaying message. w - Available value ranges from 100 to 50000.
level[x]	It determines the level of data displayed. x –Available value ranges from 0 to 12. The larger the number is, the detailed the data is displayed.
feature [on/off][y]	It is used to specify the function of the log. Supported features

	include SYS and DSL (Case-Insensitive). Default setting is "on" for "DSL".
voip_feature [on/off][vf_name]	It means VoIP feature. Type on to enable the feature or type off to disable the feature. vf_name: available settings include DRVTAPI, DRVVMMC, DRVMPS, DRVFXO, DRVHAL, PSMPHONE, PSMSUPP, PSM, FXO, PSMISDN, DTMFPSER, CALLERID (Case-Insensitive).
log	It means the dump log buffer.

Example

```
> sys diag_log status
 Status:
 diag_log is Enabled.
 lineno : 10000.
 level : 3.
 Enabled feature: SYS DSL
> sys diag_log log
0:00:02    [DSL] Current modem firmware: AnnexA_548006_544401
0:00:02    [DSL] Modem firmware feature: 5, ADSL_A, VDSL2
0:00:02    [DSL] xtseCfg=04 00 04 00 0c 01 00 07
0:00:02    [DSL] don't have last showtime mode!! set next mode to VDSL!!
0:00:02    [DSL] Status has changed: Stopped(0) -> FwWait(3)
0:00:02    [DSL] Status has changed: FwWait(3) -> Starting(1)
0:00:02    [DSL] Status has changed: Starting(1) -> Running(2)
0:00:02    [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:02    [DSL] Status was switched: Init(5) to Restart(10)
0:00:02    [DSL] Status was switched: Restart(10) to FirmwareRequest(1)
0:00:02    [DSL] Line state has changed: 00000000 -> 000000FF
0:00:02    [DSL] Entering VDSL2 mode
0:00:03    [DSL] modem code: [05-04-08-00-00-06]
0:00:05    [DSL] Status was switched: FirmwareRequest(1) to firmwareReady(3)
0:00:05    [DSL] Status was switched: firmwareReady(3) to Init(5)
0:00:05    [DSL] >> nXtseA=0d, nXtseB=00, nXtseV=07, nFwFeatures=5
0:00:05    [DSL] >> nHsToneGroupMode=0, nHsToneGroup=106, nToneSet=43,
nCamState
=2
0:00:05    [DSL] Line state has changed: 000000FF -> 00000100
0:00:05    [DSL] Line state has changed: 00000100 -> 00000200
0:00:05    [DSL] Status was switched: Init(5) to Train(6)
```

Telnet Command: sys arp_AutoReq

This command is used to enable / disable the function that Vigor router sends ARP request to the connected device(s) periodically.

Syntax

sys arp_AutoReq -d *<value>*

Syntax Description

Parameter	Description
-d <value>	Disable the function of ARP auto request. 0 – Enable 1 – Disable

Example

```
> sys arp_AutoReq -d 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 <ttl>	Set the TTL limit value in the DNS cache table <ttl>: 0(no limit) or an number greater than 5.
-c	Clear the DNS cache table.

Example

```
> sys dnsCacheTbl -t 50
% Set TTL limit: 50 seconds.
% When TTL larger than 50s , delete the DNS entry in the router's DNS cache
tabl
e.
> sys dnsCacheTbl -v
% TTL limit: 50 seconds
% When TTL larger than 50s , delete the DNS entry in the router's DNS cache
table.
>
```

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.
-l <1/0>	Enable (1) or disable (0) WLAN Log.
-r <1/0>	Enable (1) or disable (0) Router/DSL Information.
-p	Update the server IP address.
-W <1/0>	Set the mode for writing Syslog. 0: overwrite oldest logs; 1: stop logging.
-U <1/0>	Set the unit for the Syslog saved to a USB disk. 0:GB; 1:MB
-S <capacity>	Set the folder capacity for the syslog saved in the USB disk. 1 ~16(GB); 1 ~1024(MB)

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 Interface (Physical) Any/WAN1/WAN2/WAN... and etc.
-x <WAN IP Alias index>	Set WAN IP Alias. Index 1 is reserved and must set an interface first.
-i <SMTP Server IP>	Set IP Address for SMTP server.
-o <SMTP Server Port>	Set port number for SMTP server..
-a <Mail Address>	Set E-maiil address for alert mail reciver.
-r <Mail Address>	Set E-mail Address for mail return.
-s <0/1>	Enable/disable the function of Use SSL. 0 – Disable. 1 – Enable.
-h <0/1>	Enable/disable SMTP Authentication. 0 – Disable. 1 – Enable.
-u <Username>	Set username for SMTP Authentication.
-p <Password>	Set password for SMTP Authentication.

-l <type><0/1>	Enable / disable mail alert for different types. Number 0 ~ 6 represent different types. "0 <0/1>" : Enable/Disable Mail Alert of the DoS Attack. "1 <0/1>" : Enable/Disable Mail Alert of the APPE. "2 <0/1>" : nable/Disable Mail Alert of the VPN Log. "6 <0/1>" : Enable/Disable Mail Alert of the Reboot Debug Log. In which, 0 – Disable. 1 – Enable.
-f	Reset Mail Alert setting to factory default.
-v	Show current Mail Alert setting.
-R <0/1>	Set Mail Alert Reboot debug log mode. 0: Limited Mode 1: Unlimited Mode.

Example

```
> sys mailalert -e 1
Set Enable Mail Alert.
> sys mailalert -v
------ Current setting for Mail Alert ------
Mail Alert: Enable
SMTP Server IP Address: 0.0.0.0
SMTP Server Port: 25
Alert Mail Reciver E-maiil Address:
Mail Return E-mail Address:
Use SSL: Disable
SMTP Authentication: Disable
Username for SMTP Authentication:
Password for SMTP Authentication:
Mail Alert for DoS Attack: Enable.
Mail Alert for APPE: Enable.
Mail Alert for VPN Log: Enable.
Mail Alert for APPE Signature: Disable.
Mail Alert for Reboot Debug Log: Disable, Mode: Limited.
-------------------------------------------
```

Telnet Command: sys time

This command is used to configure system time and date.

Syntax

sys time server *<domain>*

sys time inquire

sys time show

sys time zone *<index>*

Syntax Description

Parameter	Description
domain	Enter the domain name of the time server. The maximum length is 39 bytes.
index	Different number means different time zone. 1 - GMT-12:00 Eniwetok, Kwajalein

	2 - GMT-11:00 Midway Island, Samoa 3 - GMT-10:00 Hawaii 4 - GMT-09:00 Alaska 5 - GMT-08:00 Pacific Time (US & Canada) 6 - GMT-08:00 Tijuana 7 - GMT-07:00 Mountain Time (US & Canada) 8 - GMT-07:00 Arizona 9 - GMT-06:00 Central Time (US & Canada) 10 - GMT-06:00 Saskatchewan 11 - GMT-06:00 Mexico City, Tegucigalpa 12 - GMT-05:00 Eastern Time (US & Canada) 13 - GMT-05:00 Indiana (East) 14 - GMT-05:00 Bogota, Lima, Quito 15 - GMT-04:00 Atlantic Time (Canada) 16 - GMT-04:00 Caracas, La Paz 17 - GMT-04:00 Santiago 18 - GMT-03:30 Newfoundland 19 - GMT-03:00 Brasilia 20 - GMT-03:00 Buenos Aires, Georgetown 21 - GMT-02:00 Mid-Atlantic 22 - GMT-01:00 Azores, Cape Verde Is. 23 - GMT Greenwich Mean Time : Dublin 24 - GMT Edinburgh, Lisbon, London 25 - GMT Casablanca, Monrovia 26 - GMT+01:00 Belgrade, Bratislava 27 - GMT+01:00 Budapest, Ljubljana, Prague 28 - GMT+01:00 Sarajevo, Skopje, Sofija 29 - GMT+01:00 Warsaw, Zagreb 30 - GMT+01:00 Brussels, Copenhagen 31 - GMT+01:00 Madrid, Paris, Vilnius 32 - GMT+01:00 Amsterdam, Berlin, Bern 33 - GMT+01:00 Rome, Stockholm, Vienna 34 - GMT+02:00 Bucharest 35 - GMT+02:00 Cairo 36 - GMT+02:00 Helsinki, Riga, Tallinn 37 - GMT+02:00 Athens, Istanbul, Minsk 38 - GMT+02:00 Jerusalem 39 - GMT+02:00 Harare, Pretoria 40 - GMT+03:00 Volgograd 41 - GMT+03:00 Baghdad, Kuwait, Riyadh 42 - GMT+03:00 Nairobi 43 - GMT+03:00 Moscow, St. Petersburg 44 - GMT+03:30 Tehran 45 - GMT+04:00 Abu Dhabi, Muscat 46 - GMT+04:00 Baku, Tbilisi 47 - GMT+04:30 Kabul 48 - GMT+05:00 Ekaterinburg 49 - GMT+05:00 Islamabad, Karachi, Tashkent 50 - GMT+05:30 Bombay, Calcutta 51 - GMT+05:30 Madras, New Delhi 52 - GMT+06:00 Astana, Almaty, Dhaka 53 - GMT+06:00 Colombo 54 - GMT+07:00 Bangkok, Hanoi, Jakarta 55 - GMT+08:00 Beijing, Chongqing 56 - GMT+08:00 Hong Kong, Urumqi 57 - GMT+08:00 Singapore 58 - GMT+08:00 Taipei 59 - GMT+08:00 Perth 60 - GMT+09:00 Seoul 61 - GMT+09:00 Osaka, Sapporo, Tokyo 62 - GMT+09:00 Yakutsk 63 - GMT+09:30 Darwin 64 - GMT+09:30 Adelaide 65 - GMT+10:00 Canberra, Melbourne, Sydney 66 - GMT+10:00 Brisbane 67 - GMT+10:00 Hobart 68 - GMT+10:00 Vladivostok

	69 - GMT+10:00 Guam, Port Moresby 70 - GMT+11:00 Magadan, Solomon Is. 71 - GMT+11:00 New Caledonia 72 - GMT+12:00 Fiji, Kamchatka, Marshall Is. 73 - GMT+12:00 Auckland, Wellington

Example

```
> sys time zone 8
  Set Time Zone OK

> sys time show
  ***************  System Time  ***************
  Current System Time: [2000 Jan 01 Sat 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: testmail

This command is used to display current settings for sending test mail.

Example

```
> testmail
Send out test mail
 Mail Alert:[Disable]
 Interface :Any
 WAN_Alias index:[0]
 SMTP_Server:[0.0.0.0]
 SMTP_Port:[25]
 Mail to:[]
 Return-Path:[]
 Connection Security:[Plaintext]
```

Telnet Command: upnp off

This command can close UPnP function.

Example

```
>upnp off
UPNP say bye-bye
```

Telnet Command: upnp on

This command can enable UPnP function.

Example

```
>upnp on
UPNP start.
```

Telnet Command: upnp nat

This command can display IGD NAT status.

Example

```
> upnp nat ?
******************  IGD NAT Status  ****************

((0))
InternalClient >>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
Vigor> 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

```
Vigor> upnp tmpvs
******************  Temp virtual server status  ****************

((0))
real_addr  >>192.168.1.10<<, pseudo_addr >>172.16.3.229<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>TCP<<
time >>0<<

((1))
real_addr  >>0.0.0.0<<, pseudo_addr >>0.0.0.0<<
real_port >>0<<, pseudo_port >>0<<
hit_portmap_index >>0<<
The protocol >>0<<
time >>0<<
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

Telnet Command: upnp wan

This command is used to specify WAN interface to apply UPnP.

Syntax

upnp wan *<n>*

Syntax Description

Parameter	Description
n	It means to specify WAN interface to apply UPnP. n=0 ~3, it means to auto-select WAN interface. n=1, WAN1 n=2, WAN2 .....

Example

```
> upnp wan 1
use wan1 now.
```

Telnet Command: usb list

This command is use to display the information about the brand name and model name of the USB modems which are supported by Vigor router.

Example

```
> usb list ?
Brand      Module             Standard
-------------------------        --------
Aiko         Aiko 83D             3.5G              Y
```

```
Alcatel      Alcatel L100V          LTE              Y
Alcatel      Alcatel W100           LTE              Y
BandRich     Bandluxe C170         3.5G              Y
BandRich     Bandluxe C270         3.5G              Y
BandRich     Bandluxe C321         3.5G              Y
BandRich     Bandluxe C330         3.5G              Y
BandRich     Bandluxe C502         3.5G              Y
D-Link       D_LINK DWM221 B1       LTE              M
D-Link       D_LINK DWM222          LTE              Y
Huawei       Huawei E169u          3.5G              Y
Huawei       Huawei E173u          3.5G              Y
Huawei       Huawei E220           3.5G              Y
Huawei       Huawei E303D          3.5G              Y
Huawei       Huawei E3131          3.5G              Y
Huawei       Huawei E3276s          LTE              Y
Huawei       Huawei E3372s-153       LTE             Y
Huawei       Huawei E392           LTE               Y
Huawei       Huawei E398           LTE               Y
Huawei       Huawei K3770          3.5G              M
Huawei       Huawei K3772          3.5G              M
Huawei       Huawei K4605          3.5G              Y
- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -
```

Telnet Command: usb user

This command is used to set profiles for FTP/SMB users.

Syntax Description

usb user add *<Index> <Username> <Password> <Permission> <Home path>*

usb user rm *<Index>*

usb user enable *<Index>*

usb user disable *<Index>*

usb user list

Syntax Description

Parameter	Description
add <Index> <Username> <Password> <Permission> <Home path>	Add a new user profile. <Index>: It means the index number of the user profile. There are 16 profiles allowed to be configured. So the range of such option is 1 ~ 16. <Username>: Enter a text (maximum 131 characters) as the username for the user profile. <Password>: Enter a text (maximum 131 characters) as the password for the user profile. <Permission>: Specify the action (RWDLCR) permitted. If one of the actions is not allowed, simple type "-" instead. R – Read File. W – Write File. D – Delete File. L – List directory. C – Create directory. R – Remove selected directory. <Home path>: Set the path (maximum 159 characters) for the USB

	user profile.
rm <Index>	Delete an existed user profile. <Index>: It means the index number of the user profile.
enable <Index>	Enable a user profile. <Index>: It means the index number of the user profile.
disable <Index>	Disable a user profile. <Index>: It means the index number of the user profile.
list	Display all of the user profile.

Example

```
> usb user add 1 root 1234 R-DLCR /usr
>
```

Telnet Command: usb temp

This command is to configure USB temperature.

Syntax Description

usb temp set *<-c| -f| -a| -b| -m| -u| -l| -r>*
usb temp show
usb temp all_data

Syntax Description

Parameter	Description
set -c	Set the temperature unit (Celsius).
set -f	Set the temperature unit (Fahrenheit).
set -a	Set the temperature sensor by using a probe or the built-in sensor automatically. The probe will be detected and used first, and fall back to the built-in sensor if the probe is not detected.
set -b	Set to use the built-in sensor.
set -m	Enable or disable the Alarm Setting. 1: Enable 0: Disable
set -u <value>	Set the upper temperature limit. <value>: Enter a value, e.g., 30.35.
set -l <value>	Set the lower temperature limit. <value>: Enter a value, e.g., 10.35.
set -r	Shows the setting of temperature unit and sensor type.
show	Displays current temperature.
all_data	Displays all temperature data.

Example

```
> usb temp set -r
Show setting:temp set -r

Alarm Settings: 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
-l <LAN_idx>	LAN_idx – Indicate the LAN interface. 1 – LAN1 2 – LAN2

	3 – LAN3 4 – LAN4
-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 1 -l 1 -e 1
[WAN1] IPv4 bridge is enable. Set subnet[LAN1]
```

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: Running
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><p1/p2/p3/s1/s2/s3/s4>*

Syntax Description

Parameter	Description
id	It means the group 0 to 7 for VLAN.
set	It indicates each port can join more than one VLAN group.
set_ex	It indicates each port can join one VLAN group at one time.
p1/p2/p3	It indicates LAN port 1 to LAN port 4. To group LAN1, LAN2, LAN3 and/or LAN4 under one VLAN group, please Enter the port number(s) you want.
s1/s2/s3/s4	It is only available for WALN models.

Example

```
> vlan group 3 set p1 s3 s4
 VLAN   p1   p2   p3   p4   s1   s2   s3   s4
 ---------------------------------------------
   3    V                        V    V
>
```

Telnet Command: vlan off

This command allows you to disable VLAN function.

Syntax

vlan off

Example

```
> vlan off
 VLAN is Disable!
 Force subnet LAN2/3/4 to be disabled!!
```

Telnet Command: vlan on

This command allows you to enable VLAN function.

Syntax

vlan on

Example

```
> vlan on
 VLAN is Enable!
```

Telnet Command: vlan pri

This command is used to define the priority for each VLAN profile setting.

Syntax

vlan pri *n pri_no*

Syntax Description

Parameter	Description
n	It means VLAN ID number. n=VLAN ID number (from 0 to 7).
pri_no	It means the priority of VLAN profile. pri_no=0 ~7 (from none to highest priority).

Example

```
> vlan pri 1 2
 VLAN1: Priority=2
```

Telnet Command: vlan restart

This command can make VLAN settings restarted with newest configuration.

Syntax

vlan restart

Example

```
> vlan restart ?
 VLAN restarts!!!
```

Telnet Command: vlan status

This command display current status for VLAN.

Syntax

vlan status

Example

```
> vlan status
VLAN  is Enable :
```

```
-----------------------------------------------------
VLAN Enable VID  Pri   p1 p2 p3 s1 s2 s3 s4  subnet
-----------------------------------------------------
 0    OFF    0   0                              1:LAN1
 1    OFF    0   2                              1:LAN1
 2    OFF    0   0                              1:LAN1
 3    OFF    0   0    V                 V  V    1:LAN1
 4    OFF    0   0                              1:LAN1
 5    OFF    0   0                              1:LAN1
 6    OFF    0   0                              1:LAN1
 7    OFF    0   0                              1:LAN1
-----------------------------------------------------
 Note: they are only untag for s1/s2/s3/s4, but they can join tag vlan with
lan ports.
 Permit untagged device in P1 to access router: ON.
```

Telnet Command: vlan subnet

This command is used to configure the LAN interface used by the VLAN group.

Syntax

vlan subnet group_id *<1/2/3/4>*

Syntax Description

Parameter	Description
1/2/3/4	It means interfaces, LAN1 ~ LAN4.

Example

```
> vlan subnet group_id 2
% Vlan Group-0 using LAN2      !

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

Telnet Command: vlan submode

This command changes the VLAN encapsulation mechanisms in the LAN driver.

Syntax

vlan submode *<on|off|status>*

Syntax Description

Parameter	Description
on	It means to enable the promiscuous mode.
off	It means to enable the normal mode.
status	It means to display if submode is normal mode or promiscuous mode.

Example

```
> vlan submode status
% vlan subnet mode : normal mode
```

```
> vlan submode on
% vlan subnet mode modified to promiscuous mode.
> vlan submode status
% vlan subnet mode : promiscuous mode
```

Telnet Command: vlan tagged

This command is used to enable or disable the incoming of untagged packets.

Syntax

vlan tagged *<n> <on/off>*

vlan tagged *<unlimited> <on/off>*

vlan tagged *<p1_untag> <on/off>*

Syntax Description

Parameter	Description
<n>	It means VLAN channel. The ranage is from 0 to 7.
<on/off>	It means to enable/disable the tagged VLAN.
<unlimited> <on/off>	unlimited on: It allows the incoming of untagged packets even all VLAN are tagged. unlimited off: It does not allows the incoming of untagged packets.
<p1_untag> <on/off>	P1_untag on: It allows the incoming of untagged packets form LAN port 1. P1_untag off: It does not allow the incoming of untagged packets from LAN port 1.

Example

```
> vlan tagged unlimited on
 unlimited mode is ON
```

Telnet Command: vlan vid

This command is used to configure VID number for each VLAN channel.

Syntax

vlan vid *<n> <vid_no>*

Syntax Description

Parameter	Description
<n>	It means VLAN channel. The ranage is from 0 to 7.
<vid_no>	It means the value of VLAN ID. 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
show	It means to show the scope of VLAN ID used internally.
n	It means the value to be set as VLAN ID. The range is from 0 to 4018.

Example

```
> vlan sysvid 100
 You have set system VLAN ID to range: 100 ~ 177,
 We recommend that you reboot the system now.

> vlan sysvid 200
 You have set system VLAN ID to range: 200 ~ 263,
 We recommend that you reboot the system now.
> vlan sysvid show
 The system VLAN ID is in range: 200 ~ 263
```

Telnet Command: vpn l2lset

This command allows users to set advanced parameters for LAN to LAN function.

Syntax

vpn l2lset *<list index>* **peerid** *<peerid>*
vpn l2lset *<list index>* **localid** *<localid>*
vpn l2lset *<list index>* **main** *<auto/proposal index>*
vpn l2lset *<list index>* **aggressive** *<g1/g2>*
vpn l2lset *<list index>* **pfs** *<on/off>*
vpn l2lset *<list index>* **phase1** *<lifetime>*
vpn l2lset *<list index>* **phase2** *<lifetime>*
vpn l2lset *<list index>* **x509localid** *<0/1>*

Syntax Description

Parameter	Description
<list index>	It means the index number of L2L (LAN to LAN) profile.
peerid <peerid>	It means the peer identity for aggressive mode.
localid <localid>	It means the local identity for aggressive mode.
main <auto/proposal index>	It means to choose proposal for main mode. <auto>: Choose default proposals. <proposal index>: choose specified proposal.
aggressive <g1/g2>	It means the chosen DH group for aggressive mode.

pfs <on/off>	It means "perfect forward secrete". <on/off>: Turn on or off the PFS function.
phase1 <lifetime> / *phase2 <lifetime>*	It means phase 1 or 2 of IKE. <lifetime>: Set the lifetime value (in second) for phase 1 and phase 2.
x509localid <0/1>	It means to enable (1) or disable (0) the X509 local ID.

Example

```
> vpn l2lset 1 peerid 10226
>
```

Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

Syntax

vpn l2lDrop *l2lname <name>*
vpn l2lDrop *l2lidx <idx>*
vpn l2lDrop *h2lname <name>*
vpn l2lDrop *h2idx <idx>*
vpn l2lDrop *<ifno>*
vpn l2lDrop

Syntax Description

Parameter	Description
l2lname <name>	It means to drop VPN connection by specifying the name of the LAN to LAN profile.
l2lidx <idx>	It means to drop VPN connection by specifying the index number of LAN to LAN profile.
h2lname <name>	It means to drop VPN connection by specifying the name of the remote dial-in user profile.
h2idx <idx>	It means to drop VPN connection by specifying the index number of the remote dial-in user profile.
<ifno>	It means to drop VPN connection by using VPN ifno.
l2lDrop	It means to drop all VPN connections.

Example

```
> vpn l2lDrop
 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 32).
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** *<0~9999>*
vpn dinset *<list index>* **dintype** *<Type> <on/off>*
vpn dinset *<list index>* **subnet** *<0~4>*
vpn dinset *<list index>* **assignip** *<on/off>*
vpn dinset *<list index>* **srnode** *<on/off>*
vpn dinset *<list index>* **remoteip** *<Remote_Client_IP_Address>*
vpn dinset *<list index>* **peer** *<Peer_ID>*
vpn dinset *<list index>* **naming** *<pass/block>*
vpn dinset *<list index>* **multicastvpn** *<pass/block>*
vpn dinset *<list index>* **prekey** *<on/off>*
vpn dinset *<list index>* **assignkey** *<Pre_Shared_Key>*
vpn dinset *<list index>* **digsig** *<on/off>*
vpn dinset *<list index>* **ipsec** *<Method> <on/off>*
vpn dinset *<list index>* **localid** *<Local_ID>*

Syntax Description

Parameter	Description
<list index>	It means the index number of the profile.
<list index> <on/off>	It means to enable or disable the profile. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<list index> motp <on/off>	It means to enable or disable the authentication with mOTP function. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
<list index> pin_secret <pin> <secret>	It means to set PIN code with secret. <list index> - Enter the index number of the VPN profile. <pin> - Type the code for authentication (e.g, 1234). <secret> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6)

<list index> timeout <0~9999>	It means to set idle timeout. The default is 300 (seconds). <list index> - Enter the index number of the VPN profile. <0~9999> - Enter a value.
<list index> dintype <Type> <on/off>	It means to enable/disable the allowed dial-in type. <list index> - Enter the index number of the VPN profile. <Type> - 0 to 3. In which, 0 means PPTP; 1 means IPsec Tunnel; 2 means L2TP with IPsec Policy; 3 means SSL Tunnel. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> subnet <0~4>	It means to set the LAN subnet for the selected VPN profile. <list index> - Enter the index number of the VPN profile. <0~4> - Enter a number to specify the LAN subnet. In which, 0 means LAN1 1 means LAN2 2 means LAN3 3 means LAN4 4 means DMZ
vpn dinset <list index> assignip <on/off>	It means to enable or disable the function of assigning the static IP address. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> srnode <on/off>	It means to enable or disable the function of specifying the remote node. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> remoteip <Remote_Client_IP_Address>	It means to enable or disable the function of assigning remote client IP. <list index> - Enter the index number of the VPN profile. <Remote_Client_IP_Address> - Set the IP address of the remote client.
vpn dinset <list index> peer <Peer_ID>	It means to assign the peer ID. <list index> - Enter the index number of the VPN profile. <Peer_ID> - Enter the string of the peer ID.
vpn dinset <list index> naming <pass/block>	It means to set the Netbiod Naming Packet for the VPN profile. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
vpn dinset <list index> multicastvpn <pass/block>	It means to set the multicast via VPN for IGMP, IP-CAM, DHCP relay, and etc. <list index> - Enter the index number of the VPN profile. <pass/block> - Let the packet pass or block the packet.
vpn dinset <list index> prekey <on/off>	It means to enable/disable the Pre-Shared Key setting for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.
vpn dinset <list index> assignkey <Pre_Shared_Key>	It means to set the Pre-Shared Key for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <Pre_Shared_Key> - Enter a string as PSK.
vpn dinset <list index> digsig <on/off>	It means to enable/disable the digital signature (X.509) for IKE Authentication Method. <list index> - Enter the index number of the VPN profile. <on/off> - on: Enable; off: Disable.

vpn dinset <list index> ipsec <Method> <on/off>	It means to enable / disable and set the protocol for IPsec security method. <list index> - Enter the index number of the VPN profile. <Method> - Enter a number (0 to 3) to specify the protocol. 0 means Medium(AH) High(ESP), 1 means DES 2 means 3DES 3 means AES <on/off> - on: Enable; off: Disable.
vpn dinset <list index> localid <Local_ID>	It means to set local ID (optional) for IPsec Security Method. <list index> - Enter the index number of the VPN profile. <local_ID> - Enter the string of local ID.

Example

```
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Deactive

Mobile OTP: Disabled

Password:

Idle Timeout: 300 sec

> vpn dinset 1 on
% set profile active

> vpn dinset 1 motp on
% Enable Mobile OTP mode!>
> vpn dinset 1 pin_secret 1234 e759bb6f0e94c7ab4fe6
> vpn dinset 1

Dial-in profile index 1

Profile Name: ???
Status: Active

Mobile OTP: Enabled

PIN: 1234

Secret: e759bb6f0e94c7ab4fe6

Idle Timeout: 300 sec
```

Telnet Command: vpn subnet

This command allows users to specify a subnet selection for the specified remote dial-in VPN profile.

Syntax

vpn subnet *<index> <1/2/3/4>*

Syntax Description

Parameter	Description
<index>	It means the index number of the VPN profile.
<1/2/3/4>	1 – it means LAN1 2 – it means LAN2. 3 – it means LAN3 4 – it means LAN4.

Example

```
> vpn subnet 1 2
>
```

Telnet Command: vpn setup

This command allows users to setup VPN for different types.

Syntax

Command of PPTP Dial-Out

vpn setup *<index> <name>* **pptp_out** *<ip> <usr> <pwd> <nip> <nmask>*

Command of IPSec Dial-Out

vpn setup *<index> <name>* **ipsec_out** *<ip> <key> <nip> <nmask>*

Command of L2Tp Dial-Out

vpn setup *<index> <name>* **l2tp_out** *<ip> <usr> <pwd> <nip> <nmask>*

Command of Dial-In

vpn setup *<index> <name>* **dialin** *<ip> <usr> <pwd> <key> <nip> <nmask>*

Syntax Description

Parameter	Description
For PPTP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the PPTP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 pptp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For IPsec Dial-Out	

<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 ipsec_out 1.2.3.4 1234 192.168.1.0 255.255.255.0
For L2TP Dial-Out	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address to dial to.
<usr> <pwd>	It means the user and the password required for the L2TP connection.
<nip> <nmask>	It means the remote network IP and the mask. e.g.,, vpn setup 1 name1 l2tp_out 1.2.3.4 vigor 1234 192.168.1.0 255.255.255.0
For Dial-In	
<index>	It means the index number of the profile.
<name>	It means the name of the profile.
<ip>	It means the IP address allowed to dial in.
<usr> <pwd>	It means the user and the password required for the PPTP/ L2TP connection.
<key>	It means the value of IPsec Pre-Shared Key.
<nip> <nmask>	It means the remote network IP and the mask. e.g., vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0

Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server :  ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile (including Common Settings, Dial-Out Settings, Dial-In Settings, and TCP/IP Network Settings)

Syntax

vpn option *<index> <cmd1>=<param1> [<cmd2>=<para2> | ...]*

Syntax Description

Parameter	Description
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
For Common Settings	
<index>	It means the index number of the profile.
pname	It means the name of the profile.
ena	It means to enable or disable the profile. on – Enable off - Disable
thr	It means the way that VPN connection passes through. Available settings are wlf, wlo, w2f, and w2o. w1f – WAN1 First. w1o – WAN1 Only. w2f – WAN2 First. w2o – WAN2 Only.
nnpkt	It means the NetBios Naming Packet. on – Enable the function to pass the packet. off – Disable the function to block the packet.
dir	It means the call direction. Available settings are b, o and i. b – Both o – Dial-Out i – Dial-In.
idle=[value]	It means Always on and Idle Time out. Available values include: -1 – it means always on for dial-out. 0 – it means always on for dial-in. Other numbers (e.g., idle=200, idle=300, idle=500) mean the router will be idle after the interval (seconds) configured here.
palive	It means to enable PING to keep alive. -1 – disable the function. 1,2,3,4 – Enable the function and PING IP 1.2.3.4 to keep alive.
For Dial-Out Settings	
ctype	It means "Type of Server I am calling". "ctype=t" means PPTP. "ctype=s" means IPSec. "ctype=l" means L2TP(IPSec Policy None). "ctype=l1" means L2TP(IPSec Policy Nice to Have). "ctype=l2" means L2TP(IPSec Policy Must).
dialto	It means Server IP/Host Name for VPN. (such as draytek.com or

	123.45.67.89).
ltype	It means Link Type. "ltype=0" means "Disable". "ltype=1" means "64kbps". "ltype=2" means "128kbps". "ltype=3" means "BOD".
oname	It means Dial-Out Username. "oname=admin" means to set Username = admin.
opwd	It means Dial-Out Password "opwd=1234" means to set Password = 1234.
pauth	It means PPP Authentication. "pauth=pc" means to set PPP Authentication = PAP&CHAP. "pauth=p" means to set PPP Authentication = PAP Only
ovj	It means VJ Compression. "ovj=on/off" means to enable/disable VJ Compression.
okey	It means IKE Pre-Shared Key. "okey=abcd" means to set IKE Pre-Shared Key = abcd.
ometh	It means IPSec Security Method. "ometh=ah/" means AH. "ometh=espd/espda/" means ESP DES without/with Authentication. "ometh=esp3/esp3a/" means ESP 3DES without/with Authentication. "ometh=espa/espaa" means ESP AES without/with Authentication.
sch	It means Index(1-15) in Schedule Setup. sch=1,3,5,7 Set schedule 1->3->5->7
rcallb	It means Require Remote to Callback. "rcallb=on/off" means to enable/disable Set Require Remote to Callback.
ikeid	It means IKE Local ID. "ikeid=vigor" means Set Local ID = vigor.
For Dial-In Settings	
itype	It means Allowed Dial-In Type. Available settings include: "itype=t" means PPTP. "itype=s" means IPSec. "itype=L1" means L2TP (None). "itype=L1" means L2TP(Nice to Have). "itype=l2" means L2TP(Must).
peer	It means specify Peer VPN Server IP for Remote VPN Gateway. Type "203.12.23.48" means to allow VPN dial-in with IP address of 203.12.23.48. Type "off" means any remote IP is allowed to dial in.
peerid	It means the peer ID for Remote VPN Gateway. Type "draytek" means the word is used as local ID.
iname	It means Dial-in Username. "iname=admin" means to set username as "admin".
ipwd	It means Dial-in Password. "ipwd=1234" means to set password as "1234".
ivj	It means VJ Compression.

	"ivj=on/off" means to enable / disable VJ Compression.
ikey	It means IKE Pre-Shared Key. "ikey=abcd" means to set IKE Pre-Shared Key = abcd.
imeth	It means IPSec Security Method "imeth=h" means "Allow AH". "imeth=d" means "Allow DES". "imeth=3" means "Allow 3DES". "imeth=a" means "Allow AES.
For TCP/IP Settings	
mywip	It means My WAN IP. "mywip=1.2.3.4" means to set My WAN IP as "1.2.3.4".
rgip	It means Remote Gateway IP. "rgip=1.2.3.4" means to set Remote Gateway IP as "1.2.3.4".
rnip	It means Remote Network IP. "rnip=1.2.3.0" means to set Remote Network IP as "1.2.3.0".
rnmask	It means Remote Network Mask. "rnmask=255.255.255.0" means to set Remote Network Mask as "255.255.255.0".
rip	It means RIP Direction. "rip=d" means to set RIP Direction as "Disable". "rip=t" means to set RIP Direction as "TX". "rip=r" means to set RIP Direction as "RX". "rip=b" means to set RIP Direction as "Both".
mode	It means the option of "From first subnet to remote network, you have to do". "mode=r" means to set Route mode. "mode=n" means to set NAT mode.
droute	It means to Change default route to this VPN tunnel (Only single WAN supports this). droute=on/off means to enable/disable the function.

Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
> vpn option l3show
% Out of list index
```

Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

Syntax

vpn mroute *<index>* **list**

vpn mroute *<index>* **add** *<network ip>/<mask>*

vpn mroute *<index>* **del** *<network ip>/<mask>*

Syntax Description

Parameter	Description
list	It means to display all of the route settings.
add	It means to add a new route.
del	It means to delete specified route.
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32
<network ip>/<mask>	Enter the IP address with the network mask address.

Example

```
> vpn mroute 1 add 192.168.5.0/24
% 192.168.5.0/24
% Add new route 192.168.5.0/24 to profile 1
```

Telnet Command: vpn list

This command allows users to view LAN to LAN VPN profiles.

Syntax

vpn list *<index>* **all**

vpn list *<index>* **com**

vpn list*<index>* **out**

vpn list *<index>* **in**

vpn list*<index>* **net**

Syntax Description

Parameter	Description
all	It means to list configuration of the specified profile.
com	It means to list common settings of the specified profile.
out	It means to list dial-out settings of the specified profile.
in	It means to list dial-in settings of the specified profile.
net	It means to list Network Settings of the specified profile.
<index>	It means the index number of the profile. Available index numbers: 1 ~ 32

Example

```
> vpn list 32 all
% Common Settings

% Profile Name            : ???
% Profile Status          : Disable
% 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/SSLVPN* service.

Syntax

vpn remote *<PPTP/IPsec/L2TP/SSLVPN> <on/off>*

Syntax Description

Parameter	Description
<PPTP/IPsec/L2TP/SSLVPN>	There are four types to be selected.
on/off	on – enable VPN remote setting. off – disable VPN remote setting.

Example

```
> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!
```

Telnet Command: vpn trunk

This command allows users to configure VPN Backup, GRE over IPsec, and Binding tunnel policy.

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 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 <ON/OFF> *lb more_syslog <ON/OFF>* *bind more_syslog <ON/OFF>*	These commands are used for RD debug.
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.
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 show_usable
% Available Lan to Lan Dial-out profile list :
  <Index>   < Name >   <Connection-Type>   <VPN Server IP - Private Network >
     1      name1       PPTP      1.2.3.4 - 192.168.1.0
     2      market      PPTP      5.6.7.8 - 192.168.1.31
==========================================================================
>
```

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 *<H2l/L2l> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2l/L2l>	H2l means Remote Access User Accounts. L2l means LAN-to-LAN Profile. Specify which one will be applied by NetBios.
<index>	The index number of the profile.
<Block/Pass>	**Pass** – Have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, set it block data transmission of Netbios Naming Packet inside the tunnel.

Example

```
> vpn NetBios set H2l 1 Pass
% Remote Dial In Profile Index [1] :
% NetBios Block/Pass: [PASS]
```

Telnet Command: vpn mss

This command allows users to configure the maximum segment size (MSS) for different TCP types.

Syntax

vpn mss show

vpn mss default

vpn mss set *<connection type> <TCP maximum segment size range>*

Syntax Description

Parameter	Description
show	It means to display current setting status.
default	TCP maximum segment size for all the VPN connection will be set as 1360 bytes.
set	Use it to specify the connection type and value of MSS.
<connection type>	1~4 represent various type. 1 – PPTP 2 – L2TP 3 – IPSec 4 – L2TP over IPsec 5 - GRE ove r IPsec 6 - SSL Tunnel
<TCP maximum segment size	Each type has different segment size range.

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

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 *<H2I/L2I> <index> <Block/Pass>*

Syntax Description

Parameter	Description
<H2I/L2I>	H2I means Host to LAN (Remote Access User Accounts). L2I means LAN-to-LAN Profile.
<index>	The index number of the profile.

<Block/Pass>	Set Block/Pass the Multicast Packets. The default is Block.

Example

```
> vpn Multicast set L2l 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

Syntax

vpn pass2nd *<on/off>*

Syntax Description

Parameter	Description
on/off	on –the packets can pass through NAT. off –the packets cannot pass through NAT.

Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

Syntax

vpn pass2nat *<on/off>*

Syntax Description

Parameter	Description
on/off	on –the packets can pass through NAT. off –the packets cannot pass through NAT.

Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

Telnet Command: vpn passAPM

This command allows packets from APM to pass the VPN tunnel or not.

Syntax

vpn passAPM *on*

vpn passAPM *off*

Example

```
> vpn passAPM on
% APM broadcast is allowed to pass VPN tunnel!
```

Telnet Command: vpn sameSubnet

This command allows users to build VPN between clients via virtual subnet.

Syntax

vpn sameSubnet *-i <value>*
vpn sameSubnet *–E <0/1>*
vpn sameSubnet *–e <value>*
vpn sameSubnet *-I <Virtual Subnet>*
vpn sameSubnet *-o <add/del>*
vpn sameSubnet *-v*
vpn sameSubnet *-m*

Syntax Description

Parameter	Description
-i <value>	Specify the index number of VPN profile.
–E <0/1>	Enable or disable the IPsec with the same subnet. 1 – enable. 0 – disable.
–e <value>	Translate specified LAN to virtual subnet. 1 – LAN1 2 – LAN2 3 – LAN3 **...**
-I <Virtual Subnet>	Set the virtual subnet (e.g., 172.16.3.250).
-v	Display current status of virtual subnet.
-m <1/2>	Set the Translated Type. *<1/2>* - 1 for Whole Subnet, 2 for Specific IP.

Example

```
> vpn sameSubnet  -i 1 -E 1 -e 1 -I 10.10.10.0 -o add
 Enable IPsec with Same Subnet !!

 Add entry Succcess!!
> vpn sameSubnet -v
IPsec with the same subnet:
VPN profile 1 enable,
 % translated LAN1 to Virtual subnet: 10.10.10.0
```

Telnet Command: vpn ovpn

This command allows users to build VPN between clients via 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 ovpn *hmacmode <0/1/2>*

Syntax Description

Parameter	Description
mode <0/1>	Enable or disable the OpenVPN function. 1 – enable. 0 – disable.
show	Displays current OpenVPN settings.
udp_mode <0/1>	Enable or disable the UDP mode. 1 – enable. 0 – disable.
tcp_mode <0/1>	Enable or disable the TCP mode. 1 – enable. 0 – disable.
udp_port <1-65535>	Enter a port number (1-65535) for UDP mode.
tcp_port <1-65535>	Enter a port number (1-65535) for TCP mode.
replay <0/1>	Enable or disable the replay option. 1 – enable. 0 – disable.
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 mode 1
Enable openvpn
> 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: AES256
HMAC Algorithm: SHA256
Certificate uid: 65535
Trust CA uid: 13
```

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 / wan mtu2

This command allows users to adjust the size of MTU for WAN1/ WAN2.

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 - WAN1 2 - WAN2
<dns_select>	Specify primary and / or secondary DNS server. pri – It means primary DNS server. sec – It means secondary DNS server.
<ipv4_addr>	Enter the IP address of DNS server.

Example

```
> wan dns 1 pri 168.95.1.1
% Set WAN1 primary DNS done.
% Now: 168.95.1.1
```

Telnet Command: wan DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

Syntax

wan DF_check *<on/off>*

Syntax Description

Parameter	Description
on/off	It means to enable or disable DF.

Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

Telnet Command: wan disable

This command allows you to disable WAN connection.

Example

```
> wan disable WAN
```

```
%WAN disabled.
```

Telnet Command: wan enable

This command allows you to disable wan connection.

Example

```
> wan enable WAN
%WAN1 enabled.
```

Telnet Command: wan wan2lan

This command allows you to switch WAN interface into LAN interface. When WAN2 is disabled or WAN2 is set as wireless physical mode, Ethernet port can be configured as LAN

Syntax

wan wan2lan *<wan> <on/off/status>*

Syntax Description

Parameter	Description
<wan> <on/off/status>	<wan> - Enter 1 (WAN1) or 2 (WAN2). <on/off/status> - Enable (on) or disable (off) the port switch. <status> - Displays current mode.

Example

```
> wan wan2lan 1 on <--- 實際操作 使用 wan1 行不通
> wan wan2lan 2 on  <--- 改用 wan2 好像就 OK
% WAN2 convert to LAN4, WAN2 interface will disable
% Usage: show the WAN to LAN setting, currently only support WAN2
% When WAN2 is disabled or WAN2 is set wireless physical mode, eth port is
confi
gured as LAN
% Current WAN2 eth port is LAN mode
>
```

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
AN1: 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

AN2: 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

VC_WAN3: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0

VC_WAN4: Offline, stall=N
Mode: ---, Up Time=00:00:00
IP=---, GW IP=---
TX Packets=0, TX Rate(bps)=0, RX Packets=0, RX Rate(bps)=0

VC_WAN5: Offline, stall=N
...
```

Telnet Command: wan modem / wan modem2

This command, wan modem, allows you to configure 3G/ 4G USB Modem (PPP mode) of WAN3.

The command, wan modem2, allows you to configure 3G/ 4G USB Modem (PPP mode) of WAN4.

Syntax

wan modem *<init/ init2/ dial/ pin><string>*

wan modem paponly *<on/ off>*

wan modem backup_wait *<value>*

wan modem pipe *<Int><Din><Dout> (for USB WAN3 only)*

wan modem wakeup *<on/ off/ value> (for USB WAN3 only)*

wan modem vid *<id>*

wan modem pid *<id>*

wan modem status

Syntax Description

Parameter	Description

init	Set initial modem AT command (default value is "AT&FE0V1X1&D2&C1S0=0").
Init2	Set the second initial modem AT command.
dial	Set dial modem AT command (default value is "ATDT*99#").
pin	Set PIN code for SIM card. "0": disable
paponly	It means PAP Only. Set the PPP authentication of the USB WAN. on: None. off: PAP or CHAP.
backup_wait	Set waiting time after boot if USB WAN is in backup mode. This waiting time is reserved for the dial of main WANs so that the backup USB WAN will not go up first. Available setting is from 1 to 255. Unit is second.
pipe	It is for RD debug only. Please don't use it without our advice.
wakeup [on/off]	It is for RD debug only. Please don't use it without our advice.
vid	Set VID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
pid	Set PID of VID/PID match to bind the USB modem to specify WAN interface. By default, this match is not set (0x0/0x0) and the router specifies WAN interface by USB port.
status	Display current status of USB modem.

Example

```
> wan modem pin 0000
> wan modem status
 Modem Link Speed=0
 Current Signal Strength=0
 Last Fail Message:
 Current Connect Stage:
```

Telnet Command: wan wimax

This command allows you to enable or disable WAN 3G/4G DHCP mode for Vigor router.

Syntax

wan wimax *<on/off>*

Syntax Description

Parameter	Description
On	It means to enable WAN 3G/4G DHCP mode.
off	It means to disable WAN 3G/4G DHCP mode.

Example

```
> wan wimax ?
 Current status is wimax OFF
 DHCP client Disabled
 Current wimax zone=0
 Current wimax username=
 Current wimax password=
```

```
 Current wimax identity=
> wan wimax on
>
```

Telnet Command: wan lte

This command allows you to configure LTE WAN (for L model only).

Syntax

wan lte auth *<0/1>*

wan lte band

wan lte del *<index #/all>*

wan lte pass *<string>*

wan lte quota *[-<command><parameter>|...]*

wan lte read *<index #/all>*

wan lte reboot *[-<command><parameter>|...]*

wan lte reply *[-<command><parameter>|...]*

wan lte send *<number><message>*

wan lte sms

wan lte scan <*all|4g|3g|2g***>**

wan lte set

wan lte stus

wan lte tag *<index #/all>*

wan lte user *<string>*

wan lte wms *<send<cdma/gwpp> recv <cdma/gwgw>/setting>*

Syntax Description

Parameter	Description
auth <0/1>	Set PPP authentication of LTE WAN. 0: None. 1: PAP or CHAP.
band	Display working band information for LTE network connection.
del <index #/all>	Delete an SMS from the LTE SIM card by specifying the index number. Use "all" to delete all.
pass <string>	Set the password of LTE WAN.
quota [-<command><parameter>|...]	Set settings of SMS Quota Limit function. Available commands with parameter are listed below: [...] means that you can type in several commands in one line. -a <0/1>: Set whether to send an e-mail alert when SMS quota exceeded. (0: no 1: yes) -c <cycle>: Set the order of today in refresh cycle. -d <day>: Set the refresh day. -e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable) -h <hour>: Set the refresh hour. -m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2:

	periodically) -n <number>: Set SMS quota. The avaible number is between 1 and 1000000. -s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes)
read <index #/all>	Display information of an SMS in the LTE SIM card by specifying the index number. Use "all" to display all.
reboot	Set settings of Reboot on SMS Message function. <command> <parameter> | ... The available commands with parameters are listed below. [...] means that you can type in several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
reply	Set settings of Reply with Router Status Message function. <command> <parameter> | ... The available commands with parameters are listed below. [...] means that you can type in several commands in one line. -a <0/1>: Enable or disable Access Control List. (0: disable 1: enable) -c <0/1>: Set whether to reply with MAC address. (0: no 1: yes) -e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable) -f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes) -g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes) -h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes) -i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes) -j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes) -k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes) -l <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes) -m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes) -n <0/1>: Set whether to reply with Router name. (0: no 1: yes) -p <password>: Set the Password / PIN. This setting is necessary if this function is enabled. -u <0/1>: Set whether to reply with Router system uptime. (0: no 1: yes) -v <0/1>: Set whether to reply with Router firmware version. (0: no 1: yes) -x <number>: Set the first phone number in Access Control List. -y <number>: Set the second phone number in Access Control List. -z <number>: Set the third phone number in Access Control List.
send <number><message>	Send an SMS message to the specified phone number through the LTE SIM card.
sms	It means to set advanced settings for SMS. -a <0/1> : Alerts admin with e-mail when SMS inbox is full. -d <0/1> : Delete oldest read SMS when SMS inbox is full.

	-f <0/ 1> : Forward new SMS by e-mail to admin. -s <0/ 1> : Store SMS outbox cache with USB disk. (0: disable 1: enable)
scan <all| 4g| 3g| 2g>	It means to scan visible networks. [all| 4g| 3g| 2g]: Scan all, 4g, 3g or 2g network. Show: Display the scanning result.
set	It means to set APN name, keep alive time and so on. apn <apn_name> : Set a string as APN. pin <pin_code>: Set a pin code. power_recycle <backoff_time(0~20)>: Set the power recycle time (seconds) for redialing after power off. dial_on: Turn of the dialing function. It is used for RD debug. dial_off: Turn off the dialing function. It is used for RD debug. keep_alive_on <IP>: Turn of the function of Keep Alive On. Specify the IP address (x.x.x.x). keep_alive_off: Turn off the function of Keep Alive On. dhcp<on/ off>: Turn on or off the DHCP server, depending on your ISP configuration. fixed <IP>: Specify an IP address if DHCP is set as "off". Also, it depends on your ISP configuration. manual_dns <on/ off>: On, set the DNS server manually; Off, use the default DNS server setting. The default is "off". primary_dns <IP>: Set the primary DNS IP (x.x.x.x) address obtained from your ISP if manual_dns is set as "on". secondary_dns <ip): Set the secondary DNS IP (x.x.x.x) address obtained from your ISP if manual_dns is set as "on". specific_mccmnc <on/ off>: Turn on or off the specific MCC and MNC. mcc <mcc_value> : Set the value (0~999) for MCC (Mobile Country Code) mnc <mnc_value>: Set the value(0~999) for MNC (Mobile Network Code).
stus	Display status of LTE connection.
tag	Set an SMS in the LTE SIM card as read state by specifying the index number. Use "all" to set all SMS as read state.
user	Set the UserName of LTE WAN.
wms	This command is for RD debug only. We use it to test new USB modems. Please don't use it without our advice.

Example

```
> wan lte band

Access technology : LTE
Access band information : E-UTRA Op Band 3
Interfere with 2.4G WLAN : NO
Active channel: 1725
>wan lte stus
Status: Operational. (Online)
Access Tech: LTE
Band: E-UTRA Op Band 3
ISP: Chunghwa
MCC: 466, MNC: 92, LAC: 65534, Cell ID: 81023501
Max Channel TX Rate: 50000000 bps
Max Channel RX Rate: 100000000 bps
IMEI: 356318040749422
IMSI: 466924200859808
```

```
RSSI: -61 dBm
Unread SMS: 4
SMSC address: +886932400821
SMS service status : Ready
Number of SMS sent : 0
```

Telnet Command: wan detect

This command allows you to configure WAN connection detection. When Ping Detection is enabled (for Static IP or DHCP or PPPoE mode), Router pings specified IP addresses to detect the WAN connection.

Syntax

wan detect *<wan1/wan2><on/off/strict/always_on>*

wan detect *<wan1/wan2><on/off>***-t<***time>*

wan detect *<wan1/wan2> <on/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
<on/off/strict/always_on>	On: Enable ping detection. The IP address of the target shall be set. Off: Enable ARP detection (default). Time and interval should be set. strict: Enable the strict ARP detection. Time and interval should be set. always_on: Disable link detect, always connected(only support static IP)
-t <time>	Set the time for ARP detect or strict ARP detection.
-i <interval>	Set the interval for ARP detect or strict ARP detection.
target <ip addr>	Set the ping target. <ip addr>: It means the IP address used for detection. Type an IP address (e.g., 192.168.1.10) in this field.
target2<ip addr>	Set the secondary ping target. <ip addr>: It means the IP address used for detection. Type an IP address (e.g., 192.168.1.10) in this field.
target_gw <1/0>	Set whether to use gateway as ping target. 1: yes 0: no Note that USB WAN (PPP mode) cannot support PING gateway
ttl <1-255>	It means to set the ping TTL value (work as trace route) If you do not set any value for ttl here or just type 0 here, the system will use default setting (255) as the ttl value.
interval <interval>	Set the interval between each ping operation. Available setting is between 1 and 3600. The unit is second. *<interval>:* Type a value.

retry <retry>	Set how many ping operations are retried before the Router judges that the WAN connection is disconnected. Available setting is between 1 and 255. The unit is times. <retry>: Type a number.
status	It means to show the current status.

Example

```
> wan detect status
 WAN1: arp detect, send time=30, Interval = 5
 WAN2: arp detect, send time=30, Interval = 5
 WAN3: arp detect, send time=30, Interval = 5
 WAN4: arp detect, send time=30, Interval = 5
 WAN5: arp detect, send time=30, Interval = 5
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK

> wan detect status
WAN1: ping detect, Target=192.168.1.78, TTL=255, Target2=0.0.0.0,
TargetGW=off,
Interval=1, Retry=10
WAN2: arp detect, send time=30, Interval = 5
WAN3: arp detect, send time=30, Interval = 5
WAN4: arp detect, send time=30, Interval = 5
WAN5: arp detect, send time=30, Interval = 5
>
```

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.
status	Show the current status.

Example

```
> wan lb status
 WAN1: on
```

```
 WAN2: on
 WAN3: on
 WAN4: on
 WAN5: on
 Load balance mode is IP based
>
```

Telnet Command: wan lbel

This command allows you to set load balance exception list.

Syntax

wan lbel *<idx> <enable> <protocol> <ip type> <obj_grp idx> <port> <port_end> <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, TCP+UDP.
ip type	Set the IP type (0, 1 or 2) for the selected profile. 0: Any 1: IP object 2: IP group
obj_grp idx	Enter the index number (1 to 32 for IP group; 1 to 192 for IP object). If it is set with "0", then the IP type will be set as "Any".
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.
port_end	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	Show the current status.

Example

```
> wan lbel 1 1 tcp 0 1 0 300 testforload
> wan lbel status 1
 list[1] status:enable, protocol:tcp, IP type:any, IP idx:0, port:0~300, comment
:testforload
 list[2] status:enable, protocol:udp, IP type:any, IP idx:0, port:19302~19302, c
omment:Google STUN
 list[3] status:enable, protocol:tcp+udp, IP type:any, IP idx:0, port:5060~5060,
 comment:SIP
 list[4] status:disable, protocol:tcp, IP type:any, IP idx:0, port:80~80, commen
t:HTTP
 list[5] status:disable, protocol:tcp, IP type:any, IP idx:0, port:443~443, comm
ent:SSL
...
```

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

Syntax

wan mvlan *<pvc_no/status/save/enable/disable> <on/off/clear/tag tag_no> <service type/vlan priority> <px ... >*

wan mvlan *keeptag <pvc_no> <on/off>*

Syntax Description

Parameter	Description
pvc_no	It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured. However, bridge mode can be set on PVC number 2 to 9.
status	It means to display the whole Bridge status.
save	It means to save the configuration into flash of Vigor router.
enable/disable	It means to enable/disable the Multi-VLAN function.
on/off	It means to turn on/off bridge mode for the specific channel.
clear	It means to turn off/clear the port.
tag tag_no	It means to tag a number for the VLAN. -1: No need to add tag number. 1-4095: Available setting numbers used as tagged number.
service type	It means to specify the service type for VLAN. 0: Normal. 1: IGMP.
vlan priority	It means to specify the priority for the VALN setting. Range is from 0 to 7.
px	It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage.
keeptag	It means Multi-VLAN packets will keep their VLAN headers to LAN.

Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> wan mvlan 7 on p2 p3 p4
PVC  Bridge   p1   p2   p3   Service Type    Tag      Priority
 ------------------------------------------------------------------------
   7    ON     0    0    1       Normal      0(OFF)     0
>
```

Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

Syntax

wan multifno *<channel #><WAN interface #>*

wan multifno *status*

Syntax Description

Parameter	Description
channel #	There are 4 (?) channels including VLAN and PVC. Available settings are: 1=Channel 1 3=Channel 3 4=Channel 4 5=Channel 5
WAN interface #	Type a number to indicate the WAN interface. 1=WAN1 2=WAN2
status	It means to display current bridge status.

Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
> wan multifno status
% Channel 3 uplink ifno: 3
% Channel 4 uplink ifno: 3
% Channel 5 uplink ifno: 3
% Channel 6 uplink ifno: 3
% Channel 7 uplink ifno: 3
>
```

Telnet Command: wan vlan

This command allows you to configure the VLAN tag of WAN1 or WAN2.

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 stat

% Interface    Pri    Tag    Enabled
% ======================================
% WAN1          0      0
% WAN2          0      0
```

Telnet Command: wan budget

This command allows you determine the data *traffic volume* for each WAN interface respectively to prevent from overcharges for data transmission by the ISP.

Syntax

wan budget wan *<#> rdate <day><hour>*
wan budget wan *<#> <enable|disable>*
wan budget wan *<#>* **thres** *<budget limit (MB)>*
wan budget wan *<#>* **gthres** *<budget limit (GB)>*
wan budget wan *<#>* **mode** *<monthly|periodic|none>*
wan budget wan *<#>* **psday** *<th day in periodic>*
wan budget wan *<#> custom_mode <0/1>*
wan budget wan *<#> custom_mode_reset_hour <hour>*
wan budget wan *<#>* **action** *<action bitmap>*
wan budget status

Syntax Description

Parameter	Description
wan <#> rdate <day><hour>	wan <#>: Specify the WAN interface. *rdate <day><hour>:* Specify the WAN budget refresh time. day –Available settings are from 1 to 30. hour –Available settings are from 1 to 23. E.g., `wan budget wan 1 rdate 5 10` If monthy mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month. If periodic mode is selected: WAN budget will be refreshed every 5 days and 10 hours.
enable/disable	enable - Enable the function of wan budget. disable - Disable the function of wan budget.
thres <budget limit (MB)>	Specify the maximum value for WAN budget limit. (Unit: MB) budget limit –Type a number.
gthres <budget limit (GB)>	Specify the maximum value of wan budget limit. (Unit: GB) budget limit –Type a number.
mode <monthly|periodic|none>	Specify the calculation mode (monthly, periodically, or none) for WAN budget.
psday <th day in periodic>	It is used only when mode is set with "periodic". Specify the order of "today" in the cycle. E.g., `wan budget wan 5 psday` → It means "today" is the 5th day in the billing cycle.
custom_mode <0/1>	Set the custom mode (cycle in hours or in days). 0: cycle_in_hours 1: cycle_in_days
custom_mode_reset_hour <hour>	Set the reset hour value. hour: Enter 1 to 23.
action <action bitmap>	Determine the action to be performed when it reaches the WAN budget limit. *action bitmap* –Type a total number of actions to be executed. Different numbers represent different actions. 1: shotdown wan 2: send mail alert 4: send sms alert For example, if you type "5" (5=1+4), the system will send SMS alert when WAN shotdown is detected.
status	Display current configuration status of WAN budget.

Example

```
> wan budget wan 1 action 5
% WAN 1 budget action set to 5
> wan budget wan 1 gthres 10
% WAN 1 budget limit set to 10 GB
```

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** *<number>* *-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. base_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. Value: 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 -i 8.8.8.8 -s 1500 -d 30 -w 2 -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/IPv6 address>* **–s** *<mtu_size>* **–w** *<number>*

Syntax Description

Parameter	Description
-I <host/IPv6 address>	Specify the IPv6 target to detect. It must be an IPv6 IP address or host name. IPv6 address: Type the IPv6 address 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: 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 2.
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 4. 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 4. 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 2.

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
> wan failover show 3
  wan3 Active Mode : Always ON.
```

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 -p *<profile> [-l <lan>] [-s <ssid>] ...*

hsportal -p *<profile> -c*

Syntax Description

Parameter	Description
-p <profile>	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.
-s	Apply to WLAN interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-a	Apply to WLAN5G interfaces. E.g., apply SSID1 and SSID2: -s 1, 2.
-m	Select login mode. 0:skip 1:click 2:social 3:pin 4:social or pin
-f <0/1>	Configure facebook login. 0: disable. 1: enable.
-g <0/1>	Configure google login. 0: disable. 1: enable.
-h <0/1>	Enable HTTPS redirection. 0: disable. 1: enable.
-v <0/1>	Enable portal detection. 0: disable. 1: enable.
-i <string>	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 <string>	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 <0/1/2>	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 <1/2/3/4>	Reset the specified profile. <1/2/3/4>: Enter the index number of profile. For example, > hsportal set -p 1 -c Reset profile 1 ... [OK]
-o	Clear profiles for all clients.
-t <value>	Set the expire time for the specified profile. <value>: Enter a number of time period (unit: minutes). For example, k> hsportal setup -p 1 -t 300 Profile 1 set expire time 300 mins ... [OK]

Example

```
> hsportal -p 1 -c
Reset profile 1 ... [OK]
> hsportal -p 1 -r 0
Profile 1 set landing page mode 0 ... [OK]
> hsportal -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 / -c / -n / -a / -m / -s>*

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 <value>	Set email notigication object. [1~10]- Index number of object profile.
-s <value>	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: wl acl

This command allows the user to configure wireless access control settings.

Syntax

wl acl enable *<ssid1 ssid2 ssid3 ssid4>*

wl acl disable *<ssid1 ssid2 ssid3 ssid4>*

wl acl add *<MAC><ssid1 ssid2 ssid3 ssid4><isolate>*

wl acl del *<MAC>*

wl acl mode *<ssid1 ssid2 ssid3 ssid4><white/black>*

wl acl show

wl acl showmode

wl acl clean

Syntax Description

Parameter	Description
enable <ssid1 ssid2 ssid3 ssid4>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable <ssid1 ssid2 ssid3 ssid4>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add <MAC><ssid1 ssid2 ssid3 ssid4><isolate>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
del <MAC>	It means to delete a MAC address entry defined in the access control list.
mode <ssid1 ssid2 ssid3 ssid4><white/black>	It means to set white/black list for each SSID.
wl acl show	It means to show access control status.
wl acl showmode	It means to show the mode for each SSID.
wl acl clean	It means to clean all access control setting.

Example

```
> wl acl showmode
 ssid1: none
 ssid2: none
 ssid3: none
 ssid4: none
> wl acl add 00-50-70-ff-12-70 ssid1 ssid2 isolate
 Set Done !!
> wl acl show
 ----------Enable Mac Address Filter---------
 ssid1: dis   ssid2: dis   ssid3: dis   ssid4: dis
 ----------MAC Address Filter----------
 Index   Attribute      MAC Address        Associated SSIDs
    1       s          00:50:70:ff:12:70   ssid1 ssid2

 s: Isolate the station from LAN
>
```

Telnet Command: wl config

This command allows users to configure general settings and security settings for wireless connection.

Syntax

wl config mode *<value>*
wl config mode show
wl config channel *<number>*
wl config channel show
wl config preamble *<enable>*
wl config txburst *<enable>*
wl config ssid *<ssid_num enable ssid_name <hidden_ssid>>*
wl config security *<SSID_NUMBER><mode>*
wl config ratectl *<ssid_num enable upload download >*
wl config isolate *<ssid_num lan member>*
wl config dtim *<value>/ show*
wl config beaconperiod *<value> / show*
wl config radio *<1/ 0>/ show*
wl config frag *<value>/ show*
wl config rts *<value> / show*
wl config rate_alg *<value> / show*
wl config country *<value> / show*

Syntax Description

Parameter	Description
mode <value>	It means to select connection mode for wireless connection. Available settings are: "11bgn", "11gn", "11n", "11bg", "11g", or "11b".
mode show	It means to display what the current wireless mode is.
channel <number>	It means the channel of frequency of the wireless LAN. The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13. number=0, means Auto number=1, means Channel 1

	... number=13, means Channel 13.
preamble <enable>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
txburst <enable>	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the funciton.
ssid <ssid_num enable ssid_name <hidden_ssid>>	It means to set the name of the SSID, hide the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID. *hidden_ssid*: Type 0 to hide the SSID or 1 to display the SSID
security <SSID_NUMBER><mode><key ><index>	It means to configure security settings for the wirelesss connection. *SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *mode*: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK wep: WEP *key, index*: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
ratectl <ssid_num enable upload download>	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control for data upload. The unit is kbps. *download*: It means to configure the rate control for data download. The unit is kbps.
isolate <ssid_num lan member>	It means to isolate the wireless connection for LAN and/or Member. *lan* – It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *member* – It can make the wireless clients (stations) with the same SSID not accessing for each other.
dtim <value> / show	Set the DTIM value. value: 1 to 255 show: Display the DTIM setting.

beaconperiod <value> / show	Set the beaconperiod value. value: 20 to 1023 (milli-second) show: Display the beaconperiod etting.
radio <1/0>/ show	Enble or disable the wireless radio. 1/0: Type 1 to enable; 0 to disable. show: Display the radio setting.
frag<value>/ show	Set the fragment value. value: 256 to 2346 show: Display the fragment setting.
rts <value> / show	Set the RTS value. value: 1 to 2347 show: Display the RTS setting.
rate_alg <value>/ show	Set the algorithm for ALG rate. value: 0 for old algorithm; 1 for new algorithm. show: Display the ALG rate setting.
country <value>/ show	Set the country code for a country. value: two capital letters, e.g., TW, UK show: Display the country cod setting.

Example

```
> wl config mode 11bgn
 Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
 Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
 Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
 SSID  Enable  Hide_SSID  Name
 1     1       0         dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
% SSID1
%%  Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
> wl config country TW
 Set wireless country code TW
% <Note> Please restart wireless after you set the parameters.
```

Telnet Command: wl set

This command allows users to configure basic wireless settings.

Syntax

wl set *<SSID><CHAN[En]>*

wl set txburst *<enable>*

Syntax Description

Parameter	Description
SSID	It means to Enter the SSID for the router. The maximum character that you can use is 32.
CHAN[En]	It means to specify required channel for the router. *CHAN:* The range for the number is between 1 ~ 13. *En*: type *on* to enable the function; type *off* to disable the function.
txburst <enable>	It means to enhance the performance in data transmission about 40%* more (by enabling **Tx Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. 0: disable the function. 1: enable the function.

Example

```
> wl set MKT 2 on
% New Wlan Setting is:
% SSID=MKT
% Chan=2
% Wl is Enable
```

Telnet Command: wl act

This command allows users to activate wireless settings.

Syntax

wl act *[En]*

Syntax Description

Parameter	Description
En	It means to enable or disable the function of VPN isolation. 0: diable 1: enable

Example

```
> wl act on
% Set Wlan to Enable.
```

Telnet Command: wl stamgt

This command is used to configure connection time and reconnection time for each SSID that wireless client used for accessing into Internet.

Syntax

wl stamgt *<enable/disable><ssid_num>*

wl stamgt <*show><ssid_num>*

wl stamgt set *<ssid_num><c><r>*

wl stamgt reset *<ssid_num>*

Syntax Description

Parameter	Description

enable/disable	It means to enable/disable the station management control.
ssid_num	It means channel selection. Available channel for 2.4G: 0/1/2/3 Available channel for 5G: 4/5/6/7.
show	It means to display status or configuration of the selected channel.
c	It means connection time. The unit is minute.
r	It means reconnection time. The unit is minute.

Example

```
> wl stamgt enable 1
% Station Management Status: enabled
> wl stamgt set 1 60 60
> wl stamgt show 1
NO. SSID           BSSID              Connect time  Reconnect time
1.  Draytek      00:11:22:aa:bb:cc  0d:0:58:26      0d:0:0
```

Telnet Command: wl iso_vpn

This command allows users to activate the function of VPN isolation.

Syntax

wl iso_vpn *<ssid> <En>*

Syntax Description

Parameter	Description
ssid	It means the number of SSID. 1: SSID1 2: SSID2 3: SSID3 4: SSID4
En	It means to enable or disable the function of VPN isolation. 0: disable 1: enable

Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

Syntax

wl wmm ap *Queldx Aifsn Cwmin Cwmax Txop ACM*
wl wmm bss *Queldx Aifsn Cwmin Cwmax Txop ACM*
wl wmm ack *Que0_Ack Que1_Ack Que2_Ack Que3_Ack*
wl wmm enable *SSID0 SSID1 SSID2 SSID3*
wl wmm apsd *value*
wl wmm show

Syntax Description

Parameter	Description
ap	It means to set WMM for access point.
bss	It means to set WMM for wireless clients.
ack	It means to map to the Ack policy settings of AP WMM.
enable	It means to enable the WMM for each SSID. 0: disable 1: enable
Apsd [value]	It means to enable / disable the ASPD(automatic power-save delivery) function. 0: disable 1: enable
show	It displays current status of WMM.
QueIdx	It means the number of the queue which the WMM settings will be applied to. There are four queues, best effort, background, voice, and video.
Aifsn	It controls how long the client waits for each data transmission.
Cwmin/ Cwmax	**CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Specify the value ranging from 1 to 15.
Txop	It means transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It can restrict stations from using specific category class if it is enabled. 0: disable 1: enable

Example

```
> wl wmm ap 0 3 4 6 0 0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
> wl wmm enable 1 0 1 0
 WMM_SSID0 =1, WMM_SSID1 =0,WMM_SSID2 =1,WMM_SSID3 =0
> wl wmm show
 Enable WMM: SSID0 =1, SSID1 =0,SSID2 =1,SSID3 =0
 APSD=0
 QueIdx=0: APAifsn=3,APCwmin=4,APCwmax=6, APTxop=0,APACM=0
 QueIdx=1: APAifsn=7,APCwmin=4,APCwmax=10, APTxop=0,APACM=0
 QueIdx=2: APAifsn=1,APCwmin=3,APCwmax=4, APTxop=94,APACM=0
 QueIdx=3: APAifsn=1,APCwmin=2,APCwmax=3, APTxop=47,APACM=0
 QueIdx=0: BSSAifsn=3,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
 QueIdx=1: BSSAifsn=7,BSSCwmin=4,BSSCwmax=10, BSSTxop=0,BSSACM=0
 QueIdx=2: BSSAifsn=2,BSSCwmin=3,BSSCwmax=4, BSSTxop=94,BSSACM=0
 QueIdx=3: BSSAifsn=2,BSSCwmin=2,BSSCwmax=3, BSSTxop=47,BSSACM=0
 AckPolicy[0]=0: AckPolicy[1]=0,AckPolicy[2]=0,AckPolicy[3]=0
```

Telnet Command: wl ht

This command allows you to configure wireless settings.

Syntax

wl ht bw *value*

wl ht gi *value*

wl ht badecline *value*

wl ht autoba *value*

wl ht rdg *value*

wl ht msdu *value*

wl ht txpower *value*

wl ht antenna *value*

wl ht greenfield *value*

Syntax Description

Parameter	Description
wl ht bw value	The value you can type is 0 (for BW_20) and 1 (for BW_40).
wl ht gi value	The value you can type is 0 (for GI_800) and 1 (for GI_4001)
wl ht badecline value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht autoba value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht rdg value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht msdu value	The value you can type is 0 (for disabling) and 1 (for enabling).
wl ht txpower value	The value you can type ranges from 1 – 6 (level).
wl ht antenna value	The value you can type ranges from 0-3. 0: 2T3R 1: 2T2R 2: 1T2R 3: 1T1R
wl ht greenfield value	The value you can type is 0 (for mixed mode) and 1 (for green field).

Example

```
> wl ht bw value 1
 BW=0
 <Note> Please restart wireless after you set new parameters.
> wl restart
 Wireless restart.................
```

Telnet Command: wl restart

This command allows you to restart wireless setting.

Example

```
> wl restart
 Wireless restart.................
```

Telnet Command: wl wds

This command allows you to configure WDS settings.

Syntax

wl wds mode *<value>*

wl wds security *<value>*

wl wds ap *<value>*

wl wds hello *<value>*

wl wds status

wl wds show

wl wds mac *<value>*

wl wds flush

Syntax Description

Parameter	Description
mode <value>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security <value>	It means to configure security mode with encrypted keys for WDS. *mode*: Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK *key*: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. e.g., *wl dual wds security disable* *wl dual wds security wep 12345* *wl dual wds security wpa2psk 12345678*
ap <value>	It means to enable or disable the AP function. Value: 1 – enable the function. 0 – disable the function.
hello <value>	It means to send hello message to remote end (peer). Value: 1 – enable the function.

	0 –disable the function.
status	It means to display WDS link status for 2.4GHz connection.
show	It means to display current WDS settings.
mac add <index addr>	add *[index addr]* –Add the peer MAC entry in Repeater/ Bridge WDS MAC table.
mac clear/ disable/ enable <index/ all>	clear/ disable/ enable *[index/ all]*- Clear, disable, enable the specifed or all MAC entries in Repeater/ Bridge WDS MAC table. e.g, `wl dual wds mac enable 1`
flush	It means to reset all WDS setting.

Example

```
> wl wds status
Please enable WDS hello function first.

> wl wds hello 1
% <Note> Please restart router after you set the parameters.

> wl wds status
```

Telnet Command: wl apcli

This command allows users to configure AP client mode for wireless connection (2.4GHz).

Syntax

wl apcli show

wl apcli enable *<1/ 0>*

wl apcli security *<mode>*

wl apcli ssid *<ssid_name>*

wl apcli bssid *<mac address>*

Syntax Description

Parameter	Description
show	Display current status of wireless AP client.
enable [1/ 0]	It means to enable wireless 2.4GHz AP client mode. 1 –enable 0 –disable
security [mode]	There are several modes to be selected: Disable –disable the security settings. wpapsk [key] –WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] –WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpamixpsk [key] –WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wep [key] [index] –WEP key will be used. You need to Enter the key string and specify the index number of the profile to be

	applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
ssid <ssid_name>	Specify the SSID for wireless 2.4GHz AP client.
bssid <mac address>	Enter the MAC address for wireless 2.4GHz AP client.

Example

```
> wl apcli enable 1
Wireless AP-Clinet is enabled
> wl apcli show
% Wireless AP-Clinet is enabled
% Current SSID is test
%%  Security Mode: disable
% Wireless client is disconnected
%% data rate=---, mode=---, signal=0%
```

Telnet Command: wl btnctl

This command allows you to enable or disable wireless button control.

Syntax

wl btnctl <*value***>**

Syntax Description

Parameter	Description
value	0: disable 1: enable

Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

Telnet Command: wl iwpriv

These command is reserved for RD debug. Do not use it.

Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl stalist

Example

```
> wl stalist
wl stalist show    : show station list
wl stalist num     : show number of stations
wl stalist neighbor : show neighbor station list
```

Telnet Command: wl bndstrg

This command allows users to configure settings for Band Steering (2.4GHz).

Syntax

wl bndstrg show

wl bndstrg enable *<1/0>*

wl bndstrg chk_time *<value>*

Syntax Description

Parameter	Description
show	Display current status for Band Steering function.
enable <1/0>	It means to enable wireless 2.4GHz AP client mode. 1 – enable 0 – disable
chk_time <value>	If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for Vigor router to detect the wireless client. *<value> – 1 to 60 seconds.*

Example

```
> wl bndstrg show
band steering: disable
chk_time: 15 sec
> wl bndstrg chk_time 50 30
argv[0]:chk_time, argv[1]:50, argv[2]:30

%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

Telnet Command: wl artfns

This command allows users to configure airtime fairness function for wireless (2.4GHz) connection.

Syntax

wl artfns enable *<value>*

wl artfns trg_num *<value>*

wl artfns show

Syntax Description

Parameter	Description
enable <value>	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
Trg_num <value>	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
show	Display current status (enable or disable) and triggering client

	number for airtime fairness function.

Example

```
> wl artfns enable 1
> wl artfns trg_num 3
> wl artfns show
airtime fairness: enable
trg_num: 3
>
```

Telnet Command: wl drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl drayrs *set <mode><rs_low><rs_low_security><delta>*

wl drayrs *restart*

wl drayrs *show*

Syntax Description

Parameter	Description
set <mode> <rs_low> <rs_low_security><delta>	Select a mode for roaming. 0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl drayrs show
% Mode : Disable
%  rs_low         : -73
%  rs_low_secure  : -66
%  delta          : 5
>
```

Telnet Command: wl_dual acl

This command allows the user to configure wireless (5GHz) access control settings.

Syntax

wl_dual acl enable *<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl disable *<ssid1 ssid2 ssid3 ssid4>*

wl_dual acl add <*MAC***><***ssid1 ssid2 ssid3 ssid4***><***isolate***>**

wl_dual acl del <*MAC***>**

wl_dual acl mode *<ssid1 ssid2 ssid3 ssid4> <white/black>*

wl_dual acl show

wl_dual acl showmode

wl_dual acl clear

Syntax Description

Parameter	Description
enable <ssid1 ssid2 ssid3 ssid4>	It means to enable the settings for SSID1, SSID2, SSID3 and SSID4.
disable <ssid1 ssid2 ssid3 ssid4>	It means to disable the settings for SSID1, SSID2, SSID3 and SSID4.
add <MAC><ssid1 ssid2 ssid3 ssid4><isolate>	It means to associate a MAC address to certain SSID interfaces' access control settings. The isolate setting will limit the wireless client's network capabilities to accessing the wireless LAN only. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
isolate	It means to isolate the wireless connection of the wireless client (identified with the MAC address) from LAN.
del <MAC>	It means to delete a MAC address entry defined in the access control list. [MAC] format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx or xx.xx.xx.xx.xx.xx
mode <ssid1 ssid2 ssid3 ssid4> <white/black>	It means to set white/black list for each SSID.
show	It means to display current status of access control.
showmode	It means to show the mode for each SSID.
clear	It means to clear all of the access control settings.

Example

```
> wl_dual acl showmode
 SSID1: None
 SSID2: None
 SSID3: None
 SSID4: None
> wl_dual acl add 00-50-70-ff-12-80 ssid1 ssid2 isolate
 Set Done !!
> wl_dual acl show
---------- Mac Address Filter Status ---------
 SSID1: Disable SSID2: Disable SSID3: Disable SSID4: Disable
 ---------- MAC Address List ----------
```

```
 Index   Attribute      MAC Address        Associated SSIDs        Comment
   1       s          00:50:70:ff:12:80   SSID1 SSID2

 s: Isolate the station from LAN
```

Telnet Command: wl_dual apscan

This command is used to scan Access Point installed near the location of Vigor router.

Syntax

wl_dual apscan *start*

wl_dual apscan *show*

Syntax Description

Parameter	Description
start	It means to execute the AP scanning.
show	It means to display the content of the AP list.

Example

```
> wl_dual apscan start
> wl_dual apscan show
 AP scan is ongoing.
> wl_dual apscan ?
% wl_dual apscan [start/show]
% start: do AP scan
% show: show AP list

> wl_dual apscan show
5G Access Point List :
BSSID            Channel   SSID
```

Telnet Command: wl_dual config

This command allows users to configure general settings and security settings for wireless connection (5GHz).

wl_dual config enable *<value>*
wl dual config enable show
wl_dual config mode *<value>*
wl_dual config mode show
wl_dual config channel *<number>*
wl_dual config channel show
wl_dual config preamble *<enable>*
wl_dual config preamble show
wl_dual config ssid *<ssid_num enable ssid_name>*
wl_dual config ssid hide *<ssid_num enable>*
wl_dual config ssid show
wl_dual config ratectl *<ssid_num enable upload download>*
wl_dual config ratectl show
wl_dual config isolate lan *<ssid_num enable>*
wl_dual config isolate member *<ssid_num enable>*
wl_dual config isolate vpn *<ssid_num enable>*
wl_dual config isolate show
wl_dual config frag *<value>*
wl_dual config frag show
wl_dual config rts *<value>*
wl_dual config rts show
wl_dual config country *<value>*
wl_dual config txpower *<value>*
wl_dual config nss *<value>*

Syntax Description

Parameter	Description
enable <value>	It means to enable/ disable the 5GHz wireless function. 1: enable 0: disable
show	It means to display if 5G wireless function is enabled or not.
mode <value>	It means to select connection mode for wireless connection. Available settings are: "11a", "11n_5g", "11n" and "11an".
mode show	It means to display what the current wireless mode is.
channel <number>	It means the channel of frequency of the wireless LAN. The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140. number=0, means Auto number=36, means Channel 36 ... Number=52, means Channel 52.
channel show	It means to display what the current channel is.
preamble <enable>	It means to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However,

	some original 11b wireless network devices only support long preamble. 0: disable to use long preamble. 1: enable to use long preamble.
preamble show	It means to display if preamble is enabled or not.
ssid <ssid_num enable ssid_name>	It means to set the name of the SSID, hide the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *ssid_name*: Give a name for the specified SSID.
ssid hide <ssid_num enable>	It means to hide the name of the SSID if required. *ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. enable: Type 0 to hide the SSID or 1 to display the SSID.
ssid show	It means to display a table of SSID configuration.
ratectl <ssid_num enable upload download>	It means to set the rate control for the specified SSID. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable. *upload*: It means to configure the rate control for data upload. The unit is kbps. *download*: It means to configure the rate control for data download. The unit is kbps. (example: `wl dual config ratectl 1 1 25 25`)
ratectl show	It means to display the data transmission rate (upload and download) for SSID1, SSID2, SSID3 and SSID4.
isolate lan <ssid_num enable>	It means to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable
isolate member <ssid_num enable>	It means to isolate the wireless connection from Member. It can make the wireless clients (stations) with the same SSID not accessing for each other. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate vpn <ssid_num enable>	It means to isolate the wireless connection from VPN. *ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *enable*: It means to enable such function. 0: disable and 1:enable.
isolate show	It means to display the status of wireless isolation.
frag <value>	It means to set the fragment threshold. value: Enter a number (256 to 2346).
frag show	It means to display current value of fragment threshold.
rts <value>	It means to set the RTS threshold. value: Enter a number (1 to 2347).
rts show	It means to display current value of RTS threshold.
country <value>	It means to set the country code. Each country will be represented with two digits. value: Enter two capital letters (e.g., TW, UK, CN..)
txpower <value>	It means to set TX power. Value: Enter a number (1 to 6).

nss <value>	It means to set NSS. Value: Enter a number (0 to 4).

Example

```
> wl_dual config mode 11a
 Current mode is 11a
% <Note> Please restart 5G wireless after you set the channel
> wl_dual config channel 60
 Current channel is 60
% <Note> Please restart 5G wireless after you set the channel.
> wl_dual config preamble 1
Long preamble is enabled
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid 1 enable dray
SSID  Enable  Hide_SSID  Name
 1     1       0         dray
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual config ssid show
 SSID  Enable  Hide_SSID  Name
 1     1       0         dray
 2     0       0         DrayTek_5G_Guest
 3     0       0
 4     0       0
```

Telnet Command: wl_dual restart

This command allows you to restart wireless setting (5GHz).

Example

```
> wl_dual restart
 5G wireless restart.................
```

Telnet Command: wl_dual security

This command allows users to configure security settings for the wireless connection (5GHz).

Syntax

wl_dual security <*SSID_NUMBER*><*mode*><*key*><*index*>

wl_dual security show

Syntax Description

Parameter	Description
security <*SSID_NUMBER*> <*mode*><*key*><*index*>	*SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4. *mode*: Available settings are: disable: No security. wpa1x: WPA/802.1x Only wpa21x: WPA2/802.1x Only wpamix1x: Mixed (WPA+WPA2/802.1x only) wep1x: WEP/802.1x Only wpapsk: WPA/PSK wpa2psk: WPA2/PSK wpamixpsk: Mixed (WPA+WPA2)/PSK

	wep: WEP *key, index*: Moreover, you have to add keys for *wpapsk, wpa2psk, wpamixpsk* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format.
show	It means to display current mode selection for each SSID.

Example

```
> wl_dual security 1 wpa2psk 123456789e
% <Note> Please restart 5G wireless after you set the parameters.

> wl_dual security show
%% 5G Wireless LAN Security Settings:
% SSID1
%%  Mode: WPA2/PSK
% SSID2
%%  Mode: Disable
% SSID3
%%  Mode: Disable
% SSID4
%%  Mode: Disable
```

Telnet Command: wl_dual stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

Syntax

wl_dual stalist show

wl_dual stalist num

wl_dual stalist neighbor

wl_dual stalist validtime *<time>*

wl_dual stalist maxmum *<num>*

Syntax Description

Parameter	Description
validtime <time>	Set the valid time of the neighbor station list. <time> - 0 to 300000.
Maxnum <num>	Set the maximum number of neighbor station list. <value> - 10 to 512

Example

```
> wl_dual stalist neighbor
5G Wireless Neighbor Station List :
MAC Address      |Vendor Name     |RSSI(%)|RSSI(dbm)|SSID|time(ms)
F2:C6:DB:2B:25:E0|                |24     |-84      |none|20
D6:FC:CB:DC:C1:E8|                |24     |-84      |none|0
80:00:0B:04:CE:5A|Intel           |11     |-88      |none|7230880
00:1D:AA:80:FE:D6|DrayTek         |15     |-87      |none|7210610
```

```
A6:99:E2:27:7F:A0|              |50    |-76     |none|20
0A:32:AB:06:88:2C|              |40    |-79     |none|0
F8:63:3F:56:06:C6|              |15    |-87     |none|881950
1E:B9:C9:03:04:52|              |87    |-62     |none|20
8E:DF:E3:0A:F4:02|              |3     |-92     |none|20
E2:41:8F:4B:1A:11|              |50    |-76     |none|20
BA:96:81:7D:11:BD|              |24    |-84     |none|10
7C:2A:31:10:1B:11|              |2     |-93     |none|0
>
```

Telnet Command: wl_dual wds

This command allows users to configure WDS for wireless connection (5GHz).

Syntax

wl_dual wds mode *<value>*
wl_dual wds security *<value>*
wl_dual wds ap *<value>*
wl_dual wds hello *<value>*
wl_dual wds status
wl_dual wds show
wl_dual wds mac add *<index addr>*
wl_dual wds mac clear/disable/enable *<index/all>*
wl_dual wds flush

Syntax Description

Parameter	Description
mode <value>	It means to specify connection mode for WDS. [value]: Available settings are : d: Disable b: Bridge r: Repeapter
security <value>	It means to configure security mode with encrypted keys for WDS. *mode*: Available settings are: disable: No security. wep: WEP wpapsk [key]: WPA/PSK wpa2psk [key]: WPA2/PSK *key*: Moreover, you have to add keys for *wpapsk, wpa2psk,* and *wep*, and specify index number of schedule profiles to be followed by the wireless connection. WEP keys must be in 5/13 ASCII text string or 10/26 Hexadecimal digit format; WPA keys must be in 8~63 ASCII text string or 64 Hexadecimal digit format. e.g., *wl_dual wds security disable* *wl_dual wds security wep 12345* *wl_dual wds security wpa2psk 12345678*
ap <value>	It means to enable or disable the AP function. Value: 1 –enable the function. 0 –disable the function.
hello <value>	It means to send hello message to remote end (peer).

	Value: 1 – enable the function. 0 – disable the function.
status	It means to display WDS link status for 5GHz connection.
show	It means to display current WDS settings.
mac add <index addr>	**add** *[index addr]* – Add the peer MAC entry in Repeater/ Bridge WDS MAC table.
mac clear/ disable/ enable <index/ all>	**clear**/**disable**/**enable** *[index/ all]*- Clear, disable, enable the specifed or all MAC entries in Repeater/ Bridge WDS MAC table. e.g, *wl_dual wds mac enable 1*
flush	It means to reset all WDS setting.

Example

```
> wl_dual wds status
Please enable WDS hello function first.

> wl_dual wds hello 1
% <Note> Please restart router after you set the parameters.
> wl_dual wds security wep
>
> wl_dual wds show
 Mode : Disable
> wl_dual wds wep 12345
% <Note> Please restart router after you set the parameters.
```

Telnet Command: wl_dual wps

This command allows users to configure WPS for wireless connection (5GHz).

Syntax

wl_dual wps enable *<value>*

wl dual wps pbc

wl_dual wps pin *<code>*

wl_dual wps show

Syntax Description

Parameter	Description
enable <value>	It means to enable WPS. 1 – enable 0 – disable
pbc	It means to start WPS by pressing the WLAN ON/ OFF WPS button on Vigor router.
pin <code>	It means to start WPS by using client PIN code. [code]: Client PIN code (digit number).
show	It means to display current WPS settings.

Example

```
> wl_dual wps enable 1
 WPS is enabled.
> wl_dual wps pin 88563337
 WPS has triggered by PIN code.
```

```
The AP will wait for WPS request from your client for 2 minutes...
```

Telnet Command: wl_dual apcli

This command allows users to configure AP client mode for wireless connection (5GHz).

Syntax

wl_dual apcli show

wl_dual apcli enable *<value>*

wl_dual apcli security *<mode>*

wl_dual apcli ssid *<ssid_name>*

wl_dual apcli bssid

Syntax Description

Parameter	Description
show	Display current status of wireless AP client.
enable <value>	It means to enable wireless 5GHz AP client mode. 1 – enable 0 – disable
security <mode>	There are several modes to be selected: Disable – disable the security settings. wpapsk [key] – WPA Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpa2psk [key] – WPA2 Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wpamixpsk [key] – WPA Mixed Pre-shared Key will be used. Keys must start with 0x to be identified as a Hexadecimal number key. WPA keys must be in 8~63 ASCII string or 64 Hexadecimal digit format. wep [key] [index] – WEP key will be used. You need to Enter the key string and specify the index number of the profile to be applied. WEP keys must be in 5/13 ASCII string or 10/26 Hexadecimal digit format.
ssid <ssid_name>	Specify the SSID for wireless 5GHz AP client.
bssid	Enter the MAC address for wireless 5GHz AP client.

Example

```
> wl_dual apcli enable 1
Wireless 5G AP-Clinet is enabled
> wl_dual apcli show
% Wireless 5G AP-Clinet is enabled
% Current SSID is
%%  Security Mode: disable
% Wireless 5G client is disconnected
%% data rate=---, mode=---, signal=0%
> wl_dual apcli ssid carrie
% <Note> Please restart wireless 5g after you set the parameters.
 Current SSID is carrie
```

Telnet Command: wl_dual artfns

This command allows users to configure airtime fairness function for wireless (5GHz) connection.

Syntax

wl_dual artfns enable *<value>*

wl_dual artfns trg_num *<value>*

wl_dual artfns show

wl_dual artfns status

Syntax Description

Parameter	Description
enable <value>	It means to enable wireless airtime fairness function. 1 – enable 0 – disable
trg_num <value>	Set a threshold when the active station number achieves this number, the airtime fairness function will be applied. Available values will be 2 to 64.
show	Display current status (enable or disable) and triggering client number for airtime fairness function.
status	Display whether the function of airtime fairness is enabled or disabled.

Example

```
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!

> wl_dual artfns enable 0
> wl_dual artfns trg_num 2
> wl_dual artfns show
airtime fairness for 5G: disable
trg_num: 2
> wl_dual artfns status
airtime fairness for 5G is disabled !!!
```

Telnet Command: wl_dual drayrs

This command allows the user to configure settings for Roaming for wireless clients.

Syntax

wl_dual drayrs *set <mode> <rs_low> <rs_low_security> <delta>*

wl_dual drayrs *restart*

wl_dual drayrs *show*

Syntax Description

Parameter	Description
set <mode> <rs_low>	Select a mode for roaming.

<rs_low_security> <delta>	0 - disable 1 - Strictly Minimum RSSI 2 - Minimum RSSI rs_low – Set a value of Strictly Minimum RSSI (62~86). rs_low_security – Set a value of Minimum RSSI (62~86). delta – Set a value of Adjacent AP RSSI (1~20).
restart	Restart to activate roaming function.
show	Dispaly current configuration of roaming function.

Example

```
> wl_dual drayrs show
% Mode : Disable
%  rs_low          : -73
%  rs_low_secure   : -66
%  delta           : 5
> wl_dual drayrs set 1 68 66 2
> wl_dual drayrs show
% Mode : Strictly Minimun RSSI
%  rs_low         : -68
%  rs_low_secure   : -66
%  delta          : 2
```

Telnet Command: wol

This command allows Administrator to set the white list of WAN IP addresses/Subnets, that the magic packet from these IP addresses/Subnets will be eligible to pass through NAT and wake up the LAN client. You also need to set NAT rule for LAN client.

Syntax

wol up *<MAC Address> / <IP 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_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 <0/1>	It means to set login service. 0:HTTPS 1:HTTP e.g.,*-s 1*
-u user [user name] *-u ip [ip address]*	Unblock specifies user or IP address. *user name* –type the user name that you want to unblock. *ip address* —type the IP address that you want to unblock.
User edit	
PROFILE_IDX	Type the index number of the profile that you want to edit.
-a <0/1>	Enable(1) or disable(0) the internal RADIUS.
-d	Disable User profile function.
-e	Enable User profile function.
-f <0/1>	Enable(1) or disable(0) the local 802.1x user.
-i <0-255>	It means to set idle time (from 0 to 255, 0 means unlimited). e.g., *-i 60*
-o <0-65535>	It means to set auto-logout (from 0 to 65535, 0 means unlimited).
-m <0-2000>	It means to set the maximum (from 0 to 2000) login user number. e.g., *-m 200*
-n <param>	It means to set a user name for a profile. Param: Enter a string, e.g.,*-n fortest.*
-p <param>	It means to configure user password. Param: Enter a string, e.g., *-p 60fortest.*
-q <param>	It means to set time quota (0-65535) of the user profile. Param: Enter a value, e.g., *-q 200.*
-r <param>	It means to set data quota. Param: Enter a value, e.g., *-r 1000.*
-s <sch_idx1,sch_idx2,sch_idx3 , and sch_idx4>	It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4.
-t <0/1>	It means to enable / disable time quota limitation for user profile 0:Disable 1:Enable
-u <0/1>	It means to enable / disable data quota limitation for user profile 0:Disable 1:Enable
-v	It means to view user profile(s).
-w <MB/GB>	It means to specify the data quota unit (MB/GB). e.g., -w MB
-x <0-3>	It means to set external server authentication 0: None 1: LDAP 2: Radius 3: TACAS e.g., *-x 2*
-l <0-3>	It means to set log type. 0:None

	1:Login 2:Event 3:All
-P <0/1>	It means to enable / disable pop browser tracking window for user profile 0:Disable 1:Enable
-T <0/1>	It means to enable / disable authentication by telnet. 0:Disable 1:Enable
-H <0/1>	It means to enable / disable authentication by web page. 0:Disable 1:Enable
-A <0/1>	It means to enable / disable authentication by alert tool. 0:Disable 1:Enable
-L <index>	It means to set active directory / LDAP profiles. Index: Specify the index number (profile_idx1 to profile_idx8) of the profile.
-D	It means to list all active directory / LDAP profiles.
-O <0/1>	It means to reset the quota automatically. 0:Disable 1:Enable
-Q <param>	It means to set the default time quota. param: Enter a number (1 to 65535).
-R <param>	It means to set the default data quota. param: Enter a number (1 to 65535).
-M <param>	It means to set the default quota type. 0: when login permission schedule expired. 1: at the start time of schedule.
I <param>	It means to specify the default quota schedule index to perform the job at the start time.
-S	It means to display the reset default quota type and the schedule index.
User account	
USER_NAME	It means to type a name of the user account.
-d <0/1>	It means to enable / disable data quota limitation for user account. 0:Disable 1:Enable
-q	It means to set account time quota. e.g., *-q 200*
-r	It means to set account data quota. e.g., *-r 1000*
-t <0/1>	It means to enable / disable time quota limitation for user account. 0:Disable 1:Enable
-w	It means to set data quota unit (MB/GB).

Example

```
> user account admin -d 1
 Enable the [admin] data quota limited
```

Telnet Command: appqos

The command is used to configure QoS for APP.

Syntax

appqos view

appqos enable <*0/1*>
appqos traceable <*-v | -e AP_INDEX CLASS | -d AP_INDEX*>
appqos untraceable <*-v | -e AP_INDEX CLASS | -d AP_INDEX*>

Syntax Description

Parameter	Description
view	It means to display current status of APP QoS.
enable <0/1>	It means to enable or disable the function of APP QoS.
traceable/ untraceable	The APPs are divided into traceable and untraceable based on their properties.
-v	It means to view the content of all traceable APs. Use "appqos traceable –v" to display all of the traceable APS with speficed index number. Use "appqos untraceable –v" to display all of the untraceable APS with speficed index number.
-e	It menas to enable QoS for application(s) and assign QoS class.
AP_INDEX	Each index number represents one application. Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceabel APPs. Index number: 0~49, 55~59, 61, 67, 69, and 70~123 are used for 125 untraceable AP.
CLASS	Specifies the QoS class of the application, from 1 to 4 1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class
-d	It means to disable QoS for application(s).

Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

Telnet Command: 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   : Vigor2915 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 []
```