DrayTek

# Vigor2927 Series

## Dual-WAN Security Router




# USER'S GUIDE

V1.0

# Vigor2927 Series
# Dual-WAN Security Router

# User's Guide

**Version: 1.0**

**Firmware Version: V4.2.0.1**

**(For future update, please visit DrayTek web site)**

**Date: August 5, 2020**

### Copyrights

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

### Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 7, 8, 10 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

### Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

### Warranty

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

### Be a Registered Owner

- Web registration is preferred. You can register your Vigor router via http://www.DrayTek.com.

### Firmware & Tools Updates

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

  http://www.DrayTek.com

# *Table of Contents*


**Part I Installation ..... i**

I-1 Introduction ..... 1

I-1-1 Indicators and Connectors ..... 2

*I-1-1-1 Vigor2927 ..... 2*
*I-1-1-2 Vigor2927L ..... 4*
*I-1-1-3 Vigor2927ac / Vigor2927ax / Vigor2927Lac ..... 6*
*I-1-1-4 Vigor2927Vac ..... 10*

I-1-2 Notes for Antenna Installation (for "L" model) ..... 12

I-2 Hardware Installation ..... 14

I-2-1 Installing Vigor Router ..... 14

I-2-2 Wall-Mounted Installation ..... 15

I-2-3 Installing USB Printer to Vigor Router ..... 16

I-3 Accessing Web Page ..... 23

I-4 Changing Password ..... 25

I-5 Dashboard ..... 27

I-5-1 Virtual Panel ..... 28

I-5-2 Name with a Link ..... 29

I-5-3 Quick Access for Common Used Menu ..... 30

I-5-4 GUI Map ..... 31

I-5-5 Web Console ..... 32

I-5-6 Config Backup ..... 33

I-5-7 Logout ..... 33

I-5-8 Online Status ..... 34

*I-5-8-1 Physical Connection ..... 34*
*I-5-8-2 Virtual WAN ..... 37*

I-6 Quick Start Wizard ..... 38

I-6-1 For WAN1/WAN2 (Ethernet) ..... 39

I-6-2 For WAN3/WAN4 (Wireless 2.4G/Wireless 5G) ..... 48

I-6-3 For WAN5/WAN6 (USB) ..... 54

I-7 Service Activation Wizard ..... 56

I-8 Registering Vigor Router ..... 58

**Part II Connectivity ..... 61**

II-1 WAN ..... 62

Web User Interface ..... 64

II-1-1 General Setup ..... 64

*II-1-1-1 WAN1/WAN2 (Ethernet) ..... 67*
*II-1-1-2 WAN3/WAN4 (Wireless 2.4G or 5G) ..... 69*
*II-1-1-3 WAN5 / WAN6 (USB) or WAN5 (LTE) ..... 70*

II-1-2 Internet Access ..... 72

*II-1-2-1 Details Page for PPPoE in WAN1/WAN2 (Physical Mode: Ethernet) ..... 75*

*II-1-2-2 Details Page for Static or Dynamic IP in WAN1/WAN2 (Physical Mode: Ethernet) ..... 78*
*II-1-2-3 Details Page for PPTP/L2TP in WAN1/WAN2 (Physical Mode: Ethernet) ..... 82*
*II-1-2-4 Details Page for Static or Dynamic IP in WAN3/WAN4 (Physical Mode: Wireless 2.4G/ Wireless 5G) ..... 84*
*II-1-2-5 Details Page for 3G/4G USB Modem (PPP mode) in WAN5 / WAN6 ..... 86*
*II-1-2-6 Details Page for 3G/4G USB Modem (DHCP mode) in WAN5 / WAN6 ..... 88*
*II-1-2-7 Details Page for IPv6 – Offline in WAN1~WAN6 ..... 90*
*II-1-2-8 Details Page for IPv6 – PPP in WAN1/WAN2 ..... 91*
*II-1-2-9 Details Page for IPv6 – TSPC in WAN1~WAN6 ..... 92*
*II-1-2-10 Details Page for IPv6 – AICCU in WAN1~WAN6 ..... 94*
*II-1-2-11 Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2 ..... 95*
*II-1-2-12 Details Page for IPv6 – Static IPv6 in WAN1/WAN2 ..... 97*
*II-1-2-13 Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2 ..... 98*
*II-1-2-14 Details Page for IPv6 – 6rd in WAN1/WAN2 ..... 100*
II-1-3 Multi-VLAN ..... 102
II-1-4 WAN Budget ..... 108
*II-1-4-1 General Setup ..... 108*
*II-1-4-2 Status ..... 112*
Application Notes ..... 113
*A-1 How to set up Multi-PVC for triple play deployment? ..... 113*
II-2 LAN ..... 118
Web User Interface ..... 120
II-2-1 General Setup ..... 120
*II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup ..... 122*
*II-2-1-2 Details Page for LAN2 ~ LAN8 and DMZ ..... 126*
*II-2-1-3 Details Page for IP Routed Subnet ..... 128*
*II-2-1-4 Details Page for LAN IPv6 Setup ..... 130*
*II-2-1-5 DHCP Server Options ..... 133*
II-2-2 VLAN ..... 135
II-2-3 Bind IP to MAC ..... 139
II-2-4 LAN Port Mirror ..... 142
II-2-5 Wired 802.1x ..... 143
II-3 Hardware Acceleration ..... 144
II-3-1 Setup ..... 144
II-4 NAT ..... 146
Web User Interface ..... 147
II-4-1 Port Redirection ..... 147
II-4-2 DMZ Host ..... 151
II-4-3 Open Ports ..... 154
II-4-4 Port Triggering ..... 156
II-4-5 ALG ..... 158
II-5 Applications ..... 158
Web User Interface ..... 161
II-5-1 Dynamic DNS ..... 161
II-5-2 LAN DNS / DNS Forwarding ..... 167
II-5-3 DNS Security ..... 171
*II-5-3-1 General Setup ..... 171*

*II-5-3-2 Domain Diagnose* ..... *172*
II-5-4 Schedule ..... 173
II-5-5 RADIUS/TACACS+ ..... 176
*II-5-5-1 External RADIUS* ..... *176*
*II-5-5-2 Internal RADIUS* ..... *177*
*II-5-5-3 External TACACS+* ..... *180*
II-5-6 Active Directory/LDAP ..... 181
*II-5-6-1 General Setup* ..... *181*
*II-5-6-2 Active Directory / LDAP Profiles* ..... *182*
II-5-7 UPnP ..... 183
II-5-8 IGMP ..... 185
*II-5-8-1 General Setting* ..... *185*
*II-5-8-2 Working Status* ..... *186*
II-5-9 Wake on LAN ..... 187
II-5-10 SMS / Mail Alert Service ..... 188
*II-5-10-1 SMS Alert* ..... *188*
*II-5-10-2 Mail Alert* ..... *189*
II-5-11 Bonjour ..... 190
II-5-12 High Availability ..... 193
*II-5-12-1 General Setup* ..... *194*
*II-5-12-2 Config Sync* ..... *196*
II-5-13 Local 802.1X General Setup ..... 198
Application Notes ..... 200
*A-1 How to use High Availability?* ..... *200*
*A-2 How to use DrayDDNS?* ..... *208*
*A-3 How to Implement the LDAP/AD Authentication for User Management?* ..... *213*
*A-4 How to Configure Customized DDNS?* ..... *216*
II-6 Routing ..... 220
Web User Interface ..... 221
II-5-1 Static Route ..... 221
II-6-2 Load-Balance /Route Policy ..... 226
*Diagnose for Route Policy* ..... *231*
II-6-3 BGP ..... 234
*II-6-3-1 Basic Settings* ..... *234*
*II-6-3-2 Static Network* ..... *235*
Application Notes ..... 236
*A-1 How to set up Address Mapping with Route Policy?* ..... *236*
*A-2 How to use destination domain name in a route policy?* ..... *238*
*A-3 Introduction to Load Balance/Route Policy* ..... *240*
II-7 LTE ..... 242
Web User Interface ..... 243
II-7-1 General Settings ..... 243
*II-7-1-1 SMS Quota* ..... *243*
*II-7-1-2 SMS Inbox/Outbox* ..... *244*
II-7-2 SMS Inbox ..... 245
II-7-3 Send SMS ..... 248
II-7-4 Router Commands ..... 249

II-7-5 Status ..... 251

**Part III Wireless LAN ..... 253**

III-1 Wireless LAN (2.4GHz/5GHz) ..... 254

Web User Interface ..... 257

III-1-1 Wireless Wizard ..... 257

III-1-2 General Setup ..... 261

III-1-3 Security ..... 263

III-1-4 Access Control ..... 265

III-1-5 WPS ..... 267

III-1-6 WDS (for 5GHz) ..... 270

III-1-7 Advanced Setting ..... 272

III-1-8 Station Control ..... 276

III-1-9 Bandwidth Management ..... 277

III-1-10 AP Discovery ..... 278

III-1-11 Airtime Fairness ..... 279

III-1-12 Band Steering (2.4 GHz) ..... 281

III-1-13 Roaming ..... 285

III-1-14 Station List ..... 286

**Part IV VPN ..... 289**

IV-1 VPN and Remote Access ..... 290

Web User Interface ..... 291

IV-1-1 VPN Client Wizard ..... 291

IV-1-2 VPN Server Wizard ..... 297

IV-1-3 Remote Access Control ..... 305

IV-1-4 PPP General Setup ..... 306

IV-1-5 SSL General Setup ..... 308

IV-1-6 IPsec General Setup ..... 309

IV-1-7 IPsec Peer Identity ..... 312

IV-1-8 VPN Matcher Setup ..... 314

IV-1-9 OpenVPN ..... 316

*IV-1-9-1 OpenVPN Server Setup ..... 316*

*IV-1-9-2 Client Config ..... 318*

IV-1-10 Remote Dial-in User ..... 320

IV-1-11 LAN to LAN ..... 324

IV-1-12 VPN Trunk Management ..... 333

IV-1-13 Connection Management ..... 340

Application Notes ..... 342

*A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode ... 342*

*A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2 ..... 347*

IV-2 Certificate Management ..... 350

Web User Interface ..... 351

IV-2-1 Local Certificate ..... 351
IV-2-2 Trusted CA Certificate ..... 356
IV-2-3 Certificate Backup ..... 359
IV-2-4 Self-Signed Certificate ..... 360

**Part V Security ..... 361**

V-1 Firewall ..... 362
Web User Interface ..... 364
V-1-1 General Setup ..... 364
V-1-2 Filter Setup ..... 369
V-1-3 Defense Setup ..... 379
*V-1-3-1 DoS Defense ..... 379*
*V-1-3-2 Spoofing Defense ..... 382*
V-1-4 Diagnose ..... 383
V-2 Central Security Management (CSM) ..... 386
Web User Interface ..... 387
V-2-1 APP Enforcement Profile ..... 387
V-2-2 APPE Signature Upgrade ..... 389
V-2-3 URL Content Filter Profile ..... 391
V-2-4 Web Content Filter Profile ..... 395
V-2-5 DNS Filter Profile ..... 398
Application Notes ..... 400
*A-1 How to Create an Account for MyVigor ..... 400*
*A-2 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter ..... 405*

**Part VI Management ..... 411**

VI-1 System Maintenance ..... 412
Web User Interface ..... 413
VI-1-1 System Status ..... 413
VI-1-2 TR-069 ..... 415
VI-1-3 Administrator Password ..... 418
VI-1-4 User Password ..... 421
VI-1-5 Login Page Greeting ..... 424
VI-1-6 Configuration Backup ..... 426
VI-1-7 Syslog/Mail Alert ..... 429
VI-1-8 Time and Date ..... 432
VI-1-9 SNMP ..... 433
VI-1-10 Management ..... 435
VI-1-11 Panel Control ..... 439
VI-1-12 Self-Signed Certificate ..... 444
VI-1-13 Reboot System ..... 446
VI-1-14 Firmware Upgrade ..... 447

VI-1-15 Firmware Backup ..... 448
VI-1-16 Internal Service User List ..... 449
VI-1-17 Dashboard Control ..... 450
VI-2 Bandwidth Management ..... 451
Web User Interface ..... 452
VI-2-1 Sessions Limit ..... 452
VI-2-2 Bandwidth Limit ..... 454
VI-2-3 Quality of Service ..... 456
VI-2-4 APP QoS ..... 462
VI-3 User Management ..... 463
Web User Interface ..... 464
VI-3-1 General Setup ..... 464
VI-3-2 User Profile ..... 466
VI-3-3 User Group ..... 470
VI-3-4 User Online Status ..... 471
Application Notes ..... 473
*A-1 How to authenticate clients via User Management ..... 473*
*A-2 How to use Landing Page Feature ..... 482*
VI-4 Hotspot Web Portal ..... 486
Web User Interface ..... 486
VI-4-1 Profile Setup ..... 486
*VI-4-1-1 Login Method ..... 487*
*VI-4-1-2 Steps for Configuring a Web Portal Profile ..... 487*
VI-4-2 User Information ..... 503
*VI-4-2-1 User Info ..... 503*
*VI-4-2-2 Database Setup ..... 504*
VI-4-3 Quota Management ..... 506
VI-4-4 PIN Generator ..... 509
*VI-4-4-1 PIN Status ..... 509*
*VI-4-4-2 PIN Generator ..... 510*
*VI-4-4-3 PIN Voucher ..... 511*
Application Notes ..... 513
*A-1 How to create Facebook APP for Web Portal Authentication? ..... 513*
*A-2 How to create Google APP for Web Portal Authentication? ..... 519*
VI-5 Central Management (VPN) ..... 521
Web User Interface ..... 522
VI-5-1 General Setup ..... 522
*VI-5-1-1 General Settings ..... 522*
*VI-5-1-2 IPsec VPN Settings ..... 523*
VI-5-2 CPE Management ..... 524
*VI-5-2-1 Managed Device List ..... 524*
*VI-5-2-2 CPE Maintenance ..... 527*
*VI-5-2-3 Google Map ..... 529*
VI-5-3 VPN Management ..... 531
VI-5-4 Log & Alert ..... 532

Application Notes ..... 533
*A-1 CVM Application - How to manage the CPE (router) through Vigor2927 series? . 533*
*A-2 CVM Application - How to build the VPN between remote devices and Vigor2927 series? ..... 537*
*A-3 CVM Application - How to upgrade CPE firmware through Vigor2927 series? .... 539*
VI-6 Central Management (AP) ..... 542
Web User Interface ..... 543
VI-6-1 Dashboard ..... 543
VI-6-2 Status ..... 544
VI-6-3 WLAN Profile ..... 545
VI-6-4 AP Maintenance ..... 550
VI-6-5 AP Map ..... 551
VI-6-6 Traffic Graph ..... 556
VI-6-7 Event Log ..... 557
VI-6-8 Total Traffic ..... 558
VI-6-9 Station Number ..... 558
VI-6-10 Load Balance ..... 559
VI-7 Central Management (Switch) ..... 561
Web User Interface ..... 562
VI-7-1 Status ..... 562
*VI-7-1-1 Switch Status ..... 562*
*VI-7-1-2 Switch Hierarchy ..... 564*
VI-7-2 Profile ..... 565
VI-7-3 Group ..... 568
VI-7-4 Maintenance ..... 570
VI-7-5 Alert and Log ..... 571
*VI-7-5-1 Alert Setup ..... 571*
*VI-7-5-2 Switch and Port Setup ..... 571*
*VI-7-5-3 Alert Logs ..... 573*
VI-7-6 Database Setup ..... 574
VI-7-7 Support List ..... 575
VI-8 Central Management (External Devices) ..... 576

**Part VII Others ..... 579**

VII-1 Objects Settings ..... 580
Web User Interface ..... 581
VII-1-1 IP Object ..... 581
VII-1-2 IP Group ..... 584
VII-1-3 IPv6 Object ..... 586
VII-1-4 IPv6 Group ..... 588
VII-1-5 Service Type Object ..... 590
VII-1-6 Service Type Group ..... 592
VII-1-7 Keyword Object ..... 594
VII-1-8 Keyword Group ..... 596

VII-1-9 File Extension Object ..... 597
VII-1-10 SMS/Mail Service Object ..... 599
VII-1-11 Notification Object ..... 604
VII-1-12 String Object ..... 607
VII-1-13 Country Object ..... 608
VII-1-14 Objects Backup/Restore ..... 611
Application Notes ..... 612
*A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection ..... 612*
VII-2 USB Application ..... 616
Web User Interface ..... 617
VII-2-1 USB General Settings ..... 617
VII-2-2 USB User Management ..... 618
VII-2-3 File Explorer ..... 620
VII-2-4 USB Device Status ..... 621
VII-2-5 Temperature Sensor ..... 622
VII-2-6 Modem Support List ..... 625
VII-2-7 SMB Client Support List ..... 626
Application Notes ..... 627
*A-1 How can I get the files from USB storage device connecting to Vigor router? ... 627*

**Part VIII Troubleshooting ..... 631**

VIII-1 Diagnostics ..... 632
Web User Interface ..... 633
VIII-1-1 Dial-out Triggering ..... 633
VIII-1-2 Routing Table ..... 634
VIII-1-3 ARP Cache Table ..... 635
VIII-1-4 IPv6 Neighbour Table ..... 636
VIII-1-5 DHCP Table ..... 637
VIII-1-6 NAT Sessions Table ..... 638
VIII-1-7 DNS Cache Table ..... 639
VIII-1-8 Ping Diagnosis ..... 640
VIII-1-9 Data Flow Monitor ..... 641
VIII-1-10 Traffic Graph ..... 644
VIII-1-11 VPN Graph ..... 645
VIII-1-12 Trace Route ..... 646
VIII-1-13 Syslog Explorer ..... 647
VIII-1-14 IPv6 TSPC Status ..... 648
VIII-1-15 High Availability Status ..... 648
VIII-1-16 Authentication Information ..... 650
VIII-1-17 DoS Flood Table ..... 652
VIII-1-18 Route Policy Diagnosis ..... 653

VIII-2 Checking If the Hardware Status Is OK or Not ..... 655
VIII-3 Checking If the Network Connection Settings on Your Computer Is OK or Not ..... 656
VIII-4 Pinging the Router from Your Computer ..... 659
VIII-5 Checking If the ISP Settings are OK or Not ..... 661
VIII-6 Problems for 3G/4G Network Connection ..... 662
VIII-7 Backing to Factory Default Setting If Necessary ..... 663
VIII-8 Contacting DrayTek ..... 664
Appendix I: VLAN Applications on Vigor Router ..... 665

**Part IX Telnet Commands ..... 673**

Accessing Telnet of Vigor2927 ..... 674

**Index ..... 928**

# 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.**

Vigor2927 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 4-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 (e.g., Vigor2927lac) each of the wireless SSIDs can also be grouped within one of the VLANs.

In addition, Vigor2927 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2927 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 Vigor2927

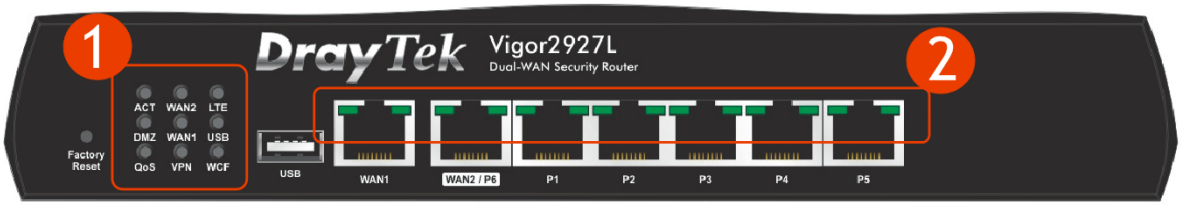



| No. | LED | Status | Explanation |
|---|---|---|---|
| (1) | ACT | Off | The router is powered off. |
| | | Blinking | The router is powered on and running normally. |
| | WAN2/WAN1 | On | Internet connection is ready. |
| | | Off | Internet connection is not ready. |
| | | Blinking | The data is transmitting. |
| | USB1/USB2 | On | USB device is connected and ready for use. |
| | | Off | No USB device is connected. |
| | | Blinking | The data is transmitting. |
| | DMZ | On | The DMZ function is enabled. |
| | | Off | The DMZ function is disabled. |
| | | Blinking | The data is transmitting. |
| | QoS | On | The QoS function is active. |
| | | Off | The QoS function is inactive. |
| | VPN | On | The VPN tunnel is active. |
| | | Off | VPN services are disabled |
| | | Blinking | Traffic is passing through VPN tunnel. |
| | WCF | On | The Web Content Filter is active. (It is enabled from **Firewall >> General Setup**). |
| | | Off | WCF is disabled. |
| (2) | WAN1,WAN2 / P6 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps. |
| | LAN P1-P5 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps |

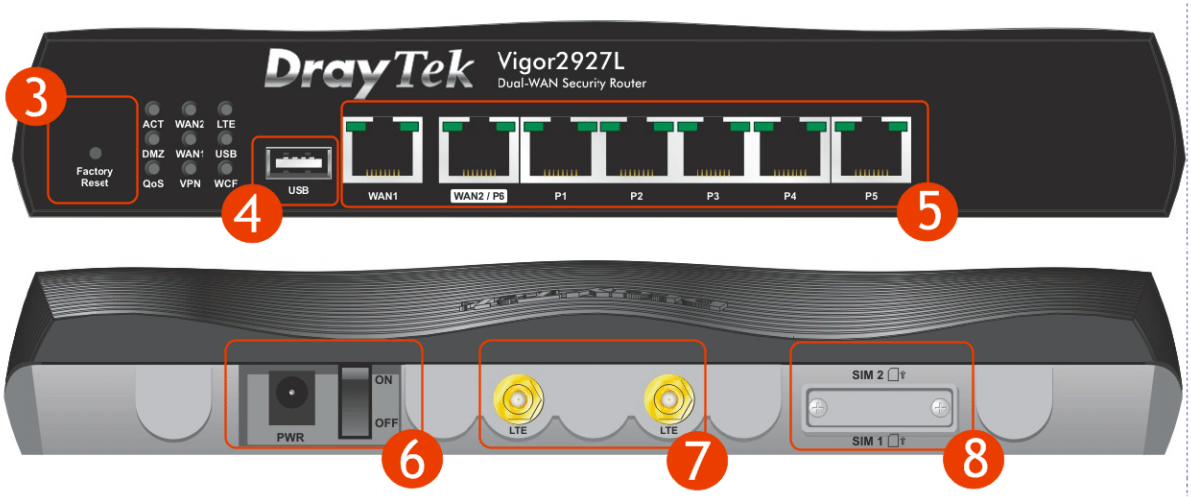



| No. | Interface | Description |
|---|---|---|
| (3) | Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| (4) | USB | Connecter for a USB device (for 3G/4G USB Modem or printer or thermometer). |
| (5) | WAN1 | Connecter for local network devices or modem for accessing Internet. |
| | WAN2 / P6 | Connecter for local network devices or modem for accessing Internet. It is a switchable port. It can be used for LAN connection or WAN connection according to the settings configured in WUI. |
| | LAN P1-P5 | Connecters for local network devices. |
| (6) | PWR | Connecter for a power adapter. |
| | ON/OFF | Power Switch. |

### I-1-1-2 Vigor2927L

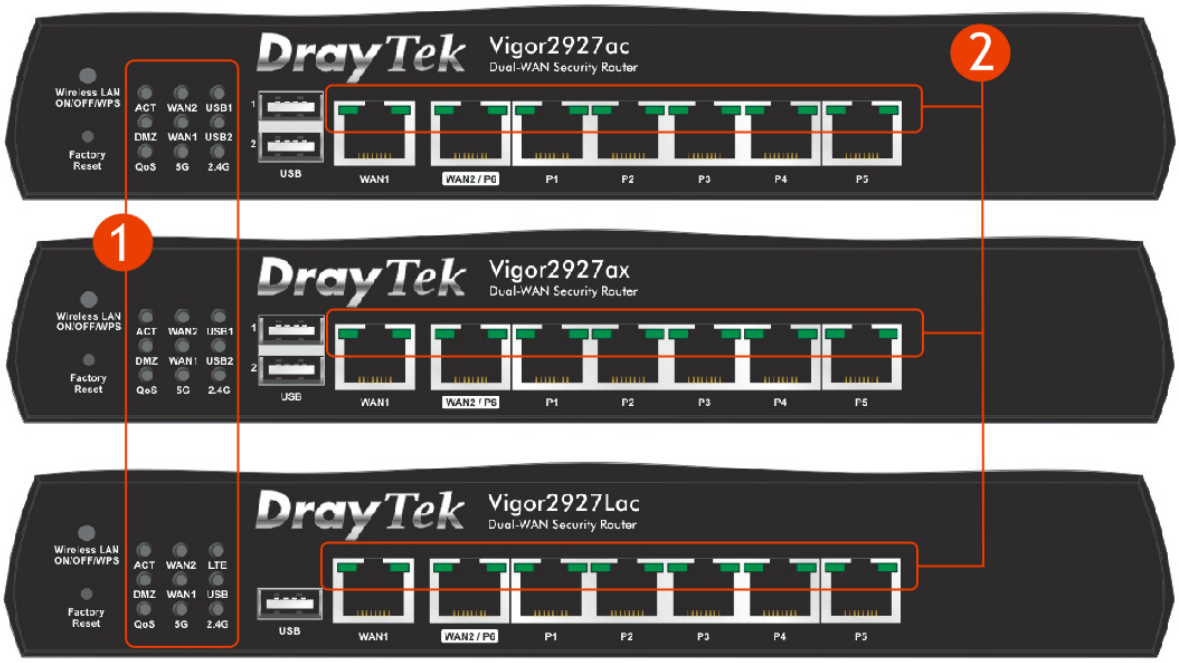



| No. | LED | Status | Explanation |
|---|---|---|---|
| (1) | ACT | Off | The router is powered off. |
| | | Blinking | The router is powered on and running normally. |
| | WAN2/WAN1 | On | Internet connection is ready. |
| | | Off | Internet connection is not ready. |
| | | Blinking | The data is transmitting. |
| | LTE | On | LTE device is connected and ready for use. |
| | | Off | LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). |
| | | Blinking | Slowly: LTE device is in dialing up.<br>Quickly: The data is transmitting. |
| | DMZ | On | The DMZ function is enabled. |
| | | Off | The DMZ function is disabled. |
| | | Blinking | The data is transmitting. |
| | USB | On | USB device is connected and ready for use. |
| | | Off | No USB device is connected. |
| | | Blinking | The data is transmitting. |
| | QoS | On | The QoS function is active. |
| | | Off | The QoS function is inactive. |
| | VPN | On | The VPN tunnel is active. |
| | | Off | VPN services are disabled |
| | | Blinking | Traffic is passing through VPN tunnel. |
| | WCF | On | The Web Content Filter is active. (It is enabled from **Firewall >> General Setup**). |
| | | Off | WCF is disabled. |
| (2) | WAN1,WAN2 / P6 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps. |
| | LAN P1-P5 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps |



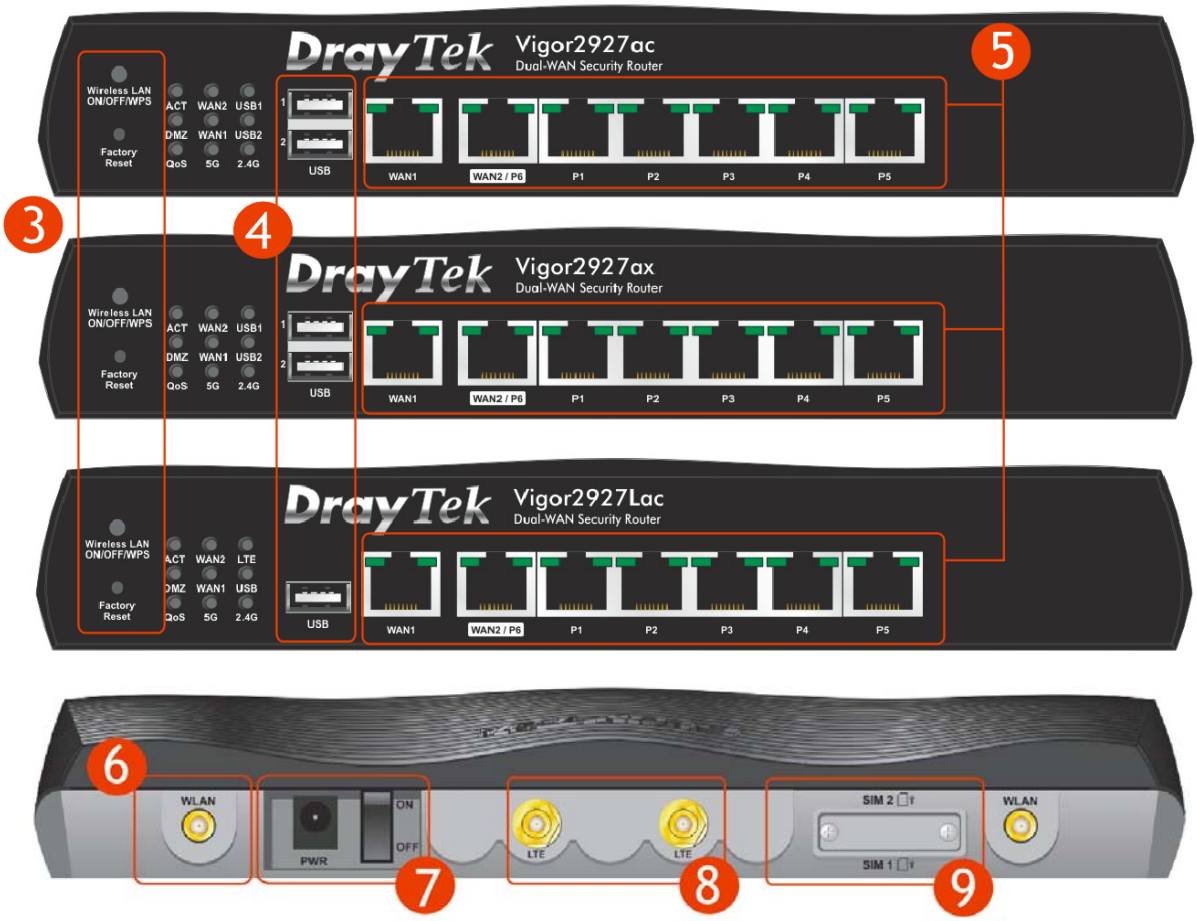

| No. | Interface | Description |
|---|---|---|
| (3) | Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| (4) | USB | Connecter for a USB device (for 3G/4G USB Modem or printer or thermometer). |
| (5) | WAN1 | Connecter for local network devices or modem for accessing Internet. |
| | WAN2 / P6 | Connecter for local network devices or modem for accessing Internet. It is a switchable port. It can be used for LAN connection or WAN connection according to the settings configured in WUI. |
| | LAN P1-P5 | Connecters for local network devices. |
| (6) | PWR | Connecter for a power adapter. |
| | ON/OFF | Power Switch. |
| (7) |  | Connecter for installing LTE antennas. |
| (8) | SIM 2/1 | Slots for installing SIM card. |

## I-1-1-3 Vigor2927ac / Vigor2927ax / Vigor2927Lac




| No. | LED | Status | Explanation |
|---|---|---|---|
| (1) | ACT | Off | The router is powered off. |
| | | Blinking | The router is powered on and running normally. |
| | WAN2/WAN1 | On | Internet connection is ready. |
| | | Off | Internet connection is not ready. |
| | | Blinking | The data is transmitting. |
| | USB1/USB2 | On | USB device is connected and ready for use. |
| | | Off | No USB device is connected. |
| | | Blinking | The data is transmitting. |
| | LTE | On | LTE device is connected and ready for use. |
| | | Off | LTE device is not detected, or has serious problem (e.g., no SIM card, SIM pin error, SIM deactivated, and etc.). |
| | | Blinking | Slowly: LTE device is in dialing up.<br>Quickly: The data is transmitting. |
| | DMZ | On | The DMZ function is enabled. |
| | | Off | The DMZ function is disabled. |
| | | Blinking | The data is transmitting. |

| | | | |
|---|---|---|---|
| (1) | QoS | On | The QoS function is active. |
| | | Off | The QoS function is inactive. |
| | 5G / 2.4G | On | 5G / 2.4G: Wireless access point with bandwidth of 5GHz/2.4GHz is ready.<br>WLAN: Wireless access point is ready. |
| | | Off | Wireless function is disabled. |
| | | Blinking | It will blink slowly while wireless traffic goes through.<br>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.) |
| (2) | WAN1,WAN2 / P6 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps. |
| | LAN P1-P5 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps |



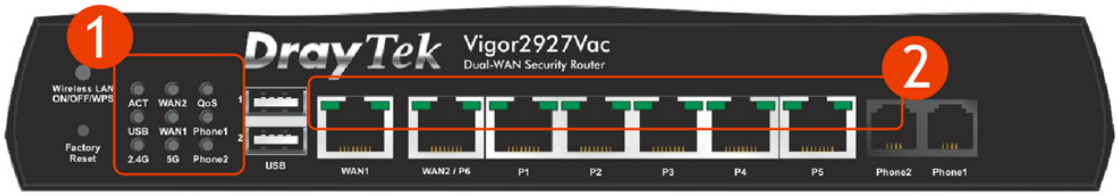




| No. | Interface | Description |
|---|---|---|
| (3) | Wireless LAN ON/OFF/WPS | Wireless band will be switched /changed according to the button pressed and released. For example,<br>● 2.4G (On) and 5G (On) – in default.<br>● 2.4G (Off) and 5G (On) – pressed and released the button once.<br>● 2.4G (On) and 5G (Off) – pressed and released the button twice.<br>● 2.4G (Off) and 5G (Off) – pressed and released the button three times.<br>When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. |
| | Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| (4) | USB1~2 / USB | Connecter for a USB device (for 3G/4G USB Modem or printer or thermometer). |
| (5) | WAN1 | Connecter for local network devices or modem for accessing Internet. |
| | WAN2 / P6 | Connecter for local network devices or modem for accessing Internet.<br>It is a switchable port. It can be used for LAN connection or WAN connection according to the settings configured in WUI. |
| | LAN P1-P5 | Connecters for local network devices. |
| (6) |  | Connecter for installing WLAN antennas.<br>(For ac model) |
| (7) | PWR | Connecter for a power adapter. |

| | | |
|---|---|---|
| | ON/OFF | Power Switch. |
| (8) |  | Connecter for installing LTE antennas.<br>(For L model). |
| (9) | SIM 2/1 | Slots for installing SIM card.<br>(For L model). |

### I-1-1-4 Vigor2927Vac



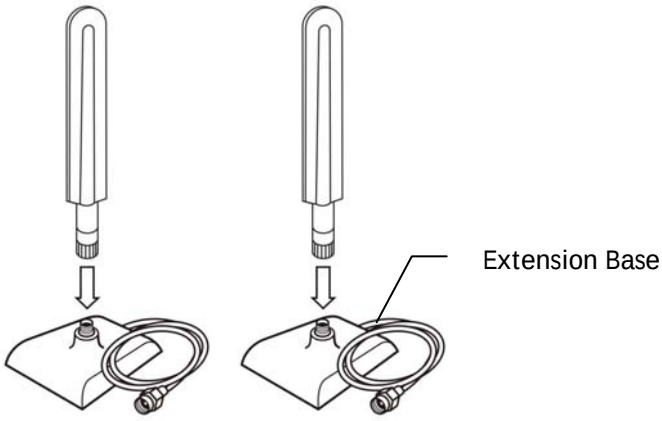

| No. | LED | Status | Explanation |
|---|---|---|---|
| (1) | ACT | Off | The router is powered off. |
| | | Blinking | The router is powered on and running normally. |
| | WAN2/WAN1 | On | Internet connection is ready. |
| | | Off | Internet connection is not ready. |
| | | Blinking | The data is transmitting. |
| | QoS | On | The QoS function is active. |
| | | Off | The QoS function is inactive. |
| | USB | On | USB device is connected and ready for use. |
| | | Off | No USB device is connected. |
| | | Blinking | The data is transmitting. |
| | Phone1/Phone 2 | On | The phone connected to this port is off-hook. |
| | | Off | The phone connected to this port is on-hook. |
| | | Blinking | A phone call comes. |
| | 2.4G/5G | On | 5G / 2.4G: Wireless access point with bandwidth of 5GHz/2.4GHz is ready.<br>WLAN: Wireless access point is ready. |
| | | Off | Wireless function is disabled. |
| | | Blinking | It will blink slowly while wireless traffic goes through.<br>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.) |
| (2) | WAN1,WAN2 / P6 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps. |
| | LAN P1-P5 | | |
| | Left LED | On | The port is connected. |
| | | Off | The port is disconnected. |
| | | Blinking | The data is transmitting. |
| | Right LED | On | The port is connected with 1000Mbps. |
| | | Off | The port is connected with 10/100Mbps |




| No. | Interface | Description |
|---|---|---|
| (3) | Wireless LAN ON/OFF/WPS | Wireless band will be switched /changed according to the button pressed and released. For example,<br>● 2.4G (On) and 5G (On) – in default.<br>● 2.4G (Off) and 5G (On) – pressed and released the button once.<br>● 2.4G (On) and 5G (Off) – pressed and released the button twice.<br>● 2.4G (Off) and 5G (Off) – pressed and released the button three times.<br>When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. |
| | Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| (4) | USB1~2 / USB | Connecter for a USB device (for 3G/4G USB Modem or printer or thermometer). |
| (5) | WAN1 | Connecter for local network devices or modem for accessing Internet. |
| | WAN2 / P6 | Connecter for local network devices or modem for accessing Internet.<br>It is a switchable port. It can be used for LAN connection or WAN connection according to the settings configured in WUI. |
| | LAN P1-P5 | Connecters for local network devices. |
| (6) |  | Connecter for installing WLAN antennas.<br>(For ac model) |
| (7) | PWR | Connecter for a power adapter. |
| | ON/OFF | Power Switch. |

## I-1-2 Notes for Antenna Installation (for "L" model)

Magnetic antenna must be installed on the extension base before connecting to Vigor router.




There are two mounting holes for installing antennas with extension base on Vigor router. Please install them as shown below.

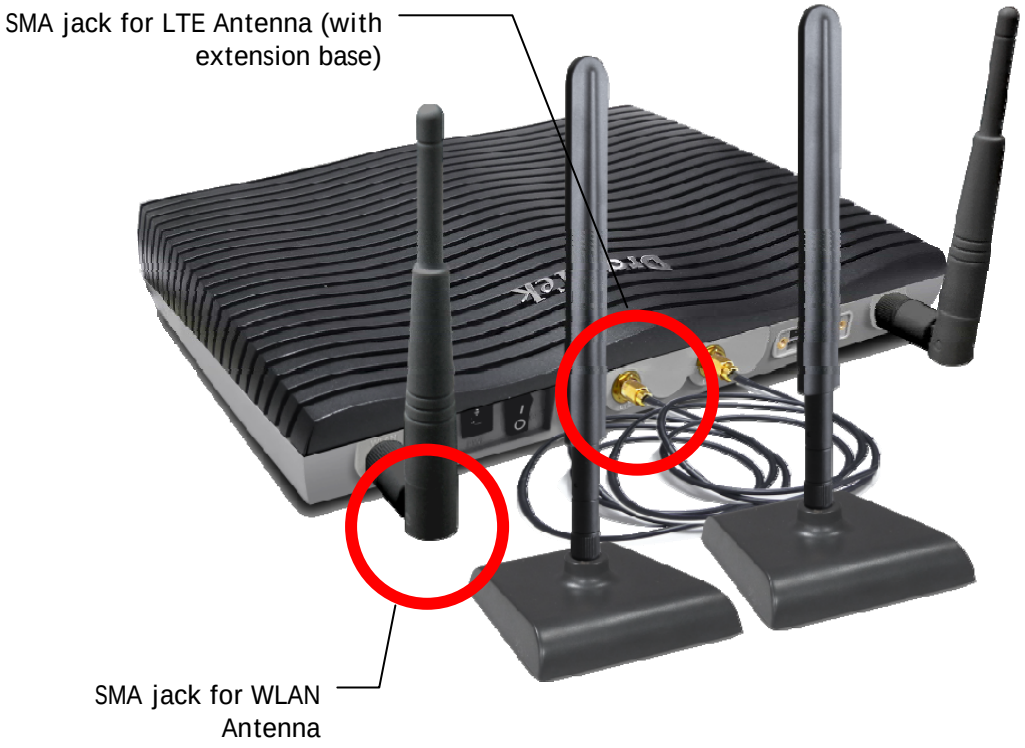



Note, if only one antenna shall be installed, please use the mounting hole (major signal transmitted hole) near to the power switch.

While installing the SIM card into the card slot, note that back plate of the SIM card slot must be removed first and the direction of card notch must be on the left side.




There are two types of antennas provided for Vigor2927Lac, which must be installed in different locations carefully and correctly. Wrong installation might cause bad signal of wireless connection. Therefore, pay attention to the installation of antennas by referring to the following illustration.



# I-2 Hardware Installation

## I-2-1 Installing Vigor Router

Before starting to configure the router, you have to connect your devices correctly. (For the hardware connection, we take *"ac"* model as an example.)

1. Connect the DSL interface to the land line jack with a DSL line cable.

   Connect the cable Modem/DSL Modem/Media Converter to the WAN port of router with Ethernet cable (RJ-45).

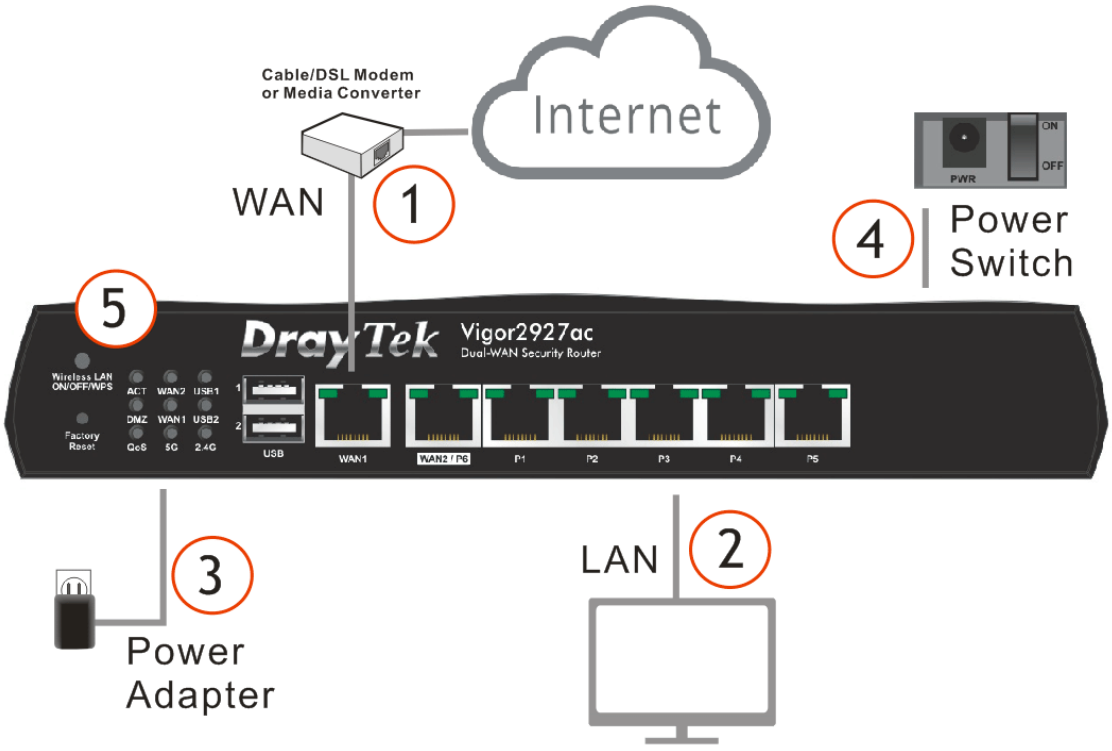
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.

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.

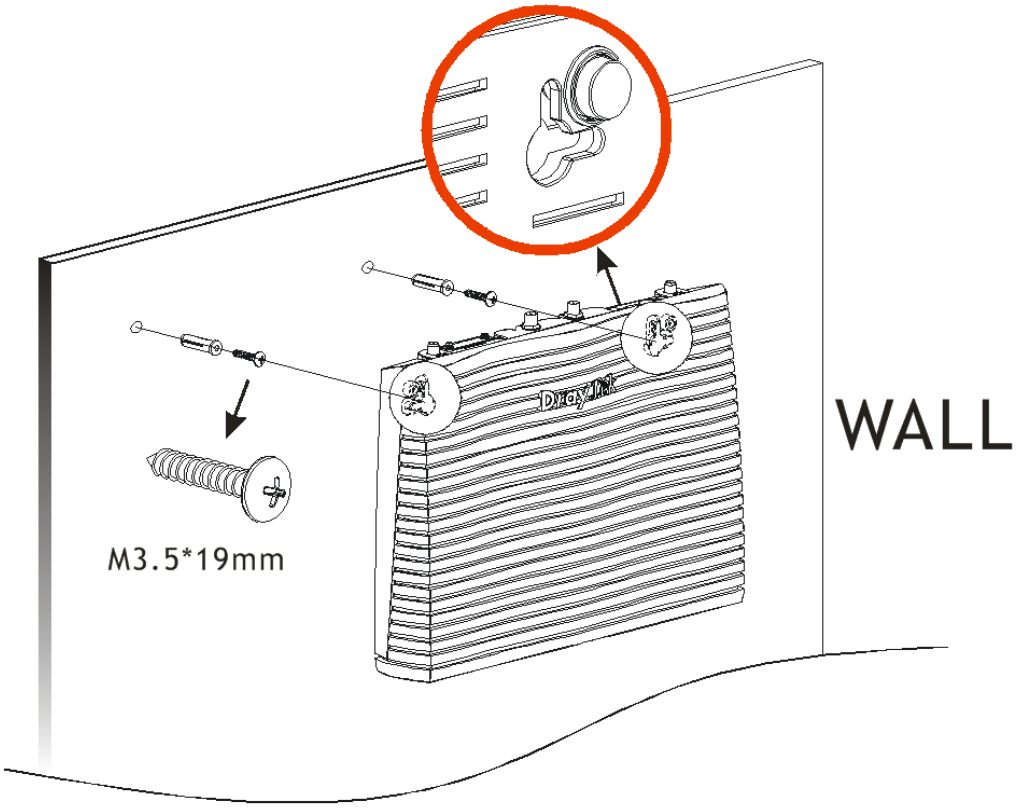
(For the hardware connection, we take *"ac"* model as an example.)



## I-2-2 Wall-Mounted Installation

Vigor router has keyhole type mounting slots on the underside.

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

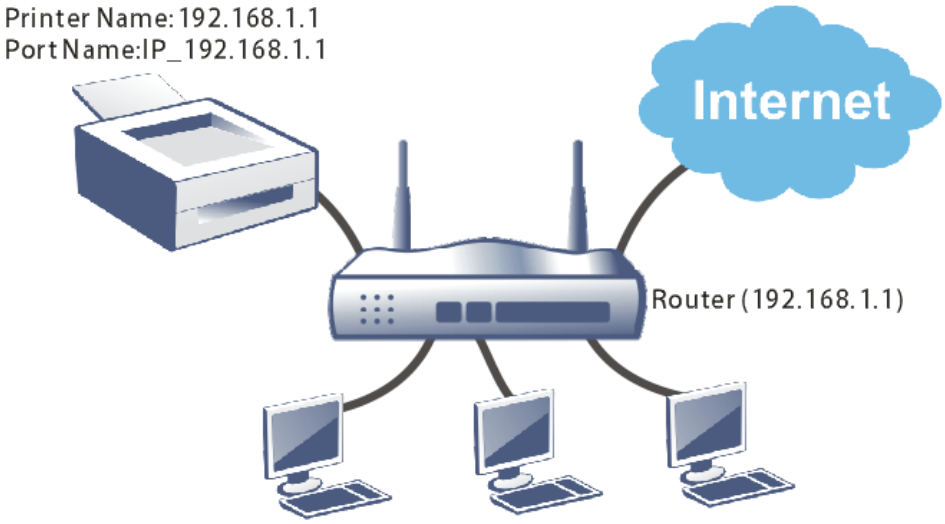



| | |
|---|---|
| **Info** | The recommended drill diameter shall be 6.5mm (1/4”). |

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

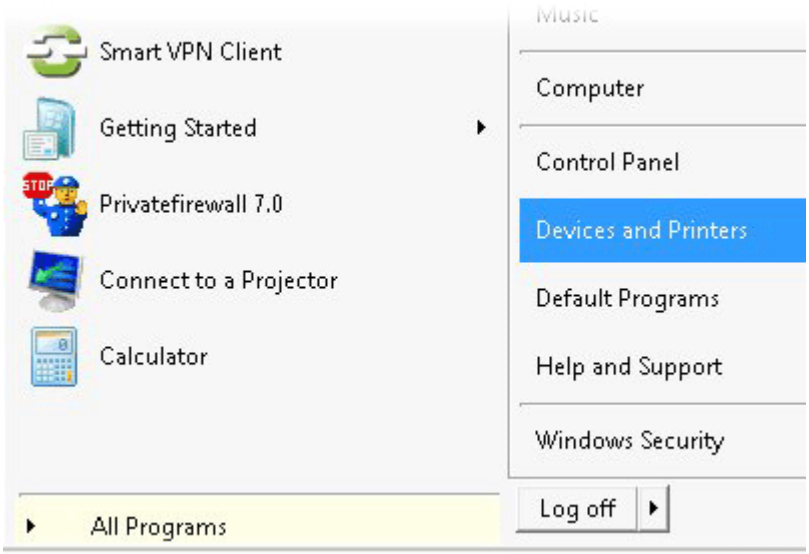
## I-2-3 Installing USB Printer to Vigor Router

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**.

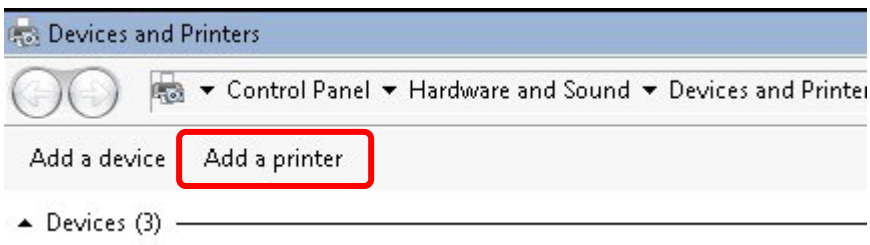



Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

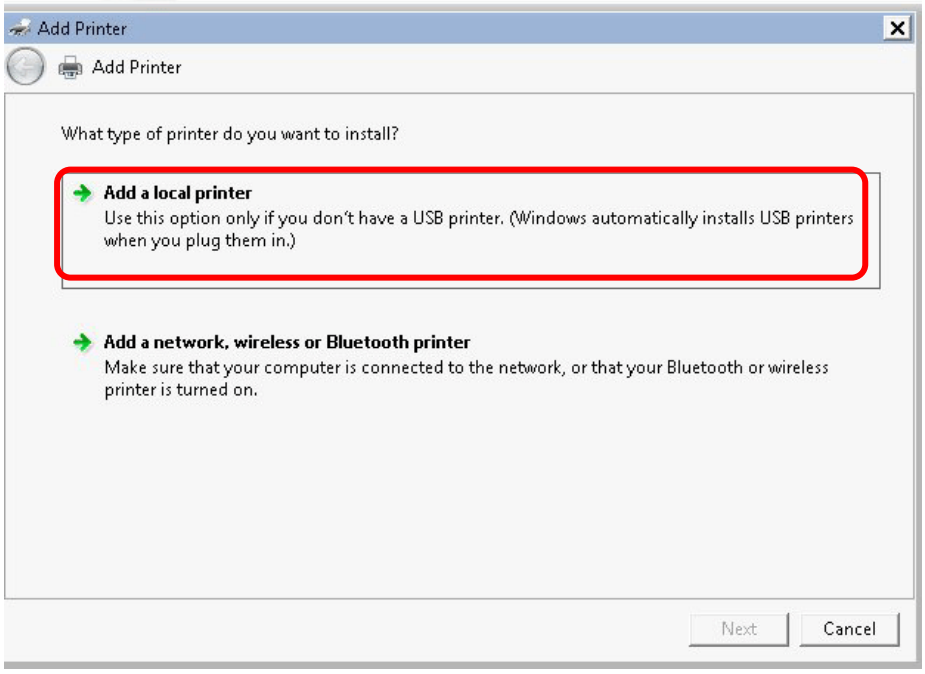
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



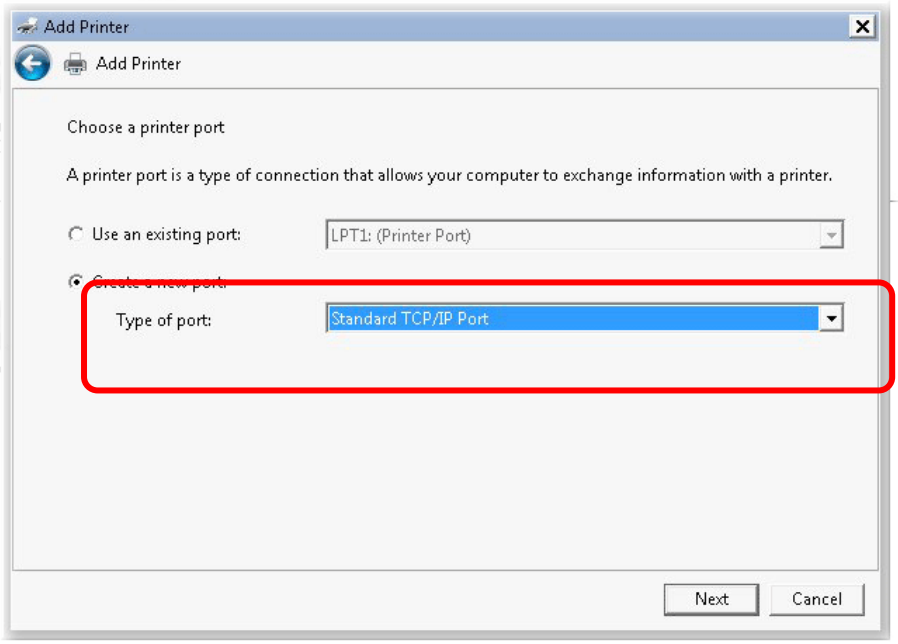

3. Click **Add a printer**.



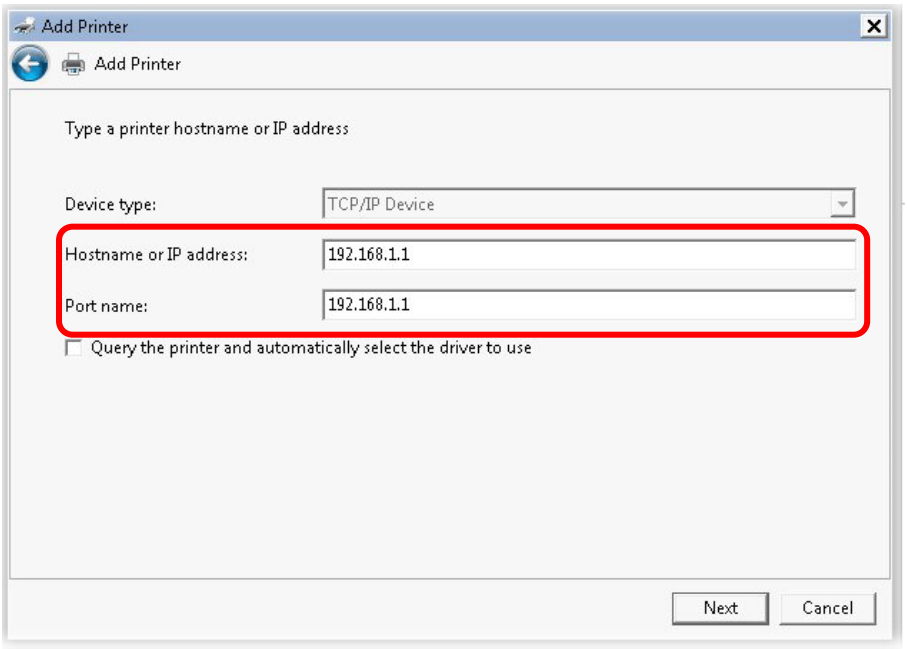
4. A dialog will appear. Click **Add a local printer** and click **Next**.



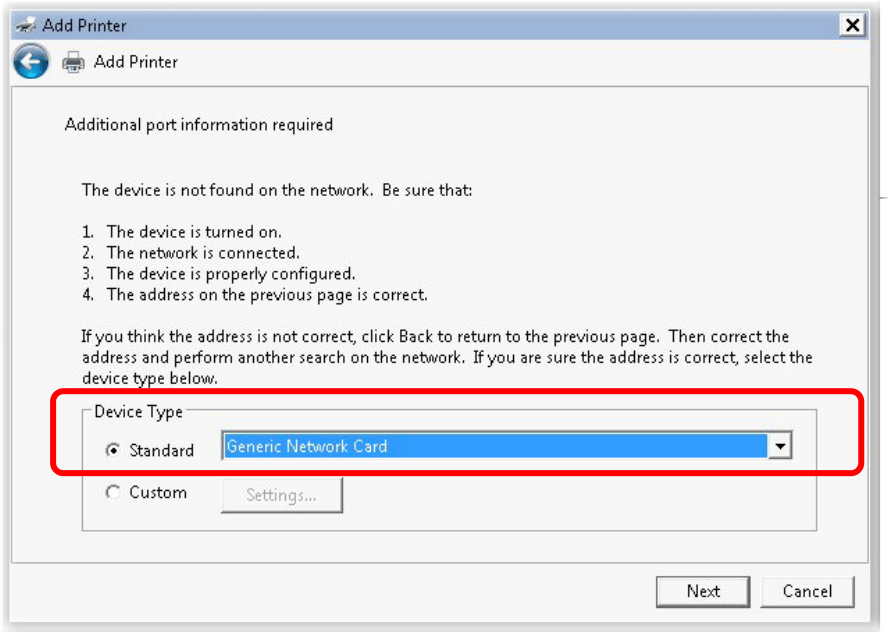

5. In this dialog, choose **Create a new port.** In the field of **Type of port,** use the drop down list to select **Standard TCP/IP Port**. Then, click **Next**.



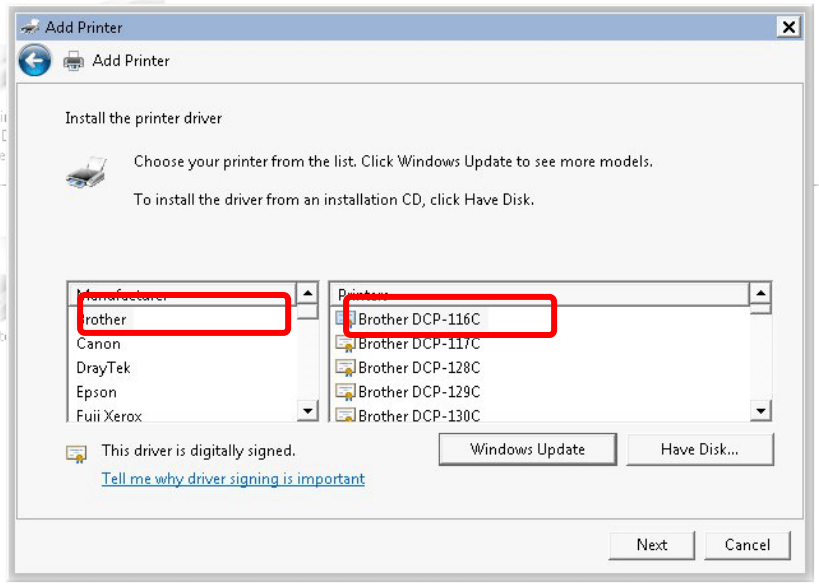
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.



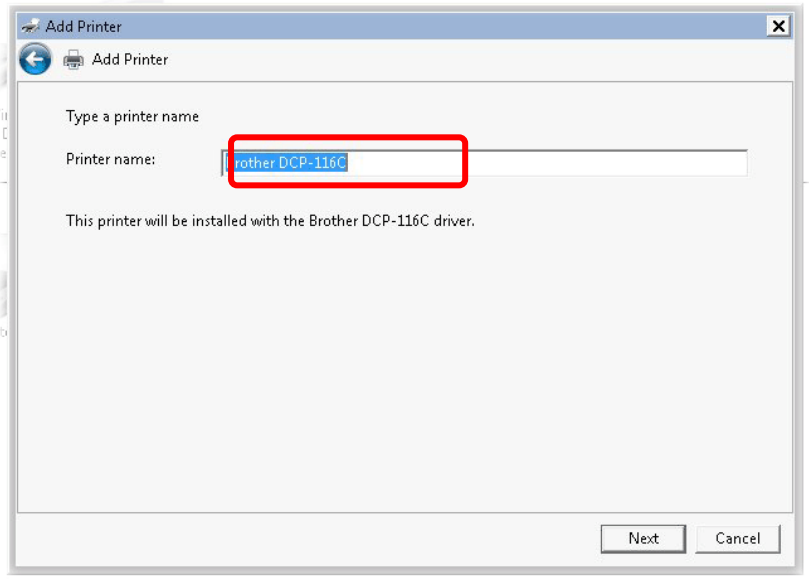

7. Click **Standard** and choose **Generic Network Card**.



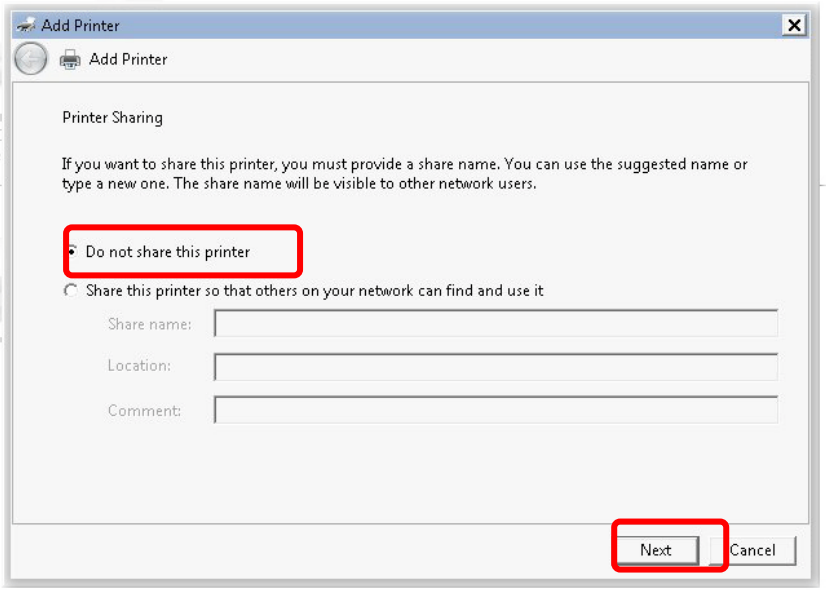
8. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



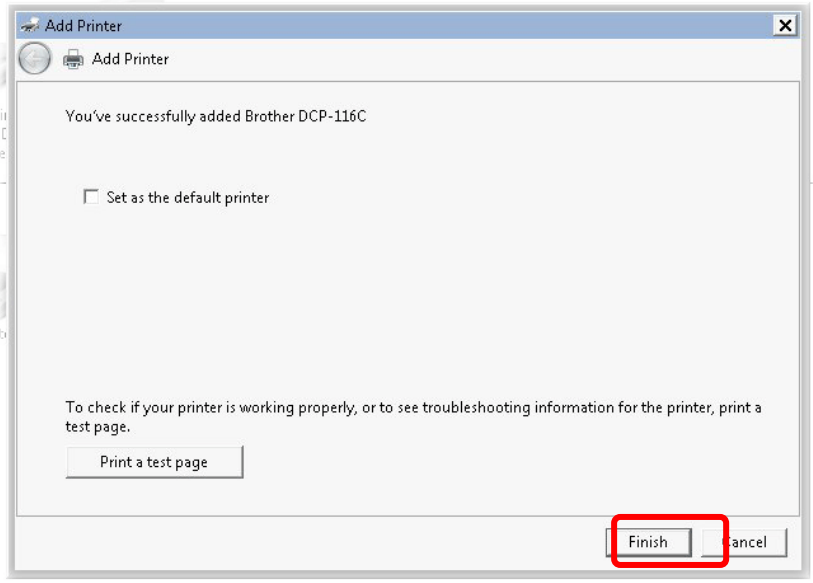

9. Type a name for the chosen printer. Click **Next.**



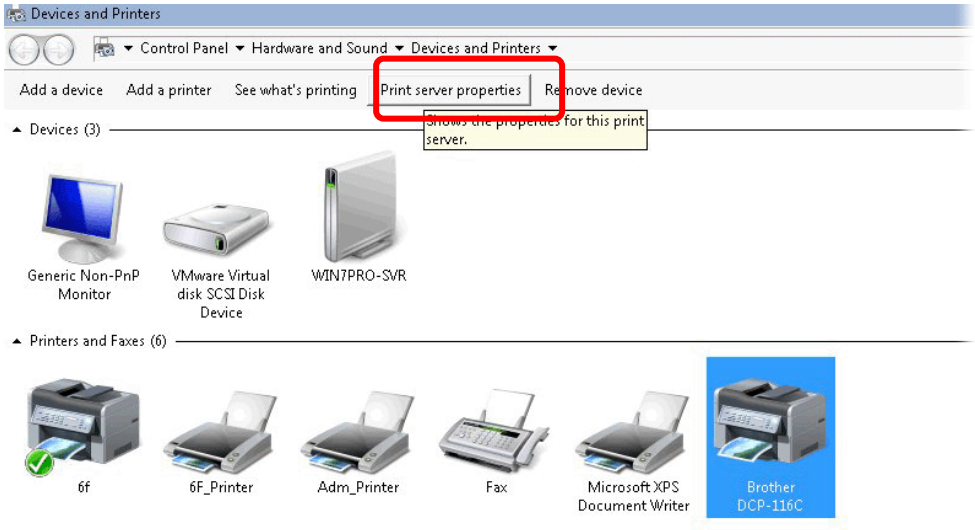
10. Choose **Do not share this printe**r and click **Next**.



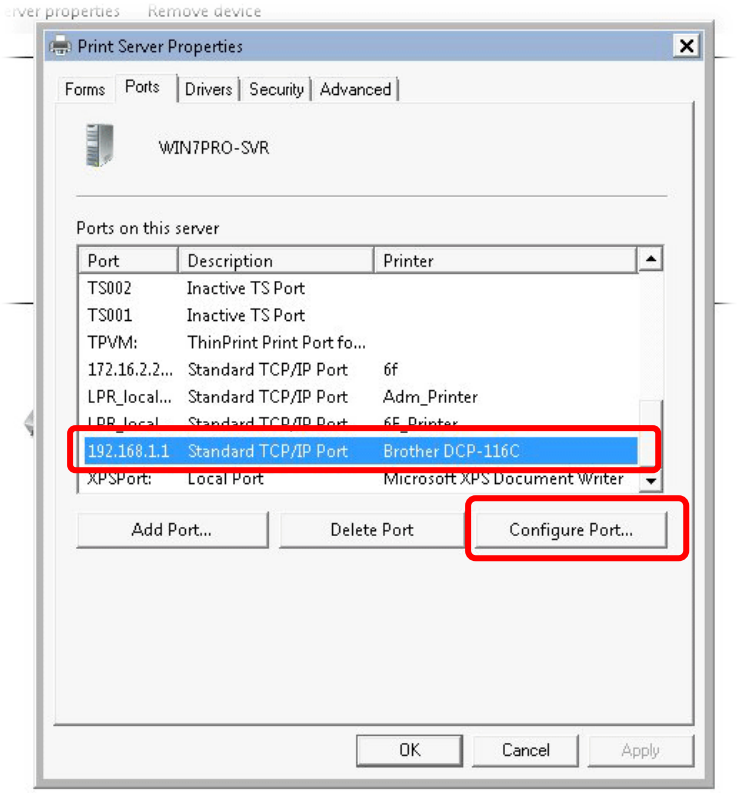

11. Then, in the following dialog, click **Finish**.



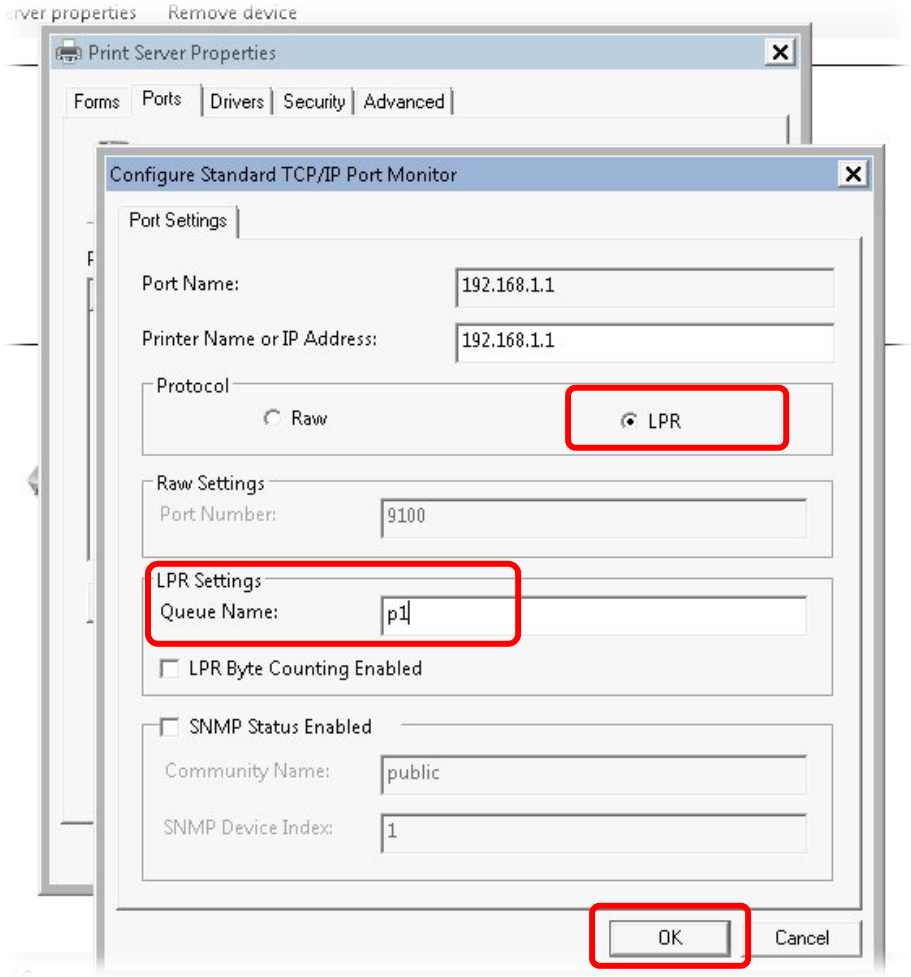
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.




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.

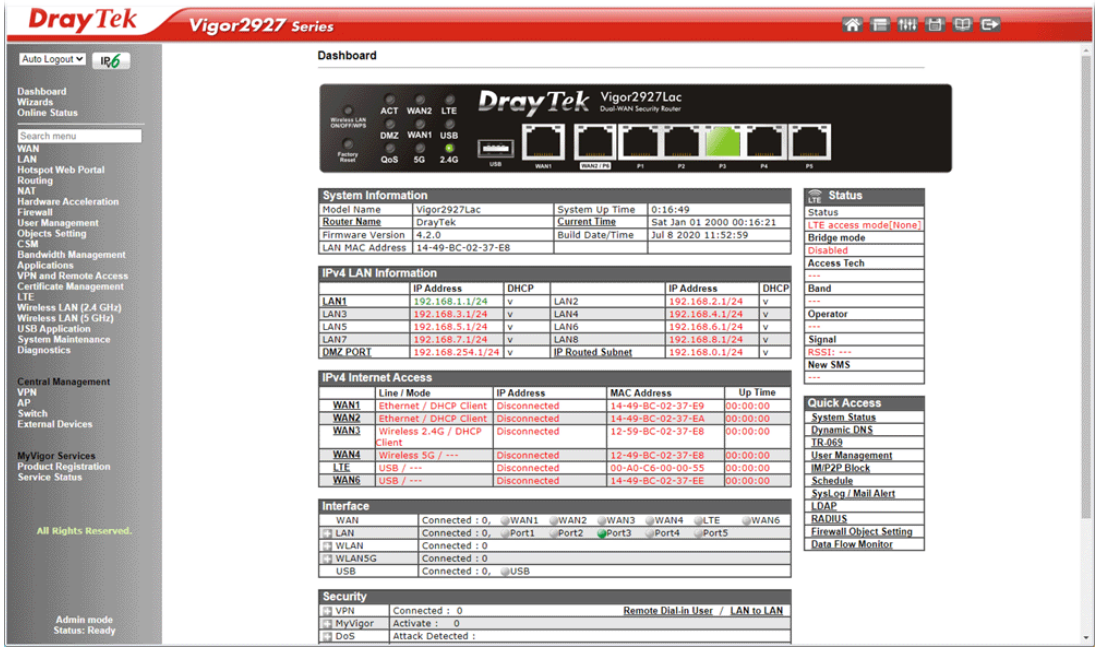
2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.




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

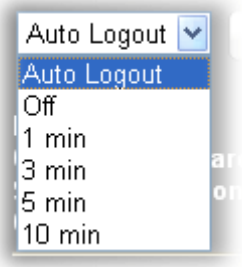
| **Info** | If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem. |
|---|---|

4. Now, the **Main Screen** will appear. Take Vigor2927ac as an example.




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

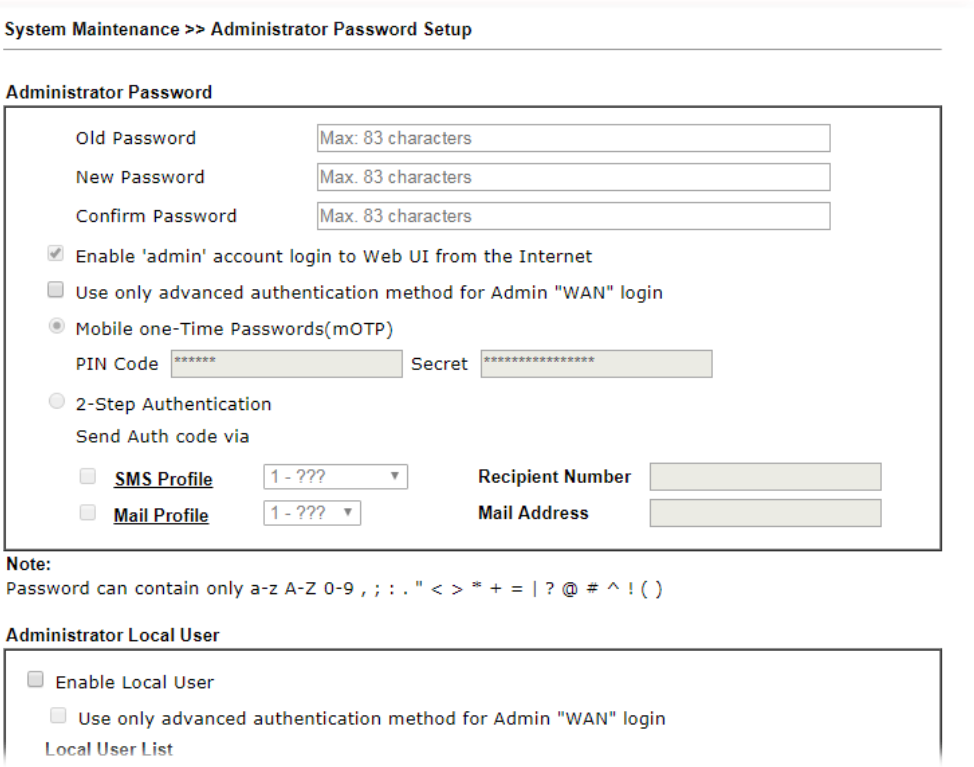
5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



# I-4 Changing Password

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

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




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

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

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

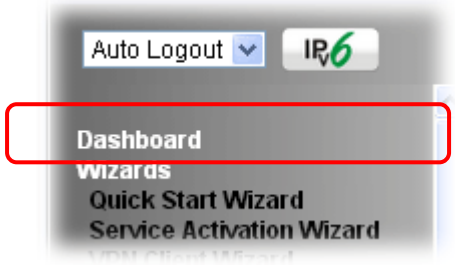



| | |
|---|---|
| Info | Even the password is changed, the Username for logging onto the web user interface is still “admin”. |

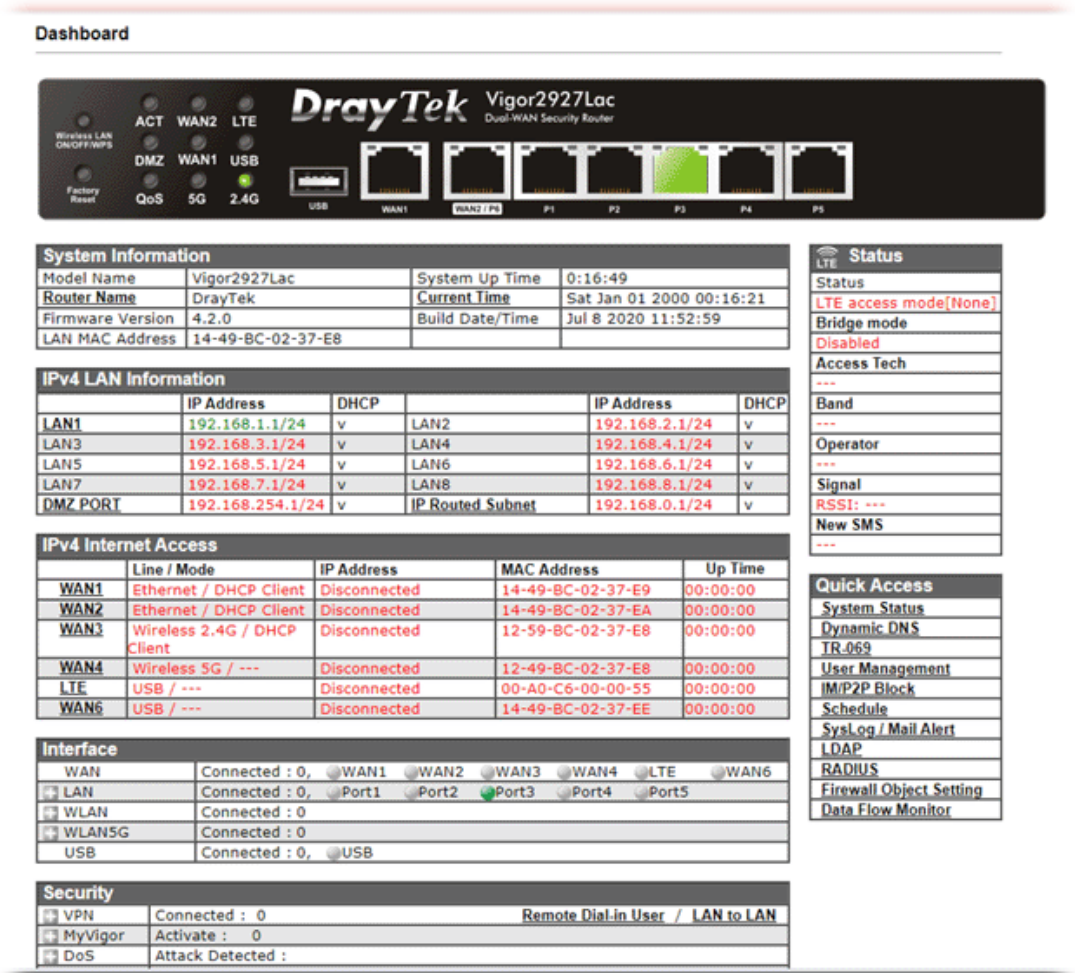
# I-5 Dashboard

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

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




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



## I-5-1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds. When you move and click the mouse cursor on LEDs (except ACT), USB ports, WAN2/P6, or LAN1 – LAN5 (P1~P5), related web setting page will be open for you to configure if required.

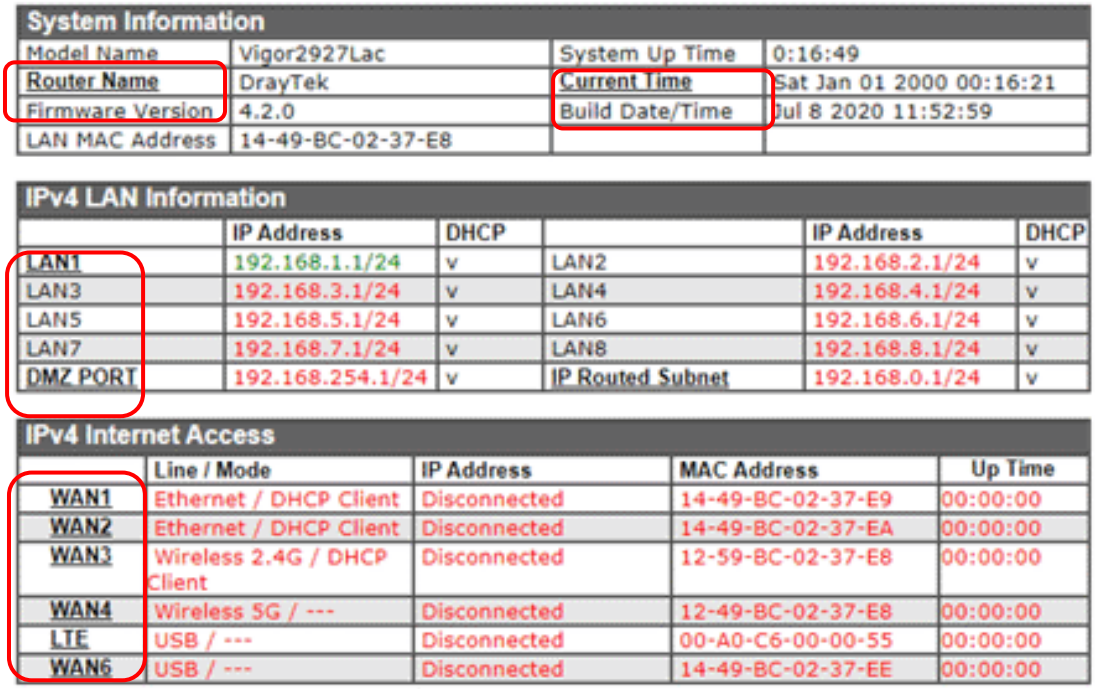



| Port | Color | Description |
|---|---|---|
| WAN2/P6 | Black | WAN2 port is disconnected. |
| | Green | WAN2 port is connected at 1 Gbps. |
| | Orange | WAN2 port is connected at 10/100 Mbps. |
| LAN 1 ~ 5 | Black | LAN port is disconnected. |
| | Green | LAN port is connected at 1 Gbps. |
| | Orange | LAN port is connected at 10/100 Mbps. |

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

## I-5-2 Name with a Link

A name with a link (e.g., Router Name, Current Time, WAN1~6 and etc.) below means you can click it to open the configuration page for modification.



**System Information**

| | | | |
|---|---|---|---|
| Model Name | Vigor2927Lac | System Up Time | 0:16:49 |
| Router Name | DrayTek | Current Time | Sat Jan 01 2000 00:16:21 |
| Firmware Version | 4.2.0 | Build Date/Time | Jul 8 2020 11:52:59 |
| LAN MAC Address | 14-49-BC-02-37-E8 | | |

**IPv4 LAN Information**

| | IP Address | DHCP | | IP Address | DHCP |
|---|---|---|---|---|---|
| LAN1 | 192.168.1.1/24 | v | LAN2 | 192.168.2.1/24 | v |
| LAN3 | 192.168.3.1/24 | v | LAN4 | 192.168.4.1/24 | v |
| LAN5 | 192.168.5.1/24 | v | LAN6 | 192.168.6.1/24 | v |
| LAN7 | 192.168.7.1/24 | v | LAN8 | 192.168.8.1/24 | v |
| DMZ PORT | 192.168.254.1/24 | v | IP Routed Subnet | 192.168.0.1/24 | v |

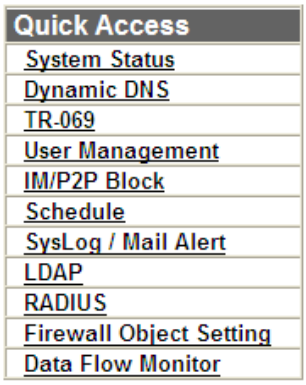
**IPv4 Internet Access**

| | Line / Mode | IP Address | MAC Address | Up Time |
|---|---|---|---|---|
| WAN1 | Ethernet / DHCP Client | Disconnected | 14-49-BC-02-37-E9 | 00:00:00 |
| WAN2 | Ethernet / DHCP Client | Disconnected | 14-49-BC-02-37-EA | 00:00:00 |
| WAN3 | Wireless 2.4G / DHCP Client | Disconnected | 12-59-BC-02-37-E8 | 00:00:00 |
| WAN4 | Wireless 5G / --- | Disconnected | 12-49-BC-02-37-E8 | 00:00:00 |
| LTE | USB / --- | Disconnected | 00-A0-C6-00-00-55 | 00:00:00 |
| WAN6 | USB / --- | Disconnected | 14-49-BC-02-37-EE | 00:00:00 |

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

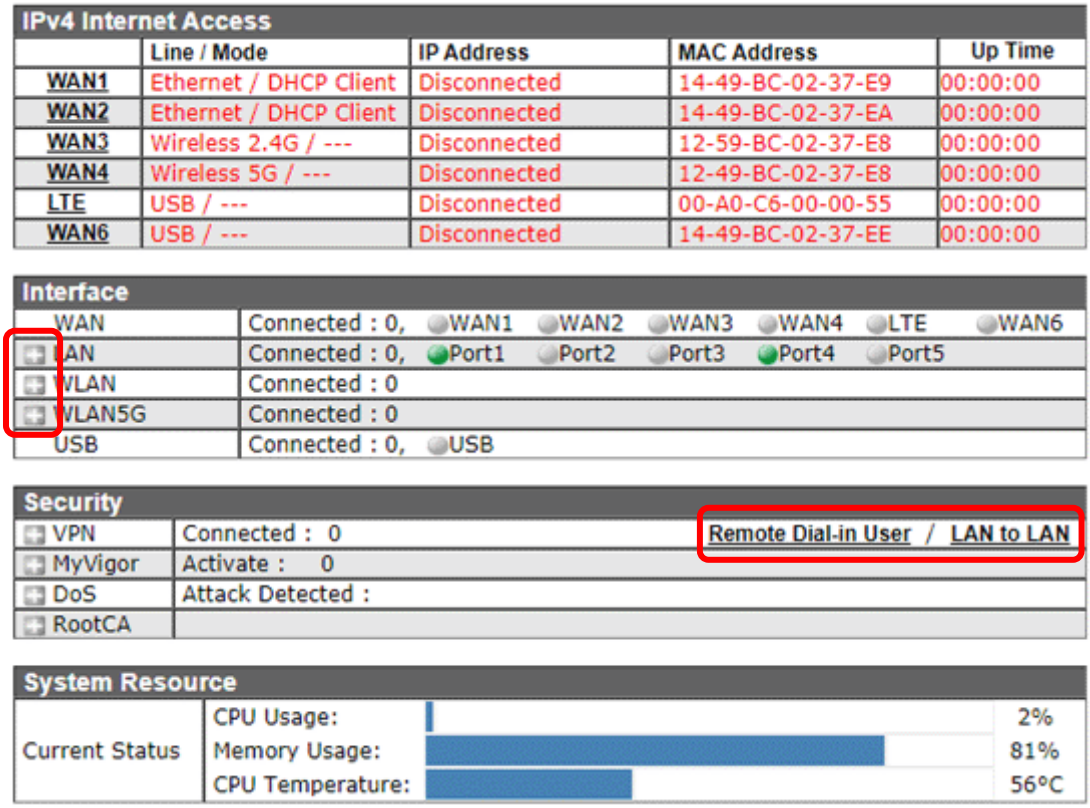
All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

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

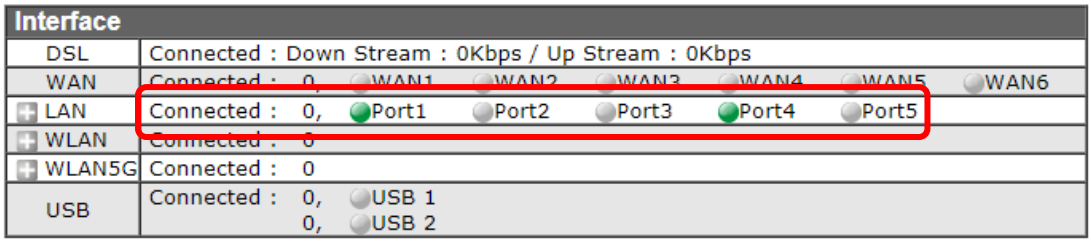



The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, LDAP, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be 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 VPN/LAN. Click it to review the VPN connection(s) used presently.



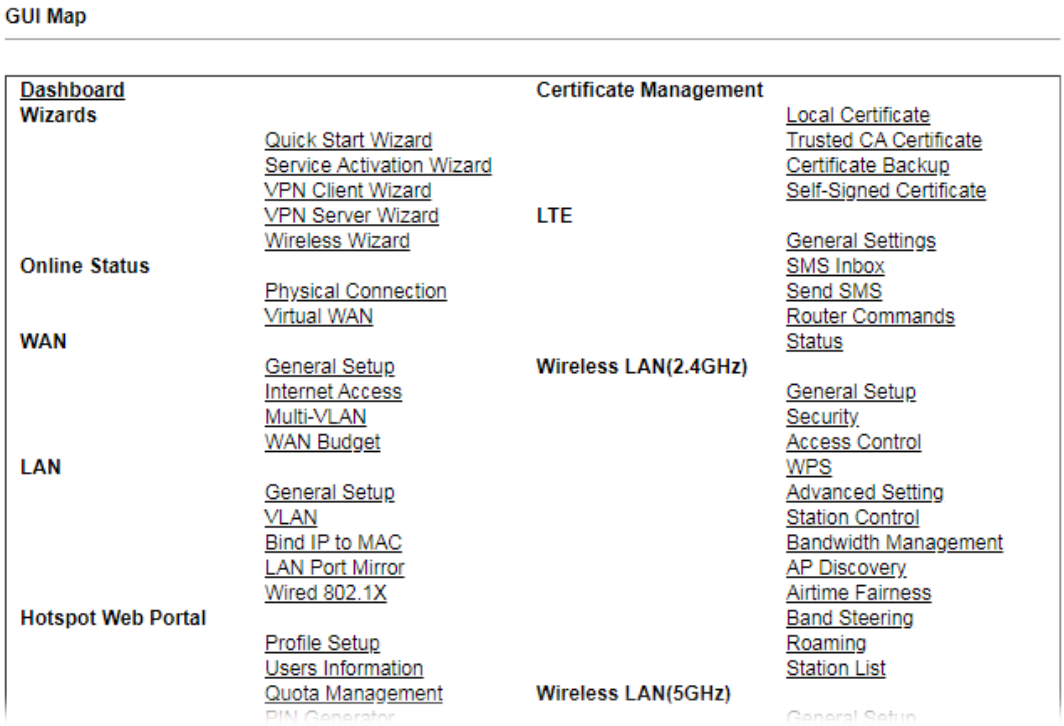

Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

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.

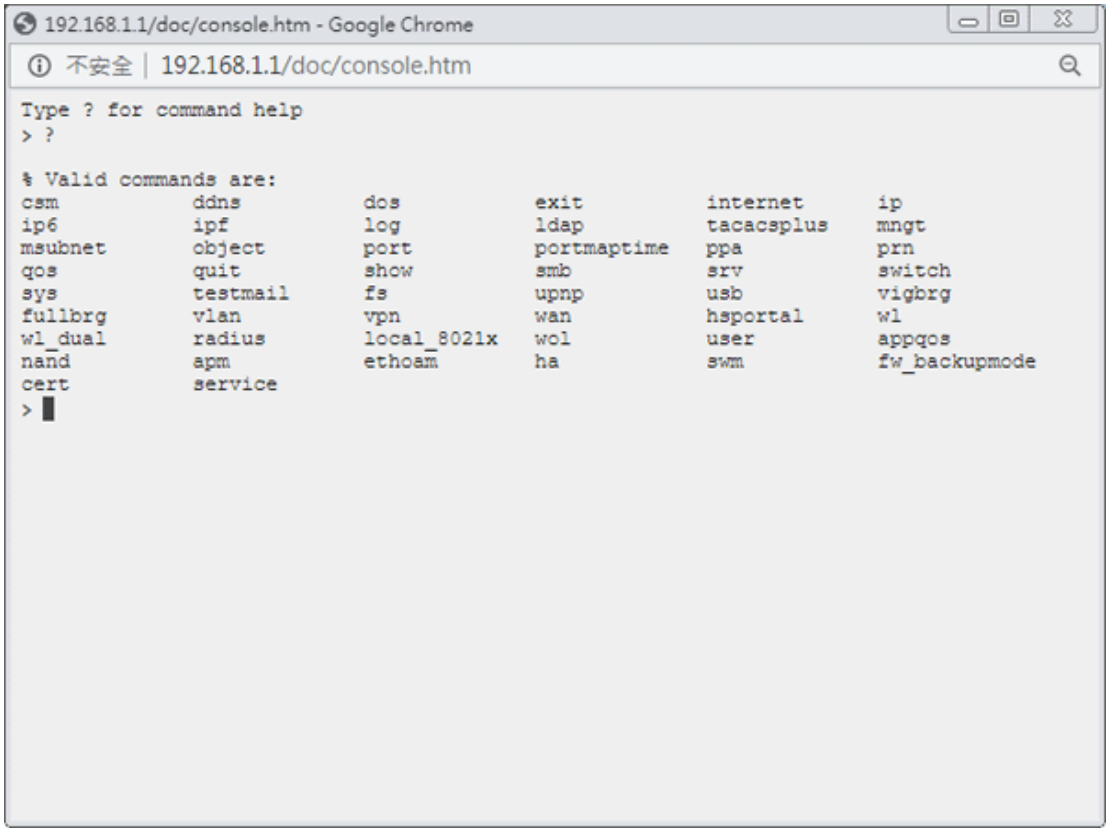


## I-5-5 Web Console




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 Logout




Click this icon to exit the web user interface.

# I-5-8 Online Status




## I-5-8-1 Physical Connection

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

### Physical Connection for IPv4 Protocol

Online Status

Physical Connection — System Uptime: 4days 23:49:54

IPv4 | IPv6

**LAN Status**

| IP Address | TX Packets | RX Packets | Router Primary DNS: | Router Secondary DNS: |
|---|---|---|---|---|
| 192.168.1.1 | 289,820 | 206,065 | 8.8.8.8 | 8.8.4.4 |

**WAN 1 Status** >> Renew

| Enable | Line | Name | Mode | Up Time | |
|---|---|---|---|---|---|
| Yes | Ethernet | | DHCP Client | 00:00:00 | |
| IP | GW IP | TX Bytes | TX Rate(bps) | RX Bytes | RX Rate(bps) |
| --- | --- | 0 (B) | 0 | 0 (B) | 0 |

**WAN 2 Status** >> Renew

| Enable | Line | Name | Mode | Up Time | |
|---|---|---|---|---|---|
| Yes | Ethernet | | DHCP Client | 00:00:00 | |
| IP | GW IP | TX Bytes | TX Rate(bps) | RX Bytes | RX Rate(bps) |
| --- | --- | 0 (B) | 0 | 0 (B) | 0 |

**WAN 3 Status**

| Enable | Line | Name | Mode | Up Time | |
|---|---|---|---|---|---|
| No | Wireless 2.4G | | --- | 00:00:00 | |
| IP | GW IP | TX Bytes | TX Rate(bps) | RX Bytes | RX Rate(bps) |
| --- | --- | 0 (B) | 0 | 0 (B) | 0 |

| SSID | Channel | Security | PHY Mode | Rate | Signal Strength |
|---|---|---|---|---|---|
| | 6 | Disable | --- | --- | 0% |

**WAN 4 Status**

| Enable | Line | Name | Mode | Up Time | |
|---|---|---|---|---|---|
| No | Wireless 5G | | --- | 00:00:00 | |
| IP | GW IP | TX Bytes | TX Rate(bps) | RX Bytes | RX Rate(bps) |
| --- | --- | 0 | 0 | 0 | 0 |

| SSID | Channel | Security | PHY Mode | Rate | Signal Strength |
|---|---|---|---|---|---|
| | 36 | Disable | --- | --- | 0% |

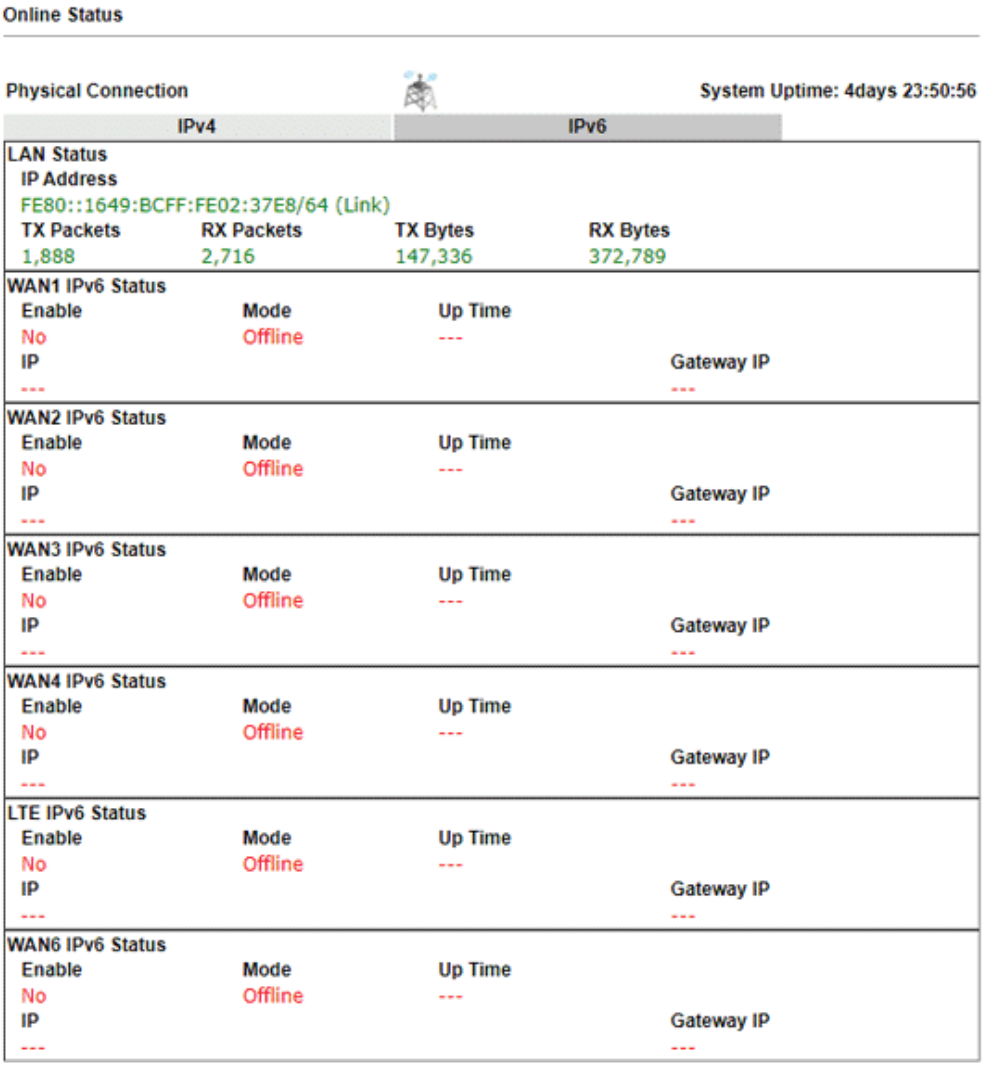
**LTE Status**

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

**WAN 6 Status**

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

Physical Connection for IPv6 Protocol




Detailed explanation (for IPv4) is shown below:

| Item | Description |
|---|---|
| **LAN Status** | **Primary DNS-**Displays the primary DNS server address for WAN interface.<br>**Secondary DNS -**Displays the secondary DNS server address for WAN interface.<br>**IP Address**-Displays the IP address of the LAN interface.<br>**TX Packets**-Displays the total transmitted packets at the LAN interface.<br>**RX Packets**-Displays the total received packets at the LAN interface. |
| **WAN1/WAN2/WAN3 /WAN4/WAN5/WAN6 Status** | **Enable – Yes** in red means such interface is available but not enabled. **Yes** in green means such interface is enabled.<br>**Mode** - Displays the type of WAN connection (e.g., PPPoE).<br>**Up Time** - Displays the total uptime of the interface.<br>**IP** - Displays the IP address of the WAN interface.<br>**GW IP** - Displays the IP address of the default gateway.<br>**TX Packets** - Displays the total transmitted packets at the |

| Item | Description |
|---|---|
| | WAN interface.<br>**TX Rate** - Displays the speed of transmitted octets at the WAN interface.<br>**RX Packets** - Displays the total number of received packets at the WAN interface.<br>**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..<br>**TX Packets**-Displays the total transmitted packets at the LAN interface.<br>**RX Packets**-Displays the total received packets at the LAN interface.<br>**TX Bytes** - Displays the speed of transmitted octets at the LAN interface.<br>**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.<br>**Mode** - Displays the type of WAN connection (e.g., TSPC).<br>**Up Time** - Displays the total uptime of the interface.<br>**IP** - Displays the IP address of the WAN interface.<br>**Gateway IP** - Displays the IP address of the default gateway. |

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

### I-5-8-2 Virtual WAN

Such page displays the virtual WAN connection information.

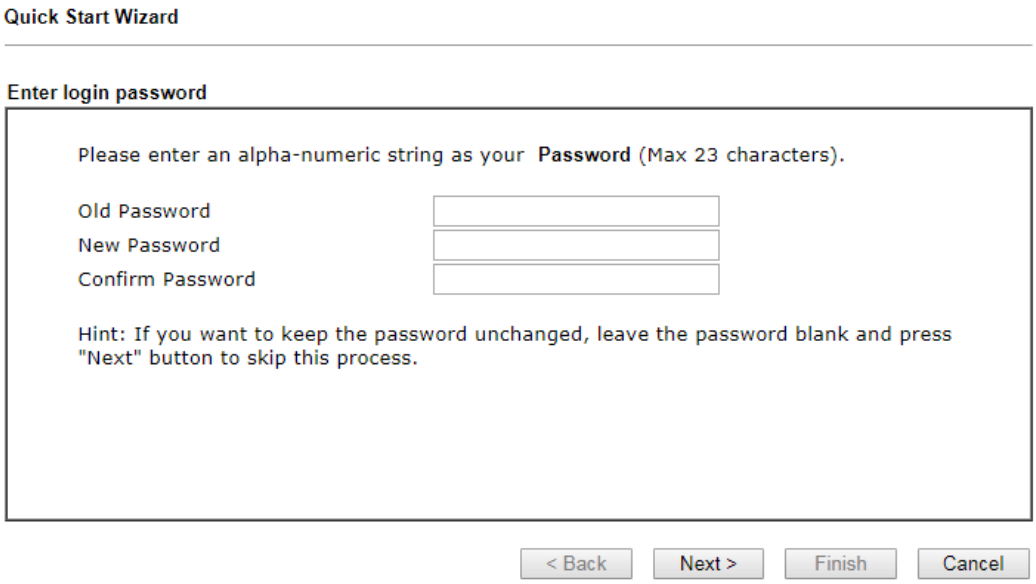
Virtual WAN are used by TR-069 management, VoIP service and so on.

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

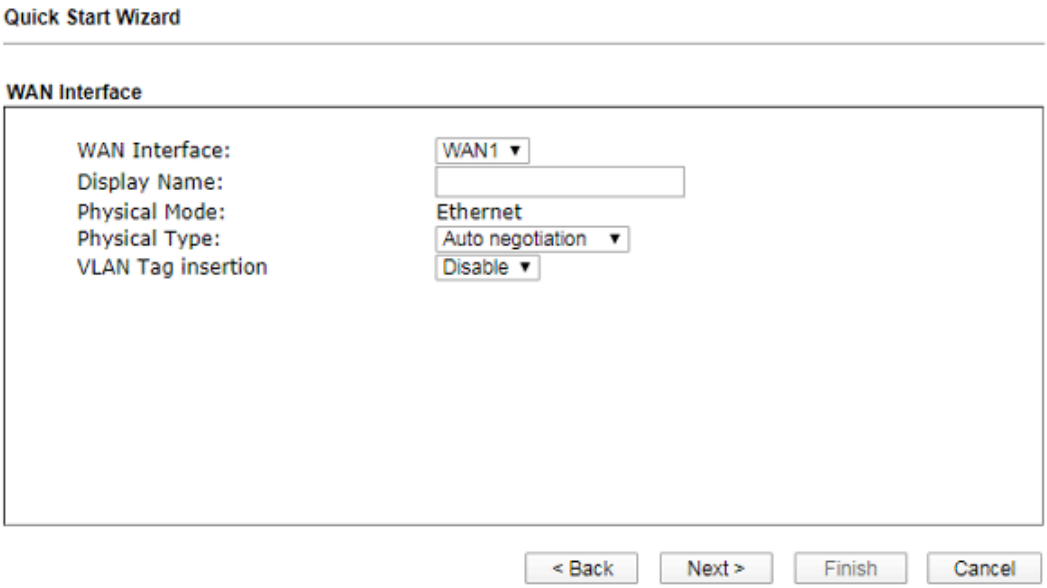
# I-6 Quick Start Wizard

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**.



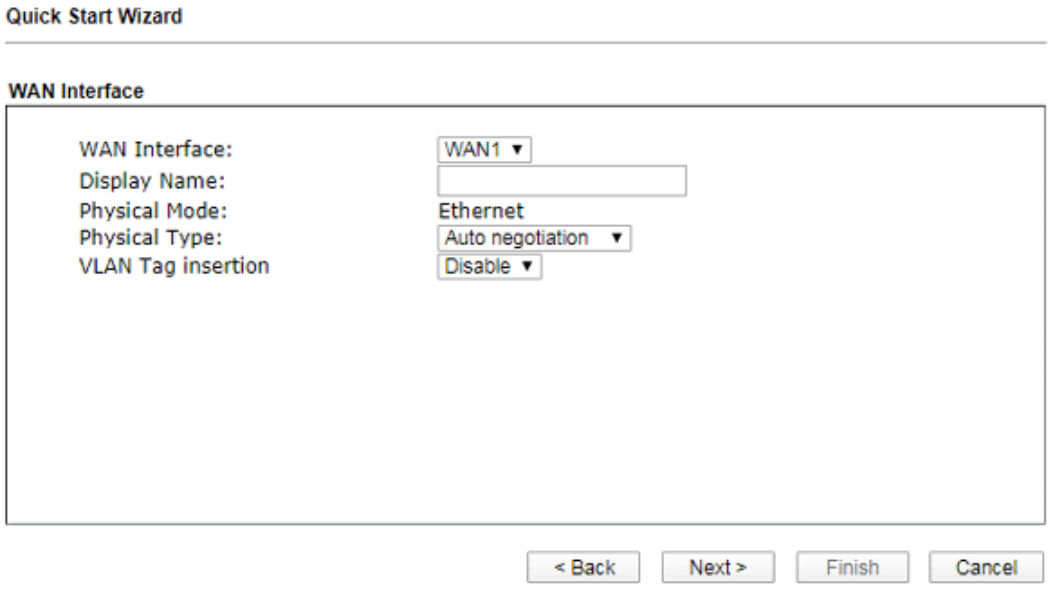

On the next page as shown below, please select the WAN interface that you use. If Ethernet interface is used, please choose WAN1/WAN2; if 3G USB modem is used, please choose WAN3 or WAN4. Then click **Next** for next step.




WAN1, WAN2, WAN3, WAN4, WAN5 and WAN6 will bring up different configuration page. Refer to the following for detailed information.

## I-6-1 For WAN1/WAN2 (Ethernet)

WAN2 can be configured for physical mode of Ethernet.



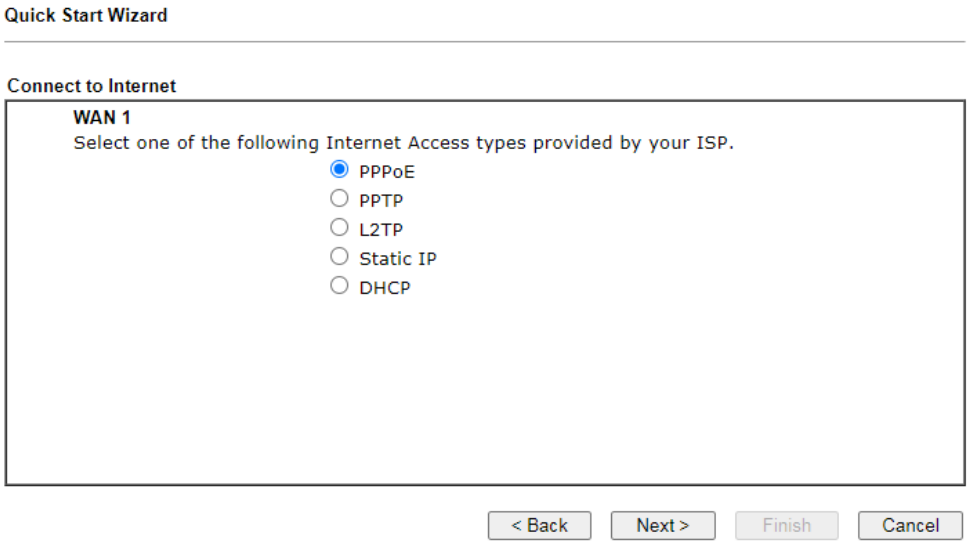

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Display Name** | Enter a name for the router. |
| **Physical Type** | This setting is available when **Ethernet** is selected as **Physical Mode**. In general, **Auto negotiation** is suggested. |
| **VLAN Tag insertion** | The settings configured in this field are available when **Ethernet** is selected as **Physical Mode**.<br>**Disable** – Disable the function of VLAN with tag.<br>**Enable** – Enable the function of VLAN with tag.<br>The router will add specific VLAN number to all packets on the WAN while sending them out.<br>Please Enter the tag value and specify the priority for the packets sending by WAN2.<br>● **Tag value** – Enter the value as the VLAN ID number. The range is form 0 to 4095.<br>● **Priority** – Enter the packet priority number for such VLAN. The range is from 0 to 7. |

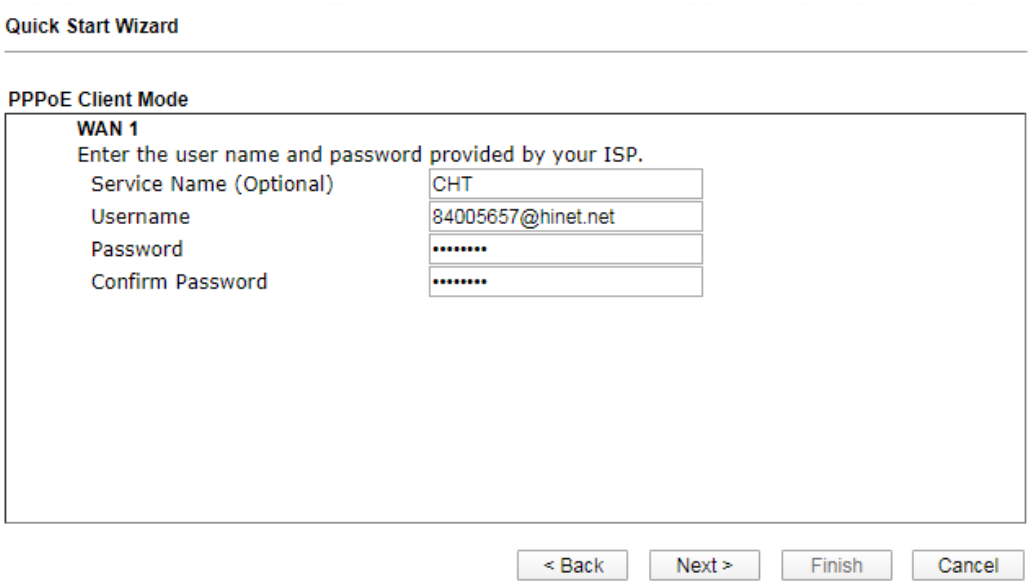
On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

## Ethernet WAN1/2 - PPPoE

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




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

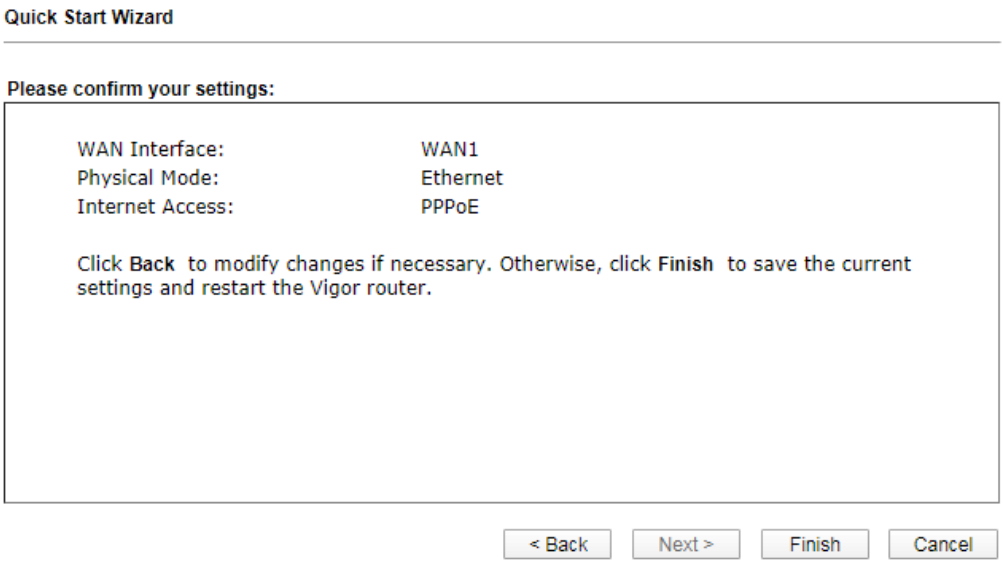



Available settings are explained as follows:

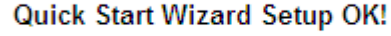
| Item | Description |
|---|---|
| **Service Name (Optional)** | Enter the description of the specific network service. |
| **Username** | Assign a specific valid user name provided by the ISP.<br>**Note:** The maximum length of the user name you can set is 63 characters. |
| **Password** | Assign a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

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

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



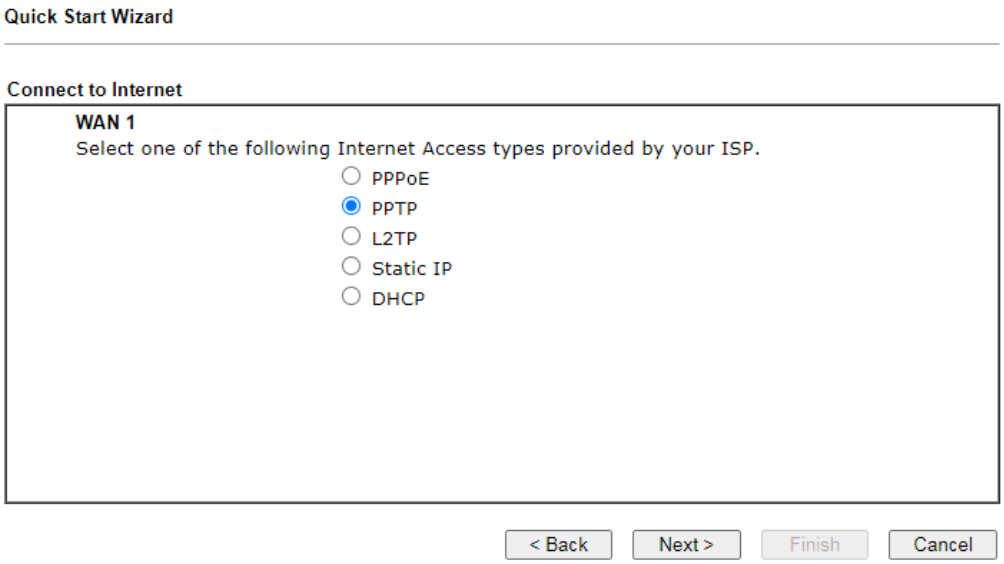

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



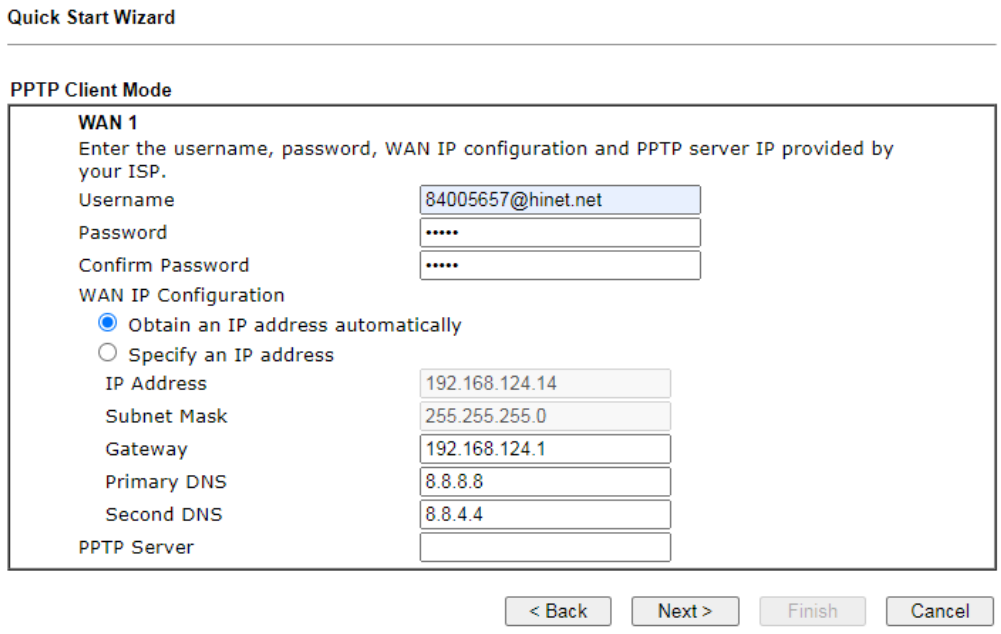

5. Now, you can enjoy surfing on the Internet.

## Ethernet WAN1/2 - PPTP/L2TP

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




2. Click **PPTP/L2TP** 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.<br>**Note:** The maximum length of the user name you can set is 63 characters. |
| **Password** | Assign a valid password provided by the ISP.<br>**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.<br>**Specify an IP address** – You have to type relational settings manually.<br>**IP Address** - Enter the IP address.<br>**Subnet Mask** – Enter the subnet mask.<br>Gateway – Enter the IP address of the gateway.<br>**Primary DNS** – Enter the primary IP address for the router.<br>**Second DNS** – Enter secondary IP address for necessity in the future. |
| **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 Enter the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.



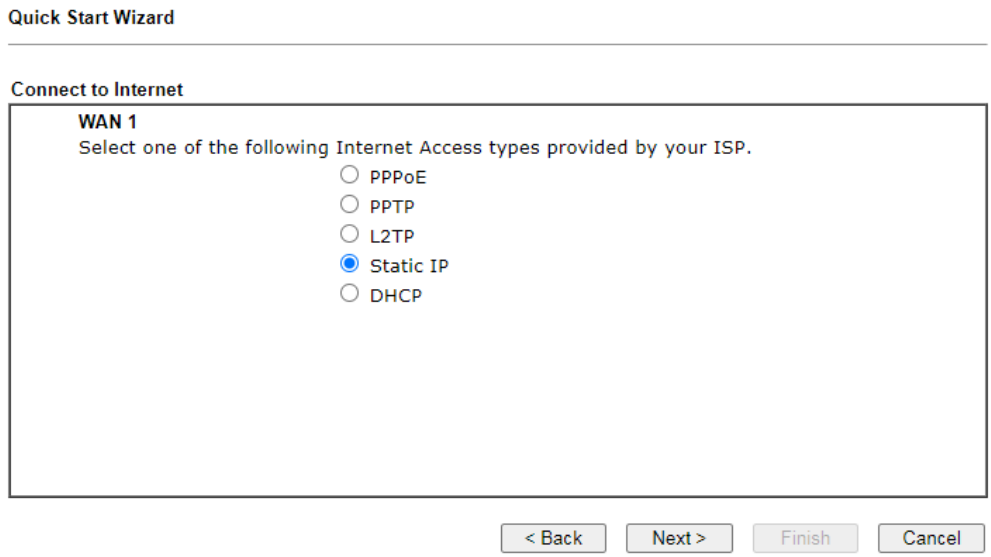

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



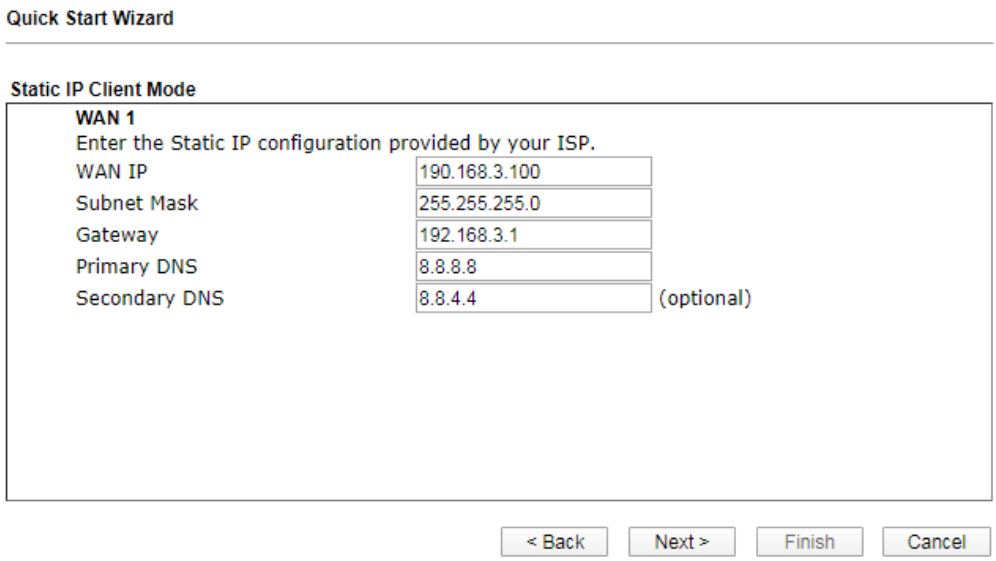

5. Now, you can enjoy surfing on the Internet.

## Ethernet WAN1/2 - Static IP

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




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

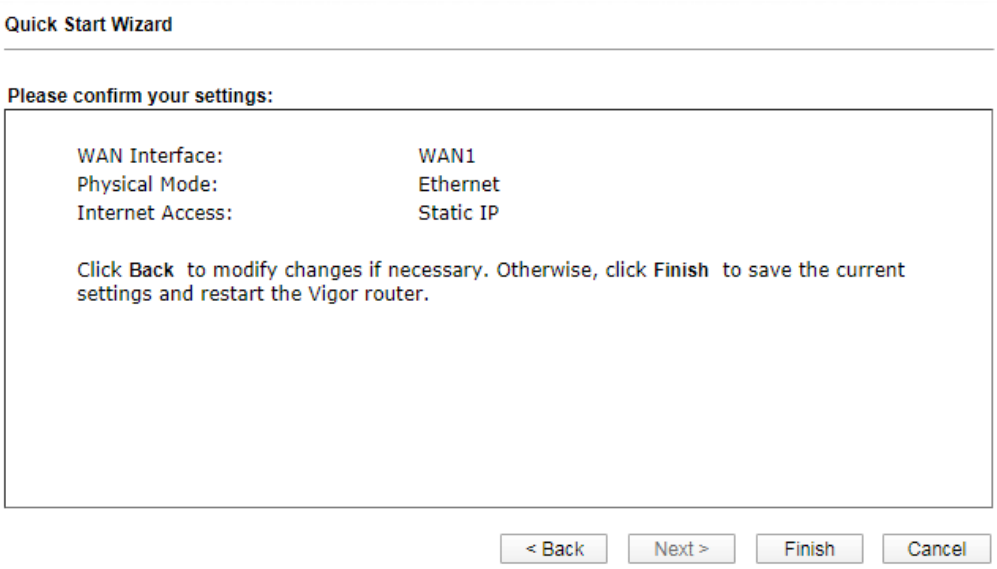



Available settings are explained as follows:

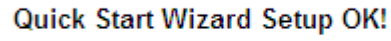
| Item | Description |
|---|---|
| **WAN IP** | Enter the IP address. |
| **Subnet Mask** | Enter the subnet mask. |
| **Gateway** | Enter the IP address of gateway. |
| **Primary DNS** | Enter the primary IP address for the router. |
| **Secondary DNS** | Enter the secondary IP address for necessity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

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

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



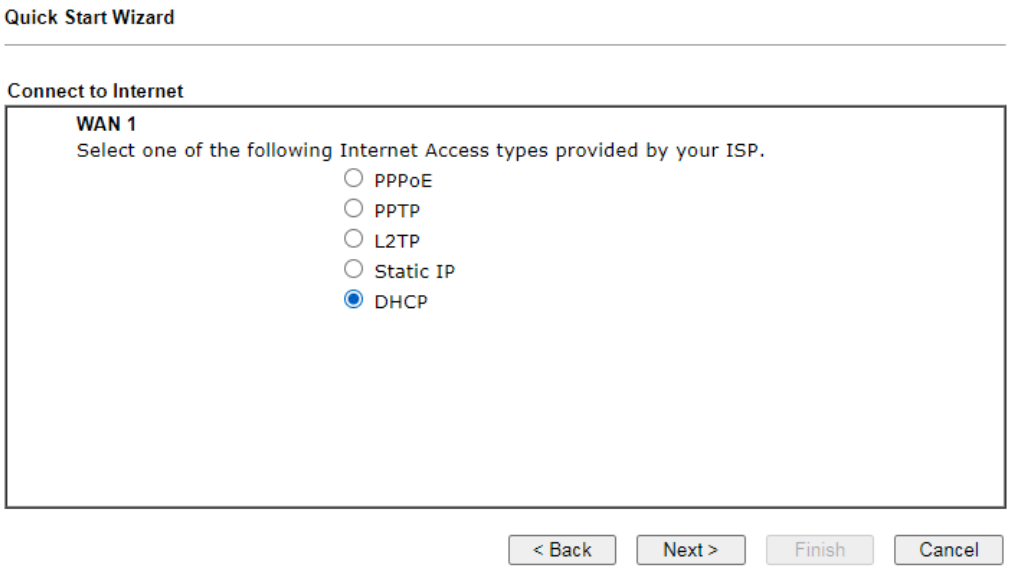

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.



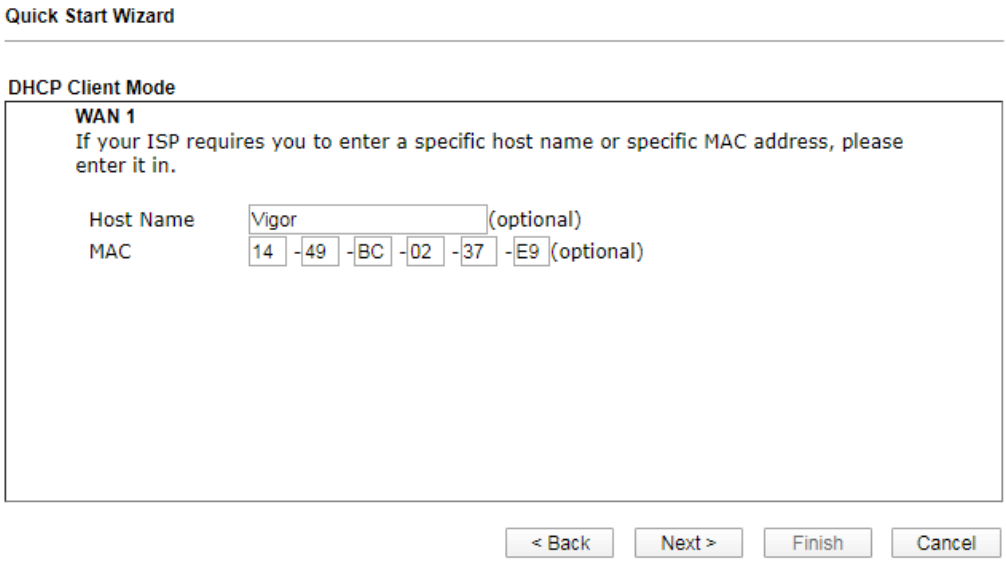

5. Now, you can enjoy surfing on the Internet.

## Ethernet WAN1/2 - DHCP

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




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

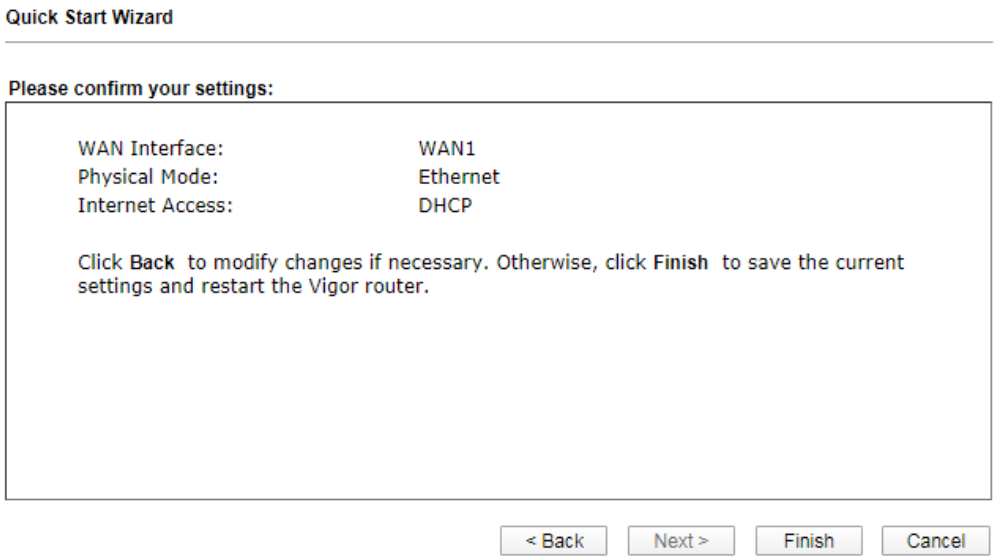



Available settings are explained as follows:

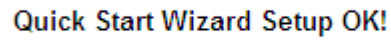
| Item | Description |
|---|---|
| **Host Name** | Enter the name of the host.<br>**Note:** The maximum length of the host name you can set is 39 characters. |
| **MAC** | Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.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

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

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




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



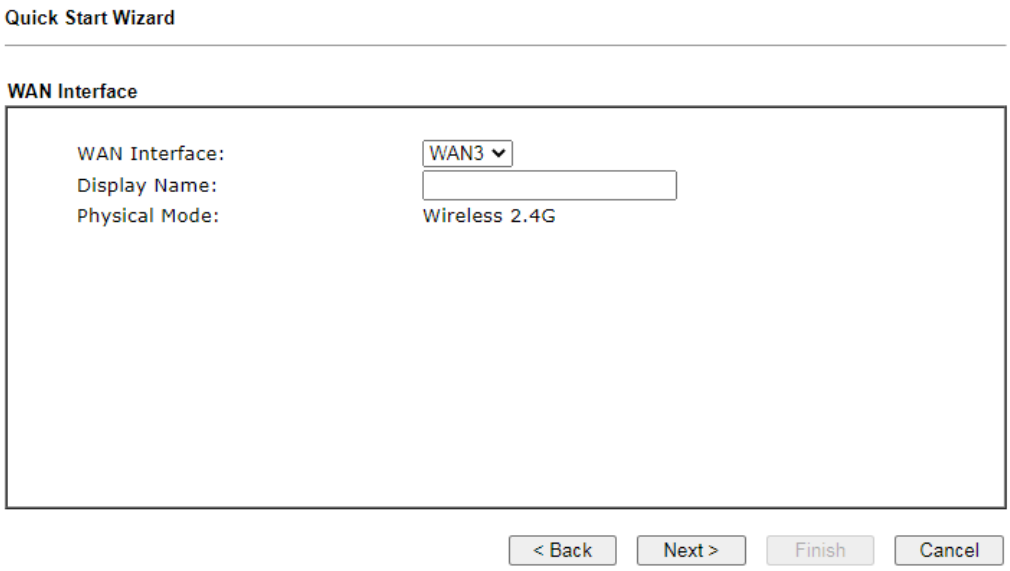

5. Now, you can enjoy surfing on the Internet.

## I-6-2 For WAN3/WAN4 (Wireless 2.4G/Wireless 5G)

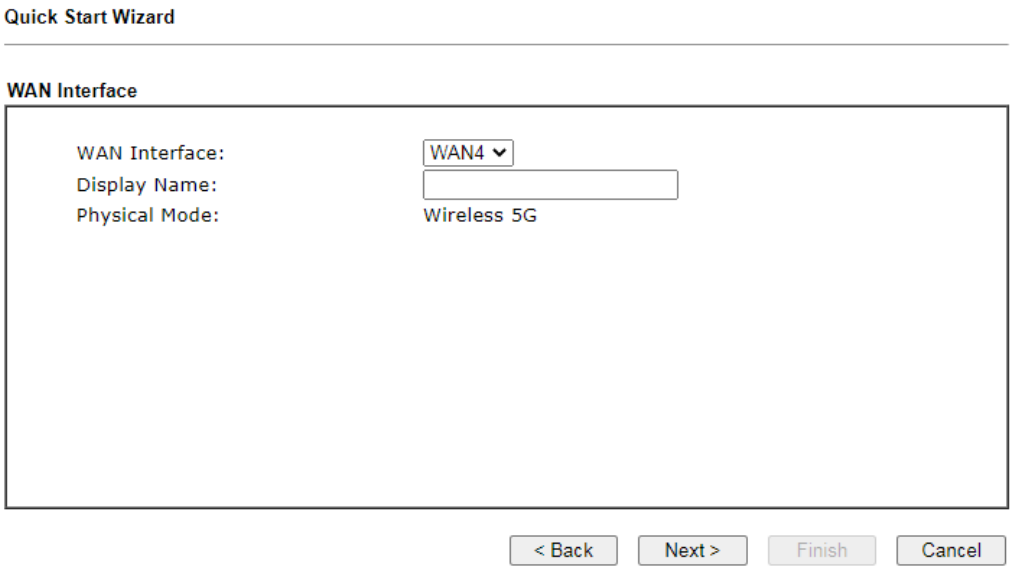
WAN3/WAN4 shall be used for wireless (2.4G or 5G) connection.

### Wireless WAN3/WAN4 - Static IP

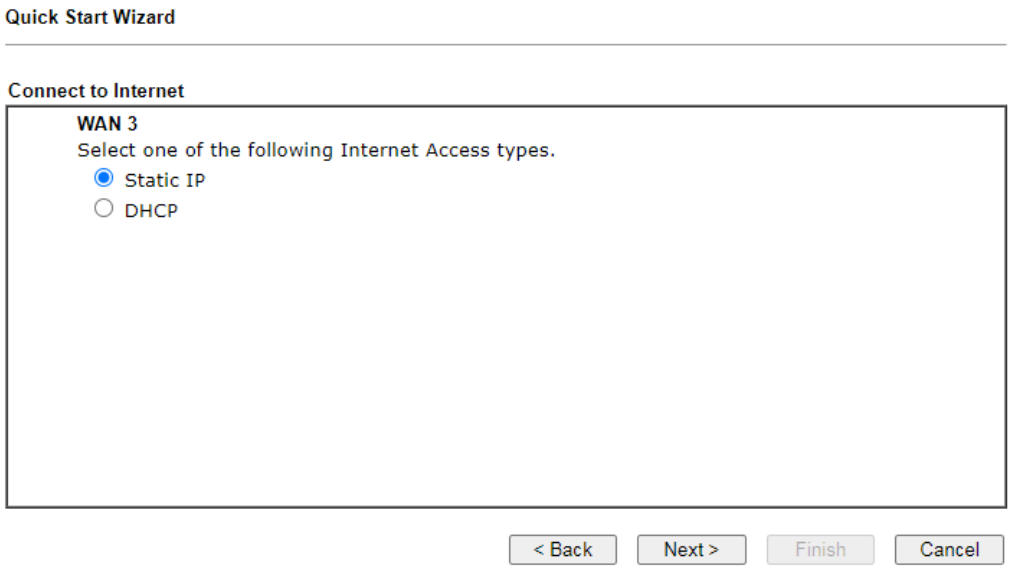
1. Choose **WAN3/WAN4** as WAN Interface and chooose **Wireless 2.4G** or **Wireless 5G** as the physical mode.



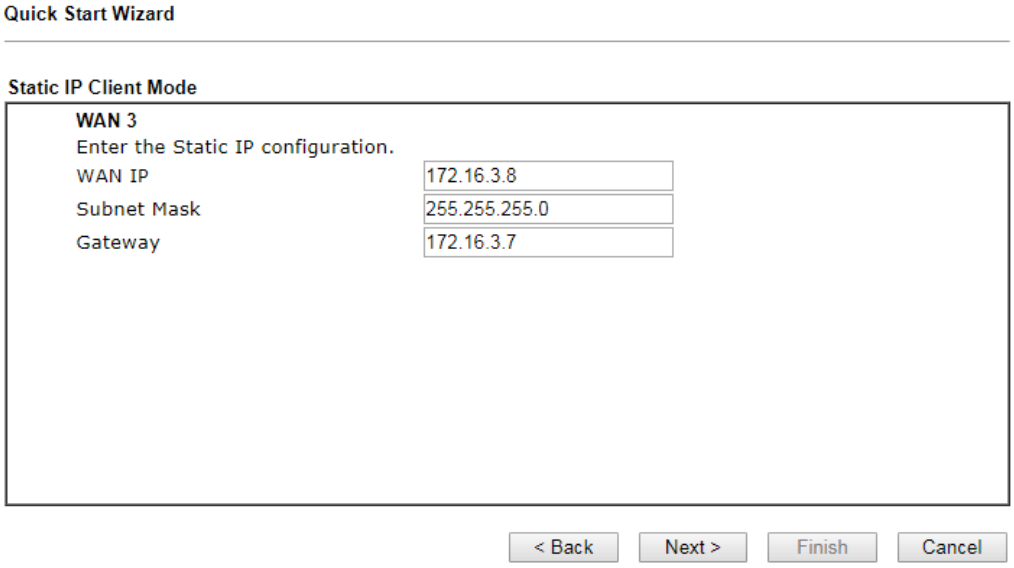

or



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



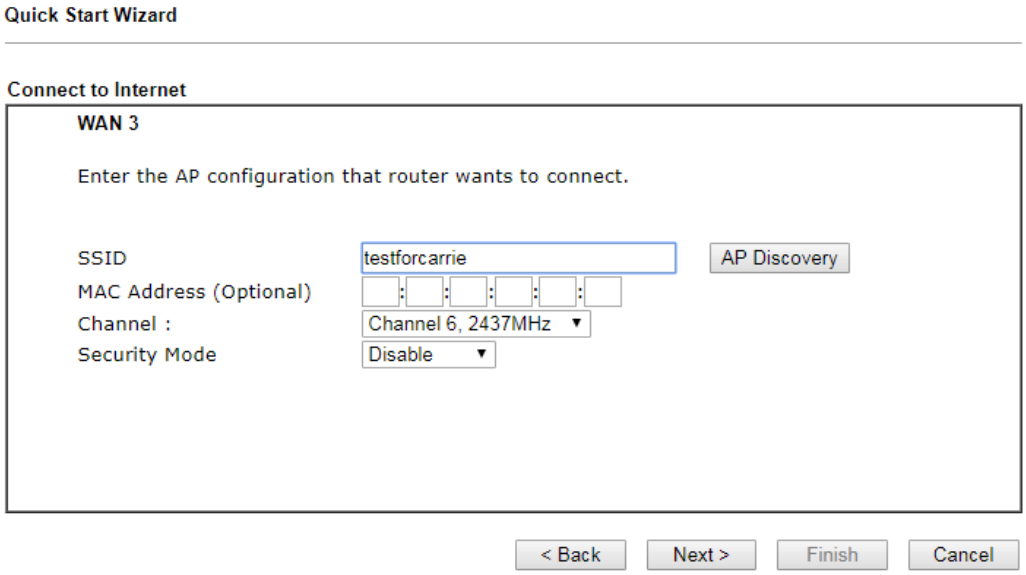

3. After click **Static IP** as the Internet Access type, you will get the following page. Enter the required information and click **Next** to continue.




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. |
| **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. |

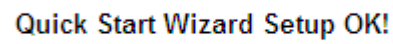
4. From the following page, enter the SSID of an existed AP as the wireless connection server for this WAN. Or click **AP Discovery** to find an access point as the server for this WAN interface. Click **Next** to continue.




5. Then, a summary of the connection will be shown on the screen.



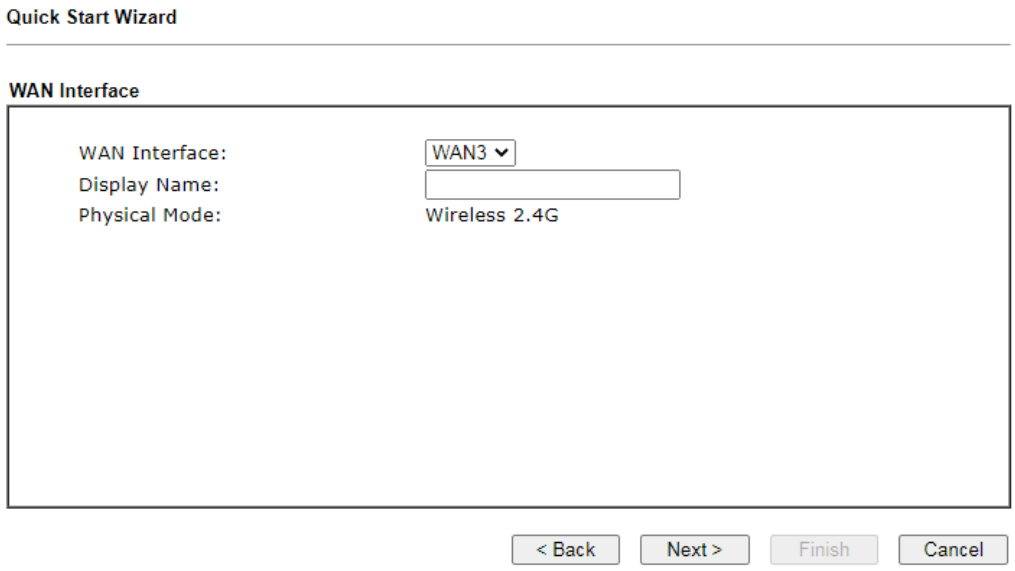

6. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.




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

## Wireless WAN3/WAN4 - DHCP

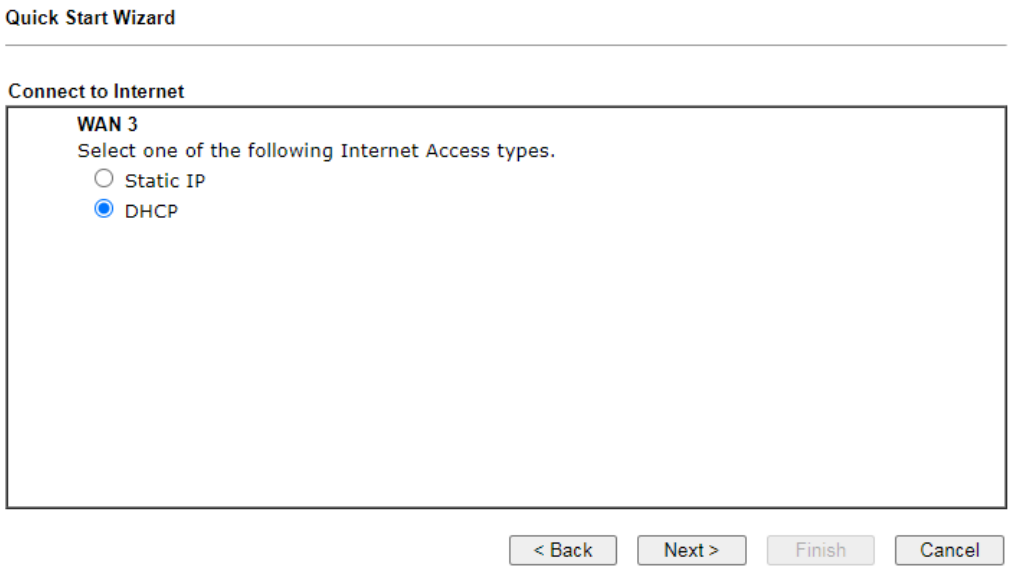
1. Choose **WAN3/WAN4** as WAN Interface and chooose **Wireless 2.4G** or **Wireless 5G** as the physical mode.



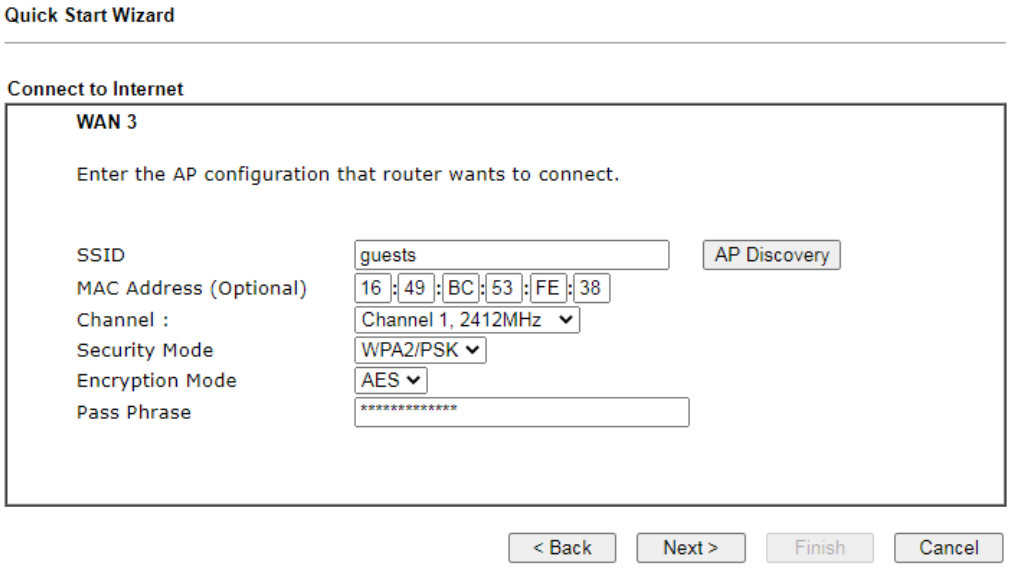

or



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




3. After click **DHCP** as the Internet Access type, you will get the following page. Eenter the SSID of an existed AP as the wireless connection server for this WAN. Or click **AP Discovery** to find an access point as the server for this WAN interface. Click **Next** to continue.

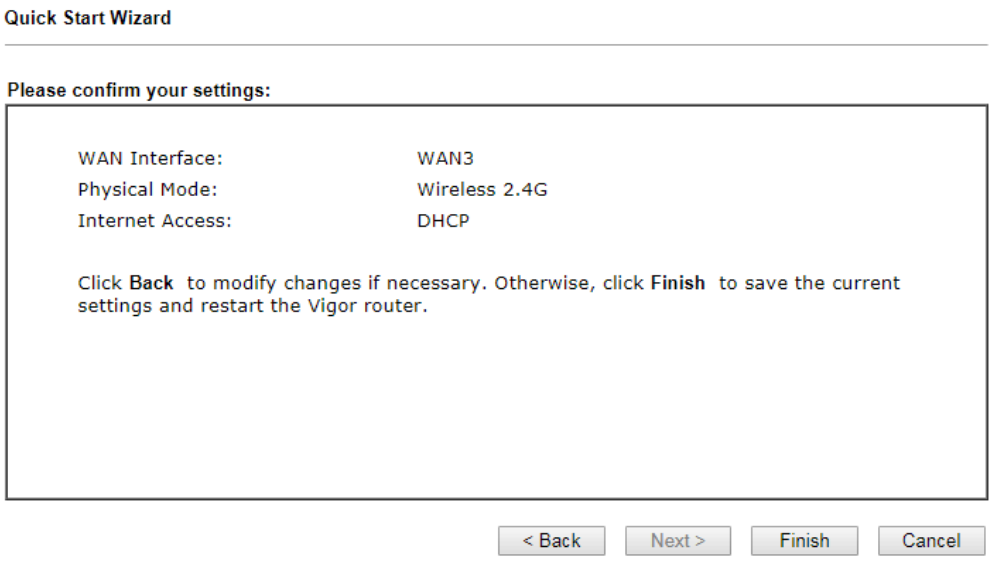



Available settings are explained as follows:

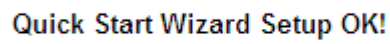
| Item | Description |
|---|---|
| **SSID** | Enter the SSID of an existed AP. Or click **AP Discovery** to find an access point as the server for this WAN interface |
| **MAC Address** | Enter the MAC address of an existed AP. |
| **Channel** | Choose a channel of frequency of the Wireless AP. |
| **Securithy Mode** | The Router connects to the wireless AP as a WEP, WPA or WPA2 client.<br>Select a mode to connect to the Wireless AP. |
| **Encryption Mode** | WPA/PSK uses TKIP as Encryption Mode. WPA2/PSK uses AES as Encryption Mode. |

| | |
|---|---|
| **Pass Phrase** | It is available when WPA/PSK or WPA2/PSK is enabled. |
| **WEP Keys** | It is available when WEP is enabled. |
| **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. |

4. Then, a summary of the connection will be shown on the screen.




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

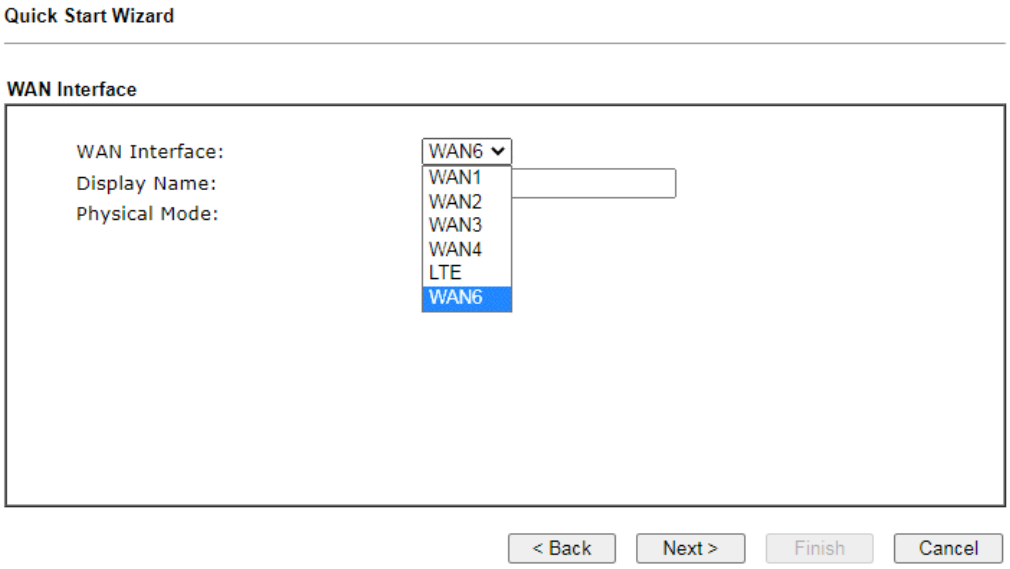



6. Now, you can enjoy surfing on the Internet.

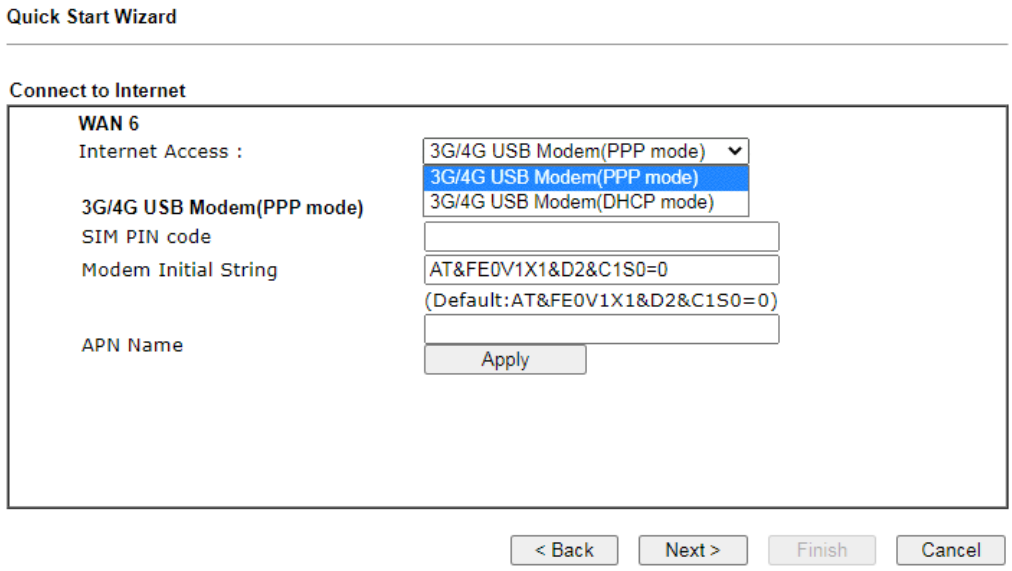
## I-6-3 For WAN5/WAN6 (USB)

WAN3/WAN4 is dedicated to physical mode in USB.

1. Choose **WAN5/WAN6** as WAN Interface. For "L" model, the WAN5 will be changed as LTE.




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




Available settings are explained as follows:

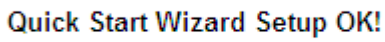
| Item | Description |
|---|---|
| **Internet Access** | Choose one of the selections as the protocol of accessing the internet. |
| **3G/4G USB Modem (PPP mode)** | **SIM Pin code** –Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.<br>**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**. |
| **3G/4G USB Modem (DHCP mode)** | **SIM Pin code** – Type PIN code of the SIM card that will be used to access Internet.<br>**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.<br>**APN Name** – APN means Access Point Name which is provided and required by some ISPs. |
| **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. 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.

# I-7 Service Activation Wizard

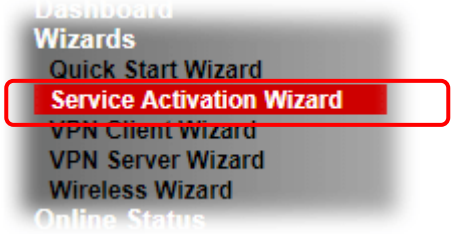
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.**

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

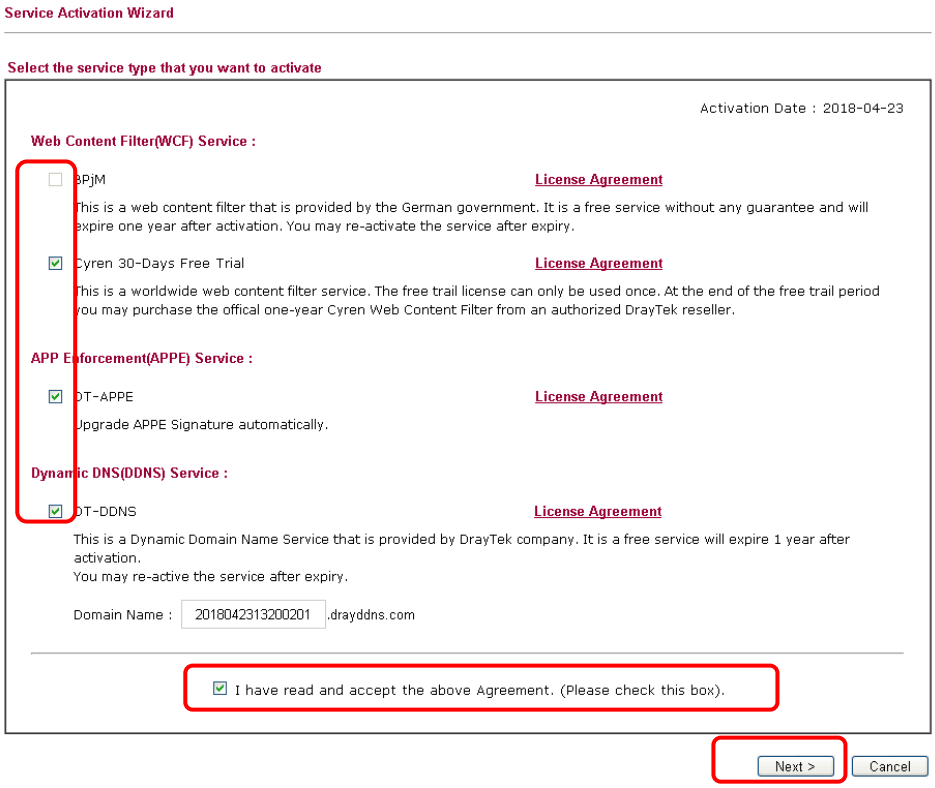
Now, follow the steps listed below to activate WCF feature for your router.

| | |
|---|---|
| Info | Such function is available only for Admin Mode. |

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



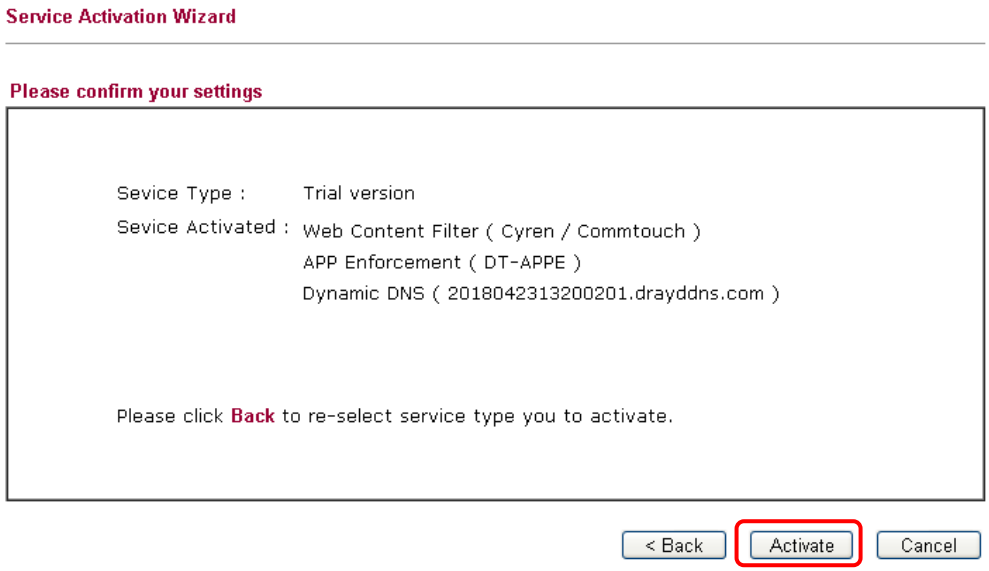

2. The screen of **Service Activation Wizard** will be shown as follows. You can activate the Web content filter services and/or APPE enforcement service and / or DDNS service at the same time or individually. When you finish the selection, please click **Next**.



Info

- BPjM is web content filter (WCF) for German Speaking users. It is ideal for your family to provide more Internet security for youngsters.
- Cryan 30-day trial is WCF which offers 30-day trial period.
- DT-APPE, developed by DrayTek, offers a mechanism to upgrade APPE signature automatically.
- DT-DDNS, developed by DrayTek, offers one year free charge service of dynamic DNS service for internal use.

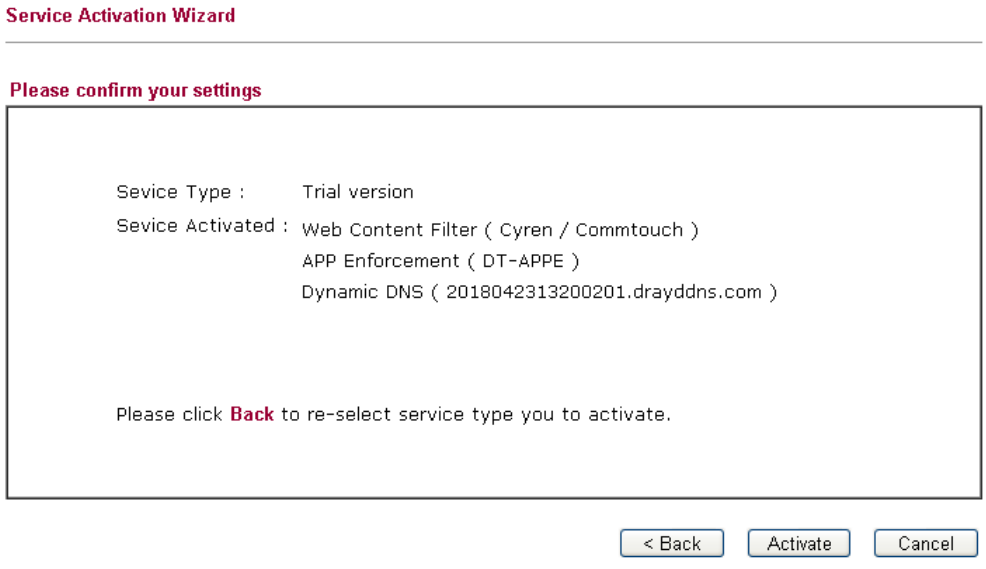
3. Setting confirmation page will be displayed as follows, please click **Activate**.




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).



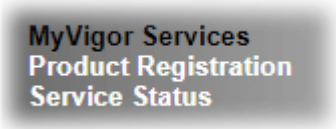
# I-8 Registering Vigor Router

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

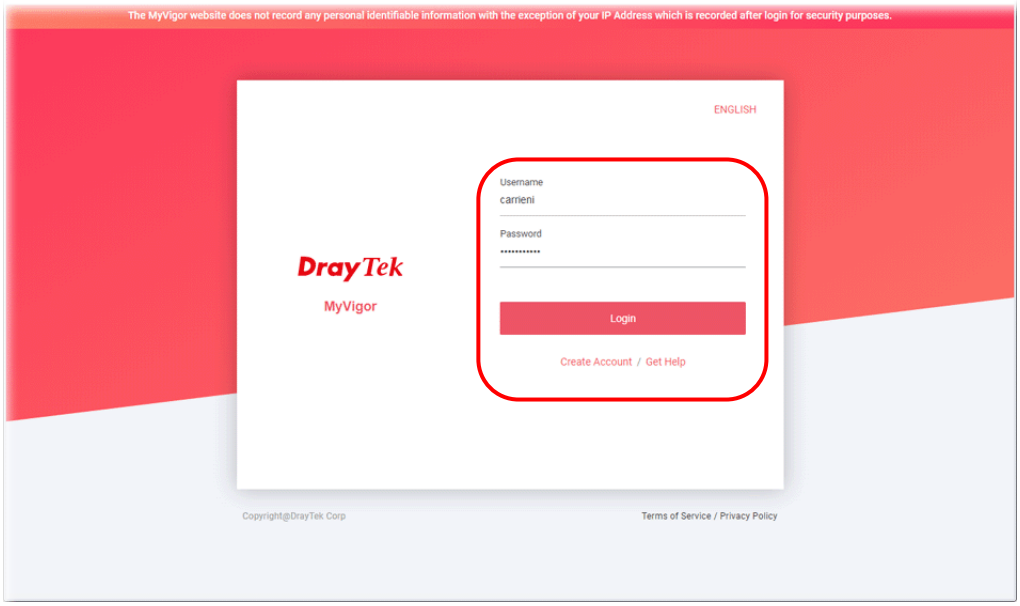
1 Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.




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



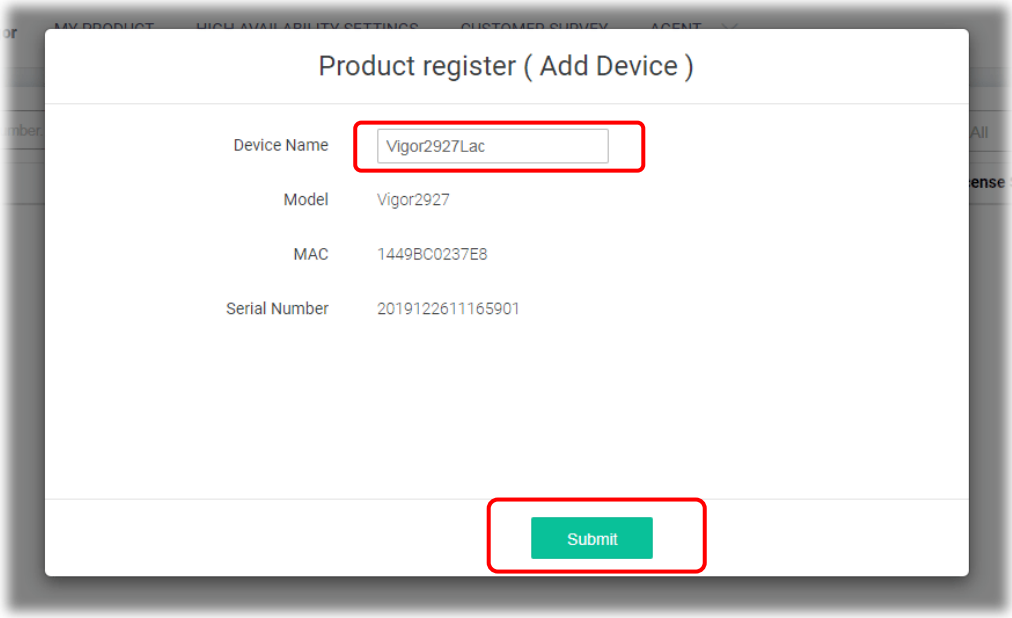

3 A **Login** page will be shown on the screen. Please Enter the account and password that you created previously. And click **Login**.



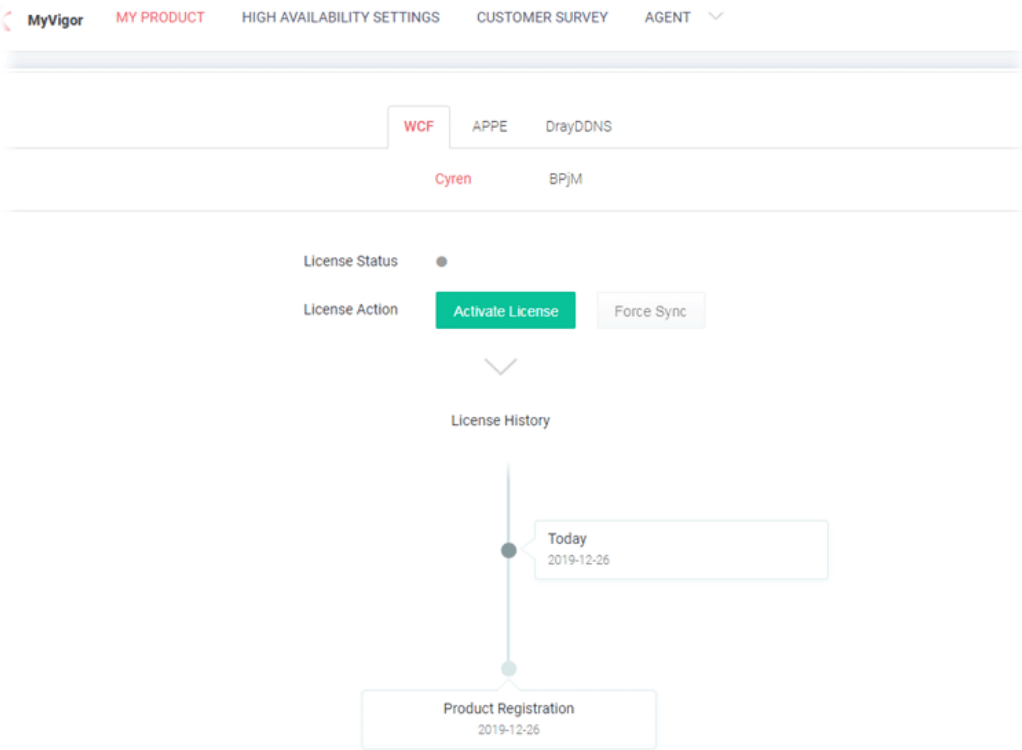
**Info**

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

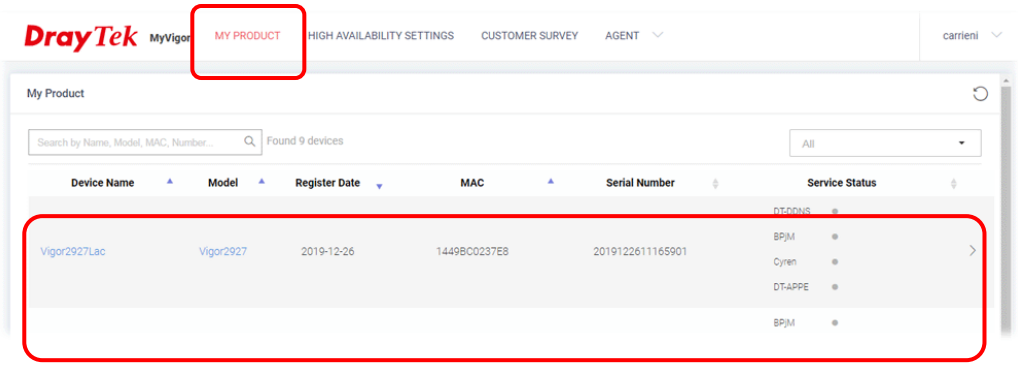
4 The following page will be displayed after you logging in MyVigor. Type a nickname for the router, then click **Submit**.




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



6 Clicking **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.




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




Static Route, Load-Balance/Route Policy

# II-1 WAN

It allows users to access Internet.

## Basics of Internet Protocol (IP) Network

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

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

## What are Public IP Address and Private IP Address

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

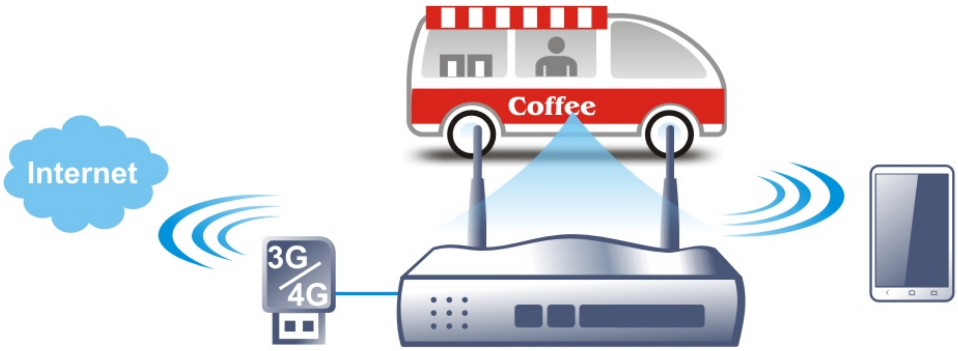
## Get Your Public IP Address from ISP

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

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

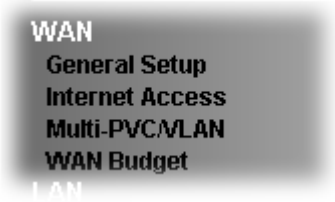
## Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2927 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2927, it can support LTE/HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G/4G standard (HSUPA, etc). Vigor2927n with 3G/4G USB Modem allows you to receive 3G/4G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use LAN ports on the router to access Internet. Also, they can access Internet via 802.11(a/b/g/n/ac) wireless standard, and enjoy the powerful firewall, bandwidth management, and VPN features of Vigor2927n series.




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

# Web User Interface

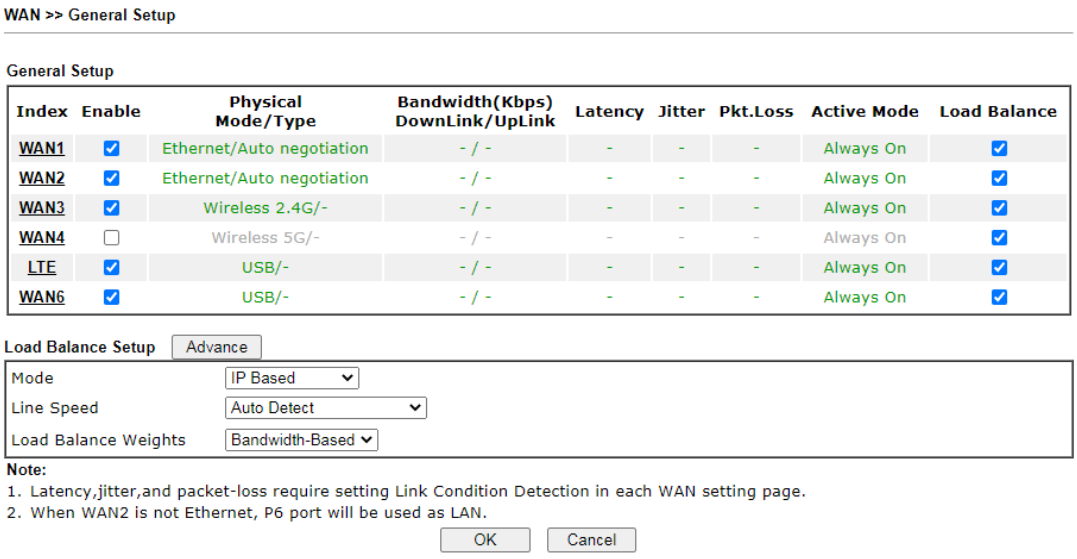



## II-1-1 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1, WAN2, WAN3, WAN4, WAN5/LTE and WAN6 in details.

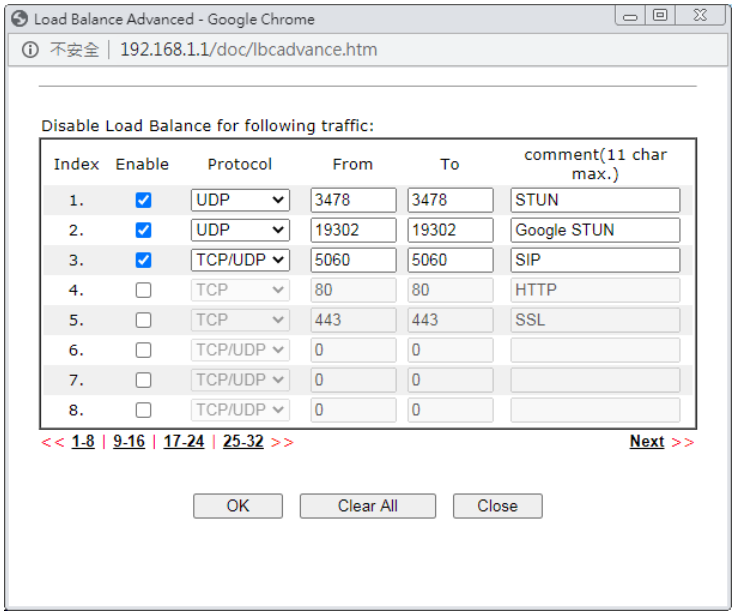
This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1, WAN2, WAN3, WAN4, WAN5/LTE and WAN6 settings.

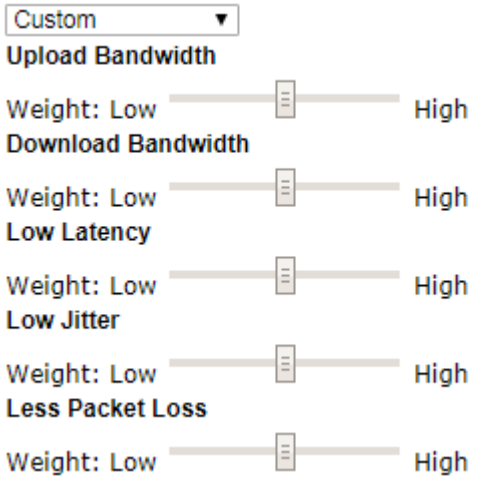
This webpage allows you to set general setup for WAN1, WAN2, WAN3, WAN4, WAN5/LTE and WAN6 respectively.




Available settings are explained as follows:

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

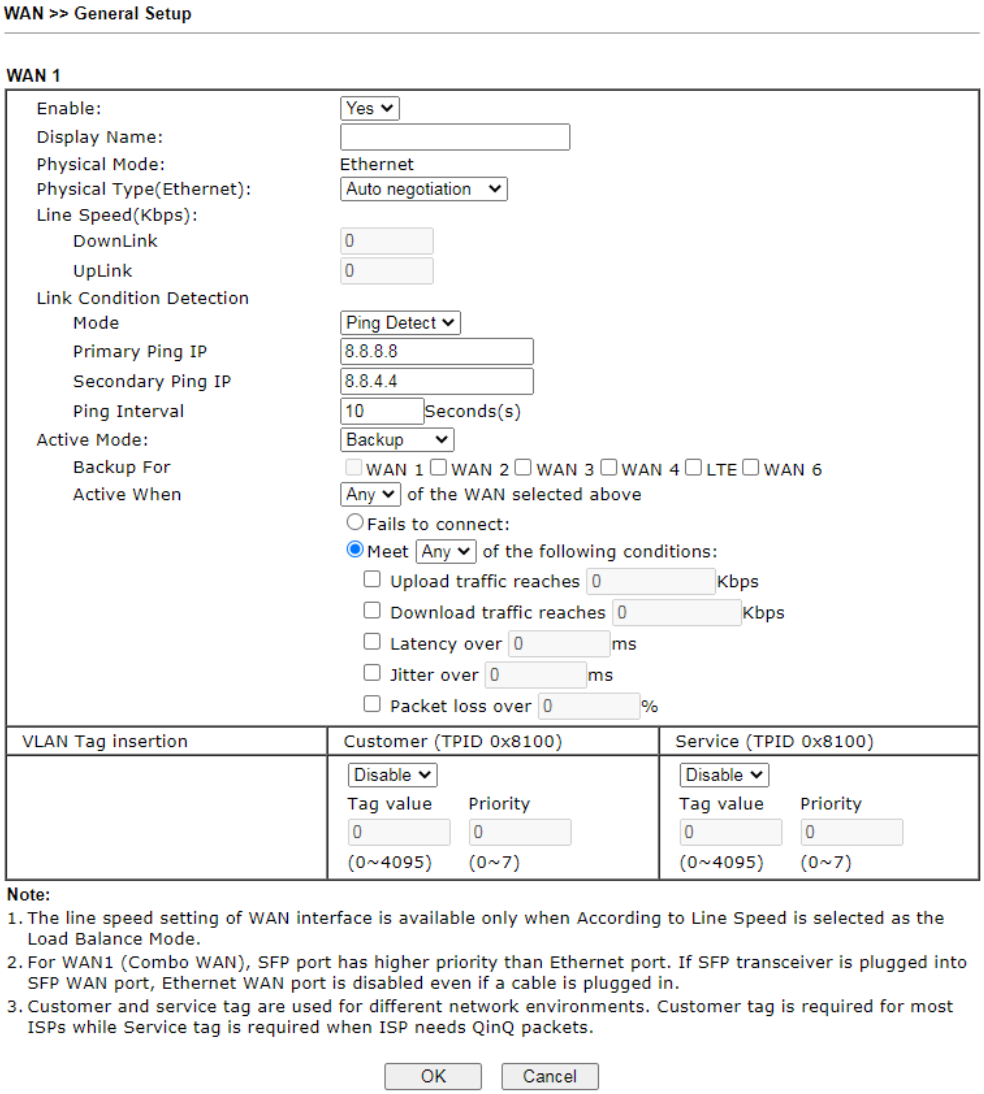
| | |
|---|---|
| |  <br>● **Upload / Download Bandwidth** - The higher the weight is, the WAN interface with higher bandwidth will get higher usage.<br>● **Low Latency** - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight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

| | |
|---|---|
| Info | Wired router (e.g., Vigor2927) does not support WAN3 and WAN4. |

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

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

WAN1/WAN2 can be configured for physical mode of Ethernet.




Available settings are explained as follows:

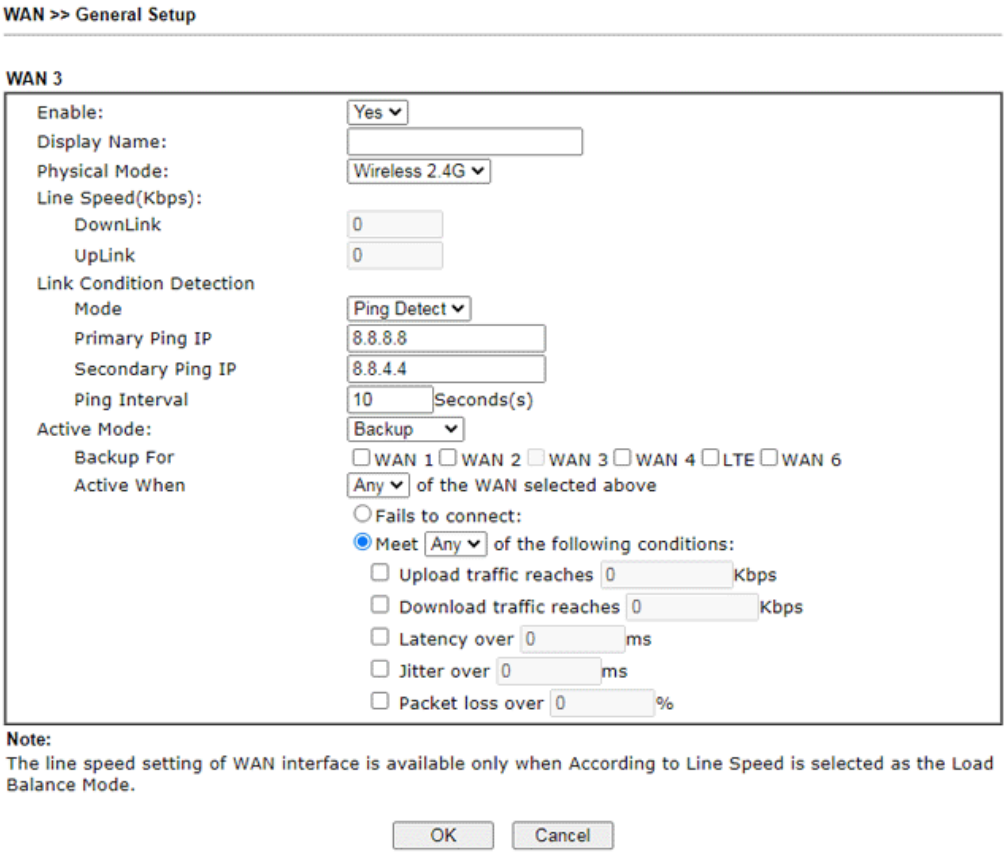
| Item | Description |
|---|---|
| **Enable** | Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface. |
| **Display Name** | Enter the description for such WAN interface. |
| **Physical Mode** | Display the physical mode (Ethernet) of the interface. |
| **Physical Type** | You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system. |
| **Line Speed (Kbps)** | If your choose **According to Line Speed** as the **Line Speed** on **WAN>>General Setup**, please enter the line speed for downloading and uploading for such WAN interface. The unit is kbps. |
| **Link Condition Detection** | In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface.<br>**Mode** - Choose Ping Detect, Http Detect, or Disable as |

| | |
|---|---|
| | detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option.<br>**Primary Ping IP** - Enter an IP address.<br>**Secondary Ping IP** - Enter an IP address.<br>**Ping Interval** - Set a time interval (unit:second) for the system to ping the IP address specified above. |
| **Active Mode** | **Always On** - Choose **Always On** to make the WAN connection being activated always.<br>**Backup** – Choose it to make the WAN connection as a backup connection.<br>● **Backup For** - Specify the WAN interface by checking the WAN box.<br>● **Active When** - Set the condition for backup connection.<br>- **Any** – The selected WAN(s) will be activated when any master WAN interface disconnects.<br>- **All** – All of the backup WANs will be activated only when all master WAN interface disconnects.<br>- **Fails to connect** – When the active WAN failed, the WAN selected above will be activated as the main network connection.<br>- **Meet All/Any of the following conditions** – When the upload traffic, download traffic, latency, jitter and/or packet loss of active WAN reaches the traffic threshold (specified here), the backup WAN will be enabled automatically to share the overloaded data traffic. |
| **VLAN Tag insertion** | Such feature is offered to the user with the environment supporting IEEE_802.1ad. In which, service is used for outer tag; customer is used for inner tag.<br>It is available only when **Ethernet** is selected as **Physical Mode**.<br>**Disable** – Disable the function of VLAN with tag.<br>**Enable** –Enable the function of VLAN with tag.<br>The router will add specific VLAN number to all packets on the WAN while sending them out.<br>Please Enter the tag value and specify the priority for the packets sending by WAN1.<br>● **Tag value** – Enter the value as the VLAN ID number. The range is form 0 to 4095.<br>● **Priority** – Enter the packet priority number for such VLAN. The range is from 0 to 7. |

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

## II-1-1-2 WAN3/WAN4 (Wireless 2.4G or 5G)

WAN3/WAN4 can be configured for physical mode of Wireless 2.4G or Wireless 5G.




Available settings are explained as follows:

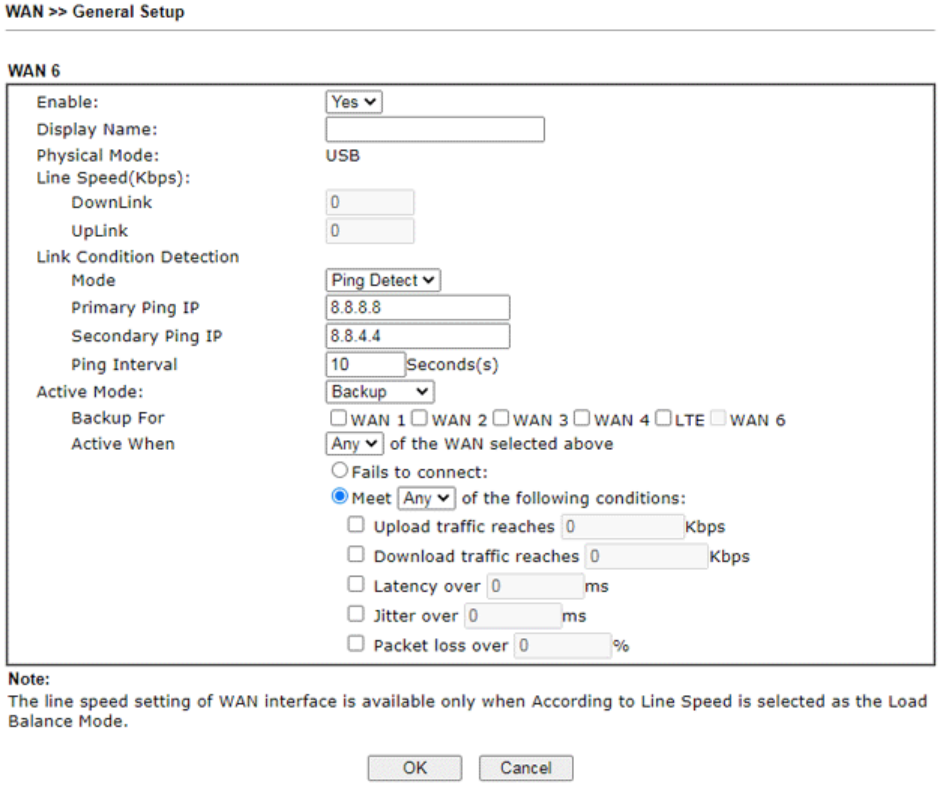
| Item | Description |
|---|---|
| **Enable** | Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface. |
| **Display Name** | Enter the description for such WAN interface. |
| **Physical Mode** | Choose the physical mode (Wireless 2.4G / Wireless 5G) of the interface. |
| **Line Speed (Kbps)** | If your choose **According to Line Speed** as the **Line Speed** on **WAN>>General Setup**, please enter the line speed for downloading and uploading for such WAN interface. The unit is kbps. |
| **Link Condition Detection** | In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface.<br>**Mode** - Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option.<br>**Primary Ping IP** - Enter an IP address.<br>**Secondary Ping IP** - Enter an IP address.<br>**Ping Interval** - Set a time interval (unit:second) for the system to ping the IP address specified above. |
| **Active Mode** | **Always On** - Choose **Always On** to make the WAN connection being activated always. |

| | |
|---|---|
| | **Backup** – Choose it to make the WAN connection as a backup connection.<br>● **Backup For** - Specify the WAN interface by checking the WAN box.<br>● **Active When** - Set the condition for backup connection.<br>- **Any** – The selected WAN(s) will be activated when any master WAN interface disconnects.<br>- **All** – All of the backup WANs will be activated only when all master WAN interface disconnects.<br>- **Fails to connect** – When the active WAN failed, the WAN selected above will be activated as the main network connection.<br>- **Meet All/Any of the following conditions** – When the upload traffic, download traffic, latency, jitter and/or packet loss of active WAN reaches the traffic threshold (specified here), the backup WAN will be enabled automatically to share the overloaded data traffic. |

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

## II-1-1-3 WAN5 / WAN6 (USB) or WAN5 (LTE)

To use 3G/4G network connection through 3G/4G USB Modem, please configure **WAN5 or LTE / WAN6** interface.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Choose **Yes** to invoke the settings for this WAN interface.<br>Choose **No** to disable the settings for this WAN interface. |

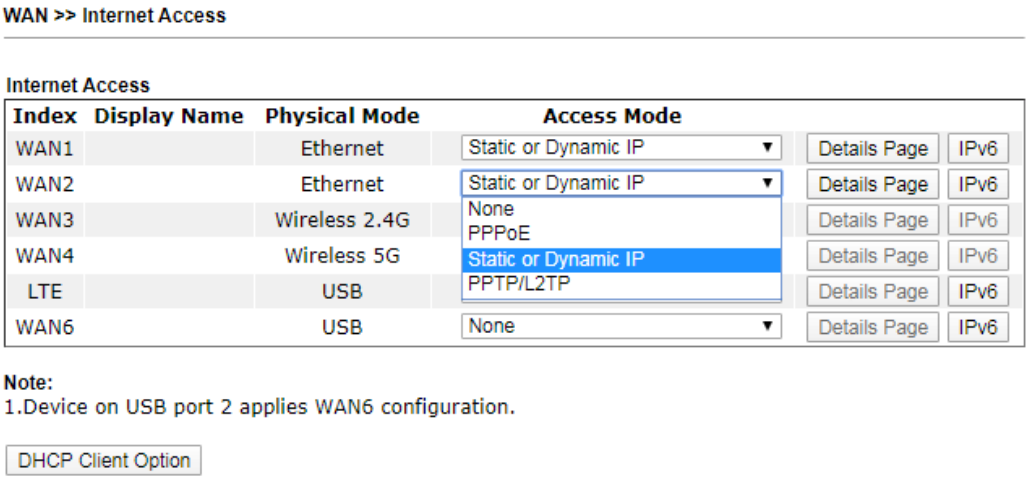
| | |
|---|---|
| **Display Name** | Enter the description for such WAN interface. |
| **Physical Mode** | Display the physical mode of such WAN interface. |
| **Line Speed (Kbps)** | If your choose **According to Line Speed** as the **Line Speed** on **WAN>>General Setup**, please enter the line speed for downloading and uploading for such WAN interface. The unit is kbps. |
| **Link Condition Detection** | In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface.<br>**Mode** - Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option.<br>**Primary Ping IP** - Enter an IP address.<br>**Secondary Ping IP** - Enter an IP address.<br>**Ping Interval** - Set a time interval (unit:second) for the system to ping the IP address specified above. |
| **Active Mode** | **Always On** - Choose **Always On** to make the WAN connection being activated always.<br>**Backup** – Choose it to make the WAN connection as a backup connection.<br>● **Backup For** - Specify the WAN interface by checking the WAN box.<br>● **Active When** - Set the condition for backup connection.<br>- **Any** – The selected WAN(s) will be activated when any master WAN interface disconnects.<br>- **All** – All of the backup WANs will be activated only when all master WAN interface disconnects.<br>- **Fails to connect** – When the active WAN failed, the WAN selected above will be activated as the main network connection.<br>- **Meet All/Any of the following conditions** – When the upload traffic, download traffic, latency, jitter and/or packet loss of active WAN reaches the traffic threshold (specified here), the backup WAN will be enabled automatically to share the overloaded data traffic. |

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

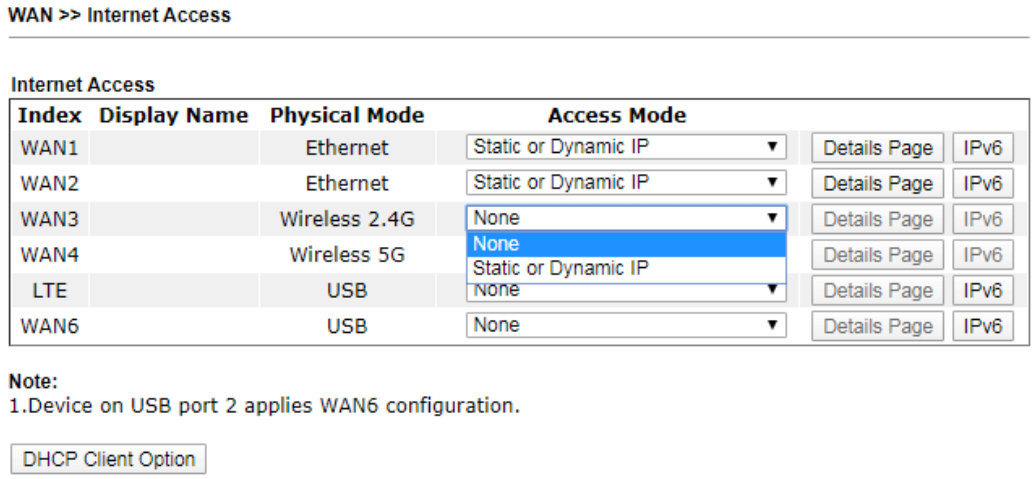
## II-1-2 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1, WAN2, WAN3 or LTE, WAN4) 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.

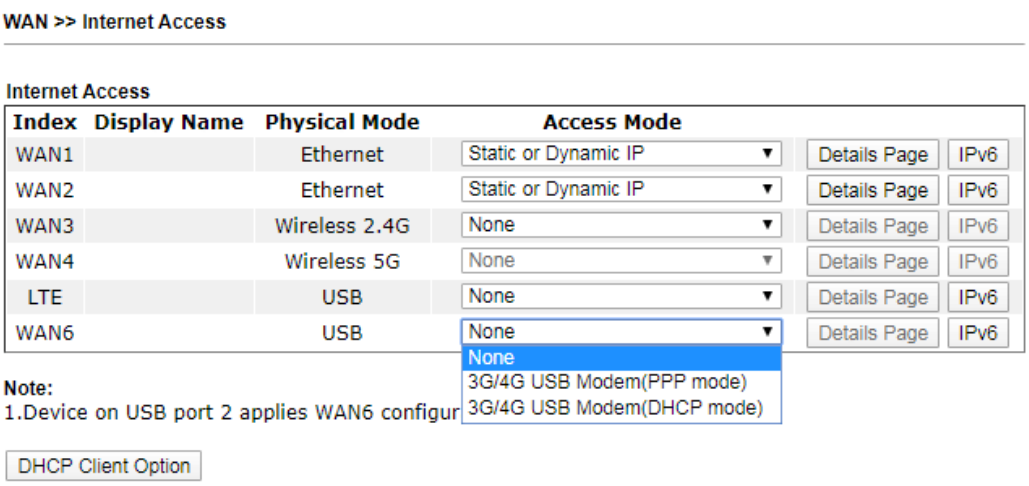
Access Mode for Etherenet,




Access Mode for Wireless 2.4G/5G,

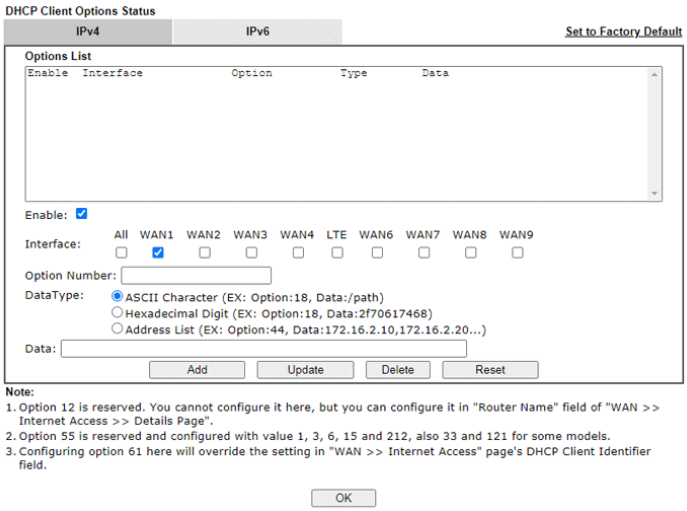


Access Mode for USB,




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Index** | Display the WAN interface. |
| **Display Name** | It shows the name of the WAN1/WAN2/WAN3/WAN4/WAN5 or LTE/WAN6 that entered in general setup. |
| **Physical Mode** | It shows the physical connection for WAN interfaces 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.<br>Note that **Details Page** will be changed slightly based on physical mode specified on **WAN>>General Setup**. |
| **IPv6** | This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. |
| **DHCP Client Option** | This button allows you to configure DHCP client options.<br>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. WAN7 ~ WAN9 can be located under **WAN>>Multi-PVC/VLAN**.

**Option Number** – Type a number for such function.

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

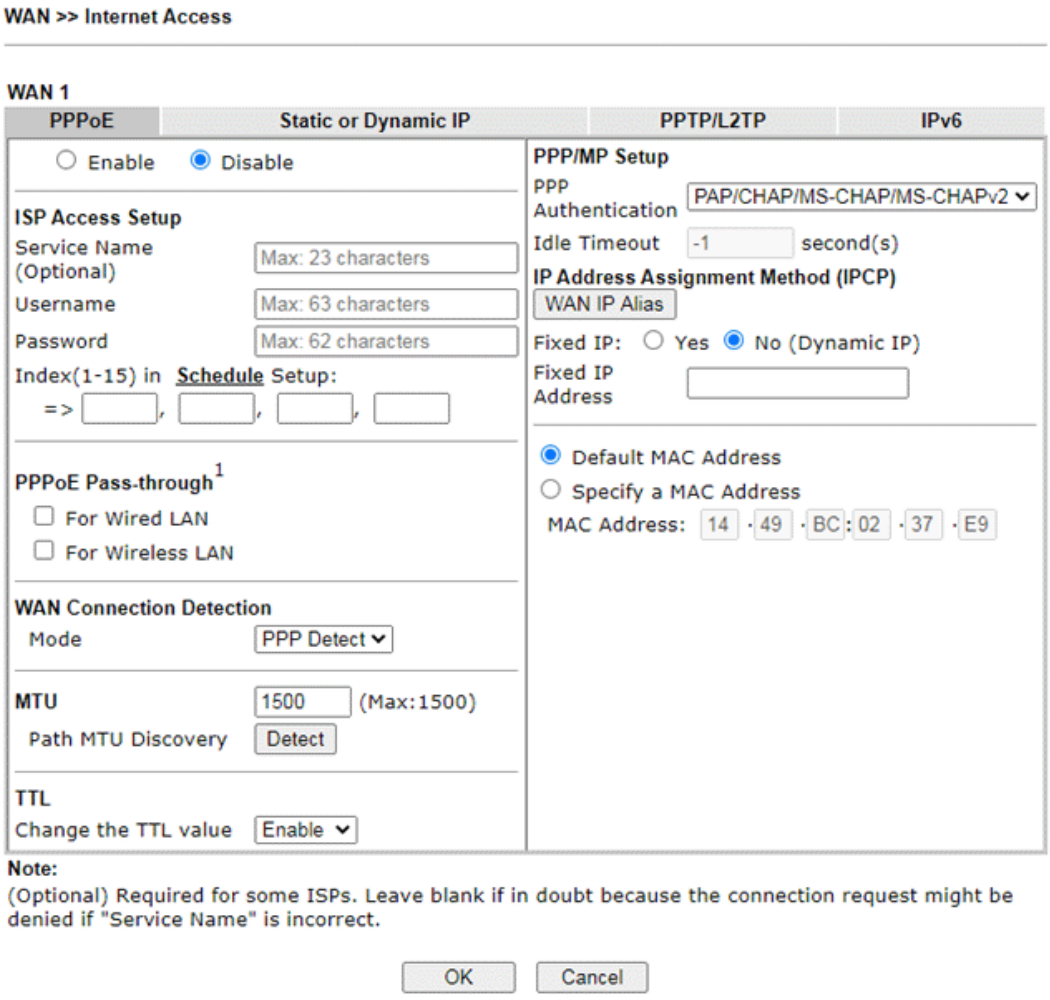
**Data** – Enter the content of the data to be processed by the function of DHCP option.

**Info**

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

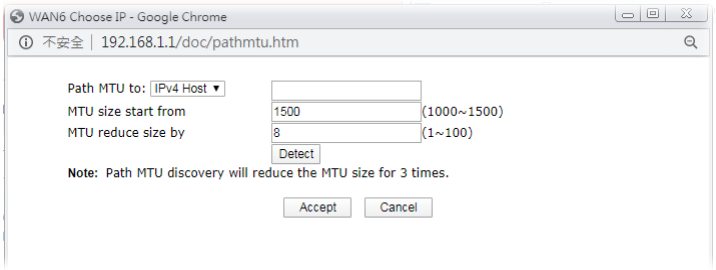
## II-1-2-1 Details Page for PPPoE in WAN1/WAN2 (Physical Mode: Ethernet)

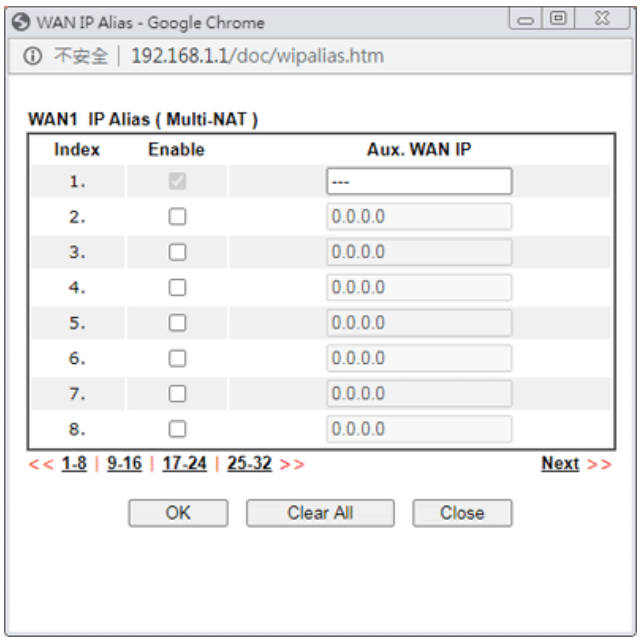
To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN1/2** page. The following web page will be shown.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable/Disable** | Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid. |
| **ISP Access Setup** | Enter your allocated username, password and authentication parameters according to the information provided by your ISP.<br>**Service Name (Optional)** - Enter the description of the specific network service.<br>**Username** – Enter the username provided by ISP in this field.<br>The maximum length of the user name you can set is 63 characters.<br>**Password** – Enter the password provided by ISP in this field.<br>The maximum length of the password you can set is 62 characters.<br>**Index (1-15) in Schedule Setup -** You can Enter four sets of time schedule for your request. All the schedules can be set previously in **Applications >> Schedule** web page and you |

| | |
|---|---|
| | can use the number that you have set in that web page. |
| **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.<br>**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.<br>**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.<br>**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.<br>● **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.<br>● **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.<br>● **TTL (Time to Live)** – Set TTL value of PING operation.<br>● **Ping Interval –** Enter the interval for the system to execute the PING operation.<br>● **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.<br>**Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.<br>Click **Detect** to open the following dialog.<br>  <br>● **Path MTU to** – Enter the IP address as the specific transmit path.<br>● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500. |

| | |
|---|---|
| | • **MTU reduce size by** – It determines the decreasing size of MTU value. For example, the number specified in this field is "8". The maximum MTU size is "1500". After clicking the "detect" button, the system will calculate and get the suitable MTU value such as 1500, 1492, 1484 and etc., automatically.<br>• **Detect** – Click it to detect a suitable MTU value<br>• **Accept** – After clicking it, the detected value will be displayed in the field of MTU. |
| **TTL** | **Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.<br>• **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".<br>• **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. |
| **PPP/MP Setup** | **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.<br>**Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action.<br>**IP Address Assignment Method (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.<br>**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.<br>  <br>**Fixed IP Address** – Enter a fixed IP address. |

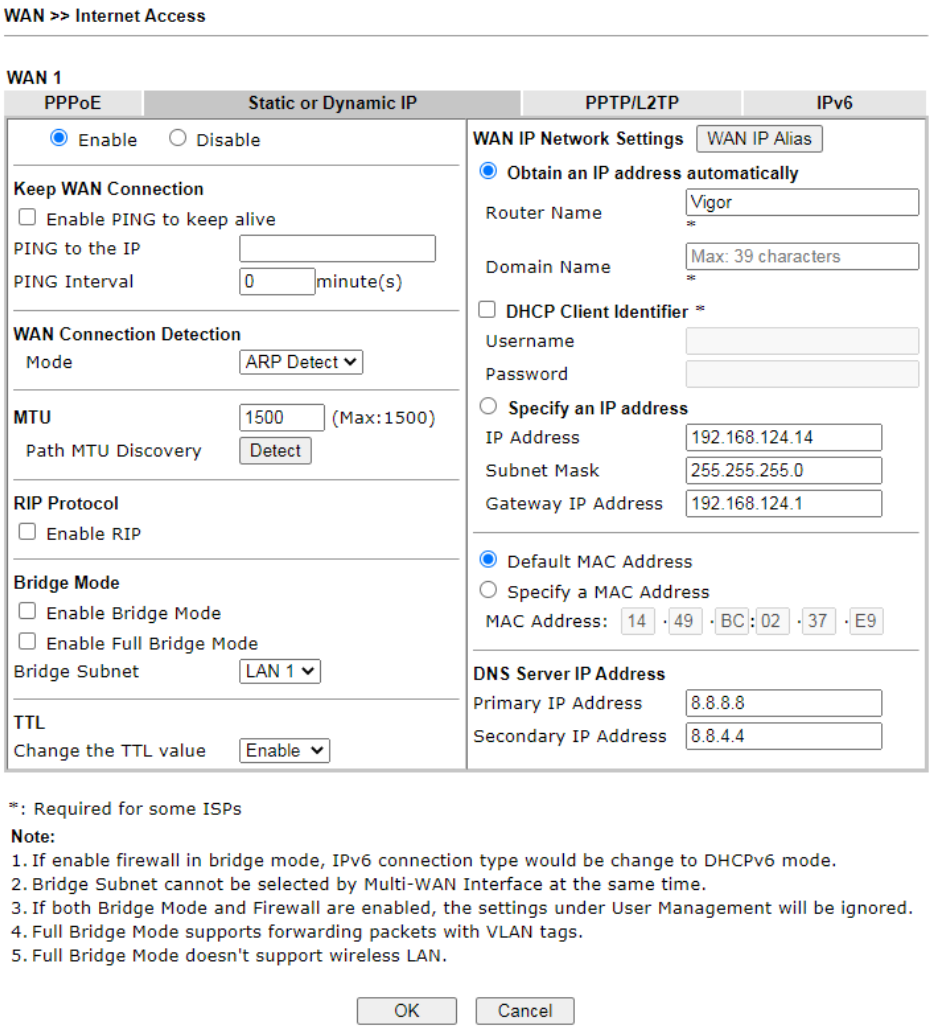
| | |
|---|---|
| | **Default MAC Address** – Enter MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.<br>**Specify a MAC Address** – Enter the MAC address for the router manually. |

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)

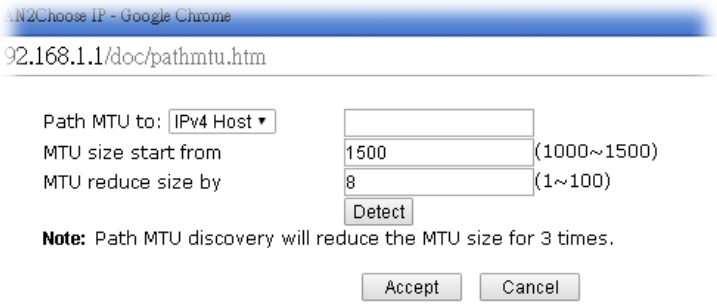
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you 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. |
| **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.<br>**PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.<br>**PING Interval** - Enter the interval for the system to execute the PING operation. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.<br>**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.<br>● **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.<br>● **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.<br>With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL (Time to Live)** – Set TTL value of PING operation.<br>● **Ping Interval –** Enter the interval for the system to execute the PING operation.<br>● **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.<br>**Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.<br>Click **Detect** to open the following dialog.<br>  <br>● **Path MTU to** – Enter the IP address as the specific transmit path.<br>● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500.<br>● **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, |

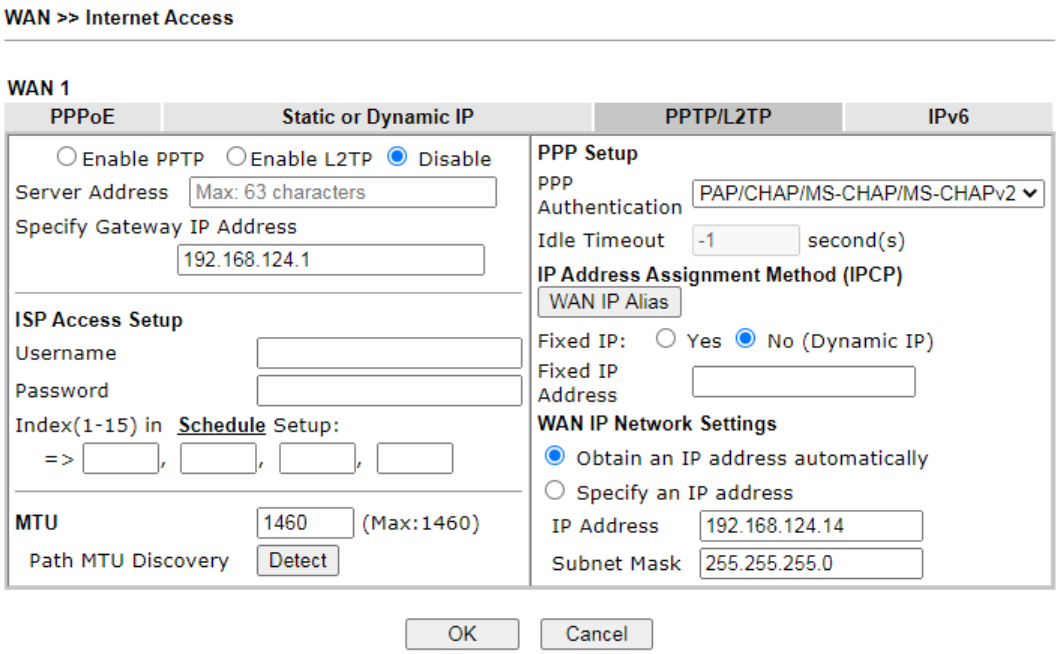
| | |
|---|---|
| | 1492, 1484 and etc., automatically.<br>● **Detect** – Click it to detect a suitable MTU value<br>● **Accept** – After clicking it, the detected value will be displayed in the field of MTU. |
| **RIP Protocol** | Routing Information Protocol is abbreviated as RIP（RFC1058） specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function. |
| **Bridge Mode** | **Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded.<br>**Enable Full Bridge Mode** – If the function is enabled, the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.<br>**Bridge Subnet** – Make a bridge between the selected LAN subnet and such WAN interface. |
| **TTL** | **Change the TTL value –** Enable or disable the TTL (Time to Live) for a packet transmitted through Vigor router.<br>● **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".<br>● **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. |
| **WAN IP Network Settings** | This group allows you to obtain an IP address automatically and allows you Enter IP address manually.<br>**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.<br>**Obtain an IP address automatically** – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.<br>● **Router Name**: Enter the router name provided by ISP.<br>● **Domain Name**: Enter the domain name that you have assigned.<br>**DHCP Client Identifier:** Check the box to specify username and password as the DHCP client identifier for some ISP.<br>● **Username:** Type a name as username. The maximum length of the user name you can set is 63 characters.<br>● **Password:** Type a password. The maximum length of the password you can set is 62 characters.<br>**Specify an IP address** – Click this radio button to specify some data if you want to use **Static IP** mode.<br>● **IP Address**: Enter the IP address.<br>● **Subnet Mask**: Enter the subnet mask.<br>● **Gateway IP Address**: Enter the gateway IP address.<br>**Default MAC Address**: Click this radio button to use default MAC address for the router.<br>**Specify a MAC Address**: Some Cable service providers specify a specific MAC address for access authentication. In |

| | |
|---|---|
| | such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field. |
| **DNS Server IP Address** | Enter the primary IP address for the router if you want to use **Static IP** mode. If necessary, Enter secondary IP address for necessity in the future. |

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

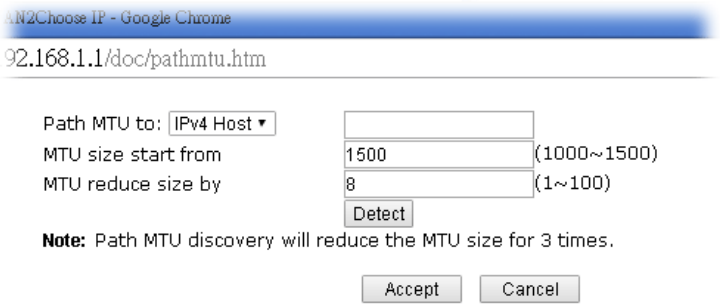
## II-1-2-3 Details Page for PPTP/L2TP in WAN1/WAN2 (Physical Mode: Ethernet)

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.<br>**Enable L2TP** - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.<br>**Disable** – Click this radio button to close the connection through PPTP or L2TP.<br>**Server Address** - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.<br>**Specify Gateway IP Address** – Specify the gateway IP address for DHCP server. |
| **ISP Access Setup** | **Username** -Enter the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.<br>**Password** -Enter the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.<br>**Index(1-15) in Schedule Setup -** You can Enter four sets of time schedule for your request. All the schedules can be set previously in **Applications >> 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.<br>**Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.<br>Click **Detect** to open the following dialog. |

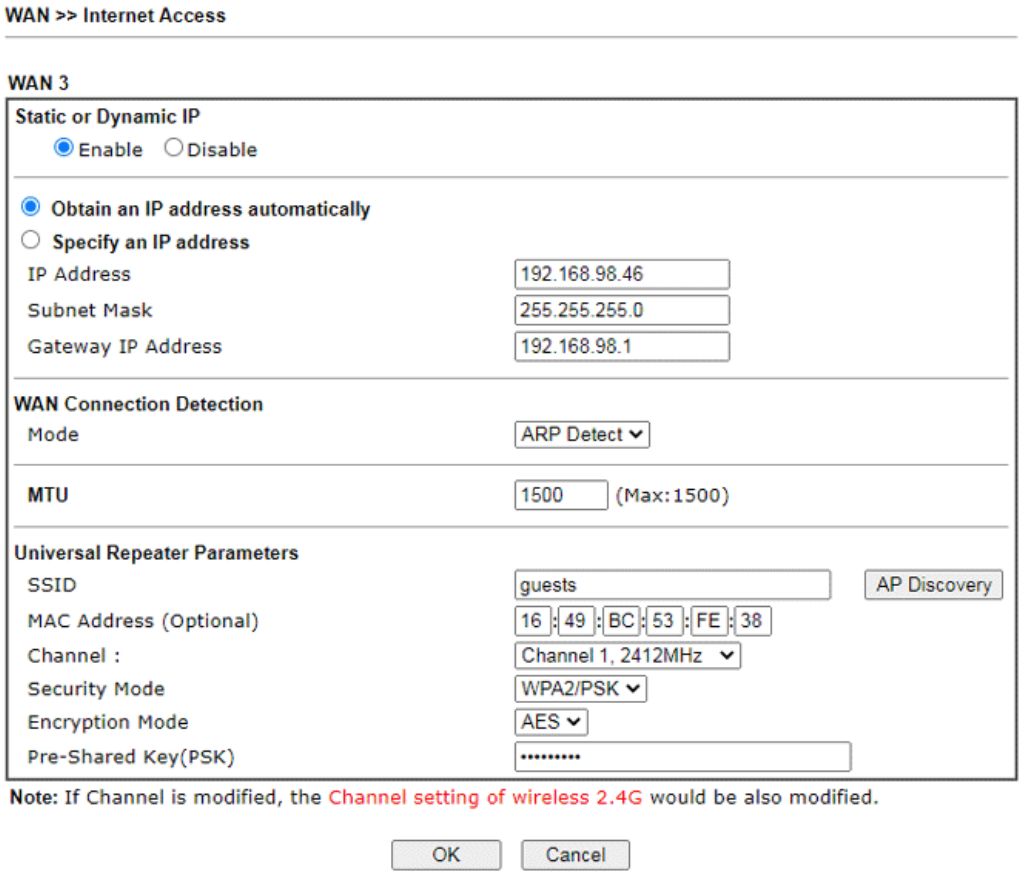
| | |
|---|---|
| |  <br>● **Path MTU to** – Enter the IP address as the specific transmit path.<br>● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500.<br>● **MTU reduce size by**– It determines the decreasing size of MTU value. For example, the number 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.<br>● **Detect** – Click it to detect a suitable MTU value<br>● **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.<br>**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.<br>**Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and Enter a fixed IP address in the box.<br>**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.<br>**Specify an IP address** – Click this radio button to specify some data.<br>● **IP Address** – Enter the IP address.<br>● **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 Static or Dynamic IP in WAN3/WAN4 (Physical Mode: Wireless 2.4G/ Wireless 5G)

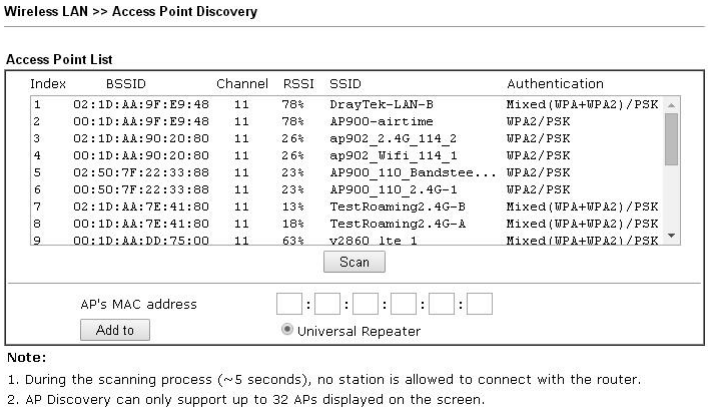
When Wireless 2.4G is selected as Physical Mode, WAN uses wireless station mode to access Internet. The Router acts as a 2.4GHz wireless station and connects to the specific Wireless AP.

To use **Static or Dynamic IP** as the accessing protocol of the internet, please select **Static or Dynamic IP** from the **WAN>>Internet Access>>WAN2** page. The following web page will be shown.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable/Disable** | Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid. |
| **Obtain an IP address automatically** | Click this radio button to obtain the IP address automatically if you want to use **Dynamic IP** mode. |
| **Specify an IP address** | Click this radio button to specify dome data if you want to use **Static IP** mode.<br>**IP address** - Enter the IP address.<br>**Subnet Mask** - Enter the subnet mask.<br>**Gateway IP Address** - Enter the gateway IP address. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.<br>**Mode** – Choose **ARP Detect, Ping Detect** or **Always On** for the system to execute for WAN detection. If you choose Ping |

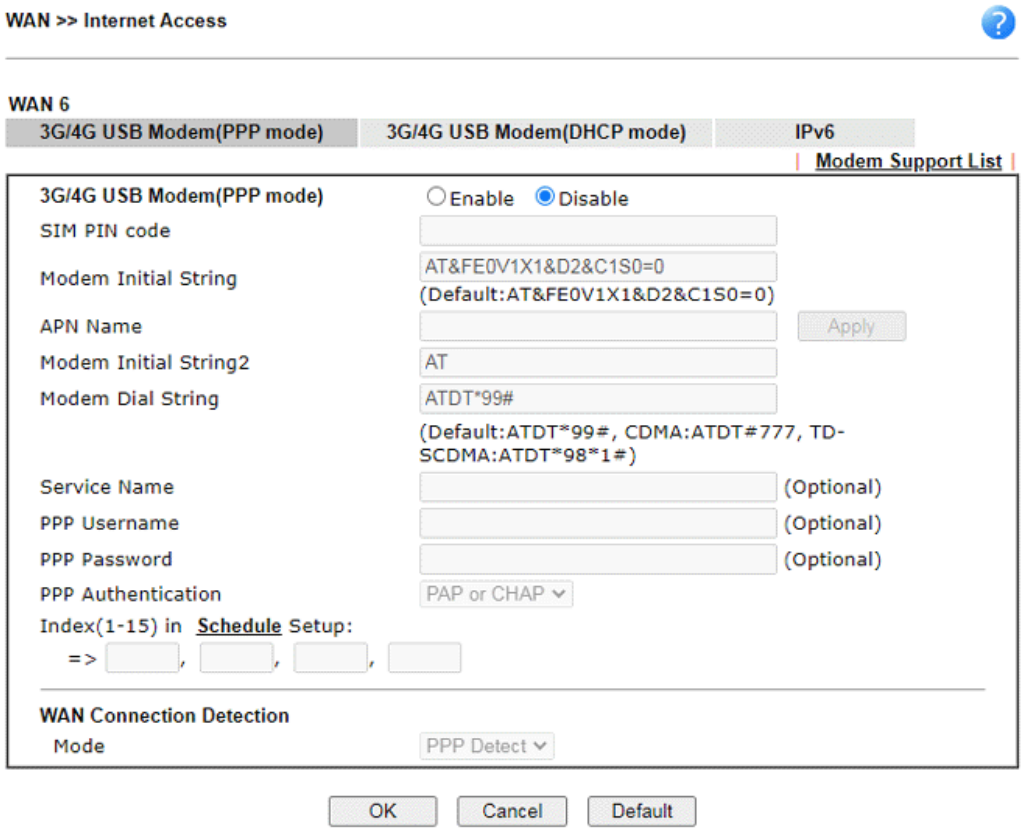
| | |
|---|---|
| | Detect as the detection mode, you have to type required settings for the following items.<br>● **Ping IP** – If you choose **Ping Detect** as detection mode, you also can enable this setting to use current WAN gateway IP address for pinging.<br>With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL (Time to Live)** – Set TTL value of PING operation. |
| **MTU** | It means Max Transmit Unit for packet. |
| **Universal Repeater Parameters** | **AP Discovery** - Click this button to open the Access Point Discovery window. Let wireless 2.4GHz do AP discovery and choose the Wireless AP you wan to connect to.<br>  <br>Wireless LAN >> Access Point Discovery<br>Access Point List<br>Index BSSID Channel RSSI SSID Authentication<br>1 02:1D:AA:9F:E9:48 11 78% DrayTek-LAN-B Mixed(WPA+WPA2)/PSK<br>2 00:1D:AA:9F:E9:48 11 78% AP900-airtime WPA2/PSK<br>3 02:1D:AA:90:20:80 11 26% ap902_2.4G_114_2 WPA2/PSK<br>4 00:1D:AA:90:20:80 11 26% ap902_Wifi_114_1 WPA2/PSK<br>5 02:50:7F:22:33:88 11 23% AP900_110_Bandstee... WPA2/PSK<br>6 00:50:7F:22:33:88 11 23% AP900_110_2.4G-1 WPA2/PSK<br>7 02:1D:AA:7E:41:80 11 13% TestRoaming2.4G-B Mixed(WPA+WPA2)/PSK<br>8 00:1D:AA:7E:41:80 11 18% TestRoaming2.4G-A Mixed(WPA+WPA2)/PSK<br>9 00:1D:AA:DD:75:00 11 63% v2860_lte_1 Mixed(WPA+WPA2)/PSK<br>Scan<br>AP's MAC address : : : : : :<br>Add to Universal Repeater<br>Note:<br>1. During the scanning process (~5 seconds), no station is allowed to connect with the router.<br>2. AP Discovery can only support up to 32 APs displayed on the screen.<br>**SSID** - The identification of the Wireless AP.<br>**MAC Address (Optional)-** The MAC Address of the Wireless AP.<br>**Channel** - The channel of frequency of the Wireless AP.<br>**Security Mode** - The mode to connect to the Wireless AP.<br>● **Disable** – The Router connects to the wireless AP without any encryption mechanism.<br>● **WEP** – The Router connects to the wireless AP as a WEP client and the encryption key should be entered in WEP Key.<br>- **64-Bit** - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)<br>- **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).<br>- **WEP keys** – 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.<br>● **WPA/PSK** – The Router connects to the wireless AP as a WPA client and the encryption key should be entered in PSK.<br>● **WPA2/PSK** – The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.<br>- **Encryption Mode** - WPA/PSK uses TKIP as Encryption Mode. WPA2/PSK uses AES as Encryption |

| | |
|---|---|
| | Mode.<br>- **Pre-Shared Key (PSK)** – The PSK. Either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). |

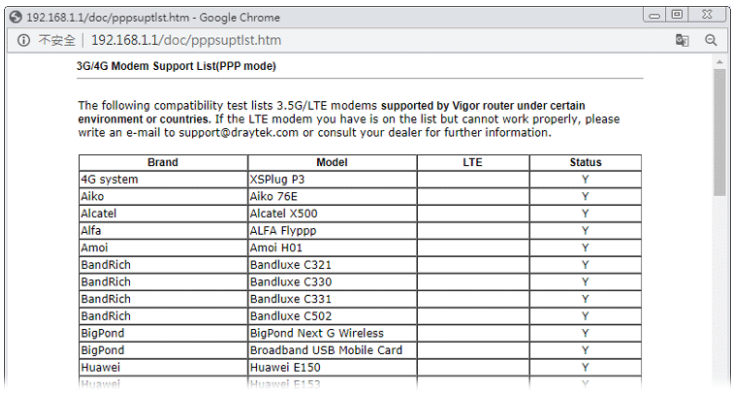
After finishing all the settings here, please click **OK** to activate them.

## II-1-2-5 Details Page for 3G/4G USB Modem (PPP mode) in WAN5 / WAN6

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 WAN5/WAN6. 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.<br>  |
| **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 |

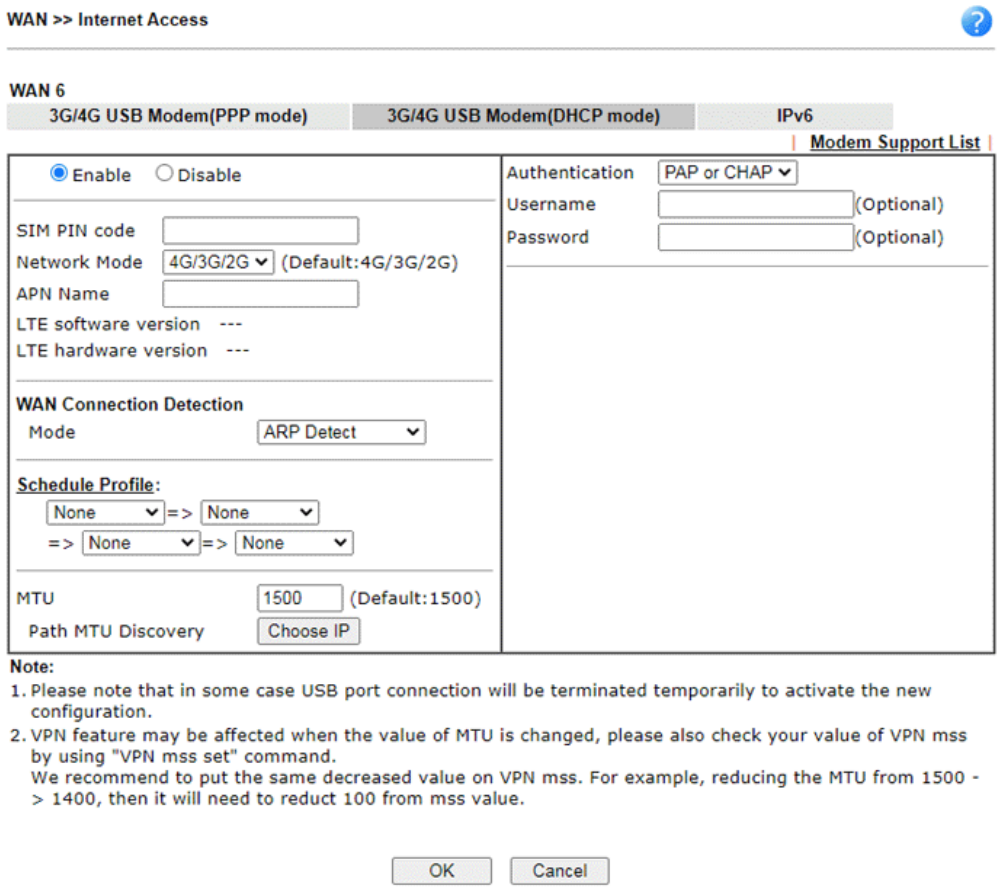
| | |
|---|---|
| | adjusted in this page will be invalid. |
| **SIM PIN code** | Type PIN code of the SIM card that will be used to access Internet.<br>The maximum length of the PIN code you can set is 15 characters. |
| **Modem Initial String** | Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.<br>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**.<br>The maximum length of the name you can set is 43 characters. |
| **Modem Initial String2** | The initial string 1 is shared with APN.<br>In some cases, user may need another initial AT command to restrict 3G band or do any special settings.<br>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.<br>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. |
| **Index (1-15) in Schedule Setup** | 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. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through PPP Detect or Ping Detect.<br>**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.<br>● **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.<br>● **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.<br>With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL (Time to Live)** – Set TTL value of PING operation.<br>● **Ping Interval –** Enter the interval for the system to |

| | |
|---|---|
| | execute the PING operation.<br>● **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.

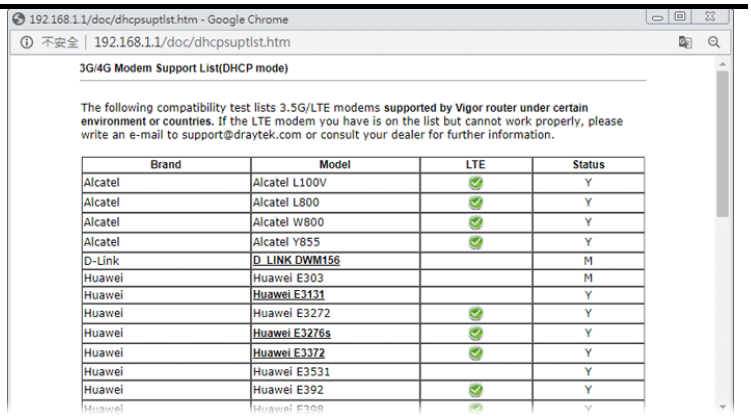
## II-1-2-6 Details Page for 3G/4G USB Modem (DHCP mode) in WAN5 / WAN6

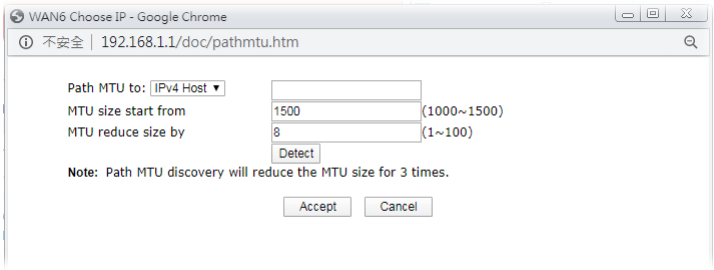
To use **3G/4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (DHCP mode)** for WAN5/WAN6. The following web page will be shown.




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.<br>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.**<br>The maximum length of the name you can set is 47 characters. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through ARP Detect, Strict ARP Detect or Ping Detect.<br>**Mode** – Choose **ARP Detect, Strict ARP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose Ping Detect as the detection mode, you have to type required settings for the following items.<br>● **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.<br>● **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.<br>With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL (Time to Live)** – Set TTL value of PING operation.<br>● **Ping Interval –** Enter the interval for the system to execute the PING operation.<br>● **Ping Retry –** Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| **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 |

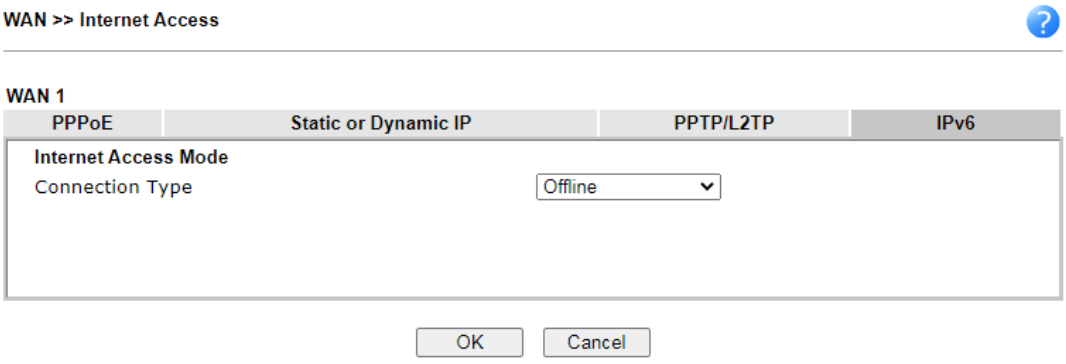
| | |
|---|---|
| | work. |
| **MTU** | It means Max Transmit Unit for packet.<br>**Path MTU Discovery** – It is used to detect the maximum MTU size of a packet not to be segmented in specific transmit path.<br>Click **Choose IP** to open the following dialog.<br>  <br>● **Path MTU to** – Enter the IP address as the specific transmit path.<br>● **MTU size start from** – Determine the starting point value of the packet. Default setting is 1500.<br>● **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.<br>● **Detect** – Click it to detect a suitable MTU value<br>● **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.<br>**Username** – Enter the username for authentication (optional).<br>**Password** – Enter the password for authentication (optional). |



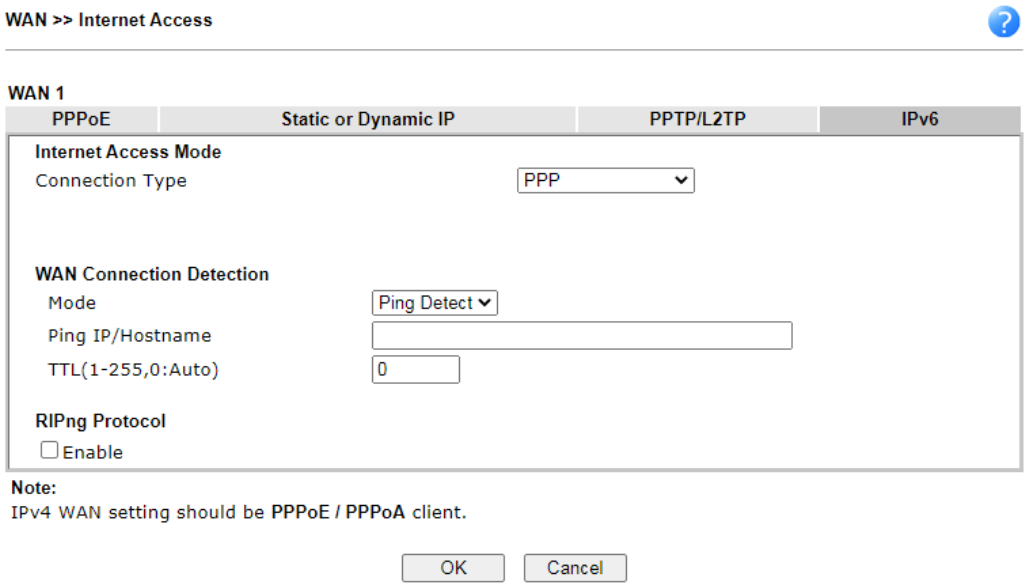
After finishing all the settings here, please click **OK** to activate them.

## II-1-2-7 Details Page for IPv6 – Offline in WAN1~WAN6

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



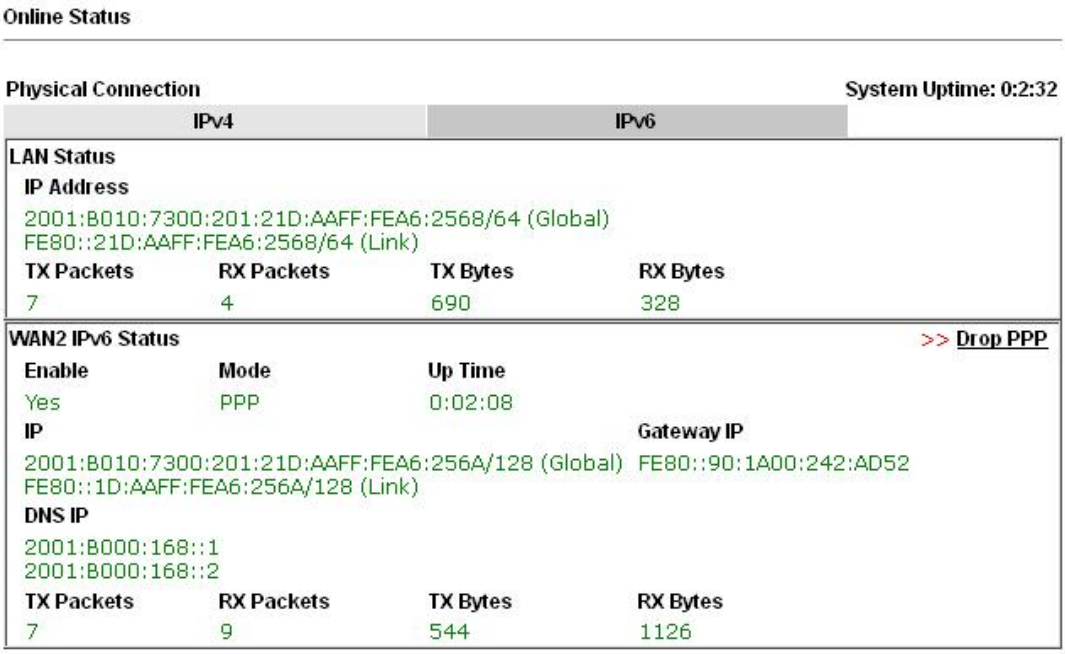
## II-1-2-8 Details Page for IPv6 – PPP in WAN1/WAN2




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.<br>**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.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **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.



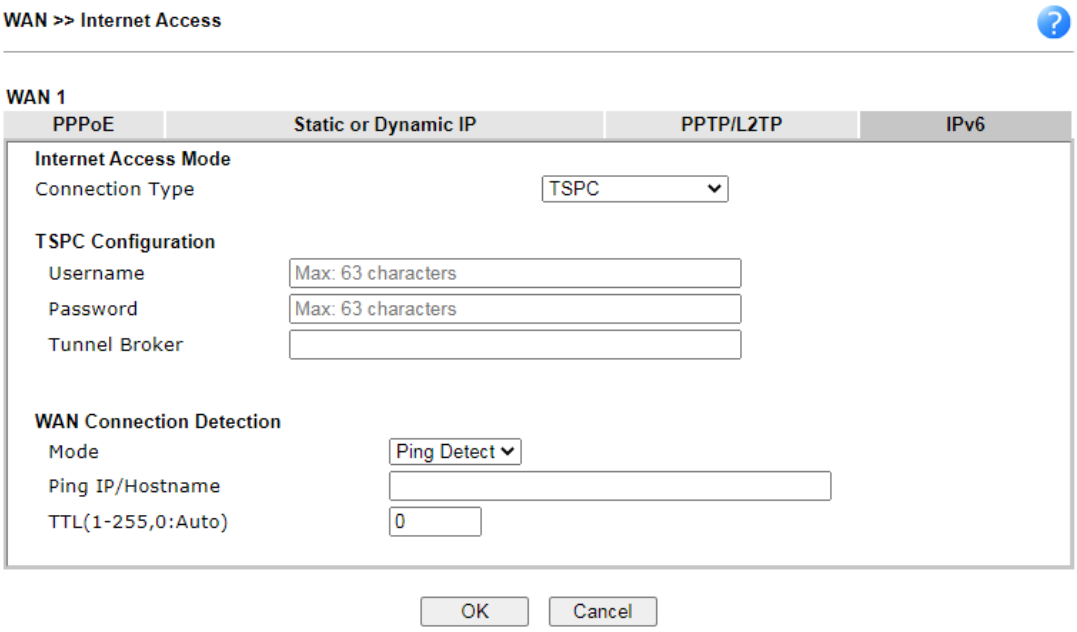

Info At present, the IPv6 prefix can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

## II-1-2-9 Details Page for IPv6 – TSPC in WAN1~WAN6

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

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

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

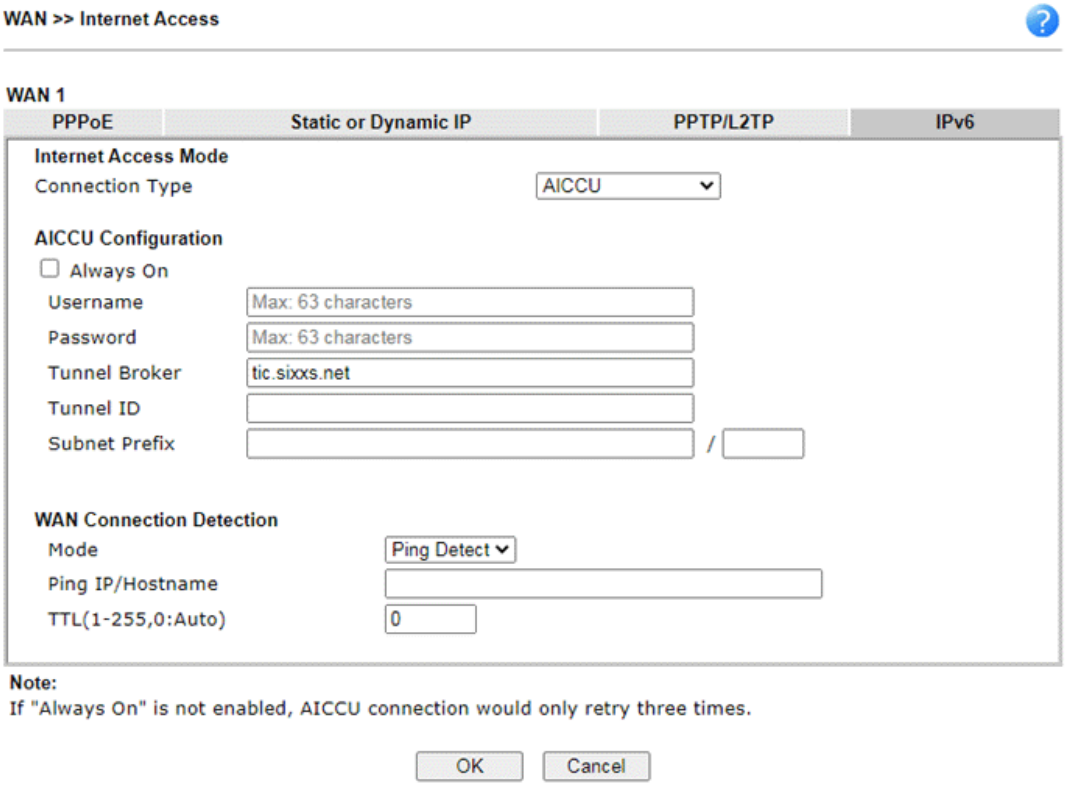



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Username** | It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.<br>The maximum length of the name you can set is 63 characters. |
| **Password** | Enter the password assigned with the user name.<br>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.<br>**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.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **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 – AICCU in WAN1~WAN6




Available settings are explained as follows:

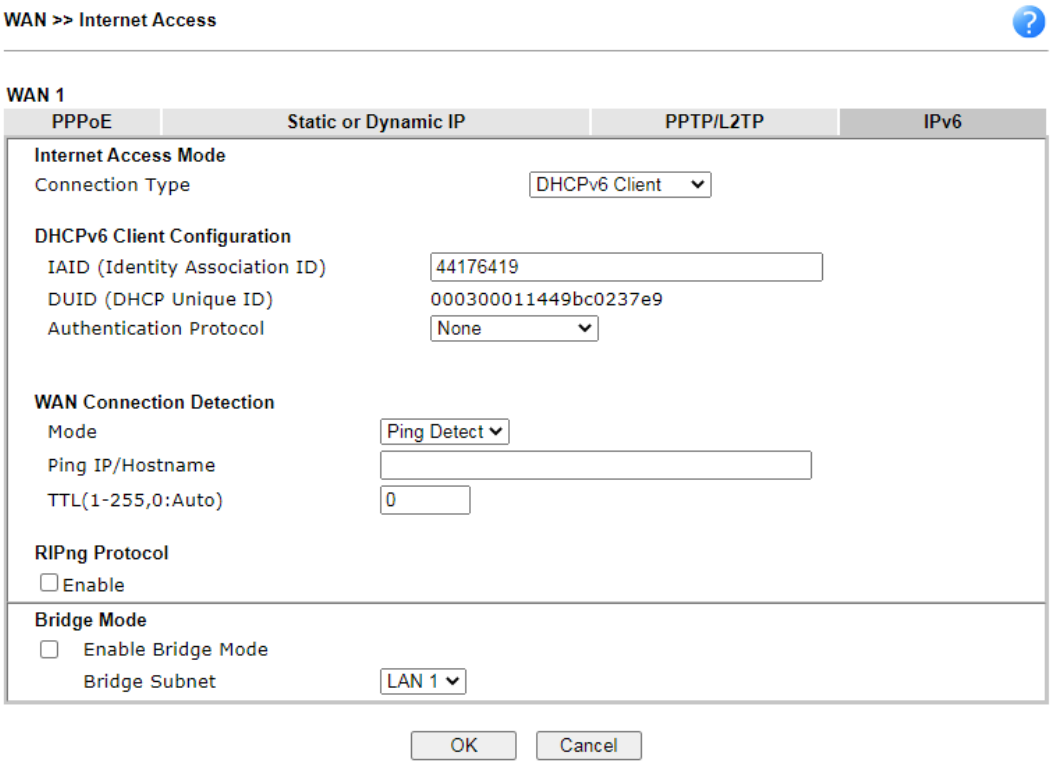
| Item | Description |
|---|---|
| **Always On** | Check this box to keep the network connection always. |
| **Username** | Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.<br>The maximum length of the name you can set is 19 characters. |
| **Password** | Enter the password assigned with the user name.<br>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.<br>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).<br>Enter the ID offered by Tunnel Broker. |
| **Subnet Prefix** | Enter the subnet prefix address obtained from service provider.<br>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.<br>**Mode** – Choose **Always On** or **Ping Detect** for the system to |

| | |
|---|---|
| | execute for WAN detection.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **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-1-2-11 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:

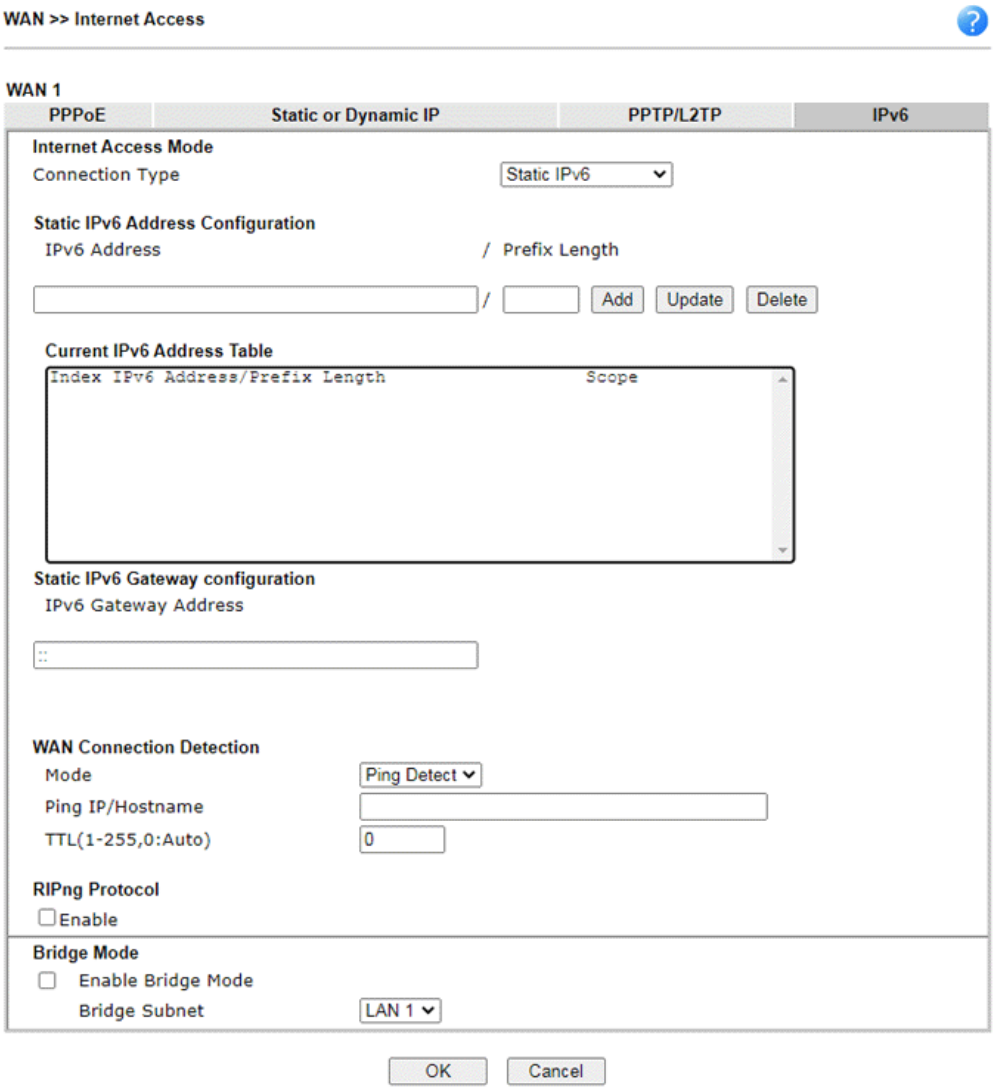
| Item | Description |
|---|---|
| **DHCPv6 Client Configuration** | **IAID** - Type a number as IAID.<br>**DUID** – Display the DHCP unique ID used by such WAN interface.<br>**Authentication Protocol** – Such protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**. In general, the default setting is None.<br>● **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically.<br>● **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields.<br>**Key ID** – Type a value (range from 1 to 65535) which will |

| | |
|---|---|
| | be used to generate HMAC-MD5 value.<br>**Realm** – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.<br>**Secret** – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through NS Detect or Ping Detect.<br>**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.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **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.<br>**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.<br>**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 – 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.<br>**Prefix Length –** Enter the fixed value for prefix length.<br>**Add –** Click it to add a new entry.<br>**Update** - Click it to modify an existed entry.<br>**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.<br>**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.<br>● **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.<br>**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.<br>**Bridge Subnet** – Make a bridge between the selected LAN subnet and such WAN interface. |

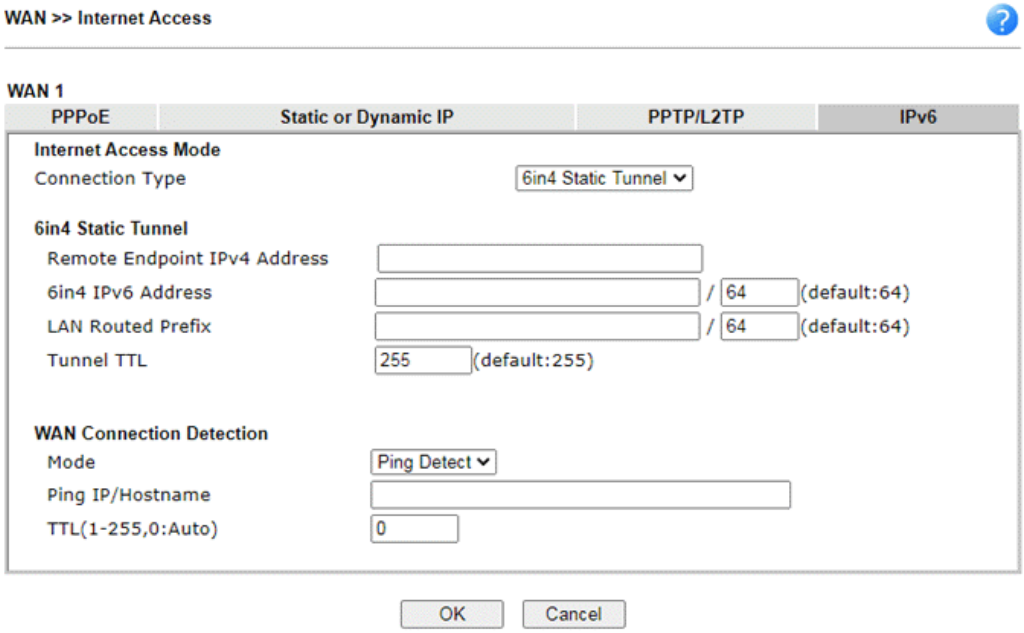
After finished the above settings, click **OK** to save the settings.

## II-1-2-13 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.



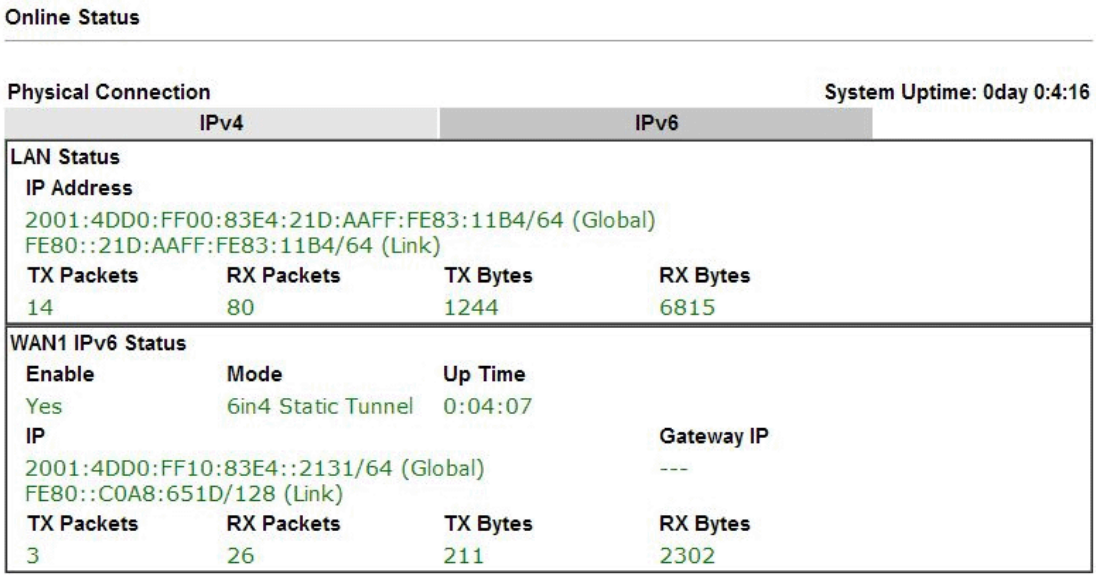

Available settings are explained as follows:

| Item | Description |
|---|---|
| **6in4 Static Tunnel** | **Remote Endpoint IPv4 Address -** Enter the static IPv4 address for the remote server.<br>**6in4 IPv6 Address** - Enter the static IPv6 address for IPv4 tunnel with the value for prefix length.<br>**LAN Routed Prefix** - Enter the static IPv6 address for LAN |

| | |
|---|---|
| | routing with the value for prefix length.<br>**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.<br>**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.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value. |

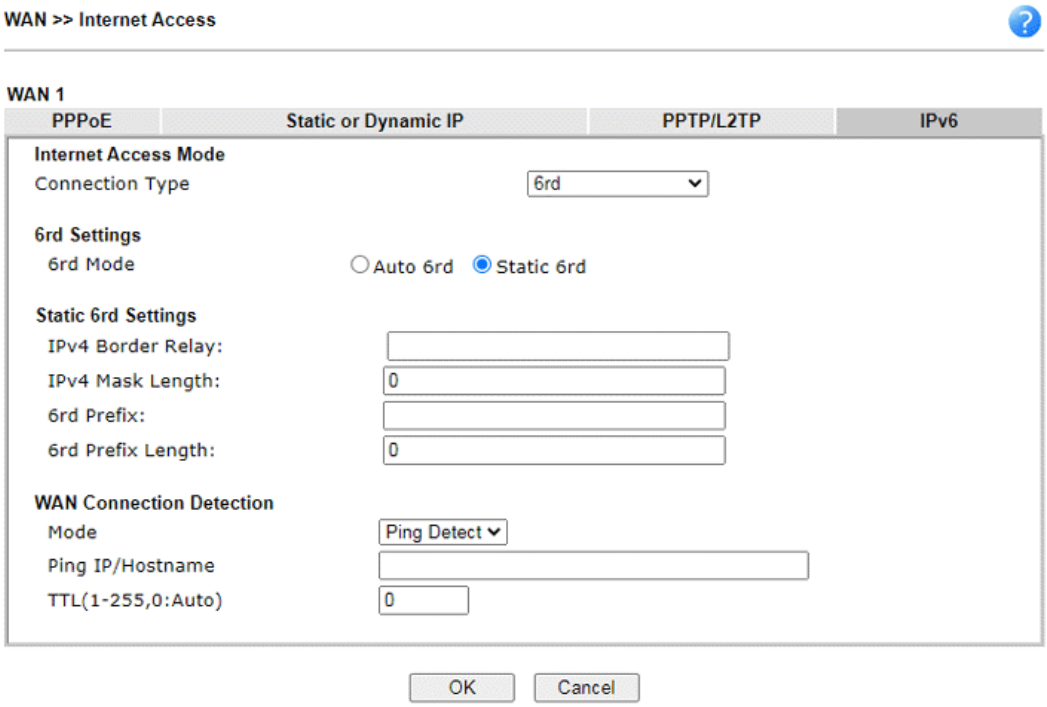
After finished the above settings, click **OK** to save the settings.

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



## II-1-2-14 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".<br>**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.<br>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.<br>**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.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **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.

**Online Status**

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

| IPv4 | IPv6 |
|---|---|

**LAN Status**

**IP Address**

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

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

**WAN1 IPv6 Status**

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

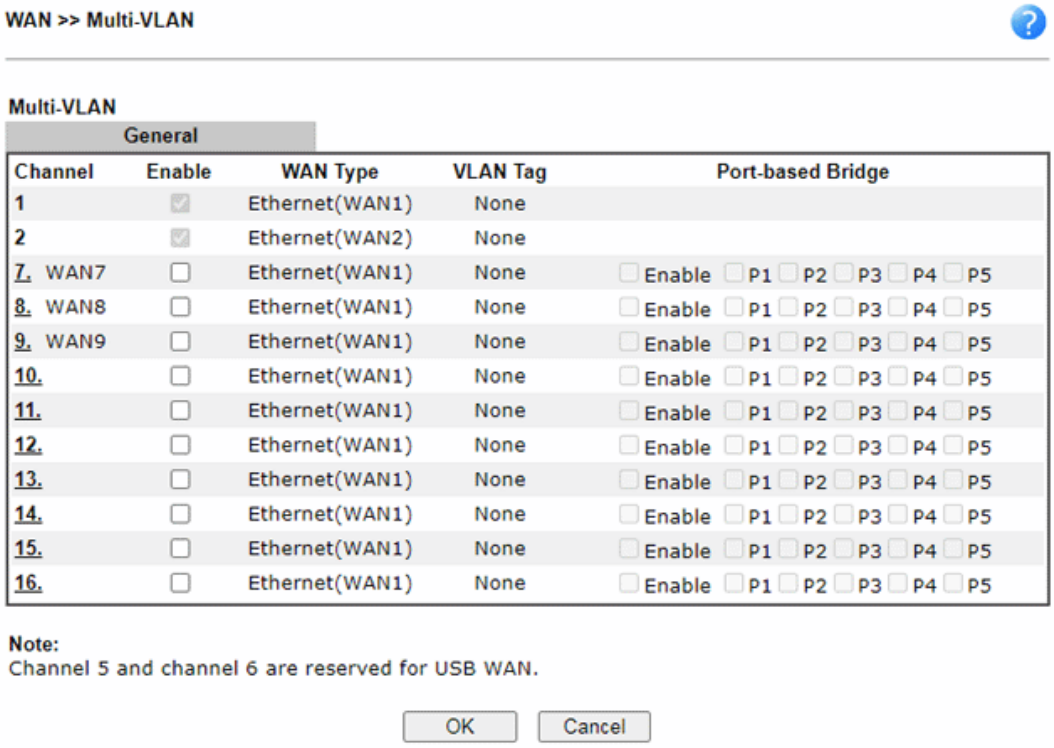
## II-1-3 Multi-VLAN

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

- Channel 1/2: Ethernet on WAN1/WAN2.
- Channel 3: Wireless 2.4GHz on WAN3.
- Channel 4: Wireless 5GHz on WAN4.
- Channel 5/6: USB1/USB2 (WAN5/WAN6).

**Channels 7 through 16** can be bridged to one or more of the 4 LAN ports P2 through P5. In addition, **Channels 7 through 9** can be configured as virtual WANs (WAN7 through WAN9).

### General



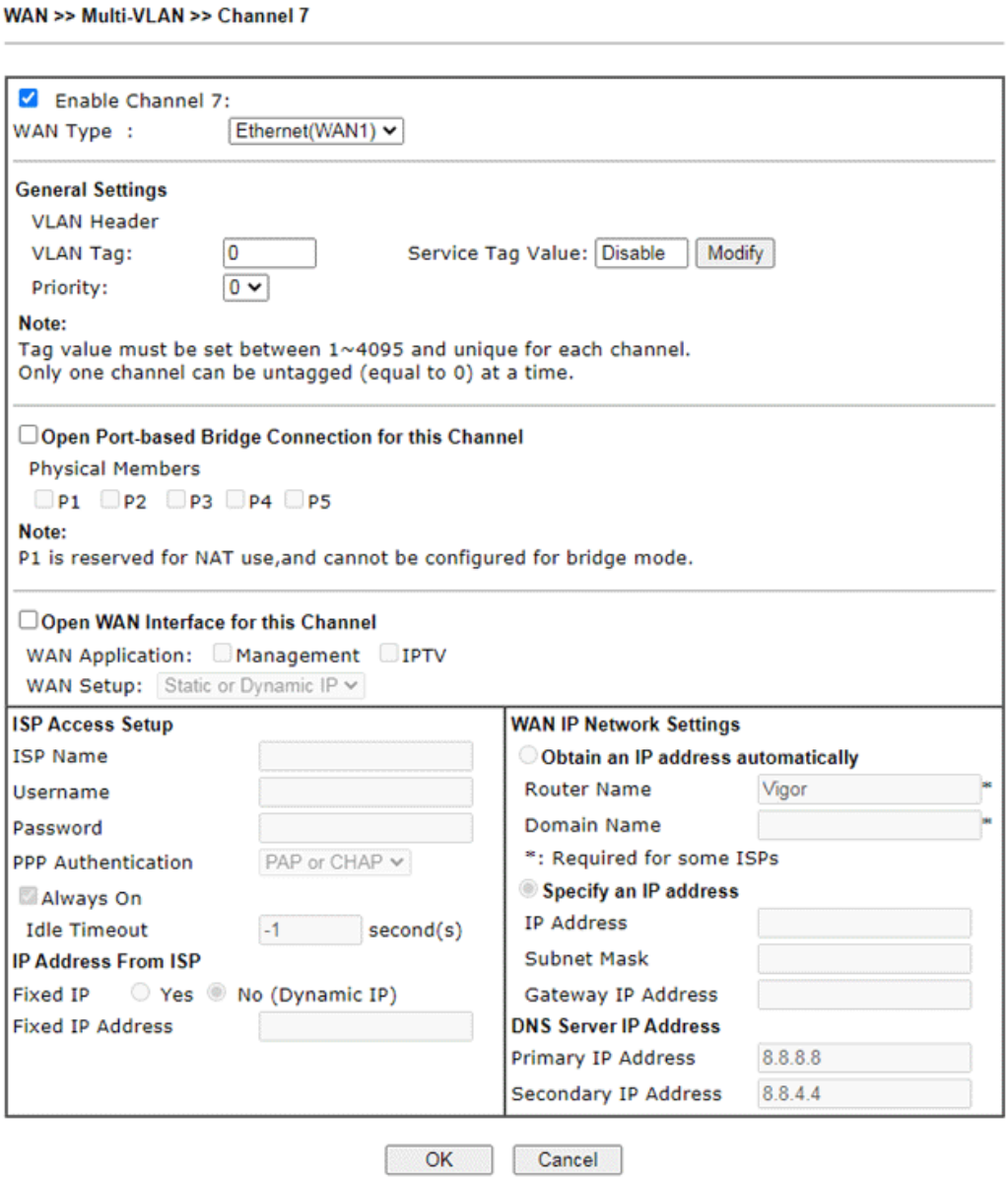

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Channel** | Display the number of each channel.<br>Channels 7 ~ 16 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.<br>**Enable** - Check this box to enable the port-based bridge function on this channel.<br>**P1 ~ P5** – Check the box(es) to build bridge connection on LAN. |

To configure a PVC channel, click its channel number.

WAN links for Channel 7, 8 and 9 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 7, 8 and 9 to configure your router.




Available settings are explained as follows:

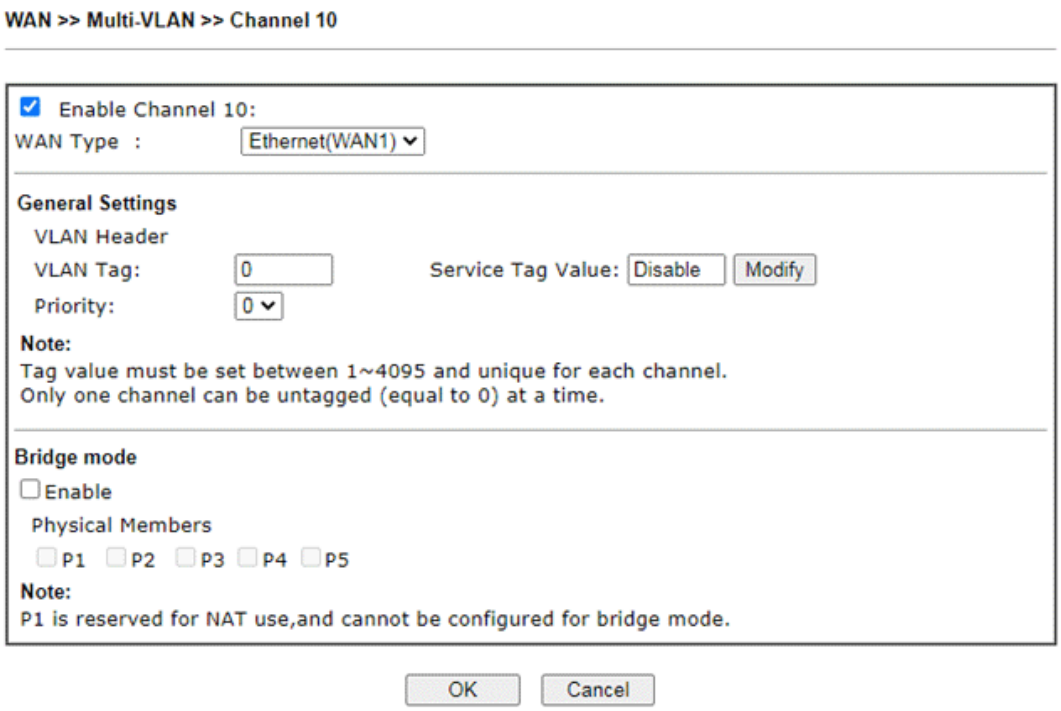
| Item | Description |
|---|---|
| **Enable Channel 7/8/9** | Check it to enable this channel. |
| **WAN Type** | Specify a WAN type of the VLAN.<br>**Ethernet (WAN1/2)** - A VLAN will be created on WAN1/2. |
| **General Settings** | **VLAN Tag –** Enter the value as the VLAN ID number. Valid settings 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.<br>**Priority –** Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.<br>**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.<br>**Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.<br>**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.<br>**WAN Application -**<br>● **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.<br>● **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.<br>**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.<br>**ISP Name** – PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank.<br>**Username** – Name provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters.<br>**Password** – Password provided by the ISP for PPPoE/PPPoA authentication. Maximum length is 62 characters.<br>**PPP Authentication** –The protocol used for PPP authentication.<br>● **PAP only**- Only PAP (Password Authentication Protocol) is used.<br>● **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.<br>**Always On** – If selected, the router will maintain the PPPoE/PPPoA connection.<br>**Idle Timeout** – Maximum length of time, in seconds, of idling allowed (no traffic) before the connection is dropped.<br>**IP Address From ISP** - Specifies how the WAN IP address of the channel configured.<br>● **Fixed IP**<br>**Yes** - IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN.<br>**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.<br>● **Router Name** – Sets the value of DHCP Option 12, which is used by some ISPs.<br>● **Domain Name** – Sets the value of DHCP Option 15, which is used by some ISPs.<br>**Specify an IP address** – Select this option to manually enter the IP address.<br>● **IP Address** – Type in the IP address.<br>● **Subnet Mask** – Type in the subnet mask.<br>● **Gateway IP Address** – Type in gateway IP address.<br>**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 (10~16) to get the following web page:




Available settings are explained as follows:

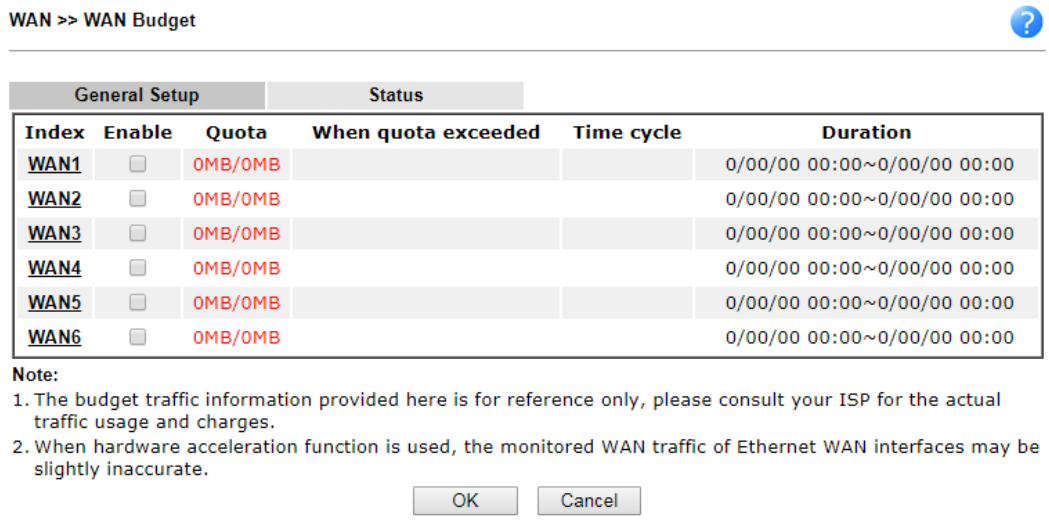
| Item | Description |
|---|---|
| **Enable Channel 10~16** | Click it to enable the configuration of this channel. |
| **WAN Type** | The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is 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.<br>**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.<br>**Physical Members –** Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.<br>**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.

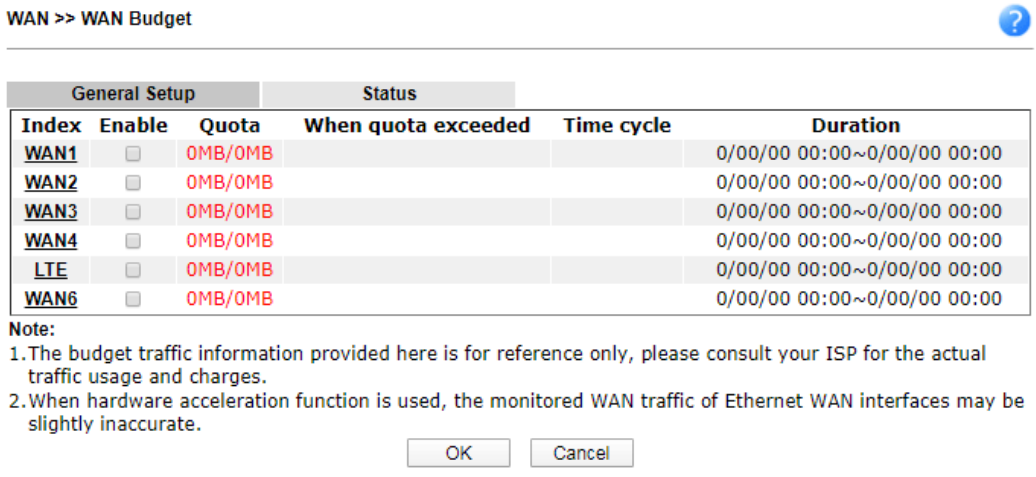
## II-1-4 WAN Budget

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



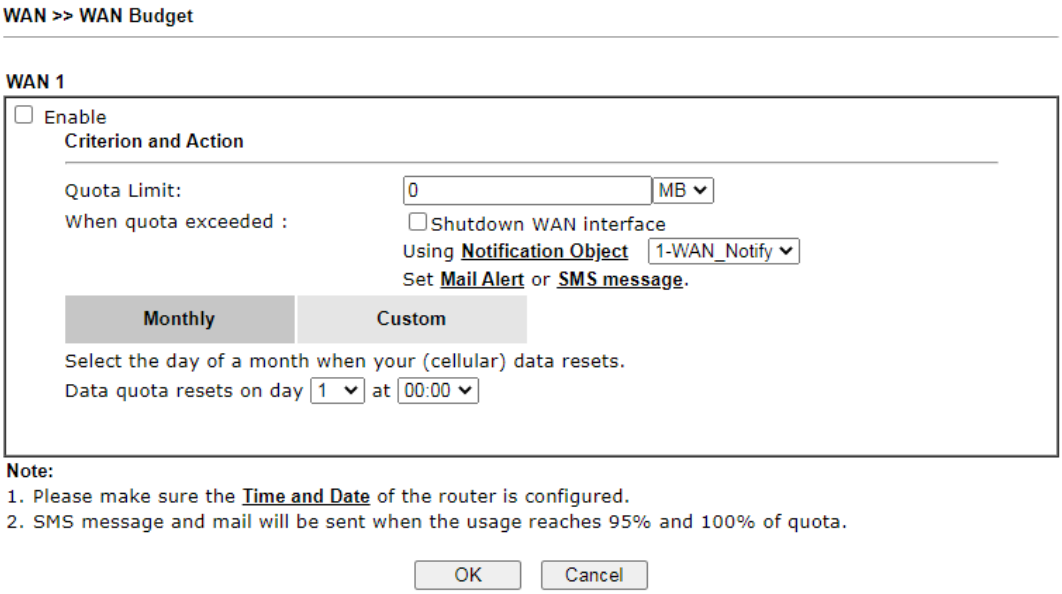

or




| Item | Description |
|---|---|
| **Index** | The WAN port.<br>Click to configure WAN Budget for a particular WAN. |
| **Enable** | **v -** WAN Budget is enabled on this WAN.<br>**x -** WAN Budget is disabled on this WAN. |
| **Quota** | The current cycle's Internet usage is expressed as *x*/*y* where *x* is the cumulative usage and *y* is the upper limit. For example, 100MB/200MB means the usage thus far in this cycle is 100MB, and the upper limit is 200MB. |

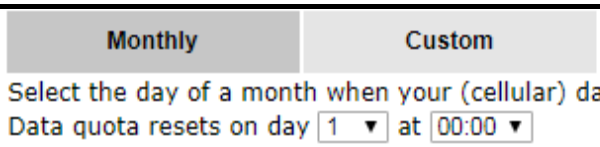
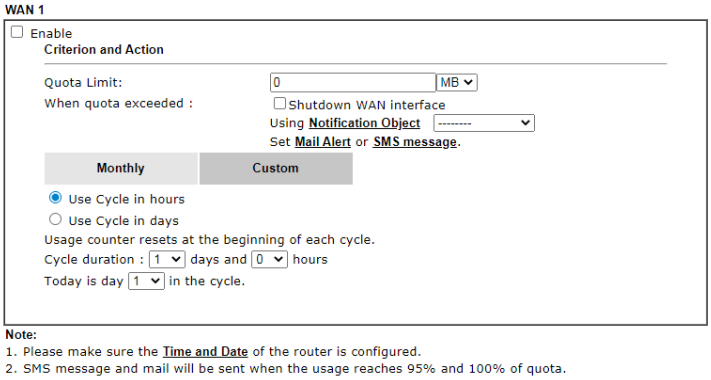
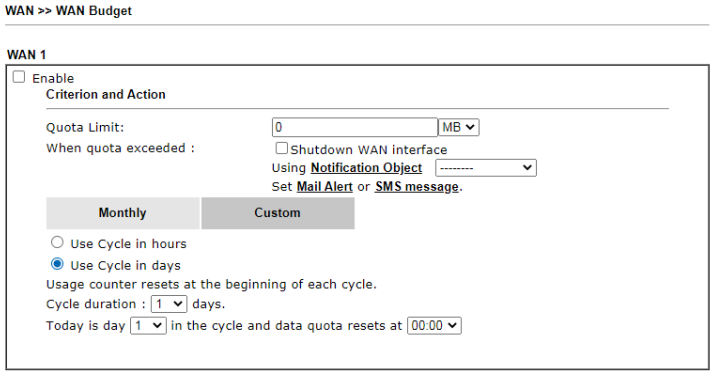
| | |
|---|---|
| **When quota exceeded** | Actions to be taken once the quota is reached.<br>**Shutdown** – WAN will be disabled.<br>**Mail Alert** – Email will be sent to the administrator. |
| **Time cycle** | Reset frequency of the usage data.<br>**Monthly** – The Monthly option in the **Criterion and Action** tab was used to set up the usage quota.<br>**User Defined**: The User Defined option in the **Criterion and Action** tab was used to set up the usage qota. |
| **Duration** | Start and end timestamps of the current cycle. |

Click WAN1 (to WAN6) or LTE 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.<br>**Shutdown WAN interface** – All the outgoing traffic through such WAN interface will be terminated.<br>● **Using Notification Object** – The system will send out a notification based on the content of the notification object.<br>● **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.<br>● **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. |

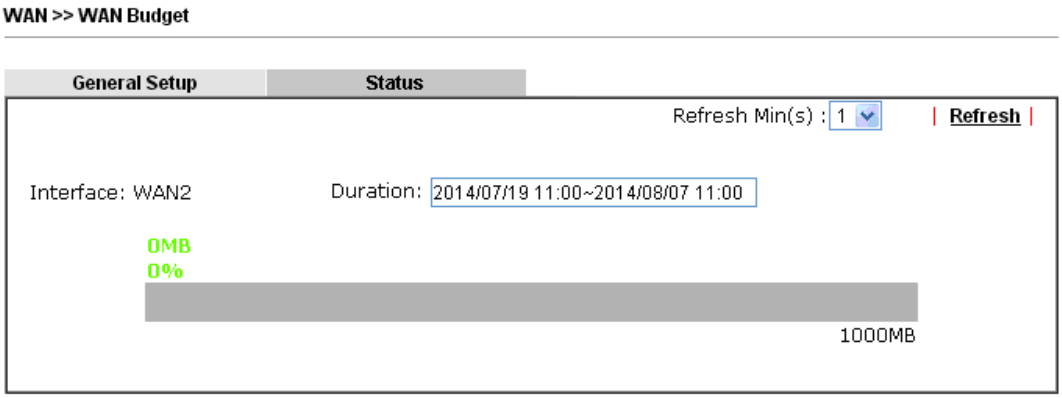
| | |
|---|---|
| |  <br>**Data quota resets on day …** – You can determine the starting day in one month. |
| **Custom** | This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle.<br>Monthly is default setting. 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.<br>**Use Cycle in hours** –<br>  <br>● **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.<br>● **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.<br>**Use Cycle in days** -<br>  <br>● **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.<br>● **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. |

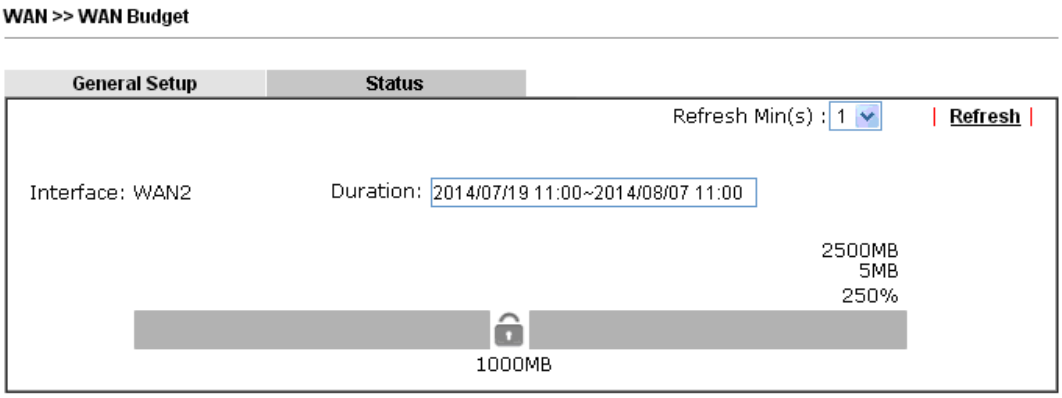
After finished the above settings, click **OK** to save the settings.

## 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.

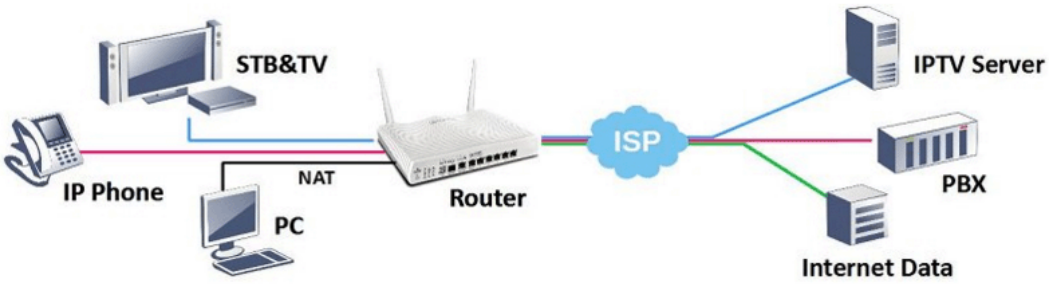


# Application Notes

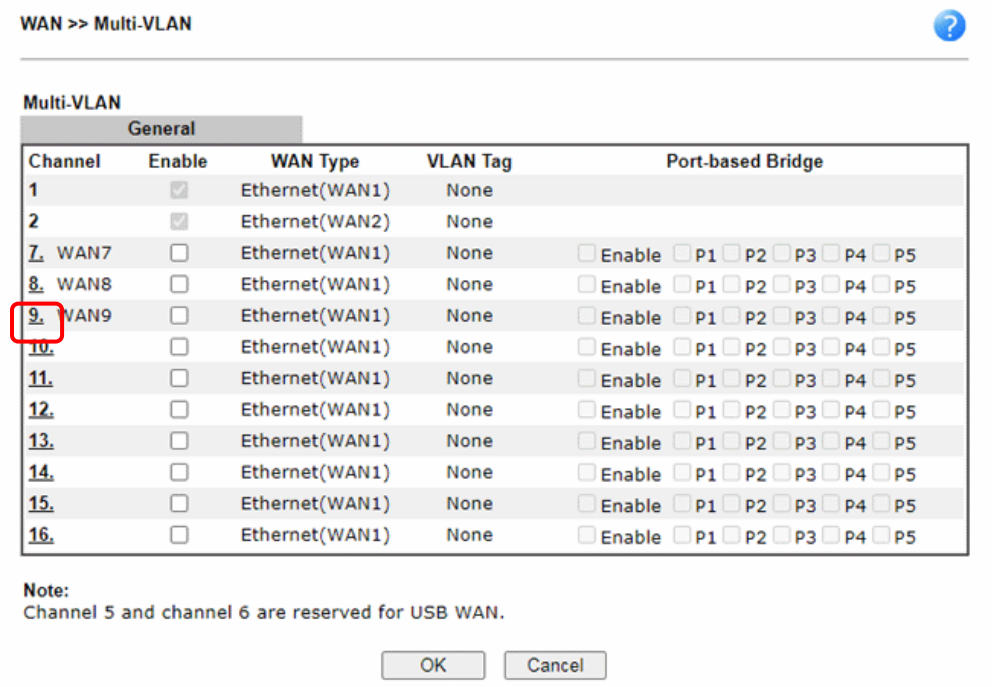
## A-1 How to set up Multi-PVC for triple play deployment?

By adding VLAN tags to differentiate the traffic, the service provider is able to deliver video, voice, and data to the subscribers over a single connection, which is also known as the triple play service. This document is going to demonstrate how to configure the Multi-PVC feature for triple play deployment. There are two types of setup, one is doing port-based bridge that will connect the media, such as the set-top box (STB), directly to the service provider via a specific LAN port; the other is opening a virtual WAN interface and doing NAT for the application.

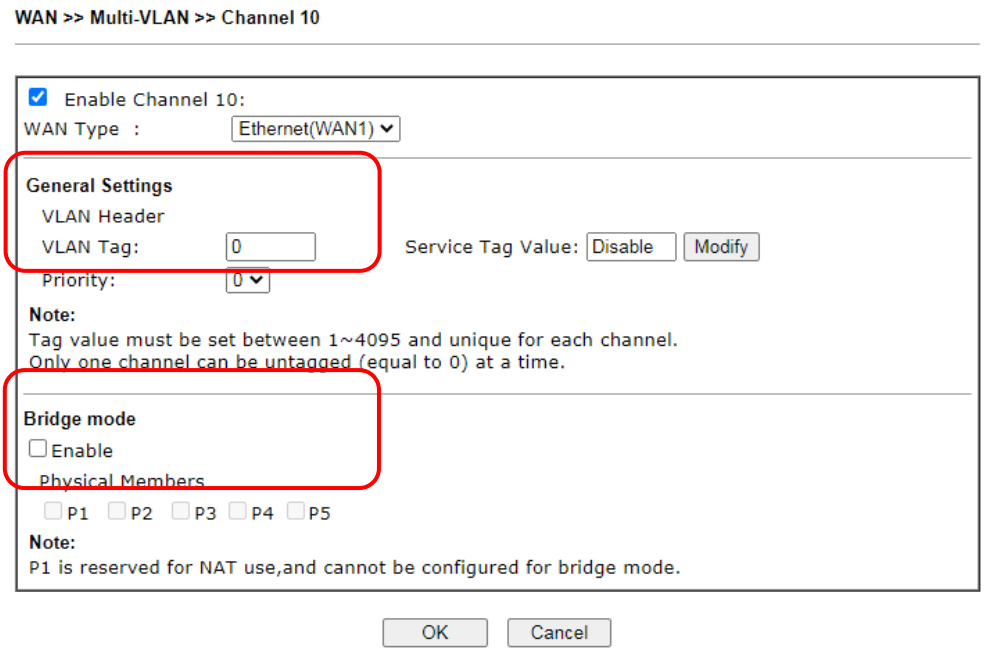
### Bridge the Virtual WAN to a LAN port




1. Go to **WAN >> Multi-VLAN**, click on a channel to configure.



2. Configure the channel as follows,




(a) enable this channel.

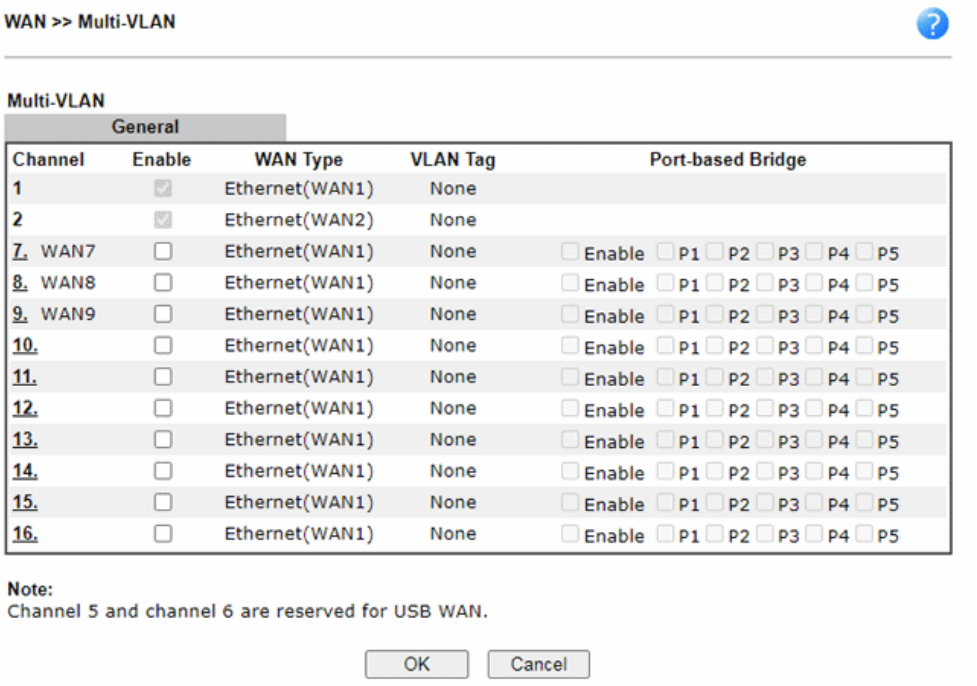
(b) set WAN Type to the WAN interface that the service provider is on.

(c) set up VPI and VCI if the WAN is an ADSL line.

(d) enable Add VLAN Header and enter the VLAN Tag and Priority as the service provider requires.

(e) check Enable for Bridge Mode, and select the physical port member to which you're going to connect the STB.

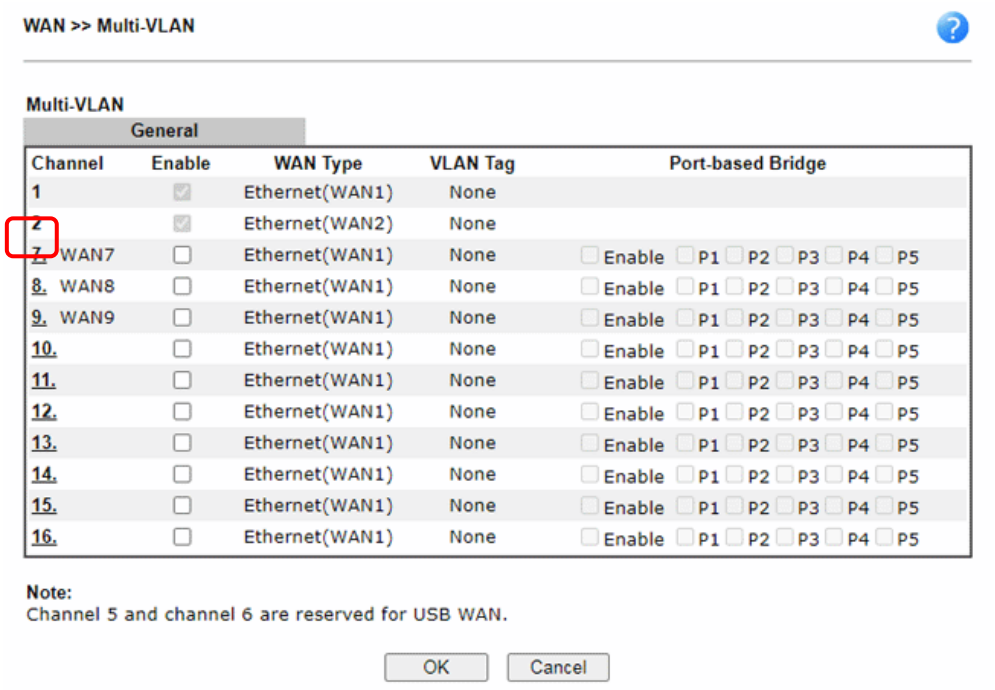
3. Click **OK** to save the configuration, the configuration will be displayed on the main page. And now you may connect the STB to the Bridged port to use the IPTV service.



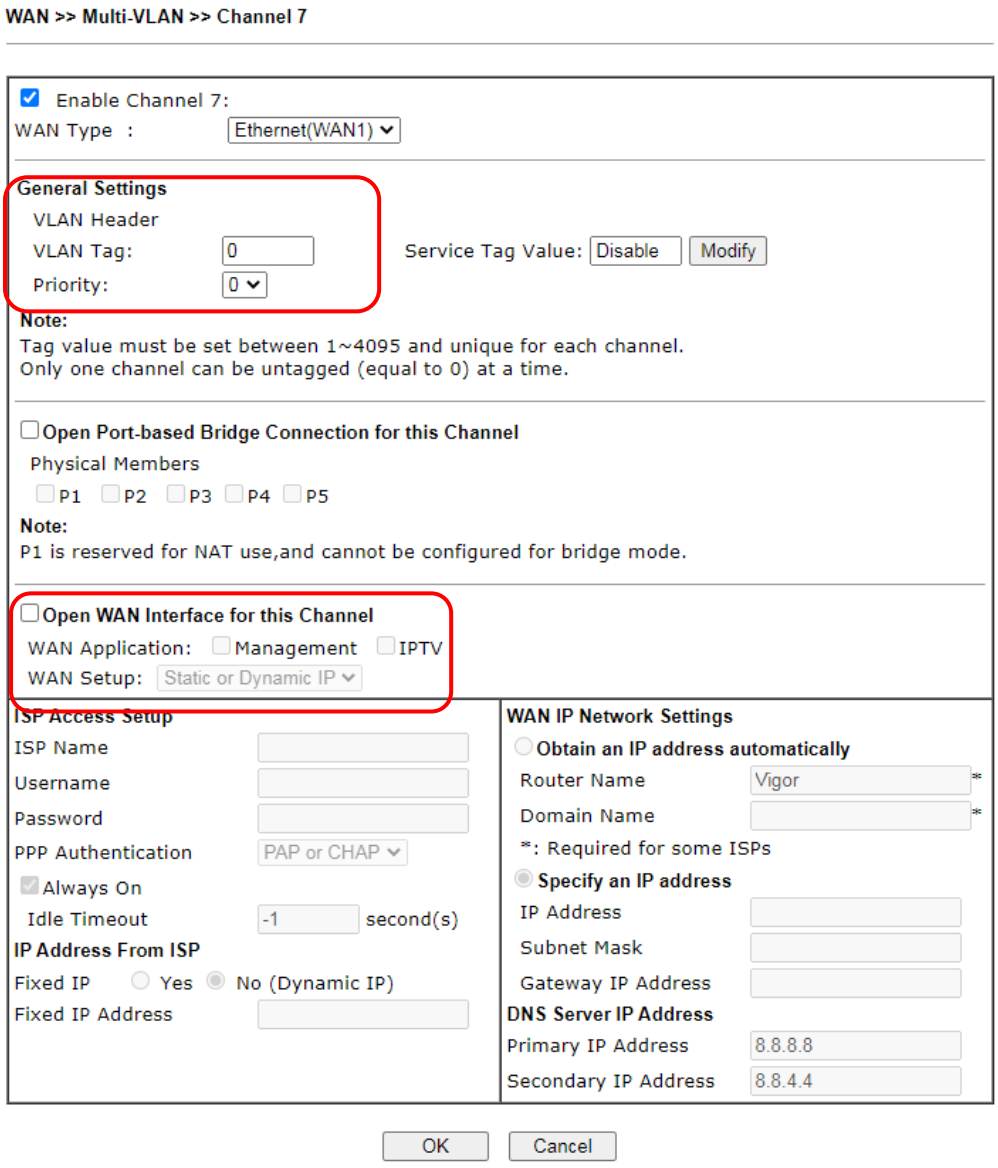
## Open a Virtual WAN Interface




1. Go to **WAN >> Multi-PVC/VLAN**, click on channel 7, 8 or 9 to configure.



2. Configure the channel as follows,




(a) enable this channel.

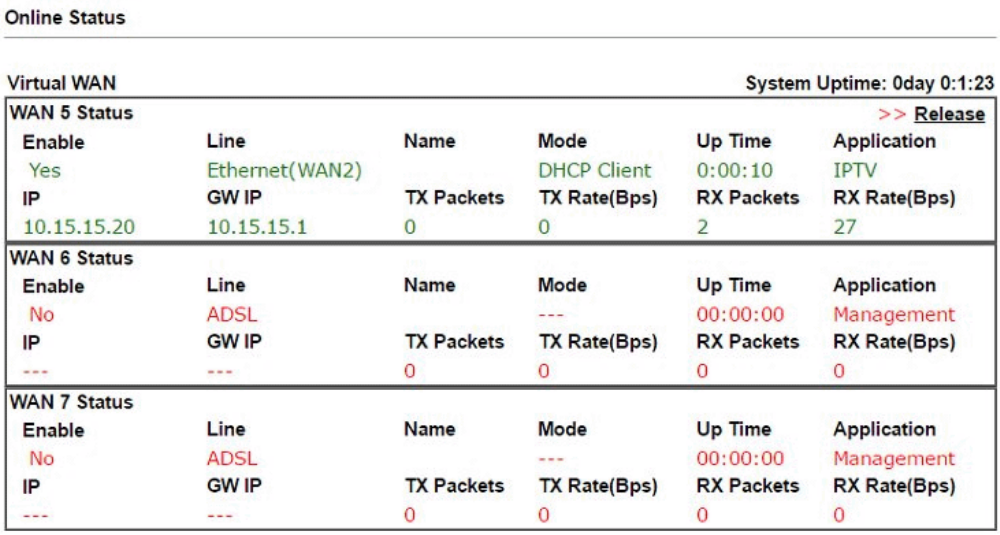
(b) set WAN Type to the WAN interface that the service provider is on.

(c) enter the VLAN Tag and Priority as the service provider requires.

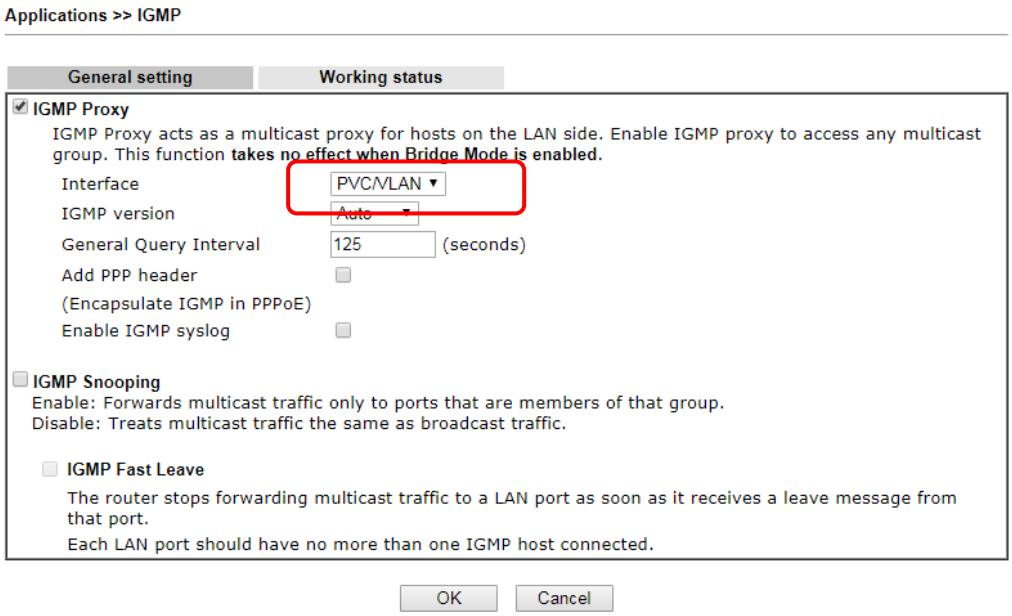
(d) enable "Open WAN Interface for this Channel", and select the kind of Application will be used on this channel. (Note: this option is only available on channel 5-7)

(e) set up the Internet Access type as the ISP requires.

3. Click OK to save the profile and reboot the router to apply the settings. After the router restart, go to **Online Status >> Virtual WAN** to make sure the WAN interface is up and has obtained an IP address.



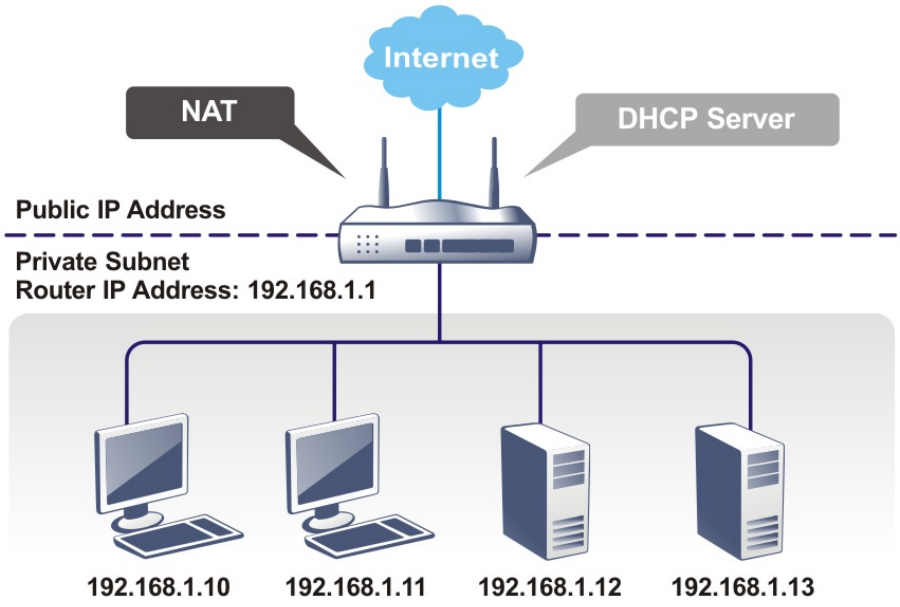

4. Now, you may use the virtual WAN interface for applications such as IGMP Proxy, this can be done by selecting the WAN interface as "PVC/VLAN".



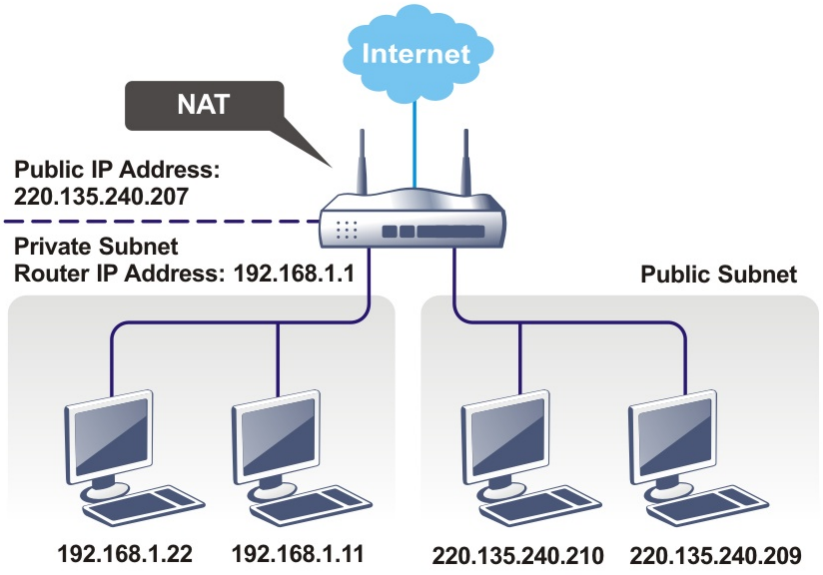
# II-2 LAN

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)

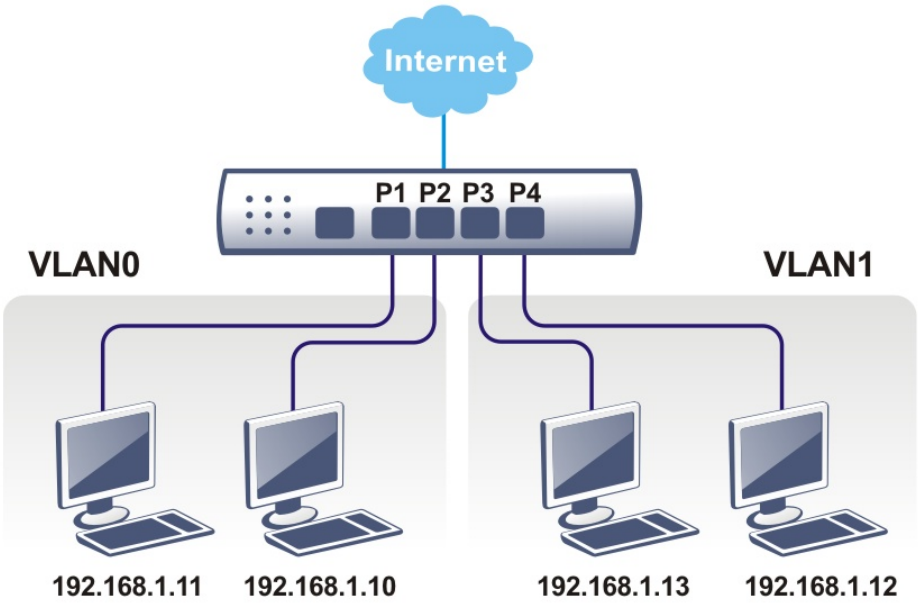
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### 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 Vigor2927.

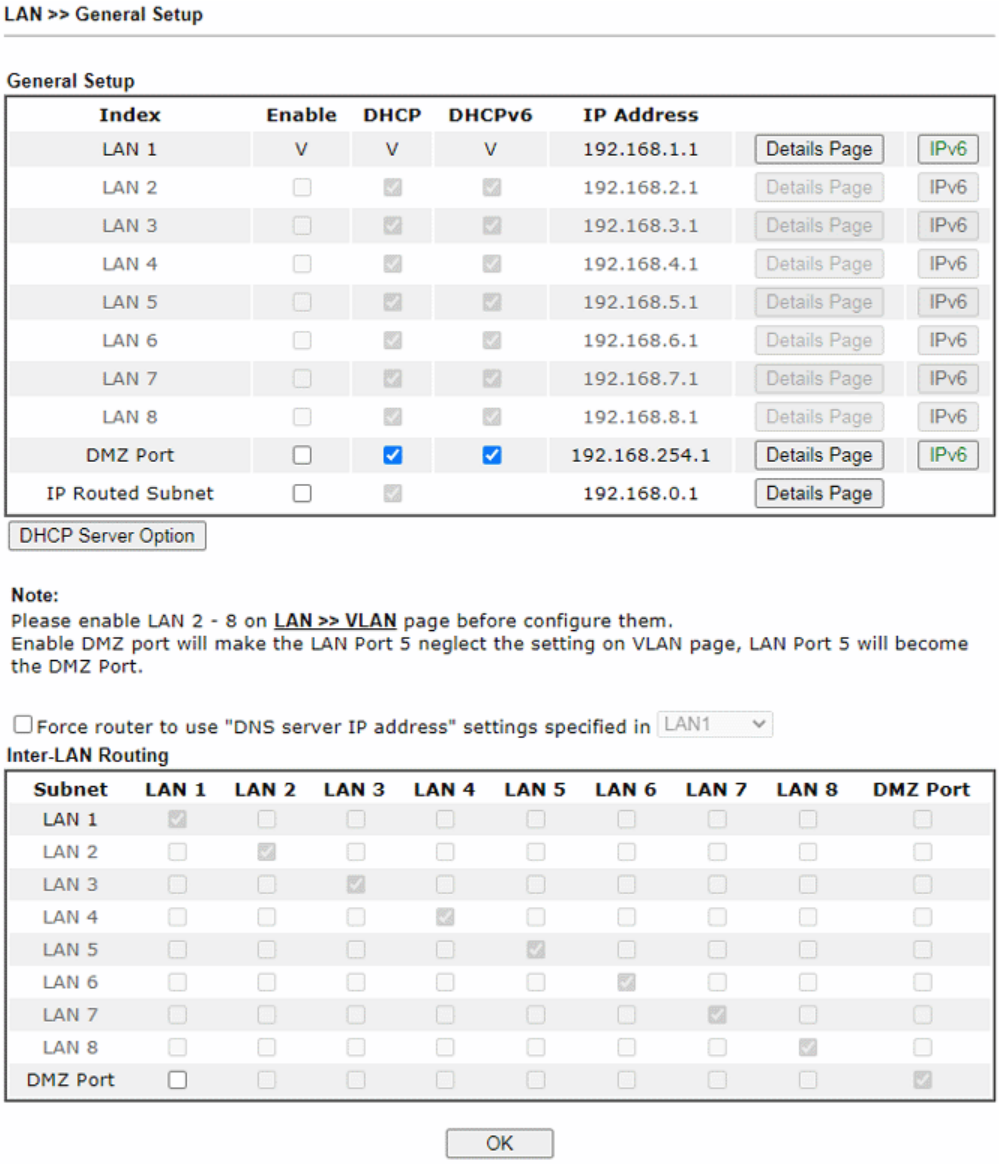
To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router (such as the Vigor 2862) that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach 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 eight subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN8). 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 – LAN8 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.<br>**Index -** Display all of the LAN items.<br>**Status-** Basically, LAN1 status is enabled in default. LAN2 –LAN8 and IP Routed Subnet can be observed by checking the box of **Status**.<br>**DHCP/DHCPv6-** LAN1 is configured with DHCP/DHCPv6 in default. If required, please check the DHCP box for each LAN.<br>**IP Address -** Display the IP address for each LAN item. Such information is set in default and you can not modify it.<br>**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.**<br>**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.<br>For detailed information, refer to later section. |

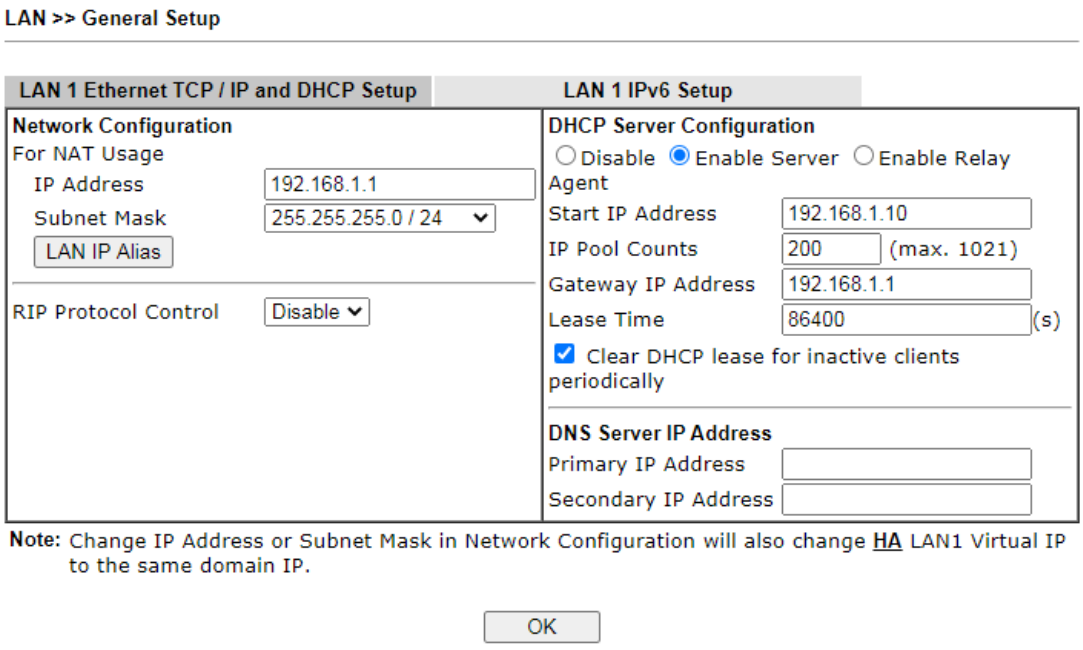
| | |
|---|---|
| **Force router to use "DNS server IP address ….."** | Force Vigor router to use DNS servers configured in LAN1/LAN2/LAN3/LAN4/LAN5/LAN6/LAN7/LAN8/DMZ Port instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server). |
| **Inter-LAN Routing** | Check the box to link two or more different subnets (LAN and LAN).<br>Inter-LAN Routing allows different LAN subnets to be interconnected or isolated.<br>It is only available when the VLAN functionality is enabled. Refer to section II-2-2 VLAN on how to set up VLANs.<br>In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other. |

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

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

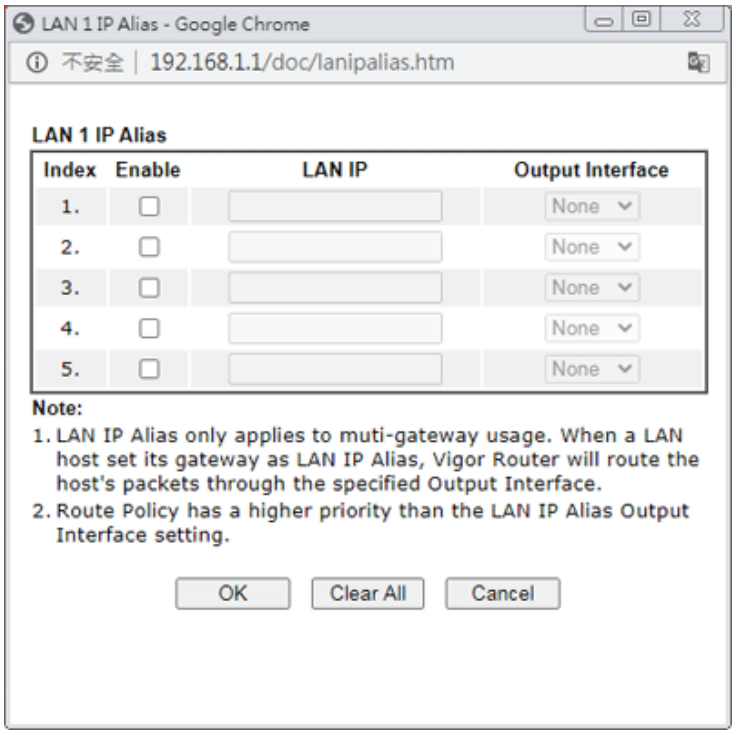
## II-2-1-1 Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

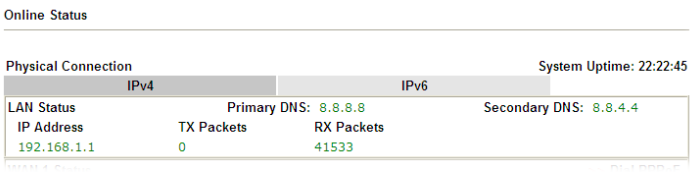
There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Network Configuration** | **For NAT Usage,**<br>**IP Address** - This is the IP address of the router. (Default: 192.168.1.1).<br>**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).<br>**LAN IP Alias** –Such feature allows specifying multiple gateways (under a switch) with different WAN interfaces for accessing the Internet via the Vigor router.<br>  <br><br>**RIP Protocol Control,**<br>**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.<br>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.<br>**Disable –** Let you manually assign IP address to every host in the LAN.<br>**Enable Server -** Let the router assign IP address to every host in the LAN.<br>● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients.<br>● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 200. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller.<br>● **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.<br>● **Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.<br>● **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.<br>**Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following:<br>■ Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30<br>■ Clear DHCP lease when the client is not responding ARP replies.<br>**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.<br>● **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.<br>**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.<br>**Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.<br>The default DNS Server IP address can be found via Online Status:<br>  <br>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.<br>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. |

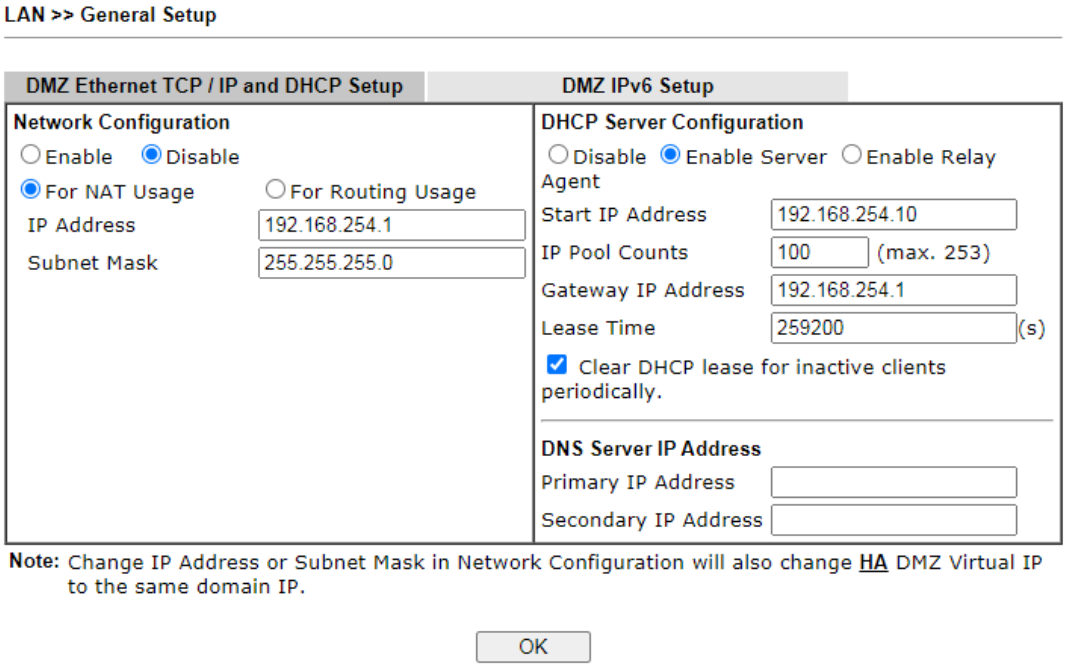
When you finish the configuration, please click **OK** to save and exit this page.

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.

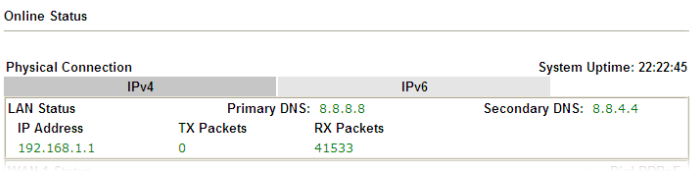
Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude 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 ~ LAN8 and DMZ



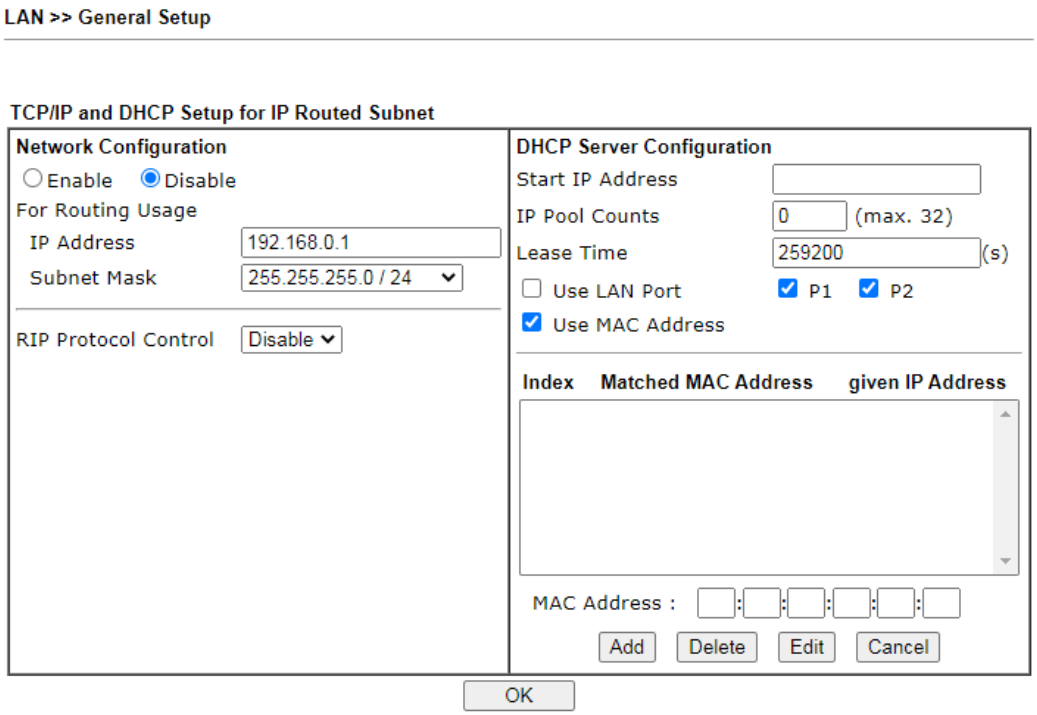

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Network Configuration** | **Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration.<br>**For NAT Usage -** Click this radio button to invoke NAT function.<br>**For Routing Usage -** Click this radio button to invoke this function.<br>**IP Address** - This is the IP address of the router. (Default: 192.168.1.1).<br>**Subnet Mask -** The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0/ 24). |
| **DHCP Server Configuration** | **Disable –** Let you manually assign IP address to every host in the LAN.<br>**Enable Server -** Let the router assign IP address to every host in the LAN.<br>● **Start IP Address -** The beginning LAN IP address that is given out to LAN DHCP clients.<br>● **IP Pool Counts -** The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 1021. The actual number of IP addresses available for assignment is the IP Pool Counts, or 1021 minus the last octet of the Start IP Address, whichever is smaller.<br>● **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.<br>● **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.<br>**Note**: When Clear DHCP lease for inactive clients periodically is enabled, router will do the following:<br>- Check activities of DHCP clients by ARP requests every minute when the available DHCP IP addresses are less than 30<br>- Clear DHCP lease when the client is not responding ARP replies.<br>**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.<br>● **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.<br>**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.<br>**Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.<br>The default DNS Server IP address can be found via Online Status:<br>  <br>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.<br>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:

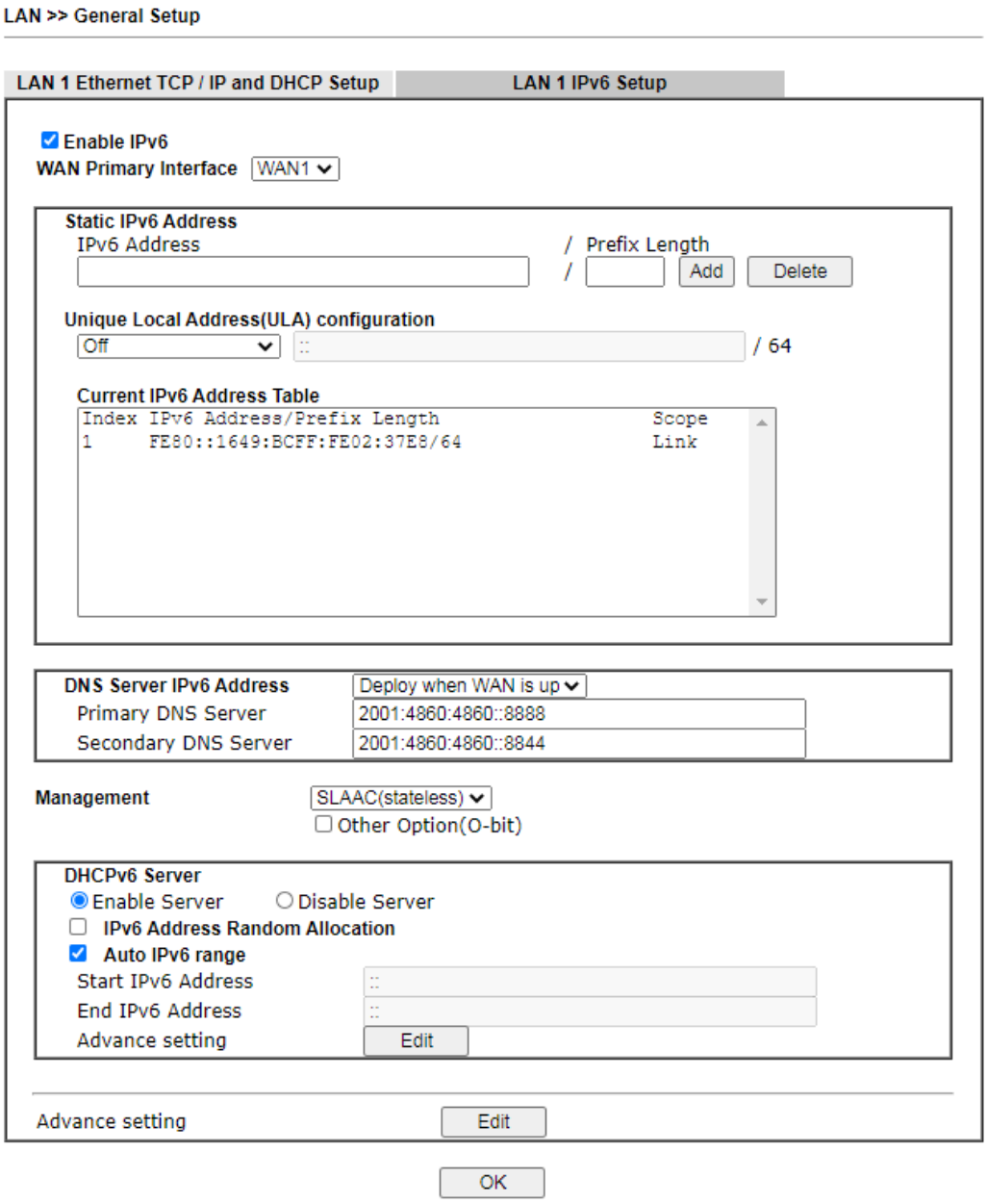
| Item | Description |
|---|---|
| **Network Configuration** | **Enable/Disable -** Click **Enable** to enable such configuration; click **Disable** to disable such configuration.<br>**For Routing Usage,**<br>**IP Address** - This is the IP address of the router. (Default: 192.168.1.1).<br>**Subnet Mask -** 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).<br>**RIP Protocol Control,**<br>**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.<br>**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.<br>**IP Pool Counts -** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.<br>**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.<br>**Use MAC Address -** Check such box to specify MAC address.<br>● **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.<br>**Add –** Enter the MAC address in the boxes and click this button to add.<br>**Delete** – Click it to delete the selected MAC address.<br>**Edit** – Click it to edit the selected MAC address.<br>**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/LAN5/LAN6/LAN7/LAN8/DMZ Port, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

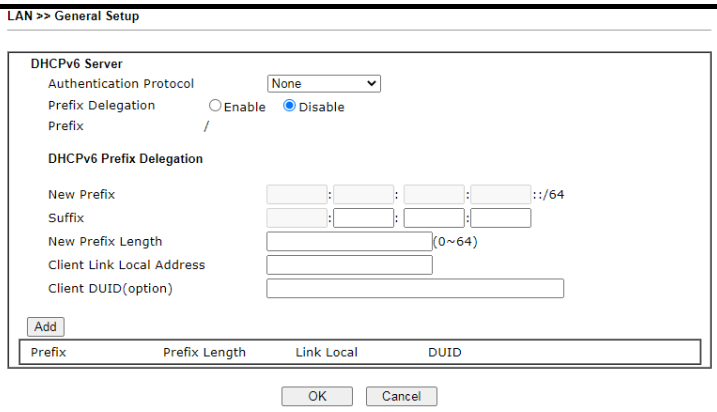



It provides 2 daemons for LAN side IPv6 address configuration. One is **SLAAC**(stateless) and the other is **DHCPv6** (Stateful) server.

Available settings are explained as follows:

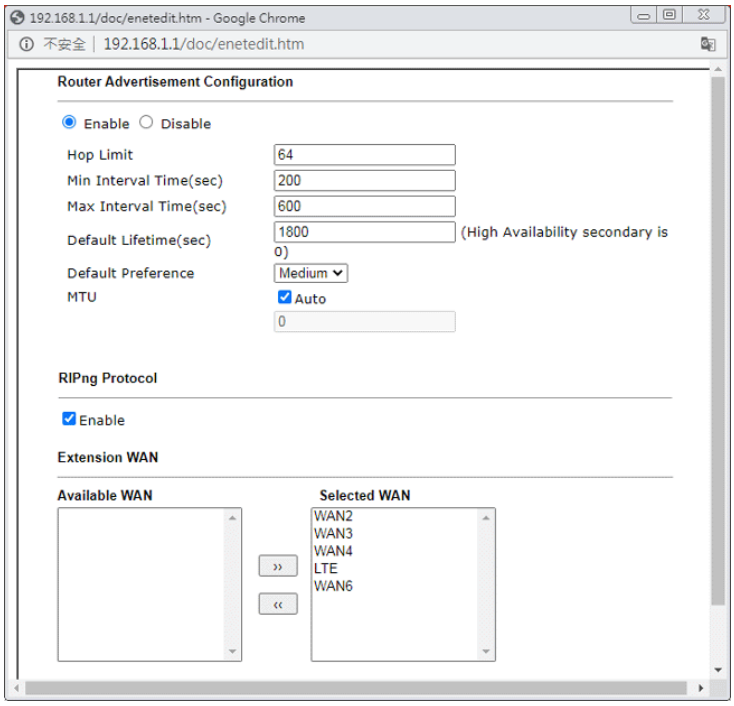
| Item | Description |
|---|---|
| **Enable** | Check the box to enable the configuration of LAN 1 IPv6 Setup. |
| **WAN Primary Interface** | Use the drop down list to specify a WAN interface for IPv6. |
| **Static IPv6 Address configuration** | **IPv6 Address** –Type static IPv6 address for LAN.<br>**Prefix Length** – Enter the fixed value for prefix length. |

| | |
|---|---|
| | **Add –** Click it to add a new entry.<br>**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.<br>**Off -** ULA is disabled.<br>**Manually ULA Prefix -** LAN clients will be assigned ULAs generated based on the prefix manually entered.<br>**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.<br>**Enable** – The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.<br>● **Primary DNS Sever** – Enter the IPv6 address for Primary DNS server.<br>● **Secondary DNS Server** –Type another IPv6 address for DNS server if required.<br>**Disable** – DNS server will not be used. |
| **Management** | Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.<br>● **Off** - No configuration information is sent using Route Advertisements.<br>● **SLAAC(stateless) -** M-bit is unset.<br>● **DHCPv6(stateful**) - M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor2860, or a separate DHCPv6 server.<br>**Other Option (O-bit)** - Check this box to enable the O-bit for obtaining additional information (e.g., DNS) from DHCPv6. |
| **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.<br>**Disable Server** –Click it to disable DHCPv6 server.<br>**Auto IPv6 range –** After check the box, Vigor router will assign the IPv6 range automatically.<br>**Start IPv6 Address** / **End IPv6 Address** –Enter the start and end address for IPv6 server.<br>**Advance setting** – Click the Edit button to configure advanced IPv6 settings for DHCPv6 server. |




**Advance setting**

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




**Router Advertisement Configuration** – Click **Enable** to enable router advertisement server. The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.

**Disable** – Click it to disable router advertisement server.

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

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

**Default Lifetime (sec) -**Within such period of time, Vigor router 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.

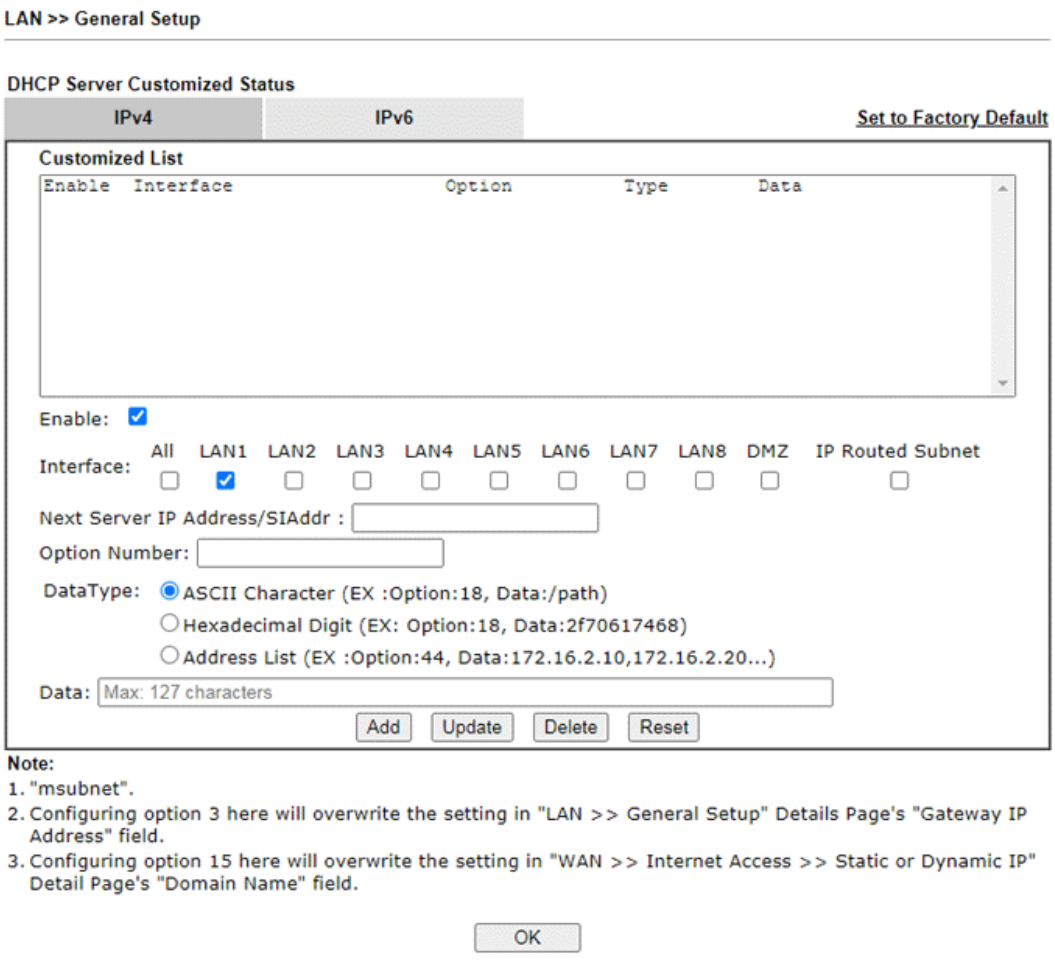
**MTU –** It means Max Transmit Unit for packet. If **Auto** is

| | |
|---|---|
| | selected, the router will determine the MTU value for LAN.<br>**RIPng Protocol -**RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.<br>**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.<br>**Available WAN** – Additional WANs available but not currently selected to carry IPv6 traffic.<br>**Selected WAN** – Additional WANs selected to carry IPv6 traffic. |

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

## II-2-1-5 DHCP Server Options

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Customized List** | Shows all the DHCP options that have been configured in the system. |

| | |
|---|---|
| **Enable** | If selected, DHCP option entry is enabled.<br>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:<br>**ASCII Character** - A text string. Example: /path.<br>**Hexadecimal Digit -** A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.<br>**Address List -** One or more IPv4 addresses, delimited by commas. |
| **Data** | Data of this DHCP option. |

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

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

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

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

## II-2-2 VLAN

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

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

### Tagged VLAN

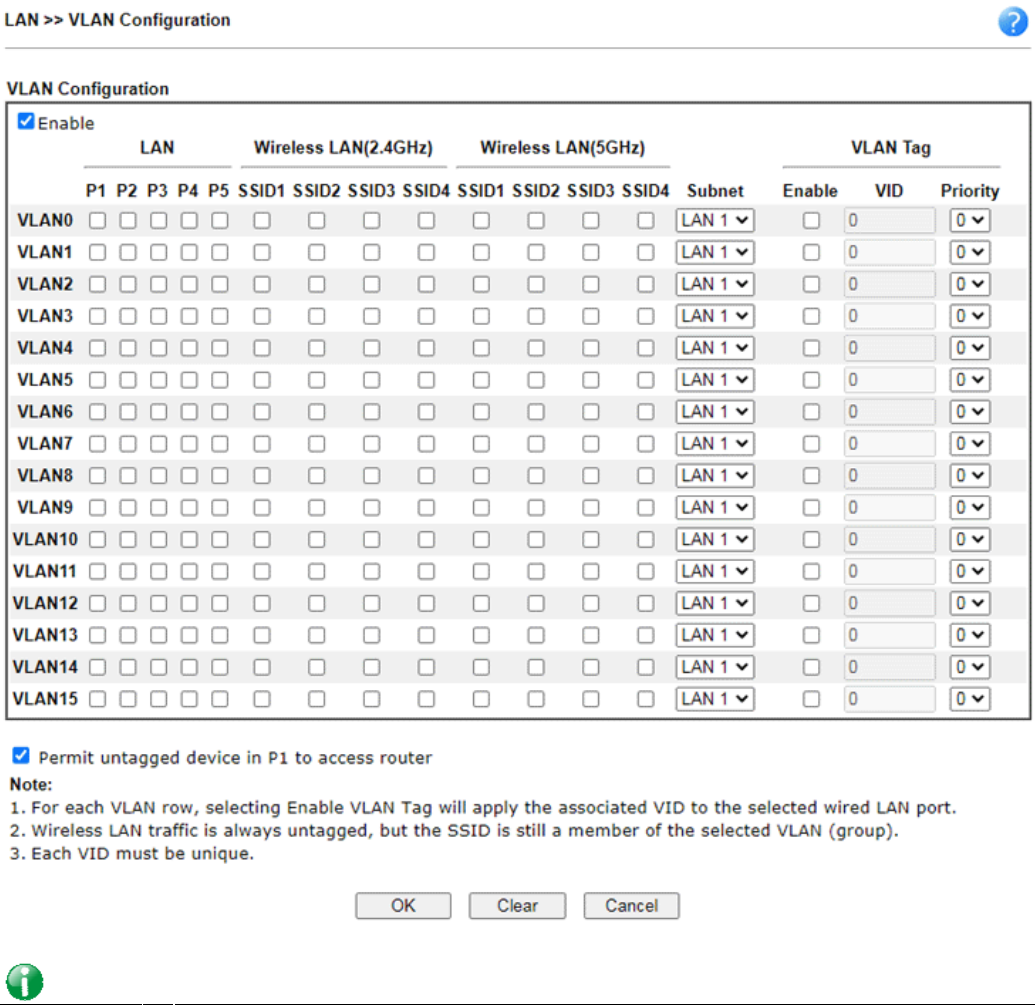
The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each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

### Port-Based VLAN

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

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

Below is an example page in Vigor2927ac:



| | |
|---|---|
| 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 – P5** – 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. |
| **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.<br>The router will add specific VLAN number to all packets on the LAN while sending them out.<br>Please Enter the tag value and specify the priority for the packets sending by LAN.<br>**VID** – Enter the value as the VLAN ID number. The range is form 0 to 4095. VIDs must be unique.<br>**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 15 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

| Subnet | LAN 1 | LAN 2 | LAN 3 | LAN 4 | LAN 5 | LAN 6 | LAN 7 | LAN 8 | DMZ Port |
|---|---|---|---|---|---|---|---|---|---|
| LAN 1 | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| LAN 2 | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| LAN 3 | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| LAN 4 | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ |
| LAN 5 | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ |
| LAN 6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ |
| LAN 7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ |
| LAN 8 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ |
| DMZ Port | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ |

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.

Vigor2927 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.

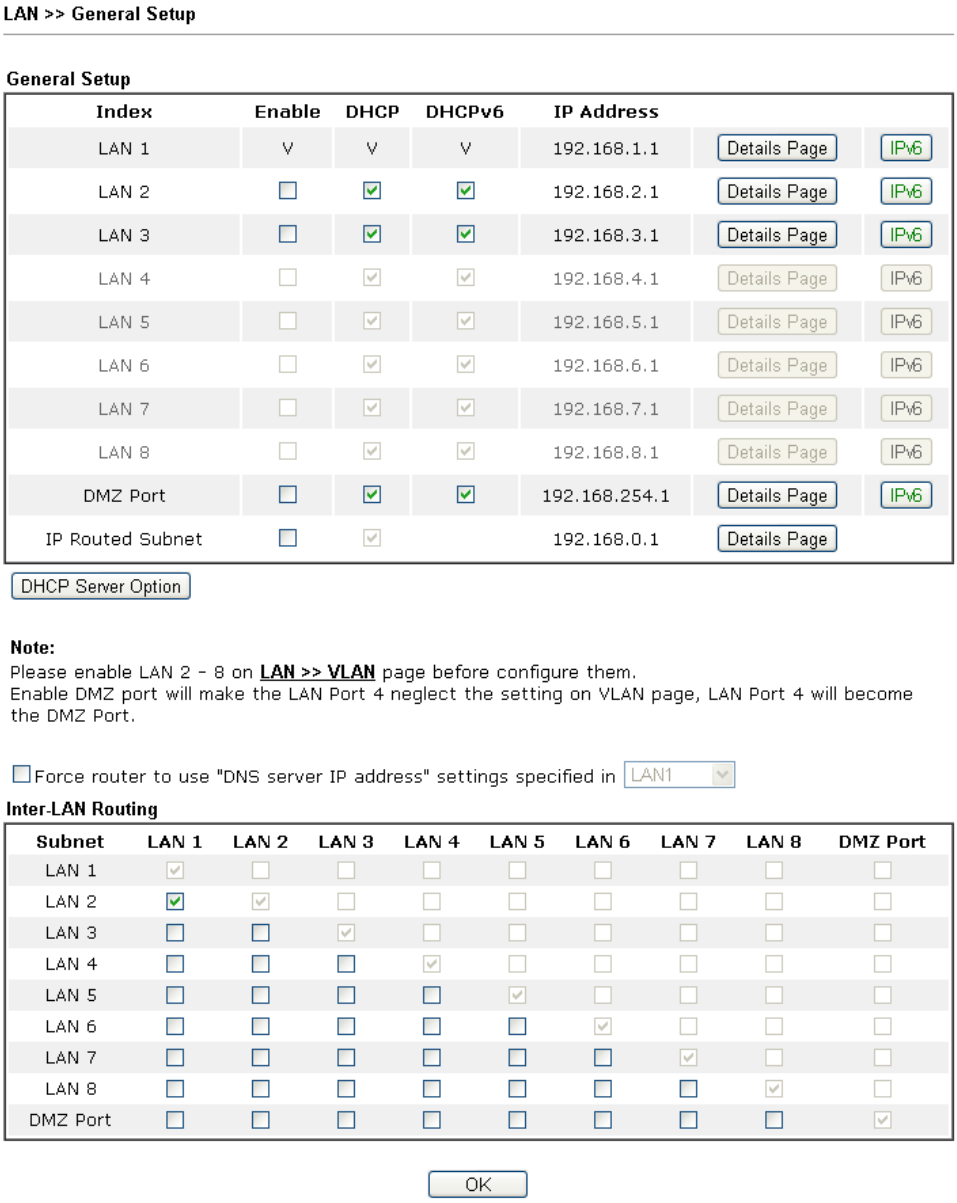
LAN >> VLAN Configuration

VLAN Configuration

☑ Enable

| | LAN | | | | | Wireless LAN(2.4GHz) | | | | Wireless LAN(5GHz) | | | | | VLAN Tag | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | P1 | P2 | P3 | P4 | P5 | SSID1 | SSID2 | SSID3 | SSID4 | SSID1 | SSID2 | SSID3 | SSID4 | Subnet | Enable | VID | Priority |
| VLAN0 | ☑ | ☑ | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |
| VLAN1 | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | LAN 2 | ☐ | 0 | 0 |
| VLAN2 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 3 | ☐ | 0 | 0 |
| VLAN3 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |
| VLAN4 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |
| VLAN5 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |
| VLAN6 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |
| VLAN7 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | LAN 1 | ☐ | 0 | 0 |

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.**



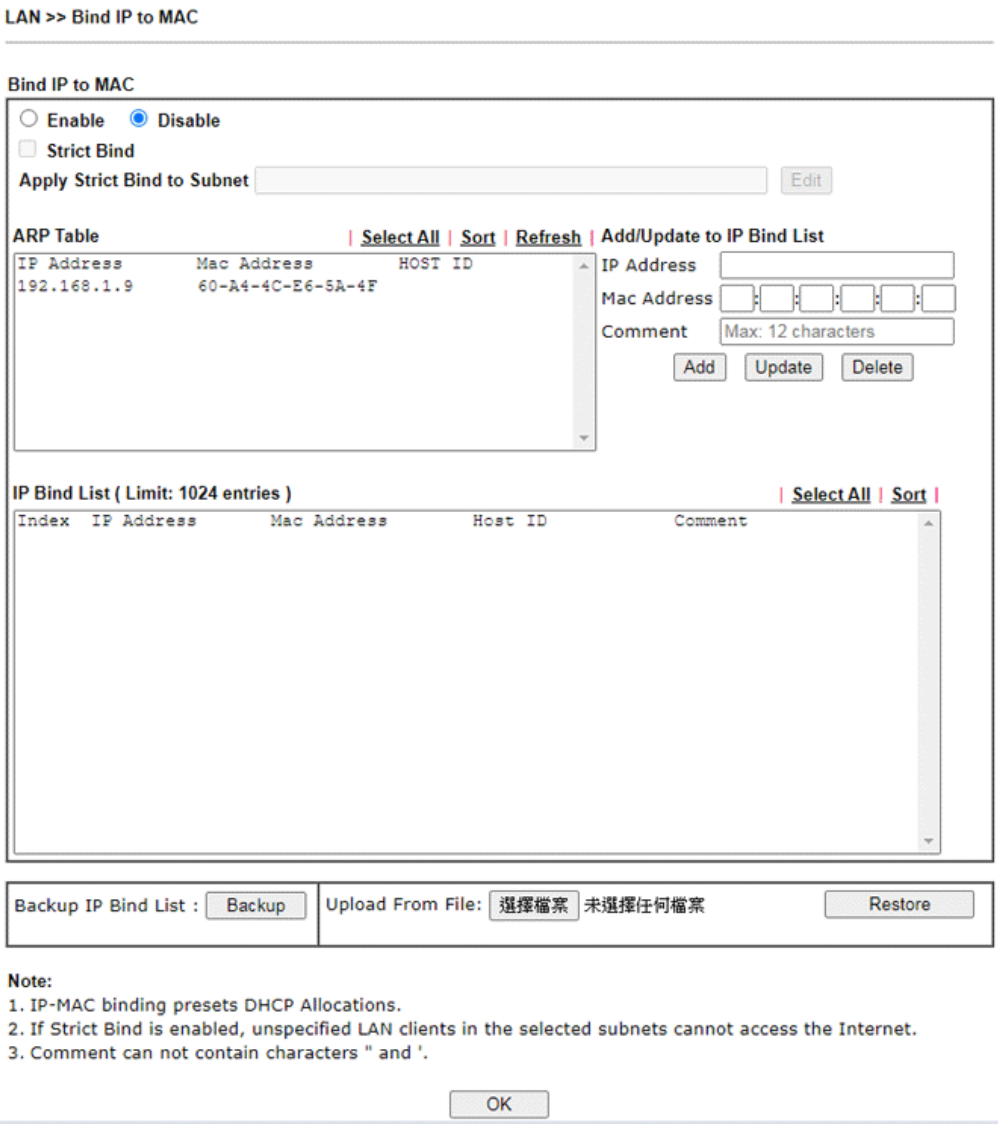

Vigor router supports up to six private IP subnets on LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

| 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

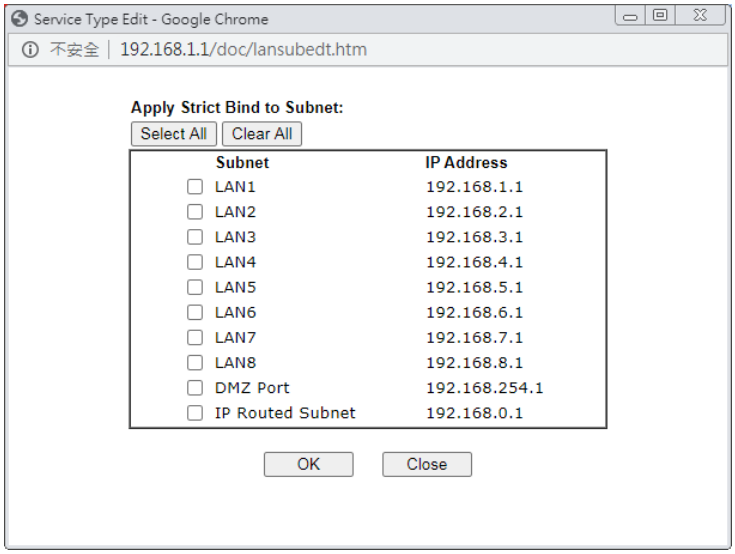
This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

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.<br>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.<br>**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.<br>**Apply Strict Bind to Subnet** – Choose the subnet(s) for applying the rules of Bind IP to MAC.<br>  |
| **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 or Update to IP Bind List** | **IP Address** – Enter the IP address to be associated with a MAC address.<br>**Mac Address** – Enter the MAC address of the LAN client's network interface.<br>**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**

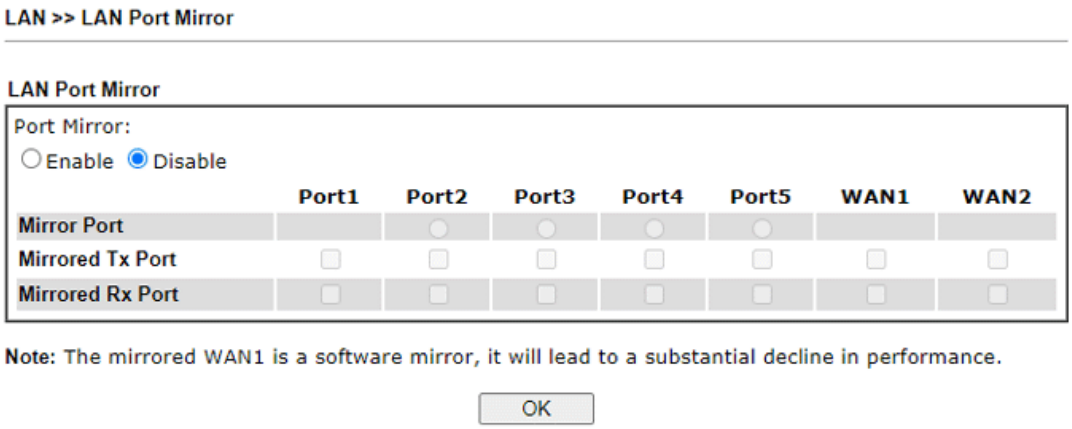
Before you select Strict Bind, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

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:

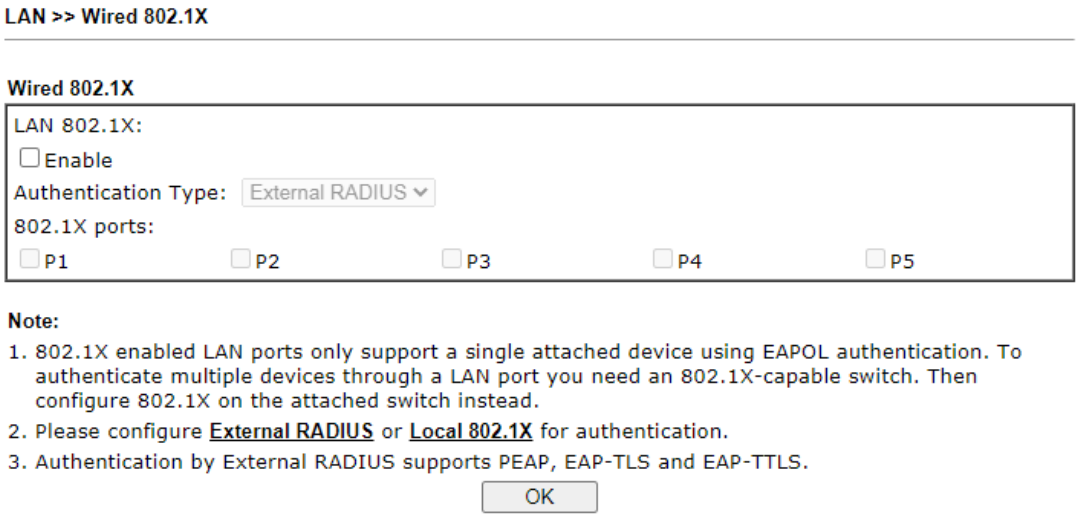
| Item | Description |
|---|---|
| **Port Mirror** | Enables or disables LAN Port Mirroring. |
| **Mirror Port** | One and only one port is selected as the mirror port, to which traffic is to be forwarded. |
| **Mirrored Tx Port** | Port(s) whose outbound traffic will be forwarded to the mirror port. |
| **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-2-5 Wired 802.1x

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check the box to enable LAN 802.1x function. |
| **Authentication Type** | **External RADIUS -** An external RADIUS server is to be used for 802.1X authentication. Go to **Applications >> RADIUS / TACACS+>>External RADIUS** to specify the RADIUS server.<br>**Local 802.1X** - Use the user database on the router to authenticate clients. Go to **User Management >> User Profile** to set up users by entering user names, passwords and ensure that Local 802.1X service is enabled for the profiles. |
| **802.1X ports** | 802.1X authentication will be available for the selected LAN ports. |

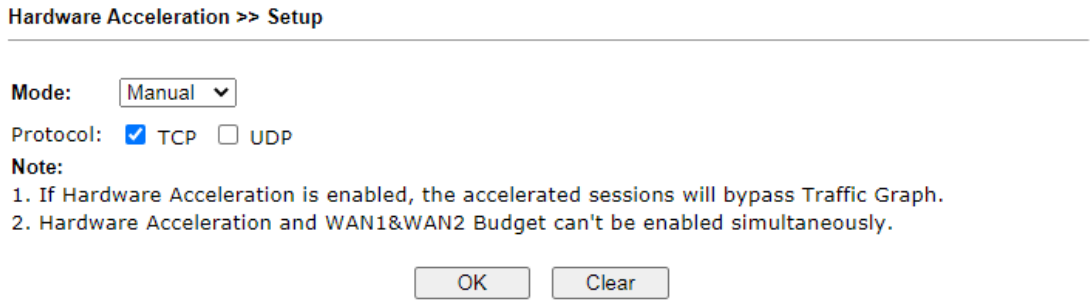
After finishing all the settings here, please click **OK** to save the configuration.

# II-3 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:

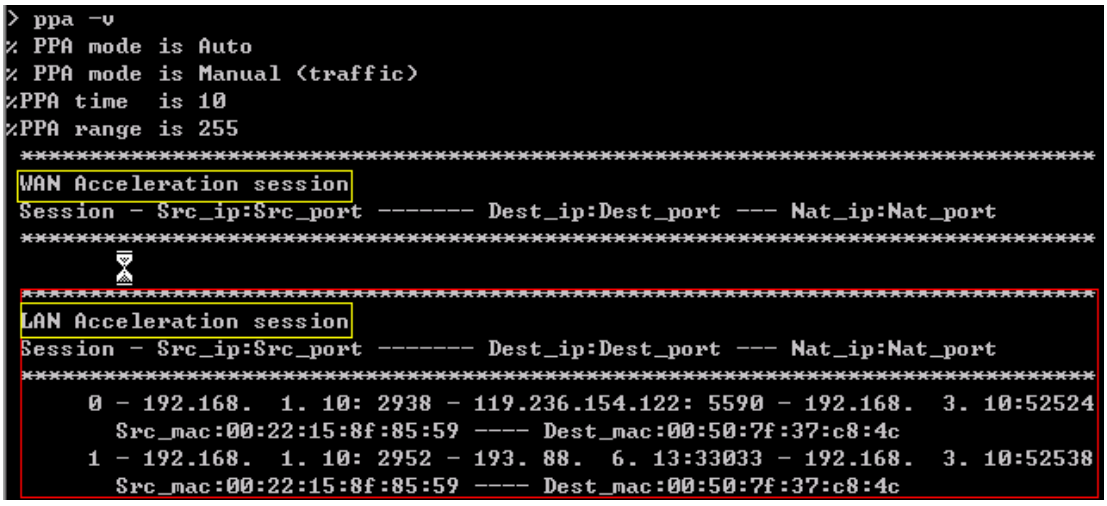



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Mode** | **Disable –** The default setting.<br>**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.<br>**Manual -** Support TCP and UDP protocol. |
| **Protocol** | There are two types supported by this function, TCP and UDP. |

**Checking the PPA status**

For checking whether the rule of PPA is working or not, a user can login to Vigor2926 series by using telnet. User can view how many sessions are transferring in each direction of PPA table after entering "**ppa -v**".



# 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**

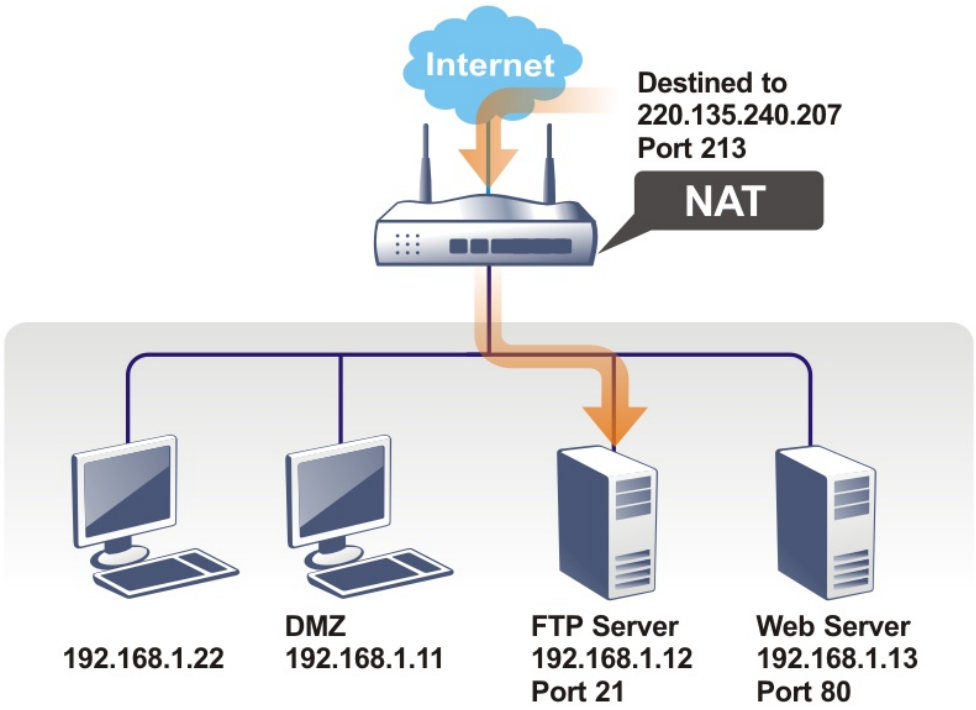
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

# Web User Interface



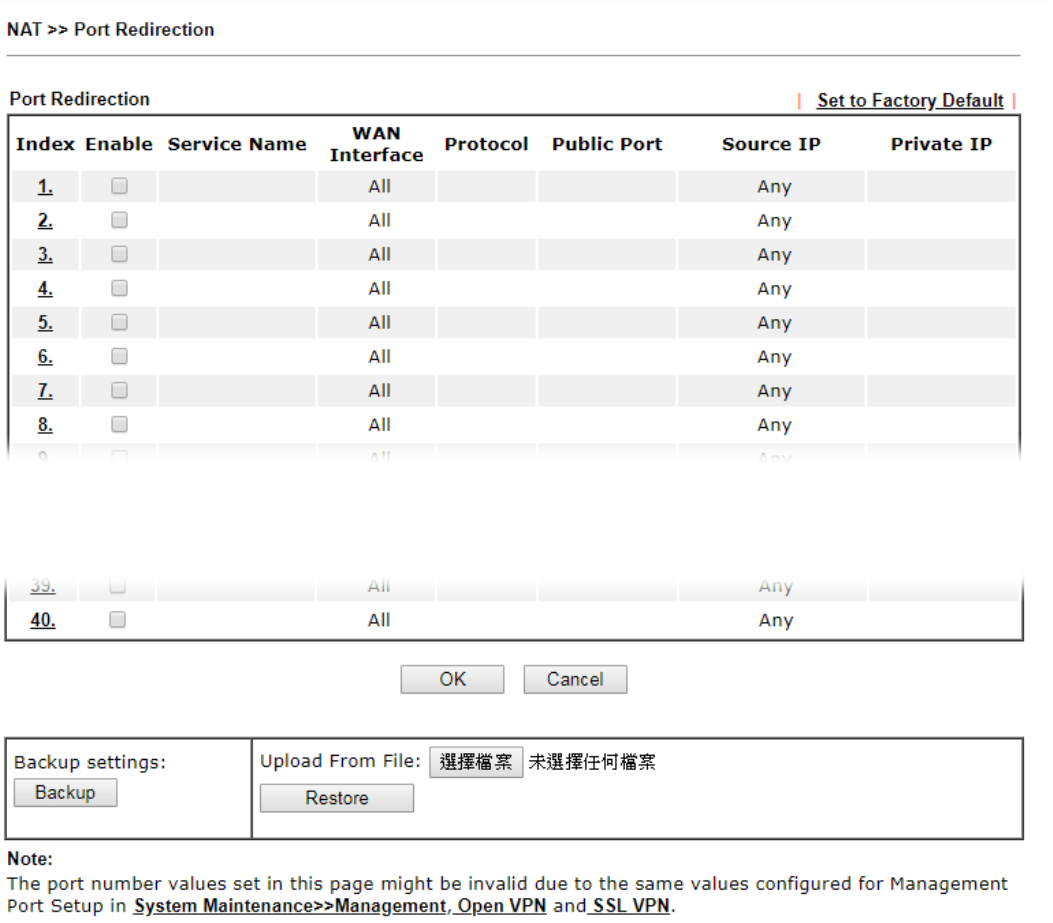

## II-4-1 Port Redirection

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.

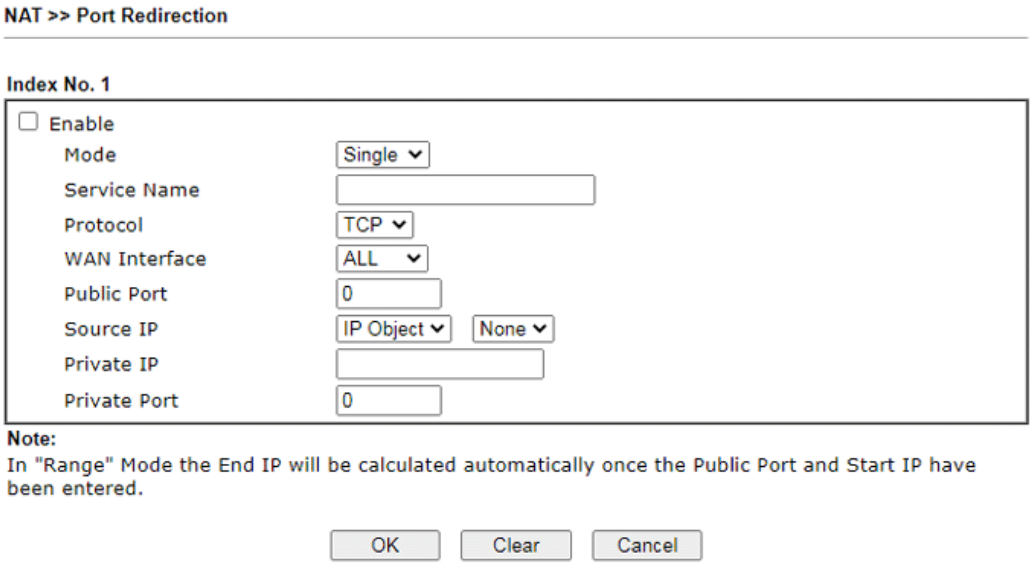
To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 40 port-mapping entries for the internal hosts.




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. |
| **Backup** | Click it to backup the configuration of port redirection settings. |
| **Restore** | Click it to restore the configuration of port redirection settings. Before clicking, make sure upload the configuration file onto Vigor router. |

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



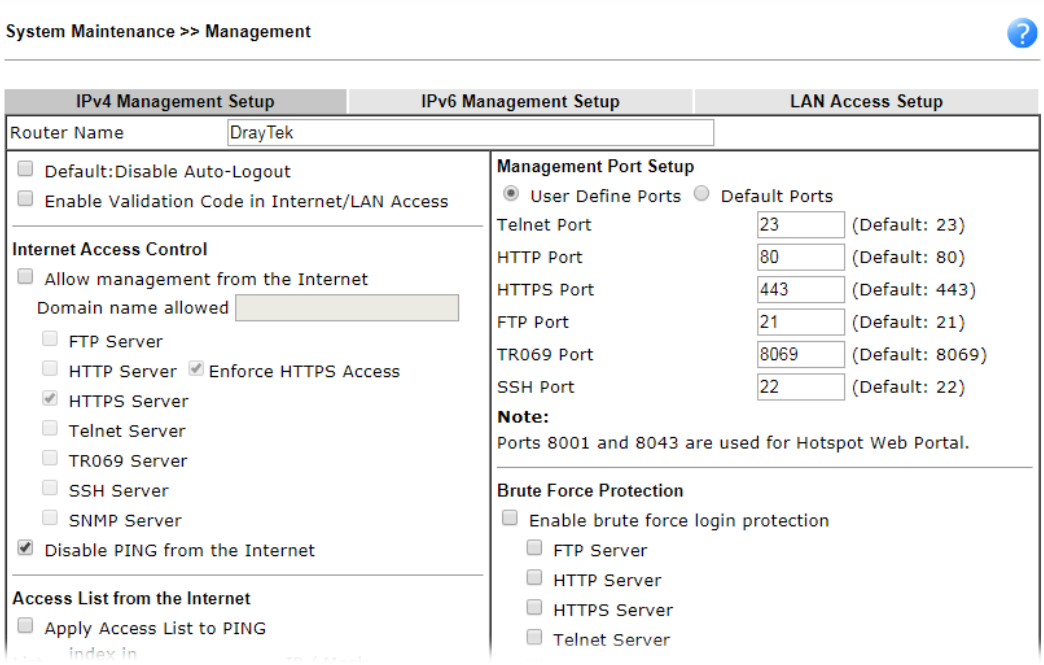

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | 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 interface 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 specified range of IP address and port. |
| **Public Port** | Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Enter the required number on the first box (as the starting port) and the second box (as the ending port). |
| **Source IP** | **IP Object** - Use the drop down list to specify an IP object profile.<br>**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.

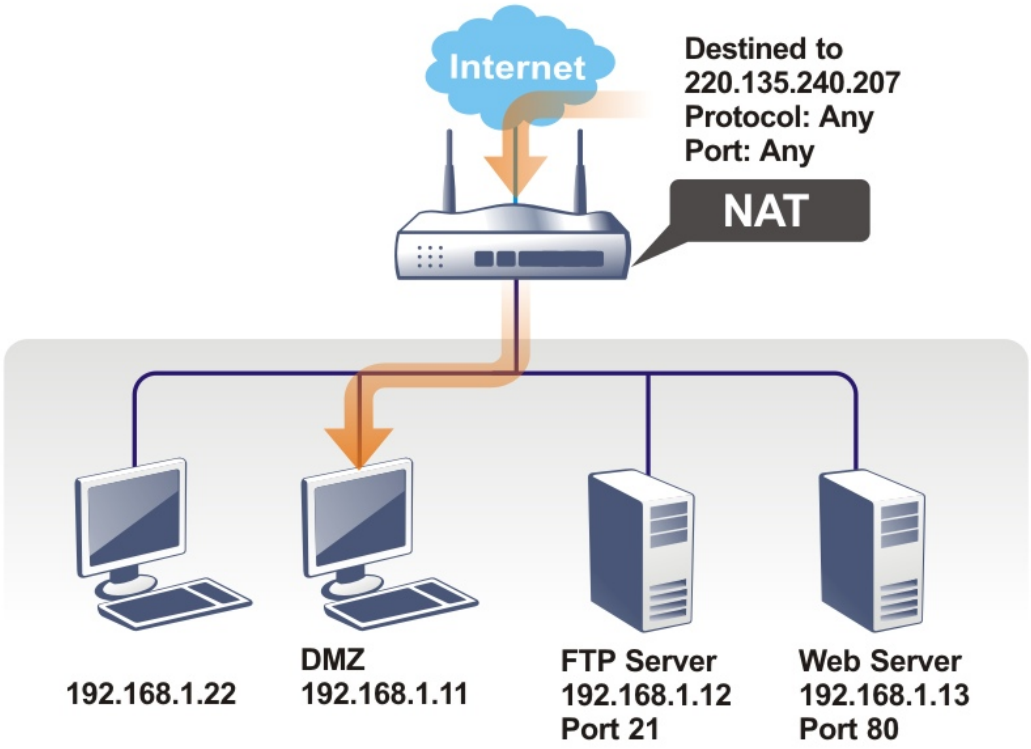
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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.



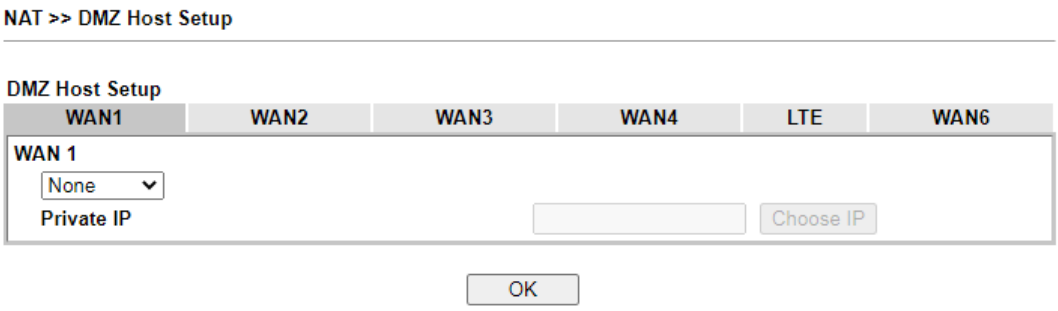
## II-4-2 DMZ Host

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.

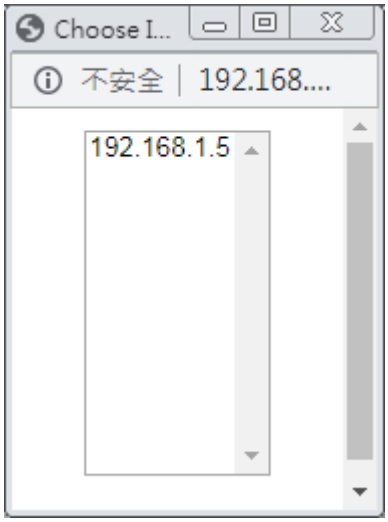
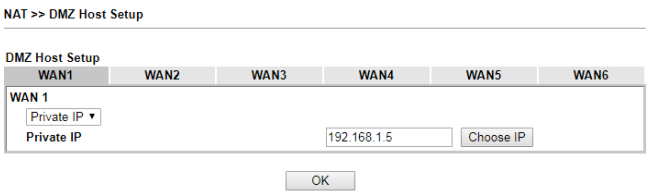



The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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.

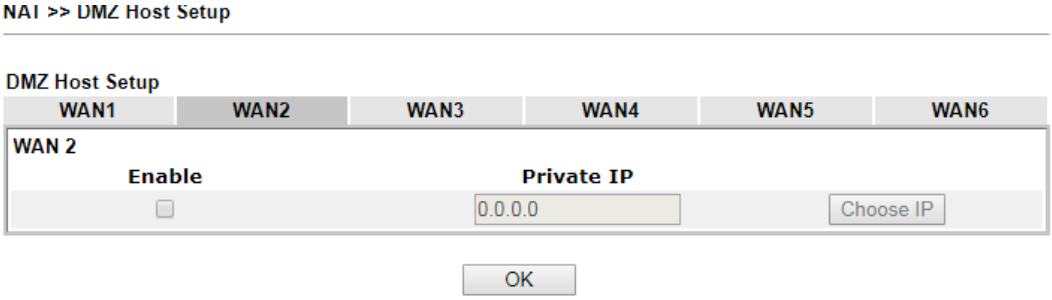


Available settings are explained as follows:

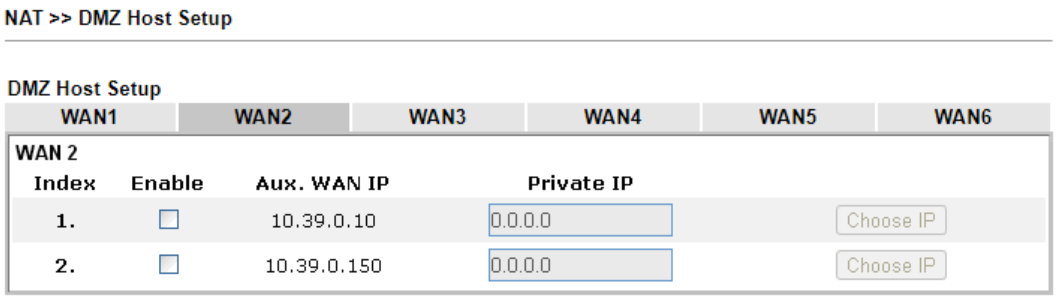
| Item | Description |
|---|---|
| **WAN 1** | Choose **Private IP** or **None** first. |
| **Private IP** | Enter the private IP address of the DMZ host, or click Choose PC to select one. |
| **Choose IP** | Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.<br>  <br>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.<br>  |

DMZ Host for WAN2, WAN3, LTE or WAN4 is slightly different with WAN1. **Active True IP** selection is available for WAN1 only.

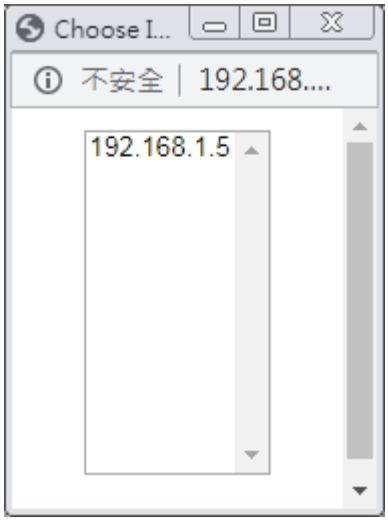
See the following figure.




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




Available settings are explained as follows:

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

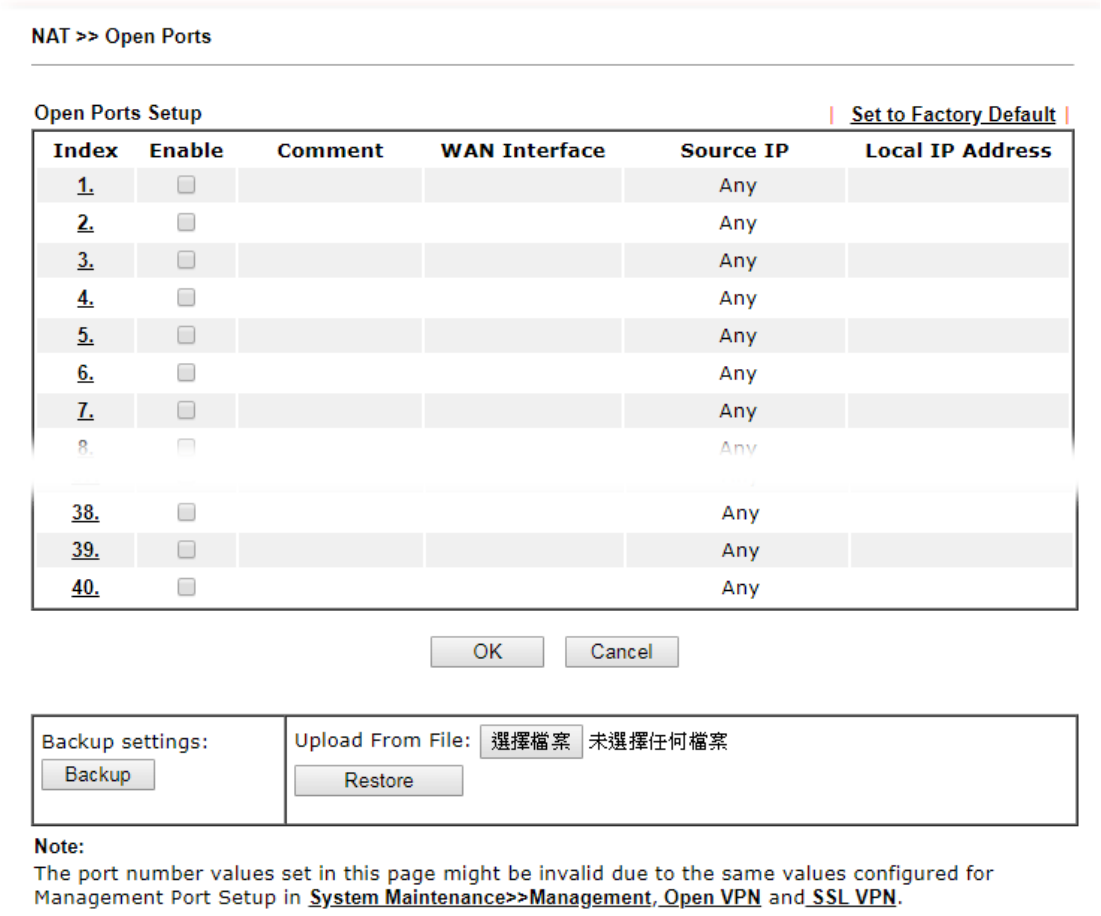
After finishing all the settings here, please click **OK** to save the configuration.

## 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:

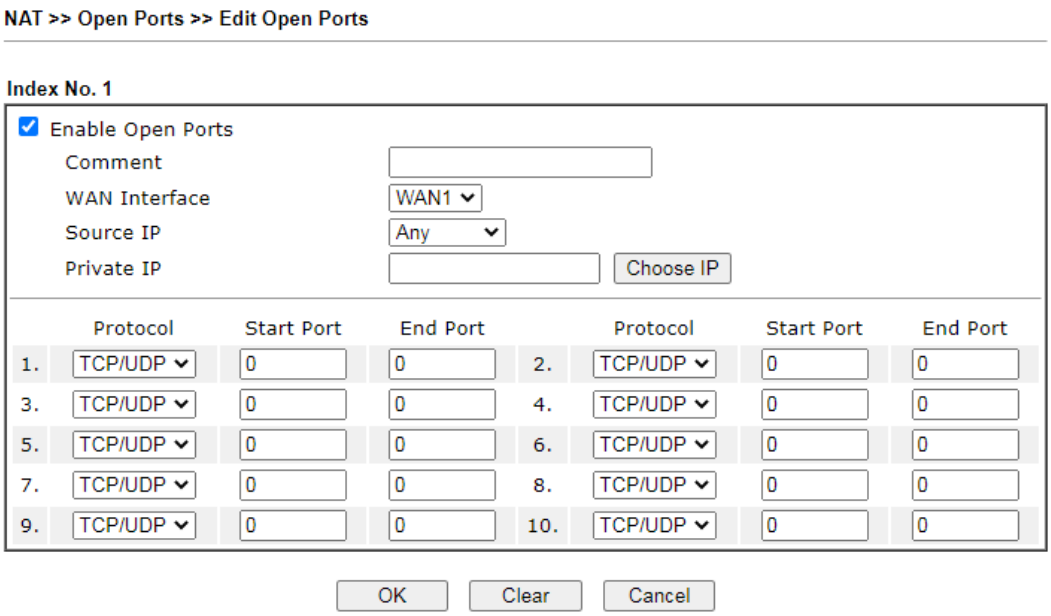



Available settings are explained as follows:

| 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.<br>If no IP alias setting exists, such field will not appear. |
| **Source IP** | Display the name of the IP object. |
| **Local IP Address** | Display the private IP address of the local host offering the service. |

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

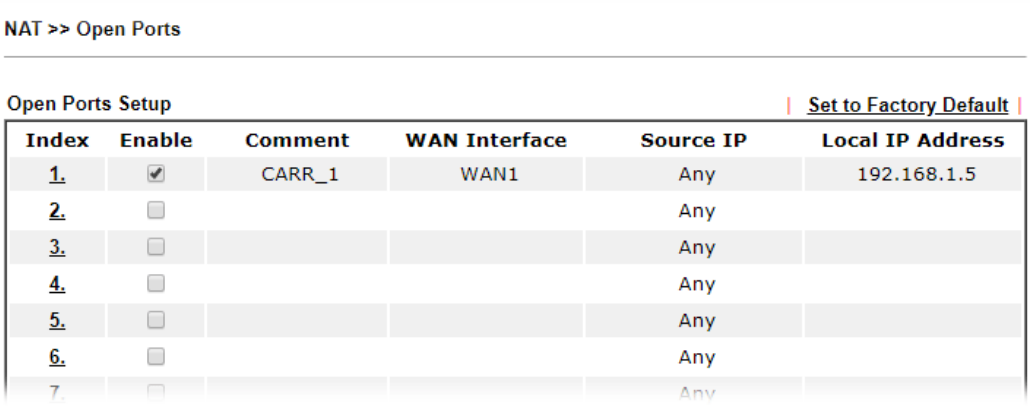
To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Open Ports** | 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** | **Any -** Any IP can be used as the source IP.<br>**IP Object** - Use the drop down list to specify an IP object proifle.<br>**IP Group** - Use the drop down list to specify an IP group profile. |
| **WAN IP** | Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured. |
| **Private IP** | Enter the private IP address of the local host or click **Choose PC** to select one.<br>**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.

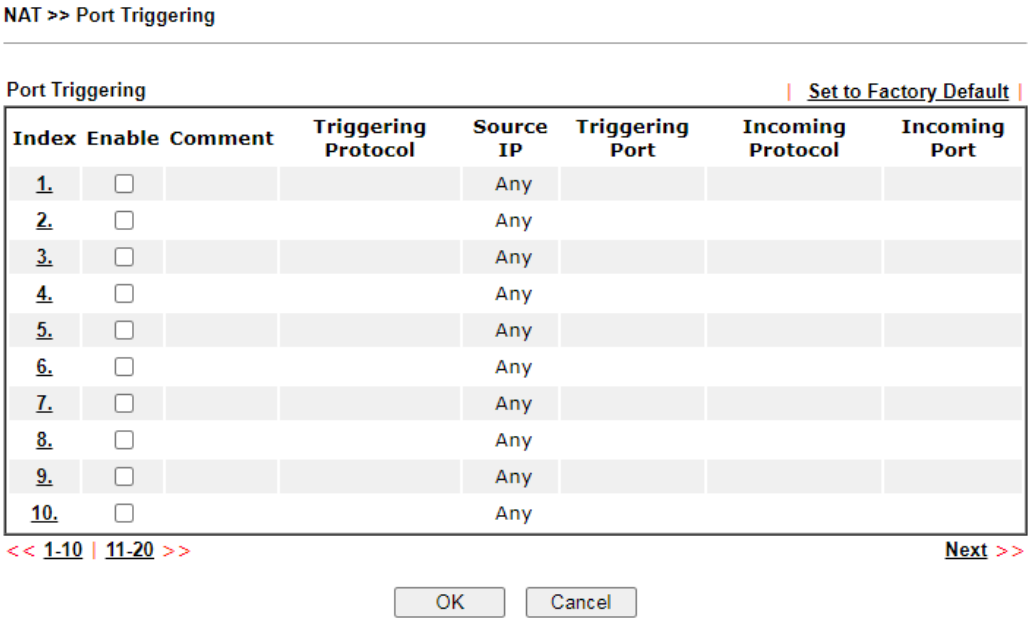
  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

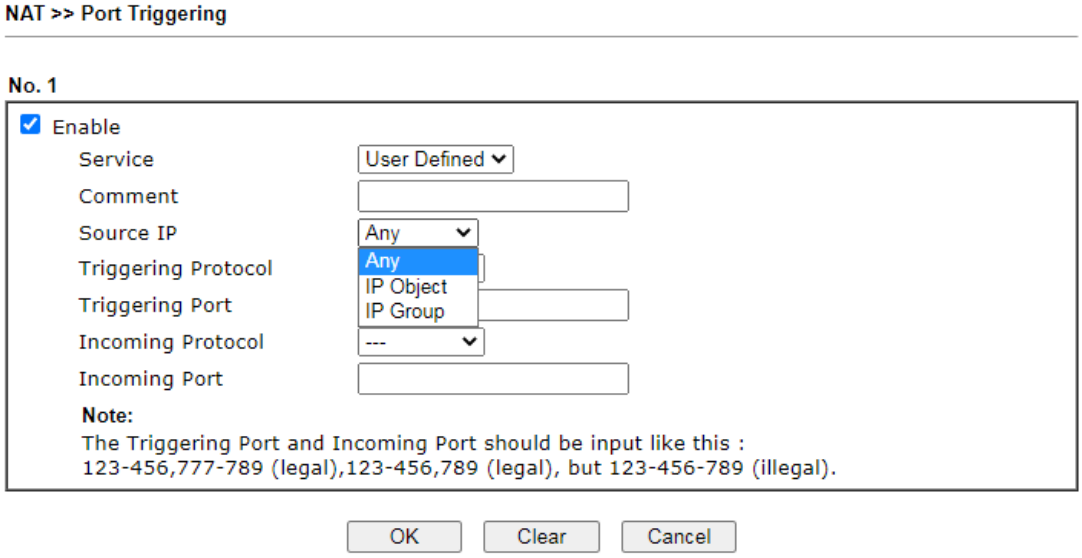
  TCP SYN: 60 sec.




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. |
| **Source IP** | Display the name of the IP object. |
| **Triggering Port** | Display the port of the triggering packets. |
| **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 service type to apply for such trigger profile. |
| **Comment** | Enter the text to memorize the application of this rule. |
| **Source IP** | **Any -** Any IP can be used as the source IP.<br>**IP Object** - Use the drop down list to specify an IP object proifle.<br>**IP Group** - Use the drop down list to specify an IP group profile. |
| **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. |

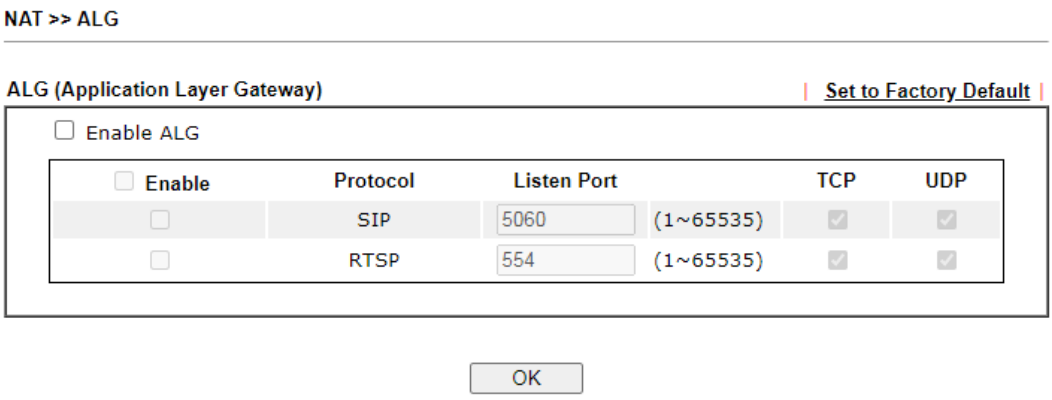
After finishing all the settings here, please click **OK** to save the configuration.

## 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

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

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

### LAN DNS / DNS Forwarding

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

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

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

### Schedule

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

### RADIUS/TACACS+

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

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

### LDAP /Active Directory Setup

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

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

### UPnP

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

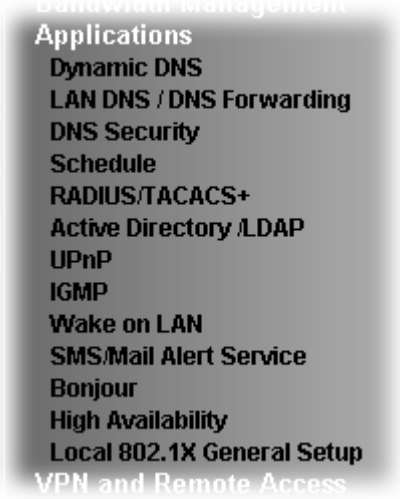
Examples of applications and devices that support UPnP include file-sharing applications such as uTorrent, Vuze and eMule, gaming consoles such as the Sony PlayStations 3 and 4 Xbox 360 and Xbox One, media streaming applications such as Plex and XBMC, and messaging and calling applications such as Skype.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

## Wake on LAN

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

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

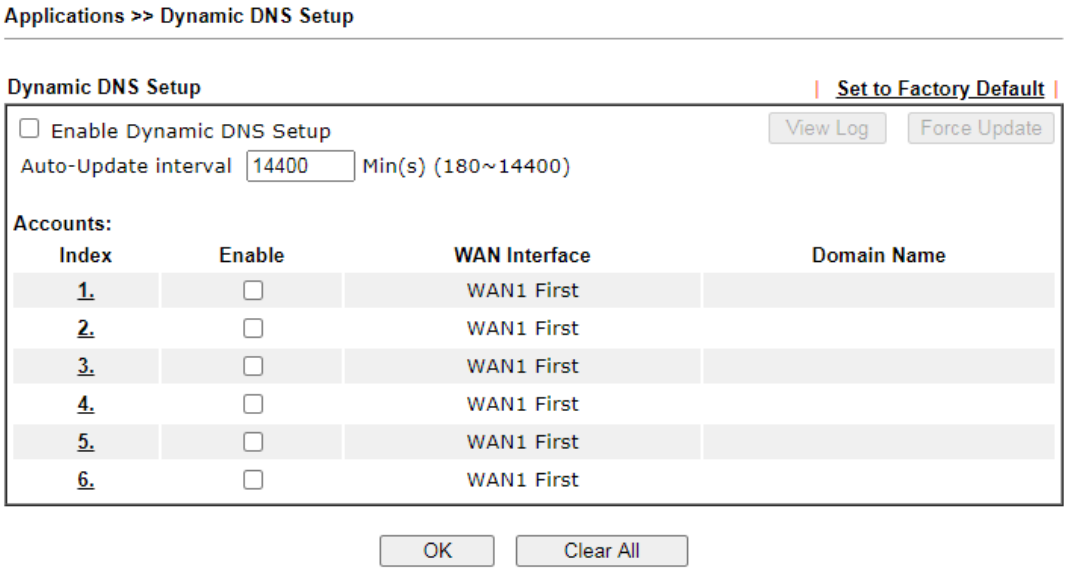
# Web User Interface




## II-5-1 Dynamic DNS

### Enable the Function and Add a Dynamic DNS Account

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

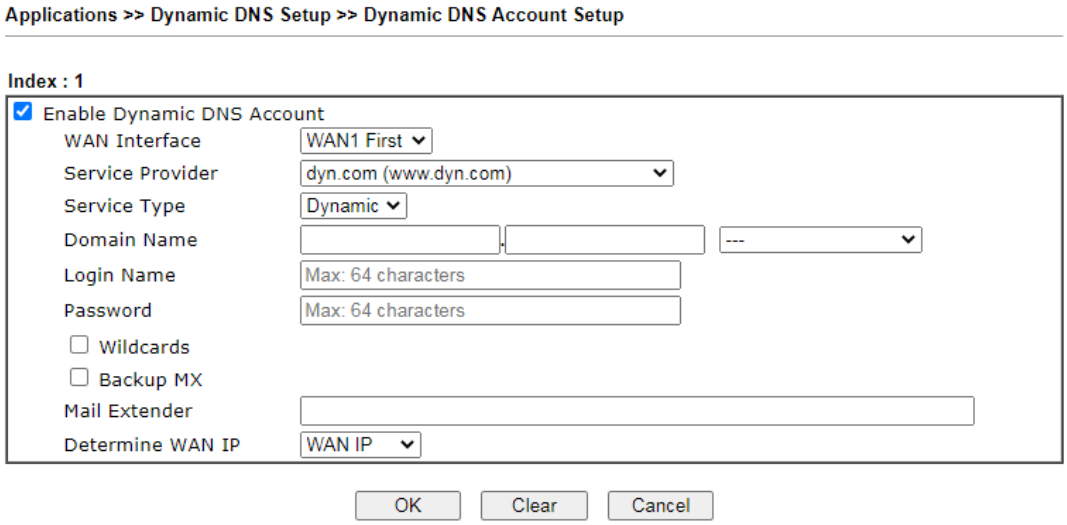



Available settings are explained as follows:

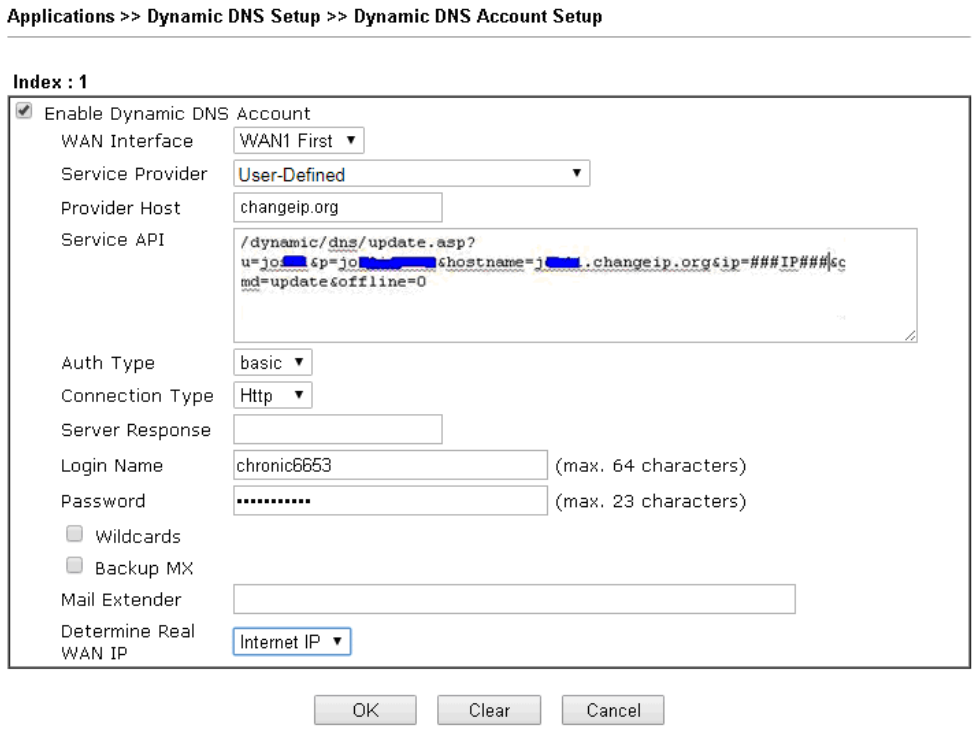
| Item | Description |
|---|---|
| **Enable Dynamic DNS Setup** | Select to enable DDNS function. |
| **Set to Factory Default** | Click to clear all profiles to factory settings. |
| **View Log** | Select to display the most recent DDNS update messages. |
| **Force Update** | Click to connect immediately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

| | |
|---|---|
| **Auto-Update interval** | The frequency, in minutes, at which the router connects to DDNS servers to update IP address information. |
| **Index** | Click to bring up the configuration page of the DDNS profile. |
| **Enable** | Check the box to enable such account. |
| **WAN Interface** | Shows the WAN interface associated with the DDNS profile. |
| **Domain Name** | Shows the domain name with which the profile is associated. |

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

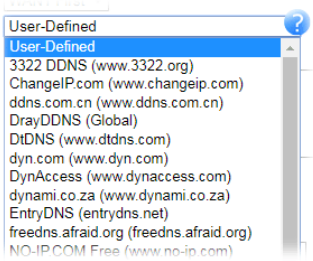



If **User-Defined** is specified as the service provider, the web page will be changed slightly as follows:




Available settings are explained as follows:

| Item | Description |
|---|---|

| | |
|---|---|
| **Enable Dynamic DNS Account** | Select to enable this DDNS profile. |
| **WAN Interface** | Select the WAN interface to monitor for IP address changes.<br>**WANx First** – The specified WAN interface will be examined first. If it is online, its IP address will be used in the DDNS update.<br>**WANx Only** – Only the specified WAN interface will be examined. If the WAN interface is online, its IP address will be used in the DDNS update. Otherwise no update will be performed for this DDNS profile. |
| **Service Provider** | Select the DDNS provider. If your DDNS provider is not listed, select **User-Defined** and manually configure the profile.<br>  <br>● **Provider Host** - Enter the IP address or the domain name of the host which provides related service.<br>Note that such option is available when Customized is selected as Service Provider.<br>● **Service API** - Enter the API information obtained from DDNS server.<br>Note that such option is available when Customized is selected as Service Provider.<br>(e.g:<br>/dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP###&cmd=update&offline=0)<br>● **Auth Type** - Two types can be used for authentication.<br>**Basic** – Username and password defined later can be shown from the packets captured.<br>**URL** - Username and password defined later can be shown in URL.<br>(e.g., http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com)<br>Note that such option is available when Customized is selected as Service Provider.<br>● **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.<br>● **Server Response** - Type any text that you want to receive from the DDNS server.<br>Note that such option is available when Customized is selected as Service Provider.<br>If other service provider is selected, you have to configure Service Type, Domain Name, Login Name and Password.<br>● **Service Type** - Select the service type that matches that of your DynDNS account. If you are unsure which service type to select, try Dynamic first. This options is |

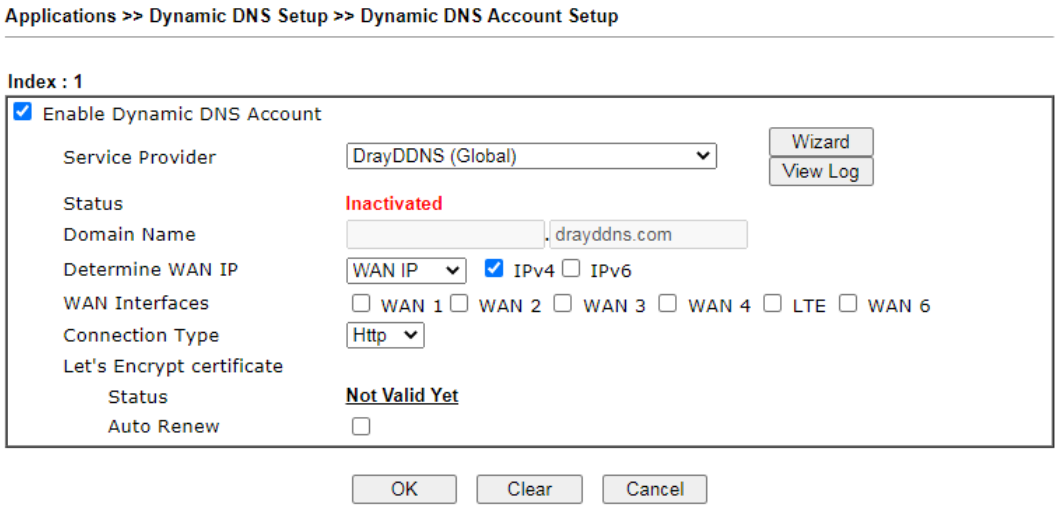
| | |
|---|---|
| | applicable to DynDNS only.<br>● **Domain Name** - The domain and subdomain to be updated. |
| **Login Name** | The login name of the DDNS account. |
| **Password** | The password of the DDNS account. |
| **Wildcard and Backup MX** | The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites. |
| **Mail Extender** | If the mail server is defined with another name, please enter the name in this area. Such mail server will be used as backup mail exchange. |
| **Determine WAN IP** | If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP.<br>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.<br>There are two methods offered for you to choose:<br>● **WAN IP** - The IP address of the router's WAN interface will be used.<br>● **Internet IP** – The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address. |

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

## DrayDDNS Settings

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Dynamic DNS Account** | Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2). |
| **Service Provider** | Choose **DrayTek Global** as the service provider.<br>**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**.<br>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.<br>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.<br>There are two methods offered for you to choose:<br>● **WAN IP** - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.<br>● **Internet IP** – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place. |
| **WAN Interfaces** | **WANx** - While connecting, the router will use WANx as the channel for such account. |
| **Let's Encrypt certificate** | **Create -** Click it to generate a certificate issued by Let's Encrypt for applying to such DDNS account.<br>**Auto Update** – Check the box to make the system update the certificate automatically. |

### Disable the Function and Clear all Dynamic DNS Accounts

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

### Delete a Dynamic DNS Account

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

**DDNS updates take place when:**

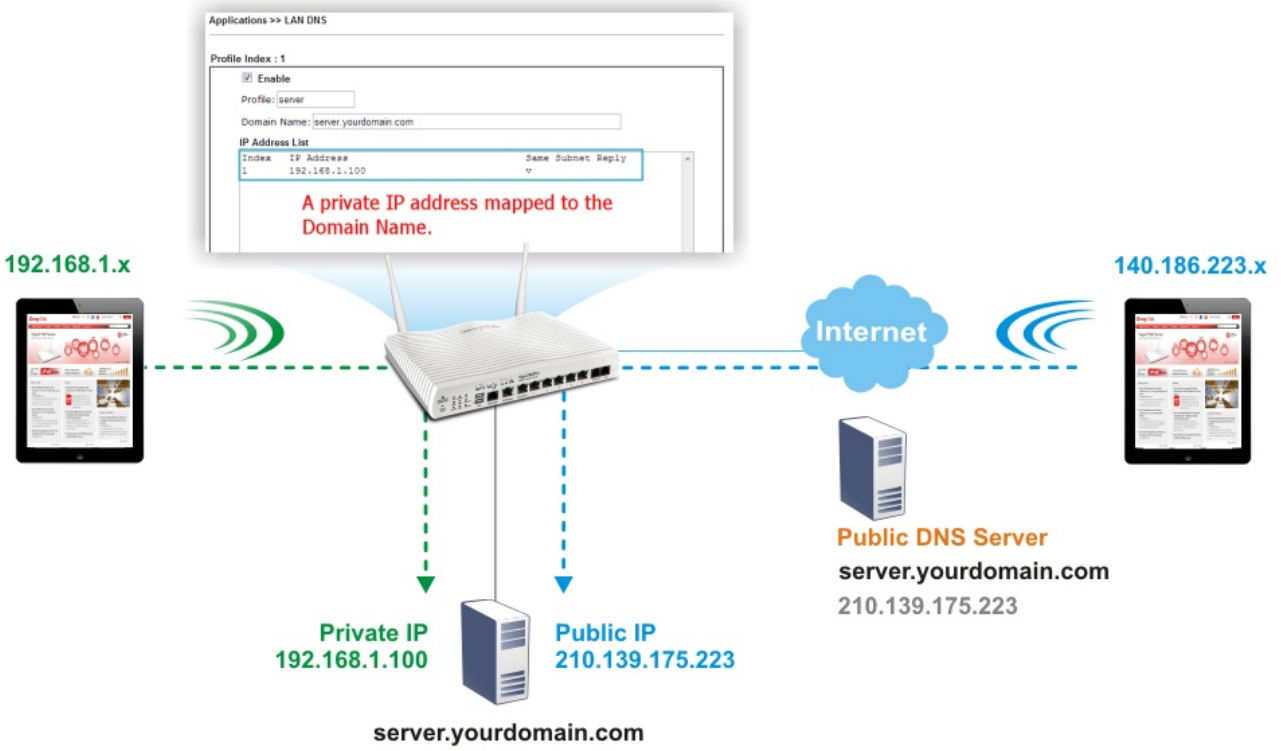
- The router is powered on or rebooted.
- The public IP address of any WAN interface changes.
- The online status of a WAN interface changes (going from online to offline or vice versa).
- The DDNS function is changed from disabled to enabled.
- A DDNS entry is modified and enabled.
- The Auto-Update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

**Procedures for Setting up a Dynamic DNS Entry**

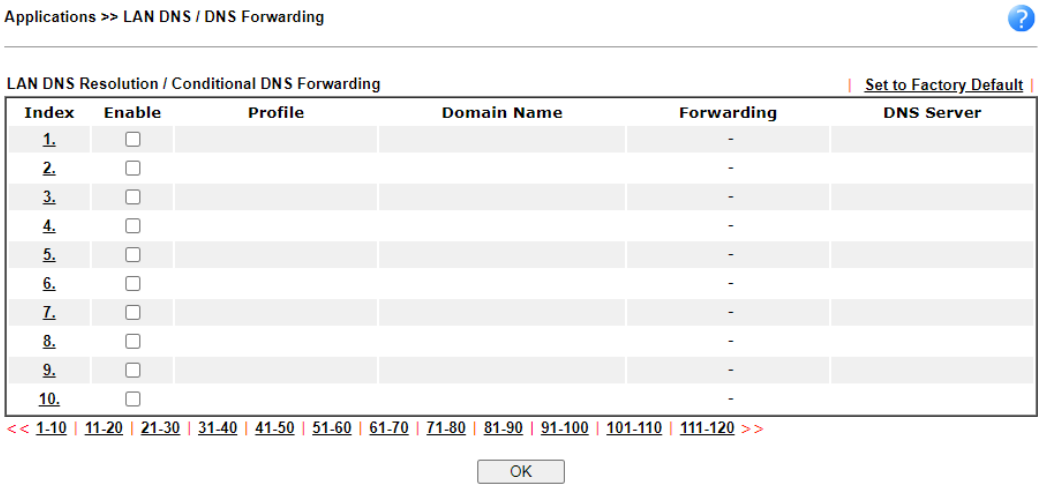
1. Contact the dynamic DNS provider of your choice and have service set up. Most DDNS providers accept signups on their websites. Service could be provided free of charge or for a fee.
2. Create a DDNS entry on the router by selecting the appropriate DDNS provider and enter the account information.
3.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

## II-5-2 LAN DNS / DNS Forwarding

LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2927 series will respond the specified private IP address.




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

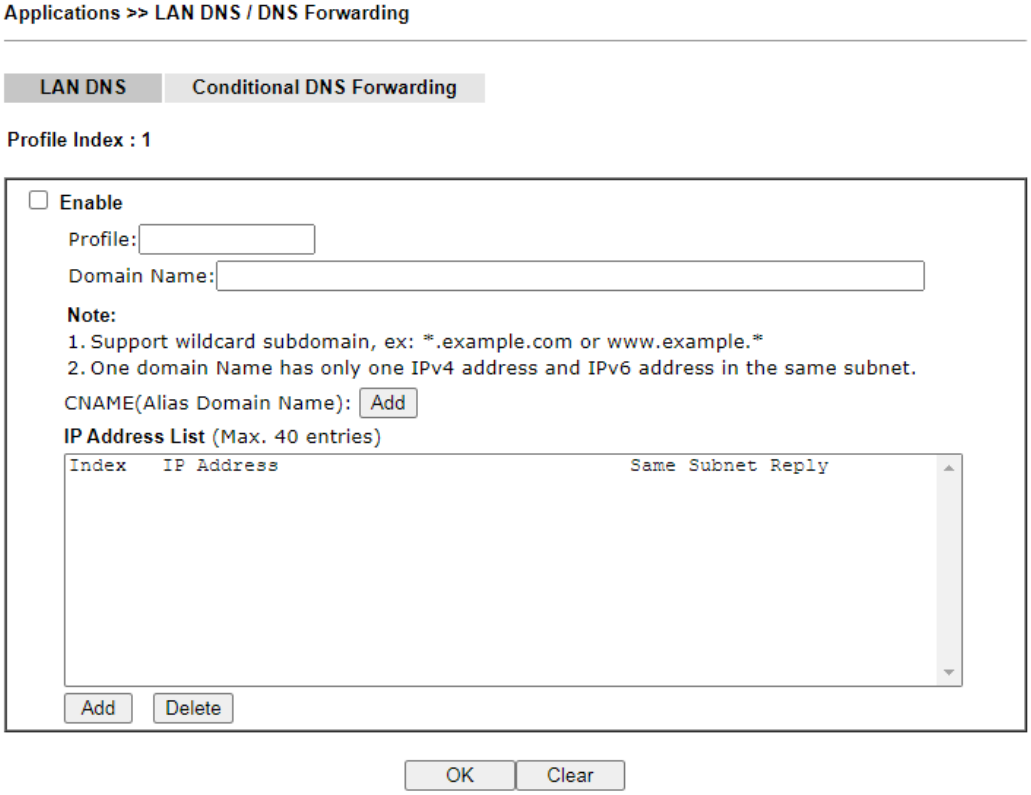



Each item is explained as follows:

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

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

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



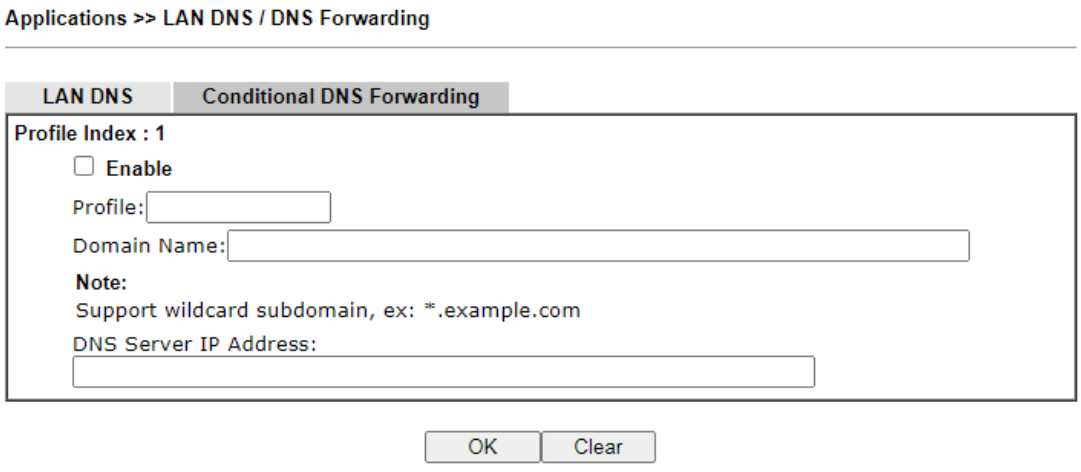

Available settings are explained as follows:

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

| | |
|---|---|
| | Click Delete next to an alias entry to delete it. |
| **IP Address List** | The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name.<br>**Add** –Click **Add** to bring up the Add IP Address dialog box:<br>  <br>● **Host's IP Address –** Enter the IP address to be returned in response to a DNS query for the configured domain names and aliases.<br>● **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.<br>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.<br>**Delete** –To delete an IP address, click on it and then click Delete. |

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check this box to enable such profile. |

| | |
|---|---|
| **Profile** | Type a name for such profile.<br>**Note:** If you type a name here for conditional DNS forwarding and click **OK** to save the configuration, the name also will be applied to LAN DNS automatically. |
| **Domain Name** | Enter the domain name for such profile. |
| **DNS Server IP Address** | Enter the IP address of the DNS server you want to use for DNS forwarding. |

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

## II-5-3 DNS Security

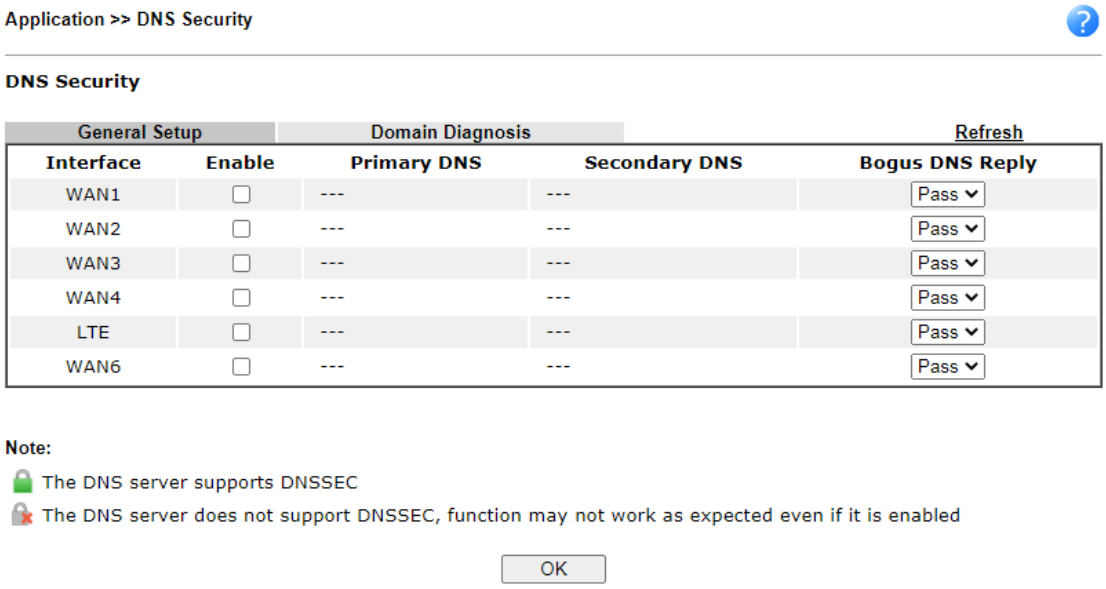
Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.

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

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

### II-5-3-1 General Setup

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



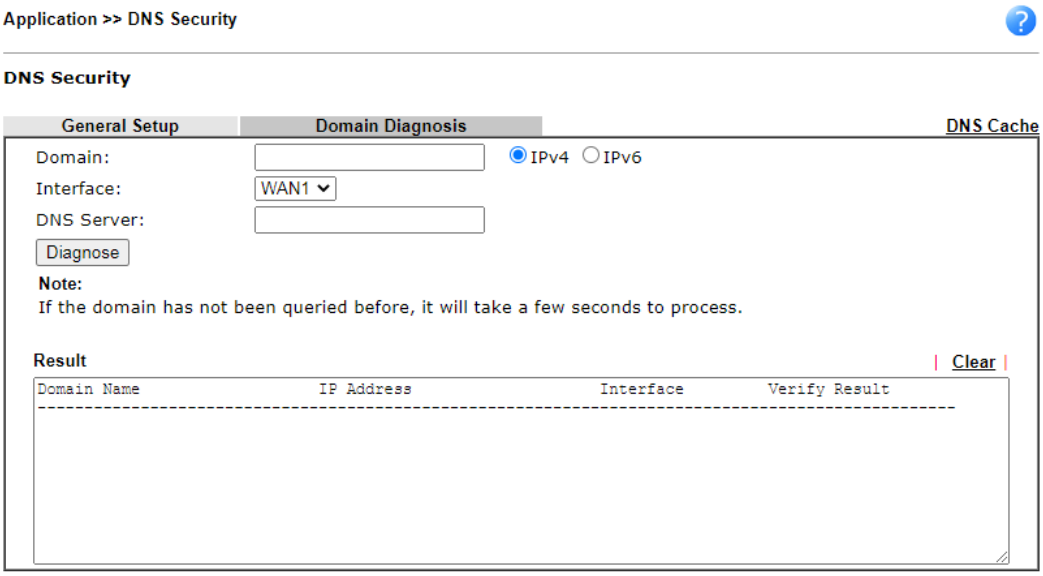

Available settings are explained as follows:

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

Press **OK** to save changes.

## II-5-3-2 Domain Diagnose

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

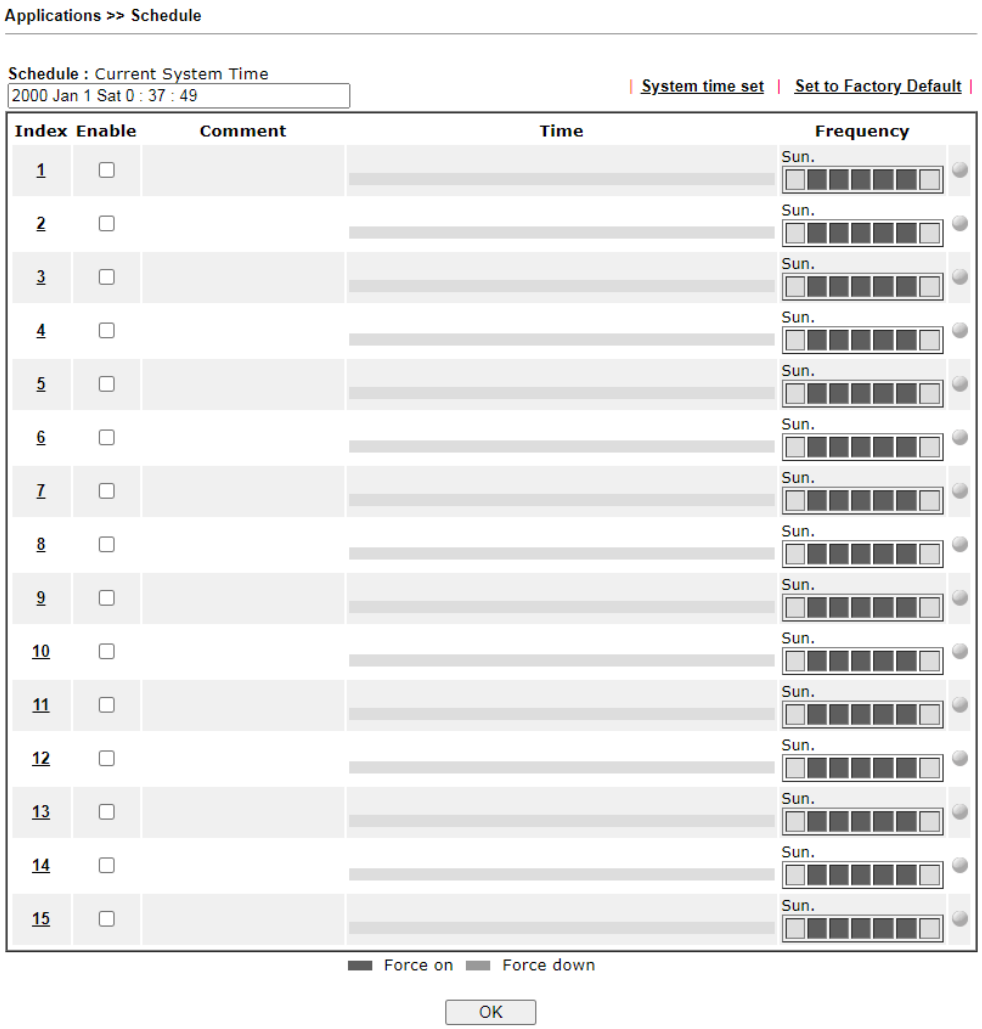



Available settings are explained as follows:

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

## II-5-4 Schedule

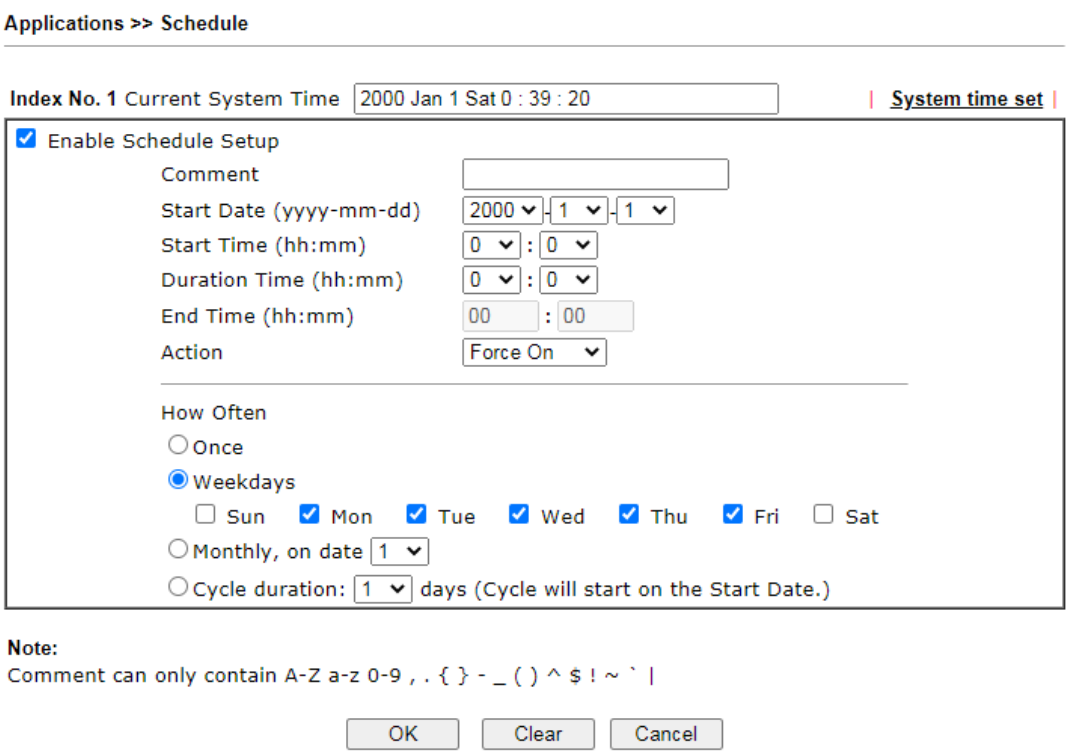
Time schedules can be created and used with router features that support them, so that those features can be turned on and off automatically at preconfigured times.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Current System Time** | Shows the current time of the router. |
| **System time set** | Click to navigate to **System Maintenance >> Time and Date** to set the system time and date. |
| **Set to Factory Default** | Reset all schedules to factory default values. |
| **Index** | Shows the index number of the schedule entry. |
| **Enable** | Select to enable the schedule; clear to disable it. |
| **Comment** | Shows the name given to the schedule. |
| **Time** | Shows the start and end times of the schedule. The time interval of the schedule is indicated in dark grey. |
| **Frequency** | Shows the days of the week configured for the schedule. Selected days are shown in dark grey.<br>- If it lights in green, it means such schedule is active. |

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Schedule Setup** | Select to enable the schedule; clear to disable it. |
| **Comment** | Name to identify this schedule entry. |
| **Start Date (yyyy-mm-dd)** | The date when the entry comes into effect. |
| **Start Time (hh:mm)** | The time when the schedule is triggered. See the **How Often** setting below for details. |
| **Duration Time (hh:mm)** | How long the action lasts when the scheduled is triggered. |
| **End Time (hh:mm)** | It will be calculated automatically when Start Time and Duration Time are configured well. |
| **Action** | Action to take when the schedule is triggered.<br>**Force On** – The feature with which this schedule is associated will be turned on.<br>**Force Down** – The feature with which this schedule is associated will be turned off. |
| **How Often** | How frequently the schedule is triggered.<br>● **Once** - The schedule is triggered once, on the **Start Date** at the **Start Time**, for the **Duration Time**.<br>● **Weekdays** - The schedule will be triggered repeatedly, starting on the **Start Date** at the **Start Time**, on the selected days of the week, at the **Start Time**, for the **Duration Time**.<br>● **Monthly, on date –** The router will only execute the action applied such schedule on the date (1 to 28) of a month.<br>● **Cycle duration –** Type a number as cycle duration. Then, any action applied such schedule will be |

| | |
|---|---|
| | executed per several days. For example, "3" is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date. |

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

**Example**

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

**Office Hour:**

**(Force On)**





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

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

## II-5-5 RADIUS/TACACS+

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

The router supports external TACACS+ and internal and external RADIUS servers for user authentication. Services that require user authentication include WLAN and VPN.

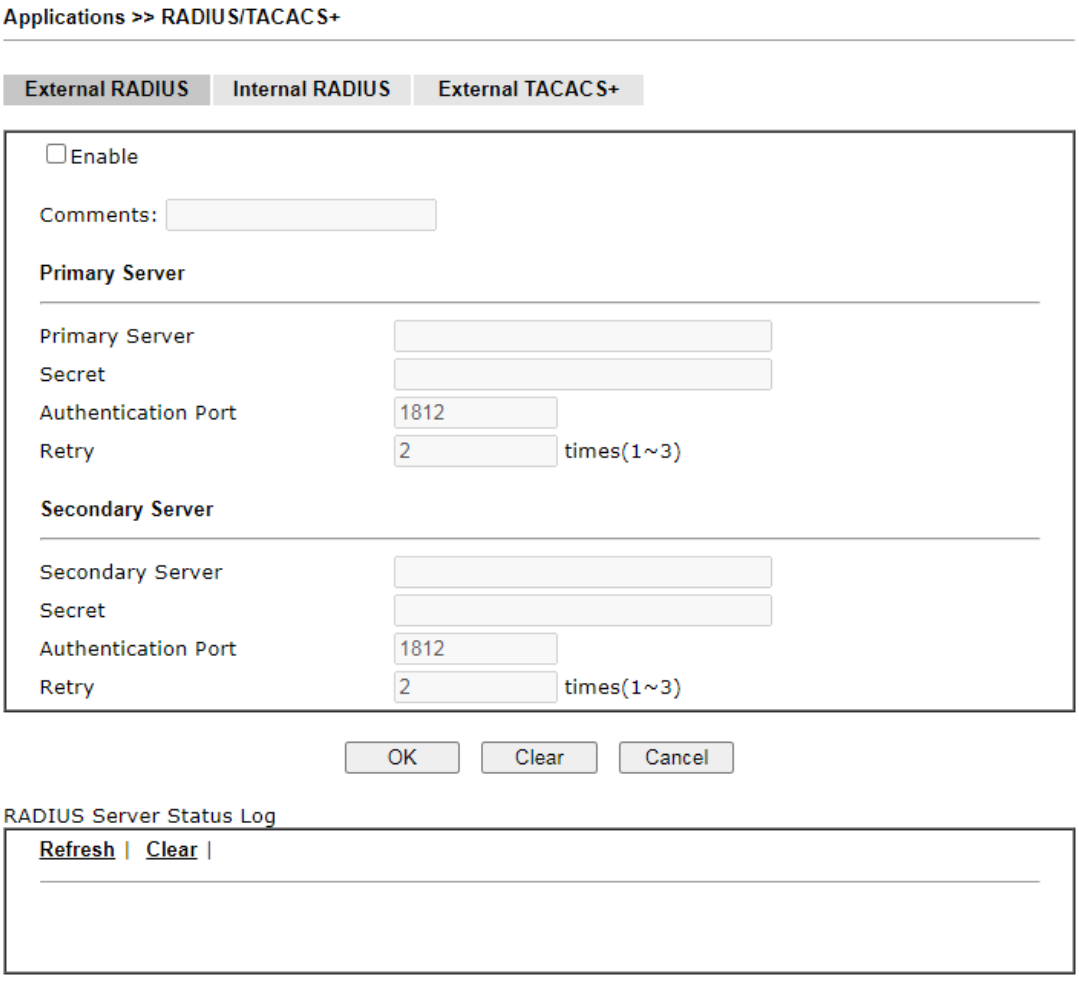
To configure RADIUS or TACACS+ servers, from the Main Menu select **Applications >> RADIUS/TACACS+**.

### II-5-5-1 External RADIUS

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

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

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




Available settings are explained as follows:

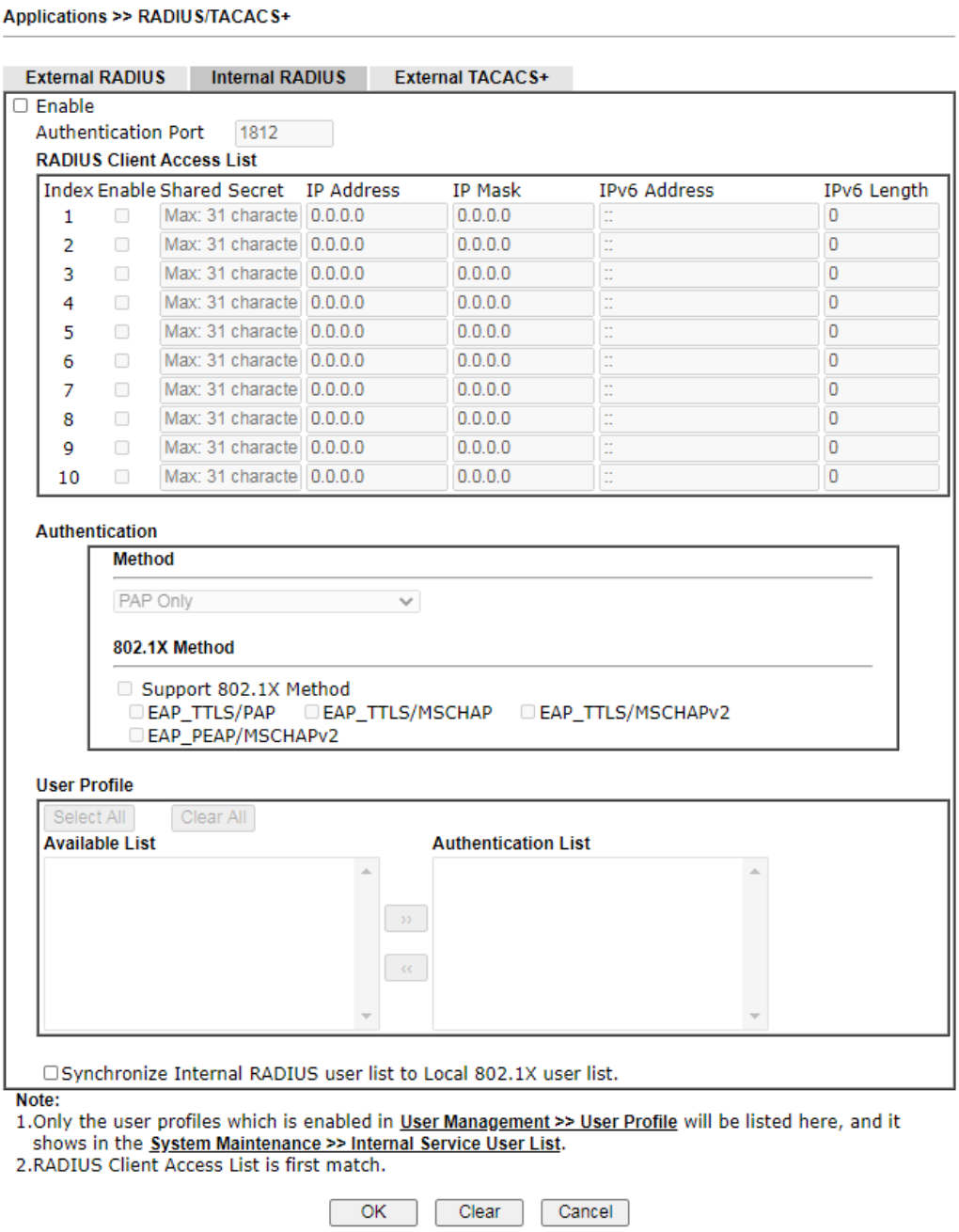
| Item | Description |
|---|---|
| **Enable** | Check to enable RADIUS client profile.<br>**Comments** - Enter a brief description for this profile. |
| **Primary Server** | **Primary Server** - Enter the IP address of RADIUS server.<br>**Secret** - The RADIUS server and client share a secret that is 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.<br>**Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.<br>**Retry** - Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server. |
| **Secondary Server** | **Secondary Server** - Enter the IP address of RADIUS server.<br>**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.<br>**Authentication Port** - The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.<br>**Retry** - Set the number of attempts to perform reconnection. If the connection (with the Secondary Server) still fails, stop the connection attempt. The client authentication would be determined as "failed". |
| **RADIUS Server Status Log** | Display the record of current status of RADIUS server. |

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

### II-5-5-2 Internal RADIUS

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

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




Available settings are explained as follows:

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

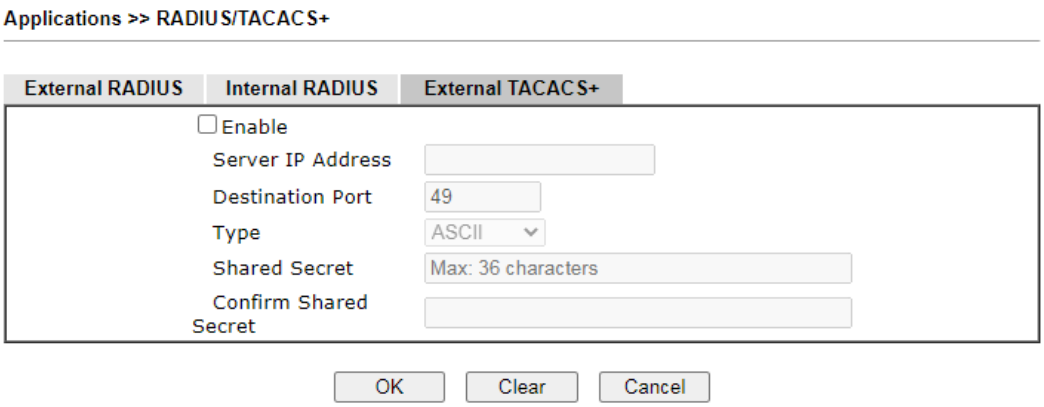
| | |
|---|---|
| | block.<br>**IPv6 Address** - Base address of the IPv6 block.<br>**IPv6 Length** - The prefix length of the IPv6 block. |
| **Authentication** | Configures the authentication settings.<br>Specify the way to authenticate the wireless client.<br>**PAP –** Only the Password Authentication Protocol will be used to validate users.<br>**PAP/CHAP/MS-CHAP/MS-CHAPv2 –** PAP, CHAP (Challenge-Handshake Authentication Protocol), and Microsoft versions of CHAP can be used to validate users.<br>**Support 802.1X Method** – The built in RADIUS server offered by Vigor router can act as the AAA server. Select to enable 802.1X support. |
| **User Profile** | During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in **User Management>>User Profile** first.<br>**Select All** – Click to move all user profiles under the Available List to the Authentication List.<br>**Clear All** - Click to remove all user profiles from the Authentication List.<br>**Available List** – The user profiles **without** RADIUS server enabled in **User Management >> User Profile** will be listed in this field.<br>**Authentication List** –The user profiles with RADIUS server enabled in **User Management >> User Profile** will be listed in this field. |
| **Synchronize Internal RADIUS user list to Local 802.1X user list** | Users can be authenticated by RADIUS server and local 802.1X to get certain network service. It is not necessary to create new user profiles (containing user accounts and user passwords) for RADIUS and local 802.1X respectively.<br>Simply select to update the 802.1X authentication list to match the RADIUS authentication list. |

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

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

## II-5-5-3 External TACACS+

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Select to enable the use of an external TACACS+ server. |
| **Server IP Address** | The IP address of the TACACS+ server. |
| **Destination Port** | The port used by the TACACS+ server. Port 49 is most common. |
| **Shared Secret** | A text string that is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters. |
| **Confirm Shared Secret** | Enter the shared secret again for verification. |

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

## II-5-6 Active Directory/LDAP

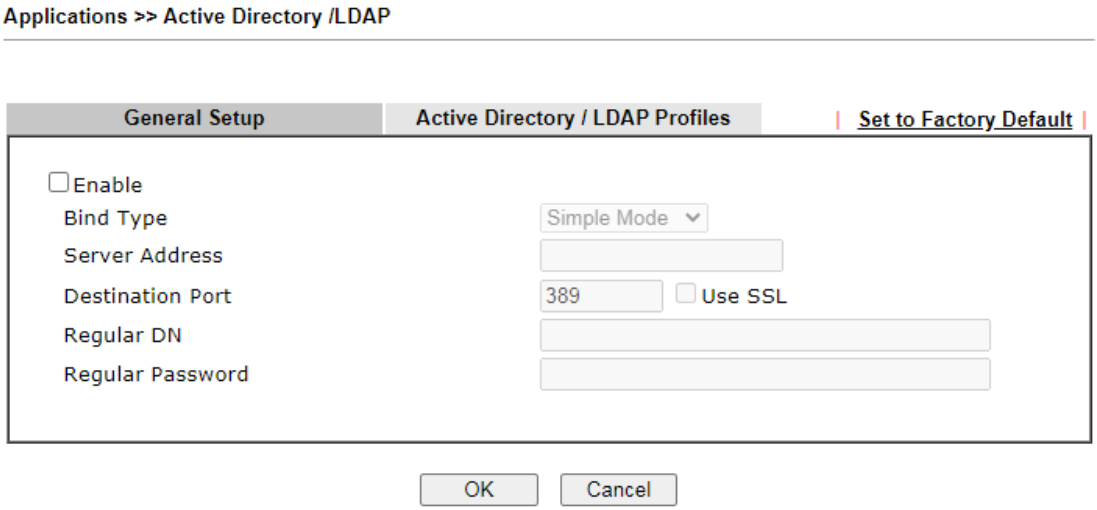
Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

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

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

### II-5-6-1 General Setup

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Select to enable LDAP client. |
| **Bind Type** | Select from one of 3 bind types:<br>● **Simple Mode** – Initiate bind operation (authentication) without performing user search. This mode can be used when all users belong to the same branch in the LDAP structure.<br>● **Anonymous** – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user search. This mode can be used when not all users belong to the same branch and the server allows anonymous searches.<br>● **Regular Mode** – Same as Anonymous mode, except that the DN and password are sent to the server. This mode can be used when not all users belong to the same branch and the server does not allow anonymous searches.<br>For the regular mode, you'll need to Enter the **Regular DN** and **Regular Password**. |
| **Server Address** | The network address of the LDAP server. |
| **Destination Port** | The network port that the LDAP server listens on. The default ports are 389 for unsecured connections and 636 for LDAPS (LDAP over SSL) connections. |

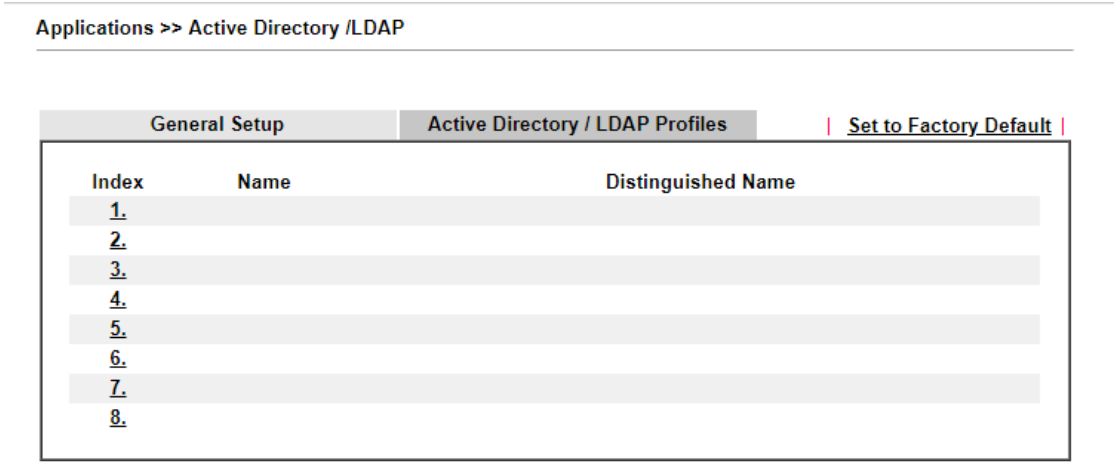
| | |
|---|---|
| **Use SSL** | Select to use Secure Sockets Layer (SSL) for LDAP traffic. |
| **Regular DN** | Enter the LDAP Distinguished Name for authentication if **Bind Type** is set to **Regular Mode**. |
| **Regular Password** | Enter the LDAP Password for authentication if **Bind Type** is set to **Regular Mode**. |

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

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

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

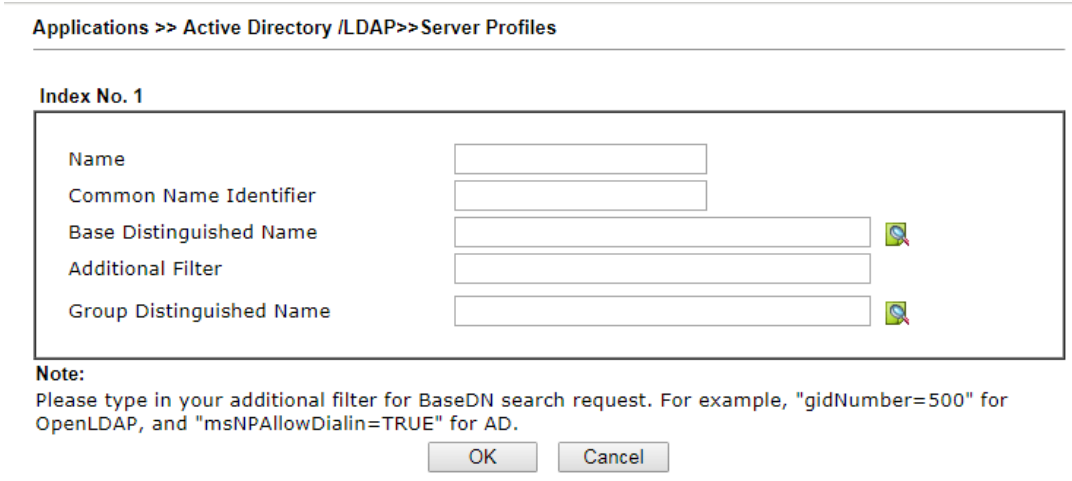
Click on the Active Directory / LDAP Profiles to bring up the index page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Index** | The index of the LDAP profile. Click to show the profile settings page. |
| **Name** | Displays the user-defined name that identifies this entry. |
| **Distinguished Name** | Displays the distinguished name (DN) configured in the profile. |

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



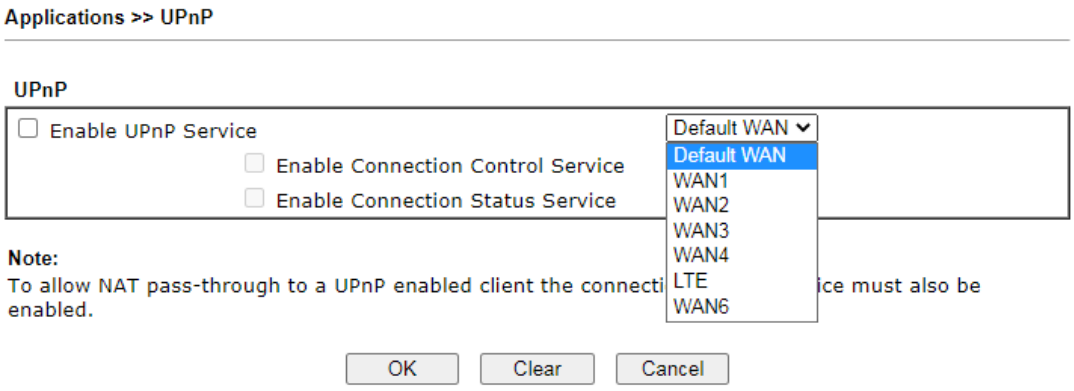
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 19 characters. |
| **Common Name Identifier** | The common name attribute, which is typically “cn” in most LDAP configurations. |
| **Base Distinguished Name** | The starting point of user search in the LDAP directory, for example, dc=draytek,dc=com.<br>  – click this icon to display a list of valid DNs in the LDAP directory. |
| **Additional Filter** | Additional filter to be applied to the search request to identify eligible users.<br>For example,<br>– “OpenLDAP: (gidNumber=500)”<br>Here group ID 500 is the group of dial-in users.<br>– “ActiveDirectory: (msNPAllowDialin=TRUE)”<br>The msNPAllowDialin attribute indicates that the user has permission to dial in remotely. |
| **Group Distinguished Name** | The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com.<br>  - click this icon to display a list of valid DNs in the LDAP directory. |

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

## II-5-7 UPnP

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable UPNP Service** | Select to enable UPnP. |

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

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

The reminder as regards concern about Firewall and UPnP:

**Can't work with Firewall Software**

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

**Security Considerations**

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

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



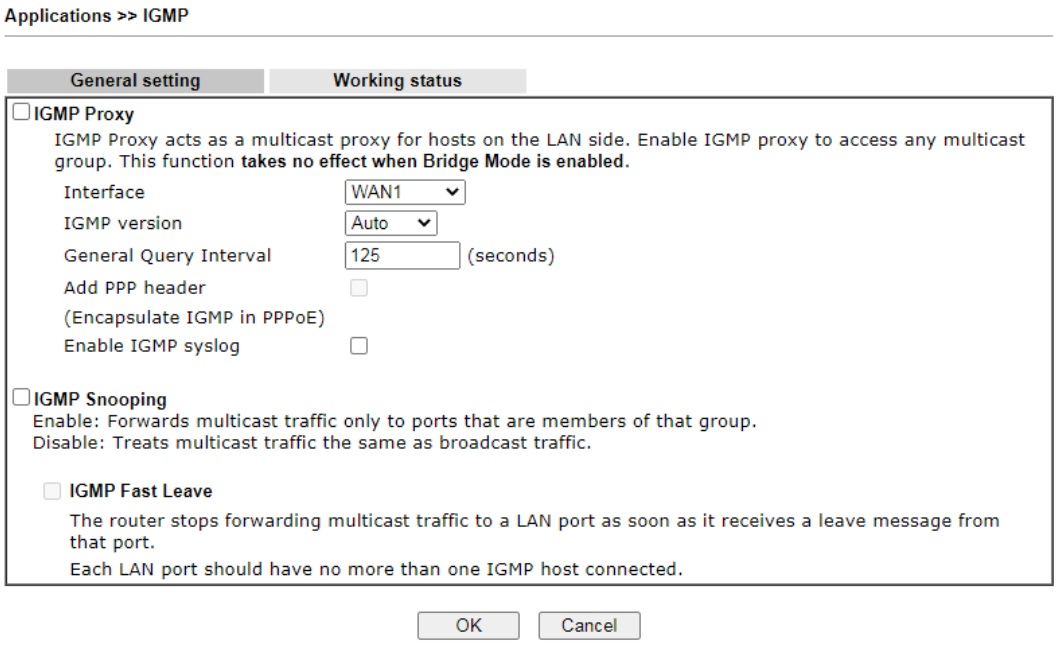
| | |
|---|---|
| **Info** | UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security. |

## II-5-8 IGMP

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

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

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




Available settings are explained as follows:

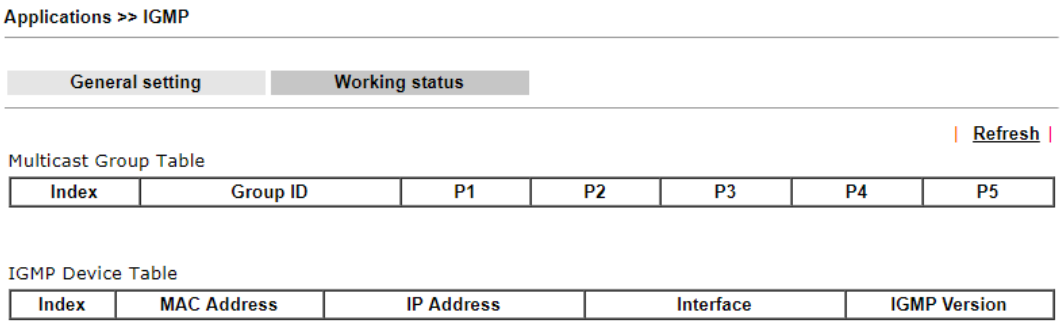
| Item | Description |
|---|---|
| **IGMP Proxy** | Check this box to enable this function. The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode.<br>**Interface** – Specify an interface for packets passing through.<br>**IGMP version** – At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe.<br>**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.<br>**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.<br>**Enable IGMP syslog** - Check the box to store the IGMP status onto Syslog. |
| **IGMP Snooping** | Select to enable IGMP Snooping so that multicast traffic are forwarded to IGMP clients that have joined a multicast group. |

| | |
|---|---|
| **IGMP Fast Leave** | This option is shown only when IGMP Snooping is enabled. Select to enable IGMP Fast Leave.<br>Normally when the router receives a "leave" message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message. |

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

## II-5-8-2 Working Status

Displays a list of active multicast groups.




Available settings are explained as follows:

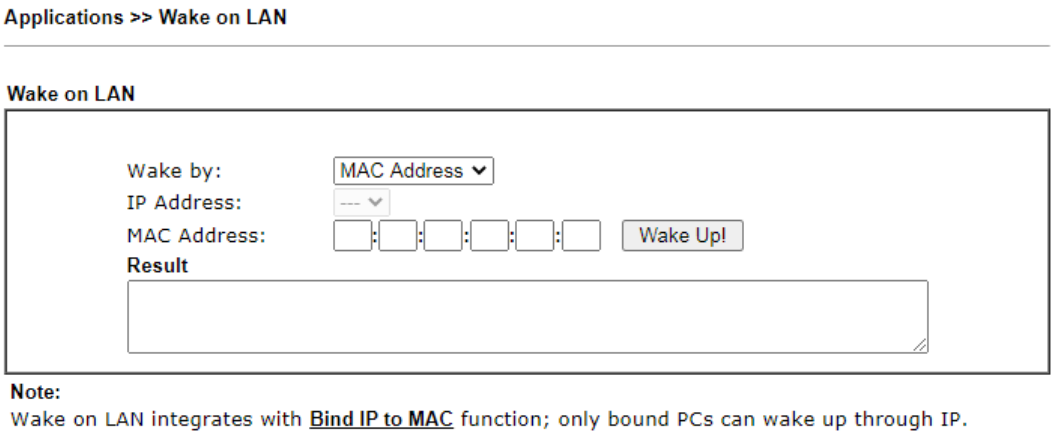
| Item | Description |
|---|---|
| **Refresh** | Click to reload the Multicast Group Table with the latest information. |
| **Index** | Index number of the multicast group. |
| **Group ID** | ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254. |
| **P1 to P5** | LAN ports that have IGMP hosts joined to this multicast group. |

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

## II-5-9 Wake on LAN

If you wish to be able to select the IP address of the Wake-on-LAN client, its MAC address must first be bound to a static IP address using the Bind IP to MAC function (see section 8.5 Bind IP to MAC).

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Wake by** | Two types provide for you to wake up the binded IP.<br>● If you choose Wake by **MAC Address**, you have to Enter the correct MAC address of the host in MAC Address boxes.<br>● 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. |

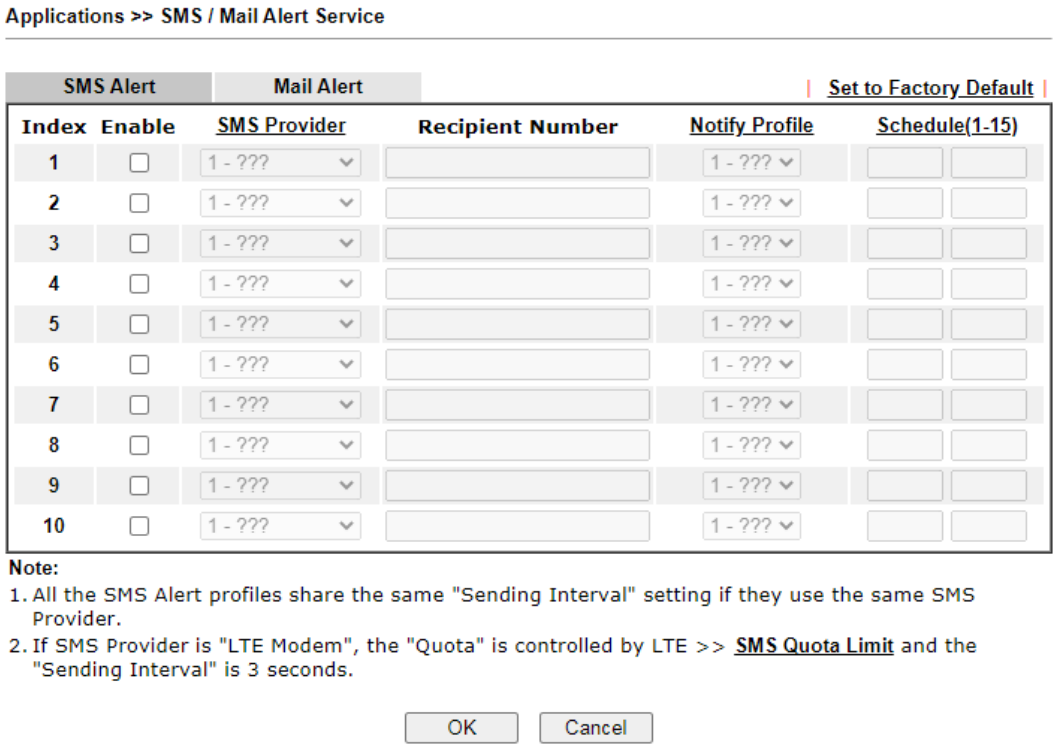
## II-5-10 SMS / Mail Alert Service

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.



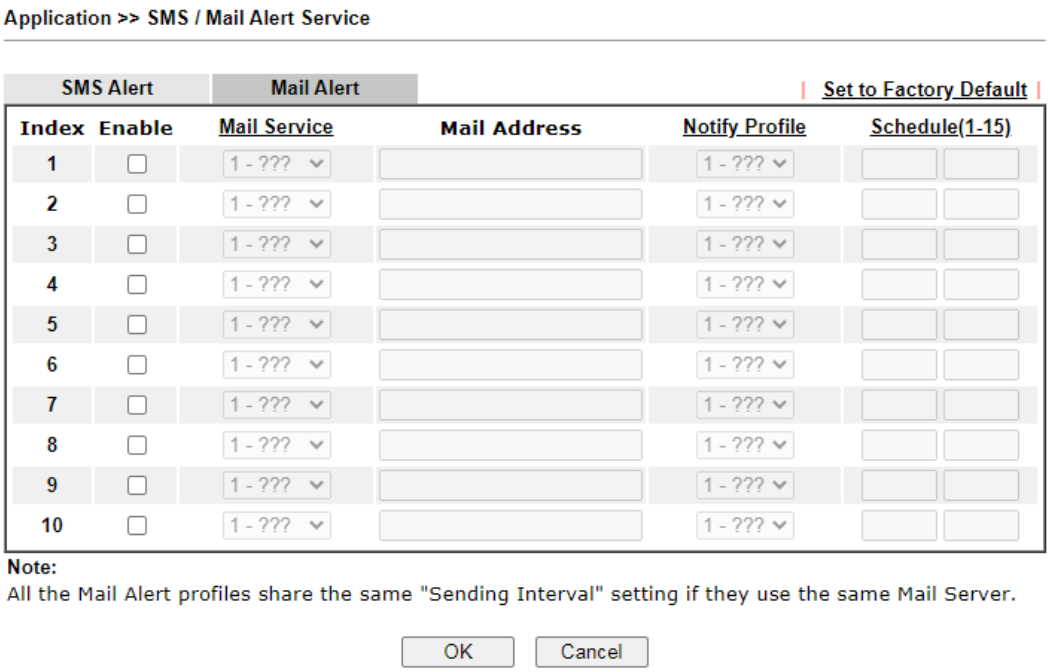

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check the box to enable or disable the profile. |
| **SMS Provider** | Use the drop down list to choose SMS service provider.<br>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.<br>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.<br>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 / disable this 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.<br>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.<br>You can click the **Schedule(1-15)** link to define the schedule. |

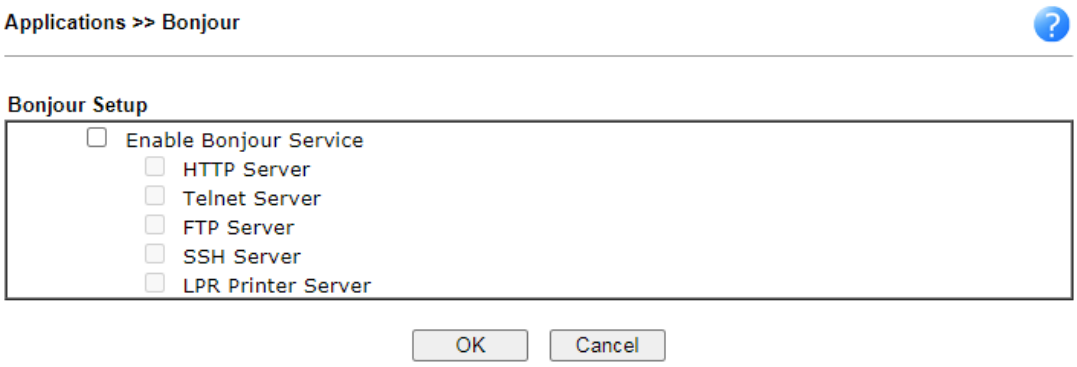
After finishing all the settings here, please click **OK** to save the configuration.

## 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.

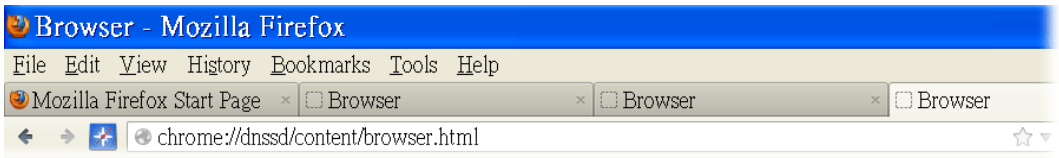
Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer 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.

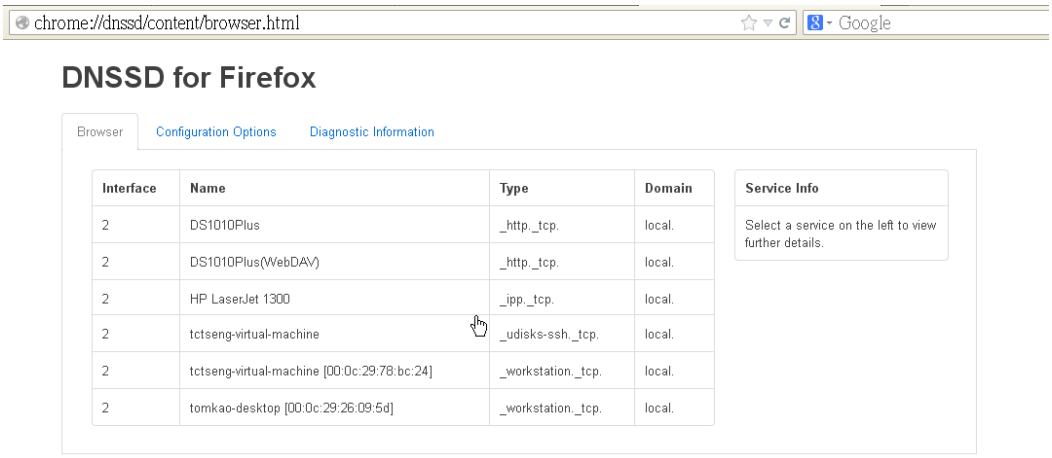



Below shows an example for applying the bonjour feature that Vigor router can be used as the FTP server.

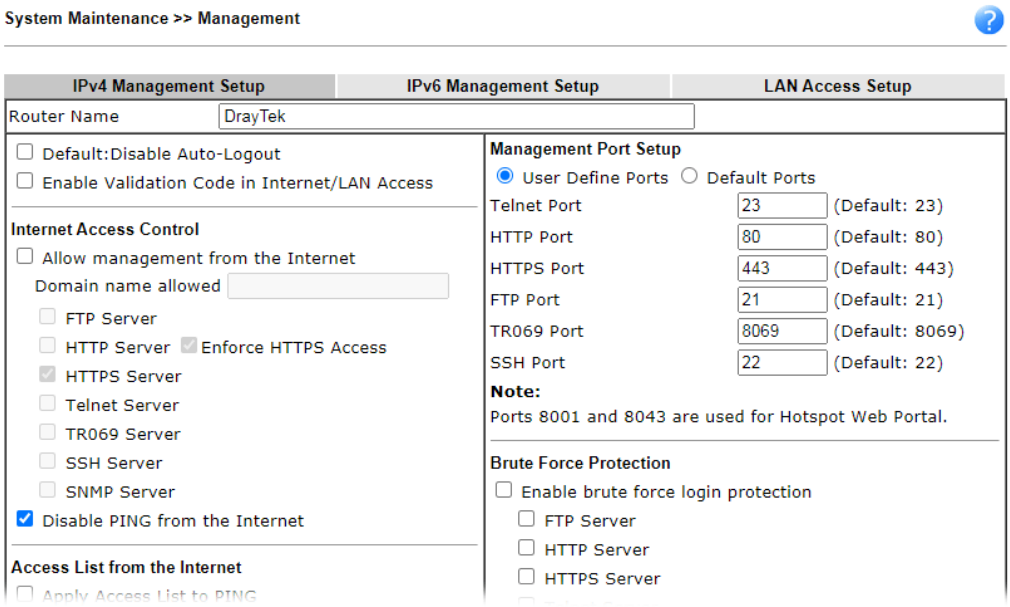
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



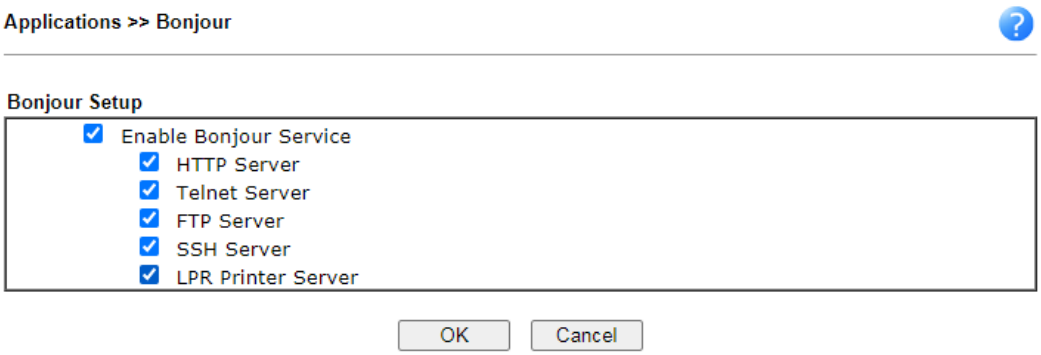
2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



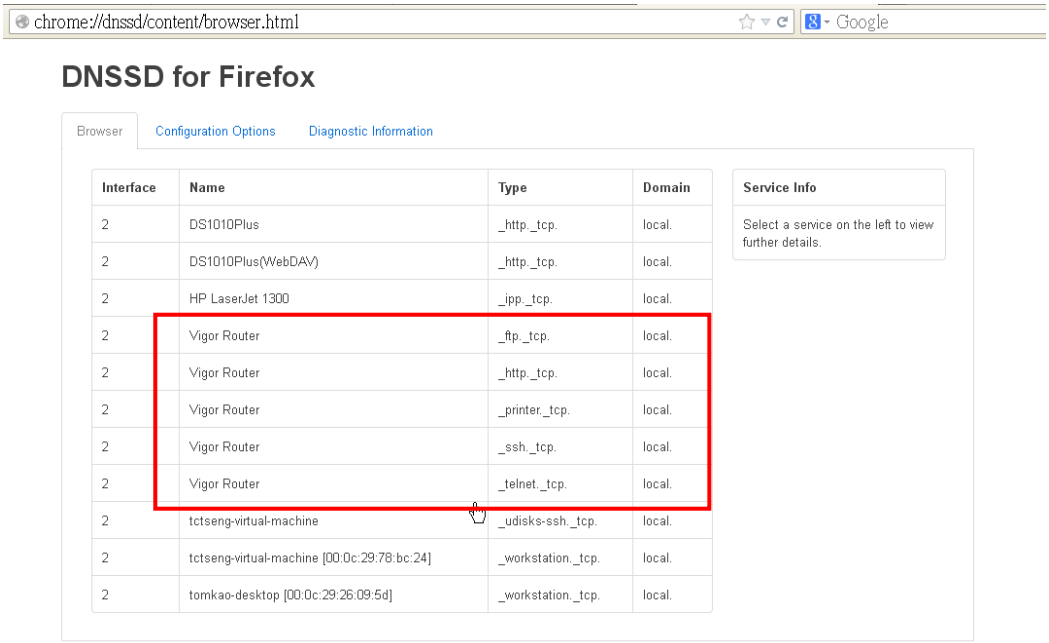

3. Open **System Maintenance>>Management**. Type a name as the Router Name and click **OK**.



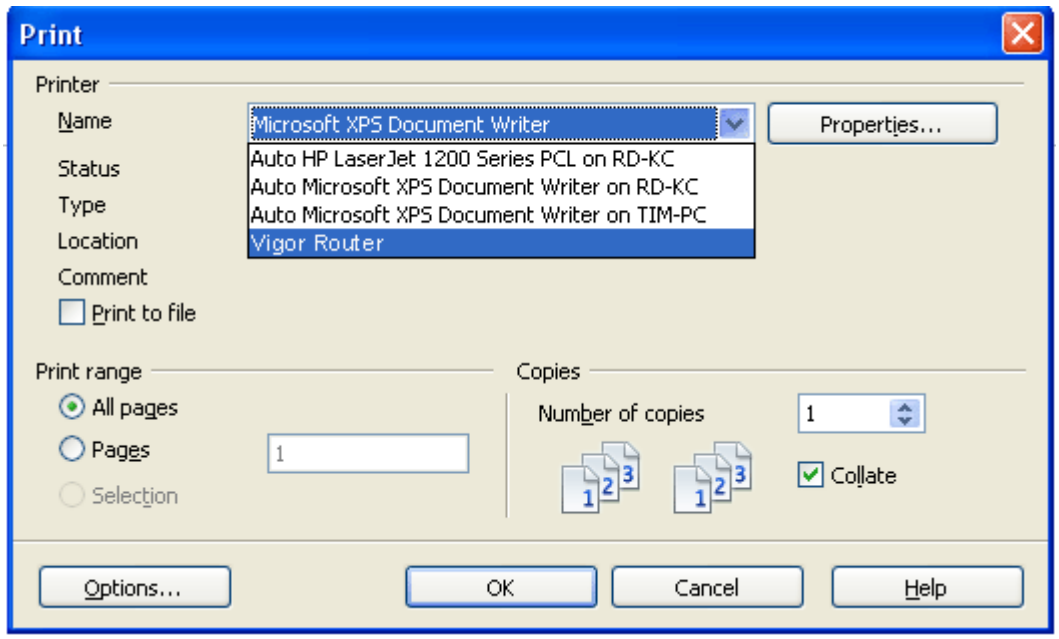

4. Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.




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).



## II-5-12 High Availability

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

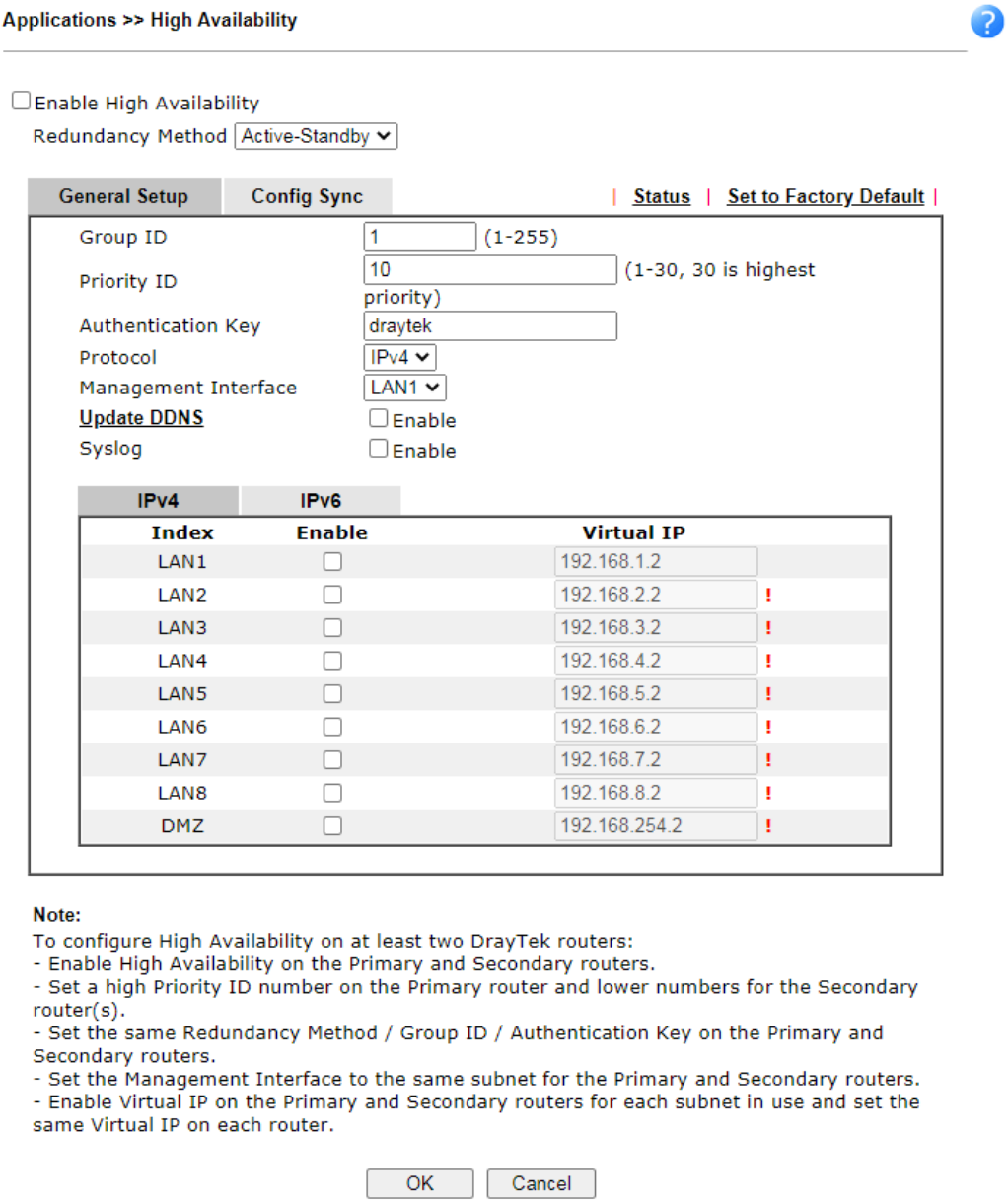
The HA of the Vigor2927 Series is designed to avoid single points-of-failure. When failures occur, the failover process transfers the network load handled by the failed component (the primary router) to the backup component (the secondary router), and the availability of network resources are preserved and partially failed transactions are recovered. In a matter of seconds the system returns to normal operation.

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

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

## II-5-12-1 General Setup

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable High Abailablity** | Check this box to enable HA function. |
| **Redundancy Method** | Select the redundancy method for high availability.<br>**Hot-Standby -**<br>Such method is suitable when there is only one ISP account. When this method is selected,<br>● During normal operation the secondary router will be idling. When the primary router fails to operate normally, the secondary router(s) will take over.<br>● WAN settings of the primary and secondary routers are |

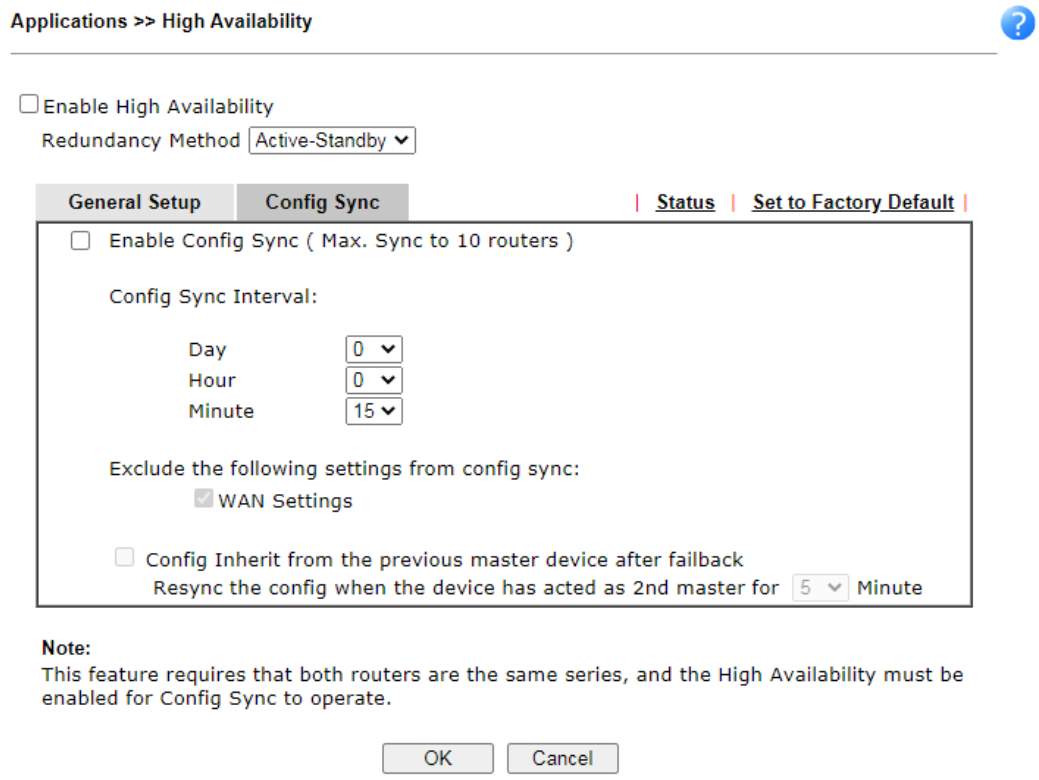
| | |
|---|---|
| | identical.<br>**Note**: When Hot-Standby is used, the wireless LAN function on secondary router will be "disabled" directlly. Clients can not connect to the secondary router any more.<br>**Active-Standby -**<br>This method is suitable when there are multiple simultaneously active ISP connections. When this method is selected,<br>● All WANs on the secondary routers can be up at the same time. LANs that are not configured under high availability can be routed to secondary routers.<br>● WAN settings of primary and secondary routers are independently configured.<br>● Config Sync may be enabled to synchronize most configuration settings between the primary and secondary routers.<br>● All routers must be set to the same redundancy method. |
| **Group ID** | Enter a value (1~255).<br>In LAN environment, multiple routers can be devided into several groups. Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group.<br>Only one of the routers in the same group will be selected as the primary router. |
| **Priority ID** | Enter a value (1~30).<br>Different routers must be configured with different IDs.<br>All routers within a group must be assigned a priority ID. Within a group, the router with the largest priority ID (i.e., the highest priority) will be the primary router. When multiple routers in a group are assigned the same priority ID, routers with lower LAN IP addresses (configured on the LAN >> General Setup page) have higher priority. |
| **Authentication Key** | Enter an authentication key up to 31 characters long. This is used to encrypt the DARP (DrayTek Address Redundancy Protocol) traffic to guard against malicious attacks. |
| **Protocol** | Select the IP protocol to be used for DARP. |
| **Management Interface** | Select the interface to be used for DARP negotiation between routers. Only interfaces which are enabled in **LAN>>General Setup** are available for selection.<br>However, LAN1 is always enabled. |
| **Update DDNS** | **Enable –** Check the box to update the DDNS server for the secondary device when the primary router fails.<br>If the primary device fails, and the secondary device must take over the job of data transmitting and receiving. Then the system will update the DDNS server to make the user connect to the specified domain name. |
| **Syslog** | **Enable –** Check the box to record required information on Syslog. |
| **LAN1 ~ LAN8, DMZ** | **Enable –** Check the box to enable the interface.<br>**Virtual IP -** Enter the IP address of the router plays the role |

| | |
|---|---|
| | of Primary device. |

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

## II-5-12-2 Config Sync

This page is used to specify the synchronization time for such Vigor router.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Config Sync (Max. Sync to 10 routers)** | Check this box to enable configuration synchronization.<br>To sync configuration from primary to secondary router, both primary and seconday routers need to enable "config sync". Note that config sync can be enabled by **Hot-Standby** redundancy method only. |
| **Config Sync Interval** | **Day / Hour / Minute** - The primary router will synchronize its configuration with secondary routers at every specified time interval. |
| **Exclude the following settings from config sync** | This setting is available when the Redundancy Method is set to **Hot Standby**.<br>Select the configuration settings to be excluded from synchronization. |
| **Config Inherit from the previous master device after failback** | The configuration inherits will be executed only when the device (router) plays the role of the master device.<br>Once another device with the priority ID higher than this device is ready to take over the management as the master device, after acting as the primary master for a while, this device will sync the configuration to all members in the same group and return to the role of the backup device (secondary |

| | |
|---|---|
| | master).<br>**Config Inherit**... for ( ) minute - Enter a value. |

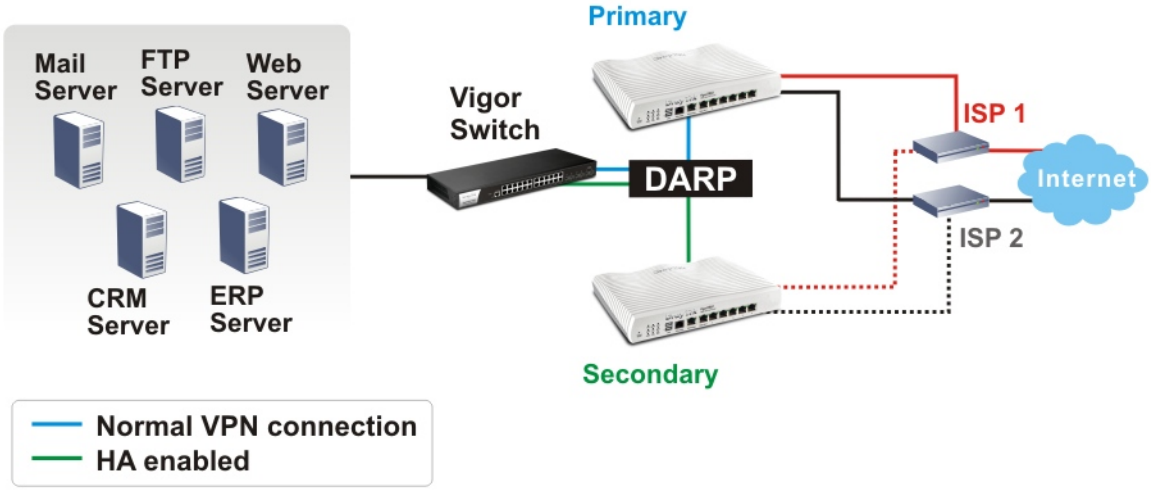
When you finish the configuration, please click **OK** to save and exit this page.

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

- WAN (user selectable)
- LAN
- LAN IPv6
- router name
- admin and user passwords

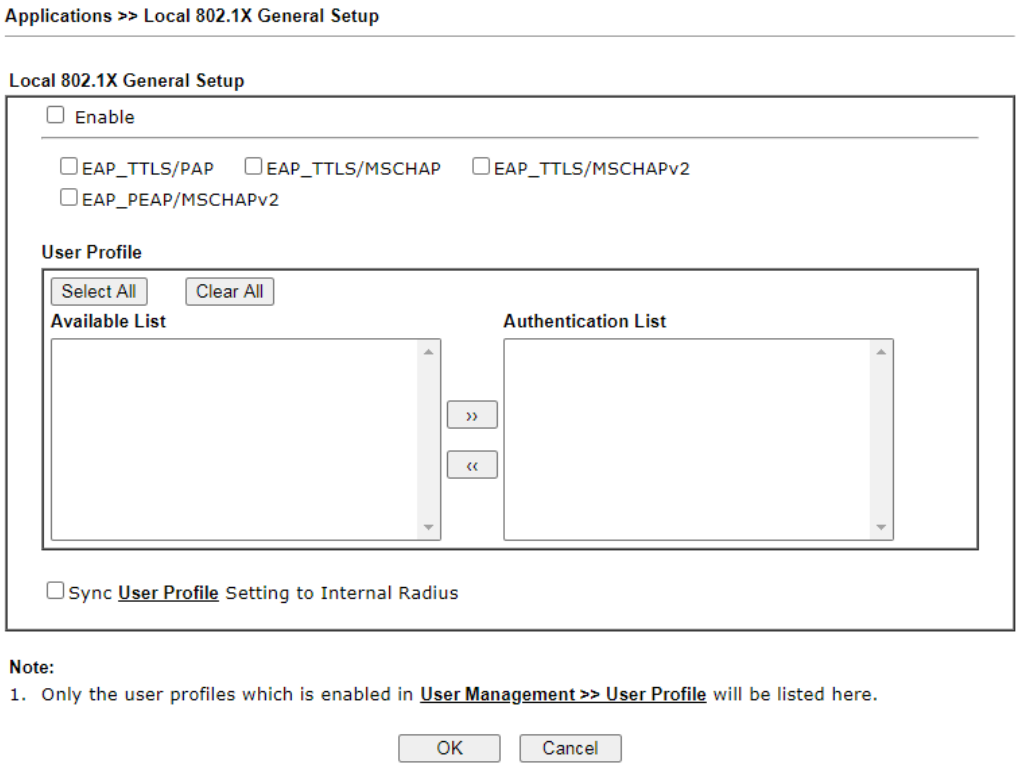
Example:

In the following example, the first Vigor2927 is configured as the primary device, and the other Vigor2927 is the secondary device. When the primary Vigor2927 breaks down, the secondary device assumes the role of the primary device by taking over all responsibilities as soon as possible. However, when the primary device recovers, the secondary device will once again be the standby device.



## II-5-13 Local 802.1X General Setup

Such page allows you to configure general settings for Local 802.1X server built in Vigor router. The local 802.X server can be used to authenticate wired and wireless LAN clients.




Available settings are explained as follows:

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

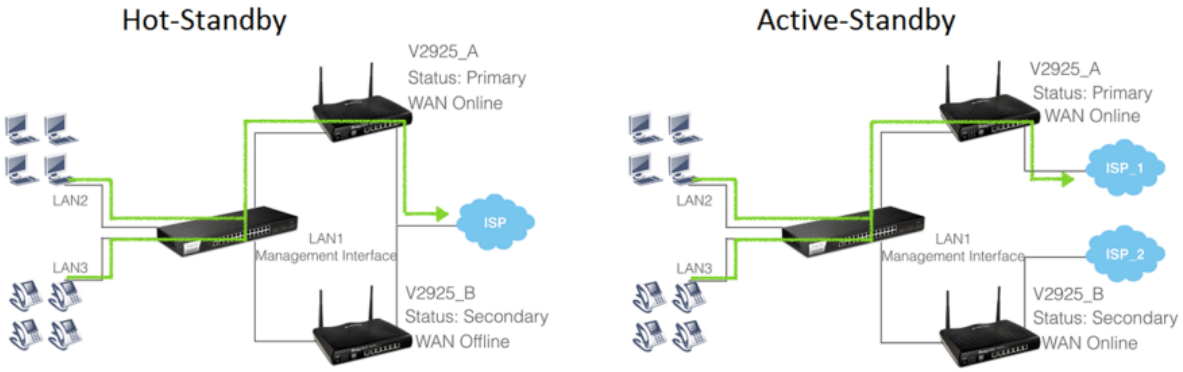
| | |
|---|---|
| |  |
| **OK** | Click it to save the settings. |
| **Cancel** | Click it to give up all settings configuration. |

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

# Application Notes

## A-1 How to use High Availability?

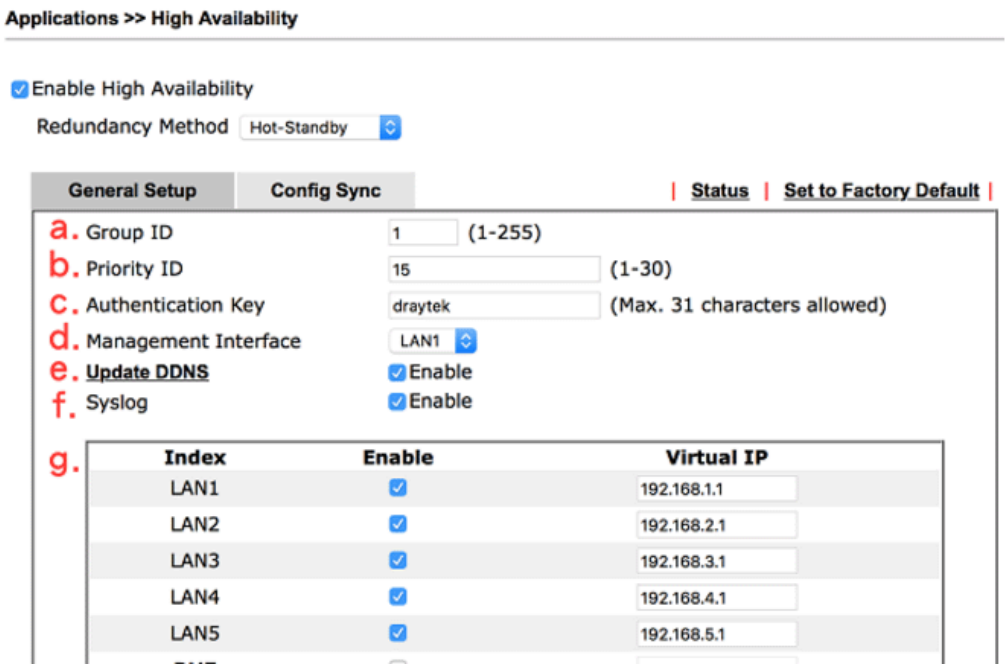
High Availability provides hardware redundancy to the LAN clients. DrayTek Router has two modes for High Availability feature: Hot-Standby and Active-Standby.




In Hot-Standby Mode, Primary and Secondary router share the same WAN source. Usually, only the Primary is online. When Primary goes down, Secondary comes up and use the same WAN line to dial up, and continue to provide Internet service to LAN clients.

Active-Standby mode is almost same as Hot-Standby mode, only that in the Active-Standby mode, the Primary and Secondary connect to the different WAN sources; also, the Secondary will always be online.

1. On the primary router, choose Redundancy Method you would like to use, then set the following configurations:




(a) Group ID is used to identify who are the group members, enter the same ID on all the members. The default value is 1, we may leave it as default here.

(b) Priority ID is used to decide which router should be the primary one, and 30 is the highest. If 2 or more routers are having the same Priority ID, their LAN IP addresses (for management Interface) will be considered, e.g., 192.168.1.2 has higher priority than 192.168.1.3…, etc.

(c) Authentication Key: enter the same authentication key on all the members.

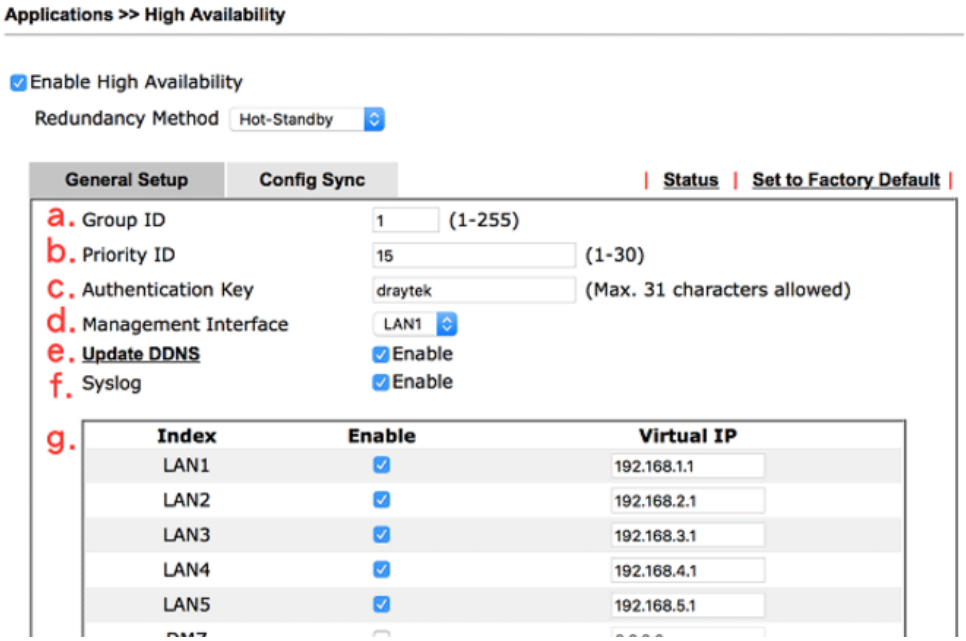
(d) Management Interface: the packets for communication (including deciding the primary, configuration sync, and some maintenance…,etc) between members will be sent in the management interface, in other word, clients in other LAN subnet won't be able to see these packets. In order to have best communication and for security purpose, we recommend to choose an interface that is less possible to have interruption for the communication (loop/broadcast storm from other LAN clients…). In our scenario, we reserve LAN 1 for High Availability only, and put all other LAN clients in LAN2~LAN5.

(e) Update DDNS: for dynamic WAN IP users, enable this function so once the secondary router becomes primary and dials up the WAN, it will also update its new WAN IP address to the same DDNS profile, so your network will be accessible with the same DDNS domain.

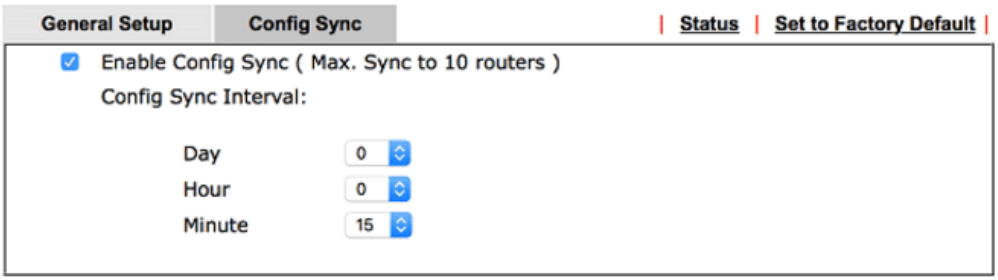
(f) Syslog: enable to show all the High Availability related logs in syslog.

(g) Enable the LAN Subnet to join High Availability. Any existing LAN without joining High Availability will not be served with hardware redundancy.

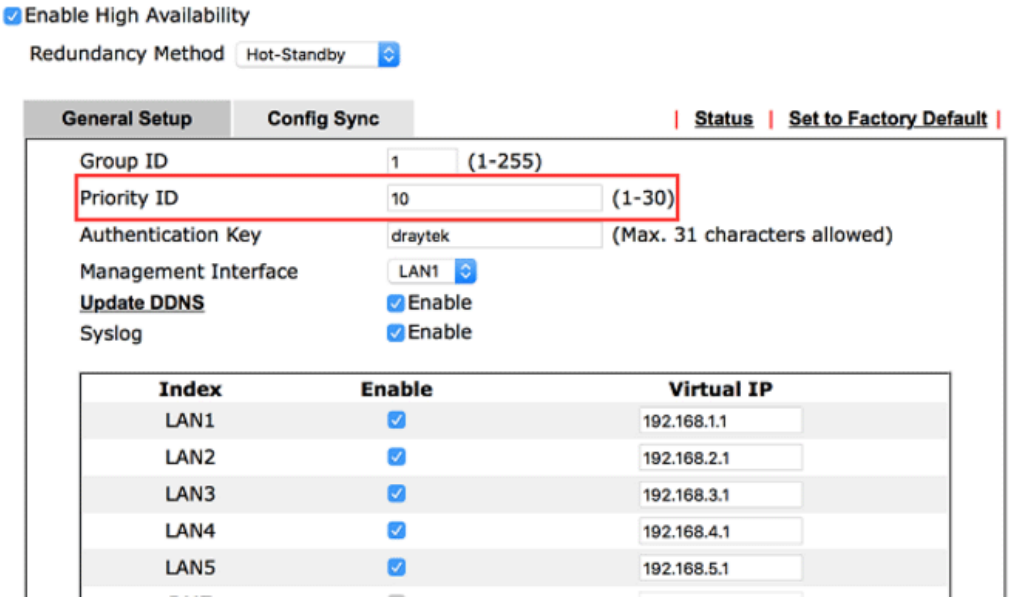
Virtual IP: name the virtual IP here, please note that the virtual IP can NOT be the same with any member LAN IP.



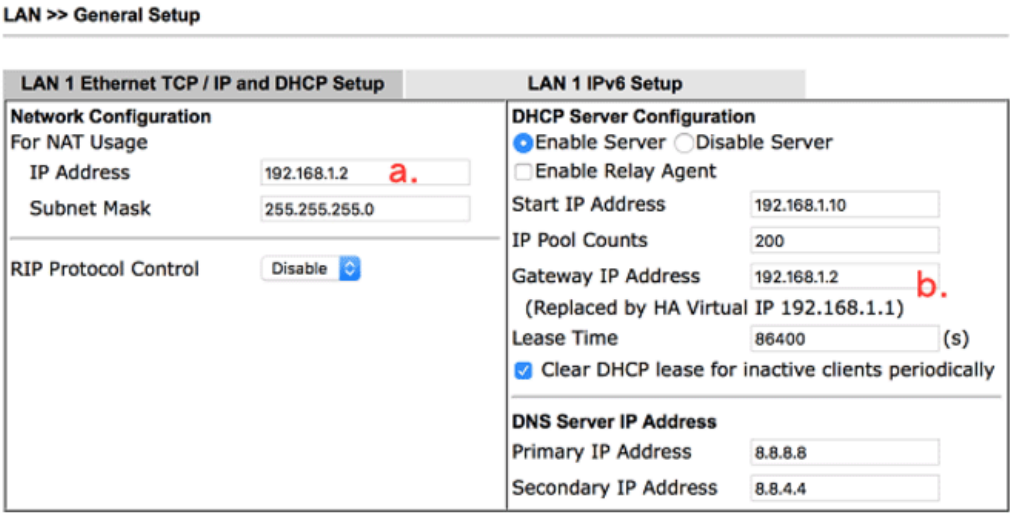

2. Enable Configuration Sync and set the Sync Interval. Default is every 15 minutes.




3. Configure High Availability on the secondary router. Mind that the Priority should be lower than the primary router. Besides priority, all other settings should be the same.



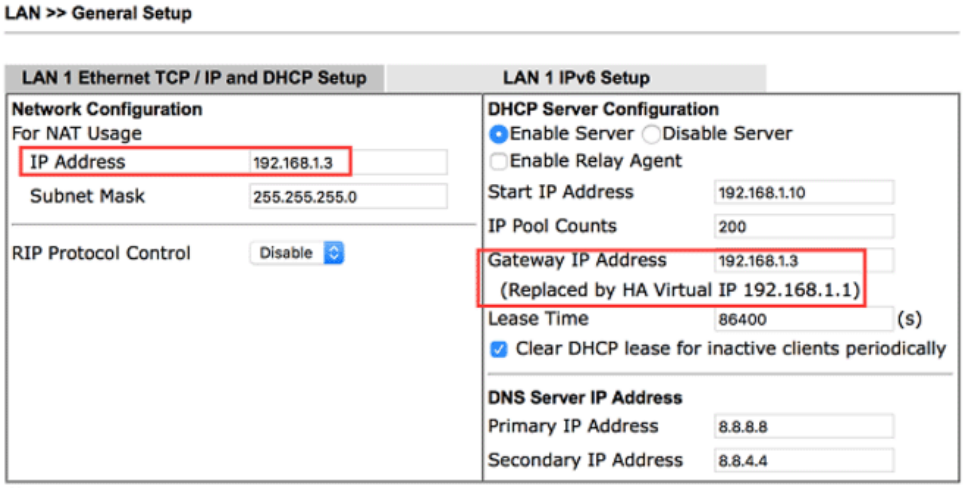

4. Configuring LAN on the primary router.




(a) Set up the LAN IP address, it has to be different from the Virtual IP and the LAN IP of secondary router. Again, for any routers with the same Priority ID, their IP addresses will be compared, so we suggest to use a IP with lower number on the Primary one.

(b) Gateway IP is the same with LAN IP, and the note in parentheses indicates that the gateway IP provided to LAN clients will be replaced by the Virtual IP.

5. Configure LAN on the secondary router. Mind that the IP should be different and larger than it on the primary router.

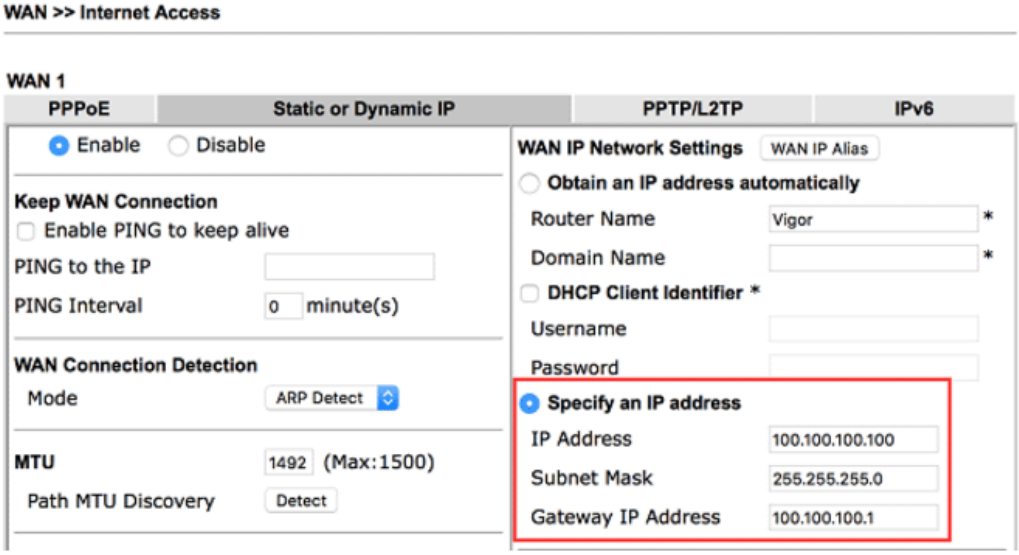



**Info**

If you have more than one LAN, you should set all the LAN IP of each LAN on Primary and Secondary routers to different IP addresses to avoid IP conflict. Here is the example, there are several LAN and all of them are under the protection of hardware redundancy:

| | Subnet | Primary Router | Secondary Router | Virtual IP |
|---|---|---|---|---|
| LAN1 | 192.168.1.0 | 192.168.1.2 | 192.168.1.3 | 192.168.1.1 |
| LAN2 | 192.168.2.0 | 192.168.2.2 | 192.168.2.3 | 192.168.2.1 |
| LAN3 | 192.168.3.0 | 192.168.3.2 | 192.168.3.3 | 192.168.3.1 |
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |
| LANx | 192.168.x.0 | 192.168.x.2 | 192.168.x.3 | 192.168.x.1 |

6. We have setup High Availability on both routers, and before we link up both routers, it's time to setup all other functions on the primary router so later we can see the configuration sync taking place. If your primary router is already settled please proceed to the next step. Here we configure the WAN as the representative example.

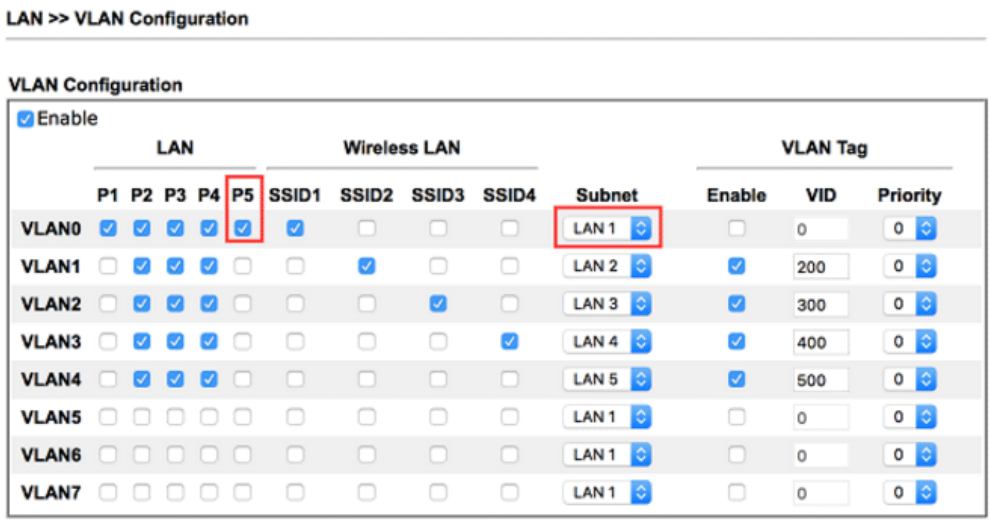


Then confirm the WAN setup by seeing WAN online.

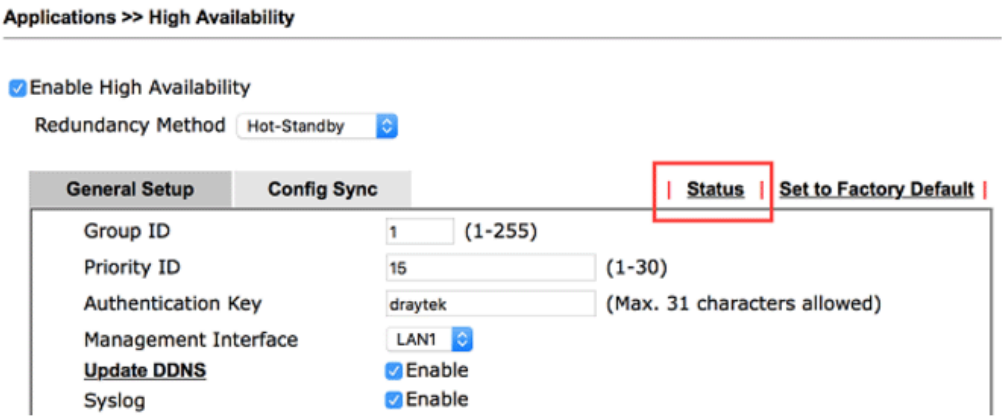
| System Information | | | |
|---|---|---|---|
| Model Name | Vigor2862ac | System Up Time | 100:23:32 |
| **Router Name** | DrayTek | **Current Time** | Wed Jan 05 2000 04:23:26 |
| Firmware Version | 3.8.8_RC10_STD | Build Date/Time | Feb 6 2018 18:42:30 |
| DSL Version | 772801 HW: A | LAN MAC Address | 00-1D-AA-5D-C9-E0 |

| IPv4 LAN Information | | | | | |
|---|---|---|---|---|---|
| | **IP Address** | **DHCP** | | **IP Address** | **DHCP** |
| **LAN1** | 192.168.1.3/24 | v | **LAN2** | 192.168.2.1/24 | v |
| **LAN3** | 192.168.3.1/24 | v | **LAN4** | 192.168.4.1/24 | v |
| **LAN5** | 192.168.5.1/24 | v | **LAN6** | 192.168.6.1/24 | v |
| **LAN7** | 192.168.7.1/24 | v | **LAN8** | 192.168.8.1/24 | v |
| **DMZ PORT** | 192.168.17.1/24 | v | **IP Routed Subnet** | 192.168.0.1/24 | v |

7. After all the functions are set properly on the primary router, we link up the management interface LAN so both routers can start detecting each other, deciding which one should be the primary and syncing the configuration. Since the routers will communicate via the Management Interface, it's required to use the ports that belong to the Management Interface LAN (LAN1 in this scenario). We can check for this information in LAN >> VLAN. In this scenario we can use the port 5 on both routers, so we use an Ethernet cable to wire up LAN port 5 on both routers.




8. We may check the High Availability status by visiting the Status page.




For the first time the two routers link up, we can see they are syncing the configuration from the primary to the secondary (showing "Progressing" on the secondary router):

Diagnostics >> High Availability Status

| Details | HA Setup | Renew | Refresh |

| Status | Router Name | IPv4 | State | Stable | WAN | Config Sync Status | Cached Time |
|---|---|---|---|---|---|---|---|
| O | V2925_A | 192.168.1.2 | Primary | Yes | At Least One Up - Eth | Ready Sync | - |
| O | V2925_B | 192.168.1.3 | Secondary | Yes | All WANs Down | Progressing | 5 min up |

Note: The "Cached Time" indicates the time that router has got the information from the other router ago. Click "Renew" to update the information of remote router, click "Refresh" to update the information of local router.

When a sync is finished or the routers are already having the same configuration, it will show the "Equal" result:

Diagnostics >> High Availability Status

| Details | HA Setup | Renew | Refresh |

| Status | Router Name | IPv4 | State | Stable | WAN | Config Sync Status | Cached Time |
|---|---|---|---|---|---|---|---|
| O | V2925_A | 192.168.1.2 | Primary | Yes | At Least One Up - Eth | Ready Sync | - |
| O | V2925_B | 192.168.1.3 | Secondary | Yes | All WANs Down | Equal | 3 min 6 sec |

Note that the router will check if there's any un-synced modification when it reaches the time interval we set in step 2. We may force to sync by clicking the "Sync" button. The secondary router will reboot after the config sync.

9. Now we may inspect if the secondary router received the configuration from the primary router. In this scenario we check the secondary router online status.

| System Information | | | |
|---|---|---|---|
| Model Name | Vigor2925Vn | System Up Time | 0:01:13 |
| Router Name | V2925_B | Current Time | 2015 Oct 19 Mon 11:40:29 |
| Firmware Version | 3.8.2 | Build Date/Time | Oct 14 2015 21:25:18 |
| LAN MAC Address | 00-1D-AA-BE-92-60 | | |

| IPv4 Internet Access | | | | |
|---|---|---|---|---|
| | Line / Mode | IP Address | MAC Address | Up Time |
| WAN1 | Ethernet / Static IP | Disconnected-HA | 00-1D-AA-BE-92-61 | 00:00:00 |
| WAN2 | Ethernet / Static IP | Disconnected-HA | 00-1D-AA-BE-92-62 | 00:00:00 |
| WAN3 | USB / --- | Disconnected-HA | 00-1D-AA-BE-92-63 | 00:00:00 |
| WAN4 | USB / --- | Disconnected-HA | 00-1D-AA-BE-92-64 | 00:00:00 |

Before syncing we didn't configure the WAN, now seeing WAN1 and WAN2 having "Static IP" indicates it did receive the corresponding configurations. And the "Disconnected-HA" means this router is not dialing up the WAN due to the primary router in the High Availability group is working, so as a secondary router it doesn't need to be online now. You may also check other configurations on your secondary router.

10. We may also check the Details page.

**Diagnostics >> High Availability Status >> Details**

[ Local Router ] | Back | HA Setup | Renew | Refresh |

| V2925_A | | | | 192.168.1.2 |
|---|---|---|---|---|
| State | Stable | WAN | Config Sync Status | Cached Time |
| Primary | Yes | At Least One Up - Eth | Ready Sync | - |
| MAC | | 00:1d:aa:c6:4b:d8 | HTTPs Port | 4430 |
| Model | | Vigor2925Vn | Firmware Version | 3.8.2 |
| Enable High Availability | | On | Redundancy Method | Hot-Standby |
| Group ID | | 1 | Priority ID | 15 |
| Authentication Key | | draytek | Management Interface | LAN1 |
| Update DDNS | | On | | |
| Virtual IP | | On | LAN1 | 192.168.1.1 |
| | | | LAN2 | 192.168.2.1 |
| | | | LAN3 | 192.168.3.1 |
| | | | LAN4 | 192.168.4.1 |
| | | | LAN5 | 192.168.5.1 |
| Enable Config Sync | | On | Config Sync Interval | 0 Day 0 Hour 15 Minute |

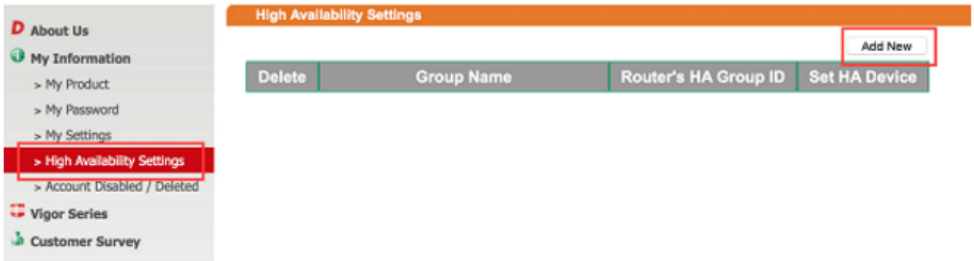
[ Other Router ]
Secondary

| V2925_B | | | | 192.168.1.3 |
|---|---|---|---|---|
| State | Stable | WAN | Config Sync Status | Cached Time |
| Secondary | Yes | All WANs Down ! | Progressing | 5 min up |
| MAC | | 00:1d:aa:be:92:60 | HTTPs Port | 4430 |
| Model | | Vigor2925Vn | Firmware Version | 3.8.2 |
| Enable High Availability | | On | Redundancy Method | Hot-Standby |
| Group ID | | 1 | Priority ID | 10 |
| Authentication Key | | draytek | Management Interface | LAN1 |
| Update DDNS | | Off | | |
| Virtual IP | | On | LAN1 | 192.168.1.1 |
| | | | LAN2 | 192.168.2.1 |
| | | | LAN3 | 192.168.3.1 |
| | | | LAN4 | 192.168.4.1 |
| | | | LAN5 | 192.168.5.1 |
| Enable Config Sync | | On | Config Sync Interval | 0 Day 0 Hour 15 Minute |

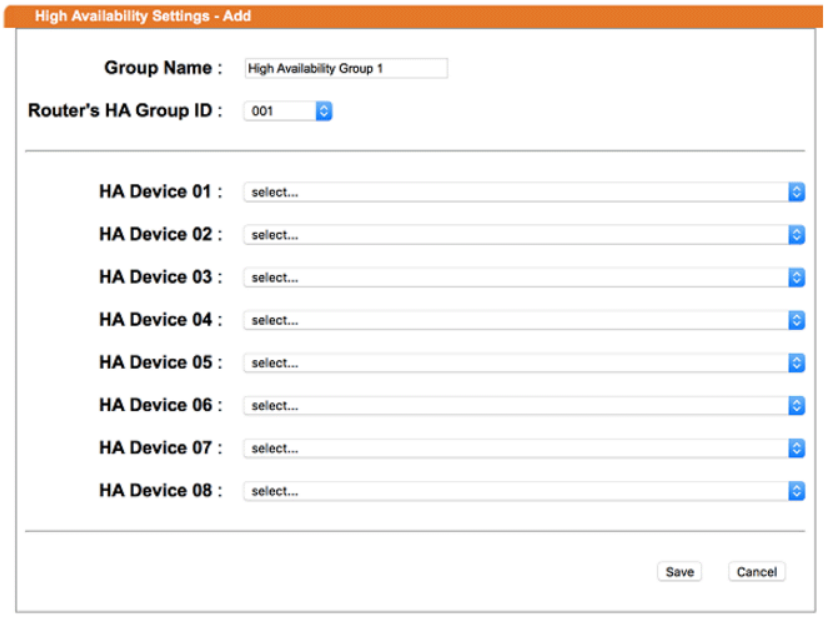
## Sharing the WCF License

11. Now the routers are set, if you have WCF license, you may create a group on MyVigor so these routers can share the same license.

    (a) First, login to myvigor.draytek.com, find High Availability Settings on left hand side and click Add New

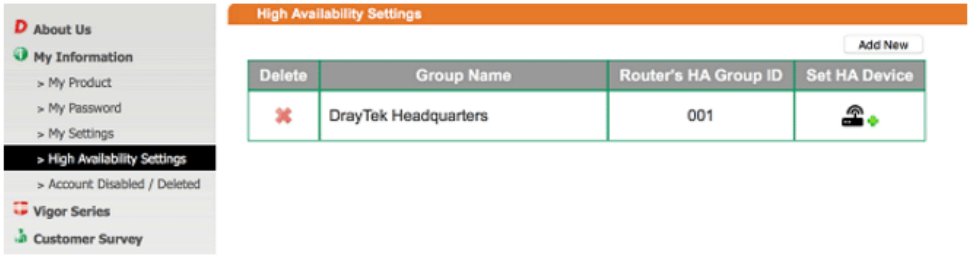


(b) Give a Group Name, select an HA unused Group ID, and select the member routers in the HA Device drop-down menu:




Note that the drop-down menu only lists out the devices that are registered under this MyVigor account. If you don't find the router you are using, please find out which account this device is registered under.

(c) Save the profile, and we can see the group entry:




## Send the Notification to Network Administrator

We can set Vigor Router to notify the network administrator by sending email or SMS when the following events occur:

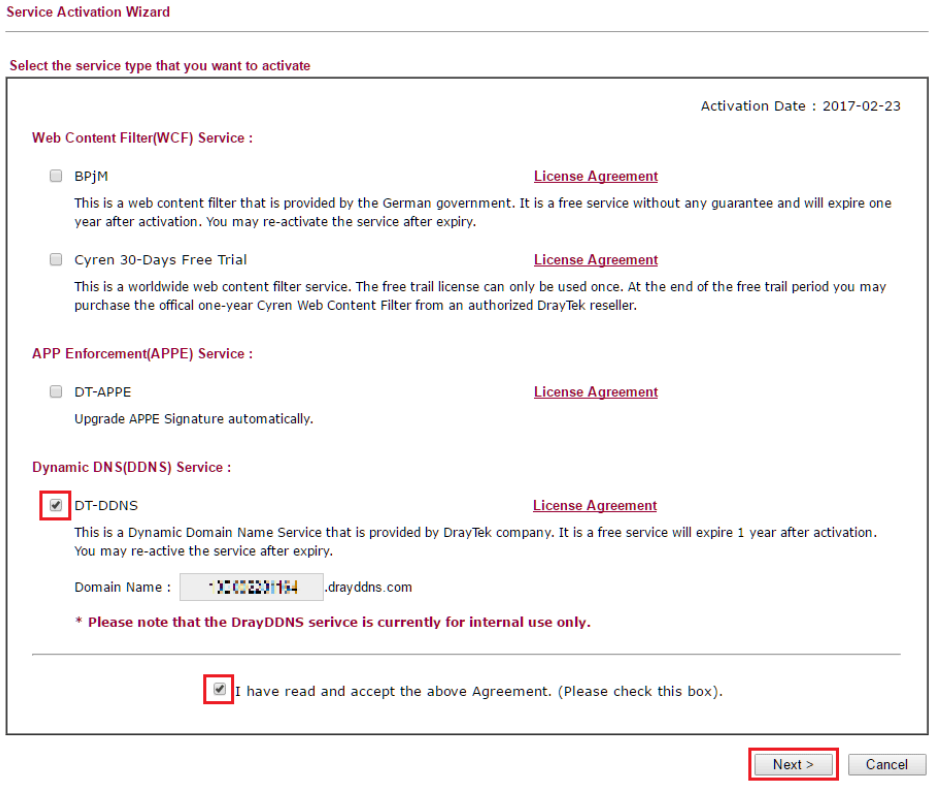
1. Failover Occurred: the WAN of the primary router goes down and the secondary router takes over,
2. Configuration Sync Failed: the configuration sync between primary and secondary router fails,
3. Router Unstable: one of the routers becomes unstable.

## A-2 How to use DrayDDNS?

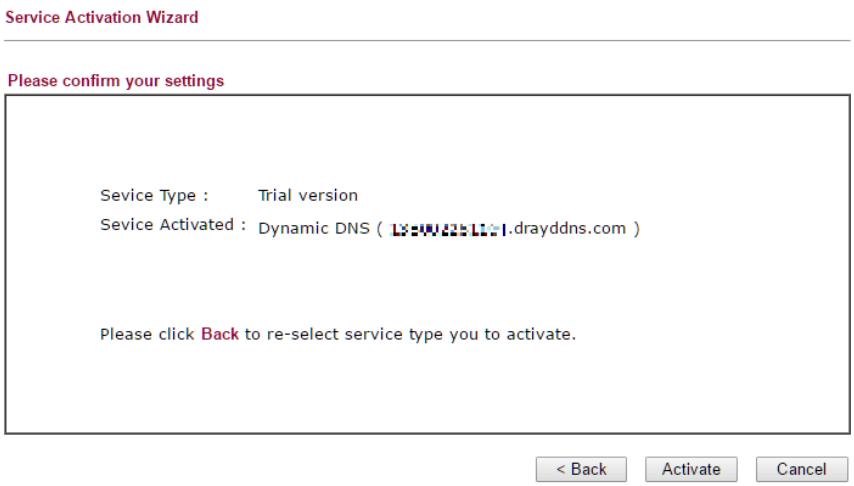
Vigor router supports various DDNS service providers, user can set up user-defined profile to update the DDNS even the service provider is not on the list. Now, DrayTek starts to support our own DDNS service - DrayDDNS. We will provide a domain name for each Vigor Router, this single domain name can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

### Activate DrayDDNS License

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




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




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

**DrayTek Service Activation**

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

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

## Configure DDNS Profile

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

   a. Tick **Enable Dynamic DNS Setup**

   b. Click an available profile index

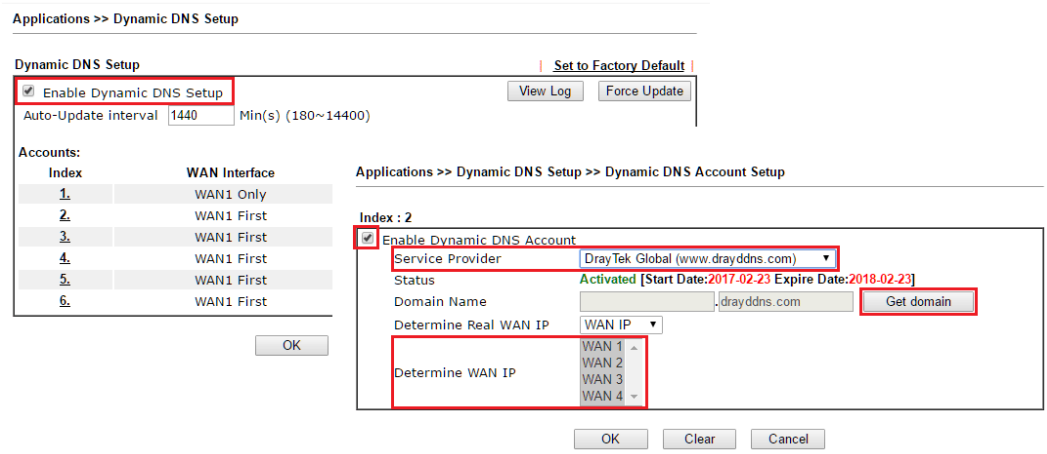
   c. Tick **Enable Dynamic DNS Account**

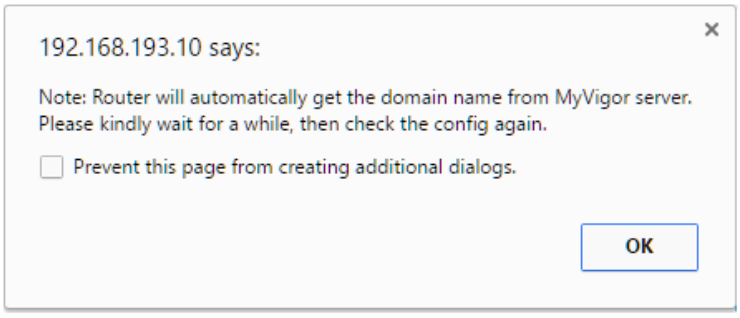
   d. Select **DrayTek Global (www.drayddns.com)** as **Service Provider**

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

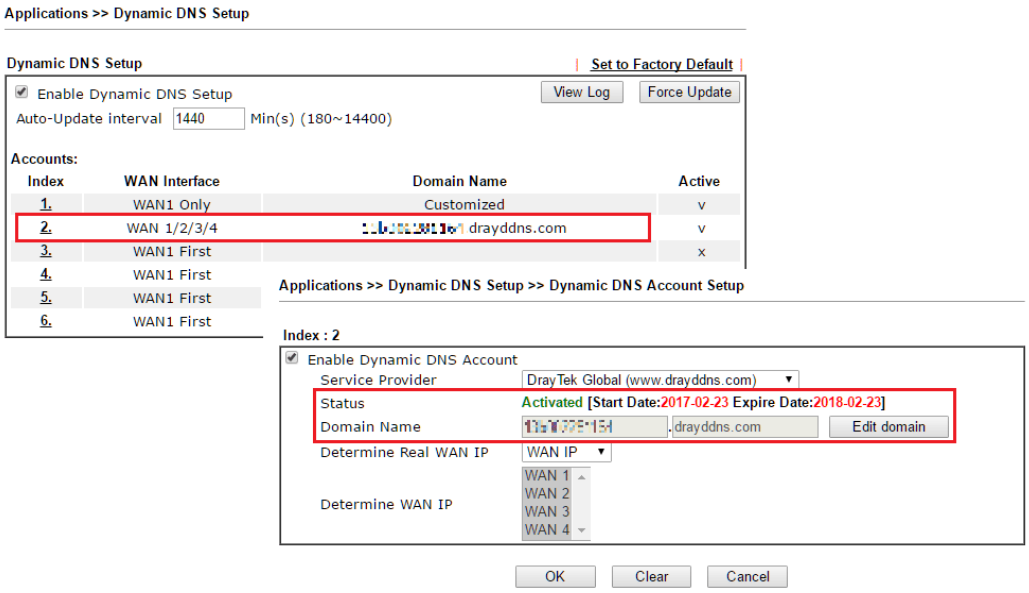
   f. Click **Get domain**

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



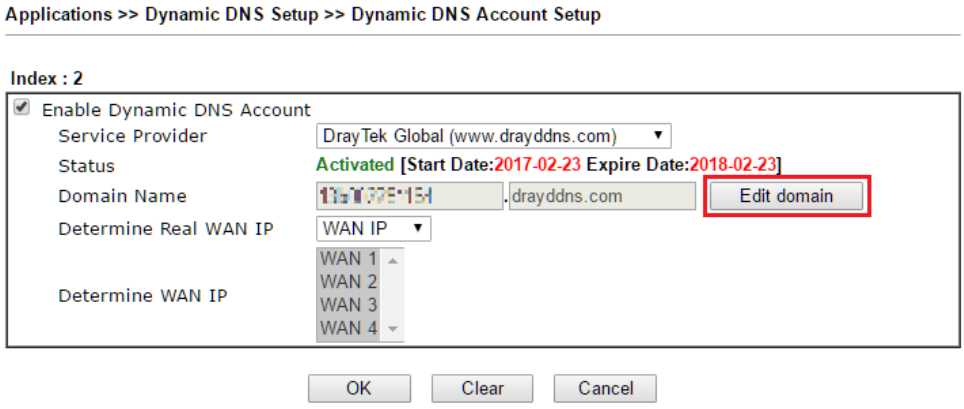
2. Wait few seconds for router to get the domain name, then, we can click the profile to check the information of license and domain name.



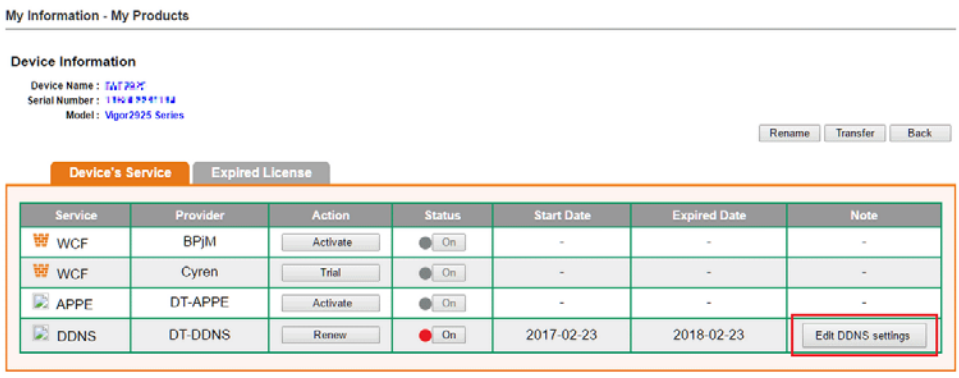

## Modify Domain Name

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

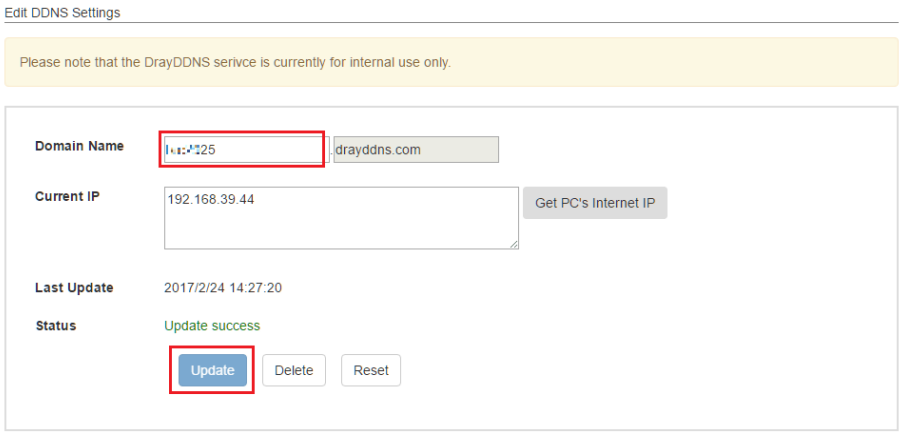
1. Please visit https://myvigor.draytek.com/ or go to **Applications >> Dynamic DNS Setup >> DrayDDNS** profile and click **Edit domain**.



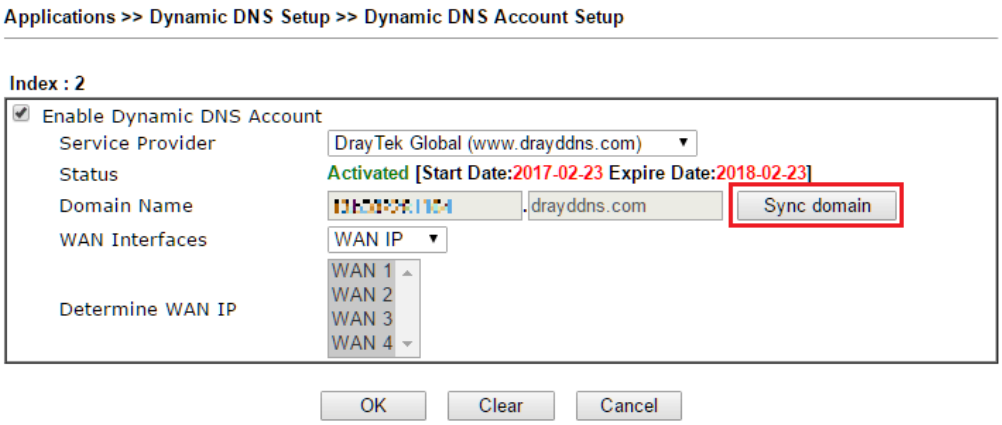

2. Log in to MyVigor Website, choose the profile, then click **Edit DDNS settings**.



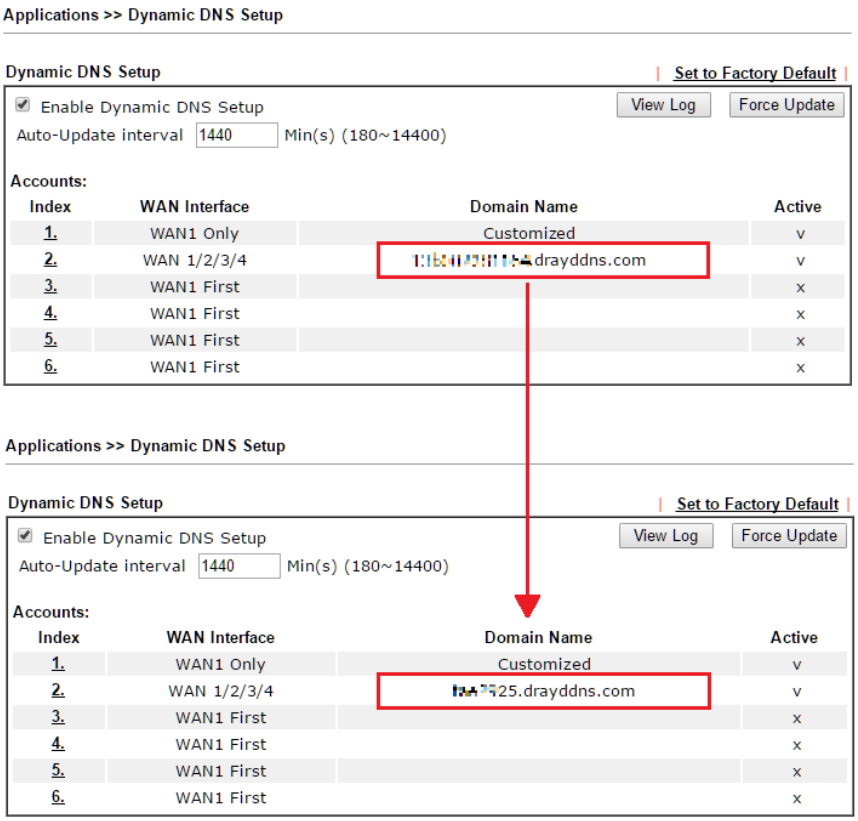
3. Input the desired **Domain name (e.g., XXXX25)** and click **Update.**




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




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


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

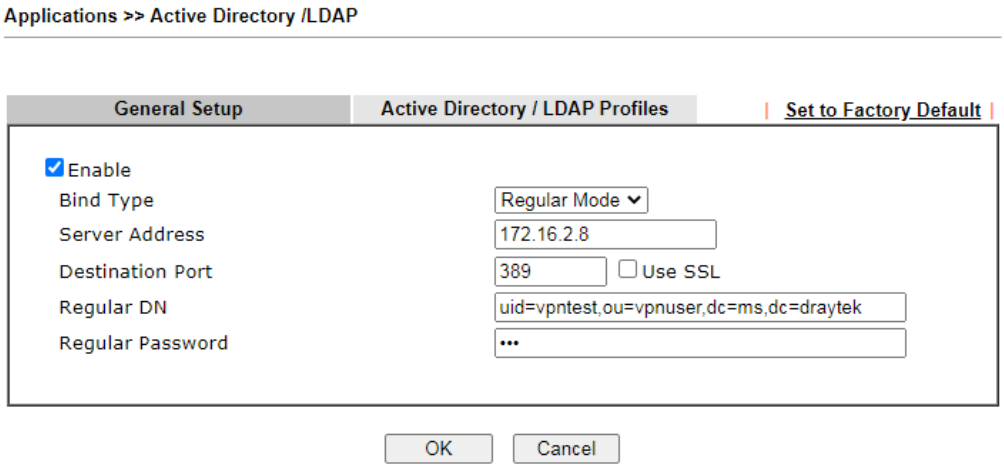
## A-3 How to Implement the LDAP/AD Authentication for User Management?

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

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

Below shows the configuration steps:

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

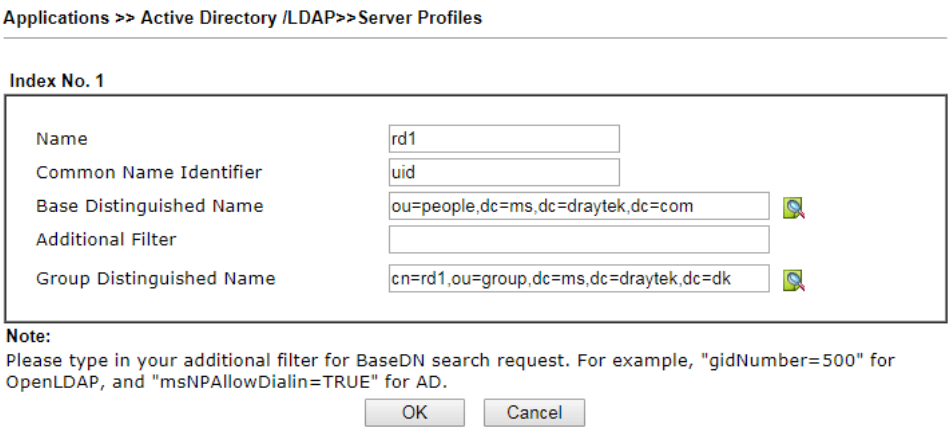



There are three types of bind type supported:

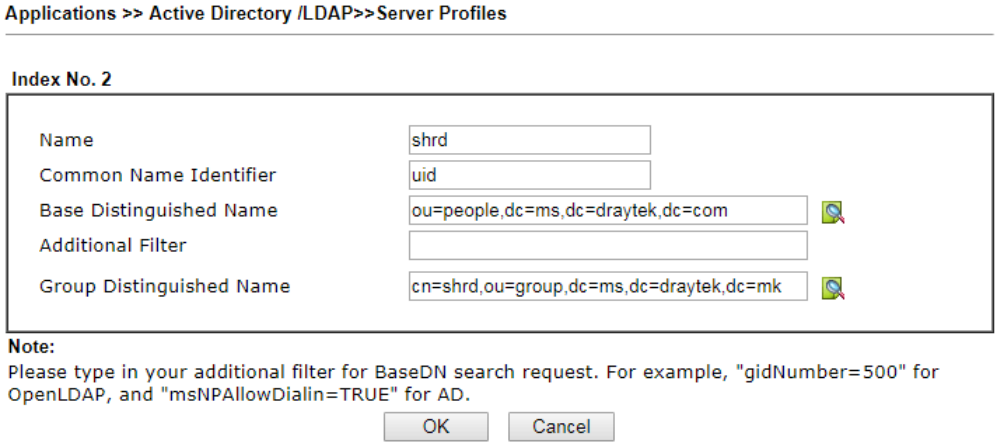
- **Simple Mode** – Just simply do the bind authentication without any search action.
- **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check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

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

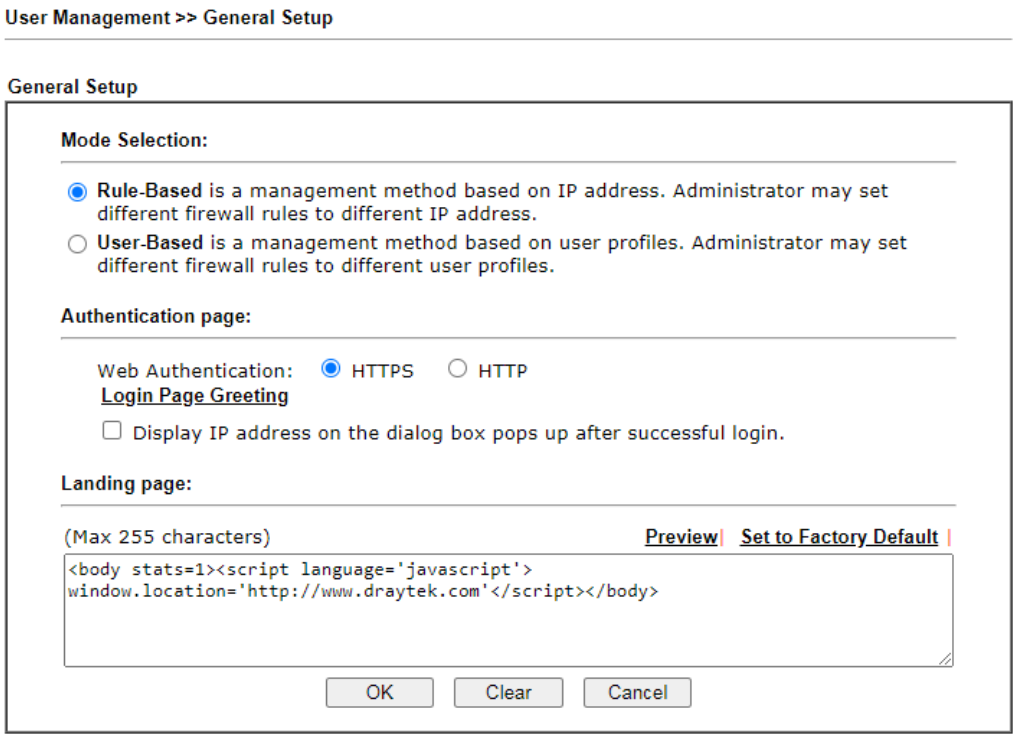
   If we have two groups “**RD1**” and “**SHRD**” on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.



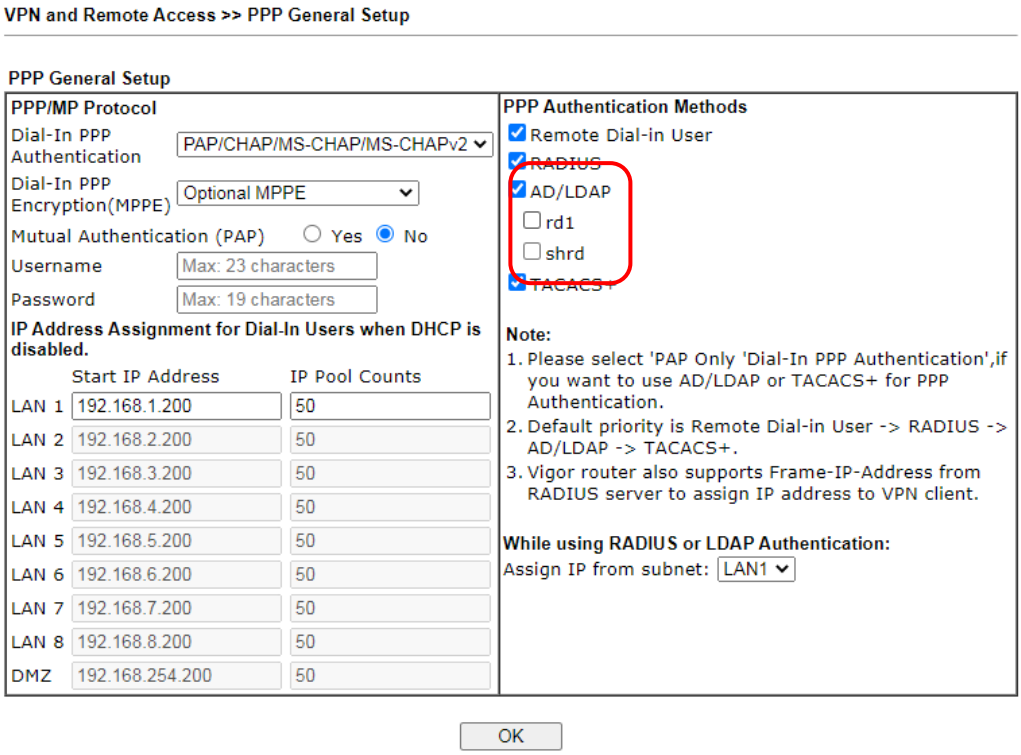
and




4. Click **OK** to save the settings above.
5. Open **User Management>>General Setup.** Select **User-Based** as the **Mode** option.



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




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

## A-4 How to Configure Customized DDNS?

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

### Part A : Changeip.org

**Online Status**

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

| IPv4 | IPv6 |
|---|---|

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

**WAN 1 Status** — >> Drop PPPoE

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

Note that,

Username: jo***

Password: jo********

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

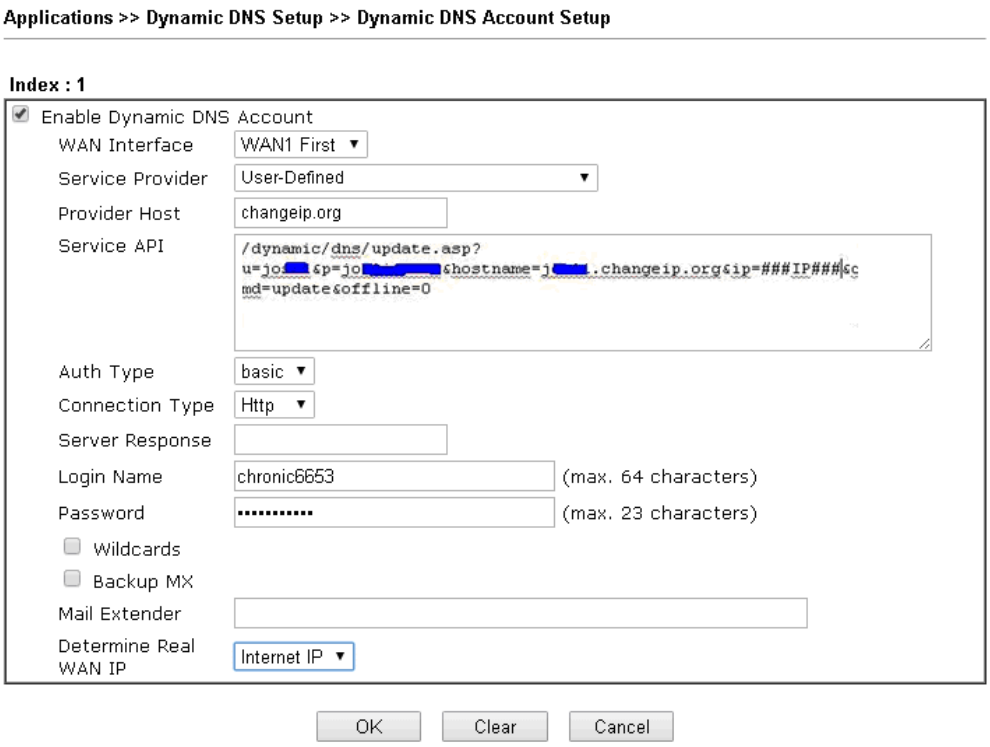
WAN IP address: 1.169.185.242

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



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

3. Please go to **Applications >> Dynamic DNS** to create a profile for customized DDNS client.




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

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

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

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

## Part B : 3322.net

| WAN 1 | |
|---|---|
| Link Status | : Connected |
| MAC Address | : 00-50-7F-C8-C6-A1 |
| Connection | : PPPoE |
| IP Address | : 111.243.178.53 |
| Default Gateway | : 168.95.98.254 |
| Primary DNS | : 168.95.192.1 |
| Secondary DNS | : 168.95.1.1 |

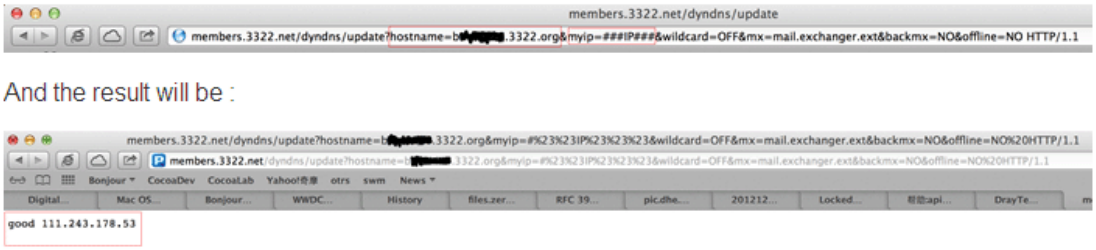
Username: bi*******

Password: 88********

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

WAN IP address: 111.243.178.53

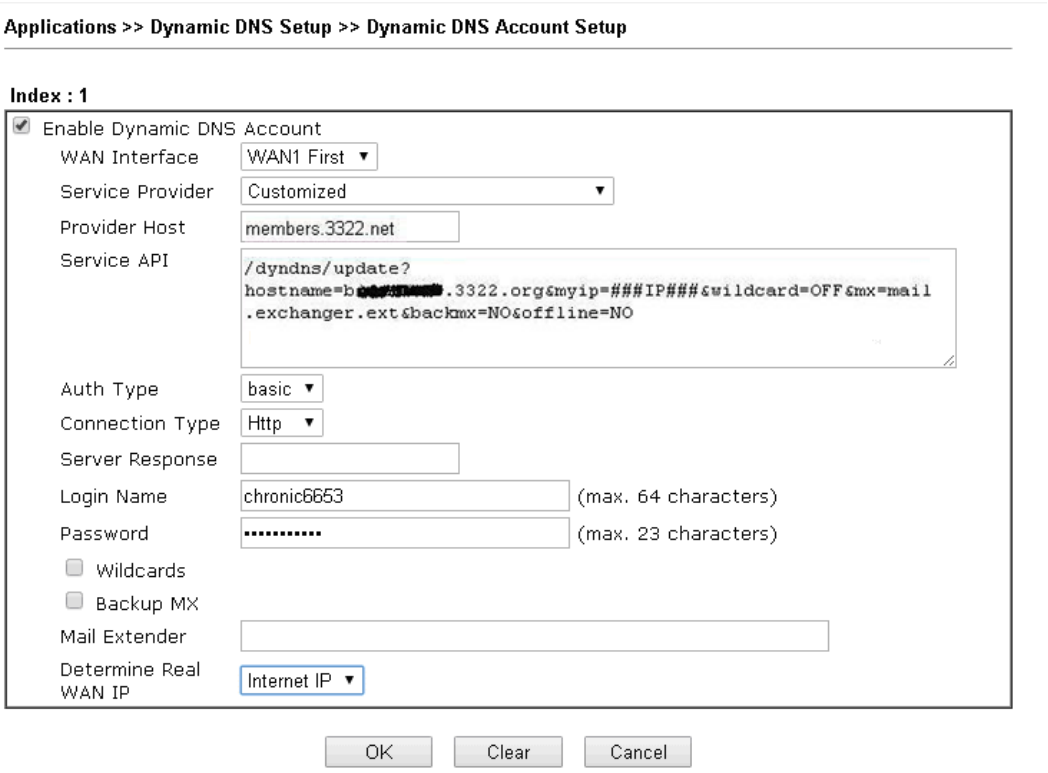
To update the IP to the DDNS server via editing the HTML script, we can Enter the following script on the browser:




"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.




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

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

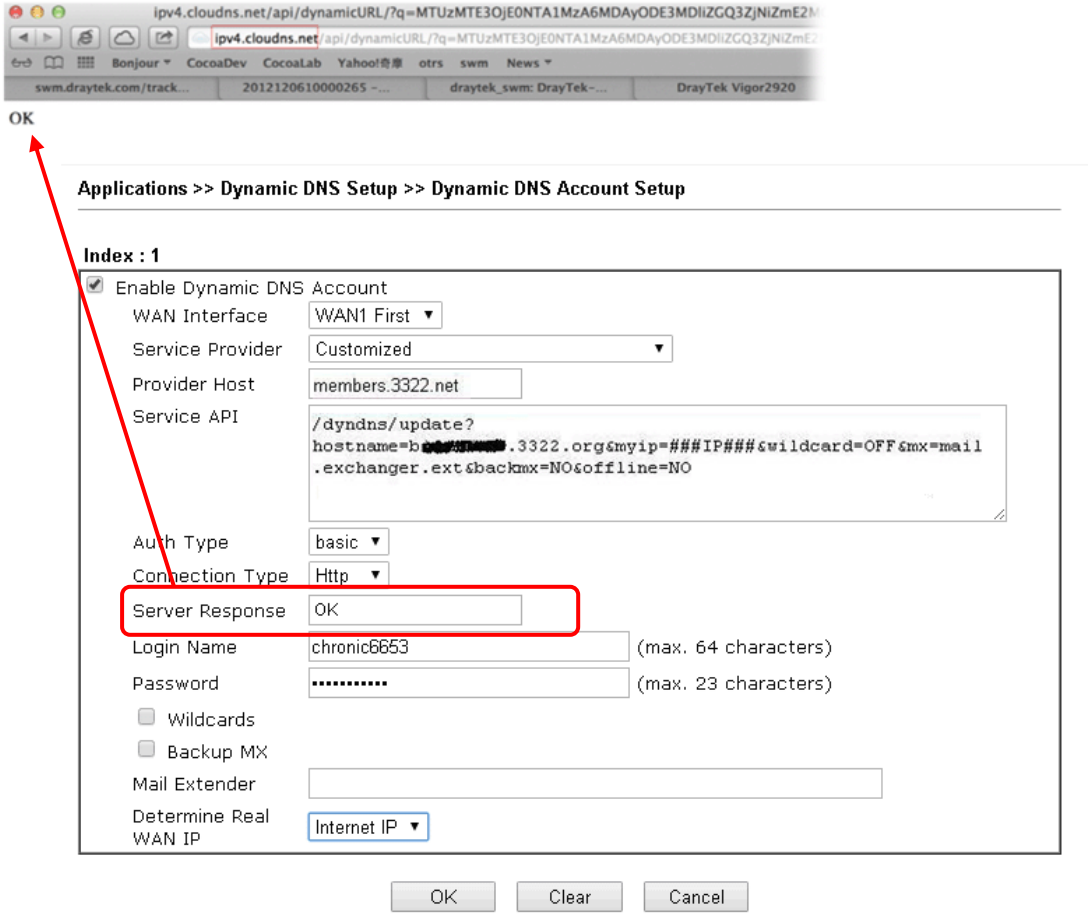
6. Set the Service API as:
/dyndns/update?hostname=yourhost.3322.org&myip=###IP###&wildcard=OFF&mx=mail
.exchanger.ext&backmx=NO&offline=NO

7. Enter your account and password.

8. 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 Note on www.draytek.com. |

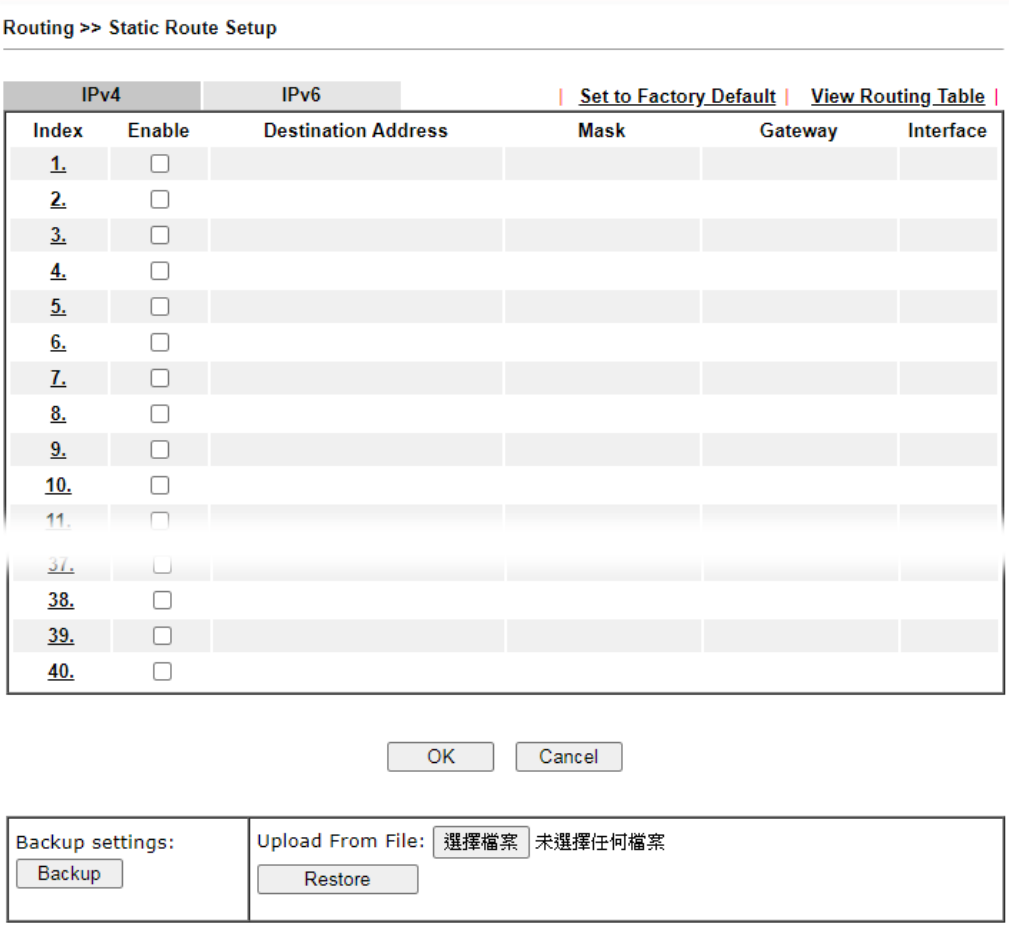
# Web User Interface




## II-5-1 Static Route

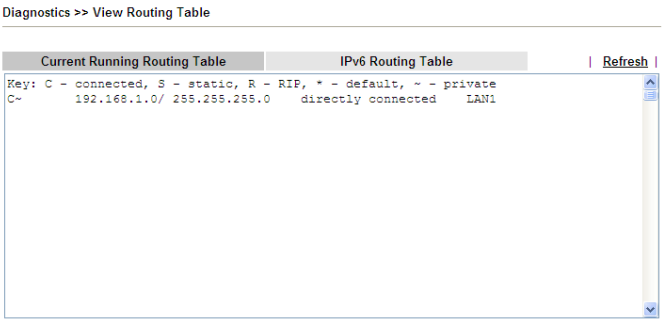
Go to **Routing** >> **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

### 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. |

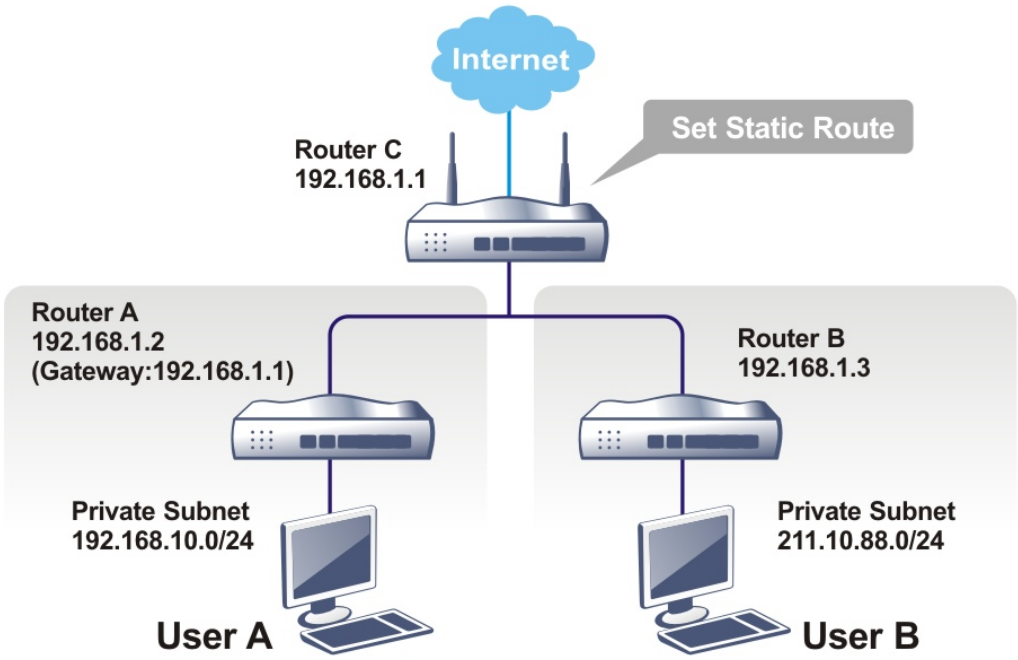
| | |
|---|---|
| **Set to Factory Default** | Clear all of the settings and return to factory default settings. |
| **Viewing Routing Table** | Displays the routing table for your reference.<br>  |
| **Backup** | Click it to backup the configuration of static route settings. |
| **Restore** | Click it to restore the configuration of static route settings. Before clicking, make sure upload the configuration file onto Vigor router. |

## Add Static Routes to Private and Public Networks

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

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

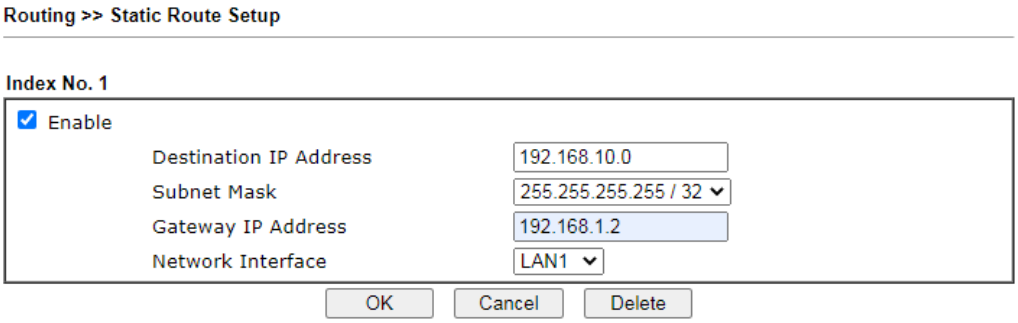
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.




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

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

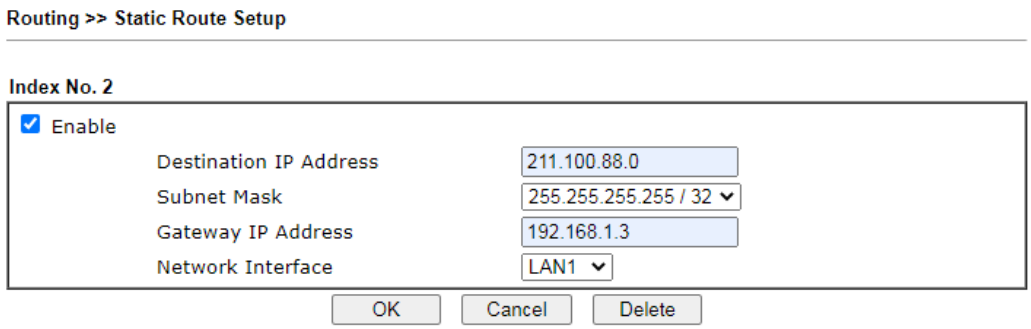
2. Click the **LAN >> Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



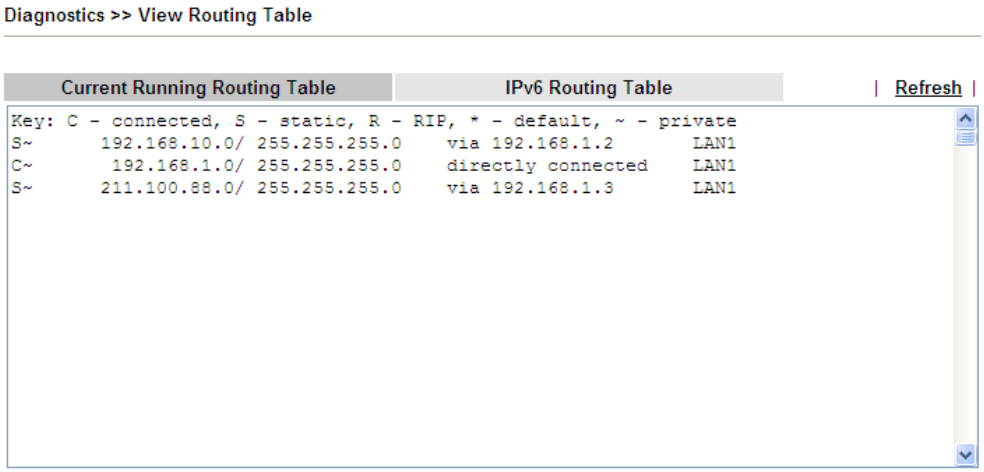

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click it to enable this profile. |
| **Destination IP Address** | Enter 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**.

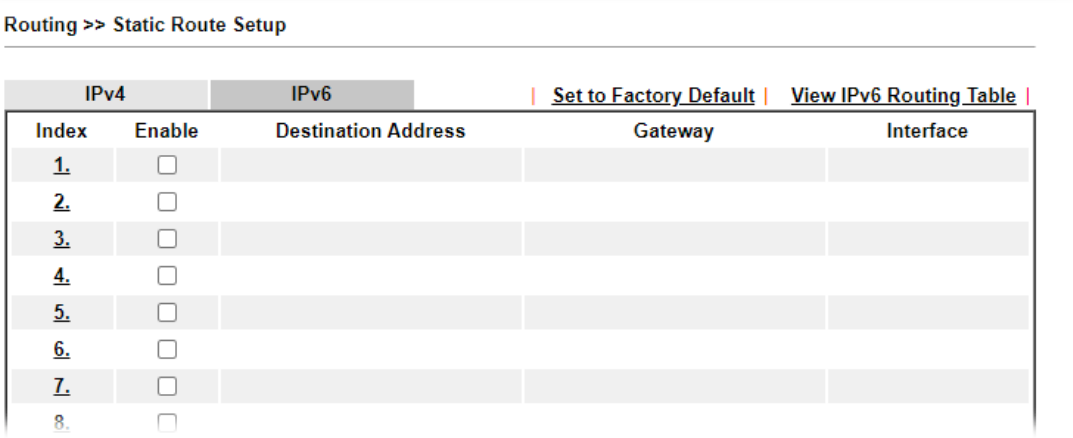


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.




## Static Route for IPv6

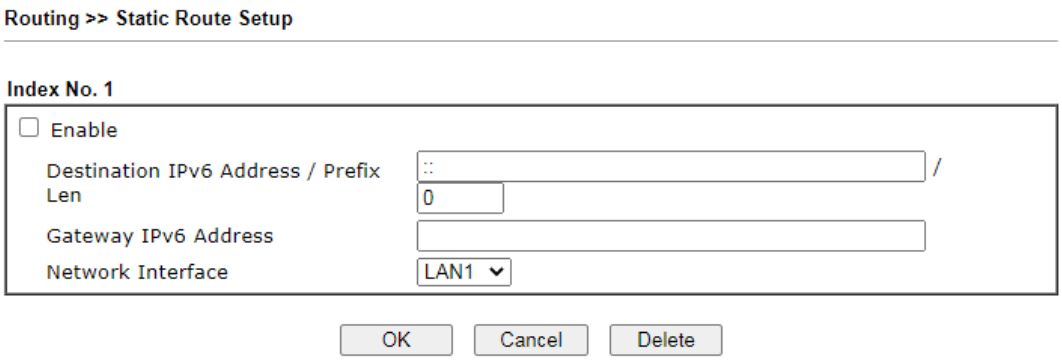
You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:




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. |
| **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 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:

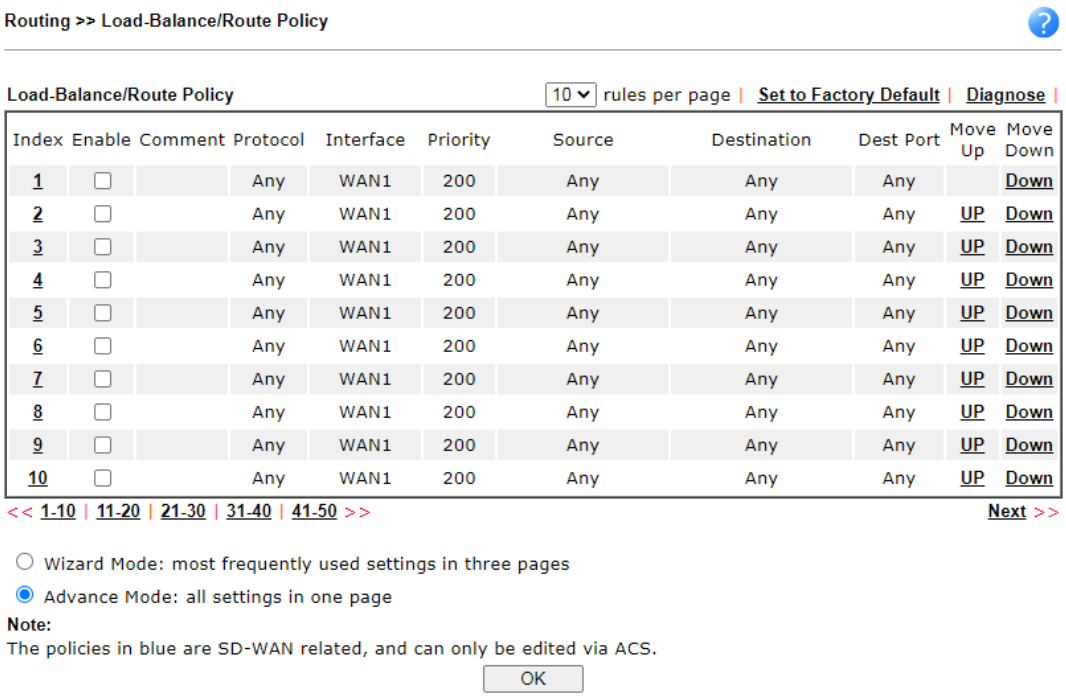
| Item | Description |
|---|---|
| **Enable** | Click it to enable this profile. |
| **Destination IPv6 Address / Prefix Len** | Enter the IP address with the prefix length for this entry. |
| **Gateway IPv6 Address** | Enter the gateway address for this entry. |
| **Network Interface** | Use the drop 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

It 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 >> Internet Access**, and always has lower priority than the **Firewall** Rules. Administrator may also define a priority to this policy.

This page lists all the policies and shows whether the policy is enabled/disabled, 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.



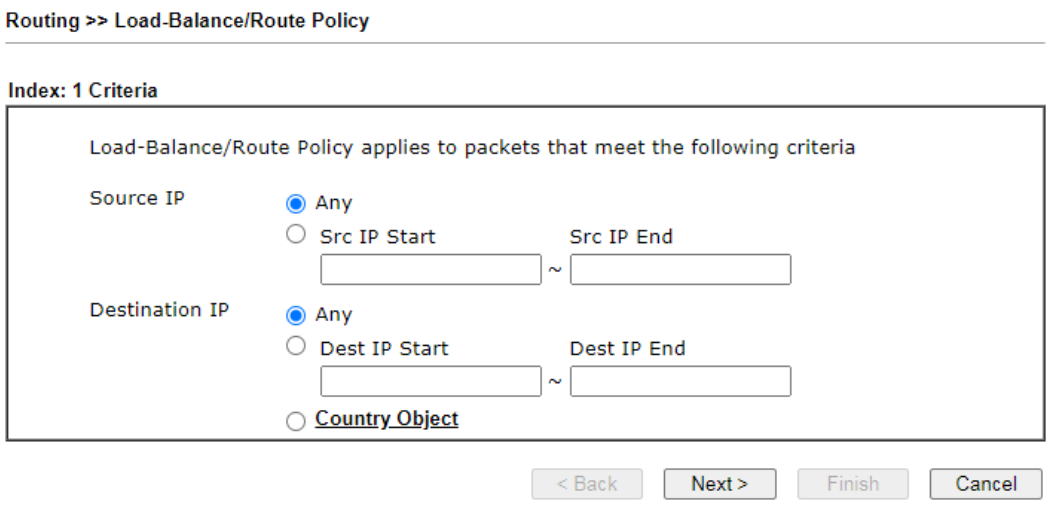

Available settings are explained as follows:

| 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 (simple and basic) 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:

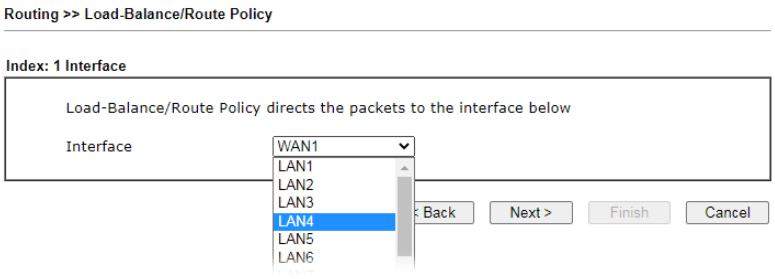
1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Source IP** | **Any** – Any IP can be treated as the source IP.<br>**Src IP Start -** Enter the source IP start for the specified WAN interface.<br>**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.<br>**Dest IP Start-** Enter the destination IP start for the specified WAN interface.<br>**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.<br>**Country Object** – Specify a country object. All the IPs coming from the country (countries) specified in the object will be passed through the WAN interface. |

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



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Interface** | 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. Specify an interface and click **Next.** The following page will appear only if you choose WAN1 ~WAN9 as Interface.




Available settings are explained as follows:

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

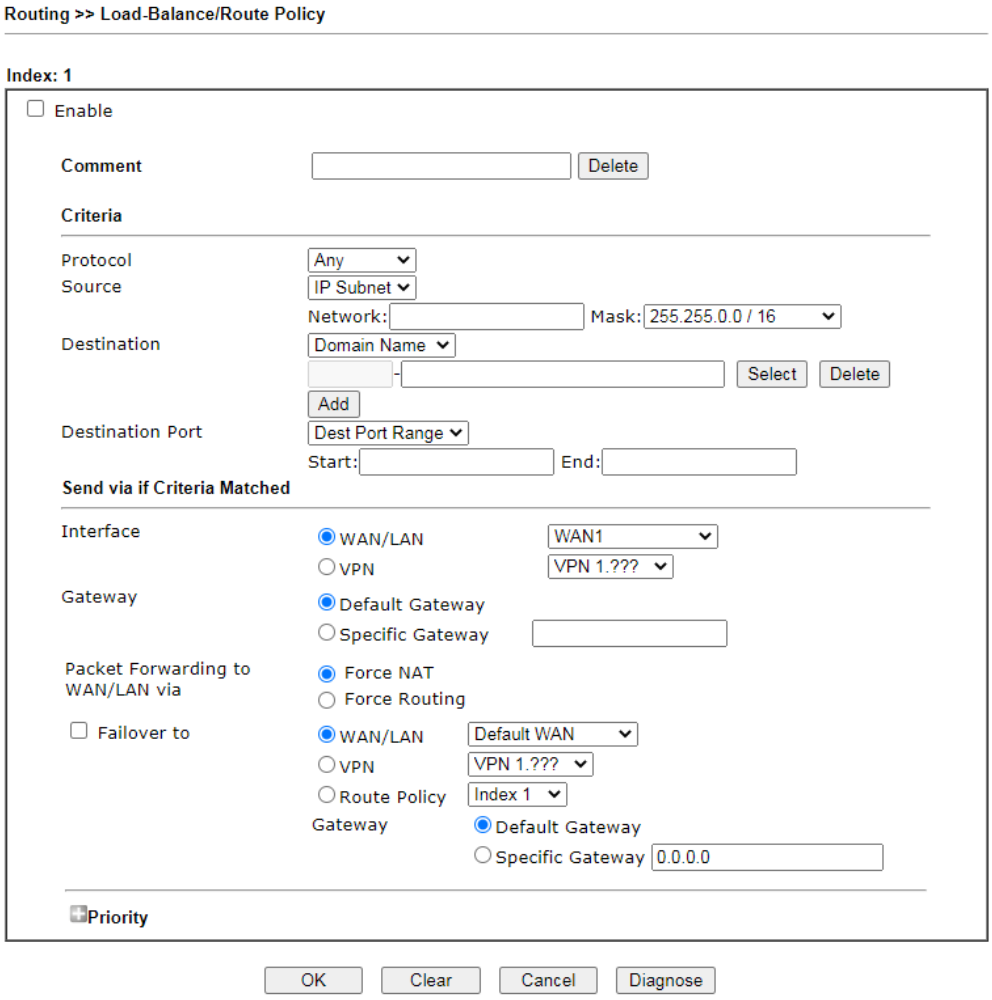
5. After choosing the mechanism, click **Next** to get the summary page for reference.




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

To 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 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.<br>**IP Range** – Define a range of IP address as source IP addresses.<br>● **Start -** Type an address as the starting IP for such profile.<br>● **End -** Type an address as the ending IP for such profile.<br>**IP Subnet** – Define a subnet containing IP address and mask address.<br>● **Network** – Type an IP address here.<br>● **Mask** – Use the drop down list to choose a suitable mask |

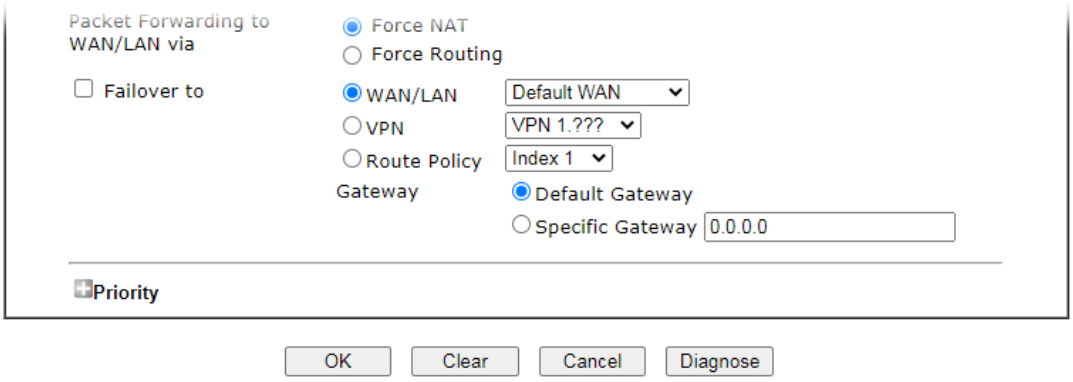
| | |
|---|---|
| | for the network.<br>**IP Object / IP Group**– Use the drop down list to choose a preconfigured IP object/group. |
| **Destination** | **Any** – Any IP can be treated as the destination IP.<br>**IP Range** – Define a range of IP address as destination IP addresses.<br>● **Start -** Type an address as the starting IP for such profile.<br>● **End -** Type an address as the ending IP for such profile.<br>**IP Subnet** – Define a subnet containing IP address and mask address.<br>● **Network** – Type an IP address here.<br>● **Mask** – Use the drop down list to choose a suitable mask for the network.<br>**Domain Name** – Specify a domain name as the destination.<br>● **Select** – Click it to choose an existing domain name defined in Objects Setting>>String Object.<br>● **Delete** – Remove current used domain name.<br>● **Add** – Create a new domain name as the destination.<br>**IP Object / IP Group**– Use the drop down list to choose a preconfigured IP object/group.<br>**Country Object** – Use the drop dwon list to choose a preconfigured object. Then all IPs within that country will be treated as the destination IP. |
| **Destination Port** | **Any** – Any port number can be treated as the destination port.<br>**Dest Port Range –**<br>● **Start -** Enter the destination port start for the destination IP.<br>● **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.<br>**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.<br>**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**.<br>**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.<br>● **WAN/LAN –** Use the drop down list to choose an interface as an auto failover interface.<br>● **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.<br>● **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.<br>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. |

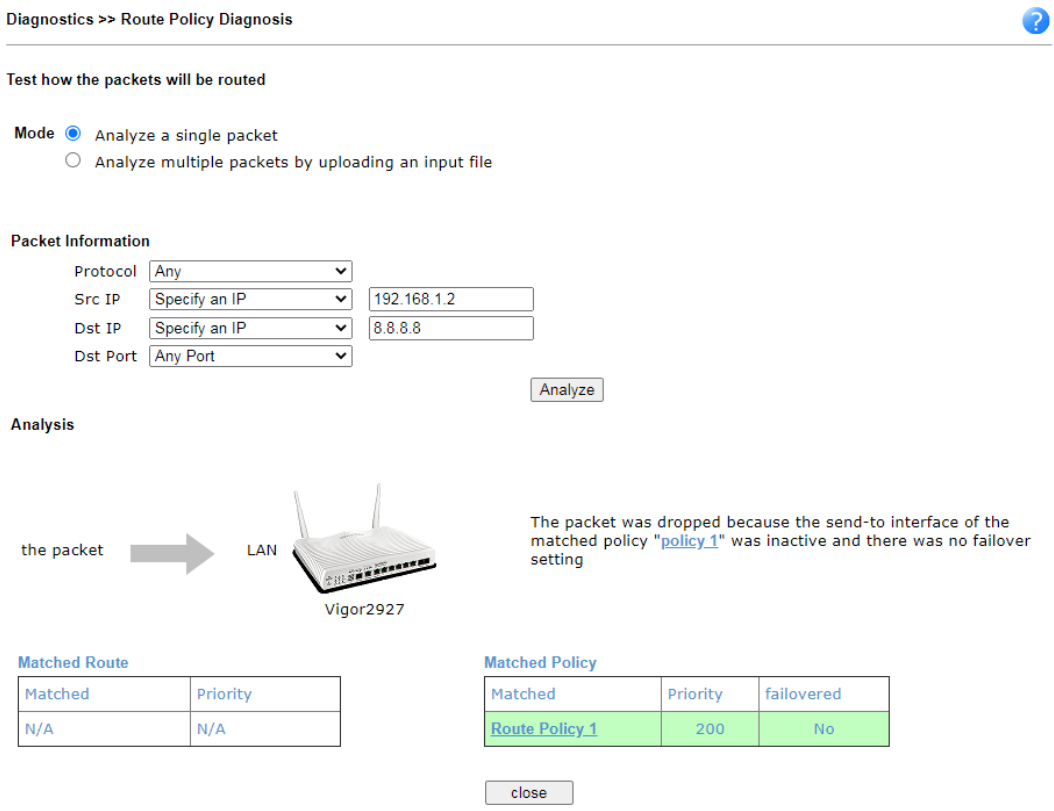
3. When you finish the configuration, please click **OK** to save and exit this page.

## Diagnose for Route Policy

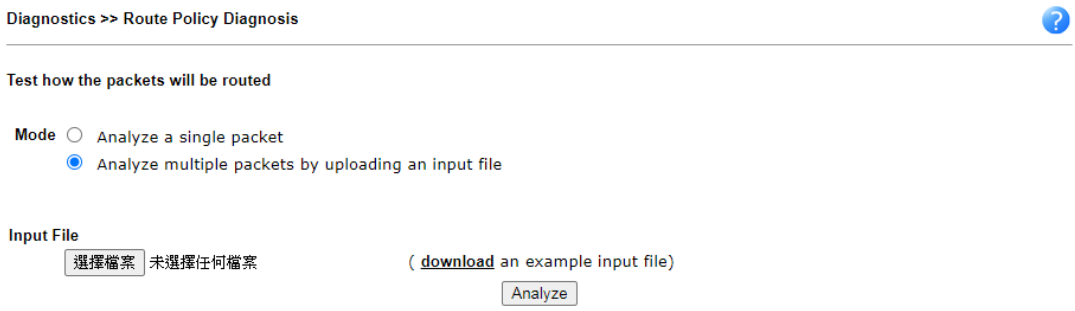
The button of **Diagnose** located below the Load-Balance /Route Policy profile is used to trace possible path of the packets sent out of the router.



Click **Diagnose** to get the following page.

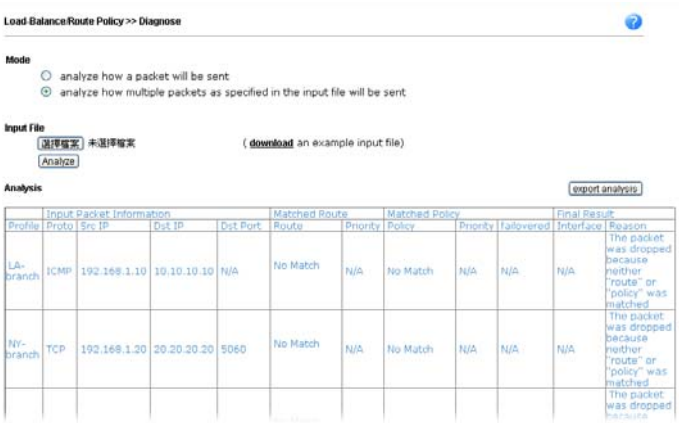



or




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.<br>**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.<br>**Protocol -** Specify a protocol for diagnosis.<br>**Src IP** – Type an IP address as the source IP.<br>**Dst IP** – Type an IP address as the destination IP.<br>**Dst Port** – Use the drop down list to specify the destination port.<br>**Analyze** – Click it to perform the job of analyzing. The |

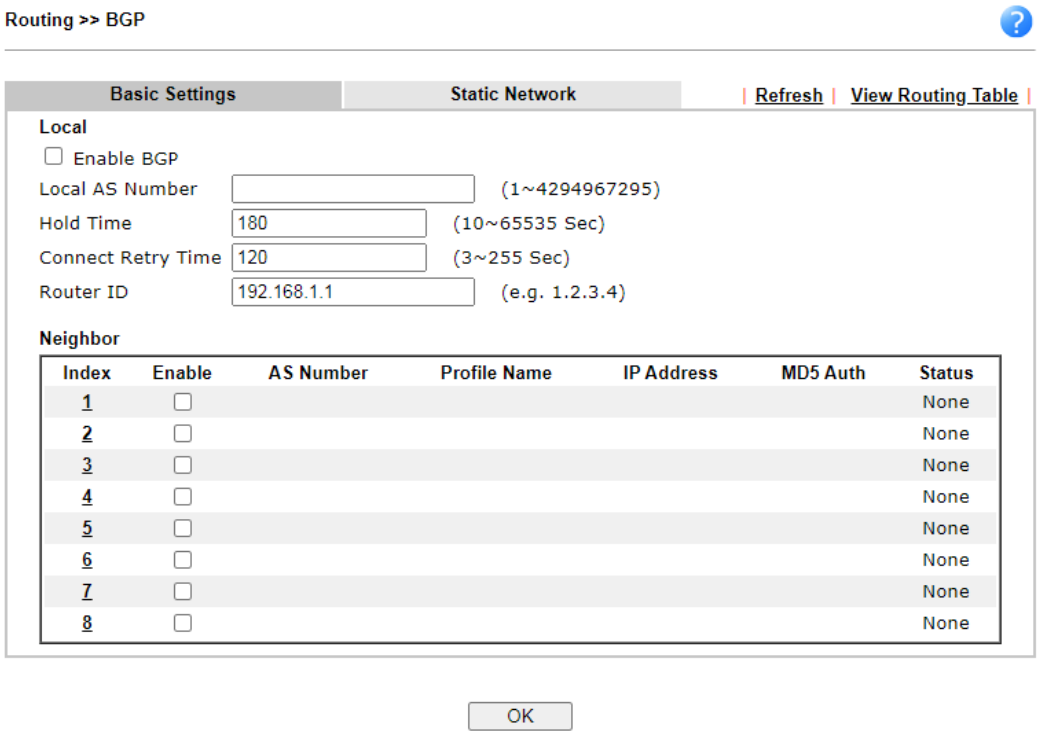
| | |
|---|---|
| | analyzed result will be shown on the page. If required, click **export analysis** to export the result as a file. |
| **Input File** | **Select** – Click the download link to get a blank example file. Then, click such button to select that blank ".csv" file for saving the result of analysis.<br>  <br>**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.<br>  <br>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. |

## II-6-3 BGP

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

### II-6-3-1 Basic Settings

Set general settings for for local router and neighboring routers.



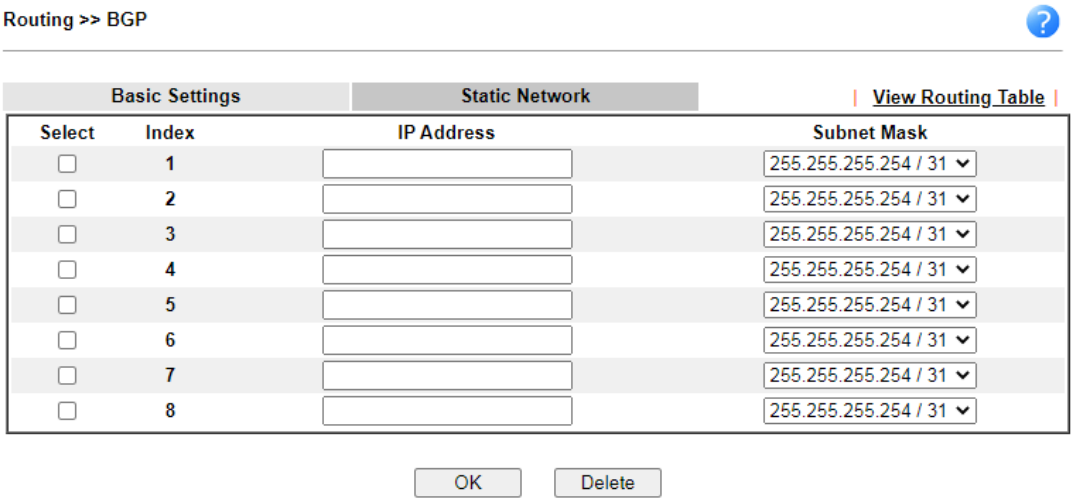

Available settings are explained as follows:

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

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

## II-6-3-2 Static Network

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




Available settings are explained as follows:

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

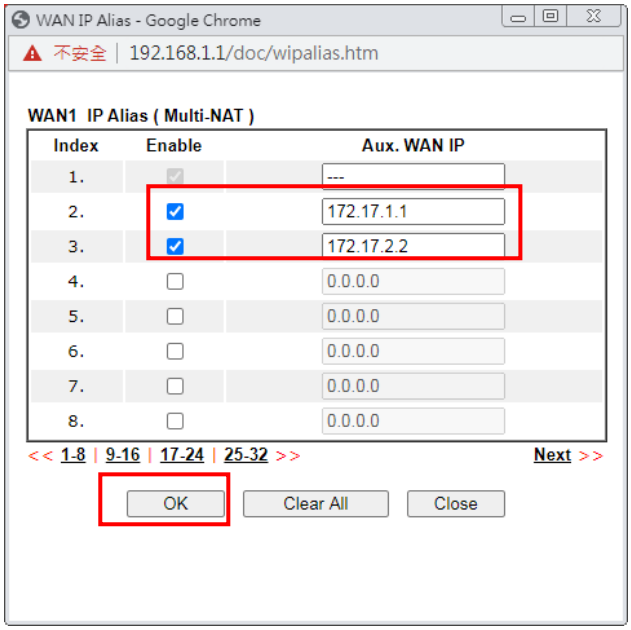
# Application Notes

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

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

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

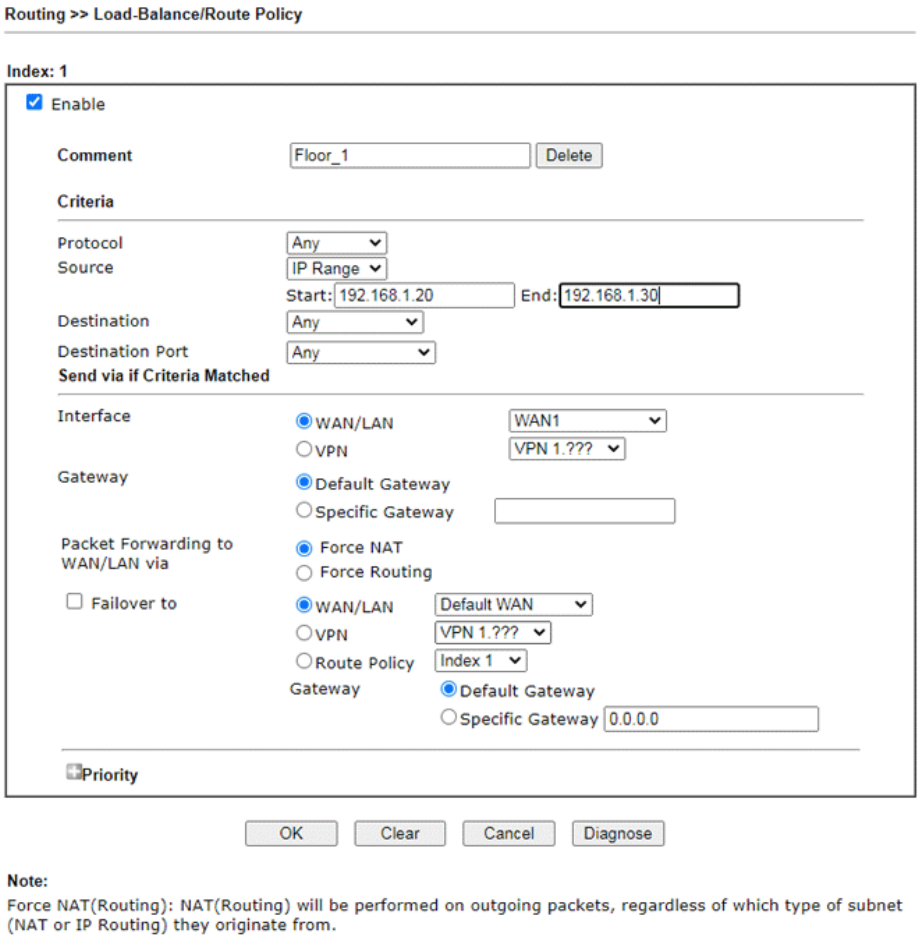
1. Set up WAN IP Alias. Go to **WAN >> Internet Access >> Details** Page, and click on **WAN IP Alias** button.




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

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

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



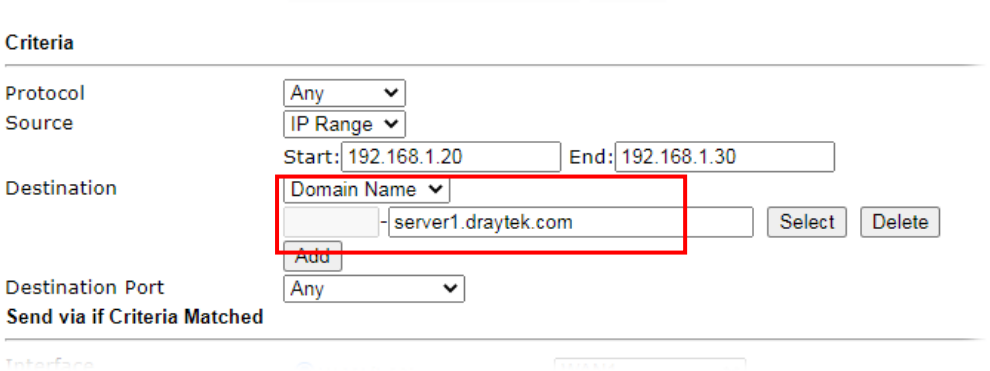

- Enable this policy.
- Enter **Source IP** as the range of private IP address.
- Leave the Destination IP and Port as **Any**.
- Select **Interface** as WAN, and then select Interface address from the drop-down list. (The List can be edited in **WAN IP Alias** setting.)
- Enable **Failover to** other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

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

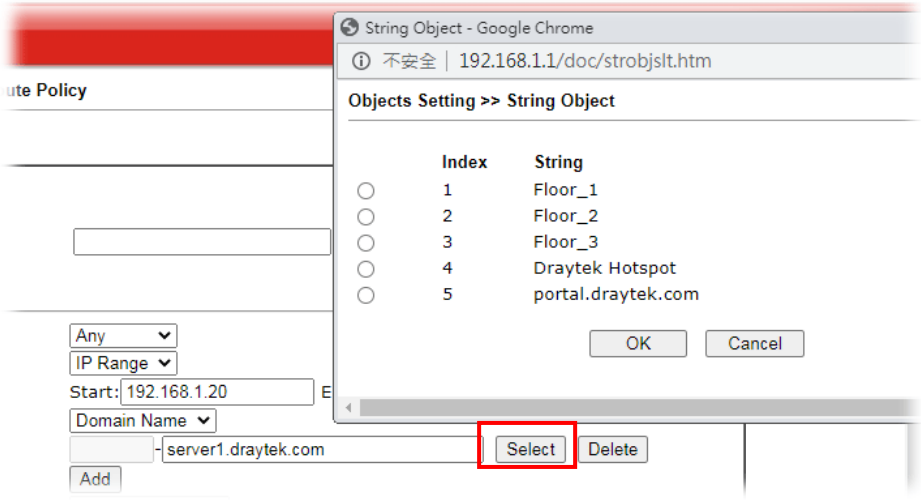
## A-2 How to use destination domain name in a route policy?

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

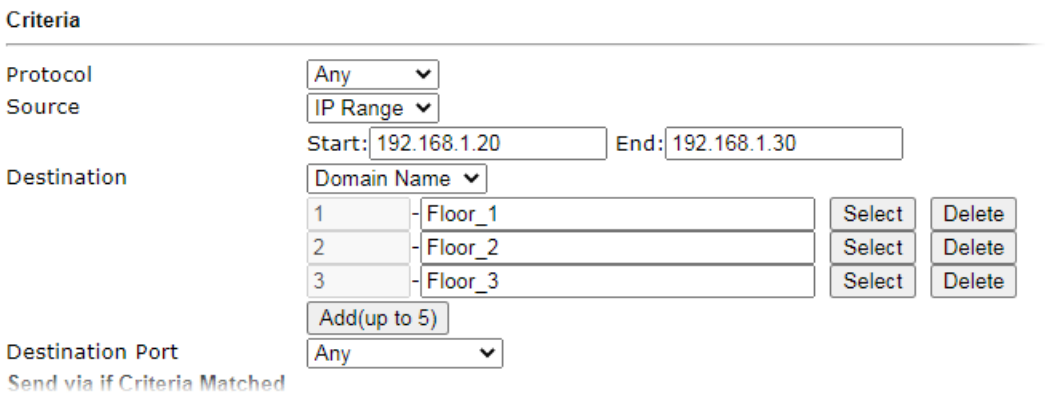
To use a destination domain name as criteria, just select **Domain Name** as **Destination** in Criteria, and enter the domain name in the empty field.




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

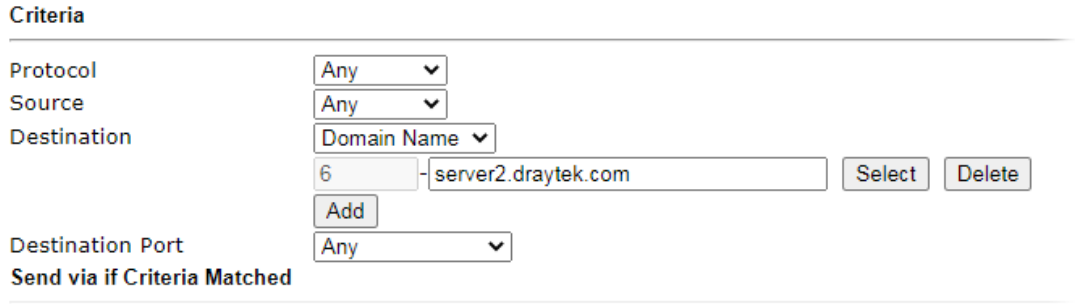



Click **Add** too add more domain names, we can set up to 5 domain names in one route policy.

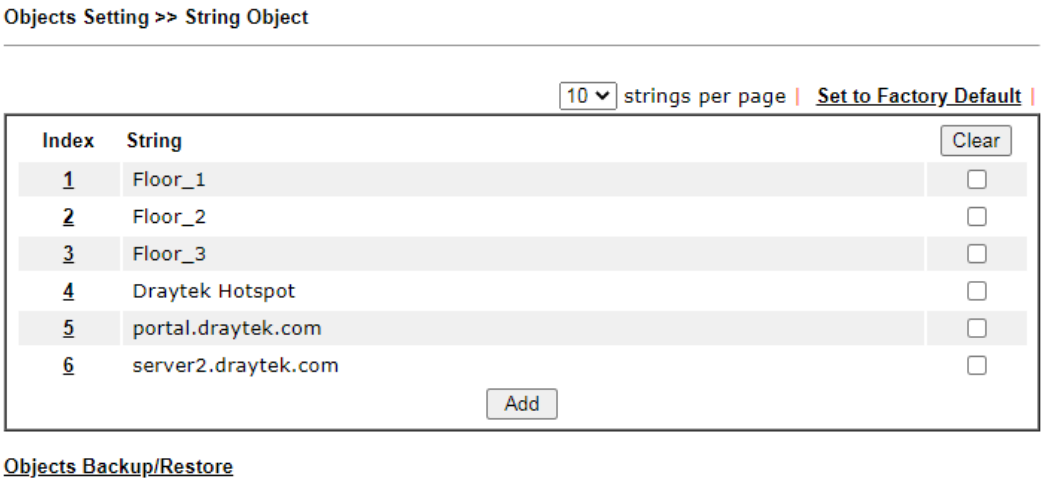


## Auto-create String Objects

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




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

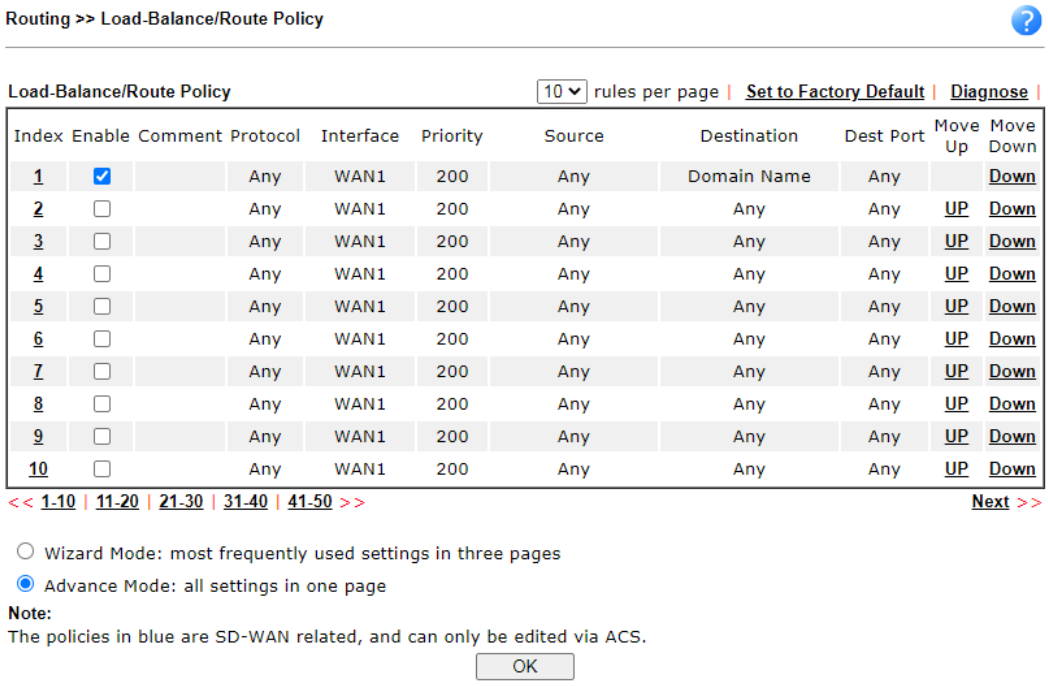


## A-3 Introduction to Load Balance/Route Policy

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

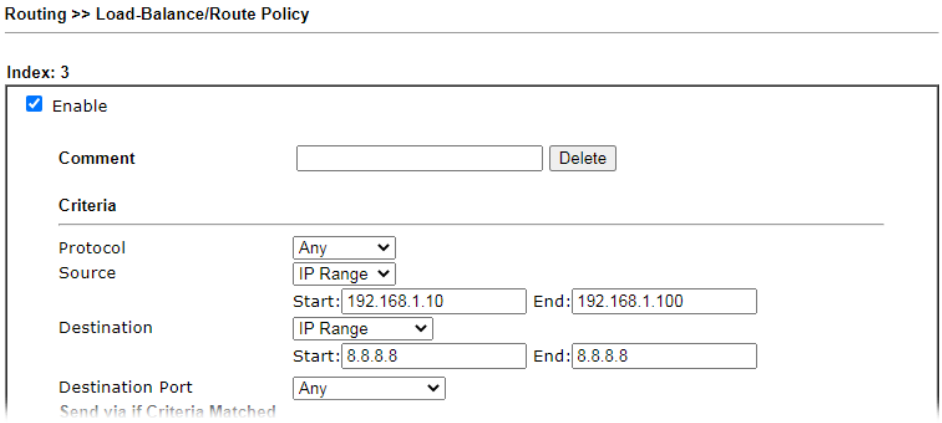
The Policy set in Load-Balance/Route Policy always has higher priority than Default Route and Auto Load Balance set in **WAN >> General Setup**, and always has lower priority than the Firewall Rules. Administrator may also define a priority to this policy.

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.

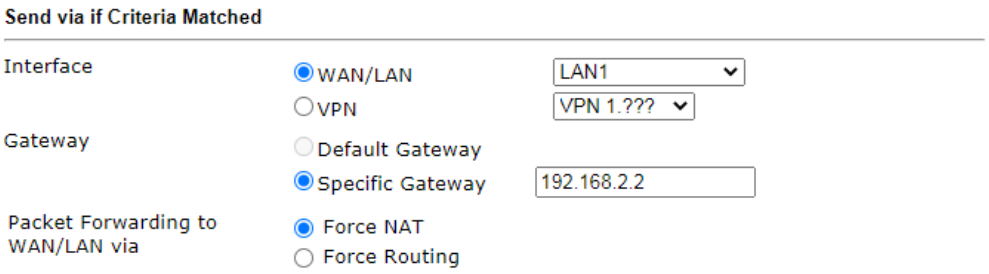
   b. Enter the Source IP address range, the Source IP could be a single address if the Start and End are the same.

   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.

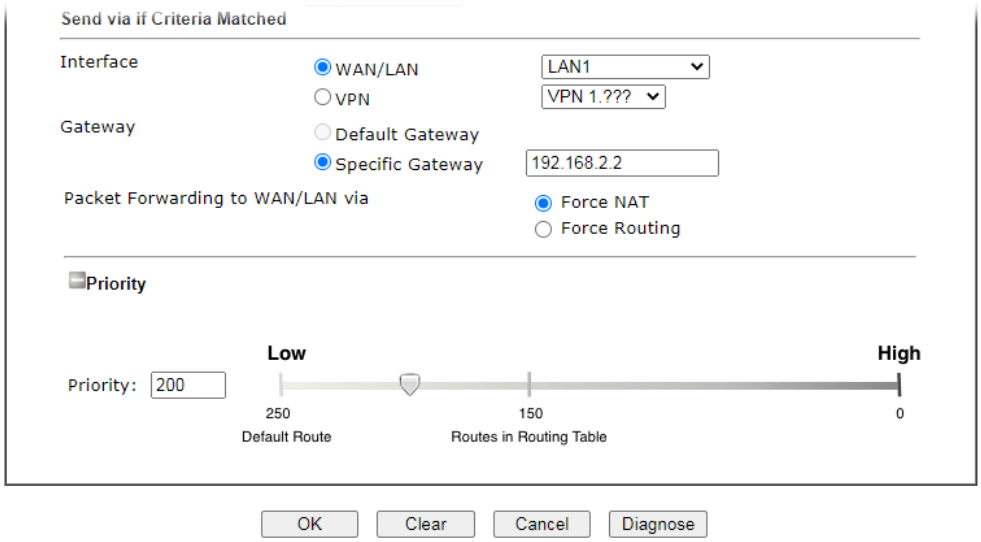



a. Select an Interface.

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:



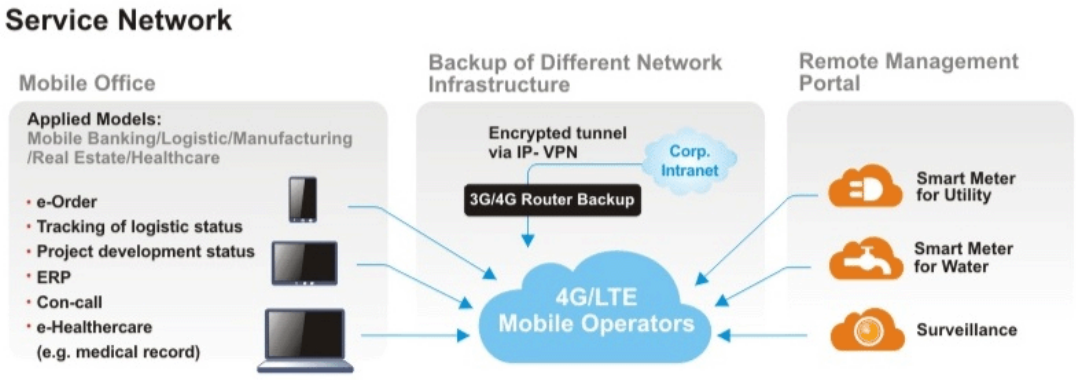

- **Priority**: Administrator may set priority between 1 and 249 for this Route policy, where smaller number indicates higher priority. When two policies are having the same priority, the first (according to the policy index order) matched policy will be implemented.

# II-7 LTE

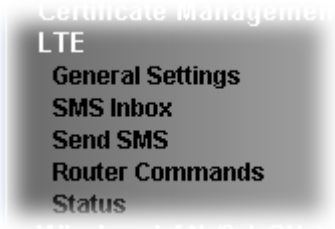
LTE WAN with SIM card can provide convinent Internet access for Vigor router. However, we can't stop thinking about what can Vigor router utilize this SIM card to provide more useful functions for user? Now, we have developed some useful functions for user, such as sending SMS from a router to report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

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

| | |
|---|---|
| **Info** | This function is used for "L" models only. |



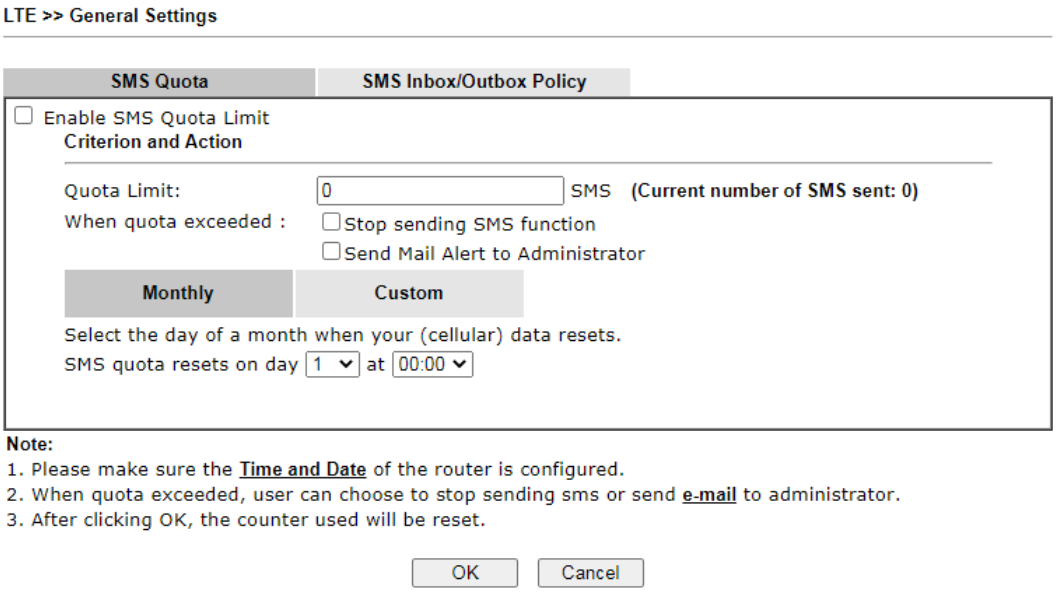
# Web User Interface




## II-7-1 General Settings

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

### II-7-1-1 SMS Quota



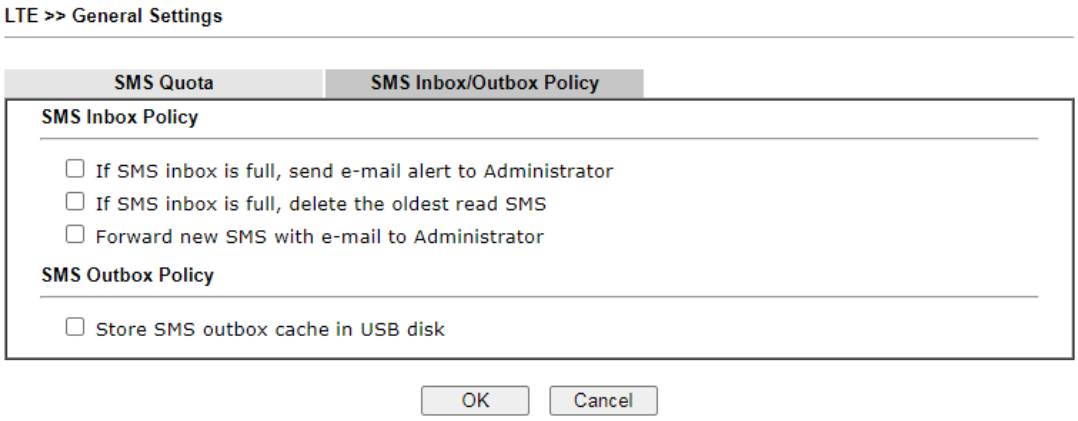

Available settings are explained as follows:

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

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

## II-7-1-2 SMS Inbox/Outbox

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



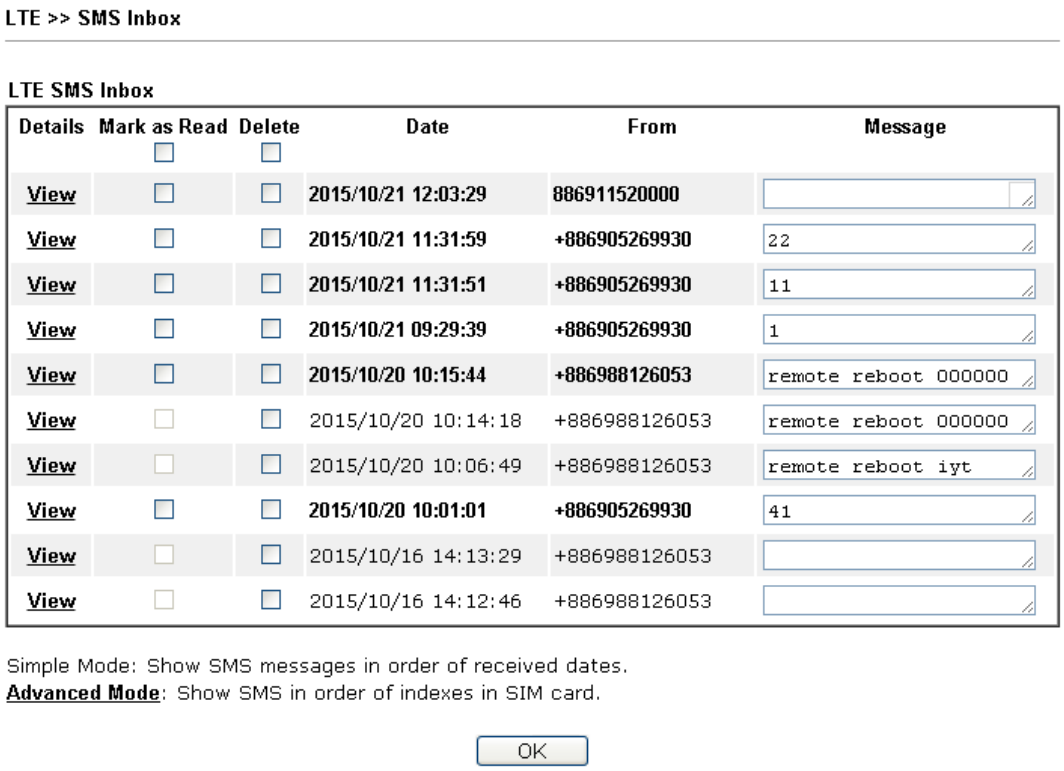
## II-7-2 SMS Inbox

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

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

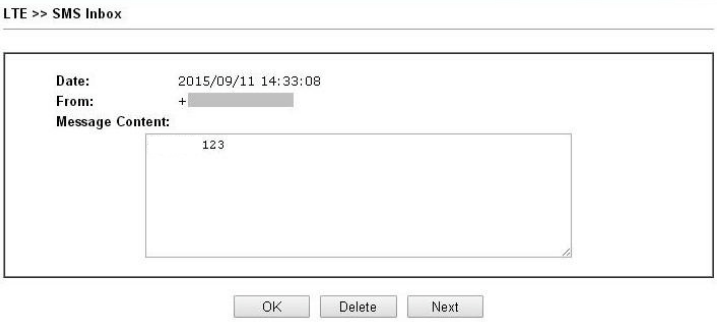
Click the Simple Mode link or the Advanced Mode link below to switch between these two modes.

### II-7-2-1 Simple Mode



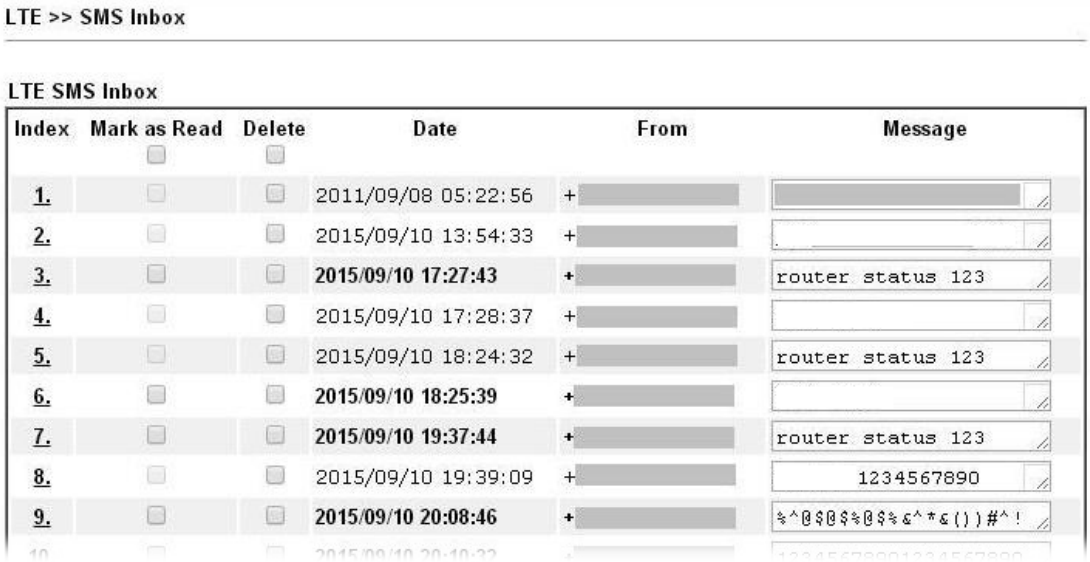

Available settings are explained as follows:

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



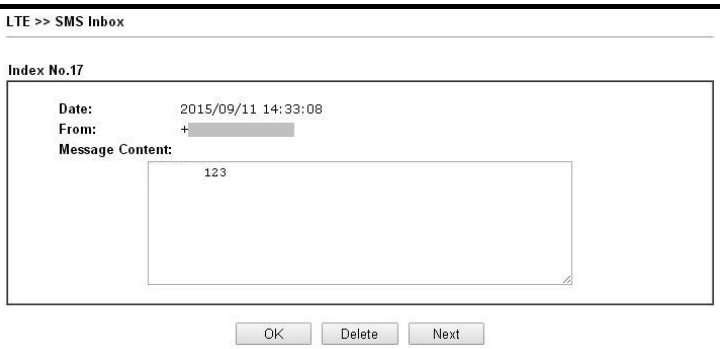

- **Message Content** - Display the full content of the message.
- **OK** - Return to previous page.
- **Delete** - Click it to delete this message and return to previous page.
- **Next** - Click it to see the content of next message.

## II-7-2-1 Advanced Mode




Available settings are explained as follows:

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




**Message Content** - Display the full content of the message.

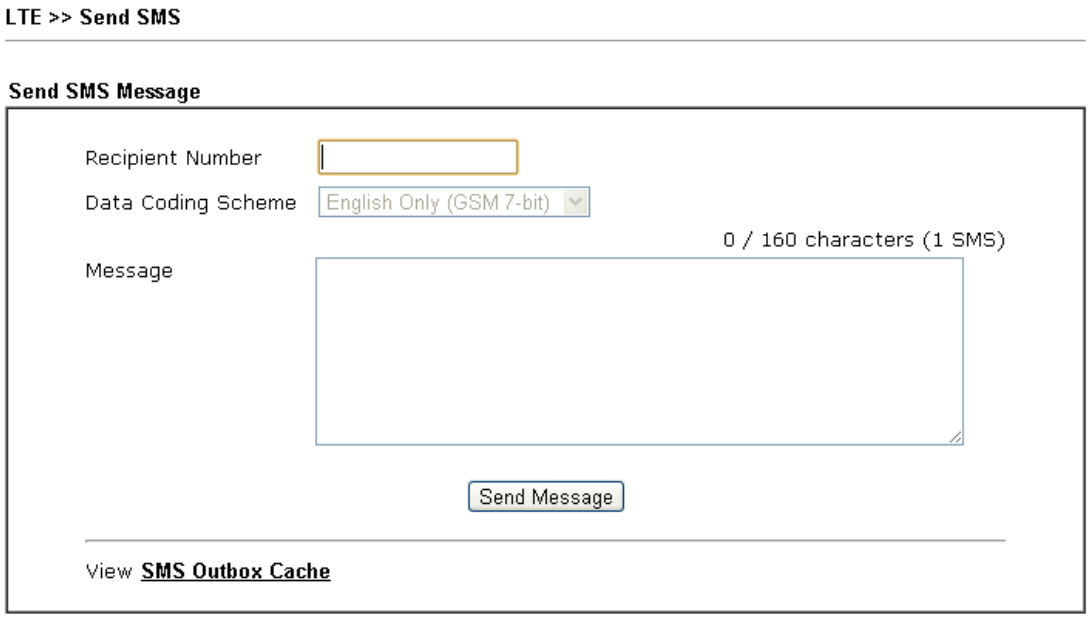
**OK** - Return to previous page.

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

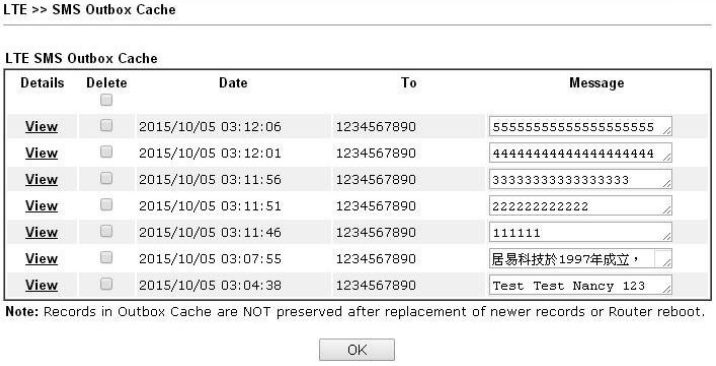
**Next -** Click it to see the content of next SMS index.

## II-7-3 Send SMS

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




Available settings are explained as follows:

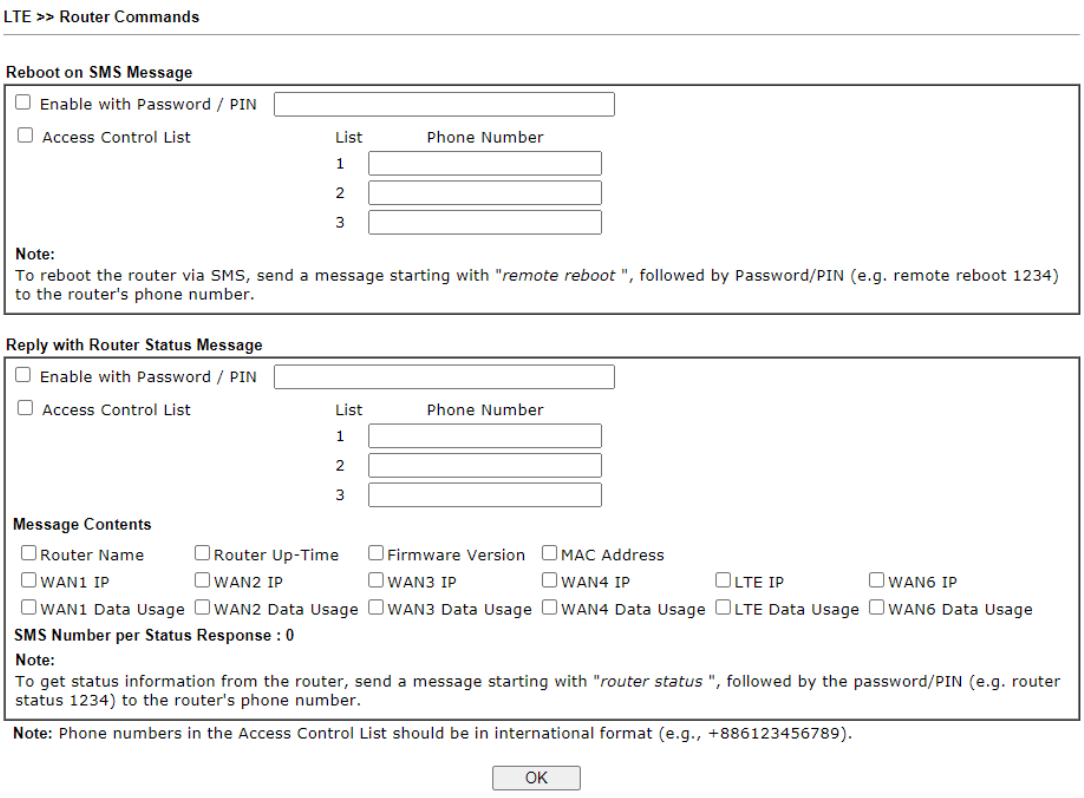
| Item | Description |
|---|---|
| **Recipient Number** | Enter the phone number of the recipient.<br>The format can be an international phone number ( +8869123455678) or a general phone number(0912345678). |
| **Data Coding Scheme** | The router will automatically select a suitable Data Coding Scheme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

## II-7-4 Router Commands

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




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




Available settings are explained as follows:

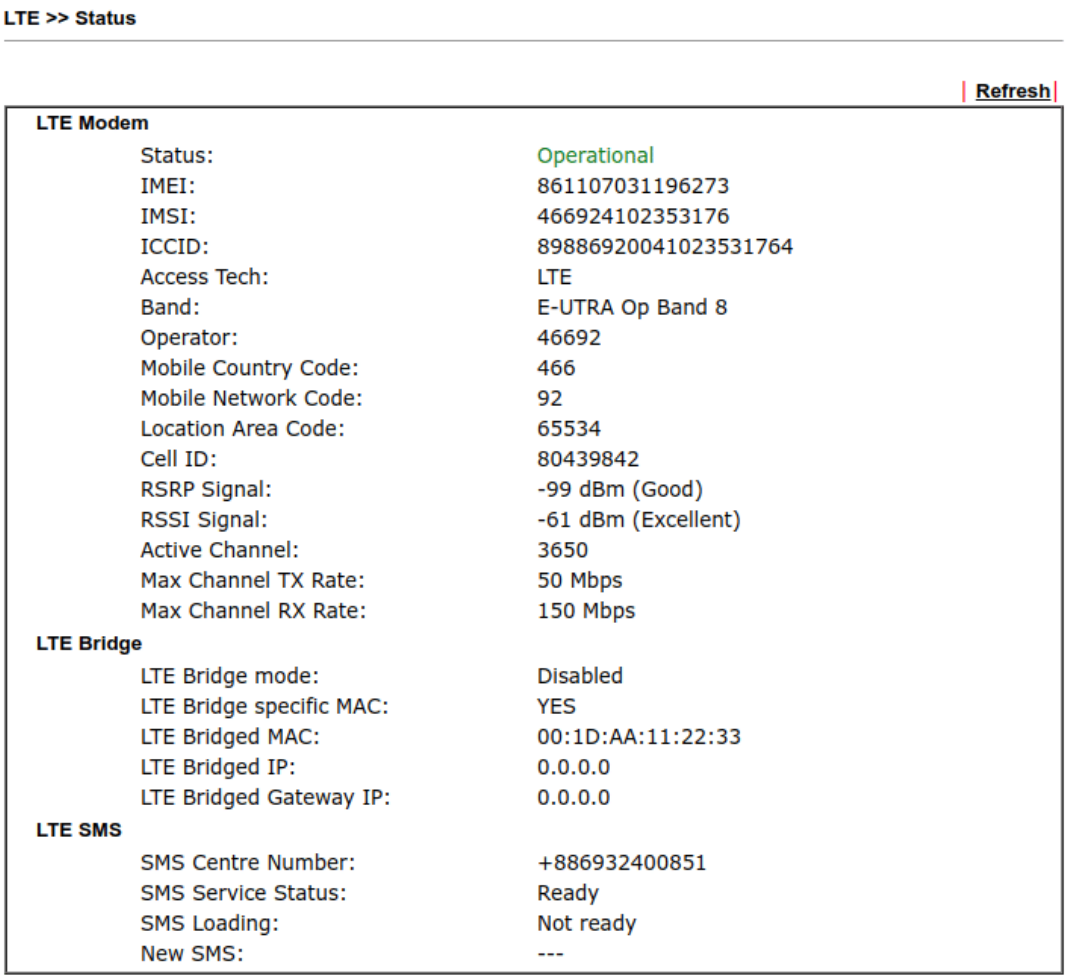
| Item | Description |
|---|---|
| **Reboot on SMS Message** | |
| **Enable with Password / PIN** | To reboot Vigor router remotely via SMS, please check such box and Enter the password/PIN number (treated as authentication for any mobile phone).<br>The password shall be composed by letters, numbers and baseline. |
| **Access Control List** | Check the box to type or modify (up to 3) phone numbers.<br>The phone number specified here is capable of sending SMS |

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

## II-7-5 Status

Vigor router with LTE function is capable of accessing into Internet and able to send SMS to specified mobile phone. In addition, it can be treated as a LTE modem.

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




Each item is explained as follows:

| Item | Description |
|---|---|
| **LTE Modem** | |
| **Status** | LTE WAN status. |
| **IMEI** | International Mobile Equipment Identity of the embedded LTE module. |
| **IMSI** | International Mobile Subscripber Identity of the LTE SIM card. |
| **Access Tech** | Type of LTE connection (CDMA/GSM/WCDMA/LTE/TD-SCDMA). |
| **Band** | Band of LTE connection. |
| **Operator** | ISP name of LTE connection. |

| | |
|---|---|
| **Mobile Country Code / Mobile Network Code / Location Area Code / Cell ID :** | Base station information. |
| **Signal** | Signal strength of LTE connection. |
| **Active Channel** | Frequency of LTE connection. |
| **Interference with 2.4GHz WLAN** | Whether the current LTE frequency causes interference with 2.4G wireless. If Yes, the interfered 2.4G wireless channels will be indicated. |
| **Max Channel TX Rate / Max Channel RX Rate** | Maximum TX/RX link rate of LTE connection. |
| **LTE SMS** | |
| **SMS Centre Number** | The phone number for SMS service of the LTE SIM card. |
| **SMS Service status** | Whether the SMS service of the LTE SIM card is ready. |
| **SMS Loading** | Whether the received SMS messages in the LTE SIM card have been loaded to the Router. |
| **New SMS** | The number of unread SMS in SMS Inbox. |

# Part III Wireless LAN




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

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

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

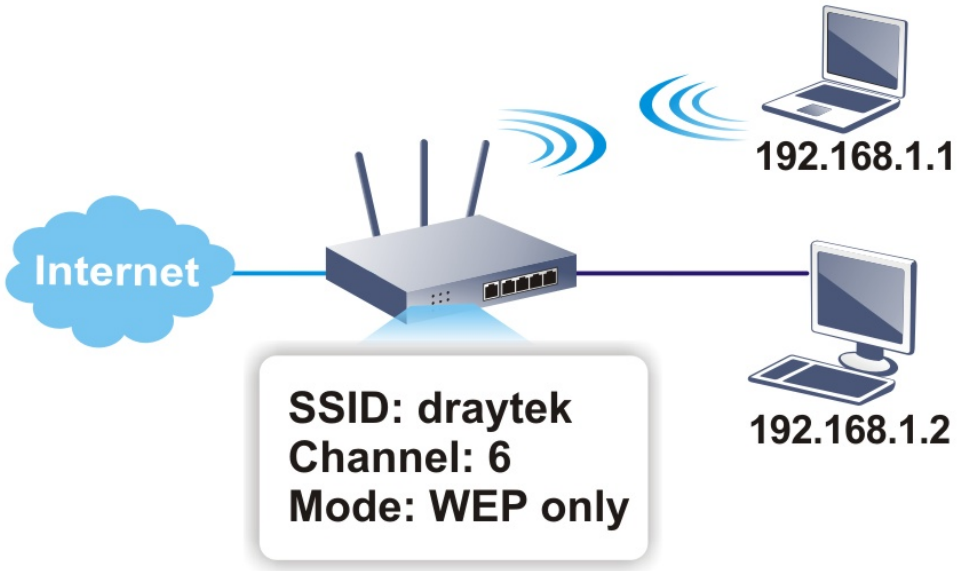
In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches virtually every location on earth. Billions of people exchange information daily with wireless communication products. The Vigor2860 series of wireless routers (with "n", "n-plus", or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

All Vigor2927 wireless routers support 2.4 GHz. ac models add support for 5 GHz frequencies. Channel operations of 20 and 40 MHz are possible on the 2.4 GHz spectrum, and 20, 40 and 80 MHz are supported on the 5 GHz spectrum. "ac" models (2865ac) support data rates of up to 1.3 Gbps on 802.11ac 80 MHz channels, whereas "n" models support data rates of up to 300 Mbps on 802.11n 40 MHz channels.

**Info**

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

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The wireless network settings, such as SSID, channels, encryption protocol, can be configured in General Settings.




## Multiple SSIDs

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

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

### Real-time Hardware Encryption

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

### Complete Security Standard Selection

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

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

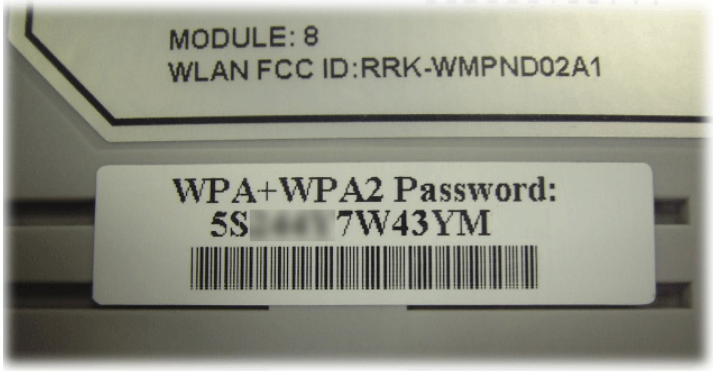
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

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

**Info**

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




### Separate the Wireless and the Wired LAN- WLAN Isolation

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

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

### Manage Wireless Stations - Station List

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

### DFS Restrictions

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

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

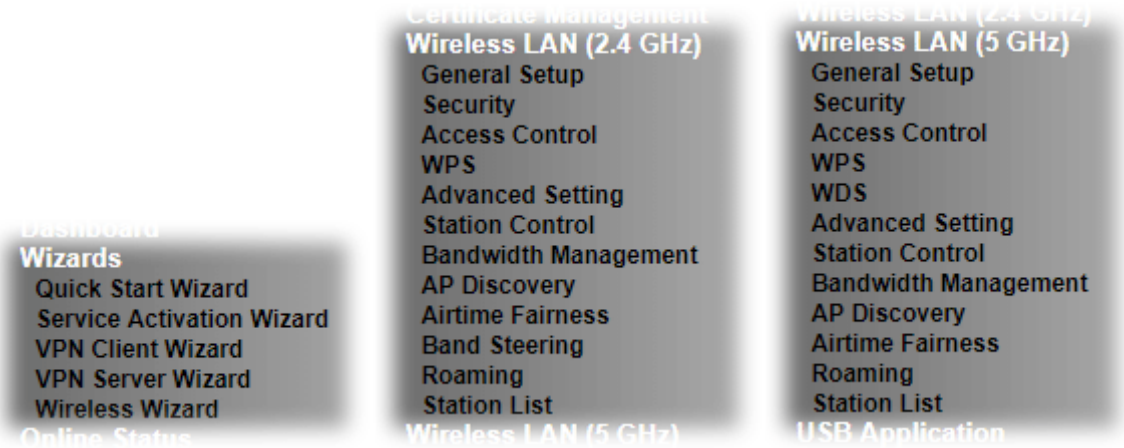
In the rest of world, there are restrictions on DFS channels as well. Uncertified DFS channels will be unavailable for selection depending on the country code programmed in the router.

### WPS

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



# Web User Interface



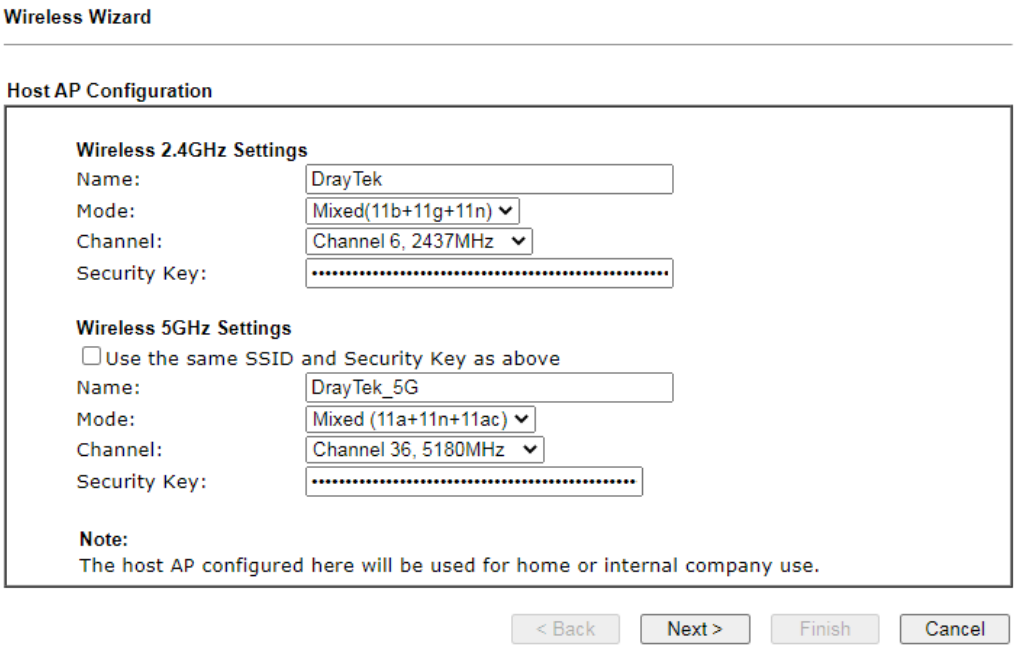

## III-1-1 Wireless Wizard

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

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

Follow the steps listed below:

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



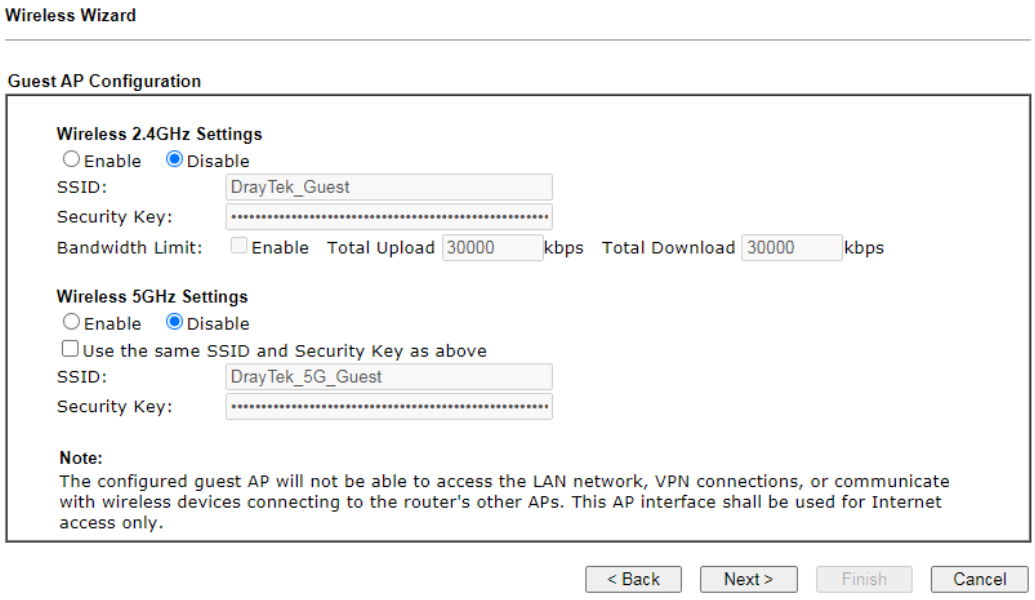

Available settings are explained as follows:

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

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

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

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




   Available settings are explained as follows:

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

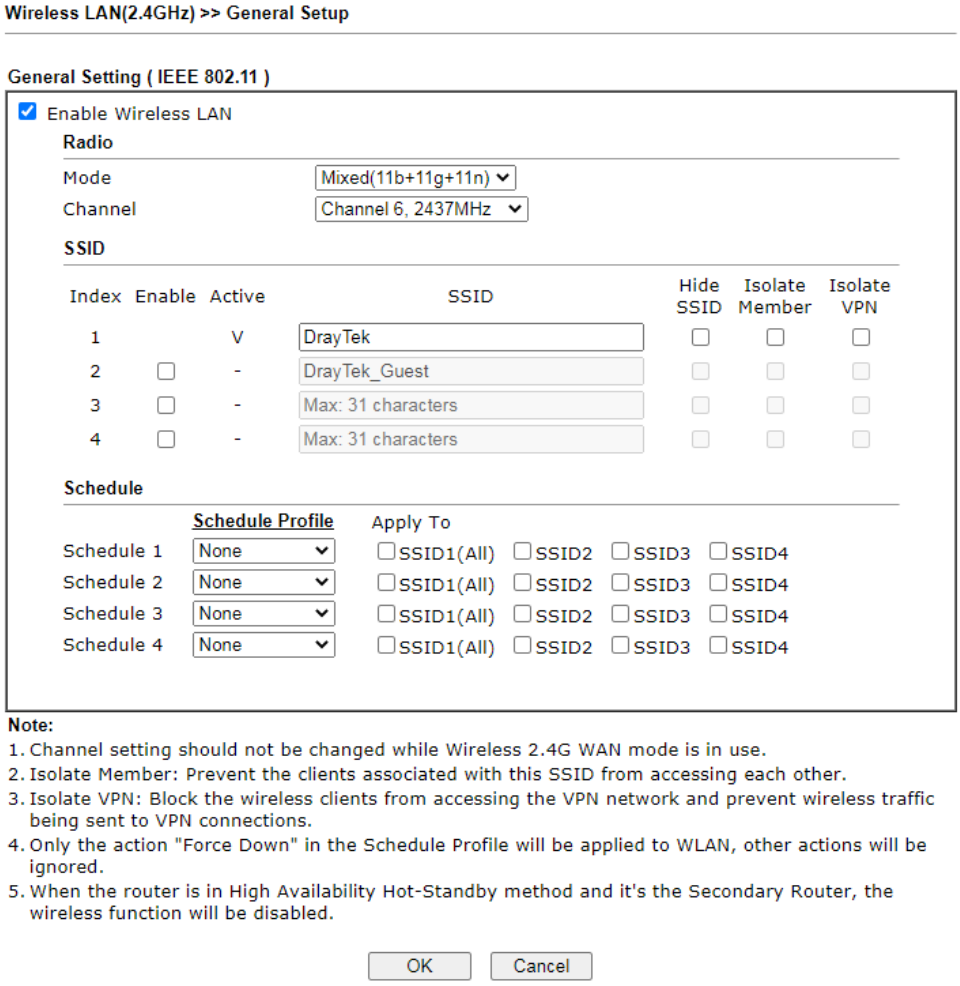
4. Click **Next** to proceed to the Configuration Summary page.




5. The **Configuration Summary** page displays all the settings you have entered. Click **Finish** to save the settings, **Back** to make changes, or **Cancel** to exit the wizard without saving the settings.

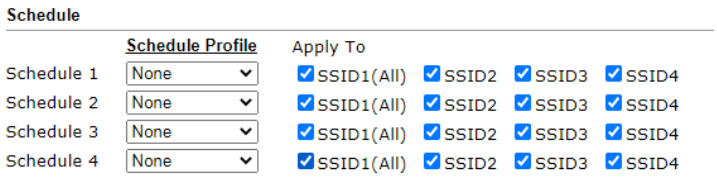
## III-1-2 General Setup

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




Available settings are explained as follows:

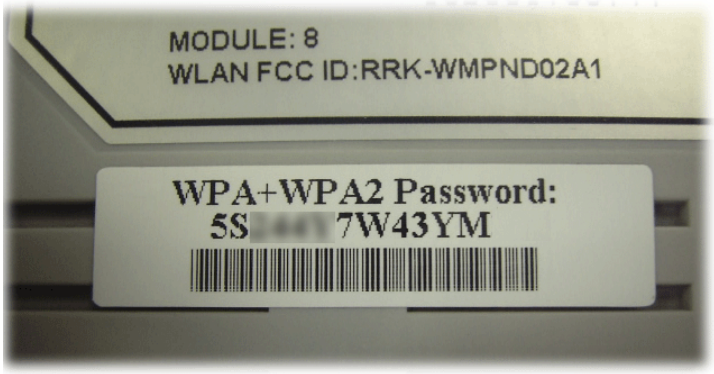
| Item | Description |
|---|---|
| **Enable Wireless LAN** | Check the box to enable wireless function. |
| **Mode** | Select the 802.11 mode allowed on the band.<br>On the 2.4 GHz band, the following wireless mode options are available:<br>• 11b Only<br>• 11g Only<br>• 11n Only (2.4 GHz)<br>• Mixed (11b+11g)<br>• Mixed (11g+11n)<br>• Mixed (11b+11g+11n)<br>On the 5 GHz band on ac models (e.g., 2927ac), the following options are available:<br>• 11a Only<br>• 11n Only (5 GHz)<br>• Mixed (11a+11n) |

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

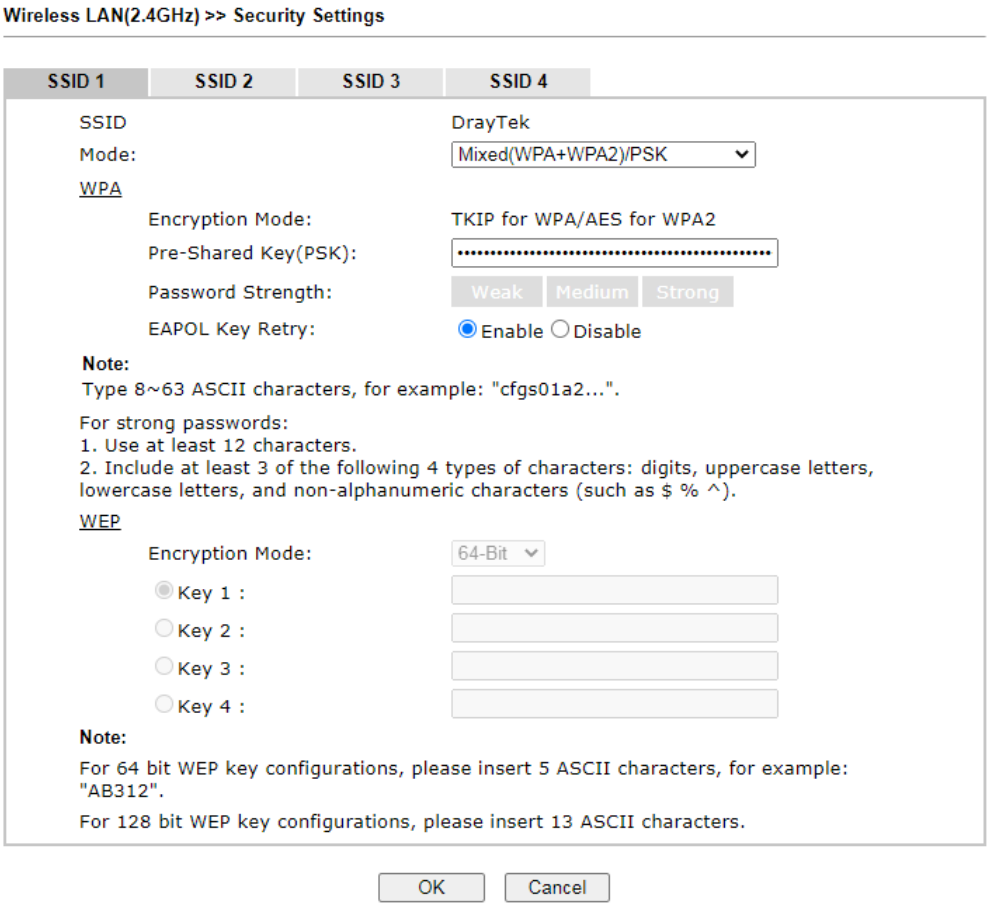
To save changes on the General Settings page, select **OK**; to discard changes, select **Cancel**.

## III-1-3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.




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




Available settings are explained as follows:

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

| | |
|---|---|
| | **Info** You should also set **Wireless LAN(2.4GHz) 802.1X Setting** simultaneously if 802.1x mode is selected.<br>**Disable** – Encryption mechanism is disabled.<br>**WEP** – Allow only connections from WEP clients. Encryption key should be entered in the WEP Key section.<br>**WEP/802.1x Only -** Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.<br>Allow only connections from WEP clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol.<br>**WPA/802.1x Only -** Allow only connections from WPA clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol.<br>**WPA2/802.1x Only-** Allow only connections from WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol.<br>**Mixed (WPA+WPA2/802.1x only) -** Allow connections from both WPA and WPA2 clients. Encryption key is obtained from a RADIUS server using the 802.1X protocol.<br>**WPA/PSK -** Allow connections only from WPA clients. Encryption key should be entered in the PSK field.<br>**WPA2/PSK -** Allow connections only from WPA2 clients. Encryption key should be entered in the PSK field.<br>**Mixed (WPA+ WPA2)/PSK -** Allow connections from both WPA and WPA2 clients. Encryption key should be entered in the PSK field. |
| **WPA** | WPA encrypts each frame transmitted from the radio using the key, which is either entered in the PSK (Pre-Shared Key) field, or or automatically negotiated via 802.1x authentication from a RADIUS server.<br>**Pre-Shared Key (PSK)** - Enter 8~63 ASCII characters, for example, “012345678..” , or 64 hexadecimal digits with a leading “0x”, for example, "0x321253abcde...".<br>**Password Strength** – The system will display the strength of the password, indicated by the words “weak”, “medium” or “strong”.<br>**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** | WEP keys can either be 64-bit or 128-bit.<br>**64-Bit** - Either 5 ASCII characters, for example “12345”, or 10 hexadecimal digitals with a leading “0x”, such as “0x4142434445”.<br>**128-Bit** - Either 13 ASCII characters, for example “ABCDEFGHIJKLM”, or 26 hexadecimal digits with a leading “0x”, for example “0x41424344454647484 94A4B4C4D”.<br>Up to four keys can be entered here, but only one key can be selected at any time. The keys can be entered in ASCII or Hexadecimal.<br>All wireless devices intending to connect to the same SSID must support the same WEP encryption bit size and have the |

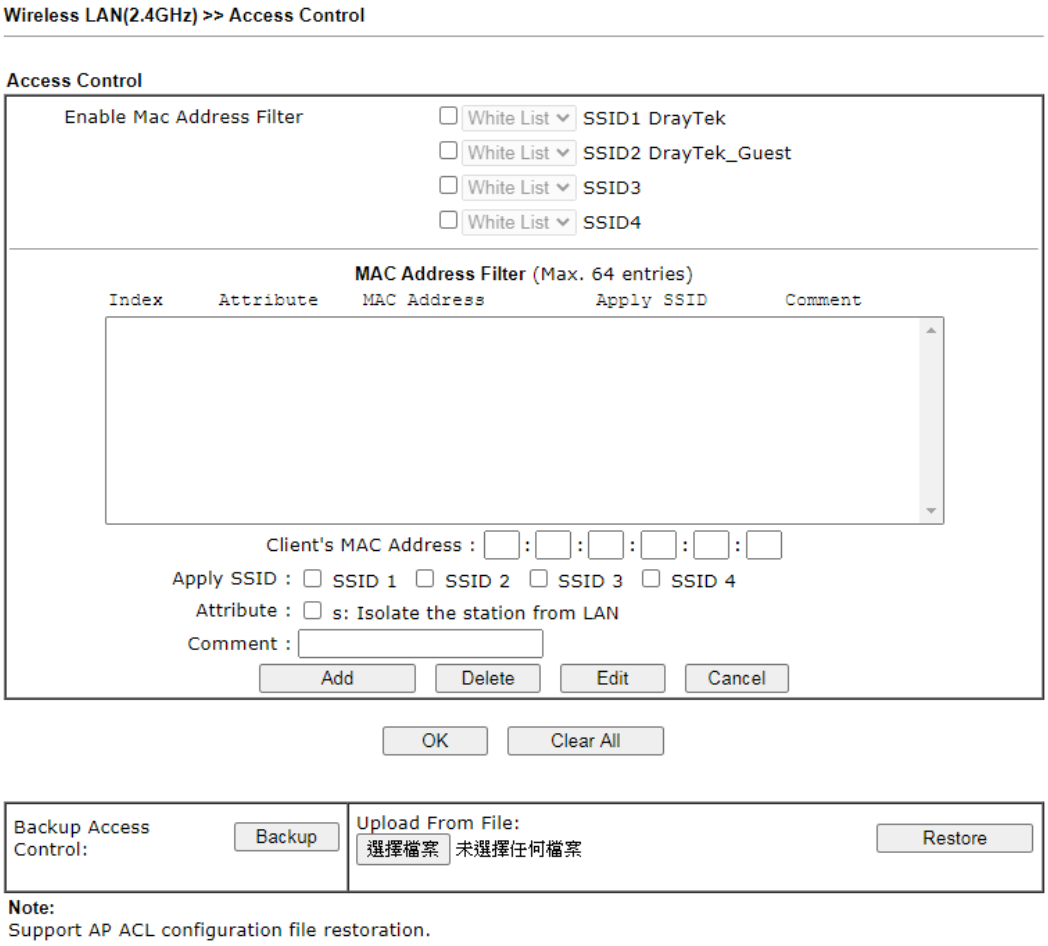
| | |
|---|---|
| | same key. |

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

## III-1-4 Access Control

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Mac Address Filter** | Select the SSIDs that you would like to have MAC Address filter enabled. Select **White List** or **Black List** in the combo box next to each enabled SSIDs.<br>**White List** - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list.<br>**Black List** - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list. |
| **MAC Address Filter** | Displays all MAC addresses in the filter list. |
| **Client's MAC Address** | Manually enter the MAC address of wireless client. |

| | |
|---|---|
| **Apply SSID** | Select the SSIDs to which the above MAC address filter will be applied. |
| **Attribute** | **s: Isolate the station from LAN -** select to isolate the wireless client from LAN. |
| **Comment** | Enter a brief description for the specified client's MAC address. |
| **Add** | Add a new filter entry to the MAC Address filter list using the information entered above. |
| **Delete** | Delete the selected MAC address from the list. |
| **Edit** | Update the selected MAC address in the list using the information entered above. |
| **Cancel** | Clear the contents of all the above fields. This will discard all changes without saving to the MAC Address Filter list. |
| **OK** | Click to save the MAC Address Filter list. |
| **Clear All** | Remove all entries from the MAC Address Filter list. |
| **Backup Access Control** | Settings on this web page can be saved as a file which can be restored in the future by this device or other device. |
| **Upload From File** | Restore wireless access control settings and applied onto this device. |

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

## III-1-5 WPS

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



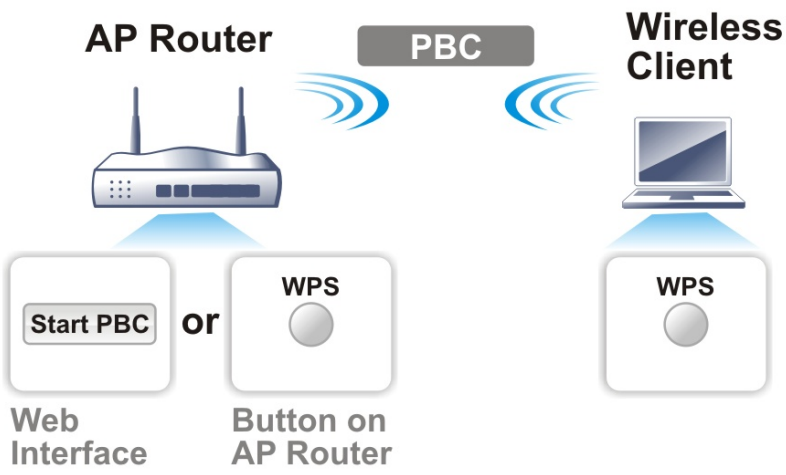

| | |
|---|---|
| **Info** | WPS works with wireless stations with WPS or WPS2 support. It does not work with WEP. |

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

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

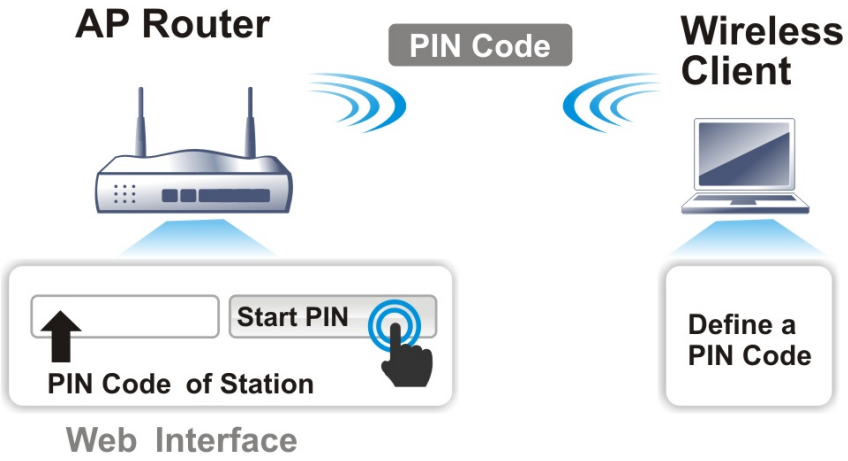
### Using the PBC button

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

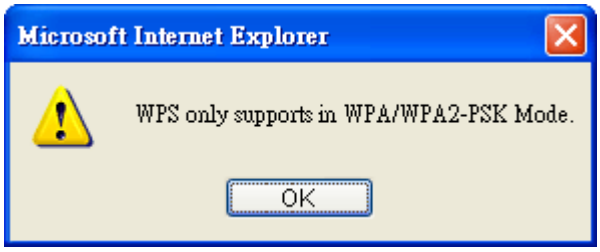



### Using a PIN code

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

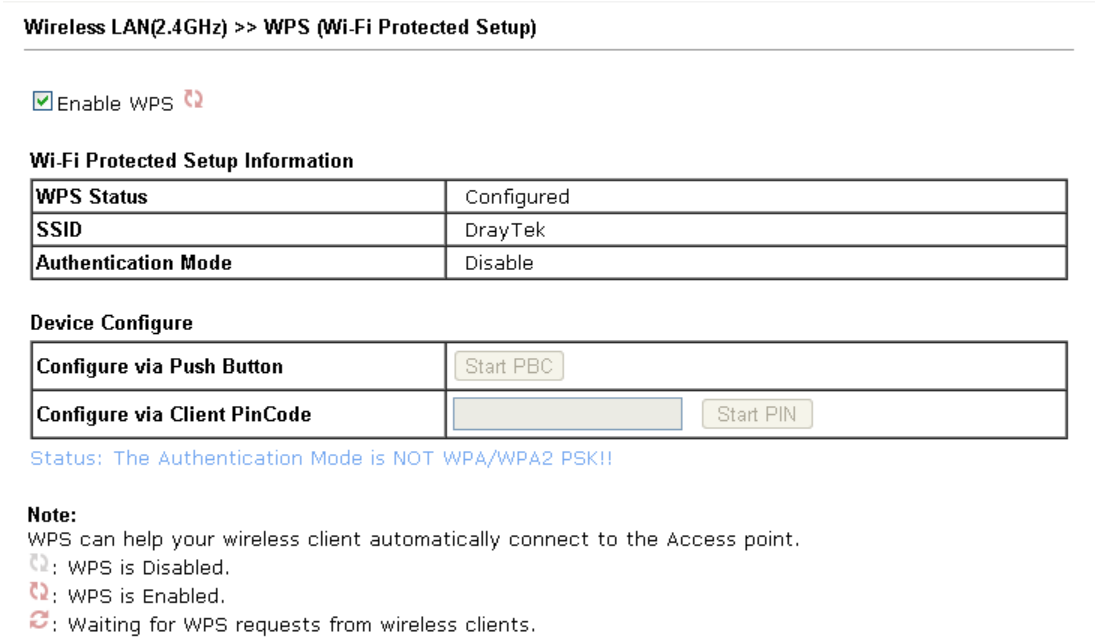



WPS is only supported when the encryption protocol is set to WPA-PSK or WPA2-PSK. If other protocols (such as WEP) have been selected in **Wireless LAN>>Security**, you will see the following message box:




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

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




Available settings are explained as follows:

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

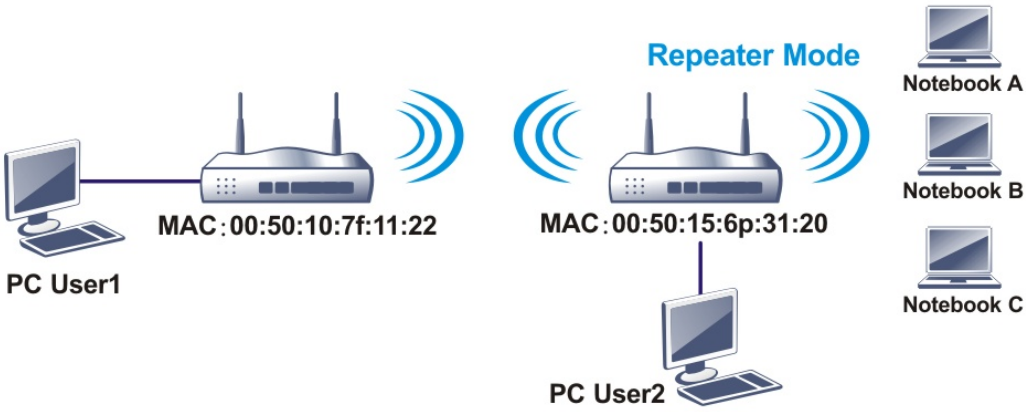
## III-1-6 WDS (for 5GHz)

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

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

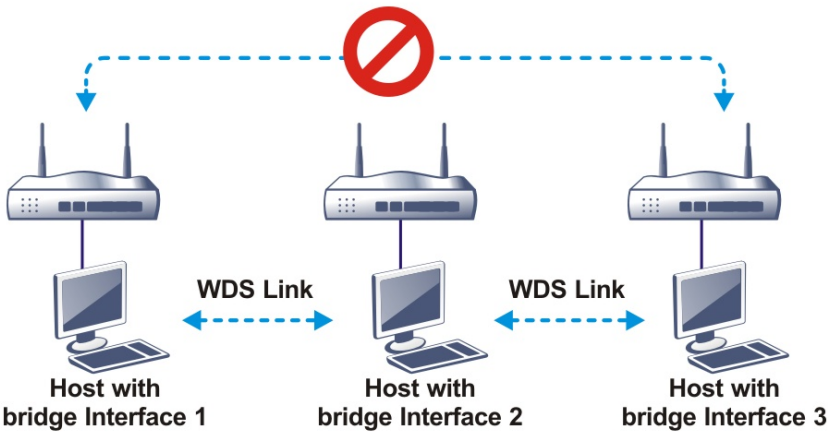



- **Repeater mode**, which extends the coverage range of a WLAN.

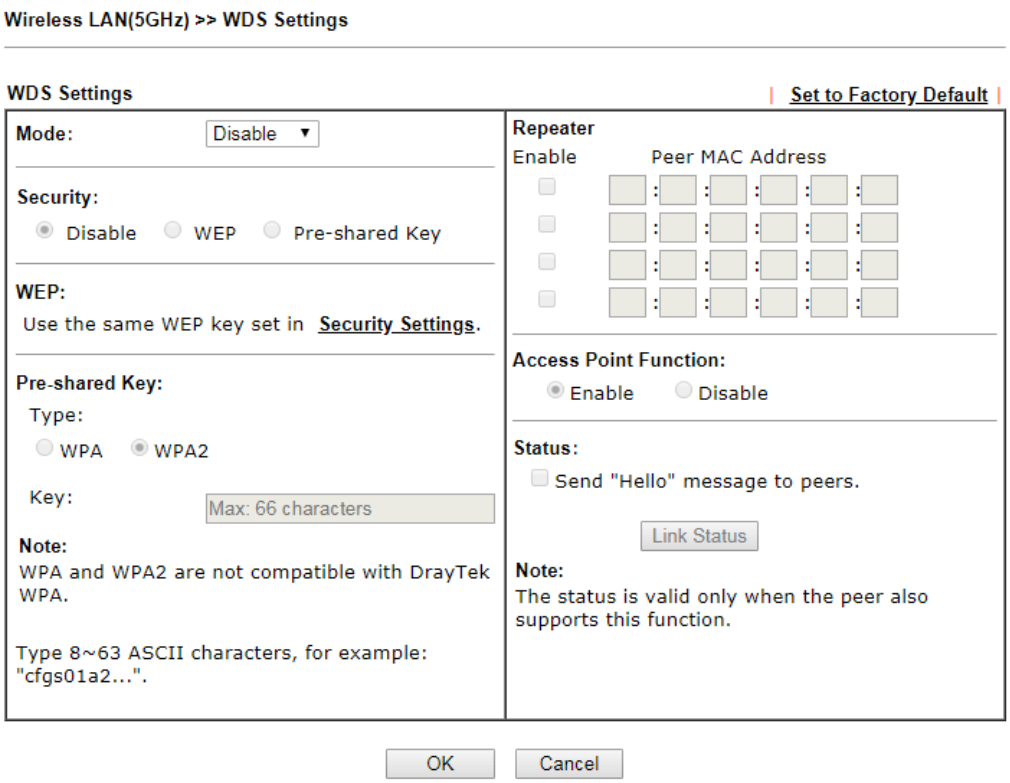



The main difference between these two modes is that, in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links, whereas in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words,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

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



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




Available settings are explained as follows:

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

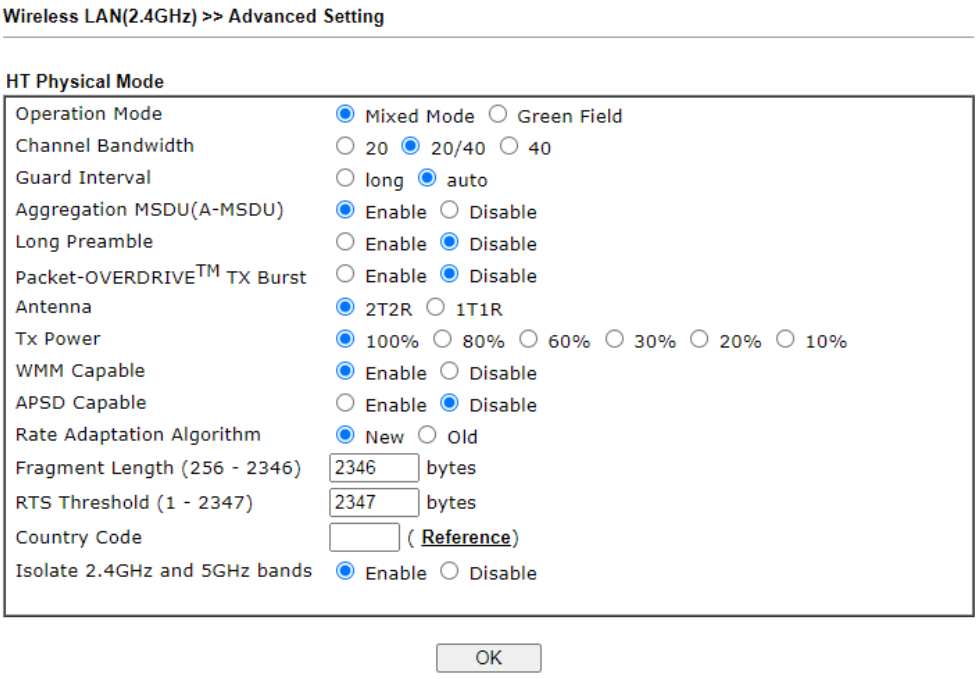
To save changes on this page, select **OK**; to discard changes, select **Cancel**.

## III-1-7 Advanced Setting

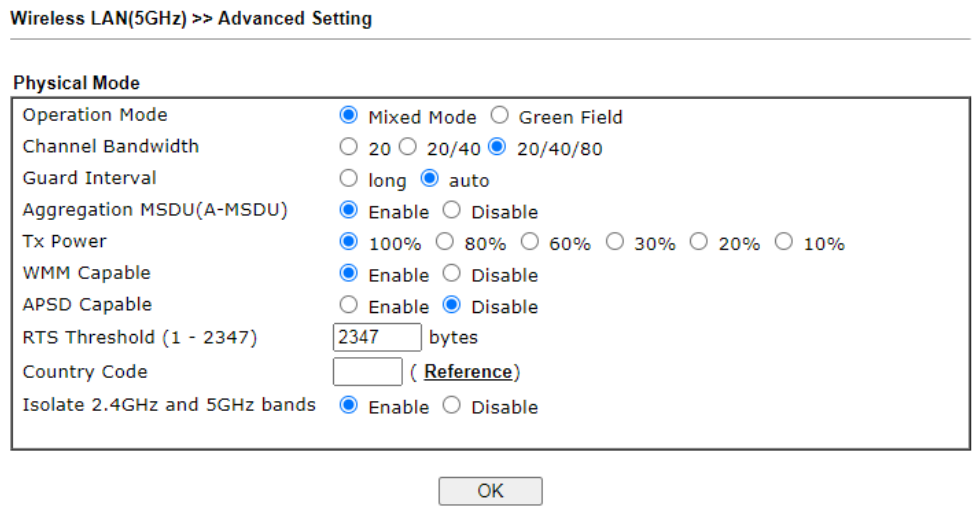
On this page you can configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

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

### 2.4 GHz Advanced Setting page



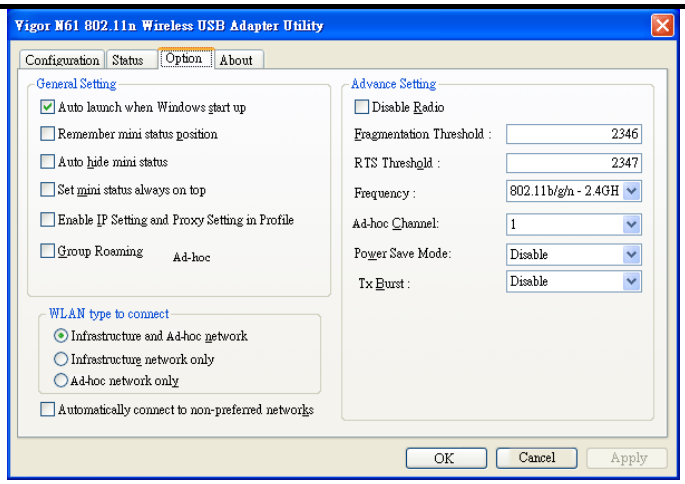

### 5 GHz Advanced Setting page:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Operation Mode** | **Mixed Mode** – The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless transmissions will be slowed down |

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

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

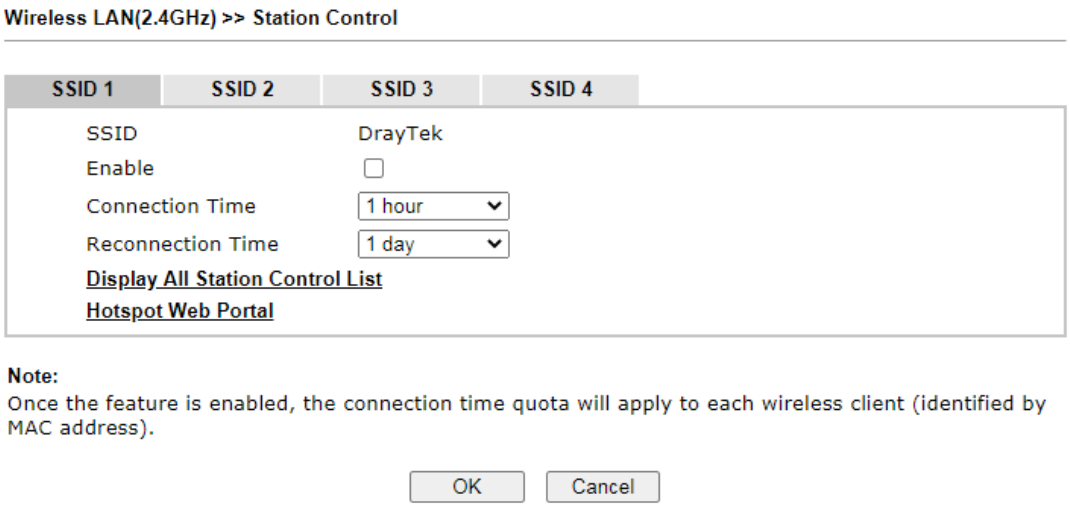
| | |
|---|---|
| **RTS Threshold (1 – 2347)** | Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.<br>Set the RTS threshold. Do not modify default value if you don't know what it is, default value is 2347.<br>Adjusts the 802.11 maximum transmit frame size, which might reduce chances of collision with hidden stations. You are advised to leave the default value, 2347, untouched. |
| **Country Code** | Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless stations will detect/scan access points looking for country codes to determine which country it is in, and utilize channels appropriate to the country. The wireless client might get confused if there are multiple access points in the vicinity broadcasting different country codes. In such cases, it might be necessary to change the country code of the access point to ensure these clients can successfully establish a wireless connection. |
| **Isolate 2.4GHz and 5GHz bands** | The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa.<br>For WLAN 2.4GHz and 5GHz set with the same SSID name:<br>● 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.<br>● Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other. |

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

## III-1-8 Station Control

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

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



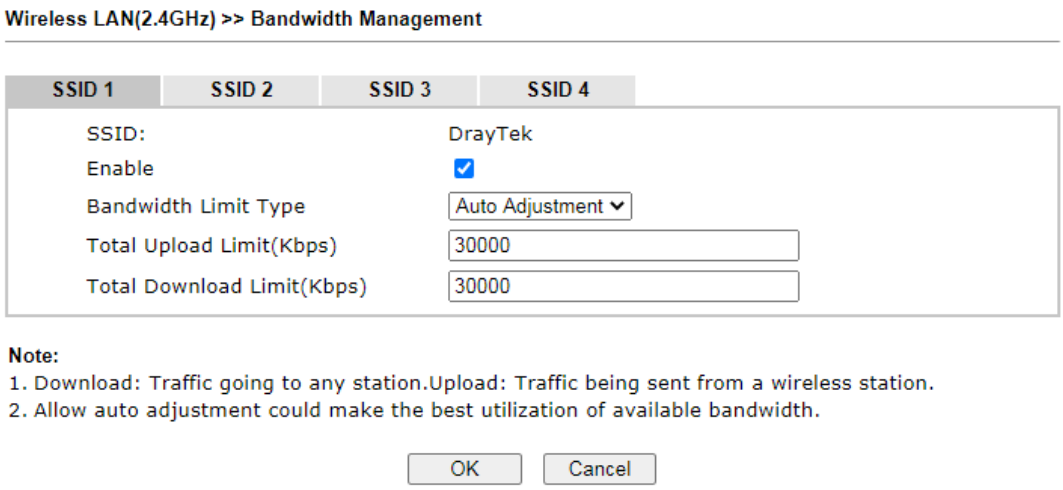

Available settings are explained as follows:

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

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

## III-1-9 Bandwidth Management

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




Available settings are explained as follows:

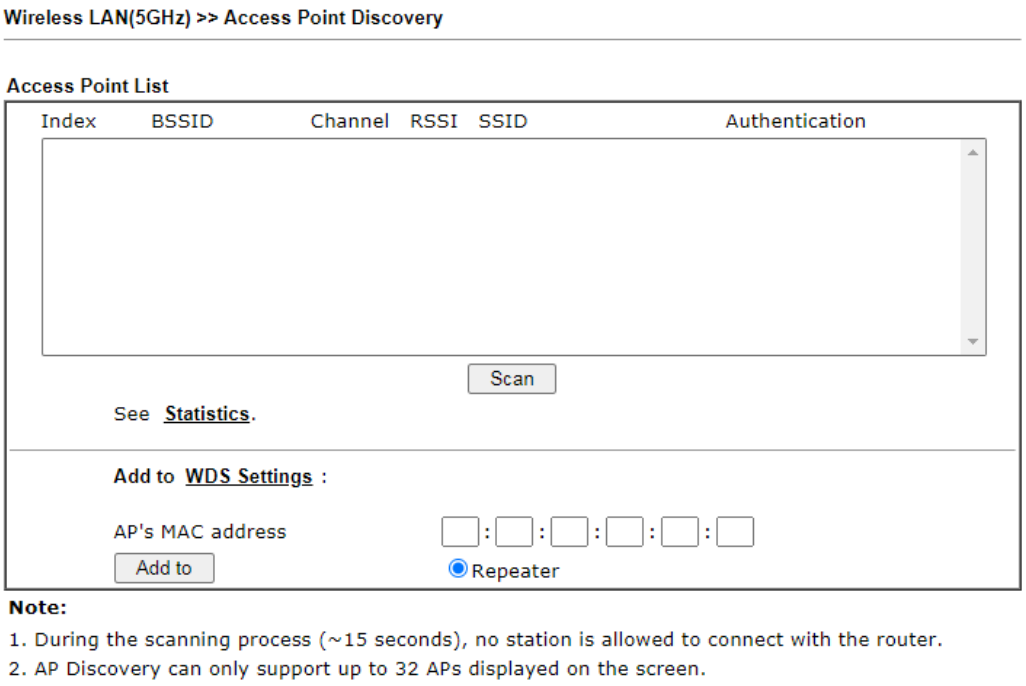
| Item | Description |
|---|---|
| **SSID** | Display the specific SSID name. |
| **Enable** | Check this box to enable the bandwidth management for clients. |
| **Bandwidth Limit Type** | **Auto Adjustment -** Bandwidth limit is determined by the system automatically.<br>**Per Station Limit** – Bandwidth limit is determined according to the limitation of the wireless client. |
| **Total Upload Limit** | It is available when Auto Adjustment is selected.<br>Type a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to Vigor2927. |
| **Total Download Limit** | It is available when Auto Adjustment is selected.<br>Type a value to define the maximum data client(stations) connecting to Vigor2927. |
| **Upload Limit** | It is available when Per Station Limit is selected.<br>Type a value to define the maximum data traffic (uploading) for each wireless client connecting to Vigor2927. |
| **Download Limit** | It is available when Per Station Limit is selected<br>Type a value to define the maximum data traffic (downloading) for each wireless client connecting to Vigor2927. |

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

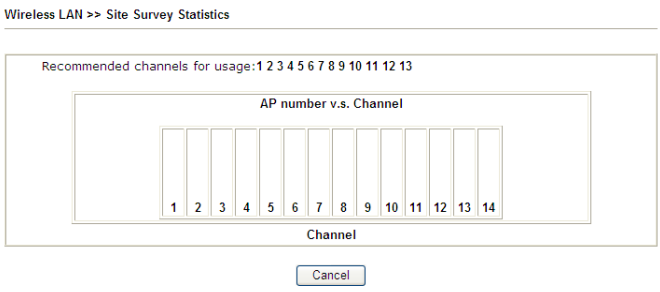
## III-1-10 AP Discovery

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

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




Available settings are explained as follows:

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

## III-1-11 Airtime Fairness

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

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

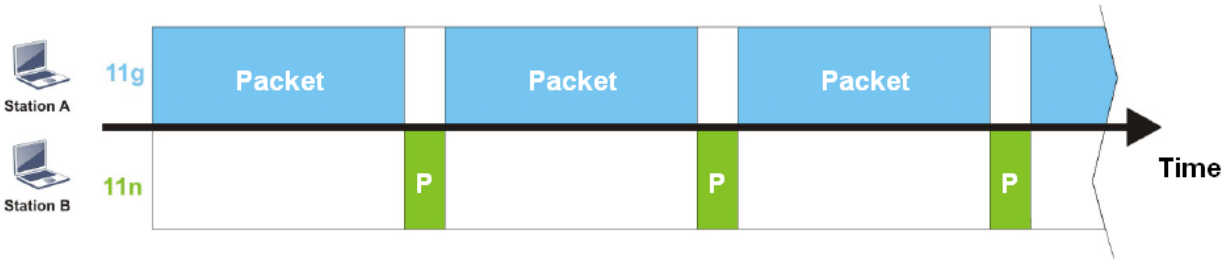
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

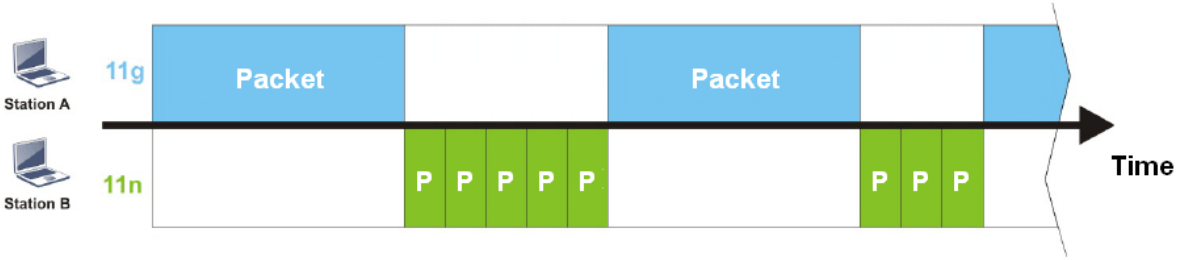
The principle behind the IEEE802.11 channel access mechanisms is that each station has *equal probability* to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

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

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




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



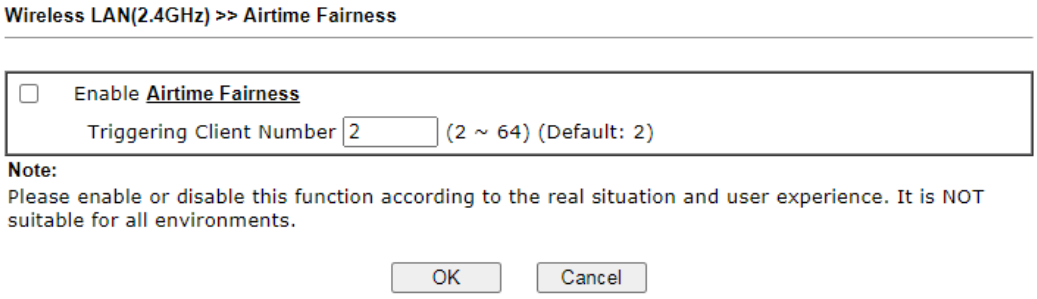
This is similar to automatic Bandwidth Limit, where the dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4 GHz and 5 GHz bands are independent, but stations connected to different SSIDs on the same band are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

Environments that can benefit by applying airtime fairness:

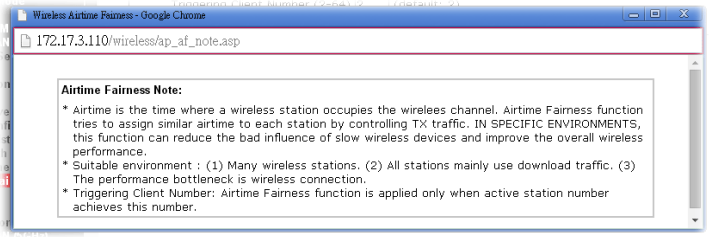
(1) Many wireless stations.

(2) All stations mainly use download traffic.

(3) The performance bottleneck is wireless connection.




Available settings are explained as follows:

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

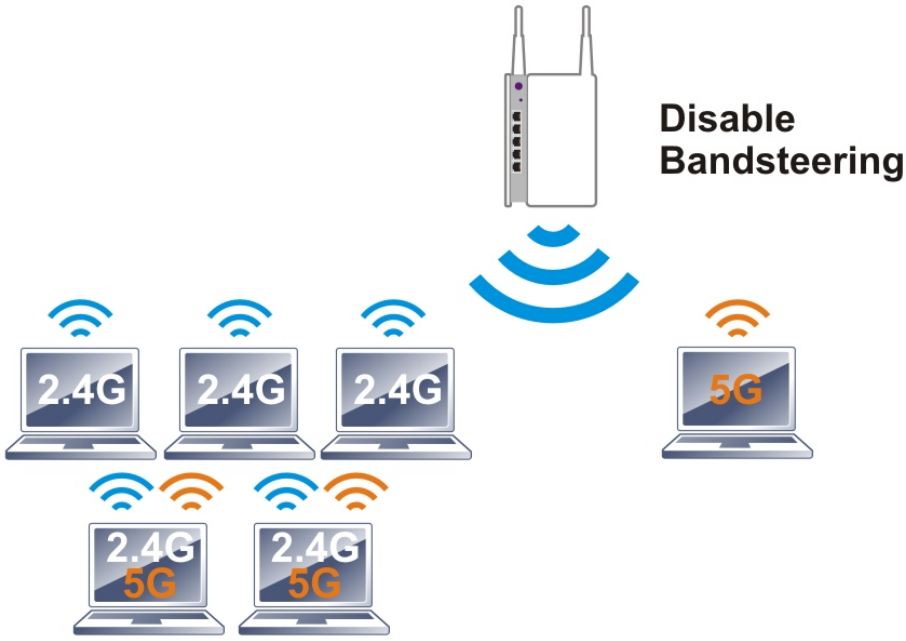


To save changes on this page, select **OK**; to discard changes, select **Cancel**.

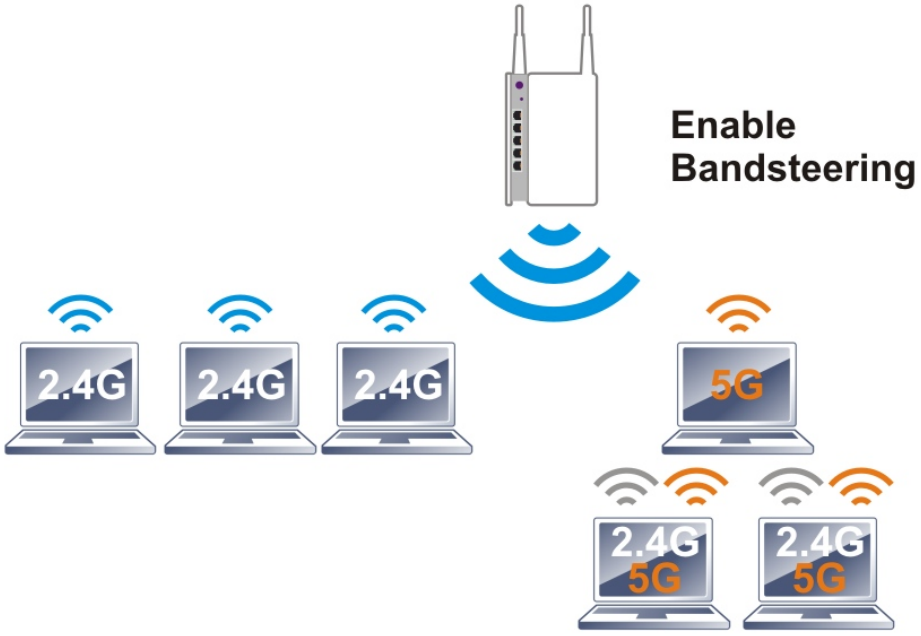
| | |
|---|---|
| **Info** | Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously. |

## III-1-12 Band Steering (2.4 GHz)

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



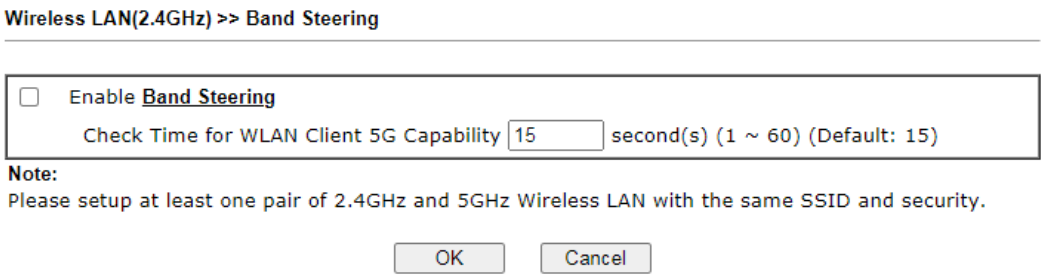

If a dual-band client is detected, the AP will let the wireless client connect to the less congested wireless band, such as the 5GHz band, to reduce network congestion.




**Info**

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

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

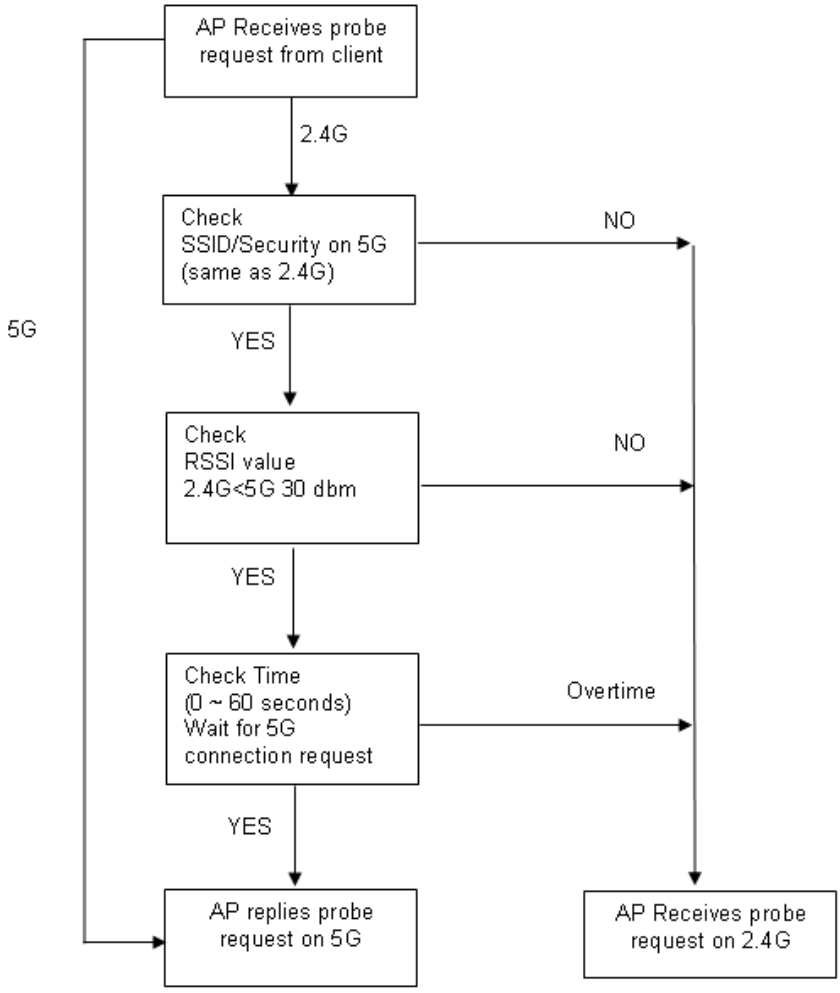



Available settings are explained as follows:

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

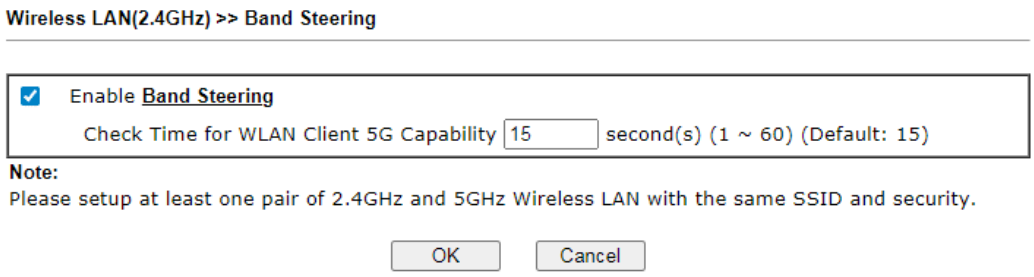
To save changes on this page, select **OK**; to discard changes, select **Cancel**.

The following diagram shows how Band Steering works.

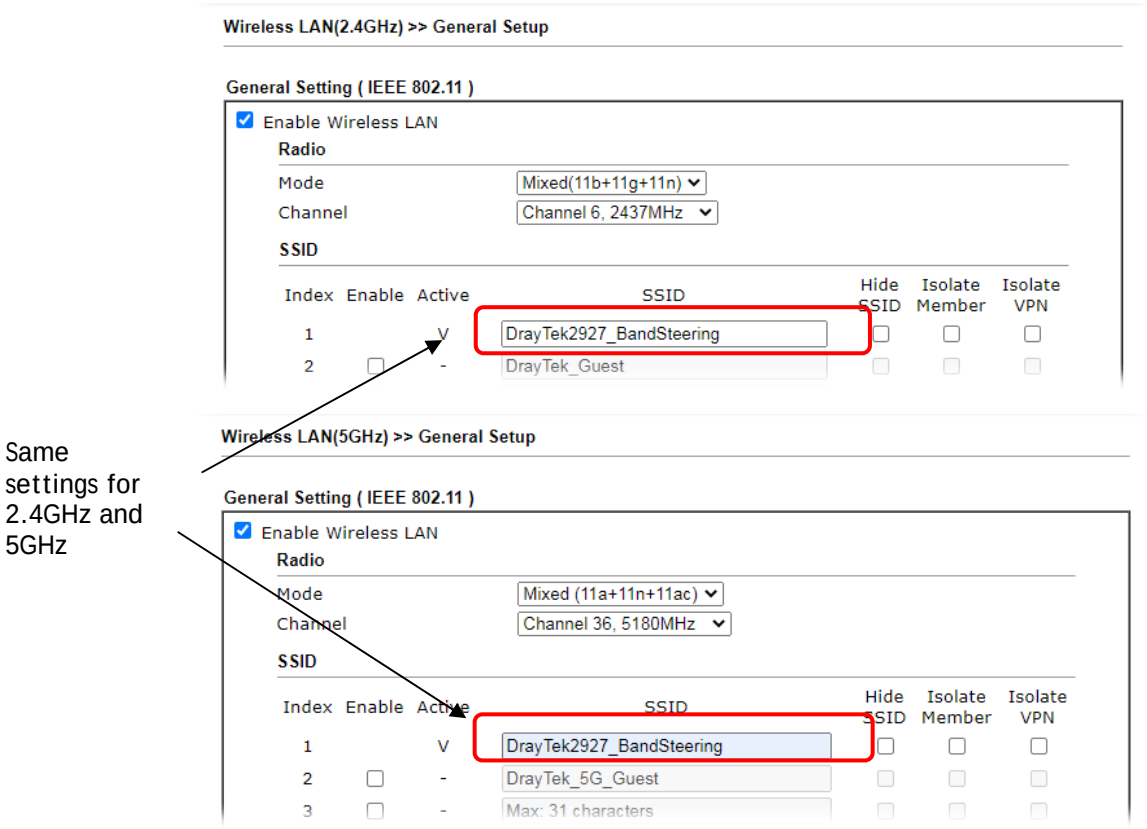



**Example: How to Use Band Steering?**

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




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




Same settings for 2.4GHz and 5GHz

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



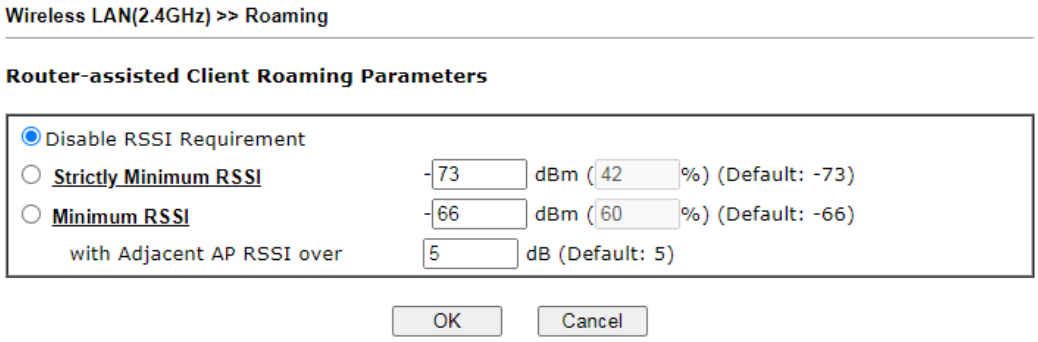

Same value for 2.4GHz and 5GHz

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

## III-1-13 Roaming

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

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




Available settings are explained as follows:

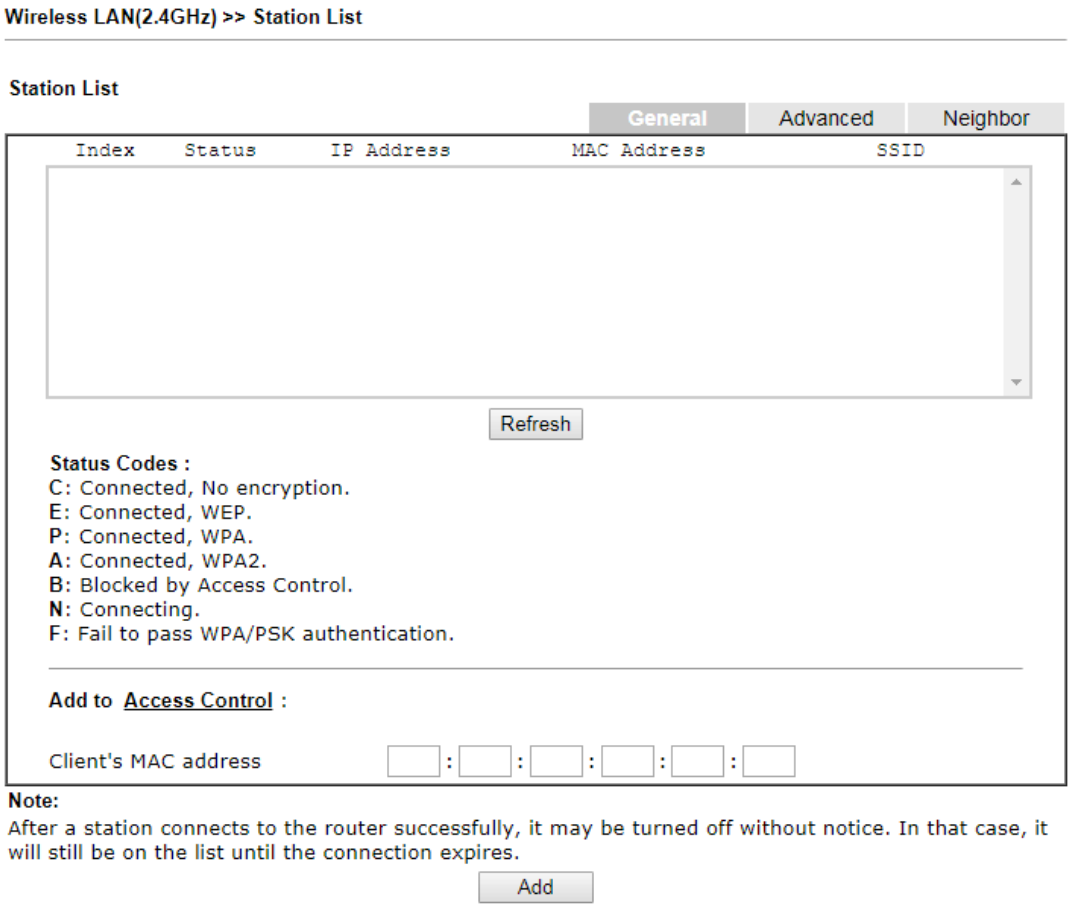
| Item | Description |
|---|---|
| **Disable RSSI Requirement** | The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations. |
| **Strictly Minimum RSSI** | The Vigor router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

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

## III-1-14 Station List

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

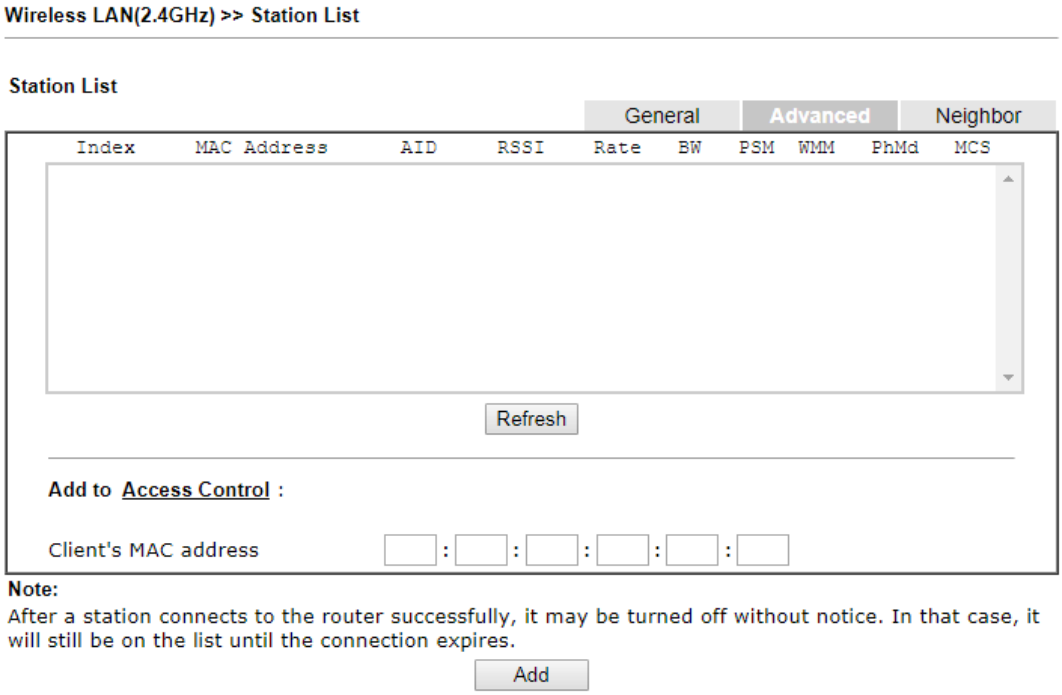
There are 3 tabs on the Station List screen: General, Advanced and Neighbor. Both General and Advanced show wireless stations connected to the Vigor router, whereas Neighbor shows nearby wireless stations connected to other access points that are detected by the Vigor router.



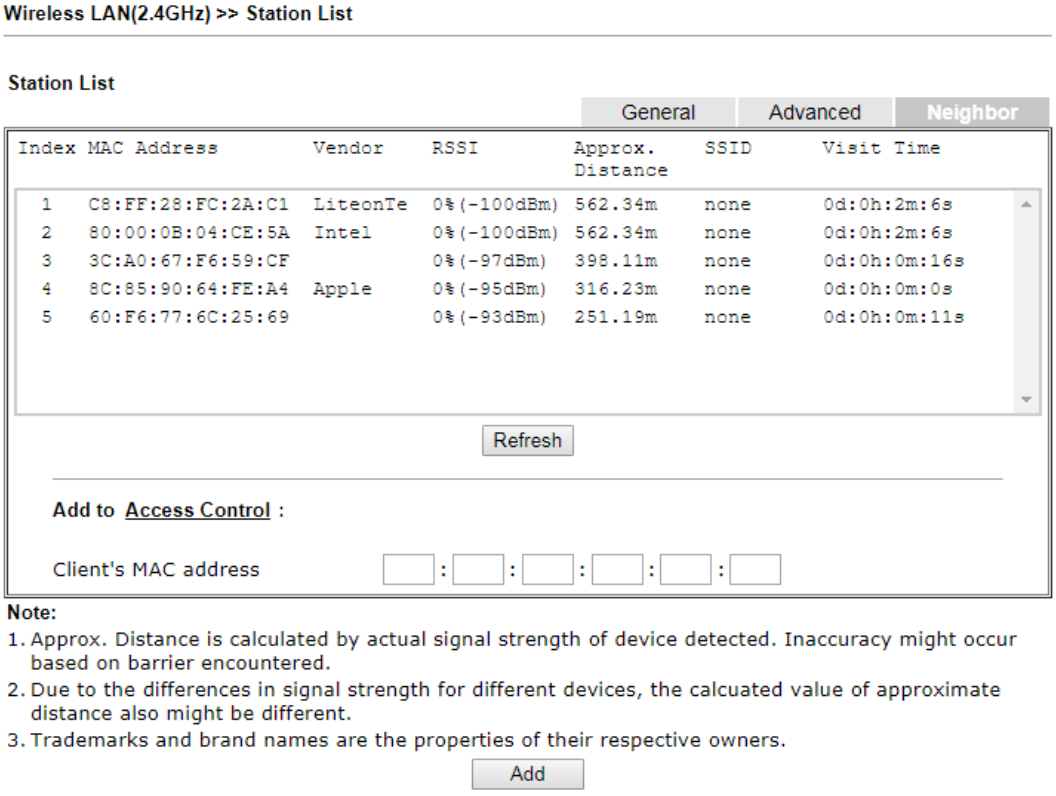

Available settings are explained as follows:

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

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




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



This page is left blank.

# Part IV VPN




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




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



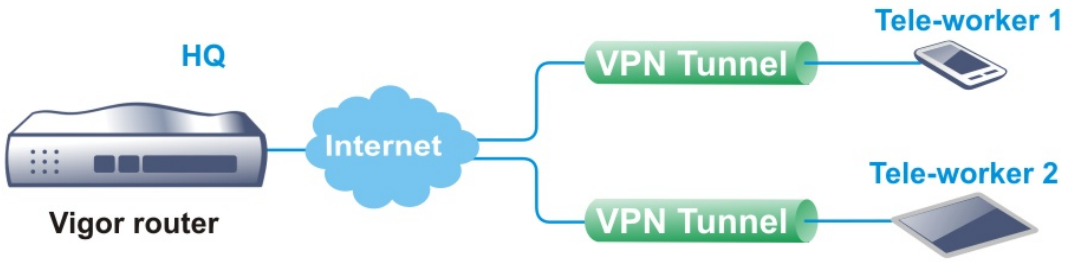

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is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

# IV-1 VPN and Remote Access

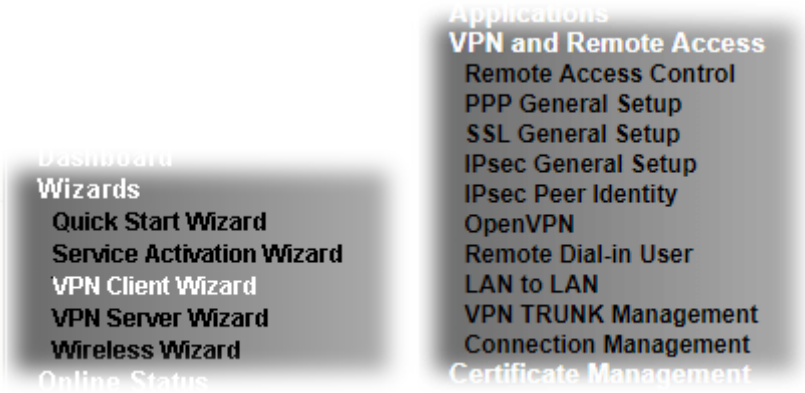
A Virtual Private Network (VPN) is an extension of a private network that allows users to access network resources that available on the private network across shared or public networks such as the Internet, as if users are directly connected to the private network.

Here are some uses of VPNs:

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



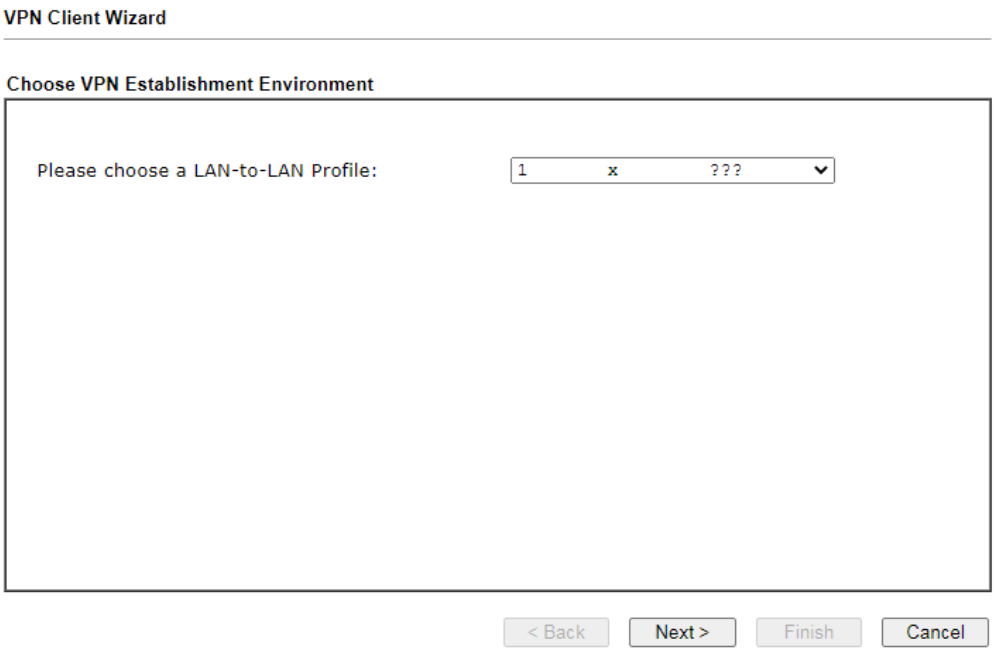
# Web User Interface




## IV-1-1 VPN Client Wizard

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

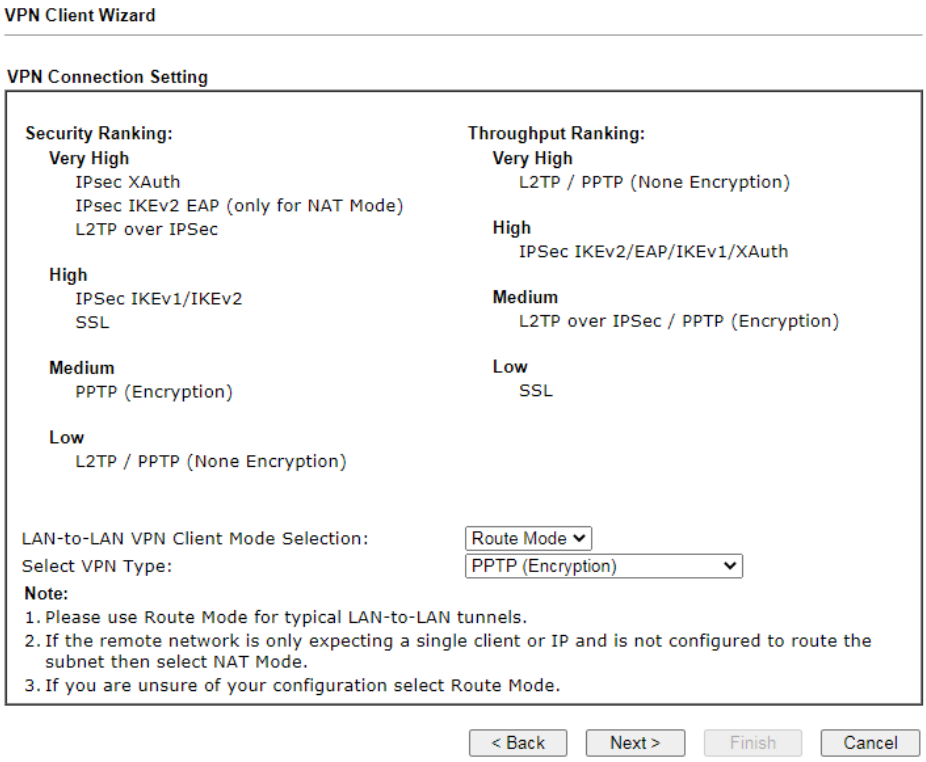
1. On the menu bar, click on **Wizards,** and then **VPN Client Wizard**.




Available settings are explained as follows:

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

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

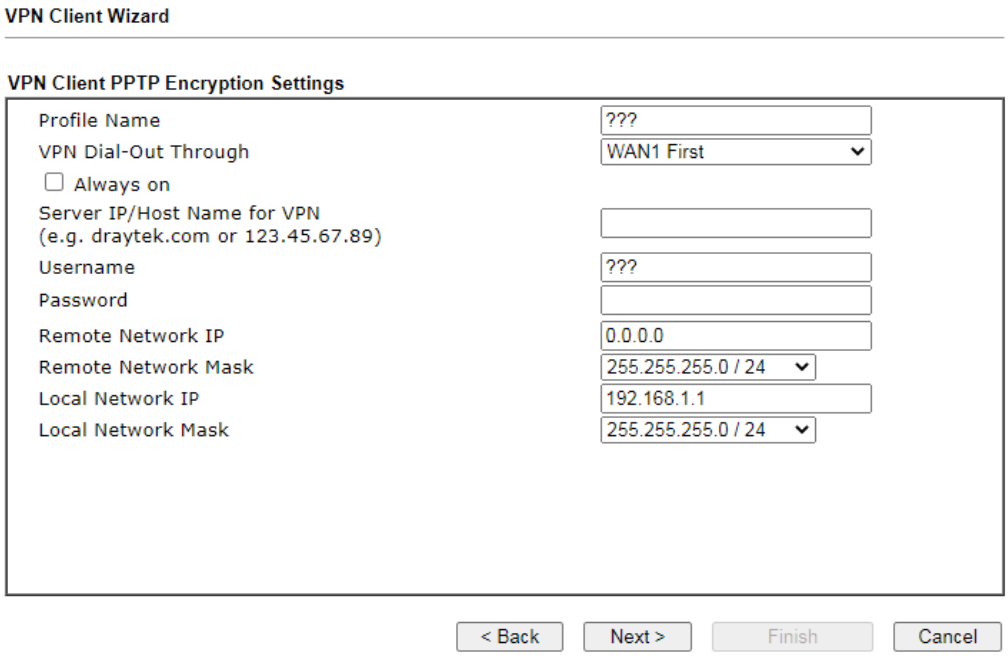



Available settings are explained as follows:

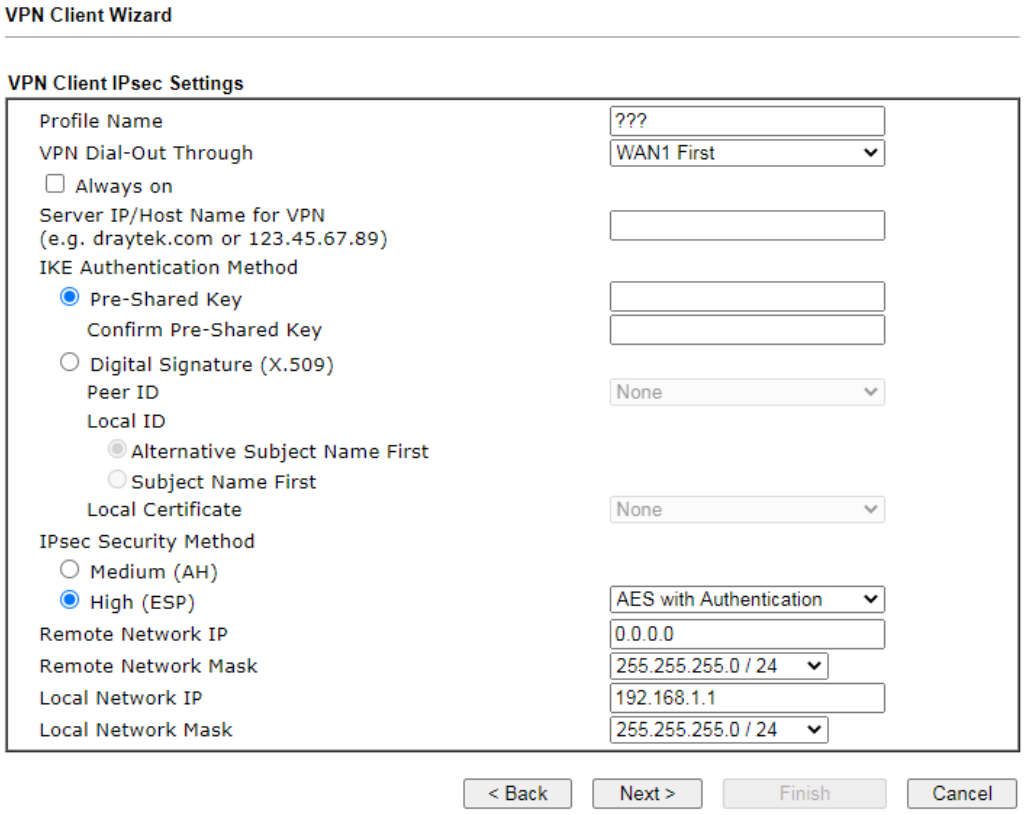
| Item | Description |
|---|---|
| **LAN-to-LAN Client Mode Selection** | **Route Mode –** All traffic between the local network and the remote network bear the originating IP addresses. Select this if the VPN server can establish routes to handle inter-LAN traffic routing.<br>**NAT Mode –** The VPN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

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

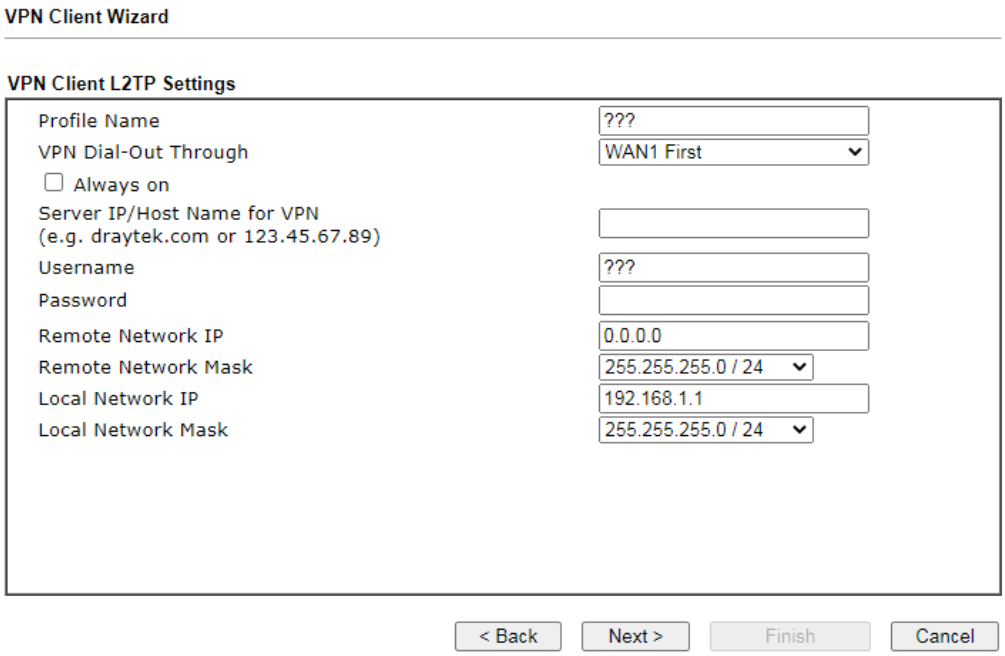
If you have selected **PPTP (None Encryption)** or **PPTP (Encryption)**, the following configuration screen appears.



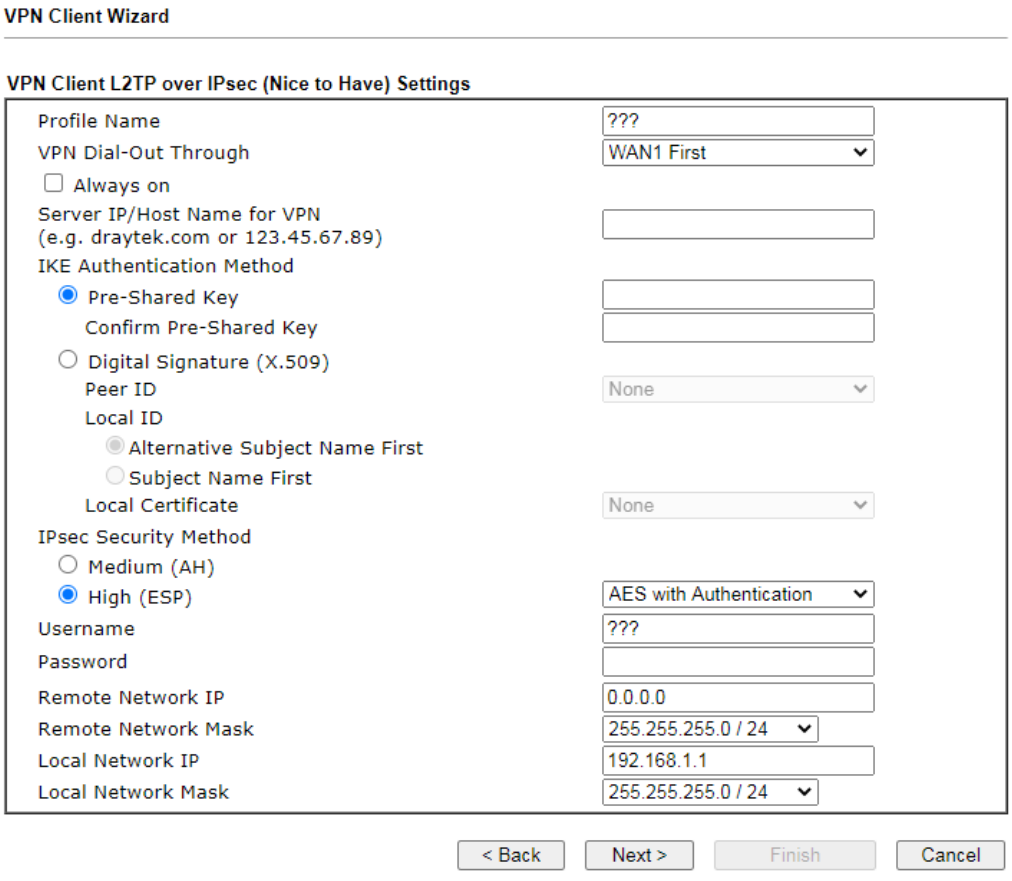

If you have selected **IPsec**, the following configuration screen appears.



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



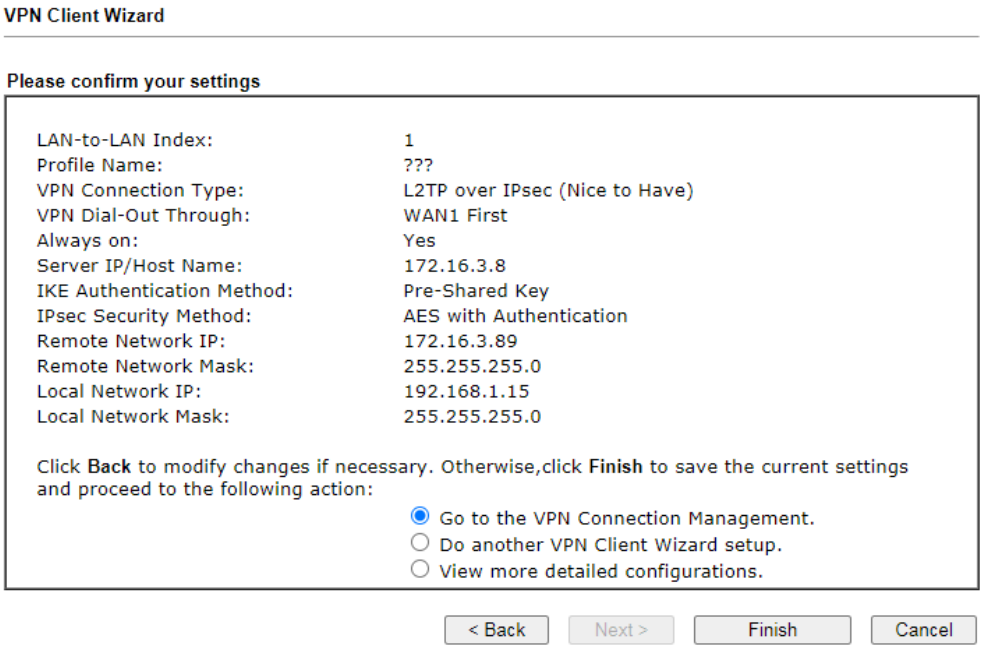

If you have selected **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must)**, the following configuration screen appears.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. The maximum length of the Profile Name is 10 characters. |
| **VPN Dial-Out Through** | The WAN interface to be used for dialing out to establish the VPN tunnel.<br>**WANx First (or LTE First)** - The Router first attempts to establish the VPN tunnel using this WAN interface. When that is unsuccessful, it will attempt to use other WAN interfaces.<br>**WANx Only (or LTE Only)** - The Router will establish the VPN tunnel using this WAN interface only.<br>**WANx Only: Only establish VPN if WANy down** - The Router will establish the VPN tunnel using this WAN interface if the other WAN interface is offline. |
| **Always On** | If selected, the router will maintain the VPN connection. |
| **Server IP/Host Name for VPN** | Enter the IP address or hostname of the server of the remote VPN server. |
| **IKE Authentication Method** | IKE Authentication Method to be used. Choose between **Pre-shared Key** and **Digital Signature (X.509)**.<br>**Pre-shared Key**<br>● **Pre-Shared Key-** Specify a key for IKE authentication.<br>● **Confirm Pre-Shared Key-**Confirm the pre-shared key.<br>**Digital Signature (X.509)**<br>● **Peer ID** – Select Peer ID from the dropdown list. Peer IDs are managed using VPN and Remote Access >> IPsec Peer Identity.<br>● **Local ID** – Select **Alternative Subject Name First** or **Subject Name Firs**t.<br>● **Local Certificate** – Select a certificate from the dropdown list. Local certificates are managed using **Certificate Management >> Local Certificate.** |
| **IPsec Security Method** | **Medium** - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.<br>**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. |
| **Username** | This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.<br>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.<br>The length of the password is limited to 11 characters. |
| **Remote Network IP** | Please enter one LAN IP address (according to the real location of the remote host) for building VPN connection. |
| **Remote Network Mask** | Please enter the network mask (according to the real location of the remote host) for building VPN connection. |
| **Local Network IP** | Enter the local network IP for TCP / IP configuration. |
| **Local Network Mask** | Enter the local network mask for TCP / IP configuration. |

3. After you have entered all the required information, click **Next** to proceed to the confirmation page. The confirmation page shows a summary of all the settings. If you need to make adjustments to the settings, click **Back** to return to the previous page. Otherwise, select one of the following actions and click **Finish** to save the changes to the LAN-to-LAN VPN profile.




Available settings are explained as follows:

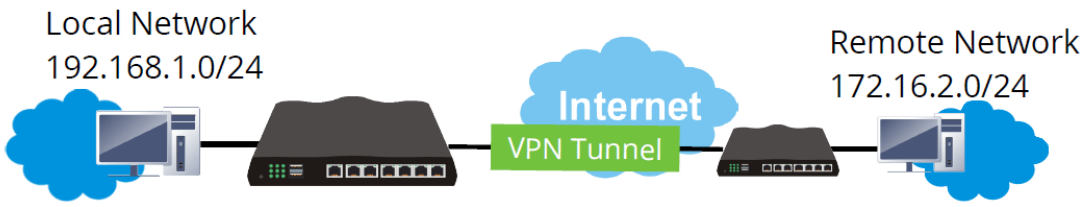
| Item | Description |
|---|---|
| **Go to the VPN Connection Management** | Proceed to **VPN and Remote Access>>Connection Management** to manage VPN sessions. |
| **Do another VPN Client Wizard Setup** | Rerun the VPN Client Wizard to configure another LAN-to-LAN VPN profile. |
| **View more detailed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

## IV-1-2 VPN Server Wizard

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

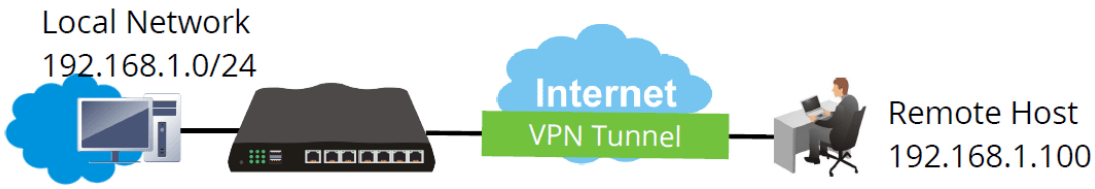
### Site-to-Site (LAN-to-LAN)

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



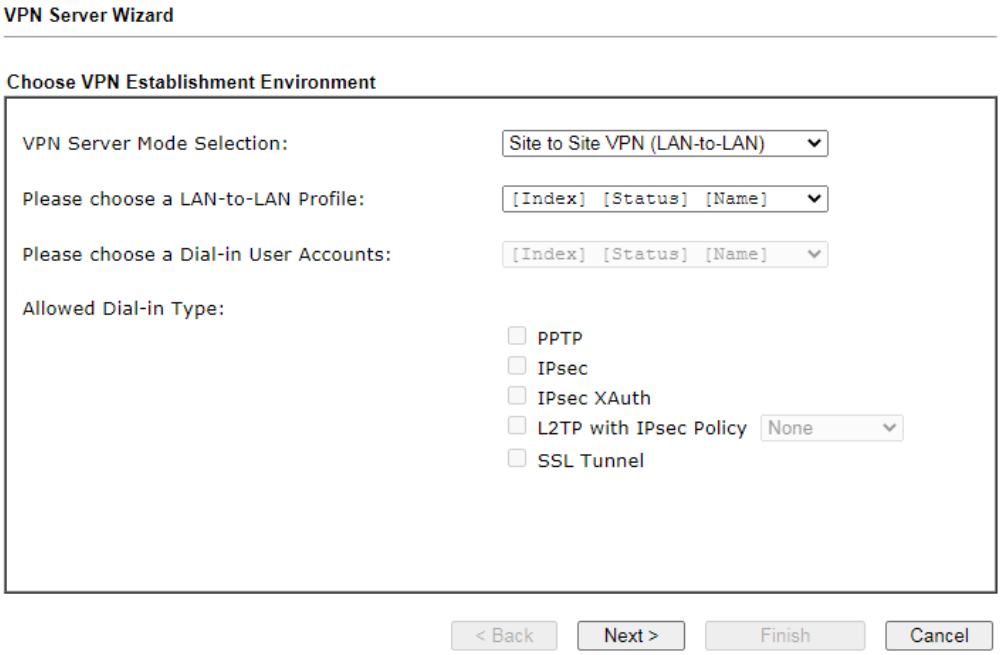

### Remote Access (Remote Dial-in)

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



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

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

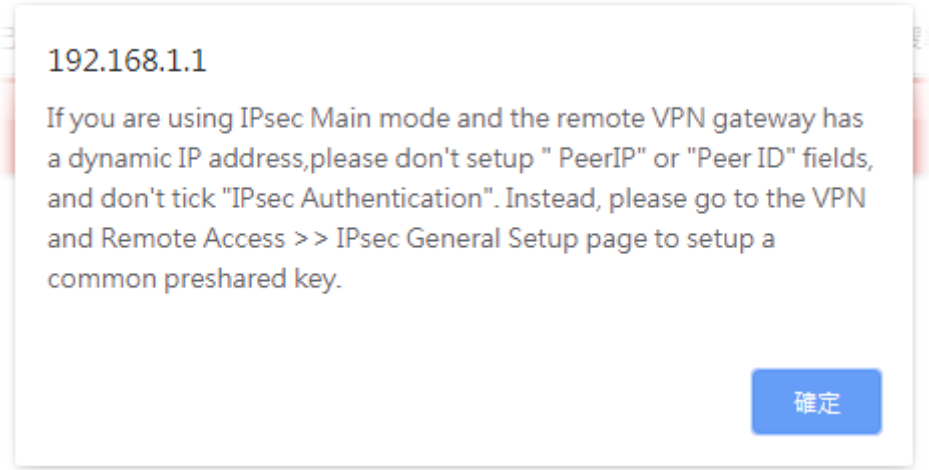



Available settings are explained as follows:

| Item | Description |
|---|---|
| **VPN Server Mode Selection** | Type of VPN Server to be configured.<br>**Site to Site VPN (LAN-to-LAN)** - Configures the VPN server for inbound connections from other routers.<br>**Remote Dial-in User (Teleworker)** - Configures VPN server for inbound connections from remote users. |
| **Please choose a LAN-to-LAN Profile** | If the VPN Server Mode selected was **Site to Site VPN (LAN-to-LAN)**, choose a LAN-to-LAN profile to store this configuration. |
| **Please choose a Dial-in User Accounts** | If the VPN Server Mode selected was **Remote Dial-in User (Teleworker)**, choose a Dial-in user profile to store this configuration. |
| **Allowed Dial-in Type** | Select all VPN protocols that are allowed for this LAN-to-LAN Profile or Dial-in User Account.<br>Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected. |

2. After making the choices for the server profile, please click **Next**.

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

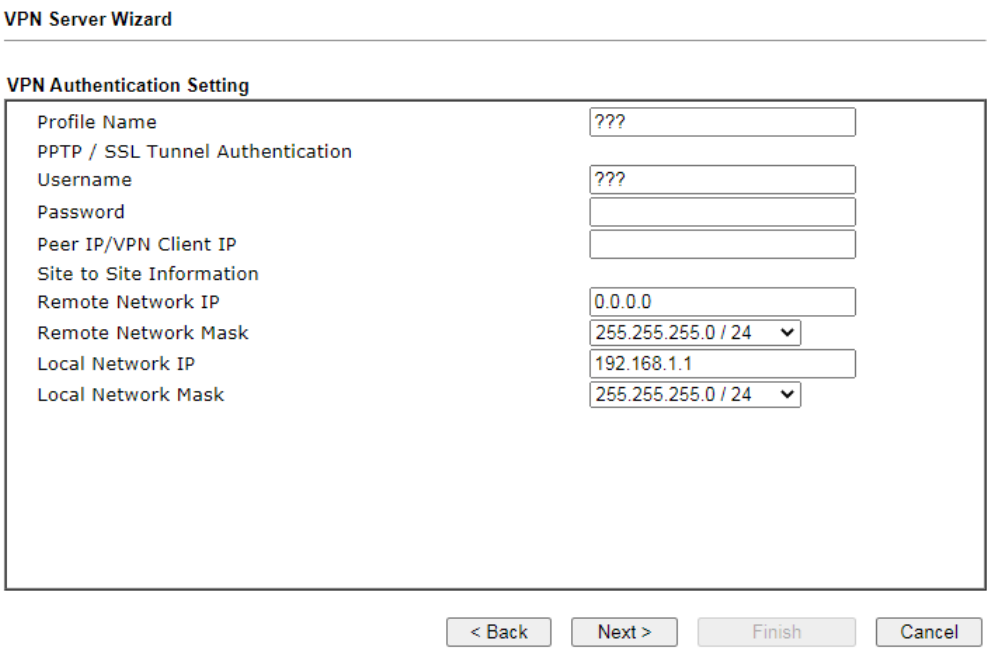



Click **OK** to dismiss the dialog box and proceed to the next page.

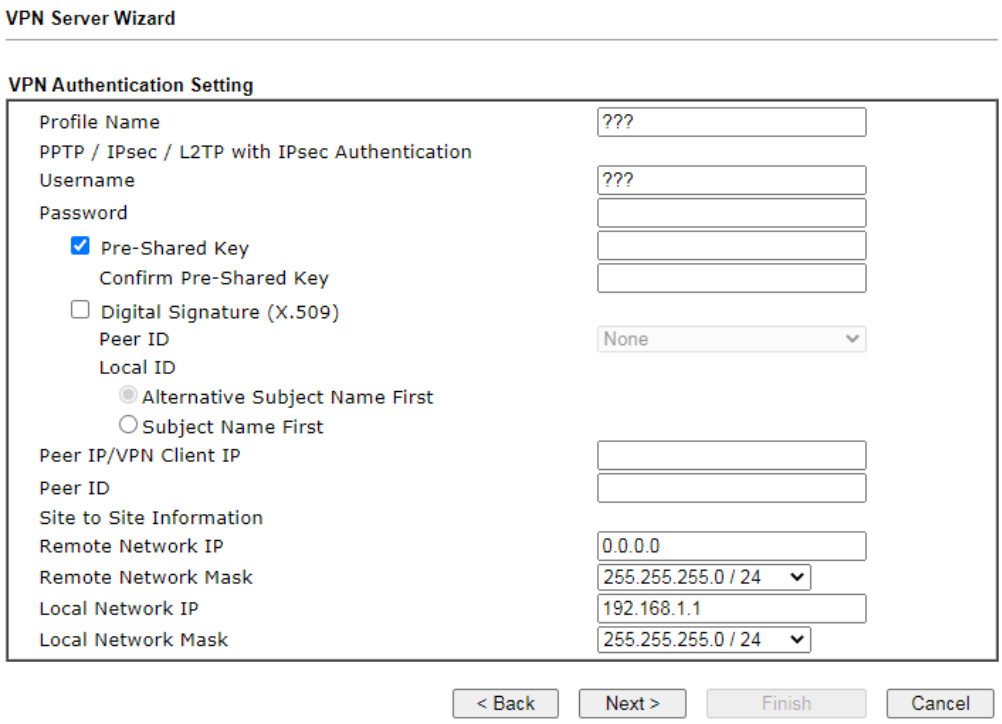
If you have chosen to configure a LAN-to-LAN VPN profile, proceed to step 4.

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

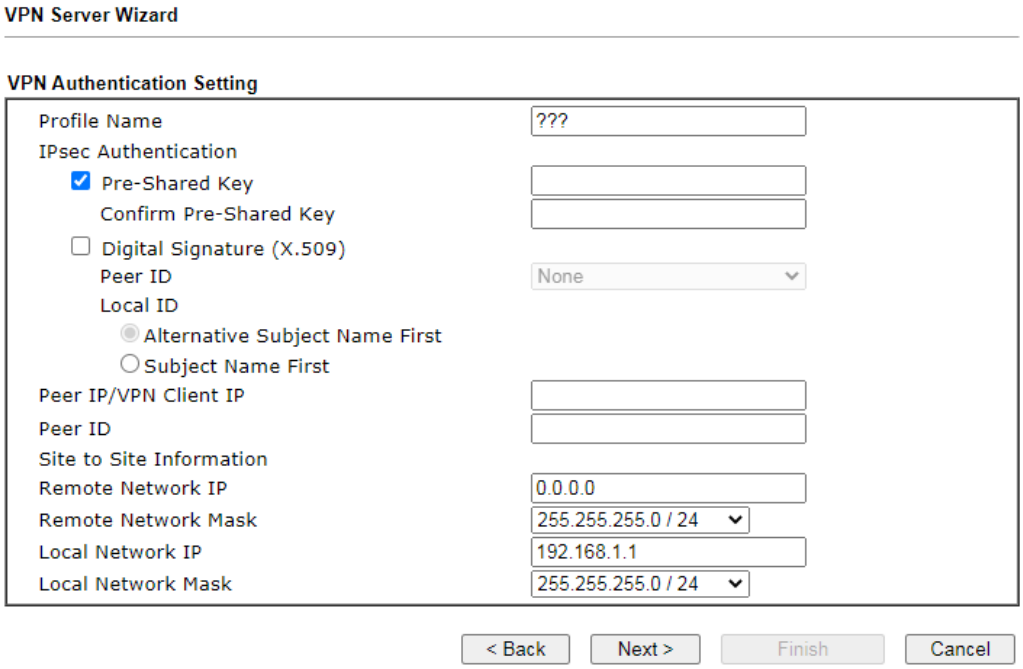
4. The **Site to Site VPN (LAN-to-LAN)** configuration page appears as follows if you have selected **PPTP/SSL**.



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




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

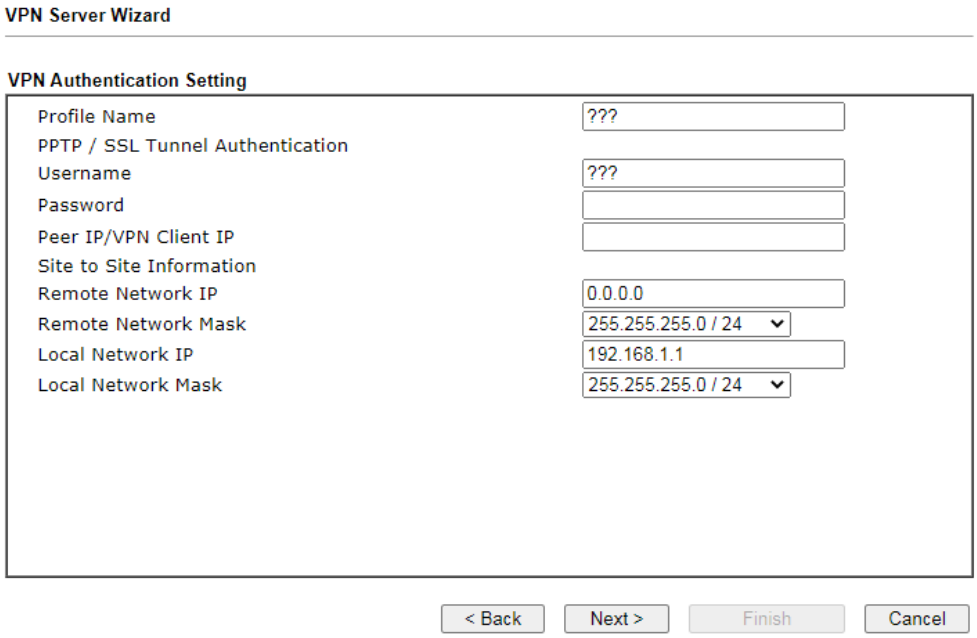



Available settings are explained as follows:

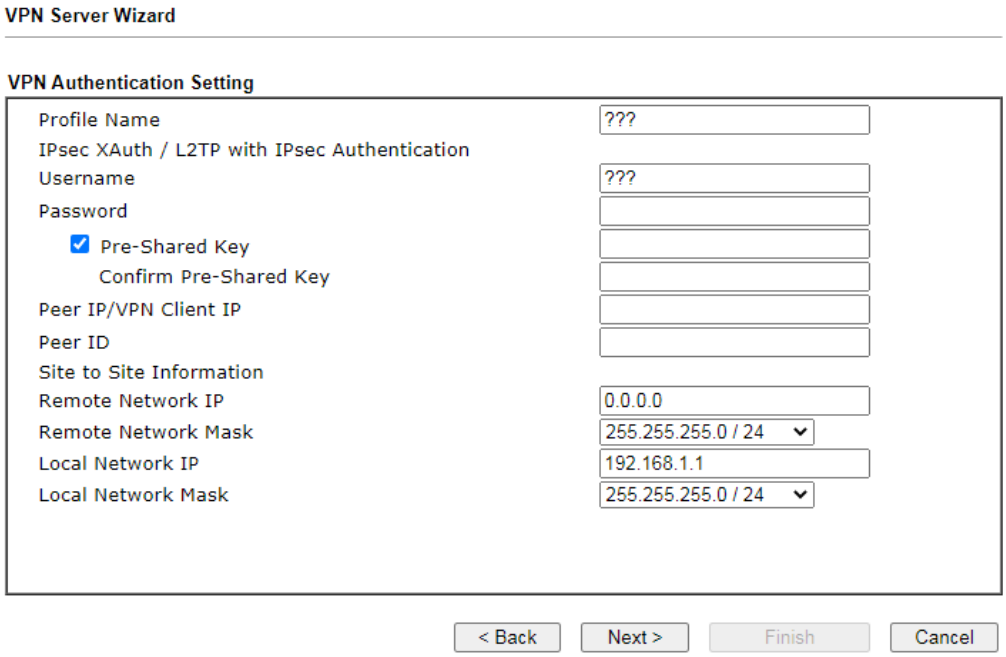
| Item | Description |
|---|---|
| **Profile Name** | Name to identify this VPN profile. |
| **User Name** | Used by the remote LAN to establish a VPN connection. |

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

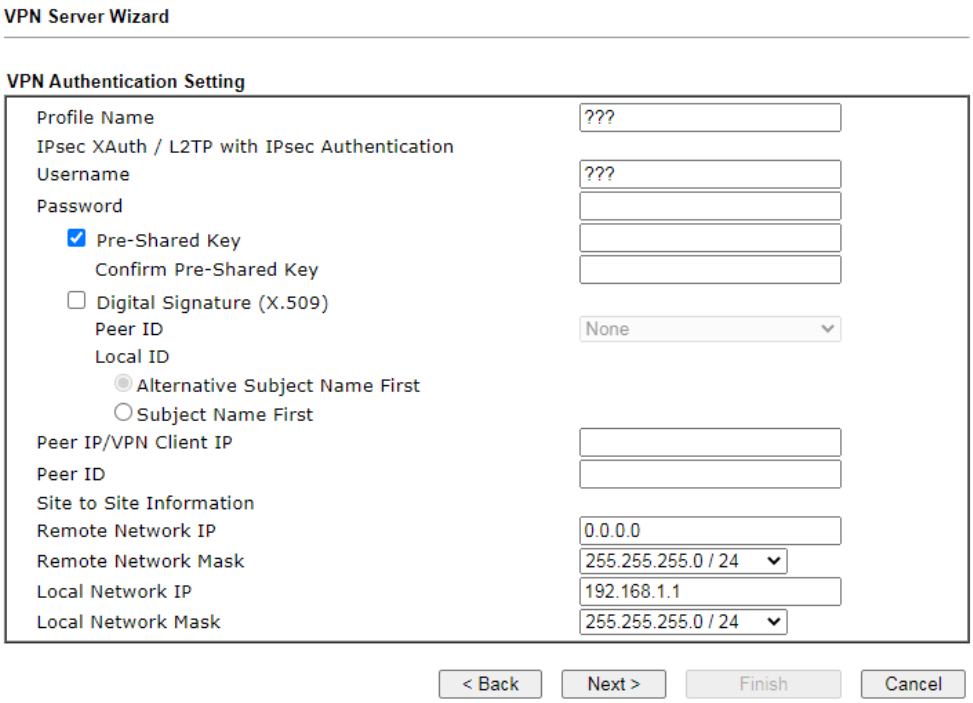
5. The Remote Dial-in User (Teleworker) VPN configuration page appears as follows if you have selected **PPTP/SSL**.




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



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

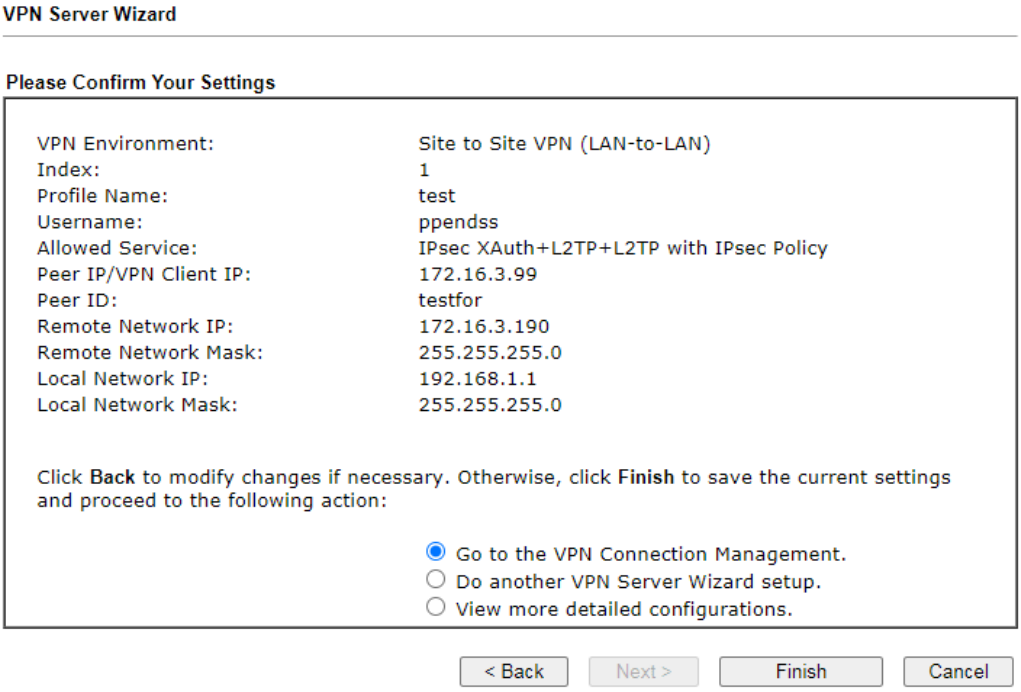



Available settings are explained as follows:

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

| | |
|---|---|
| | specified IP address and/or having the specified Peer ID will be accepted. |
| **Peer ID** | Enter the ID name for the remote client.<br>The maximum length of the peer ID is 47 characters.<br>If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted. |
| **Local Network IP** | Enter the local network IP for TCP / IP configuration. |
| **Local Network Mask** | Enter the local network mask for TCP / IP configuration. |

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




Available settings are explained as follows:

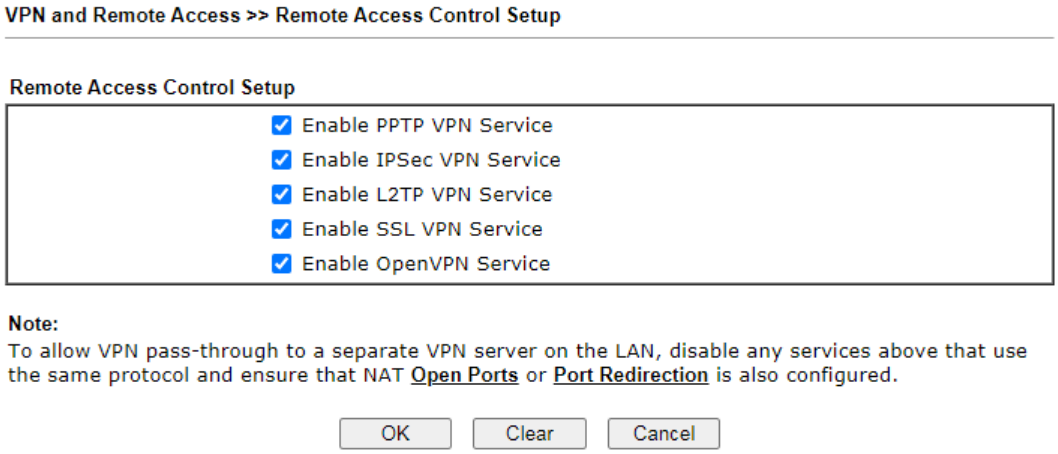
| Item | Description |
|---|---|
| **Go to the VPN Connection Management** | Proceed to **VPN and Remote Access>>Connection Management** to manage VPN sessions. |
| **Do another VPN Server Wizard Setup** | Rerun the VPN Server Wizard to configure another LAN-to-LAN VPN profile. |
| **View more detailed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

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

## IV-1-3 Remote Access Control

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

If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port. Open **VPN and Remote Access>>Remote Access Control**.

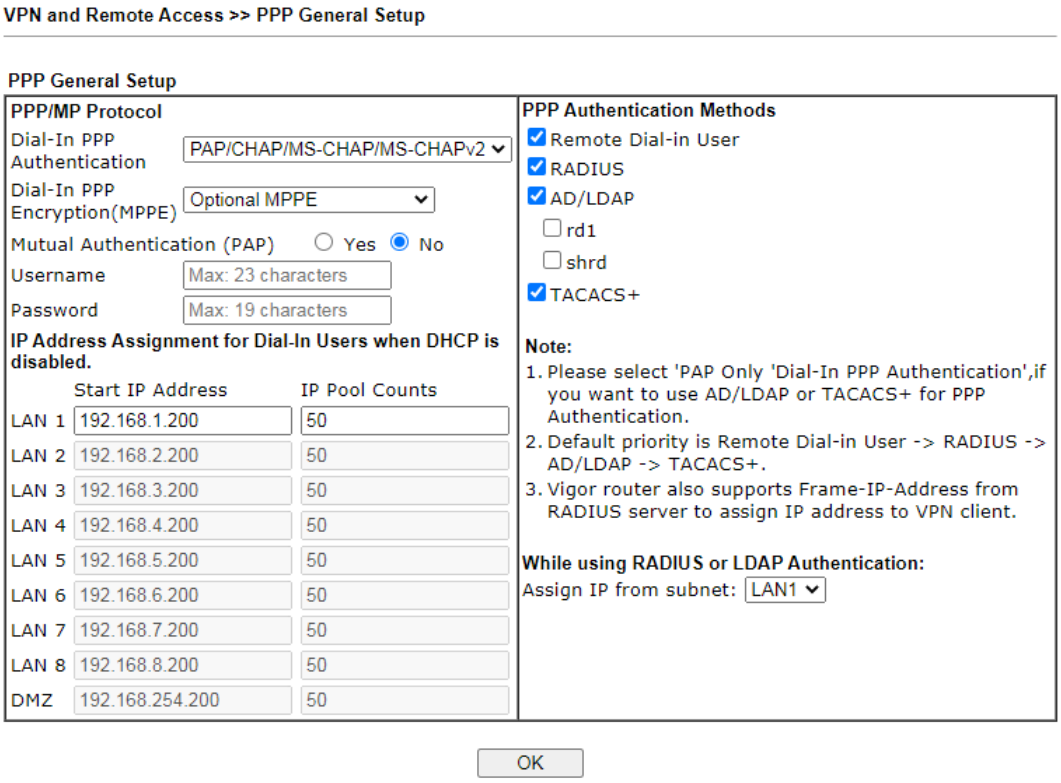



| Item | Description |
|---|---|
| **Enable PPTP VPN Service** | This is the one of the earliest VPN protocols and is natively supported by all Microsoft Windows versions since Windows 95, all Android devices, iOS devices before version 10, and Mac OS X before version 10.12. It is easy to set up, has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

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

## IV-1-4 PPP General Setup

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Dial-In PPP Authentication** | **PAP Only** - Authenticate dial-in users using the PAP protocol only.<br>**PAP/CHAP/MS-CHAP/MS-CHAPv2** - Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP. |
| **Dial-In PPP Encryption (MPPE)** | Specifies if PPP encryption (MPPE) is to be used for dial-in VPN connections.<br>**Optional MPPE** - MPPE is optional. If the VPN client supports MPPE, PPP data will be encrypted.<br>**Require MPPE (40/128bits) -** Require PPP encryption for dial-in VPN connections. Both 40- and 128-bit encryption schemes are allowed. The remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.<br>**Maximum MPPE -** Require 128-bit PPP encryption for all dial-in VPN connections. |
| **Mutual Authentication (PAP)** | Specifies if mutual authentication is to be used. Some VPN peers (e.g., certain Cisco routers) require bi-directional |

| | |
|---|---|
| | authentication used for providing stronger security.<br>When mutual authentication is enabled, Username and Password fields should also be populated using values from the VPN peer. The maximum lengths of these fields are 23 and 19 characters, respectively.<br>**Yes** – Enable mutual authentication.<br>**No** – Disable mutual authentication. |
| **IP Address Assignment for Dial-In Users when DHCP is disabled** | **LAN1** - When the router's DHCP server is disabled, the router will assign IP addresses to dial-in VPN users starting with the IP address specified in Start IP Address. The total number of dial-in VPN IP addresses to be given out is specified in IP Pool Counts.<br>LAN2 ~ LAN8 and DMZ will be available if it is enabled. Refer to LAN>>General Setup for enabling the LAN interface. |
| **PPP Authentication Methods** | The credentials to be used for PPP authentication will be obtained from the selected sources, in the following order:<br>**Remote Dial-in User** – The usernames and passwords in VPN and Remote Access >> Remote Dial-in User section will be used.<br>**RADIUS** – An external RADIUS server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section.<br>**AD/LDAP** – An Active Directory/LDAP server is to be used for authentication. Please be sure to configure AD and LDAP settings in Applications >> Active Directory/LDAP.<br>**TACACS+** – A TACACS+ server is to be used for authentication. Please be sure to set up the RADIUS server in Applications >> RADIUS/TACACS+ section. |
| **PPTP LDAP Profile** | Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.<br>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** | When the dial-in VPN user is authenticated using credentials from the Remote Dial-in User section, an IP address from the LAN specified in the user profile will be assigned. When the user is authenticated using credentials from other sources (RADIUS, AD, TACACS+), the assigned IP address will be drawn from the address pool of the LAN specified here. |

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

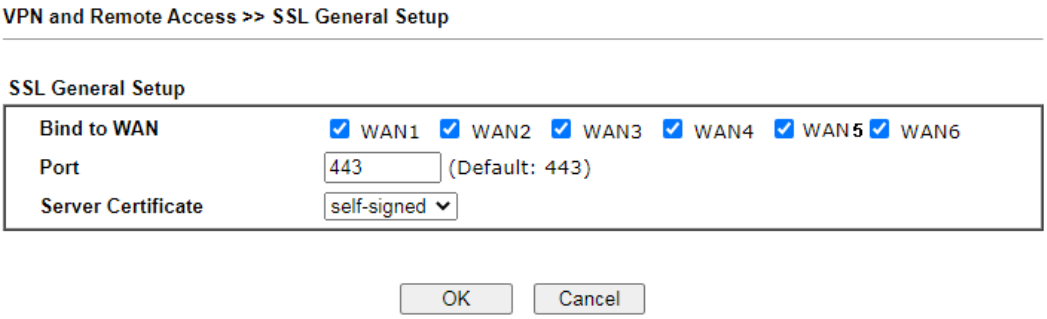
## IV-1-5 SSL General Setup

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

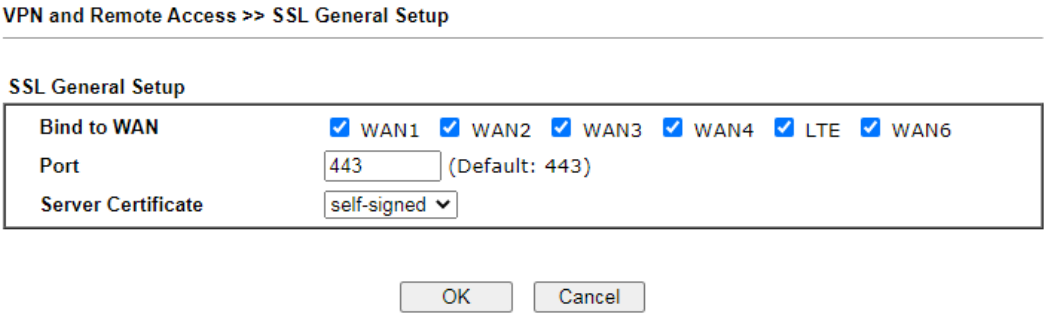
In short,

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

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




or




Available settings are explained as follows:

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

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

## IV-1-6 IPsec General Setup

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

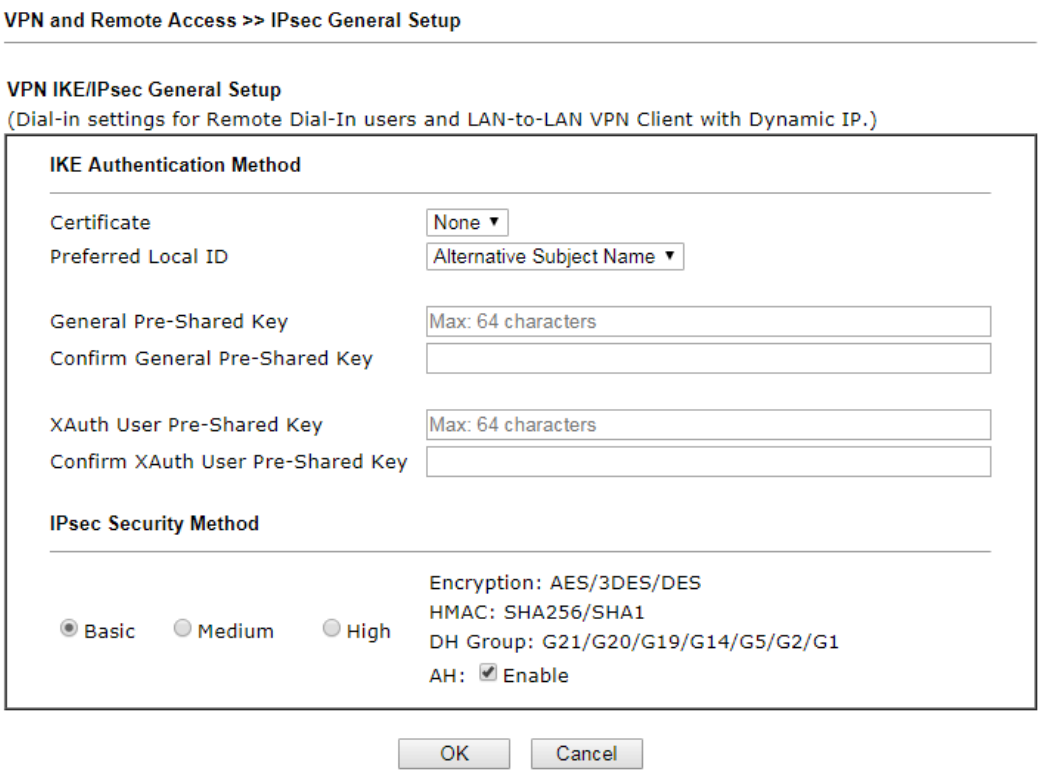
There are two phases of IPsec.

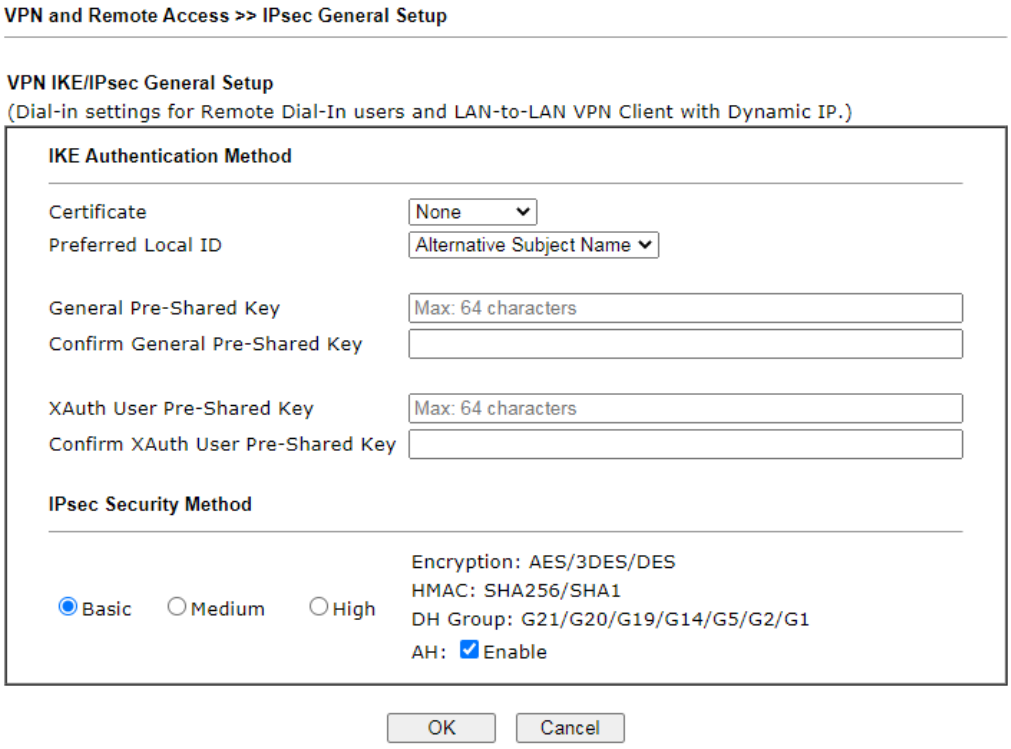
- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies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

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

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

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






Available settings are explained as follows:

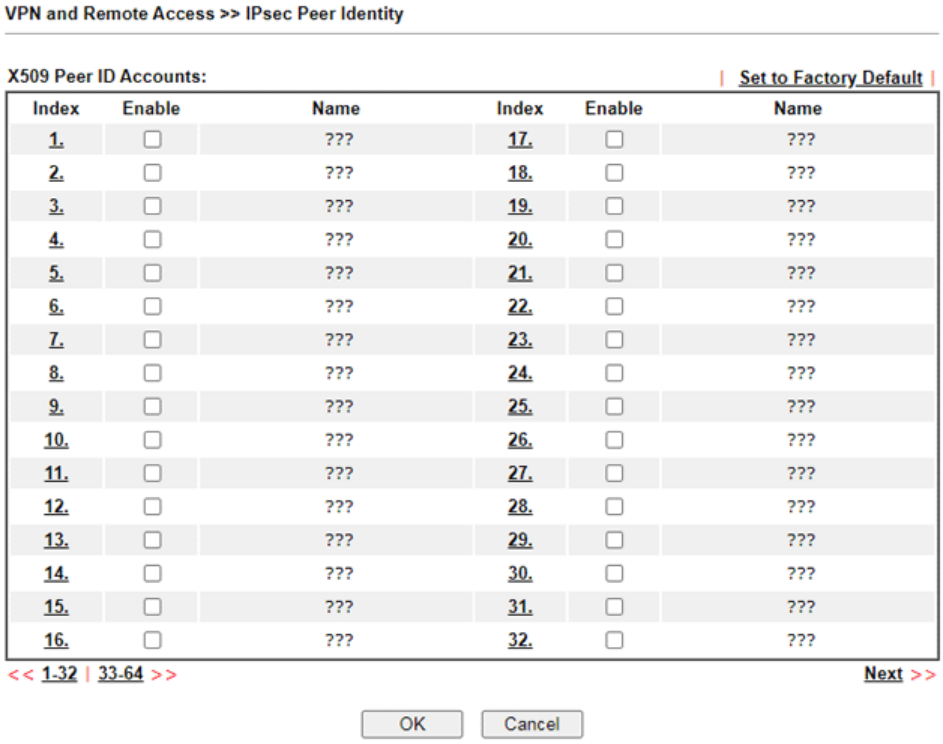
| Item | Description |
|---|---|
| **IKE Authentication Method** | This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, **Certificate (X.509)** and **Pre-Shared Key**.<br>**Certificate** – X.509 certificates can be used for IKE authentication. To set up certificates on the router, go to the Certificate Management section.<br>**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).<br>**General Pre-Shared Key-** Define the PSK key for general authentication.<br>**Confirm General Pre-Shared Key-** Re-enter the characters to confirm the pre-shared key.<br>**XAuth User Pre-Shared Key -** Define the PSK key for IPsec XAuth authentication.<br>**Confirm XAuth User Pre-Shared Key-** Re-enter the characters to confirm the pre-shared key for IPsec XAuth authentication.<br>**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.<br>**Basic -** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.<br>**Medium -** When this option is selected, the Authentication Header (AH) protocol can be used to provide authentication to IPsec traffic.<br>**High** - When this option is selected, the Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security. |

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

# IV-1-7 IPsec Peer Identity

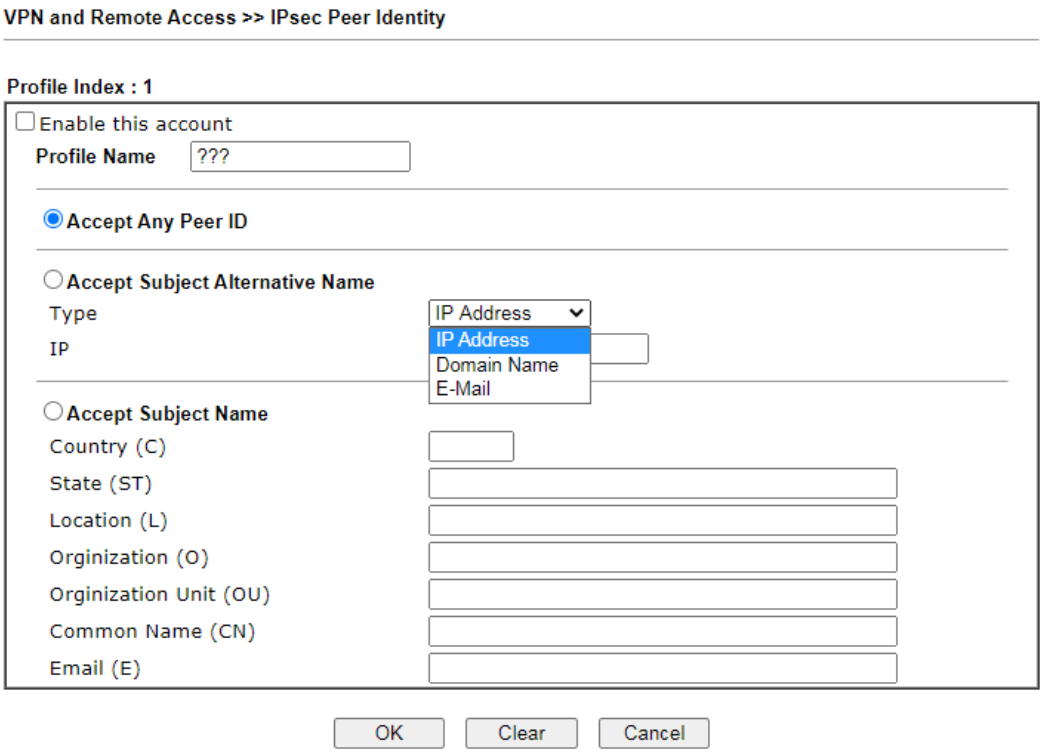
This screen allows creating profiles of subject alternative names (SANs) and distinguished names/subject names that can be used for IPsec peer authentication in LAN-to-LAN or remote user dial-in VPN connections.




Available settings are explained as follows:

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

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



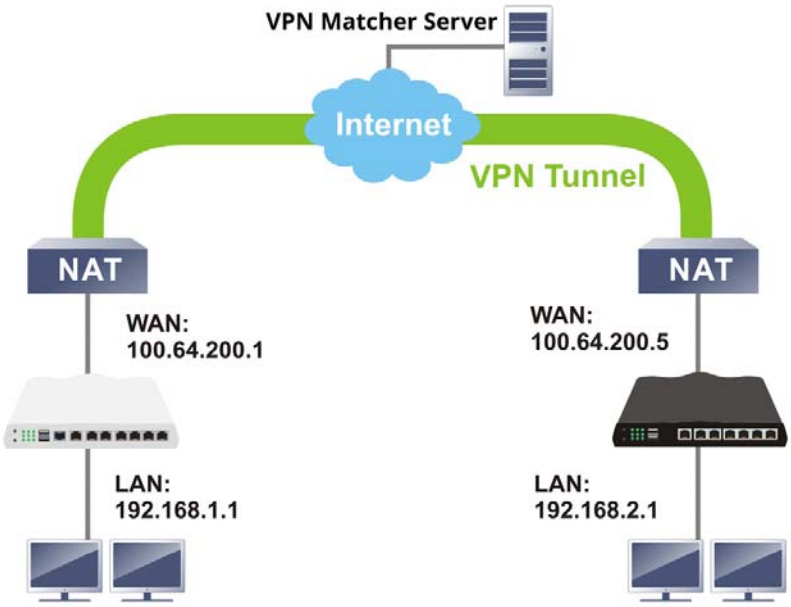

Available settings are explained as follows:

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

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

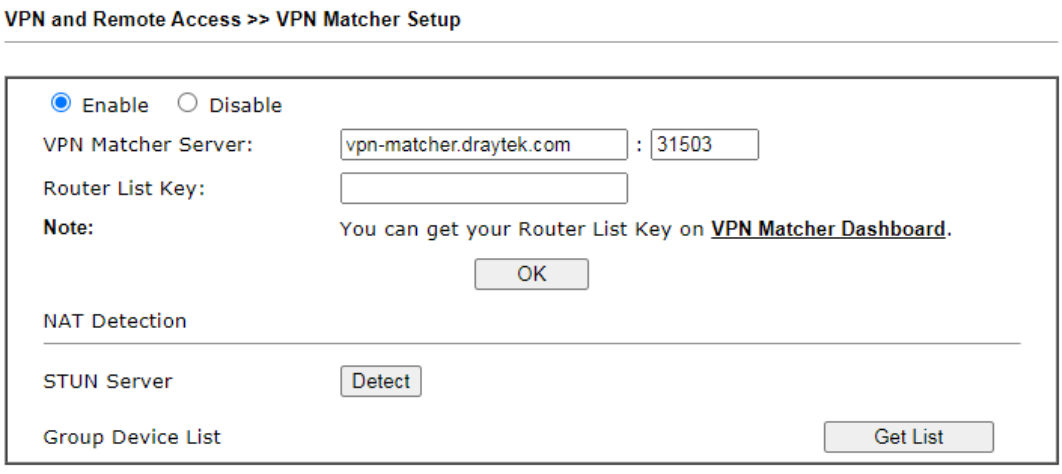
## IV-1-8 VPN Matcher Setup

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




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

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




Available settings are explained as follows:

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

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

## IV-1-9 OpenVPN

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

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

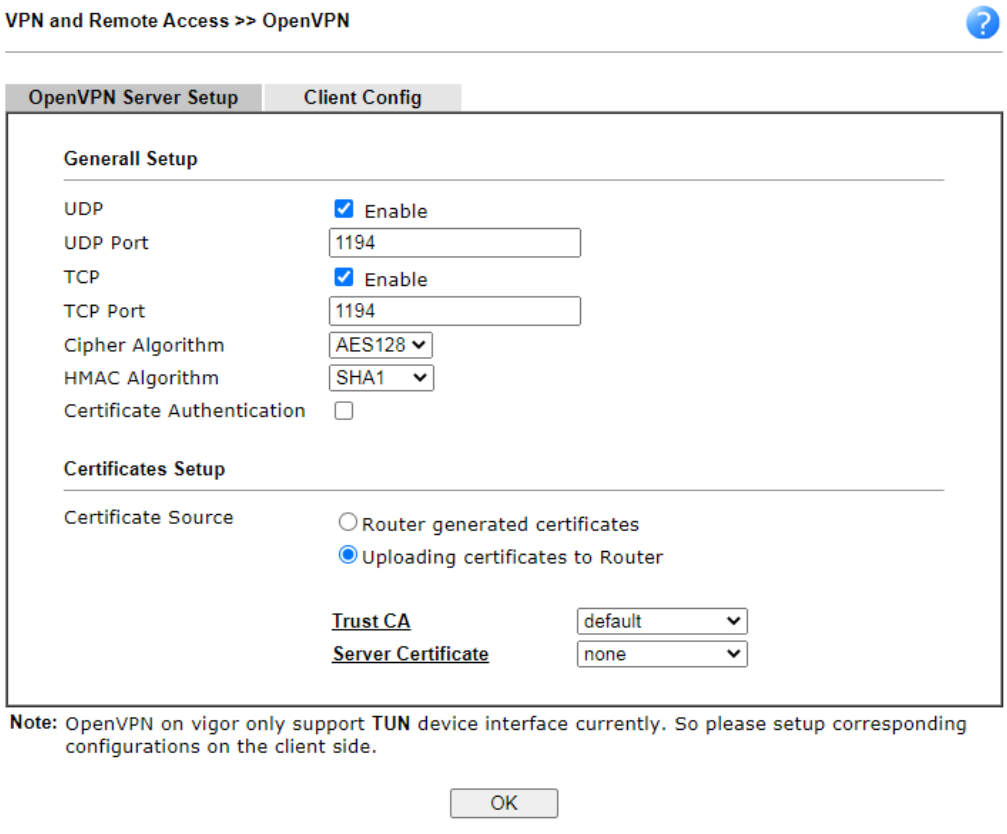
OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

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

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

### IV-1-9-1 OpenVPN Server Setup

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



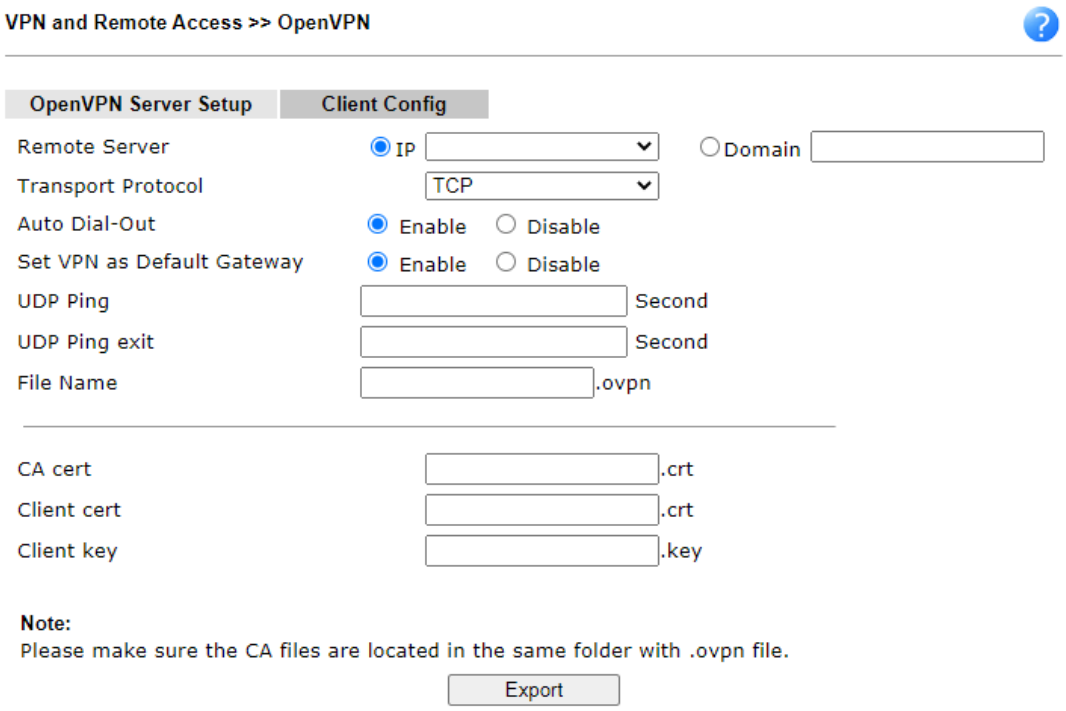
Available settings are explained as follows:

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

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




Available settings are explained as follows:

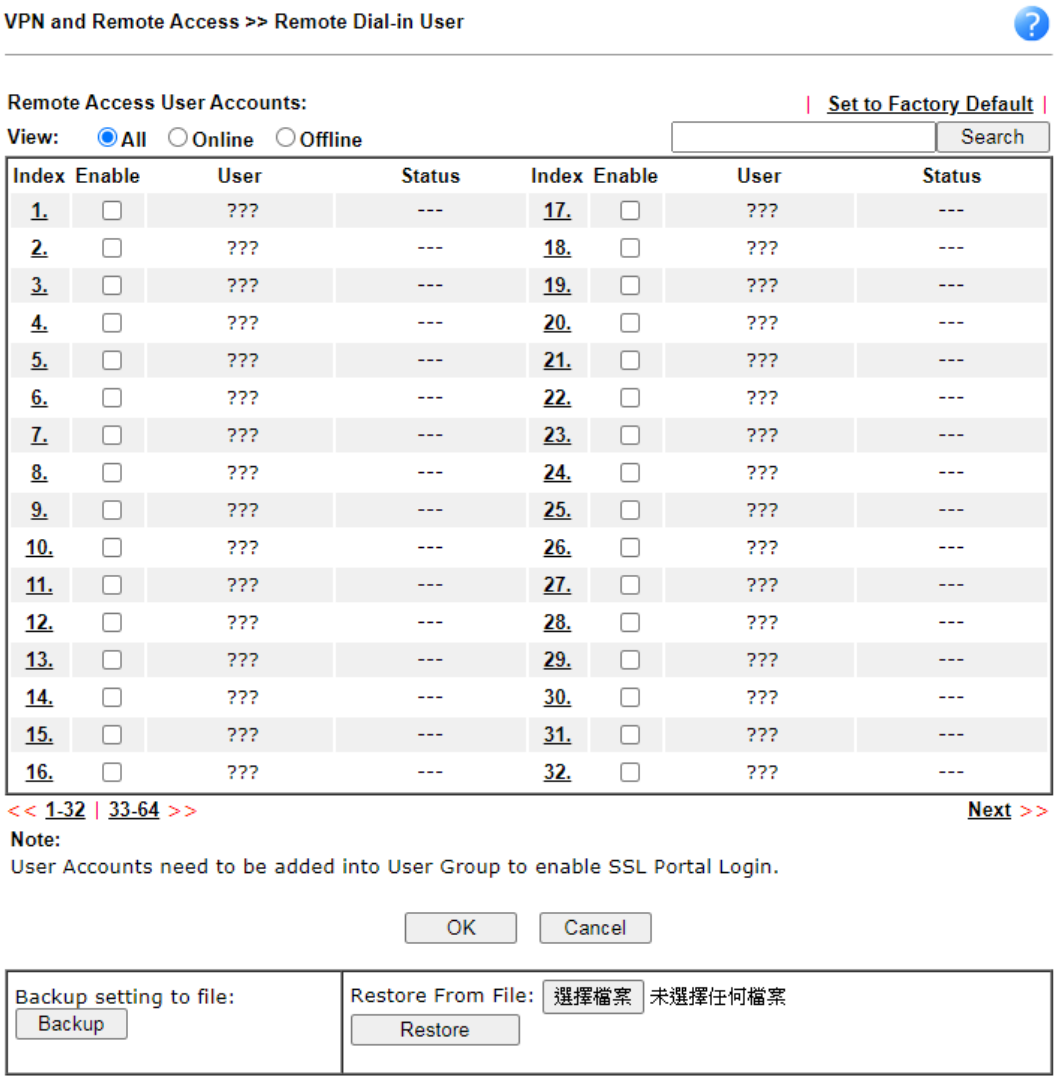
| Item | Description |
|---|---|
| **Remote Server** | The OpenVPN client will use the IP address or domain name to connect to the router. Select either IP or Domain.<br>**IP** – The OpenVPN configuration file will use the numeric IP address as the server address.<br>**Domain** – The OpenVPN configuration file will use the domain as the server address. You need to ensure that the domain resolves to the IP address of a router WAN port. |
| **Transport Protocol** | Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router. |
| **Auto Dial-Out** | **Enable** - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel.<br>**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.<br>**Disable** - Select to disable the function. |
| **File Name** | Enter the filename of the configuration file to be downloaded from the router. |
| **CA cert** | Enter the certificate authority (CA) file name obtained from 3rd party provider. |
| **Client cert** | Enter the filename of the client certificate obtained from 3rd party provider. |

| | |
|---|---|
| **Client key** | Enter the filename of the private key obtained from the 3rd party provider. |
| **Export** | Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections. |

## IV-1-10 Remote Dial-in User

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

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



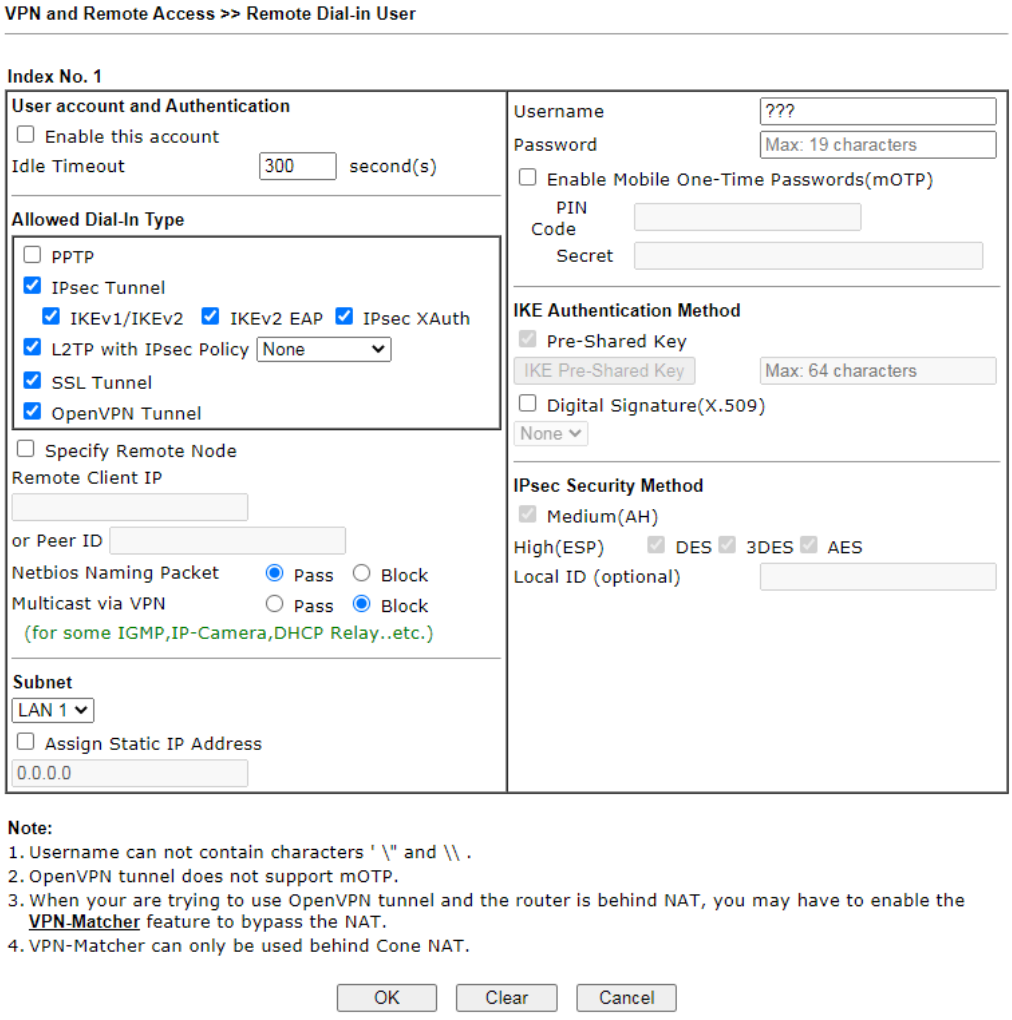

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Click to clear all remote-dial-in user profiles. |
| **Index** | Click the index number of the profile the view or edit its settings. |
| **Enable** | Check to enable the user profile. |
| **User** | Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty. |
| **Status** | Shows the LAN subnet and IP address assignment method. Example: LAN1-DHCP means that the IP address of the VPN |

| | |
|---|---|
| | connection will be drawn from the DHCP pool of the LAN1 subnet.<br>The color of the status indicates the current state of the profile:<br>Green – Profile is being used by a dial-in VPN connection.<br>Red – Profile is not being used.<br>Black – Profile is disabled. |
| **Backup** | Click **Backup** to save the configuration. |
| **Restore** | Click **Select** to choose a configuration file. Then click **Restore** to apply the file. |

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **User account and Authentication** | **Enable this account** - Select to enable this profile to be used by remote dial-in users.<br>**Idle Timeout** - Allowed idle time before the router disconnects the VPN connection. Default timeout value is 300 seconds. |

| | |
|---|---|
| **Allowed Dial-In Type** | Select all VPN protocols allowed for this profile.<br>For L2TP, specify how IPsec should be applied. Options are:<br>● **None** – IPsec cannot be used with L2TP connections.<br>● **Nice to Have** – IPsec is preferred but not mandatory for L2TP connections.<br>● **Must** – IPsec is required when establish L2TP connections.<br>**Specify Remote Node** - The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified. The router will reject the connection if either of these values are entered in the profile but the remote client does not pass the value, or passes the wrong value.<br>**Netbios Naming Packet -** Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.<br>● **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.<br>● **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.<br>**Multicast via VPN** - Specifies whether to allow multicast packets to traverse through the VPN tunnel.<br>● **Pass** – Click this button to let multicast packets pass through the router.<br>● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. |
| **Subnet** | The VPN client will receive an IP address from the DHCP pool or IP address range specified in IP Address Assignment for Dial-In Users for the selected LAN subnet.<br>**Assign Static IP Address** – Alternatively, a static IP address can be set by selecting the Assign Static IP Address checkbox.<br>**User Name** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the name is limited to 23 characters.<br>**Password** - Used for PPTP, L2TP or SSL Tunnel dial-in type. The length of the password is limited to 19 characters.<br>**Enable Mobile One-Time Passwords (mOTP) -** Select to enable one-time passwords (Mobile-OTP). Enter the PIN Code and Secret. DrayTek's SmartVPN client has built-in support for mOTP. Third-party mOTP clients can be used to generate passwords when using other VPN clients. For more information on mOTP, visit Mobile-OTP's homepage.<br>● **PIN Code** – Enter the code for authentication (e.g, 1234).<br>● **Secret** – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6). |
| **IKE Authentication Method** | **Pre-Shared Key** - This checkbox is available when Remote Client IP or Peer ID is specified. Check the checkbox and click IKE Pre-shared Key to enter an IKE PSK (1~63 characters) that will be used only for this profile.<br>**Digital Signature (X.509) –** To enable authentication using X.509 Peer IDs, check the checkbox then select an X.509 |

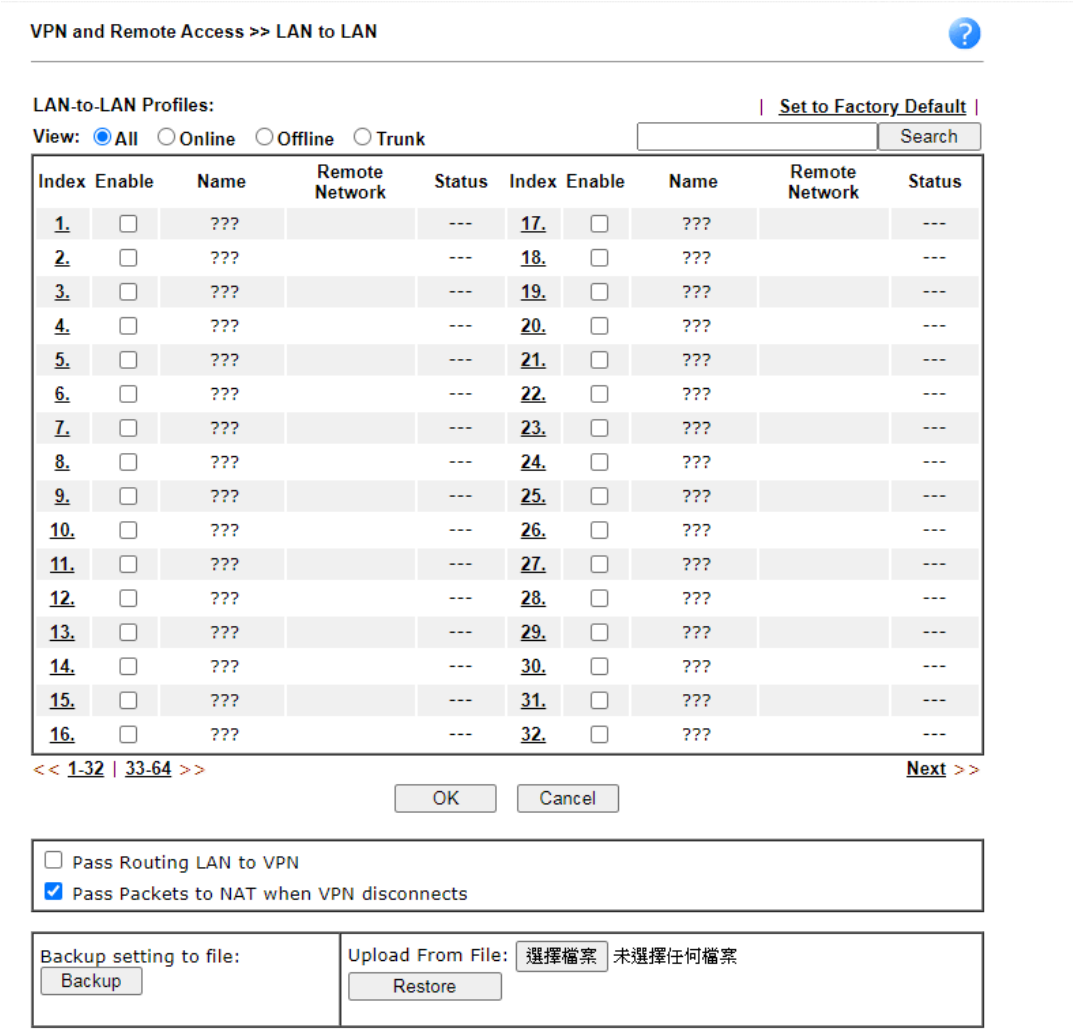
| | |
|---|---|
| | profile. X.509 profiles can be configured in **VPN and Remote Access >> IPsec Peer Identity**. |
| **IPsec Security Method** | Select all the IPsec protocols that are allowed to be used for this profile.<br>**Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.<br>**High (ESP) -** High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.<br>**Local ID (Optional)-** Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode. |

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

# IV-1-11 LAN to LAN

This section allows you to configure up to 64 LAN-to-LAN VPN connections. LAN-to-LAN connections can be configured to allow dial-in only, dial-out only, or both dial-in and dial-out.

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

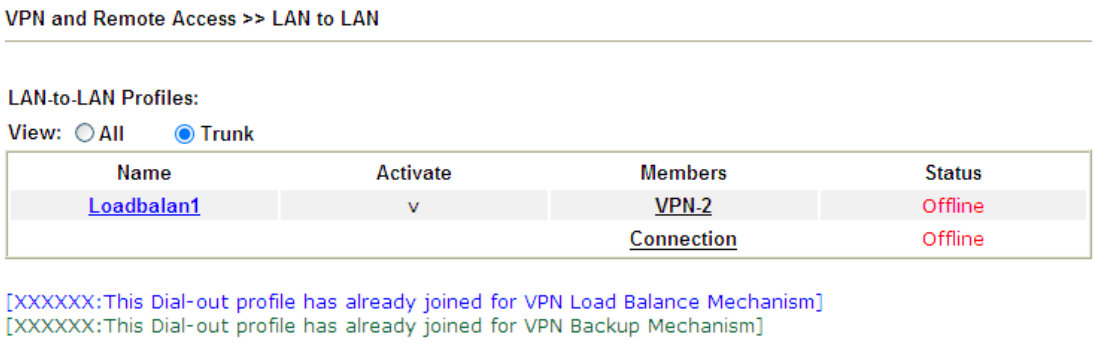



Available settings are explained as follows:

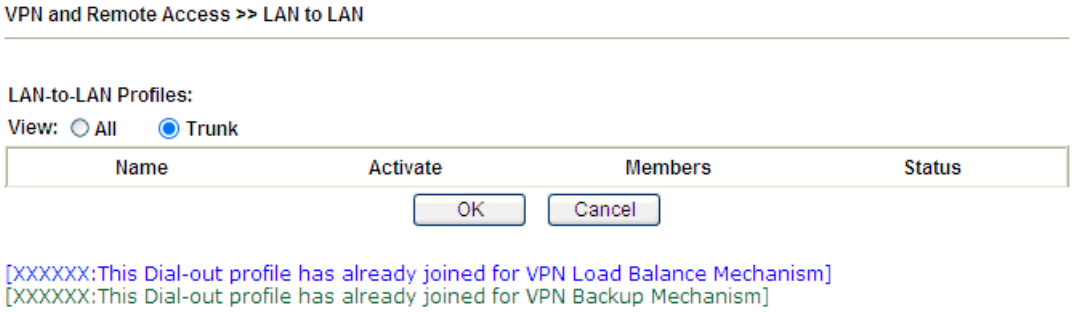
| Item | Description |
|---|---|
| **Set to Factory Default** | Click to clear all indexes. |
| **View** | **All** – Shows all LAN-to-LAN VPN profiles.<br>**Trunk** – Shows all Trunk profiles (see VPN and Remote Access >> VPN TRUNK Management). |
| **Index** | Click the index number of the profile to view or edit its settings. |
| **Enable** | Check to enable the LAN-to-LAN VPN profile. |
| **Name** | Display the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty. |
| **Remote Network** | Display the name of the remote network. |

| | |
|---|---|
| **Status** | Shows the status of the profile.<br>Online – LAN-to-LAN VPN is connected.<br>Offline – LAN-to-LAN VPN is disconnected.<br>--- – Profile is disabled. |
| **Pass Routing LAN to VPN** | If enabled, the packets from routing LAN will pass through the VPN tunnel. |
| **Pass Packets to NAT when VPN disconnects** | If enabled, the packets can pass through via NAT when the VPN disconnects. |
| **Backup** | Click **Backup** to save the configuration. |
| **Restore** | Click **Select** to choose a configuration file. Then click **Restore** to apply the file. |

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

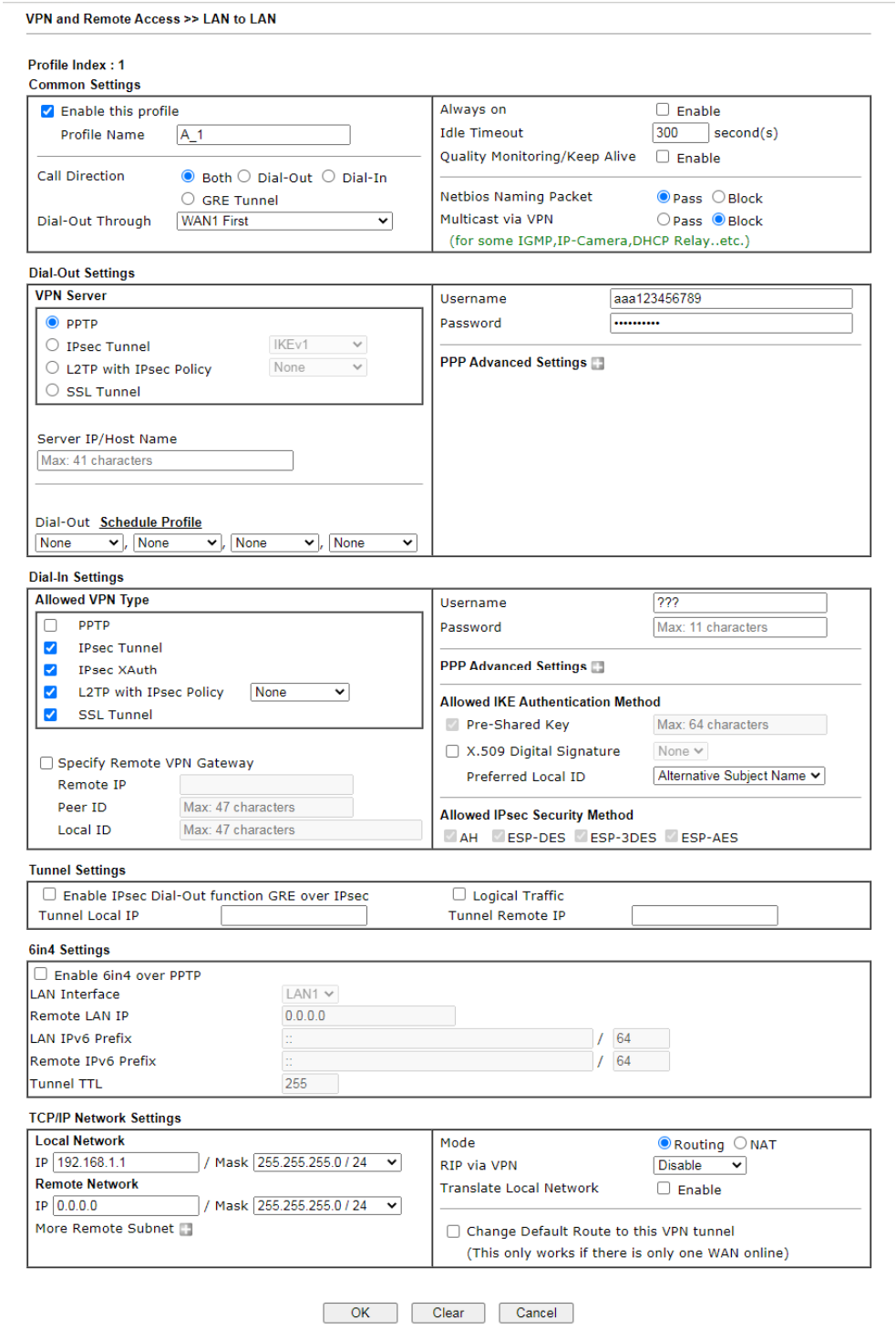



If there is no profile joined yet, this page will be shown as follows:




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

1. The setup screen is shown after a profile index has been clicked. There are 6 sections: Common Settings, Dial-Out Settings, Dial-In Settings, Tunnel Settings, 6in4 Settings and TCP/IP Network Settings.




Available settings are explained as follows:

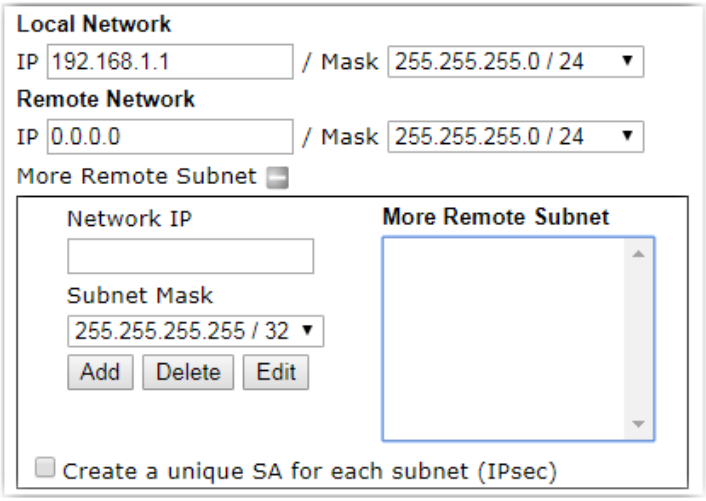
| Item | Description |
|---|---|
| **Common Settings** | **Enable this profile -** Select to enable the profile.<br>**Profile Name -** Specify a name that allows you to identify this profile.<br>**Call Direction -** Specify the allowed call direction of this LAN-to-LAN profile. Four choices are available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

| | |
|---|---|
| | accept (dial in) connections.<br>• **Dial-Out** – Profile is to be used to initiate outgoing connections.<br>• **Dial-In** – Profile is to be used to accept incoming connections.<br>• **GRE Tunnel** – Connection is by means of a GRE tunnel.<br>**Dial-Out Through -** Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.<br>• **WANx First** - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the router will use another WAN interface instead.<br>• **WANx Only or LTE Only** - While connecting, the router will use WANx or LTE as the only channel for VPN connection.<br>• **WAN1 Only: Only establish VPN if WAN2 down** - If WAN2 failed, the router will use WAN1 for VPN connection.<br>• **WAN2 Only: Only establish VPN if WAN1 down** - If WAN1 failed, the router will use WAN2 for VPN connection.<br>**Always On** - Select this option to maintain an always on dial-out connection.<br>**Idle Timeout** - The router will close connection if no activity is observed in the VPN connection for this many seconds. Default value is 300 seconds.<br>**Netbios Naming Packet** - Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel**.**<br>• **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.<br>• **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.<br>**Multicast via VPN -** Specifies whether to allow multicast packets to traverse through the VPN tunnel.<br>• **Pass** – Click this button to let multicast packets pass through the router.<br>• **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. |
| **Dial-Out Settings** | **VPN Server** - Select the VPN protocol to be used**.**<br>**Server IP/Host Name** - IP address or DNS host name of remote VPN host.<br>**Dial-Out Schedule Profile -** Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work.<br>**User Name -** Enter a username for establishing VPN connection.<br>**Password -** Enter the password for establishing VPN connection.<br>**PPP Advanced Settings** - Click it to expand the advanced settings for PPP. |

| | |
|---|---|
| | • **PPP Authentication -** PAP Only – Authenticate dial-in users using the PAP protocol only. PAP/CHAP/MS-CHAP/MS-CHAPv2 – Attempt to authenticate dial-in users using various CHAP protocols, and if the remote VPN client fails to authenticate, fall back to PAP.<br>• **VJ compression -** Specifies whether to enable Van Jacobson (VJ) header compression, which improves throughput on slow connections.<br>• **Request IP Address** - Enter the IP address. |
| **Dial-In Settings** | **Allowed VPN Type -** Select permissible VPN protocols for dial-in connections.<br>• **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.<br>• **IPsec Tunnel-** Allow the remote dial-in user to trigger an IPsec VPN connection through Internet.<br>• **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:<br>▪ **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.<br>▪ **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.<br>▪ **Must -** Specify the IPsec policy to be definitely applied on the L2TP connection.<br>• **SSL Tunnel-** Allow the remote dial-in user to trigger an SSL VPN connection through Internet.<br>**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.<br>If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings.<br>**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.<br>**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.<br>**PPP Advanced Settings** - Click it to expand the advanced settings for PPP.<br>• **VJ Compression -** Specifies whether to enable Van Jacobson header compression, which improves throughput on slow connections.<br>• **Assign Peer IP Address** - Enter the IP address of the peer.<br>**Allowed IKE Authentication Method -** This section is |

| | |
|---|---|
| | available when IPsec tunnel is selected as the dial-out protocol. Available options are IKE Pre-shared key and X.509 digital signature.<br>● **Pre-Shared Key** - To use a pre-shared key, select this radio-button and then click the IKE Pre-Shared Key button to enter the PSK.<br>● **X.509 Digital Signature** - To use an X.509 digital signature, select this radio button and then select an X.509 IPsec Peer Identity profile. To enable authentication using X.509 Peer IDs. X.509 profiles can be configured in **VPN and Remote Access >> IPsec Peer Identity**.<br>**Local ID** – Select whether to first match Subject Alternative Name or Subject Name during authentication.<br>● **Alternative Subject Name** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.<br>● **Subject Name** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.<br>**Allowed IPsec Security Method** - This setting is available when IPsec Tunnel is selected as the dial-out protocol.<br>● **AH-** Authentication Header (AH) means data will be authenticated, but not be encrypted. Select to use Authentication Header protocol. By default, this option is active.<br>● **ESP-DES/ESP-3DES/ESP-AES -** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. |
| **Tunnel Settings** | **Enable IPsec Dial-Out function GRE over IPsec**: Check this box to verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.<br>**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.<br>**Tunnel Local IP**: Enter the virtual IP for router itself for verified by peer.<br>**Runnel Remote IP**: Enter the virtual IP of peer host for verified by router. |
| **6in4 Settings** | Transmit the IPv6 packets from the local site to the remote site via IPv4 VPN tunnel with the encapsulation technology, 6in4.<br>**Enable 6in4 over PPTP -** Check to enable the function. The |

| | |
|---|---|
| | IPv6 packets can pass through WAN PPTP VPN tunnel to the remote site.<br><br>**LAN Interface -** Specify a LAN interface for transmitting the packets.<br><br>**Remote LAN IP -** Specify the IP address of the remote site.<br><br>**LAN IPv6 Prefix -** Specify the prefix (with length) of the local site.<br><br>**Remote IPv6 Prefix -** Specify the prefix (with length) of the remote site.<br><br>**Tunnel TTL -** Enter a value. |
| **TCP/IP Network Settings** | This section configures the whether the local router applies NAT when linking the local network to the remote network, and whether IP address translation occurs when.<br><br>The view changes depending on the setting of the field From first subnet to remote network, you have to do. Select NAT if the remote VPN server expects only one IP address on the local network; otherwise, select Route. TCP/IP Network Settings has different settings depending on whether NAT or Route mode is selected.<br><br>**Local Network –** The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.<br><br>● **IP / Mask -** Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.<br><br>**Remote Network -** The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.<br><br>● **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.<br><br>**More Remote Subnet** - Click to bring up a dialog box to enter additional static routes for subnets destined for the remote network. |




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

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

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

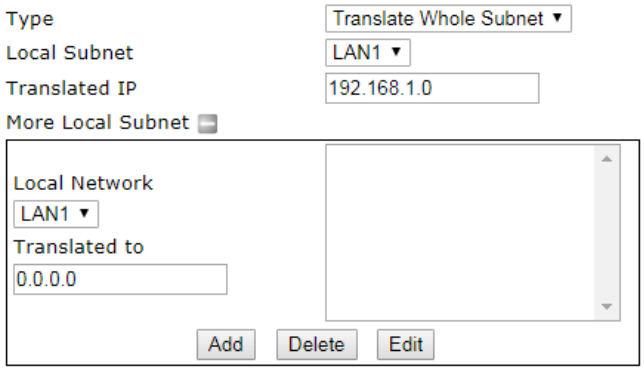
**When the Mode is set to Routing**

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

**Translate Local Network** - Check the box to enable the function. Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

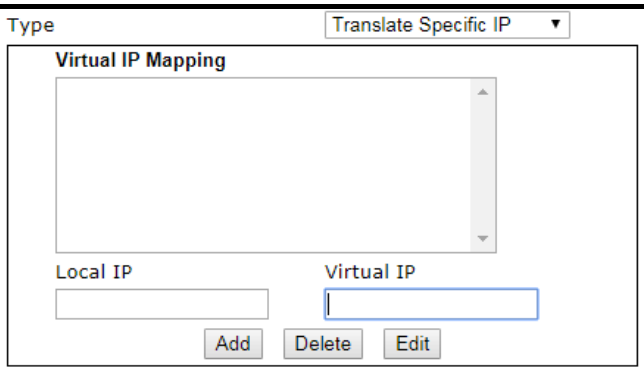
- **Type** - There are two types (**Translate Whole Subnet**, **Translate Specific IP**) for you to choose.

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




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

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

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

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

## IV-1-12 VPN Trunk Management

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

### VPN Backup

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

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

### VPN Load Balance

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

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

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

### Creating a VPN Trunk

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

VPN and Remote Access >> VPN TRUNK Management

**Backup Profile List** | Set to Factory Default |

**Note:**
[Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

| No. | Status | Name | Member1 (Active) | Type | Member2 (Active) | Type |
|---|---|---|---|---|---|---|

Advanced ▼

**Load Balance Profile List** | Set to Factory Default |

**Note:**
[Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

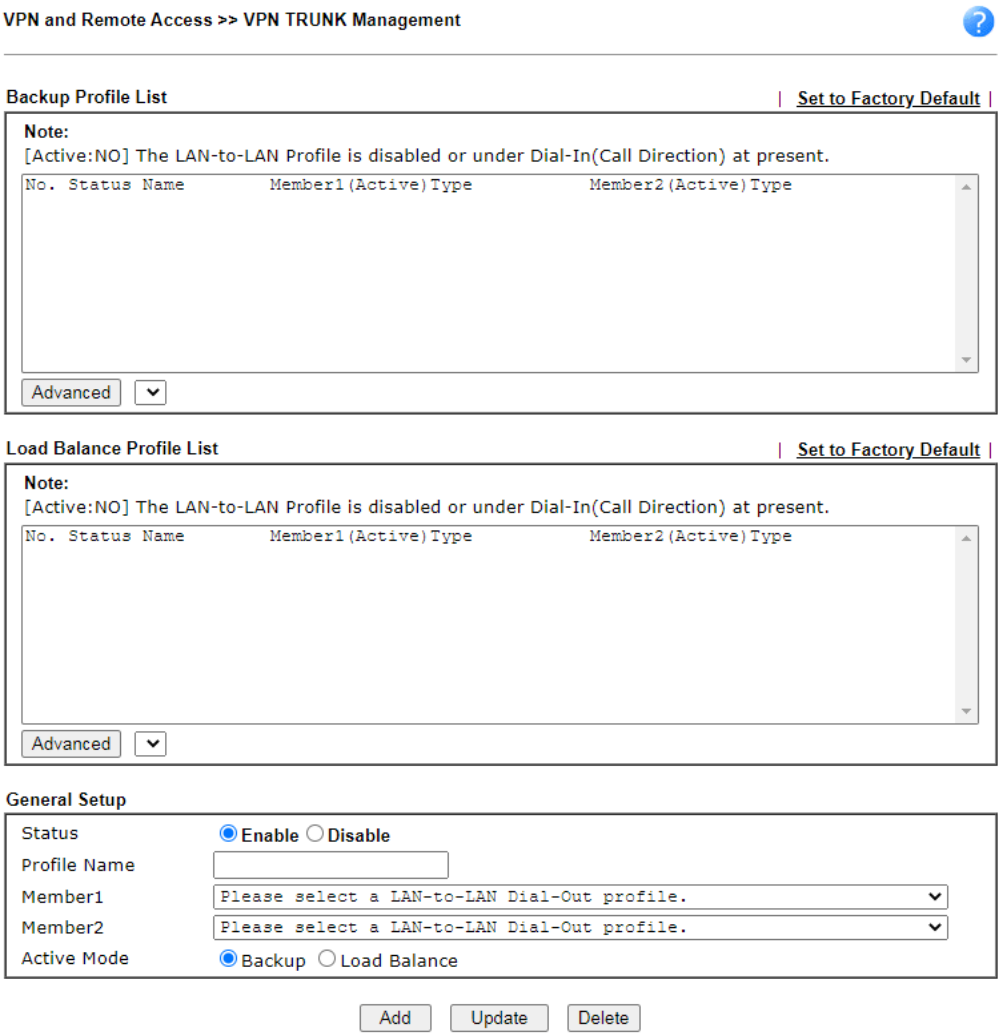
| No. | Status | Name | Member1 (Active) | Type | Member2 (Active) | Type |
|---|---|---|---|---|---|---|

Advanced ▼

**General Setup**

| | |
|---|---|
| Status | Enable Disable |
| Profile Name | |
| Member1 | Please select a LAN-to-LAN Dial-Out profile. |
| Member2 | Please select a LAN-to-LAN Dial-Out profile. |
| Active Mode | Backup Load Balance |

Add Update Delete

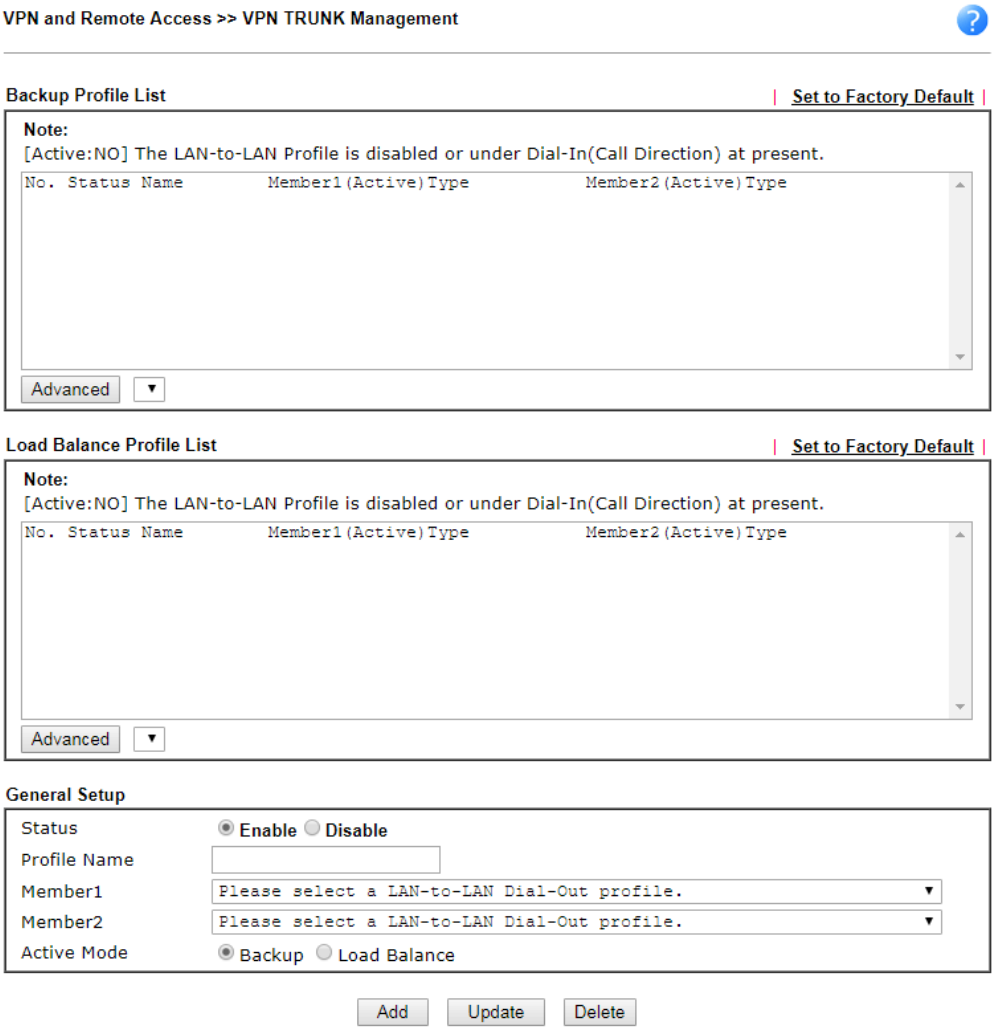



Available settings are explained as follows:

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

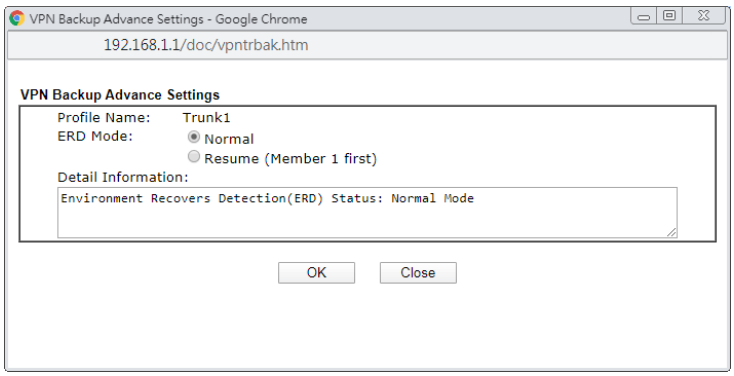
## Configuring, Modifying or Deleting a VPN Trunk

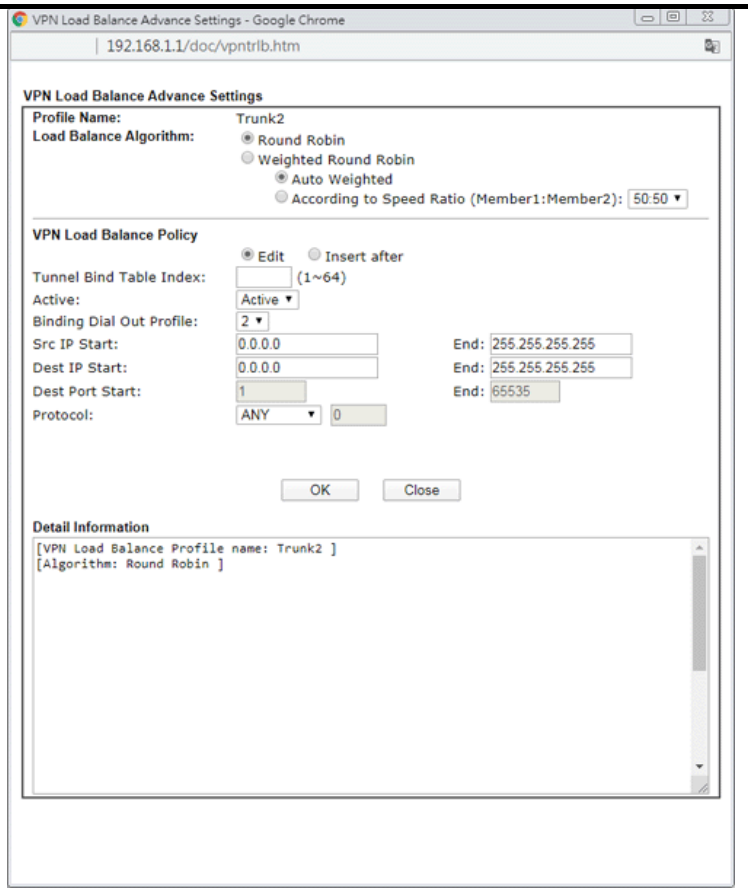
To configure or modify a VPN Trunk, go to the Profile List section that corresponds to the type of the VPN trunk (Backup or Load Balance).




Available settings are explained as follows:

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

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




**Profile Name** - User-defined name that identifies this profile.

**Load Balance Algorithm** - Configures how load balancing is performed.

- **Round Robin** – All outgoing connections that do not match to any load balance policy are evenly distributed between the tunnels.
- **Weighted Round Robin** -- All outgoing connections that do not match to any load balance policy are distributed between the tunnels based on a ratio that is either automatically determined by the router (Auto Weighted), or specified by the user (According to Speed Ratio).

**VPN Load Balance Policy** - This section allows the modification or addition of load balance policy profiles.

**Edit / Insert After** - Select Edit to modify the existing load balance profile with index specified in Tunnel Bind Table Index, or Insert After to insert a new load balance profile immediately after the index position specified in Tunnel Bind Table Index.

**Tunnel Bind Table Index**- 64 Binding tunnel tables are provided by this device. In Edit mode, the profile that matches this index will be updated.

In Insert After mode, a new profile will be inserted immediately after the policy having this index.

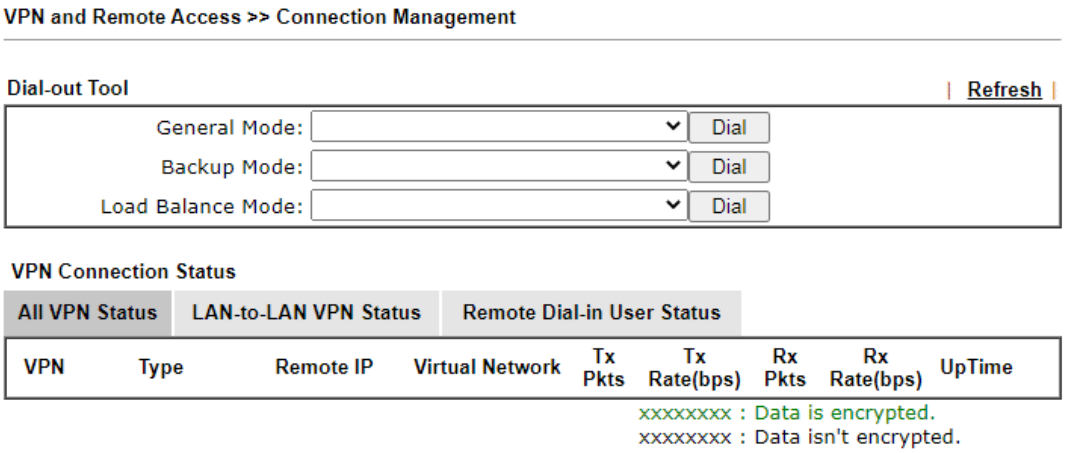
**Active** – Includes Active and Clear. In which,

- **Active** - All information will be saved into a load balance profile.
- **Clear** – The profile with index matching Tunnel Bind

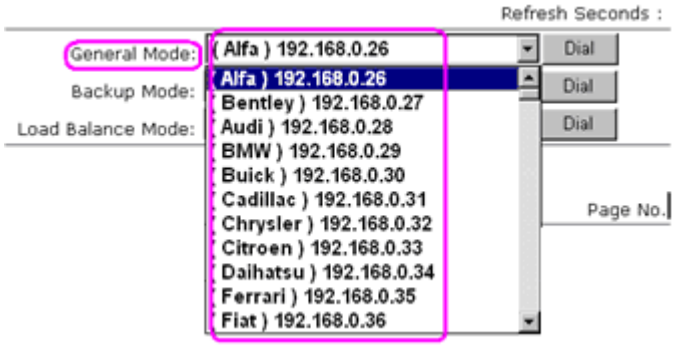
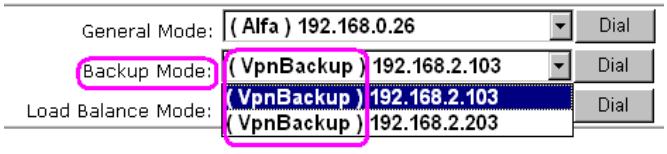
| | |
|---|---|
| | Table Index will be deleted.<br>**Binding Dial Out Profile** – The LAN-to-LAN VPN tunnel to which traffic matching this policy will be sent.<br>**Scr IP Start /End**– Specify source IP addresses as starting point and ending point.<br>**Dest IP Start/End** – Specify the target IP addresses as starting point and ending point.<br>**Dest Port Start /End**– Specify the target port range if the protocol is TCP or UDP.<br>**Protocol** – Specify the protocol of the traffic.<br>**Detail Information** - Shows all the information about the Load Balance profile.<br>To save Advanced Settings for the profile, select **OK**; to close without saving changes, select **Close**. |
| **Add** | Select it to add a VPN Trunk Profile using the entered information. |
| **Update** | Make modifications as necessary in the General Setup section.<br>Select it to save the changes to the Status (Enable or Disable), profile name, member1 or member2. |
| **Delete** | Select it to remove the VPN TRUNK profile.<br>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. |

## IV-1-13 Connection Management

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




Available settings are explained as follows:

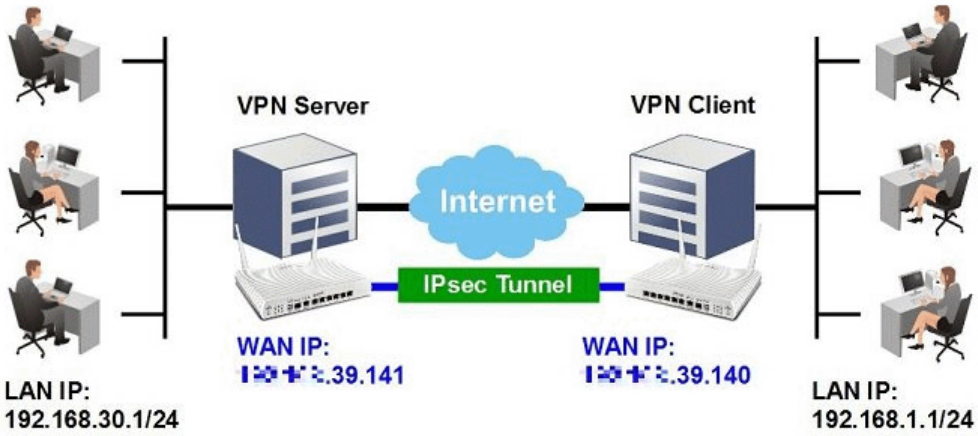
| Item | Description |
|---|---|
| **Refresh** | Click to manually reload the page to refresh VPN connection information. |
| **Dial-out Tool** | The Dial-out Tool section can be used to initiate outgoing LAN-to-LAN VPN sessions.<br>**General Mode -** It lists all LAN-to-LAN VPN profiles that do not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

| | |
|---|---|
| | **Load Balance Mode -** It lists all Load Balance VPN Trunk profiles. To manually dial a Load Balance VPN Trunk profile, select it from the combo box, and click the **Dial** button to the right.<br>**Dial -** Click this button to execute dial out function. If the connect is successfully made, it will show up in the VPN Connection Status section below. |
| **VPN Connection Status** | **VPN** - Displays the VPN profile number and the profile name.<br>**Type** - Displays the VPN protocol used for the connection<br>**Remote IP** - Displays the remote IP address of the VPN connection.<br>**Virtual Network** - Displays the IP subnet used by the VPN connection.<br>**Tx Pkts** - Displays the number of packets that have been transmitted through the VPN connection.<br>**Tx Rate(Bps)** - Displays the current upstream speed of the VPN connection.<br>**Rx Pkts** - Displays the number of packets that have been received through the VPN connection.<br>**Rx Rate(Bps)** - Displays the current downstream speed of the VPN connection.<br>**UpTime** - Displays the elapsed time of the VPN connection.<br>**Drop** - Click this button to disconnect this VPN connection. |

# Application Notes

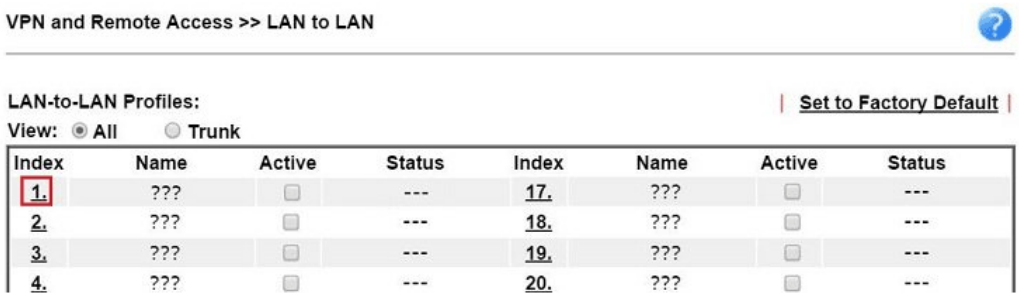
## A-1 How to Build a LAN-to-LAN VPN Between Vigor Routers via IPsec Main Mode

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.

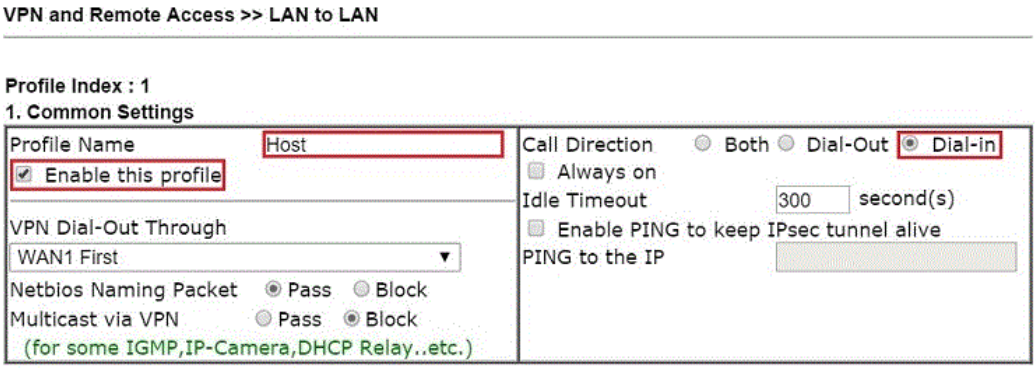



### VPN Server (Dial-In Site) Setup

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.



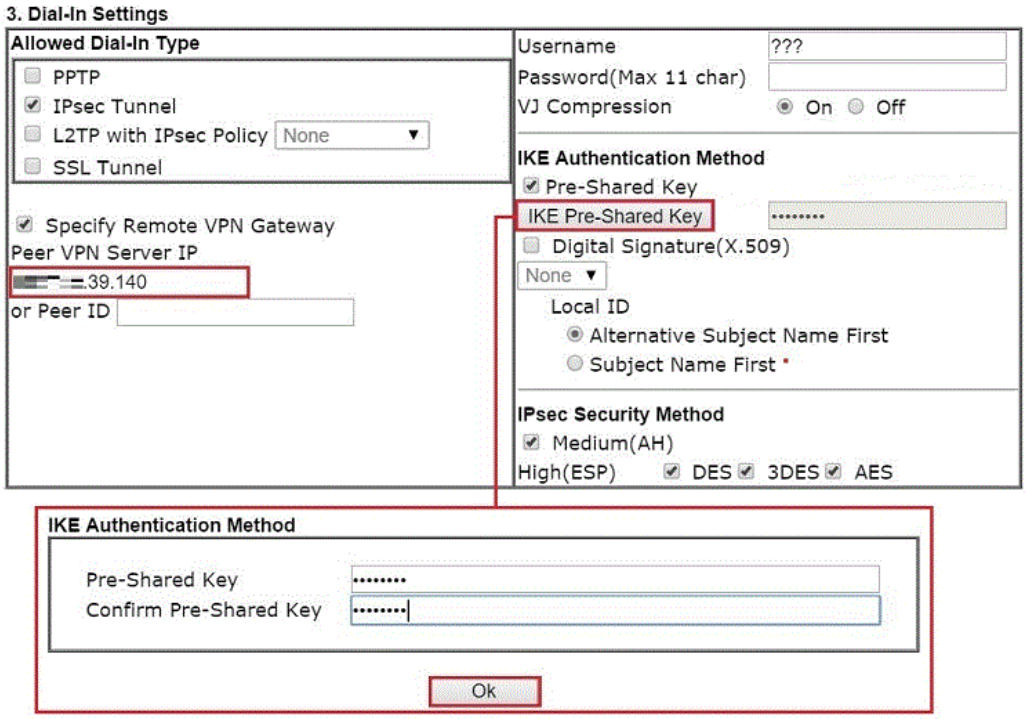

In Common Settings,

(a) Enter the **Profile Name**.

(b) Enable this profile.

(c) Set **Call Direction** to **Dial-in**.

In Dial-In Setting,



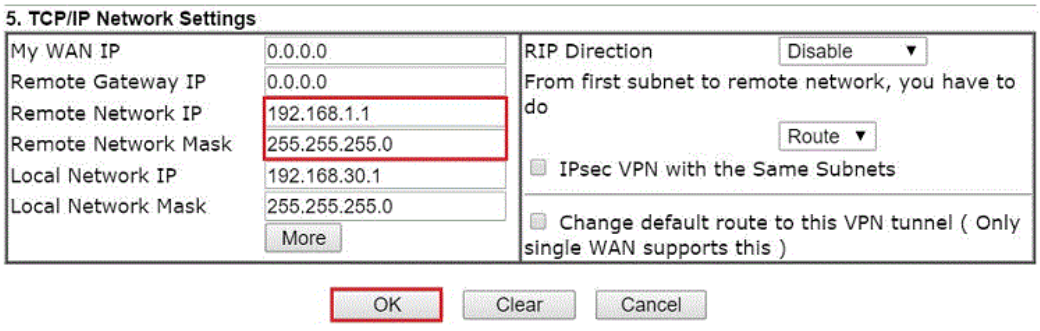

(d) Make sure Allowed Dial-in Type has **IPsec Tunnel** enabled.

(e) Enable S**pecify 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.

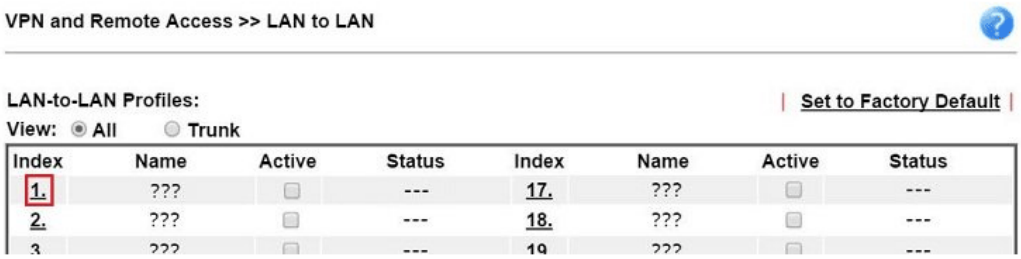
(g) Select the **IPsec Security Method** that are allowed to use.

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.



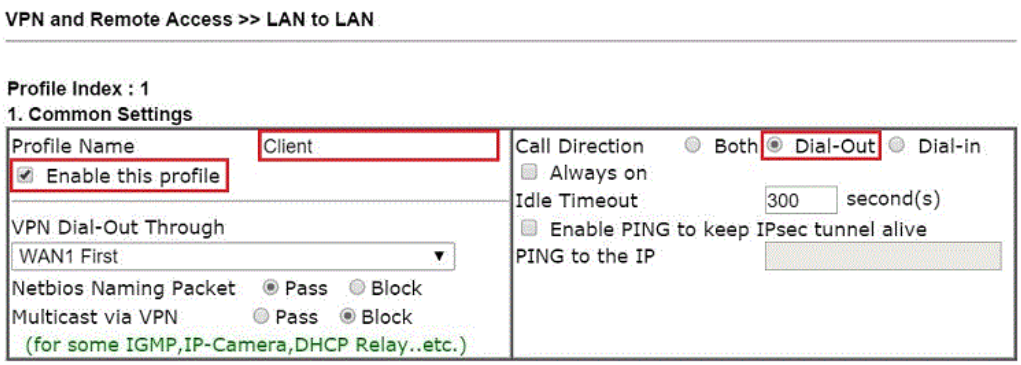
## VPN Client (Dial-out Site) Setup

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,

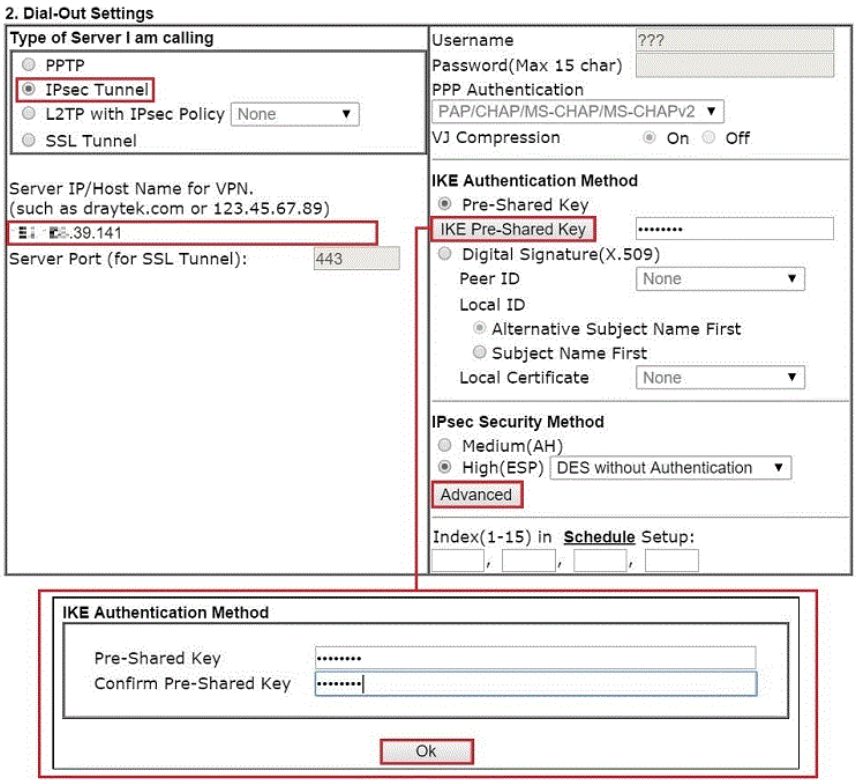



   (a) Enter a **Profile Name**.

   (b) Enable this profile.

   (c) Set **Call Direction** to **Dial-Out**.

   In Dial-out Setting,



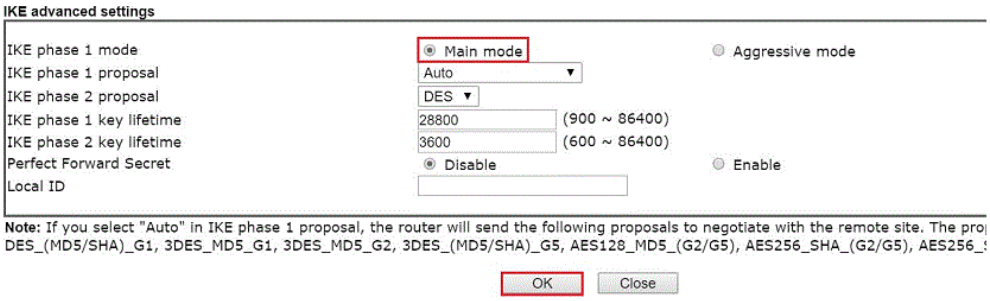

(d) Select **IPsec Tunnel** for **Type of Sever I am Calling**.

(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,

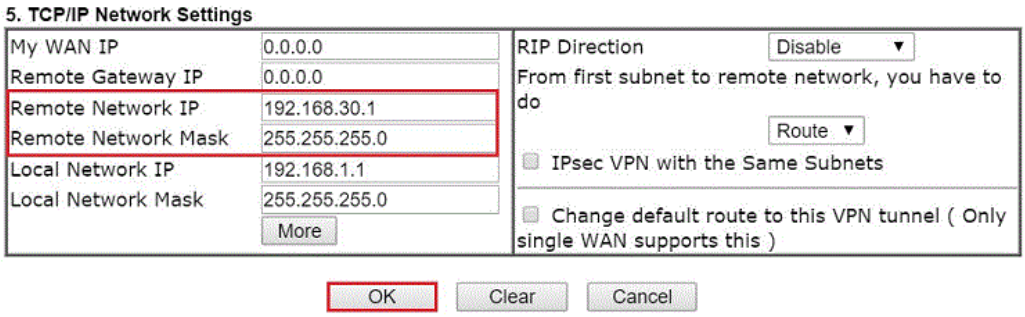



(h) Select **Main Mode** for IKE phase 1 mode.

(i) Make sure phase 1 and phase 2 proposal are using the security methods which are accepted by VPN server.

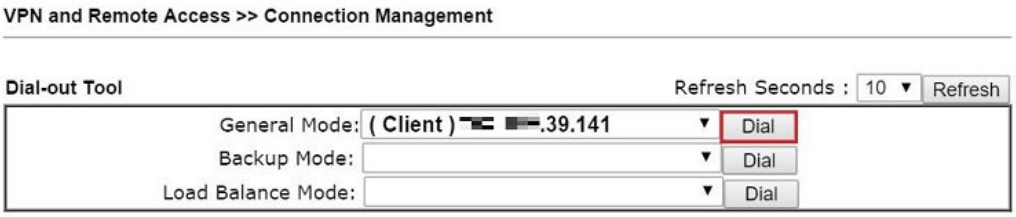
(j) Click **OK** to save.

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**.

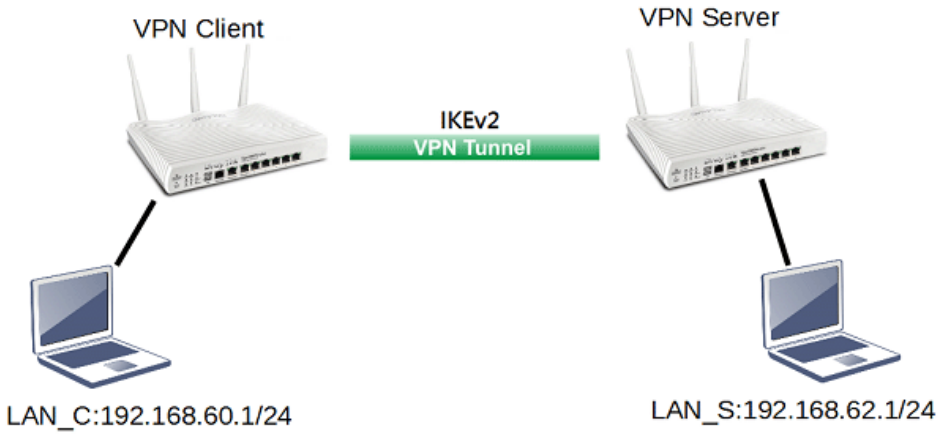



If all the settings are matched, the VPN will be established, and the statistics will be displayed on the same page.

## A-2 How to Build a LAN-to-LAN VPN Between Vigor Routers via IKEv2

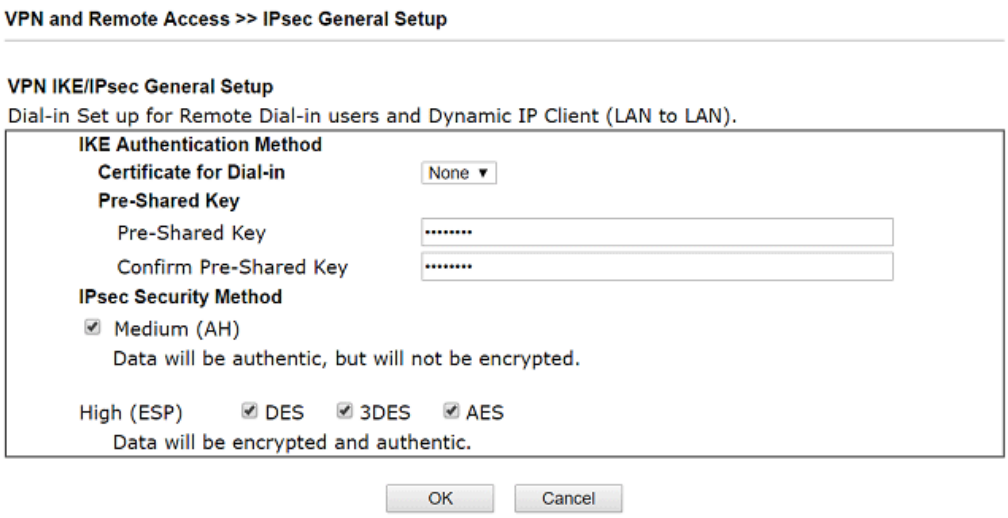
Modified from the previous version IKEv1, IKEv2 is a new VPN protocol and has lots of improvements then the former. It is more stable, more secure and faster connection establishing speed. Support newer and more complicated secure ciphers to make the connection more secure. Using new connection progress 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

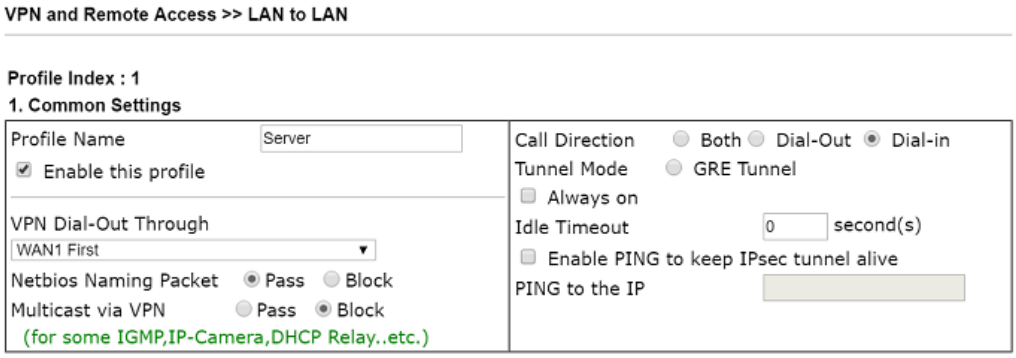
1. Go to **VPN and Remote Access >> IPsec General Setup**.




   (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**.

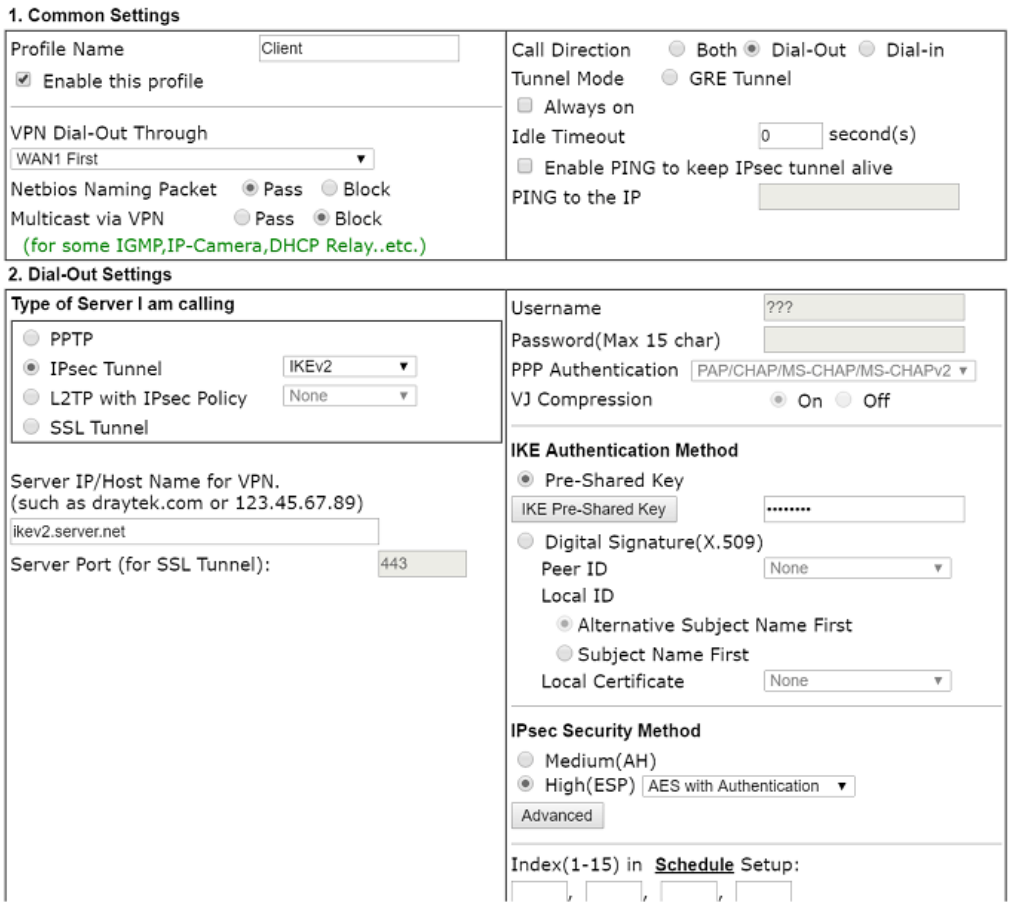
(c) Allow **IPsec Tunnel** in Dial-In Settings.

(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**.

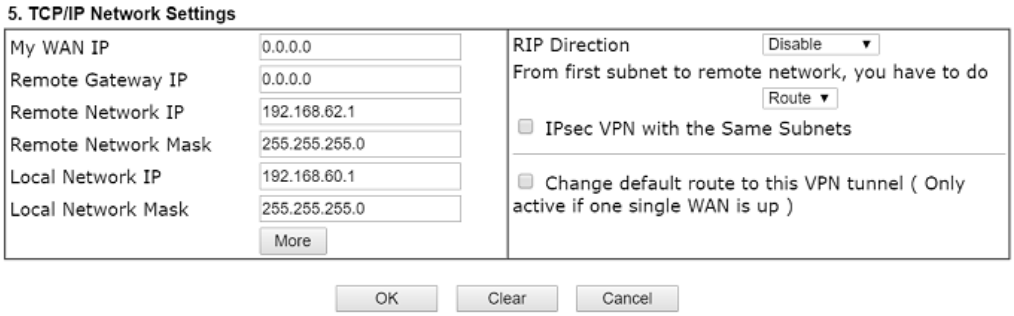
(c) Select **Dial-Out** as **Call Direction**.

(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.

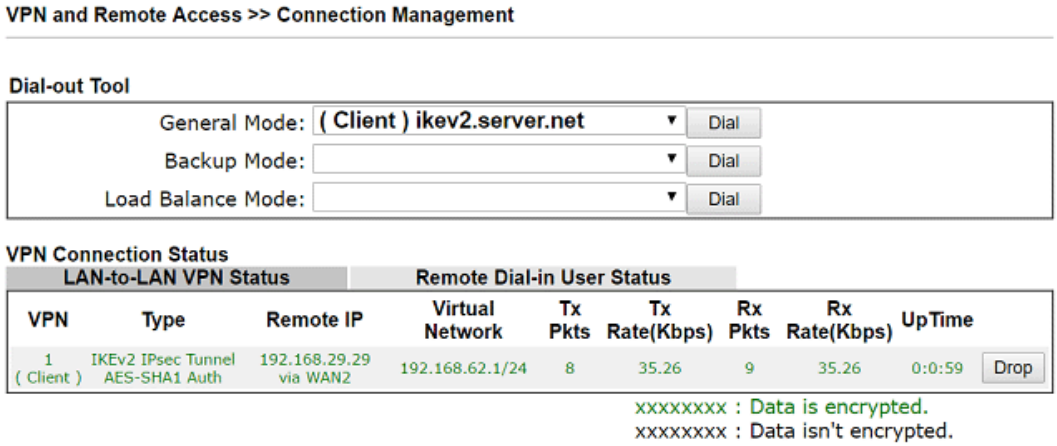



## VPN Tunnel Establishment

To initiate the VPN connection, go to **VPN and Remote Access >> Connection Management**. Select the VPN profile and click **Dial**.




After VPN is established successfully, the VPN connection status will be shown below.



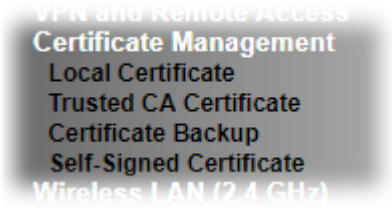
# IV-2 Certificate Management

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

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

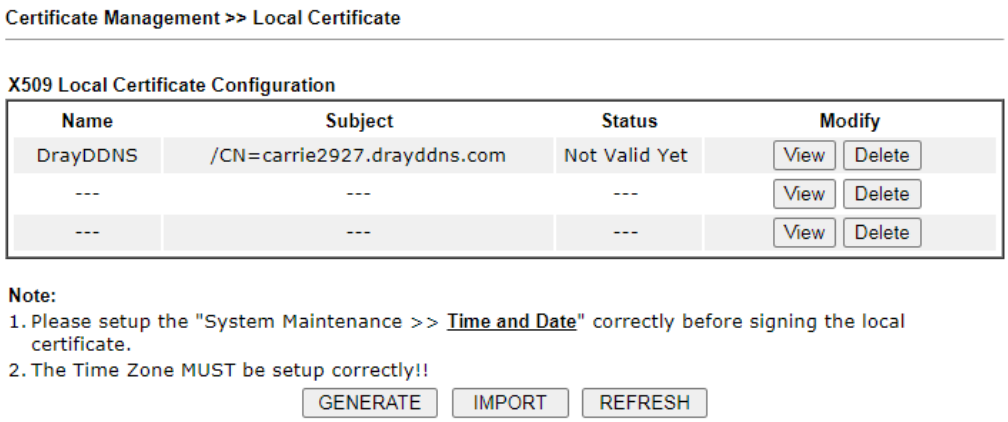
The image below shows the menu items for Certificate Management.

# Web User Interface

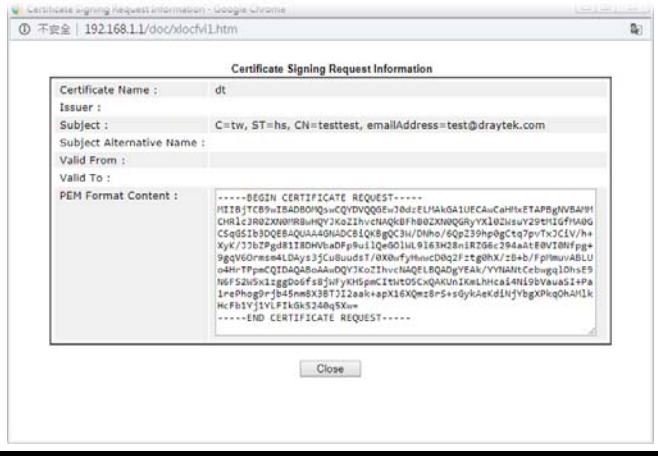



## IV-2-1 Local Certificate

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



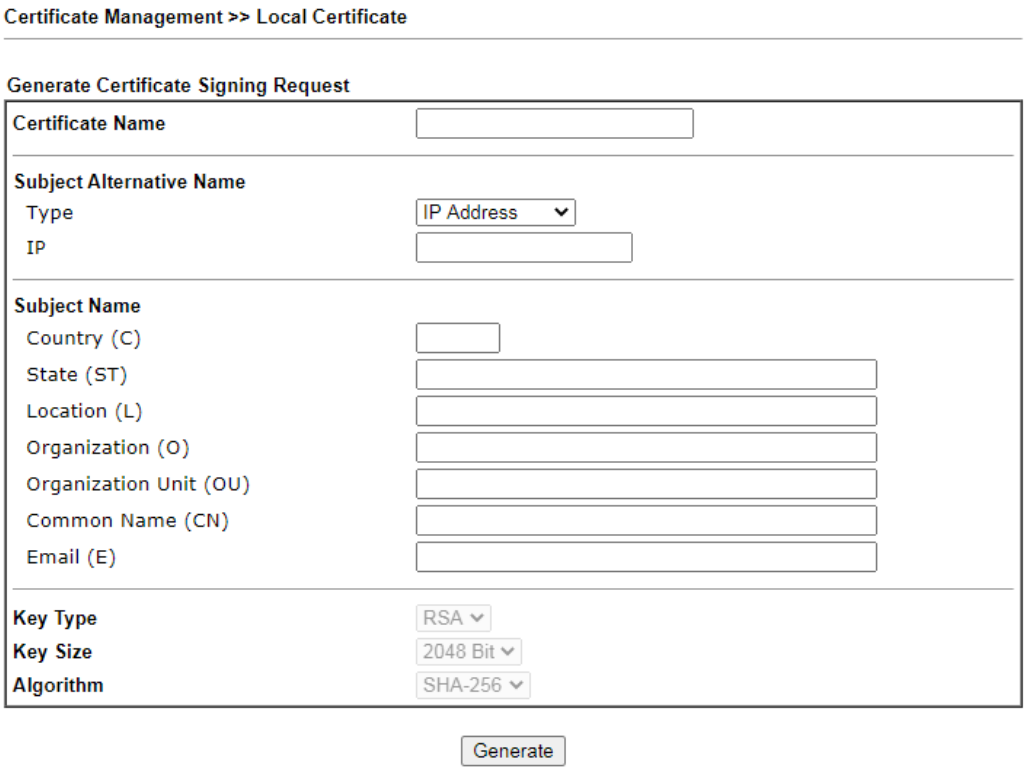

Available settings are explained as follows:

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

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

## GENERATE

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

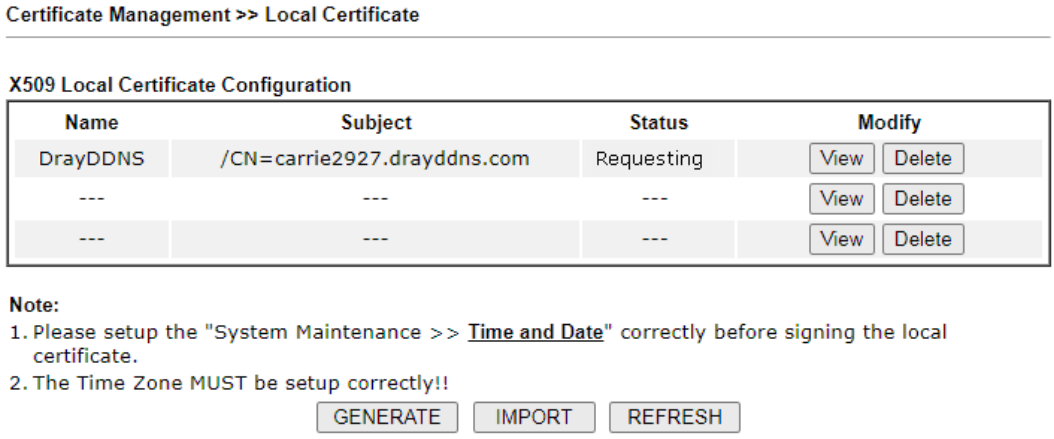



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Certificate Name** | Name that identifies the certificate. |
| **Type** | Select the type (IP address, Domain name, E-mail or None) of Subject Alternative Name and enter its value. |
| **Country (C)** | Country in which your organization is located. |
| **State (ST)** | State or province where your organization is located. |
| **Location (L)** | City where you're your organization is located. |
| **Organization (O)** | Legal name of your organization. |
| **Organization Unit (OU)** | Department within your organization that you wish to be associated with this certificate. |
| **Common Name (CN)** | Fully-qualified domain name / WAN IP that will be used to reach your server. |
| **Email (E)** | Email address of the entry. |

| | |
|---|---|
| **Key Type** | Key type is hard set to RSA. |
| **Key Size** | Choose between 1024 and 2048 bit. |
| **Algorithm** | Choose between SHA-1 and SHA-256. |
| **Generate** | Click to submit generate request to the CA server. |

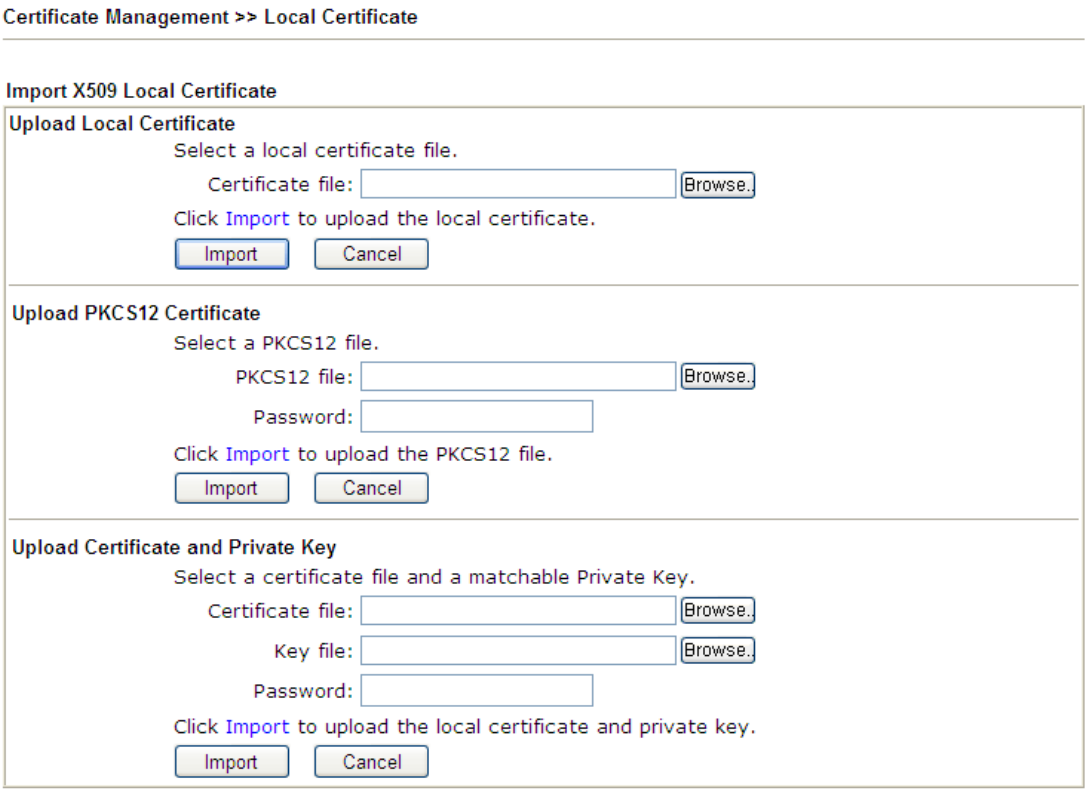
After clicking the **Generate** button, you will be taken back to the main Local Certificate screen, showing the certificate request in progress:



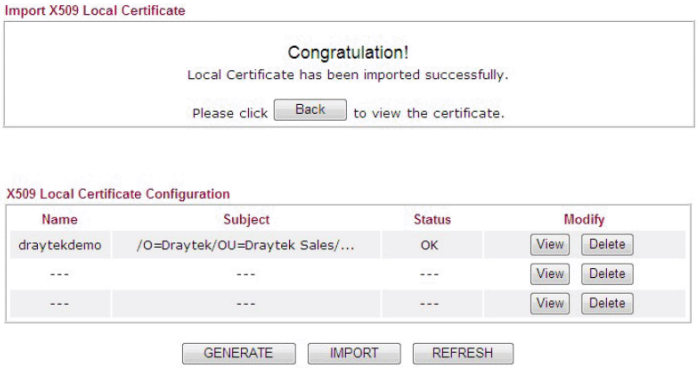

## IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as “Local Certificate”. If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

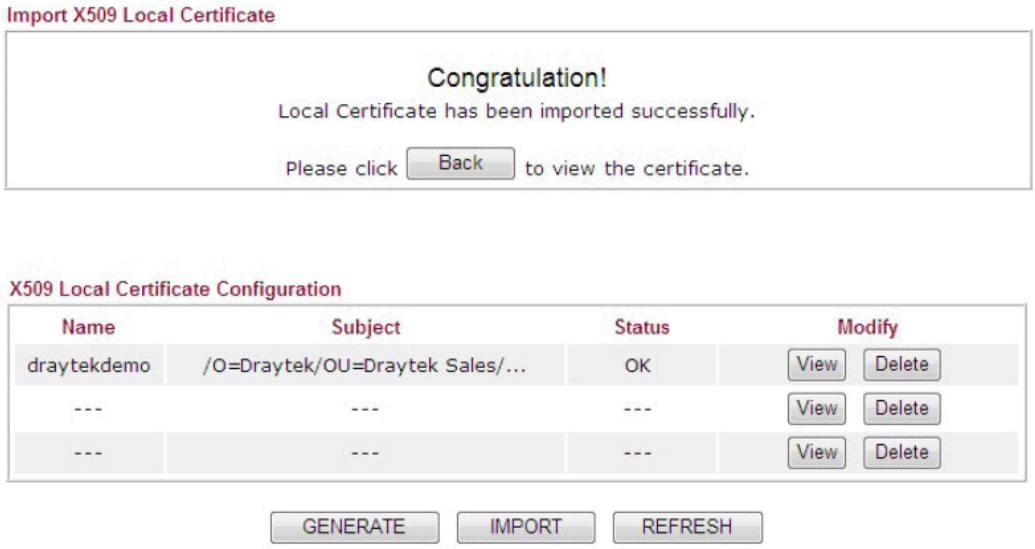
Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Upload Local Certificate** | **Certificate file -** Click **Browse** to select a local certificate file.<br>**Import -** Click to import selected certificate file to router.<br>**Cancel -** Click to return to the main Local Certificate screen.<br>If you have done well in certificate generation, the Status of the certificate will be shown as "**OK**".<br>  |
| **Upload PKCS12 Certificate** | It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.<br>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.<br>**PKCS12 file** - Click **Browse** to select a PKCS12 certificate file.<br>**Password** - Enter the password associated with the certificate and key files.<br>**Import** - Click to import selected certificate file to router.<br>**Cancel** - Click to return to the main Local Certificate screen. |
| **Upload Certificate and Private Key** | It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.<br>**Certificate file -** Click **Browse** to select a local certificate file.<br>**Key file** -<br>**Password** - Enter the password associated with the certificate and key files.<br>**Import -** Click to import selected certificate file to router.<br>**Cancel -** Click to return to the main Local Certificate screen. |

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




REFRESH

Click this button to refresh the information listed below.

## IV-2-2 Trusted CA Certificate

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

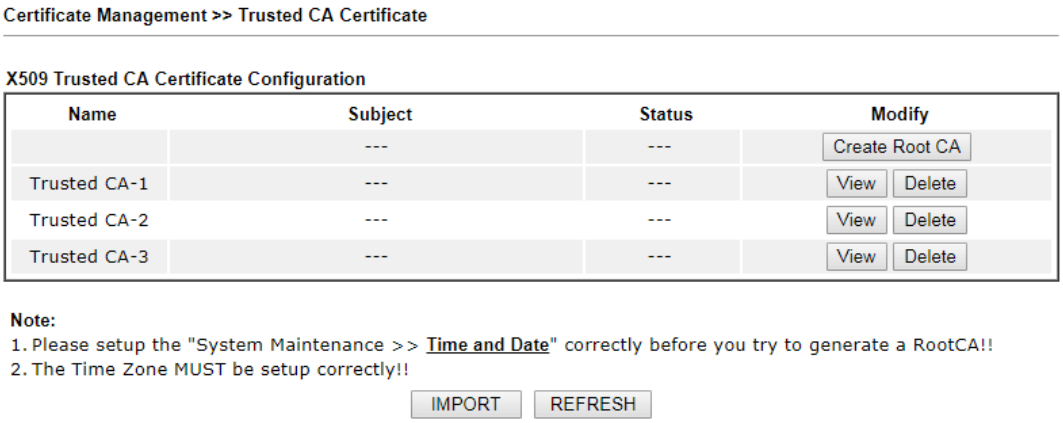
When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor router offers a mechanism which allows you to generate root CA to save time and provide convenience for general user. Later, such root CA generated by DrayTek server can perform the issuing of local certificate.

**Info**

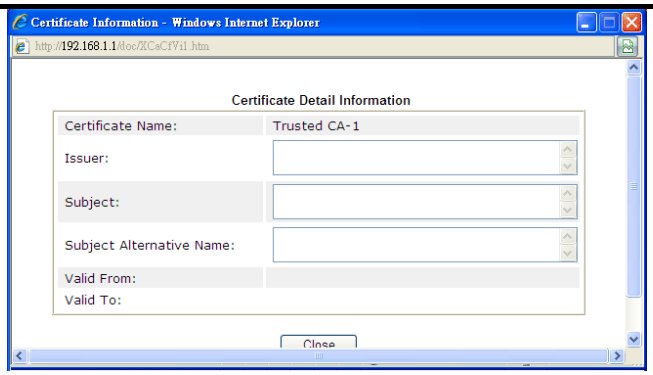
Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.

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



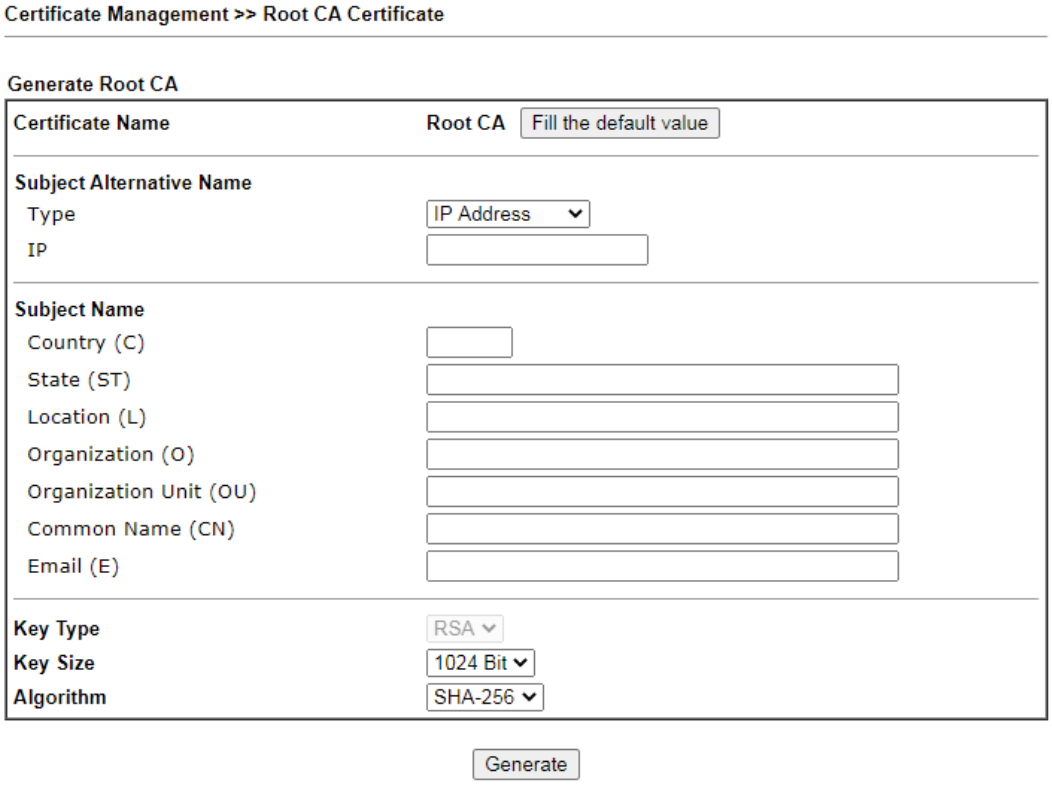

Available settings are explained as follows:

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

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

## Creating a Root CA

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



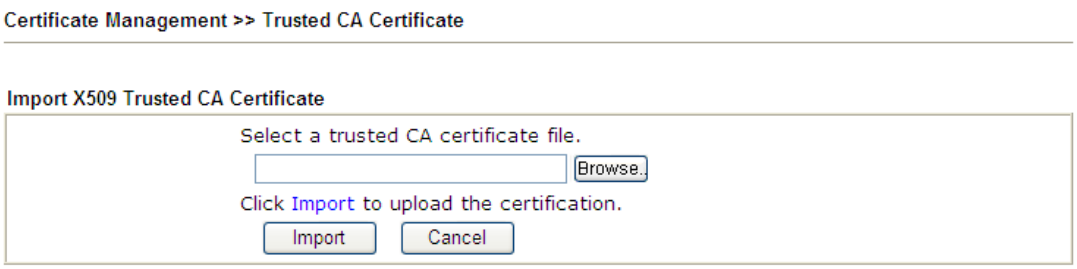

Available settings are explained as follows:

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

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

## Importing a Trusted CA

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

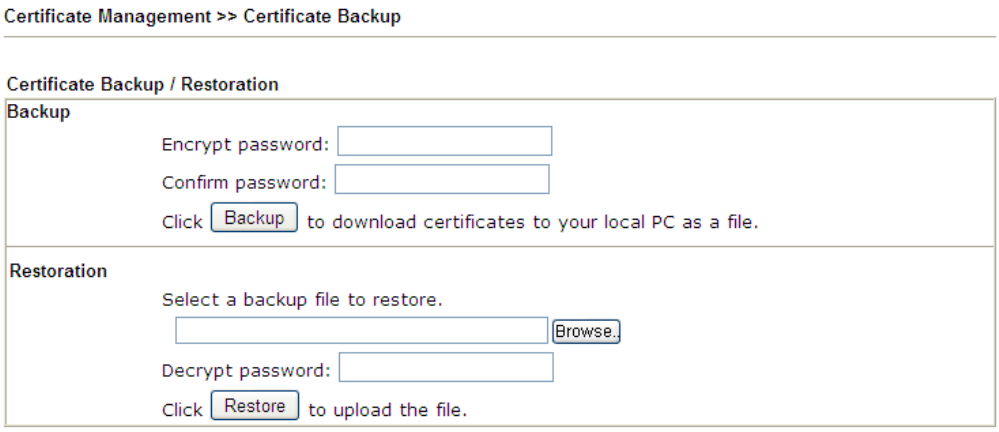



Available settings are explained as follows:

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

## IV-2-3 Certificate Backup

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



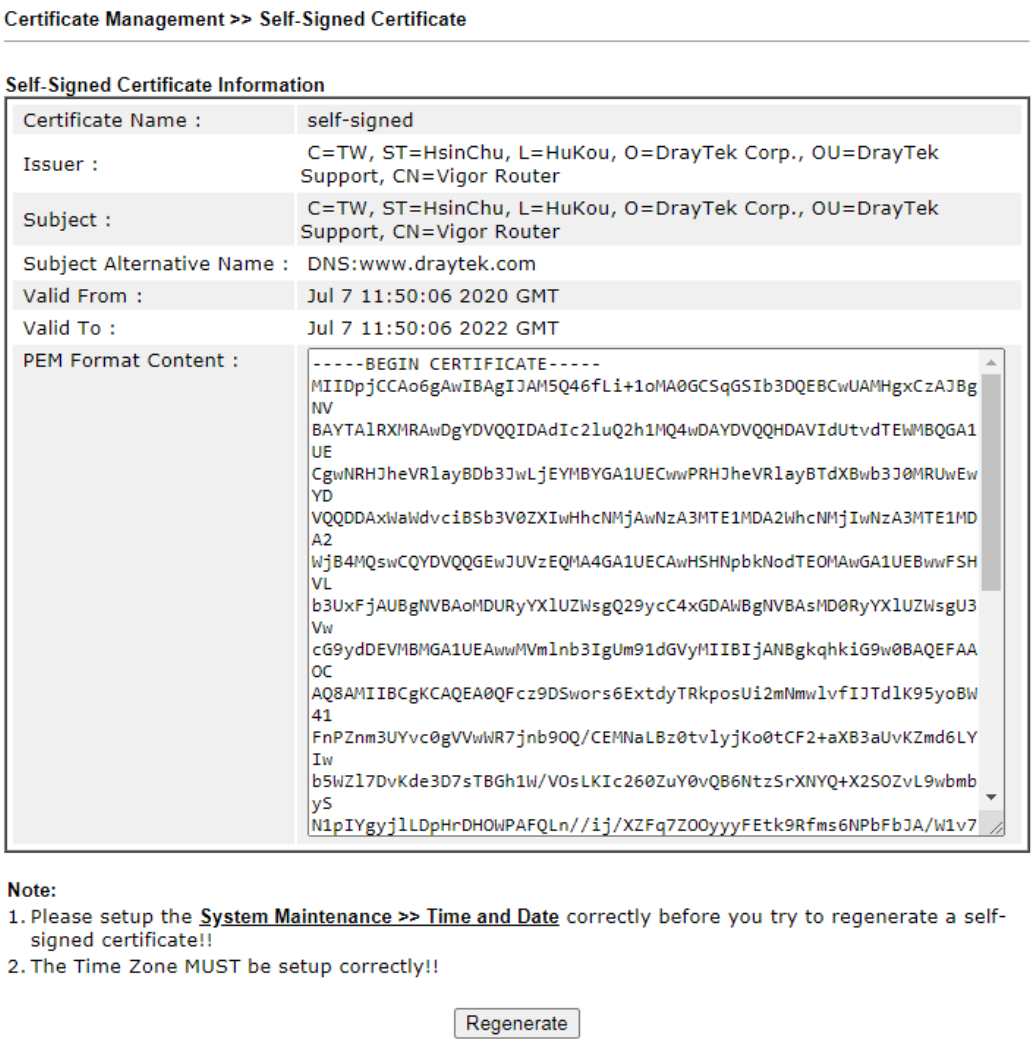

Available settings are explained as follows:

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

## IV-2-4 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate will be applied in SSL VPN, HTTPS, and so on. In addition, it can be created for free by using a wide variety of tools.




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

# Part V Security



Firewall



CSM

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

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

# V-1 Firewall

## Basic

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

## Firewall Facilities

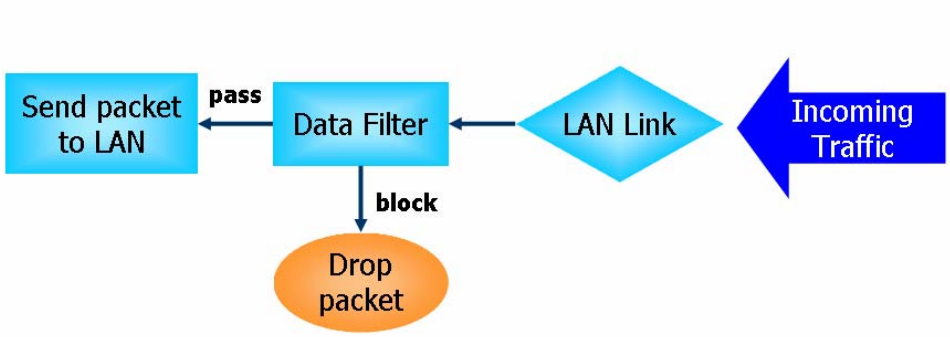
LAN users are provided with secured protection by the following firewall facilities:

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

## Data Filter

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

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




## Stateful Packet Inspection (SPI)

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

## Denial of Service (DoS) Defense

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

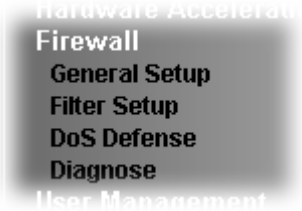
Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds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

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

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

# Web User Interface

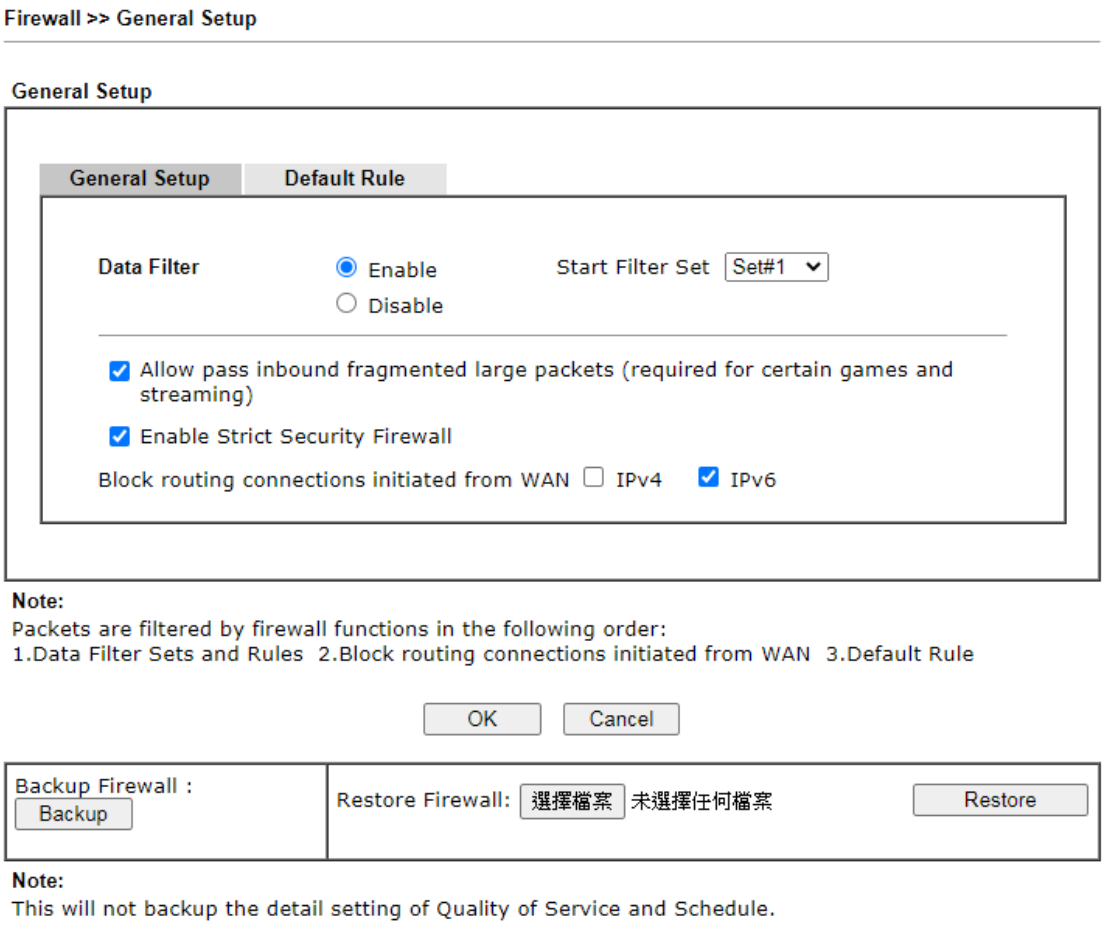
Below shows the menu items for Firewall.




## V-1-1 General Setup

### General Setup Page

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




Available settings are explained as follows:

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

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

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

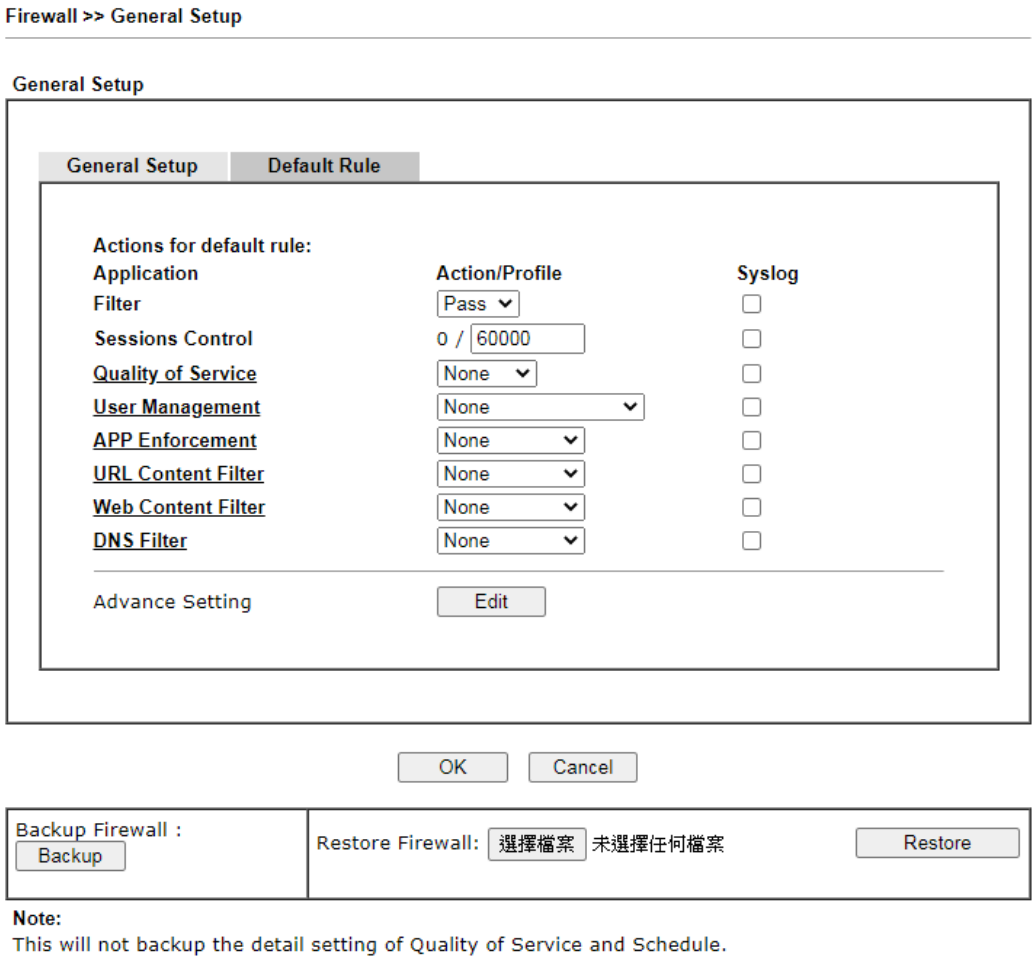
Traffic is filtered by firewall functions in the following order:

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

## Default Rule Page

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

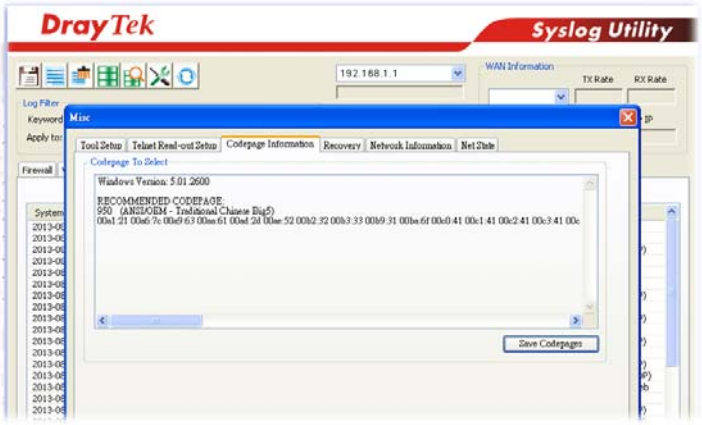
The default rule applies to all traffic that is not constrained by other filters or rules.




Available settings are explained as follows:

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

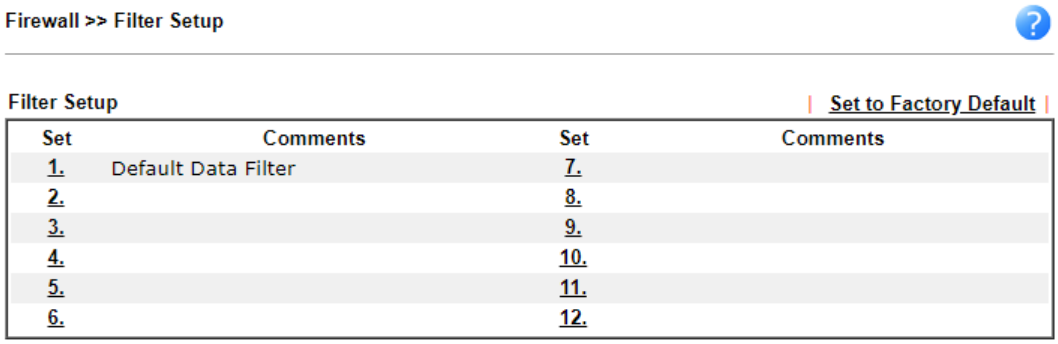
| | |
|---|---|
| | rule.<br>● **User Object**: The default rule only applies to the selected user.<br>● [**Create New User**]: Select this to create a new user.<br>● User Group: The default rule only applies to the selected User Group.<br>● [**Create New Group**]: Select this to create a new user group.<br>● **ALL**: The default rule applies to all defined users.<br>● **Create New User** or **Create New Group** item will appear for you to click to create a new one if there is no user profile or group profile existed.<br>**Syslog** - Select to allow User Management to log messages in Syslog. |
| **APP Enforcement** | Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature.<br>**Syslog** - Select to allow APP Enforcement to log messages in Syslog. |
| **URL Content Filter** | Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature.<br>**Syslog** - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log. |
| **Web Content Filter** | Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile.<br>**Syslog** - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log. |
| **DNS Filter** | Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile.<br>**Syslog** - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS Filter Profile Table section in CSM>>DNS Filter Profile, SysLog. |
| **Advance Setting** | Click **Edit** to open the configuration window for Advanced Settings. However, it is **recommended** to use the default settings. |

| | |
|---|---|
| | Firewall >> General Setup<br><br>Advance Setting<br>Codepage: ANSI(1252)-Latin I<br>Window size: 65535<br>Session timeout: 1440 Minute<br><br>OK Close<br><br>**Codepage** – Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed.<br>If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be shown in the Codepage Information tab in the Setup dialog box.<br>  <br><br>**Window size** – Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535. The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.<br>**Session timeout** – Sets the timeout sessions are allowed to idle before they are removed from the system. |
| **Backup Firewall** | Click **Backup** to save the firewall configuration. |
| **Restore Firewall** | Click **Select** to choose a firewall configuration file. Then click **Restore** to apply the file. |

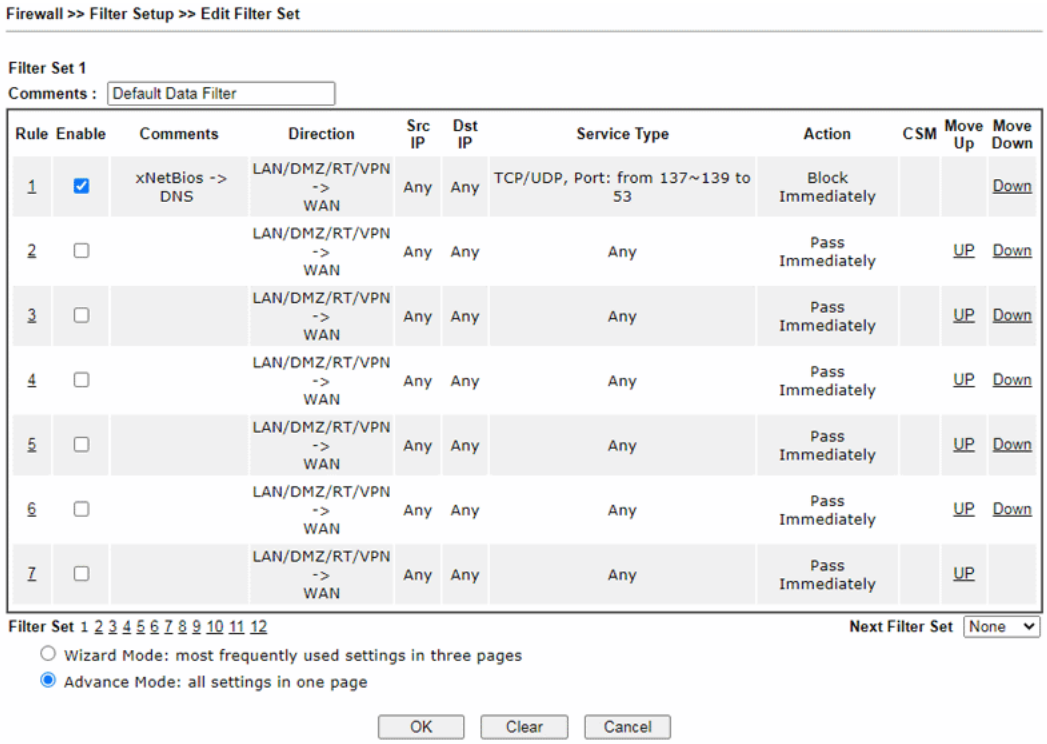
After finishing all the settings here, please click **OK** to save the configuration.

## V-1-2 Filter Setup

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




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



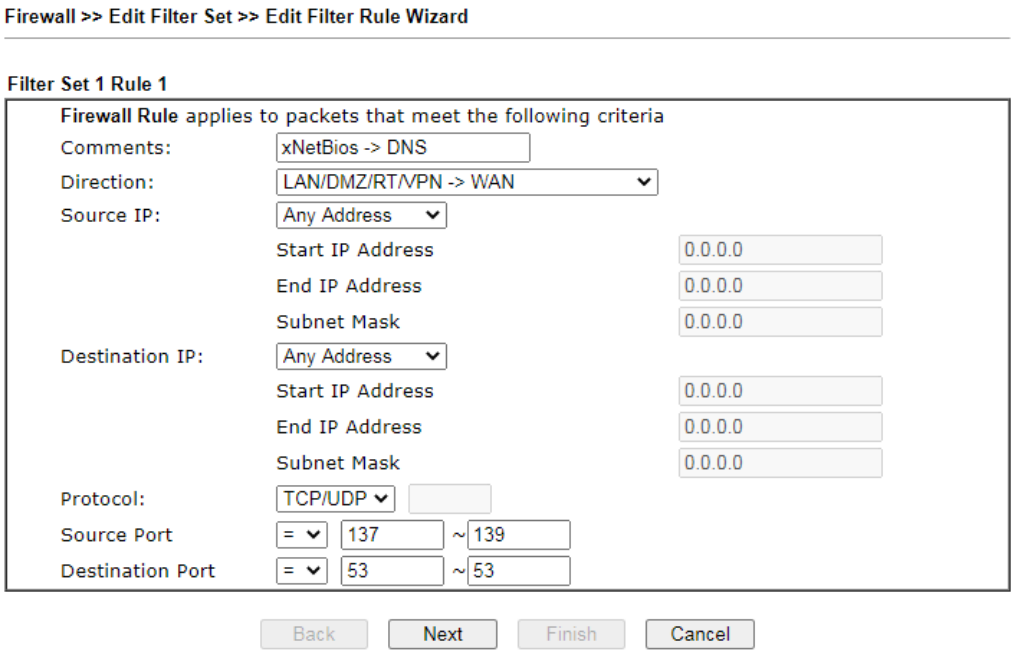

Available settings are explained as follows:

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

| | |
|---|---|
| **Action** | Displays the packets to be passed /blocked. |
| **CSM** | Displays the content security managed |
| **Move Up/Down** | Use **Up** or **Down** link to change the order of the filter rules. |
| **Next Filter Set** | Select the filter set for the firewall to process after the current filter set, or None if the current filter set is the last one to be processed. Be careful not to create a loop when setting next filter sets. |
| **Wizard Mode** | Allow to configure frequently used settings for filter rule via several setting pages. |
| **Advance Mode** | Allow to configure detailed settings of filter rule. |

To use Wizard Mode, simple do the following steps:

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Comments** | Enter filter set comments/description. Maximum length is 14- character long. |
| **Direction** | Set the direction of packet flow.<br>**Note:** RT means routing domain for 2nd subnet or other LAN. |
| **Source/Destination IP** | To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and Enter them in this dialog. |
| **Protocol** | Specify the protocol(s) which this filter rule will apply to. |

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

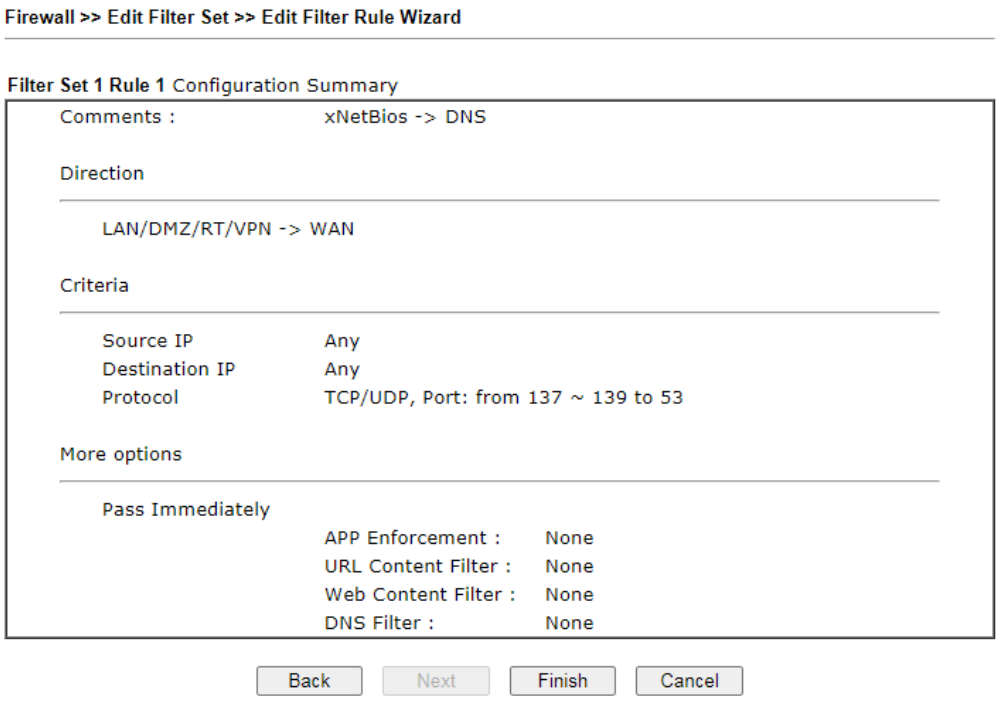
3. Click **Next** to get the following page.




Available settings are explained as follows:

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

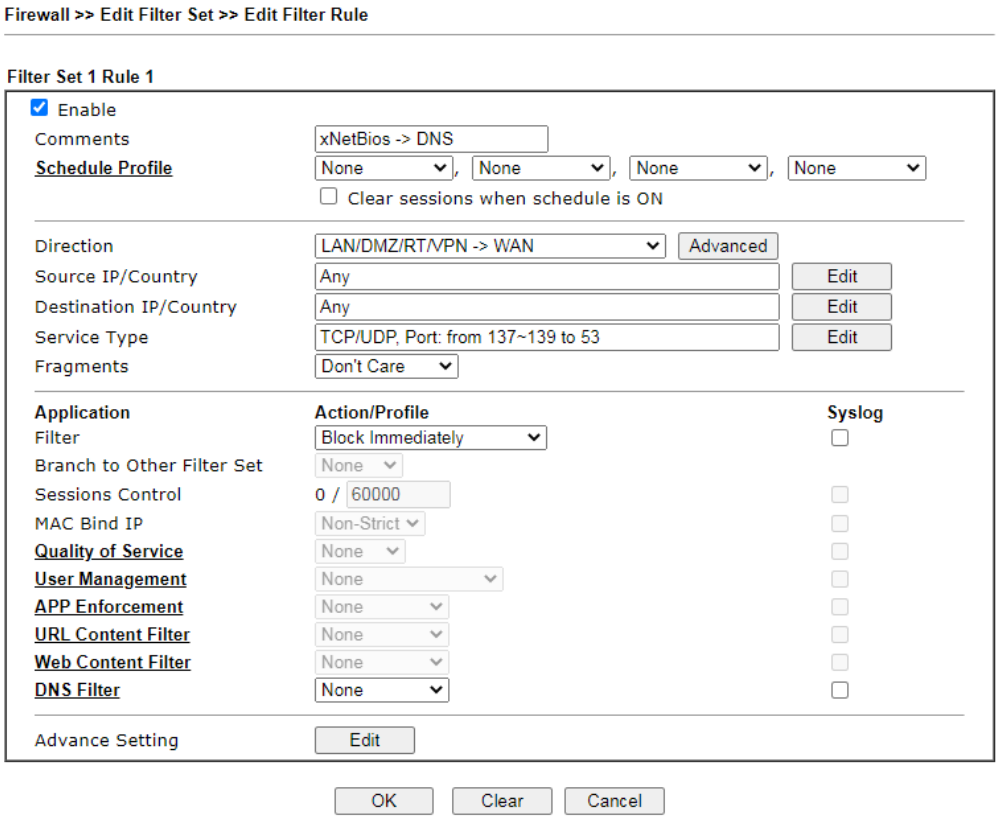
4. After choosing the mechanism, click **Next** to get the summary page for reference.



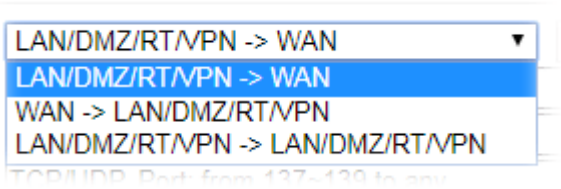

5. If there is no error, click **Finish** to complete wizard setting.

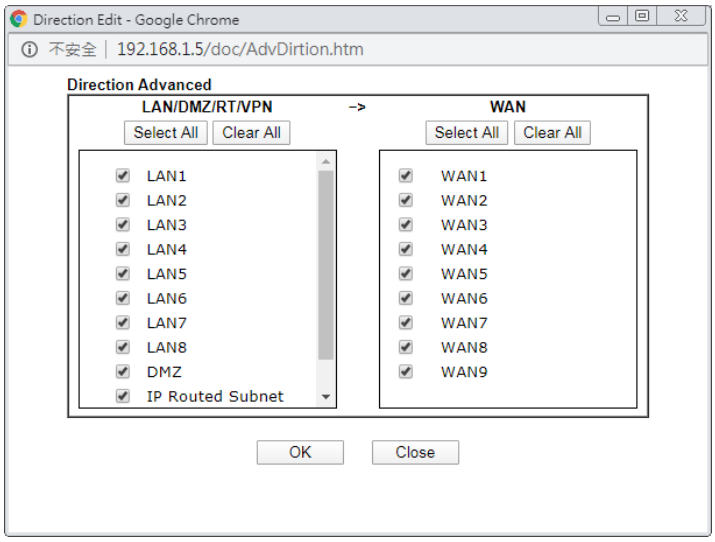
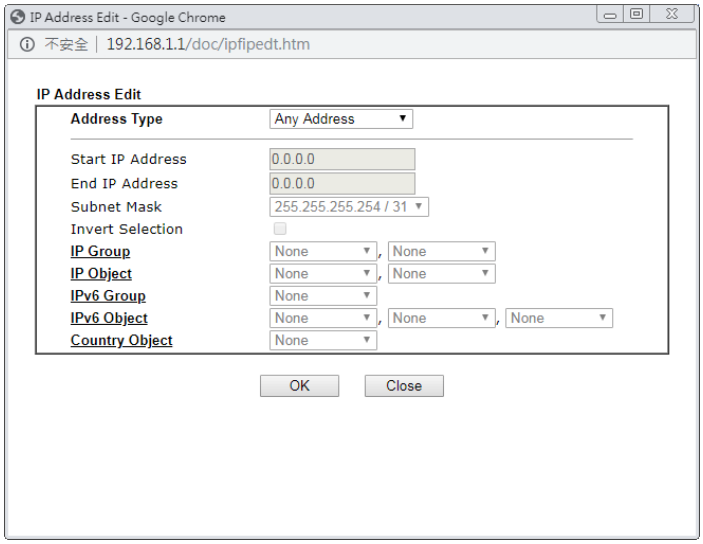
To use **Advance** Mode, do the following steps:

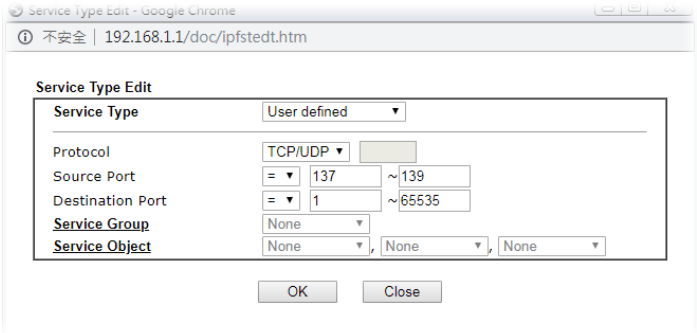
1. Click the **Advance Mode** radio button.
2. Click **Index 1** to access into the following page.



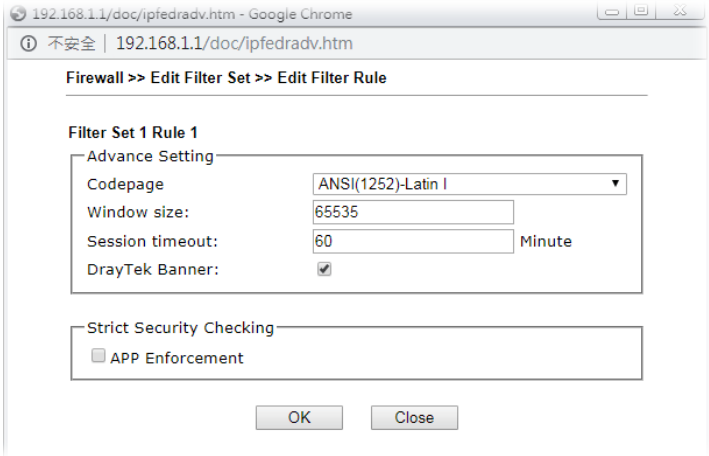
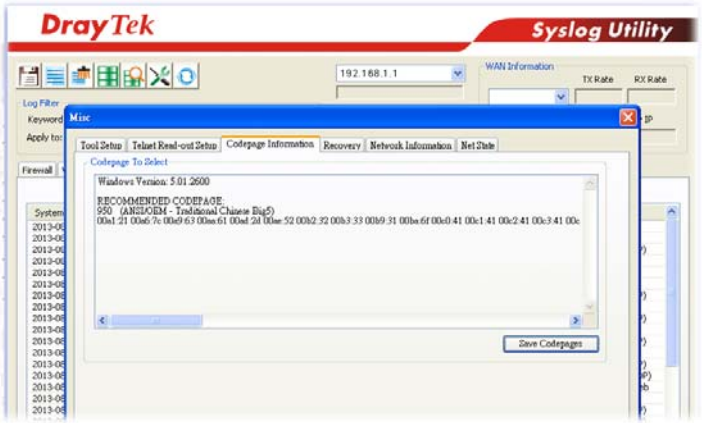

Available settings are explained as follows:

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

| | |
|---|---|
| | **Advanced** - After choosing the direction, click the Advanced button to specify interfaces for traffic flow.<br>  |
| **Source IP/ Country and Destination IP / Country** | Click **Edit** to bring up the following dialog box to configure the source and destination IP addresses or country objects.<br>  <br>To set the IP address manually, please choose an Address Type and enter required information.<br>**Address Type** – Select from one of the following:<br>● **Any Address** – All IP addresses<br>● **Single Address** – Enter one IP address in Start IP address<br>● **Range Address** – Enter the Start and End IP Addresses<br>● **Subnet Address** – Enter the Start IP Address and the Subnet Mask. Example: Start IP Address 192.168.1.1 and Subnet Mask 255.255.255.128 means is the same as having the Start IP Address as 192.168.1.1 and the End IP Address as 192.168.1.127.<br>● **Group and Objects** – Allows selection of predefined IP Groups and IP Objects. For details on IP Groups and Objects, see the chapter on Objects Setting.<br>● **Country Object** - Allows selection of predefined country objects. |
| **Service Type** | Click **Edit** to bring up the following dialog box to configure |

| | |
|---|---|
| | the Service Type.<br>  <br><br>**Service Type** - To set the service type manually, please choose **User defined** as the Service Type.<br>● **User defined** – Configure the protocol, source and destination ports manually.<br>● **Group and Objects** – Select preconfigured Service Groups or Objects.<br>**Protocol -** Specify the protocol(s) which this filter rule will apply to.<br>**Source/Destination Port -**<br>● (=) – any port that falls within the specified range<br>● (!=) – any port that falls outside of the specified range<br>● (>) – a port whose number is greater than the specified value<br>● (<) – a port whose number is smaller than the specified value<br>**Service Group/Object** - Use the drop down list to select the desired Service Groups or Objects. |
| **Fragments** | Action to be taken for fragmented packets. This option is valid for **Data Filter** rules only.<br>● **Don't care** –No action will be taken towards fragmented packets.<br>● **Unfragmented** –Apply the rule to unfragmented packets.<br>● **Fragmented** – Apply the rule to fragmented packets.<br>● **Too Short** – Apply the rule only to packets that are too short to contain a complete header. |
| **Filter** | Action to be taken when packets match the rule.<br>**Block Immediately** – Packets matching the rule will be dropped immediately.<br>**Pass Immediately** – Packets matching the rule will be passed immediately.<br>**Block If No Further Match** – Block the packet if this the last matching rule for this packet in the filter.<br>**Pass If No Further Match** – Pass the packet if this is the last matching rule for this packet in the filter. |
| **Branch to other Filter Set** | If the packet matches the filter rule, and the Filter action is **Block If No Further Match** or **Pass If No Further Match**, you can specify the next filter set to be applied, thus skipping the rest of the rules in the current filter set. |
| **Sessions Control** | The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions |

| | |
|---|---|
| | allowed, which is configurable. The default maximum is 60000, which is also the upper limit of the value. |
| **MAC Bind IP** | **Strict** – Ensure that both the MAC address and the IP address of the source and/or destination clients.<br>**Non-Strict** – Do not check the IP address when processing IP Objects that specify MAC addresses. |
| **Quality of Service** | Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. |
| **User Management** | This setting is only available when **Rule-Based** is selected in **User Management>>General Setup**. The default firewall rule will be applied to the selected user or user group. Refer to the chapter on User Management for more details on the feature.<br>● **None**: User Management does not apply to the default rule.<br>● **User Object**: The default rule only applies to the selected user.<br>● [**Create New User**]: Select this to create a new user.<br>● User Group: The default rule only applies to the selected User Group.<br>● [**Create New Group**]: Select this to create a new user group.<br>● **ALL**: The default rule applies to all defined users.<br>● **Create New User** or **Create New Group** item will appear for you to click to create a new one if there is no user profile or group profile existed.<br>**Syslog** - Select to allow User Management to log messages in Syslog. |
| **APP Enforcement** | Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on APP Enforcement for more details on the feature.<br>**Syslog** - Select to allow APP Enforcement to log messages in Syslog. |
| **URL Content Filter** | Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile. Refer to the chapter on URL Content Filter for more details on the feature.<br>**Syslog** - Select to allow URL Content Filter to log messages in Syslog. Logging action is configured at the profile level in CSM>>URL Content Filter Profile, Log. |
| **Web Content Filter** | Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. Select **[Create New]** from the dropdown list to create a new profile.<br>**Syslog** - Select to allow Web Content Filter to log messages in Syslog. Logging action is configured at the profile level in the Web Content Filter Profile Table section in CSM>>Web Content Filter Profile, Log. |
| **DNS Filter** | Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. Select **[Create New]** from |

| | |
|---|---|
| | the dropdown list to create a new profile.<br>**Syslog** - Select to allow DNS Filter to log messages in Syslog. Logging action is configured at the profile level in the DNS Filter Profile Table section in CSM>>DNS Filter Profile, SysLog. |
| **Advance Setting** | Click **Edit** to open the configuration window for Advanced Settings. However, it is recommended to use the default settings.<br>  <br>**Codepage** – Sets the codepage used by the URL content filter to match URLs against keywords in profiles. Choosing the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed.<br>If you are unsure of which codepage to use, please start the Syslog application, and the recommended codepage will be shown in the Codepage Information tab in the Setup dialog box.<br>  <br>**Window size** – Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535. The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.<br>**Session timeout** – Sets the timeout sessions are allowed to idle before they are removed from the system.<br>**DrayTek Banner** – Select to display the following screen for web pages that are blocked by the Firewall. The default setting is Enabled. |

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

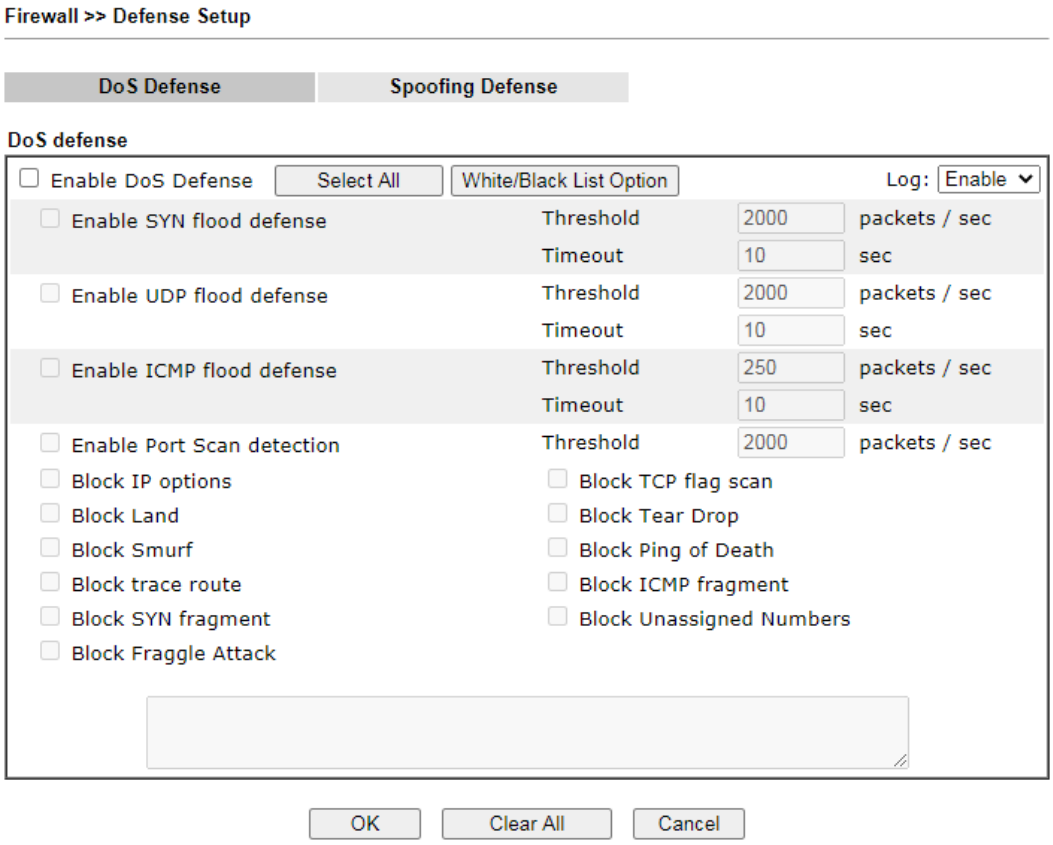
3. When you finish the configuration, please click **OK** to save and exit this page.

## V-1-3 Defense Setup

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

### V-1-3-1 DoS Defense

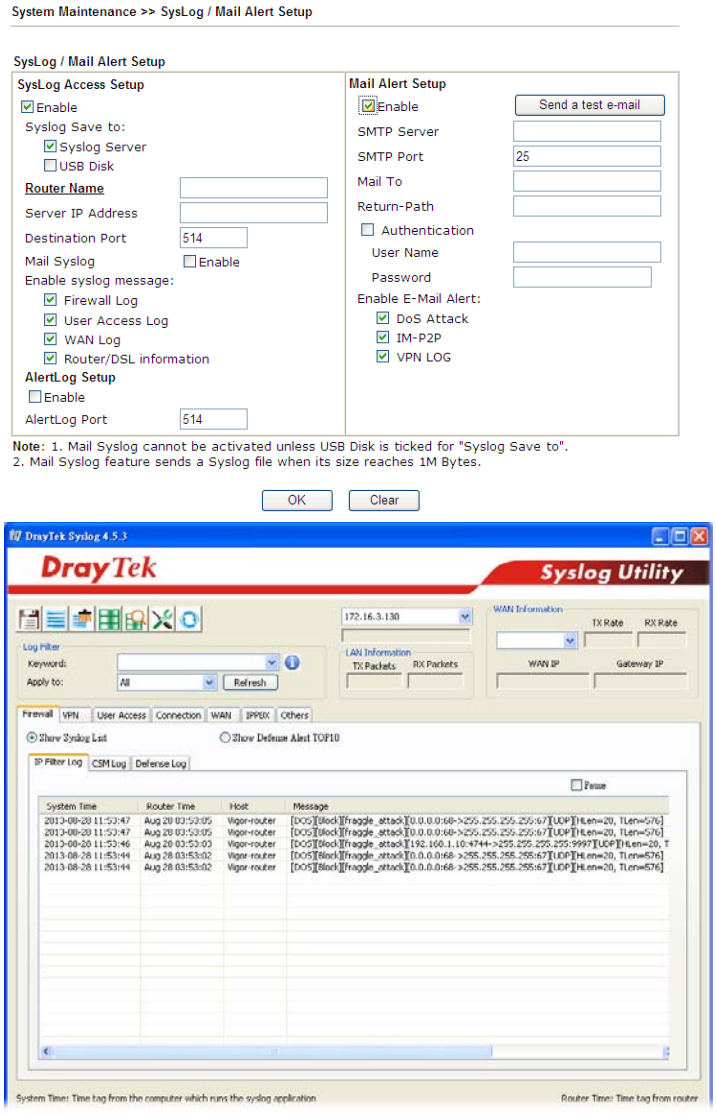
To configure DoS Defense, select DoS Defense under the Firewall menu item on the Web UI menu bar.




Available settings are explained as follows:

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

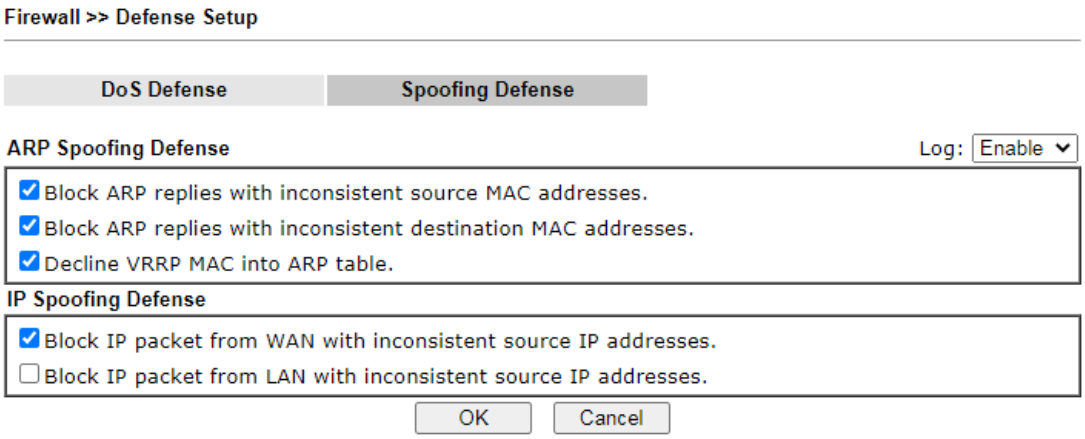
| | |
|---|---|
| | The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively. |
| **Enable ICMP flood defense** | Select to enable ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard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

| | |
|---|---|
| | more-fragments bit set are dropped. |
| **Block Unassigned Numbers** | Select to Block Unassigned Protocol Numbers, and the router will block packets having unassigned protocol numbers. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets. |
| **Warning Messages** | We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.<br>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.<br>  |

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

## V-1-3-2 Spoofing Defense

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

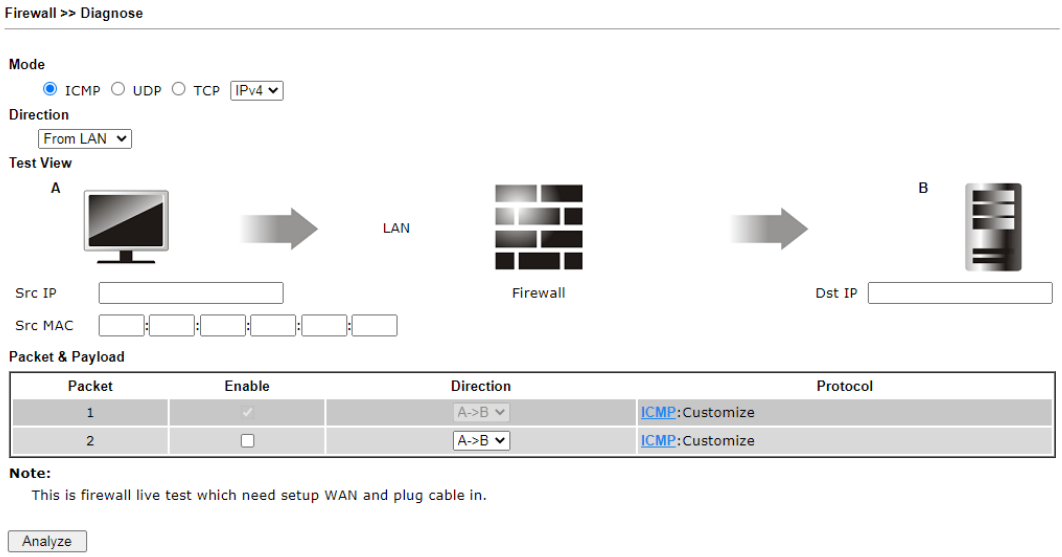


## V-1-4 Diagnose

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

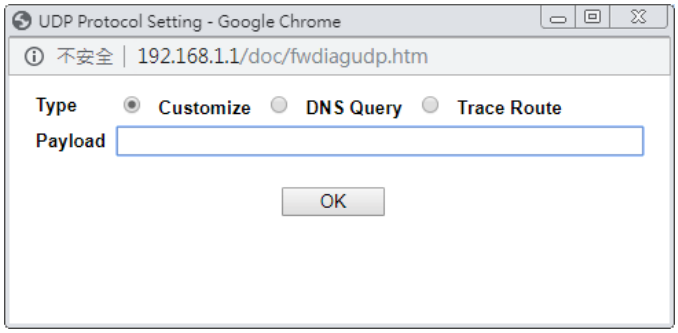
**Info**

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

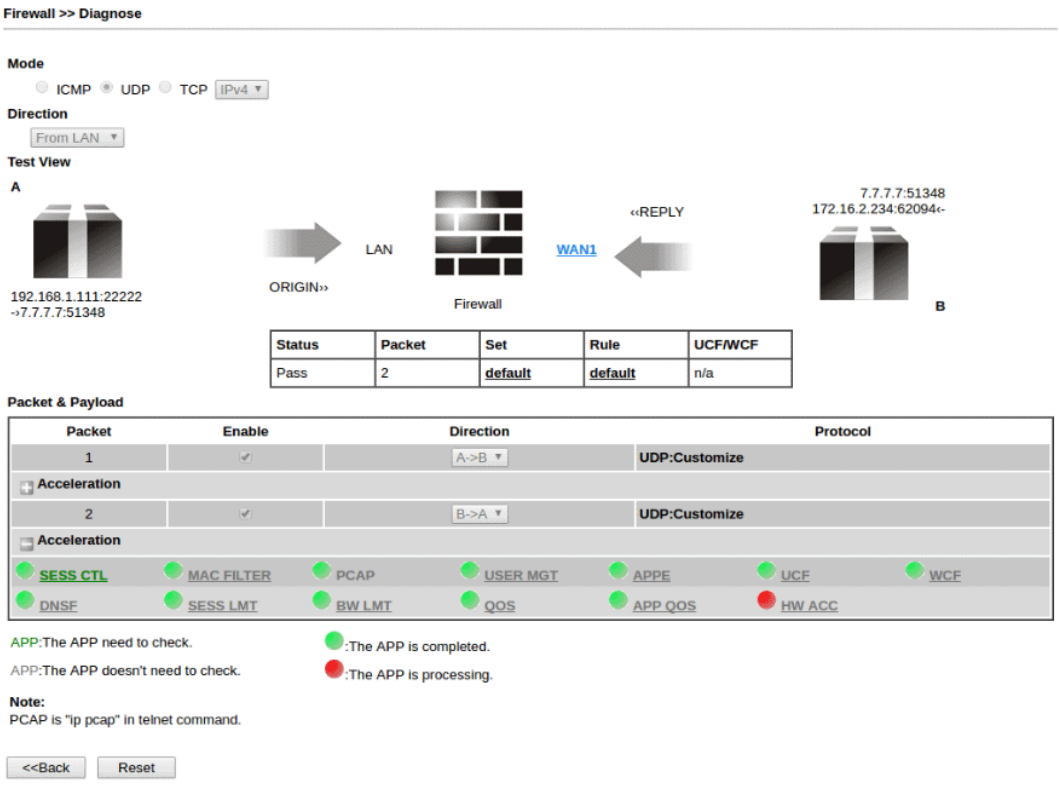



Available settings are explained as follows:

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

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

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



# V-2 Central Security Management (CSM)

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

## APP Enforcement Filter

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

## URL Content Filter

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

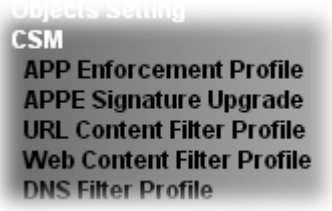
## Web Content Filter

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

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

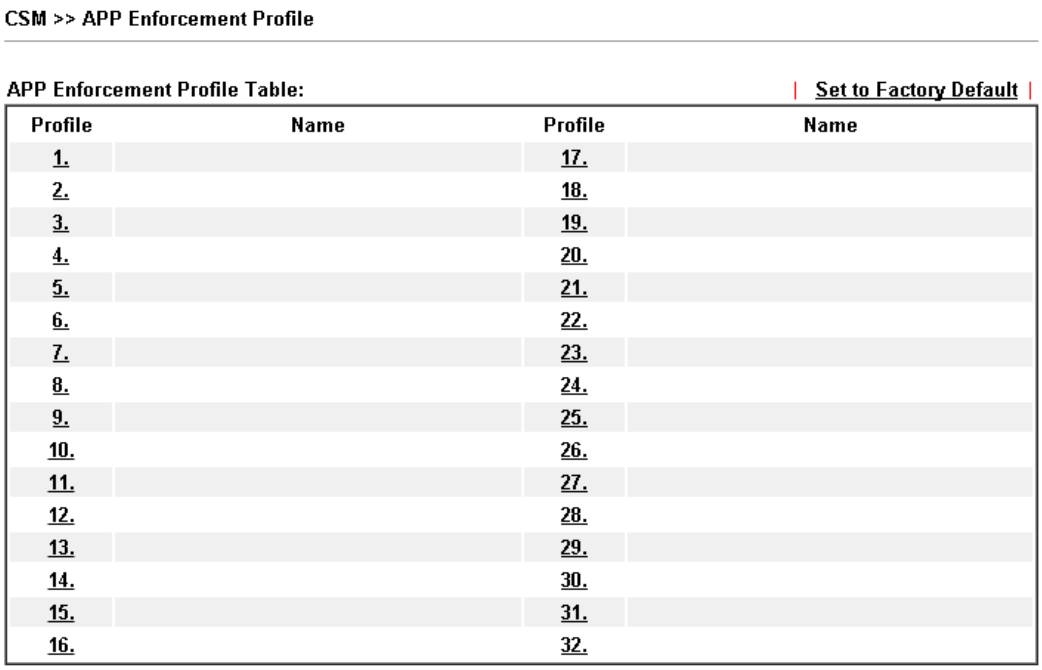
| | |
|---|---|
| **Info** | The priority of URL Content Filter is higher than Web Content Filter. |

# Web User Interface




## V-2-1 APP Enforcement Profile

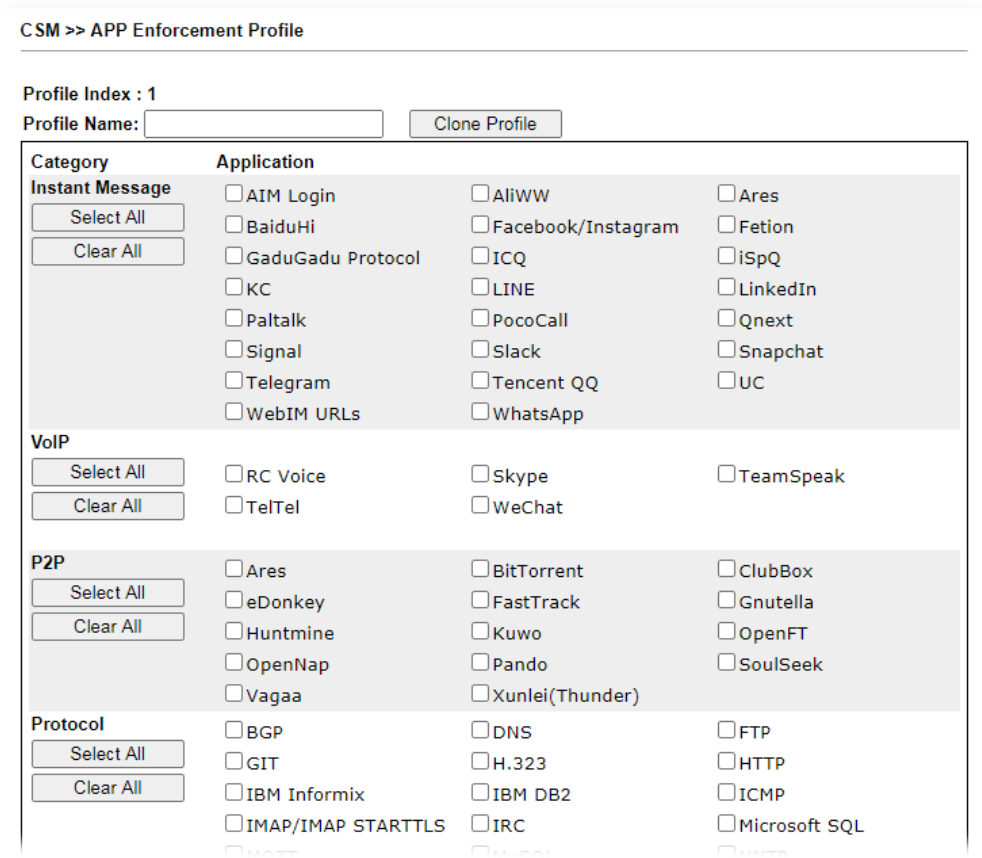
Up to 32 policy profiles for APP Enforcement can be configured.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Profile** | Index of the profile.<br>Click to bring up the configuration page of the profile. |
| **Name** | Name of the profile. |

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




Available settings are explained as follows:

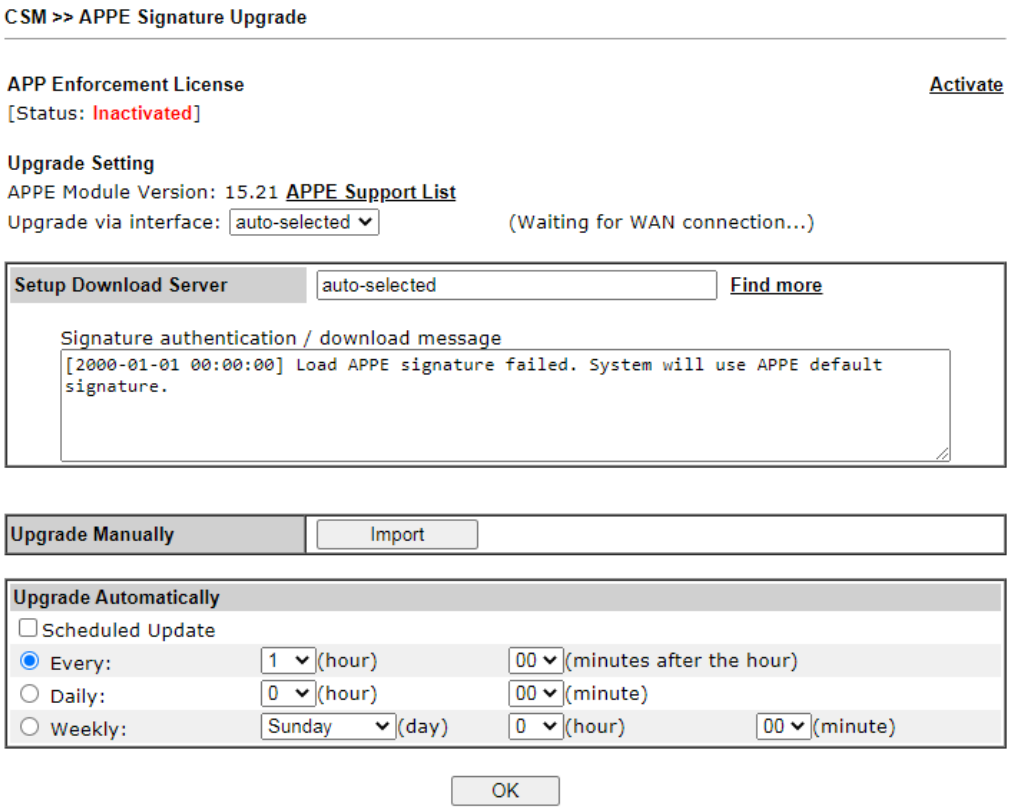
| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Category** | Apps are classified into several categories. Each category contains several apps to be blocked. |
| **Clone Profile** | Click it to clone settings configured by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

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

## V-2-2 APPE Signature Upgrade

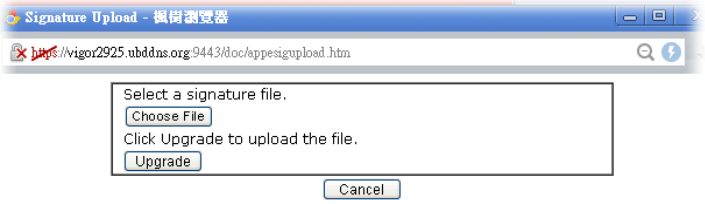
The APP Enforcement Profile feature identifies applications by matching their network traffic to signatures. DrayTek periodically releases APPE signature upgrades to ensure that new applications or new versions can be detected.

Upgrade checks can be performed manually or automatically.




Available settings are explained as follows:

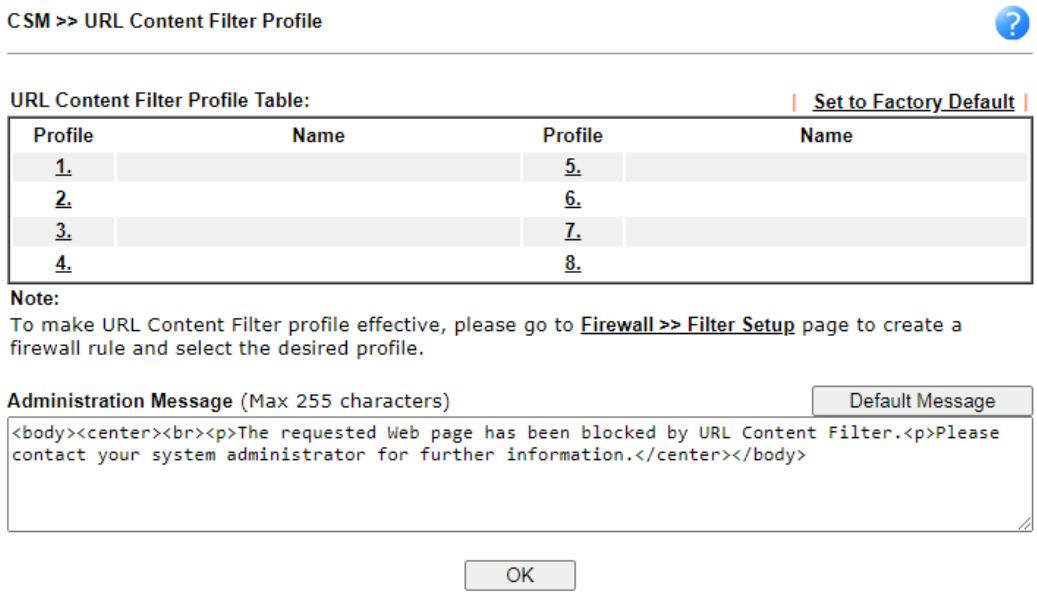
| Item | Description |
|---|---|
| **APP Enforcement License** | **Status -** Display current license status. |
| **Upgrade Setting** | **APPE Module Version** – Shows the current version of the APPE signature.<br>**New version from the Internet** – The **Download** button is enabled only when there is a newer version of APPE signature than the one present on the router. After clicking on the Download button, a dialog box will appear, displaying the release information of the new version. Click **OK** in the dialog box to proceed with the download.<br>**Upgrade via interface** – Select a WAN interface to download the new APPE signature. |
| **Setup Download Server** | Specify a download server by typing its URL of the server. Click the Find more for a list of download servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address.<br>**Signature authentication/download message** –Displays download status messages. |

| | |
|---|---|
| **Upgrade Manually** | Use this functionality if you wish to upgrade using a previously-downloaded signature file.<br>**Import** – Clicking the button brings up the following page.<br>  <br>Click **Choose File** to select the signature file. Click **Upgrade** to initiate the upgrade process. |
| **Upgrade Automatically** | **Scheduled Update -** Select to enable automatic periodic checking for signature updates. |

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

## V-2-3 URL Content Filter Profile

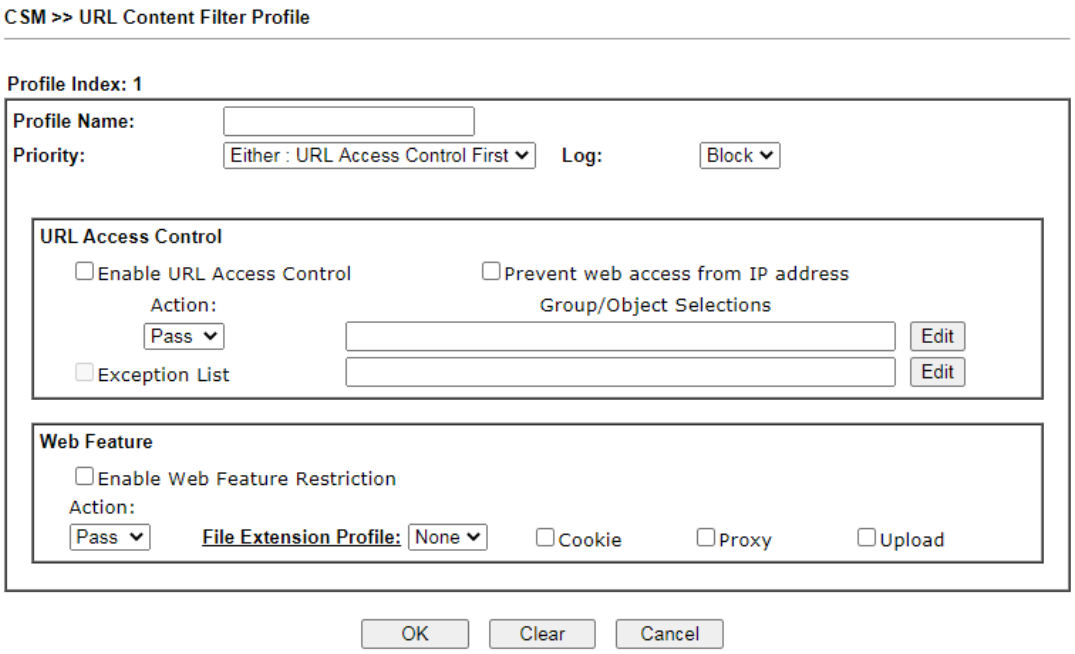
To set up URL Content Filter Profiles, click **CSM** on the Main Menu bar, and then click **URL Content Filter Profile** to open the profile setting page.




Each item is explained as follows:

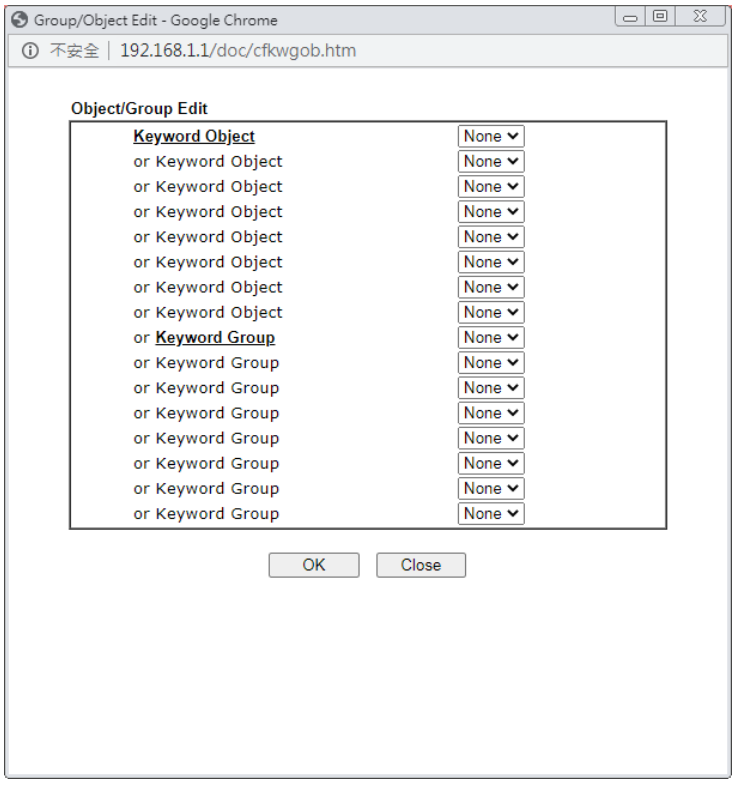
| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Profile** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Administration Message** | The message to be displayed in the browser when access to a URL has been blocked.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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Name that identifies the URL Content Filter profile. The maximum length of the Profile Name is 15 characters. |
| **Priority** | The order of evaluation of URL Access Control and Web Feature below:<br>**Both: Pass** – Router will allow access only to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Pass.<br>**Both:Block** – Router will block access to web resources that match conditions specified in both URL Access Control and Web Feature. The Action setting of both URL Access Control and Web Feature will be disabled and the values set to Block.<br>**Either: URL Access Control First** – Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. URL Access Control is applied first, followed by Web Feature.<br>**Either: Web Feature First** – Router will block or allow access to web resources that match conditions specified in either URL Access Control or Web Feature. Web Feature is applied first, followed by URL Access Control. |
| **Log** | **None** – No log file will be created for this profile.<br>**Pass** – Only passed access attempts will be recorded in Syslog.<br>**Block** – Only blocked access attempts will be recorded in Syslog.<br>**All** – Both passed and blocked access attempts will be recorded in Syslog. |
| **URL Access Control** | **Enable URL Access Control** - Select to activate URL Access Control.<br>**Prevent web access from IP address** - URLs containing IP |

| | |
|---|---|
| | addresses (e.g., 192.168.1.1) will be blocked. Only URLs with domain addresses (e.g., www.draytek.com) will be allowed. This is to prevent users from circumventing URL Access Control.<br>**Action** – This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First.<br>● **Pass –** Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked.<br>● **Block –** Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed.<br>**Exception List** – Specify the object profile(s) as the exception list which will be processed in an opposite manner to the action selected above.<br>**Group/Object Selections** – Shows the Keyword Groups and/or Objects selected for this URL Content Filter Profile.<br>To add or remove Keyword Groups and Objects to the selection, click the **Edit** button to bring up the following screen.<br>  <br>Up to 8 Keyword Objects and 8 Keyword Groups can be selected. To add, remove or modify Groups or Objects, click the Keyword Object or Keyword Group hyperlinks to bring up the **Objects Setting >> Keyword Object** or **Objects Setting >> Keyword Group** pages. |
| **Web Feature** | **Enable Restrict Web Feature -** Check to enable the web feature restriction.<br>**Action -** This setting is enabled only when Priority is set to **Either: URL Access Control First** or **Either: Web Feature First**.<br>● **Pass** – Allows access to web pages with URLs containing |

| | |
|---|---|
| | keywords that are in the selected keyword groups or objects. Access to other URLs is blocked.<br>● **Block** – Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed.<br>**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.<br>**Cookie** - Select to block cookies from Internet websites.<br>**Proxy** - Select to block web proxy servers that relay HTTP traffic.<br>**Upload** – Select to block HTTP uploads from the LAN to the Internet. |

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

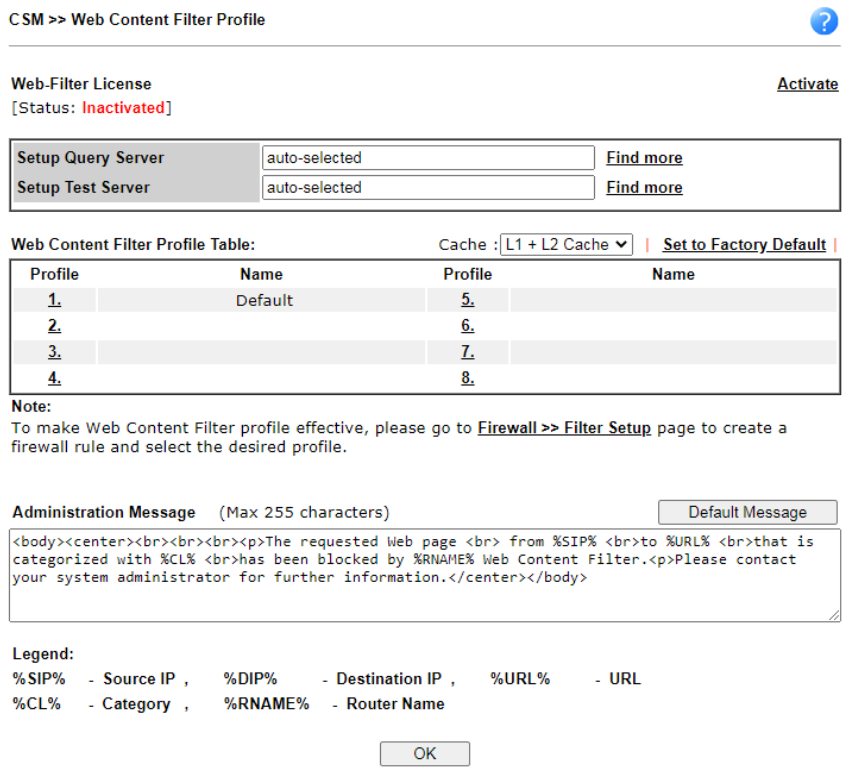
## V-2-4 Web Content Filter Profile

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

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

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

| | |
|---|---|
| **Info 1** | Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information. |
| **Info 2** | Commtouch is merged by Cyren, and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to:<br>http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html |

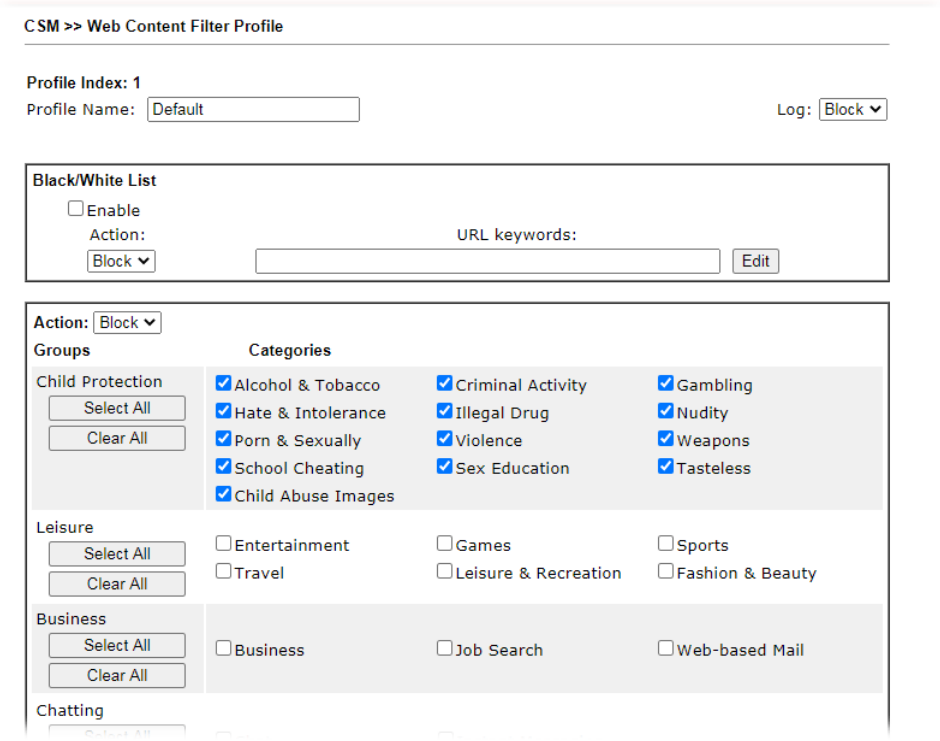



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Activate** | Click to visit the MyVigor webnsite to activate WCF service. You will need to log in to your MyVigor account to proceed with the activation process. If you do not already have a MyVigor account, you can create one at this time. |

| | |
|---|---|
| **Setup Query Server** | Specify a WCF query server by typing address of the server. Click the Find more for a list of query servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address.<br>It is recommended that the default setting auto-selected be used. |
| **Setup Test Server** | Specify a WCF test server by typing address of the server. Click the Find more for a list of test servers. When the default value auto-selected is used, the server is determined automatically by looking up the geolocation of the WAN IP address.<br>It is recommended that the default setting auto-selected be used. |
| **Cache** | **None** – The router verifies every HTTP URL requested by communicating with the WCF server on the Internet. This mode provides the most precise URL matching but has the lowest performance.<br>**L1** – The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs.<br>**L2** – After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server.<br>**L1+L2 Cache** – The router will utilize both L1 and L2 caches. |
| **Set to Factory Default** | Clear all profile settings. |
| **Profile** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Administration Message** | The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box.<br>You can embed the following variables in the message:<br>%SIP% – The source IP address that attempted the HTTP access.<br>%DIP% – The destination IP address to which access was attempted.<br>%URL% – The URL of the destination website.<br>%CL% – The category to which the URL belongs.<br>%RNAME% – The name of the router.<br>**Default Message** - Click to reset the administration message to the factory default. |

Up to 8 WCF profiles can be set up. To configure a profile, click its profile number to bring up its configuration page. Filter profile settings are specific to WCF providers. If you already have an active WCF subscription, activating a WCF subscription to a provider that is different from your current provider will clear all existing profile configuration.




Available settings are explained as follows:

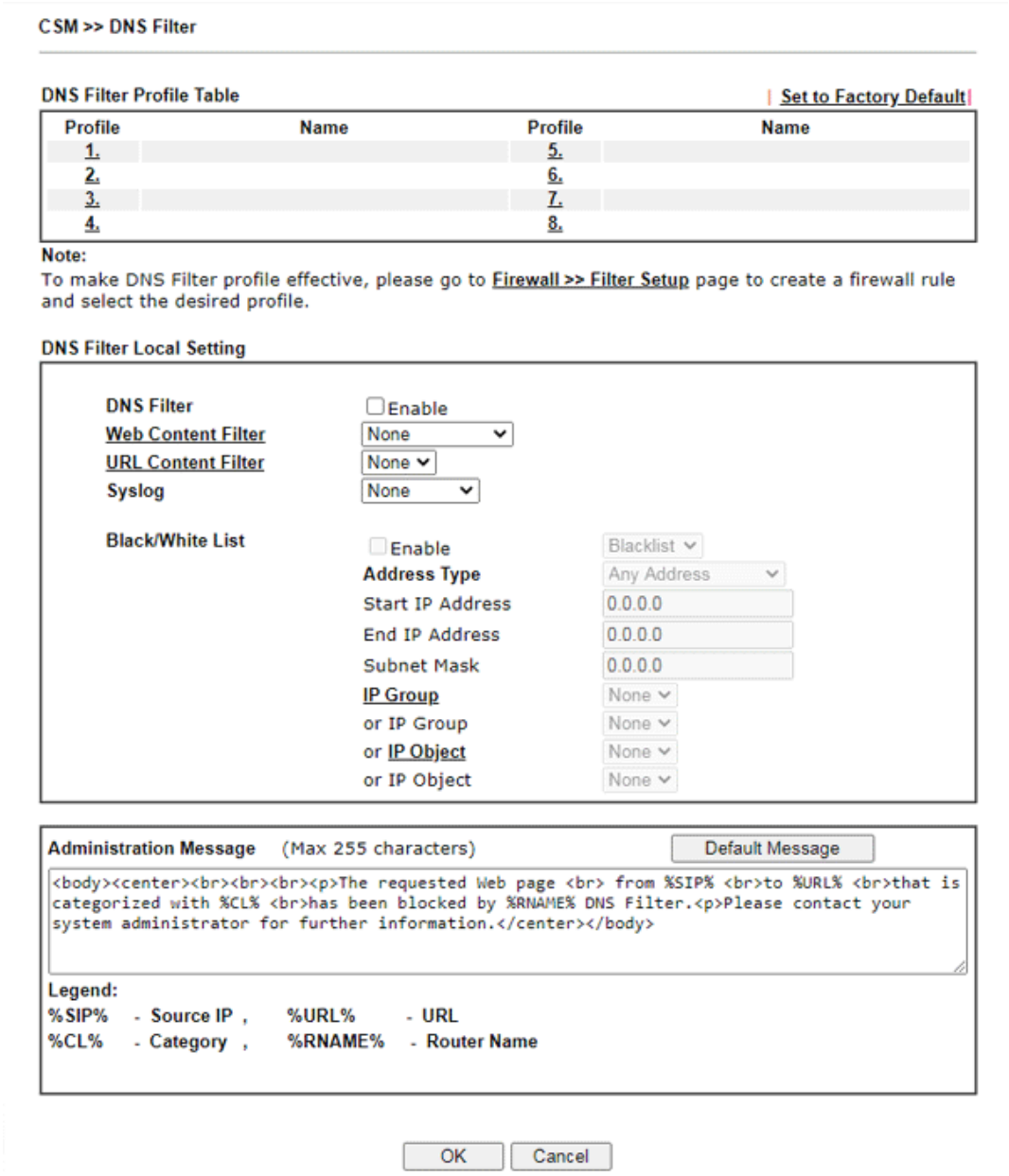
| Item | Description |
|---|---|
| **Profile Name** | Name that identifies the WCF profile. The maximum length of the Profile Name is 15 characters. |
| **Log** | **None** – No log file will be created for this profile.<br>**Pass** – Only passed access attempts will be recorded in Syslog.<br>**Block** – Only blocked access attempts will be recorded in Syslog.<br>**All** – Both passed and blocked access attempts will be recorded in Syslog. |
| **Black/White List** | Keyword objects and groups can be applied to the URL to override WCF category filtering.<br>**Enable –** Select to enable blacklisting or whitelisting.<br>**Action** - Action to take when a URL matches keyword group and object selections.<br>● **Pass** – Allow access to the URL.<br>● **Block** – Disallow access to the URL.<br>**URL Keywords –** Displays selected keyword group and objects. Click the **Edit** button to modify keyword selections. |
| **Groups and Categories** | Select categories to be included in the filter.<br>**Action** - Action to take when a URL matches keyword group and object selections.<br>● **Pass** – allow access to the URL.<br>● **Block** – disallow access to the URL.<br>**Select All -** Click to select all categories within the group.<br>**Clear All -** Click to deselect all categories within the group. |

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

## V-2-5 DNS Filter Profile

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

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **DNS Filter Profile Table** | DNS Filter Profiles take effect when DNS servers on the WAN are used for DNS queries. The router intercepts all outgoing DNS queries on UDP port 53 and applies WCF and UCF rules on the domain names before passing the queries to the DNS servers. IP addresses of the domains are then blocked or |

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

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

# Application Notes

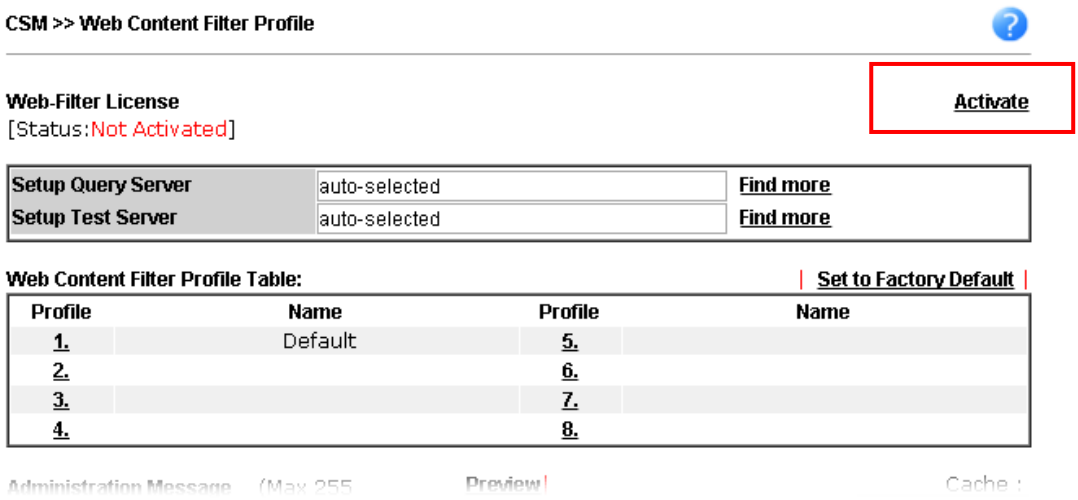
## A-1 How to Create an Account for MyVigor

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

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

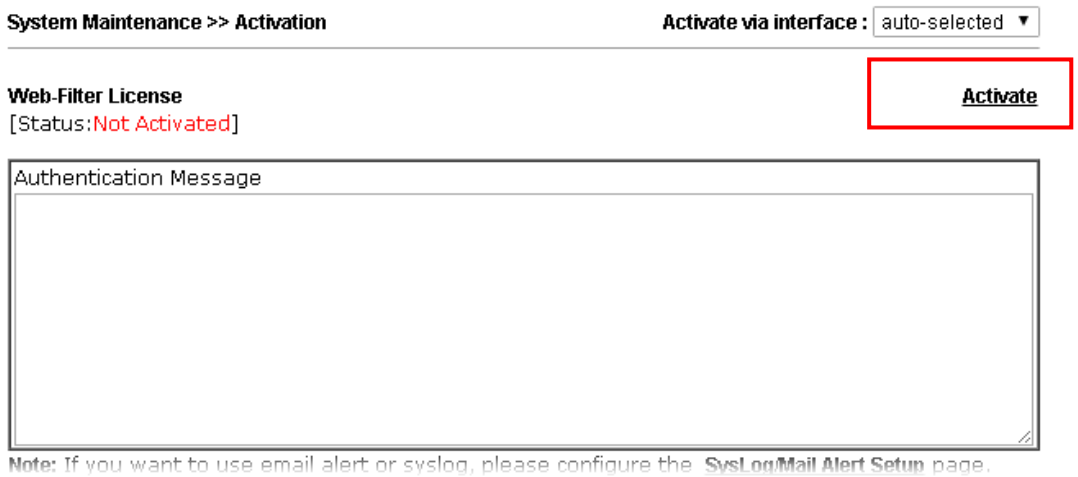
### Create an Account via Vigor Router

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

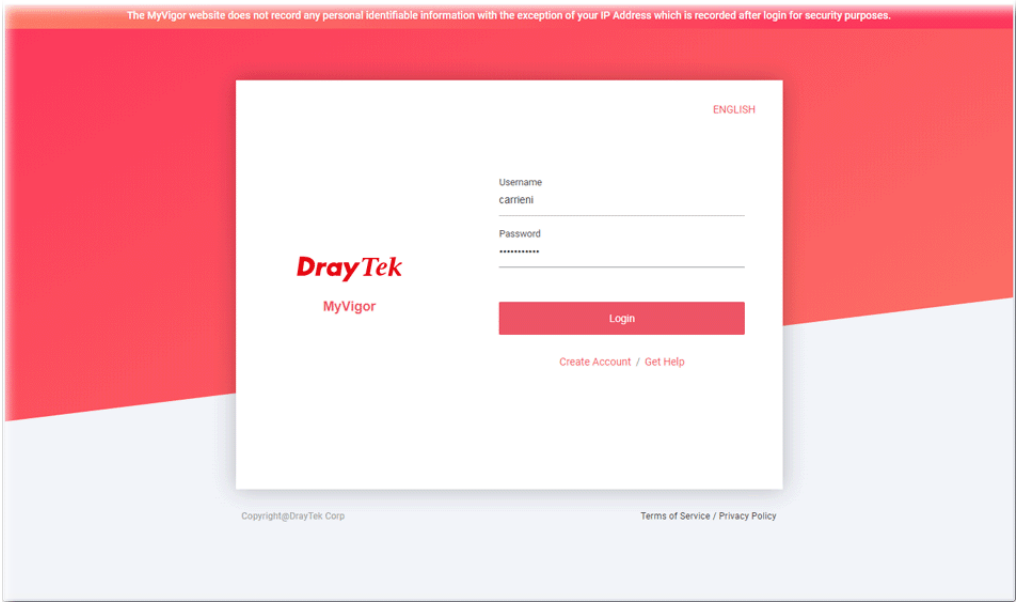



Or

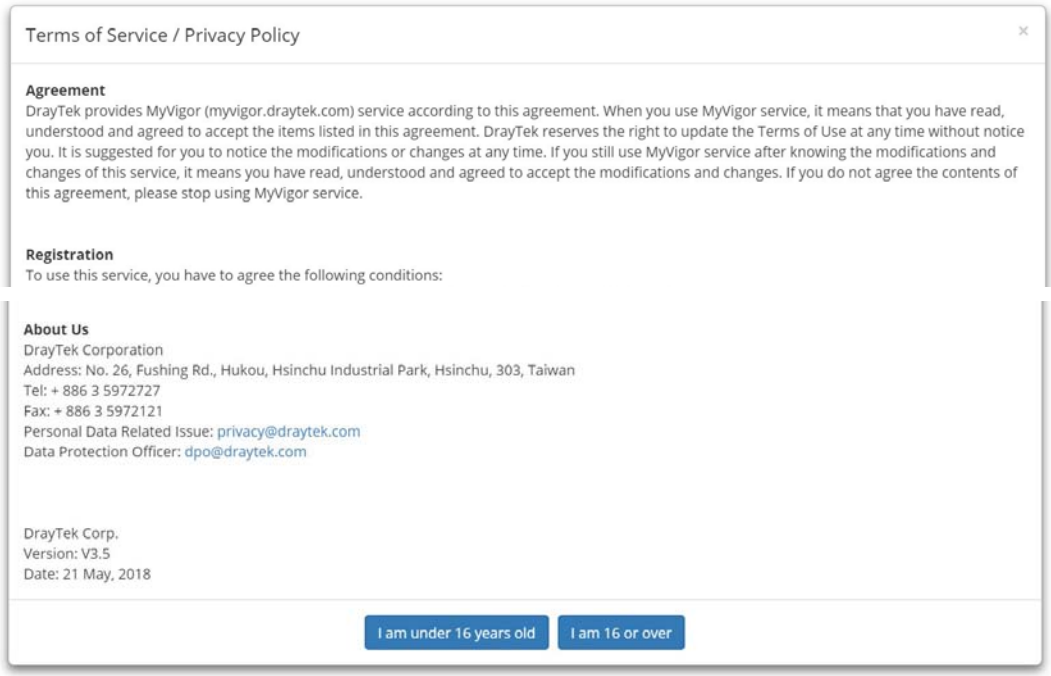
Click **System Maintenance>>Activation** to open the following page.



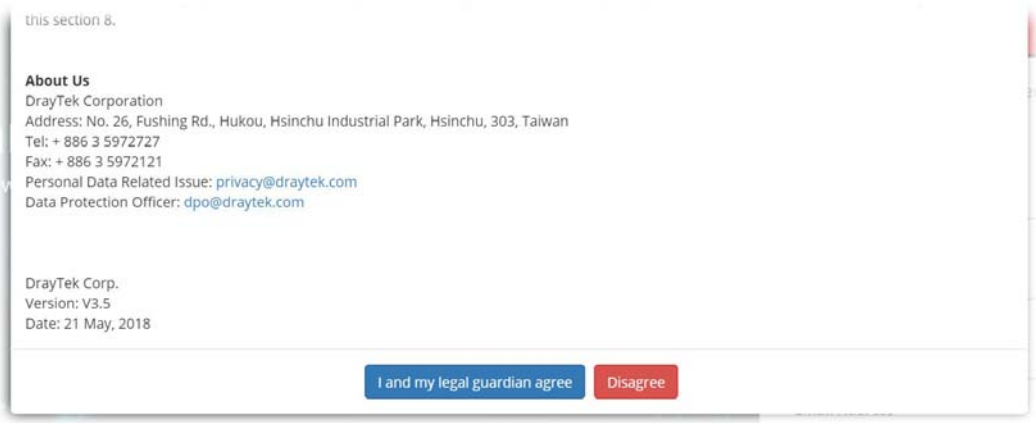
2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



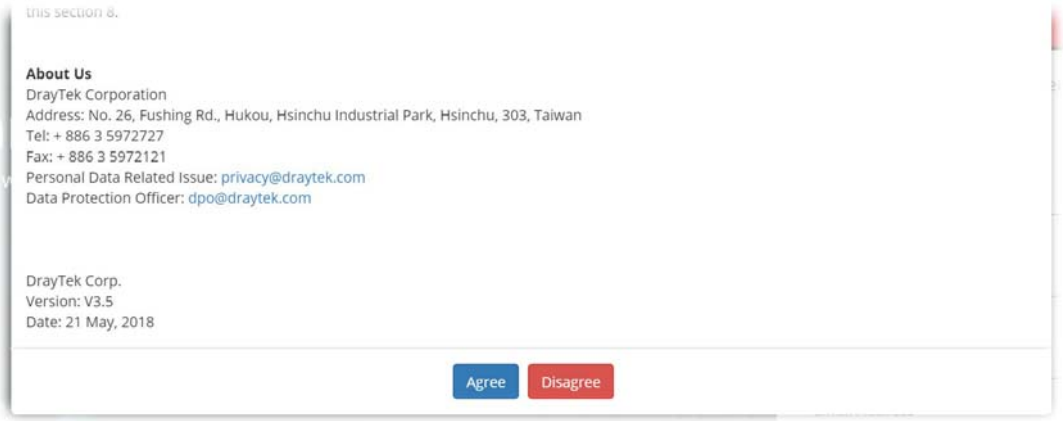

3. Click the link of **Create Account**.
4. The system will ask if you are 16 years old or over.
   - If yes, click **I am 16 or over**.



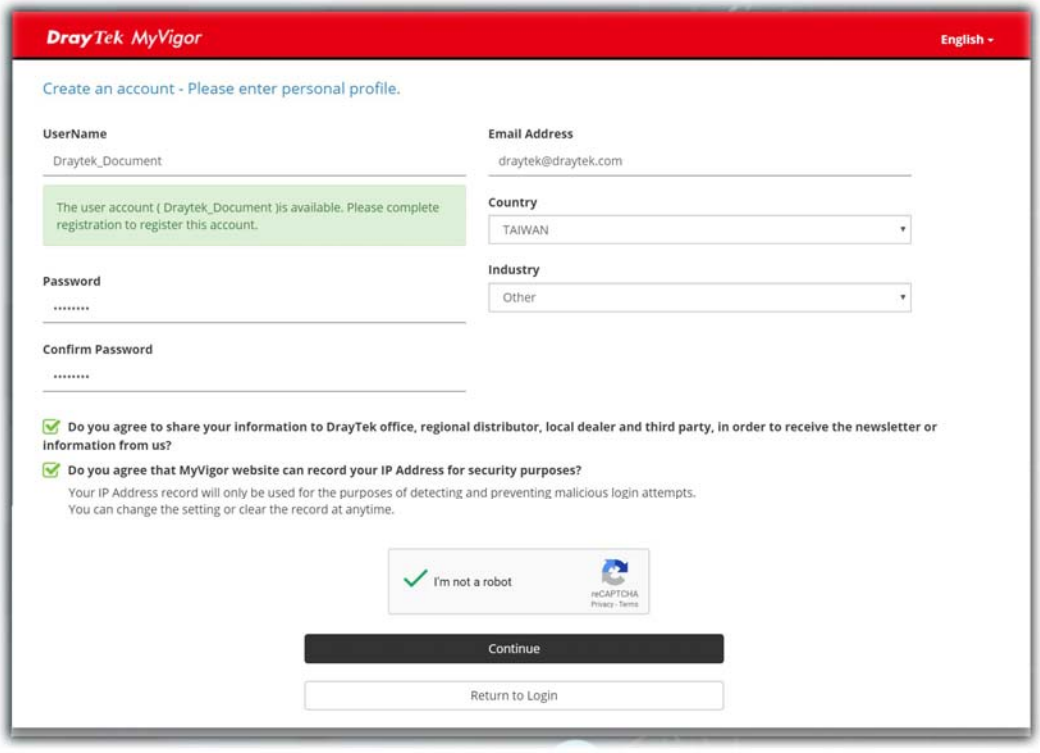
- If not, click **I am under 16 years old** to get the following page. Then, click **I and my legal guardian agree**.



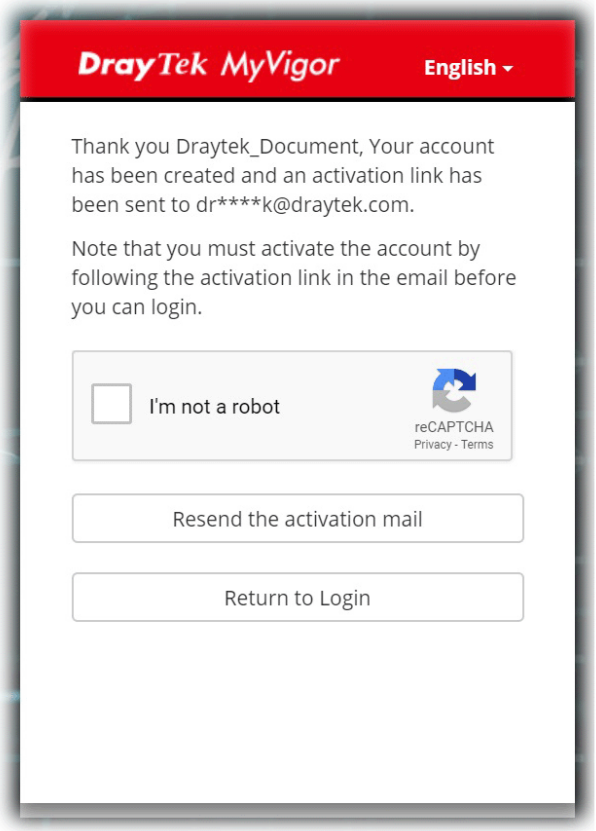

5. After reading the terms of service/privacy policy, click **Agree**.




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**.

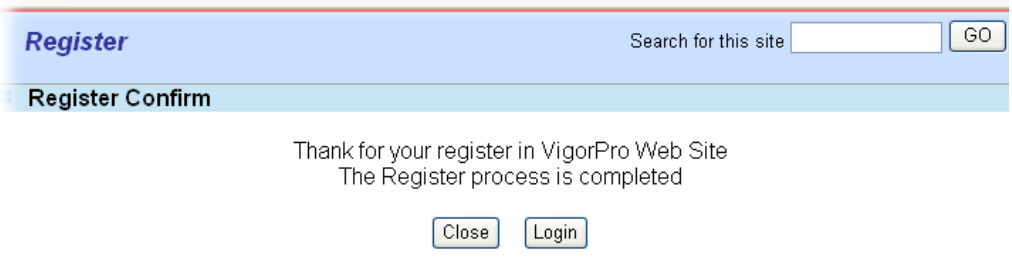
****** This is an automated message from myvigor.draytek.com. ******

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

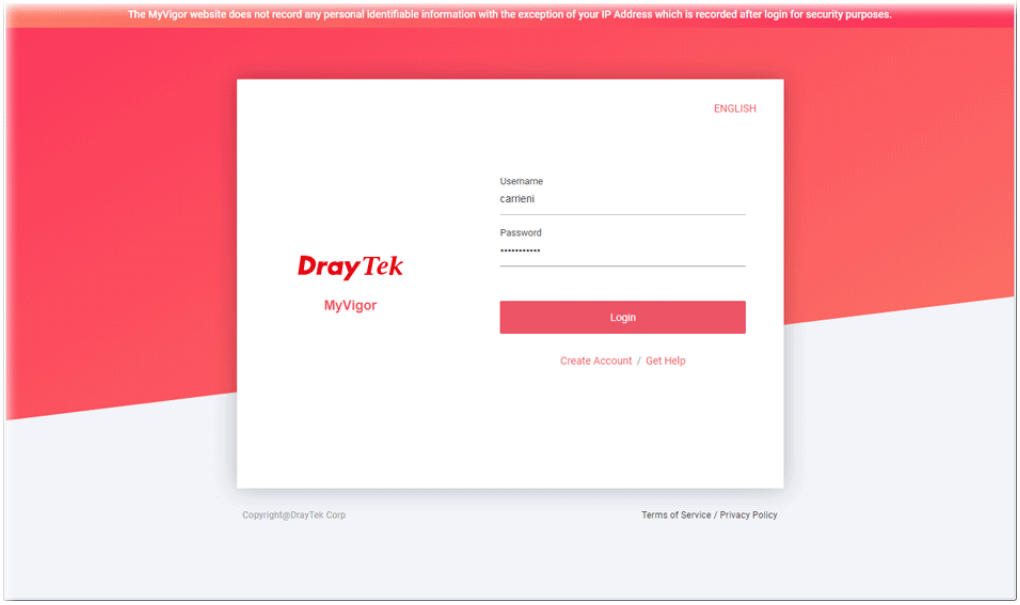
Please click on the activation link below to activate your account

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 Enter the account and password (that you just created) in the fields of **Username** and **Password**.




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

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

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

**Web Content Filter,**

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

Note: License is required.

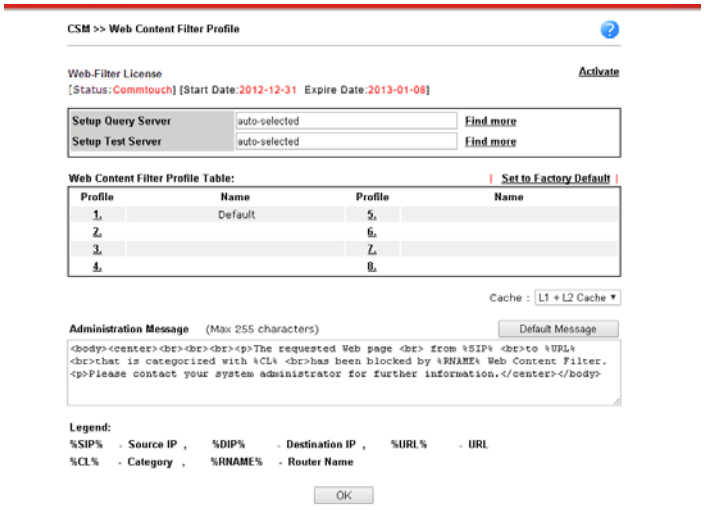
**URL Content Filter,**

Benefits: Free, flexible for customize webpage.

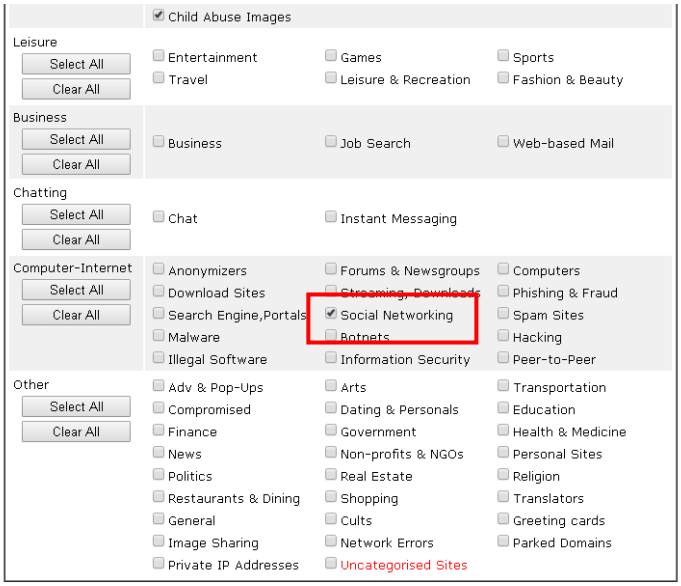
Note: Manual setting (e.g., one keyword for one website.)

### I. Via Web Content Filter

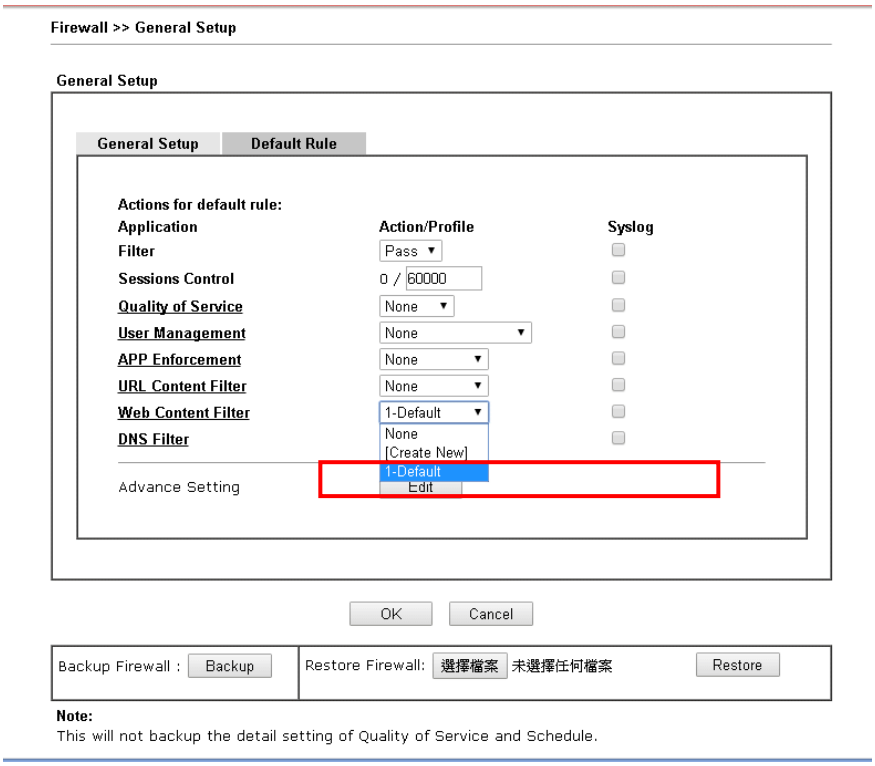
1. Make sure the Web Content Filter license is valid.




2. Open **CSM >> Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action**, Block**.




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



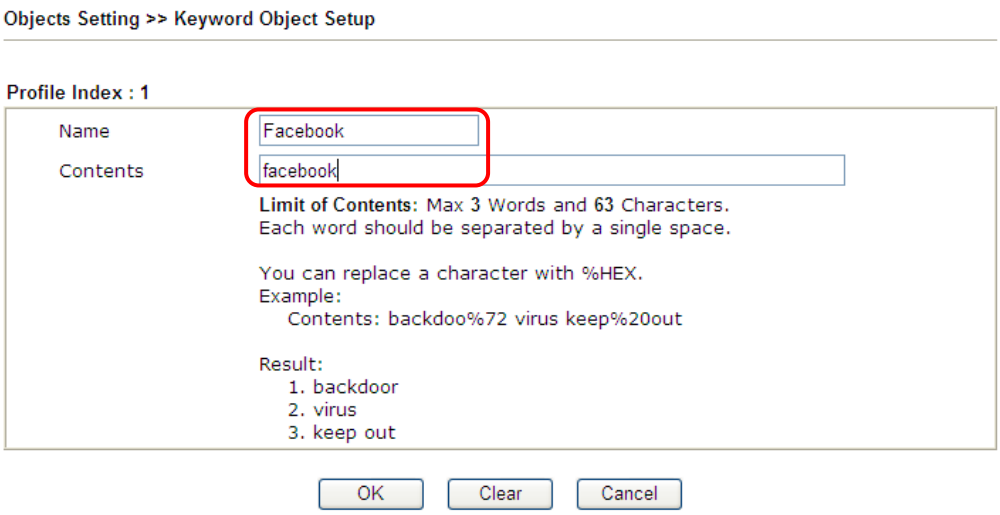

4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.




# II. Via URL Content Filter

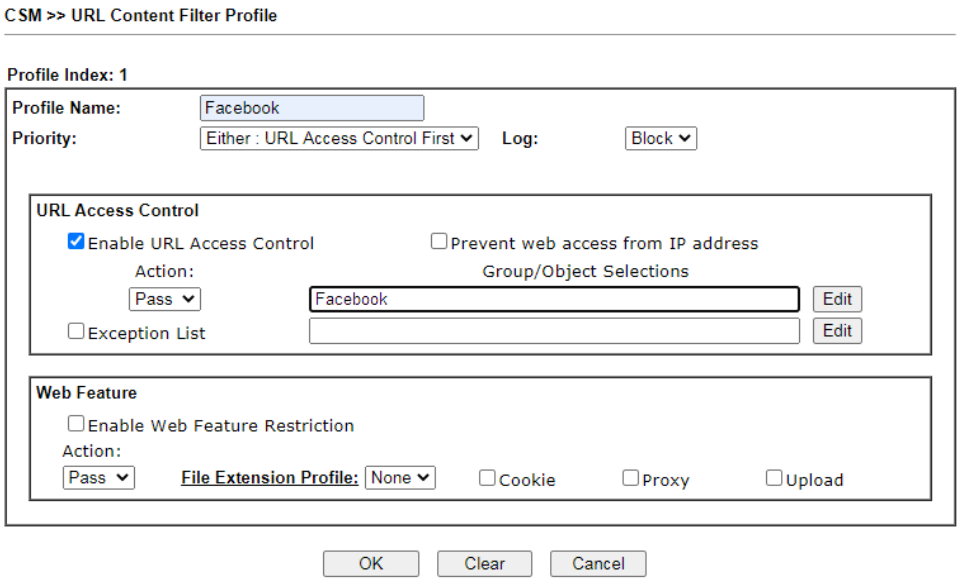
### A. Block the web page containing the word of "Facebook"

1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
2. In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.



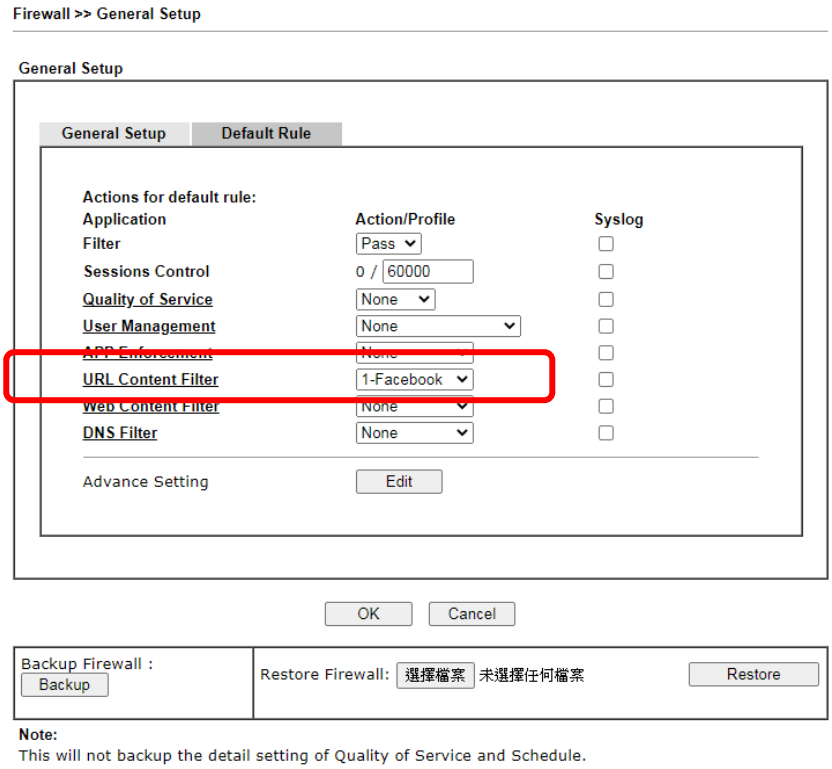

3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.




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

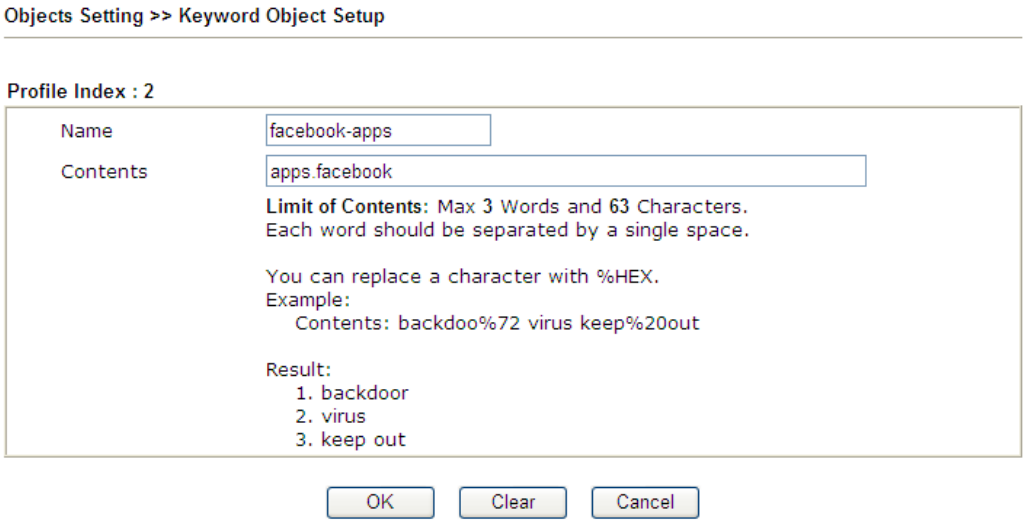
6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.




**B. Disallow users to play games on Facebook**

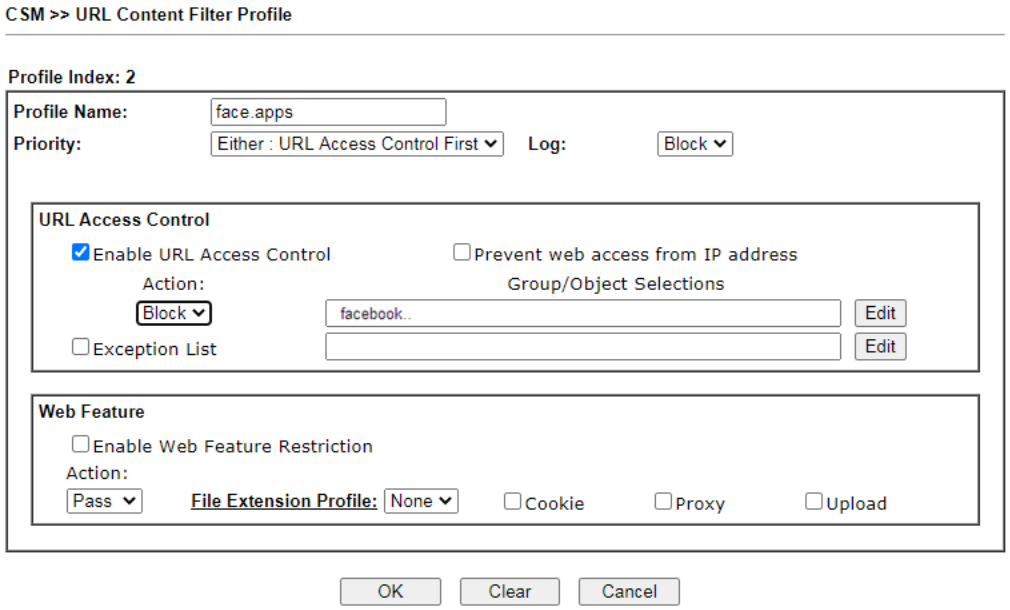
1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.

2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.



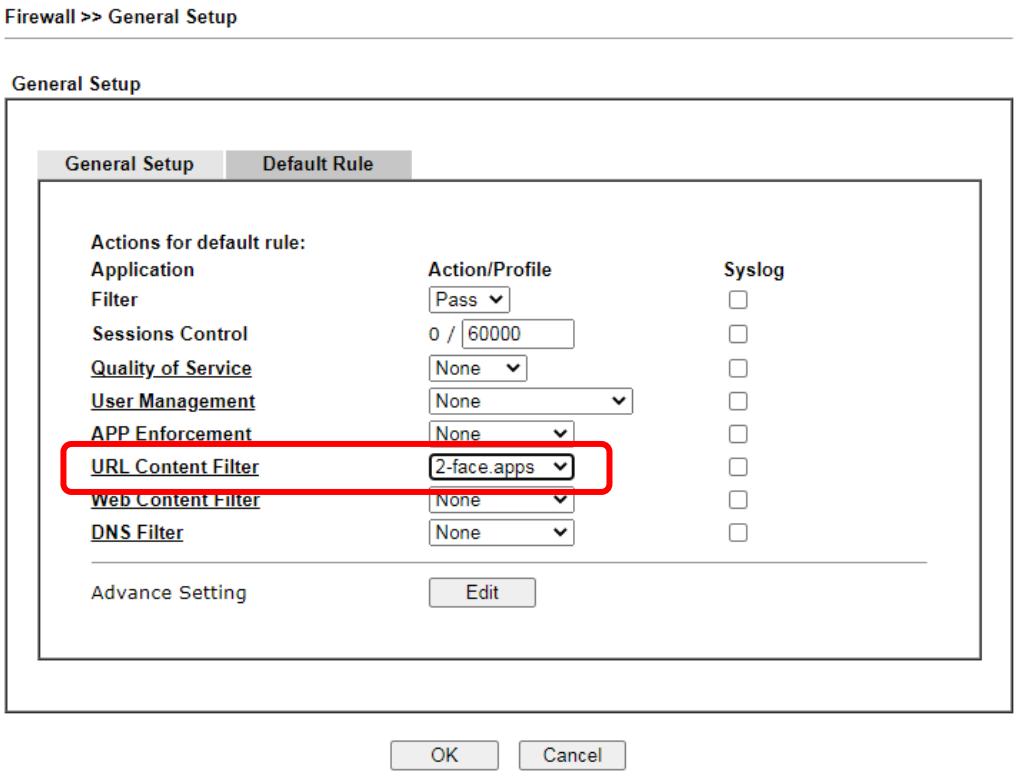
3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.

4. Configure the settings as the following figure.




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

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



This page is left blank.

# Part VI Management



System Maintenance

There are several items offered for the Vigor router system setup: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.



Bandwidth Management

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



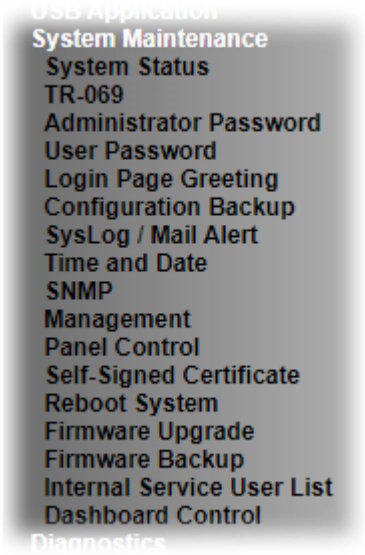
User Management

It is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password.

# VI-1 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade, Activation, Internal Service User List and Dashboard Control.

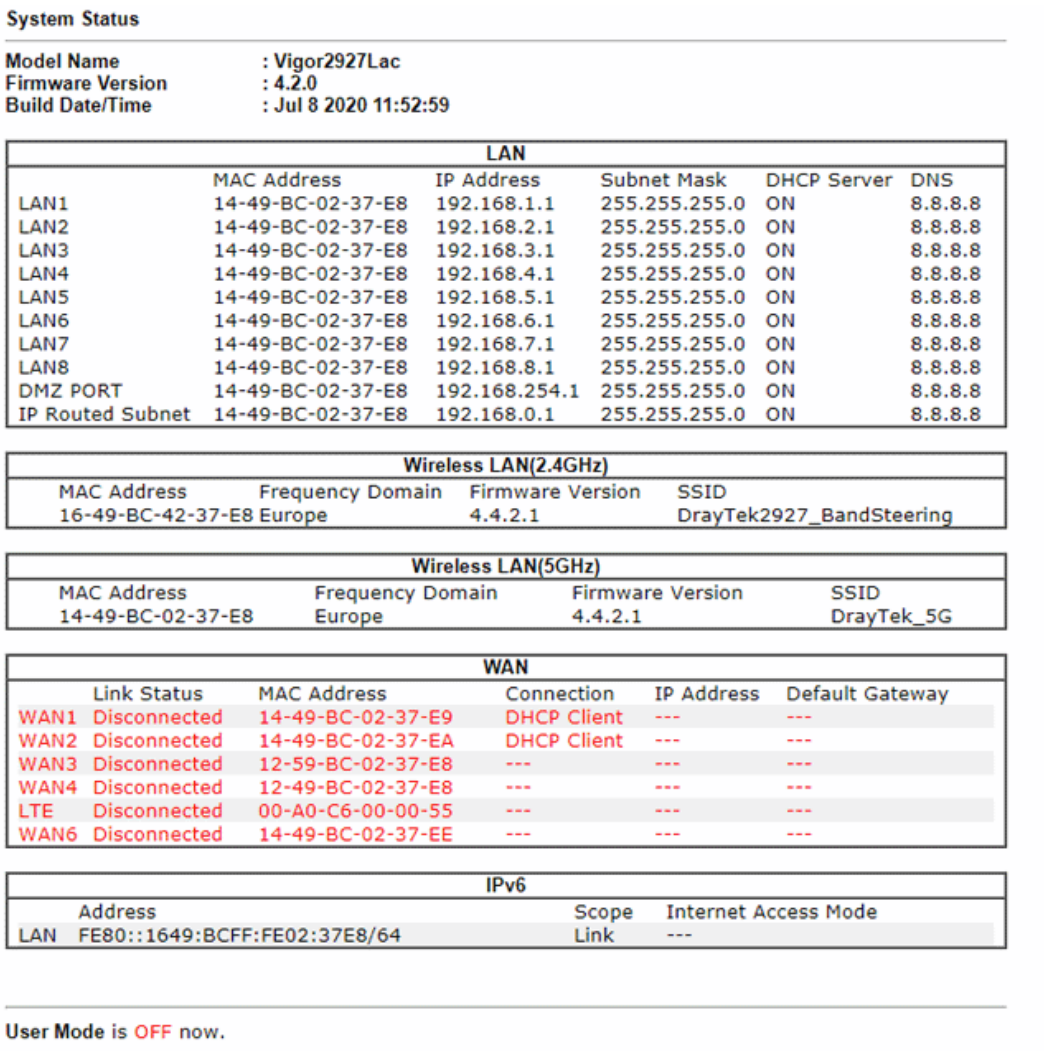
Below shows the menu items for System Maintenance.



# Web User Interface

## VI-1-1 System Status

The **System Status** displays basic network information of Vigor router including LAN and WAN interface status. Also available is the current firmware version and firmware related information.



System Status

Model Name : Vigor2927Lac
Firmware Version : 4.2.0
Build Date/Time : Jul 8 2020 11:52:59

LAN

| | MAC Address | IP Address | Subnet Mask | DHCP Server | DNS |
|---|---|---|---|---|---|
| LAN1 | 14-49-BC-02-37-E8 | 192.168.1.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN2 | 14-49-BC-02-37-E8 | 192.168.2.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN3 | 14-49-BC-02-37-E8 | 192.168.3.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN4 | 14-49-BC-02-37-E8 | 192.168.4.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN5 | 14-49-BC-02-37-E8 | 192.168.5.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN6 | 14-49-BC-02-37-E8 | 192.168.6.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN7 | 14-49-BC-02-37-E8 | 192.168.7.1 | 255.255.255.0 | ON | 8.8.8.8 |
| LAN8 | 14-49-BC-02-37-E8 | 192.168.8.1 | 255.255.255.0 | ON | 8.8.8.8 |
| DMZ PORT | 14-49-BC-02-37-E8 | 192.168.254.1 | 255.255.255.0 | ON | 8.8.8.8 |
| IP Routed Subnet | 14-49-BC-02-37-E8 | 192.168.0.1 | 255.255.255.0 | ON | 8.8.8.8 |

Wireless LAN(2.4GHz)

| MAC Address | Frequency Domain | Firmware Version | SSID |
|---|---|---|---|
| 16-49-BC-42-37-E8 | Europe | 4.4.2.1 | DrayTek2927_BandSteering |

Wireless LAN(5GHz)

| MAC Address | Frequency Domain | Firmware Version | SSID |
|---|---|---|---|
| 14-49-BC-02-37-E8 | Europe | 4.4.2.1 | DrayTek_5G |

WAN

| | Link Status | MAC Address | Connection | IP Address | Default Gateway |
|---|---|---|---|---|---|
| WAN1 | Disconnected | 14-49-BC-02-37-E9 | DHCP Client | --- | --- |
| WAN2 | Disconnected | 14-49-BC-02-37-EA | DHCP Client | --- | --- |
| WAN3 | Disconnected | 12-59-BC-02-37-E8 | --- | --- | --- |
| WAN4 | Disconnected | 12-49-BC-02-37-E8 | --- | --- | --- |
| LTE | Disconnected | 00-A0-C6-00-00-55 | --- | --- | --- |
| WAN6 | Disconnected | 14-49-BC-02-37-EE | --- | --- | --- |

IPv6

| | Address | Scope | Internet Access Mode |
|---|---|---|---|
| LAN | FE80::1649:BCFF:FE02:37E8/64 | Link | --- |

User Mode is OFF now.

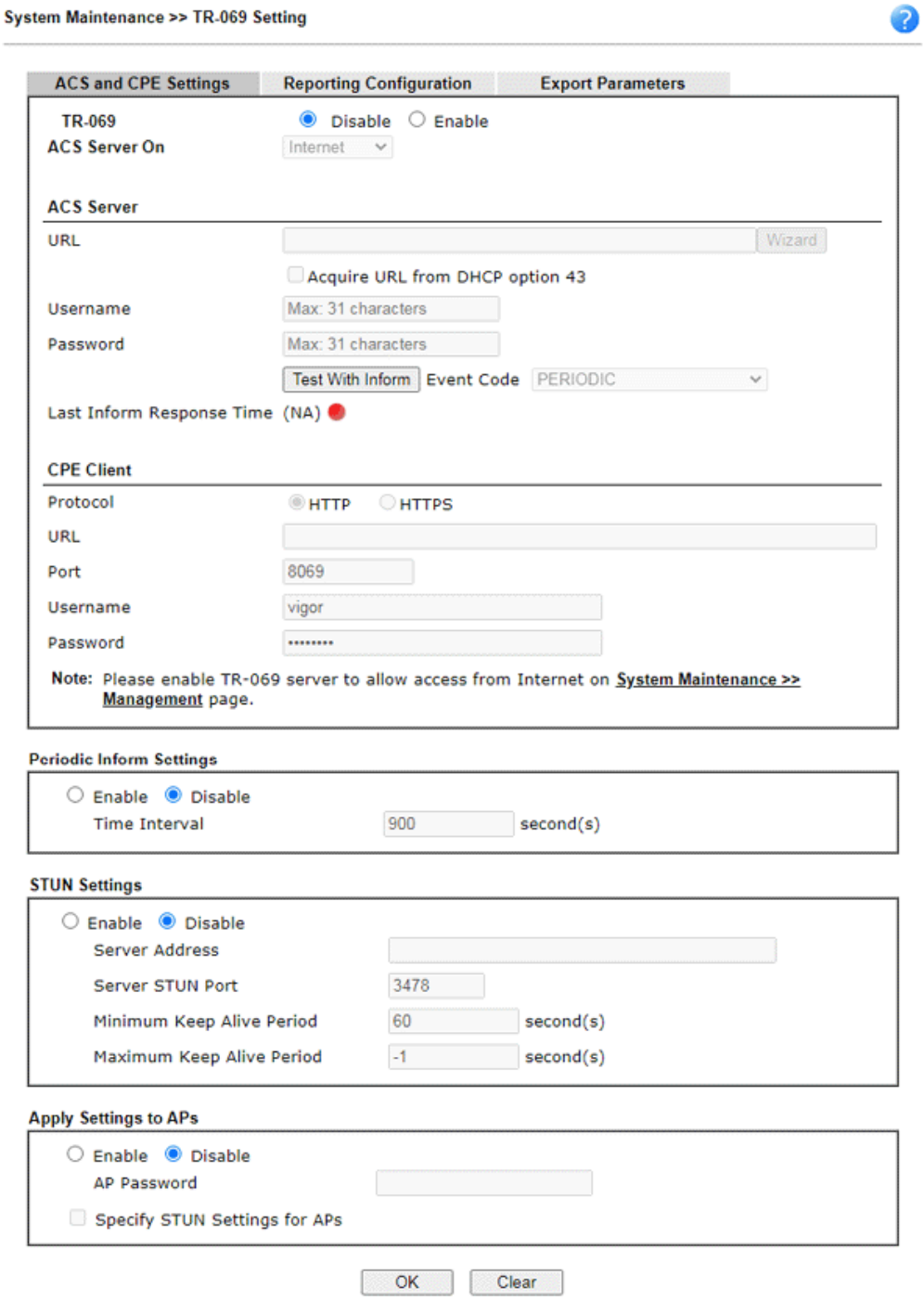
Available settings are explained as follows:

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

| | |
|---|---|
| | **-** Displays the subnet mask address of the LAN interface.<br>**DHCP Server**<br>**-** Displays the current status of DHCP server of the LAN interface.<br>**DNS**<br>**-** Displays the assigned IP address of the primary DNS. |
| **Wireless LAN** | **MAC Address**<br>**-** Displays the MAC address of the LAN Interface.<br>**Frequency Domain**<br>- Displays the frequency domain.<br>**Firmware Version**<br>- Displays the firmware version.<br>**SSID**<br>- Displays the name of the SSID. |
| **WAN** | **Link Status**<br>**-** Displays current connection status of the WAN interface.<br>**MAC Address**<br>**-** Displays the MAC address of the WAN Interface.<br>**Connection**<br>**-** Displays the connection type of the WAN interface..<br>**IP Address**<br>**-** Displays the IP address of the WAN interface.<br>**Default Gateway**<br>**-** Display the assigned IP address of the default gateway. |
| **IPv6** | **Address -** Displays the IPv6 address for LAN.<br>**Scope -** Displays the scope of IPv6 address. For example, **IPv6 Link Local** is non-routable and can only be used for local connections.<br>**Internet Access Mode –** Displays the connection mode of the WAN interface. |

## VI-1-2 TR-069

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **TR-069** | Enables or disables TR-069 functionality. |
| **ACS Server On** | Choose the interface for connecting the router to the Auto Configuration Server. |

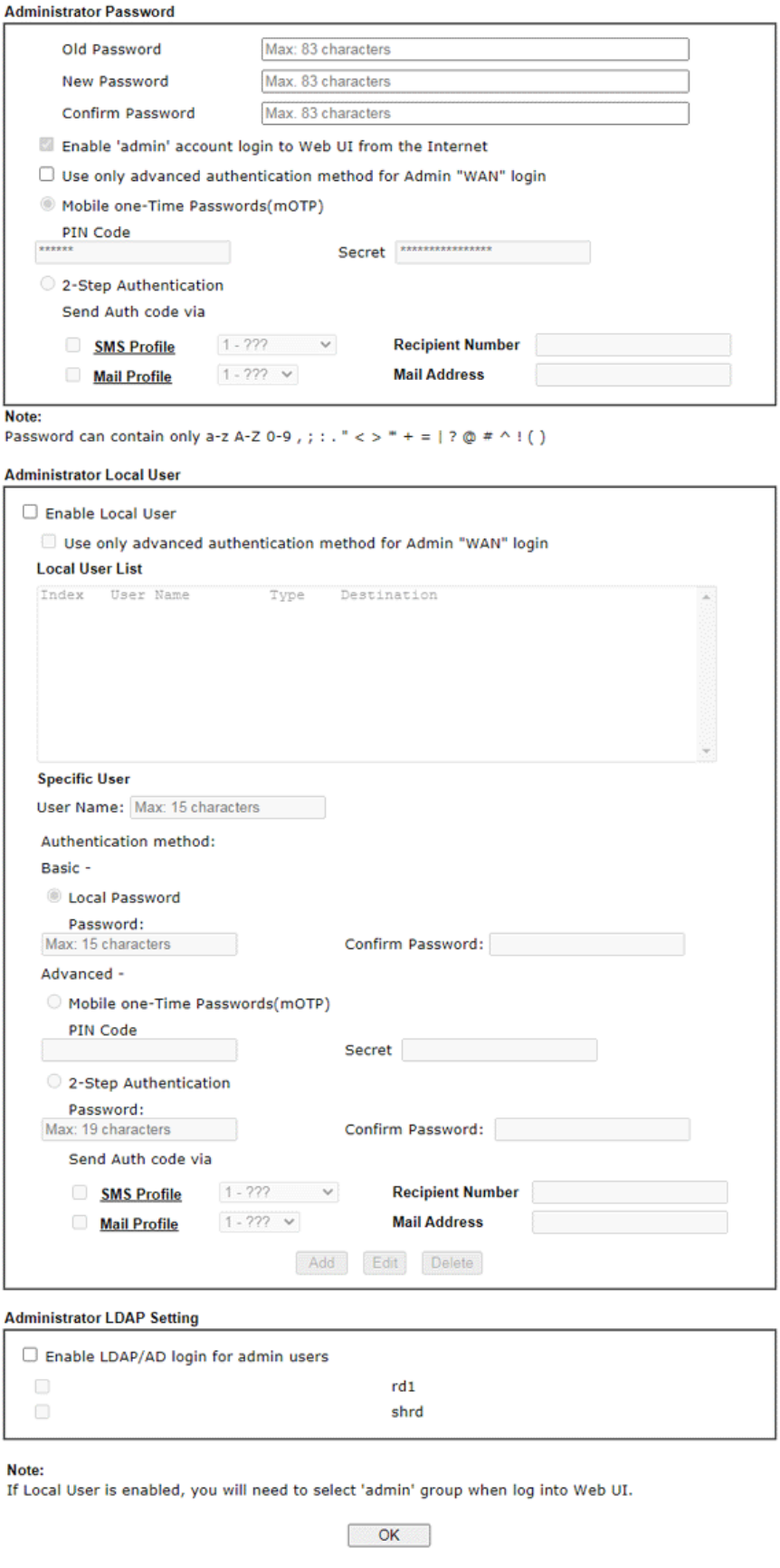
| | |
|---|---|
| **ACS Server** | This section specifies the settings of the ACS Server.<br>**URL –** Enter the URL for connecting to the ACS. Please refer to the Auto Configuration Server user's manual for detailed information.<br>● **Wizard** – Click it to enter the IP address of VigorACS server, port number and the handler.<br>● **Acquire URL form DHCP option 43** – Select to acquire the ACS URL from DHCP option 43.<br>**Username/Password –** Enter the credentials required to connect to the ACS server.<br>● **Test With Inform** – Click to send an inform message using the selected Event Code to test if the CPE is able to communicate with the VigorACS server.<br>● **Event Code** – Select an event for the inform test.<br>**Last Inform Response Time** – Displays the time of the most recent Inform Response message received from the VigorACS. |
| **CPE Client** | This section specifies the settings of the CPE Client.<br>**Http / Https** – Select Https if the connection is encrypted; otherwise select Http.<br>**Port** – In the event of port conflicts, change the port number of the CPE.<br>**Username** and **Password** – Enter the username and password that the VigorACS will use to connect to the CPE. |
| **Periodic Inform Settings** | **Enable** – The default setting is Enable, which means the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field.<br>● **Time Interval** - Set interval time or schedule time for the router to send notification to CPE.<br>**Disable** - Select **Disable** to turn off periodic notifications. |
| **STUN Settings** | STUN allows the ACS Server to connect to the CPE Client even when the client is behind a network address translator (NAT).<br>**Disable** - The default setting is Disable.<br>**Enable** - Please Enter the relational settings listed below:<br>● **Server Address –** Enter the IP address of the STUN server.<br>● **Server Port –** Enter the port number of the STUN server.<br>● **Minimum Keep Alive Period –** If STUN is enabled, the CPE must periodically transmit binding requests to the server for the purpose of maintaining the binding with the Gateway. Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. The default setting is 60 seconds.<br>● **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding with the Gateway. Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server. A value of -1 indicates that no maximum period is specified. |

| | |
|---|---|
| **Apply Settings to APs** | This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor2927 at the same time.<br>**Disable** – TR-069 and Related settings will not be applied to VigorAPs.<br>**Enable** – TR-069 settings will be applied to VigorAPs after clicking **OK**. The VigorAP password must be specified.<br>● **AP Password** – Enter the password of the VigorAP that you want to apply Vigor2927's TR-069 settings.<br>**Specify STUN Settings for APs** – After clicking the **Enable** radio button for Apply Settings to APs, if you want to apply specific STUN settings (i.e., different from the Vigor2927 STUN settings) to VigorAPs to meet specific requirements, check this box and enter the server IP address, server port, and minimum and maxmum keep alive periods respectively. |

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

## VI-1-3 Administrator Password

This page allows you to set or change the administrator password.



Available settings are explained as follows:

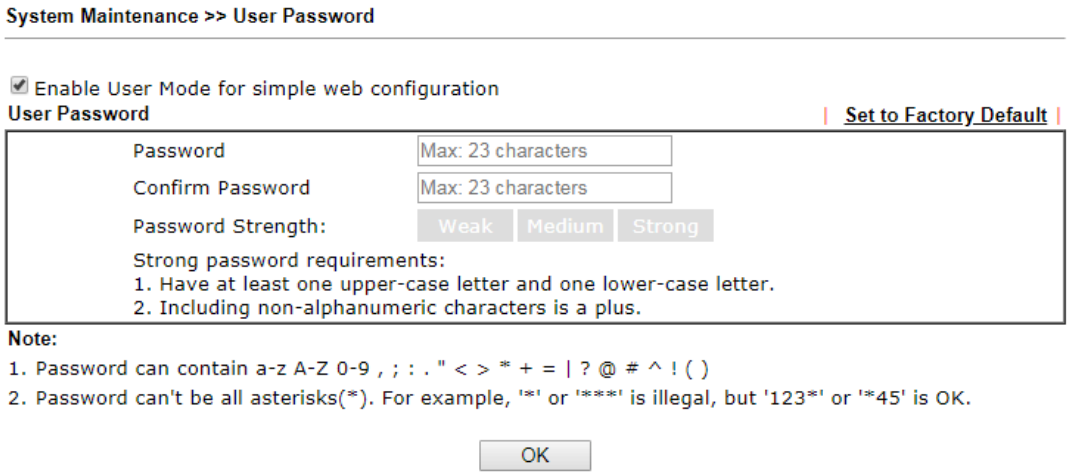
| Item | Description |
|---|---|
| **Administrator Password** | The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements.<br>**Old Password** - Enter the current password. The factory default is "admin".<br>**New Password** – Enter the new password. The maximum length of the password is 23 characters.<br>**Confirm Password** – Enter the new password again for confirmation.<br>**Enable 'admin' account login to Web UI from the Internet** – Select to allow the administrator to log in from the Internet. This option is enabled when Administrator Local User is enabled (see below).<br>**Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN.<br>● **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the PIN Code and Secret settings for getting one-time passwords.<br>● **2-Step Auth code via SMS Profile and/or Mail Profile –** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. |
| **Administrator Local User** | Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router.<br>This feature allows you to add more administrators who can then log in to the web interface, with the same privileges as the administrator.<br>**Enable Local User** – Check the box to allow other users to administer the router.<br>● **Use only advanced authentication method for Admin "WAN" login** – Advanced authentication method can offer a **more secure** network connection. In general, the above basic password setting will be used for authentication if such option is disabled. Simply check the box to enable the following settings.<br>● **Local User List** – Shows all the users that are set up to administer the router.<br>● **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.<br>➢ **User Name** – Enter a user name.<br>● **Authentication method –** Select from **Basic** or **Advanced** authentication methods.<br>**Basic** – Static passwords will be used to authenticate users.<br>➢ **Local Password** – Enter the password for the local user.<br>**Advanced** - Mobile One-time Passwords (mOTP) or |

| | |
|---|---|
| | 2-step authentication will be used to authenticate users.<br>➢ **Mobile one-Time Password (mOTP)** – Select to allow the use of mOTP passwords. Enter the mOTP PIN Code and Secret that will be used to generate the one-time passwords.<br>➢ **2-Step Authentication via SMS Profile and/or Mail Profile –** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password.<br>● **Add** – After entering the user name and password above, click this button to create a new local user. The new user will be shown on the Local User List immediately.<br>● **Edit** – If you wish to change a user in the Local User List, select it, perform the necessary modifications, and click this button to update the user.<br>● **Delete** – If you wish to delete a user in the Local User List, select it and click this button to remove it. |
| **Administrator LDAP Setting** | **Enable LDAP/AD login for admin users** – Select to allow authentication using an LDAP/Active Directory Server.<br>**LDAP Server Profiles Setup** – Click to set up the LDAP/Active Directory server. |

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

## VI-1-4 User Password

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




Available settings are explained as follows:

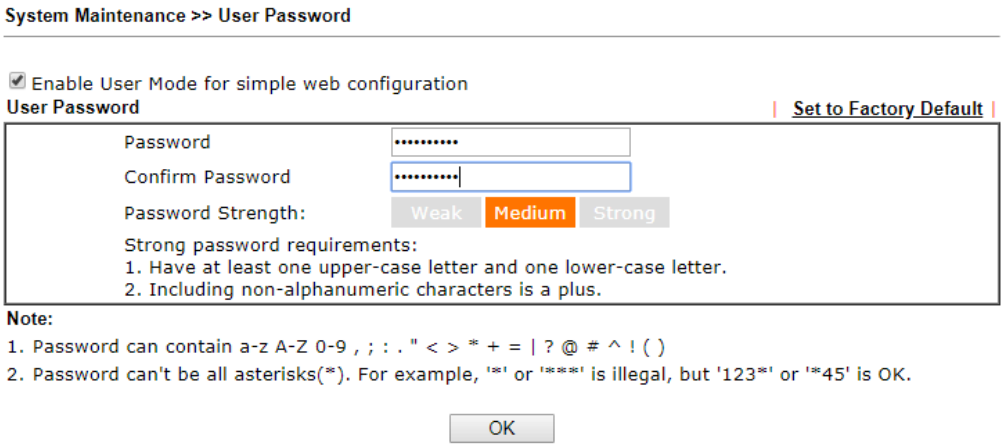
| Item | Description |
|---|---|
| **Enable User Mode for simple web configuration** | Check this box to enable User Mode for web user interface with the password typed here for simple web configuration.<br>The simple web user interface settings differ from those on the full web user interface seen when logged in using the administrator password. |
| **Password** | Enter the password. The maximum length of the password is 31 characters. |
| **Confirm Password** | Enter the password again for verification. |
| **Password Strength** | Shows the security strength of the password specified above. |
| **Set to Factory Default** | Click to return to the factory default setting. |

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

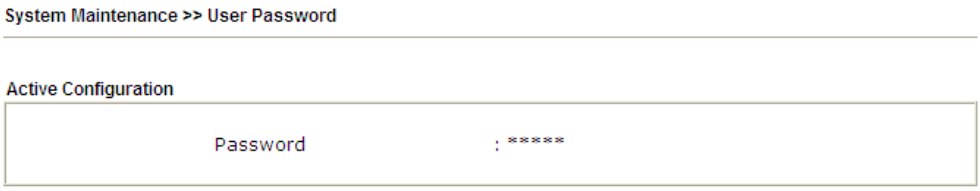
Here are the steps involved in setting up the router for User Mode Access:

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

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



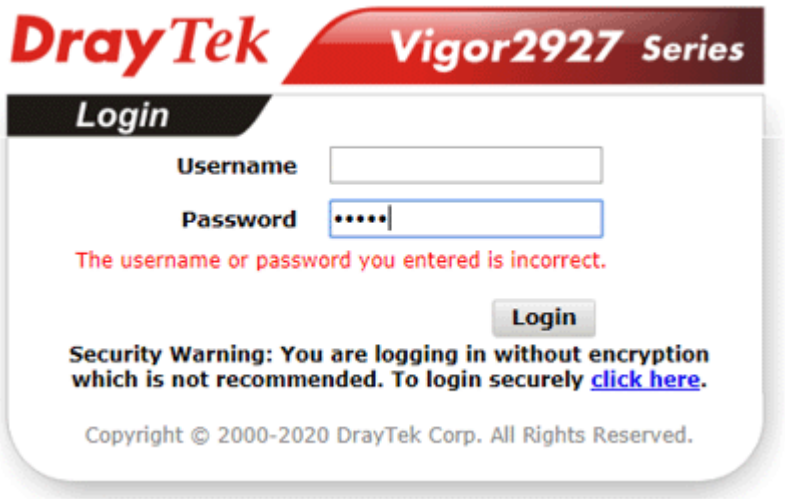

3. The following screen will appear. Click **OK**.



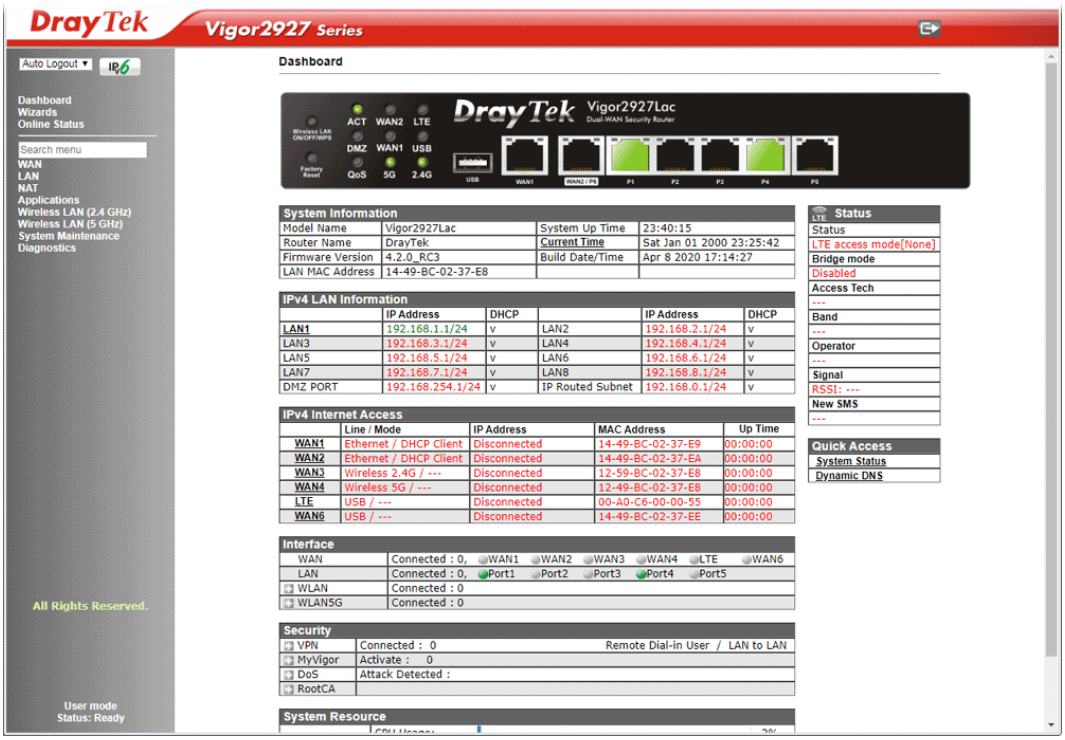

4. Log out the Vigor router web user interface by clicking the Logout button.




5. The following window will be shown. Enter the new user password in the **Password** field and click **Login**.



6. The main screen with User Mode will be shown:




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

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

## VI-1-5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Login Page Logo** | Set an image which will be shown above the log in window.<br>**Default -** The **Enable Greeting** feature is available to set the login page title.<br>**Blank -** No image / no greeting.<br>**Upload a file -** Choose an image file and click Upload. Later the selected image will be shown on the log in window. |
| **Enable Greeting** | Check this box to enable the login customization function. |
| **Login Page Title** | Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog. |
| **Welcome Message and Bulletin** | Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom.<br>Note that do not enter URL redirect link here. |
| **Preview** | Click to preview the customized login window based on the settings entered on this page. |
| **Set to Factory Default** | Click to return to the factory default setting. |

Below shows an example of a customized login page with the values entered in the **Login Page Title** and **Welcome Message and Bulletin** fields.



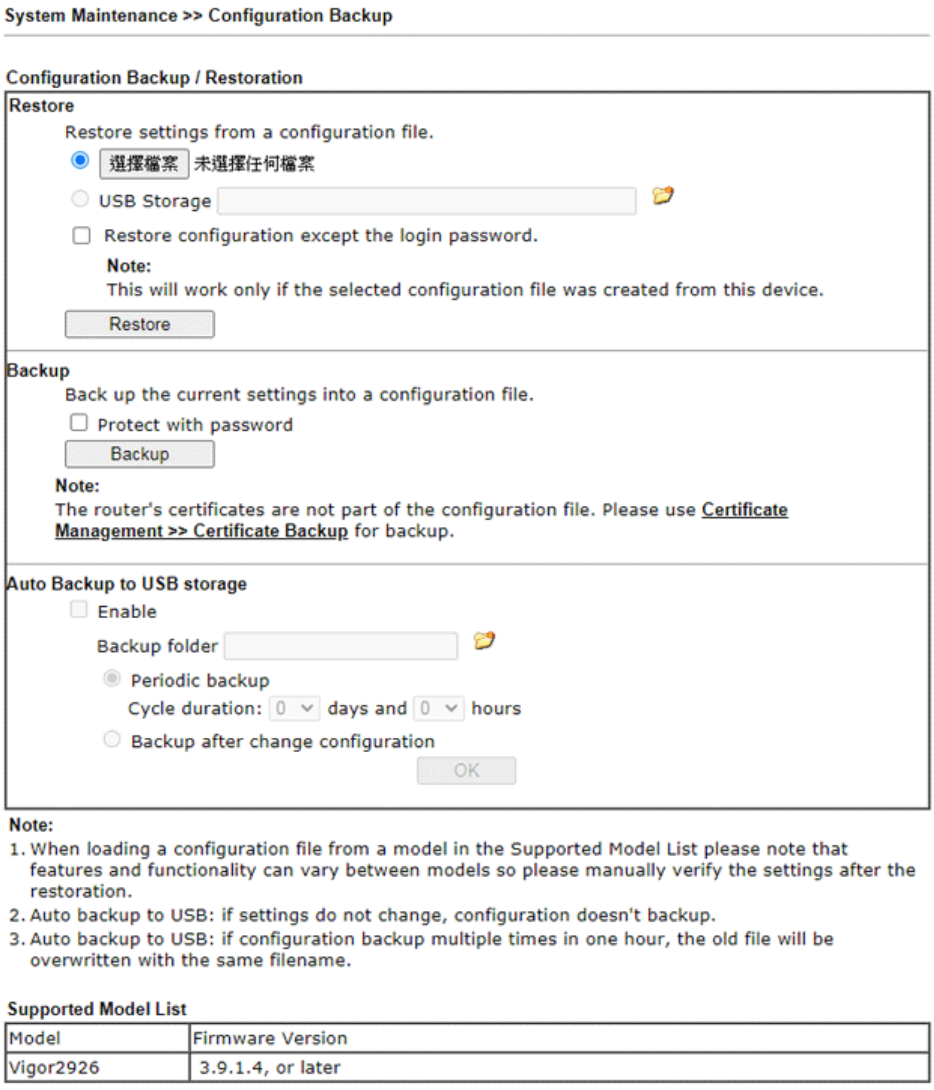
## VI-1-6 Configuration Backup

This function allows the backup and restoration of router settings. In addition to restoring Vigor2927's own configuration backup, it is possible to restore backups from certain DrayTek routers such as Vigor2820, Vigor2830 and Vigor2850 series on the Vigor2927.

### Backing up the Configuration

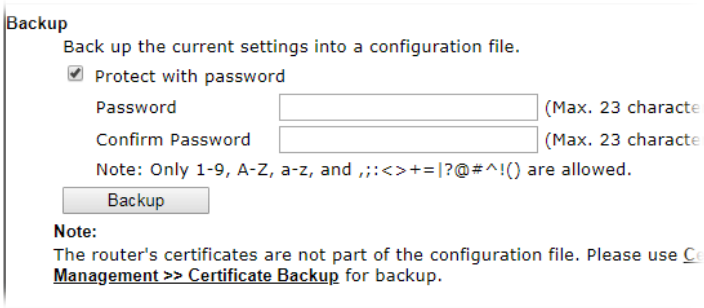
Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following page will be shown.

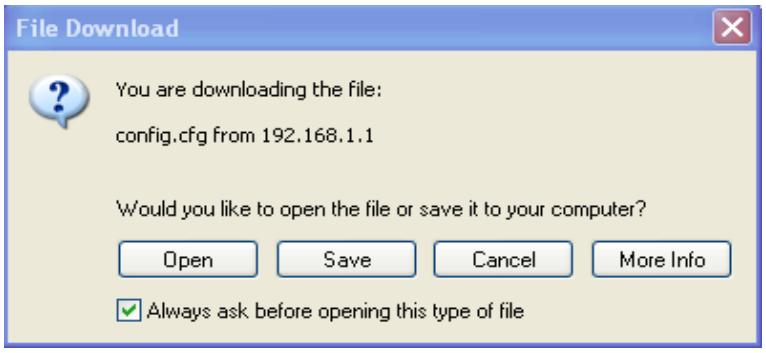



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Restore** | **Restore settings from a configuration file** – Click the **Select File** button to specify a file to be restored or click **USB Storage** (if a USB storage disk connected) to choose the configuration file.<br>**Restore configuration except the login password** – Select to exclude the password from getting restored from the backup.<br>**Restore** - Click to initiate restoration of configuration. If the |

| | |
|---|---|
| | backup file is encrypted, you will be asked to enter the password. |
| **Backup** | Click it to perform the configuration backup of this router.<br>**Protect with password-** Select to encrypt the backup with a password. You will be prompted to enter the password as shown below:<br>  <br>● **Password** – Enter a new password for encrypting the configuration file.<br>● **Confirm Password** – Enter the new password again for confirmation.<br>**Backup** - Click to initiate the backup process. |
| **Auto Backup to USB storage** | The configuration can be stored to a USB connecting to Vigor router as a backup.<br>**Enable** - Check the box to enable the function.<br>**Backup folder** – Set the path for downloading.<br>**Periodic backup** – Set the circle duration for backup.<br>**Backup after change configuration** – Backup will be executed whenever the configuration is changed. |

2. Click the **Backup** button, and the File Download dialog will be shown. Depending on your browser, you may be prompted to select a location to save the file, or the file may be saved in the default download location of your browser.



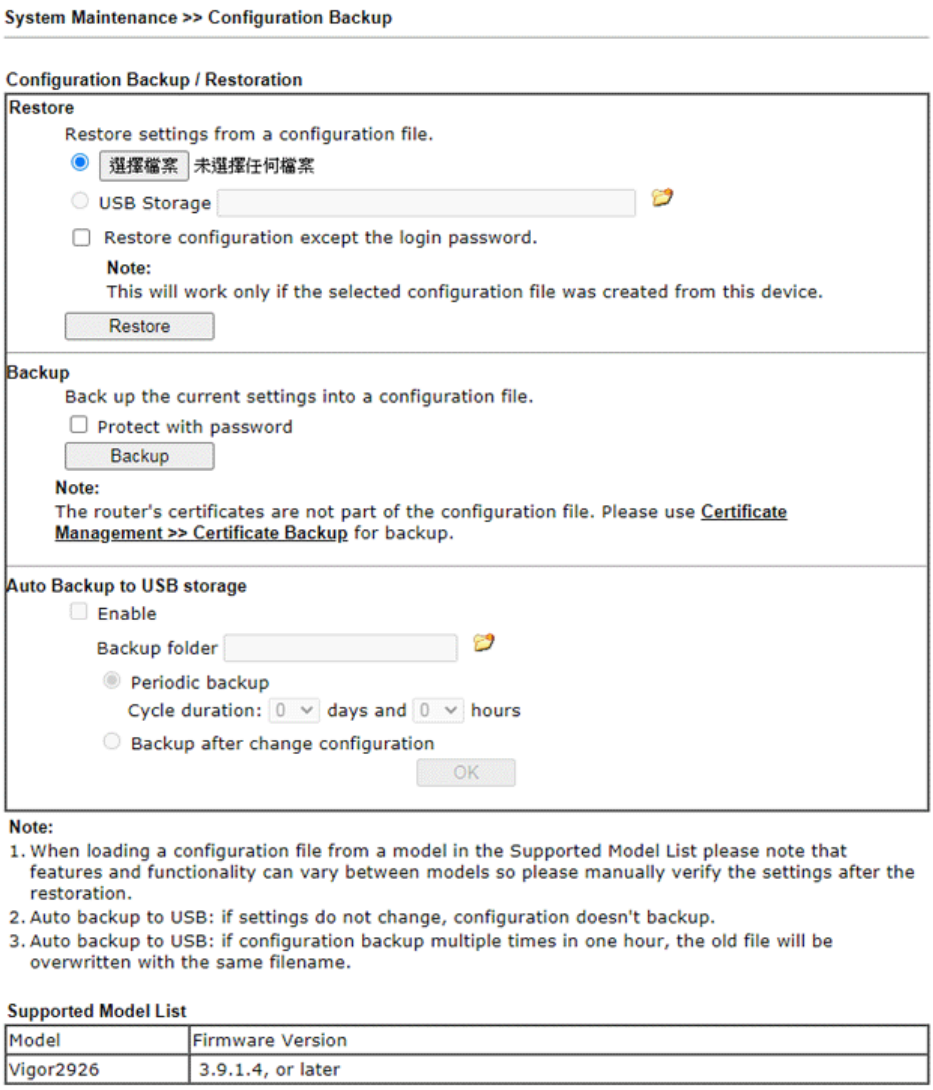

The configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

| | |
|---|---|
| **Info** | Configuration Backup does not include certificates stored on the router. Please back up certificates separately by going to **Certificate Management >> Certificate Backup**. |

## Restoring the Configuration

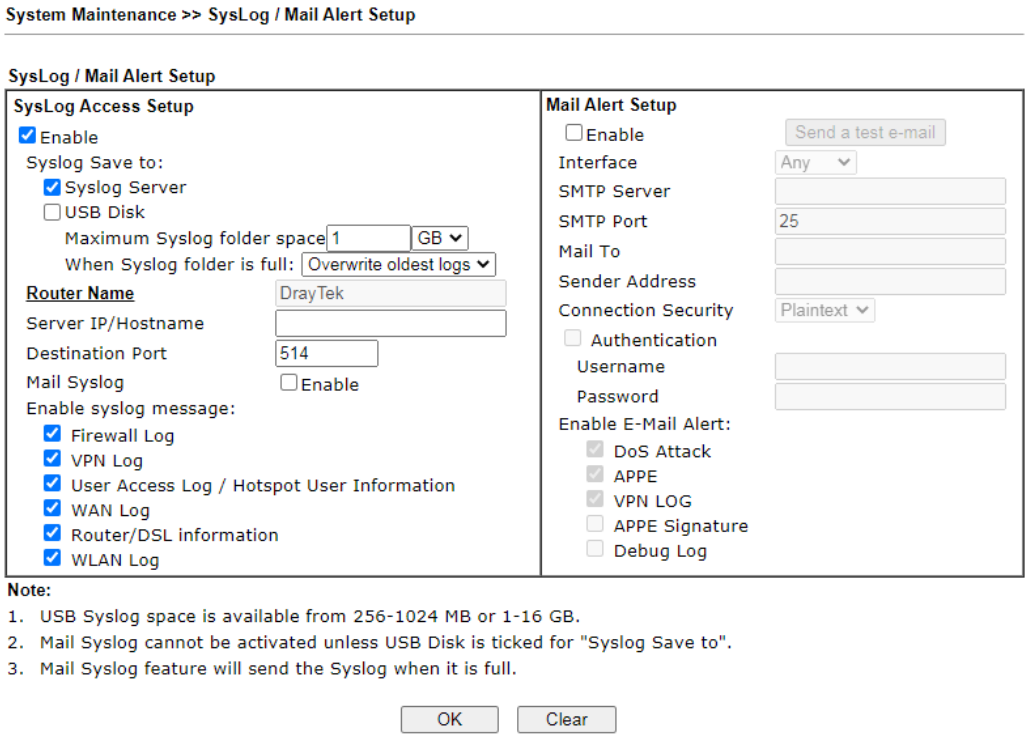
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be shown.




2. Click the **Choose File** button under **Backup** to bring up the open file dialog box to select the configuration file to be uploaded and restored.
3. Click the **Restore** button and wait for few seconds.

## VI-1-7 Syslog/Mail Alert

SysLog function is provided for users to monitor router.




Available settings are explained as follows:

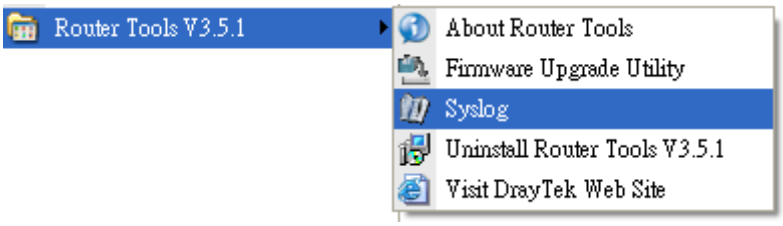
| Item | Description |
|---|---|
| **SysLog Access Setup** | **Enable** - Select to enable the Syslog function.<br>**Syslog Save to** – Check Syslog Server and / or USB Disk.<br>● **Syslog Server** – Events will be sent to a Syslog server.<br>● **USB Disk** – Events will be saved to a USB storage device connected to the router.<br>● **Maximum Syslog folder space** - Set a space (unit GB/MB) to store event logs.<br>● **When Syslog folder is full** - Specify the action (overwrite the olderest logs or stop logging) to be executed. |
| **Router Name** | Shows the name of the router set in **System Maintenance >> Management**. This name will be used to identify the router in the Syslog entries.<br>To set or modify the router name, click the hyperlink and you will be taken to **System Maintenance >> Management** where you can enter the value.<br>**Server IP Address /Hostname -** Enter the IP address / hostname of the Syslog server.<br>**Destination Port -** Enter the port for the Syslog server.<br>**Mail Syslog –** Select to enable sending Syslog messages by |

| | |
|---|---|
| | email.<br><br>**Enable syslog message -** Select the events to be recorded by syslog. |
| **Mail Alert Setup** | **Enable** - Select to enable the Mail Alert.<br><br>**Send a test e-mail -** Click to send a test email message using the settings below.<br><br>**Interface** - Specify the WAN interface for a mail passing through.<br><br>**SMTP Server** - Enter the address of the SMTP server used to send email.<br><br>**SMTP Port -** Enter the port of the SMTP server. Default setting is 25.<br><br>**Mail To -** Enter the email address of the recipient.<br><br>**Return-Path -** Enter the return path of the email messages. Email messages that cannot be delivered will be returned to this address.<br><br>**Connection Security** - Select a method (Plaintext, SSL or StartTLS) to ensure the connection security. SSL means to use port 465 for SMTP server for some e-mail server uses https as the transmission method.<br><br>● Accept using plain text if StartTLS connection failed.<br><br>● Force StartTLS. Stop if StartTLS connection failed.<br><br>**Authentication -** Select this checkbox and enter the username and password if the SMTP server requires authentication.<br><br>● **User Name -** Enter the user name for authentication.<br><br>● **Password -** Enter the password for authentication.<br><br>**Enable E-mail Alert -** Select the event types that will trigger email alerts. |

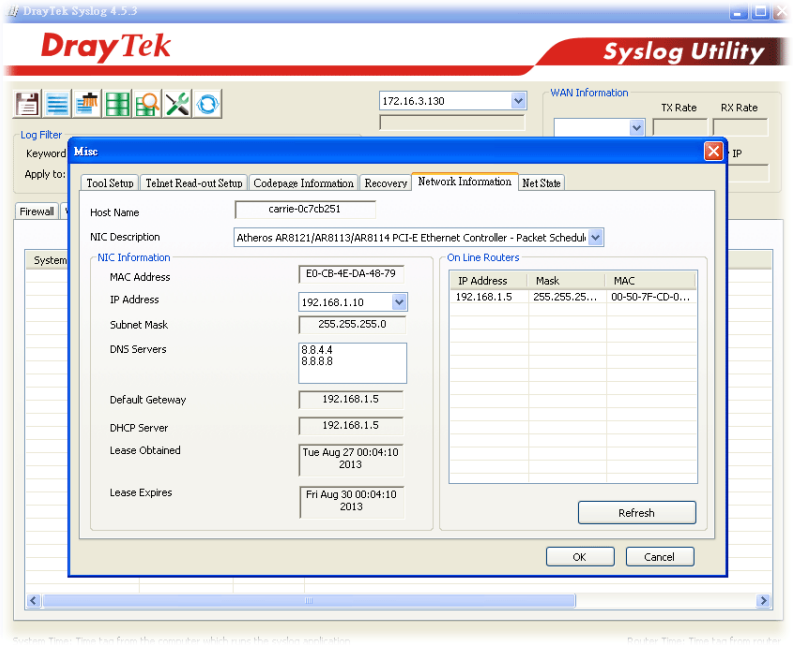
Select **OK** to save changes on the page, or **Clear** to reset all settings to factory defaults.

To view the Syslog message, please follow the steps below:

1. On the **Syslog / Mail Alert Setup** screen, enter the monitor PC's IP address in the **Server IP Address** field.
2. Install the Router Tools from DrayTek web site. After installation, start Syslog by clicking on **Router Tools>>Syslog** in the Windows Start Menu.

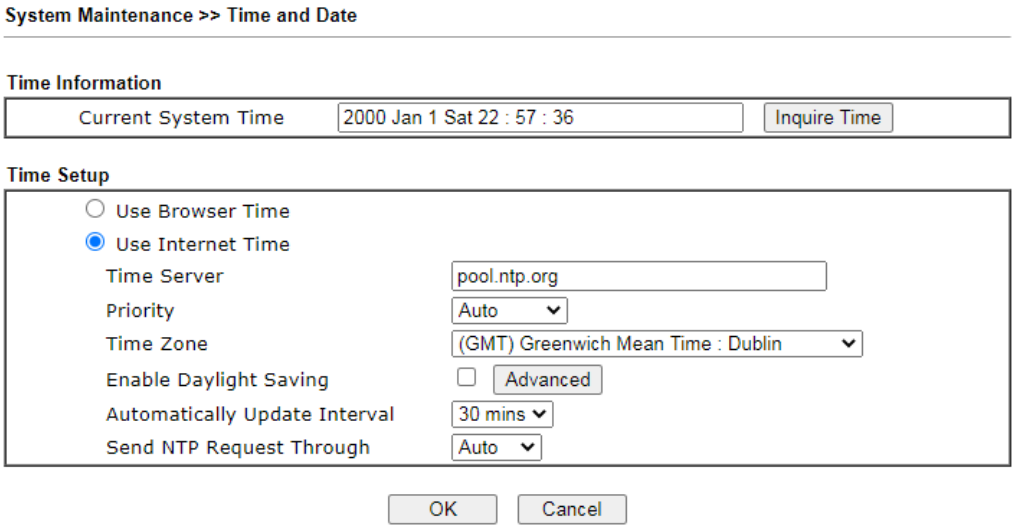


3. In the Syslog application, select the router you wish to monitor. Rember to select the network adapter to be used to connect to the router under Network Information, or else Syslog traffic cannot be received from the router.

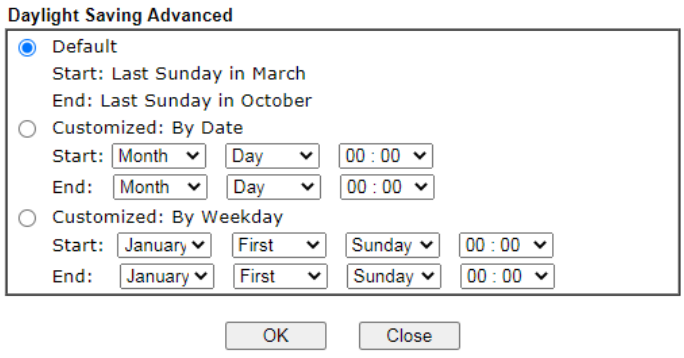


## VI-1-8 Time and Date

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Current System Time** | Click **Inquire Time** to retrieve the current time from the time server. |
| **Use Browser Time** | Select this option to let the router set its system time using the time reported by the web browser. |
| **Use Internet Time** | Select this option to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP). |
| **Time Server** | Enter the address of the time server. |
| **Priority** | Select **Auto** or **IPv6 First** as the priority. |
| **Time Zone** | Select the time zone where the router is located. |
| **Enable Daylight Saving** | Check the box to enable Daylight Saving Time (DST) if it is applicable to your location.<br>**Advanced** – Click to enter a custom schedule to enable DST.<br>  <br><br>Use the default time setting or set user defined time for your requirement.<br>**Default** – Uses the default DST schedule for the time zone. |

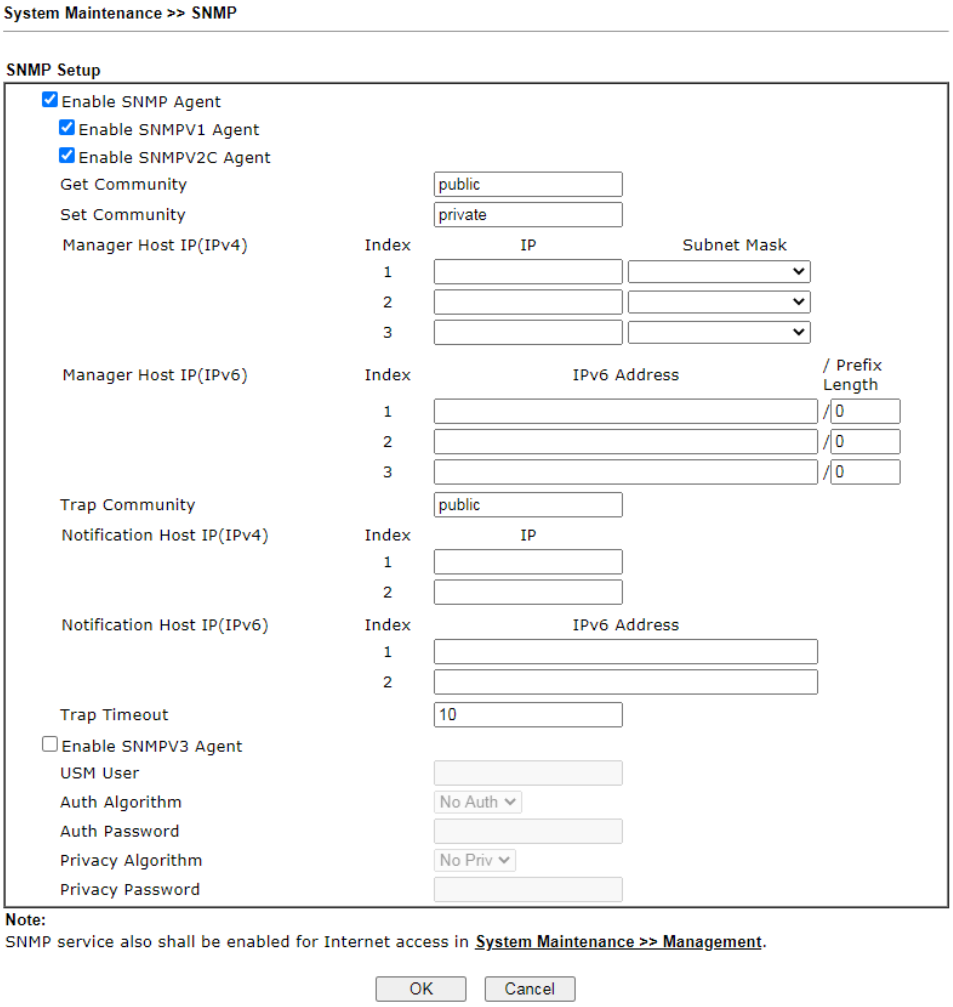
| | |
|---|---|
| | **Date Range** – Select this option if DST starts and ends on fixed dates.<br>**Yearly** – Select this option if DST starts and ends on certain days of the week. |
| **Automatically Update Interval** | Select the time interval at which the router updates the system time. |
| **Send NTP Request Through** | Specify a WAN interface to send NTP request for time synchronization. |

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

## VI-1-9 SNMP

This section allows you to configure settings for SNMP and SNMPv3 services.

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable SNMP Agent** | Check to enable SNMP function. Then, enable SNMPV1 agent/SNMPV2C agent. |
| **Get Community** | Enter the Get Community string. The default setting is **public**. Devices that send requests to retrieve information |

| | |
|---|---|
| | using get commands must pass the correct Get Community string.<br>The maximum allowed length is 23 characters. |
| **Set Community** | Enter the Set Community string. The default setting is **private**. Devices that send requests to change settings using set commands must pass the correct Set Community string.<br>The maximum length of the text is 23 characters. |
| **Manager Host IP (IPv4)** | Enter the IPv4 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv4 LAN host is allowed to issue SNMP commands. |
| **Manager Host IP (IPv6)** | Enter the IPv6 address of hosts that are allowed to issue SNMP commands. If this field is left blank, any IPv6 LAN host is allowed to issue SNMP commands. |
| **Trap Community** | Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string.<br>The maximum length of the text is 23 characters. |
| **Notification Host IP (IPv4)** | Enter the IPv4 address of hosts that are allowed to be sent SNMP traps. |
| **Notification Host IP (IPv6)** | Enter the IPv6 address of hosts that are allowed to be sent SNMP traps. |
| **Trap Timeout** | The default setting is 10 seconds. |
| **Enable SNMPV3 Agent** | Check to enable SNMPV3 function. |
| **USM User** | USM means user-based security mode.<br>Enter the username to be used for authentication. The maximum allowed length is 23 characters. |
| **Auth Algorithm** | Choose one of the hashing methods to be used with the authentication algorithm. |
| **Auth Password** | Enter a password for authentication. The maximum allowed length is 23 characters. |
| **Privacy Algorithm** | Choose an encryption method as the privacy algorithm. |
| **Privacy Password** | Enter a password for privacy. The maximum allowed length is 23 characters. |

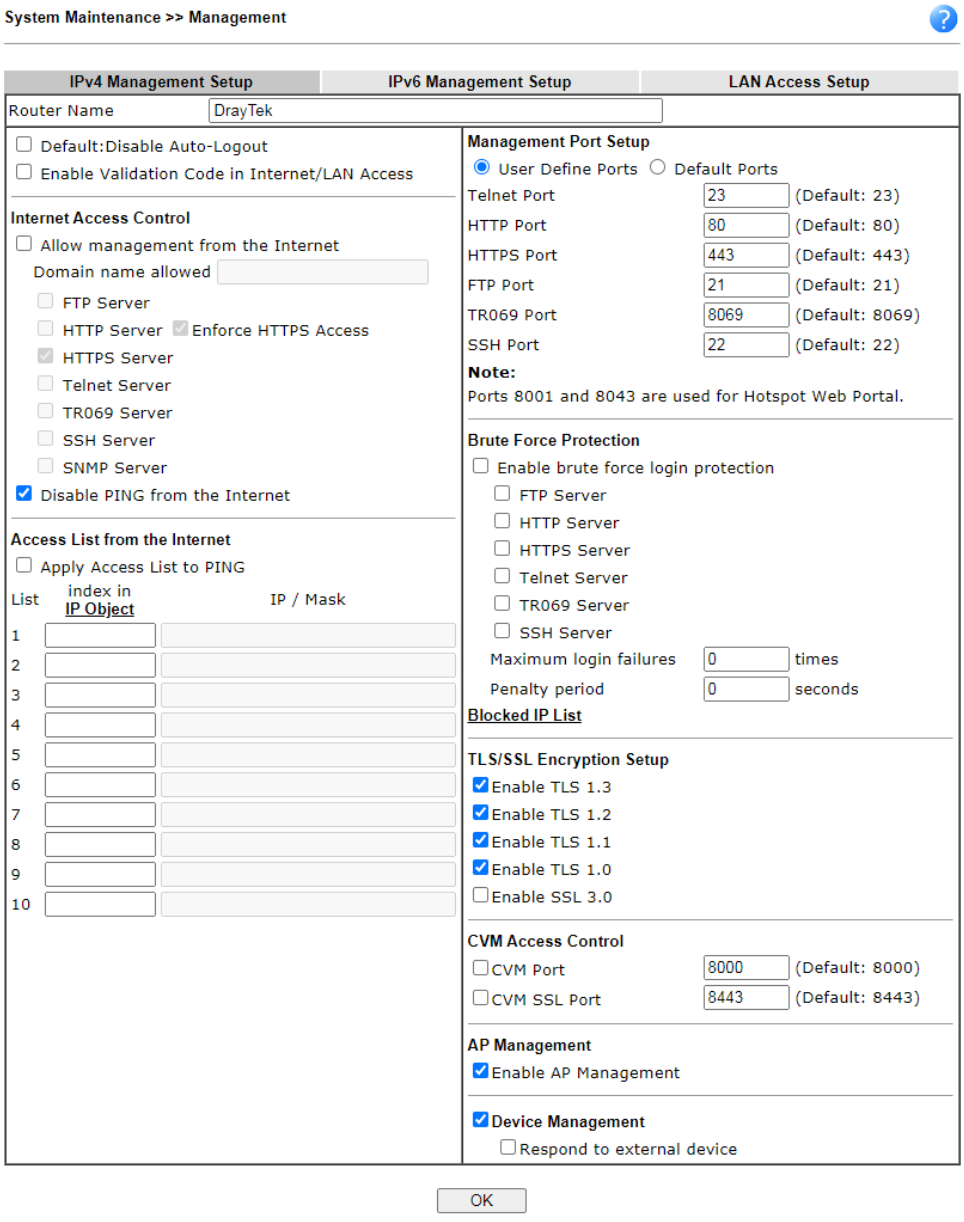
Select **OK** to save changes on the page, or **Cancel** to discard changes without saving.

# VI-1-10 Management

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

Management setup for IPv4 and IPv6 are on separate tab pages.

## IPv4 Management Setup




Available settings are explained as follows:

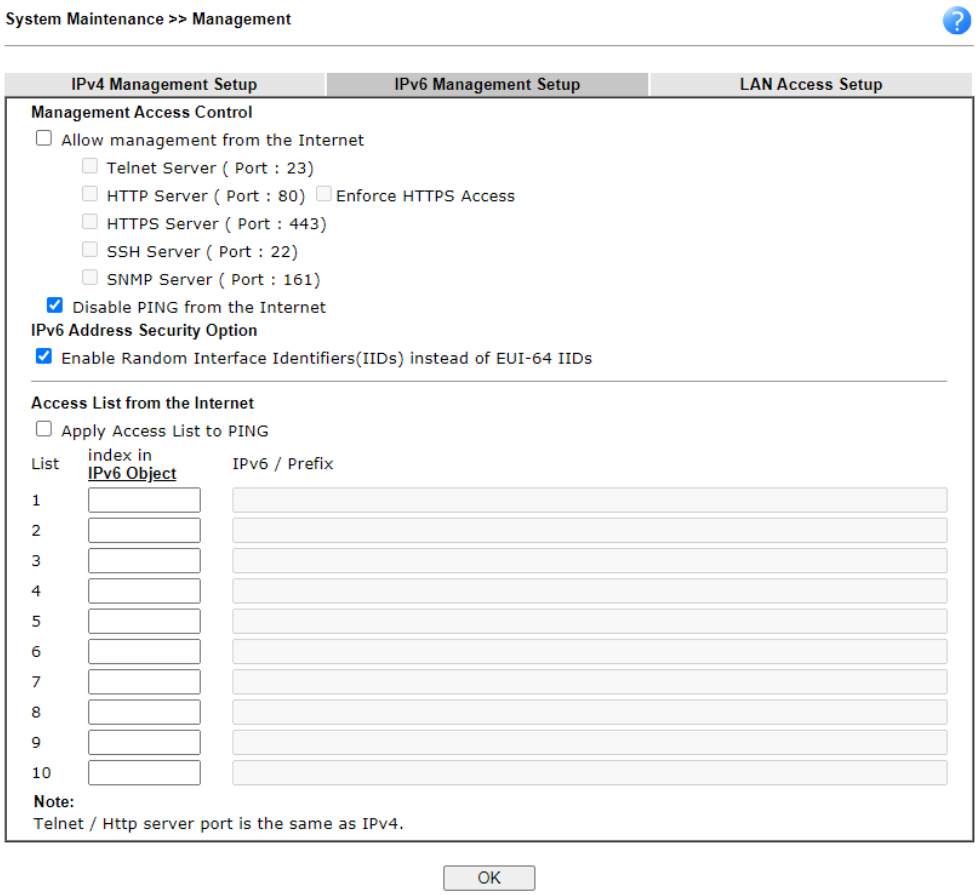
| Item | Description |
|---|---|
| **Router Name** | Enter the router name as provided by ISP. |
| **Default: Disable Auto-Logout** | If enabled, the auto-logout function for web user interface will be disabled. |

| | |
|---|---|
| |  <br>The web user interface will not terminate until you manually click the Logout icon.<br>  |
| **Enable Validation Code in Internet/LAN Access** | If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in. |
| **Internet Access Control** | **Allow management from the Internet** - Enable the checkbox to allow system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered.<br>**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.<br>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.<br>**Disable PING from the Internet -** Select to reject all PING packets from the Internet. For increased security, this setting is enabled by default. |
| **Access List from the Internet** | The ability of system administrators to log into the router can be restricted to up to 10 specific hosts or networks.<br>**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.<br>**index in IP Object**- Enter the index of a configured IP object.<br>**IP / Mask** - Shows the IP address and/or subnet mask of the selected IP object. |
| **Management Port Setup** | **User Define Ports -** Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.<br>**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.<br>**Enable brute force login protection -** Select to enable detection of brute force login attempts. |

| | |
|---|---|
| | **Maximum login failure –** Specify the maximum number of failed login attempts before further login is blocked.<br>**Penalty period –** Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed.<br>**Blocked IP List –** Display, in a new browser window, IP addresses that are currently blocked from logging into the router. |
| **TLS/SSL Encryption Setup** | **Enable SSL 3.0/1.0/1.1/1.2/1.3 –** Check the box to enable SSL 3.0/1.0/1.1/1.2/1.3 encryption protocols.<br>For improved security, the HTTPS and SSL VPN servers that are built into the router have been upgraded to TLS 1.x protocol. If you are using an old web browser (eg. IE 6.0) or an old version of the SmartVPN Client, you may need to enable SSL 3.0 to connect to the router. However, it is recommended that you instead upgrade your web browser or SmartVPN client to a version that supports TLS protocols that are far more secure than SSL. |
| **CVM Access Control** | **CVM Port –** Check the box to enable Central VPN Management port setting.<br>**CVM SSL Port –** Check the box to enable Central VPN Management SSL port setting. |
| **AP Management** | **Enable AP Management –** Check to enable the access point management function. If not, menu items related to **Central Management>>AP** will be hidden. |
| **Device Management** | Check to enable the device management function.<br>**Respond to external device –** If selected, Vigor2927 will function as a slave device. When an external device (master device) sends packets to the Vigor2927 to attempt to manage it, the Vigor2927 will respond to the request coming from the external device which is able to manage Vigor2927. |

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

## IPv6 Management Setup

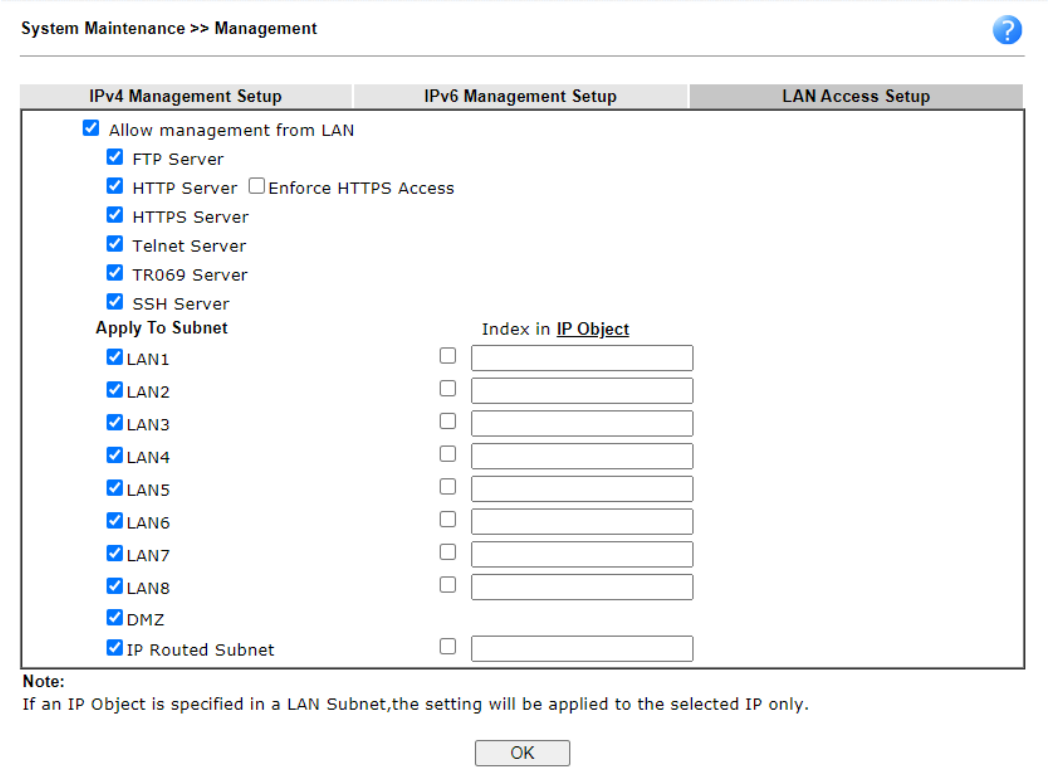



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Management Access Control** | **Allow management from the Internet** - Check to enable the function. Select the servers that system administrators are allowed to manage from the Internet.<br>**Disable PING from the Internet** - Check to reject all PING packets from the Internet. For increased security, this setting is enabled by default. |
| **IPv6 Address Security Option** | **Enable Random Interface Identifiers (IIDs)... -** The IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker. |
| **Access List from the Inernet** | You could specify that the system administrator can only login from up to 10 designated hosts or networks defined in the list.<br>**Index in IPv6 Object**- Enter the index number of the IPv6 object profile. Related IP address will appear automatically. |

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

### LAN Access Setup




Available settings are explained as follows:

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

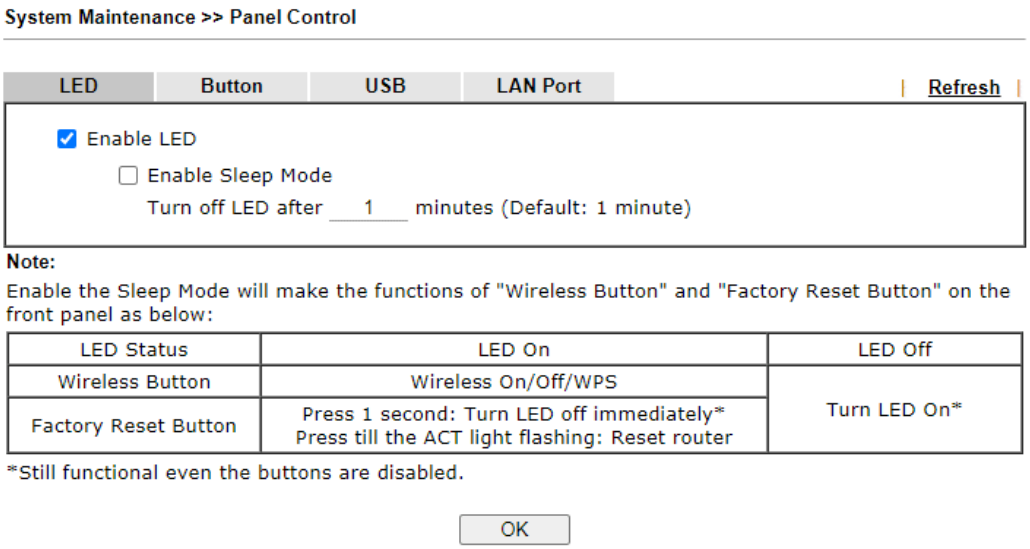
Select **OK** to save changes on the page.

## VI-1-11 Panel Control

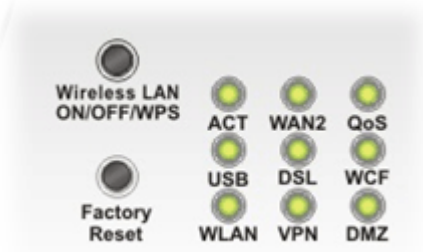
You may customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.

### For LED

By default, LEDs on the front panel illuminate or blink during operation to show the status of the various functions on the router. However, you may configure them to remain off at all times, or remain off until a button is pressed to wake them up.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Refresh** | Click to refresh the page to display the latest information. |
| **Enable LED** | Select to enable the LEDs to function according to the configured settings.<br>Deselect to disable LEDs entirely. |
| **Enable Sleep Mode** | Select to let the system turn off the LEDs after the specified number of minutes has elapsed.<br>When Sleep Mode is enabled, the LEDs can be woken up by pressing one of the following buttons:<br>● Wireless LAN ON/OFF/WPS on the front panel<br>● Factory Reset on the front panel<br>● Wake up LED on this configuration page<br>  |
| **Status** | Shows the status of the LEDs.<br>When the following is shown, the LEDs are in sleep mode.<br>**Status :** Sleep Wake up LED<br>To wake them up, do one of the following actions:<br>● press the **Wake up LED** button on this page<br>● press the **Wireless On/Off/WPS** button on the front panel |

| | |
|---|---|
| | ● press the **Factory Reset** button on the front panel.<br>When the following is shown, the LEDs are awake.<br>  <br>To put them to sleep immediately, perform one of the following actions:<br>● press the **LED sleep immediately** button on this page<br>● press the Factory Reset button on the front panel |
| **Wake up LED** | Click to resume operation of the LED after they have gone to sleep. |

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

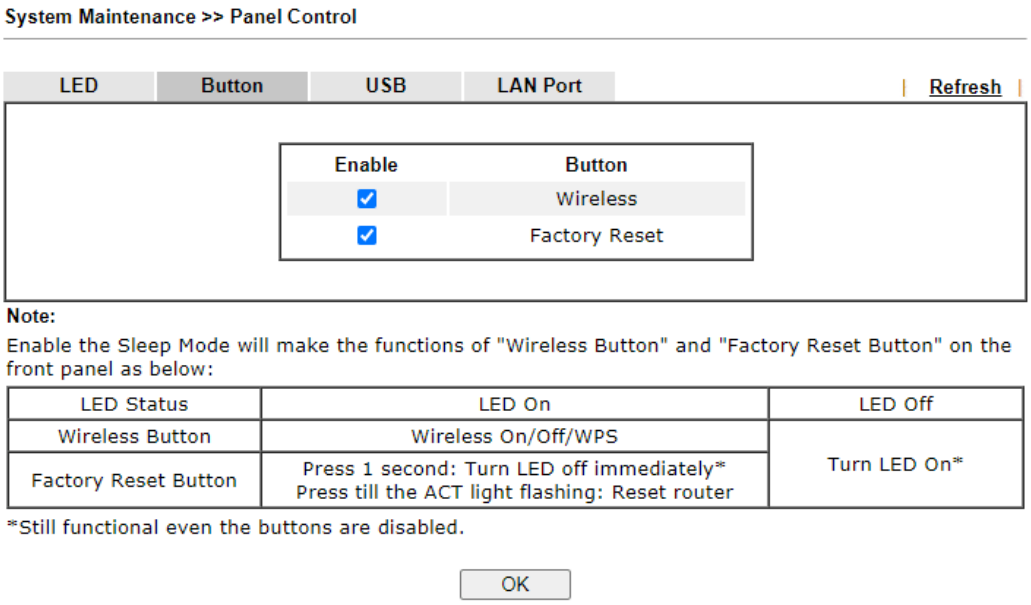
## For Button

The primary functions of the **Factory Reset** and **Wireless ON/OFF/WPS** front-panel buttons (reset to factory defaults and wireless control, respectively) are enabled by default, but they can be enabled or disabled as needed.

When the **Factory Reset** button is set to **Disabled**, the router cannot be reset during normal operation. Other functions of the reset button (such as starting up the TFTP server to upload firmware during power on, and controlling the illumination of the front panel LEDs when LED sleep mode is enabled) can still be used.

When the **Wireless ON/OFF/WPS** button is set to **Disabled**, the button cannot be used to turn on or off the wireless network, nor can it be used to start the WPS pairing process. However, the front panel LEDs can be woken up when LED sleep mode is enabled.

Click the **Button** tab to get the following page.




Available settings are explained as follows:

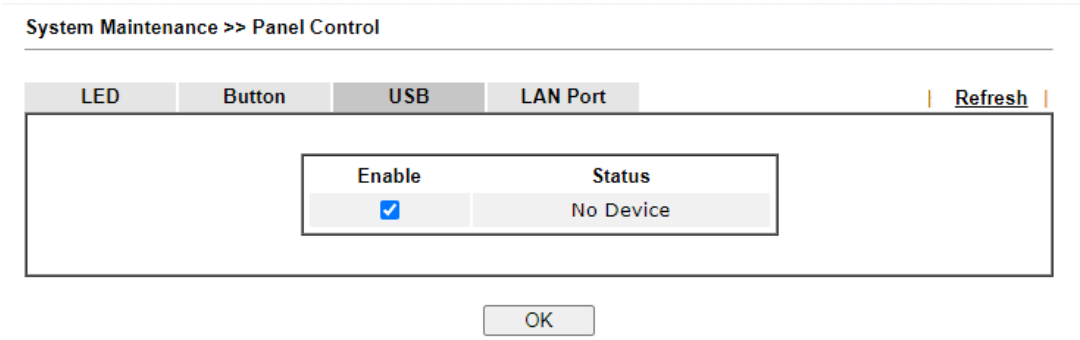
| Item | Description |
|---|---|
| **Refresh** | Click to refresh the page to display the latest information**.** |

| | |
|---|---|
| **Enable Factory Reset Button** | The default value is **Enabled**.<br>Deselect to disable the reset function of the factory reset button.<br>Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings. It can still be used to wake up the LEDs when LED sleep mode is enabled. |
| **Enable Wireless Button** | The default value is **Enabled**.<br>Deselect to disable the ability of the Wireless button to control WLAN and WPS functions.<br>Disabling the wireless button only prevents it from being used to control WLAN functions. It can still be used to wake up the LEDs when LED sleep mode is enabled. |

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

### For USB

The USB ports can be individually enabled or disabled. When a USB port is disabled, attached devices will not be recognized by the router.



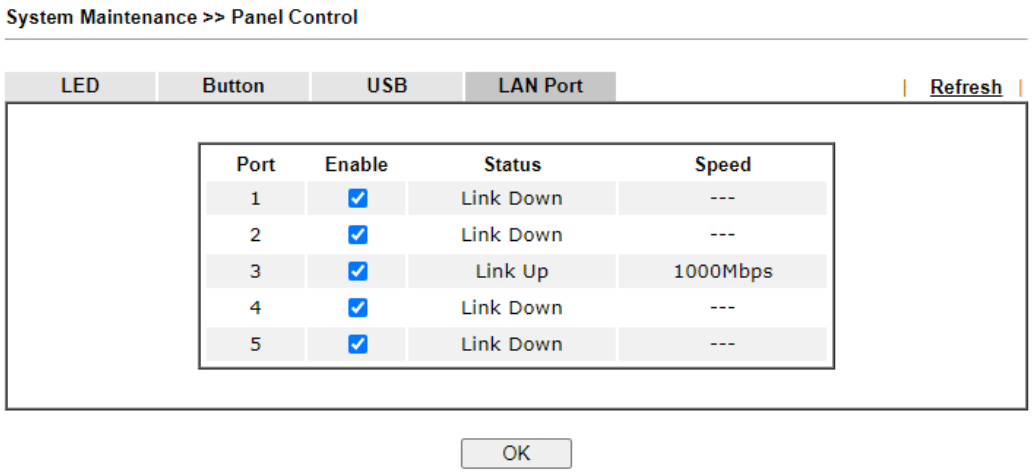

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Refresh** | Click to refresh the page to display the latest information**.** |
| **Port** | The number corresponds to the USB port number shown on the front panel. |
| **Enable** | Deselect to disable the USB port. The default value is enabled. |
| **Status** | Shows the status of the USB port.<br>**No device** – no USB device is connected to the port.<br>**Connected** – a USB device is connected to the port.<br>**---** – the USB port is disabled. |

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

## For LAN Port

The 5 LAN ports can be individually enabled or disabled. When a LAN port is disabled, attached devices will not be recognized by the router.




Available settings are explained as follows:

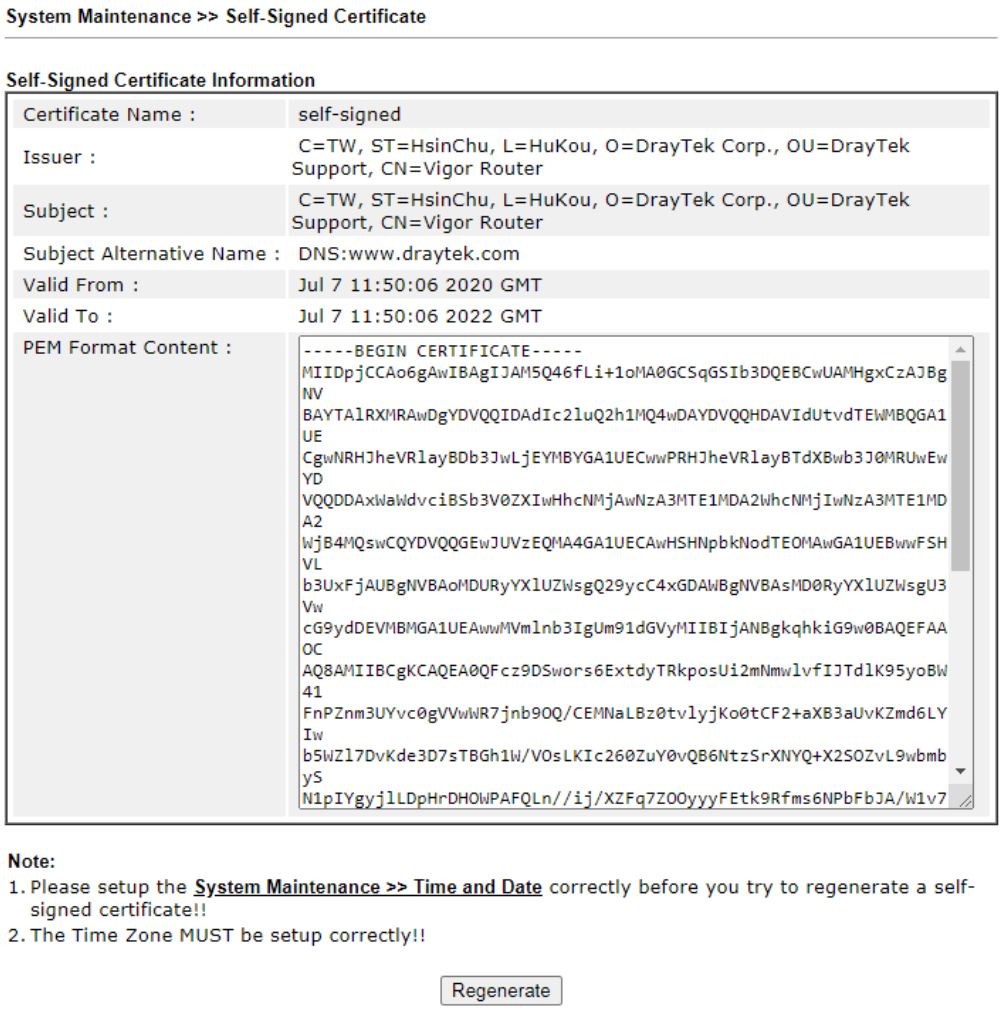
| Item | Description |
|---|---|
| **Refresh** | Click to refresh the page to display the latest information**.** |
| **Port** | The number corresponds to the LAN port number shown on the front panel. |
| **Enable** | Deselect to disable the LAN port. The default value is enabled. |
| **Status** | Shows the status of the USB port.<br>**Link Up** – An active Ethernet device is connected to the port.<br>**Link Down** – No active Ethernet device is detected.<br>**---** – The LAN port is disabled. |
| **Speed** | Shows the negotiated speed of the LAN port.<br>**1000Mbps** – Negotiated speed of the LAN port is 1000 Mbps.<br>**100Mbps** – Negotiated speed of the LAN port is 100 Mbps.<br>**10Mpbs** – Negotiated speed of the LAN port is 10 Mbps.<br>**---** – The LAN port is disabled or there is no active device connected. |

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

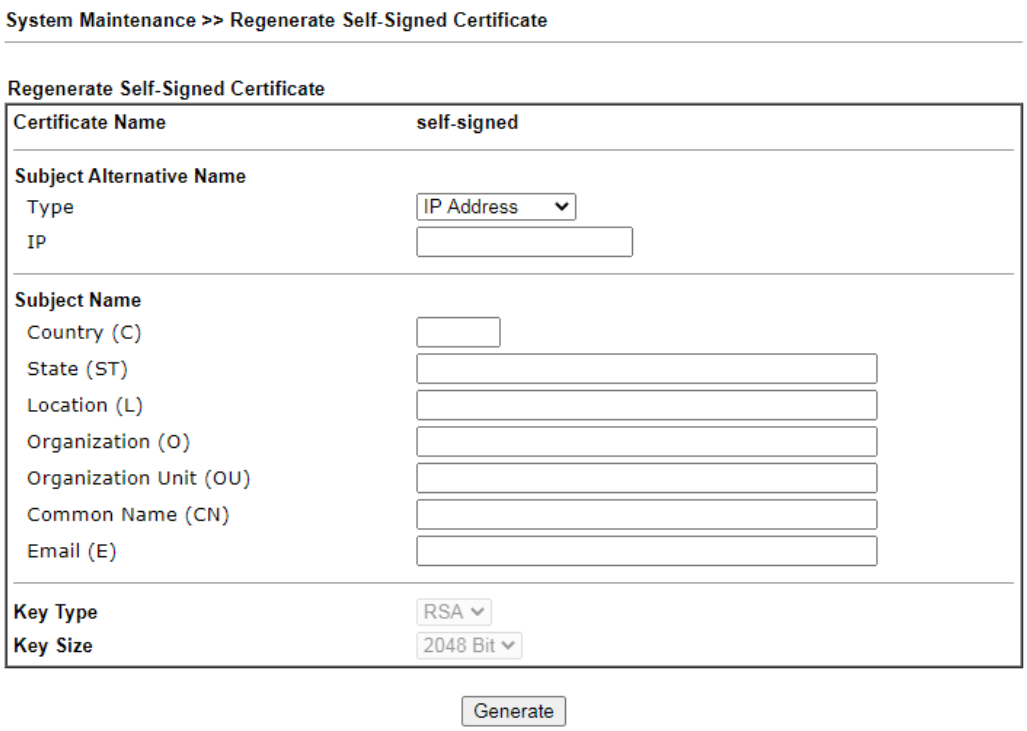
## VI-1-12 Self-Signed Certificate

A self-signed certificate is a *unique* identification for the device (e.g., Vigor router) which generates the certificate by itself to ensure the router security. Such self-signed certificate is signed with its own private key.

The self-signed certificate can be used for services such as SSL VPN and HTTPS. In addition, it can be created for free by using a wide variety of tools.



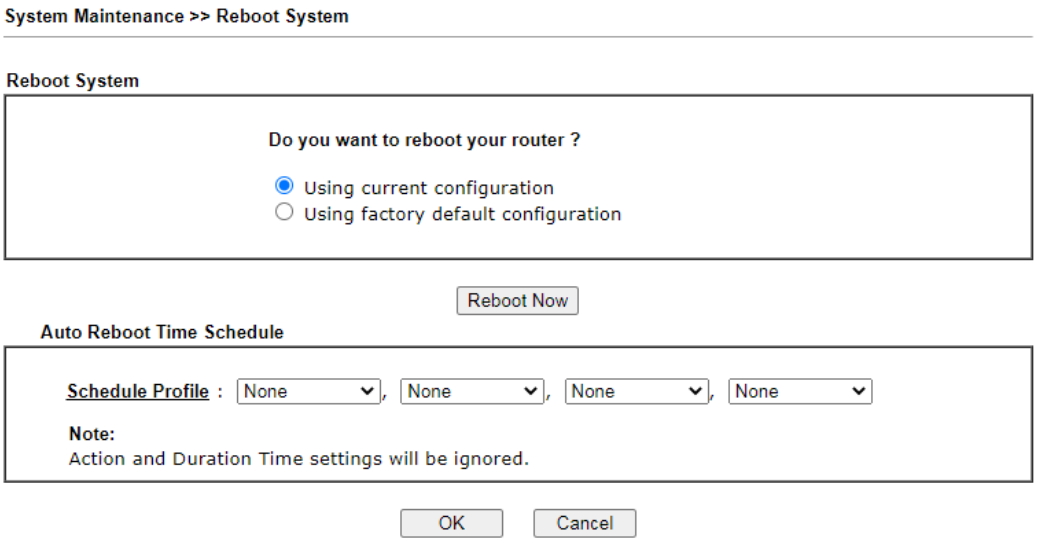

Click **Regeneration** to open **Regenerate Self-Signed Certificate** window.




Enter all requested information including certificate name (used to differentiate different certificates), subject alternative name type and relational settings for subject name. Then click **GENERATE**.

## VI-1-13 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to bring up the following page.




Available settings are explained as follows:

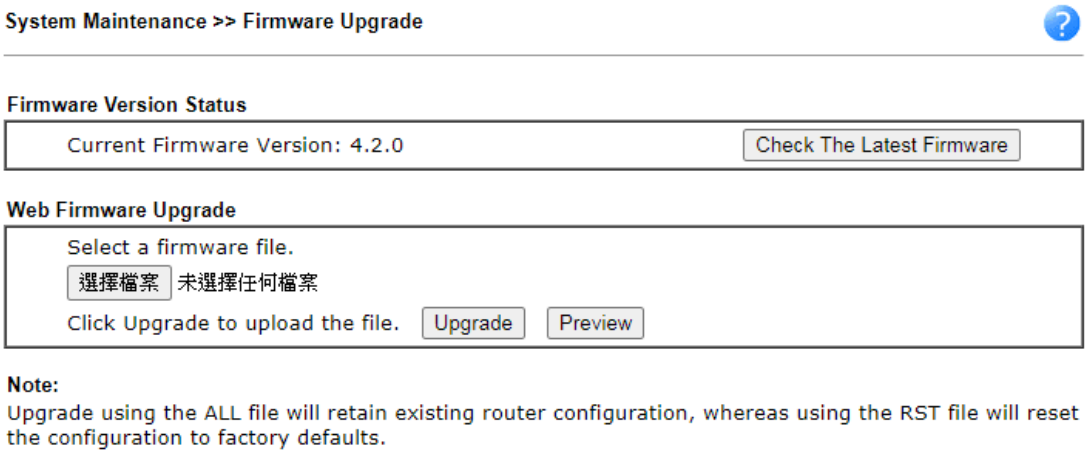
| Item | Description |
|---|---|
| **Reboot System** | Select one of the following options, and press the **Reboot Now** button to reboot the router.<br>**Using current configuration** – Select this option to reboot the router using the current configuration.<br>**Using factory default configuration** – Select this option to reset the router's configuration to the factory defaults before rebooting. |
| **Auto Reboot Time Schedule** | **Schedule Profile** - Select up to 4 user-configured schedules to reboot the router on a scheduled basis. |

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

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

## VI-1-14 Firmware Upgrade

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

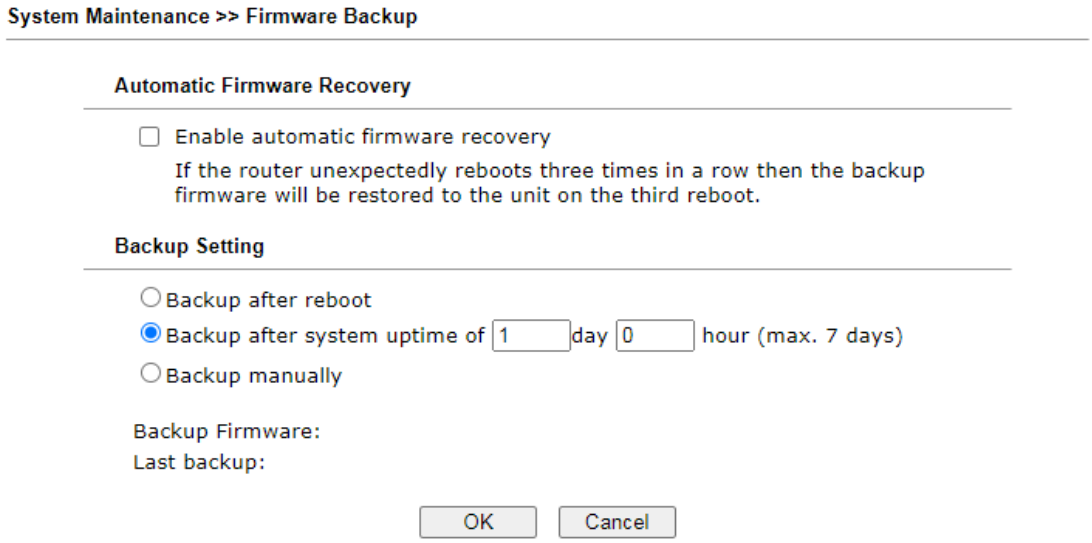



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Firmware Version Status** | **Check The Latest Firmware** – Click to check for updated firmware.<br>Any available new firmware files will be displayed and you can download any one of them by clicking **Download**. After the file has been downloaded, click Select followed by Upgrade to perform the firmware upgrade. |
| **Web Firmware Upgrade** | Click **Browse…** to select the firmware file, followed by **Upgrade** to start the upgrade process, or **Preview** to display detailed information about the selected firmware file: |

## VI-1-15 Firmware Backup

The firmware for Vigor router can be saved on the host as a backup firmware. After that, if the router crashes due to the firmware error, the backup firmware will be applied to make the router run normally.




Available settings are explained as follows:

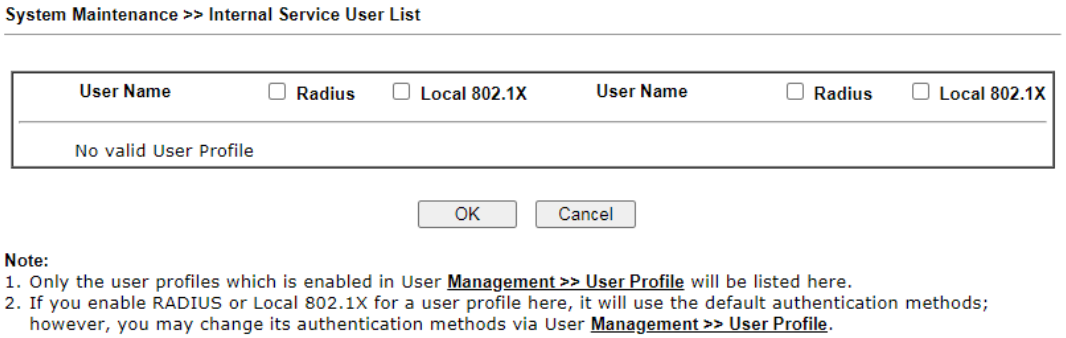
| Item | Description |
|---|---|
| **Automatic Firmware Recovery** | **Enable automatic firmware recovery**- If this option is enabled, the router will restore the most recently backed-up firmware after the router reboots unexpectedly three times. |
| **Backup Setting** | This option controls the backup behavior of the router.<br>● **Backup after reboot -** The router makes a copy of the current firmware immediately after it reboots<br>● **Backup after system uptime... -** The router makes a copy of the current firmware after it has run for the specified length of time after boot-up.<br>● **Backup manually -** the router will not automatically create a backup copy of the firmware. Click this option and click OK, firmware backup will be performed immediately.<br>**Backup Firmware** - Displays recent firmware backup version.<br>**Last backup** - Displays the time of recent firmware backup. |

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

## VI-1-16 Internal Service User List

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

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




Available settings are explained as follows:

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

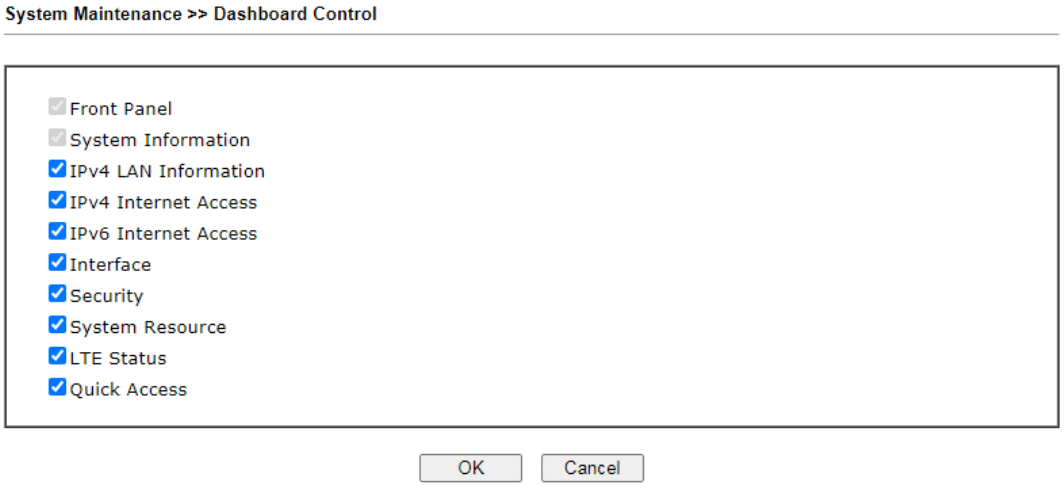
**Info**

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

For the detailed setting (such as IP address, port number) configuration of Local 802.1X, refer to **LAN>>Wired 802.1X** and **Wireless LAN>>Security**.

## VI-1-17 Dashboard Control

There are nine groups of setting information which can be displayed on Dashboard as a reference for administrator/user. Except for Front Panel and System Information, the settings information regarding to the groups listed on this page can be hidden if required.



# VI-2 Bandwidth Management

### Sessions Limit

When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is a finite number of sessions that can be tracked by the router, and by setting session limits will ensure that the router does not run out of resources. This is especially important when P2P applications are used. P2P applications, such as BitTorrent, that attempt to simultaneously establish connections to as many WAN hosts as possible.

### Bandwidth Limit

Bandwidth Limit ensures LAN clients get their fair share of network bandwidth by placing restrictions on upstream and downstream network speeds.

### Quality of Service (QoS)

QoS (Quality of Service) ensures that all LAN clients receive their fair share of bandwidth that is required for applications to function properly and efficiently.

Without QoS, it is possible that certain applications may consume excessive network resources that they degrade performance of more important applications, especially ones that are less tolerant of jitter (delay variation) or lost or delayed packets. Additionally, at times of network congestion, QoS is able to prioritize different types of traffic according to their predefined priority, thus ensuring traffic of higher importance gets processed first.

A typical QoS deployment consists of two components:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Prioritizing packets by assigning them to different queues and service types according to service levels.

### APP QoS

APP QoS allows QoS to be applied to select protocols and applications.

Protocols and applications fall into two categories: Traceable and Untraceable. Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class. Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.

# Web User Interface

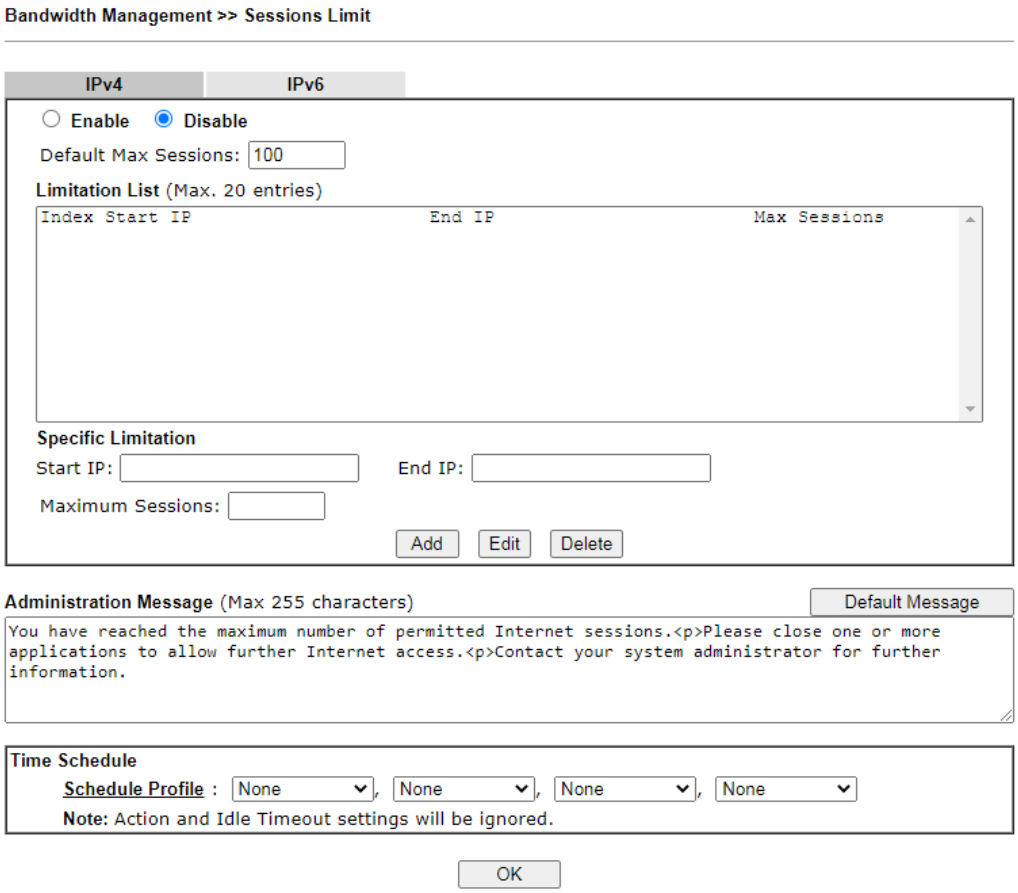
Bandwidth management ensures efficient allocation of network bandwidth for various applications.

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




## VI-2-1 Sessions Limit

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




Available settings are explained as follows:

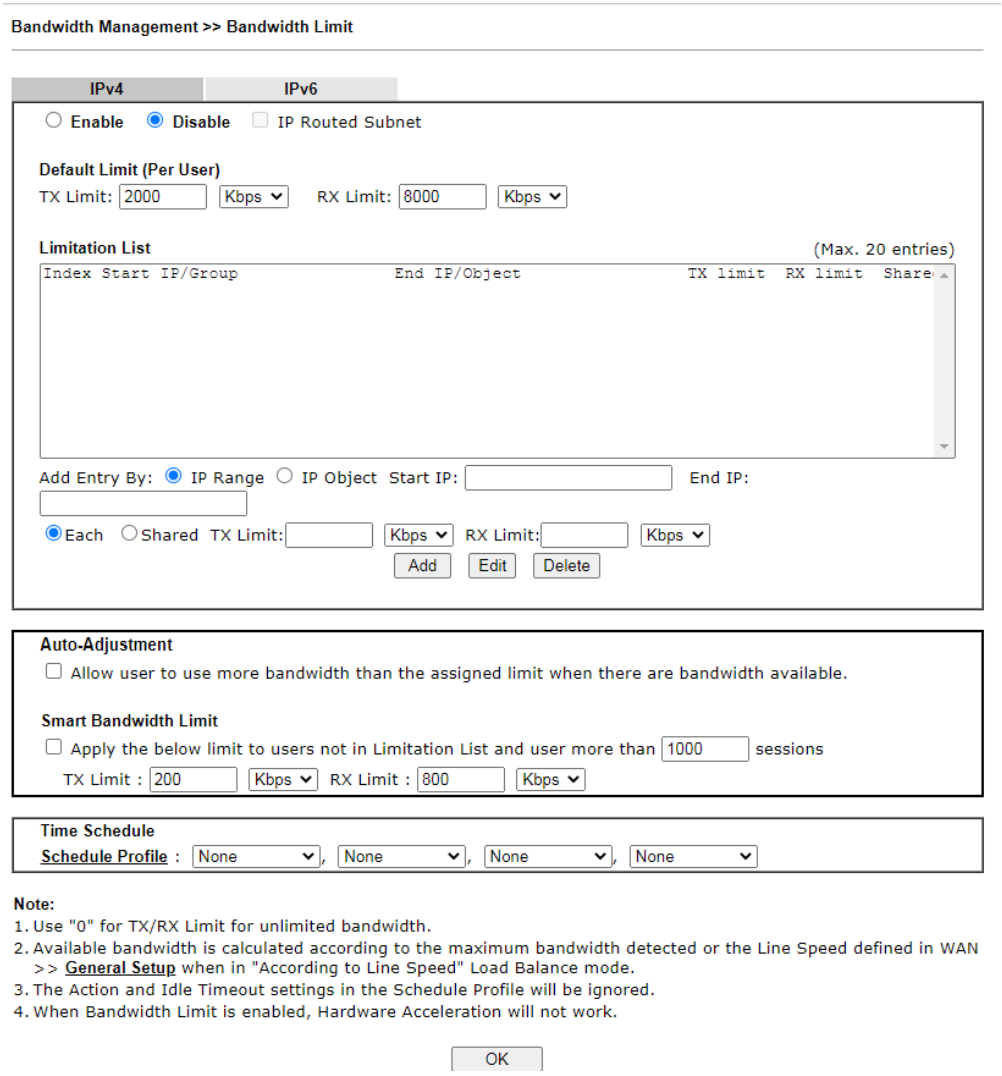
| Item | Description |
|---|---|
| **Enable / Disable** | **Enable -** Select to activate session limit function.<br>**Disable -** Select to deactivate session limit function.<br>**Default Max Session -** The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List. |

| | |
|---|---|
| **Limitation List** | Displays specific limitation entries. |
| **Specific Limitation** | **Start IP -** The beginning IP address for this limit entry.<br>**End IP -** The ending IP address for limit entry.<br>**Max Sessions -** The maximum number of NAT sessions allowed per LAN client. If no value is entered, the Default Max Sessions value is used.<br>**Add -** Creates a new limit entry using the above Specific Limitation values.<br>**Edit -** To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit.<br>**Delete -** To delete an entry, select it from the Limitation List, then click the Delete button. |
| **Administration Message** | Message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached.<br>**Default Message** - Click to reset the administration message to the factory default. |
| **Time Schedule** | **Schedule Profile** - Specify up to 4 time schedule entries to enable or disable the WAN. |

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

## VI-2-2 Bandwidth Limit

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



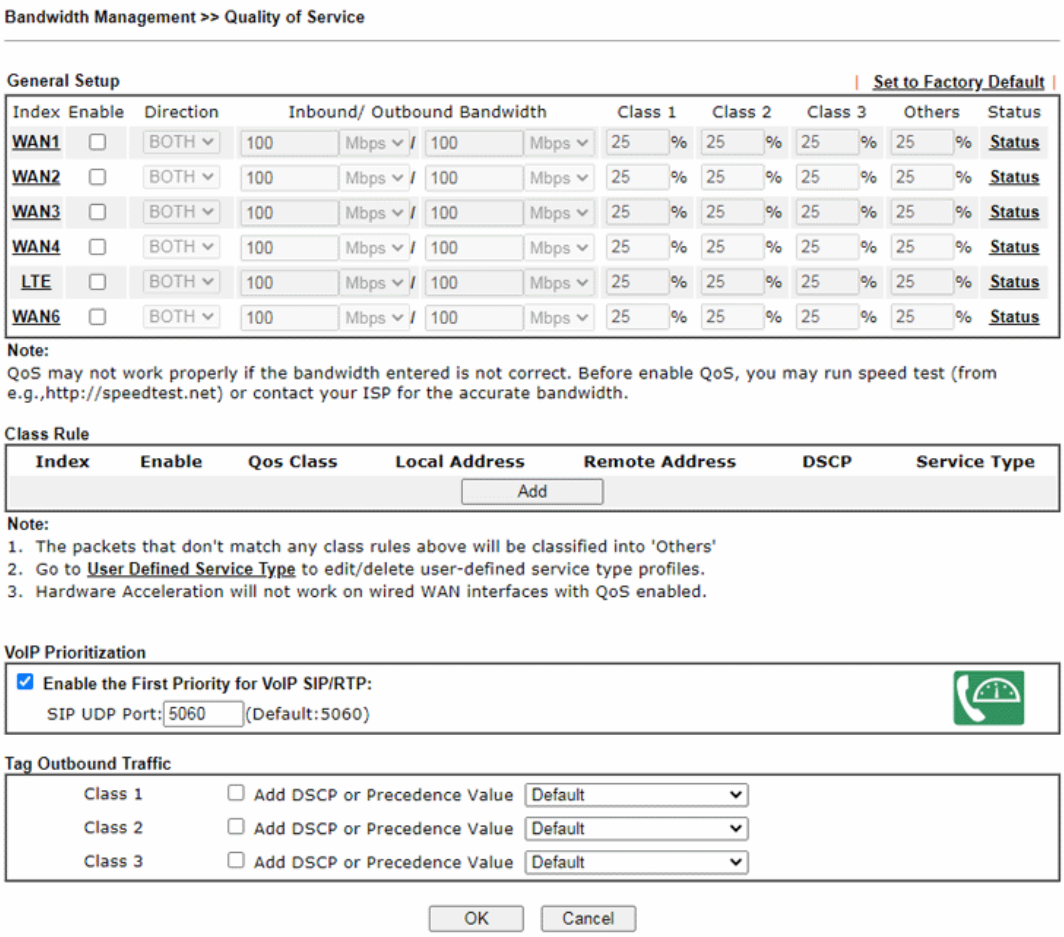

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable / Disable** | **Enable** - Select to activate bandwidth limit function.<br>● **VPN Traffic** - Check this box to apply the bandwidth limit to the VPN sessions. It is available for IPv4 settings only.<br>**Disable** - Select to deactivate bandwidth limit function.<br>**Default Limit (Per User)**<br>● **TX LImit -** Default upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.<br>● **RX limit -** Default downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited and 30000). |
| **Limitation List** | Displays specific limitation entries. |

| | |
|---|---|
| **Add Entry By** | **IP Range -** All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below.<br>● **Start IP -** The beginning IP address for this limit entry.<br>● **End IP -** The ending IP address for limit entry.<br>**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.<br>● **IP Group** – Specify an IP group by using the drop down list.<br>● **IP Object -** Specify an IP object by using the drop down list.<br>**Each** - The specified bandwidth is the limit per LAN client.<br>**Shared -** The specified bandwidth limits are the total allowed for all LAN clients within the range of IP addresses.<br>● **TX limit -** The upstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.<br>● **RX limit -** The downstream limit. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.<br>**Add -** Creates a new limit entry using the above Specific Limitation values.<br>**Edit -** To edit an existing entry, select the entry from the Limitation List, make the appropriate changes in Specific Limitation, then click Edit.<br>**Delete -** To delete an entry, select it from the Limitation List, then click the Delete button. |
| **Auto-Adjustment** | **Allow user to use more bandwidth ···-** Select to let the router automatically adjust the upstream and downstream limits based on available bandwidth. |
| **Smart Bandwidth Limit** | This option restricts the bandwidth of LAN clients that are not in the limitation list when the network sessions exceed a predefined threshold.<br>**Apply the below limit to ...** - The number of sessions a LAN client is allowed to have before Smart Bandwidth Limit activates.<br>● **TX limit -** Upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited) and 30000.<br>● **RX limit -** Downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. Value must be between 0 (unlimited and 30000). |
| **Time Schedule** | **Schedule Profile** - Specify up to 4 time schedule entries to enable or disable the WAN. |

## VI-2-3 Quality of Service

To configure **Quality of Service**, from the main menu, select **Bandwidth Management** menu, then click **Quality of Service** to bring up the configuration page.




Available settings are explained as follows:

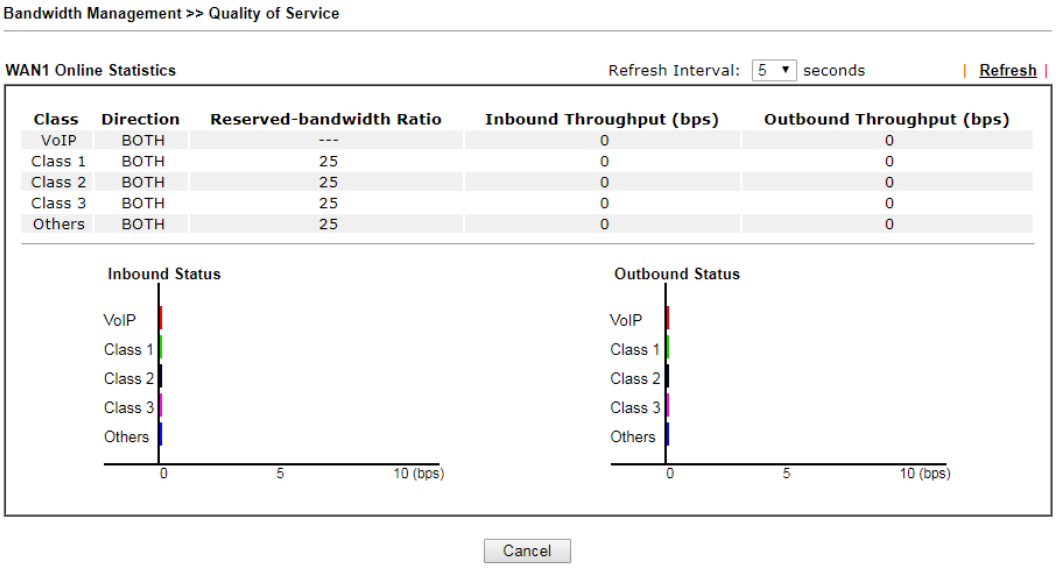
| Item | Description |
|---|---|
| **General Setup** | **Index** – Link of WAN/LTE interface.<br>**Enable** – Check the box to enable the QoS function for WAN/LTE interface. If it is enabled, you can configure general QoS setting for each WAN/LTE interface.<br>● **Direction** –Direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both).<br>- **IN -** Apply QoS to incoming traffic only.<br>- **OUT -** Apply QoS to outgoing traffic only.<br>- **BOTH -** Apply to both incoming and outgoing traffic.<br>● **Inbound/Outbound Bandwidth** – The inbound / outbound bandwidth of the WAN.<br>● **Class 1 ~ 3 / Others** – Percentage of bandwidth reserved for each class.<br>**Status** – Click to bring up the Online Statistics page that shows snapshots of statistics for the given WAN interface. |
| **Class Rule** | Define and list the Class rules.<br>**Index** – Display the class number that you can edit. |

| Item | Description |
|---|---|
| | **Enable** - Display the status of this class rule.<br>**QoS Class** - Display the QoS class level.<br>**Local Address** - Display the local IP address for the rule.<br>**Remote Address** - Display the remote IP address for the rule.<br>**DSCP** - Display the levels of the data for processing with QoS control.<br>**Service Type** – Display detailed settings for the service type.<br>**Add** - Click it to create a class rule for QoS. |
| **VoIP Prioritization** | **Enable the First Priority for VoIP SIP/RTP** - Select to allow VoIP traffic to receive the highest priority.<br>**SIP UDP Port –** Port number to be monitored for SIP traffic.<br>  - Click this icon to display the VoIP QoS Status. |
| **Tag Outbound Traffic** | Tag the outgoing traffic with the DSCP or Precedence value.<br>**Add DSCP or Precedence Value for Class 1 to Class 3** - Check to apply the DSCP or precedence value for each class. |

To save changes, click **OK**; to discard changes, click **Cancel**.

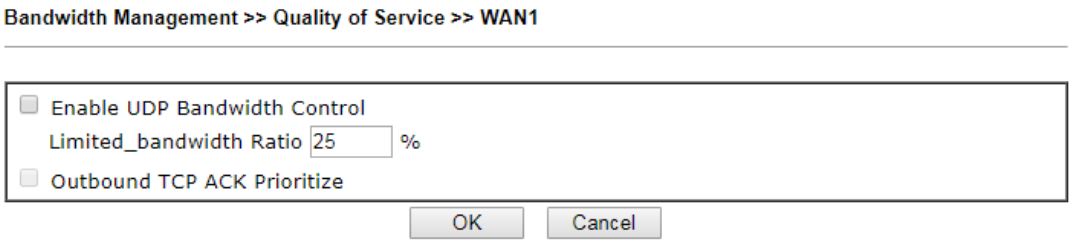
## Online Statistics

Click the Status link in the General Setup section to show real-time online statistics of the WAN interface.



## General Setup for WAN Interface

Click WAN/LTE interface number link to configure the limited bandwidth ratio for QoS of the WAN interface.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable UDP Bandwidth Control** | Select to restrict the bandwidth available to UDP traffic. The **Limited_bandwidth Ratio** value is the maximum percentage of bandwidth that can be used by UDP traffic.<br>● **Limited_bandwidth Ratio -** Enter a percentage value. |
| **Outbound TCP ACK Prioritize** | Select to give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent. |

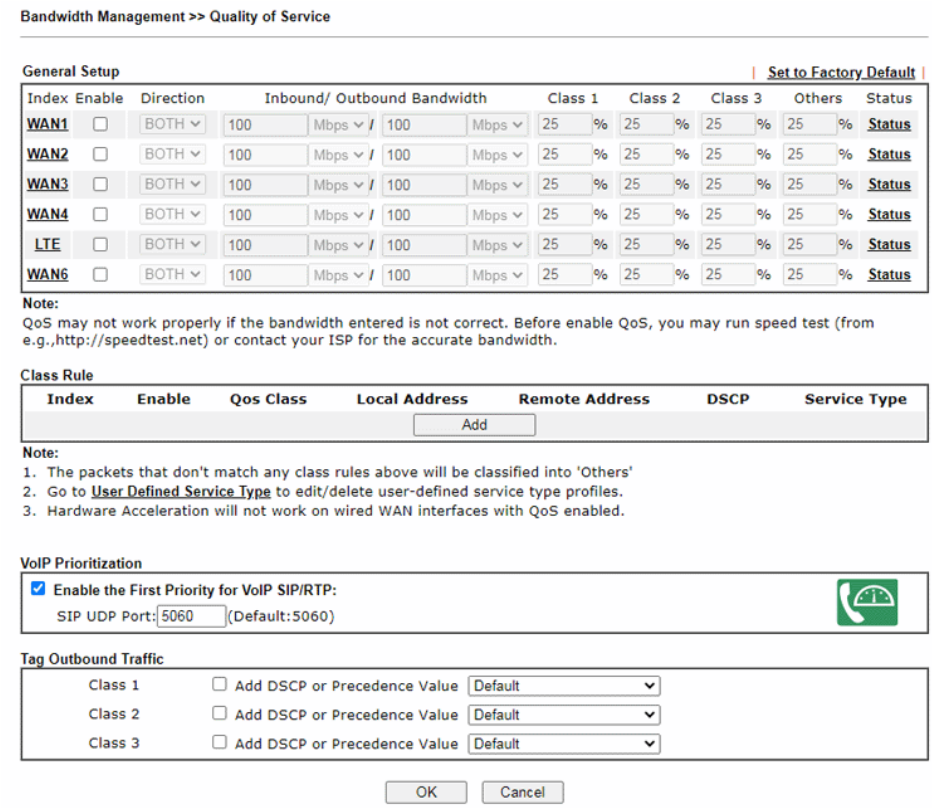
**Info**

The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

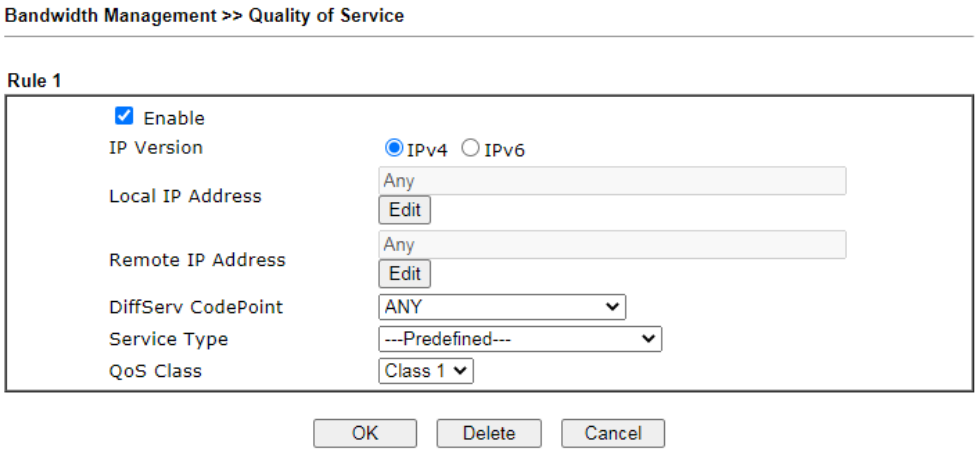
## Add / edit a Class Rule for QoS

You can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click Edit to open the rule edit page for modification.

1. To add a rule, click **Add** to bring up the configuration page. To edit an existing rule, select the rule by clicking the radio button in front of the rule, and then click **Edit** to bring up the configuration page.

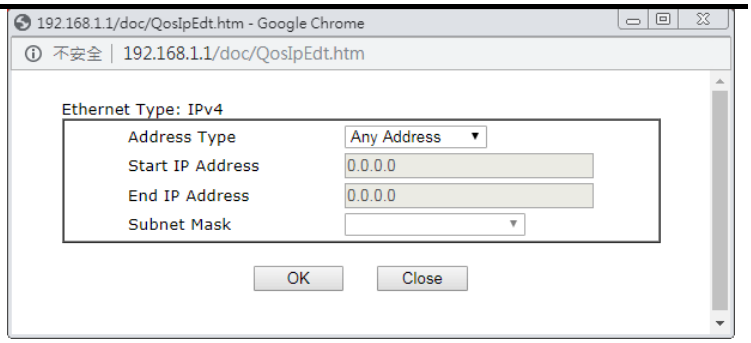



2. For adding a new rule, click **Add** to open the following page.

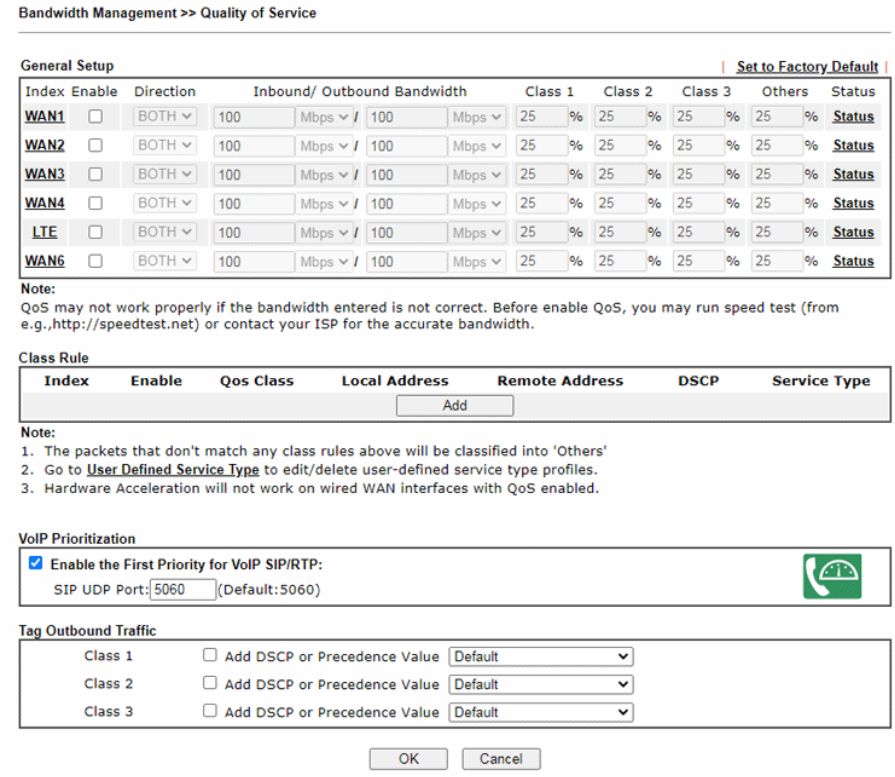



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Select to enable this rule. |
| **IP Version** | Protocol (IPv4 or IPv6) to which this rule applies. |
| **Local IP Address** | Click the **Edit** button to set the local (LAN) IP address or address range for the rule. |
| **Remote IP Address** | Click the **Edit** button to set the remote (WAN) IP address or address range for the rule. |

| | |
|---|---|
| |  <br>**Address Type** – Type of address: Any Address, Single Address, Range Address, Subnet Address.<br>● **Single Address** - Specify IP address.<br>● **Range Address** - Specify Start IP Address and End IP Address.<br>● **Subnet Address** - Specify Start IP Address and Subnet Mask. |
| **DiffServ CodePoint** | DSCP or ToS precedence of packets to which this rule applies. |
| **Service Type** | Service Type to which this rule applies.<br>Service is a predefined or user-defined type of traffic that uses certain protocols or ports. To set up a custom service, select User Defined to set the service name, the protocol, and port number. |
| **QoS Class** | Specify the QoS class (1, 2 or 3) for this rule. |

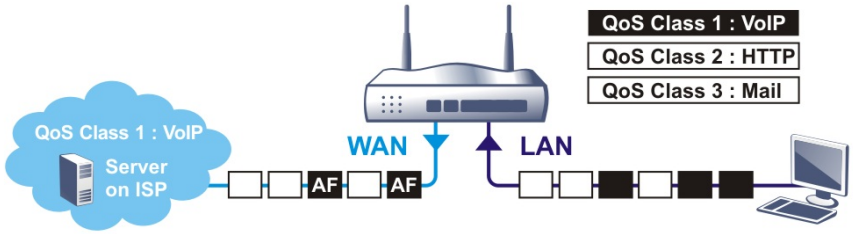
3. After finishing all the settings here, please click **OK** to save the configuration.




Retag the Packets for Identification

Packets originating from the LAN that are destined for the WAN can have the DS flag changed to a different value by enabling Tag Packet and specifying the DSCP or IP Precedence value.

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




Class Rule

| Index | Enable | Qos Class | Local Address | Remote Address | DSCP | Service Type |
|---|---|---|---|---|---|---|
| 1 | ☑ | Class 1 | Any | Any | ANY | SIP(UDP:5060) |
| 2 | ☑ | Class 1 | Any | Any | ANY | HTTP(TCP:80) |
| 3 | ☑ | Class 1 | Any | Any | ANY | SMTP(TCP:25) |

Add

Note:
1. The packets that don't match any class rules above will be classified into 'Others'
2. Go to User Defined Service Type to edit/delete user-defined service type profiles.
3. Hardware Acceleration will not work on wired WAN interfaces with QoS enabled.

VoIP Prioritization

☑ Enable the First Priority for VoIP SIP/RTP:
SIP UDP Port: 5060 (Default:5060)

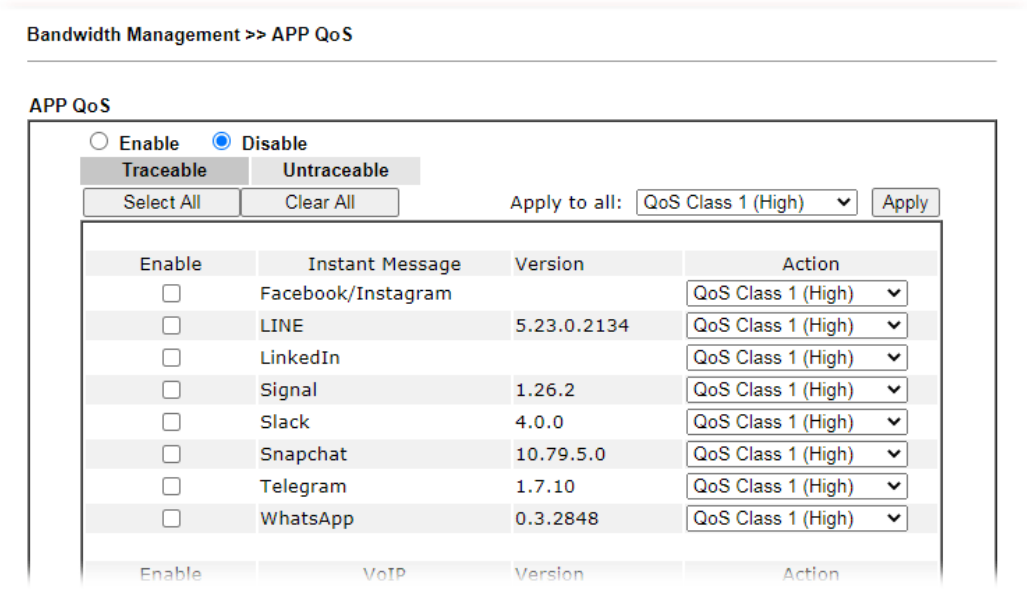
Tag Outbound Traffic

| | | |
|---|---|---|
| Class 1 | ☑ Add DSCP or Precedence Value | AF Class1 (Medium Drop) |
| Class 2 | ☑ Add DSCP or Precedence Value | AF Class2 (Low Drop) |
| Class 3 | ☑ Add DSCP or Precedence Value | AF Class3 (Medium Drop) |

OK Cancel

## VI-2-4 APP QoS

To configure APP QoS, from the main menu, select **Bandwidth Management** menu, then click **APP QoS** to bring up the configuration page.



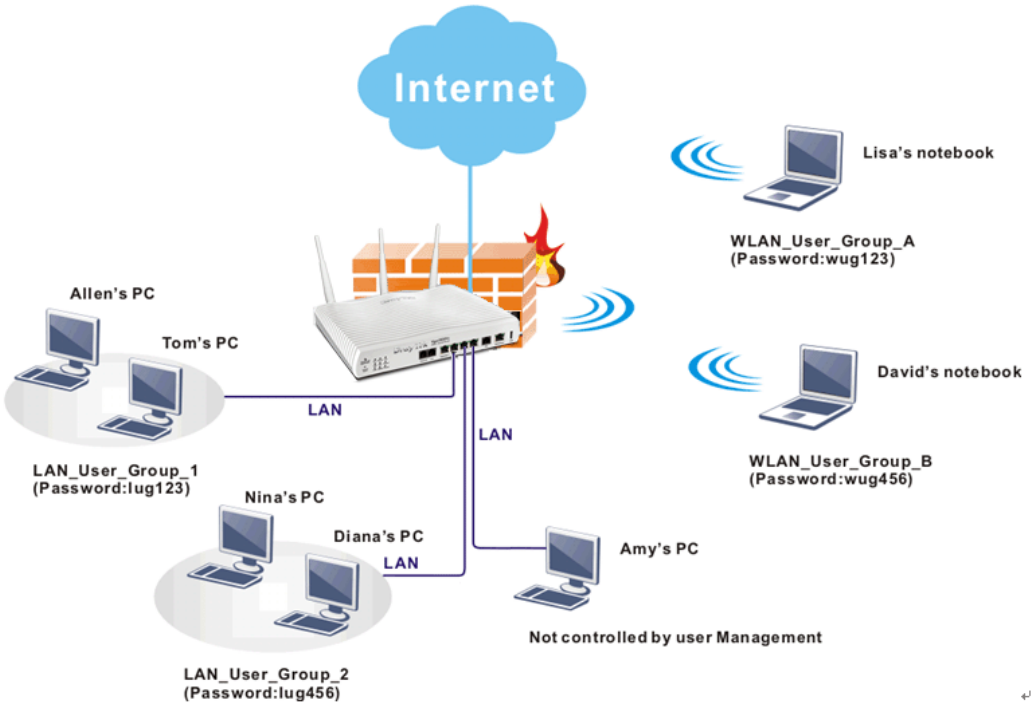

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable/Disable** | Enables or disables the APP QoS feature. |
| **Traceable** | Traceable applications are those whose traffic can be 100% traced.<br>All protocols under this tab can have a specific QoS class assigned.<br>**Enable** - Select to enable OoS for the application.<br>**Apply to all** - Select a QoS class to be applied to all protocols. You can override the QoS class for specific protocols using the Action dropdown listbox. |
| **Untraceable** | Untraceable applications are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.<br>All protocols under this tab can have a specific QoS class assigned.<br>**Enable** - Select to enable OoS for the application.<br>**Action** - Select a QoS class to be applied to all applications. |
| **Select All** | Click to select all Enabled checkboxes. |
| **Clear All** | Click to deselect all Enabled checkboxes. |

After changes have been made, click **OK** to save changes, or **Cancel** to discard.

# VI-3 User Management

User Management allows the network administrator to manage Internet access at the user level. After a user has been authenticated by means of a username and password, he or she can be granted Internet access, and optional firewall rules and WAN access policies can be applied.




**Info**

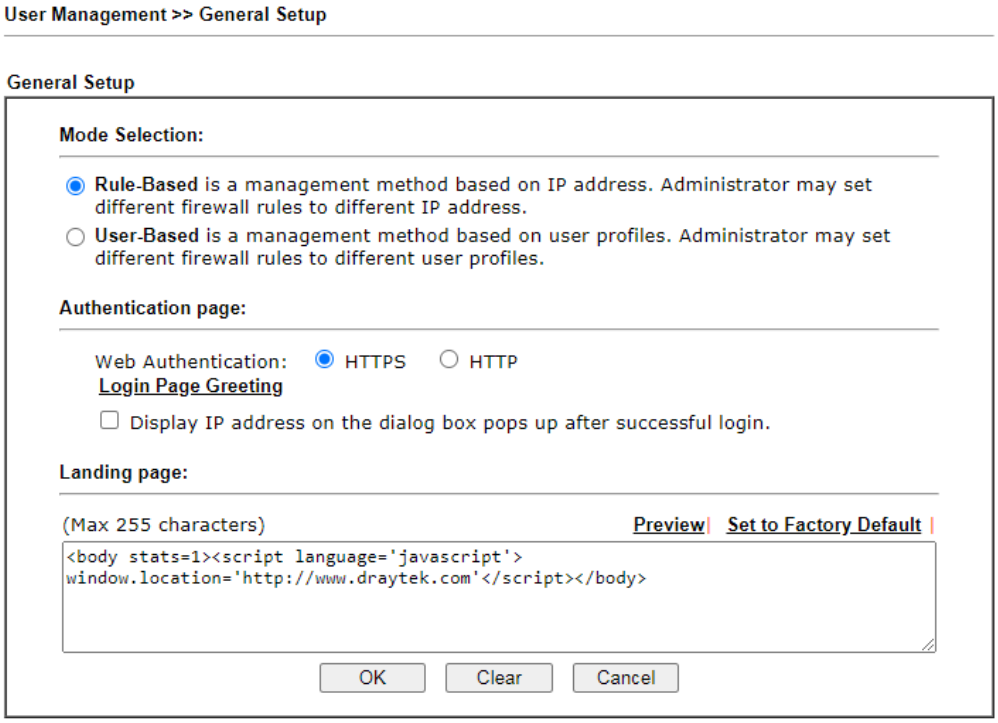
In general, filter rules configured in the Firewall apply globally. However, in user management, the filter rules can be selectively applied to user profiles.

# Web User Interface




## VI-3-1 General Setup

Global settings for User Management can be configured in this section.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Mode Selection** | The User Management Mode.<br>**User-Based** – Router applies filter rules configured in **User Management>>User Profile**.<br>**Rule-Based** – Router applies filter rules configured in **Firewall>>General Setup** and **Filter Rule**. |
| **Authentication page** | **Web Authentication** - Web protocol for the web authentication page.<br>● HTTP – Web page will be unencrypted.<br>● HTTPS – Web page will be encrypted.<br>**Login Page Greeting** - Click to be redirected to **System Maintenance >> Login Page Greeting**, where you can configure the message that is shown to the user after a successful login. |

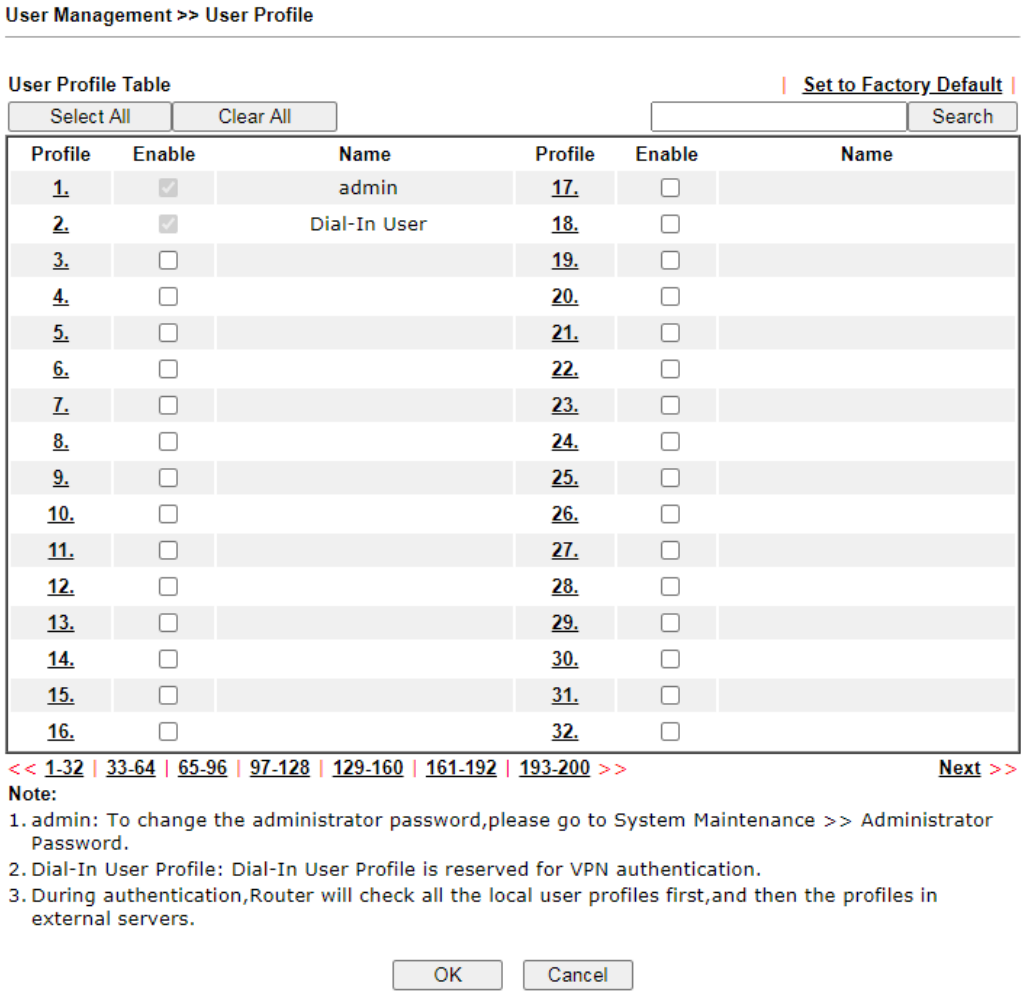
| | |
|---|---|
| | **Display IP Address on tracking window** – Select to display the IP address of the client on the tracking window. |
| **Landing Page** | HTML code to be shown on the Login Page Greeting. |

Click **OK** to save changes, **Clear** to restore settings to factory defaults, or **Cancel** to discard changes.

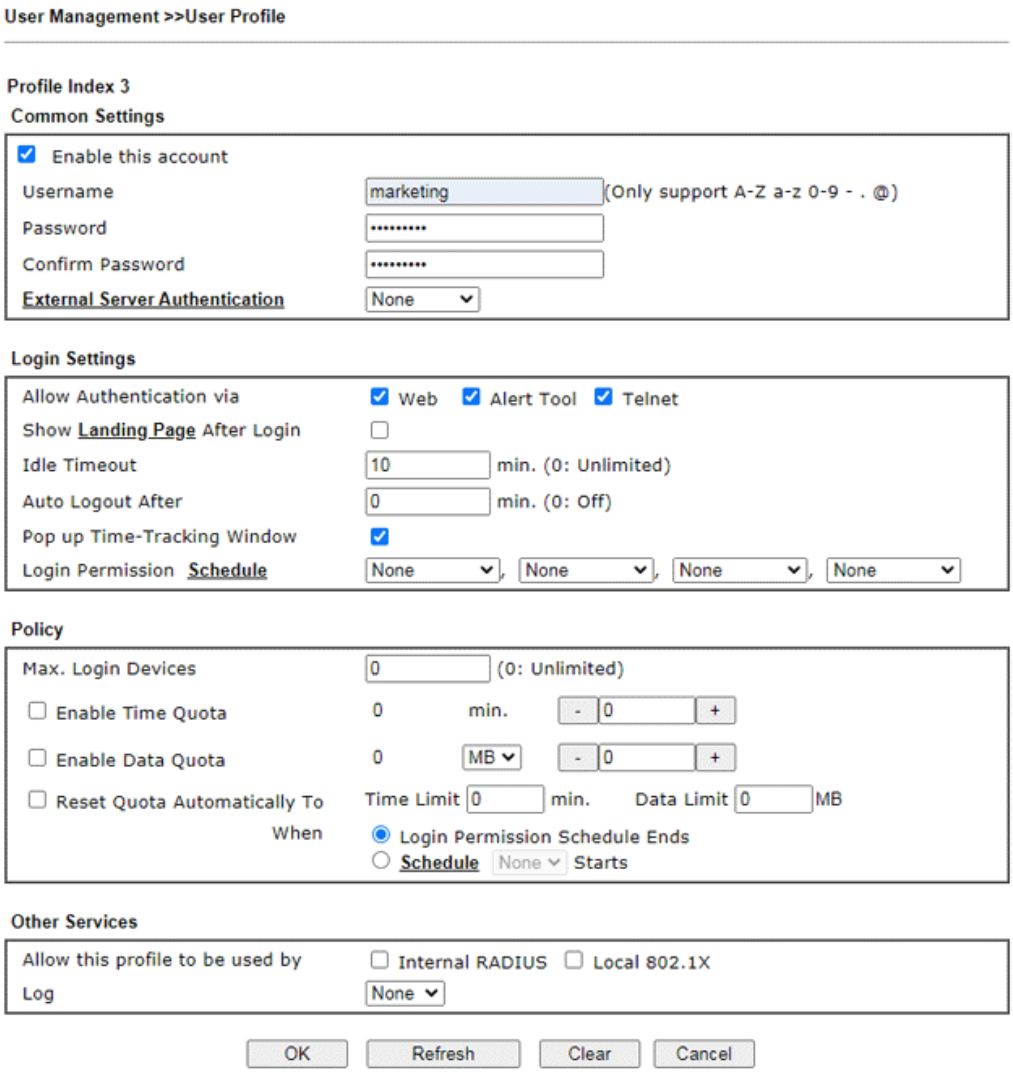
## VI-3-2 User Profile

This page allows you to create up to 200 user profiles for use with User Management.

Select **User Management>>User Profile** from the menu bar, then click a profile number to configure.



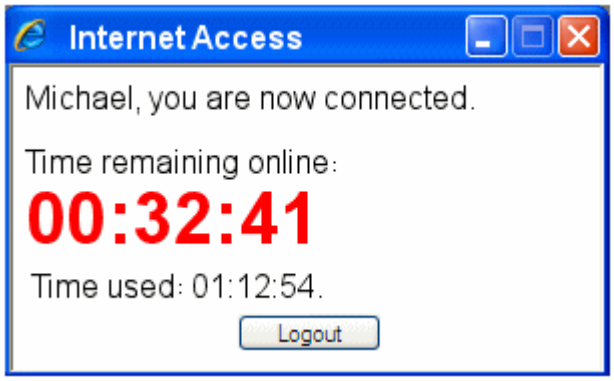

Profiles 1 (admin) and 2 (Dial-In User) are reserved profiles. The admin profile applies to the router administrator login, while the Dial-in User profile applies to all VPN dial-in users.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Common Settings** | |
| **Enable this account** | Select to enable this user profile. |
| **Username** | Login name (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc.) for this user profile. Maximum length is 24 characters. |
| **Password** | Password (e.g., *lug123*, *wug123*,*wug456*, etc.) for this user profile. Maximum length is 24 characters.<br>When a user tries to access the Internet and User Management is enabled, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session. |
| **Confirm Password** | Enter the password again for confirmation. |
| **External Service Authentication** | The router will authenticate dial-in users using either a built-in (None) or external service (LDAP, Radius or TACACS+). The Password setting is ignored when an external authentication service is used. |
| **Login Settings** | |

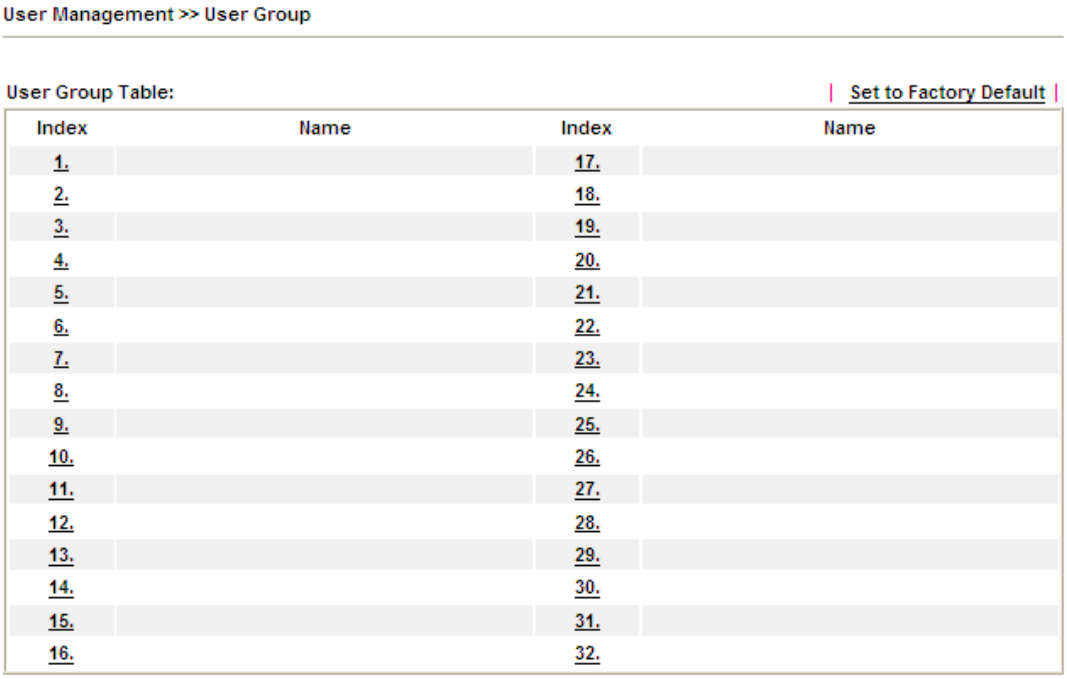
| | |
|---|---|
| **Allow Authentication via** | The authentication methods allowed for this user.<br>**Web** – If selected, user will need to authenticate by entering a username and password when attempting to access an external website for the first time. The user will be redirected to the external website after a successful authentication.<br>**Alert Tool** – If selected, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed. The Alter Tool can be downloaded from the DrayTek website.<br>**Telnet** – If selected, the user can authenticate by logging in to the router using telnet. |
| **Show Landing Page After Login** | When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in **User Management>>General Setup**.<br>Check this box to enable such function. |
| **Idle Timeout** | If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will need to re-authenticate before Internet access is once again allowed. The default Idle Timeout value is 10 minutes. |
| **Auto Logout After** | Such account will be forced to logout after a certain time set here. |
| **Pop up Time-Tracking Window** | If enabled, a browser window will pop up showing the session time remaining. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection. |
| **Login Permission Schedule** | You can enter four sets of time schedule for your request. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page. |
| **Policy** | |
| **Max. Login Devices** | The maximum number of concurrent logins allowed for this profile. The default setting is 0 which means no limit. |
| **Enable Time Quota** | If selected, the user is allowed Internet access for the specified amount of time after a successful authentication.<br>The first value is the remaining time of the current login session, whereas the second value is the value to increment or decrement from the remaining time quota by clicking + /- buttons. Both values are in minutes.<br>Click + / - to increase / decrease the time quota for such profile.<br>**Note:** A dialog will be popped up showing the remaining time remained when the user after the user has successfully authenticated. |

| | |
|---|---|
| |  <br>When the time is up, all Internet connections are terminated. |
| **Enable Data Quota** | If selected, the user is allowed to use the specified amount of data after a successful authentication.<br>The first value is the remaining data quota of the current login session, whereas the second value is the value to increment or decrement from the remaining data quota by clicking +/ - buttons. The unit for both values can be set to either MB (megabytes) or GB (gigabytes) using the MB/GB dropdown box.<br>Click + / - to increase / decrease the data quota for such profile. |
| **Reset quota automatically** | Select to enable this option.<br>Reset the time and data quotas to the preset default values when a time schedule ends.<br>**Time Limit** – Enter value for default time quota.<br>**Data Limit** – Enter value for default data quota.<br>**Login Permission Schedule Ends -** When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.<br>**Schedule** – Specify a time schedule index number for this profile. |
| **Other Services** | |
| **Allow this profile to be used by** | This option is available for profiles with index number 3 to 200.<br>**Internal RADIUS-** Check the box to enable security authenticated via internal RADIUS server.<br>**Local 802.1X -** Check the box to enable security authenticated via internal 802.1X server. |
| **Log** | Activities of the user can be recorded by Syslog.<br>**None** – Logging is disabled.<br>**Login** – Login and logout activities are logged.<br>**Event** – Allowed and blocked traffic are logged.<br>**All** – Both Login and Event types are logged. |

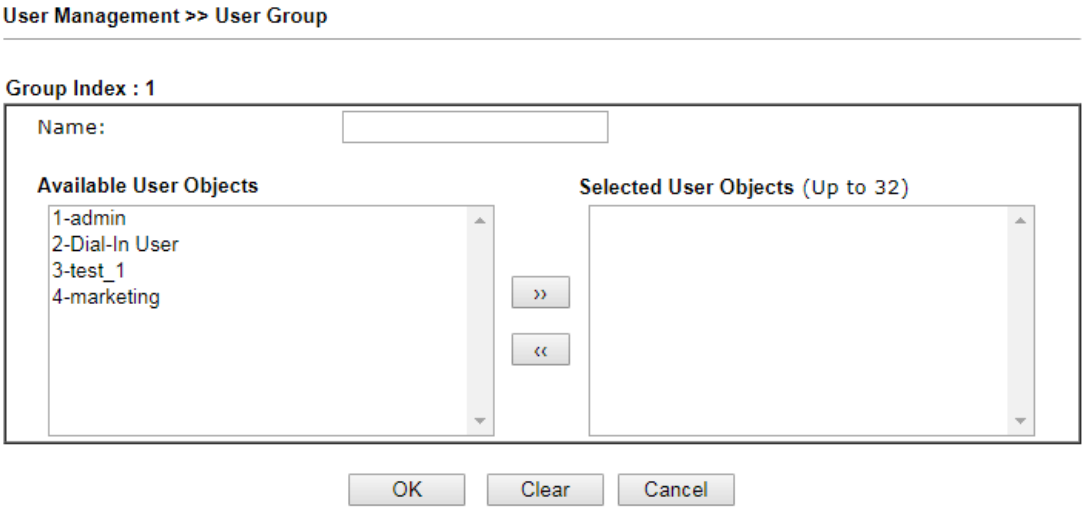
Click **OK** to save changes, **Clear** to restore settings to factory defaults, or **Cancel** to discard changes. Click **Refresh** to reload the page with the most recent data usage information (data and time quotas).

## VI-3-3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in **Firewall>>General Setup**.




Click an index number link to its setup page:




Available settings are explained as follows:

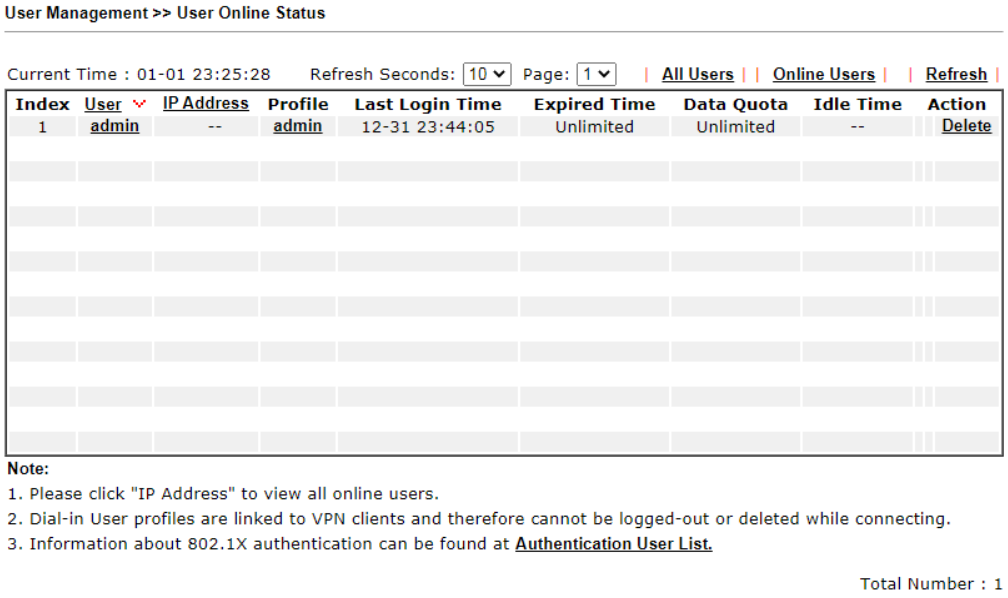
| Item | Description |
|---|---|
| **Name** | Name that identifies this user group. |
| **Available User Objects** | Shows a list of User Objects that have not been placed into the current group. |

| | |
|---|---|
| >><br><br><< | Click >> to move selected user objects in the Available User Objects on the left to the Selected User Objects on the right, thus adding them to the current group.<br>Click << to move selected user objects in the Selected User Objects on the right to the Available User Objects on the left, thus removing them from the current group. |
| **Selected Keyword Objects** | Shows a list of User Objects that have been placed into the current group. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To remove all user objects from the current group, click **Clear**.

## VI-3-4 User Online Status

This page displays the users that are currently logged into the router. The list refreshes periodically to show the most up-to-date information.




Available settings are explained as follows:

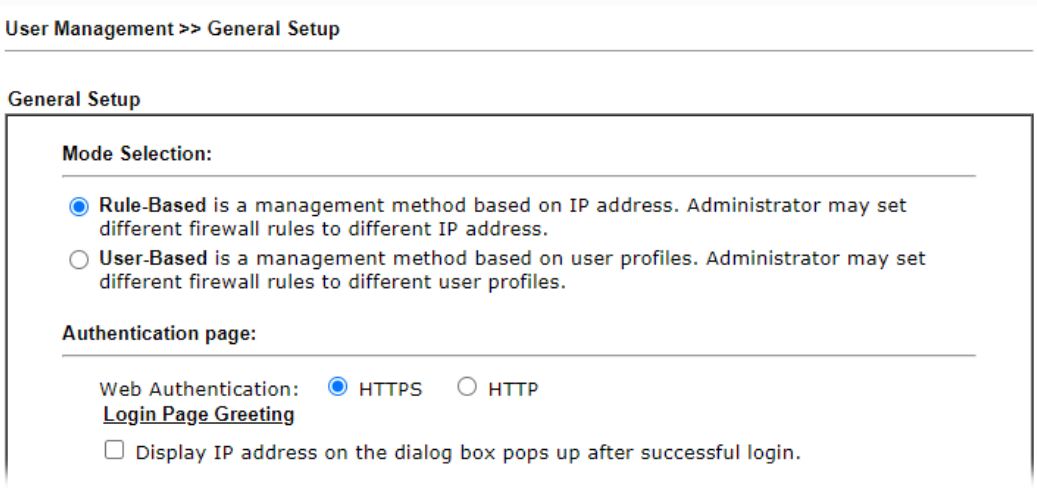
| Item | Description |
|---|---|
| **Refresh Seconds** | The time interval between automatic screen refreshes, in seconds. Select one of 10, 15 and 30 seconds. |
| **Refresh** | Click to manually refresh the displayed data. |
| **Index** | Index of the user entry. |
| **User** | The name of the user that is logged on. Clicking this will bring up the following page which allows setting time and data quotas of the user.<br>For details, refer to the description on the **Enable Time Quota** and **Enable Data Quota** items in the **User Profile** section. |
| **IP Address** | IP LAN address of the device that initiated the login. |
| **Profile** | Name of the user profile. If the logged-in user is a VPN user, Dial-in User will be displayed. Otherwise it will be the same as User. |

| | |
|---|---|
| **Last Login Time** | The most recent login time of the user. |
| **Expired Time** | The expiration time of the current login session. |
| **Data Quota** | Display the quota for data transmission.<br>The remaining data quota of this login session. |
| **Idle Time** | Amount of time the session has been idled. |
| **Action** | **Block** – Stops user from accessing the Internet.<br>**Unblock** –Resumes Internet access of a blocked user.<br>**Logout** – Terminates the current login session.<br>**Delete** – Removes the user entry from the User Online Status page. |

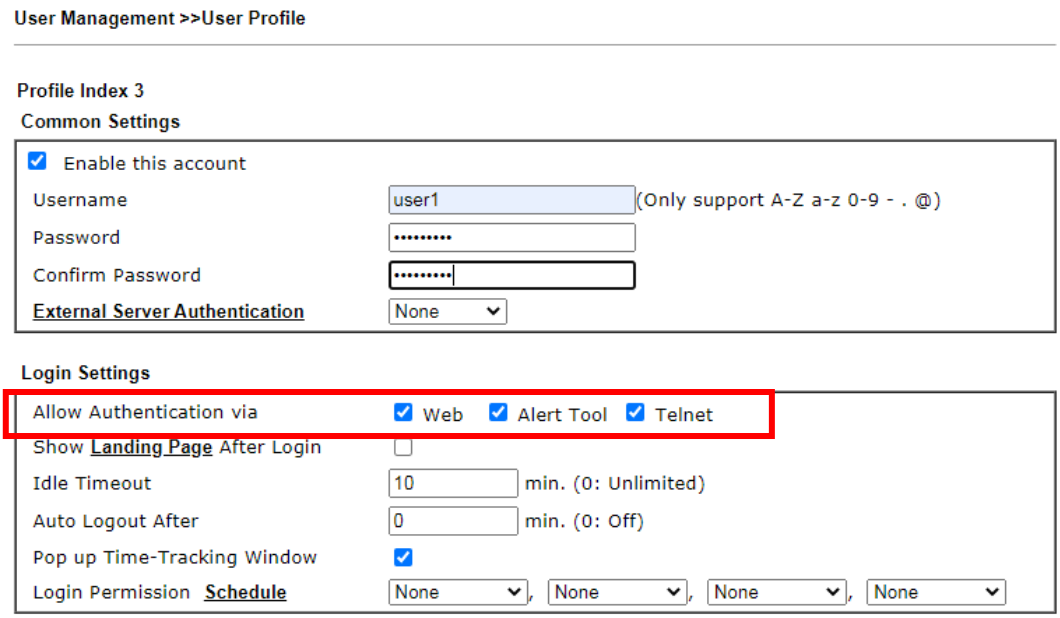
# Application Notes

## 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.

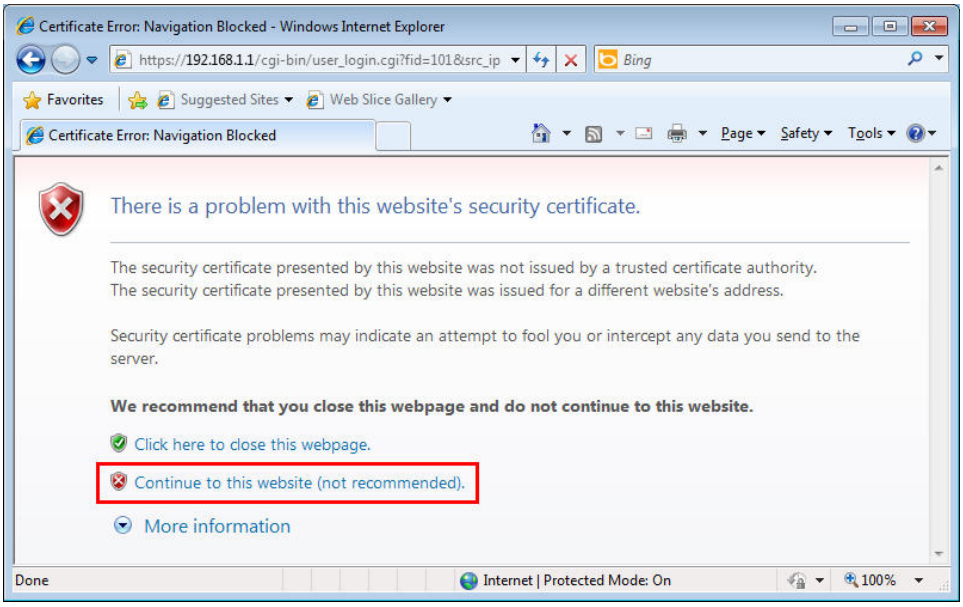



With **User Management** authentication function, before a valid username and password have been correctly supplied, a particular client will not be allowed to access Internet through the router. There are three ways for authentication: **Web**, **Telnet** and **Alert Tool**.

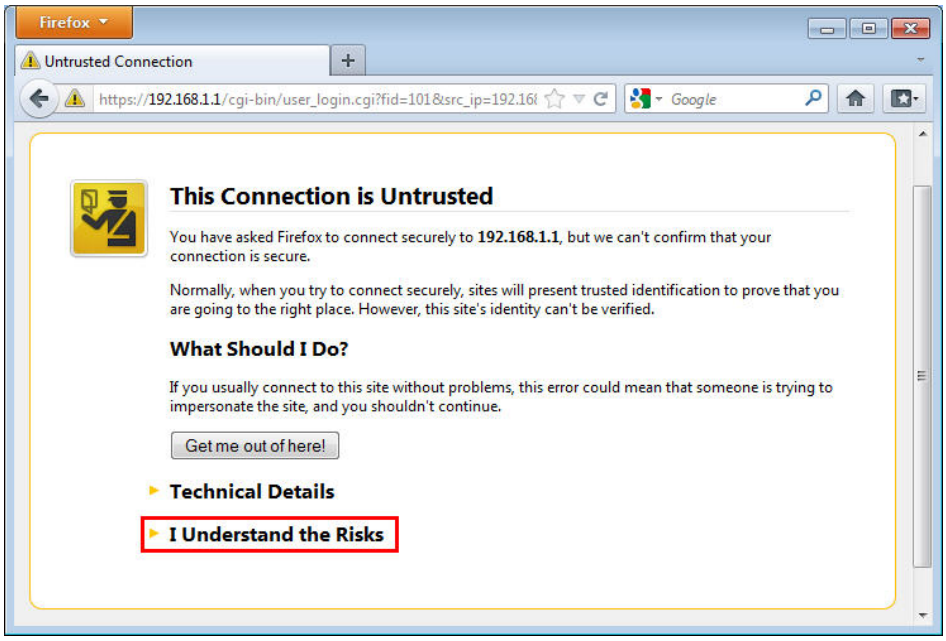



### Authentication via Web

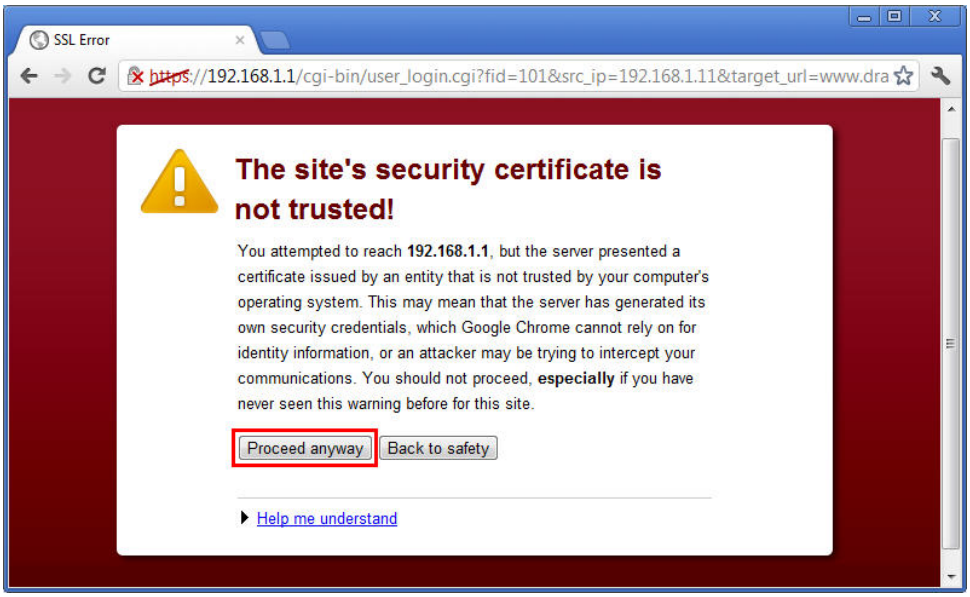
- If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access http://www.draytek.com and but brought to the Vigor router. Since this is an SSL connection,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



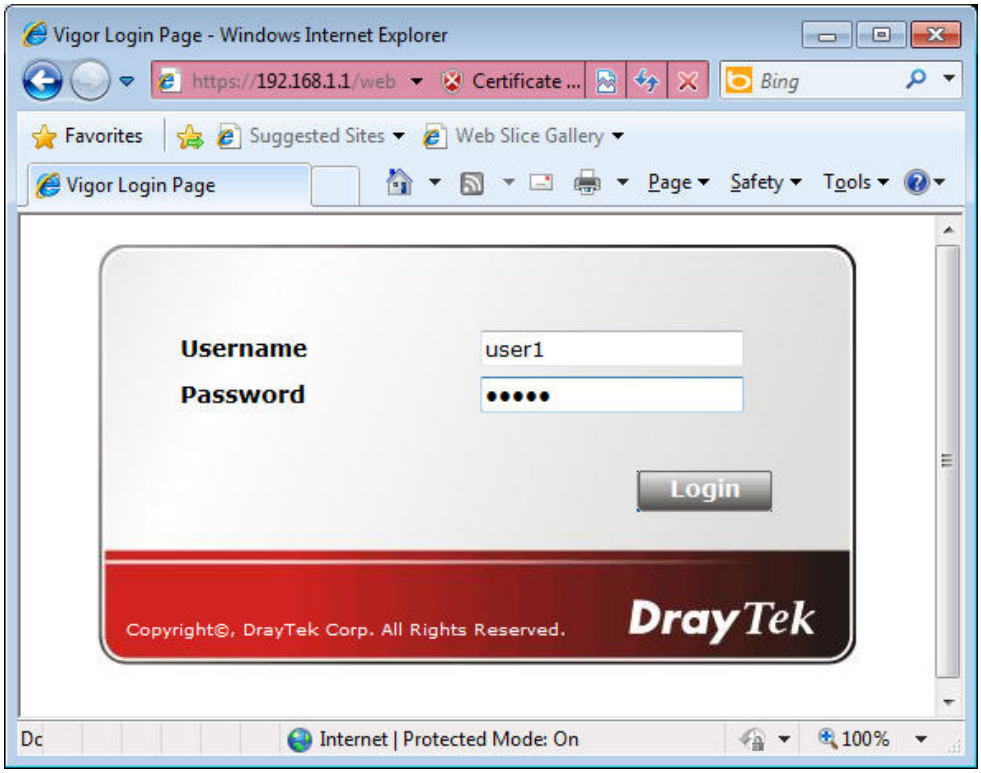

- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.



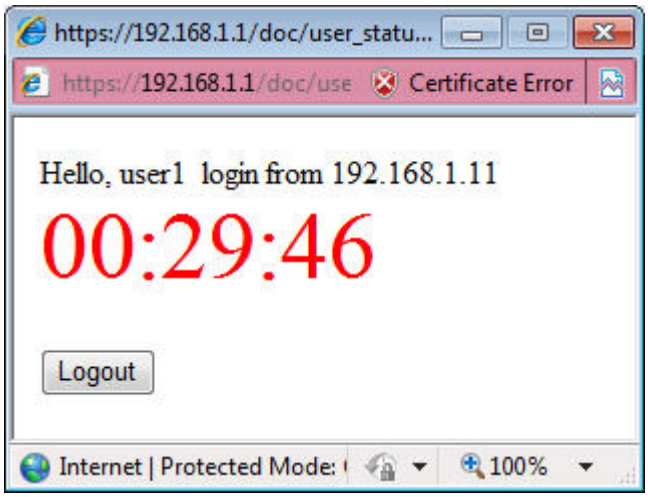
- With Chrome browser, you may get the following warning. Click **Proceed anyway**.




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**.

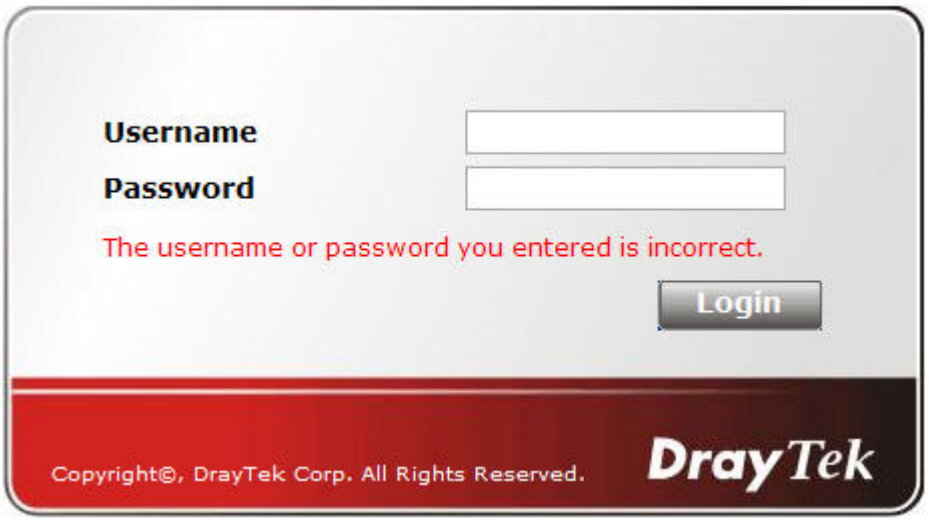



If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is http://www.draytek.com . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



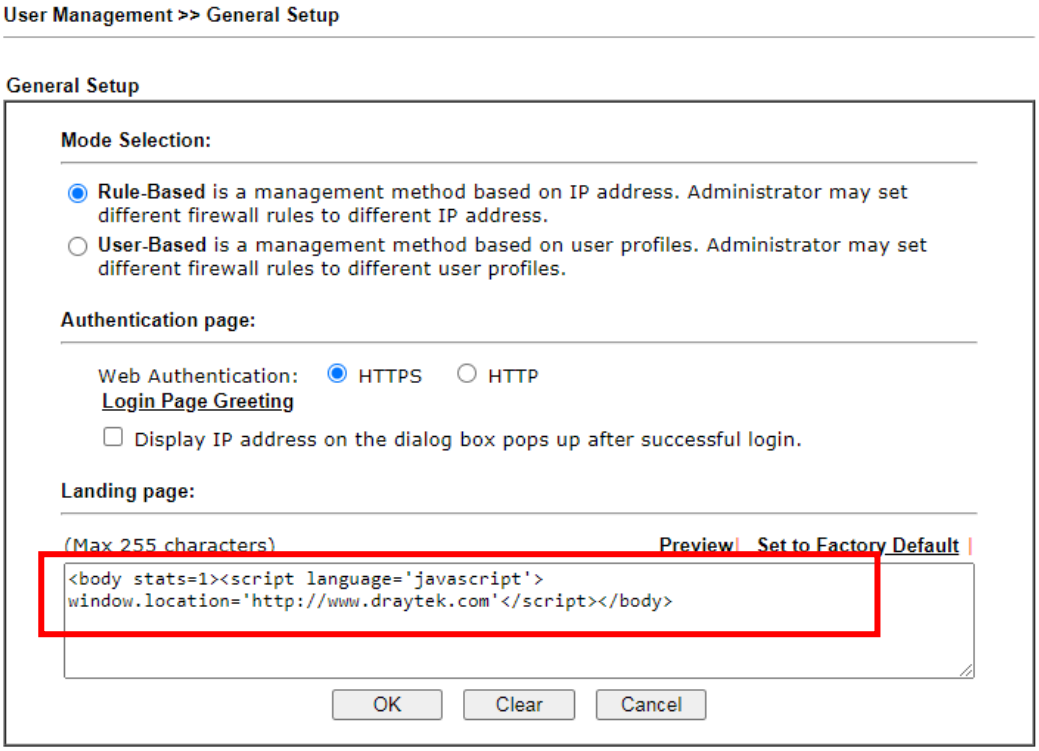

Note, if you block the web browser to pop up any window, you will not see such window.

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

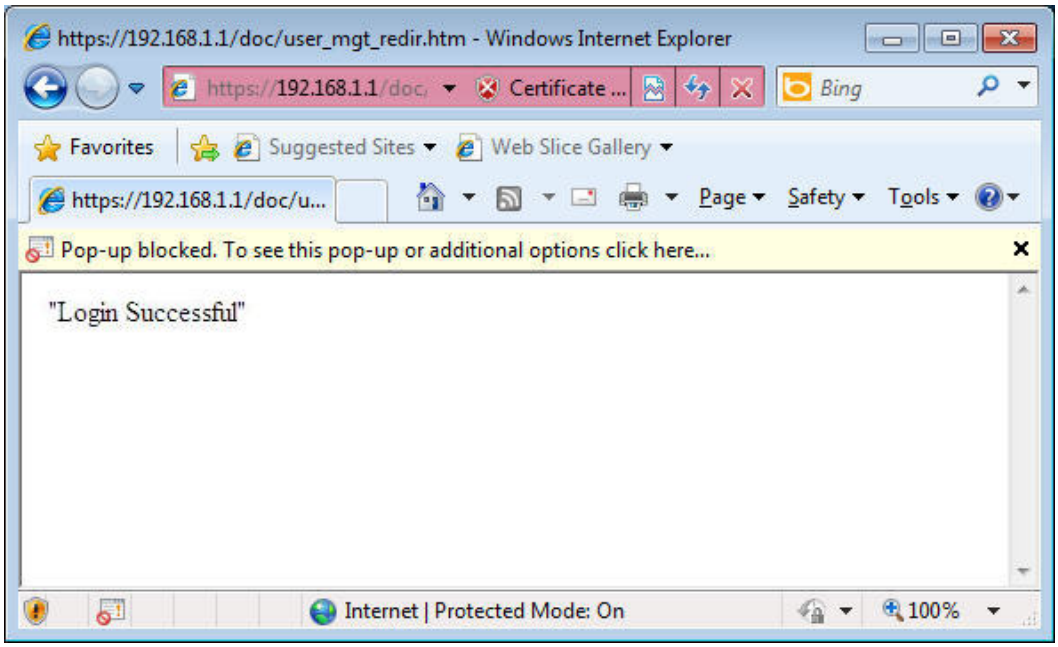



- In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example http://192.168.1.1 or https://192.168.1.1 . Replace 192.168.1.1 with your router's real IP address,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



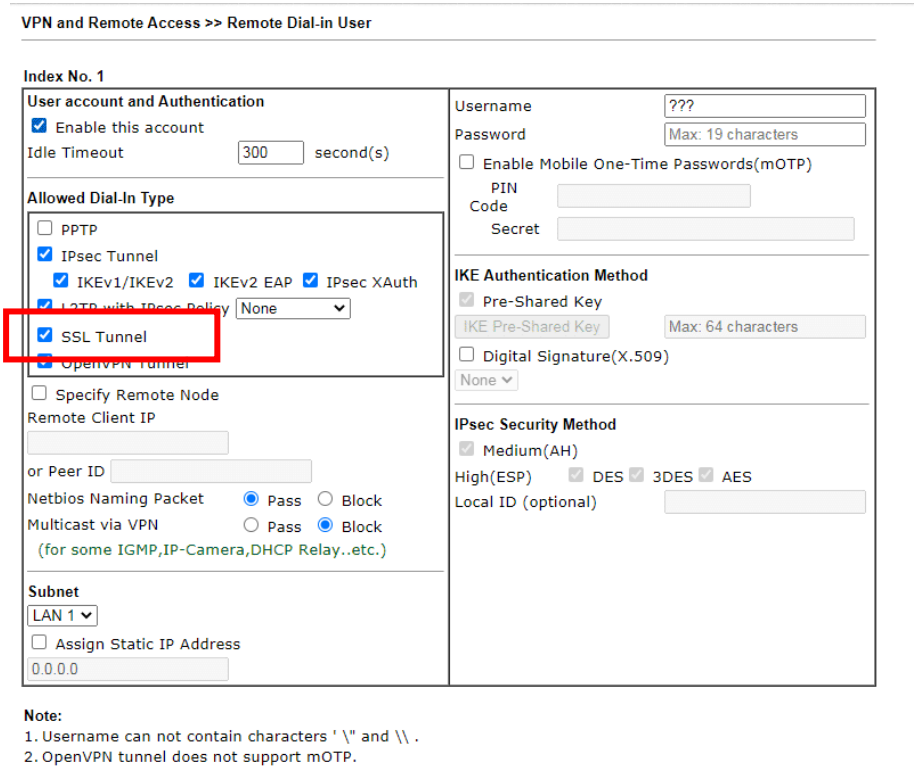

Also you will get a **Tracking Window** if you don't block the pop-up window.

- 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.

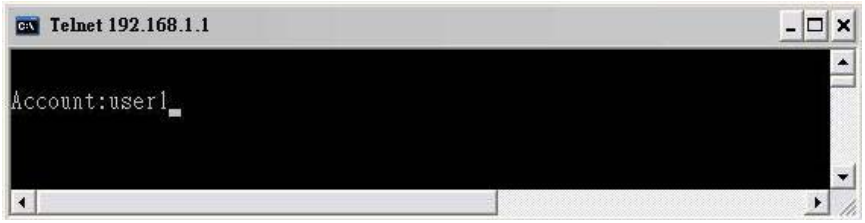



- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

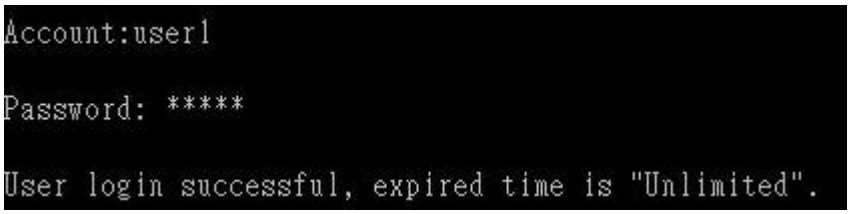
## Authentication via Telnet

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:



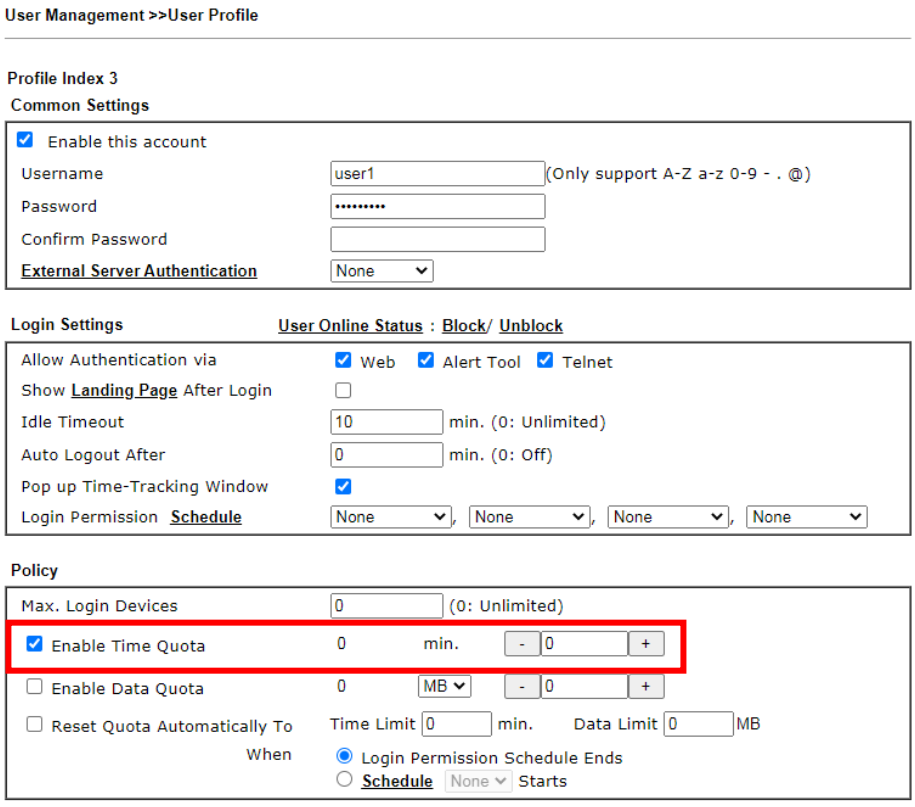

2. Enter the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).



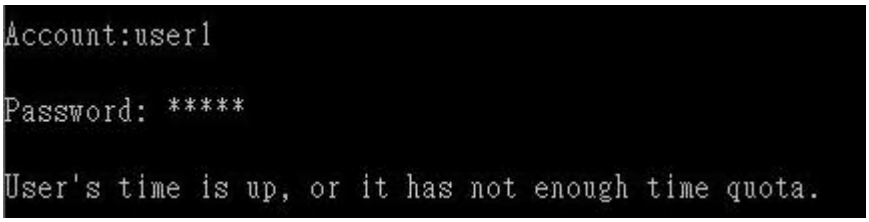

**Info**

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.

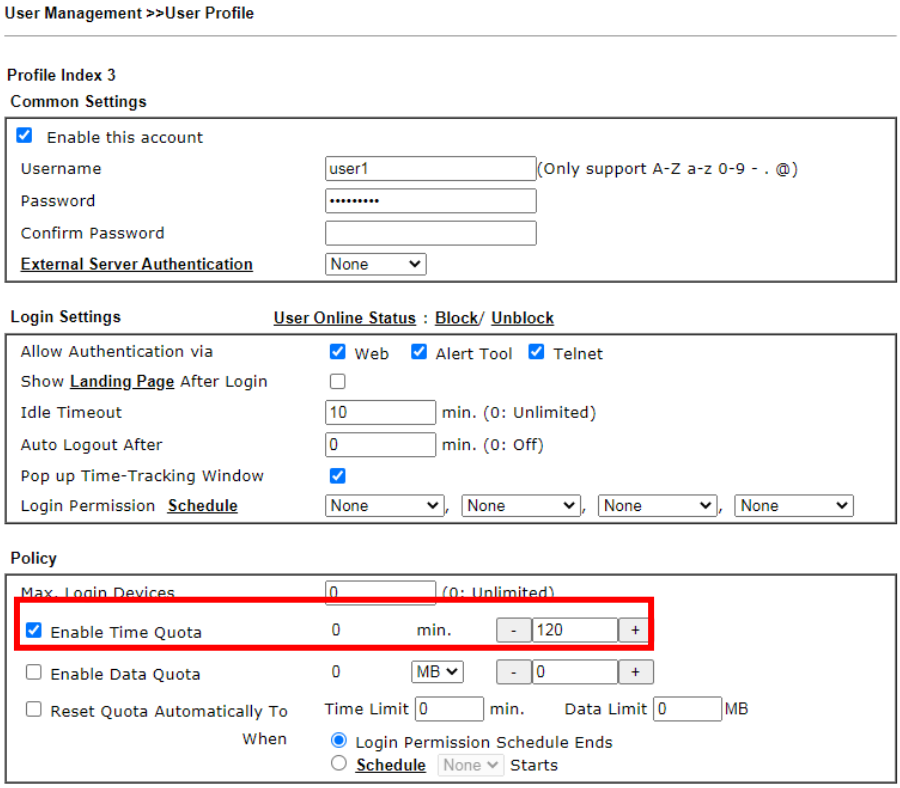
3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.



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.



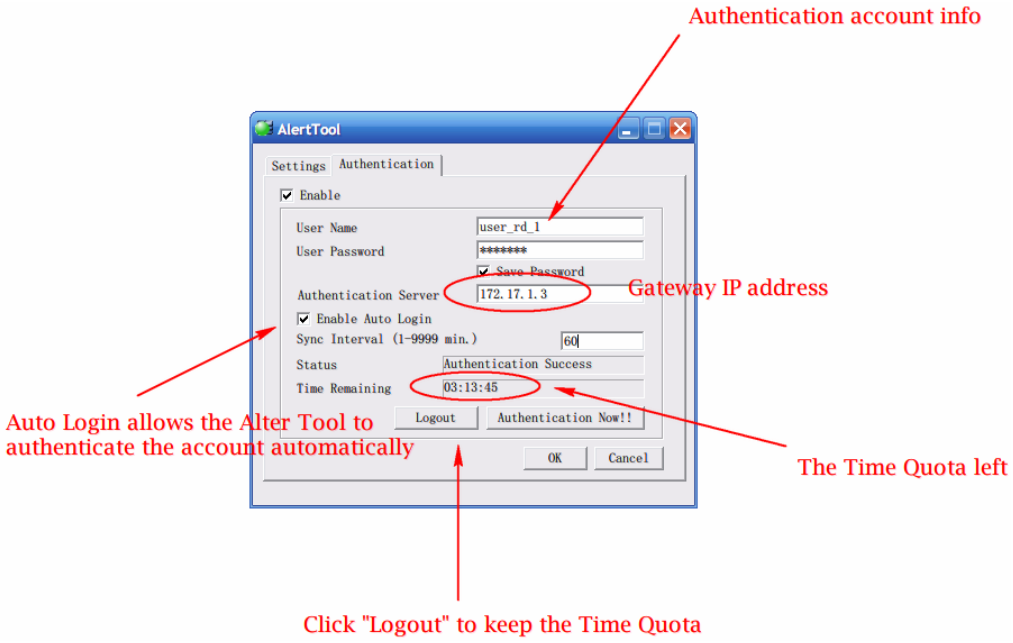

After you run out the available time, you can’t use this account any more until the administrator manually adds additional time for you.

## 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.

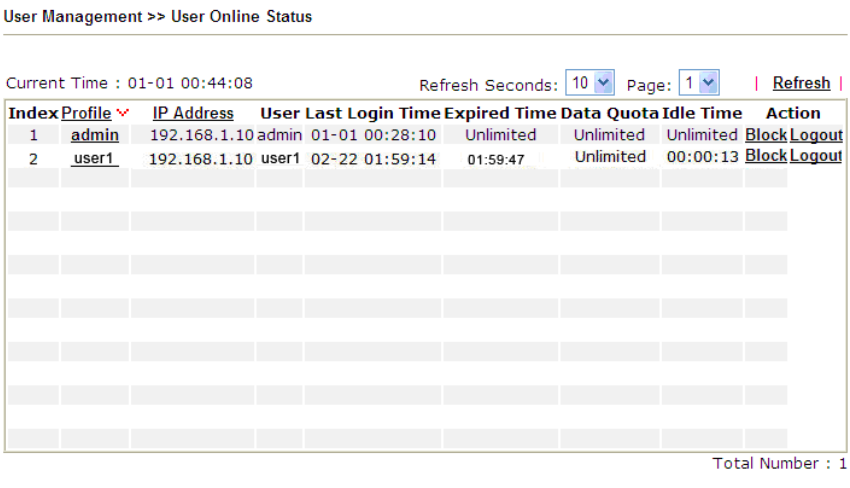
The configuration of the VigorPro Alert Notice Tool is as follows:

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. |

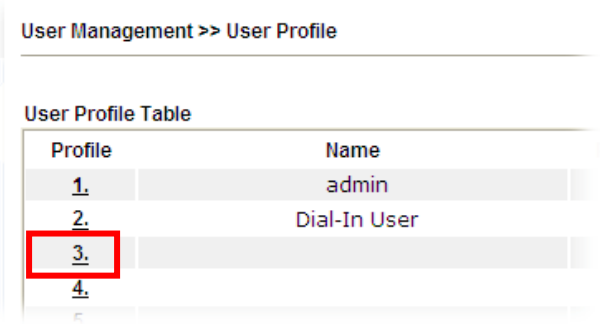


## A-2 How to use Landing Page Feature

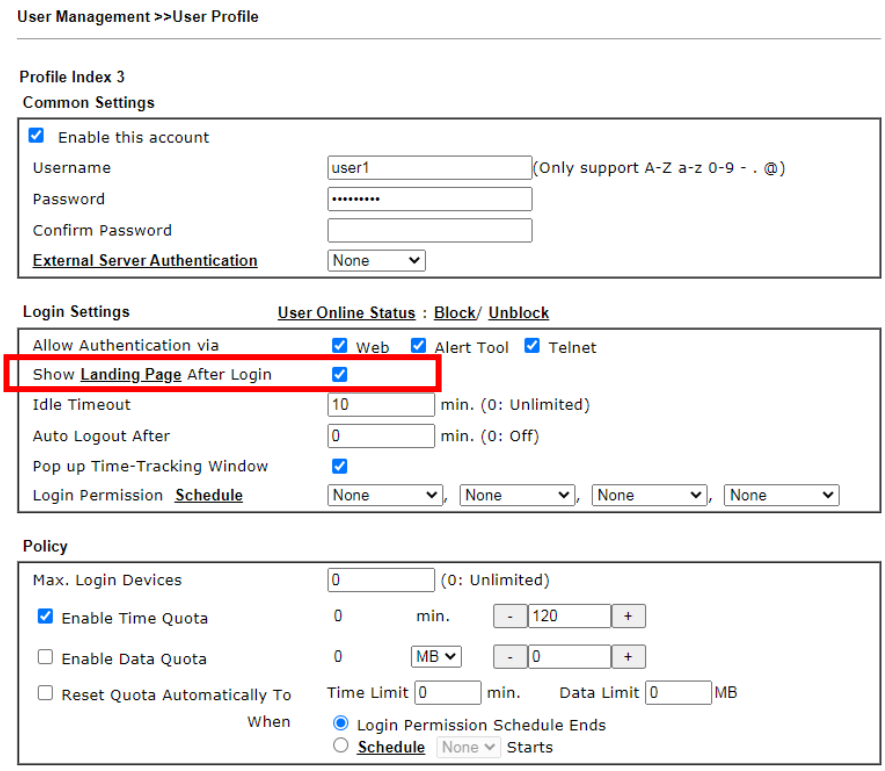
**Landing Page** is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor2927 series router as an example.

### Example 1 : Users can see the message for landing page after logging into Internet successfully

1. Open the web user interface of Vigor2927.
2. Open **User Management -> General Setup** to get the following page. In the field of **Landing Page**, please Enter the words of "**Login Success**". Please note that the maximum number of characters to be typed here is 255.
3. Now you can enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.




4. In the following page, check the box of **Landing page** and click **OK** to save the settings.



5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.




6. Click **Login**. If the logging is successful, you will see the message of Login Success from the browser you use.

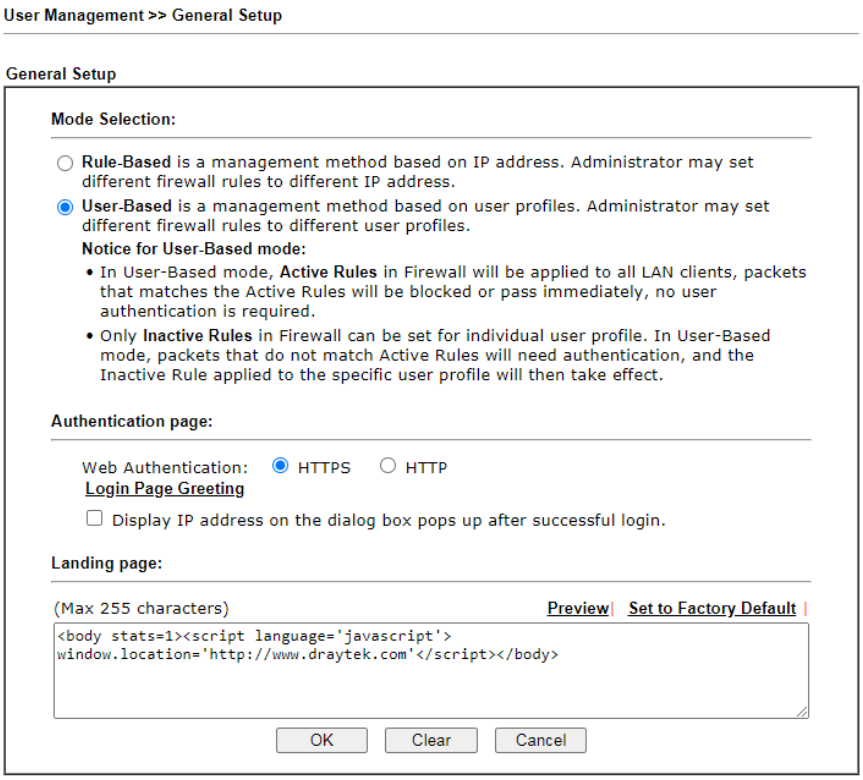


Example 2：The system will connect to http://www.draytek.com automatically after logging into Internet successfully

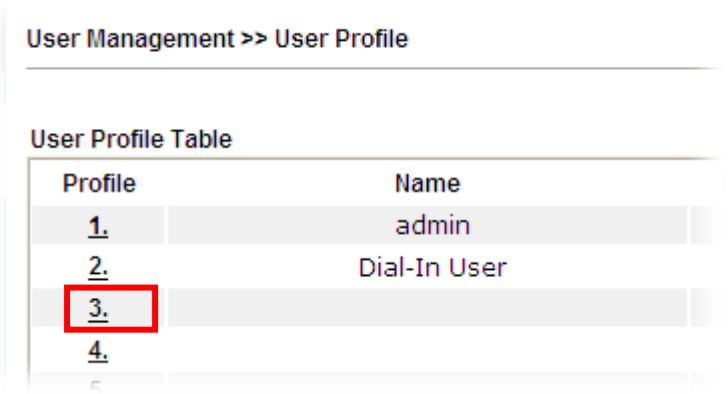
1. In the field of **Landing Page**, please Enter the words as below:

   **“ <body stats=1><script language='javascript'>**

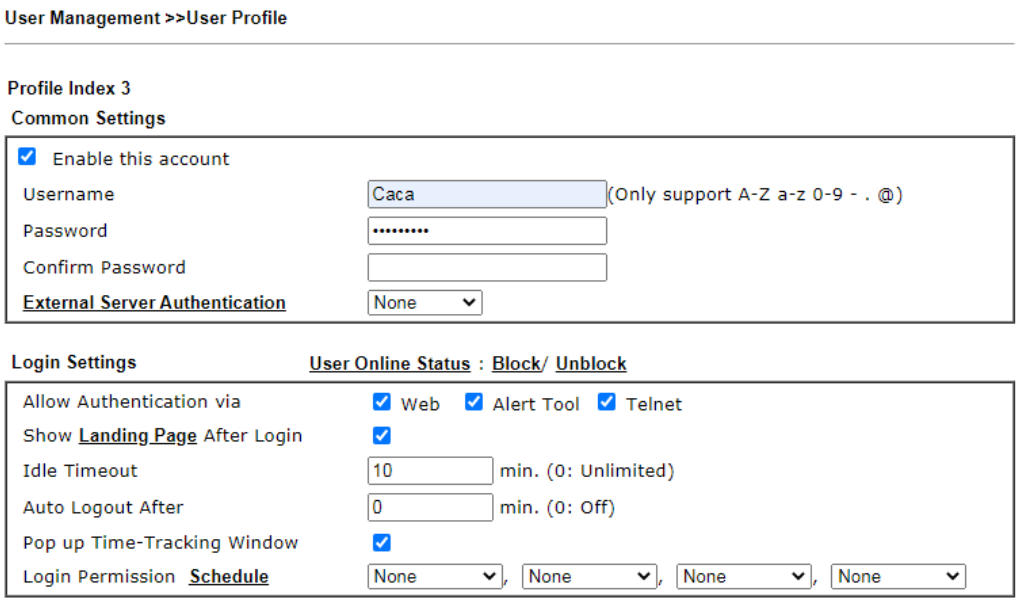
   **window.location='http://www.draytek.com'</script></body>”**




2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.



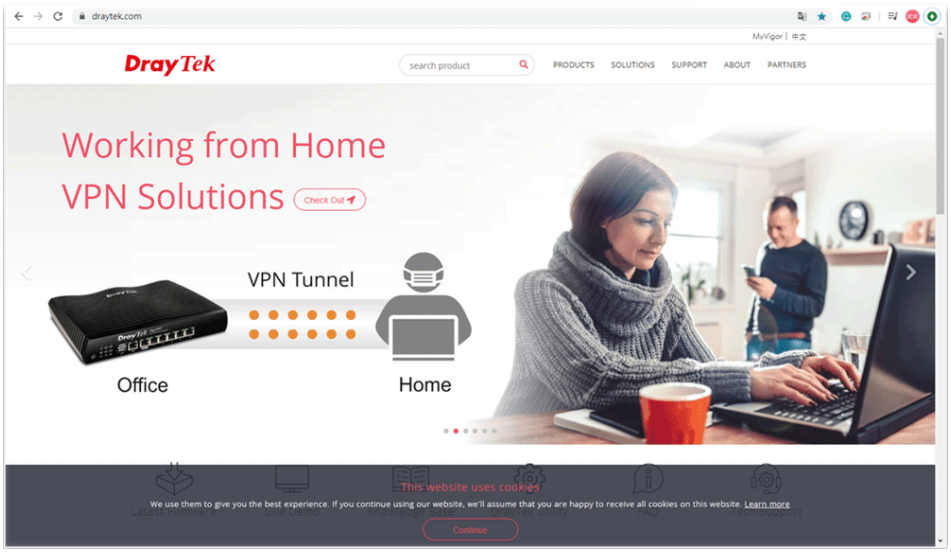
3. In the following page, check the box of **Landing page** and click **OK** to save the settings.




4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please Enter the correct username and password.




5. Click **Login**. If the logging is successful, you will be directed into the website of www.draytek.com.



# VI-4 Hotspot Web Portal

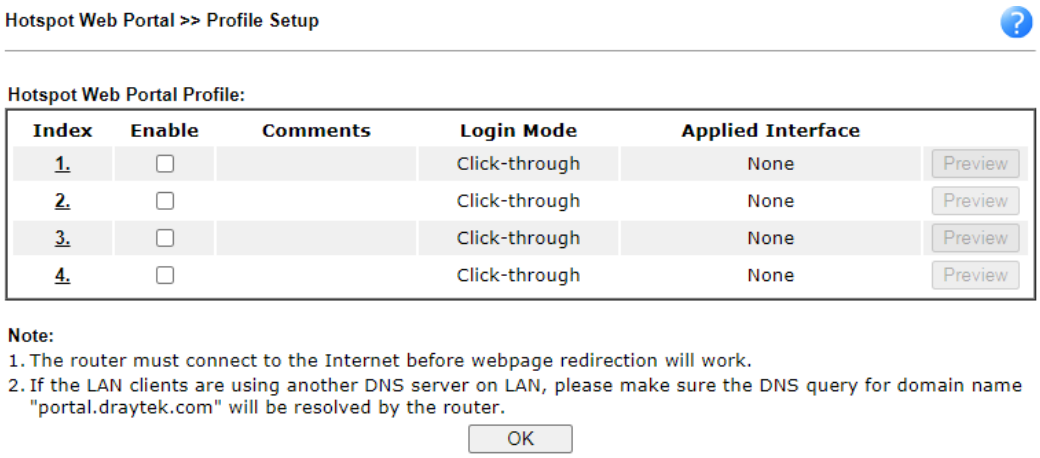
The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

# Web User Interface




## VI-4-1 Profile Setup

Select **Profile Setup** to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Index** | Click the index number link to view or update the profile settings. |
| **Enable** | Check the box to enable the profile. |
| **Comments** | Shows the description of the profile. |
| **Login Mode** | Shows the login mode used by the profile. See the section *Login Mode* for details. |
| **Applied Interface** | Shows the interfaces to which this profile applies. |

| | |
|---|---|
| **Preview** | Click this button to preview the Hotspot Web Portal page that will be displayed to users. |

## VI-4-1-1 Login Method

There are four login methods to choose from for authenticating network clients: **Skip Login**, **Click Through**, **Social Login**, **PIN Login**, and **Social or PIN Login**. Each login mode will present a different web page to users when they connect to the network.

### (A) Skip Login, landing page only

This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.

### (B) Click-through

The following page will be shown to the users when they first attempt to access the Internet through the router. After clicking **Accept** on the page, users will be directed to the landing page (defined in Captive Portal URL) and be granted access to the Internet.

### (C) Various Hotspot Login

An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account, PIN code, password for RADIUS sever, they will be directed to the landing page and be granted access to the Internet.

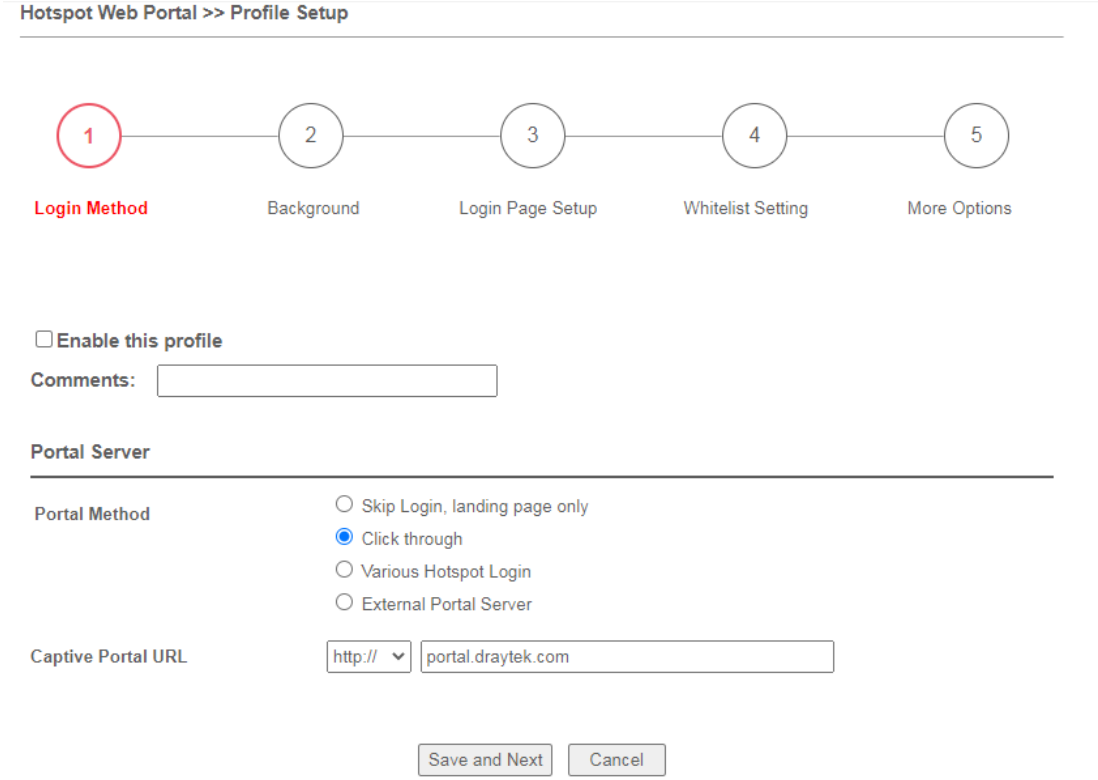
### (D) External Portal Server

External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.

## VI-4-1-2 Steps for Configuring a Web Portal Profile

1 Login Method

Click the index link (e.g., #1) of the selected profile to display the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable this profile** | Check to enable this profile. |
| **Comments** | Enter a brief description to identify this profile. |
| **Portal Server** | |
| **Portal Method** | There are four methods to be selected as for portal server.<br>Skip Login, landing page only<br>Click through<br>Various Hotspot Login<br>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.<br>**Choose Login Method -** Select one or more desired login methods.<br>Login with Facebook<br>Login with Google<br>Receive PIN via SMS<br>Receive PIN via Mail<br>PIN with Voucher<br>Login with RADIUS |

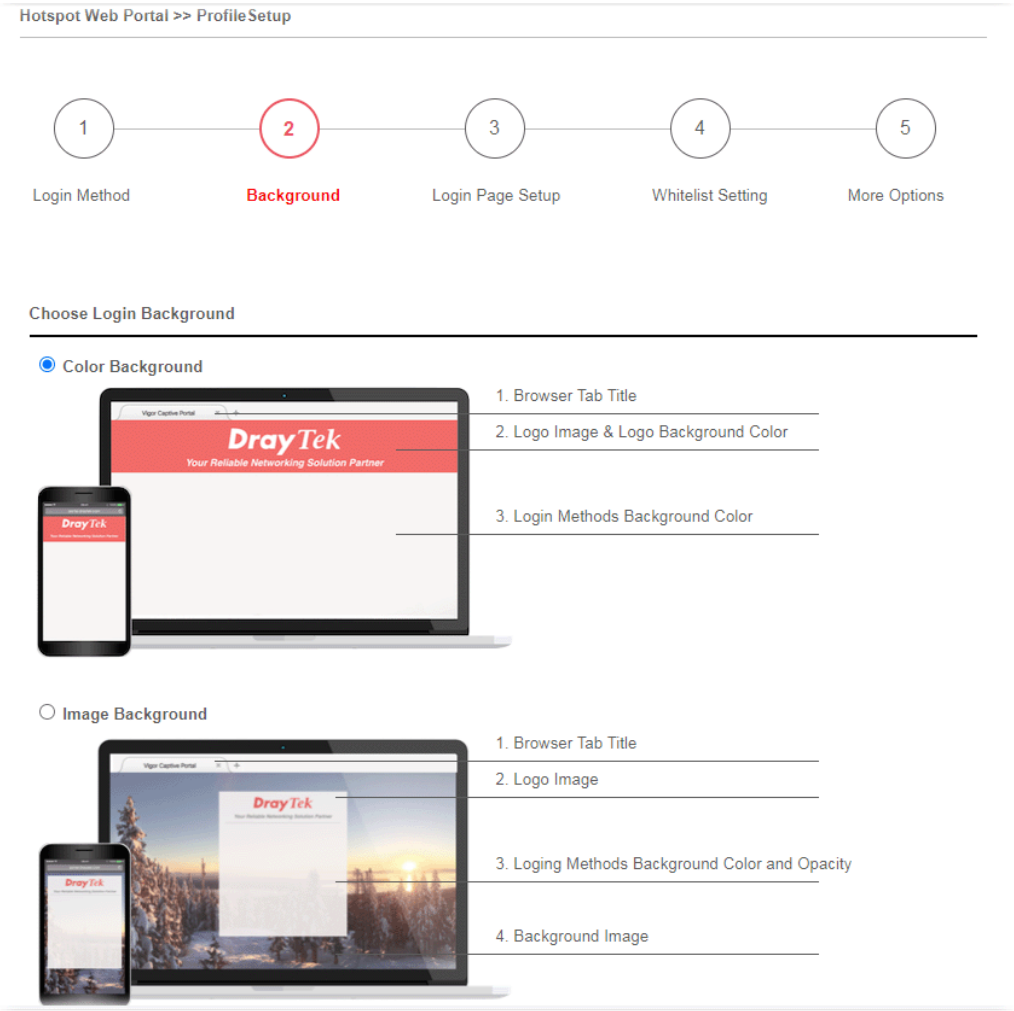
| | |
|---|---|
| **Facebook**<br>(Login with Facebook**)** | This setting is available when **Login with Facebook** is selected as the login method.<br>**Facebook APP ID** - Enter a valid Facebook developer app ID.<br>If you do not already have an app ID, refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for instructions on obtaining an APP ID.<br>**Facebook APP Secret** - Enter the secret configured for the APP ID entered above.<br>Refer to section A-1 *How to create a Facebook App ID for Web Portal Authentication* for details. |
| **Google**<br>(Login with Google) | This setting is available when **Login with Google** is selected as the login method.<br>**Google App ID** - Enter a valid Google app ID.<br>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.<br>**Google App Secret** - Enter the secret configured for the APP ID entered above.<br>Refer to section A-2 *How to create a Google APP ID for Web Portal Authentication* for details. |
| **SMS Provider**<br>(Receive PIN via SMS) | This setting is available when **Receive PIN via SMS** is selected as the login method.<br>**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**. |
| **Radius Server**<br>(Login with RADIUS) | This setting is available when **Login with RADIUS** is selected as the login method.<br>**Authentication Method** – Click link to configure the external RADIUS server for authenticating web portal clients.<br>**RADIUS MAC Authentication** – Check **Enable** to activate user authentication by MAC address.<br>**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.<br>**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.<br>**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. |
| **Logo Background Color** | Select the background color of DrayTek Logo, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Login Method Background Color** | Select the background color of the login panel from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Opacity (10 ~ 100)** | Available when **Image Background** is selected. Set the opacity of the background image. |

| | |
|---|---|
| **Background Image** | Available when **Image Background** is selected. Click **Browse…** to select an image file (.JPG or .PNG format), then click **Upload** to upload it to the router. |
| **Save and Next** | Click to save the configuration on this page and proceed to the next page. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

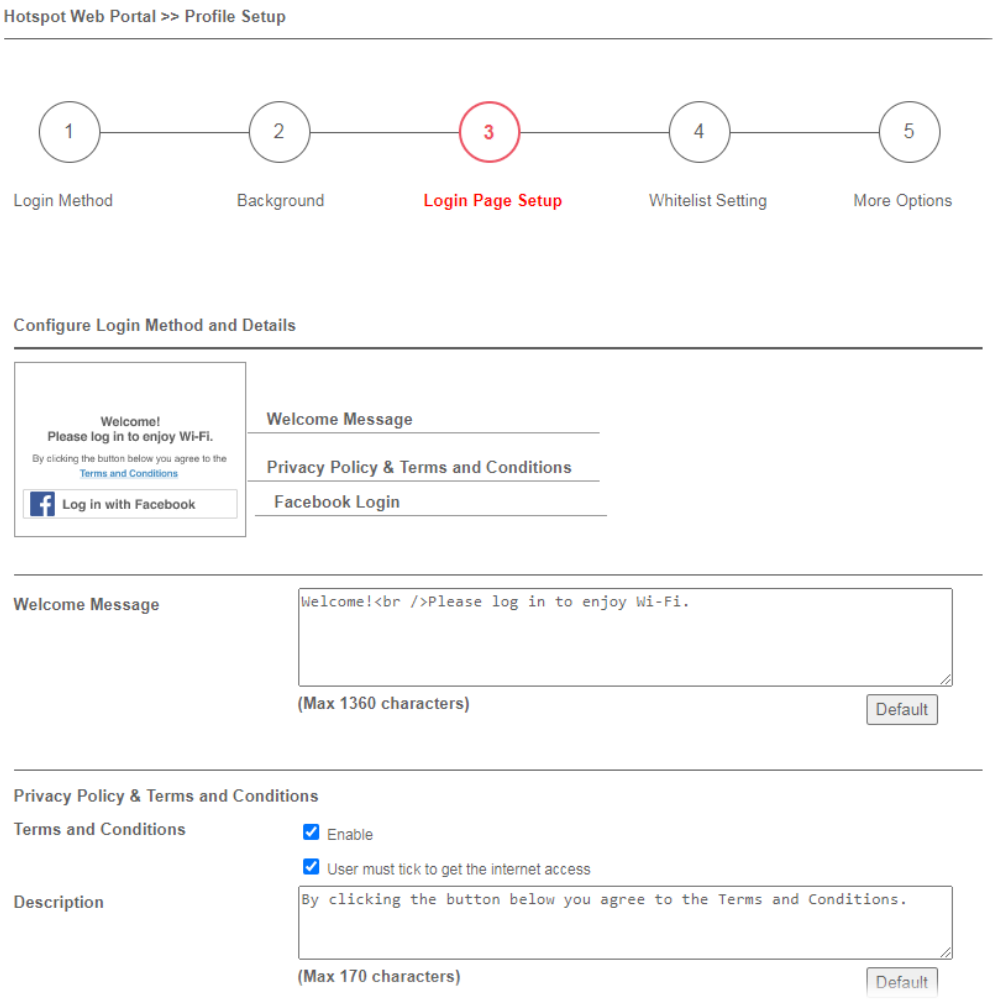
If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup.*

## 3 Login Page Setup

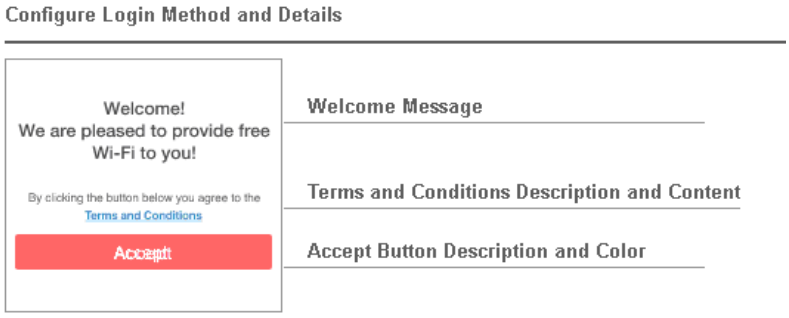
In this step you can configure settings for the login page.

### Click Through

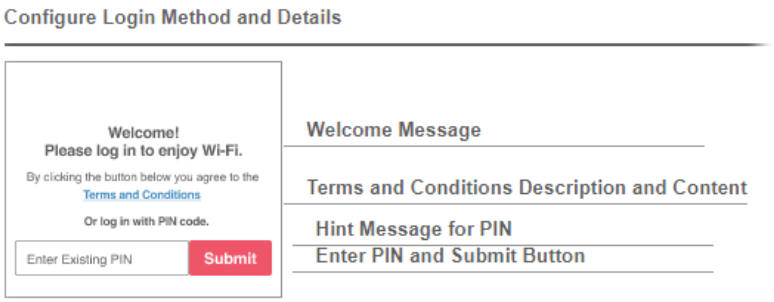
This section describes the Login Page setup if you have selected **Click Through** as the Login Method.




Available settings are explained as follows:

| Item | Description |
|---|---|
| Login dialog will be shown as follows:   | |
| However, when **PIN with Voucher** is selected as the login method, Login dialog will be | |

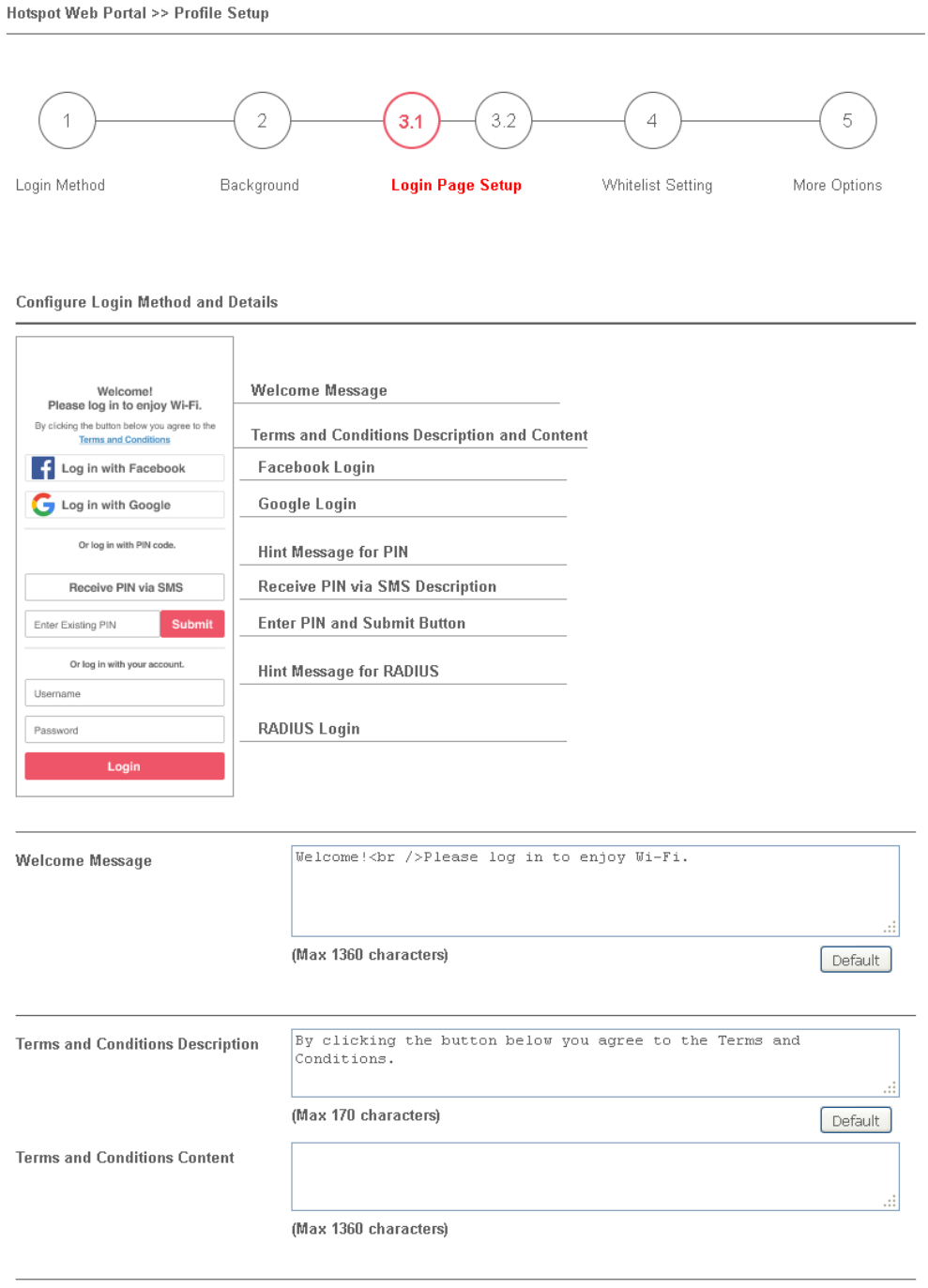
shown as follows:




| | |
|---|---|
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Terms and Conditions Description** | Enter the text to be displayed as the Terms and Conditions hyperlink text. |
| **Terms and Conditions Content** | Enter the text to be displayed in the Terms and Conditions pop-up window. |
| **Hint Message for PIN** | Enter a message to remind the PIN code. |
| **Enter PIN Description** | Enter the existing PIN code. |
| **Submit Button Description** | Enter the text to be displayed on the Submit button |
| **Submit Button Color** | Select the color of the Submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Accept Button Description** | Enter the text to be displayed on the accept button |
| **Accept Button Color** | Select the color of the accept button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Save and Next** | Click to save the configuration on this page and proceed to the next page. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

## Various Hotspot Login

This section describes the Login Page setup step if you have selected Various Hotspot Login the login method. You will see only settings that are relevant to the selected login method(s).




Settings that are common to Facebook, Google, PIN, and RADIUS authentication are:

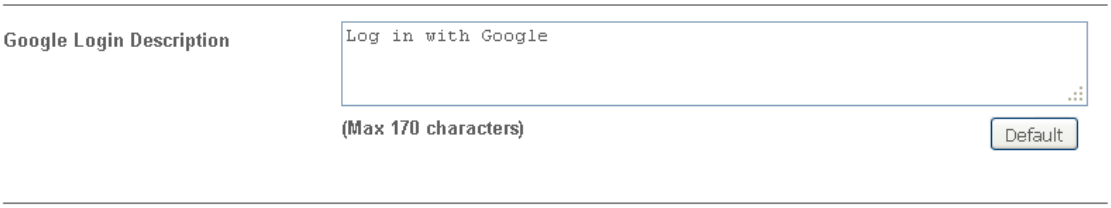
| Item | Description |
|---|---|
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Terms and Conditions Description** | Enter the text to be displayed as the Terms and Conditions hyperlink text. |
| **Terms and Conditions Content** | Enter the text to be displayed in the Terms and Conditions pop-up window. |

If you have selected Facebook login, the setting will appear:



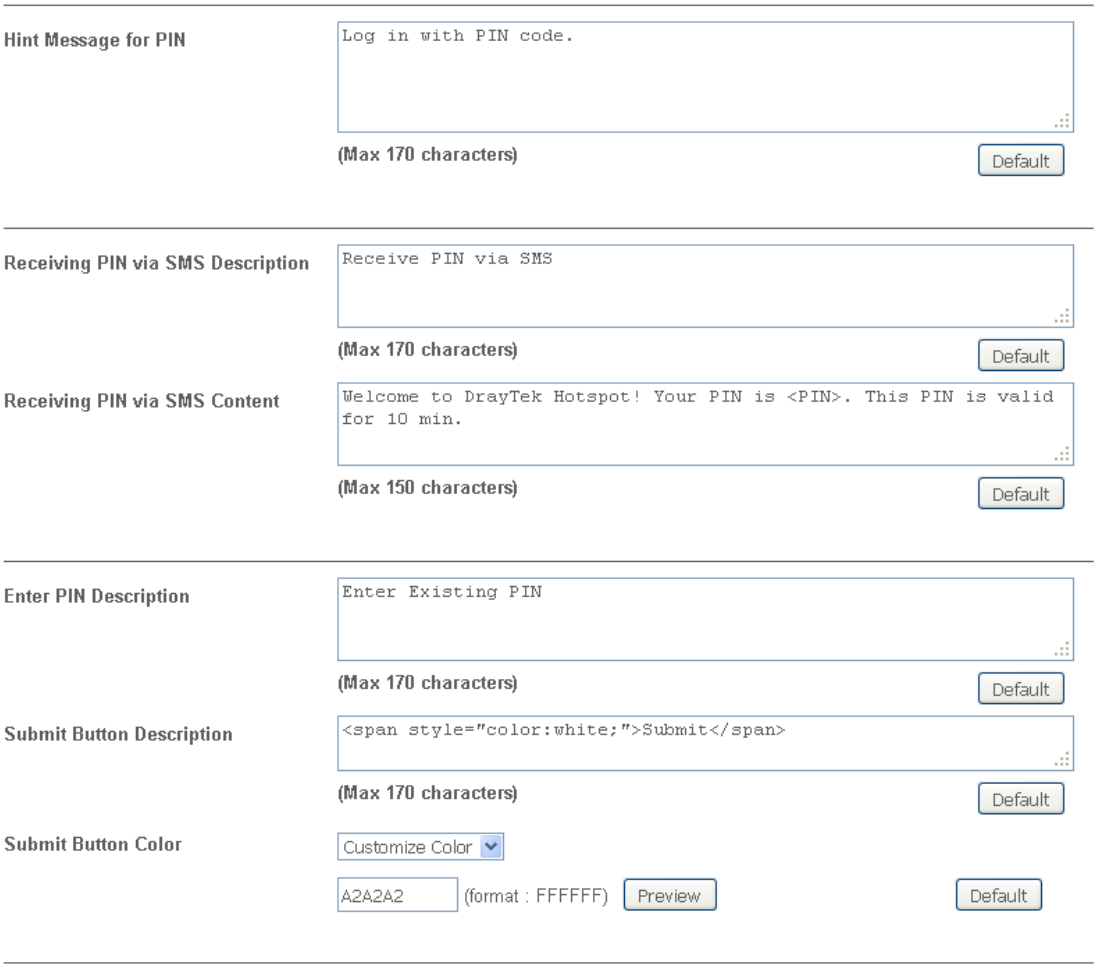

| Item | Description |
|---|---|
| **Facebook Login Description** | Enter the text to be displayed on the Facebook login button. |

If you have selected Google login, the setting will appear:



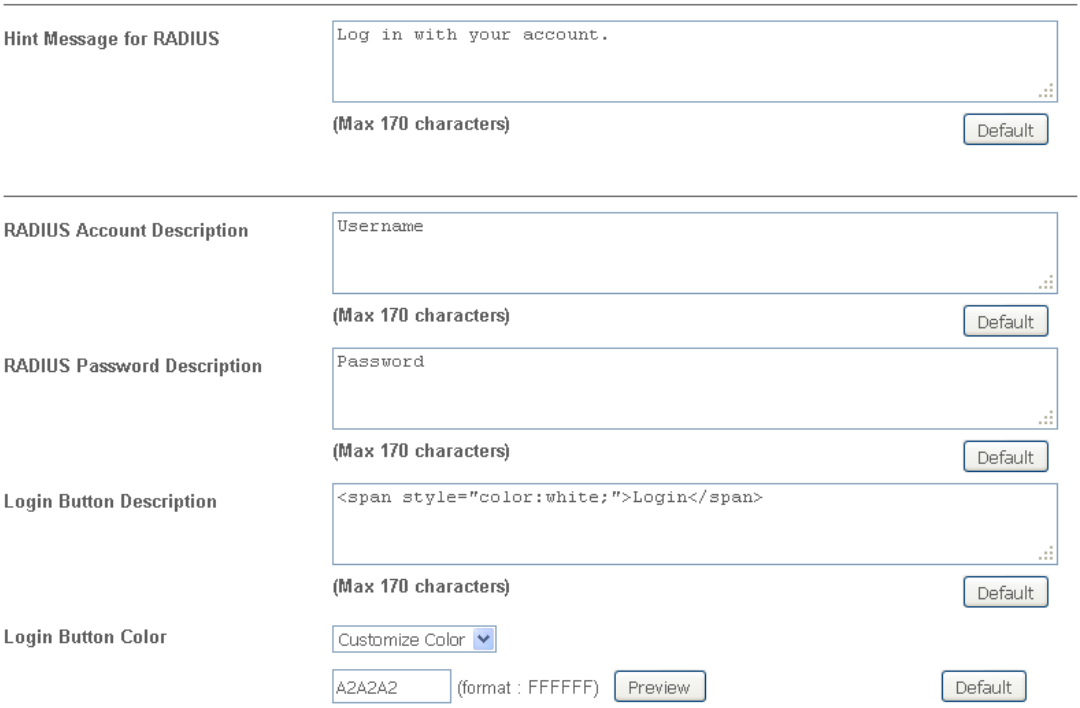

| Item | Description |
|---|---|
| **Google Login Description** | Enter the text to be displayed on the Google login button. |

If you have selected PIN login, these settings will appear:



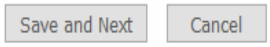

| Item | Description |
|---|---|
| **Hint Message for PIN** | Enter the text used to suggest users to choose SMS authentication. |
| **Receiving PIN via SMS Description** | Enter the text to be displayed on the button that the user clicks to receive an SMS PIN. |
| **Receiving PIN via SMS Content** | Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message. |
| **Enter PIN Description** | Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN. |
| **Submit Button Description** | Enter the text to be displayed on the submit PIN button |
| **Submit Button Color** | Select the color of the submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |

If you have selected RADIUS account login, these settings will appear:




| Item | Description |
|---|---|
| **Hint Message for RADIUS** | Enter the text used to prompt the user to login. |
| **RADIUS Account Description** | Enter the text to prompt the user to enter the username. |
| **RADIUS Password Description** | Enter the text to prompt the user to enter the password. |
| **Login Button Description** | Enter the text to be displayed on the login button. |
| **Login Button Color** | Select the color of the login button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |

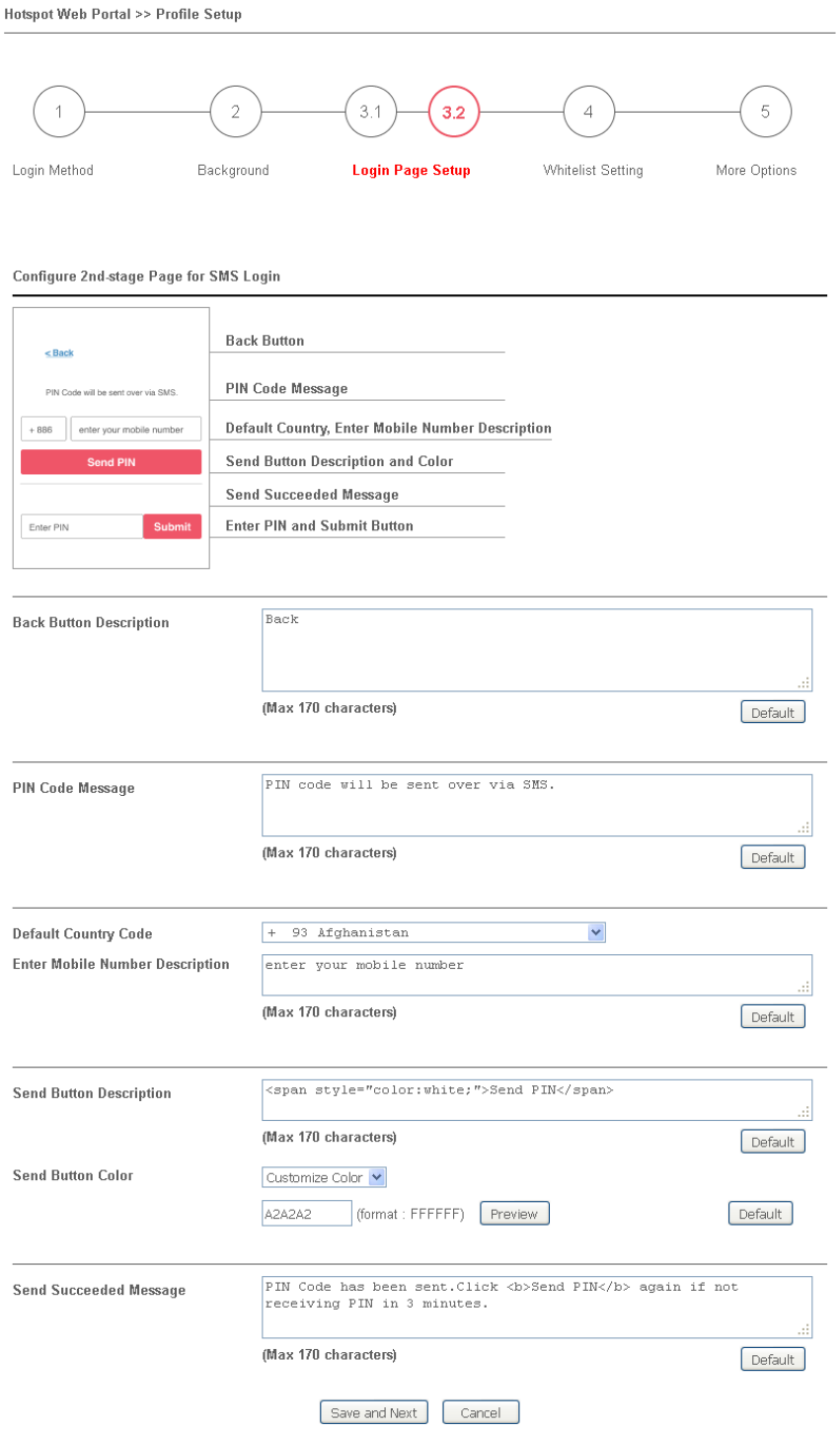
And finally, the save and cancel buttons are always displayed.




| Item | Description |
|---|---|
| **Save and Next** | Click to save the configuration on this page and proceed to the next page. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

## 2nd-stage Page for PIN Login

If you have selected **PIN Login** as the login method, you will also need to configure the page that is displayed to users when they request a PIN.



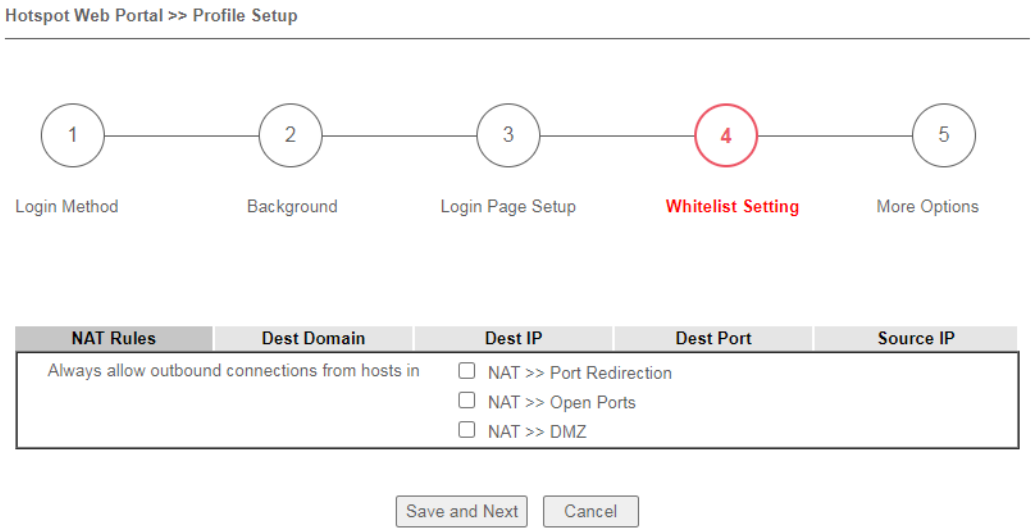

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Back Button Description** | Enter text for the label of the hyperlink to return to the previous page. |
| **PIN Code Message** | Enter text to be displayed as the body text on the page. |
| **Default Country** | Select the default country code to be displayed using the dropdown |

| | |
|---|---|
| **Code** | menu. |
| **Enter Mobile Number Description** | Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number. |
| **Send Button Description** | Enter the label text of the send button. |
| **Send Button Color** | Select the color of the send button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Send Succeeded Message** | Enter text to be displayed to notify the user after the PIN has been sent. |
| **Save and Next** | Click to save the configuration on this page and proceed to the next page. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

## 4 Whitelist Setting

In this step you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.

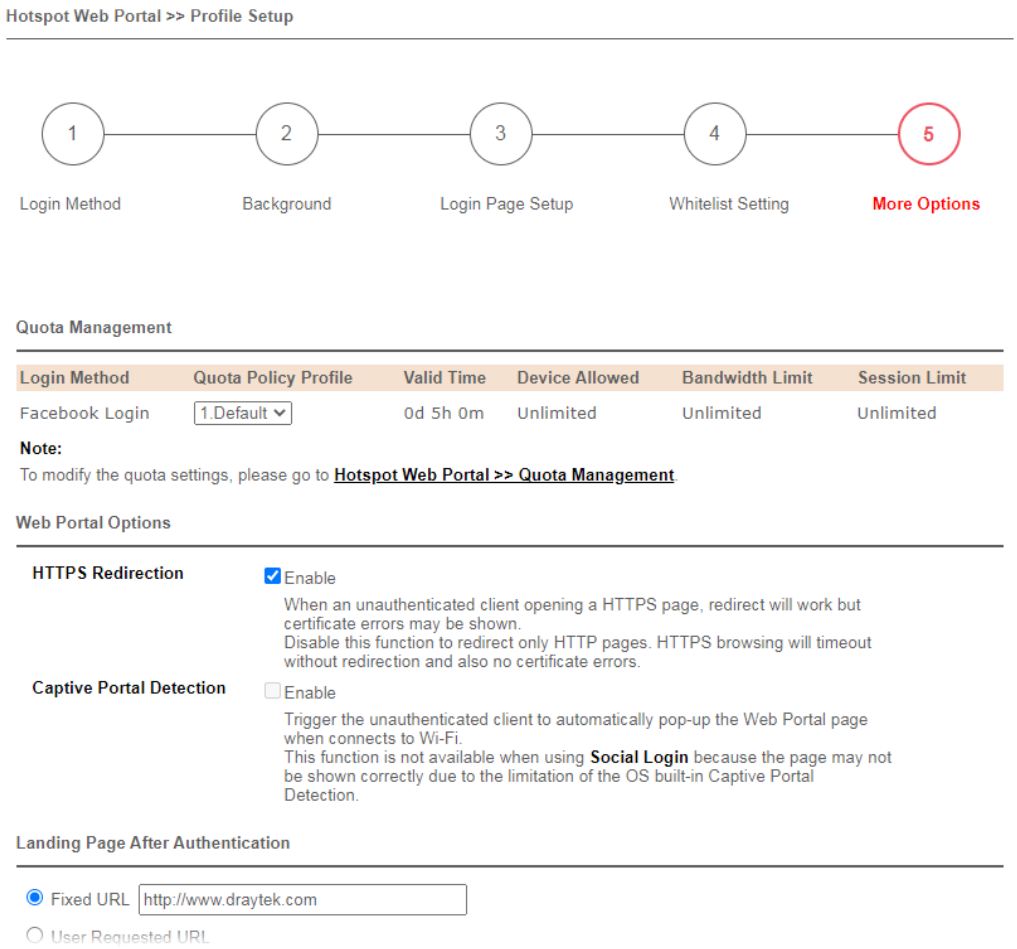



Available settings are explained as follows:

| Item | Description |
|---|---|
| **NAT Rules** | To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal. |
| **Dest Domain** | Enter up to 30 destination domains that are allowed to be accessed. |
| **Dest IP** | Enter up to 30 destination IP addresses that are allowed to be accessed. |
| **Dest Port** | Enter up to 30 destination protocols and ports that are allowed through the router. |
| **Source IP** | Enter up to 30 source IP addresses that are allowed through the router. |
| **Save and Next** | Click to save the configuration on this page and proceed to the next page. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

## 5 More Options

In this step you can configure advanced options for the Hotspot Web Portal.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Quota Management** | |
| **Quota Policy Profile** | Choose a policy profile to apply to web portal clients. |
| **Web Portal Options** | |
| **HTTPS Redirection** | If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection. |
| **Captive Portal Detection** | If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is **Social Login**, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection. |
| **Landing Page After Authentication** | |
| **Fixed URL** | Specifies the webpage that will be displayed after the user has |

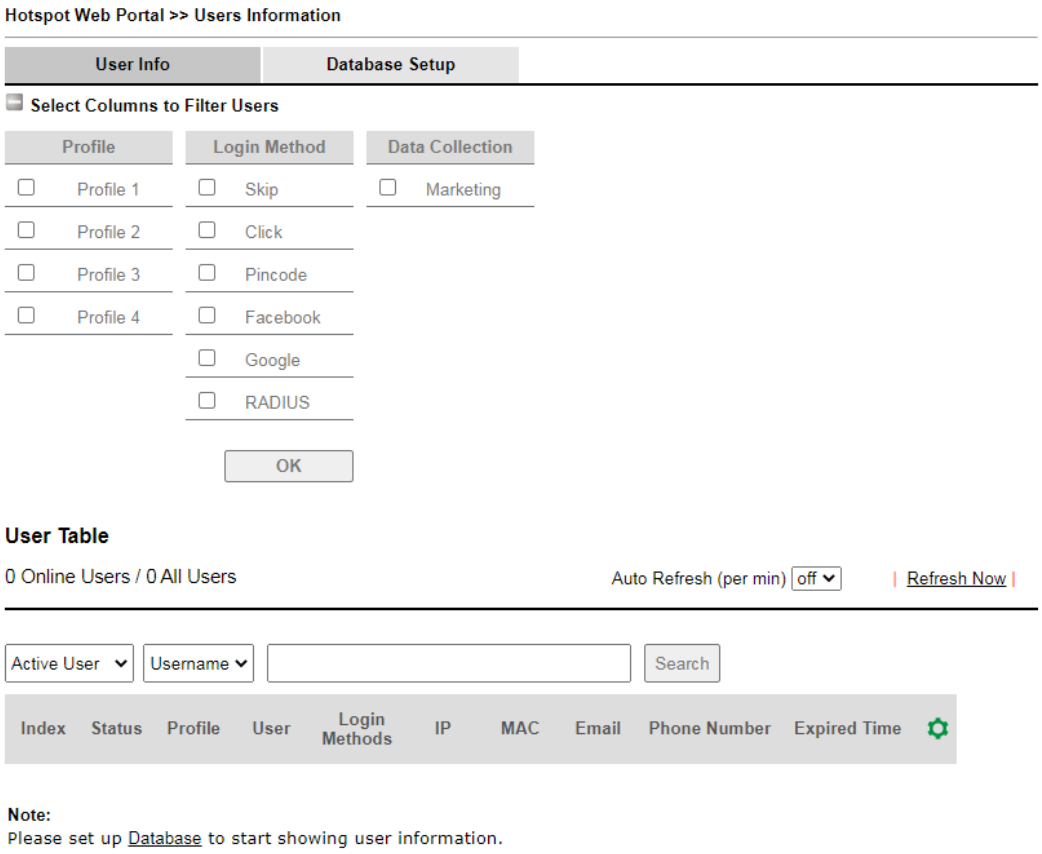
| | |
|---|---|
| | successfully authenticated.<br>The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel. |
| **User Requested URL** | The user will be redirected to the URL they initially requested. |
| **Bulletin Message** | The message configured here will be briefly shown for a few seconds to the user.<br>**Default Message –** This button is enabled when **Bulletin Message** is selected. Click to load the default text into the bulletin message textbox. |
| **Applied Interfaces** | |
| **Subnet** | The current Hotspot Web Portal profile will be in effect for the selected subnets. |
| **WLAN** | The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs. |
| **Finish** | Click to complete the configuration. |
| **Cancel** | Click to abort the configuration process and return to the profile summary page. |

## VI-4-2 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-4-2-1 User Info

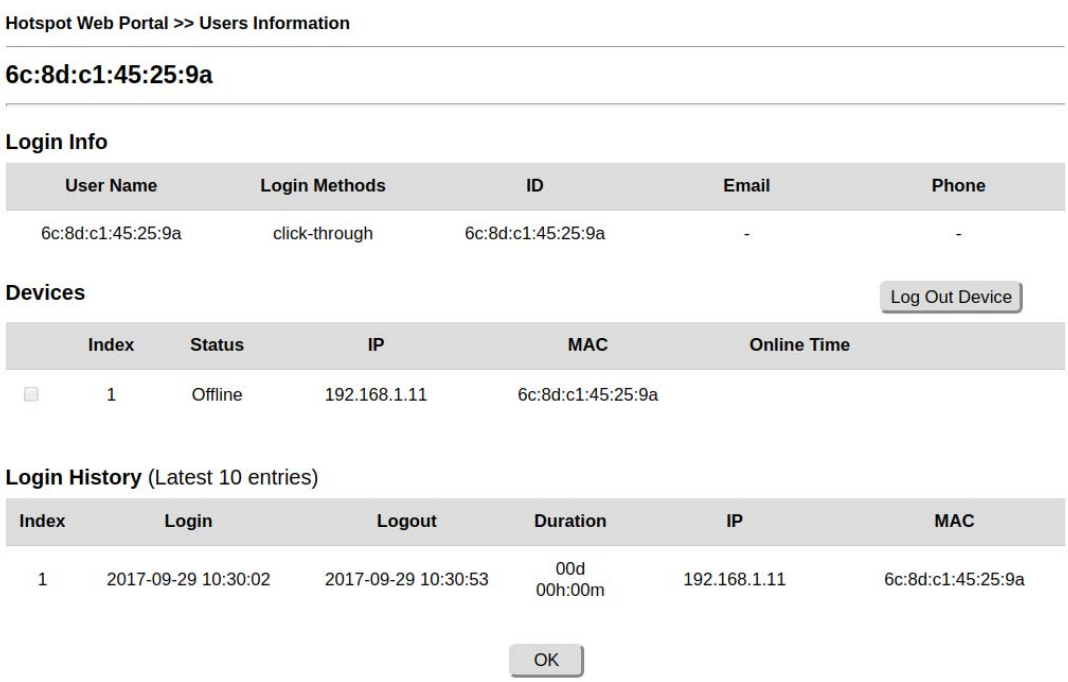
You may choose to limit the displayed user information by adding profile or login method filters.




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.



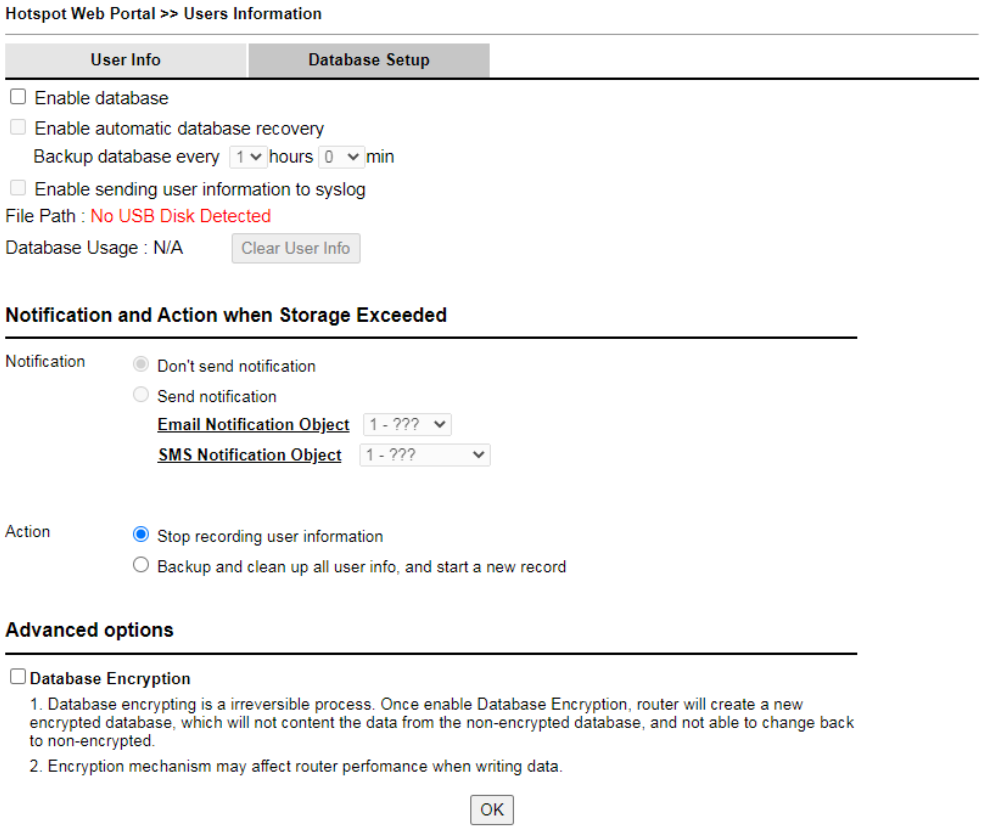

Information about the user is shown under the Login Info section.

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-4-2-2 Database Setup

This page allows the user to configure settings for database on USB disk.



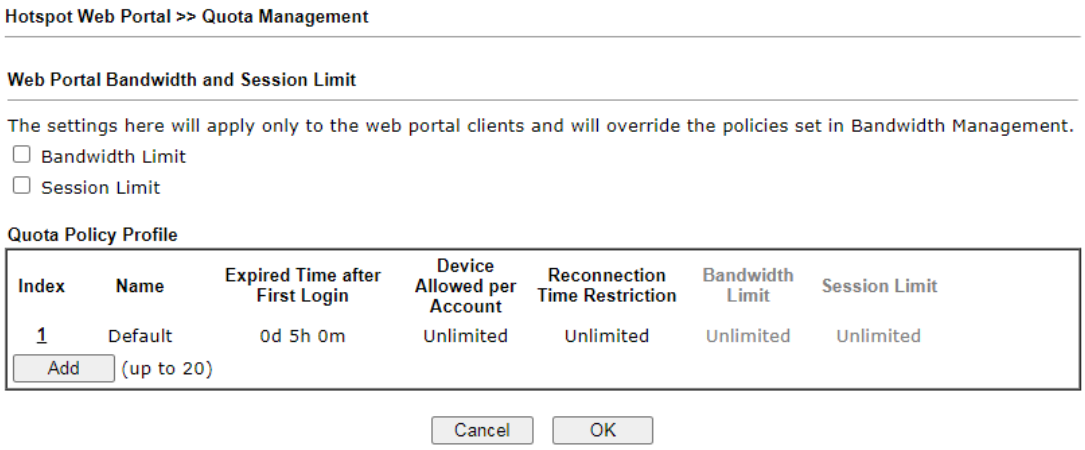
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable database** | Check the box to record user information on router's database.<br>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.<br>**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.<br>**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.<br>**Send notification** - Vigor router system will send a notification e-mail to specified receipient(s) that selected from **Email Notification Object** and **SMS Notification Object**. |
| **Action** | **Stop recording user information –** Vigor router system will stop to record the user information onto USB disk.<br>**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-4-3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

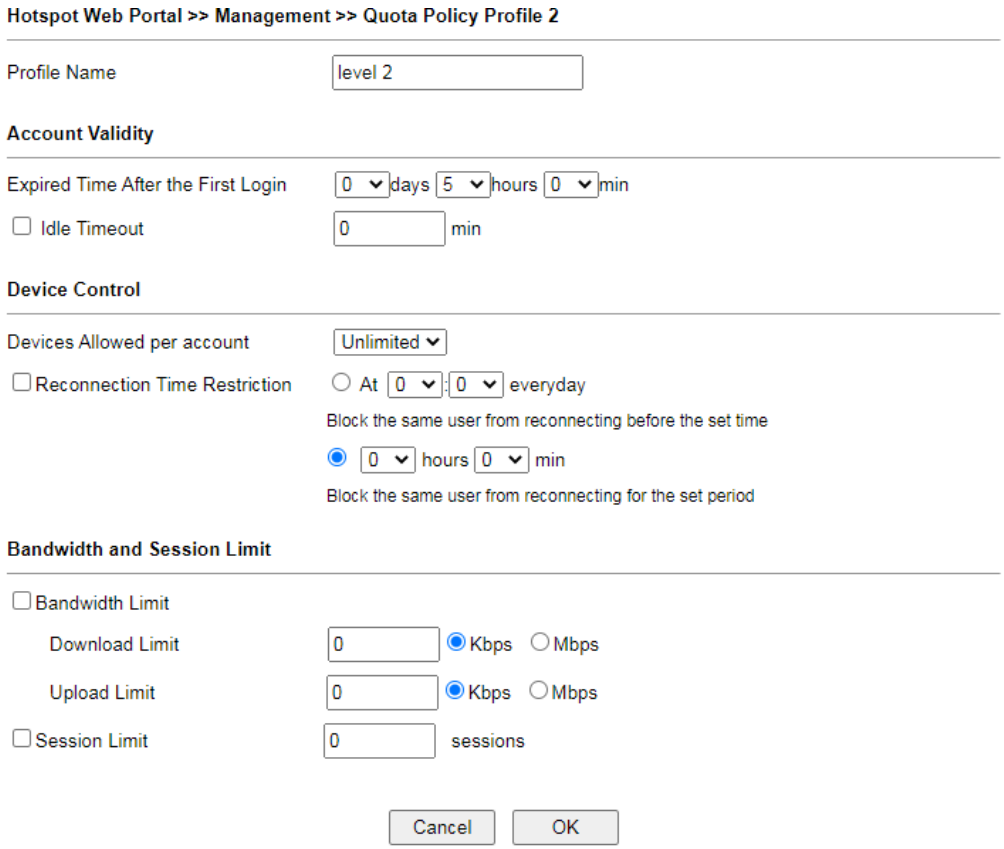
Settings configured in Quota Management will override the policies set in **Bandwidth Management>>Bandwidth Limit** and **Bandwidth Management>>Limit**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Bandwidth Limit** | Check the box to override the policy configured in **Bandwidth Management>>Bandwidth Limit.** |
| **Session Limit** | Check the box to override the policy configured in **Bandwidth Management>>Session Limit.** |
| **Quota Policy Profile** | **Add** - Create up to 20 policy profiles in such page. |

To create a new quotal policy profile, click **Add** to open the followining page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name for a new profile. |
| **Account Validity** | Set the duration for which the login is valid.<br>**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.<br>**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.<br>**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.<br>**Reconnection Time Restriction** – Blocks the account from being used to connect devices to the network in one of two ways:<br>● **At …. Everyday** – After the login expires, the account cannot be used to connect devices to the network until the set time of day.<br>● **Hours.. min** – After the login expires, the account cannot be used to connect devices to the network for a set period of time. |
| **Bandwidth and Session Limit** | **Bandwidth Limit** – Check the box to configure bandwidth limit for web portal client. |

| | |
|---|---|
| | • **Download/Upload Limits** – Set the maximum upload and download speeds.<br>**Session Limit**- Check the box to configure a maximum session limit for web portal clients. |

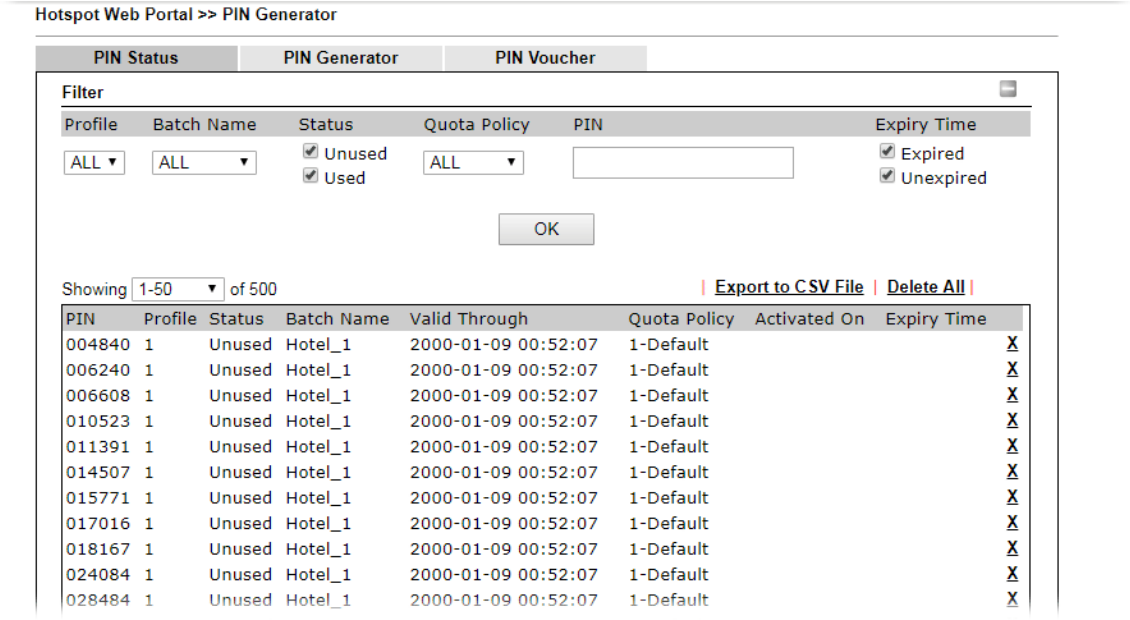
After finishing all the settings here, please click **OK** to save the configuration.

## VI-4-4 PIN Generator

The system administrator can generate multiple PIN codes for various usage. Before generating PIN codes, please make sure a **USB** has been inserted onto your Vigor device.

### VI-4-4-1 PIN Status

This page displays the PIN codes generated by PIN Generator.

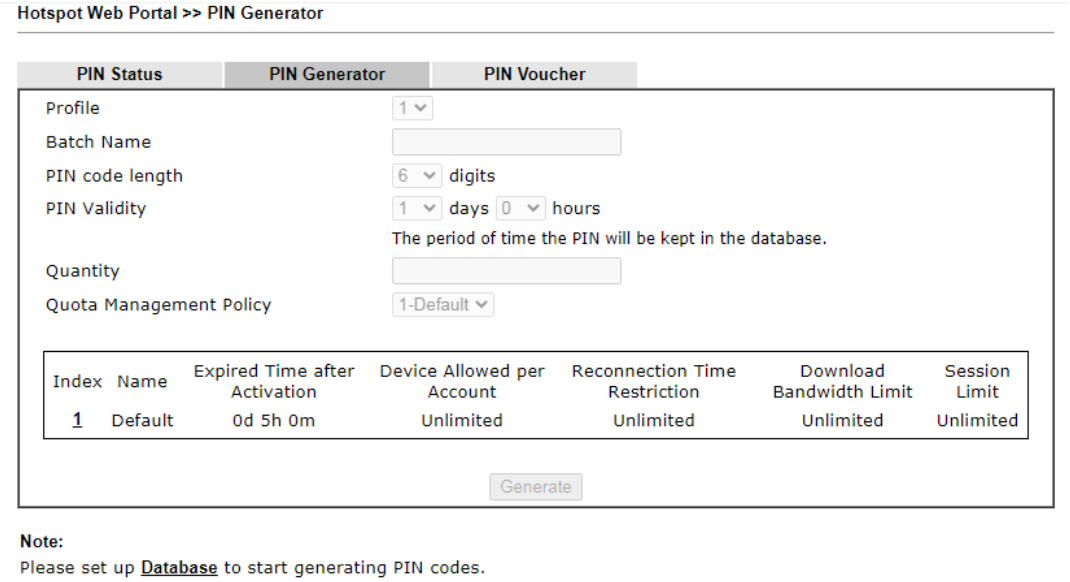



Available settings are explained as follows:

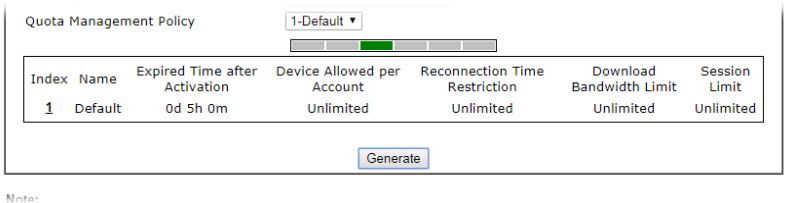
| Item | Description |
|---|---|
| **Profile** | Use the drop down menu to choose an index number (1 to 4) for PIN generator profile. |
| **Batch Name** | Use the drop down menu to choose an existed PIN profile or choose ALL to display the PIN status. |
| **Status** | **Unused** - After checking the box, only the unused PIN codes will be shown on this page.<br>**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.<br>**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. |

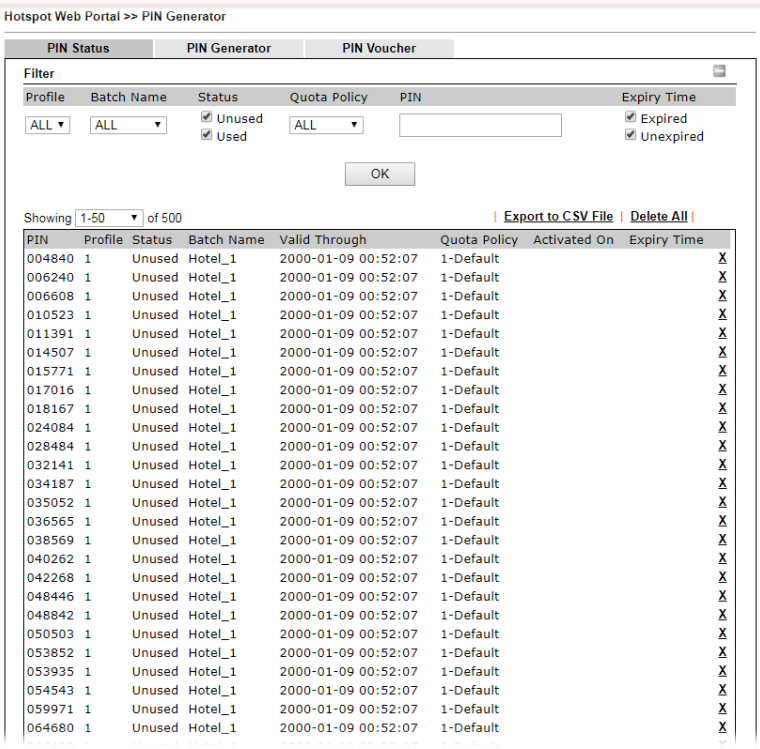
## VI-4-4-2 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.



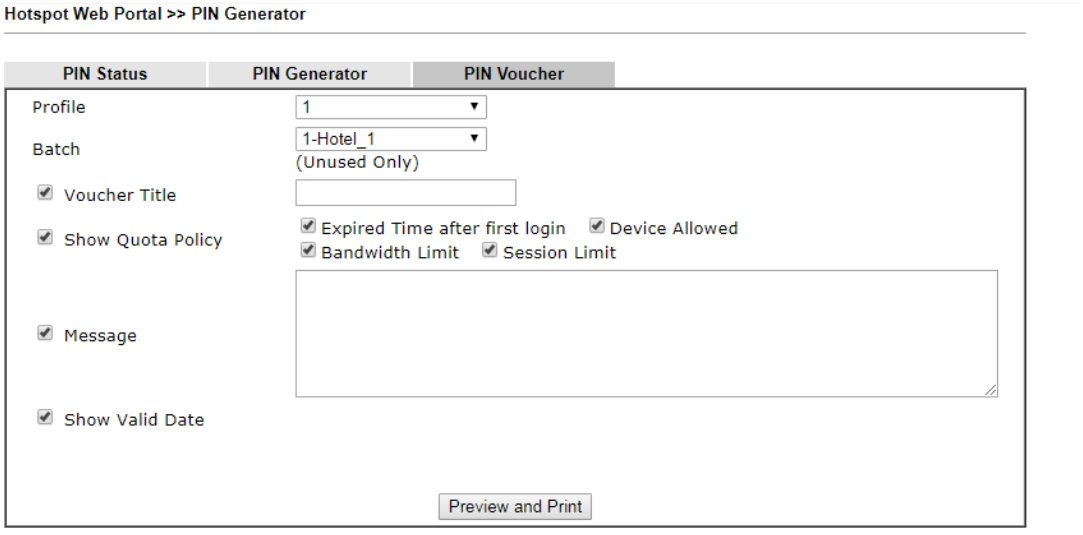

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile** | Use the drop down menu to specify an index number (from 1 to 4). |
| **Batch Name** | Enter a string as a batch name. |
| **PIN code length** | Specify the length of PIN code. |
| **PIN Validity** | Set the period of time. |
| **Quantity** | Set the quantity of the PIN code. |
| **Quota Management Policy** | Use the drop down list to choose policy profile. |
| **Generate** | Click it to generate a PIN code as a voucher.<br>The system will ask you to set up **Database** before executing the generation.<br>  <br>Later, available PIN code will be shown on PIN Status. |



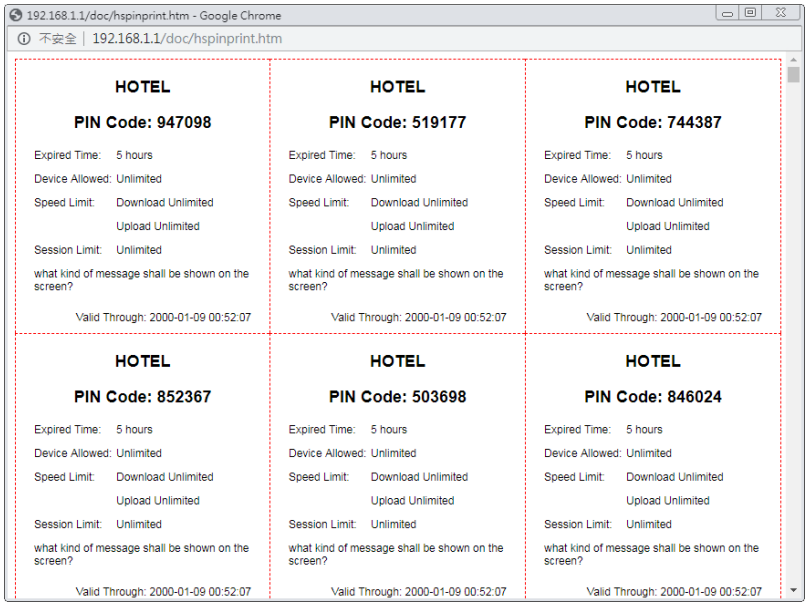

## VI-4-4-3 PIN Voucher

This page allows to print out the PIN code list.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile** | Use the drop down menu to specify an index number (from 1 to 4). |
| **Batch** | Use the drop down menu to specify an unused batch profile. |
| **Voucher Title** | Enter a string as a title which will be shown on a print out paper. |
| **Show Quota Policy** | Choose the item(s) to be shown on the print-out PIN code list. |
| **Message** | Enter a brief description that the client should know. |

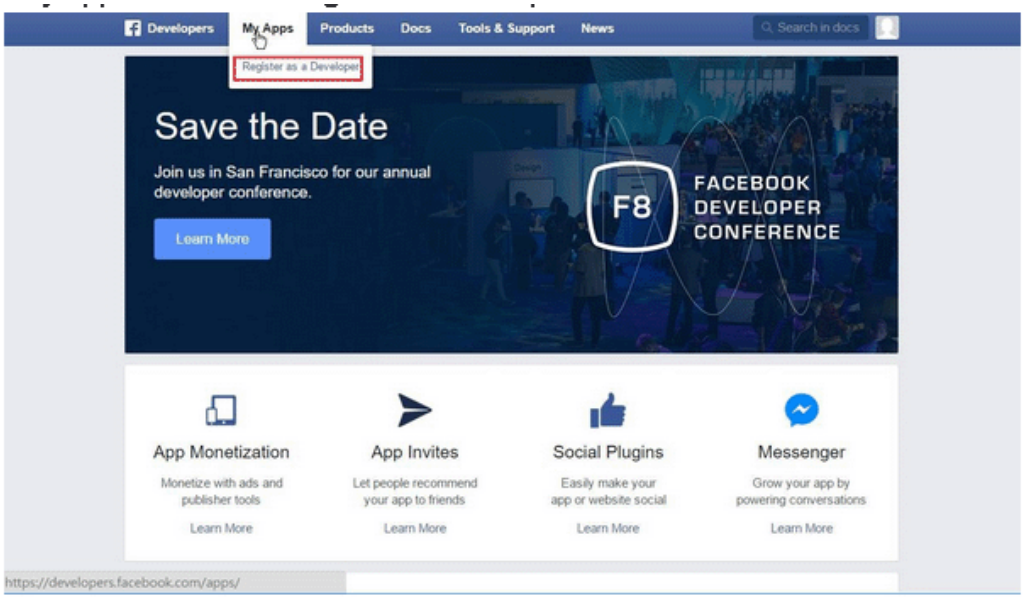
| | |
|---|---|
| **Show Valid Date** | Check the box to display the valid date and time on the printed out list. |
| **Preview and Print** | Click it to display the PIN code list. This list can be printed out if required.<br>  <br> |

# Application Notes

## A-1 How to create Facebook APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

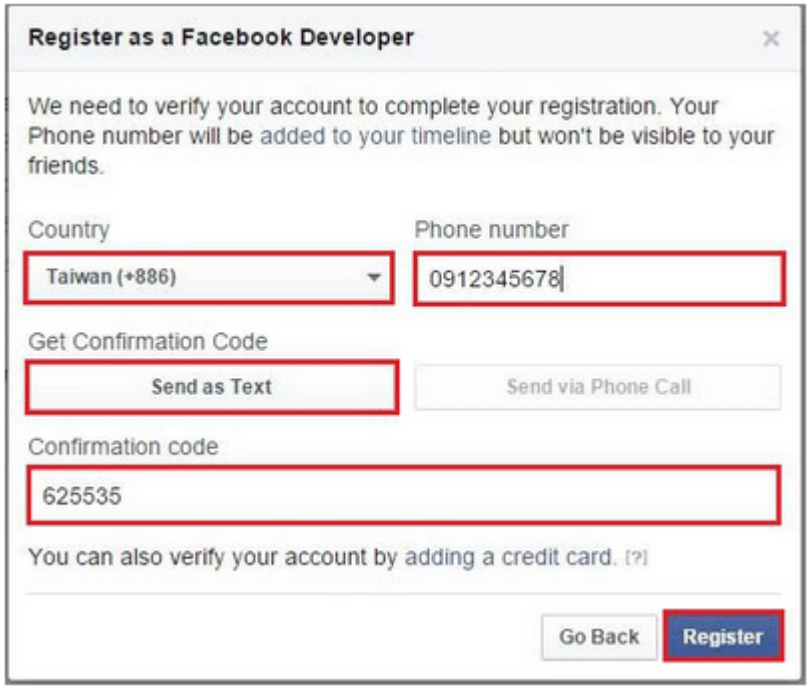
1. Register as FB Developer: Go to https://developers.facebook.com/ and login the FB account.
2. Register the Facebook account as a Developer (If the account has been verified previously, this step can be skipped.)
3. Click **My Apps** then choose **Register as Developer.**



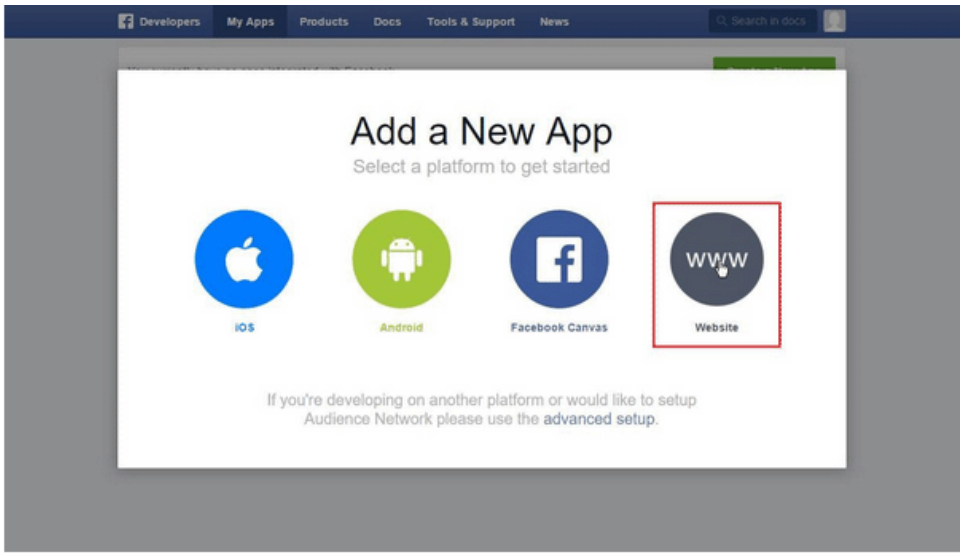

4. Switch to **YES** then click **Next** on pop-up window.



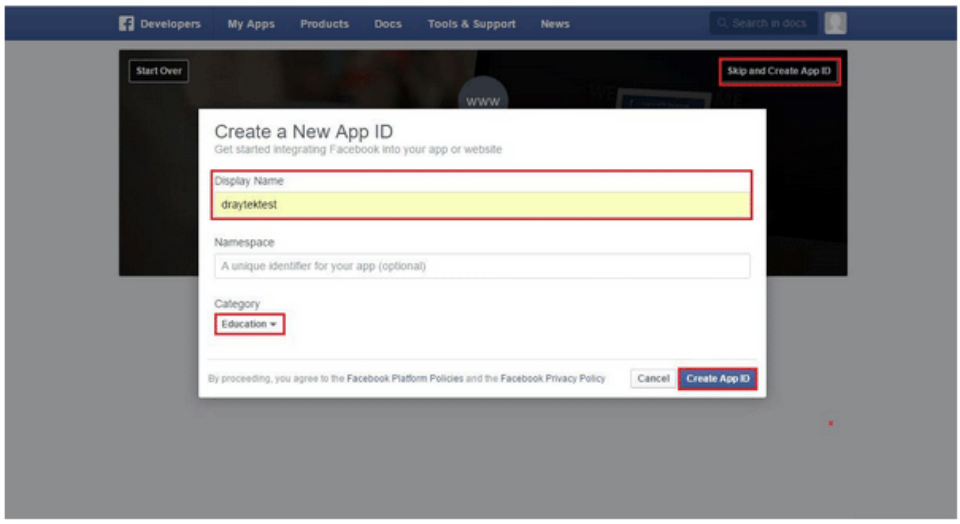

5. Choose **country** then type **phone number**, click **Send as Text** in Get Confirmation Code. Wait confirmation code message received then enter the **confirmation code.** Click **Register** to finish the register process.



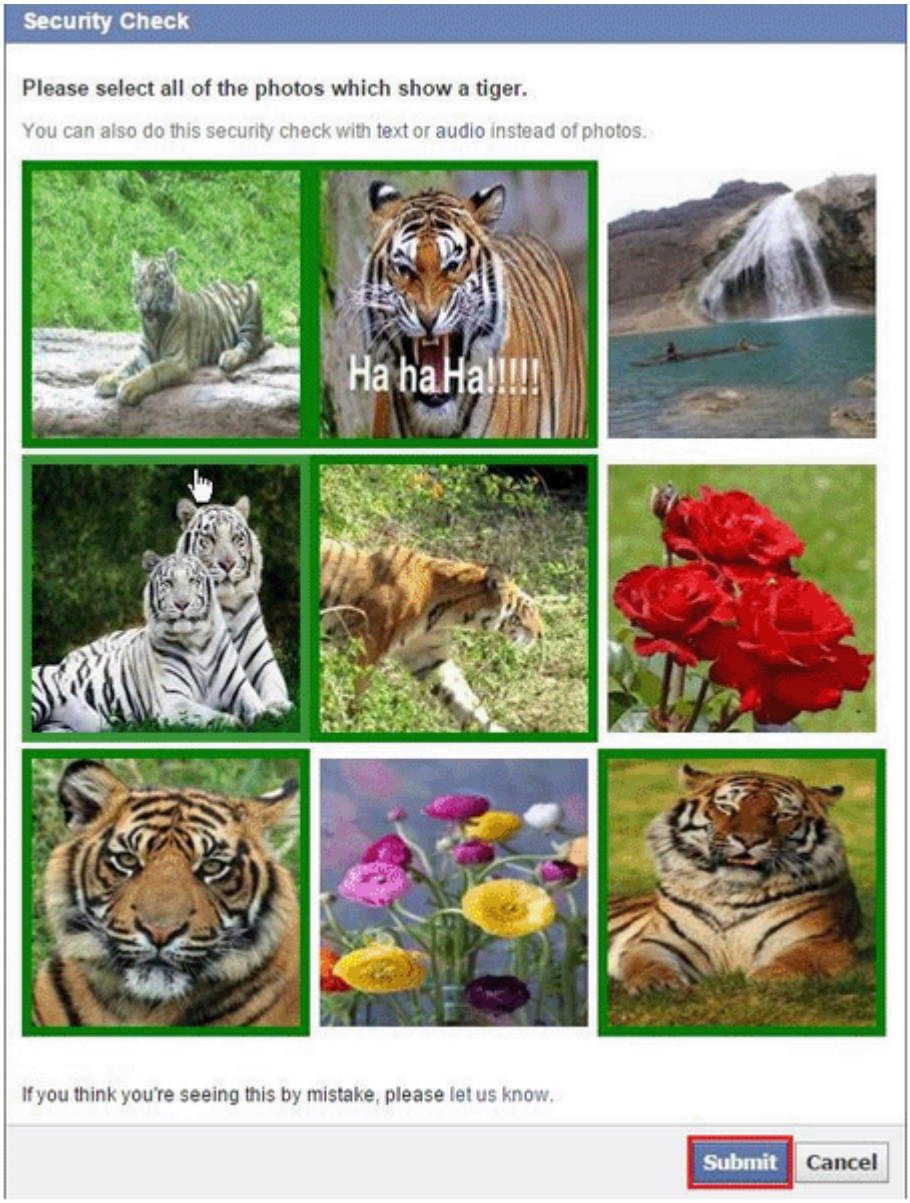

6. Add a New App. Click on **My Apps > Add a New App.** Choose **Website** platform.



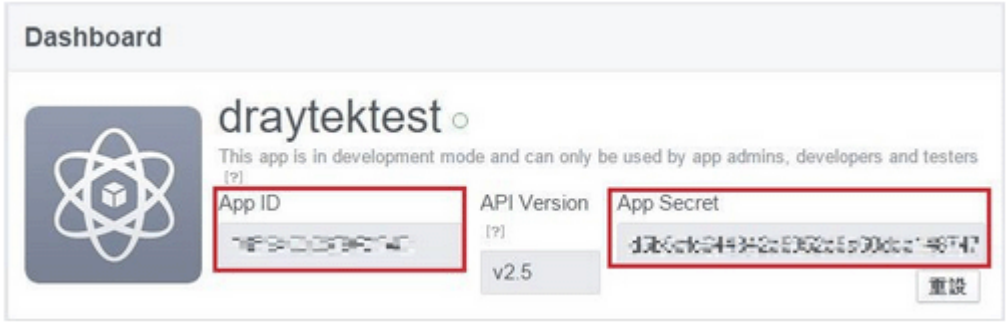

7. Click **Skip and Create App ID** on first use. Type **Display Name.** Choose **Category.** Click **Create App ID.**



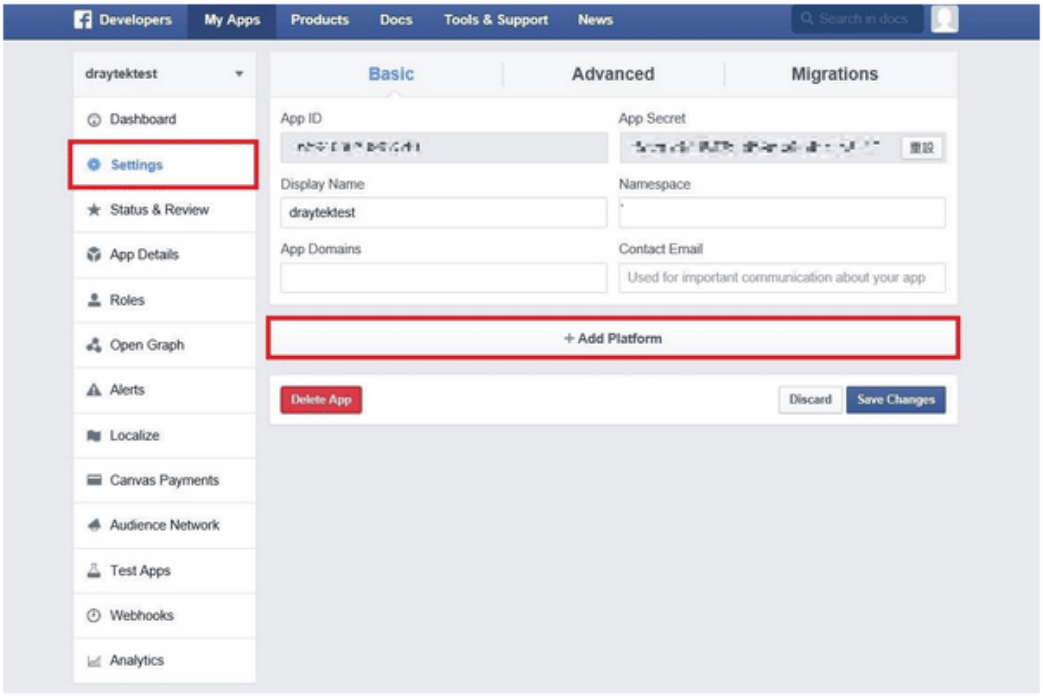

8. Pops up security check window, select the answer, and then click **Submit** to finish the process.



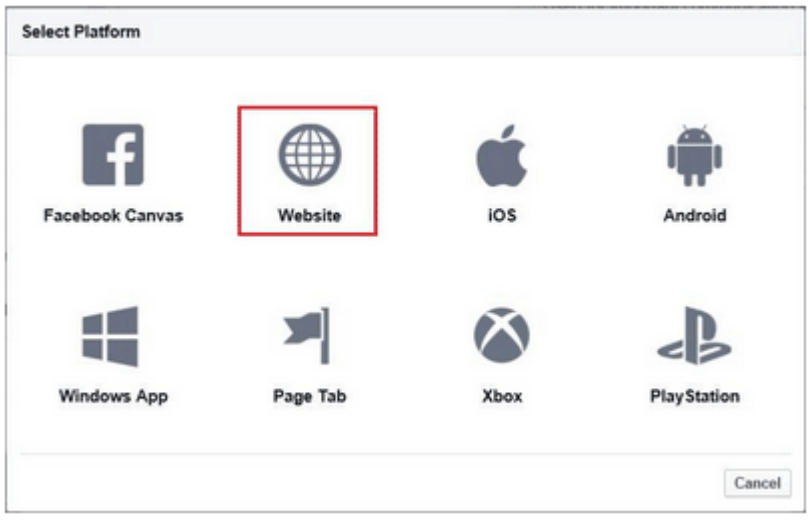
9. On Dashboard, user can get **App ID** and **App Secret**, these information will be used in Vigor Router's Web Portal Setup.



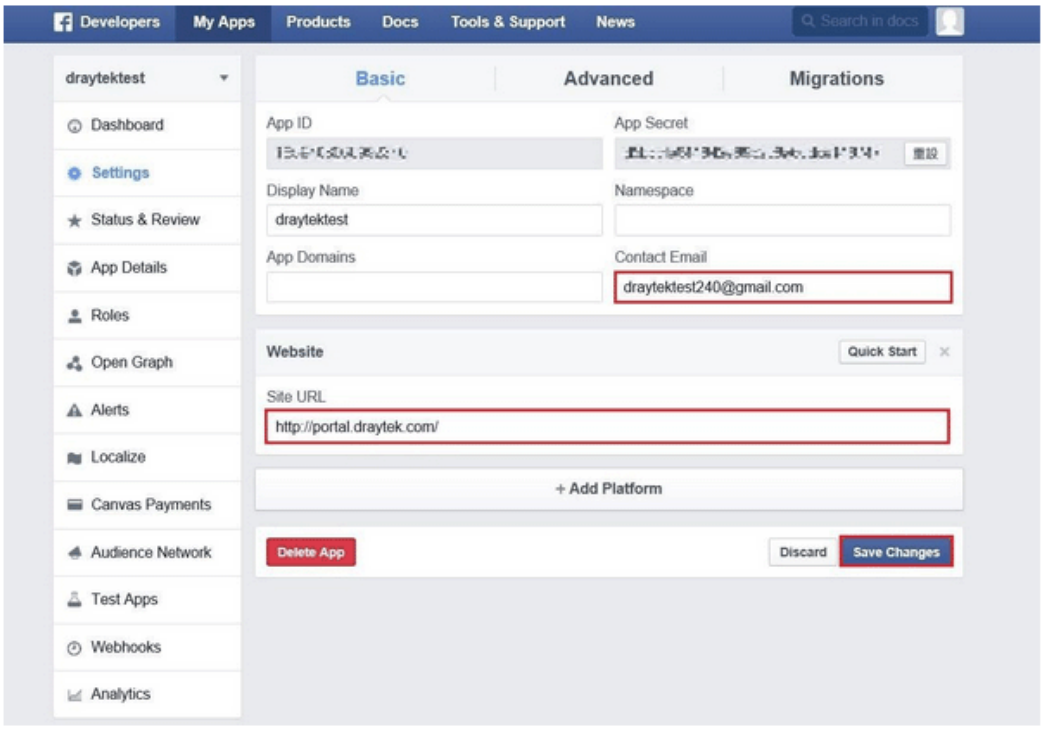

10. Add Platform on My Apps. Go to **Settings** then click **Add Platform.**



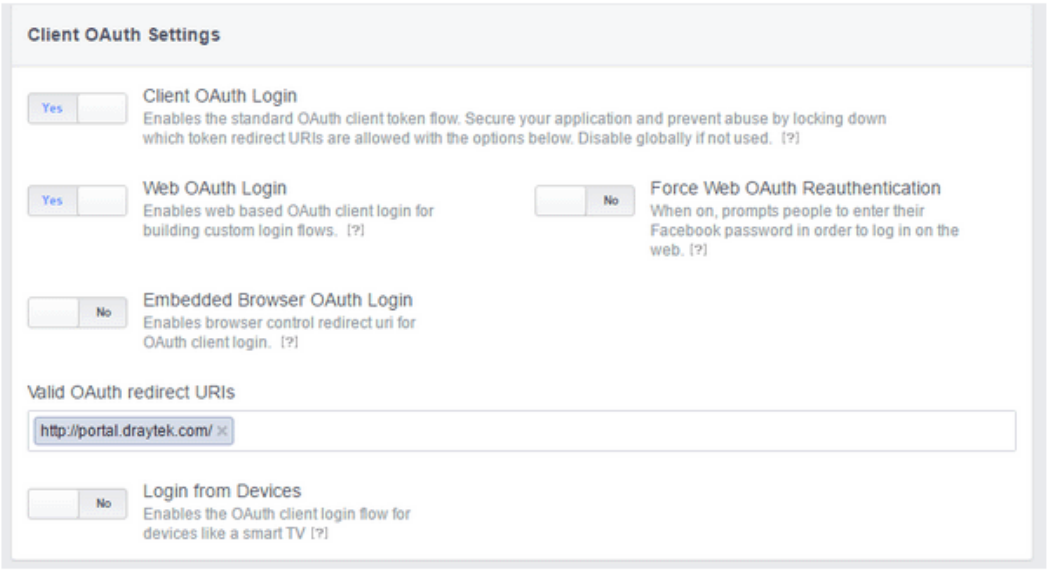

11. Choose **Website** in Select Platform window.



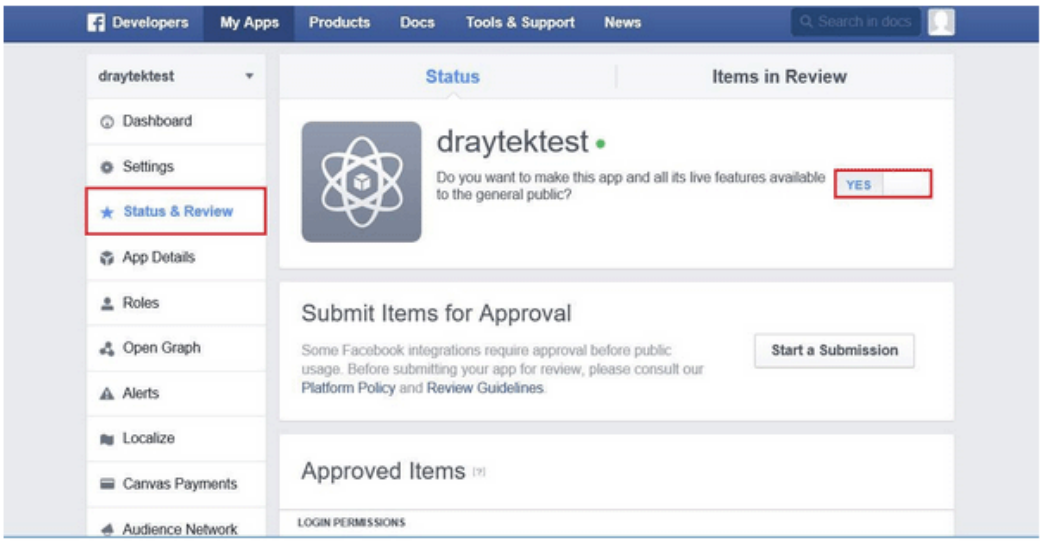

12. Enter the **Site URL** as http://portal.draytek.com. (*Note*: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put http://portal.draytek.com:8080). Enter the **Contact Email.** And **c**lick **Save Change.**




13. Set up Client OAuth. Go to **Settings** >> **Advanced** >>**Client OAuth Settings**, enter "http://portal.draytek.com" in **Valid OAuth redirect URIs**, and save changes.



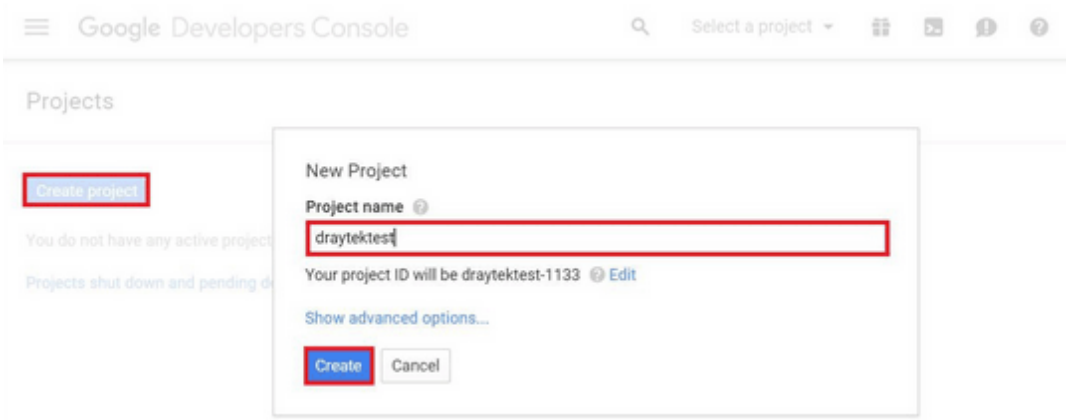

14. Go to **My Apps>>Status & Review**, and switch available status to **YES** to activate the APP.


Developers
My Apps
Products
Docs
Tools & Support
News
Search in docs
draytektest
Dashboard
Settings
Status & Review
App Details
Roles
Open Graph
Alerts
Localize
Canvas Payments
Audience Network
Status
Items in Review
draytektest
Do you want to make this app and all its live features available to the general public?
YES
Submit Items for Approval
Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.
Start a Submission
Approved Items
LOGIN PERMISSIONS

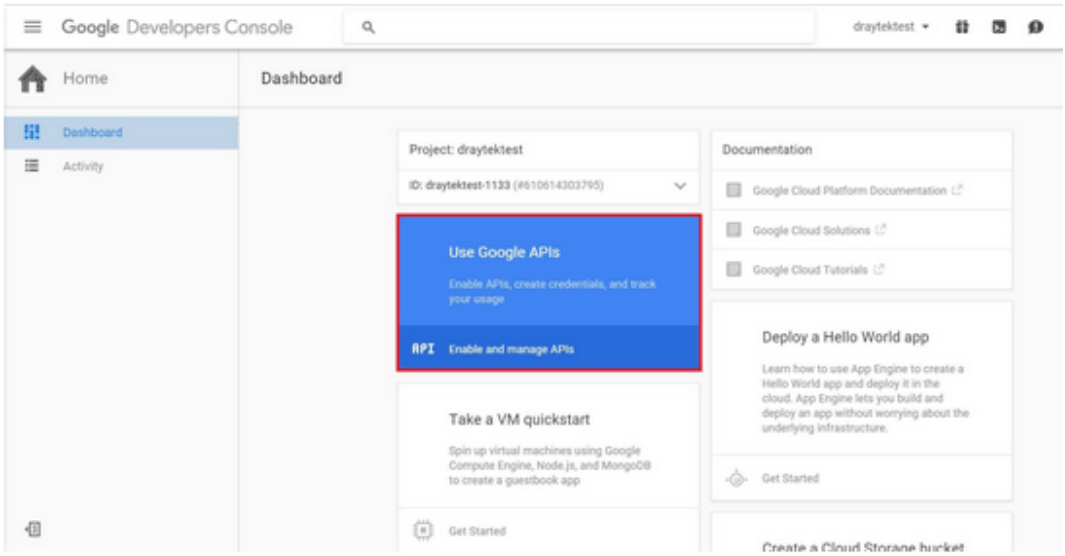
## A-2 How to create Google APP for Web Portal Authentication?

The new web portal feature support social login as authentication method, and allows network administrator to authenticate LAN clients by their Google or Facebook account. This document introduces how to create Facebook APP, and generate the APP ID and APP secret that can be used in Web Portal setup.

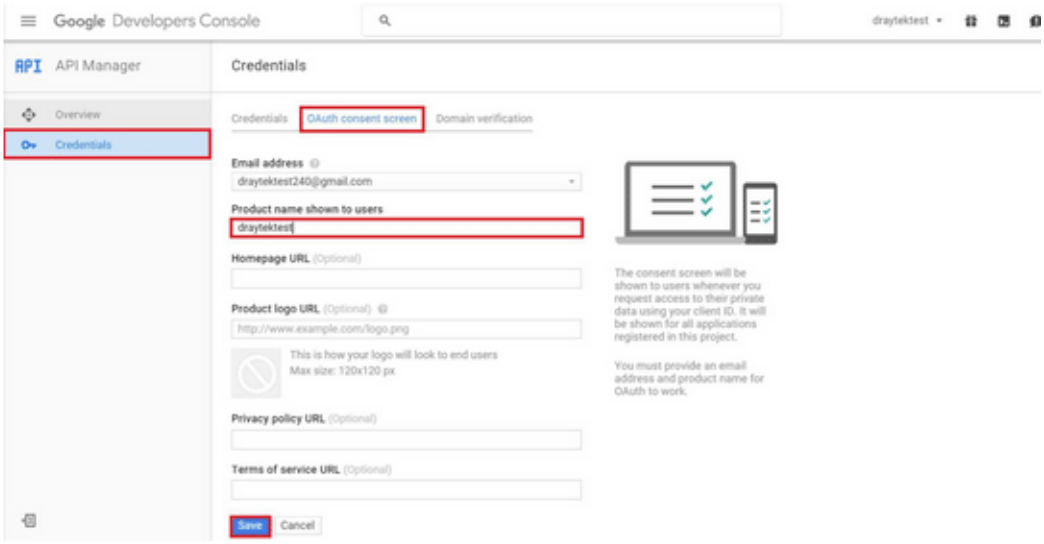
1. Create Developer project. Go to https://code.google.com/apis/console, login with a Google account then click **Create project.** Type **project name** then click **Create.**



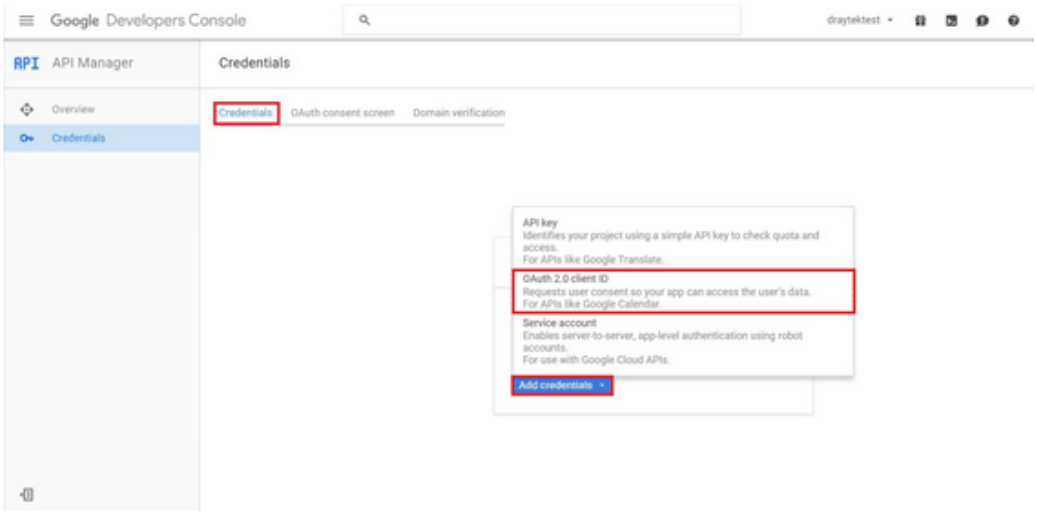

2. On Dashboard, choose **Use Google APIs**.




3. Edit Auth Consent screen. Go to **Credentials > Auth consent screen.** Enter your **email**, **product name** and other optional item then click on **Save.**




4. Create Client ID. Click **Credentials** and Click **Add credentials > OAuth2.0 client ID.**

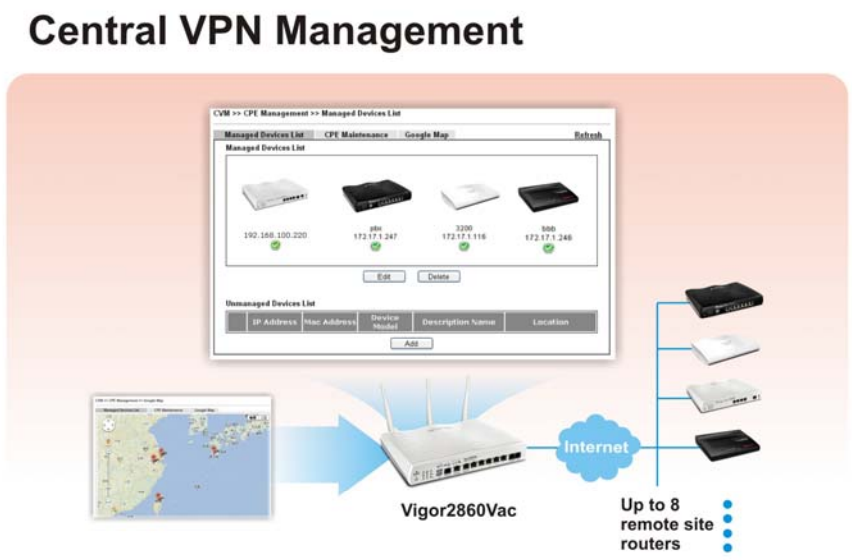



5. Choose **Web application** as Application Type, then enter **name**. Set **Authorized JavaScript origins** and **Authorized redirect URLs** as http://portal.draytek.com, and click **Create.** (*Note*: If you change http port in the vigor, please add http port in URLs. For example, we use 8080 as http port and we'll put http://portal.draytek.com:8080).
6. Get **client ID** and **client secret**. Such information will be used in Vigor Router's Web Portal Setup page.



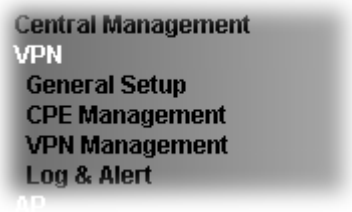
# VI-5 Central Management (VPN)

Vigor2927 can build virtual private network (VPN) between itself and any other TR-069 CPE by the function of central VPN management. In addition, it can be treated as a server (called CVM server) which can manage TR-069 CPE for periodical firmware upgrade, configuration backup and restoring configuration.



# Web User Interface

Central VPN Management menu can manage the CPE connected through WAN only.

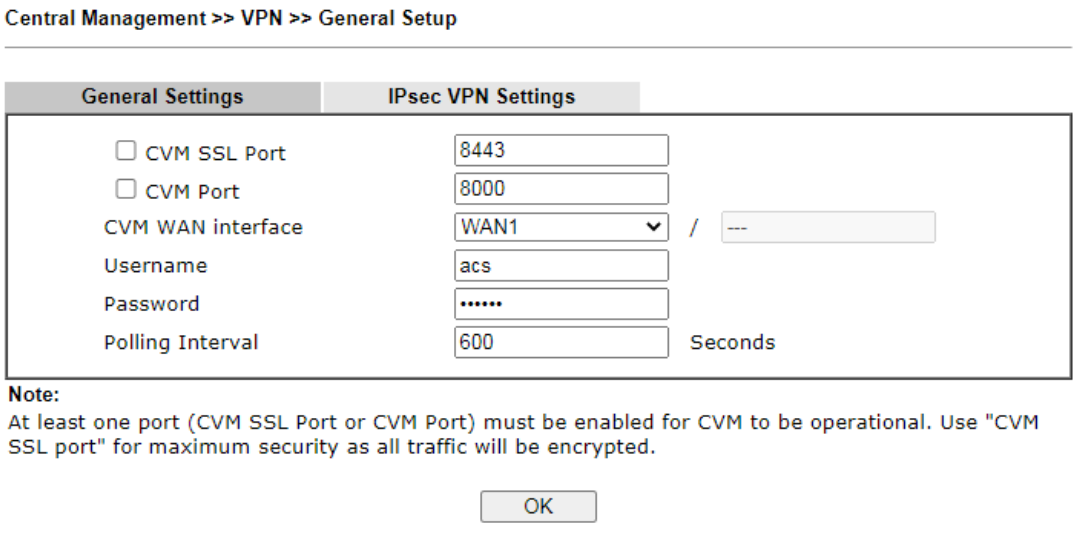



## VI-5-1 General Setup

This page is used to configure settings which will be used by the clients to register to such Vigor router. Click **General Settings** and **IPsec VPN Settings** to configure the basic settings for CVM mechanism.

### VI-5-1-1 General Settings

To enable the CVM feature, the first thing you have to do is enabling CVM port or CVM SSL Port.




Available settings are explained as follows:

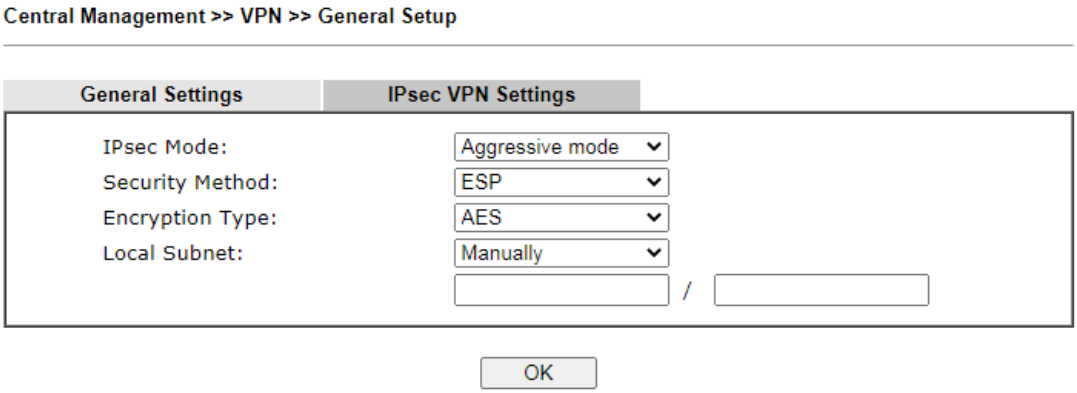
| Item | Description |
|---|---|
| **CVM SSL Port** | Check the box to enable the port setting.<br>Enter the port number in the box. |
| **CVM Port** | Check the box to enable the port setting.<br>Enter the port number in the box. |
| **CVM WAN interface** | For Vigor router can manage only the client from WAN interface, therefore you have to specify which interface will be used for such function. If you choose MANUALLY, you have to specify WAN IP address. |

| | |
|---|---|
| **Username** | Type a username which will be used by any CPE trying to connect to Vigor router. |
| **Password** | Enter the password for the user. |
| **Polling Interval** | Enter the time value (unit is second). The range is from 60 ~ 86400. |

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

## VI-5-1-2 IPsec VPN Settings

Central VPN management is operated through IPsec VPN connection.




Available settings are explained as follows:

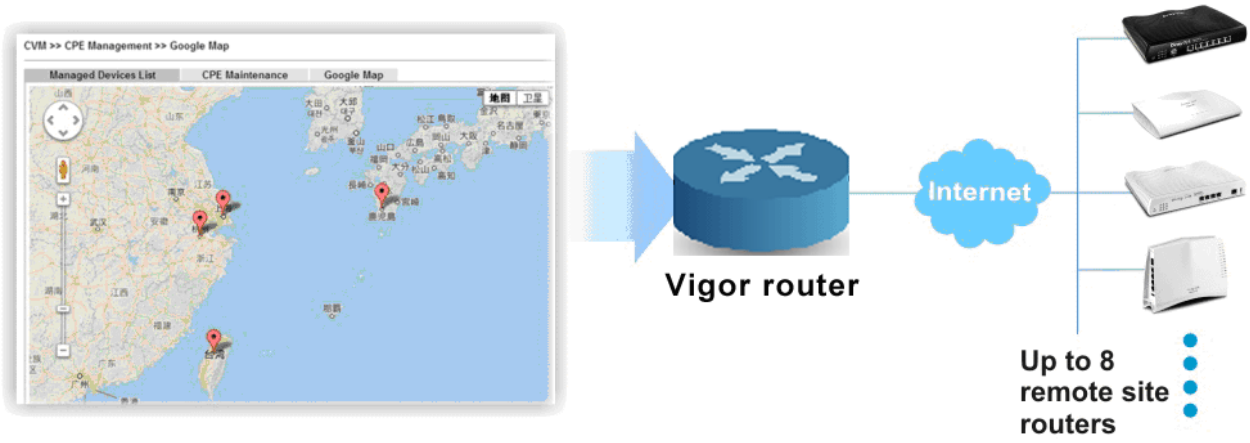
| Item | Description |
|---|---|
| **IPsec Mode** | Choose **Aggressive** or **Main** as the IPsec Mode. |
| **Security Method** | Choose one of the following methods (AH or ESP) for the security of data transmission. For example, choose **AH** to specify the IPsec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted. |
| **Encryption Type** | Choose one of the selections as the encryption type. |
| **Local Subnet** | Enter the IP address and subnet mask of local host. |

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

## VI-5-2 CPE Management

All the CPEs managed by Vigor2927 series can be seen with icons from this page.

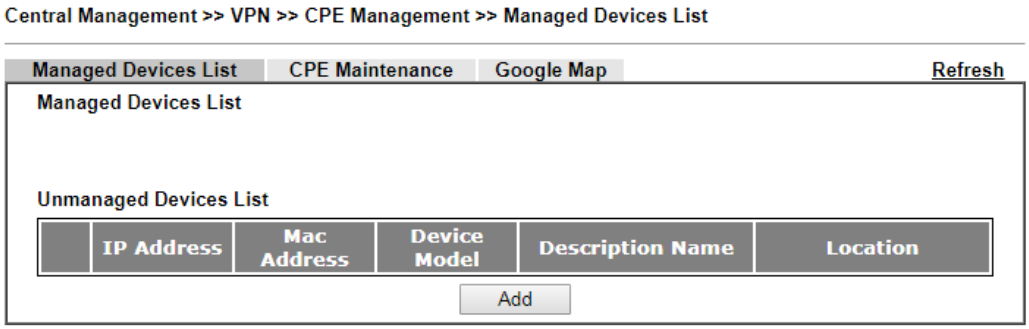
Before using such feature, make sure the CVM port has been enabled and configured properly.



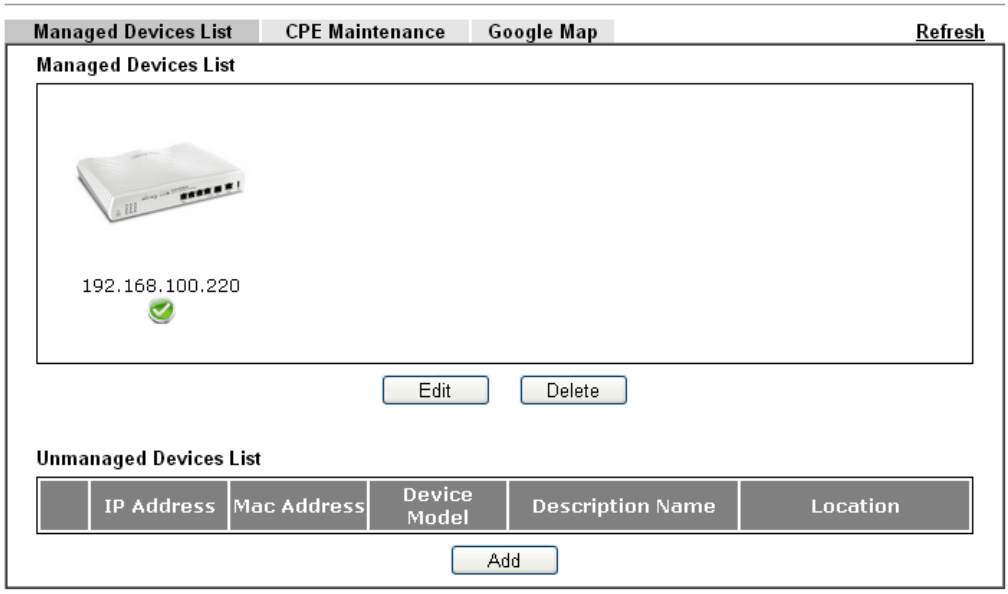

### VI-5-2-1 Managed Device List

This page allows you to manage the CPEs connected to Vigor2927 series.

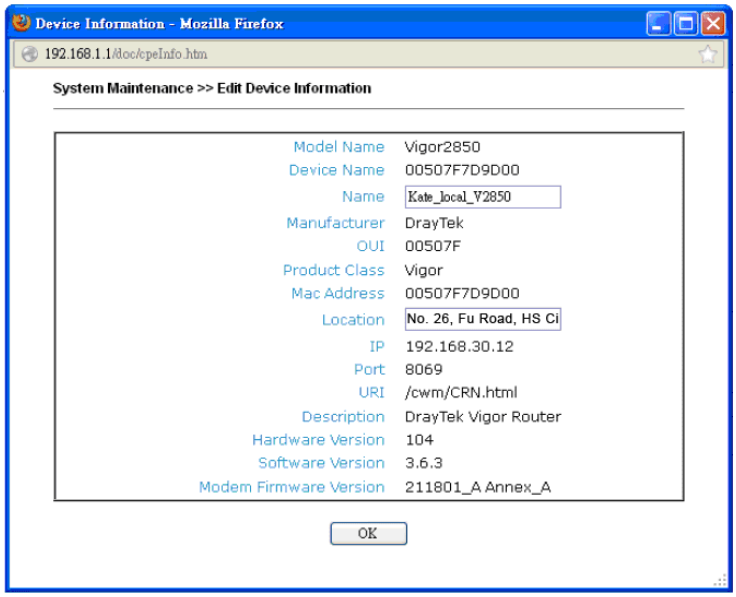
Page without CPE connected

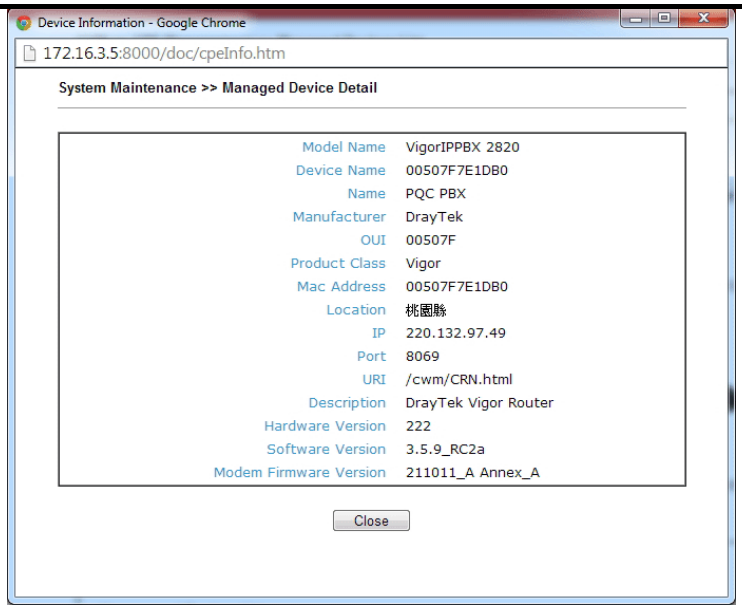


Page with CPE connected



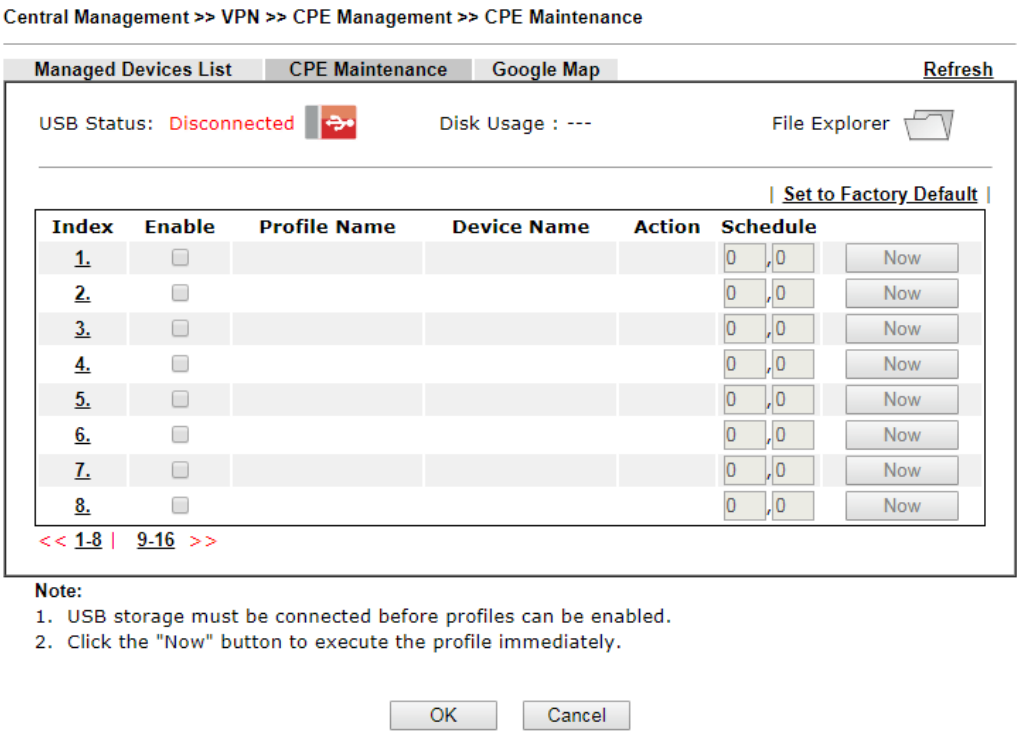

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Managed Devices List** | This area displays device icons (up to 8) for the CPE managed by Vigor2927 series.<br>**Edit** – To modify the name and location of specific CPE, click the one you want and click the **Edit** button. A pop up window will appear. Simply change the name and/or location manually.<br>  <br>**Delete** – To disconnect the management of any CPE, click the CPE icon you want and click the Delete button.<br>Double-clicking the CPE icon also can pop up the Managed Device Detail window. However, you cannot modify any data on the window. |

| | |
|---|---|
| |  |
| **Unmanaged Devices List** | Any device (CPE) which follows the standard of TR-069 can be configured and can be detected by Vigor2927 series automatically.<br>Only eight remote devices can be managed by Vigor2927 at one time. Therefore, other remote devices detected by Vigor2927 series might not be displayed in such field.<br>**Add** – Move the selected device from Unmanaged Devices List to Managed Devices List.<br>**IP Address** – Display the IP address of the remote device.<br>**Mac Address** – Display the MAC address of the remote device.<br>**Device Model** – Display the model name of the remote device.<br>**Description Name** – Define the name or Enter the additional description of CPE for identification in VPN management and CPE management.<br>**Location** – Enter the location (address) of the CPE to be displayed by Google Map. |
| **Refresh** | Click it to refresh current web page. |

## VI-5-2-2 CPE Maintenance

This area displays all the profiles which are created for applying to the managed device. This page can help the administrator to do maintenance jobs like firmware upgrade, configuration backup, configuration restoration and etc.




Available settings are explained as follows:

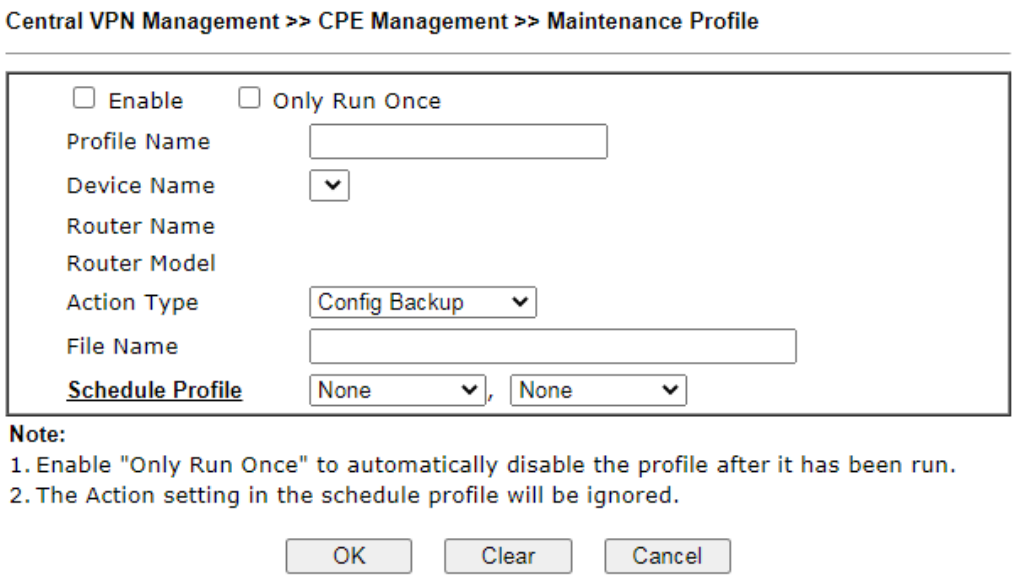
| Item | Description |
|---|---|
| **Refresh** | Click it to refresh current page. |
| **USB Disk** | USB Disk : - It means a USB disk connecting to Vigor2927.<br>USB Disk : - It means no USB disk connecting to Vigor2927. |
| **Disk Usage** | Disk Usage : 1084MB / 2009MB - When a USB disk connects to Vigor2927, the disk usage and the disk capacity will be displayed in such field.<br>Disk Usage : USB Storage Disconnected - When there is no USB disk connecting to Vigor2927, such message will be displayed in this field. |
| | Click the icon to see the content inside the USB disk. |
| **Set to Factory Default** | Click to clear all indexes. |
| **Index** | Display the number of the profile that you can edit. |
| **Enable** | Check to enable the profile. |
| **Profile Name** | Display the name of the maintenance profile. |

| | |
|---|---|
| **Device Name** | Display the name of the managed CPE that the maintenance profile will apply to. |
| **Action** | Display the action that managed CPE shall accept. |
| **Schedule** | Display the schedule profiles selected for such profile. |
| **Now** | The action will be performed for the selected CPE immediately. |

### How to add a new Maintenance Profile

Follow the steps below to create a new maintenance profile.

1. Click any index number link, e.g., Index 1.
2. The Maintenance dialog appears.




| | |
|---|---|
| **Info** | When restoring configuration to a CPE, make sure the configuration file you selected was backup from this CPE before. Because restoring from another device's configuration file may cause serious problem (e.g., Both devices have different ISP username/ password. Restoring configuration from one CPE to the other will cause Internet connection not being online). |

Available parameters are listed as follows:

| Item | Description |
|---|---|
| **Enable** | Check it to enable such profile. |
| **Only Run Once** | Check it to activate such profile running for once. |
| **Profile Name** | Enter the name of the maintenance profile. |
| **Device Name** | The drop down list will display all the CPE devices detected by Vigor2927 series. Choose the one which will be applied with such new created profile. |
| **Router Name/ Router Model** | It displays the name and model of Vigor router. |
| **Action Type** | There are three actions for you to choose for such profile. |

| | |
|---|---|
| | • **Config Backup** – It means such profile will be used for configuration backup of the selected CPE.<br>• **Config Restore** – It means such profile will be used for restoring the configuration of the selected CPE.<br>  <br>**Info** When restoring configuration to a CPE, make sure the configuration file you selected was backup from this CPE before. Because restoring from another device's configuration file may cause serious problem (e.g., Both devices have different ISP username/ password. Restoring configuration from one CPE to the other will cause Internet connection not being online).<br>• **Firmware Upgrade** – It means such profile will be used for firmware upgrade. |
| **File Path** | When **Config Restore** is selected as **Action Type,** click **Select** to upload a configuration file from the connected USB disk. Later such file will be used for saving, restoring or firmware upgrade for CPE. |
| **File Name** | Specify a file name is this field to save the configuration file when **Config Backup** is selected as **Action Type.** |
| **Schedule Profile** | Vigor2927 series will perform the specified action to the selected CPE based on the schedule configured here.<br>Specify one or two schedule profiles (represented by number) here. |

3. Enter all the settings and click **OK**.
4. A new maintenance profile has been created.

## VI-5-2-3 Google Map

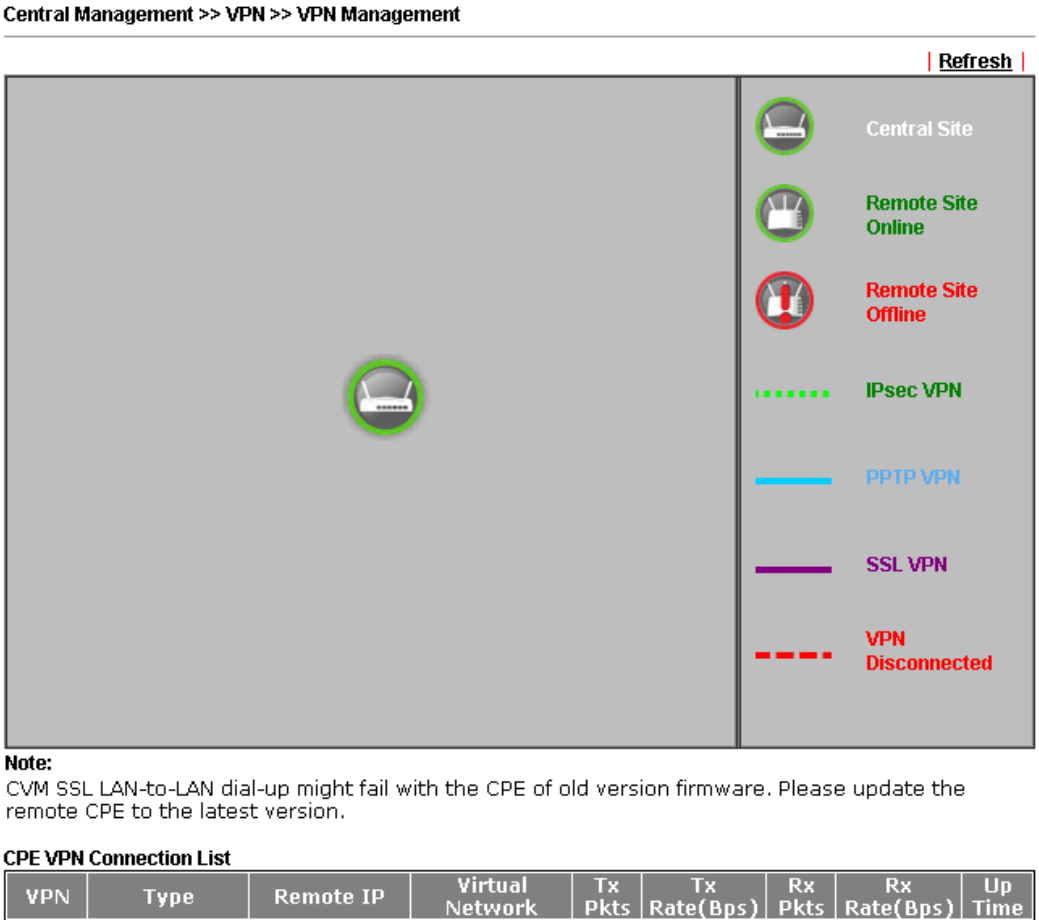
To display the **location** of the managed CPE with a bird's eye view, open **Central VPN Management>>CPE Management** and click the tab of **Google Map**.

Central Management >> VPN >> CPE Management >> Google Map



## VI-5-3 VPN Management

An easy and quick method is offered to configure VPN settings for building VPN connection automatically between Vigor2927 series (treated as VPN server) and other Vigor router (treated as CPE device, i.e., VPN client).



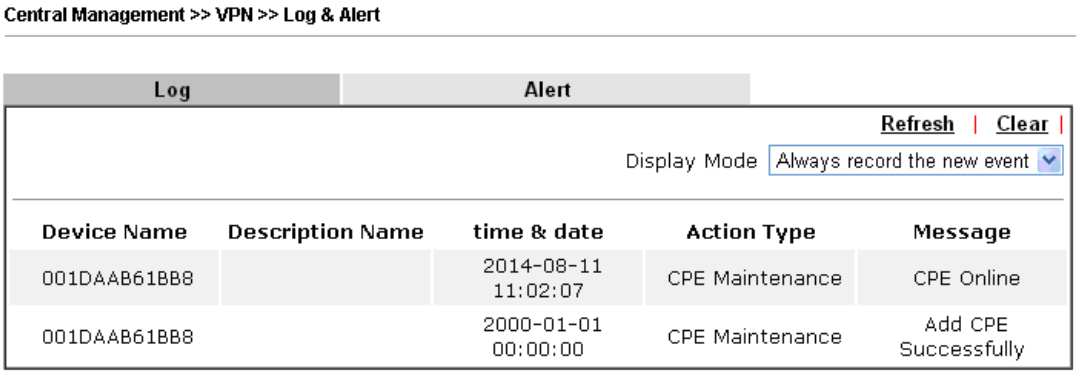

Available parameters are listed as follows:

| Item | Description |
|---|---|
| **CPE VPN Connection List** | |
| **VPN** | Display the name of the LAN-to-LAN profile.<br>It is generated automatically when you click the PPTP/IPsec/Advanced button to build the VPN connection between Vigor2927 and remote CPE. |
| **Type** | Display the dial-in type and the authentication method. |
| **Remote IP** | Display the IP address of the remote CPE and the interface. |
| **Virtual Network** | Display the IP address and subnet mask of Vigor2927 series. |
| **Tx Pkts** | Display the number of the transmitted packets. |
| **Tx Rate(Bps)** | Display the number of the transmitted rate. |
| **Rx Pkts** | Display the number of the received packets. |
| **Rx Rate(Bps)** | Display the number of the received rate. |
| **Up Time** | Display the connection time of such VPN. |

Once the device is managed (controlled) by Vigor2927 series, it will be displayed on such screen automatically. If not, refer to sections **"How to manage the CPE (router) through Vigor2927?"** for more detailed information.

## VI-5-4 Log & Alert

This page offers brief information to identify the CPE connected to Vigor2927 series.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Display Mode** | Choose the mode you want to display the related information on the following table.<br>● **Stop record when fulls -** when the capacity of CVM log is full, the system will stop recording.<br>● **Always record the new event -** only the newest events will be recorded by the system. |
| **Device Name** | Display the name of the managed CPE. |
| **Description Name** | Display the brief explanation for the managed CPE. |
| **Time & date** | Display the time and date that the managed CPE scanned by Vigor2927 series. |
| **Action Type** | Display the action that Vigor2927 series will perform for the managed CPE. |
| **Message** | Display the information for each event. |

The Alert page offers brief information to identify the CPE connected to Vigor2927 series.

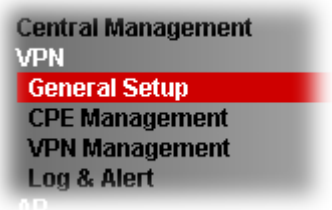
# Application Notes

## A-1 CVM Application - How to manage the CPE (router) through Vigor2927 series?

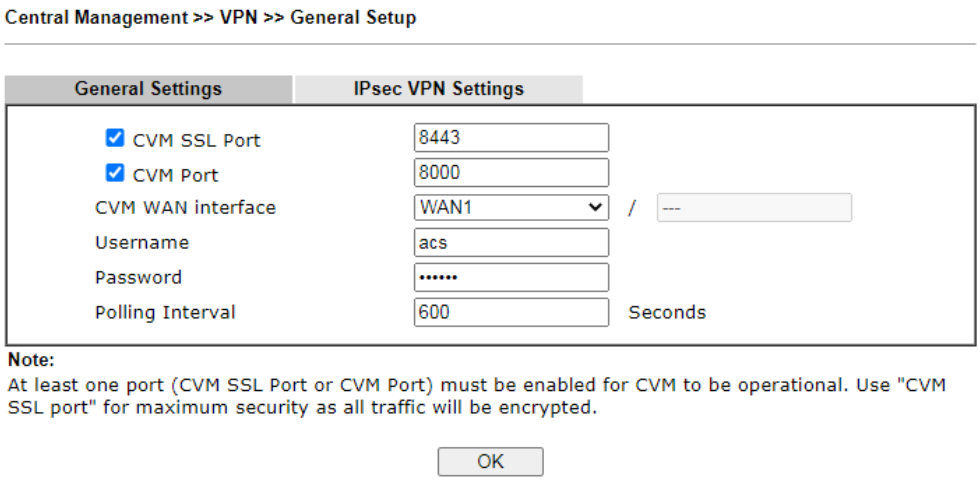
To manage CPEs through Vigor2927 series, you have to set URL on CPE first and set username and password for Vigor2927 series. For this section, we use Vigor2850 series as the example. All the CPE configuration will be done through Vigor2850 series.

### Configure CVM Settings on Vigor2927 series

1. Access into the web user interface of Vigor2927 series.
2. Open **Central Management>> VPN >>General Setup.**




3. In the following page, check the boxes for CVM Port and CVM SSL Port to enable the port setting. Enter the values for **CVM Port**, **CVM SSL Port, Username**, and **Password** respectively. Remember the values configured in this page.

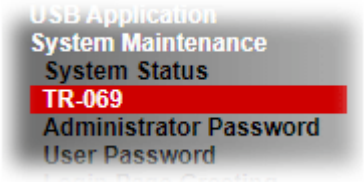



4. Click **OK** to save the settings.

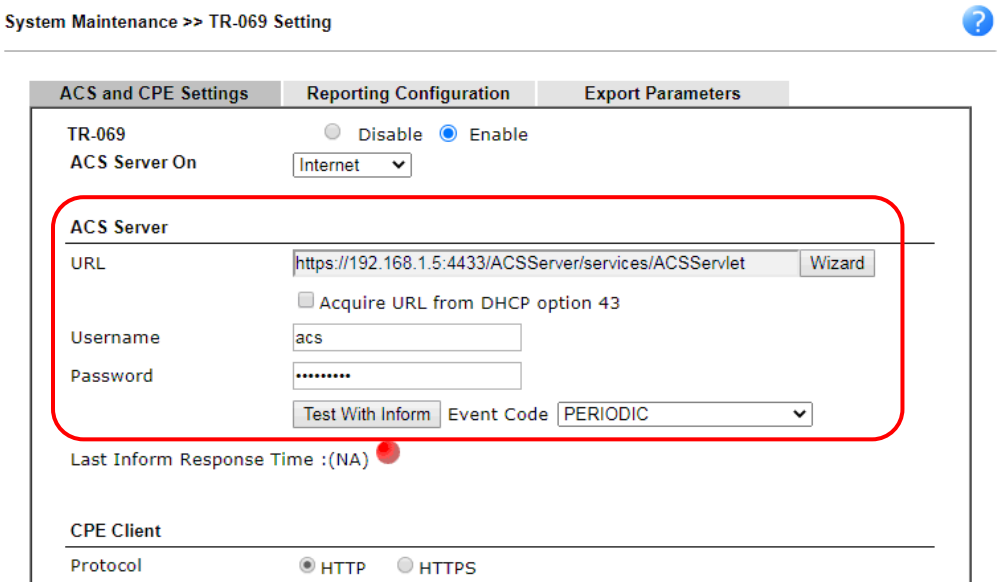
## Configure Settings on CPE

1. In the end of the CPE, access into the web user interface of the CPE (e.g., Vigor2865 series). Open a web browser (for example, **IE**, **Mozilla Firefox** or **Netscape**) and type **http://192.168.1.1.**

2. Open **System Maintenance >> TR-069**.

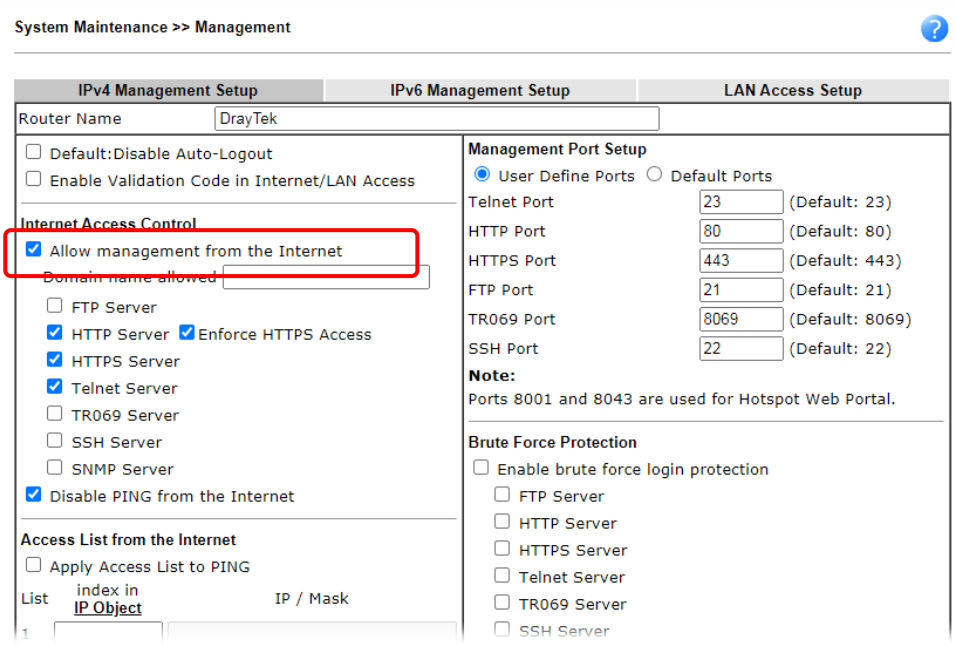



3. In the field of **ACS Server**, Enter the URL (IP address with port number) of Vigor2927 series and Enter the same Username and Password defined on the page of **Central VPN Management>>General Setup** in Vigor2927 series. Click **OK** to save the settings.



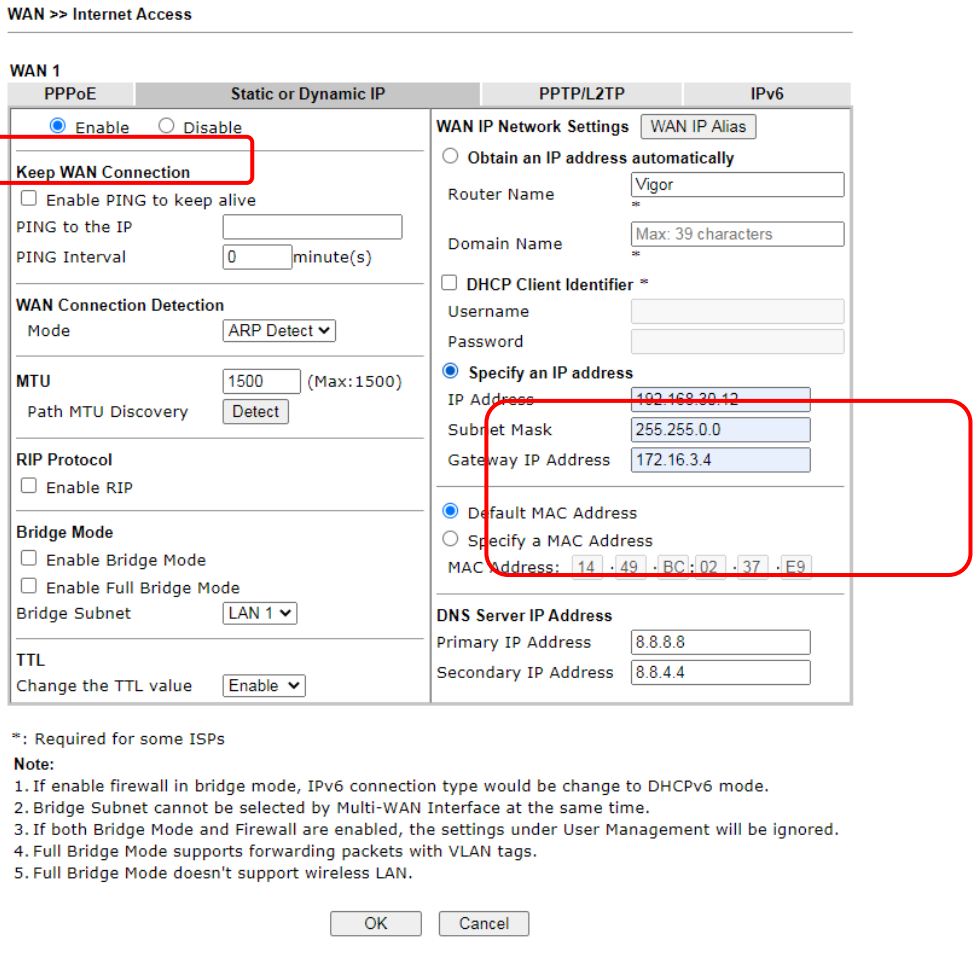

4. Open **System Maintenance>>Management Setup**.

5. Check **Allow management from the Internet** to set management access control and click **OK.**




6. Open **WAN>>Internet Access.** Use the drop down list of **Access Mode** on WAN1 to select **MPoA** (RFC1483/2684). Then, click **Details Page**.

7. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.

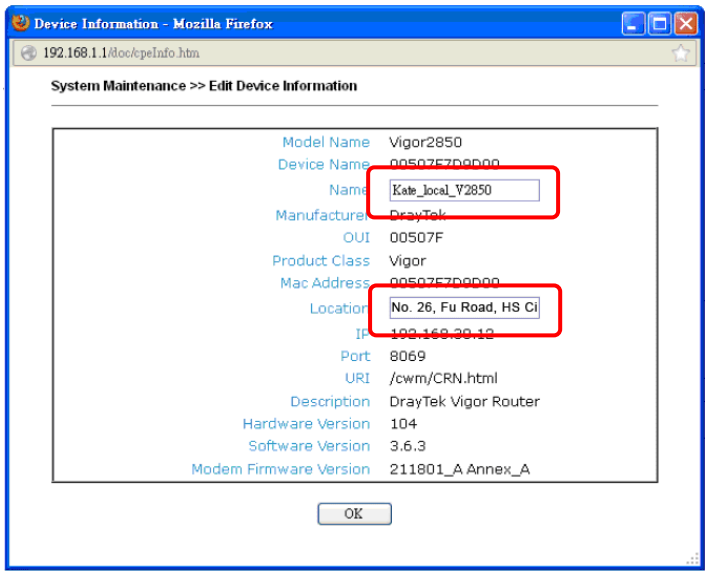


**Info**

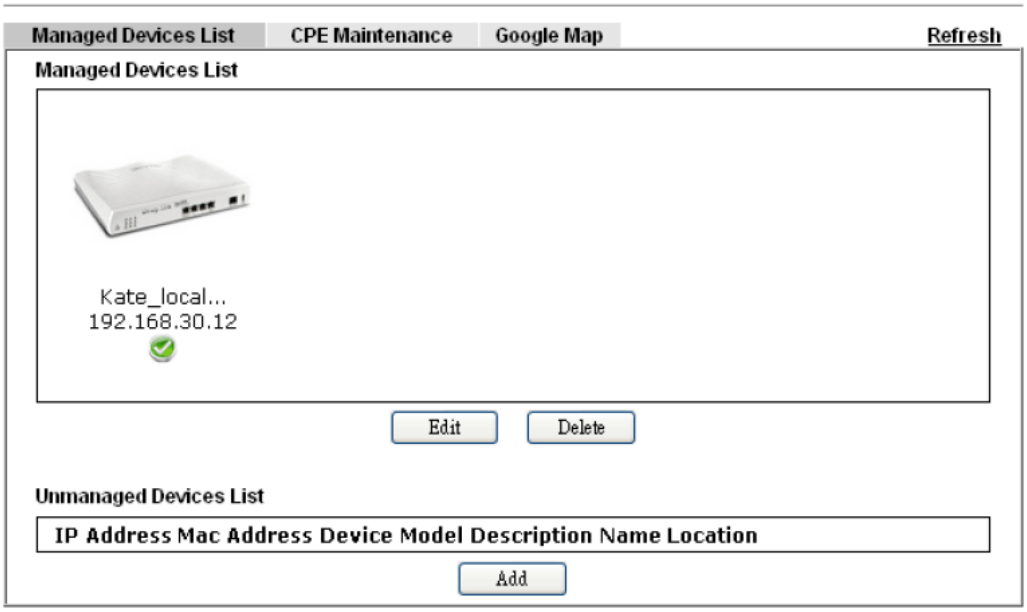
Reboot the CPE device and re-log into Vigor2927 series. CPE which has registered to Vigor2927 series will be captured and displayed on the page of Central VPN Management>>CPE Management.

## Check CPE Maintenance Page

1. Return to the web user interface of Vigor2927 series.
2. Open **Central Management>>VPN>>VPN Management**. Now there is one CPE displayed on the field of Unmanaged Devices List.
3. Choose the one (Vigor2927) from Unmanaged Devices List and click **Add**. The following dialog will be popped up. Enter the name and the location of the router respectively. Click **OK** to save the configuration.



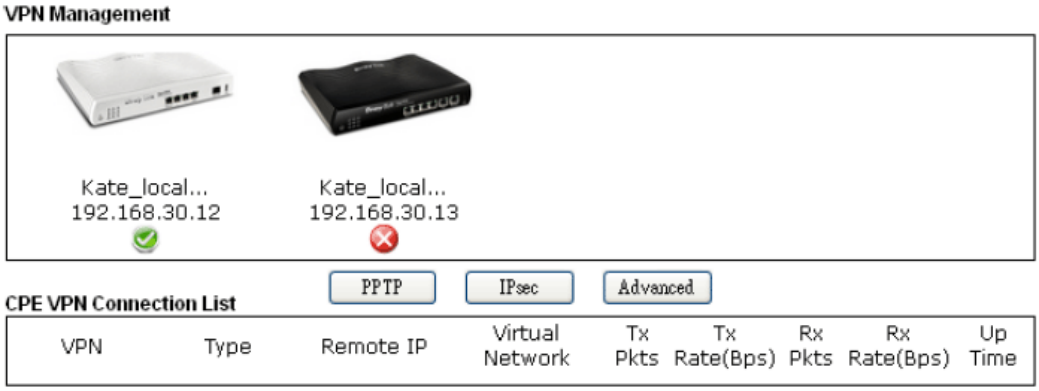

4. The selected CPE will be moved and displayed on Managed Devices List which means it is controlled / managed by Vigor2927 series from now on.



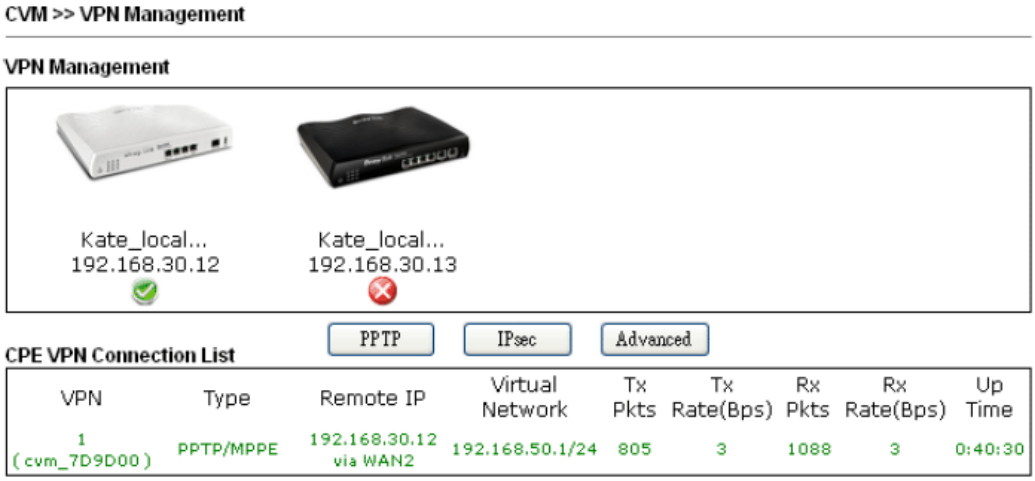
## A-2 CVM Application - How to build the VPN between remote devices and Vigor2927 series?

When a remote device is managed by Vigor2927 series, it is easy to build VPN between these two devices.

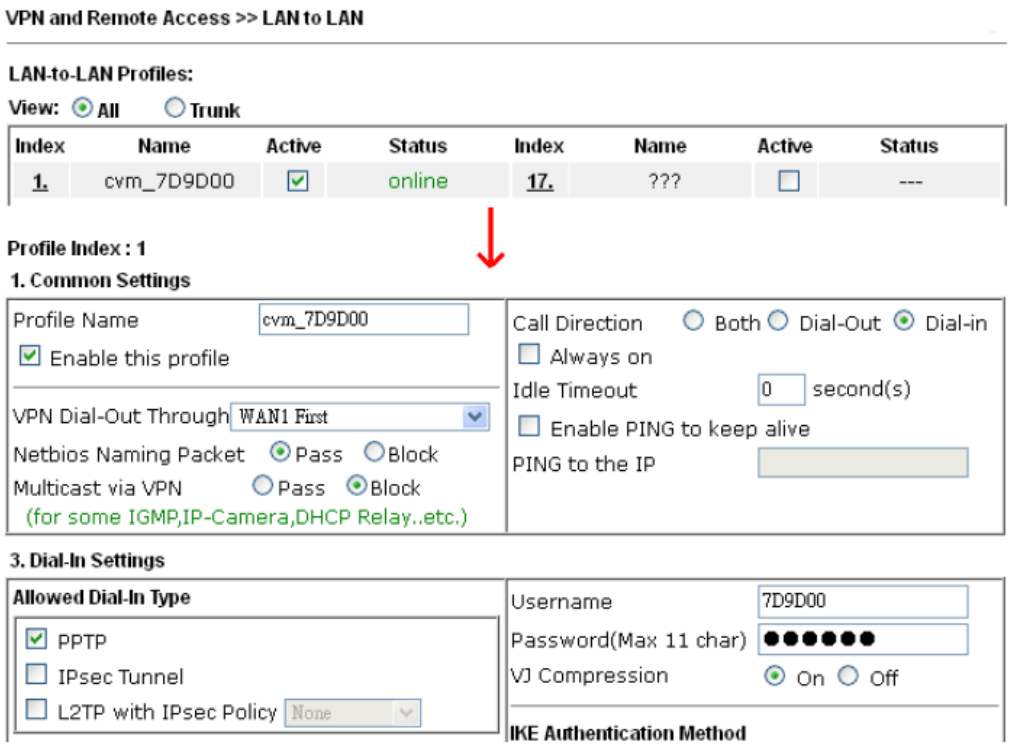
1. Access into the web user interface of Vigor2927 series.
2. Open **Central Management>> VPN >>CPE Management**.




3. Click the device icon (marked with ) and click the **PPTP/IPsec** button.
4. Wait for a moment. If VPN is built successfully, related information will be displayed on **CPE VPN Connection List**.



5. A LAN to LAN profile for such VPN will be generated automatically. You can access into **VPN and Remote Access>>LAN to LAN** of the remote device for viewing the detailed information.




**Note:** The profile name is created automatically by the system. Do not modify any value in such page to avoid VPN error.

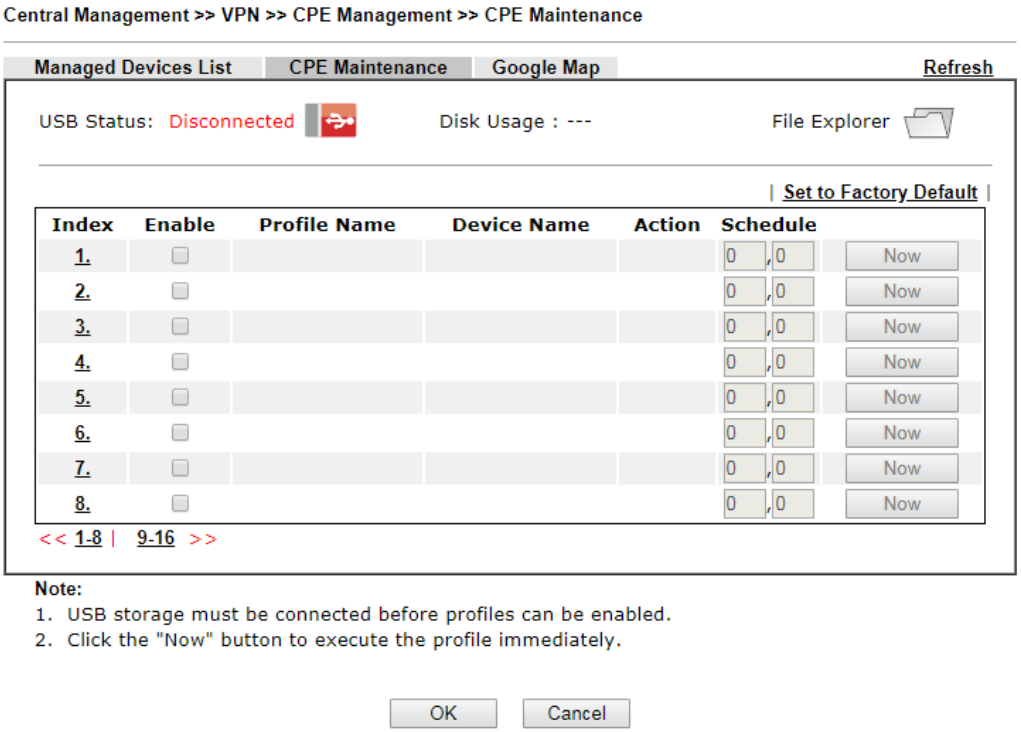
## A-3 CVM Application - How to upgrade CPE firmware through Vigor2927 series?

Download the newest firmware from your Draytek website to USB Storage Disk for the device (e.g., Vigor2850) managed by Vigor2927 series.

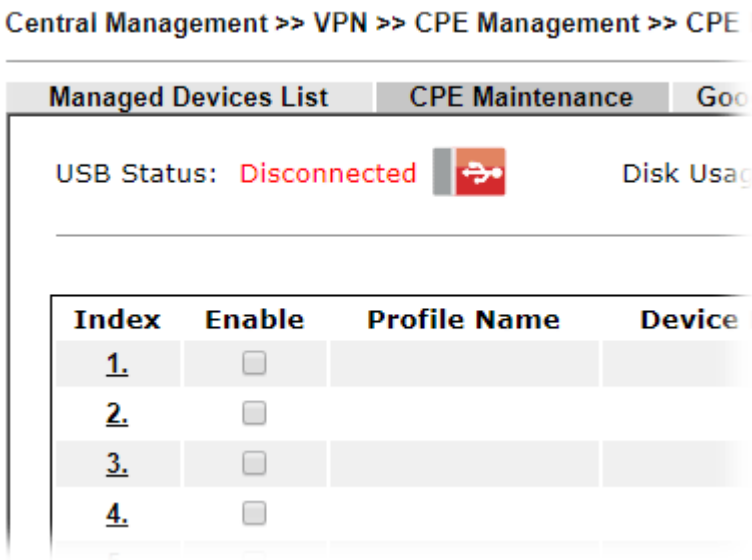
Vigor2850, as an example, is chosen for Vigor2927 to perform the CPE firmware upgrade remotely in this case.

1. Plug in USB storage disk onto Vigor2927 series via USB interface. Make sure the USB disk has been installed correctly, otherwise, the firmware upgrade will not be successful.

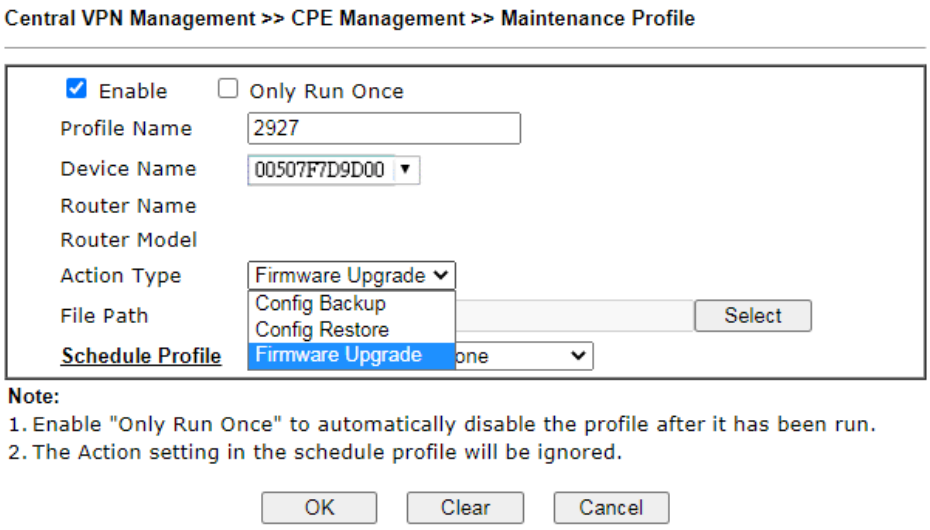
2. Access into web user interface of Vigor2927 series. Open Central **VPN Management>>CPE Management** and click the **CPE Maintenance** tab.




3. Click any index number link, e.g., Index 1.

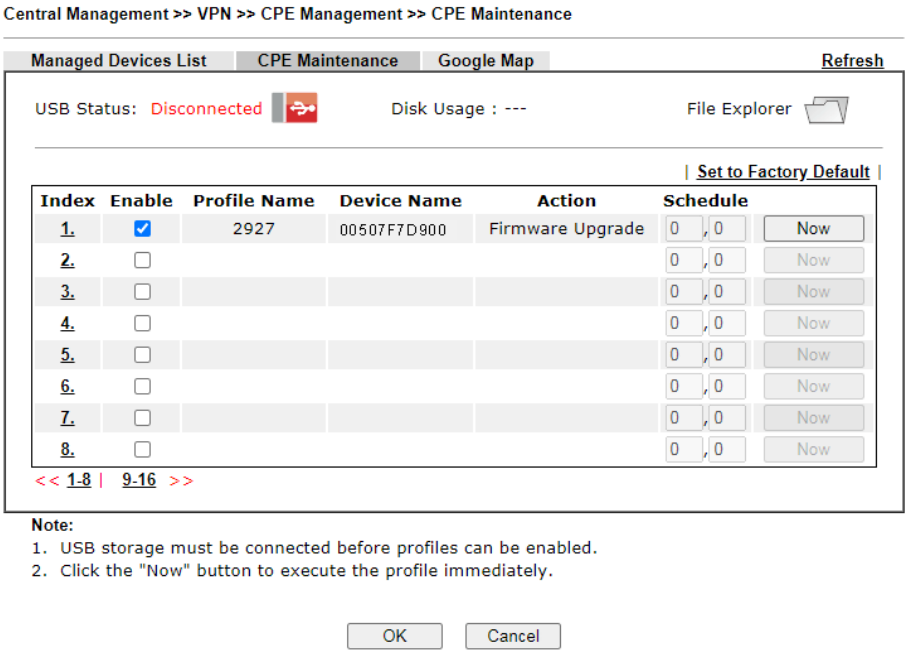


4. The Maintenance profile dialog appears.




In the field of Profile Name, type a name for such maintenance profile; check Enable; and choose the one you want to perform firmware upgrade from Device Name drop down list. From the Action Type, choose Firmware Upgrade. Enter the file/path of the newest firmware or click Select to locate it. Specify the Schedule profile. At last, click **OK**.

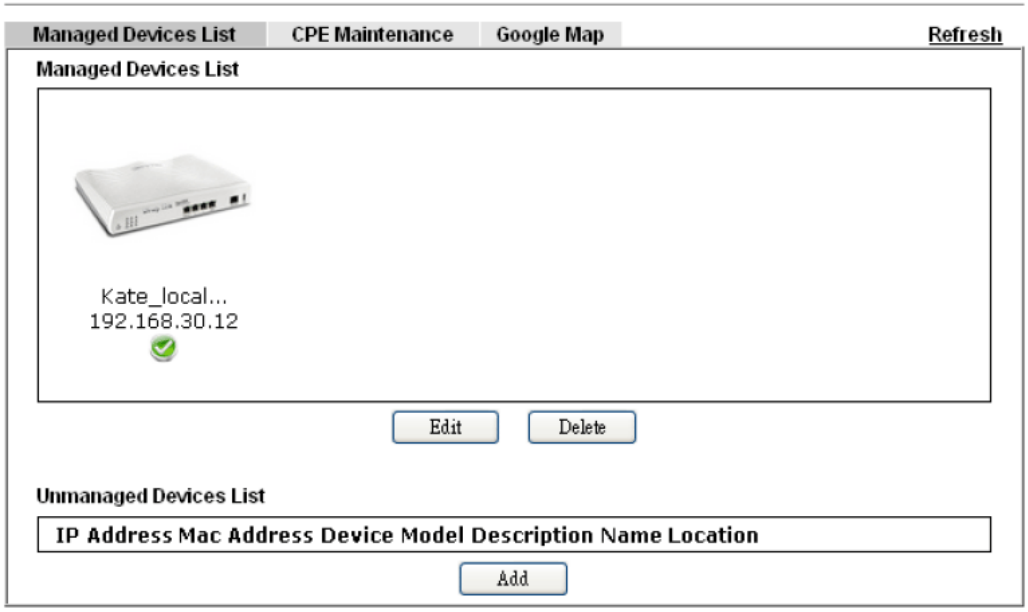
5. Now, a new maintenance profile has been created.




6. Click **Now** to perform the firmware upgrade immediately for Vigor2927.

7. Wait for several minutes for firmware upgrade.

8. Then check the device information for the managed device if the firmware upgrade is successful or not. Click **Managed Devices List**.




Click the icon of Vigor2850 and click **Edit** and view the software version. Another way to check if the firmware upgrade is completed or not, simply open **Central VPN Management>>Log & Alert**.

# VI-6 Central Management (AP)

Vigor2927 can manage the access points supporting AP management via Central AP Management.

## AP Map

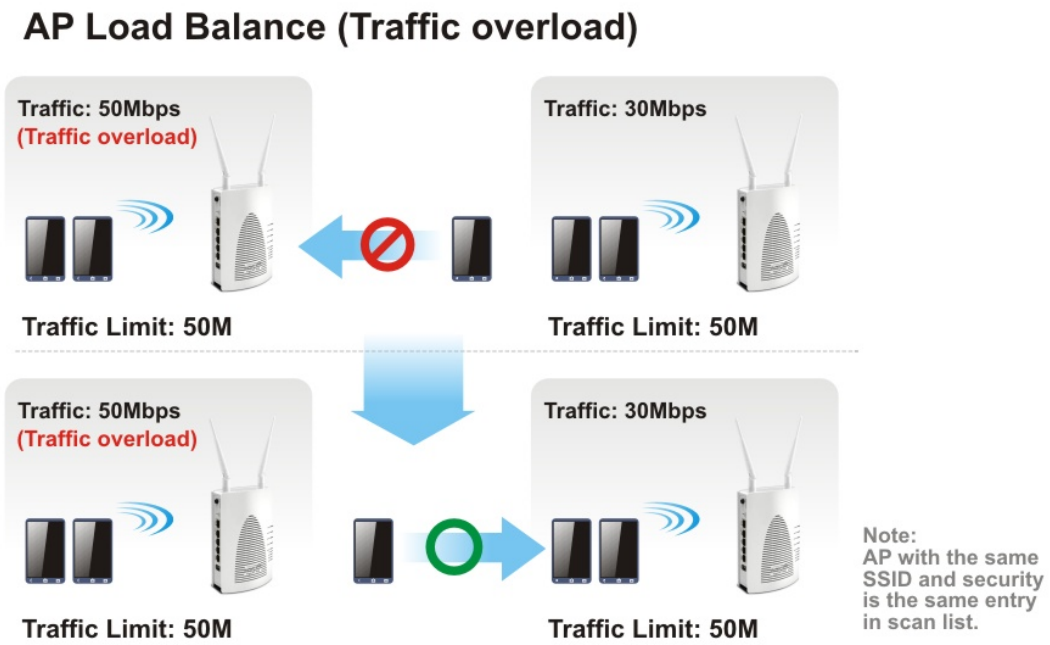
AP Map is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength

## AP Maintenance

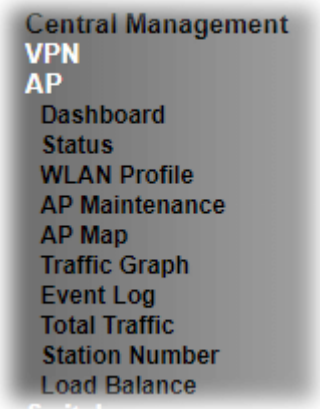
Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

## Load Balance for AP

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

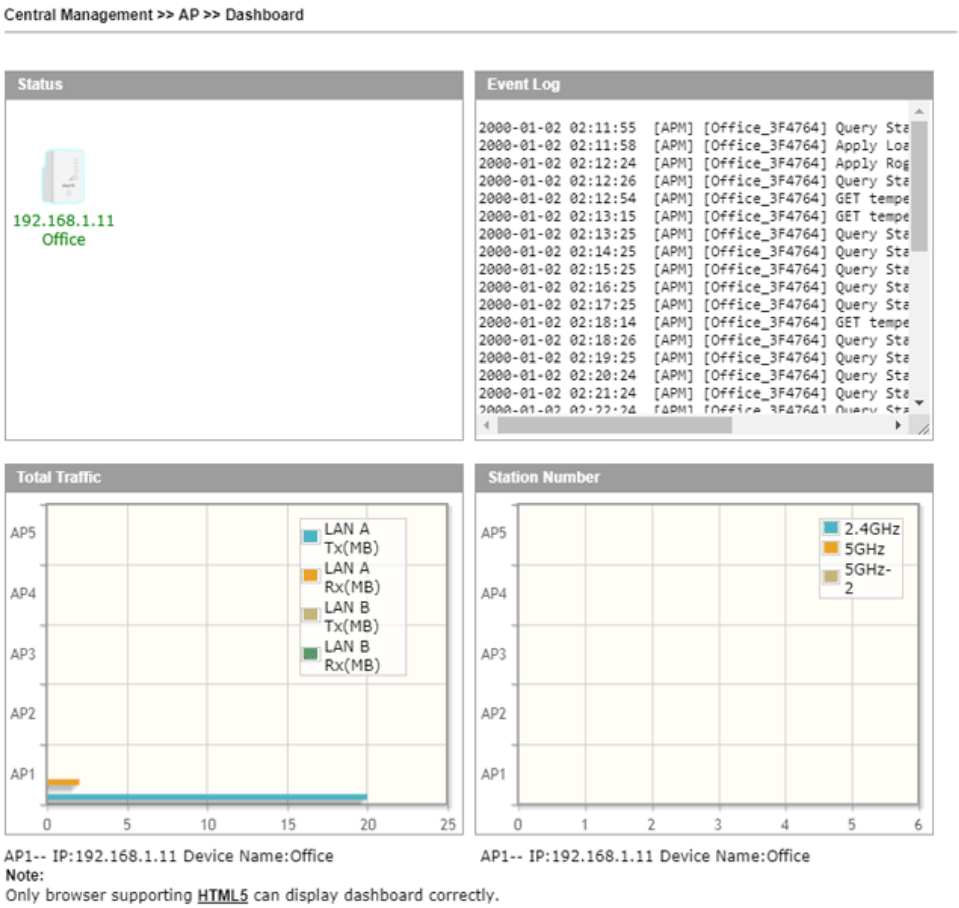


# Web User Interface




## VI-6-1 Dashboard

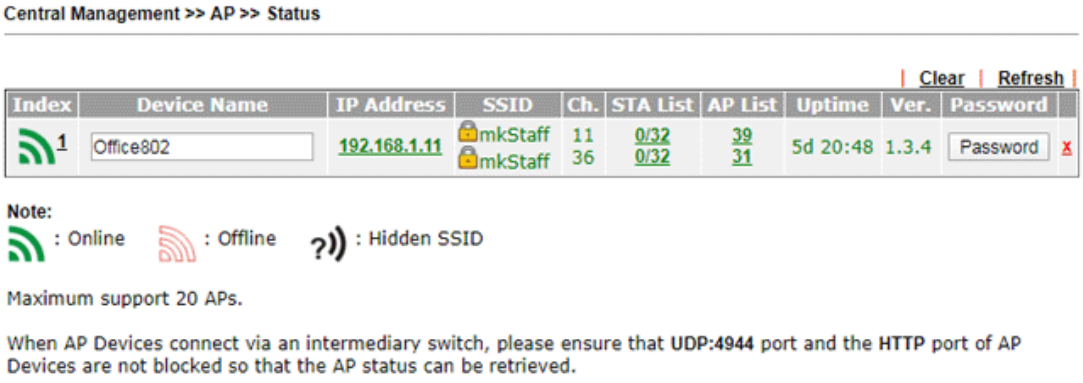
This page shows VigorAP's information about **Status, Event Log, Total Traffic** or **Station Number** by displaying VigorAP icon, text and histogram. Just move and click your mouse cursor on **Status, Event Log, Total Traffic** or **Station Number.** Corresponding web pages will be open immediately.




To access into the web user interface of VigorAP, simply move your mouse cursor on the VigorAP icon and click it. The system will guide you to access into the web user interface of VigorAP.

## VI-6-2 Status

This page displays current status (online, offline or SSID hidden, IP address, encryption, channel, version, password and etc.) of the access points managed by Vigor router. Please open **Central AP Management>>Function Support List** to check what AP Models are supported.

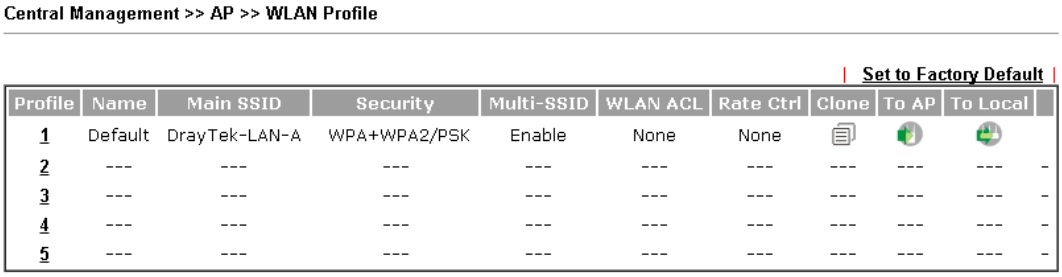



Available settings are explained as follows:

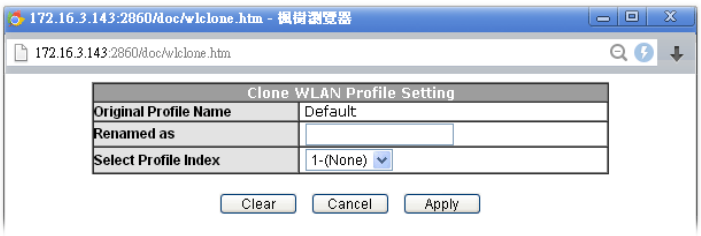
| Item | Description |
|---|---|
| **Index** | Click the index number link for viewing the settings summary of the access point. |
| **Device Name** | The name of the AP managed by Vigor router will be displayed here. |
| **IP Address** | Display the true IP address of the access point. |
| **SSID** | Display the SSID configured for the access point(s) connected to Vigor2927. |
| **Ch.** | Display the channel used by the access point. |
| **STA List** | Display the number of wireless clients (stations) connecting to the access point.<br>In which, 0/64 means that up to 64 clients are allowed to connect to the access point. But, now no one connects to the access point.<br>The number displayed on the left side means 2.4GHz; and the number displayed on the right side means 5GHz. |
| **AP List** | Display the number of the AP around the device. |
| **Uptime** | Display the duration of the AP powered up. |
| **Version** | Display the firmware version used by the access point. |
| **Password** | Vigor2927 can get related information of the access point by accessing into the web user interface of the access point.<br>This button is used to modify the logging password of the connected access point. |

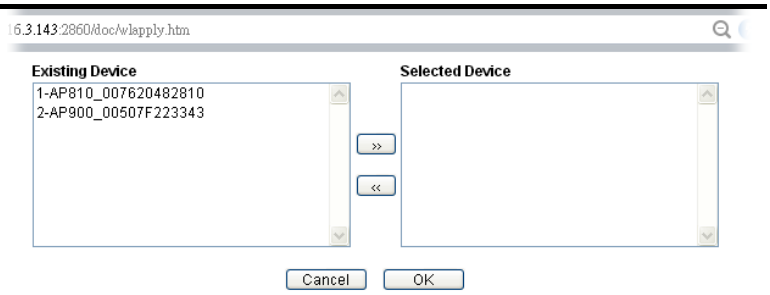
## VI-6-3 WLAN Profile

WLAN profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.



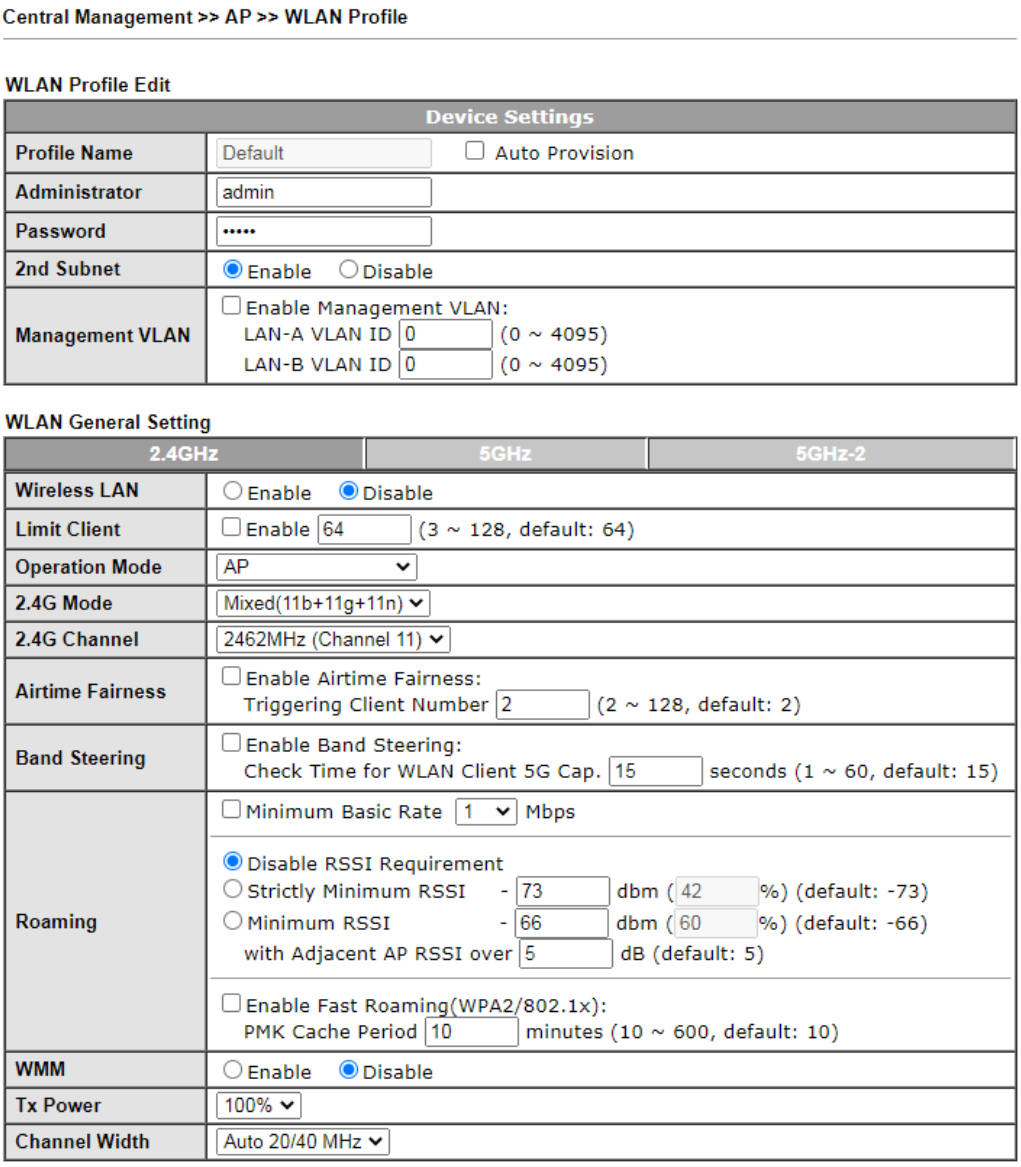

Click the number link of the selected profile to modify the content of the profile. Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile** | There are five WLAN profiles offered to be configured. Simply click the index number link to open the modification page. |
| **Name** | Display the name of the profile.<br>The default profile cannot be renamed. |
| **Main SSID** | Display the SSID configured by such wireless profile. |
| **Security** | Display the security mode selected by such wireless profile. |
| **Multi-SSID** | Enable means multiple SSIDs (more than one) are active.<br>Disable means only SSID1 is active. |
| **WLAN ACL** | Display the name of the access control list. |
| **Rate Ctrl** | Display the upload and/or download transmission rate. |
| **Clone** | It can copy settings from an existing WLAN profile to another WLAN profile.<br>First, you have to check the box of the existing profile as the original profile. Second, click **Clone**. The following dialog will appear.<br>  <br>Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of **Renamed as**. Last, click **Apply** to save the settings on this dialog.<br>The new profile has been created with the settings coming from the original profile. |
| **To AP** | Click it to apply the selected wireless profile to the specified Access Point. |

| | |
|---|---|
| |  <br>Simply choose the device you want from **Existing Device** field. Click **>>** to move the device to **Selected Device** field. Then, click **OK**.<br>The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot. |
| **To Local** | WLAN Profile configured in this page is specified for VigorAP connected to Vigor router.<br>If required, these settings also can be applied to Vigor router. Select and check one of wireless profiles and click this button to apply the settings onto the WI-Fi wireless settings configured for such Vigor router. |

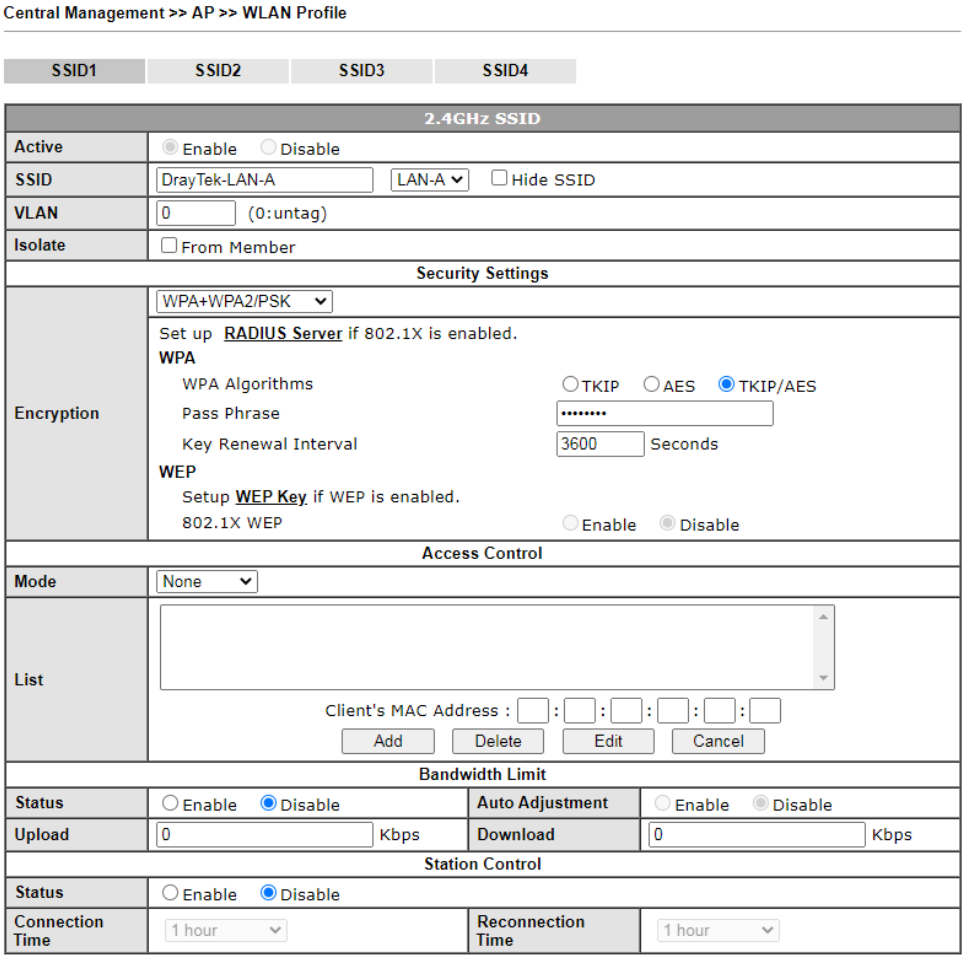
## How to edit the wireless LAN profile?

1. Select the WLAN profile (index number 1 to 5) you want to edit.
2. Click the index number link to display the following page.




**Info** The function of Auto Provision is available for the default WLAN profile.

3. After finished the general settings configuration, click **Next** to open the following page for 2.4G wireless security settings.

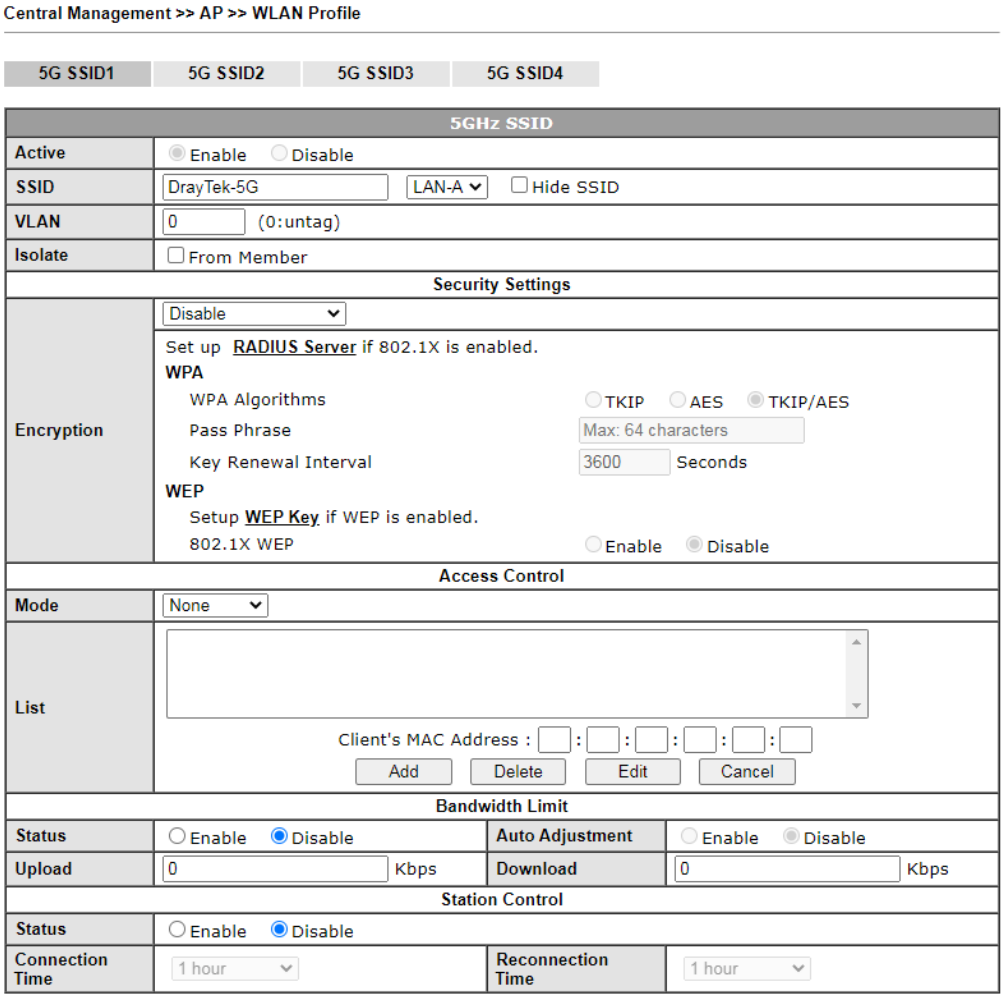


Central Management >> AP >> WLAN Profile

SSID1 | SSID2 | SSID3 | SSID4

| 2.4GHz SSID | | | |
|---|---|---|---|
| Active | Enable Disable | | |
| SSID | DrayTek-LAN-A LAN-A Hide SSID | | |
| VLAN | 0 (0:untag) | | |
| Isolate | From Member | | |
| **Security Settings** | | | |
| Encryption | WPA+WPA2/PSK<br>Set up RADIUS Server if 802.1X is enabled.<br>**WPA**<br>WPA Algorithms: TKIP AES TKIP/AES<br>Pass Phrase: ••••••••<br>Key Renewal Interval: 3600 Seconds<br>**WEP**<br>Setup WEP Key if WEP is enabled.<br>802.1X WEP: Enable Disable | | |
| **Access Control** | | | |
| Mode | None | | |
| List | Client's MAC Address : : : : : :<br>Add Delete Edit Cancel | | |
| **Bandwidth Limit** | | | |
| Status | Enable Disable | Auto Adjustment | Enable Disable |
| Upload | 0 Kbps | Download | 0 Kbps |
| **Station Control** | | | |
| Status | Enable Disable | | |
| Connection Time | 1 hour | Reconnection Time | 1 hour |

4. After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.

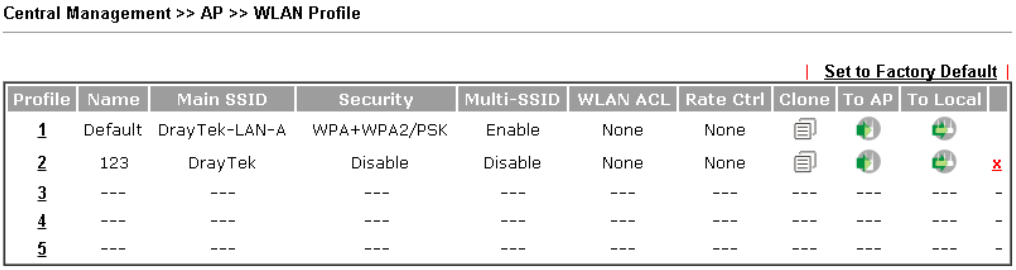


Central Management >> AP >> WLAN Profile

5G SSID1 | 5G SSID2 | 5G SSID3 | 5G SSID4

| 5GHz SSID | | | |
|---|---|---|---|
| Active | Enable Disable | | |
| SSID | DrayTek-5G LAN-A Hide SSID | | |
| VLAN | 0 (0:untag) | | |
| Isolate | From Member | | |
| **Security Settings** | | | |
| Encryption | Disable<br>Set up RADIUS Server if 802.1X is enabled.<br>WPA<br>WPA Algorithms: TKIP AES TKIP/AES<br>Pass Phrase: Max: 64 characters<br>Key Renewal Interval: 3600 Seconds<br>WEP<br>Setup WEP Key if WEP is enabled.<br>802.1X WEP: Enable Disable | | |
| **Access Control** | | | |
| Mode | None | | |
| List | Client's MAC Address : : : : : :<br>Add Delete Edit Cancel | | |
| **Bandwidth Limit** | | | |
| Status | Enable Disable | Auto Adjustment | Enable Disable |
| Upload | 0 Kbps | Download | 0 Kbps |
| **Station Control** | | | |
| Status | Enable Disable | | |
| Connection Time | 1 hour | Reconnection Time | 1 hour |

5. When you finished the above web page configuration, click **Finish** to exit and return to the first page. The modified WLAN profile will be shown on the web page.



Central Management >> AP >> WLAN Profile

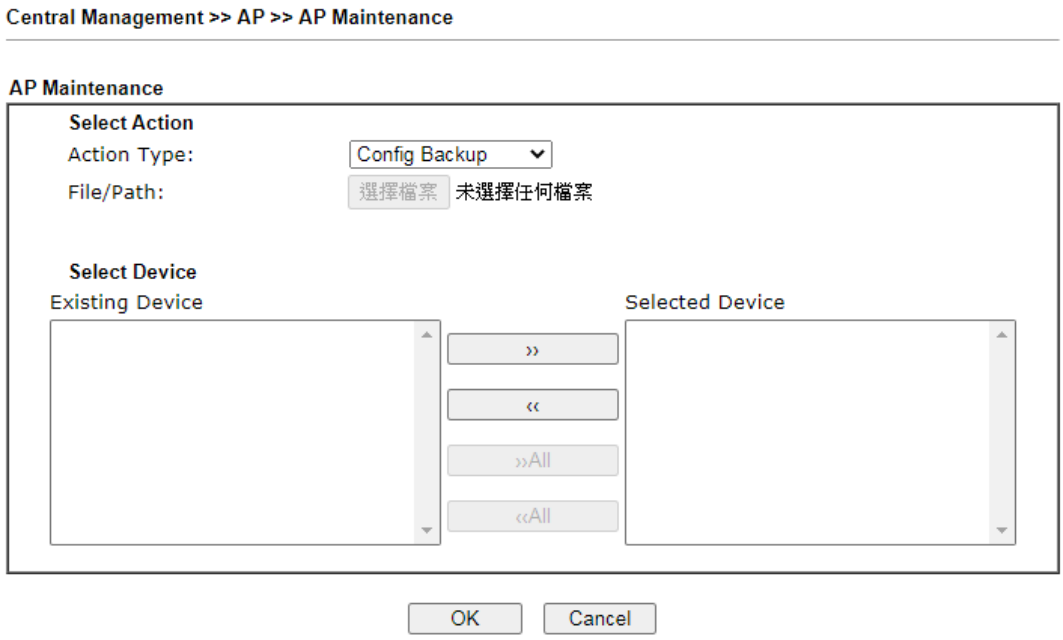
Set to Factory Default

| Profile | Name | Main SSID | Security | Multi-SSID | WLAN ACL | Rate Ctrl | Clone | To AP | To Local | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Default | DrayTek-LAN-A | WPA+WPA2/PSK | Enable | None | None | | | | |
| 2 | 123 | DrayTek | Disable | Disable | None | None | | | | x |
| 3 | --- | --- | --- | --- | --- | --- | --- | --- | --- | - |
| 4 | --- | --- | --- | --- | --- | --- | --- | --- | --- | - |
| 5 | --- | --- | --- | --- | --- | --- | --- | --- | --- | - |

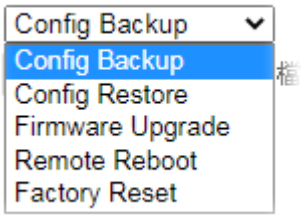
## VI-6-4 AP Maintenance

Vigor router can execute configuration backup, configuration restoration, firmware upgrade and remote reboot for the APs managed by the router. It is very convenient for the administrator to process maintenance without accessing into the web user interface of the access point.

| | |
|---|---|
| **Info** | Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot can be performed to more than one AP at one time by using Vigor2927. |




Available settings are explained as follows:

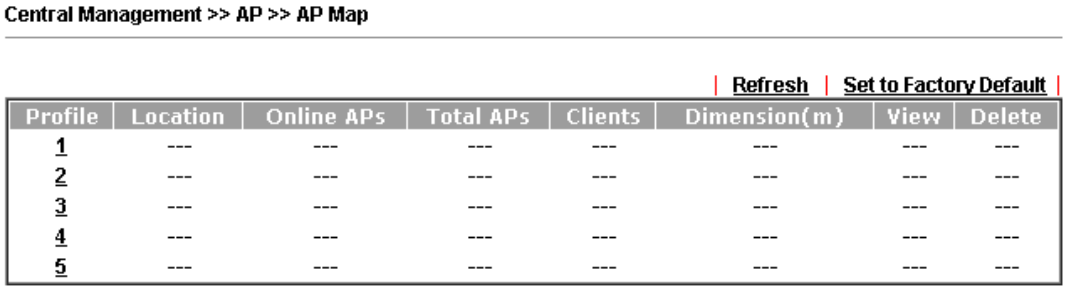
| Item | Description |
|---|---|
| **Action** | There are four actions provided by Vigor router to manage the access points.<br>  <br>Vigor router can **backup** the configuration of the selected AP, **restore** the configuration for the selected AP, perform the **firmware upgrade** of the selected AP, **reboot** the selected AP remotely and perform the **factory reset** for the selected AP. |
| **File/Path** | Specify the file and the path which will be used to perform **Config Restore** or **Firmware Upgrade**. |
| **Select Device** | Display all the available access points managed by Vigor router. Simply click << or >> to move the device(s) between |

| | |
|---|---|
| | **Select Device** and **Selected Device** areas. |
| **Selected Device** | Display the access points that will be applied by such function after clicking OK. |

After finishing all the settings here, please click **OK** to perform the action.

## VI-6-5 AP Map

This function is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength.

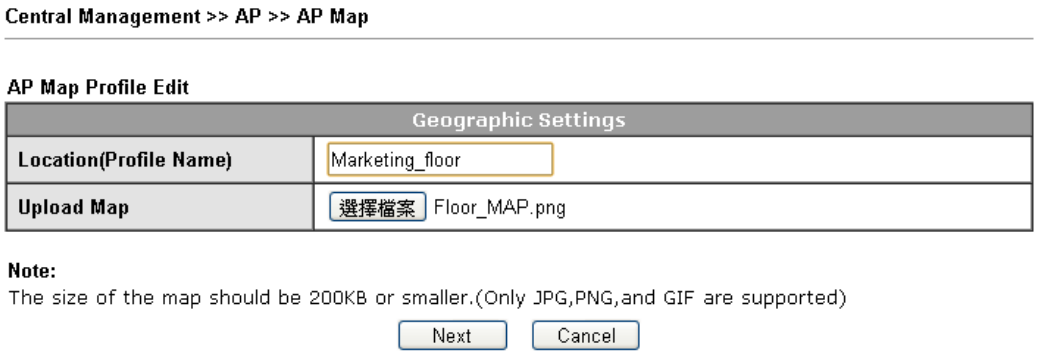



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Click the link to clear current page configuration. |
| **Profile** | Click the link to to view or edit the AP Map. |
| **Location** | Display a brief description (e.g., ground, roof) of the AP Map. |
| **Online APs** | Display the number of VigorAP configured and powered up. |
| **Total APs** | Display the total number of VigorAP configured. |
| **Clients** | Display the number of clients accessing Internet through the VigorAP. |
| **Dimension(m)** | Display the width and length of the AP map. |
| **View** | Click it to review the layout for the selected AP map. |

## Creating /Editing the AP Map Profile

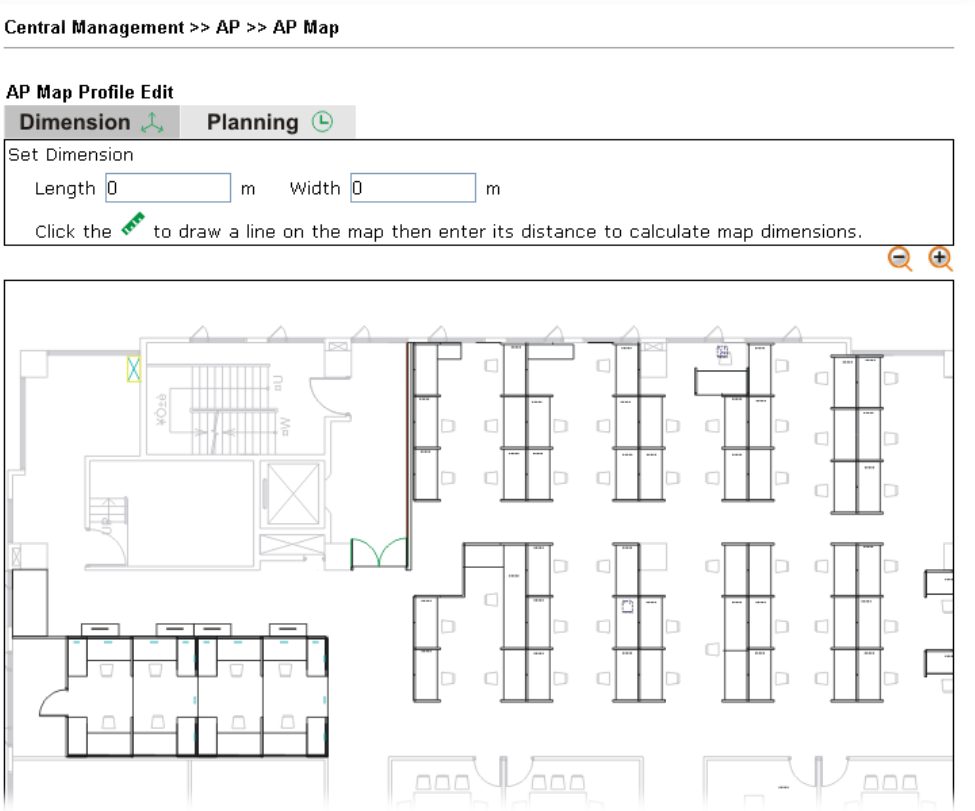
1. Select a number index and click **Edit** to open the following web page.



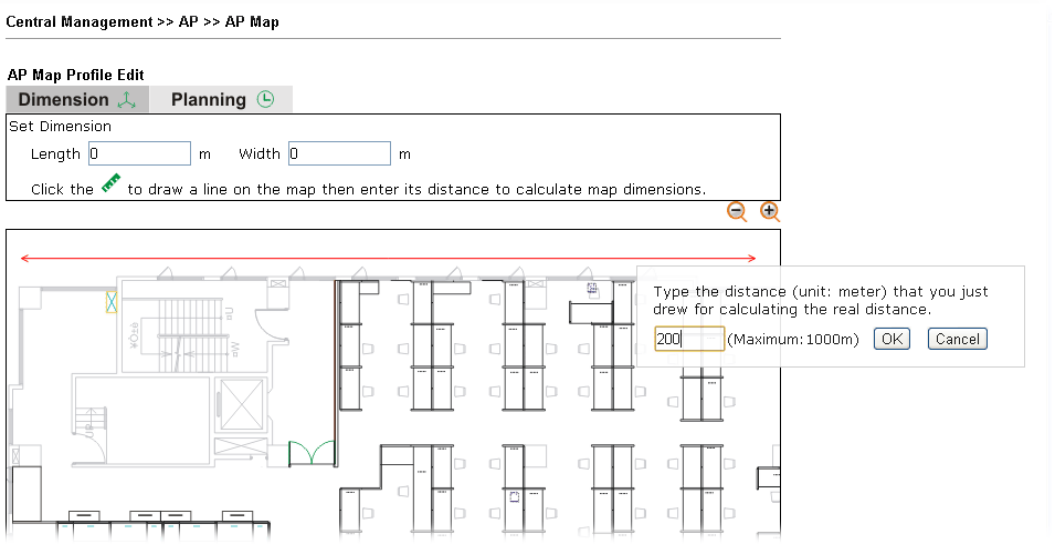

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Location (Profile Name)** | Type a name (e.g., 3F) for the AP map profile. |
| **Upload Map** | Click the **Select** button to choose an image file (only JPG and PNG are supported) for floor plan. |
| **Cancel** | Click it to cancel the configuration. |
| **Next** | Click it to go to the next configuration page. |

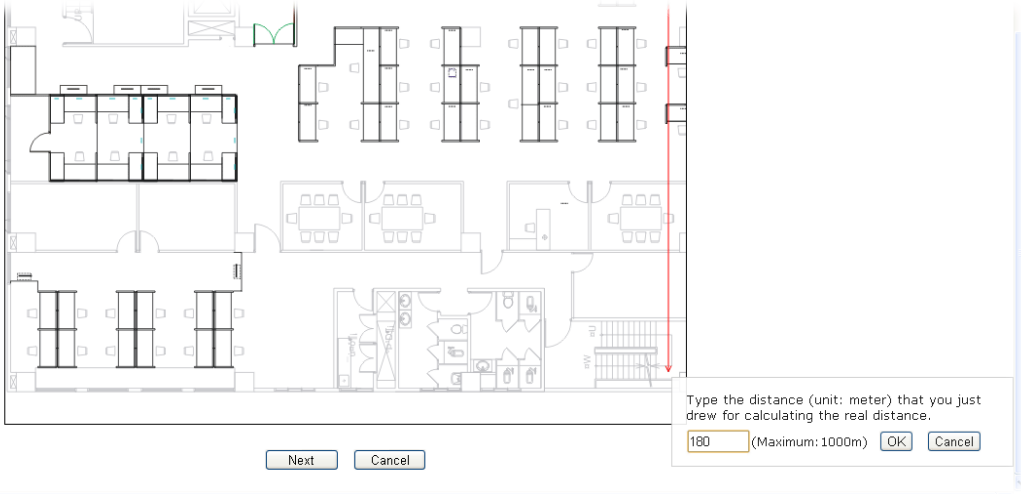
2. Click **Next**. In the web page of **Dimension**, set dimension for the map.



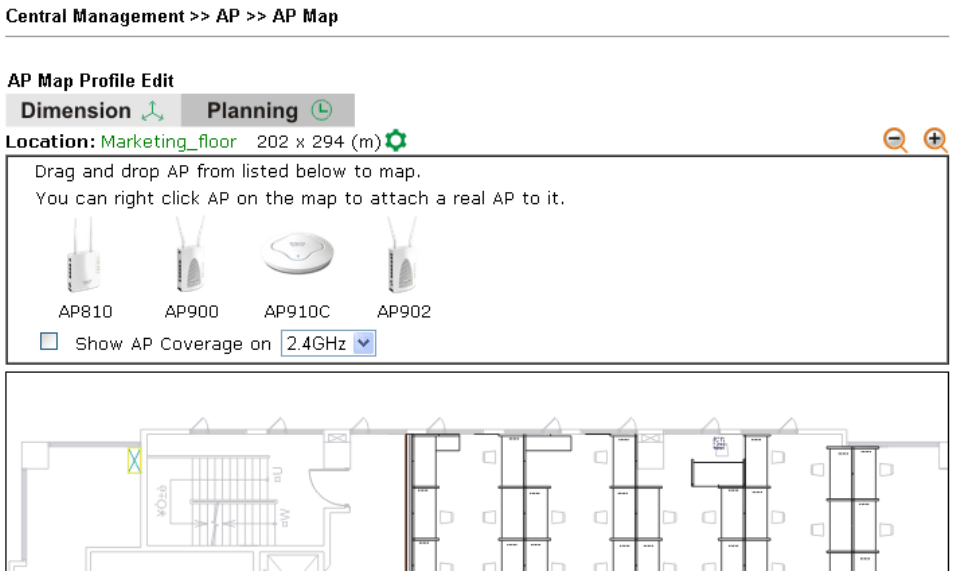
3. Follow the instruction listed on the web page to draw a red line for length / width. Then, Enter the value on the pop up dialog to determine the real distance.



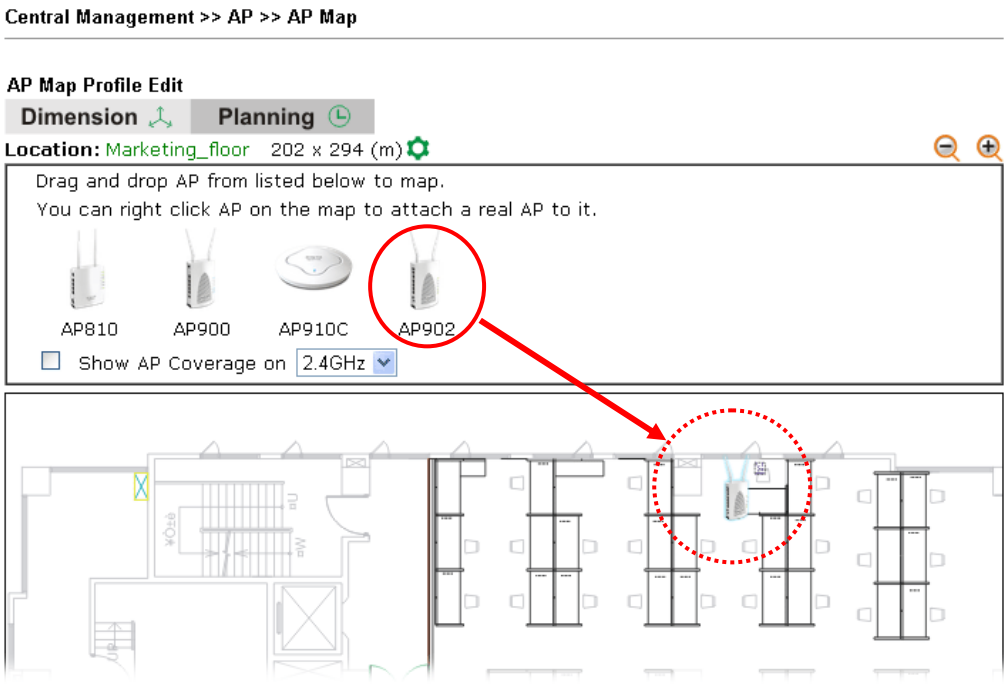

The values for length and width will be displayed on the web page.



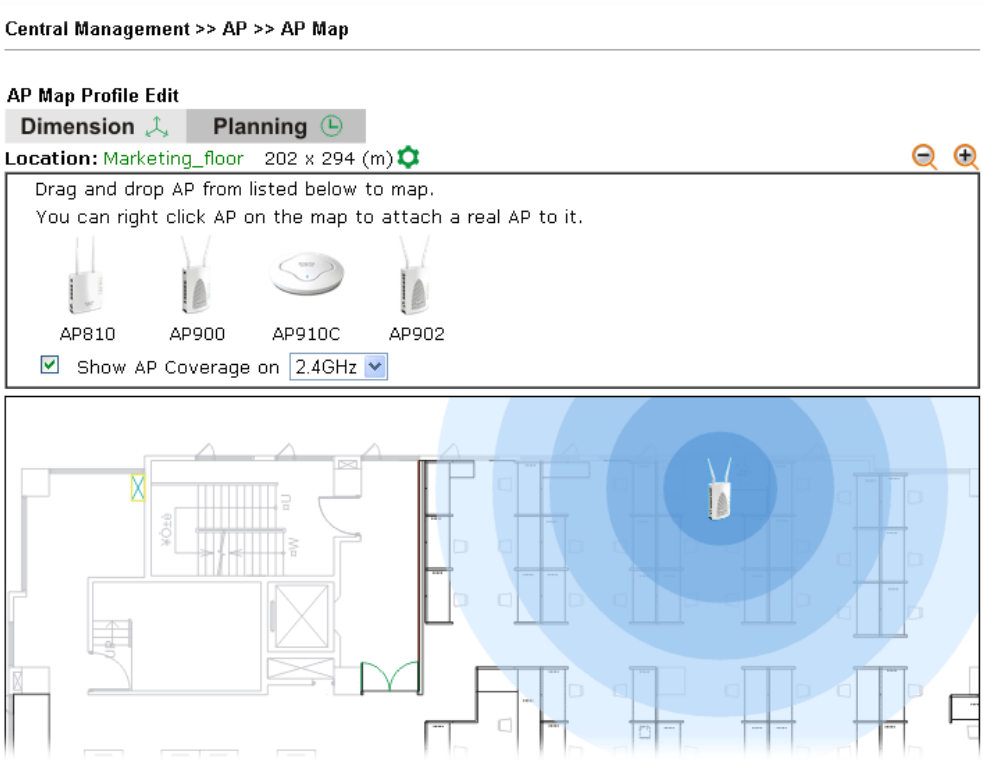

4. Click **Next** to open the web page of **Planning**. Available APs detected by Vigor router will be displayed on the upper end.



5. Select the AP you need; drag and drop an AP icon from upper end to the map on the bottom.




6. Check the box of **Show AP Coverage** and choose 2.4GHz or 5GHz of wireless signal for the AP located on the floor plan.



7. Adjust the AP on the map to find out which place can have the best wireless coverage. At last, click **Save**.

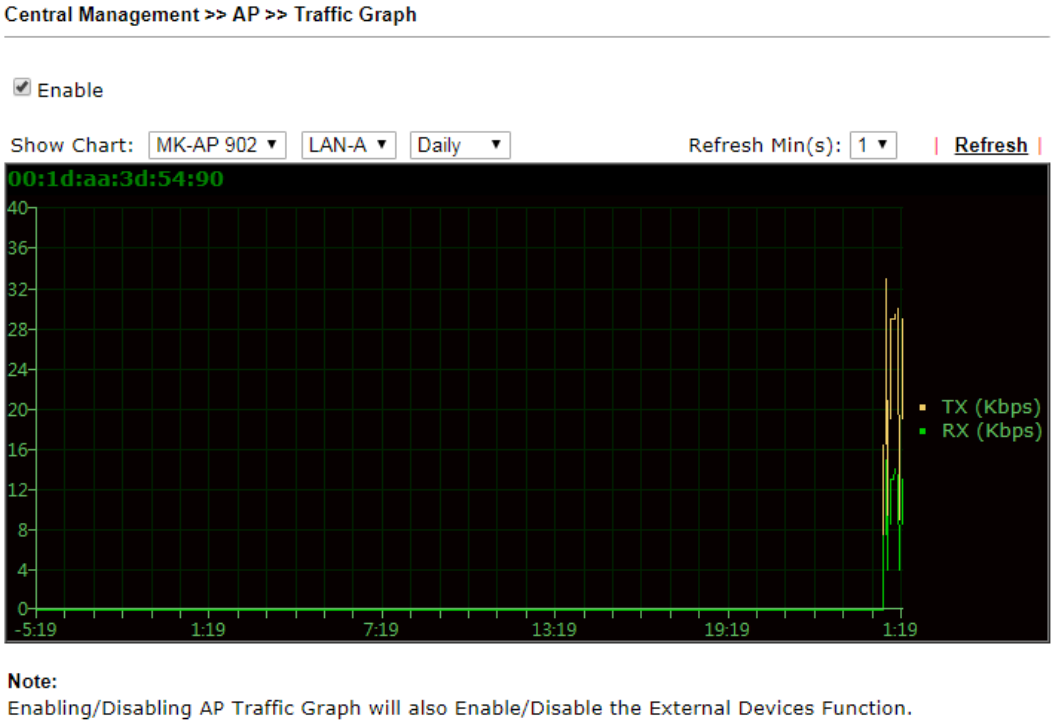
**Central Management >> AP >> AP Map**

| Refresh | Set to Factory Default |

| Profile | Location | Online APs | Total APs | Clients | Dimension(m) | View | Delete |
|---|---|---|---|---|---|---|---|
| 1 | Marketing_floor | 0 | 1 | 0 | 202X294 | | X |
| 2 | --- | --- | --- | --- | --- | --- | --- |
| 3 | --- | --- | --- | --- | --- | --- | --- |
| 4 | --- | --- | --- | --- | --- | --- | --- |
| 5 | --- | --- | --- | --- | --- | --- | --- |

## VI-6-6 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A or LAN-B, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.

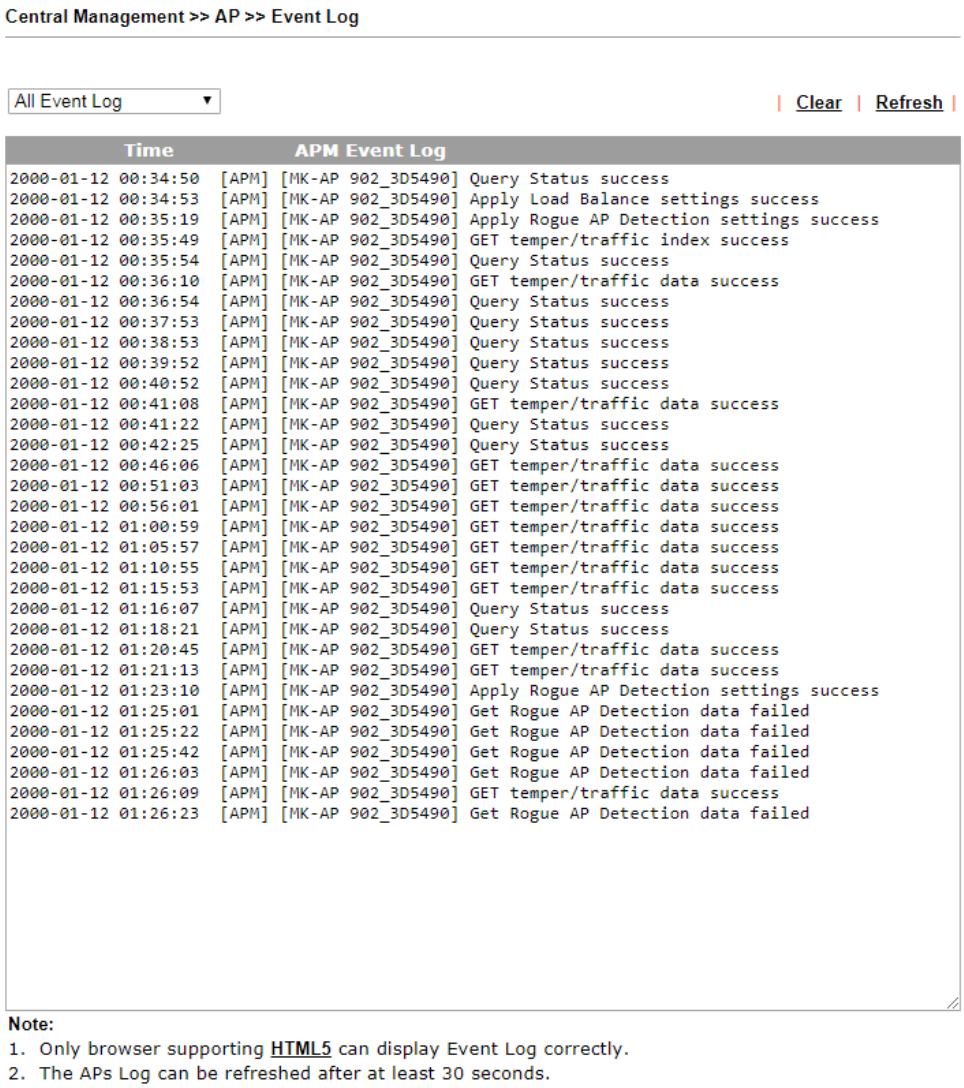



The horizontal axis represents time; the vertical axis represents the transmission rate (in kbps).

| | |
|---|---|
| **Info** | Enabling/Disabling such function will also enable/disable the External Devices function. |

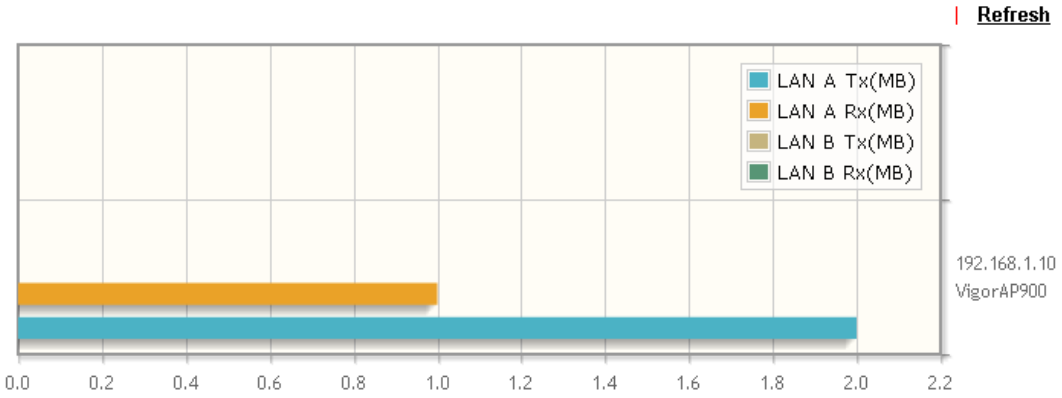
# VI-6-7 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is userful for troubleshooting if required.



## VI-6-8 Total Traffic

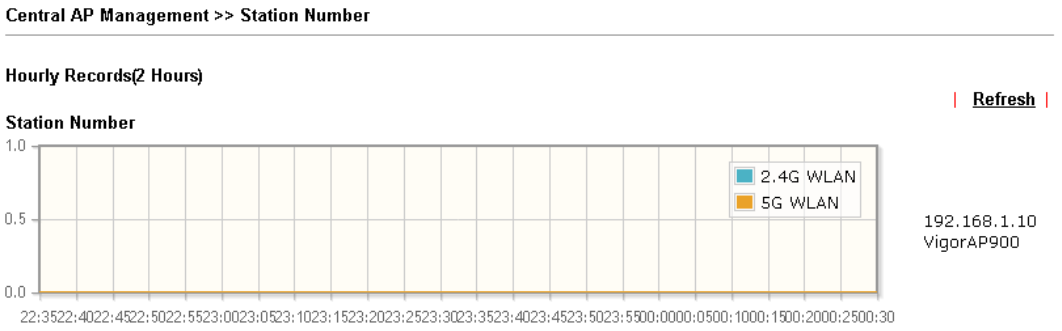
Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.




**Note:** Only browser supporting **HTML5** can display Total Traffic correctly.

## VI-6-9 Station Number

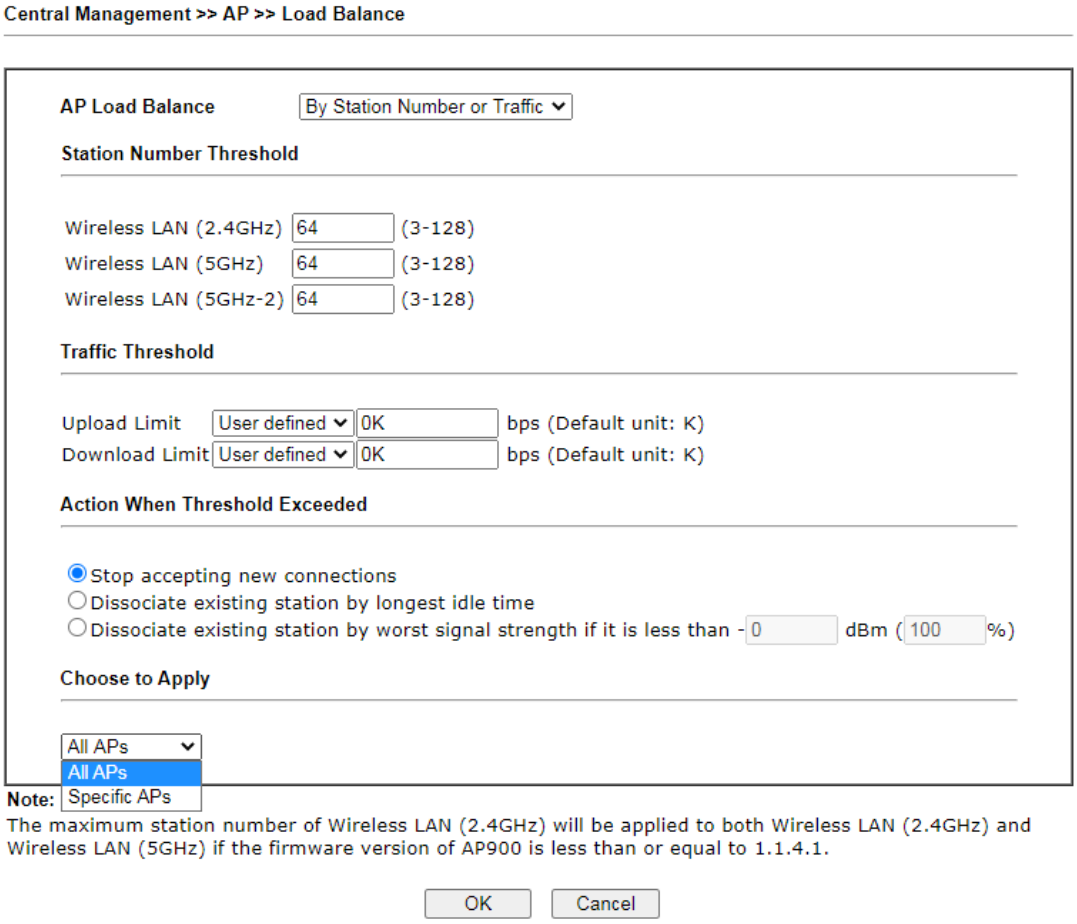
The total number of the wireless clients will be shown on this page, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.




**Note:** Only browser supporting **HTML5** can display Station Number correctly.

## VI-6-10 Load Balance

The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.




Available settings are explained as follows:

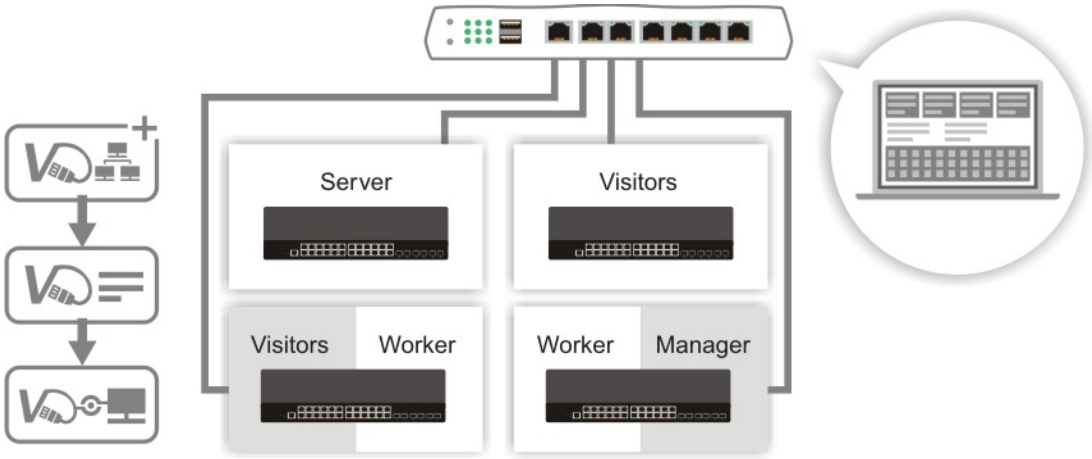
| Item | Description |
|---|---|
| **AP Load Balance** | It is used to determine the operation mode when the system detects overload between access points.<br>**Disable** – Disable the function of AP load balance.<br>**By Station Number** –The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the station connecting to the access point. The purpose is to prevent lots of stations connecting to access point at the same time and causing traffic unbalanced. Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately.<br>**By Traffic** – The operation of load balance will executed according to the traffic configuration in this page.<br>**By Station Number or Traffic** - The operation of load balance will be executed based on the station number or the traffic configuration. |
| **Station Number Threshold** | Set the number of stations as a threshold to activate AP load balance. |

| | |
|---|---|
| **Traffic Threshold** | **Upload Limit** –Use the drop down list to specify the traffic limit for uploading.<br>**Download Limit** – Use the drop down list to specify the traffic limit for downloading. |
| **Action When Threshold Exceeded** | **Stop accepting new connections –** When the number of stations or the traffic reaches the threshold defined in this web page, Vigor router will stop any new connection asked by other access point.<br>**Dissociate existing station by longest idel time** - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time.<br>**Dissociate existing station by worst signal strength if it is less than** - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station with the weakest signal. |
| **Choose to Apply** | Determine which AP shall be applied with the load balance.<br>**All APs** – All APs shall be applied with the load balance.<br>**Specific APs** – The function of load balance will be applied to the AP specified in this field. |

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

# VI-7 Central Management (Switch)

Vigor router can manage lots of VigorSwitch devices connected to it. Through profile and group settings, the administrator can execute firmware/configuration backup, restore for VigorSwitch device, reboot the device or return to factory default settings of VigorSwitch at one time.



# Web User Interface



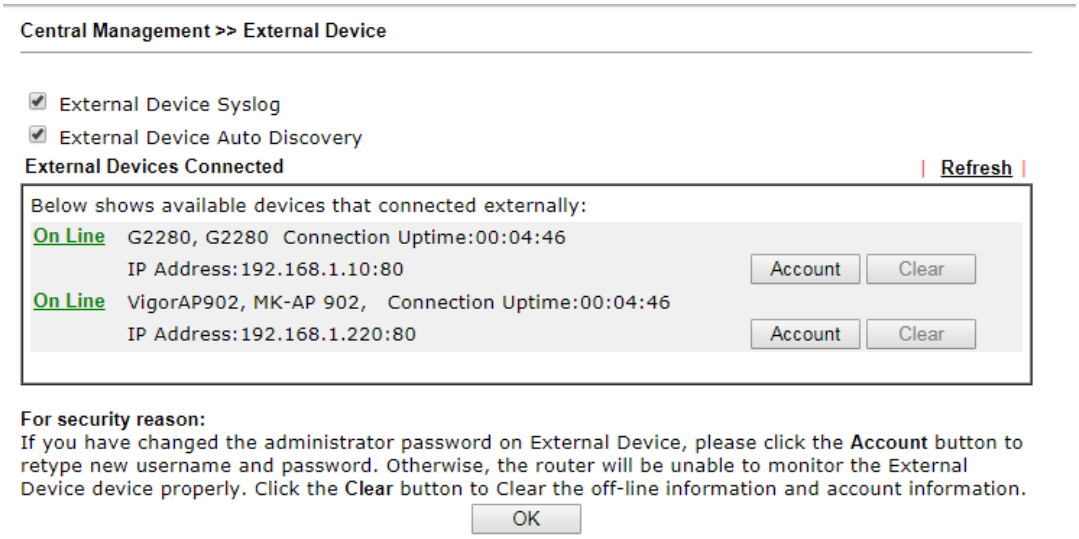

## VI-7-1 Status

### VI-7-1-1 Switch Status

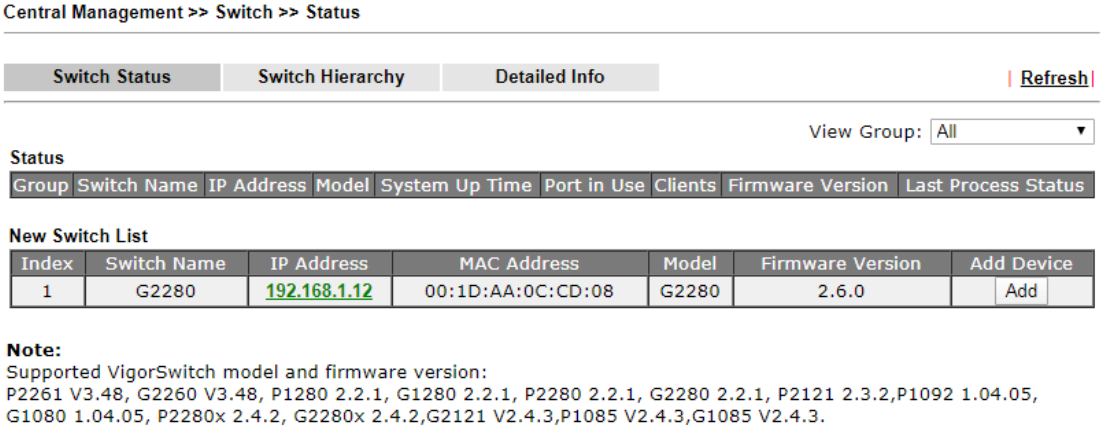
Such page displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch **connected to** Vigor2927 series.




Before checking the switch status, go to **Central Management>>External Device** to enable **External Device Auto Discovery**. Wait for the system to display available device(s).



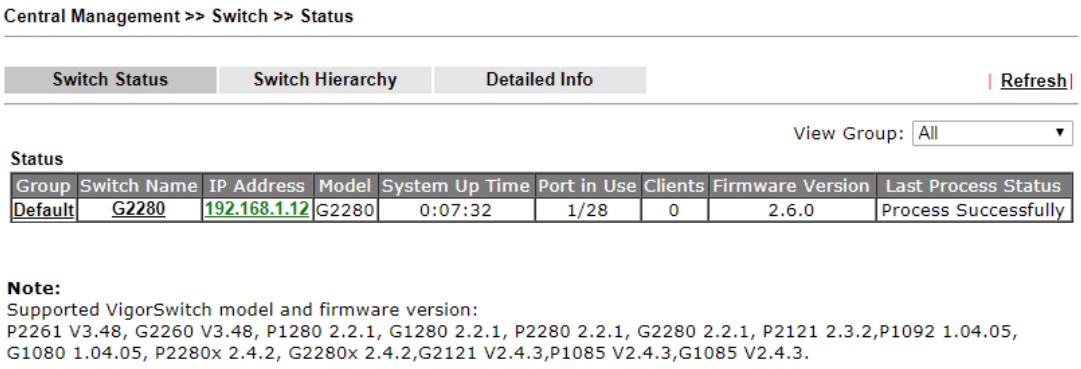
Later, open **Central Management>>Switch>>Status**. Available VigorSwitch to be managed by such router will be listed under the New Switch List.




**Info**

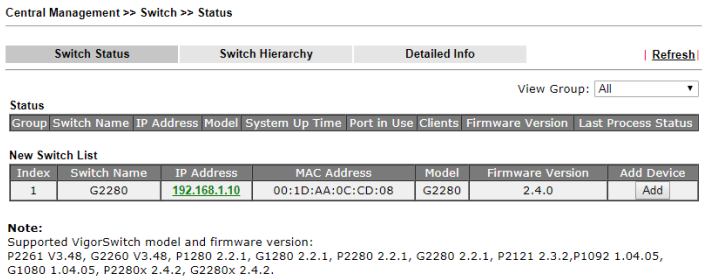
VigorSwitch listed below Status means the switch is managed by Viogr router; VigorSwitch listed below New Switch List means it is not managed by Vigor2927 yet.

Click **Add** to make the selected VigorSwitch to be managed by Vigor router.



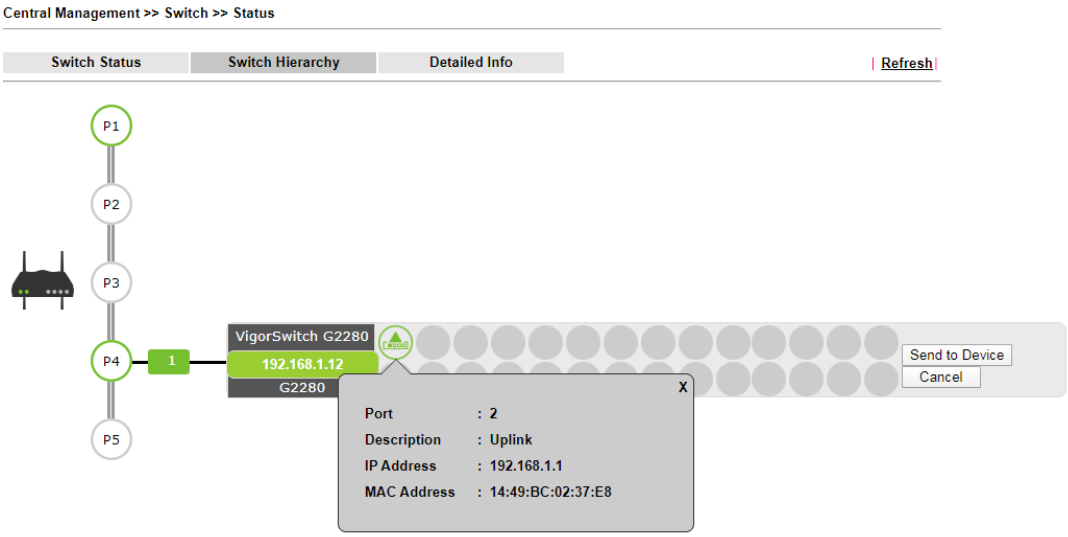

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Group** | Display the name link of the group.<br>You can click the link to modify the group settings if required. |
| **Switch Name** | Display the name link of VigorSwitch.<br>You can click the name link to access into the switch profile. |
| **IP Address** | Display the IP address of VigorSwitch. |
| **Model** | Display the model name of VigorSwitch. |
| **System Up Time** | Display the time accumulated since this Vigorwitch is powered up. |
| **Port in Use** | Display how many devices connected to VigorSwitch. |
| **Clients** | Display the number of LAN ports used in VigorSwitch. |
| **Firmware Version** | Display the firmware version that VigorSwitch current used. |

| | |
|---|---|
| **Add** | Such button will appear only when there is more than one switch connected to Vigor2927.<br>The one under New Switch List is allowed to be managed under current used group. Simply click **Add**.<br>  <br><br>It will be better to group VigorSwitch devices with the same model. |

## VI-7-1-2 Switch Hierarchy

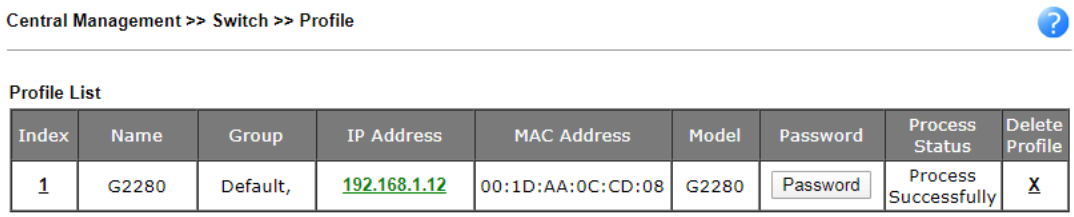
Such page displays the hierarchy of VigorSwitch(es) managed under Vigor2927.




Please note that, **Shutdown Port** is available for LAN port of VigorSwitch connects to a LAN device. When it is checked, after clicking **OK**, the network connection between that device and VigorSwitch will be terminated.

## VI-7-2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor2927 series. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.

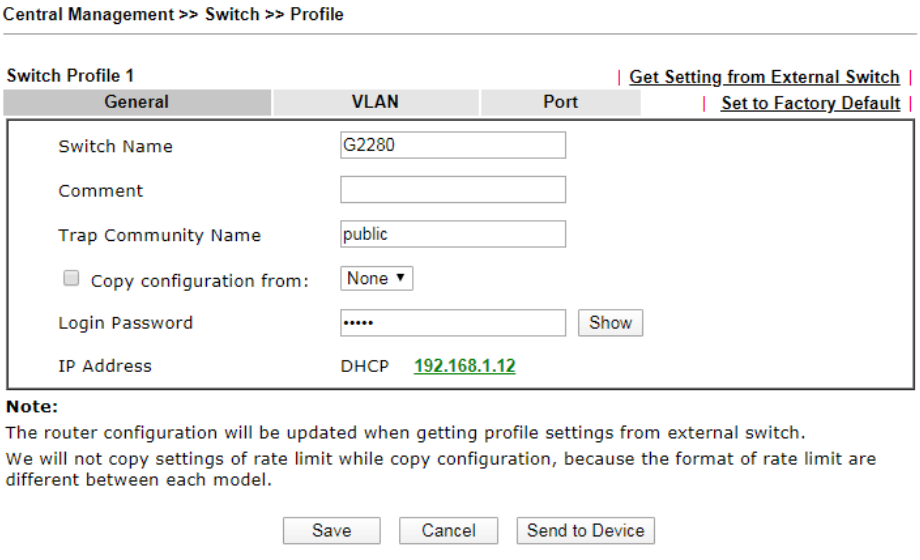



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Index** | Click the number link to access into the switch profile.<br>Note: Each connected VigorSwitch will have one setting profile. If there are many switches connected to Vigor2927, different index number will be used to represent different VigorSwitch. |
| **Name** | Display the user defined name of VigorSwitch. |
| **Group** | Display the group name of VigorSwitch(es). |
| **IP Address** | Display the IP address of VigorSwitch. |
| **MAC Address** | Display the MAC address of VigorSwitch. |
| **Model** | Display the model name of VigorSwitch. |
| **Password** | Click it to display the account information including username and password. |
| **Delete Profile** | Click the mark of "X" to delete the switch profile. |

To edit profile for the selected switch:

1. Click index number link (e.g. #1) to open the following page.

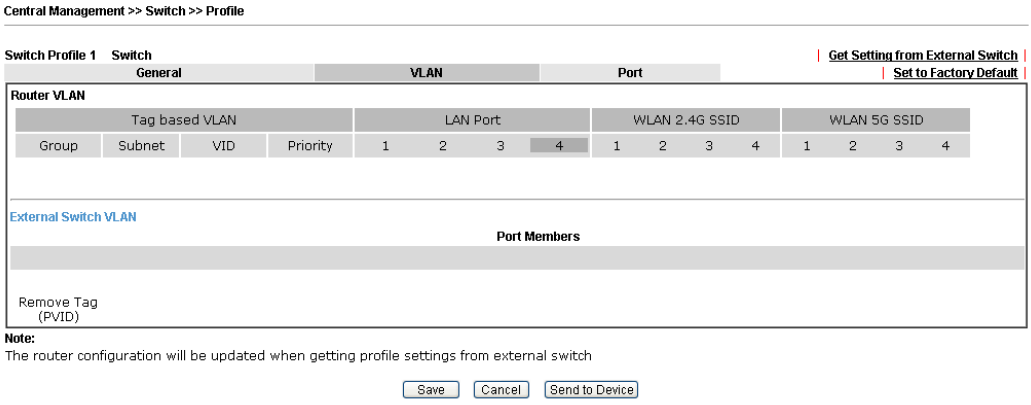


Available settings are explained as follows:

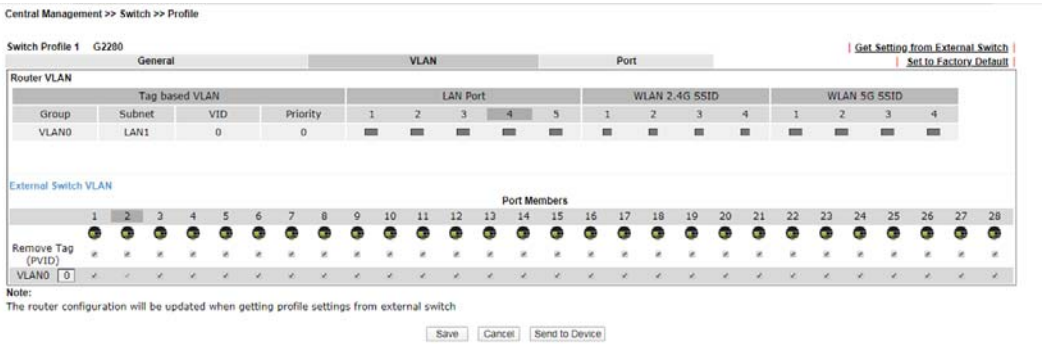
| Item | Description |
|---|---|
| **Switch Name** | Type a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor2927 seres. |
| **Comment** | Enter the text in such field if additional explanation for the switch is required. |
| **Trap Community Name** | Enter the text in such field as trap community. |
| **Copy configuration from** | Check the box to copy configuration from other device. Use the drop down list to choose the one you need.<br>Note, if there is only one VigorSwitch connected and managed by Vigor2927 series, then such field is unavailable. |
| **Login Password** | Display the original login password for the VigorSwitch.<br>However, if Group Password (in **Central Management >>Switch>>Group**) is configured with other string, then such field is not allowed to type any other password. And only the group password will be shown, instead. |
| **IP Address** | Display the dynamic IP address (of the connected switch) assigned by Vigor2927. |
| **Save** | Click it to save the settings. |
| **Cancel** | Click it to return to previous web page without saving the setting changes. |
| **Send to Device** | Click it to transfer the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately. |

2. After finished the settings, click **VLAN** tab to open following page.

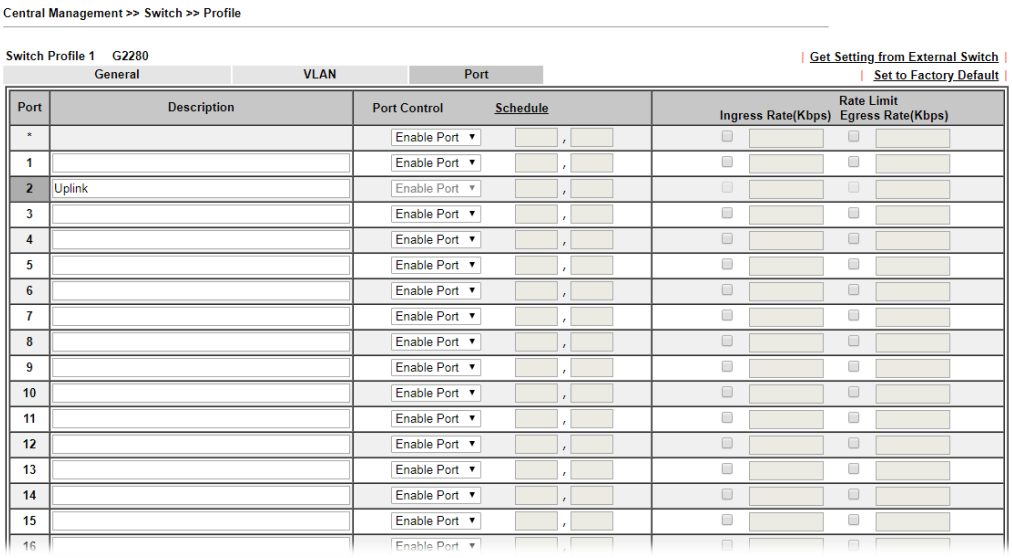
Blank page due to LAN>>VLAN not configured previously:



Setting page with **LAN>>VLAN** configured previously:



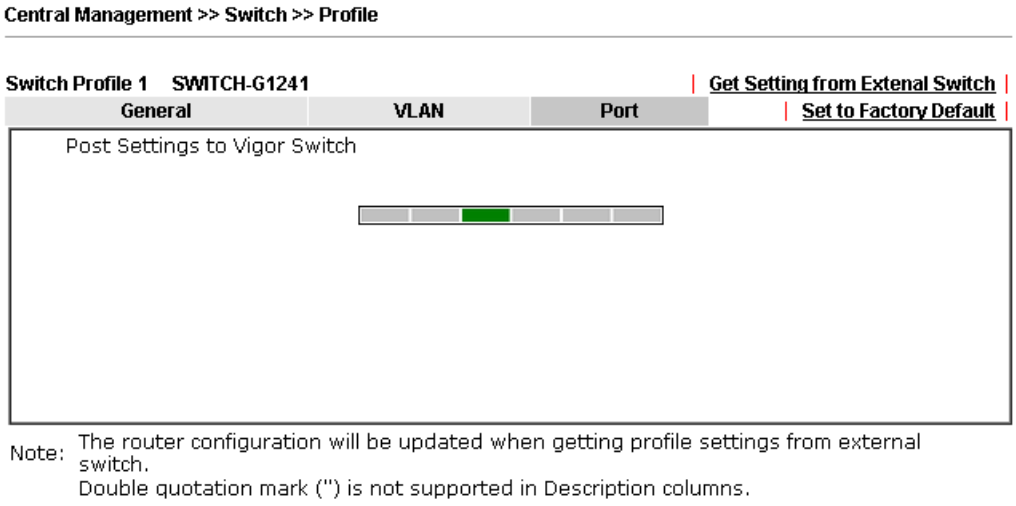

3. Click **Save** to save VLAN configuration. Then, click **Port** tab to access the following page:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Description** | If required, type a brief description to explain the device connected to VigorSwitch via the LAN port. |
| **Port Control** | **Disable Port** – The port (e.g, Port 2 in this case) which is used to connect VigorSwitch and Vigor2927 will not be shutdown by Vigor2927 series.<br>Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking Save, the network connection between that device and VigorSwitch will be terminated.<br>**Schedule** – Two sechule profiles can be specified here to force Vigor2927 executing specific action to VigorSwitch. |
| **Rate Limit** | Check the box for typing the ingress rate / egress rate for the selected VigorSwitch. After clicking **Save**, the value modified in this page will be written to VigorSwitch and enabled. |

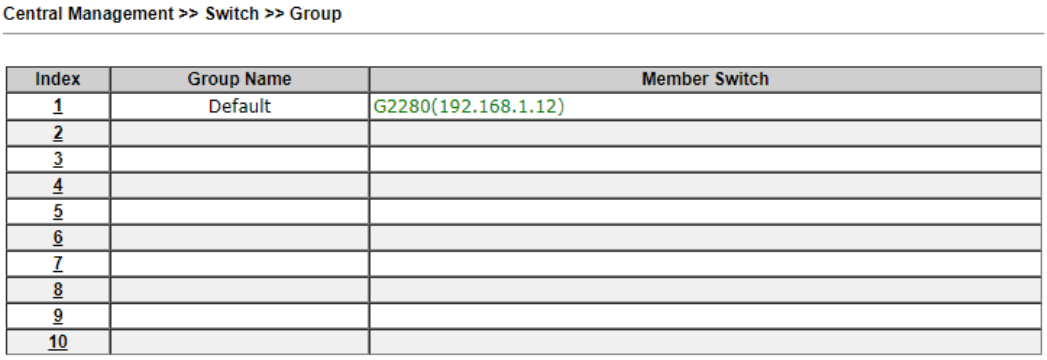
4. Click **Save** to save the changes and then click **Send to Device**. Settings will be sent to VigorSwitch immediately.



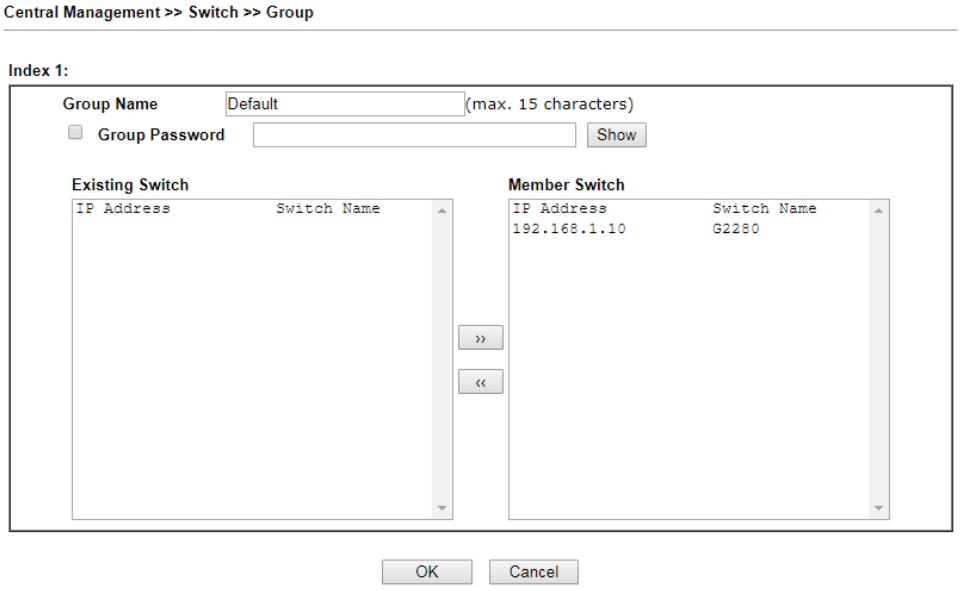

## VI-7-3 Group

Different switches can be classified into different group(s). Specifc password for a group can be defined and applied to every switch uder that group.

Through the common password setting, it is not necessary for the system administrator to remember various login passwords to access into different VigorSwitch devices.




Click any index number link to create a new switch group.

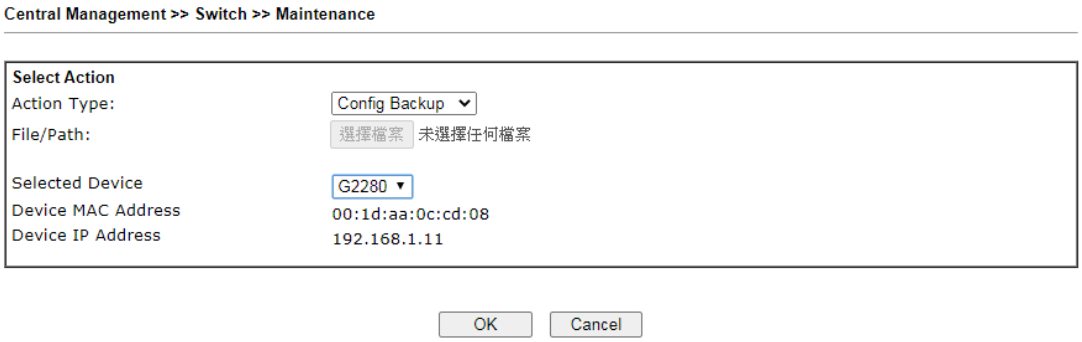


Available settings are explained as follows:

| Item | Description |
|---|---|
| **Group Name** | Type a name as the group name. Different switches can be classified within a group. |
| **Group Password** | Type a password that administrator can use to access into the managed VigorSwitch connecting to Vigor2927 series. All of the switches under the same group can be accessed into via such group password. |
| **Existing Switch** | Display all of the VigorSwitch devices connecting to Vigor2927. |
| **Member Switch** | Choose the switches you want to group and click the button ">>" to move the selected devices onto the field of Member Switch. Devices under Member Switch will be grouped under such group profile. |
| **OK** | Click it to save the configuration. |
| **Cancel** | Click it to exit the setting page without saving any change. |

## VI-7-4 Maintenance

Such feature can execute configuration backup, restore of selected VigorSwitch device(s) or reboot the VigorSwitch devices remotely or reset the VigorSwitch devices with factory default settings, without accessing into the web user interface of VigorSwitch respectively. It is convenient for system administrator to manage VigorSwitch devices.




Available settings are explained as follows:

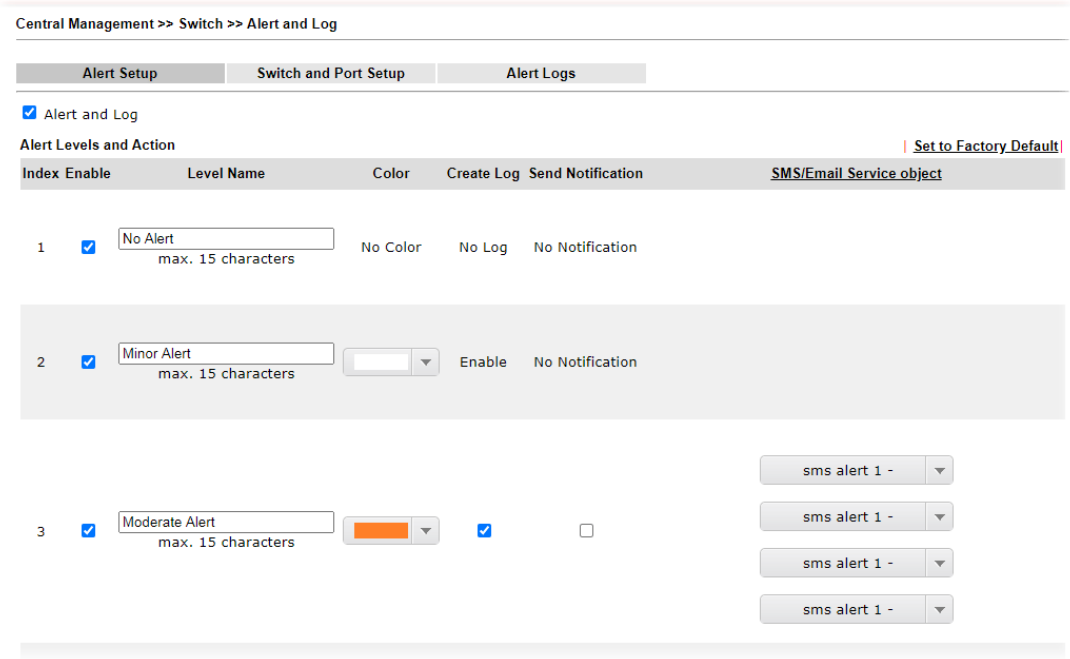
| Item | Description |
|---|---|
| **Select Action** | **Action Type** – Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor2927 to perform on VigorSwitch.<br>**File/Path** – Click the button to find out the required file. |
| **Selected Device** | Use the drop down list to specify a VigorSwitch. Then the MAC address and IP address related to the device will be displayed on this area. |
| **OK** | Click it to immediately perform the action (configuration backup, configuration restore, remote reboot and factory reset) on the device(s) listed in Selected Device. |
| **Cancel** | Click it to cancel the setting changes. |

## VI-7-5 Alert and Log

Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly. When the system detects an error, information of abnormal condition will be recorded to the database; or the system will send an alert to the specified device (via e-mail or SMS) to warn the user.

### VI-7-5-1 Alert Setup

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

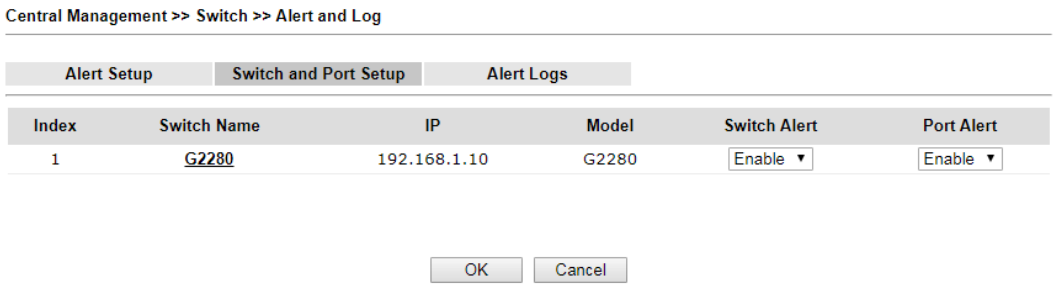



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Alert and Log** | Check it to enable this feature. |
| **Alert Levels and Action** | **Level Name –** Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined.<br>**Color** – Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed.<br>**Create Log** – Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default.<br>**Send Notification** – If it is checked, Vigor router's system will send notification to specified phone number via SMS.<br>**SMS/Email Service Object –** Choose the SMS object which will get the SMS from Vigor router. Up to 4 objects can be selected at one time. |

### VI-7-5-2 Switch and Port Setup

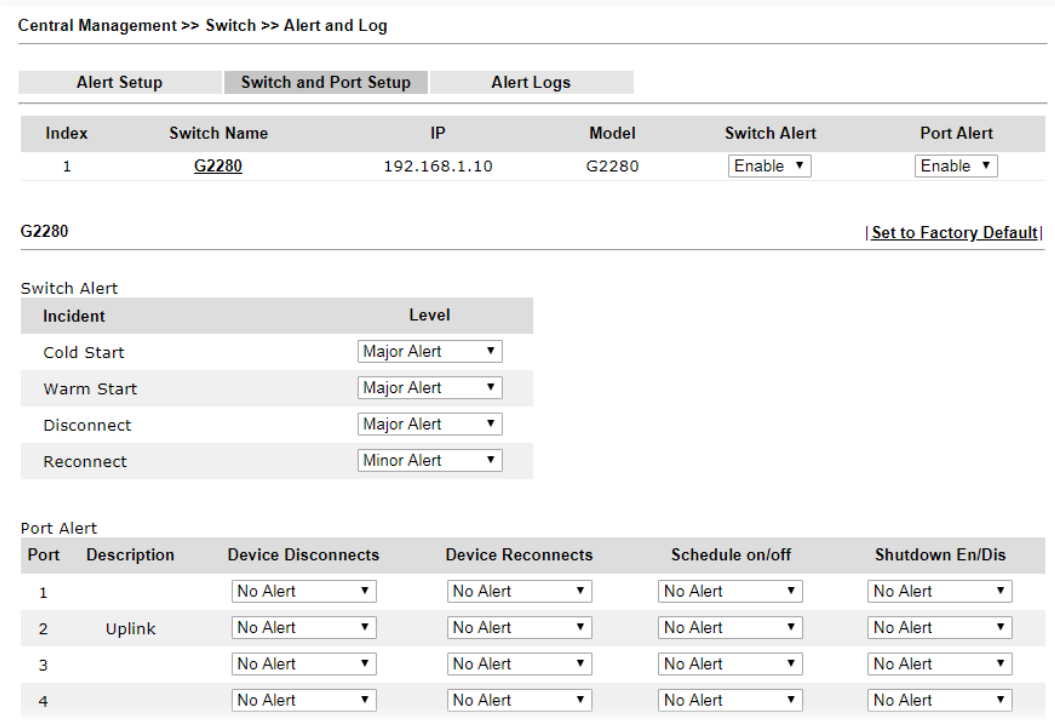
This page defines enabling switch alert and/or port alert for each switch.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Switch Alert** | **Enable –** Check it to enable alert mechanism for VigorSwitch. |
| **Port Alert** | **Enable -** Check it to enable alert mechanism for each port of VigorSwitch. |

Click the Switch Name link (e.g., G2280 in this case) to get detailed settings.



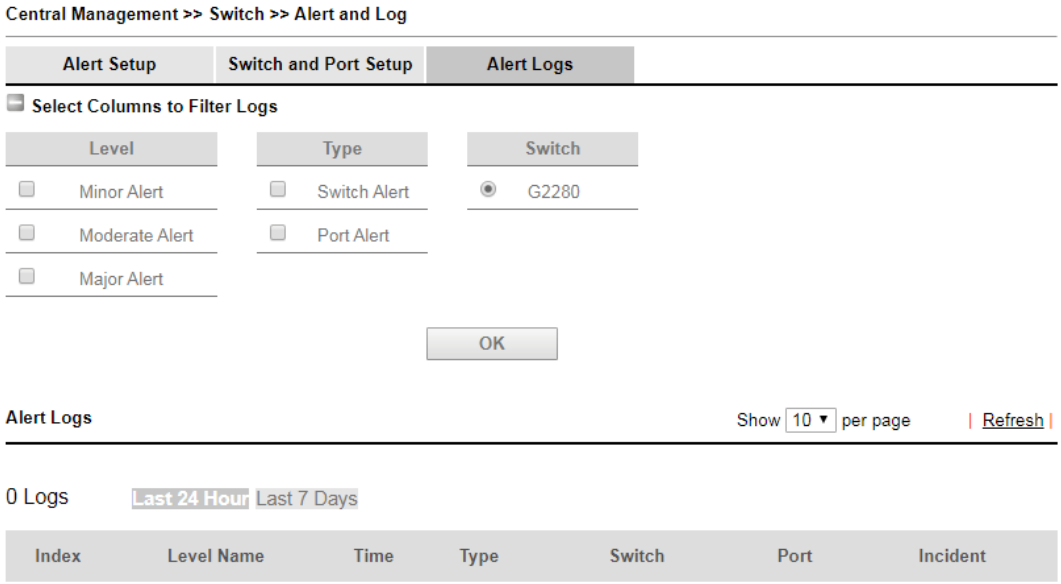

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Switch Alert** | When VigorSwitch encounters the following alert events, alert mechanism will perform corresponding actions based on the servity level of the incident encountererd.<br>**Incident –** At present, **Cold Start, Warm Start, Disconnect and Reconnect** will be treated as alert events.<br>**Level –** Specify the severity level for each incident. To defined more severity level for choosing in this page, simply open **Central Management>>Switch>>Alert and Log** and click **Alert Setup**. |
| **Port Alert** | **Port –** Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this page. Each |

| | |
|---|---|
| | port can be confgiured with different alert level for diffent alert event. |

## VI-7-5-3 Alert Logs

The user can get the information by filtering the collective information based on the conditions specified in this page.

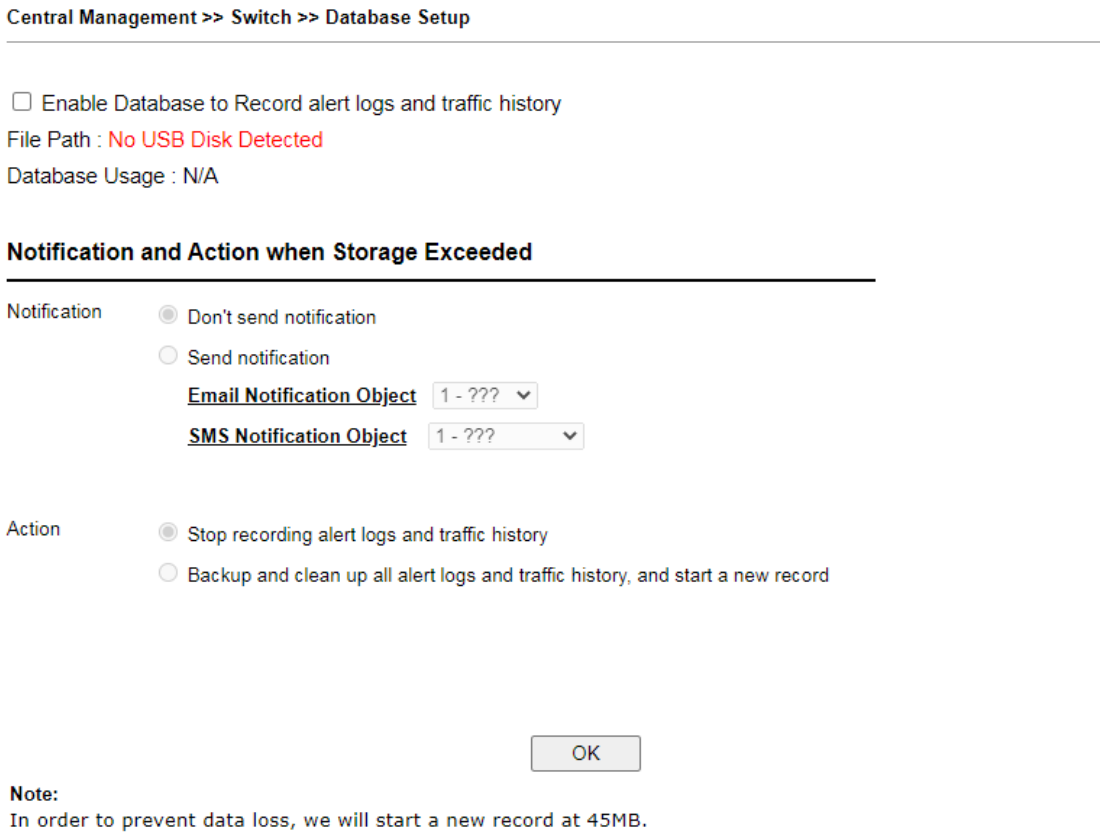



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Select Columns to Filter Logs** | **Level –** The alert can be divided into several levels, Minor Alert, Moderate Alert and Major Alert. Check the one(s) you want to check in Alert Logs list.<br>**Type –** Check the type (switch / port) of the log to be displayed in Alert Logs list.<br>**Switch –** Switch(es) connecting to Vigor router will be shown in this area. Click the one you need.<br>**OK –** Click it to save the configuration.<br>Log related to the items selected above will be shown in Alert Logs list. |
| **Alert Logs** | This area displays logs (level name, time, type, switch, port, and incident) related to VigorSwitch managed by Vigor router. |

## VI-7-6 Database Setup

The database of switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of switch.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Database to Record alert logs and traffic history** | Check the box to make the database (in USB disk) record the alert logs and traffic history. |
| **Notification and Action when Storage Exceeded** | |
| **Notification** | **Don't send notification** – No notification will be sent out when there is no capacity for storage in USB.<br>**Send notification** – A notification will be sent out when there is no capacity for storage in USB. |
| **Action** | **Stop recording alert logs and traffic history** – When the capacity of log is full, the system will stop recording.<br>**Backup and clean up all alert logs and traffic history, and start a new record** - Only the newest events will be recorded by the system. |

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

## VI-7-7 Support List

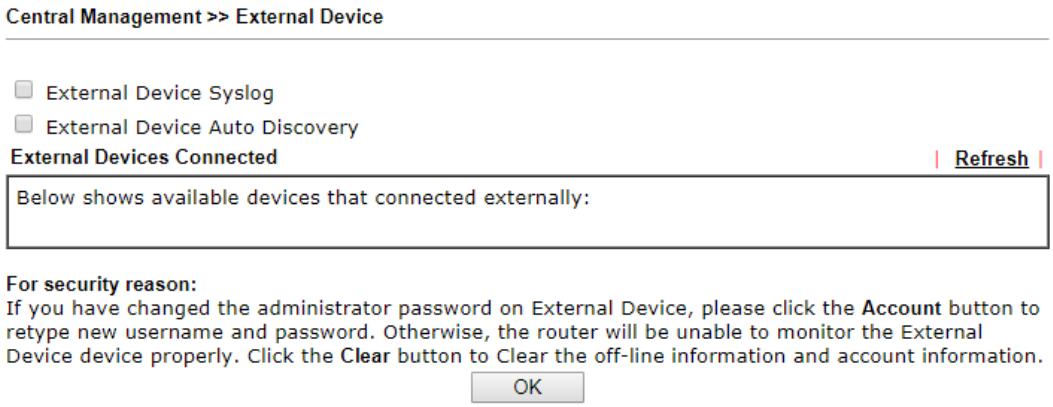
This page lists all models of VigorSwitch which can be managed by Vigor2927 via **Central Management>>Switch**.

**Central Management >> Switch >> Support List**

| Model | Status | Firmware Version |
|---|---|---|
| Vigor Switch P2261 | V | v3.48 |
| Vigor Switch G2260 | V | v3.48 |
| Vigor Switch P1280 | V | 2.2.1 |
| Vigor Switch G1280 | V | 2.2.1 |
| Vigor Switch P2280 | V | 2.2.1 |
| Vigor Switch G2280 | V | 2.2.1 |
| Vigor Switch P2121 | V | 2.3.2 |
| Vigor Switch G2121 | V | 2.4.3 |
| Vigor Switch P1092 | V | 1.04.05 |
| Vigor Switch G1080 | V | 1.04.05 |
| Vigor Switch P2500 | V | 2.4.1 |
| Vigor Switch G2500 | V | 2.4.1 |
| Vigor Switch P2280x | V | 2.4.2 |
| Vigor Switch G2280x | V | 2.4.2 |
| Vigor Switch P1085 | V | 2.4.3 |
| Vigor Switch G1085 | V | 2.4.3 |

# VI-8 Central Management (External Devices)

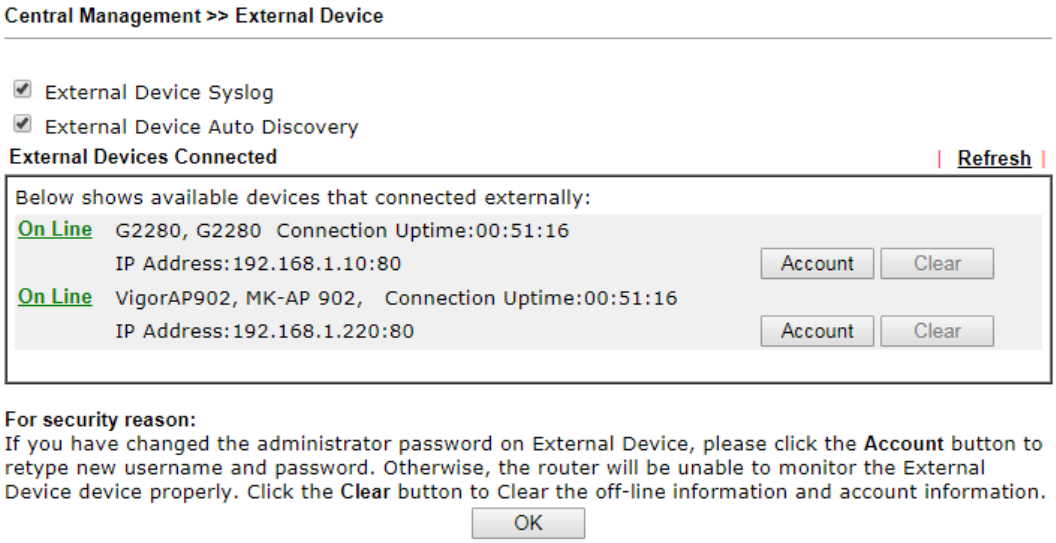
Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **External Device Syslog** | Check this box to display information of the detected device on Syslog. |
| **External Device Auto Discovery** | Check this box to detect the external device automatically and display on this page. |

From this web page, check the box of **External Device Auto Discovery** and click **OK**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.



When you finished the configuration, click **OK** to save it.

| | |
|---|---|
| **Info** | Only DrayTek products can be detected by this function. |

This page is left blank.

# Part VII Others



Objects Settings

Define objects such as IP address, service type, keyword, file extension and others. These pre-defined objects can be applied in CSM.



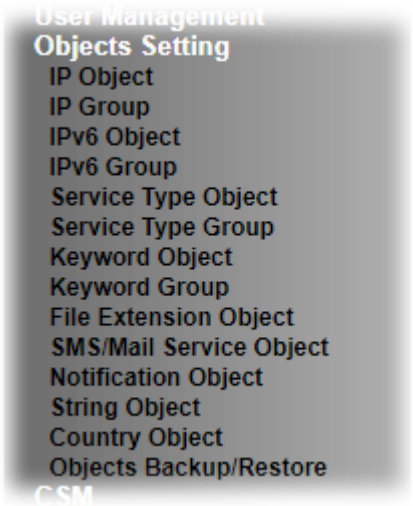
USB

USB device connected on Vigor router can be regarded as a server or WAN interface. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications.

# VII-1 Objects Settings

This section allows the creation of objects and object groups from IP addresses, service types, keywords, file extensions, SMS and email recipients, and notification types. Once set up, these objects can be applied to firewall and content management rules.

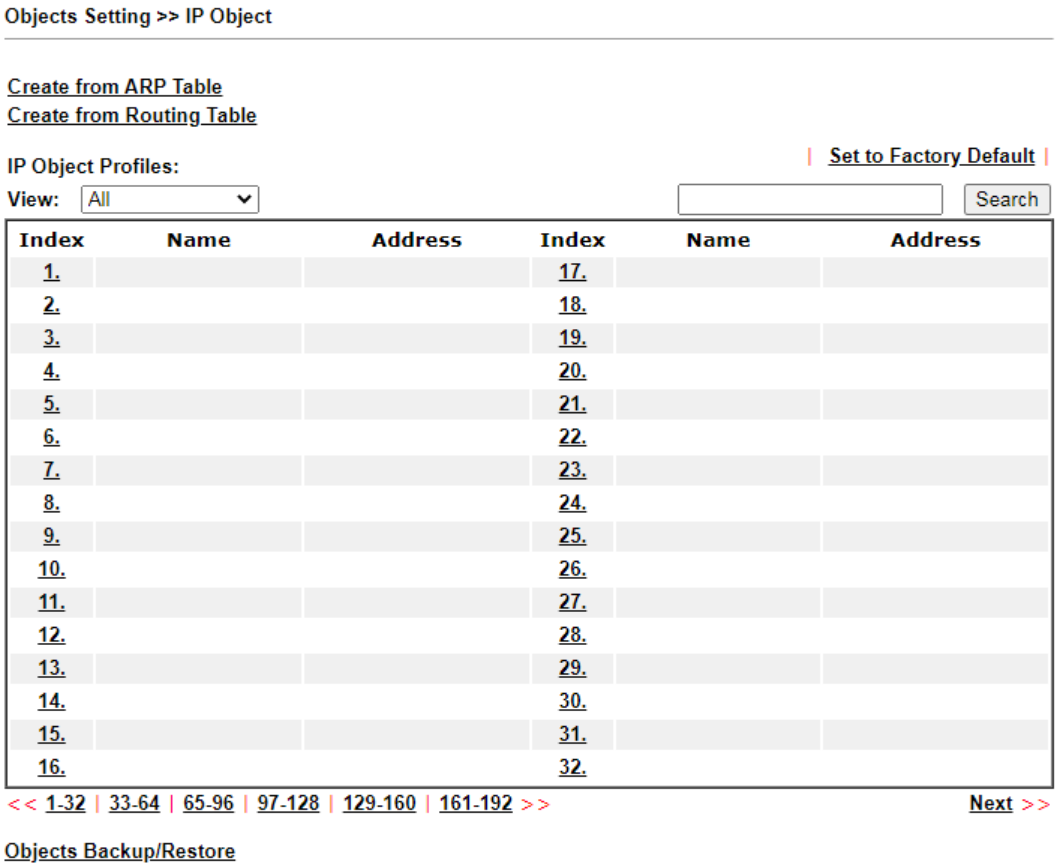
# Web User Interface




## VII-1-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group for applying it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

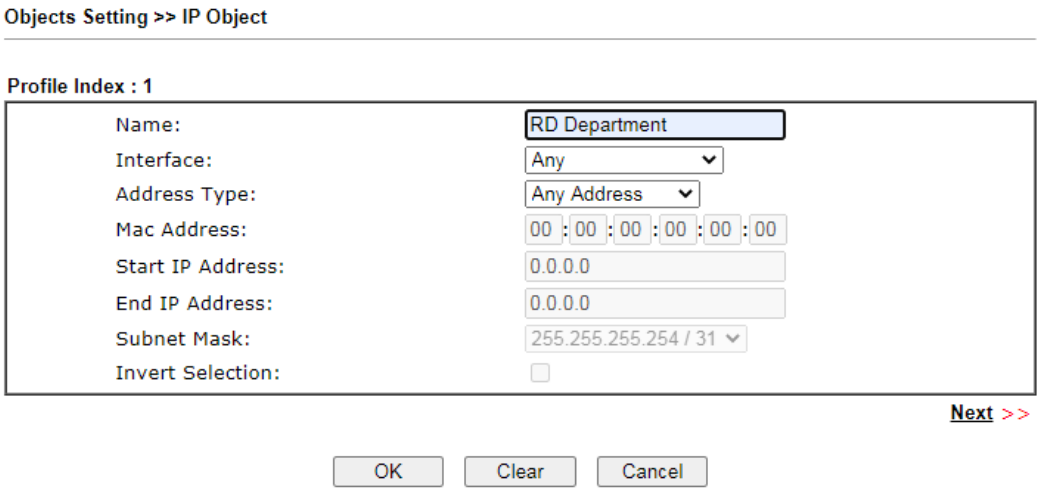
Up to 192 IP Objects can be created.



Available settings are explained as follows:

| Item | Description |
|---|---|
| **View** | Use the drop down list to choose a type (Single Address, Range Address, Subnet Address, Mac Address or all) that IP object with the selected type will be shown on this page. |
| **Set to Factory Default** | Clear all profile settings. |
| **Search** | Type a string of the IP object that you wan to search. |
| **Index** | Profile number of the IP object. |
| **Name** | Name of the object. |
| **Address** | Display the IP address configured for the object profile. |
| **Objects Backup/Restore** | Click it to backup or restore the IP object. |

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

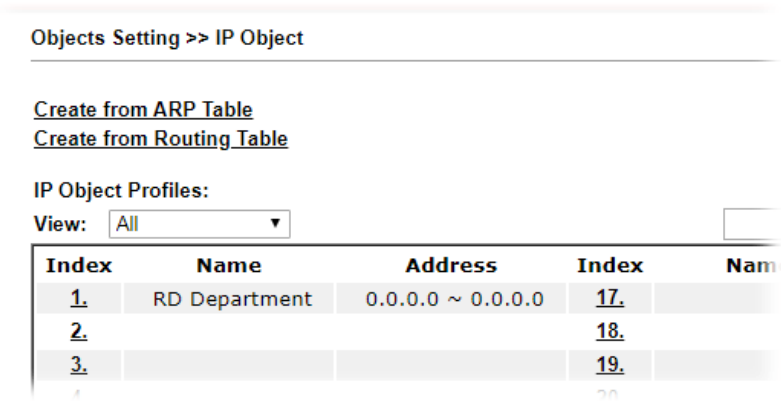



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Interface** | The network interface on which the IP address or addresses are to be found.<br>**Any** – All network interfaces.<br>**LAN/DMZ/RT/VPN** – All network interfaces except WAN.<br>**WAN** – Only WAN interfaces. |
| **Address Type** | Type of Addresses.<br>**Any Address** – Object covers all IP addresses.<br>**Single Address** – Object covers one IP address.<br>**Range Address** – Object covers a range of IP addresses.<br>**Subnet Address** – Object covers a range of IP addresses specified in subnet notation.<br>**Mac Address** – Object contains a MAC address. |
| **MAC Address** | Enter MAC address of the network device, if Address Type is Mac Address. |

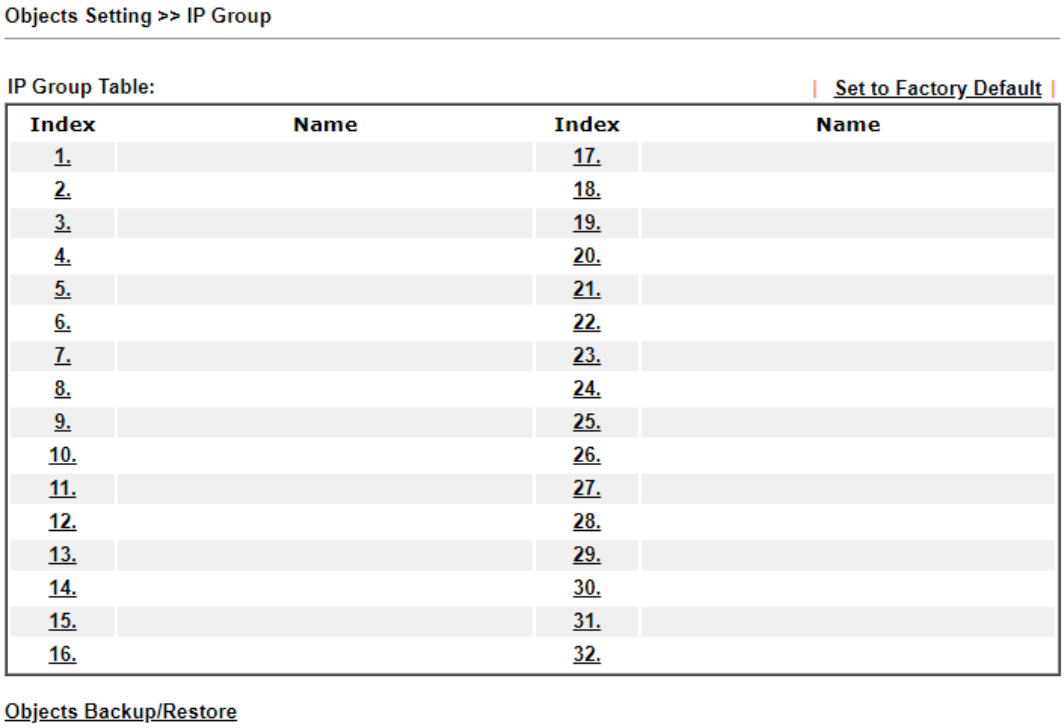
| | |
|---|---|
| **Start IP Address** | Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address. |
| **End IP Address** | Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address. |
| **Subnet Mask** | Enter subnet mask, if Address type is Subnet Mask. |
| **Invert Selection** | If selected, all addresses except the ones entered above will be used. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.



## VII-1-2 IP Group

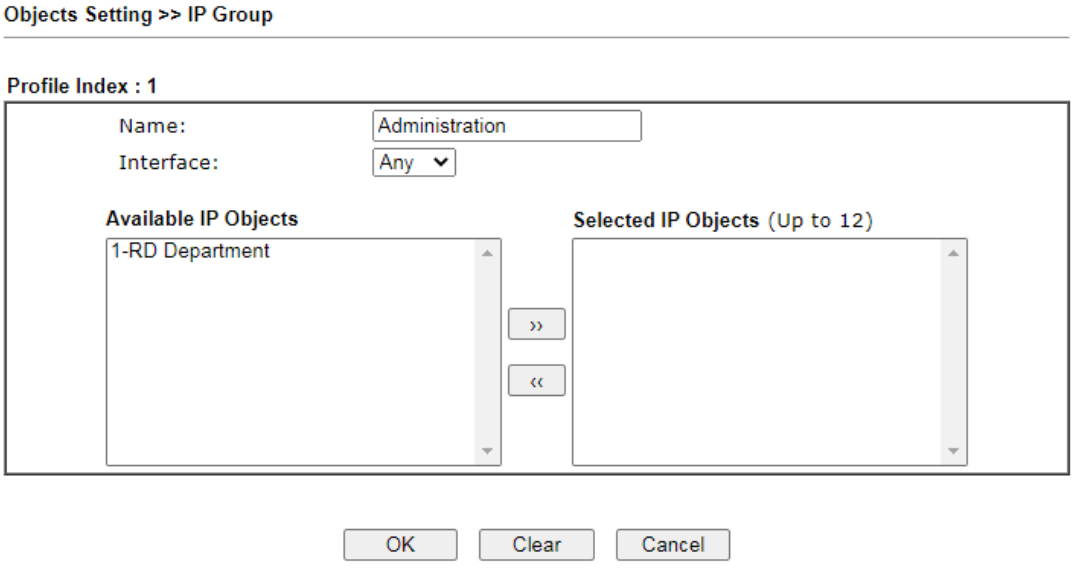
Multiple IP Objects can be placed into an IP Group.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the IP group object. |

To set up a profile, click its index to bring up the configuration page.



Available settings are explained as follows:

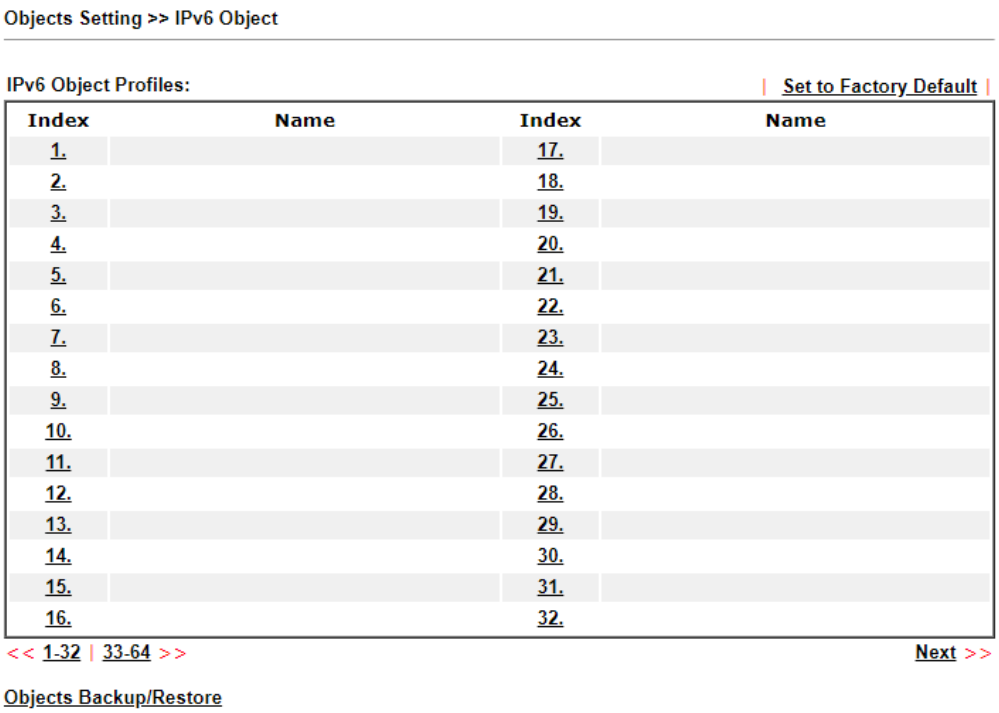
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Interface** | Select WAN, LAN or Any to filter IP objects. |
| **Available IP Objects** | All available IP objects that are associated with the selected interface. |
| **Selected IP Objects** | IP objects that have been added to this profile. |

To add an IP object to the IP Group, select it under Available IP Objects, then click the **>>** button. To remove an IP object from the IP Group, select it under Selected IP Objects, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP group, click **Clear**.

## VII-1-3 IPv6 Object

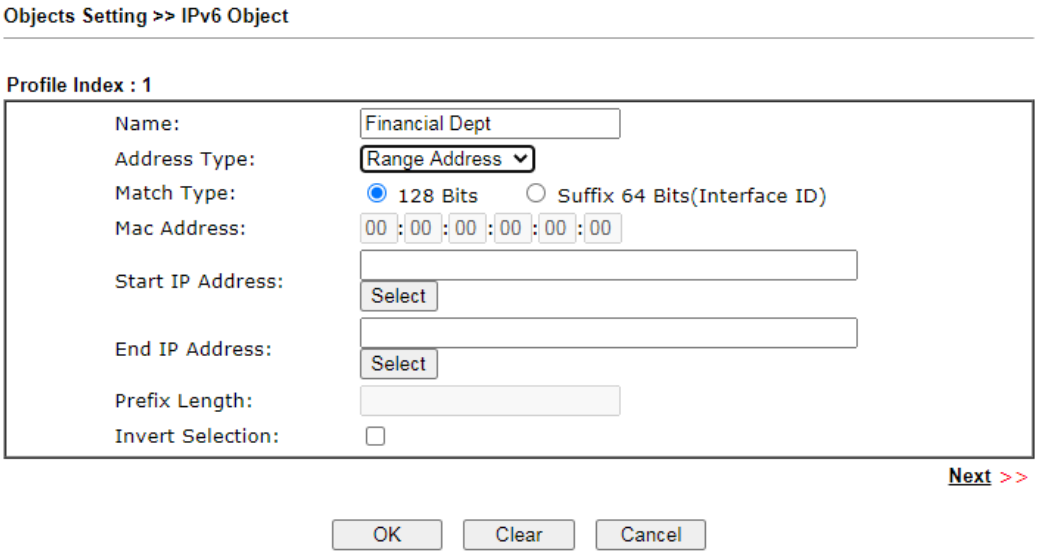
Up to 64 IPv6 Objects can be created.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the IPv6 object. |

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



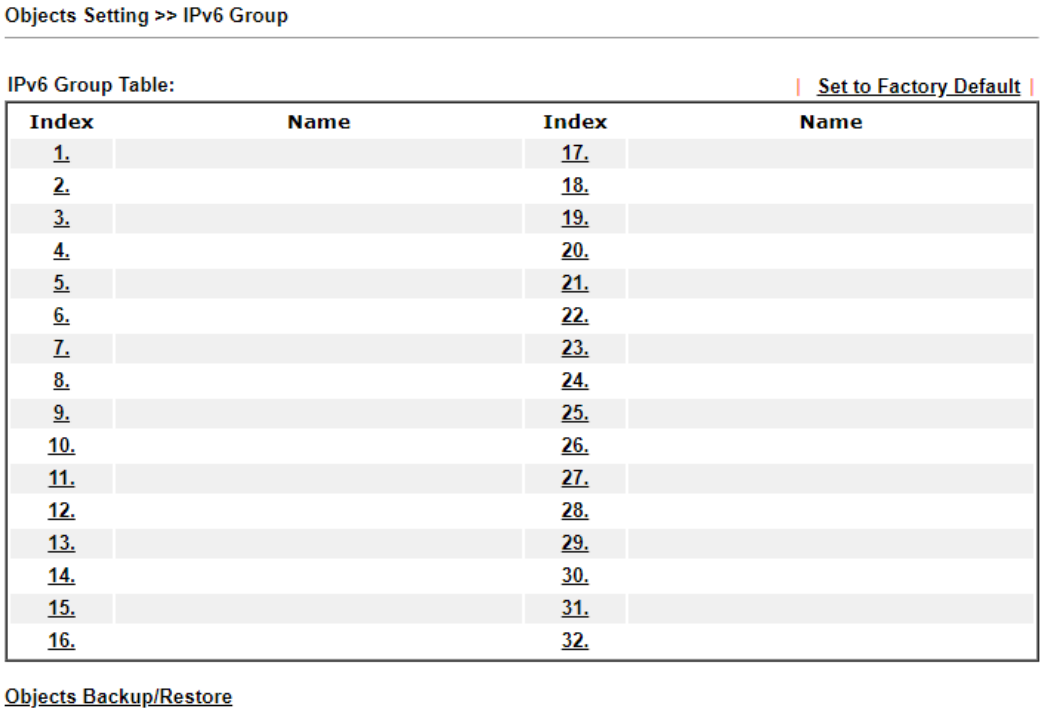

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Address Type** | Type of Addresses.<br>**Any Address** - Object covers all IPv6 addresses.<br>**Single Address** - Object covers one IPv6 address.<br>**Range Address** - Object covers a range of IPv6 addresses.<br>**Subnet Address** - Object covers a range of IPv6 addresses specified in subnet notation.<br>**Mac Address** - Object contains a MAC address. |
| **Match Type** | Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address. |
| **Mac Address** | Enter MAC address of the network device, if Address Type is Mac Address. |
| **Start IP Address** | Enter beginning IP address, if Address Type is one of Single Address, Range Address and Subnet Address. |
| **End IP Address** | Enter ending IP address, if Address type is one of Single Address, Range Address and Subnet Address. |
| **Prefix Length** | Enter IPv6 prefix length, if Address type is Subnet Address. |
| **Invert Selection** | If selected, all addresses except the ones entered above will be used. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the IPv6 object, click **Clear**.

## VII-1-4 IPv6 Group

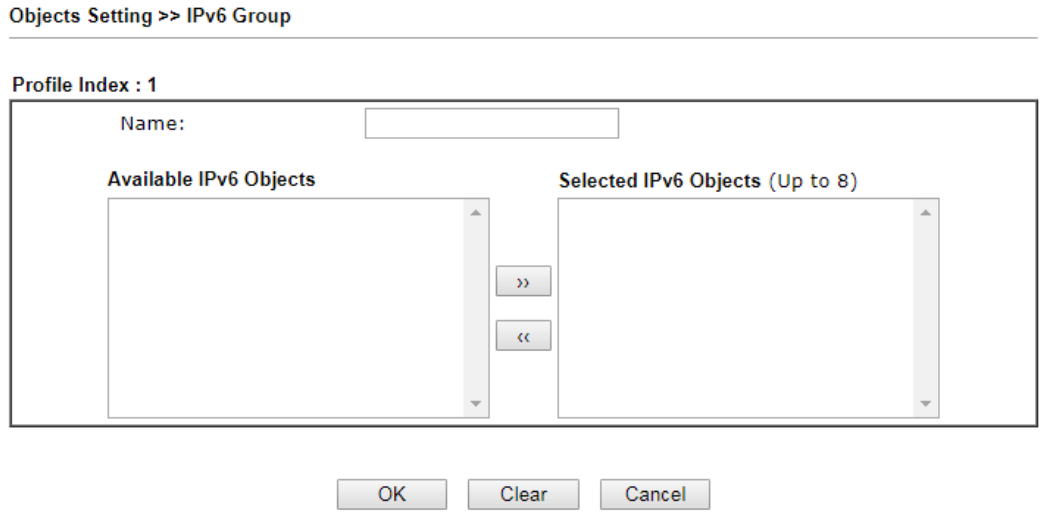
Multiple **IPv6 Objects** can be placed into an **IPv6 Group**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the IPv6 group. |

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




Available settings are explained as follows:

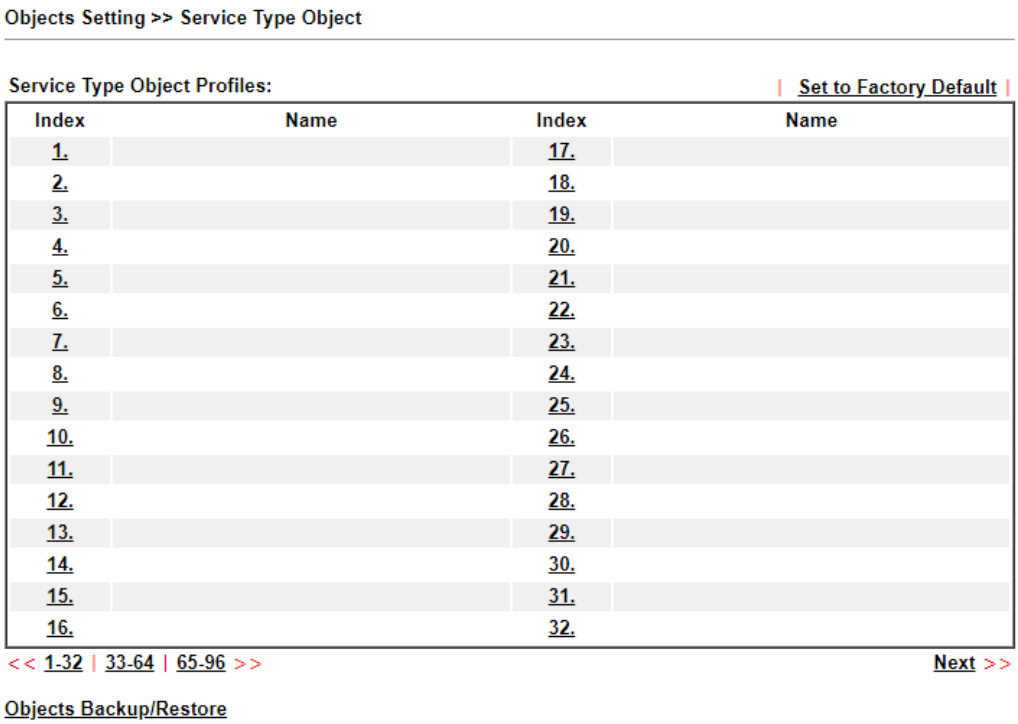
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Available IPv6 Objects** | All available IP objects that are associated with the selected interface. |
| **Selected IPv6 Objects** | IPv6 objects that have been added to this profile. |

To add an IPv6 object to the IPv6 Group, select it under Available IPv6 Objects, then click the >> button. To remove an IPv6 object from the IPv6 Group, select it under Selected IPv6 Objects, then click the << button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IPv6 group, click **Clear**.

## VII-1-5 Service Type Object

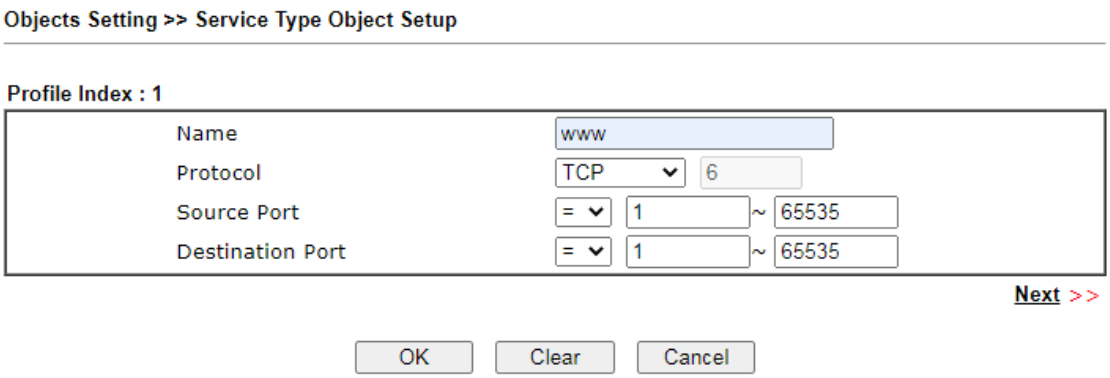
Up to 96 Service Type Objects can be created.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the service type object. |

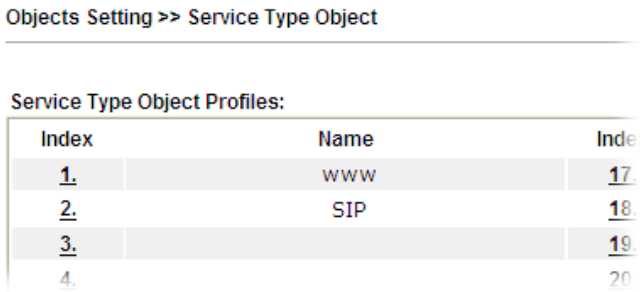
To set up a profile, click the profile number under Index column to bring up the configuration page.




Available settings are explained as follows:

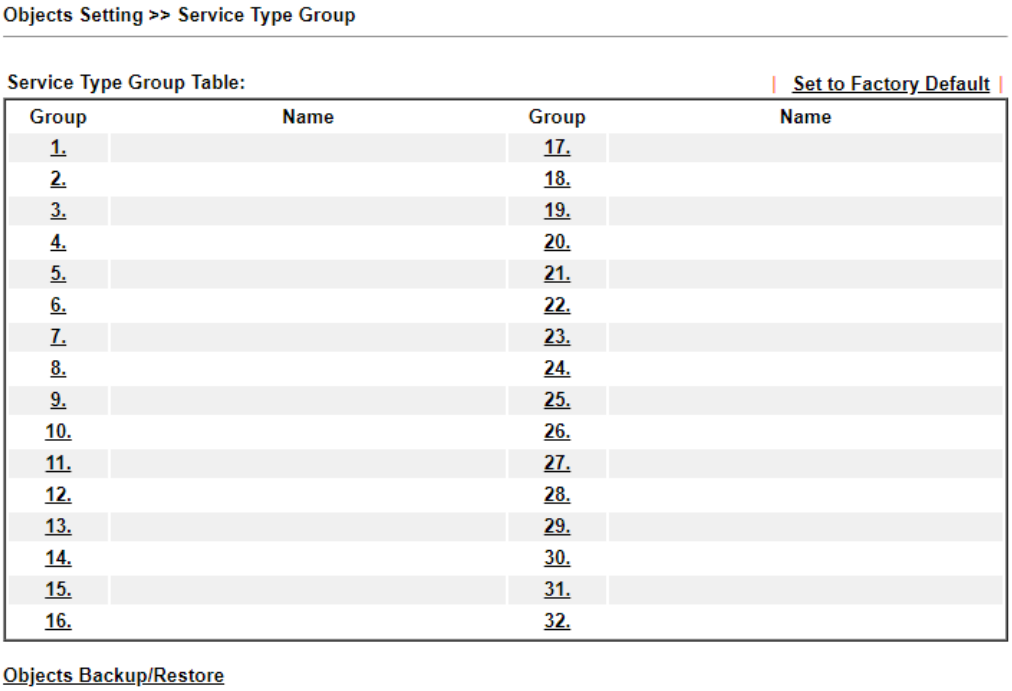
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Protocol** | Protocol(s) to which this profile applies.<br>**Any** – All protocols.<br>**ICMP** – Internet Control Message Protocol<br>**IGMP** – Internet Group Management Protocol<br>**TCP** – Transmission Control Protocol<br>**UDP** – User Datagram Protocol<br>**TCP/UDP** – Transmission Control Protocol and User Datagram Protocol<br>**Other** – Other protocols not listed above. Enter protocol number in the textbox. |
| **Source/Destination Port** | When protocol selected includes TCP or UDP, the source and destination ports can be specified.<br>= – any port that falls within the specified range.<br>!= – any port that falls outside of the specified range.<br>– all port numbers that are greater than the specified value.<br>< – all port numbers that are smaller than the specified value. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type object, click **Clear**.



## VII-1-6 Service Type Group

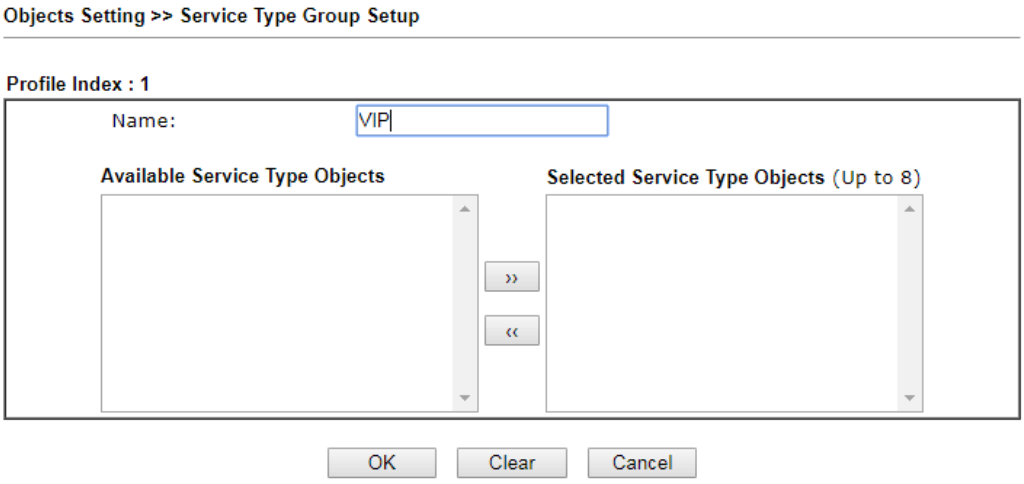
Multiple **Service Type Objects** can be placed into a **Service Type Group**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the service type group object. |

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




Available settings are explained as follows:

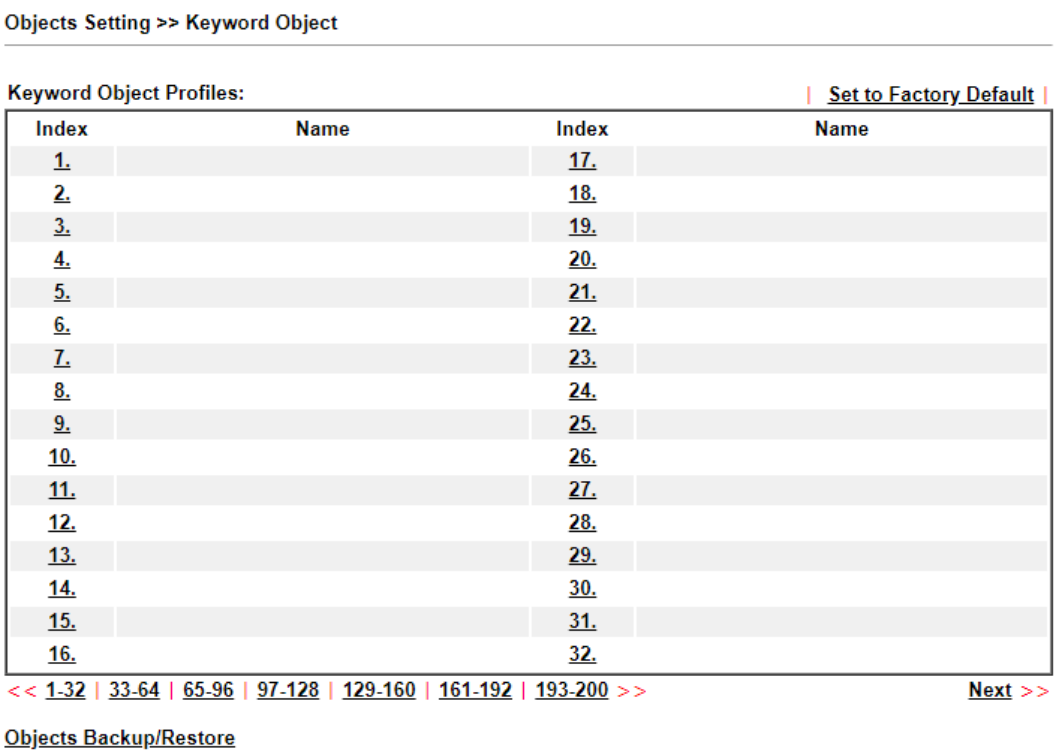
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Available Service Type Objects** | All available service type objects. |
| **Selected Service Type Objects** | Service type objects that have been added to this profile. |

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the **>>** button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current service type group, click **Clear**.

## VII-1-7 Keyword Object

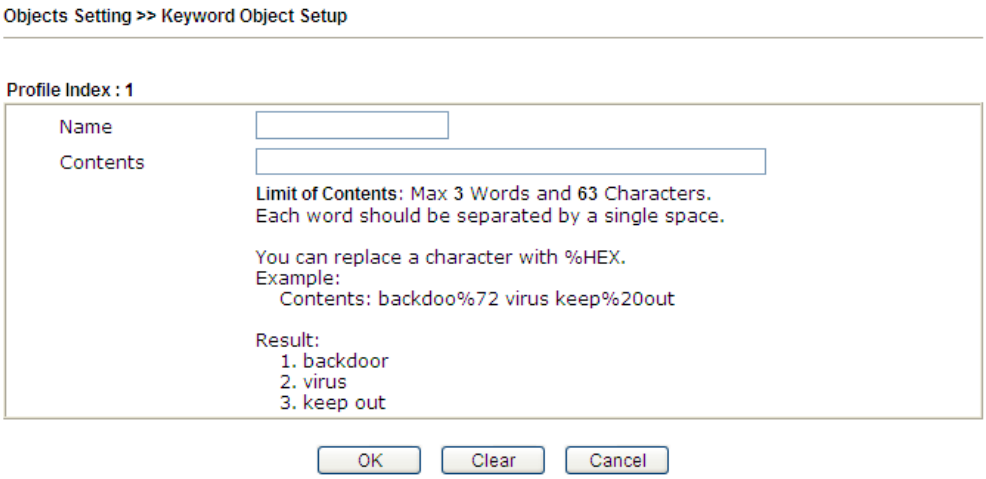
200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **Web Content Filter Profile**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the keyword object. |

To set up a profile, click its index to bring up the configuration page.




Available settings are explained as follows:

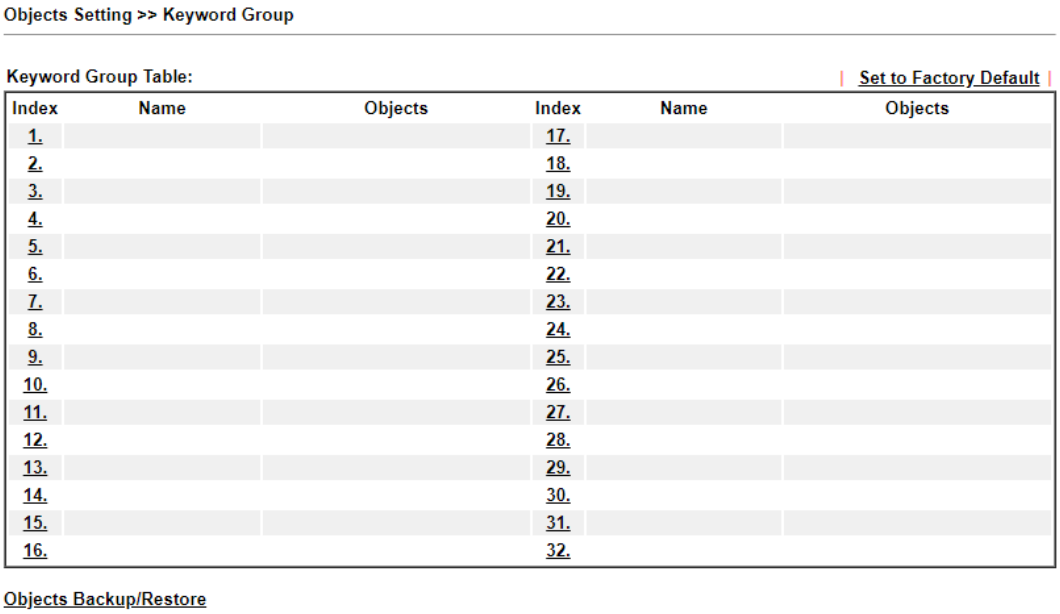
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Contents** | Keywords to be matched. Up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. For key phrases that contain spaces, replace spaces with the sequence %20. For example, the phrase “keep out” is to be entered as “keep%20out”. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword object, click **Clear**.

## VII-1-8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.

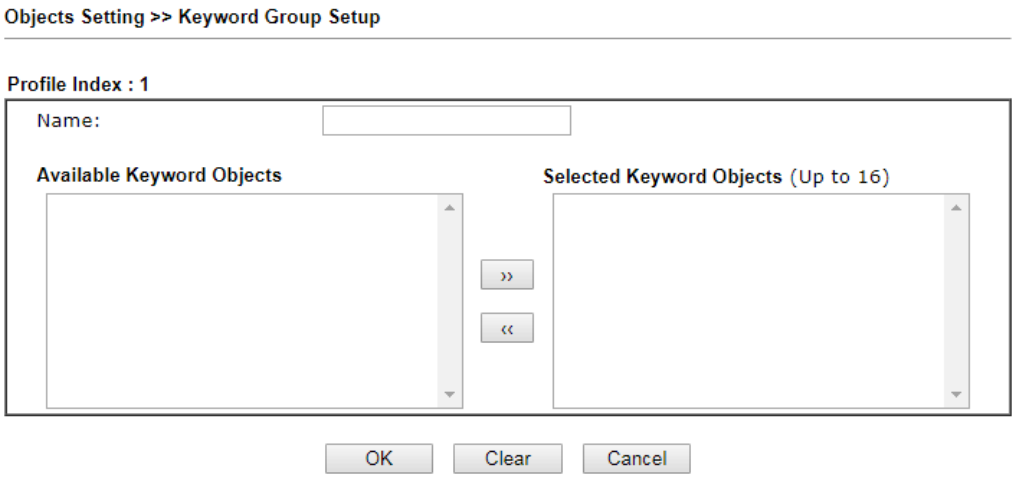
Keyword groups can be chosen as blacklists or white lists in **CSM >>URL /Web Content Filter Profile**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects** | Display the keyword objects under this group. |
| **Objects Backup/Restore** | Click it to backup or restore the keyword group. |

To set up a profile, click its index to bring up the configuration page.




Available settings are explained as follows:

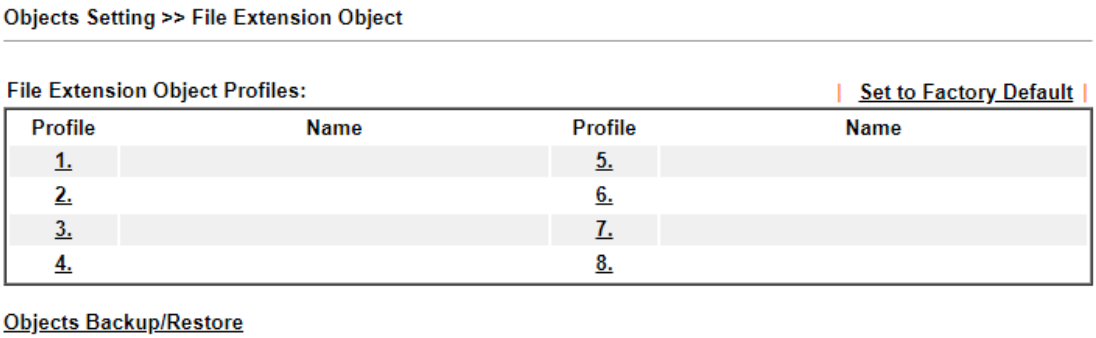
| Item | Description |
|---|---|
| **Name** | Name that identifies this profile. Maximum length is 15 characters. |
| **Available Keyword Objects** | All keyword objects that have not been added to this profile. |
| **Selected Keyword Objects** | Keyword objects that have been added to this profile. |

To add a Service Type Object to the Service Type Group, select it under **Available Service Type Objects**, then click the **>>** button. To remove a Service Type Object to the Service Type Group, select it under **Selected Service Type Objects**, then click the **<<** button.

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current keyword group, click **Clear**.

## VII-1-9 File Extension Object

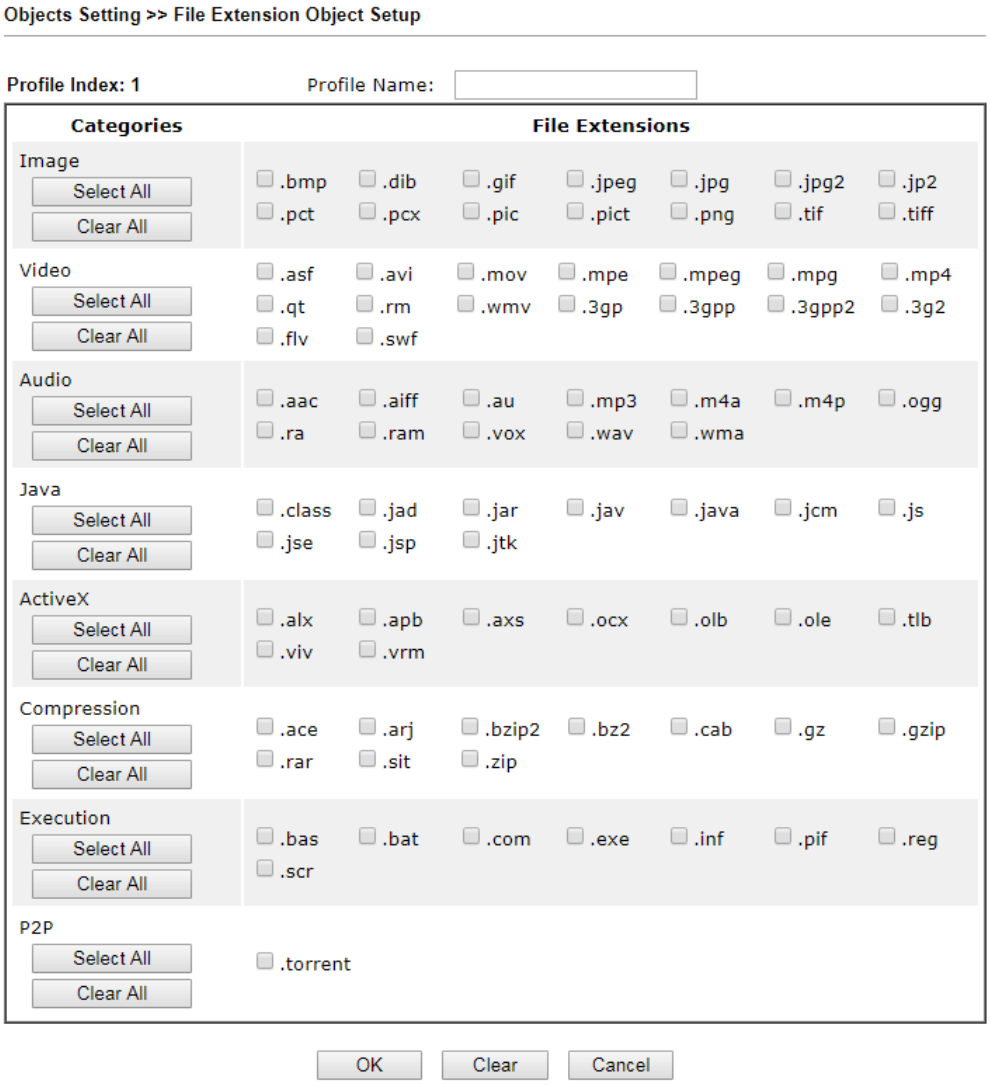
Up to 8 File Extension Objects can be set up for use with **CSM>>URL Content Filter**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the file extension object. |

To set up a profile, click its index to bring up the configuration page.




Available settings are explained as follows:

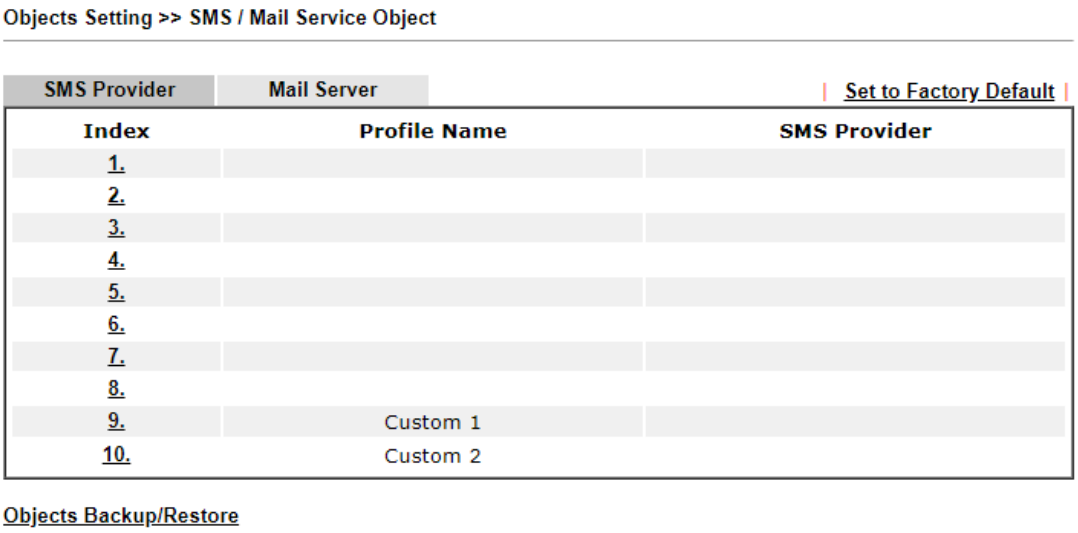
| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. Maximum length is 7 characters. |
| **Select All** | Selects all file extensions for the category. |
| **Clear All** | Deselects all file extensions for the category. |

Select the file extensions you wish to be included in the profile. To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current file extension object, click **Clear**.

# VII-1-10 SMS/Mail Service Object

## SMS Service Object

Up to 10 SMS Service Objects can be set up for use with **Application>>SMS Alert Service**.

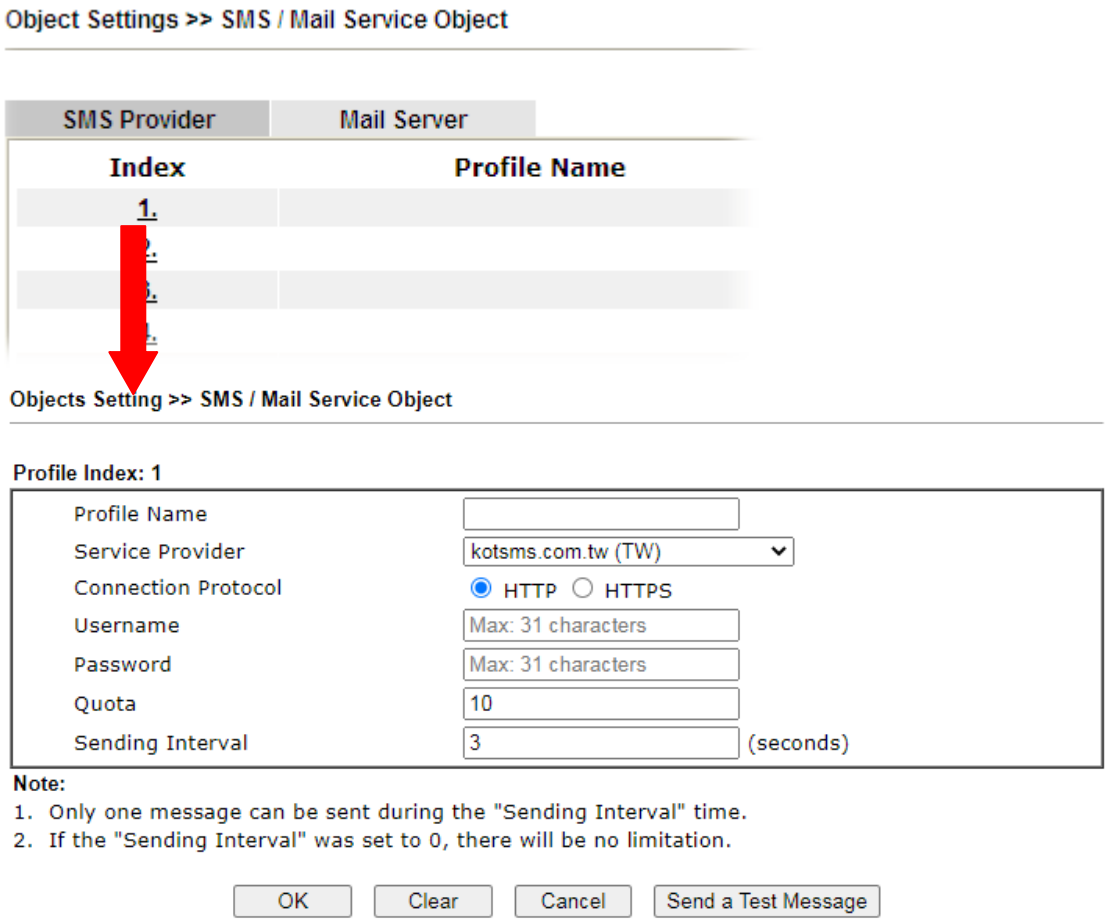



Each item is explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |
| **Profile Name** | Name that identifies the profile. |
| **SMS Provider** | The SMS provider selected for the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the service object. |

+

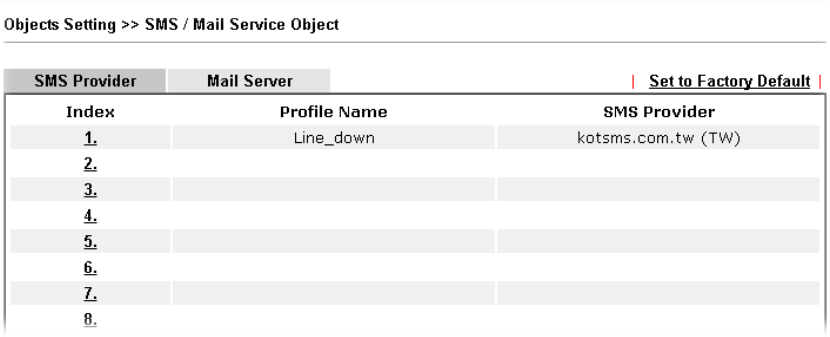
To set up a profile, click the **SMS Provider** tab, and then click its index to bring up the configuration page.




Available settings are explained as follows:

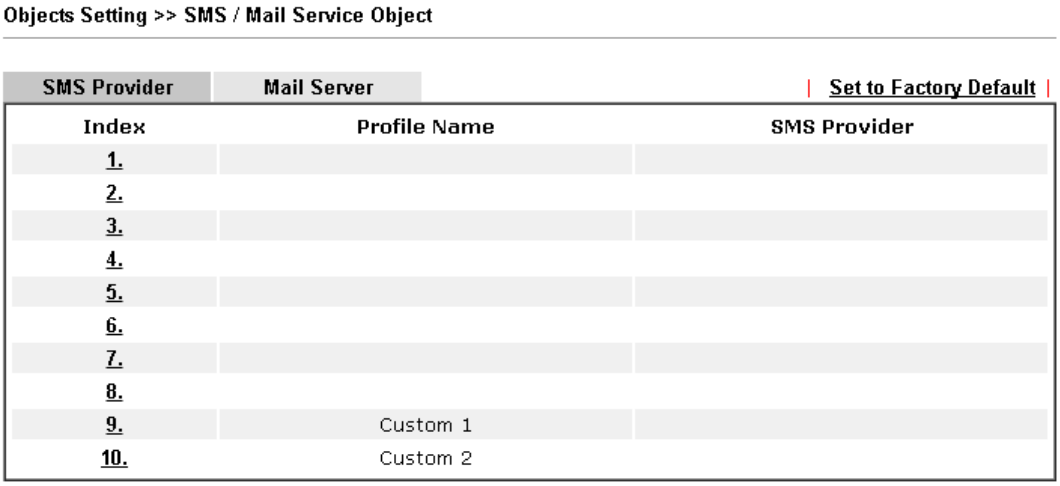
| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. Maximum length is 31 characters. |
| **Service Provider** | Select a Service Provider from the dropdown list. |
| **Connection Protocol** | Specify HTTP or HTTPS. |
| **Username** | Username used to log in to the service. Maximum length is 31 characters. |
| **Password** | Password used to log in to the service. Maximum length is 31 characters. |
| **Quota** | Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0. |
| **Sending Interval** | Minimum amount of time, in seconds, to wait between sending SMS messages. |
| **Send a Test Message** | Click it to send a test e-mail according to above configuration. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

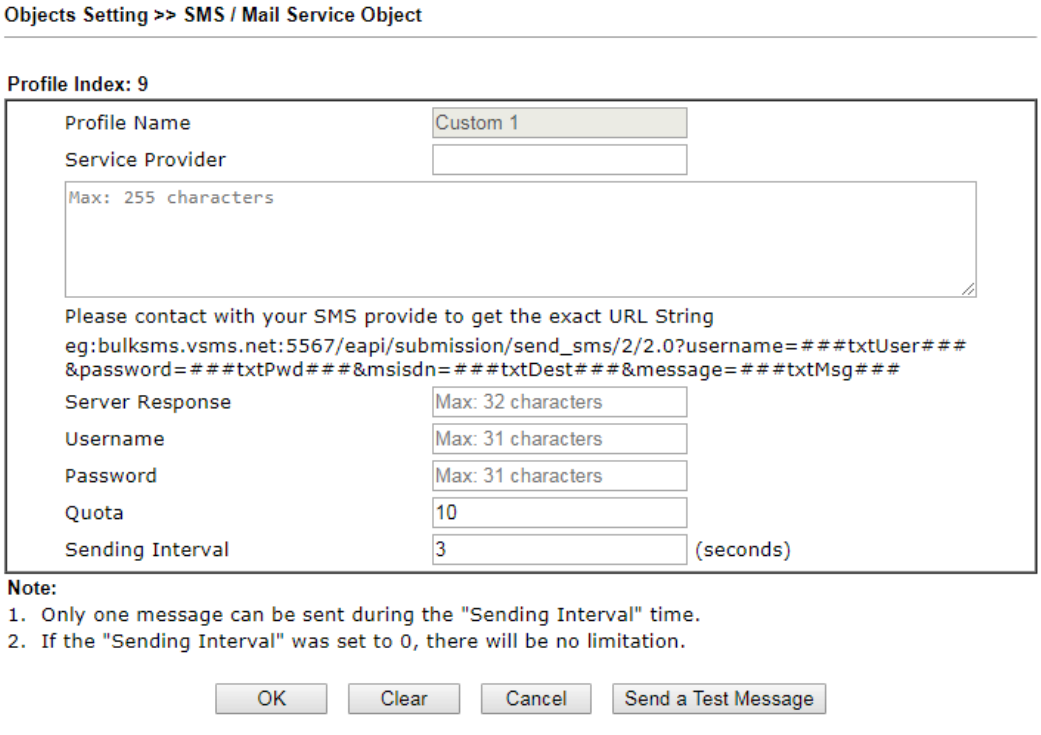



## Customized SMS Service

The router offers an extensive list of preset SMS service providers for your convenience. However, if your service provider is not among the list of supported service providers, simply use Indexes 9 and 10 to create a customized SMS service profile.




To set up a customized profile, click the SMS Provider tab, and then click one of the 2 indexes (9 and 10) to bring up the configuration page.



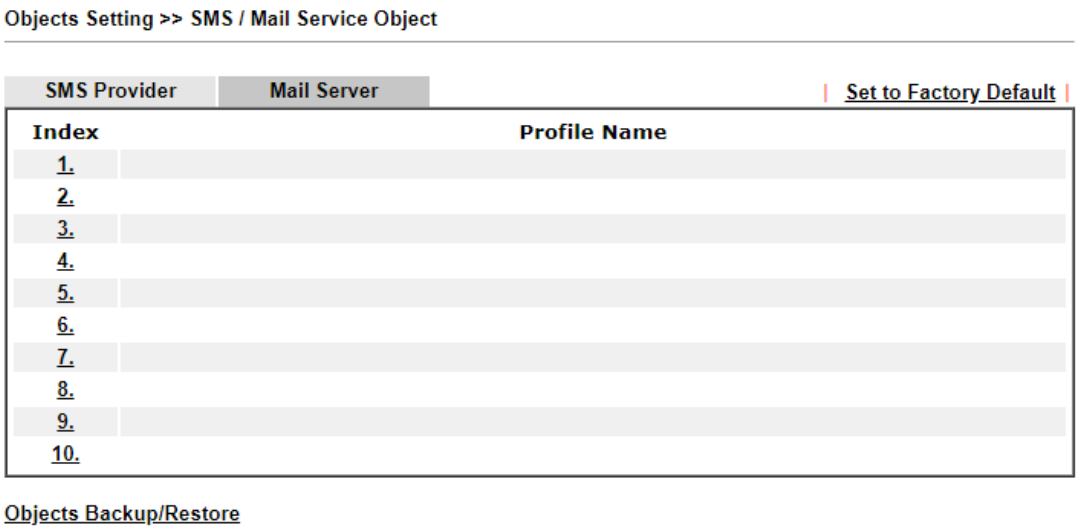
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Display-only profile name, which is Custom 1 for Index 9 and Custom 2 for Index 10. |
| **Service Provider** | Enter an identifier for the service provider. Maximum length is 23 characters. |
| **Entry box** | Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate URL to use. |
| **Server Response** | Enter the API text defined by the SMS provider. It allows Vigor router to acknowledge that the SMS server has received the request coming from the SMS server. |
| **Username** | Username used to log in to the service. Maximum length is 31 characters. |
| **Password** | Password used to log in to the service. Maximum length is 31 characters. |
| **Quota** | Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0. |
| **Sending Interval** | Minimum amount of time, in seconds, to wait between sending SMS messages. |

To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the SMS service object, click **Clear**.

## Mail Service Object

Up to 10 **Mail Service Objects** can be set up for use with Application>>Mail Alert Service.

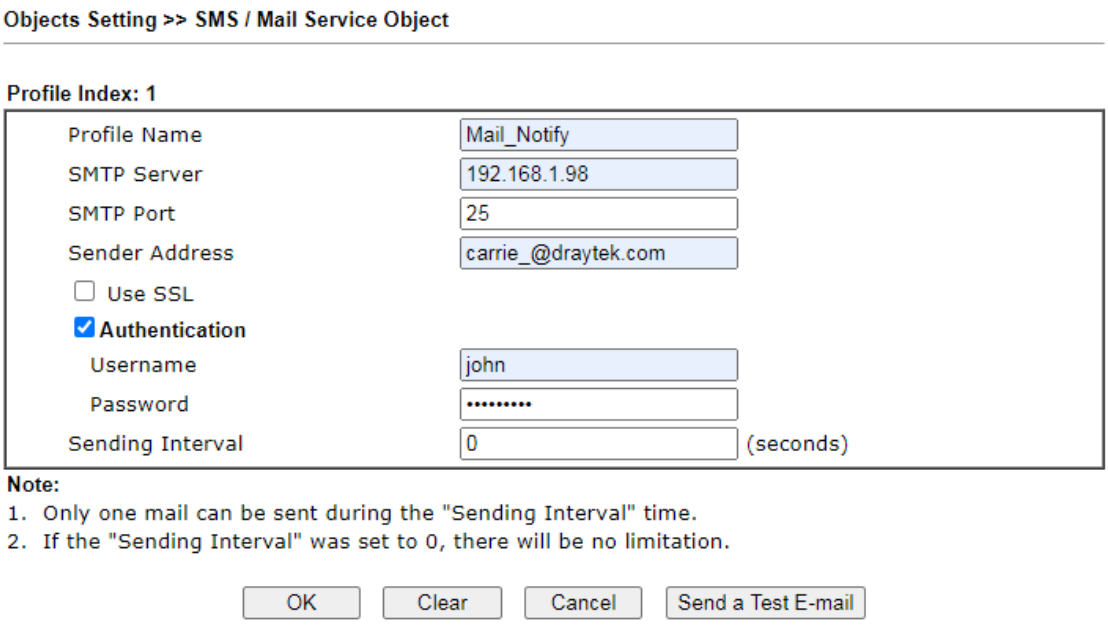



Each item is explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **Index** | Index number of the profile. |

| | |
|---|---|
| **Profile Name** | Name that identifies the profile. |
| **Objects Backup/Restore** | Click it to backup or restore the service object. |

To set up a profile, click the Mail Server tab, and then click its index to bring up the configuration page.



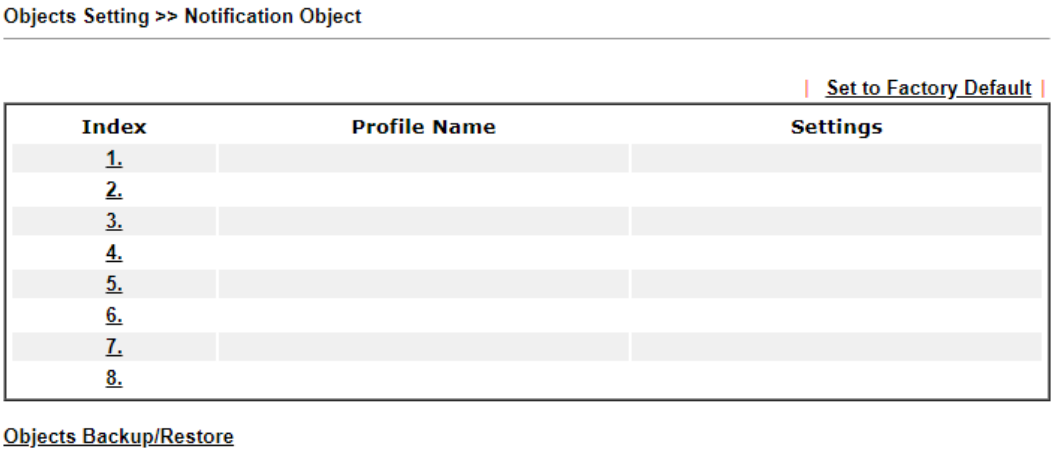

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. Maximum length is 31 characters. |
| **SMTP Server** | IP address of the SMTP server. |
| **SMTP Port** | Port number of the SMTP server. |
| **Sender Address** | E-mail address of the sender. |
| **Use SSL** | Check this box to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the de facto port used for SMTPS is 465. |
| **Authentication** | Select to send username and password to SMTP server for authentication.<br>**Username** – Username for authentication. Maximum length is 31 characters.<br>**Password** – Password for authentication. Maximum length is 31 characters. |
| **Sending Interval** | Minimum amount of time, in seconds, to wait between sending e-mail messages. |
| **Send a Test E-mail** | Click it to send a test e-mail according to above configuration. |

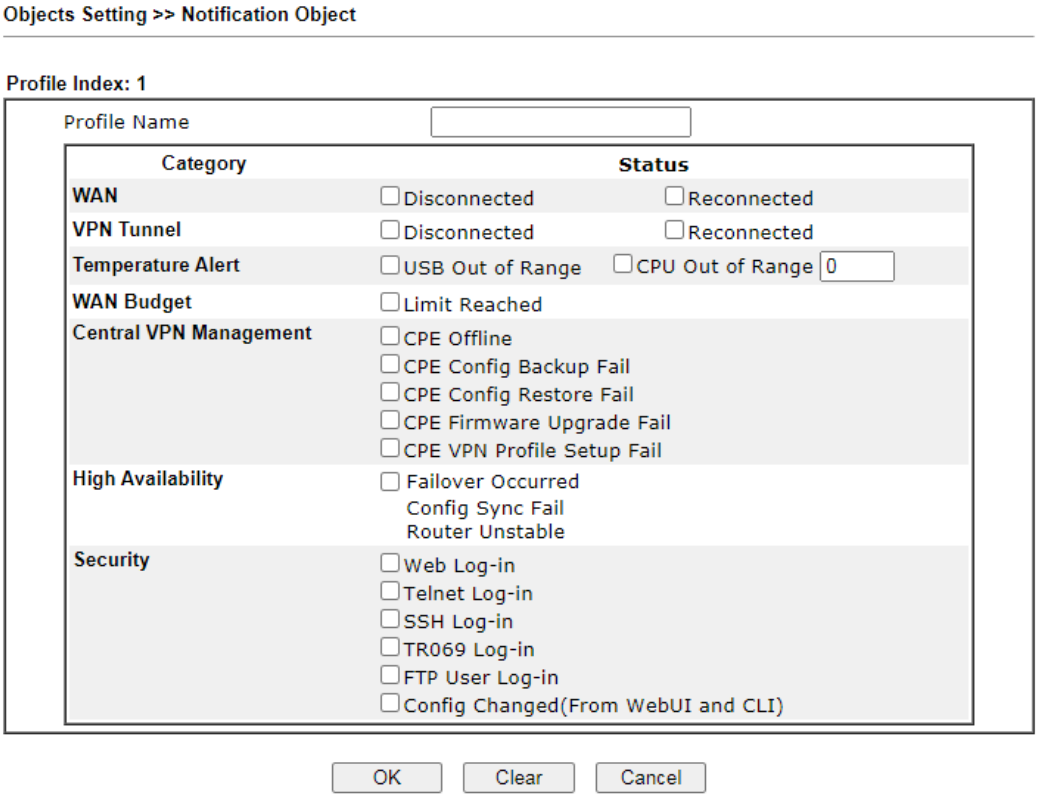
To save changes on the page, click **OK**. To discard changes, click **Cancel**. To blank out all settings in the mail service object, click **Clear**.

## VII-1-11 Notification Object

Up to 8 Notification Objects can be set up for use in **Application>>SMS Alert Service** and **Application>>Mail Alert Service**.




To set up a profile, click its index to bring up the configuration page.



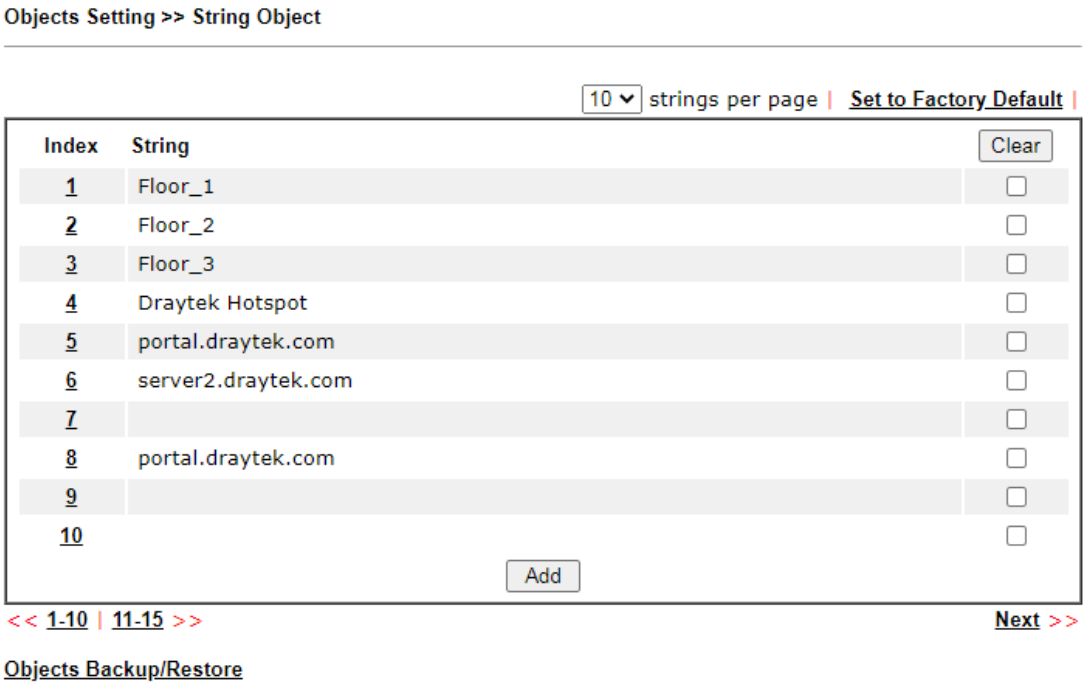

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Name that identifies this profile. Maximum length is 31 characters. |
| **Category** | Areas to be monitored. |
| **Status** | Select the states to be monitored.<br>For example, the check box of **CPE firmware upgrade fail** under the category of **Central VPN Management** is checked. Once such profile is enabled, Vigor router system will send out notification to the recipient via SMS. |

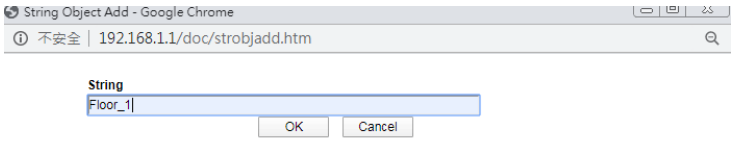
To save changes on the page, click OK. To discard changes, click Cancel. To blank out all settings in the notification object, click Clear.

# VII-1-12 String Object

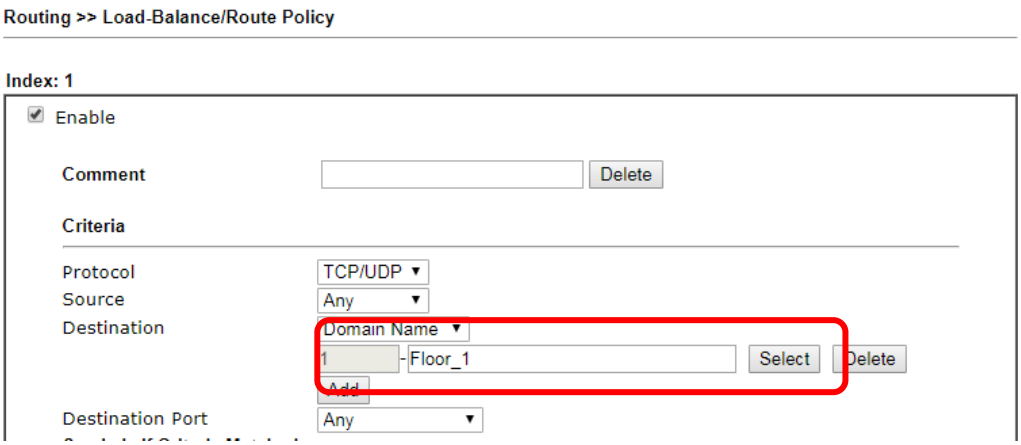
This page allows you to set string profiles which will be applied in route policy (domain name selection for destination) and etc.




Available settings are explained as follows:

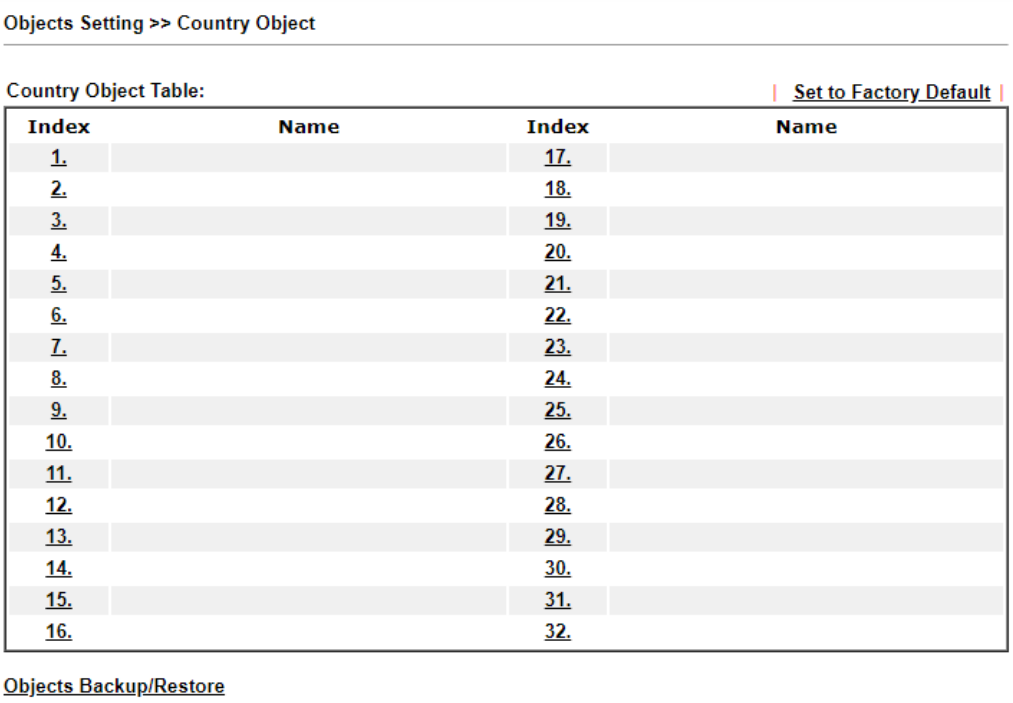
| Item | Description |
|---|---|
| **Add** | Click it to open the following page for adding a new string object.<br>  |
| **Set to Factory Default** | Click it to clear all of the settings in this page. |
| **Index** | Display the number link of the string profile. |
| **String** | Display the string defined. |
| **Clear** | Choose the string that you want to remove. Then click this check box to delete the selected string. |
| **Objects Backup/Restore** | Click it to backup or restore the string object. |

Below shows an example to apply string object (in route policy):

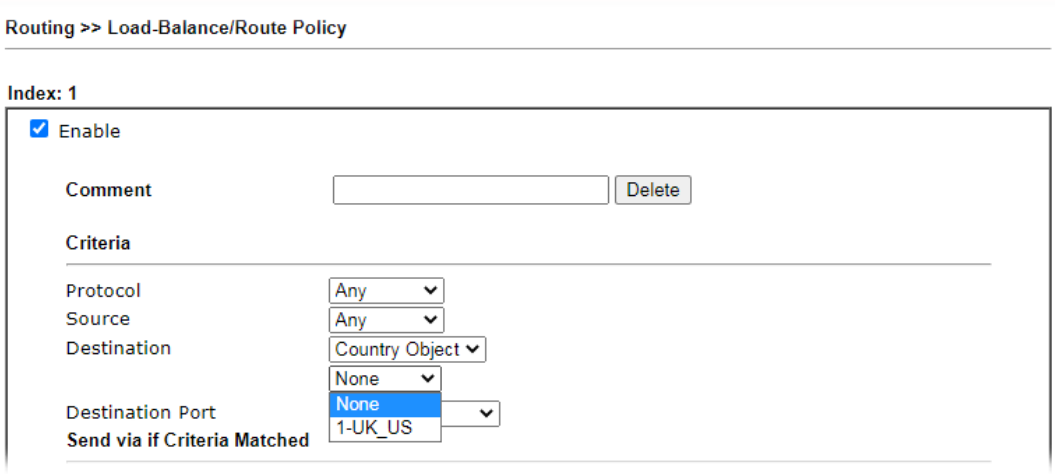



## VII-1-13 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.




The country object, by grouping IP addresses for multiple countries, can be applied by other functions such as router policy destination (refer to the following figure for example).




To set a new profile, please do the steps listed below:

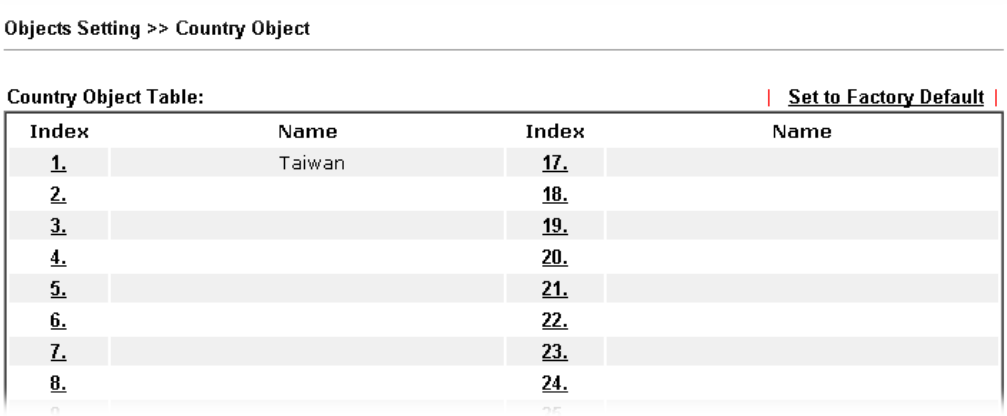
1. Open **Object Setting>>Country Object**, and click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Type a name for such profile. The maximum length of the name you can set is 15 characters. |
| **Available Country / Selected Country** | Select any country from Available Country. Click >> to move the selected country and place on Selected Country.<br>Note that one country profile can contain 1 up to 16 countries. |

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



Objects Setting >> Country Object

Country Object Table: | Set to Factory Default |

| Index | Name | Index | Name |
|---|---|---|---|
| 1. | Taiwan | 17. | |
| 2. | | 18. | |
| 3. | | 19. | |
| 4. | | 20. | |
| 5. | | 21. | |
| 6. | | 22. | |
| 7. | | 23. | |
| 8. | | 24. | |

## VII-1-14 Objects Backup/Restore

The objects settings can be backup as a file. The backup file can be imported to the device to restore the configuration in the future if required.




Available settings are explained as follows:

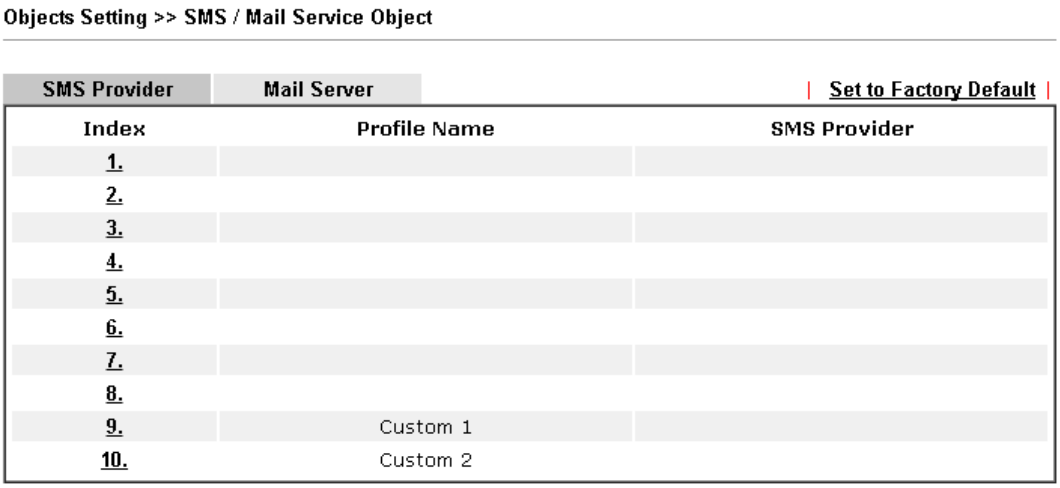
| Item | Description |
|---|---|
| **Backup** | Usually, the IP objects can be created one by one through the web page of **Objects>>IP Object**. However, to a user who wants to save more time in bulk creating IP objects, a quick method is offered by Vigor router to modify the IP objects with a single file, a CSV file.<br>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.<br>**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.<br>**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.<br>**Download** – Download the CSV file from Vigor router and store in your hard disk. |
| **Restore** | **Select** – Click it to specify a predefined CSV file.<br>**Restore** – Import the selected CSV file onto Vigor router. |

# Application Notes

## A-1 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

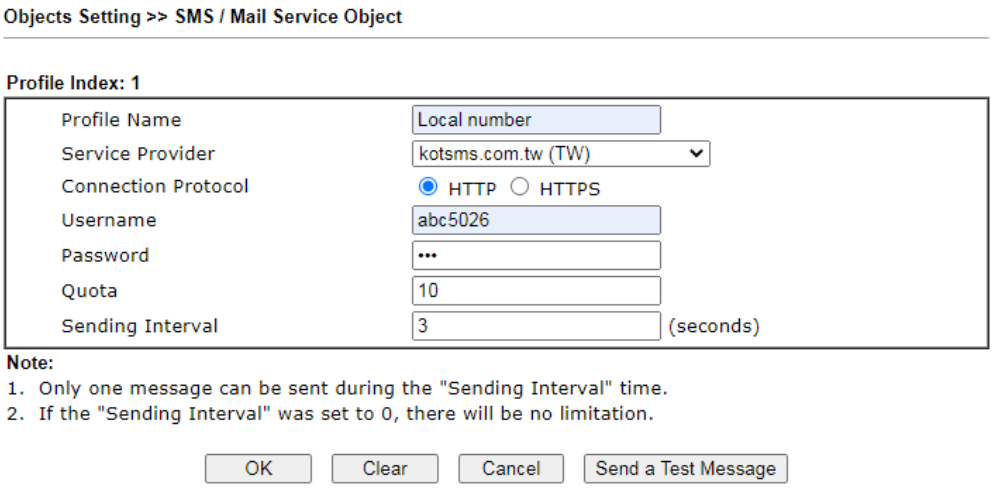
Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

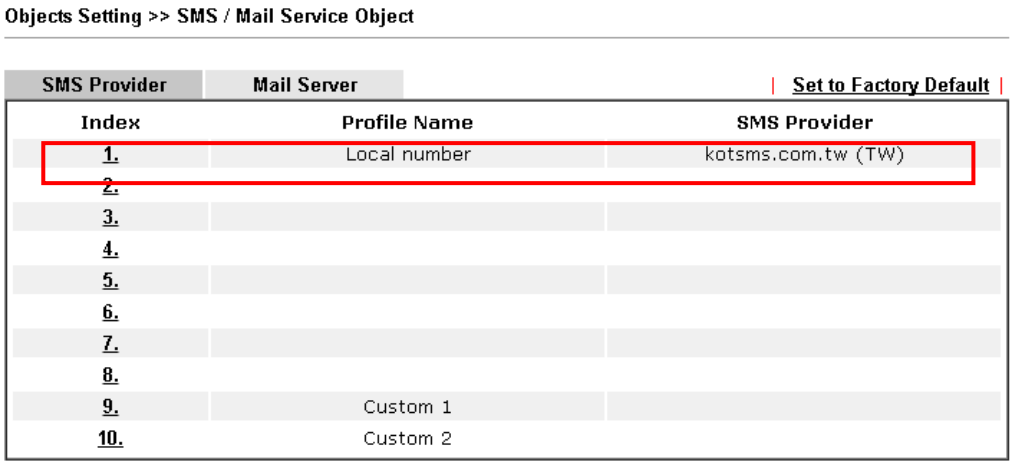



Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

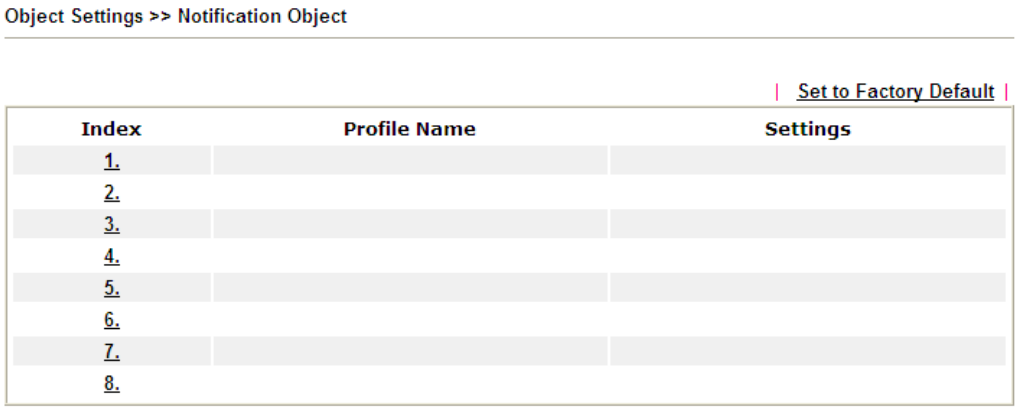
3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, Enter the username and password and set the quota that the router can send the message out.



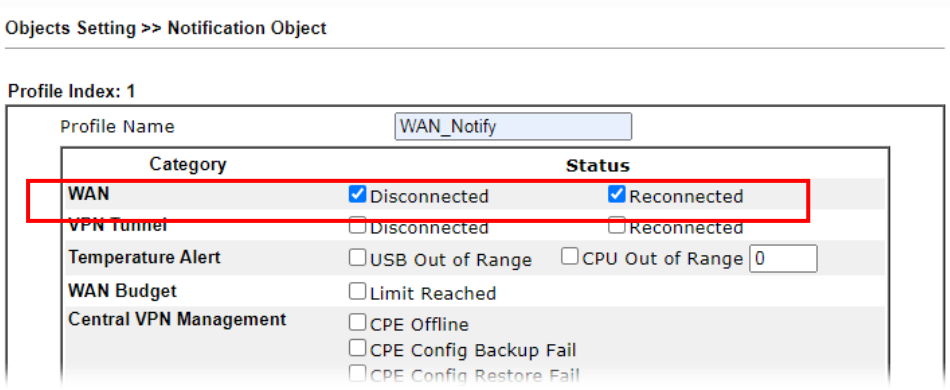
4. After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.



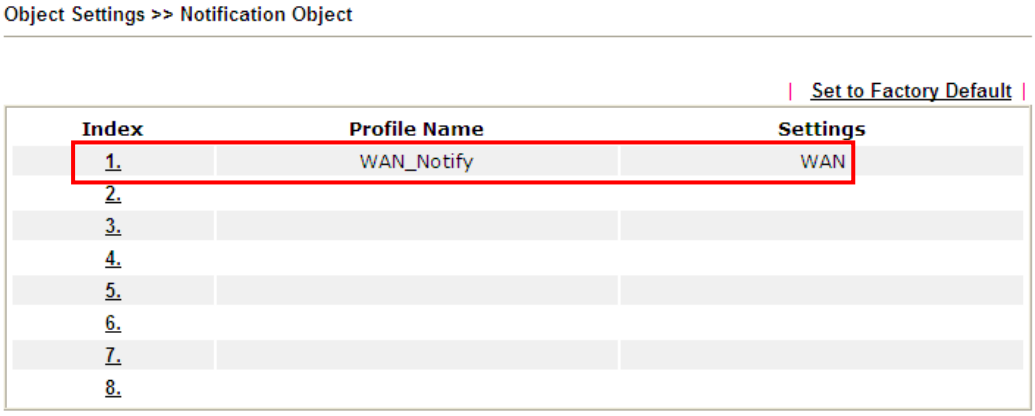

5. Open **Object Settings>>Notification Object** to configure the event conditions of the notification.



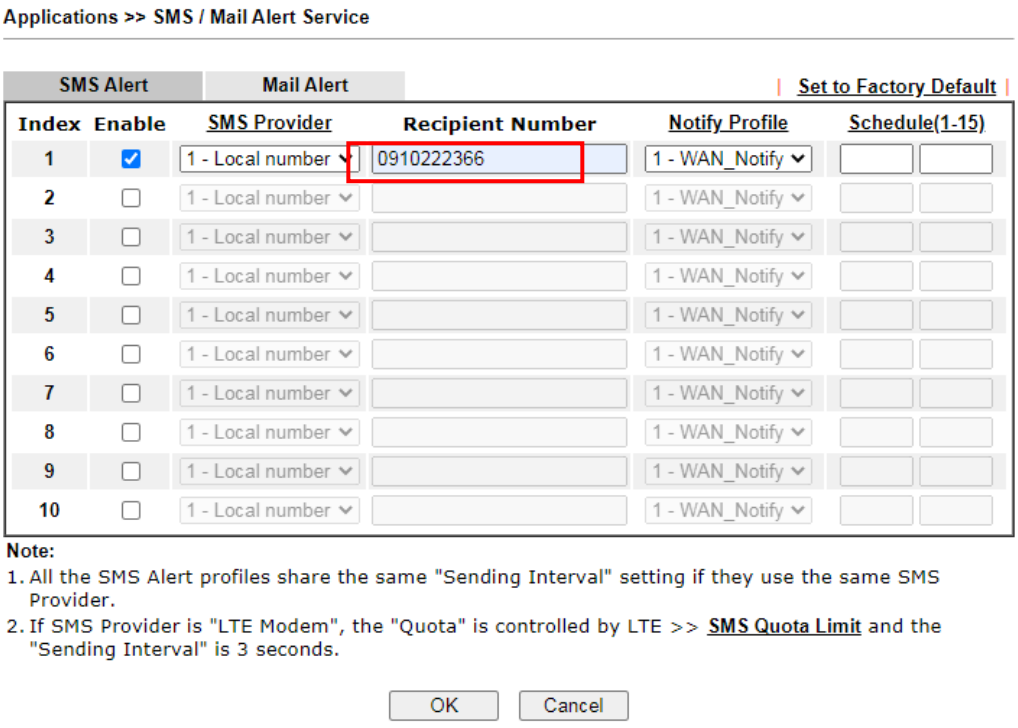

6. Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, Enter the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.



7. After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.



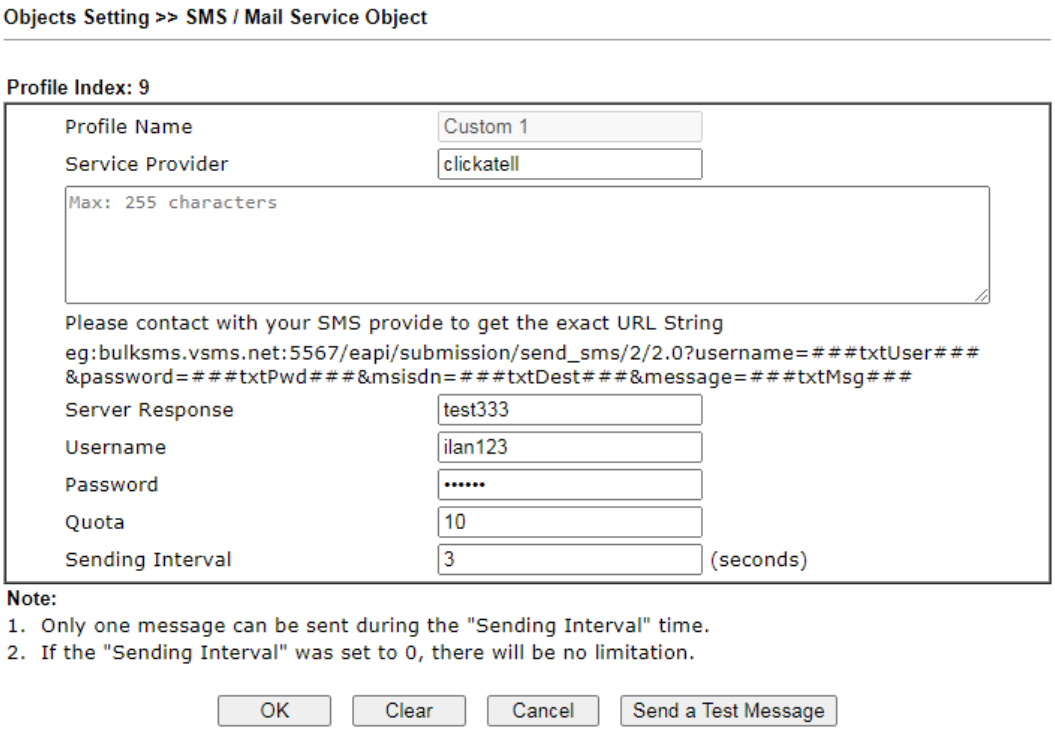

8. Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, Enter the phone number in the field of Recipient Number (the one who will receive the SMS).




9. Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

## Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, Enter the URL string of the SMS provider and Enter the username and password. After clicking **OK**, the new added SMS provider will be added and will be available for you to specify for sending SMS out.



# VII-2 USB Application

USB devices connected to the Vigor router can function as storage servers, WAN interfaces, network printers or thermometers.

After setting the configuration in USB Application, a USB storage device can be accessed using either the FTP or SMB protocol from LAN clients with the IP address of the Vigor router and the username and password entered in **USB Application>>USB User Management**.



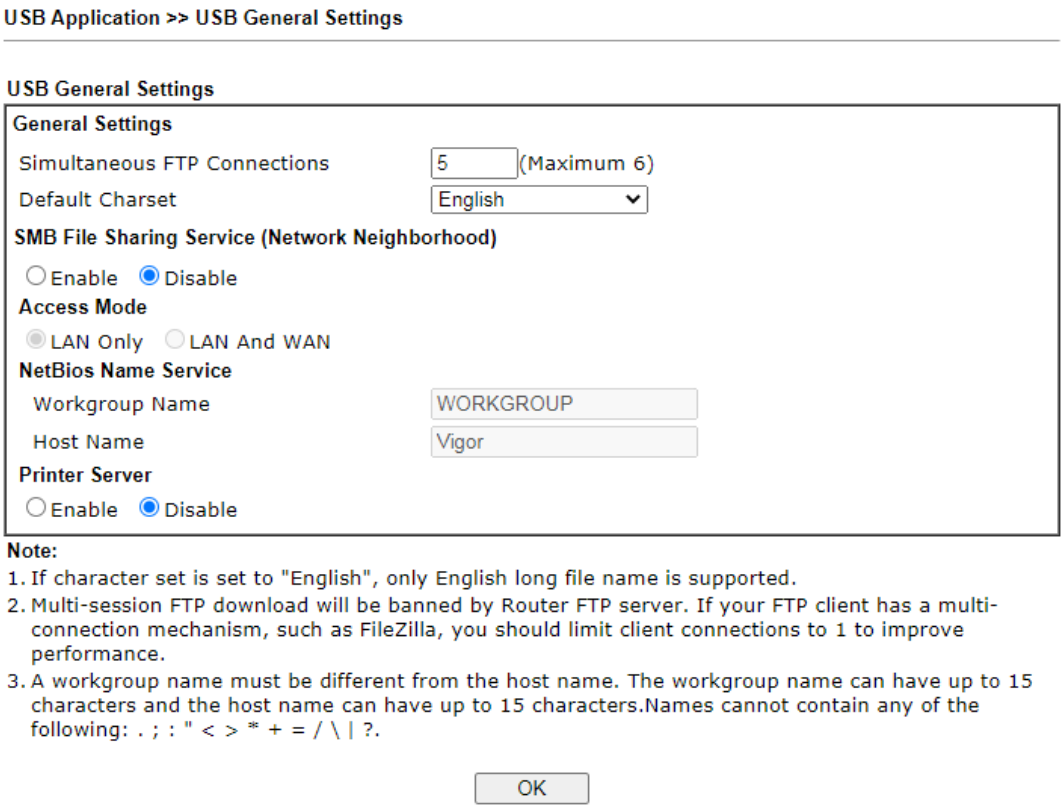
| | |
|---|---|
| **Info** | USB modems that are supported by the router are listed in **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>Internet Access** and **WAN>>General Setup** for detailed information. |

# Web User Interface




## VII-2-1 USB General Settings

This page allows you to configure the file sharing feature of the Vigor router, where USB mass storage devices such as thumb drives and hard drives can be made accessible to LAN clients. Currently, only FAT16 and FAT32 file systems are supported by the Vigor router, so verify that the USB drive contains these file systems. FAT32 is recommended because of its long filename support, which FAT16 lacks.




Available settings are explained as follows:

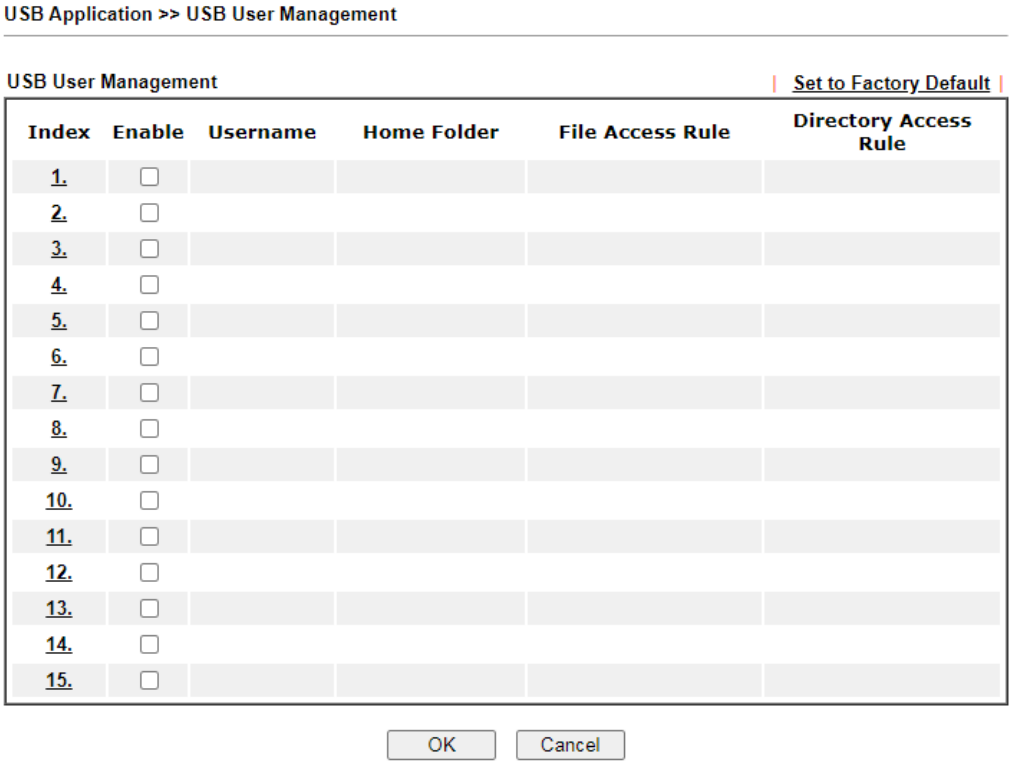
| Item | Description |
|---|---|
| **General Settings** | **Simultaneous FTP Connections -** Enter the maximum number of simultaneous FTP sessions allowed. The router allows up to 6 simultaneous sessions.<br>**Default Charset -** Select the character set for file and directory names. Currently, the Vigor router supports four |

| | |
|---|---|
| | character sets. The default charset is English. |
| **SMB File Sharing Service** | Click **Enable** to enable SMB service (file sharing). |
| **Access Mode** | **LAN Only** – Only users on the LAN can connect access the shared USB disk.<br>**LAN And WAN** - Both LAN and WAN users can access SMB server of the router. |
| **NetBios Name Service** | For SMB file sharing service, you need to specify a workgroup name and a host name. The two names cannot be identical, and neither can contain any of the following characters: ; : " < > * + = \ \| ?<br>**Workgroup Name –** Enter the workgroup name. Maximum allowed length is 15 characters.<br>**Host Name –** Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters. |
| **Printer Server** | **Enable** – Select to allow the Vigor router to act as a print server for printers connected the USB. |

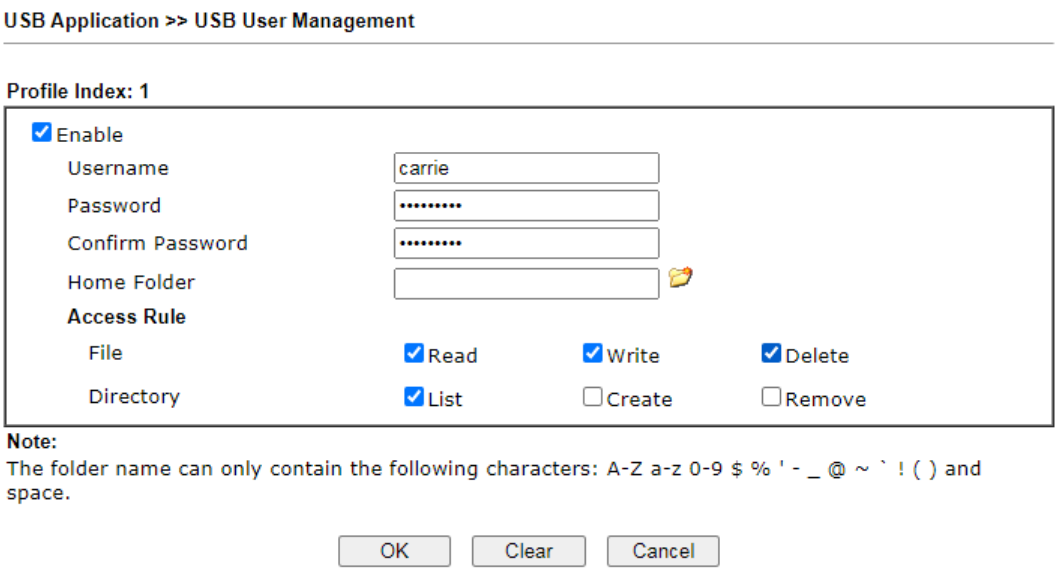
Select **OK** to save changes on the page.

## VII-2-2 USB User Management

This page allows you to set up profiles for FTP/SMB users. Any user who wants to access the USB storage disk must authenticate using a username and password that have been configured on this page. Please connect a USB storage device before adding or modifying settings on this page, or else an error message will appear requesting you to do so before allowing you to proceed.

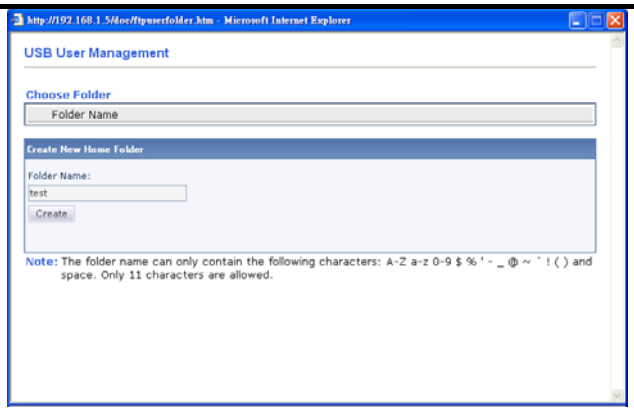



Click index number to access into configuration page.




Available settings are explained as follows:

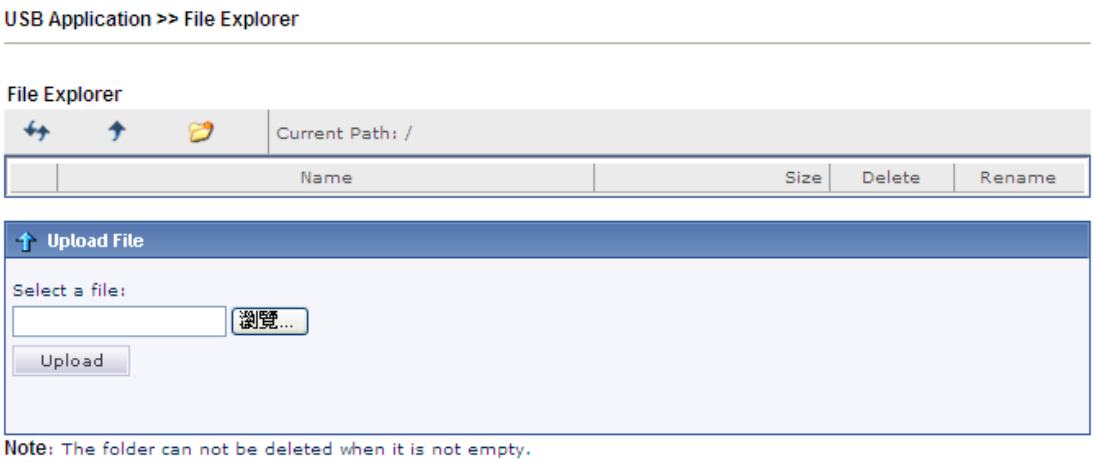
| Item | Description |
|---|---|
| **Enable** | Check to activate this profile (account) for FTP service and / or SMB service. Later, the user can use the username specified in this page to login into FTP server. |
| **Username** | Enter the username for this user profile. Maximum allowed length of the username is 11 characters.<br>**Note:** Anonymous user access is not supported.<br>**Note:** "Admin" cannot be used as a username, as it is reserved for access to web pages on the Vigor router, and for FTP firmware upgrade.<br>**Note:** Ensure that the FTP client does not use passive FTP mode as it is not supported by the Vigor router. |
| **Password** | Enter the password for this user profile. Maximum allowed length of the username is 11 characters. |
| **Confirm Password** | Enter the password again to confirm. |
| **Home Folder** | Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile. Only folders and files inside this selected root folder are accessible to the user. In addition, if the user types "/" here, the user can access into all of the disk folders and files in USB storage disk.<br>To browse the list of folders available for selection, or to create a new folder, click the icon. |

| | |
|---|---|
| |  <br>**Note**: If the USB storage device is write-protected, new folders cannot be created. Only existing folders can be selected.<br>**Note**: Only folders directly under the root can be selected as the home folder. |
| **Access Rule** | It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.<br>**File** – Check the items (Read, Write and Delete) for such profile.<br>**Directory** –Check the items (List, Create and Remove) for such profile. |

To save changes on this page, ensure that a USB storage device is connected, and click **OK**. To discard changes, click **Cancel**. To blank out all settings in the current IP object, click **Clear**.

## VII-2-3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.



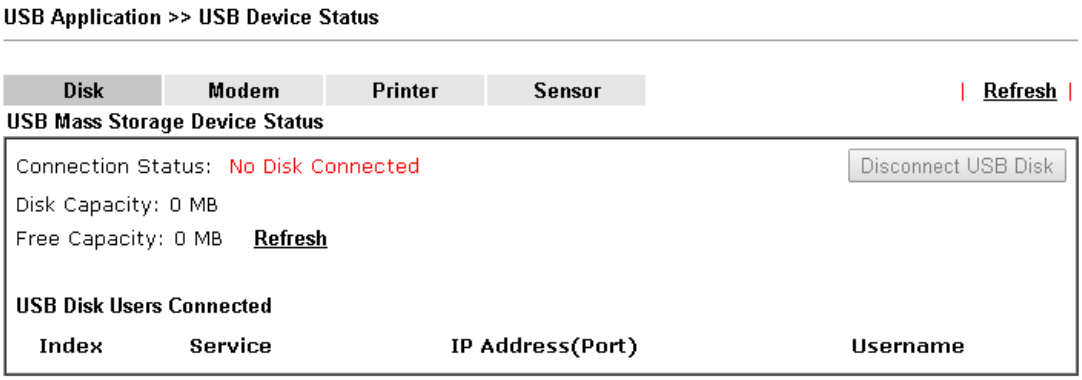

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Refresh** | Click this icon to refresh the list of files and folders. |

| | |
|---|---|
| **Back** | Click this icon to return to the parent folder. |
| **Create** | Click this icon to add a new folder. |
| **Current Path** | Shows current folder. |
| **Upload** | To upload a file to the USB storage device, click the **Browse...** button to bring up the file selection dialog box. Select the file you wish to upload, and click the **Upload** button to initiate the upload process. |

## VII-2-4 USB Device Status

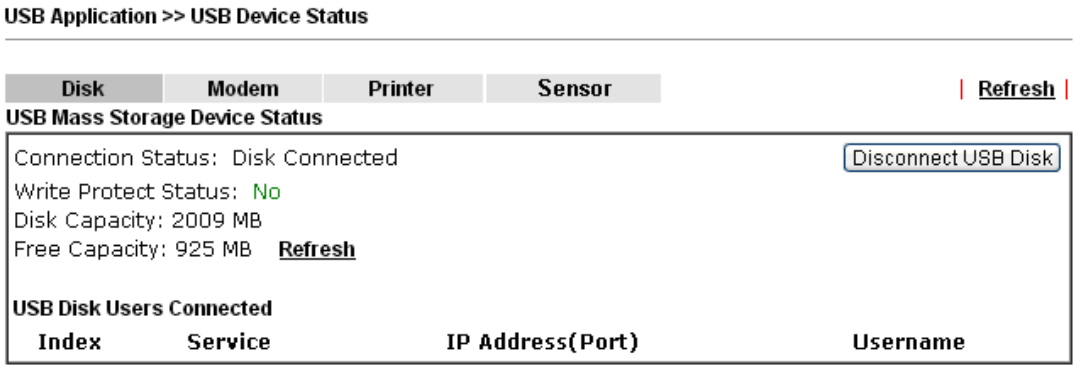
This page allows monitoring of the status of USB devices (disk, modem, printer, and sensor) connected to the Vigor router. To maintain the data integrity of a USB disk that is connected to the router, always click **Disconnect USB Disk** before unplugging the disk from the router.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Connection Status** | Shows whether a USB disk is connected or not. If there is no USB device connected to the Vigor router, "No Disk Connected" will be displayed. |
| **Disk Capacity** | Shows the total capacity of the USB storage disk. |
| **Free Capacity** | Shows the free space on the USB storage disk. Click **Refresh** at any time to get the most up-to-date free capacity. |
| **USB Disk Users Connected** | Shows the clients that are connected to the SMB/FTP server.<br>**Index** – The profile index used by the LAN client to establish the connection.<br>**Service** – Shows whether the connection is using FTP or SMB.<br>**IP Address** – Shows the client's IP address.<br>**Username** – Shows the username used to establish the connection. |
| **Disconnect USB Disk** | Before unplugging the USB storage device from the router, make sure you click this first to ensure that all data has been written to the disk and all open files are closed. |

After a USB storage device has been connected, the **Connection Status** will be updated within a few seconds.




## VII-2-5 Temperature Sensor

A USB Thermometer is now available. It complements your installed DrayTek router installations which will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

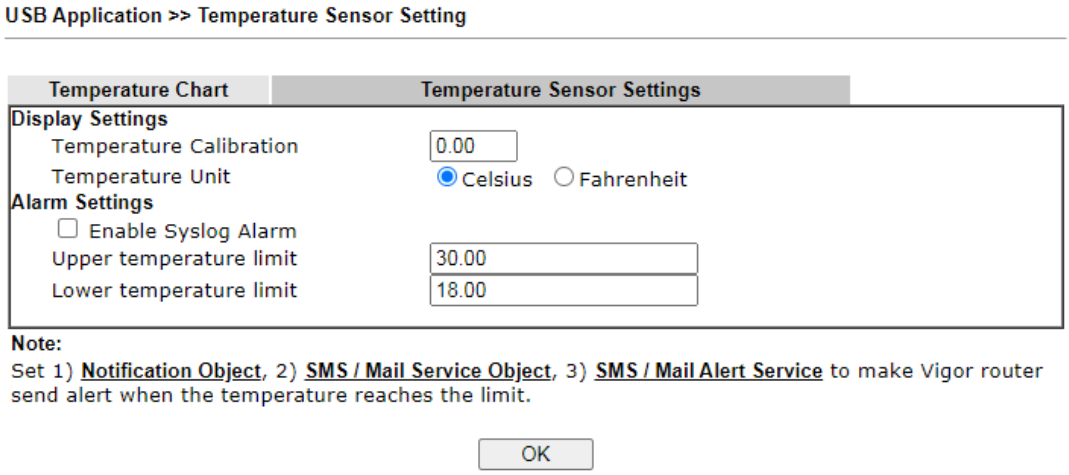



During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

For a list of supported USB thermometers, visit our website at https://www.draytek.com/en/products/usb-thermometer/ or contact your local DrayTek partner.

## Temperature Sensor Settings

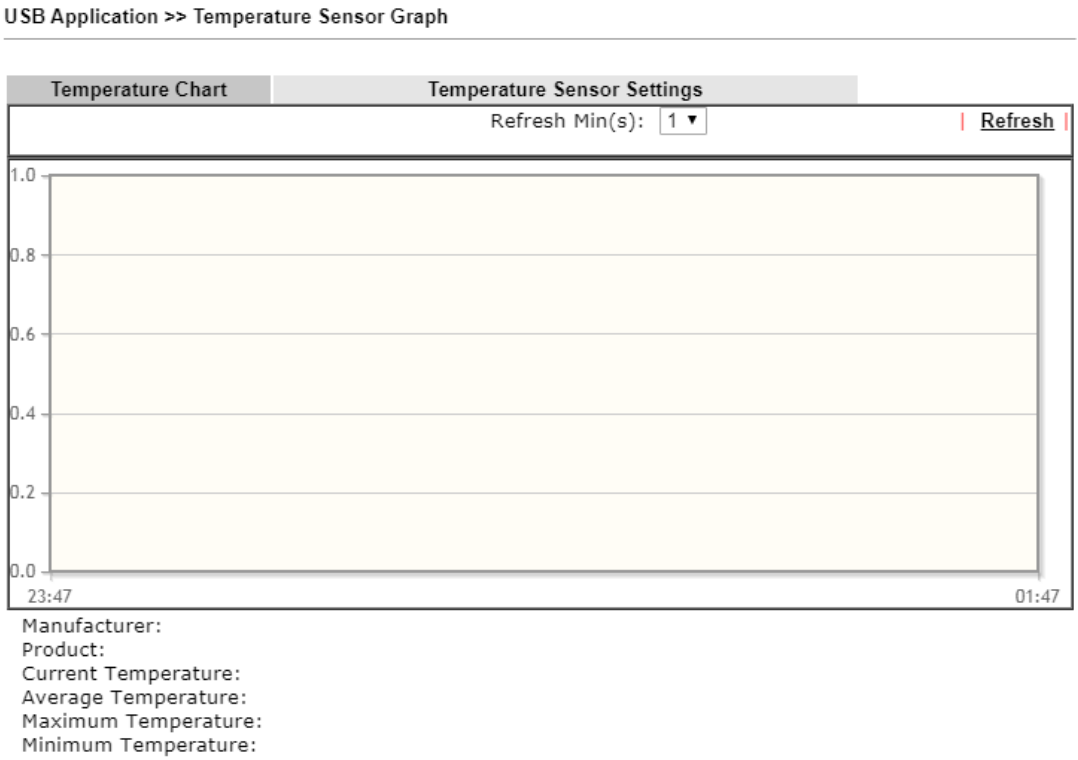



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Display Settings** | **Temperature Calibration** - Enter the difference between the actual temperature and the temperature as reported by the thermometer.<br>**Temperature Unit -** Select the temperature scale to be used. |
| **Alarm Settings** | **Enable Syslog Alarm** - Select to enable recording of the temperature in Syslog.<br>**Upper temperature limit/Lower temperature limit** - Enter the upper and lower temperature limits. If the temperature falls outside of this range, an alert will be sent. |

## Temperature Chart

Below shows an example of temperature graph:



## VII-2-6 Modem Support List

This page lists the brands and models of USB modems that are supported by the Vigor router.

This list is subject to change between different versions of firmware as support for new modems are added.

USB Application >> Modem Support List

The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries.** If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

| Brand | Model | LTE | Access Mode | Status |
|---|---|---|---|---|
| 4G system | XSPlug P3 | | PPP | Y |
| Aiko | Aiko 76E | | PPP | Y |
| Alcatel | Alcatel L100V | ✓ | DHCP | Y |
| | Alcatel L800 | ✓ | DHCP | Y |
| | Alcatel W800 | ✓ | DHCP | Y |
| | Alcatel X500 | | PPP | Y |
| | Alcatel Y855 | ✓ | DHCP | Y |
| Alfa | ALFA Flyppp | | PPP | Y |
| Amoi | Amoi H01 | | PPP | Y |
| BandRich | Bandluxe C321 | | PPP | Y |
| | Bandluxe C330 | | PPP | Y |
| | Bandluxe C331 | | PPP | Y |
| | Bandluxe C502 | | PPP | Y |
| BigPond | BigPond Next G Wireless | | PPP | Y |
| | Broadband USB Mobile Card | | PPP | Y |
| D-Link | D_LINK DWM156 | | DHCP | M |

## VII-2-7 SMB Client Support List

This page shows a list of SMB clients on various platforms, and their levels of compatibility with the Vigor router as determined by our in-house testing. This list is subject to change as support for SMB clients are added or improved.

**USB Application >> SMB Client Support List**

The following compatibility test lists suggested SMB clients supported by Vigor router.

| Platform | Application | Status |
|---|---|---|
| Microsoft® Windows® XP | Built in | I |
| Microsoft® Windows Vista™ | Built in | Y |
| Microsoft® Windows® 7 | Built in | Y |
| Microsoft® Windows® 8 | Built in | M |
| Microsoft® Windows® 10 | Built in | Y |
| OS X® 10.7.5 | Built in | Y |
| OS X® 10.10 | Built in | Y |
| Ubuntu 14.04 | Built in | Y |
| Android™ | AndSMB | Y |
| Android™ | ES File Explorer | Y |
| Android™ | File Expert | Y |
| Android™ | File Manager | Y |
| Android™ | Solid Explorer | Y |
| Android™ | SharesFinder | Y |
| iOS | eXPlayer | Y |
| iOS | nPlayer | Y |

Y: Tested and is supported.
I: Supported but has some issue.
M: Has not been tested but might be supported.

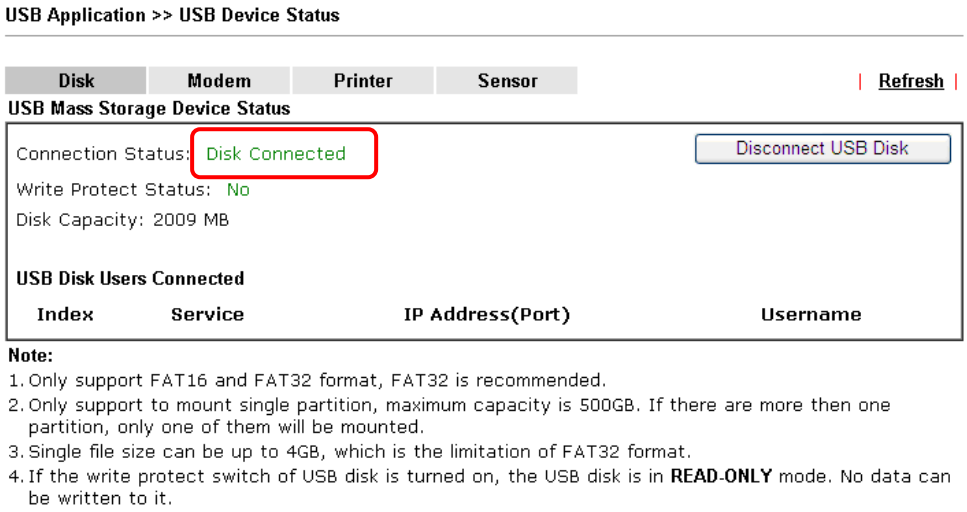
# Application Notes

## A-1 How can I get the files from USB storage device connecting to Vigor router?

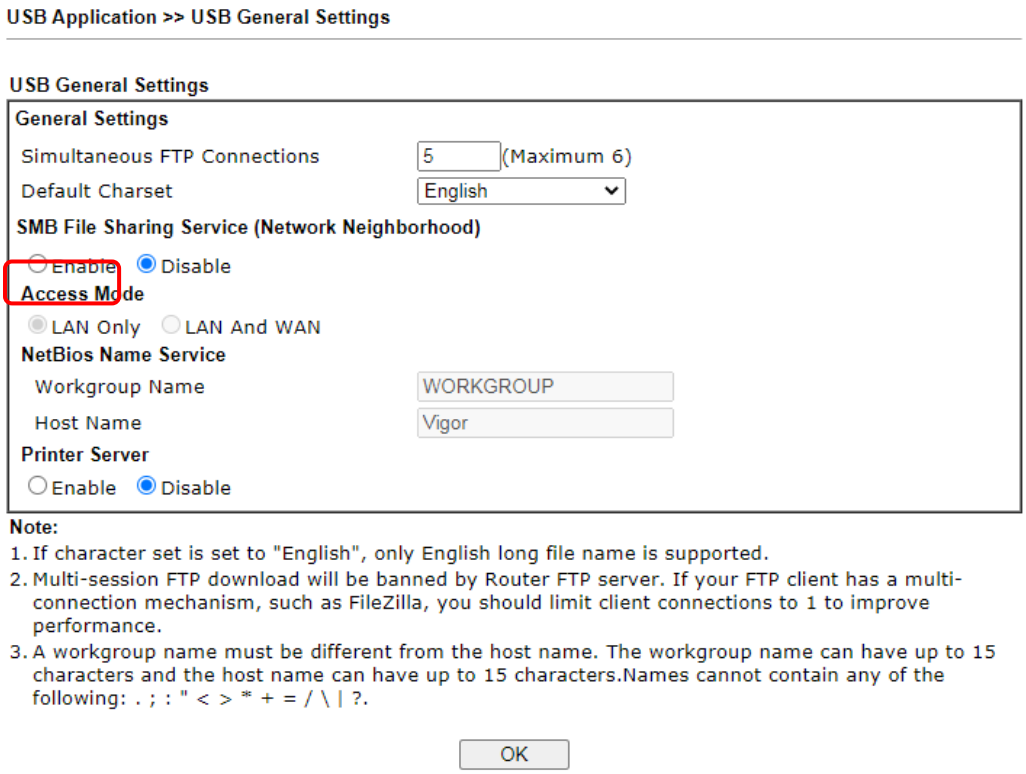
Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SMB server or FTP server.

SMB service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

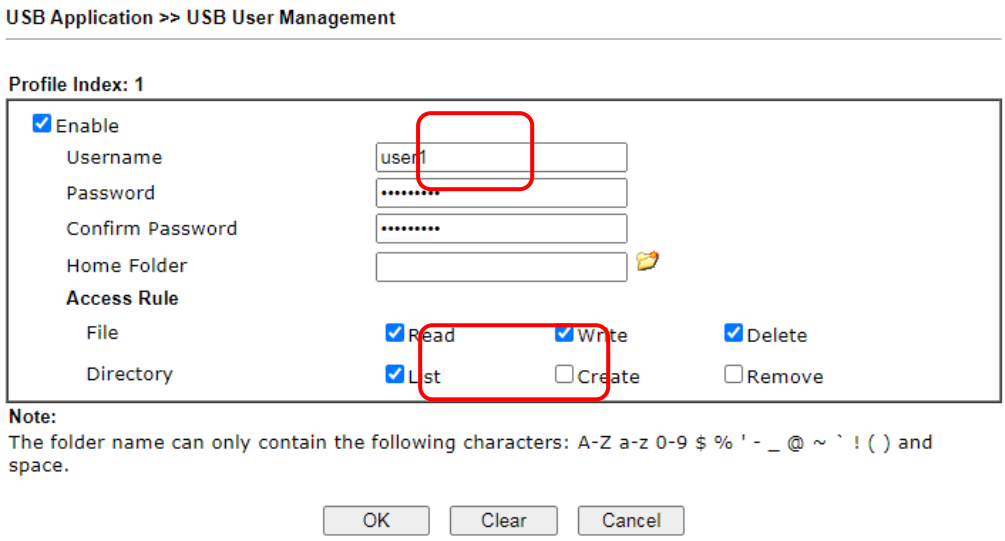
1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:




2. Then, please open **USB Application >> USB General Settings** to enable SMB service.

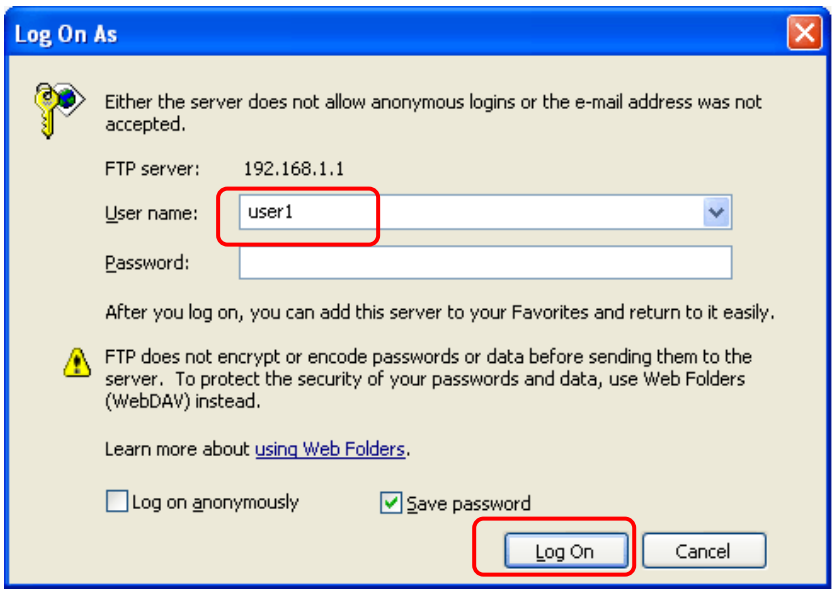

USB Application >> USB General Settings
USB General Settings
General Settings
Simultaneous FTP Connections
5
(Maximum 6)
Default Charset
English
SMB File Sharing Service (Network Neighborhood)
Enable
Disable
Access Mode
LAN Only
LAN And WAN
NetBios Name Service
Workgroup Name
WORKGROUP
Host Name
Vigor
Printer Server
Enable
Disable
Note:
1. If character set is set to "English", only English long file name is supported.
2. Multi-session FTP download will be banned by Router FTP server. If your FTP client has a multi-connection mechanism, such as FileZilla, you should limit client connections to 1 to improve performance.
3. A workgroup name must be different from the host name. The workgroup name can have up to 15 characters and the host name can have up to 15 characters.Names cannot contain any of the following: . ; : " < > * + = / \ | ?.
OK

3. Setup a user account for the FTP service by using **USB Application >>USB User Management.** Click **Enable** to enable FTP/SMB User account. In the example below, we have set up a new account with the username "user1", and granted “Read”, “Write” , "Delete" and “List” permissions to it.

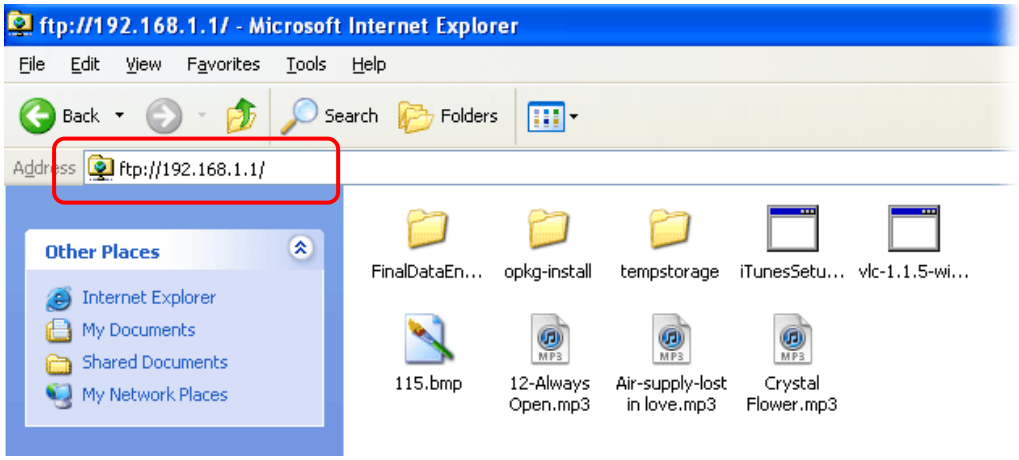



4. Click **OK** to save the configuration.

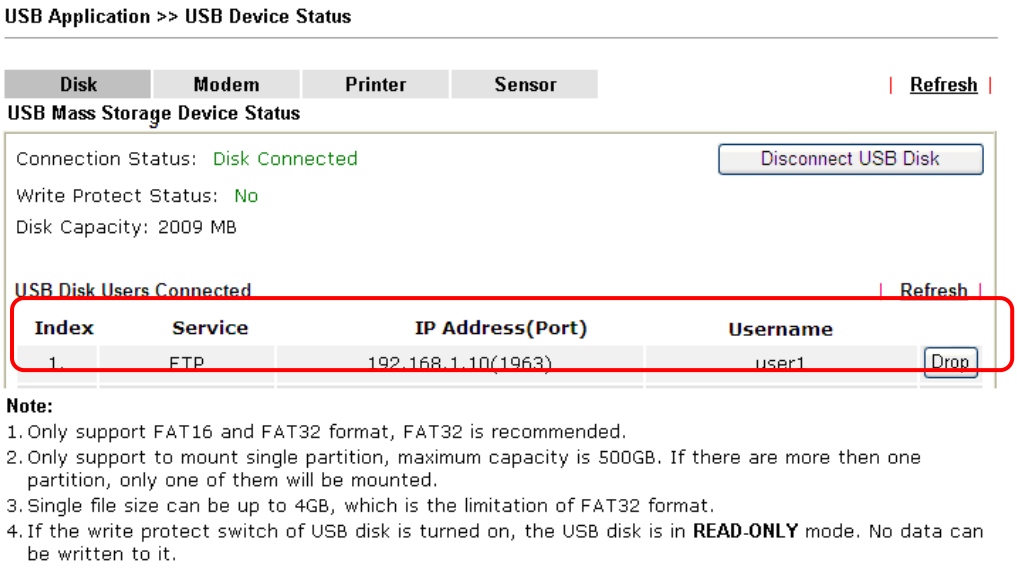
5. To verify that the FTP service is running properly, open a browser window and enter ftp://192.168.1.1 as the destination. Replace 192.168.1.1 with the actual IP address of the router. When prompted to enter the login credentials, enter the username "user1" to login.



6. When the following screen appears, you have successfully connected to the FTP server and verified that it is running properly.




7. If you check **USB Application >> USB Disk Status** on browser, you will see the FTP session initiated by user1.




**Note:**

1. Only support FAT16 and FAT32 format, FAT32 is recommended.
2. Only support to mount single partition, maximum capacity is 500GB. If there are more then one partition, only one of them will be mounted.
3. Single file size can be up to 4GB, which is the limitation of FAT32 format.
4. If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Now, users in LAN of Vigor2927 can access into the USB storage device by entering ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

# Part VIII Troubleshooting




This part will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration.

# VIII-1 Diagnostics

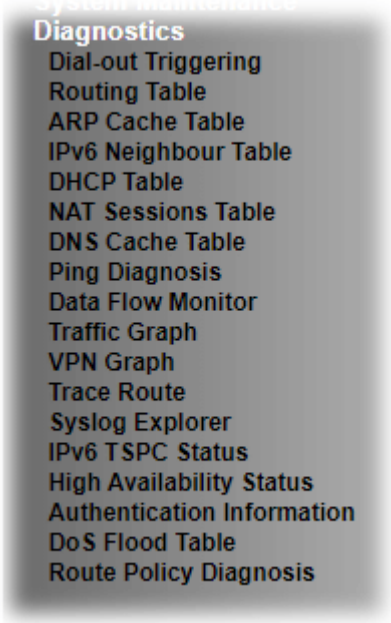
This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

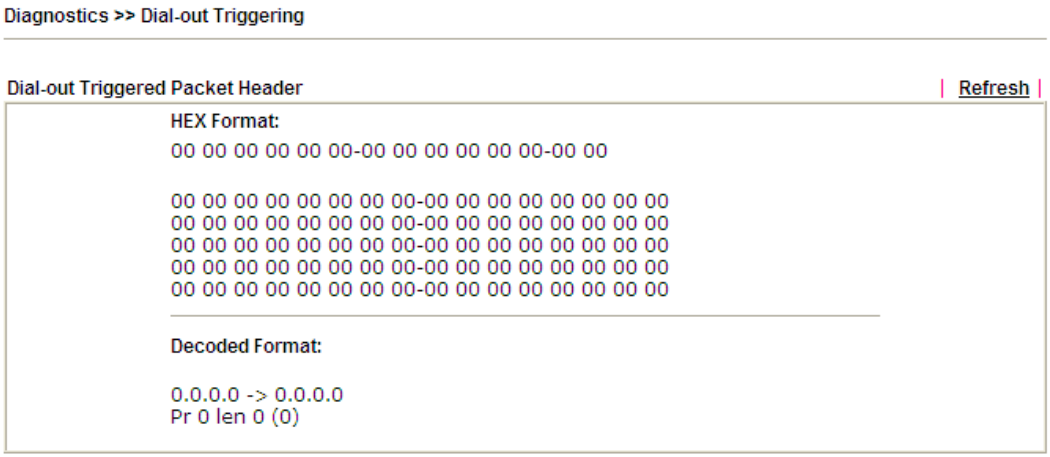
# Web User Interface

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.

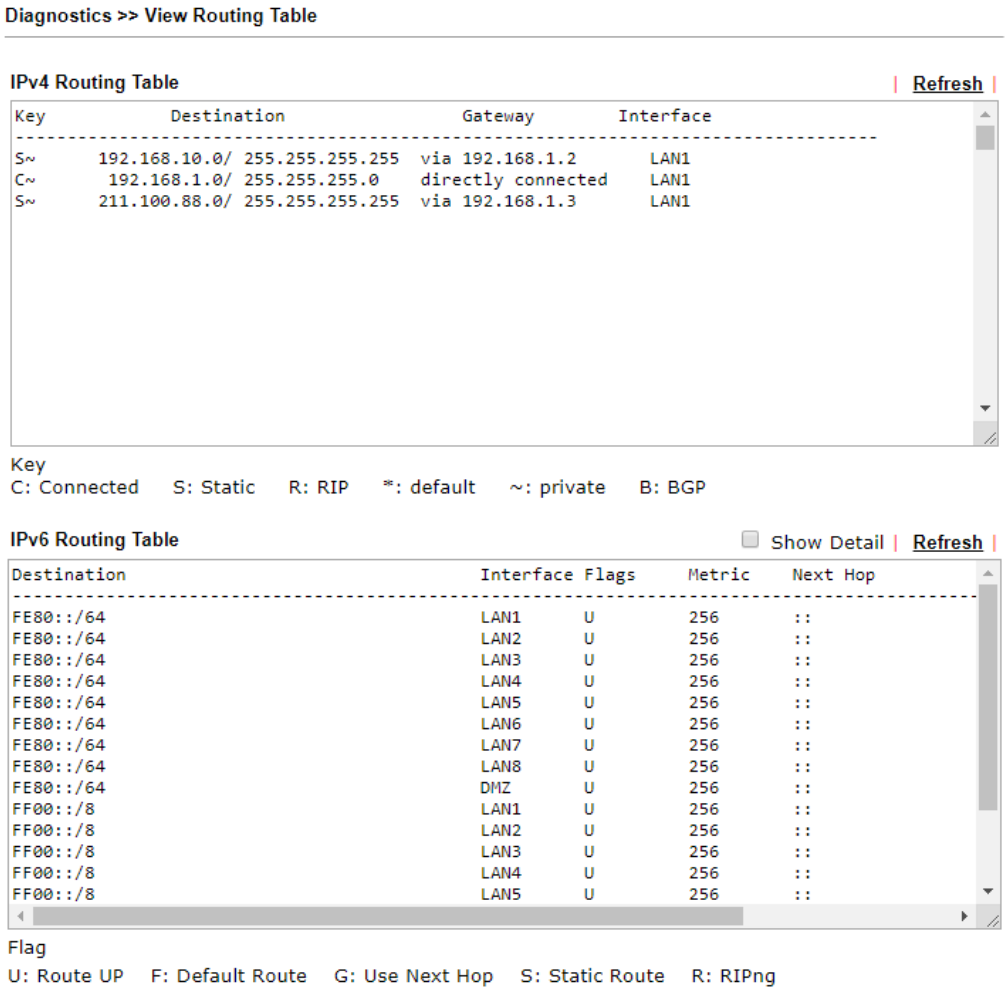



Available settings are explained as follows:

| 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.

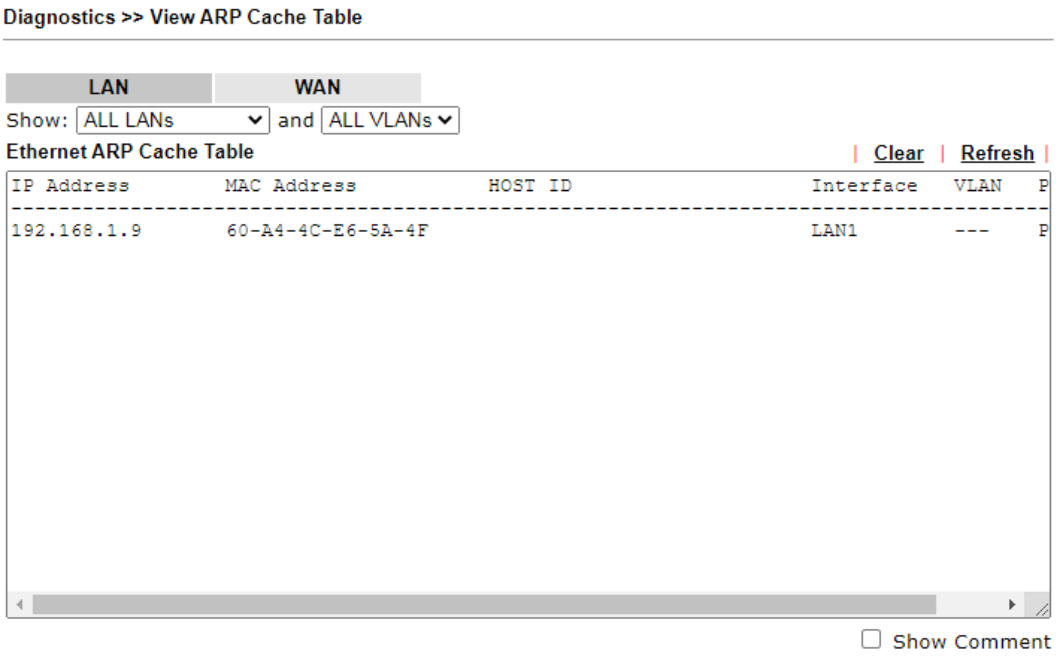



Available settings are explained as follows:

| 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.



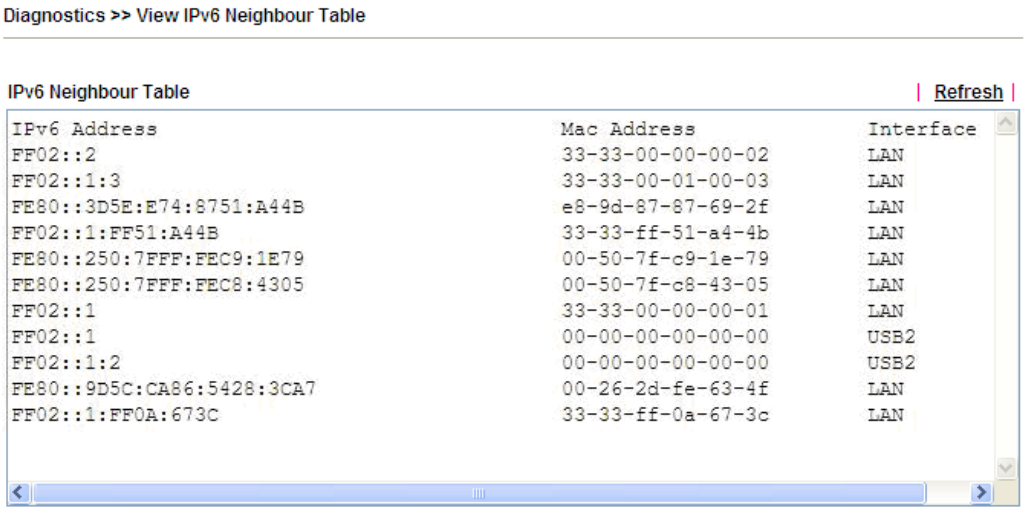

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Show** | Specify LAN and VLAN to display related information.<br>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.



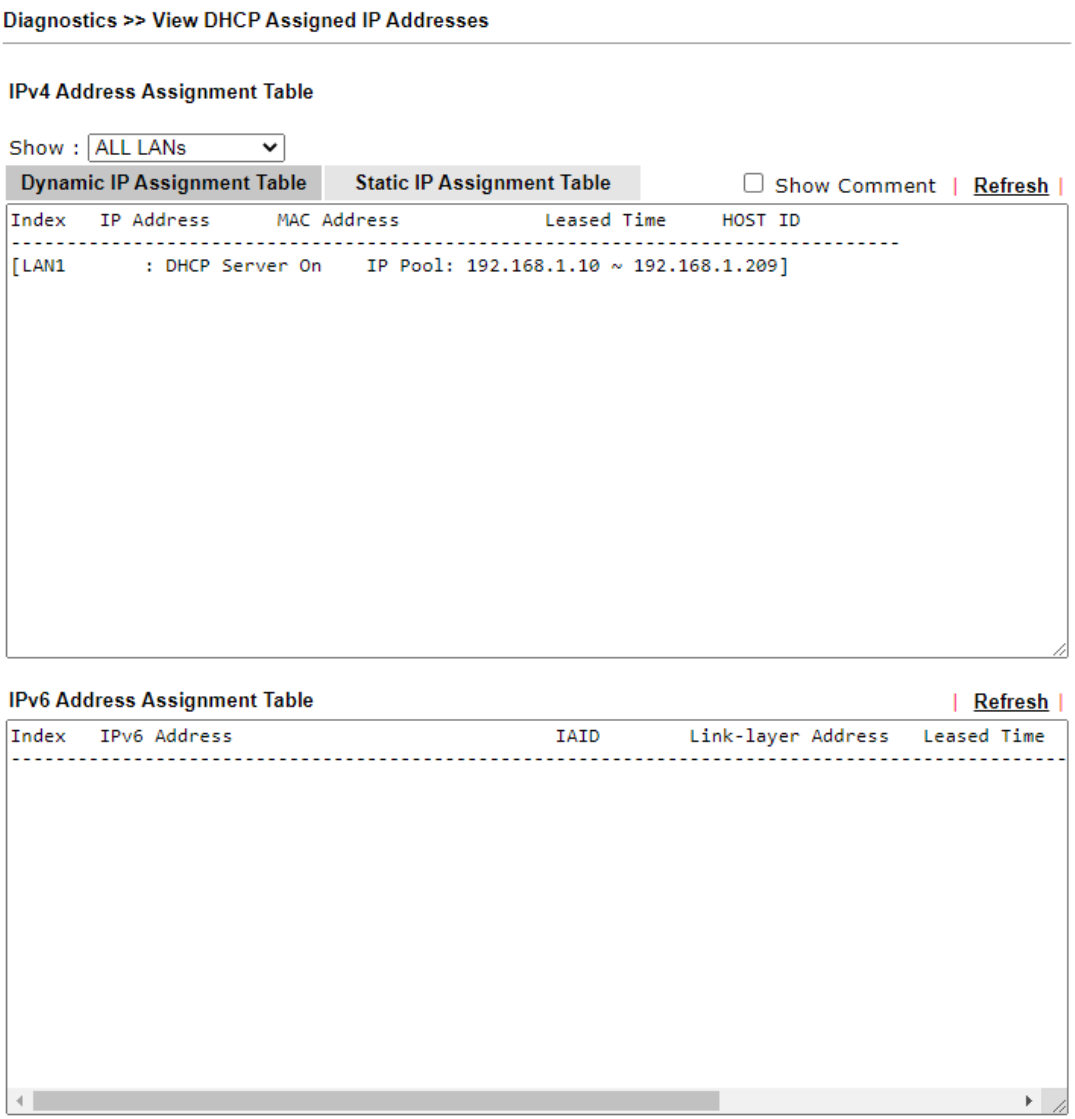

Available settings are explained as follows:

| 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.

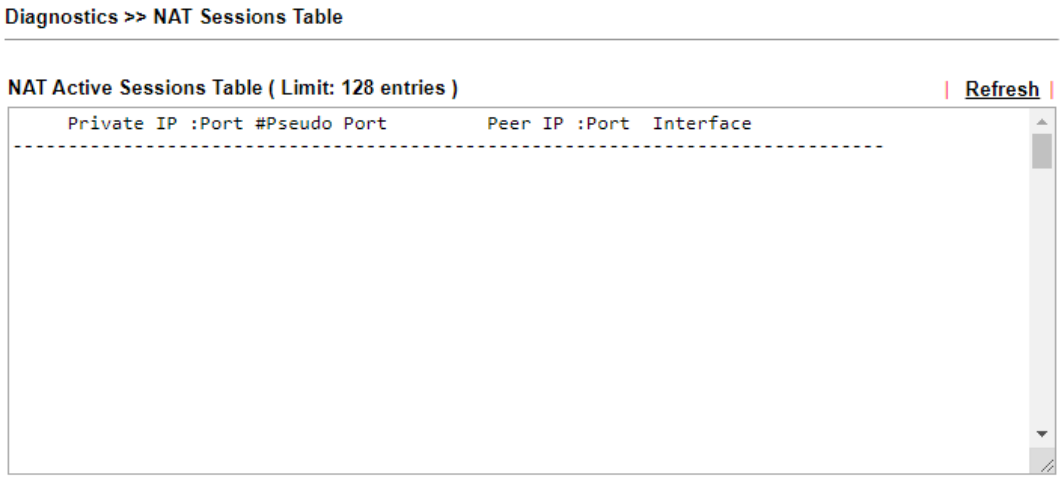



Available settings are explained as follows:

| 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**.

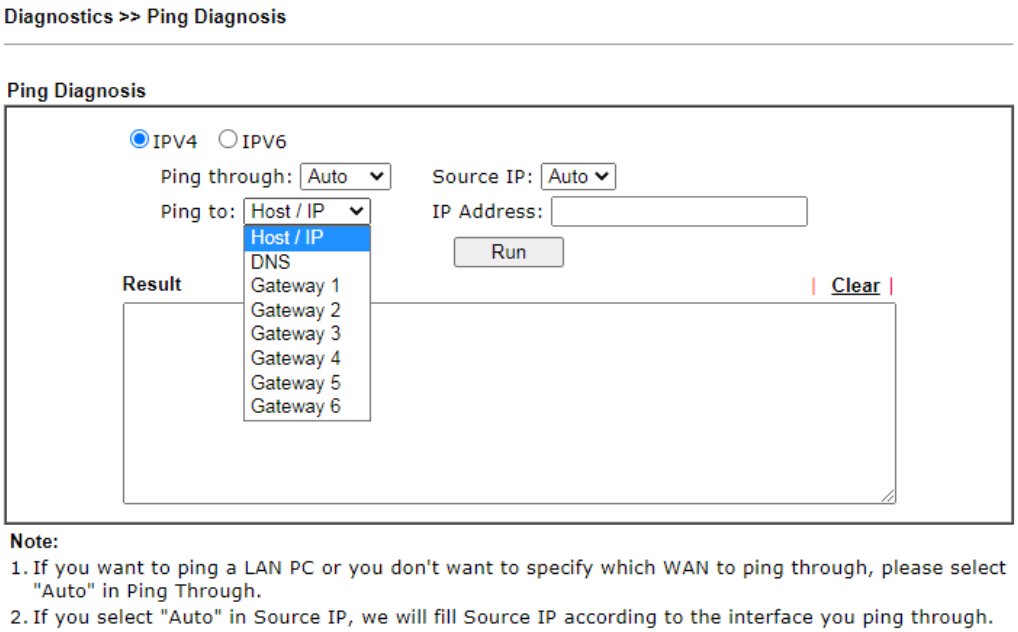



Available settings are explained as follows:

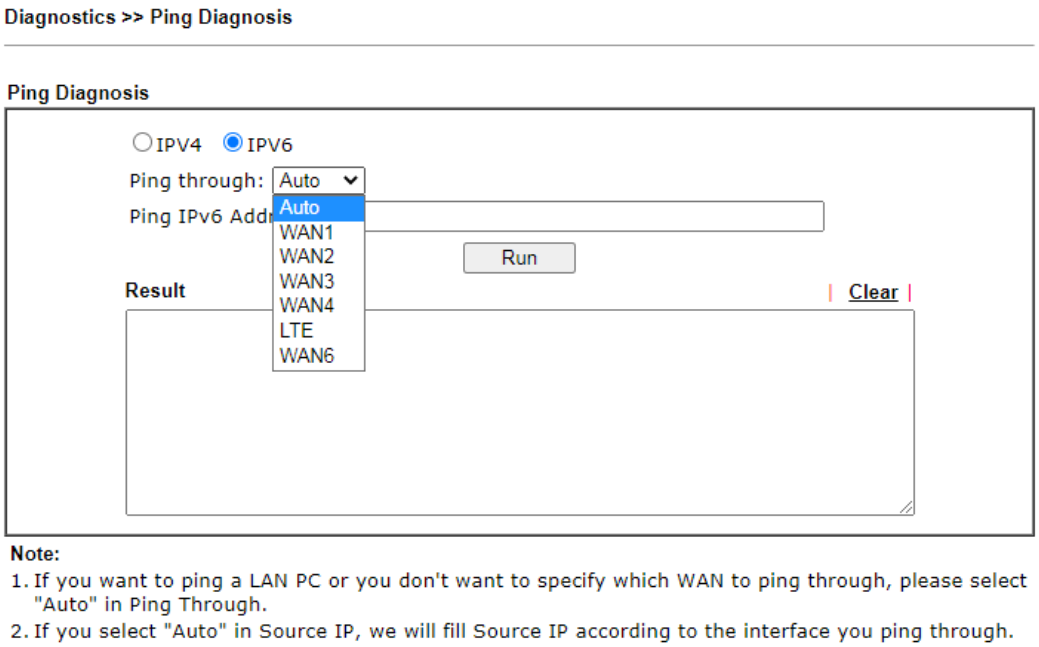
| Item | Description |
|---|---|
| **Clear** | Click this link to remove the result on the window. |
| **Refresh** | Click it to reload the page. |
| **When an entry's TTL is larger than….** | Check the box the Enter the value of TTL (time to live) for each entry. Click **OK** to enable such function.<br>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



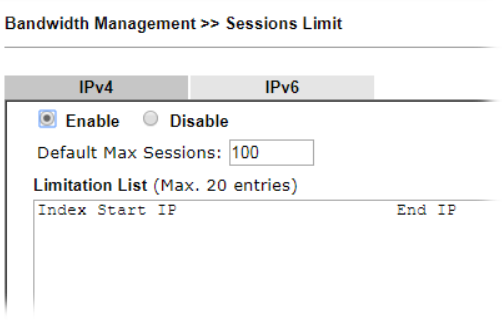

Available settings are explained as follows:

| 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. |

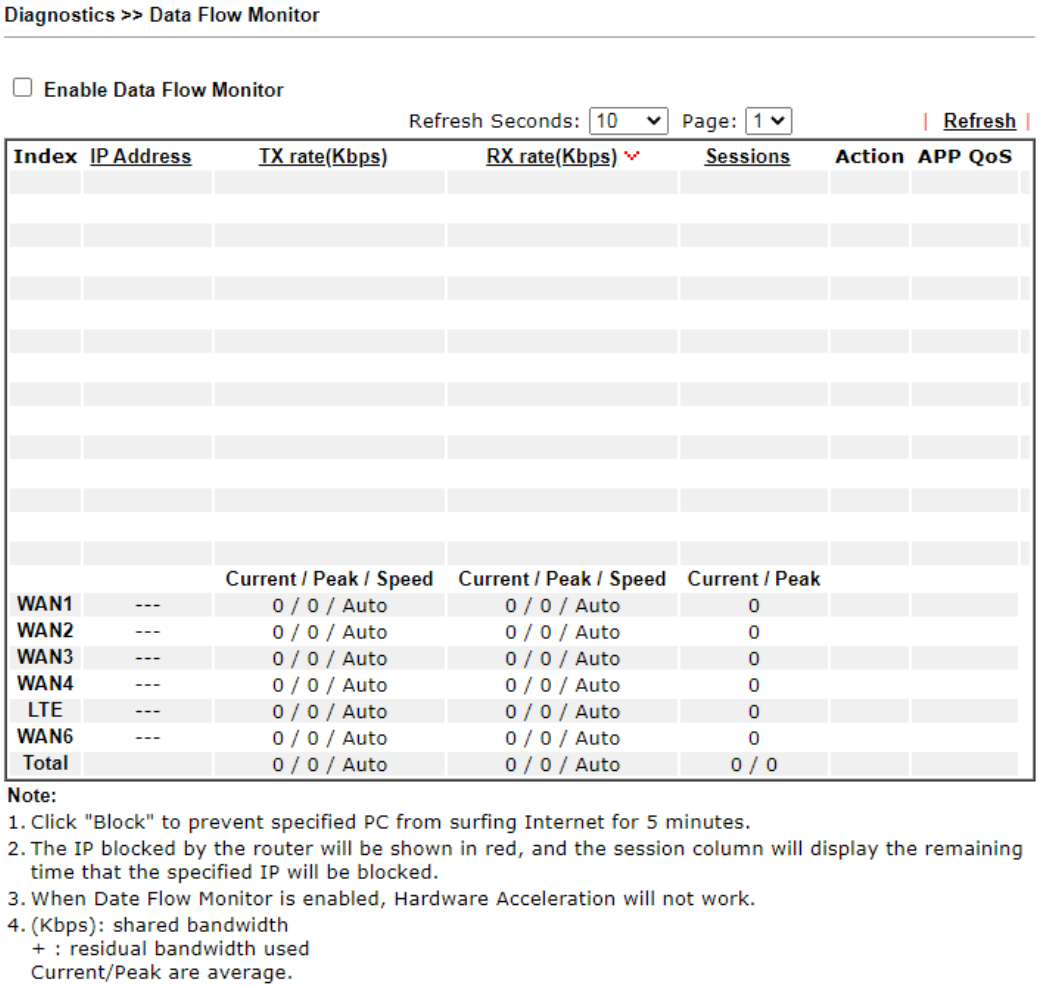
| | |
|---|---|
| **IP Address** | Enter the IP address of the Host/IP that you want to ping. |
| **Ping IPv6 Address** | Enter the IPv6 address that you want to ping. |
| **Run** | Click this button to start the ping work. The result will be displayed on the screen. |
| **Clear** | Click this link to 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.



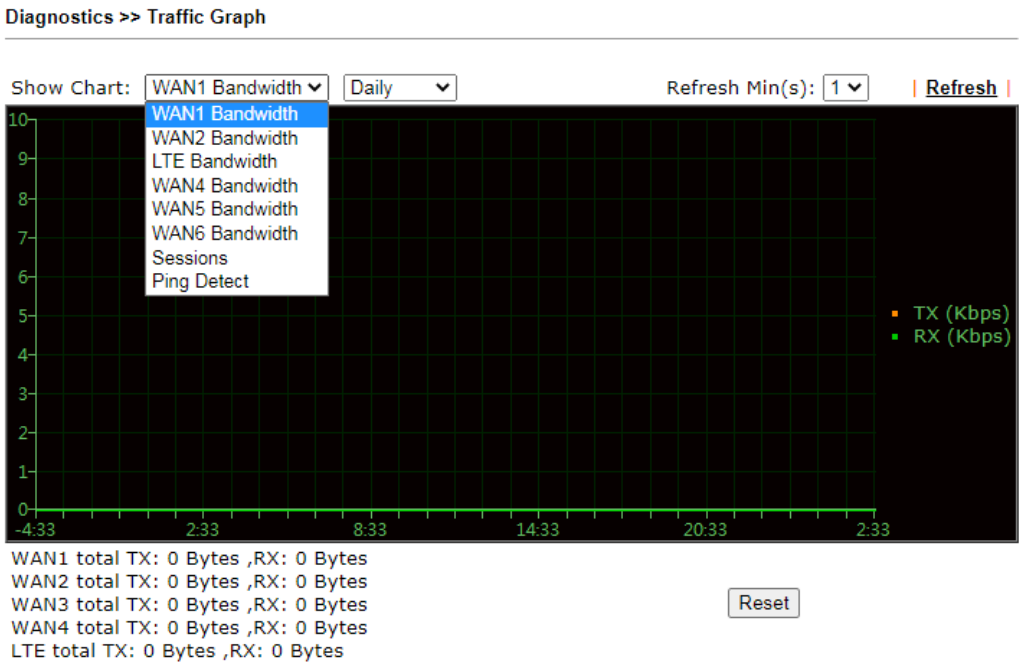

Available settings are explained as follows:

| 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.<br>**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.<br>**Peak** means the highest peak value detected by the router in data transmission.<br>**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/WAN3/WAN4/WAN5/WAN6 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.

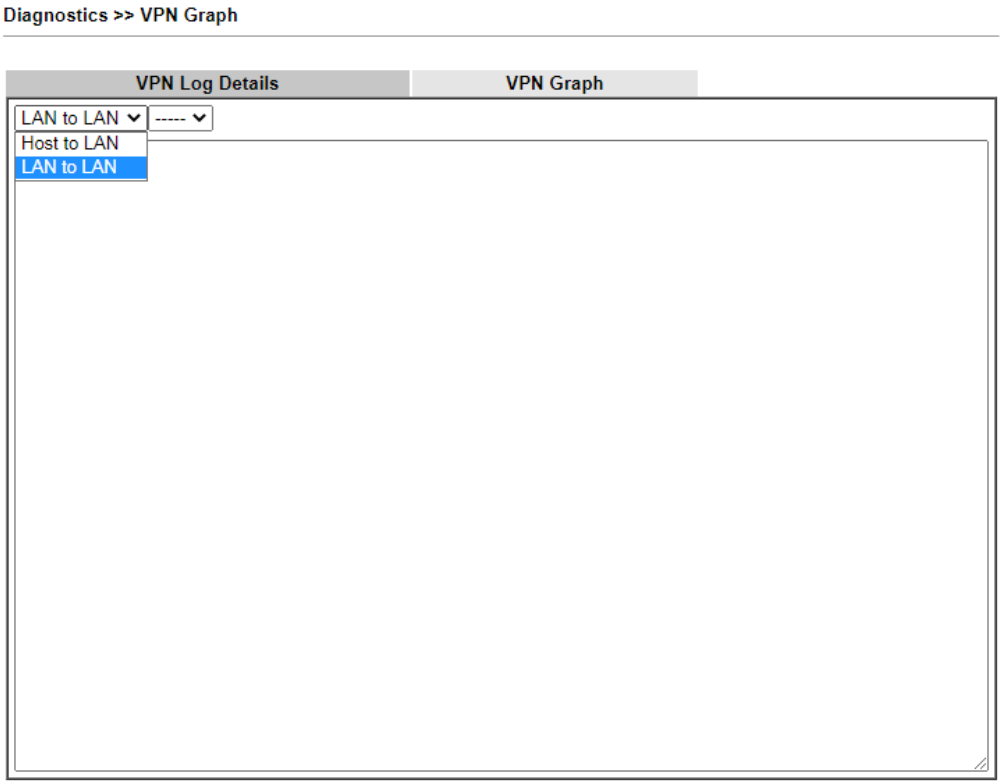



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/LTE/WAN4 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

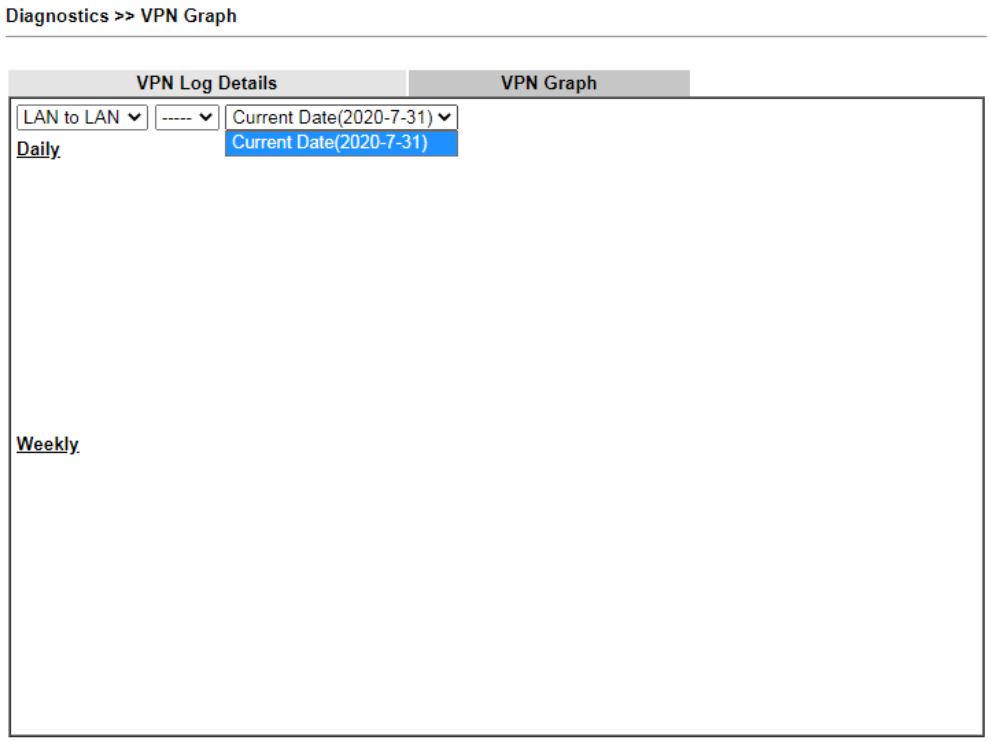
For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

## VIII-1-11 VPN Graph

Click **Diagnostics** and click **VPN Graph** to open the web page.

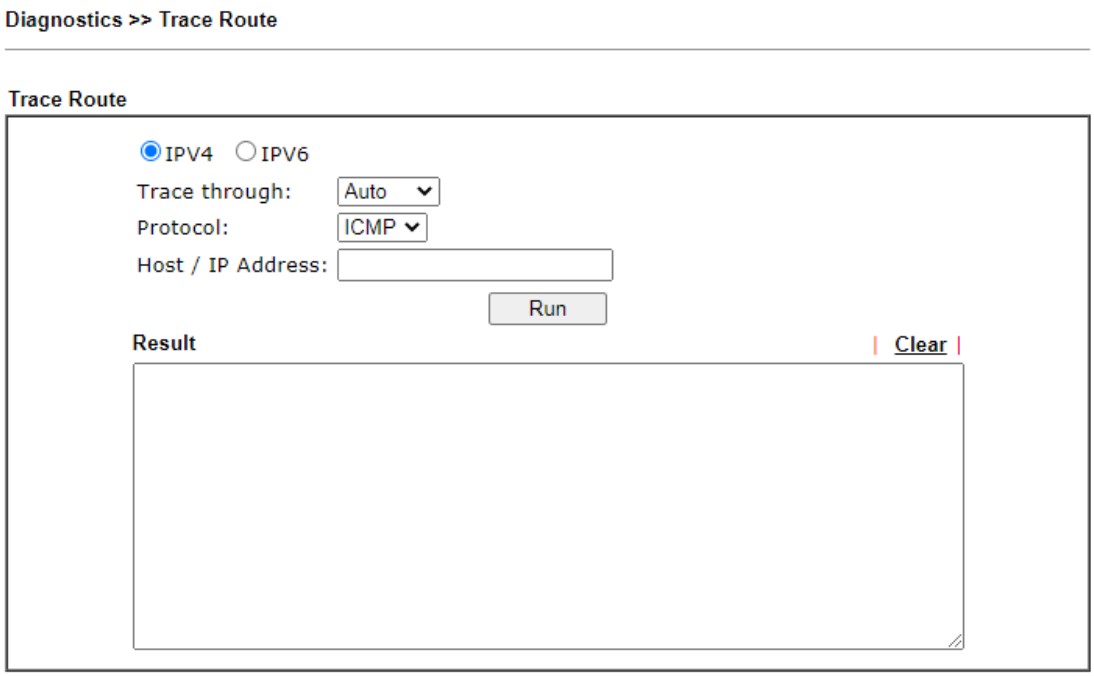



and

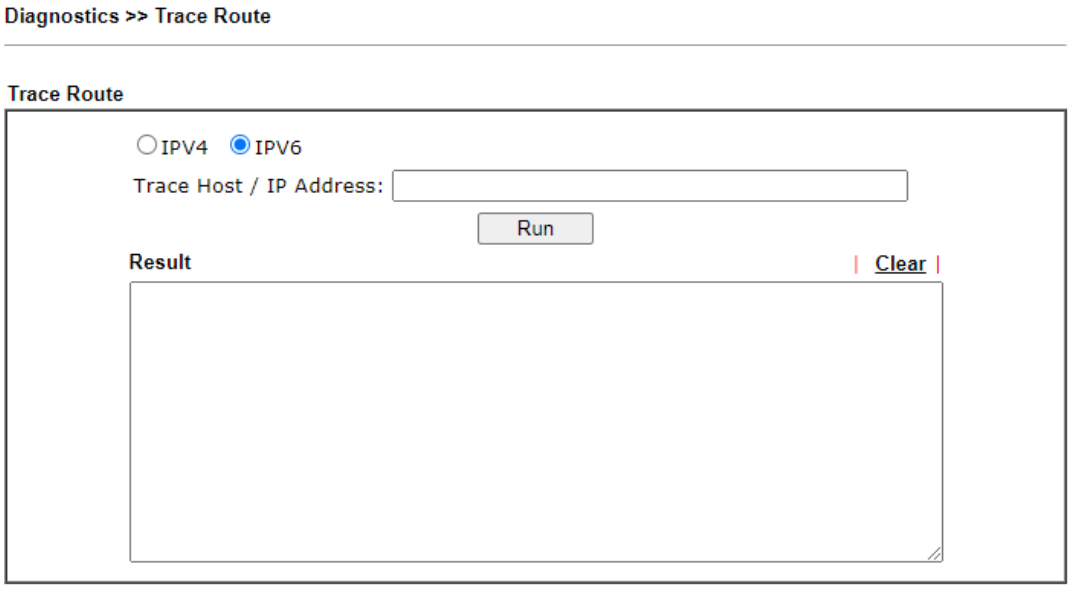


## VIII-1-12 Trace Route

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. |

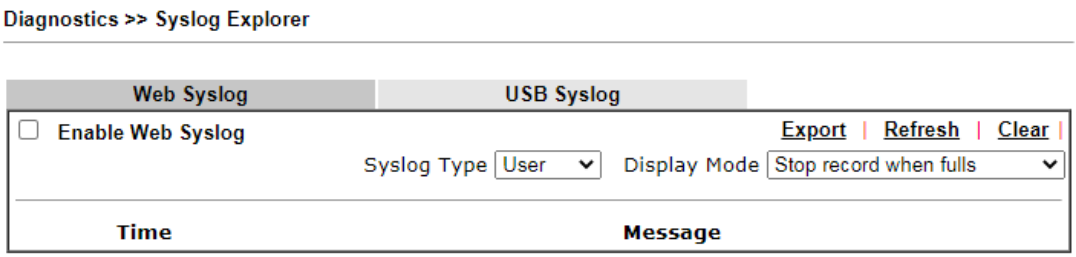
| | |
|---|---|
| **Trace through** | Use the drop down list to choose the interface that you want to ping through. |
| **Protocol** | Use the drop down list to choose the protocol that you want to ping through. |
| **Host/IP Address** | It indicates the IP address of the host. |
| **Trace Host/IP Address** | 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-1-13 Syslog Explorer

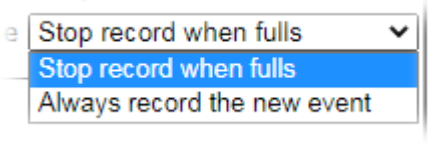
Such page provides real-time syslog and displays the information on the screen.

### 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.

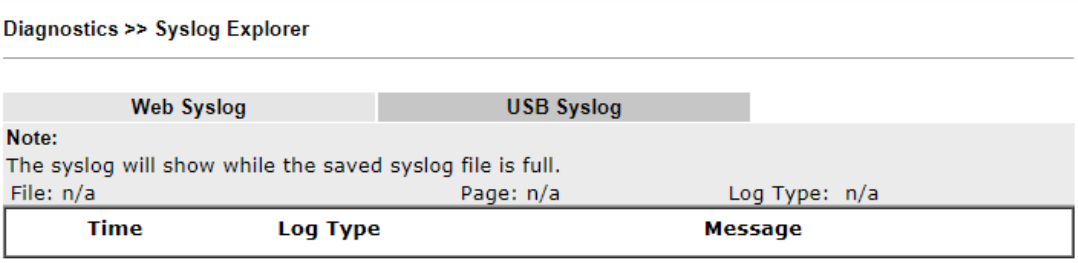



Available settings are explained as follows:

| 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.<br>  <br>**Stop record when fulls –** When the capacity of syslog is full, the system will stop recording.<br>**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.



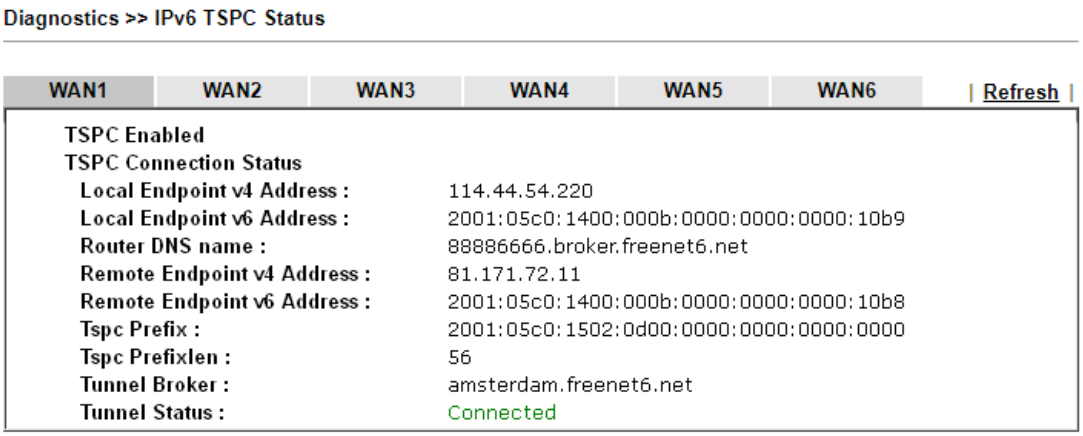

Available settings are explained as follows:

| 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-1-14 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. |

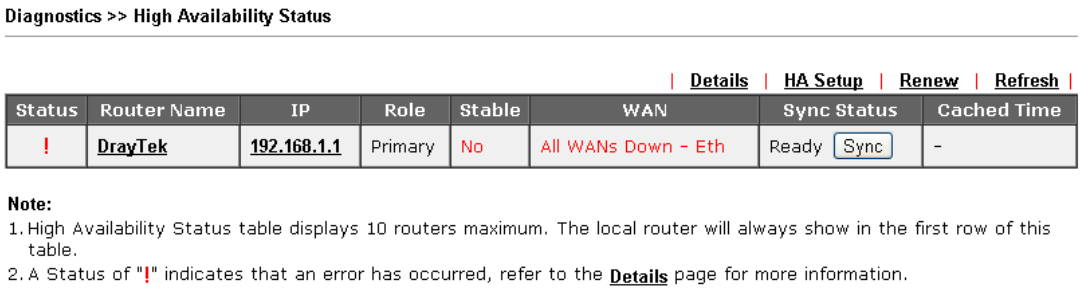
## VIII-1-15 High Availability Status

All of the routers under the same DARP (DrayTek Address resolution Protocol) group can be viewed in such page. However, only partial information of the router status will be displayed.

Vigor routers with the following condtions will be treated as the same DARP group:

- HA enabled
- the same Redundancy method
- the same Group ID
- the same Authentication Key
- the same Management Interface

Open **Diagnostics>>High Availablity Status**.

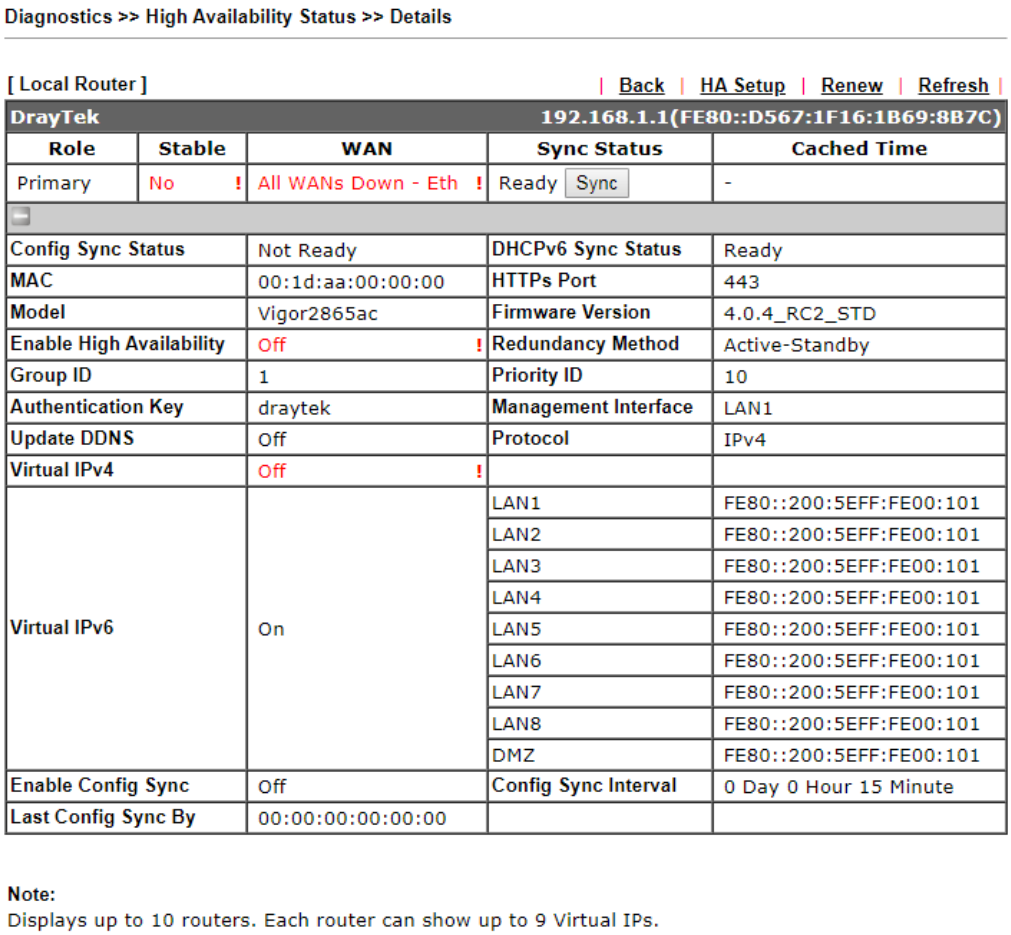



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Details/Back** | **Details –** Click it to display detailed status about HA configuration for the selected router.<br>**Back** – Return to previous page. |
| **HA Setup** | Click it to open **Applications>>High Availability** for modifying the configuration. |
| **Renew** | Click it to get the newest status of other router (except the primary router). |
| **Refresh** | Click it to get the newest status of the primary router. |
| **Status** | **"!"** means an error has occurred. Refer to **Detailed** information and modify HA settings if required. |
| **Router Name** | Display the name of the device. |
| **IP** | Display the IPv4 address of such router. |
| **Role** | "Down" means the function of HA is disabled.<br>"Primary" means such router stands for the primary router in HA.<br>"Secondary" means such router stands for the secondary router in HA. |
| **Stable** | "No" means the primary router has not been determined yet. DARP is negotiating.<br>"YES" means the primary router is determined. |
| **WAN** | "At Least One UP" means that at least one WAN interface connects to Internet.<br>"All WANs Down" means that no WAN interface connects to Internet. |
| **Sync Status** | "Not Ready" means configuration synchronization is unable to execute, or configuration synchronization is disabled, or synchronization initialization executes but fails.<br>"Ready" means configuration synchronization is ready to execute. |

| | |
|---|---|
| | “Progressing” means configuration synchronization is operating.<br>“Fail” means configuration synchronization executed and failed; or wrong model name.<br>“Equal” means the corresponding settings are equal to the primary router. |
| **Cached Time** | Display the time period since the last time to get the newest status of other router (except the primary router). |

Cick the link of **Router Name**, **IP** or **Details**, the following page will be displayed on the screen.



Diagnostics >> High Availability Status >> Details

[ Local Router ] | Back | HA Setup | Renew | Refresh |

| DrayTek | | | 192.168.1.1(FE80::D567:1F16:1B69:8B7C) | |
|---|---|---|---|---|
| **Role** | **Stable** | **WAN** | **Sync Status** | **Cached Time** |
| Primary | No ! | All WANs Down - Eth ! | Ready Sync | - |

| | | | |
|---|---|---|---|
| **Config Sync Status** | Not Ready | **DHCPv6 Sync Status** | Ready |
| **MAC** | 00:1d:aa:00:00:00 | **HTTPs Port** | 443 |
| **Model** | Vigor2865ac | **Firmware Version** | 4.0.4_RC2_STD |
| **Enable High Availability** | Off ! | **Redundancy Method** | Active-Standby |
| **Group ID** | 1 | **Priority ID** | 10 |
| **Authentication Key** | draytek | **Management Interface** | LAN1 |
| **Update DDNS** | Off | **Protocol** | IPv4 |
| **Virtual IPv4** | Off ! | | |
| **Virtual IPv6** | On | LAN1 | FE80::200:5EFF:FE00:101 |
| | | LAN2 | FE80::200:5EFF:FE00:101 |
| | | LAN3 | FE80::200:5EFF:FE00:101 |
| | | LAN4 | FE80::200:5EFF:FE00:101 |
| | | LAN5 | FE80::200:5EFF:FE00:101 |
| | | LAN6 | FE80::200:5EFF:FE00:101 |
| | | LAN7 | FE80::200:5EFF:FE00:101 |
| | | LAN8 | FE80::200:5EFF:FE00:101 |
| | | DMZ | FE80::200:5EFF:FE00:101 |
| **Enable Config Sync** | Off | **Config Sync Interval** | 0 Day 0 Hour 15 Minute |
| **Last Config Sync By** | 00:00:00:00:00:00 | | |

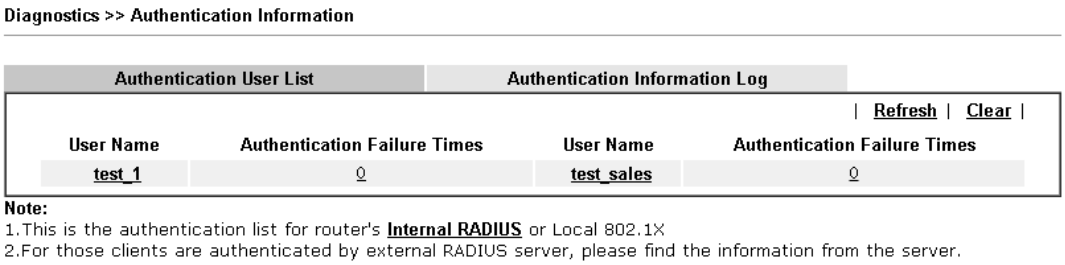
**Note:**
Displays up to 10 routers. Each router can show up to 9 Virtual IPs.

## VIII-1-16 Authentication Information

### Authentication User List

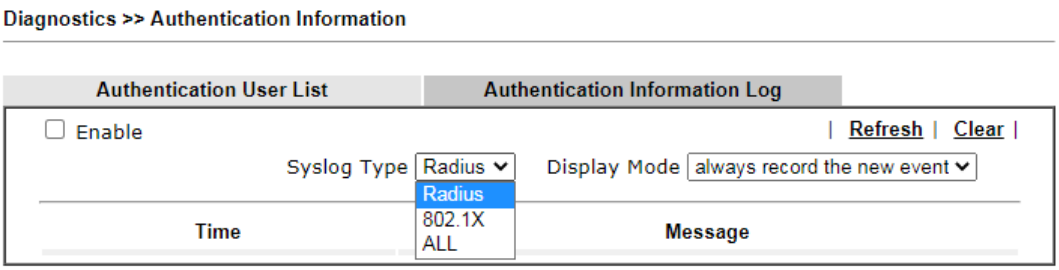
Such page displays authentication jobs made by Internal RADIUS or Local 802.1X.

When the mouse cursor moves to the name link under User Name, the connection message (including authentication failed information) about internal RADIUS or local 802.1X service will be shown by a popped up dialog box.




## Authentication Information Log

This page will display the complete authentication log information.




Available settings are explained as follows:

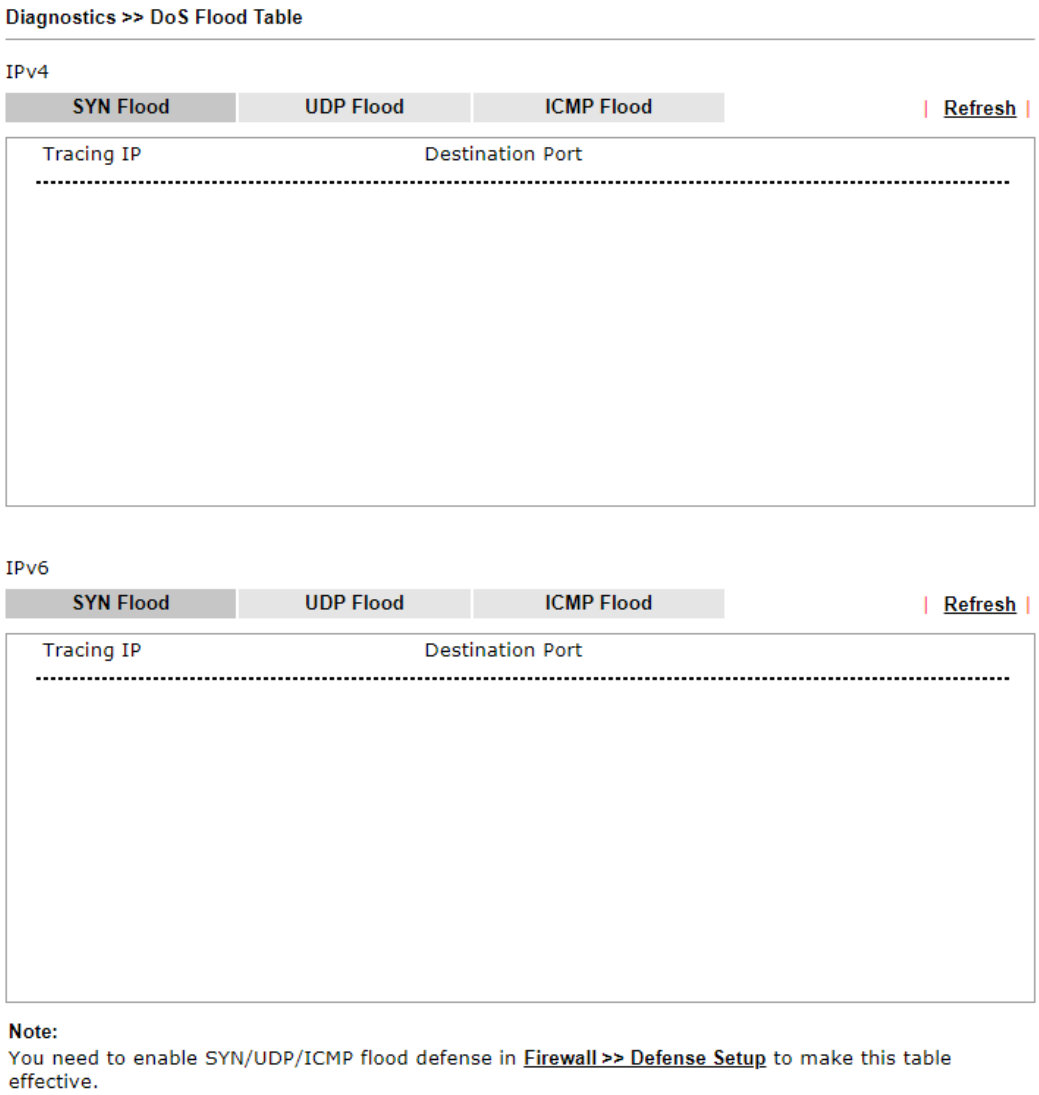
| Item | Description |
|---|---|
| **Enable** | Check the box to enable such function. |
| **Refresh** | Click it to update current page. |
| **Clear** | Click it to remove all of the records. |
| **Syslog Type** | Specify RADIUS, 802.1X or All to display related authentication information log. |
| **Display Mode** | Choose the mode you want to display the related information on the following table.<br>● **Stop record when fulls -** When the capacity of CVM log is full, the system will stop recording.<br>● **Always record the new event -** only the newest events will be recorded by the system. |
| **Time** | Display the time the user authenticated by Vigor2927 series. |
| **Message** | Display authentication information done by Vigor2927 series. |

## VIII-1-17 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.

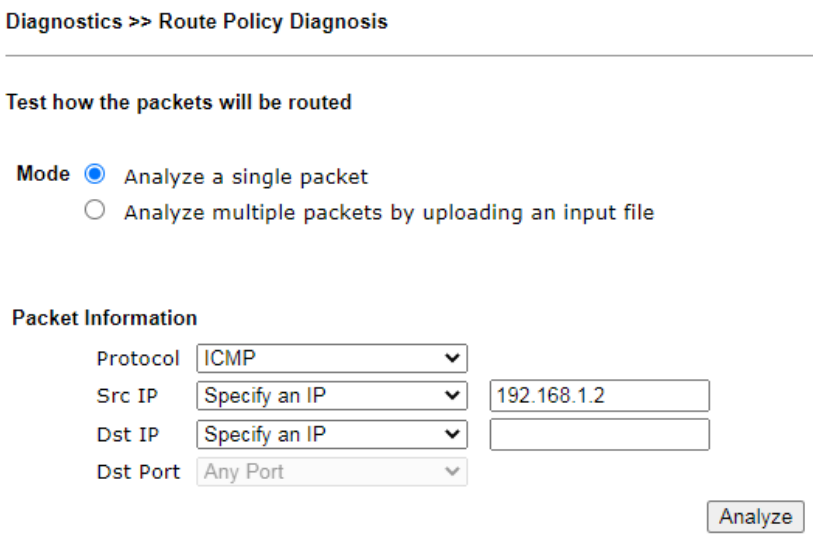



**Info**

The icon - (⊗) - means there is something wrong (e.g., attacking the system) with that IP address.

## VIII-1-18 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.

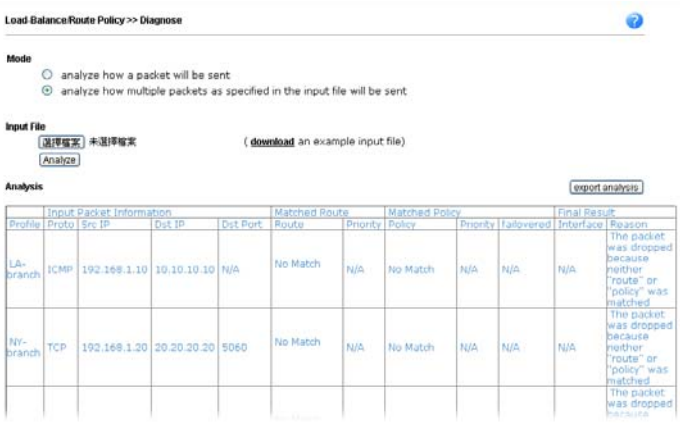



or




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.<br>**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.<br>**ICMP/UDP/TCP/ANY-** Specify a protocol for diagnosis.<br>**Src IP** – Type an IP address as the source IP. |

| | |
|---|---|
| | **Dst IP** – Type an IP address as the destination IP.<br>**Dst Port** – Use the drop down list to specify the destination port.<br>**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.**<br>**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.<br>  <br>**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.<br>  <br>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.

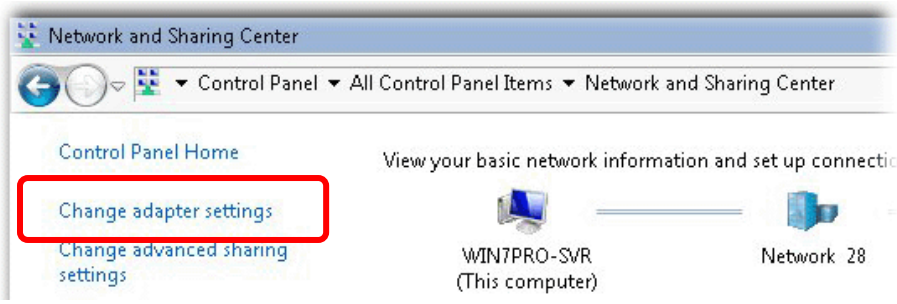
For Windows

| | |
|---|---|
| **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. |

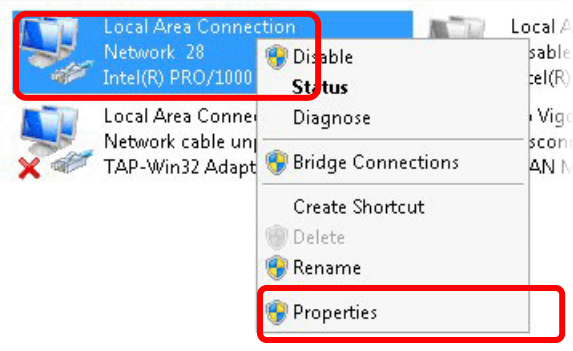
1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**



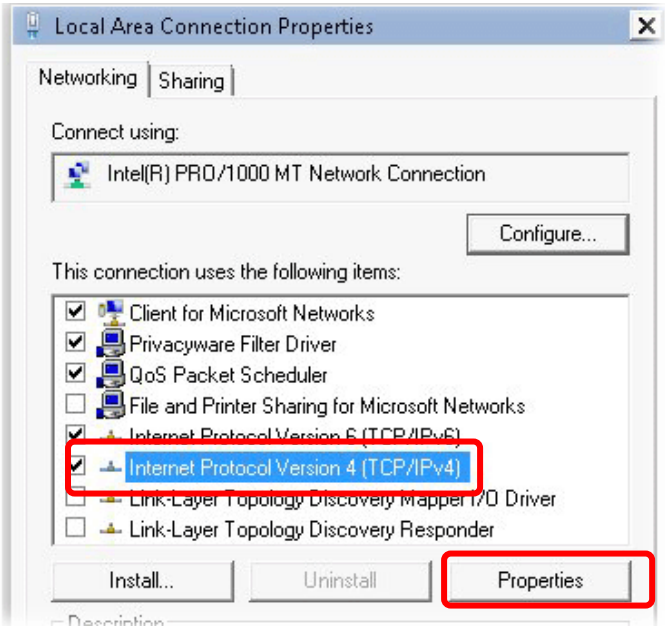

2. In the following window, click **Change adapter settings**.



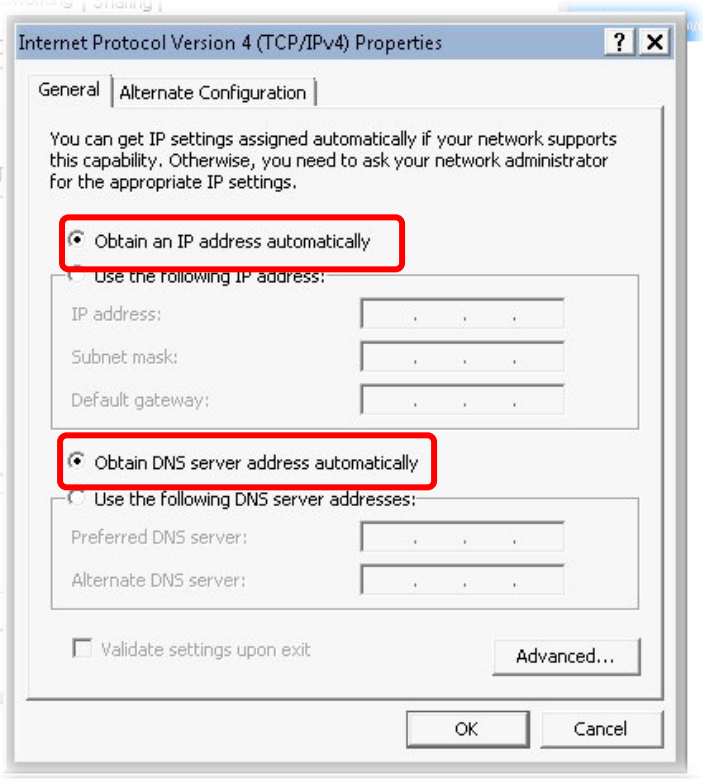

3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



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

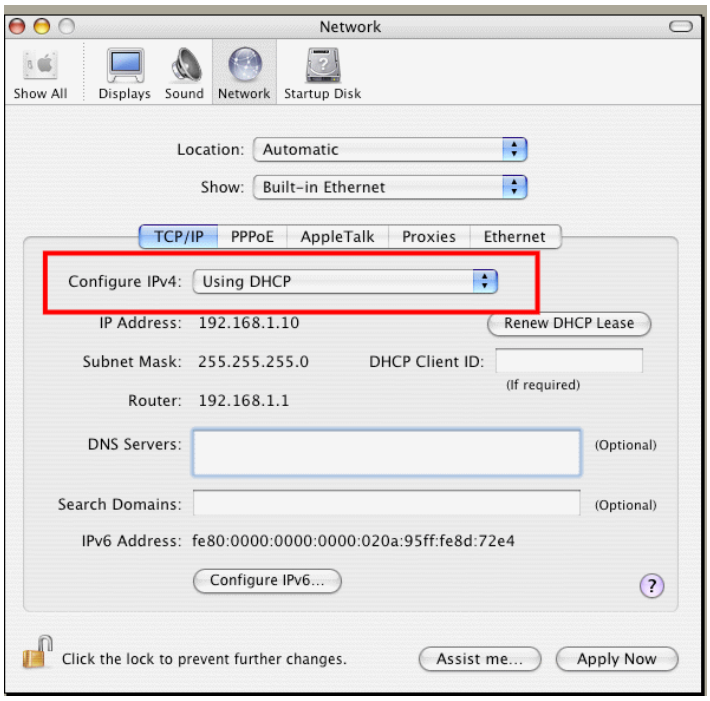



5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



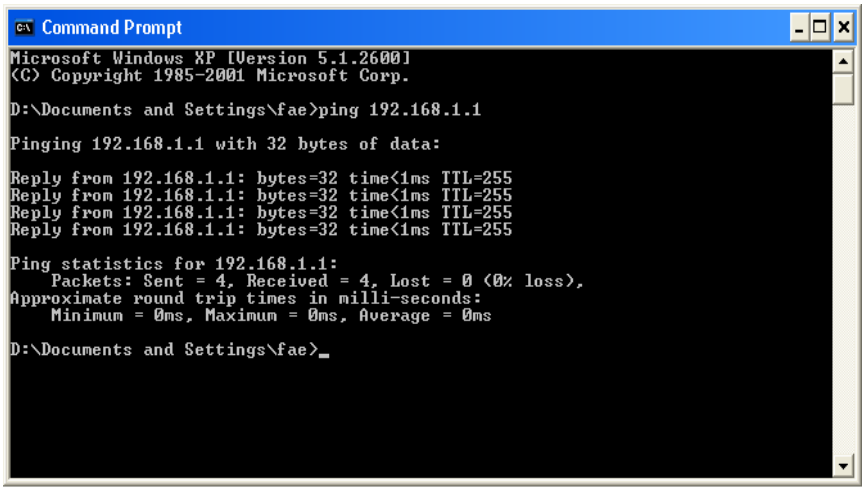
# VIII-4 Pinging the Router from Your Computer

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

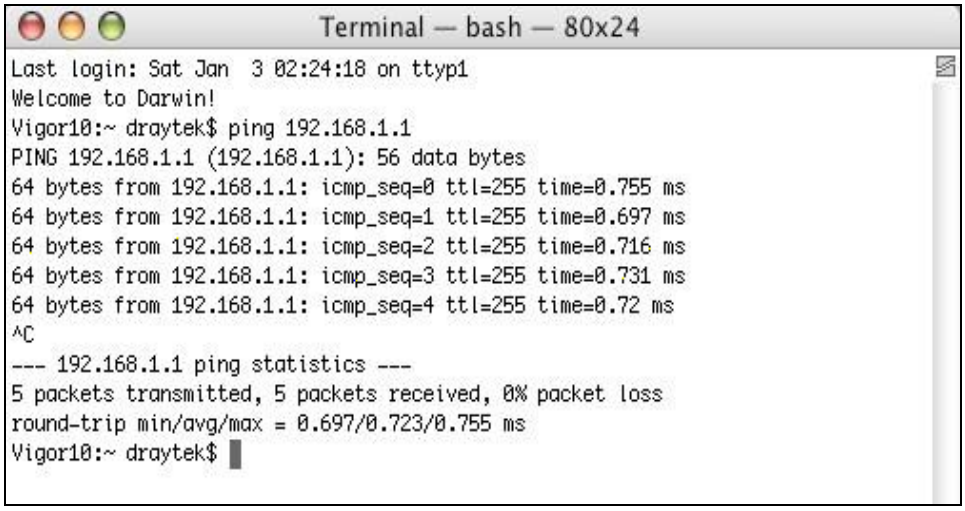
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.




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.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

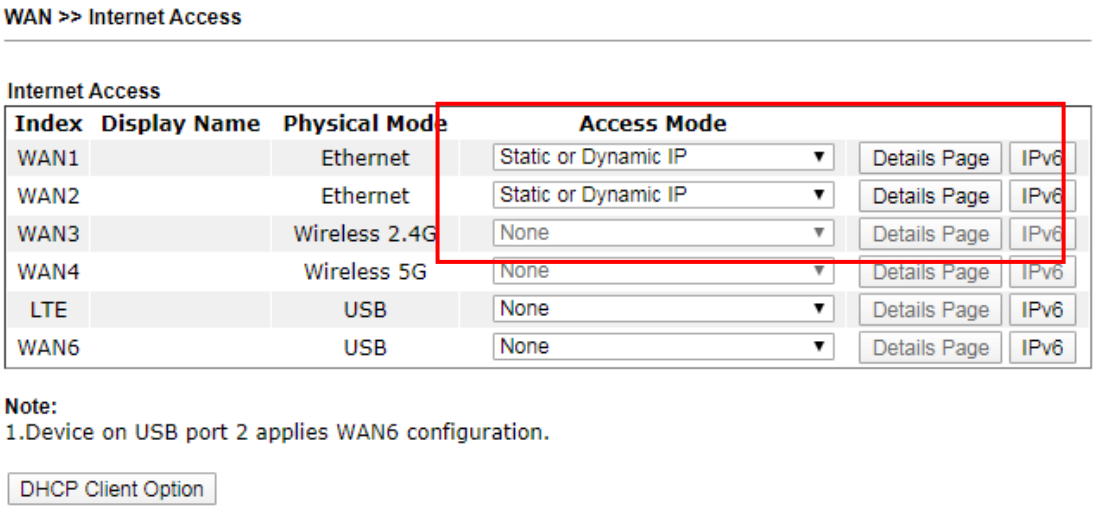
# VIII-5 Checking If the ISP Settings are OK or Not

If WAN connection cannot be up, check if the LEDs (according to the LED explanations listed on section I-1-1, Indicators and Connectors) are correct or not. If the LEDs are off, please:

- Change the **Physical Type** from **Auto negotiation** to other values (e.g., 100M full duplex).
- Next, change the physical type of modem (e.g., DSL/FTTX(GPON)/Cable modem) offered by ISP with the same value configured in Vigor router. Check if the LEDs on Vigor router are on or not.
- If not, please install an additional switch for connecting both Vigor router and the modem offered by ISP. Then, check if the LEDs on Vigor router are on or not.
- If the problem of LEDs cannot be solved by the above measures, please contact with the nearest reseller, or send an e-mail to DrayTek FAE for technical support.
- Check if the settings offered by ISP are configured well or not.

When the LEDs are on and correct, yet the WAN connection still cannot be up, please:

- Open **WAN >> Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1~WAN6 to review the settings that you configured previously.



# VIII-6 Problems for 3G/4G Network Connection

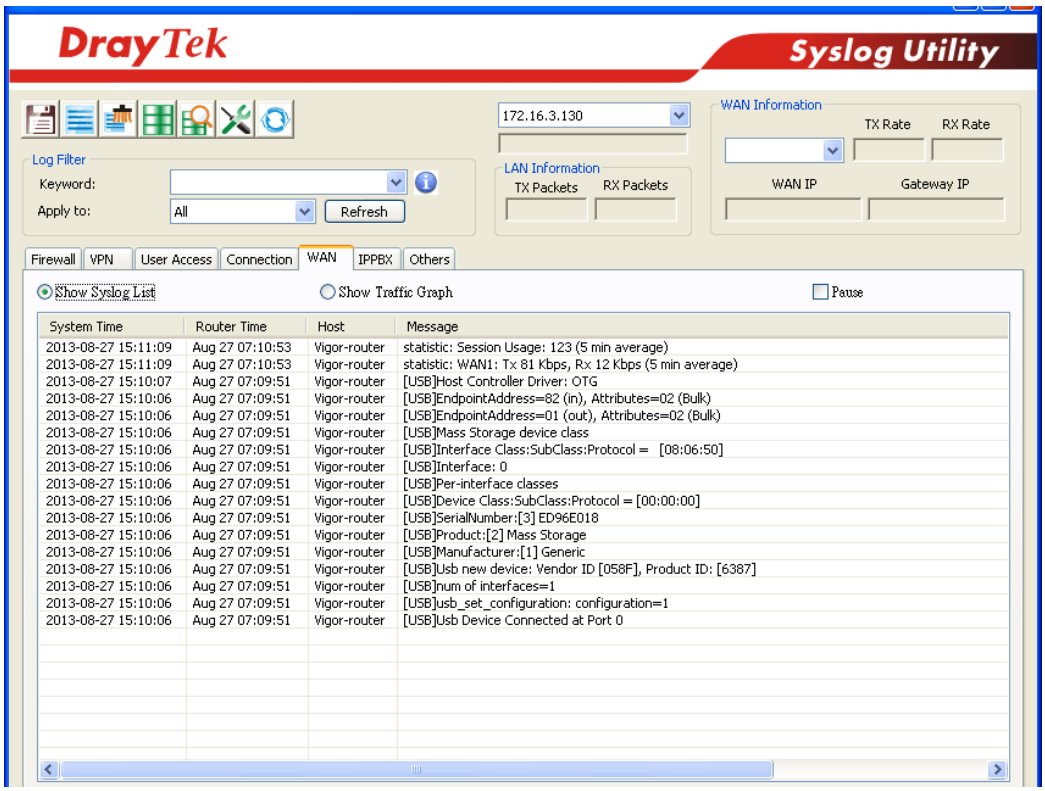
When you have trouble in using 3G/4G network transmission, please check the following:

### Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G/4G USB Modem into your Vigor2927. 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 Vigor2927.

### 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 Vigor2927. In addition, please refer to the manual of 3G/4G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

# VIII-7 Backing to Factory Default Setting If Necessary

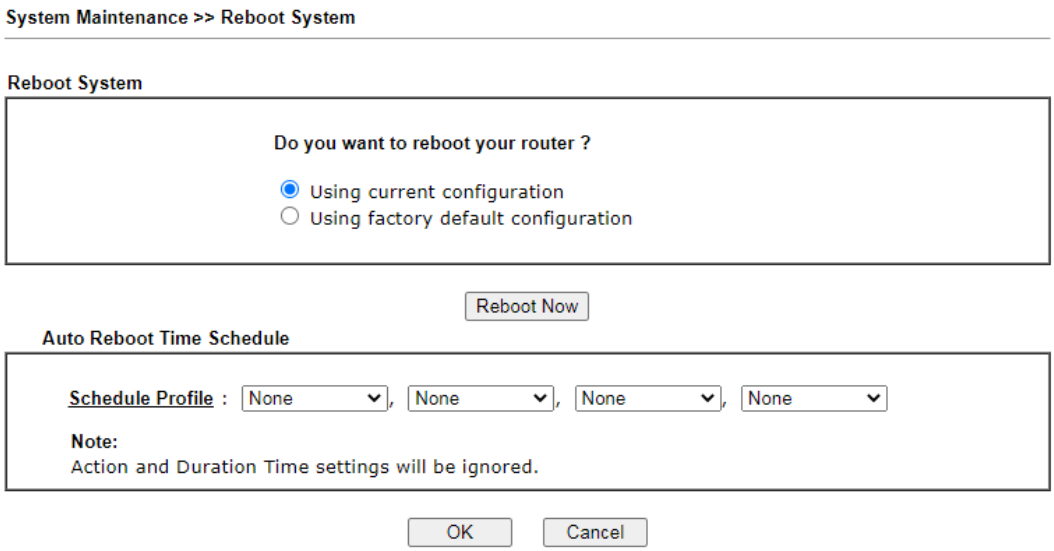
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.

| | |
|---|---|
| **Info** | After pressing factory default setting, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null. |

## Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.




## Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.




After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

# VIII-8 Contacting DrayTek

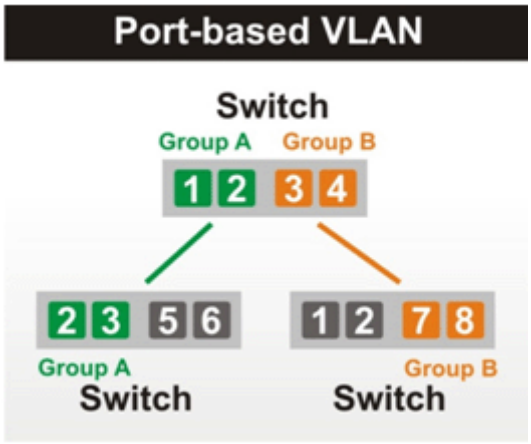
If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

# Appendix I: VLAN Applications on Vigor Router

Virtual Local Area Network is so-called VLAN. It offers the logical grouping technique to separate the physical ports of Ethernet switches, thus we can manage our local network easier, more flexible and secure. For instance, you're a networking administrator in your company and you're planning to isolate the visitors' traffics from your private network for security considerations because you cannot ensure that visitors' computer is clean. Or you want to separate your private network into several parts by divisions because there are too many computers in the same network segment and it results in the local traffics heavily. VLAN helps you to solve these situations, and DrayTek's products support bellow two popular types:

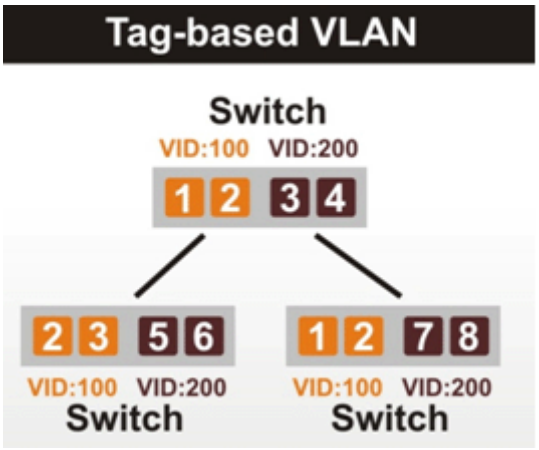
### Port-based

It uses a matrix table of the physical ports to define the traffics how to exchange between each port, and the traffics will be isolated from the ports are not being ticked in the same line. It is the easiest way to setup an isolate network, but not a flexible way to maintain a growing network. Because the idea of port-based VLAN is grouping by physical ports, but the difficulty is how to handle the traffics between two or more Ethernet switches. Thus, VLAN is suitable for some circumstances, for example, the rental apartment, SOHO office…and so on. These clients may need two or three isolated networks only and setup a network in a simple way.




### Tag-based

The idea of tag-based VLAN is to identify a virtual LAN with a specific ID, therefore, **VLAN ID** introduced by tag-based VLAN. Through VLAN ID, ports with different **VID (VLAN ID) will be** identified as in different LANs, so the traffics also will be isolated from each of VLANs. Many administrators who manage an enterprise network or even the internet service providers (ISP) adopt Tag-based VLAN popularly because it is convenient to maintain and manage a distributed network. Setting a large-scale network is easy by giving each of them with different VID and isolating the traffics at the same time. Besides the VLAN ID, there is another feature, **Trunk**, introduced. While the role of a port on an Ethernet switch is setup as a Trunk port, it means the VLAN ID will be kept while forwarding the packets between switches. By this feature, VLANs are able to distribute over two or more Ethernet switches easily, moreover design a large and secured network is possible through Trunk port. When VLAN is being enabled on Vigor routers, the LAN ports are being turned into Trunk mode automatically. Therefore, a VLAN supported switch, like VigorSwitch G2260/P2261, or VigorSwitch G1240, is needed.




Vigor routers [Note] support Tag-based feature both on LAN and WAN interfaces. The next we'll demonstrate our web design and how to configure the settings by introducing the functionalities of Vigor router.

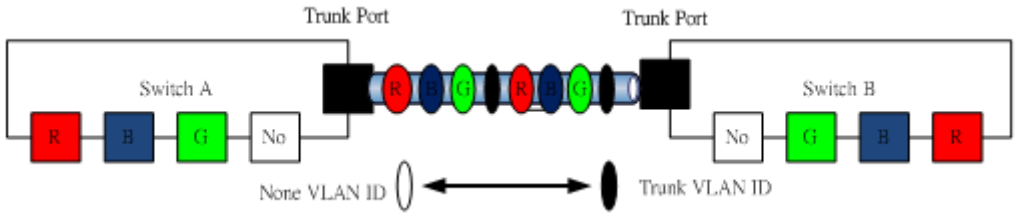
**[Note]**

**Broadband router: Vigor2920/Vigor3200/Vigor2925/Vigo2960/Vigor3900**

**Modem router: Vigor2850/Vigor2927**

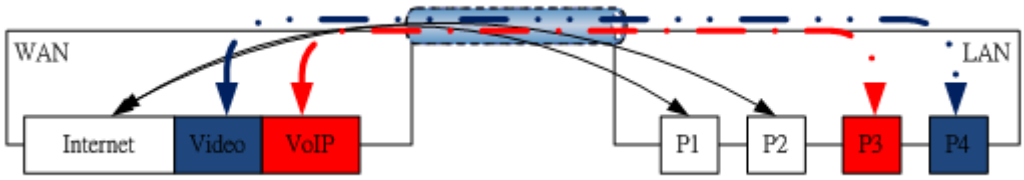
## VLAN Packets on Vigor routers

Trunk mode of LAN




Trunk Port can carry the packets with VID but replace the Non-VID packet as the VID of Trunk port while forwarding the packets to another switch.

Bridge mode of WAN

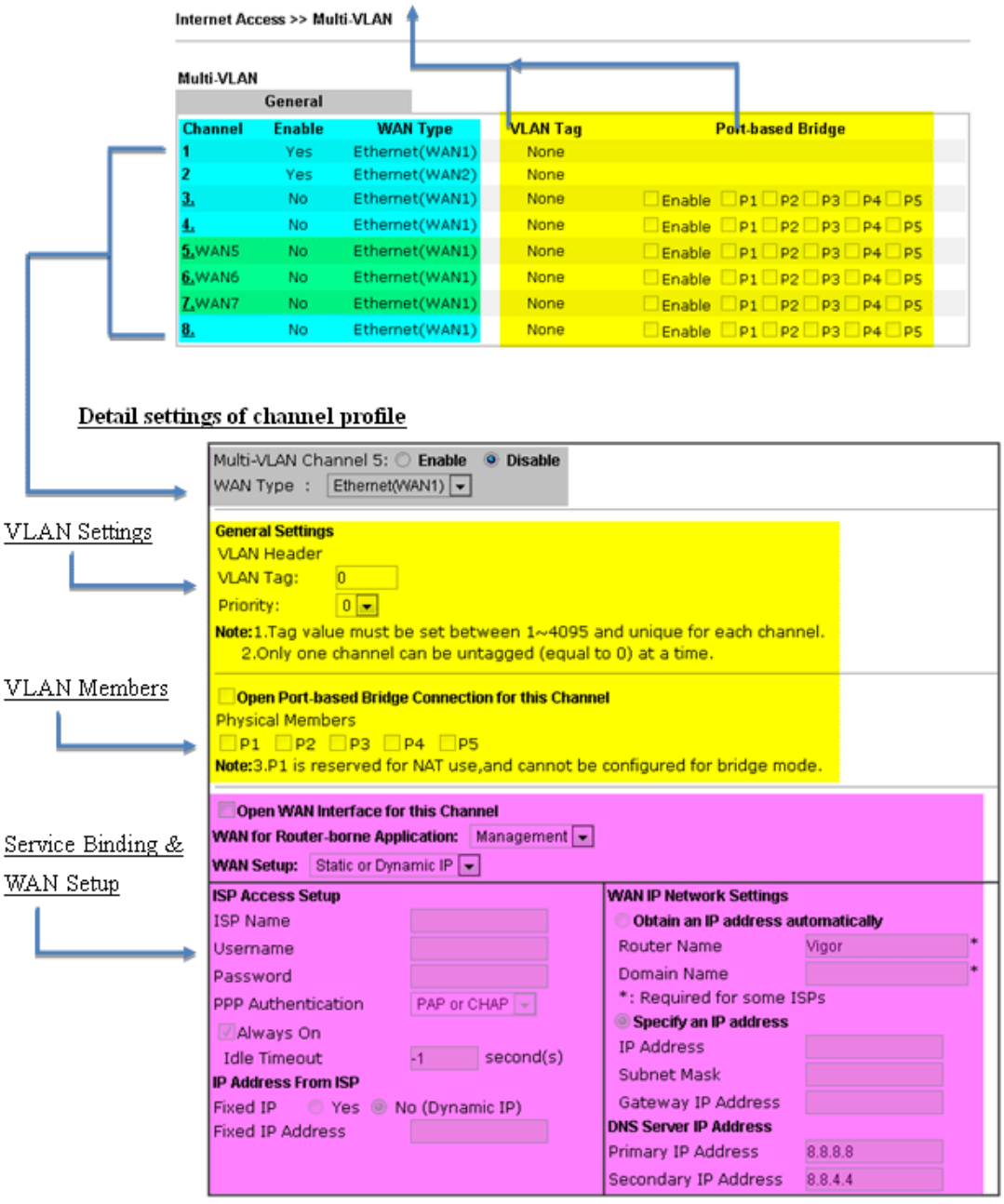



P1 and P2 are doing NAT flow to access to the internet, but P3 and P4 will forward the packets between WAN and LAN ports directly.

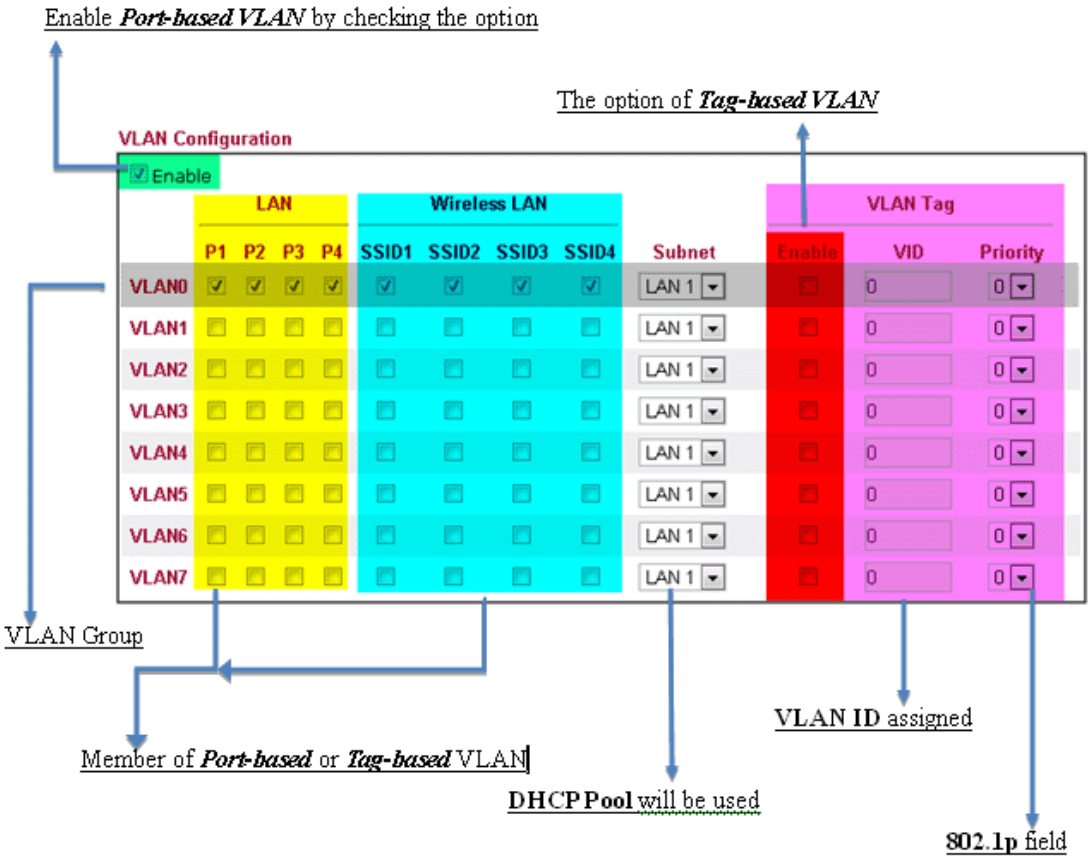
## Web User Interface

So far, there are two kinds of open system on Vigor router. One is DrayOS, which is DrayTek owned, and another is Linux-like which customized by DrayTek from OpenWRT. Here DrayOS system is going to be introduced to you because it is the most stable and superfast booting system in DrayTek products. If the UI style of yours is different from the following. It may not DrayOS system with new web style or maybe the Linux-like model.

**WAN**

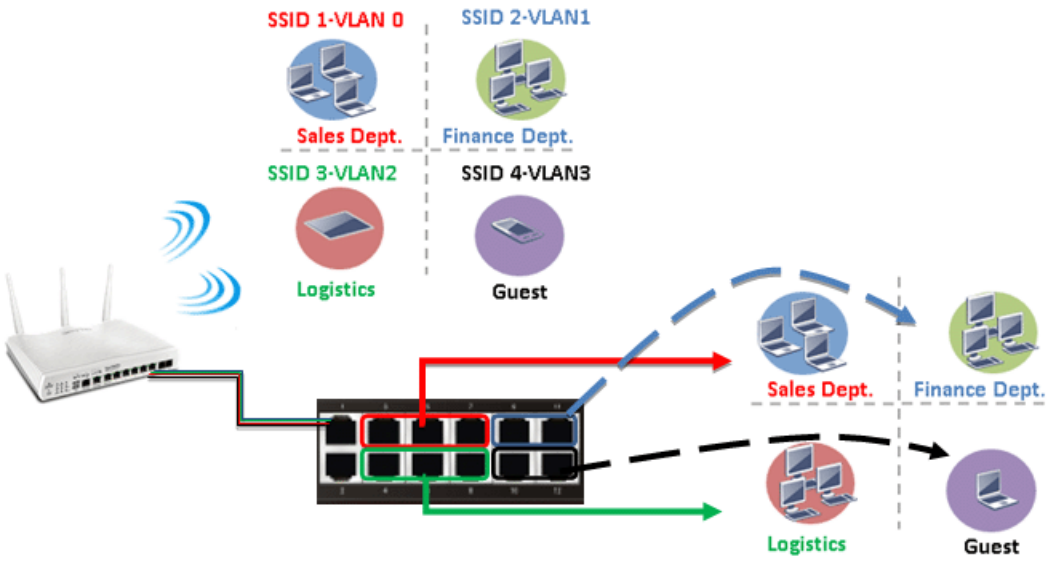

Internet Access >> Multi-VLAN
Multi-VLAN
General
Channel Enable WAN Type VLAN Tag Port-based Bridge
1 Yes Ethernet(WAN1) None
2 Yes Ethernet(WAN2) None
3. No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
4. No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
5.WAN5 No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
6.WAN6 No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
7.WAN7 No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
8. No Ethernet(WAN1) None Enable P1 P2 P3 P4 P5
Detail settings of channel profile
Multi-VLAN Channel 5: Enable Disable
WAN Type : Ethernet(WAN1)
VLAN Settings
General Settings
VLAN Header
VLAN Tag: 0
Priority: 0
Note:1.Tag value must be set between 1~4095 and unique for each channel.
2.Only one channel can be untagged (equal to 0) at a time.
VLAN Members
Open Port-based Bridge Connection for this Channel
Physical Members
P1 P2 P3 P4 P5
Note:3.P1 is reserved for NAT use,and cannot be configured for bridge mode.
Service Binding &
WAN Setup
Open WAN Interface for this Channel
WAN for Router-borne Application: Management
WAN Setup: Static or Dynamic IP
ISP Access Setup
ISP Name
Username
Password
PPP Authentication PAP or CHAP
Always On
Idle Timeout -1 second(s)
IP Address From ISP
Fixed IP Yes No (Dynamic IP)
Fixed IP Address
WAN IP Network Settings
Obtain an IP address automatically
Router Name Vigor *
Domain Name *
*: Required for some ISPs
Specify an IP address
IP Address
Subnet Mask
Gateway IP Address
DNS Server IP Address
Primary IP Address 8.8.8.8
Secondary IP Address 8.8.4.4

**LAN**

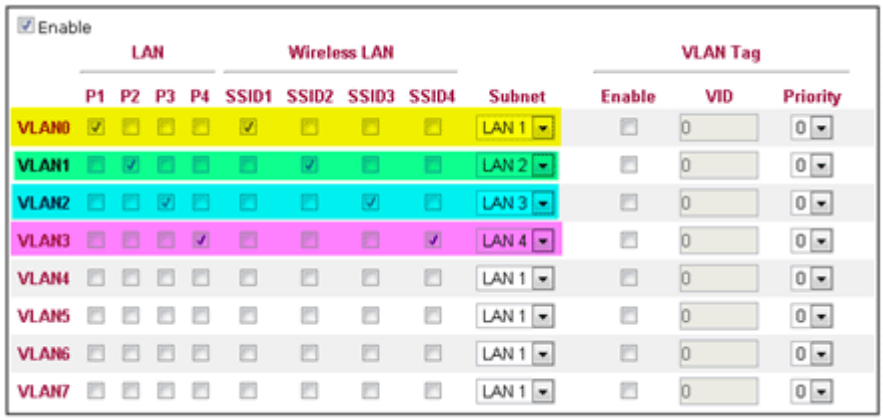



VLAN applications on Vigor router

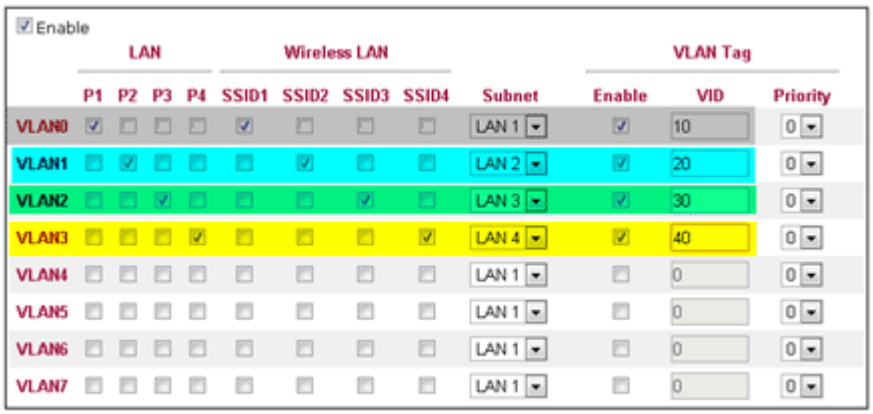
- **Multi Subnet (VLAN of LAN)**



*Port-based mode*

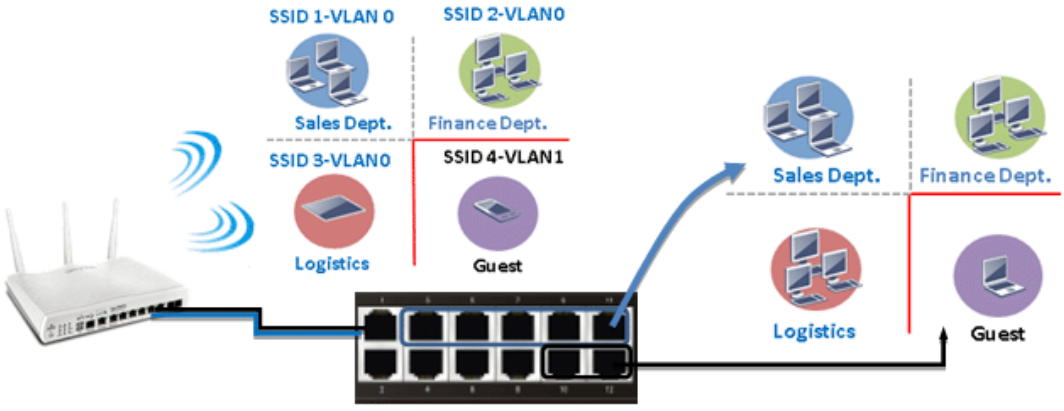



*Tag-based mode*

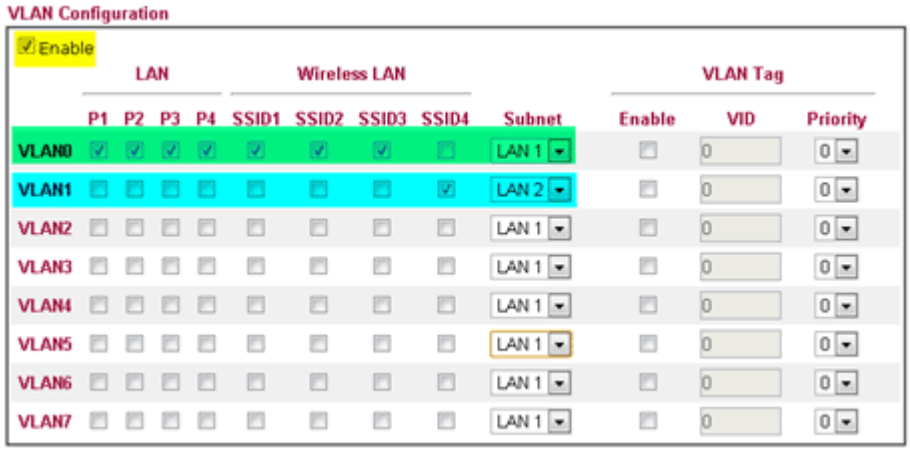



By above settings, there are four private networks will be created and computers attached with each of LAN ports or SSIDs which are able to obtain a private IP address from each DHCP server (LAN1/LAN2/LAN3/LAN4). However, the traffics of the LAN port or SSID that are NOT being grouped in the same VLAN are unable to forward to each other. The benefit of Port-based is able to extend the wired ports by installing a cheaper dumb switch as many as you need, but Tag-based offers you a flexible and well-managed network. The networks are isolated, secured and reduce the broadcasting storm effectively in each of networks with VLAN.

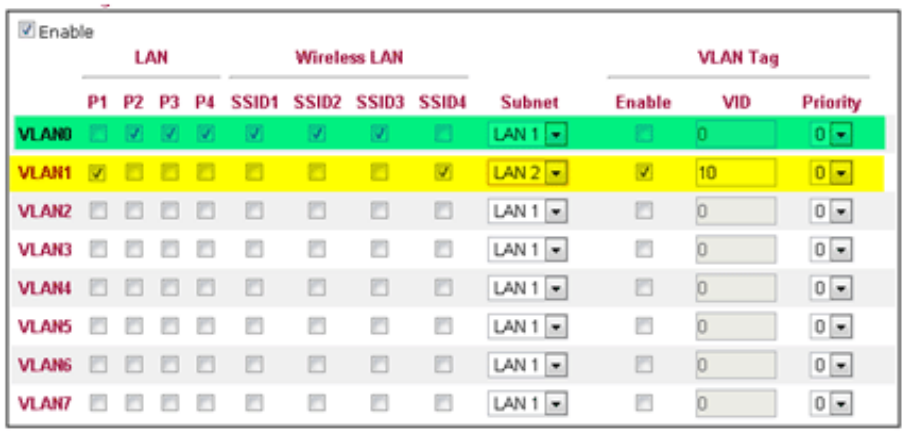
- **Guest Network**



*Port-based mode*



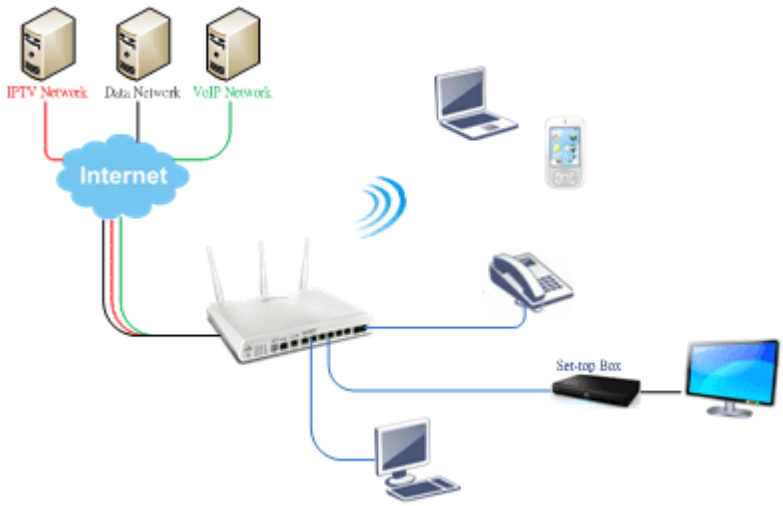

*Tag-based mode*



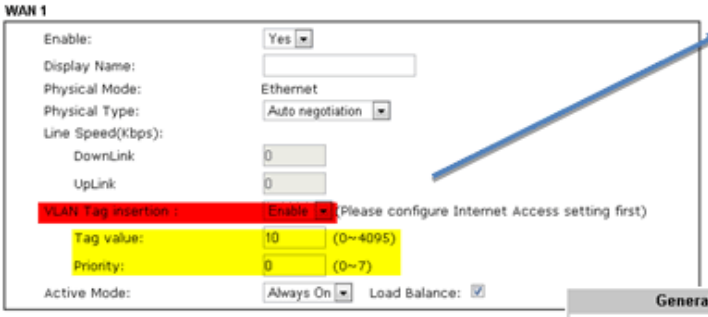

To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

- **Triple Play (Multi-WAN)**

*NAT mode with VLAN*

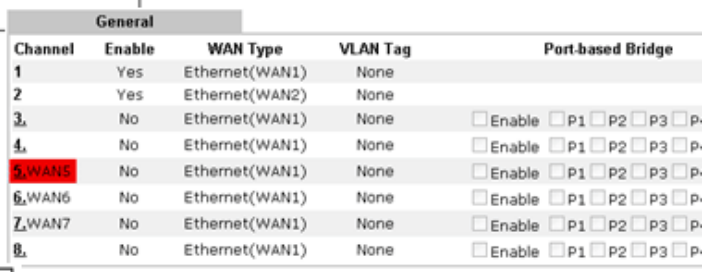



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.



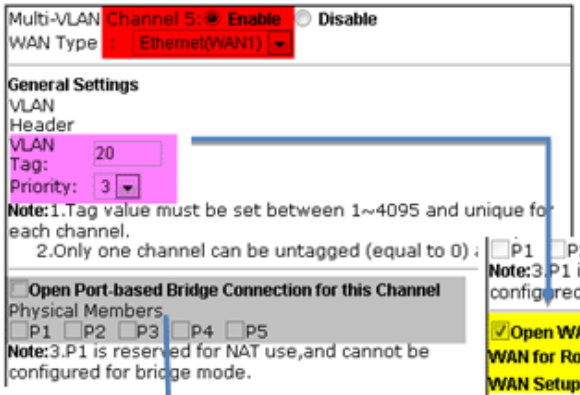

1. Setup the VLAN ID on WAN1 profiles if WAN is the primary interface of IPTV service.

2. Open the profile of WAN5 by clicking the ID.



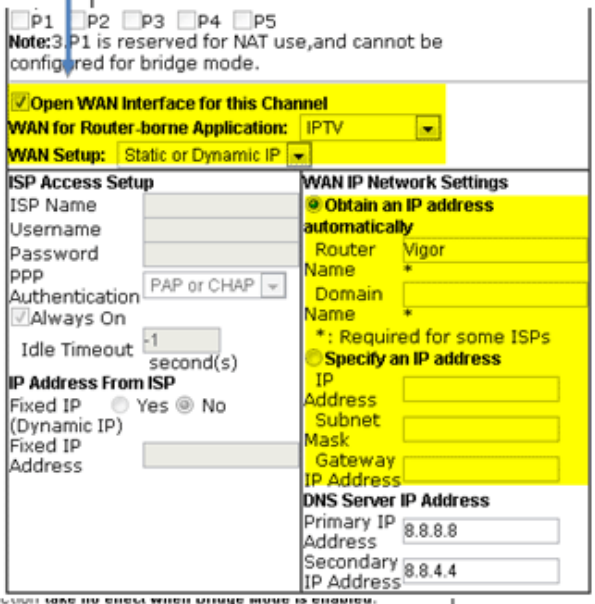
General

| Channel | Enable | WAN Type | VLAN Tag | Port-based Bridge |
|---|---|---|---|---|
| 1 | Yes | Ethernet(WAN1) | None | |
| 2 | Yes | Ethernet(WAN2) | None | |
| 3. | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |
| 4. | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |
| 5.WAN5 | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |
| 6.WAN6 | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |
| 7.WAN7 | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |
| 8. | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 |

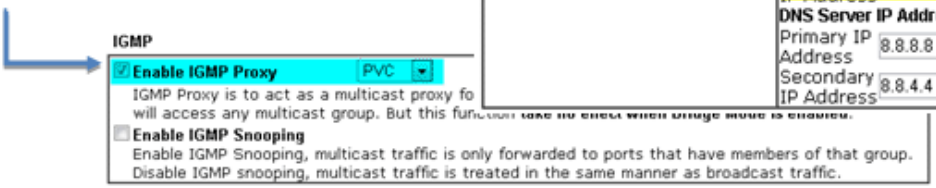



NO need to enable Port-based Bridge.

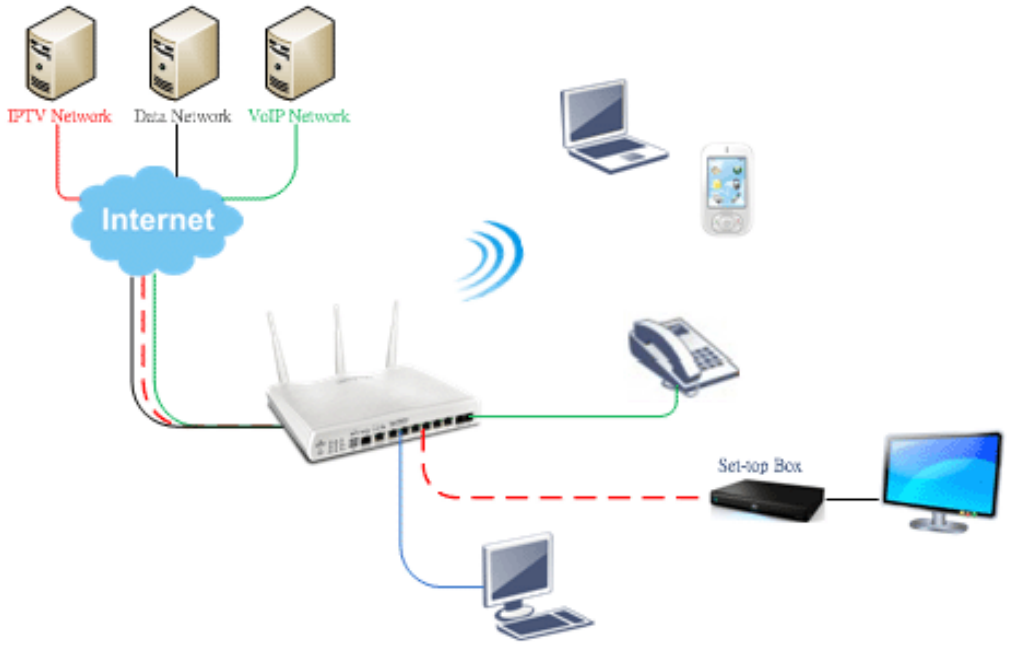
3. Setup connection of WAN 5 and bind the service onto it.




4. Go to **Application** >> **IGMP** to bind it on PVC WAN.



*Bridge mode with VLAN*




**Multi-VLAN**

**General**

| Channel | Enable | WAN Type | VLAN Tag | Port-based Bridge |
|---|---|---|---|---|
| 1 | Yes | Ethernet(WAN1) | None | |
| 2 | Yes | Ethernet(WAN2) | None | |
| 3. | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 P5 |
| 4. | No | Ethernet(WAN1) | None | Enable P1 P2 P3 P4 P5 |
| 5.WAN5 | No | | | |
| 6.WAN6 | No | | | |
| 7.WAN7 | No | | | |
| 8. | No | | | |

Multi-VLAN Channel 3: **Enable** **Disable**

WAN Type : Ethernet(WAN1)

**General Settings**

VLAN Header

VLAN Tag: 10

Priority: 4

**Note:**1.Tag value must be set between 1~4095 and unique for each channel.
2.Only one channel can be untagged (equal to 0) at a time.

**Bridge mode**

Enable

Physical Members

P1 P2 P3 P4 P5

**Note:**3.P1 is reserved for NAT use,and cannot be configured for bridge mode.

Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.

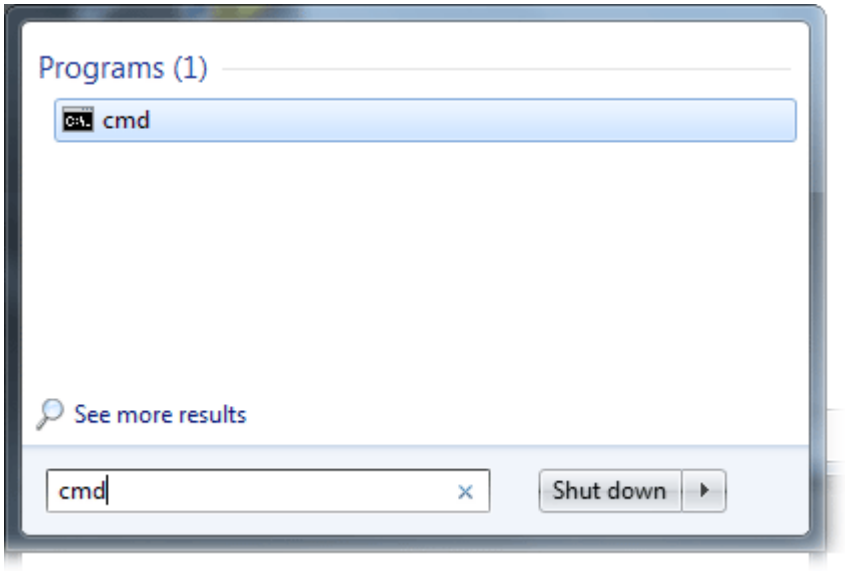
# Part IX Telnet Commands

# Accessing Telnet of Vigor2927

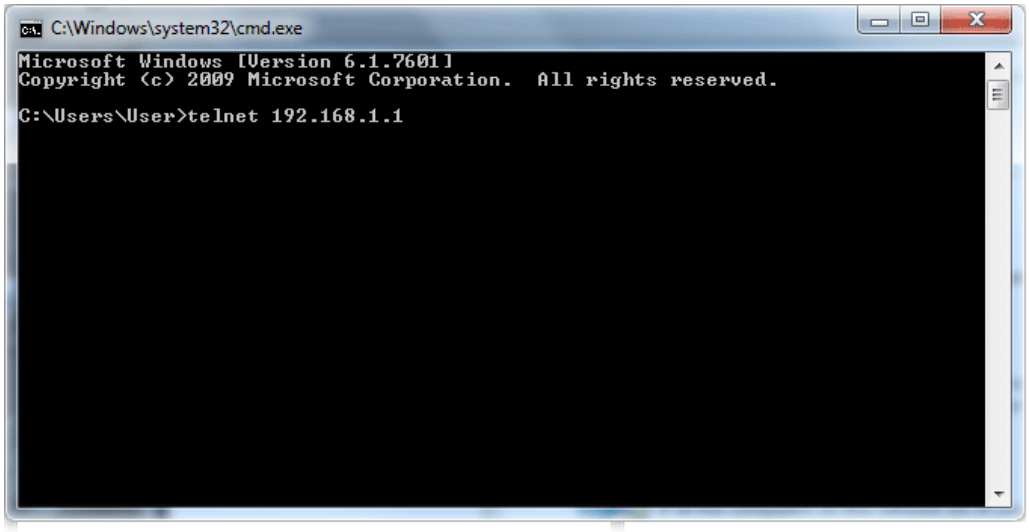
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

| | |
|---|---|
| **Info** | For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under **Control Panel>>Programs**. |

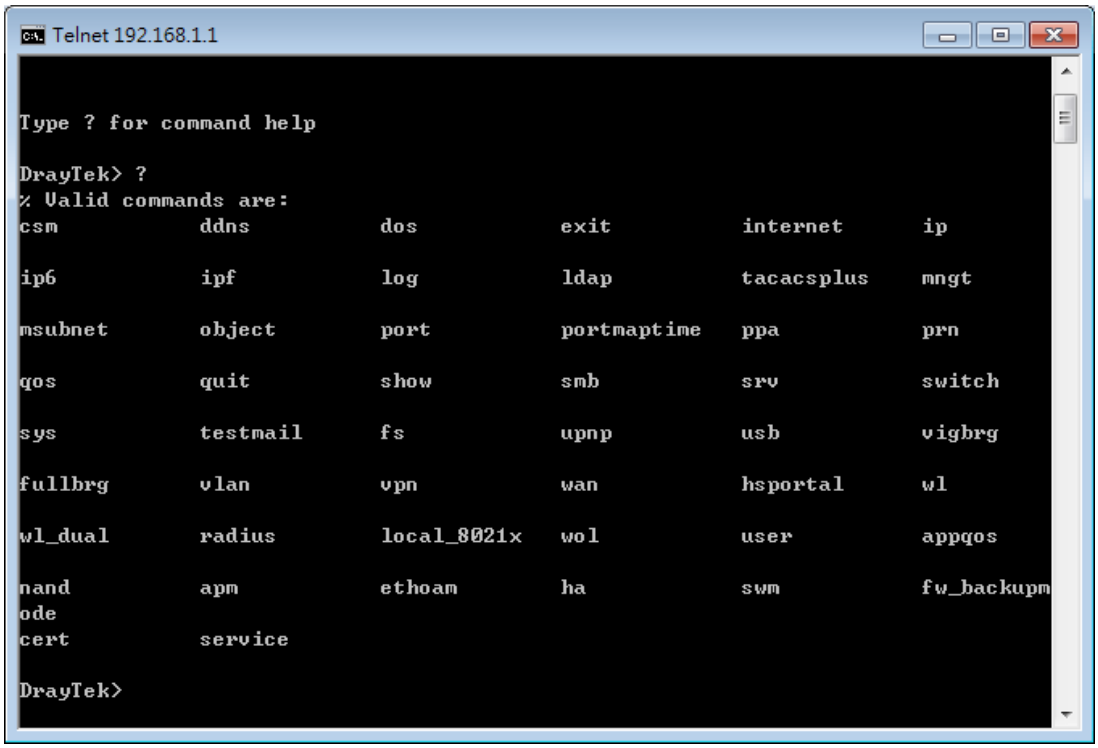
Type **cmd** and press Enter. The Telnet terminal will be open later.



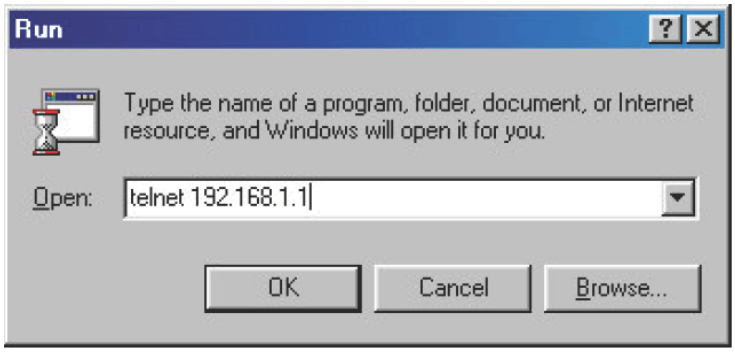

In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.




Next, enter admin/admin for Account/Password. Then, enter **?**. You will see a list of valid/common commands depending on the router that your use.




For users using previous Windows system (e.g., 2000/XP), simply click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Next, type admin/admin for Account/Password. And, type **?** to get a list of valid/common commands.



## 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| -a AP_IDX [ACTION]]*

### Syntax Description

| Parameter | Description |
|---|---|
| *INDEX* | Specify the index number of CSM profile, from 1 to 32. |
| *- v* | View the IM/P2P/Protocol and Others configuration of the CSM profile. |
| *-e* | Enable to block specific application. |
| *-d* | Disable to block specific application. |
| *-a* | Set the action of specific application |
| *GROUP* | Specify the category of the application. Available options are: IM, P2P, Protocol and Others. |
| *AP_IDX* | Each application has independent index number for identification in CLI command. |

| | |
|---|---|
| | Specify the index number of the application here. If you have no idea of the inex number, do the following (Take IM as an example):<br>Type "csm appe set –I 1 –v IM", the system will list all of the index numbers of the applications categorized under IM. |
| *ACTION* | Specify the action of the application, 0 or 1.<br>0: Block. All of the applications meet the CSM rule will be blocked.<br>1: Pass. All of the applications meet the CSM rule will be passed. |

### Example

```
>csm appe set -i 1 -a 1 1
Profile 1 - : <NULL> action set to Pass.
>
```

## Telnet Command: csm appe show

It is used to display group (IM/P2P/Protocol and Others) information APP Enforcement Profile.

**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             MS Teredo           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 | -I [P|B|A|N] | uac | wf ]*

**csm ucf obj** *INDEX -n PROFILE_NAME*

**csm ucf obj** *INDEX -p VALUE*

**csm ucf obj** *INDEX -I P|B|A|N*

**csm ucf obj** *INDEX uac*

**csm ucf obj** *INDEX wf*

### Syntax Description

| Parameter | Description |
|---|---|
| *show* | 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.<br>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.<br>0: It means Bundle: Pass.<br>1: It means Bundle: Block.<br>2: It means Either: URL Access Control First.<br>3: It means Either: Web Feature First. |
| *-l* | It means the log type of the profile. They are:<br>P: Pass,<br>B: Block,<br>A: All,<br>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.<br>B: Block. The web access meets the URL Access Control will be blocked.<br>P: Pass. The web access meets the URL Access Control will be passed. |
| *-i* | Prevent the web access from any IP address.<br>E: Enable the function. The Internet access from any IP address will be blocked.<br>D: Disable the function. |
| *-o* | Set the keyword object. |
| *KEY_WORD_Object_Index* | Specify the index number of the object profile. |
| *-g* | Set the keyword group. |
| *KEY_WORD_Group_Index* | Specify the index number of the group profile. |

## Example

```
> csm ucf obj 1 uac -i E
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
```

```
 Action:[pass]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------

> csm ucf obj 1 uac -a B
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
 Action:[block]
 [v]Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------
```

## Telnet Command: csm ucf obj INDEX wf

It means to configure the settings regarding to Web Feature (wf).

### Syntax

**csm ucf obj** *INDEX wf -v*

**csm ucf obj** *INDEX wf -e*

**csm ucf obj** *INDEX wf -d*

**csm ucf obj** *INDEX wf -a P|B*

**csm ucf obj** *INDEX wf -s WEB_FEATURE*

**csm ucf obj** *INDEX wf -u WEB_FEATURE*

**csm ucf obj** *INDEX wf -f File_Extension_Object_index*

### Syntax Description

| Parameter | Description |
|---|---|
| *INDEX* | 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.<br>B: Block. The web access meets the web feature will be blocked.<br>P: Pass. The web access meets the web feature will be passed. |
| *-s* | It means to enable the the Web Feature configuration.<br>Features available for configuration are:<br>c: Cookie<br>p: Proxy<br>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
Profile Index: 1
Profile Name:[game]
Log:[none]
Priority Select : [Bundle : Pass]

[ ]Enable URL Access Control
```

```
 Action:[block]
 [v] Prevent web access from IP address.
  No  Obj NO.    Object Name
 --- -------- ---------------------------------

  No  Grp NO.    Group Name
 --- -------- ---------------------------------

[ ]Enable Restrict Web Feature
 Action:[pass]
 File Extension Object Index : [0]       Profile Name : []
 [V] Cookie [ ] Proxy [ ] Upload
```

## Telnet Command: csm wcf

It means to configure the settings regarding to web control filter (wcf).

### Syntax

**csm wcf show**

**csm wcf look**

**csm wcf cache**

**csm wcf server WCF_SERVER**

**csm wcf msg MSG**

**csm wcf setdefault**

**csm wcf obj** *INDEX -v*

**csm wcf obj** *INDEX -a P|B*

**csm wcf obj** *INDEX -n PROFILE_NAME*

**csm wcf obj** *INDEX -I 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.<br>B: Block. The web access meets the web feature will be blocked.<br>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:<br>P: Pass,<br>B: Block,<br>A: All,<br>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.<br>E:Enable,<br>D:Disable,<br>P:Pass,<br>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:<br>"Advertisement & Pop-Ups", "Alcohol & Tobacco", "Anonymizers", "Arts", "Business", "Transportation", "Chat", "Forums & Newsgroups", "Compromised", "Computers & Technology", "Criminal & Activity", "Dating & Personals", "Down sites", "Education", "Entertainment", "Finance", "Gambling", "Games", "Government", "Hate & Intolerance", "Health & Medicine", "Illegal Drug", "Job Search", |

| | |
|---|---|
| | "Streaming Media & Downloads", "News", "Non-profits & NGOs", "Nudity", "Persional Sites", "Phishing & Fraud", "Politics", "Pornography & Sexually explicit", "Real Estate", "Religion", "Restaurants & Dining", "Search engines & Portals", "Shopping", "Social Networking", "Spam sites", "Sports", "Malware", "Translators", "Travel", "Violence", "Weapons", "Web-Based Email", "General", "Leisure & Recreation", "Botnets", "Cults", "Fashion & Beauty", "Greeting Cards", "Hacking", "Illegal Softwares", "Image Sharing", "Information Security", "Instant Messaging", "Network Errors", "Parked Domains", "Peer-to-Peer", "Private IP Address", "School Cheating", "Sex Education", "Tasteless", "Child Abuse Images", "Uncategorised Sites" |

## Example

```
> csm wcf obj 1 -n test_wcf
Profile Index: 1
Profile Name:[test_wcf]
[]White/Black list
Action:[block]
  No  Obj NO.    Object Name
 --- -------- ----------------------------------
  No  Grp NO.    Group Name
 --- -------- ----------------------------------
Action:[block]
 Log:[block]
-------------------------------------------------------------------------
-----
child Protection Group:
  [v]Alcohol & Tobacco    [v]Criminal & Activity   [v]Gambling
  [v]Hate & Intolerance    [v]Illegal Drug        [v]Nudity
  [v]Pornography & Sexually explicit  [v]Violence           [v]Weapons

  [v]School Cheating      [v]Sex Education       [v]Tasteless
  [v]Child Abuse Images
-------------------------------------------------------------------------
-----
leisure Group:
  [ ]Entertainment       [ ]Games              [ ]Sports
  [ ]Travel             [ ]Leisure & Recreation  [ ]Fashion & Beauty
```

```
.
.
>
```

## Telnet Command: csm dnsf

It means to configure the settings regarding to DNS filter.

**csm dnsf enable** *ON|OFF*

**csm dnsf syslog** *N|P|B|A* 以下有所不同 **0910**

**csm dnsf service WCF_PROFILE**

**csm dnsf service_ucf UCF_PROFILE**

**csm dnsf time CACHE_TIME**

**csm dnsf blockpage** *show/on/off*

**csm dnsf profile_show**

**csm dnsf profile_edit** *INDEX*

**csm dnsf profile_edit** *INDEX -n PROFILE_NAME*

**csm dnsf profile_edit** *INDEX -l N|P|B|A*

**csm dnsf profile_edit** *INDEX -w WCF_PROFILE*

**csm dnsf profile_edit** *INDEX -u UCF_PROFILE*

**csm dnsf profile_edit** *INDEX -c CACHE_TIME*

### Syntax Description

| Parameter | Description |
|---|---|
| *enable* | Enable or disable DNS Filter.<br>ON: enable.<br>OFF: disable. |
| *syslog* | Determine the content of records transmitting to Syslog.<br>P: Pass. Records for the packets passing through DNS filter will be sent to Syslog.<br>B: Block. Records for the packets blocked by DNS filter will be sent to Syslog.<br>A: All. Records for the packets passing through or blocked by DNS filter will be sent to Syslog.<br>N: None. No record will be sent to Syslog. |
| *service WCF_PROFILE* | WCF_PROFILE: Specify a WCF profile 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 ...). |
| *time CACHE_TIME* | CACHE_TIME: It means to set the time for cache to live (available values are 1 to 24; 1 is one hour, 2 is two hours, and so on ...) for DNS filter. |
| *blockpage* | DNS sends block page for redirect port. When a web page is |

| | |
|---|---|
| | blocked by DNS filter, the router system will send a message page to describe that the page is not allowed to be visisted.<br>ON: Enable the function of displaying message page.<br>OFF: Disable the function of displaying message page.<br>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.<br>P: Pass.<br>B: Block.<br>A: All.<br>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.<br>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. |

### Example

```
> csm dnsf service 2
dns service set up!!!
>csm dnsf service 3
wcf profile 3 is empty.....
>csm dnsf cachetime 1
dns cache time set up!!!
```

## Telnet Command: ddns log

Displays the DDNS log.

### Example

```
>ddns log
>
```

## Telnet Command: ddns time

Sets and displays the DDNS time.

### Syntax

**ddns time** <*update in minutes*>

### Syntax Description

| Parameter | Description |
|---|---|
| *Update in minutes* | Enter the value as DDNS time. The range is from 1 to 14400. |

### Example

```
> ddns time
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1440
> ddns time 1000
ddns time <update in minutes>
Valid: 1 ~ 1440
%Now: 1000
```

## Telnet Command: 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]]*

### 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). |

### Example

```
>dos –A
The Dos Defense system is Activated
>dos –s synflood 50 10
Synflood is enabled! Threshold=50 <pke/sec> timeout=10 <pke/sec>
```

## Telnet Command: exit

Type this command will leave telnet window.

## Telnet Command: Internet

This command allows you to configure detailed settings for WAN connection.

### Syntax

**internet** *-W n -M n [-<command> <parameter> | … ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-M n* | M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 3)<br>n=0: Offline<br>n=1: PPPoE<br>n=2: Dynamic IP<br>n=3: Static IP |
| *<command><parameter>\|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| -S <isp name> | It means to set ISP Name (max. 23 characters). |
| -P <on/off> | It means to enable PPPoE Service. |
| *-u <username>* | It means to set username (max. 49 characters) for Internet accessing. |

| | |
|---|---|
| *-p <password>* | It means to set password (max. 49 characters) for Internet accessing. |
| *-a n* | It means to set PPP Authentication Type and n means different types (represented by 0-1).<br>n=0: PAP/CHAP (this is default setting)<br>n=1: PAP Only |
| *-t n* | It means to set connection duration and n means different conditions.<br>n=-1: Always-on<br>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).<br>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. |
| *-V* | It means to view Internet Access profile. |
| *-C <sim pin code>* | Set (PPP mode) SIM PIN code (max. 15 characters). |
| *-O <init string>* | Set (PPP mode) Modem Initial String (max. 47 characters). |
| *-T <init string2>* | Set (PPP mode) Modem Initial String2 (max. 47 characters) |
| *-D <dial string>* | Set (PPP mode) Modem Dial String (max. 31 characters). |
| *-v <service name>* | Set (PPP mode) Service Name (max. 23 characters). |
| *-m <ppp username>* | Set (PPP mode) PPP Username (max. 63 characters). |
| *-o <ppp password>* | Set (PPP mode) PPP Password (max. 62 characters). |
| *-e n* | Set (PPP mode) PPP Authentication Type.<br>n= 0: PAP/CHAP (default),<br>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.<br><mode><br>0: ARP Detect;<br>1: Ping Detect |
| *-I <ping ip>* | Set (PPP mode or DHCP mode) WAN Connection Detection Ping IP.<br><ping ip>= ppp.qqq.rrr.sss: WAN Connection Detection Ping IP |
| *-L n* | Set (PPP mode) WAN Connection Detection TTL (1-255) value. |
| *-E <sim pin code>* | Set (DHCP mode) SIM PIN code (max. 19 characters). |
| *-G <mode>* | Set (DHCP mode) Network Mode.<br><mode><br>0: 4G/3G/2G;<br>1: 4G Only;<br>2: 3G Only;<br>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
```

## Telnet Command: ip pubsubnet

This command allows users to enable or disable the IP routing subnet for your router.

### Syntax

**ip 2ndsubnet** <*Enable/Disable*>

### Syntax Description

| Parameter | Description |
|---|---|
| *Enable* | Enable the function. |
| *Disable* | Disable the function. |

### Example

```
> ip 2ndsubnet enable
2nd subnet enabled!
```

## Telnet Command: ip pubaddr

This command allows to set the **IP routed subnet** for the router.

### Syntax

**ip pubaddr** *?*

**ip pubaddr** <*public subnet IP address*>

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | Display an IP address which allows users set as the public subnet IP address. |
| *public subnet IP address* | Specify an IP address. The system will set the one that you specified as the public subnet IP address. |

### Example

```
> ip pubaddr ?
% ip addr <public subnet IP address>
% Now: 192.168.0.1

> ip pubaddr 192.168.2.5
% Set public subnet IP address done !!!
```

## Telnet Command: ip pubmask

This command allows users to set the mask for IP routed subnet of your router.

### Syntax

**ip pubmask** *?*

**ip pubmask** <*public subnet mask*>

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | Display an IP address which allows users set as the public subnet mask. |
| *public subnet IP address* | Specify a subnet mask. The system will set the one that you specified as the public subnet mask. |

### Example

```
> ip pubmask ?
% ip pubmask <public subnet mask>
% Now: 255.255.255.0

> ip pubmask 255.255.0.0
% Set public subnet mask done !!!
```

## Telnet Command: ip aux

This command is used for configuring WAN IP Alias.

### Syntax

**ip aux add** *[IP] [Join to NAT Pool][wanX]*

**ip aux remove** *[index]*

### Syntax Description

| Parameter | Description |
|---|---|
| *add* | It means to create a new WAN IP address. |
| *remove* | It means to delete an existed WAN IP address. |
| *IP* | It means the auxiliary WAN IP address. |
| *Join to NAT Pool* | 0 (disable) or 1 (enable). |
| *wanX* | Add or remove an address for WAN interface. |
| *index* | Enter the index number of the table displayed on your screen. |

### Example

```
> ip aux add 192.168.1.65 1
% 192.168.1.65 has added in index 2.

> ip aux ?%% ip aux add [IP] [Join to NAT Pool]
%% ip aux remove [Index]

%%    Where IP = Auxiliary WAN IP Address.
%%          Join to NAT Pool = 0 or 1.
```

```
%%          Index = The Index number of table.


Now auxiliary WAN1 IP Address table:
Index no.      Status  IP address     NAT IP pool
-----------------------------------------------------
   1           Disable 0.0.0.0 Yes
   2           Enable  192.168.1.65    Yes
```

When you type *ip aux?*, the current auxiliary WAN IP Address table will be shown as the following:

```
Index no.     Status    IP address         IP pool
-----------------------------------------------
    1         Enable    172.16.3.229  Yes
    2         Enable    172.16.3.56       No
    3         Enable    172.16.3.113  No
```

## 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** *[0/1/2/3/4/5status]*

**ip arp setCacheLife** *[time]*

In which, **arp add** allows users to add a new IP address into the ARP table; **arp del** allows users to remove an IP address; **arp flush** allows users to clear arp cache; **arp status** allows users to review current status for the arp table; **arp accept** allows to accept or reject the source /destination MAC address; arp **setCacheLife** allows users to configure the duration in which ARP caches can be stored on the system. If **ip arp setCacheLife** is set with "60", it means you have an ARP cache at 0 second. Sixty seconds later without any ARP messages received, the system will think such ARP cache is expired. The system will issue a few ARP request to see if this cache is still valid.

### Syntax Description

| Parameter | Description |
|---|---|
| *IP address* | It means the LAN IP address. |
| *MAC address* | It means the MAC address of your router. |
| *LAN or WAN* | It indicates the direction for the arp function. |
| *0/1/2/3/4/5* | 0: disable to accept illegal source mac address<br>1: enable to accept illegal source mac address<br>2: disable to accept illegal dest mac address<br>3: enable to accept illegal dest mac address |

| | |
|---|---|
| | 4: Decline VRRP mac into arp table<br>5: Accept VRRP mac into arp table<br>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.<br>-h: display usage<br>-l: list all custom set DHCP options<br>-d: delete custom dhcp client option by index number<br>-e: enable/disable option feature, 1:enable, 0:disable<br>-w: set WAN number (e.g., 1=WAN1) |

| | |
|---|---|
| | -c: set option number: 0~255<br>-v: set option value by string<br>-x: set option value by raw byte (hex)<br>-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 status
I/F#3 DHCP Client Status:

DHCP Server IP        : 172.16.3.7
WAN Ipm               : 172.16.3.40
WAN Netmask           : 255.255.255.0
WAN Gateway           : 172.16.3.1
Primary DNS           : 168.95.192.1
Secondary DNS         : 0.0.0.0
Leased Time           : 259200
Leased Time T1        : 129600
Leased Time T2        : 226800
Leased Elapsed        : 259194
Leased Elapsed T1 : 129594
Leased Elapsed T2 : 226794
```

## 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] [WAN1 /PVC3/PVC4/PVC5]*

### Syntax Description

| Parameter | Description |
|---|---|
| *IP address* | It means the WAN IP address. |
| *WAN1/PVC3/PVC4/PVC5* | It means the WAN port /PVC that the above IP address passes through. |

### Example

```
>ip ping 172.16.3.229 WAN1
```

```
Pinging 172.16.3.229 with 64 bytes of Data:
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Receive reply from 172.16.3.229, time=0ms
Packets: Sent = 5, Received = 5, Lost = 0 <0% loss>
```

## Telnet Command: ip tracert

This command allows users to trace the routes from the router to the host.

### Syntax

**ip tracert** *[Host/IP address] [WAN1/WAN2/WAN3/WAN4/WAN5] [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).<br>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.<br>1: WAN1,2: WAN2, 3: PVC3,4: PVC4,5: PVC5<br>**Note**: PVC3 ~PVC5 are virtual WANs. |
| *-e* | It means to disable or enable RIP setting for specified WAN interface.<br>1: Enable the function of setting RIP of WAN IP.<br>0: Disable the function. |

### Example

```
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
 WAN[4] Rip Protocol disable
 WAN[5] Rip Protocol disable
 WAN[6] Rip Protocol enable
 WAN[7] Rip Protocol enable
> ip wanrip 5 -e 1
> ip wanrip ?
 Valid ex:ip wanrip <ifno> -e <0/1>
 <ifno> 1: WAN1,2: WAN2
       3: PVC3,4: PVC4,5: PVC5
 -e <0/1>  0: disable, 1: enable
 Now status:
 WAN[1] Rip Protocol disable
 WAN[2] Rip Protocol disable
 WAN[3] Rip Protocol disable
```

```
WAN[4] Rip Protocol disable
WAN[5] Rip Protocol enable
```

## Telnet Command: ip route

This command allows users to set static route.

### Syntax

**ip route** *add [dst] [netmask][gateway][ifno][rtype]*

**ip route** *del [dst] [netmask][rtype]*

**ip route** *status*

**ip route** *cnc*

**ip route** *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.<br>3=WAN1 5=WAN3,6=WAN4,7=WAN5<br>However,<br>WAN3, WAN4, WAN5 are router-borne WANs |
| *rtype* | It means the type of the route.<br>default : default route;<br>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.<br>1: Enable the function.<br>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*

### 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.<br>The default value is 125000 ms. |
| *ppp* | 0 – No need to set IGMP with PPP header.<br>1 – Set IGMP with PPP header. |
| *status* | It means to display current status for proxy server. |

### Example

```
> ip igmp t_home on (重抓文字)
%T-Home Setting:
%T-Home Service is turned on.
%WAN1 : Enabled, connection type: PPPoE, without tag for ADSL
%WAN5 : Enabled, connection type: DHCP, tag: 8
%: PVC4(WAN5) is bound to PVC0(WAN1), protocol=MPoA 1483 Bridge
%IGMP Proxy Interface: WAN5(PVC)
%WAN5 for Router-borne Application/ IPTV on/off: ON
> 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 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 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. |
| *Defaultlp2p [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.<br>The unit is second. |
| *[block/unblock][IP]* | It means to block/unblock the specified IP address.<br>Block: The IP cannot access Internet through the router.<br>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** *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. |
| *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 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** *show*

**ip bindmac** *add [IP][MAC][Comment]*

**ip bindmac** *del [IP]/all*

## 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. |
| *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.<br>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.<br>*[…]* means that you can Enter several commands in one line. |
| **General Setup** for Policy Route | |
| *-i [value]* | Specify an index number for setting policy route profile.<br>Value: 1 to 60. "-1" means to get a free policy index automatically. |
| *-e [0/1]* | 0: Disable the selected policy route profile.<br>1: Enable the selected policy route profile. |
| *-o [value]* | Determine the operation of the policy route.<br>Value:<br>add – Create a new policy rotue profile.<br>del – Remove an existed policy route profile.<br>edit – Modify an existed policy route profile.<br>flush – Reset policy route to default setting. |
| *-1 [any/range]* | Specify the source IP mode.<br>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.<br>Any: No need to specify an IP address for any IP address will be treated as destination IP address.<br>ip_range: Indicates a range of IP addresses.<br>ip_subnet: Indicates the IP subnet.<br>domain: Indicates the domain name. |
| *-3 [any/range]* | Specify the destination port mode.<br>Range: Indicate a range of port number.<br>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.<br>Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.0) |
| *-S [value]* | Indicate the source IP end.<br>Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.1.100) |
| *-d [value]* | Indicate the destination IP start.<br>Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.0) |
| *-D [value]* | Indicate the destination IP end.<br>Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.2.100) |
| *-p [value]* | Indicate the destination port start.<br>Value: Type a number (1 ~ 65535) as the port start (e.g., 1000). |
| *-P [value]* | Indicate the destination port end.<br>Value: Type a number (1 ~ 65535) as the port end (e.g., 2000). |
| *-y [value]* | Indicate the priority of the policy route profile.<br>Value: Type a number (0 ~ 250). The default value is "150". |
| *-I [value]* | Indicate the interface specified for the policy route profile.<br>Value: Available interfaces include,<br>LAN1 ~ LAN8, IP_Routed_Subnet,<br>DMZ_Subnet,<br>WAN1 ~ WAN5,<br>VPN_PROFILE_1 ~ VPN_PROFILE_100,<br>WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8 |
| *-g [value]* | Indicate the gateway IP address.<br>Value: The type format shall be "xxx.xxx.xxx.xxx". (e.g, 192.168.3.1) |

| | |
|---|---|
| *-I [value]* | Indicate the failover IP address.<br>Value: The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.4.1) |
| *-t [value]* | It means “protocol”.<br>Value: Available settings include “TCP”, “UDP”, “TCP/UDP”, “ICMP” and “Any”. |
| *-n [0/1]* | Indicates the function of “Force NAT”.<br>0: Disable the function.<br>1: Enable the function. |
| *-a [0/1]* | Indicates to enable the function of failover.<br>0: Disable the function.<br>1: Enable the function. |
| *-f [value]* | It means to specify the interface for failover.<br>Value: Avaialbe interfaces include,<br>NO_FAILOVER,<br>Default_WAN,<br>Policy1 ~ Policy60<br>LAN1 ~ LAN8<br>IP_Routed_Subnet,<br>DMZ_Subnet,<br>WAN1 ~ WAN5,<br>VPN_PROFILE_1 ~ VPN_PROFILE_100,<br>WAN_1_IP_ALIAS_1 ~ WAN_4_IP_ALIAS_8 |
| *-b [value]* | It means “failback”.<br>Value: Available settings include,<br>0: Disable the function of “failback”.<br>1: Enable the function of “failback”.<br>-v: View current failback setting. |
| **Diagnose** for Policy Route | |
| *-s [value]* | It means “source IP”.<br>Value: Available settings include:<br>Any: It indicates any IP address can be used as source IP address.<br>“xxx.xxx.xxx.xxx”: The type format (e.g, 192.168.1.0). |
| *-d [value]* | It means “destination IP”.<br>Value : Available settings include:<br>Any: It indicates any IP address can be used as destination IP address.<br>“xxx.xxx.xxx.xxx”: Specify an IP address. |
| *-p [value]* | It means “destination port”.<br>Value: Specify a number or type Any (indicating any number). |

| | |
|---|---|
| *-t [value]* | It means “protocol”.<br>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 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.<br>*[…]* means that you can Enter several commands in one line. |
| *-a <IP Address>* | Set forwarded DNS server IP Address. |
| *-d <DNS server mapping index number>* | Delete the selected LAN DNS profile. |
| *-e <0/1>* | 0: disable such function.<br>1: enable such function. |
| *-i <profile setting index number>* | Enter the index number of the profile. |
| *-l* | List the content of LAN DNS profile (including domain name, IP address and message). |
| *-n <domain name>* | Set domain name. |

| | |
|---|---|
| *-p <profile name>* | Set profile name for LAN DNS. |
| *-r* | Reset the settings for selected profile. |

### 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: ip6 addr

This command allows users to set the IPv6 address for your router.

### Syntax

**ip6 addr -s** *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

**ip6 addr -d** *[prefix] [prefix-length] [LAN|WAN1|WAN2|iface#]*

**ip6 addr -a** *[LAN|WAN1|WAN2|iface#]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-s* | It means to add a static ipv6 address. |
| *-d* | It means to delete an ipv6 address. |
| *-a* | It means to show current address(es) status. |
| *-u* | It means to show only unicast addresses. |
| *prefix* | It means to Enter the prefix number of IPv6 address. |
| *prefix-length* | It means to type a fixed value as the length of the prefix. |
| *LAN|WAN1|WAN2|iface#* | It means to specify LAN or WAN interface for such address. |

### 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* [*LAN*|*WAN1*|*WAN2*|*iface#] [-<*command*> <*parameter*>| ... ]

### Syntax Description

| Parameter | Description |
|---|---|
| *req_opt* | It means option-request. |
| *LAN*\|*WAN1*\|*WAN2*\|*iface#* | It means to specify LAN or WAN interface for such address. |
| *[<command> <parameter>\|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-a* | It means to show current DHCPv6 status. |
| *-s* | It means to ask the SIP. |
| *-S* | It means to ask the SIP name. |
| *-d* | It means to ask the DNS setting. |
| *-D* | It means to ask the DNS name. |
| *-n* | It means to ask NTP. |
| *-i* | It means to ask NIS. |
| *-I* | It means to ask NIS name. |
| *-p* | It means to ask NISP. |
| *-P* | It means to ask NISP name. |
| *-b* | It means to ask BCMCS. |
| *-B* | It means to ask BCMCS name. |
| *-r* | It means to ask refresh time. |
| *Parameter* | 1: the parameter related to the request will be displayed.<br>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|iface#] [-<command> <parameter>| … ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *client* | It means the dhcp client settings. |
| *[<command> <parameter>|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-a* | It means to show current DHCPv6 status. |
| *-p [IAID]* | It means to request identity association ID for Prefix Delegation. |
| *-n [IAID]* | It means to request identity association ID for Non-temporary Address. |
| *-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.<br>1: Enable<br>0: Disable |

### Example

```
> ip6 dhcp client WAN2 –p 2008::1
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_PD whose IAID equals to 2008
> ip6 dhcp client WAN2 –n 1023456
> ip6 dhcp client WAN2 –a
  Interface WAN2 has following DHCPv6 client settings:
       DHCPv6 client enabled
       request IA_NA whose IAID equals to 2008
> system reboot
```

## Telnet Command: ip6 dhcp server

This command allows you to configure DHCPv6 server.

### Syntax

**ip6 dhcp** *server [-<command> <parameter>| ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *server* | It means the dhcp server settings. |
| *[<command> <parameter>\|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-a* | It means to show current DHCPv6 status. |
| *-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. |
| *-d<addr>* | It means to set the first DNS IPv6 address. |
| *-D<addr>* | It means to set the second DNS IPv6 address. |
| *-c<parameter>* | It means to send rapid commit to server.<br>1: Enable<br>0: Disable |
| *-e<parameter>* | It means to enable or disable the DHCPv6 server.<br>1: Enable<br>0: Disable |

### Example

```
> ip6 dhcp server -d FF02::1
> ip6 dhcp server -i ff02::1
> ip6 dhcp server -x ff02::3
> ip6 dhcp server -a
% Interface LAN has following DHCPv6 server settings:
%    DHCPv6 server disabled
%    maximum address of the pool: FF02::3
%    minimum address of the pool: FF02::1
%   1st DNS IPv6 Addr: FF02::1
```

## Telnet Command: ip6 internet

This command allows you to configure settings for accessing Internet.

### Syntax

**ip6 internet** *-W n -M n [-<command> <parameter> | ... ]*

## Syntax Description

| Parameter | Description |
|---|---|
| *-W n* | **W** means to set WAN interface and **n** means different selections. Default is WAN1.<br>n=1: WAN1<br>n=2: WAN2<br>n=3: WAN3<br>.<br>.<br>n=X: WANx |
| *-M n* | M means to set Internet Access Mode (Mandatory) and n means different modes (represented by 0 – 5)<br>n= 0: Offline,<br>n=1: PPP,<br>n=2: TSPC,<br>n=3: AICCU,<br>n=4: DHCPv6,<br>n=5: Static<br>n=6:6in4-Static<br>n=7:6rd |
| *[<command> <parameter>\|...]* | The available commands with parameters are listed below.<br>*[...]* means that you can Enter several commands in one line. |
| *-m n* | It means to set IPv6 MTU.<br>N = any value (0 means "unspecified"). |
| *-u <username>* | It means to set Username.<br><username>= type a name as the username (maximum 63 characters). |
| *-p <password>* | It means to set Password.<br><password> = type a password (maximum 63 characters). |
| *-s <server>* | It means to set Tunnel Server IP.<br><server>= IPv4 address or URL (maximum 63 characters). |
| *-d <server>* | It means to set the primary DNS Server IP.<br><server>= type an IPv6 address for first DNS server. |
| *-D <server>* | It means to set the secondary DNS Server IP. |

| | |
|---|---|
| | <server>= type an IPv6 address for second DNS server. |
| *-t <dhcp/ra/none>* | It means to set IPv6 PPP WAN test mode for DHCP or RADVD.<br><dhcp/ra/none>= type IPv6 address. |
| *-V* | It means to view IPv6 Internet Access Profile. |
| *-o* | It means to set AICCU always on.<br>1=On,<br>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] [LAN|WAN1|WAN2]*

**ip6 neigh** *-d [inet6_addr] [LAN|WAN1|WAN2]*

**ip6 neigh** *-a [inet6_addr] [-N LAN|WAN1|WAN2]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-s* | It means to add a neighbour. |
| *-d* | It means to delete a neighbour. |
| *-a* | It means to show neighbour status. |
| *inet6_addr* | Type an IPv6 address |
| *eth_addr* | Type submask address. |
| *LAN|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 [LAN|WAN1|WAN2]*

**ip6 pneigh** *-d inet6_addr [LAN|WAN1|WAN2]*

**ip6 pneigh** *-a [inet6_addr] [-N LAN|WAN1|WAN2]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-s* | It means to add a proxy neighbour. |
| *-d* | It means to delete a proxy neighbour. |
| *-a* | It means to show proxy neighbour status. |
| *inet6_addr* | Type an IPv6 address |
| *LAN\|WAN1\|WAN2* | Specify an interface for the proxy neighbor. |

### Example

```
> ip6 neigh -s FE80::250:7FFF:FE12:300 LAN
%      Neighbour FE80::250:7FFF:FE12:300 successfully added!
```

## Telnet Command: ip6 route

This command allows you to

### Syntax

**ip6 route** *-s [prefix] [prefix-length] [gateway] [LAN|WAN1|WAN2|iface#> [-D]*

**ip6 route -***d [prefix] [prefix-length]*

**ip6 route -***a [LAN|WAN1|WAN2|iface#]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-s* | It means to add a route. |
| ***-d*** | It means to delete a route. |
| ***-a*** | It means to show the route status. |
| *-D* | It means that such route will be treated as the default route. |
| *prefix* | It means to Enter the prefix number of IPv6 address. |
| *prefix-length* | It means to type a fixed value as the length of the prefix. |
| *gateway* | It means the gateway of the router. |
| *LAN\|WAN1\|WAN2\|iface#* | It means to specify LAN or WAN interface for such address. |

### Example

```
> ip6 route -s FE80::250:7FFF:FE12:500 16 FE80::250:7FFF:FE12:100 LAN
%      Route FE80::250:7FFF:FE12:500/16 successfully added!
> ip6 route -a LAN

 PREFIX/PREFIX-LEN  _EXPIRES_  _NEXT-HOP_   I/F  METRIC    STATE     FLAGS
------------------------------------------------------------------------
------
 FE80::/128                                  LAN      0   UNICAST     U
                          0    ::
 FE80::250:7FFF:FE00:0/128                   LAN      0   UNICAST     U
                          0    ::
 FE80::/64                                   LAN    256   UNICAST     U
                          0
 FE80::/16                                   LAN   1024   UNICAST     UGA
                          0    FE80::250:7FFF:FE12:100
 FF02::1/128                                  LAN      0   UNICAST     UC
                          0    FF02::1
 FF00::/8                                    LAN    256   UNICAST     U
                          0
 ::/0                                        LAN     -1   UNREACHABLE !
                          0
```

## Telnet Command: ip6 ping

This command allows you to pin an IPv6 address or a host.

### Syntax

**ip6 ping** *[IPV6 address/Host] [LAN/WAN1/WAN2]*

### Syntax Description

| Parameter | Description |
|---|---|
| *IPV6 address/Host* | It means to specify the IPv6 address or host for ping. |
| *LAN/WAN1/WAN2* | It means to specify LAN or WAN interface for such address. |

### 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]*

### Syntax Description

| Parameter | Description |
|---|---|
| *IPV6 address/Host* | It means to specify the IPv6 address or host for ping. |

### Example

```
> ip6 tracert 2001:4860:4860::8888
traceroute to 2001:4860:4860::8888, 30 hops max through protocol ICMP
  1 2001:5C0:1400:B::10B8    340 ms
  2 2001:4DE0:1000:A22::1    330 ms
  3 2001:4DE0:A::1           330 ms
  4 2001:4DE0:1000:34::1     340 ms
  5 2001:7F8:1: :A501:5169:1 330 ms
  6 2001:4860::1:0:4B3       350 ms
  7 2001:4860::8:0:2DAF      330 ms
  8 2001:4860::2:0:66E       340 ms
  9 Request timed out.          *
 10 2001:4860:4860::8888     350 ms
Trace complete.
>
```

## Telnet Command: ip6 tspc

This command allows you to display TSPC status.

### Syntax

**ip6 tspc** *[ifno]*

### Syntax Description

| Parameter | Description |
|---|---|
| *ifno* | It means the connection interface.<br>Ifno=1 (means WAN1)<br>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** *–s [1|0] [lifetime]*

**ip6 radvd** *–V*

### Syntax Description

| Parameter | Description |
|---|---|
| *-s* | It means to enable or disable the default lifetime of the RADVD server.<br>1: Enable the RADVD server.<br>0: Disable the RADVD server. |
| *Lifetime* | It means to set the lifetime.<br>The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.<br>Enter the number (unit: second) you want. |
| *-V* | It means to show the RADVD configuration. |
| *-r* | It means RA default test. |
| *-r [num]* | It means RA test for item [num]. |

### Example

```
> ip6 radvd -s 1 1800
> ip6 radvd -V
%  IPv6 Radvd Config:
Radvd : Enable, Default Lifetime : 1800 seconds
```

## Telnet Command: ip6 mngt

This command allows you to manage the settings for access list.

### Syntax

**ip6 mngt list**

**ip6 mngt list** *[add<index> <prefix> <prefix-length>|remove <index>|flush]*

**ip6 mngt status**

**ip6 mngt** *[http|telnet|ping|https|ssh] [on|off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *list* | It means to show the setting information of the access list. |
| *status* | It means to show the status of IPv6 management. |
| *add* | It means to add an IPv6 address which can be used to execute management through Internet. |
| *index* | It means the number (1, 2 and 3) allowed to be configured for IPv6 management. |
| *prefix* | It means to Enter the IPv6 address which will be used for accessing Internet. |
| *prefix-length* | It means to type a fixed value as the length of the prefix. |
| *remove* | It means to remove (delete) the specified index number with IPv6 settings. |
| *flush* | It means to clear the IPv6 access table. |
| *http\|telnet\|ping\|https\|ssh* | 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 FE80::250:7FFF:FE12:1010 128
> ip6 mngt list add 2 FE80::250:7FFF:FE12:1020 128
> ip6 mngt list add 3 FE80::250:7FFF:FE12:2080 128
> ip6 mngt list
% IPv6 Access List :
Index   IPv6 Prefix    Prefix Length
========================================
1      FE80::250:7FFF:FE12:1010       128
2      FE80::250:7FFF:FE12:1020       128
3      FE80::250:7FFF:FE12:2080       128
```

```
> ip6 mngt status
% IPv6 Remote Management :
telnet : off,   http : off,    ping : off
```

## Telnet Command: ip6 online

This command allows you to check the online status of IPv6 LAN /WAN.

### Syntax

**ip6** *online [ifno]*

### Syntax Description

| Parameter | Description |
|---|---|
| *ifno* | It means the connection interface.<br>0=LAN1<br>1=WAN1<br>2=WAN2 |

### Example

```
> ip6 online 0
 % LAN 1 online status :
 % Interface : UP
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 408, Tx bytes = 32160, Rx packets = 428, Rx bytes = 33636

> ip6 online 1
 % WAN 1 online status :
 % IPv6 WAN1 Disabled
 % Default Gateway : ::
 % UpTime : 0:00:00
 % Interface : DOWN
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % IPv6 DNS Server: :: Static
 % Tx packets = 0, Tx bytes = 0, Rx packets = 0, Rx bytes = 0
```

## Telnet Command: ip6 aiccu

This command allows you to set IPv6 settings for WAN interface with connection type of AICCU.

### Syntax

**ip6 aiccu** *[ifno]*

**ip6 aiccu subnet** *[add <ifno> <prefix> <prefix-length>|remove <ifno>|show <info>]*

### Syntax Description

| Parameter | Description |
|---|---|
| *ifno* | It means the connection interface.<br>1=WAN1<br>2=WAN2 |
| *add* | It means to add an IPv6 address which can be used to execute management through Internet. |
| *prefix* | It means to Enter the IPv6 address which will be used for accessing Internet. |
| *prefix-length* | It means to type a fixed value as the length of the prefix. |
| *remove* | It means to remove (delete) the specified index number with IPv6 settings. |
| *show* | It means to display the AICCU status. |

### Example

```
> ip6 aiccu subnet add 2 2001:1111:0000::1111 64
> ip6 aiccu 2
Status: Connecting

>ip6 aiccu subnet show 2
IPv6 WAN2 AICCU Subnet Prefix Config:
2001:1111::1111/64
>
```

## 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.<br>0 – Auto<br>1 – First Query IPv6 NTP Server. |

### Example

```
> ip6 ntp -p 1
% Set NTP Priority: IPv6 First
```

## 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. |
| *-d* | It means to show the running data filter rules. |
| *-h* | It means to show the hit-number of the filter rules. |
| *-r* | It means to show the running call and data filter rules. |
| *-t* | It means to display all the information at one time. |
| *-z* | It means to clear a filter rule's statistics. |
| *-Z* | It means to clear IP filter's gross statistics. |

### Example

```
> ipf view -V -c -d
ipf: IP Filter: v3.3.1 (1824)
Kernel: IP Filter: v3.3.1
Running: yes
Log Flags: 0x80947278 = nonip
Default: pass all, Logging: available
```

## Telnet Command: ipf set

This command is used to set general rule for firewall.

### Syntax

**ipf set** *[Options]*

**ipf set** *[SET_NO] rule [RULE_NO] [Options]*

## Syntax Description

| Parameter | Description |
|---|---|
| *Options* | There are several options provided here, such as *-v*, *-c [SET_NO], -d [SET_NO],… and etc.* |
| *SET_NO* | It means to specify the index number (from 1 to 12) of filter set. |
| *RULE_NO* | It means to specify the index number (from 1 to 7) of filter rule set. |
| *-v* | Type "-v" to view the configuration of general set. |
| *-d [SET_NO]* | It means to setup Data Filter, e.g., *-d 3*. The range for the index number you can type is "0" to "12" (0 means "disable). |
| *-l [VALUE]* | It means to setup Log Flag, e.g., *-l 2*<br>Type "0" to disable the log flag.<br>Type "1" to display the log of passed packet.<br>Type "2" to display the log of blocked packet.<br>Type "3" to display the log of non-matching packet. |
| *- p [VALUE]* | It means to setup actions for packet not matching any rule, e.g., *-p 1*<br>Type "0" to let all the packets pass;<br>Type "1" to block all the packets. |
| *-M [P2P_NO]* | It means to configure IM/P2P for the packets not matching with any rule, e.g., *-M 1*<br>Type "0" to let all the packets pass;<br>Type "1" to block all the packets. |
| *-U [URL_NO]* | It means to configure URL content filter for the packets not matching with any rule, e.g., *-U 1*<br>Type "0" to let all the packets pass;<br>Type "1" to block all the packets. |
| *-a [AD_SET]* | It means to configure the advanced settings. |
| *-f [VALUE]* | It means to accept large incoming fragmented UDP or ICMP packets. |
| *-E [VALUE]* | It means to set the maximum count for session limitation. |
| *-F [VALUE]* | It means to configure the load-balance policy. |
| *-Q [VALUE]* | It means to set the QoS class. |

## Example

```
> ipf set -d 2  #set data filter start from set 2
```

```
Setting saved.
> ipf set -v

Data Filter: Enable (Start Filter Set = 2)
Log Flag   : None

Actions for packet not matching any rule:
  Pass or Block    : Pass
  CodePage        : ANSI(1252)-Latin I
  Max Sessions Limit: 60000
  Current Sessions  : 0
  Mac Bind IP      : Non-Strict
  QOS Class       : None
  APP Enforcement   : None
  URL Content Filter: None
  Load-Balance policy : Auto-select
  ------------------------------------------------------------
  CodePage               : ANSI(1252)-Latin I
  Window size             : 65535
  Session timeout          : 1440
  DrayTek Banner           : Enable
  ------------------------------------------------------------
  Apply IP filter to VPN incoming packets          : Enable
  Accept large incoming fragmented UDP or ICMP packets: Enable
  ------------------------------------------------------------
  Strict Security Checking
    [ ]APP Enforcement
>
```

## 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* | Such word means Filter Set, range form 1~12. |
| *r* | Such word means Filter Rule, range from 1~7. |

| | |
|---|---|
| *<Command><parameter>* | The following lists all of the available commands with parameters. |
| *-e* | It means to enable or disable the rule setting.<br>0- disable<br>1- enable |
| *-s o:g <obj>* | It means to specify source IP object and IP group.<br>o - indicates "object".<br>g - indicates "group".<br>obj - indicates index number of object or index number of group. Available settings range from 1-192. For example, "-s g 3" means the third source IP group profile. |
| *–s u <Address Type> <Start IP Address> <End IP Address> \| <Address Mask>* | It means to configure **source** IP address including address type, start IP address, end IP address and address mask.<br>u – It means "user defined".<br>*Address Type* - Enter the number (representing different address type).<br>0 - Subnet Address<br>1 - Single Address<br>2 - Any Address<br>3 - Range Address<br>Example:<br>Set Subnet Address => -s u 0 192.168.1.10 255.255.255.0<br>Set Single Address => -s u 1 192.168.1.10<br>Set Any Address => -s u 2<br>Set Range Address => -s u 3 192.168.1.10 192.168.1.15 |
| *–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.<br>u – It means "user defined".<br>*Address Type* - Enter the number (representing different address type).<br>0 - Subnet Address<br>1 - Single Address<br>2 - Any Address<br>3 - Range Address<br>Example:<br>Set Subnet Address => -d u 0 192.168.1.10 255.255.255.0<br>Set Single Address => -d u 1 192.168.1.10<br>Set Any Address => -d u 2<br>Set Range Address => -d u 3 192.168.1.10 192.168.1.15 |

| | |
|---|---|
| *-d o:g <obj>* | It means to specify destination IP object and IP group.<br>o – indicates “object”.<br>g – indicates “group”<br><obj>– indicates index number of object or index number of group. Available settings range from 1-192. For example, “-d g 1" means the first destination IP group profile. |
| *-S o:g <obj>* | It means to specify Service Type object and IP group.<br>o – indicates “object”.<br>g – indicates “group”<br><obj> – indicates index number of object or index number of group. Available settings range from 1-96. For example, “-S 0 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.<br>u – it means “user defined”.<br><protocol> – It means TCP(6),UDP(17), TCP/UDP(255).<br><source_port__value> –<br>1 – Port OP, range is 0-3. 0:= =, 1:!=, 2:>, 3:<<br>3 – Port range of the Start Port Number, range is 1-65535.<br>5 – Port range of the End Port Number, range is 1-65535.<br><destination_port_value>:<br>2 – Port OP, range is 0-3, 0:==, 1:!=, 2:>, 3:<<br>4 – Port range of the Start Port Number, range is 1-65535.<br>6 – Port range of the End Port Number, range is 1-65535. |
| *-F* | It means the Filter action you can specify.<br>0 –Pass Immediately,<br>1 – Block Immediately,<br>2 – Pass if no further match,<br>3 – Block if no further match. |
| *-q* | It means the classification for QoS.<br>1– Class 1,<br>2 – Class 2,<br>3 – Class 3,<br>4 – Other |
| *-l* | It means load balance policy.<br>Such function is used for “debug” only. |

| | |
|---|---|
| *-E* | It means to enable APP Enforcement. |
| *-a<index>* | It means to specify which APP Enforcement profile will be applied.<br><index> – Available settings range from 0 ~ 32. "0" means no profile will be applied. |
| *-u<index>* | It means to specify which URL Content Filter profile will be applied.<br><index> – Available settings range from 0 ~ 8. "0" means no profile will be applied. |
| *-c* | It means to set code page. Different number represents different code page.<br>0. None<br>1. ANSI(1250)-Central Europe<br>2. ANSI(1251)-Cyrillic<br>3. ANSI(1252)-Latin I<br>4. ANSI(1253)-Greek<br>5. ANSI(1254)-Turkish<br>6. ANSI(1255)-Hebrew<br>7. ANSI(1256)-Arabic<br>8. ANSI(1257)-Baltic<br>9. ANSI(1258)-Viet Nam<br>10. OEM(437)-United States<br>11. OEM(850)-Multilingual Latin I<br>12. OEM(860)-Portuguese<br>13. OEM(861)-Icelandic<br>14. OEM(863)-Canadian French<br>15. OEM(865)-Nordic<br>16. ANSI/OEM(874)-Thai<br>17. ANSI/OEM(932)-Japanese Shift-JIS<br>18. ANSI/OEM(936)-Simplified Chinese GBK<br>19. ANSI/OEM(949)-Korean<br>20. ANSI/OEM(950)-Traditional Chinese Big5 |
| *-C <Windows Size> <Session_Timeout>* | It means to set Window size and Session timeout (Minute).<br><Windows Size> - Available settings range from 1 ~ 65535.<br><Session_Timeout> - Make the best utilization of network resources. |
| *-v* | It is used to show current filter/rule settings. |

## Example

```
> ipf rule 2 1 -e 1 -s "o 1" -d "o 2" -S "o 1" -F 2
```

```
> 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).<br>Available settings are 0 ~ 65535. |
| *-t [value]* | It means to specify a protocol (e.g., -t tcp).<br>Available settings include:<br>*tcp*<br>*udp*<br>*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.<br>a: flush all logs<br>c: flush the call log<br>f: flush the IP filter log<br>w: flush the WAN log |
| *-h* | It means to show this usage help. |
| *-p* | It means to show PPP/MP log. |
| *-t* | It means to show all logs saved in the log buffer. |
| *-w* | It means to show WAN log. |
| *-x* | It means to show packet body hex dump. |

### Example

```
> log -w
25:36:25.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:33.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:41.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
```

```
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:49.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
       Next server IP = 0.0.0.0
       Relay agent IP = 0.0.0.0
25:36:57.580 ---->DHCP (WAN-5) Len = 548XID = 0x7880fdd4
       Client IP     = 0.0.0.0
       Your IP       = 0.0.0.0
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

## Telnet Command: mngt ftpport

This command allows users to set FTP port for management.

### Syntax

**mngt ftpport** *[FTP port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *FTP port* | It means to Enter the number for FTP port. The default setting is 21. |

### Example

```
> mngt ftpport 21
% Set FTP server port to 21 done.
```

## Telnet Command: mngt httpport

This command allows users to set HTTP port for management.

### Syntax

**mngt httpport** *[Http port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *Http port* | It means to enter the number for HTTP port. The default setting is 80. |

### Example

```
> mngt httpport 80
```

```
% Set web server port to 80 done.
```

## Telnet Command: mngt httpsport

This command allows users to set HTTPS port for management.

### Syntax

**mngt httpsport** *[Https port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *Https port* | It means to Enter the number for HTTPS port. The default setting is 443. |

### Example

```
> mngt httpsport 443
% Set web server port to 443 done.
```

## Telnet Command: mngt 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 ftpserver

This command can enable/disable FTP server.

### Syntax

**mngt ftpserver** *[enable]*

**mngt ftpserver** *[disable]*

### Syntax Description

| Parameter | Description |
|---|---|
| *enable* | It means to activate FTP server function. |
| *disable* | It means to inactivate FTP server function. |

### Example

```
> mngt ftpserver enable
%% FTP server has been enabled.

> mngt ftpserver disable
%% FTP server has been disabled.
```

## 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] [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* | It means to specify one of the servers/protocols for enabling or disabling. |
| *on/off* | on – enable the function.<br>off – disable the function. |

### Example

```
> mngt rmtcfg ftp on
Enable server fail
Remote configure function has been disabled
please enable by enter mngt rmtcfg enable

> mngt rmtcfg enable
%% Remote configure function has been enabled.
> mngt rmtcfg ftp on
%% FTP server has been enabled.
```

## Telnet Command: mngt lanaccess

This command allows users to manage accessing into Vigor router through LAN port.

### Syntax

**mngt lanaccess** *-e [0/1] –s [value] –i [value]*

**mngt lanaccess** *–f*

**mngt lanaccess** *–d*

**mngt lanaccess** *–v*

**mngt lanaccess** *–h*

### Syntax Description

| Parameter | Description |
|---|---|
| *-e[0/1]* | It means to enable/disable the function.<br>0-disable the function.<br>1-enable the function. |

| | |
|---|---|
| *-s[value]* | It means to specify service offered.<br>Available values include:<br>FTP, HTTP, HTTPS, TELNET, SSH, None, All |
| *-i[value]* | It means the interface which is allowed to access.<br>Available values include:<br>LAN2~LAN6, DMZ, IP Routed Subnet, None, All<br>**Note**: LAN1 is always allowed for accessing into the router. |
| *-f* | It means to flush all of the settings. |
| *-d* | It means to restore the factory default settings. |
| *-v* | It means to view current settings. |
| *-h* | It means to get the usage of such command. |

### Example

```
> mngt lanaccess -e 1
> mngt lanaccess -s FTP,TELNET
> mngt lanaccess -i LAN3
> > mngt lanaccess -v
Current LAN Access Control Setting:
* Enable:Yes
* Service:
   - FTP:Yes
   - HTTP:No
   - HTTPS:No
   - TELNET:Yes
   - SSH:No
* Subnet:
   - LAN 2: disabled
   - LAN 3: enabled
   - LAN 4: disabled
   - LAN 5: disabled
   - LAN 6: disabled
   - DMZ: disabled
   - IP Routed Subnet: disabled

Note: the settings do NOT apply to LAN1, LAN1 is always allowed to access the
router
```

## Telnet Command: mngt echoicmp

This command allows users to reject or accept PING packets from the Internet.

### Syntax

**mngt echoicmp** *[enable]*

**mngt echoicmp** *[disable]*

### Syntax Description

| Parameter | Description |
|---|---|
| *enable* | It means to accept the echo ICMP packet. |
| *disable* | It means to drop the echo ICMP packet. |

### Example

```
> mngt echoicmp enable
%% Echo ICMP packet enabled.
```

## Telnet Command: mngt accesslist

This command allows you to specify that the system administrator can login from a specific host or network. A maximum of three IPs/subnet masks is allowed.

### Syntax

**mngt accesslist** *list*

**mngt accesslist** *add [index][ip addr][mask]*

**mngt accesslist** *remove [index]*

**mngt accesslist** *flush*

### Syntax Description

| Parameter | Description |
|---|---|
| *list* | It can display current setting for your reference. |
| *add* | It means adding a new entry. |
| *index* | It means to specify the number of the entry. |
| *ip addr* | It means to specify an IP address. |
| *mask* | It means to specify the subnet mask for the IP address. |
| *remove* | It means to delete the selected item. |
| *flush* | It means to remove all the settings in the access list. |

### Example

```
> mngt accesslist add 1 192.168.1.89 255.255.255.0
%% Set OK.
> mngt accesslist list
%% Access list :
```

```
  Index IP address     Subnet mask
=========================================
  1    192.168.1.89    255.255.255.0
```

## Telnet Command: mngt snmp

This command allows you to configure SNMP for management.

### Syntax

**mngt snmp** *[-<command> <parameter> | ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command> <parameter>\|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-e <1/2>* | 1: Enable the SNMP function.<br>2: Disable the SNMP function. |
| *-g<Community name>* | It means to set the name for getting community by typing a proper character. (max. 23 characters) |
| *-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 Enter IPv4 address to specify certain host. |
| *-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 IPv4 address of the host that will receive the trap community. |
| *-T <seconds>* | It means to set the trap timeout <0~999>. |
| *-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: msubnet switch

This command is used to configure multi-subnet.

### Syntax

**msubnet switch** *[2/3/4/5/6][On/Off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *On/Off* | On means turning on the subnet for the specified LAN interface.<br>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** *[2/3/4/5/6][IP address]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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** *[2/3/4/5/6][IP address]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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** *[2/3/4/5/6]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3 |

| | |
|---|---|
| | 4=LAN4<br>5=LAN5<br>6=LAN6 |

### Example

```
> msubnet status 2
% LAN2       Off: 0.0.0.0/0.0.0.0, PPP Start IP: 0.0.0.60
% DHCP server: Off
% Dhcp Gateway: 0.0.0.0, Start IP: 0.0.0.10, Pool Count: 50
```

## Telnet Command: msubnet dhcps

This command allows you to enable or disable DHCP server for the subnet.

### Syntax

**msubnet dhcps** *[2/3/4/5/6][On/Off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *On/Off* | On means enabling the DHCP server for the specified LAN interface.<br>Off means disabling the DHCP server. |

### Example

```
> msubnet dhcps 3 off
% LAN3       Subnet DHCP Server disabled!

 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

## Telnet Command: msubnet nat

This command is used to configure the subnet for NAT or Routing usage.

### Syntax

**msubnet nat** *[2/3/4/5/6] [On/Off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *On/Off* | On – It means the subnet will be configured for NAT usage.<br>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 |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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 |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *IP counts* | Specify a total number of IP address allowed for each LAN interface.<br>The available range is from 0 to 220. |

### Example

```
> msubnet ipcnt 2 15
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

## Telnet Command: msubnet talk

This command is used to establish a route between two LAN interfaces.

### Syntax

**msubnet talk** *[1/2/3/4/5/6] [1/2/3/4/5/6] [On/Off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *1/2/3/4/5/6* | It means LAN interface.<br>1=LAN1<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |

| | |
|---|---|
| *On/Off* | On – It means<br>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 <1/2/3/4/5/6> <1/2/3/4/5/6> <On/Off>
% where 1:LAN1, 2:LAN2, 3:LAN3, 4:LAN4, 5:LAN5, 6:LAN6
% Now:
%            LAN1   LAN2   LAN3   LAN4   LAN5   LAN6
% LAN1         V
% LAN2         V     V
% LAN3                     V
% LAN4                           V
% LAN5                                  V
% LAN6                                         V
>
```

## Telnet Command: msubnet startip

This command is used to configure a starting IP address for DCHP.

### Syntax

**msubnet startip** *[2/3/4/5/6] [Gateway IP]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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 <2/3/4/5/6> <Gateway IP>
% Now: LAN2 192.168.2.90; LAN3 192.168.3.10; LAN4 192.168.4.10; LAN5
192.168.5.1
0; LAN6 192.168.6.10
```

## Telnet Command: msubnet pppip

This command is used to configure a starting IP address for PPP connection.

### Syntax

**msubnet pppip** *[2/3/4/5/6] [Start IP]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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 <2/3/4/5/6> <Start IP>
% Now: LAN2 192.168.2.250; LAN3 192.168.3.200; LAN4 192.168.4.200; LAN5
192.168.5.200; LAN6 192.168.6.200
```

## Telnet Command: msubnet nodetype

This command is used to specify the type for node which is required by DHCP option.

### Syntax

**msubnet nodetype** *[2/3/4/5/6][count]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *count* | Choose the following number for specifying different node type.<br>1= B-node<br>2= P-node<br>4= M-node<br>8= H-node<br>0= Not specify any type for node. |

### Example

```
> msubnet nodetype ?
% msubnet nodetype <2/3/4/5/6> <count>
% Now: LAN2 0; LAN3 0; LAN4 0; LAN5 0; LAN6 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 <2/3/4/5/6> <count>
% Now: LAN2 1; LAN3 0; LAN4 0; LAN5 0; LAN6 0

% count: 1. B-node 2. P-node 4. M-node 8. H-node
```

## Telnet Command: msubnet primWINS

This command is used to configure primary WINS server.

### Syntax

**msubnet primWINS** *[2/3/4/5/6] [WINS IP]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *WINS IP* | Enter the IP address as the WINS IP. |

### Example

```
> > msubnet primWINS ?
% msubnet primWINS <2/3/4/5/6> <WINS IP>
% Now: LAN2 0.0.0.0; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0

> msubnet primWINS 2 192.168.3.5
% Set LAN2 Dhcp Primary WINS IP done !!!

> msubnet primWINS ?
% msubnet primWINS <2/3/4/5/6> <WINS IP>
% Now: LAN2 192.168.3.5; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0
```

## Telnet Command: msubnet secWINS

This command is used to configure secondary WINS server.

### Syntax

**msubnet secWINS** *[2/3/4/5/6] [WINS IP]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *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 <2/3/4/5/6> <WINS IP>
% Now: LAN2 192.168.3.89; LAN3 0.0.0.0; LAN4 0.0.0.0; LAN5 0.0.0.0; LAN6 0.0.0.0
```

## Telnet Command: msubnet tftp

This command is used to set TFTP server for multi-subnet.

### Syntax

**msubnet tftp** *[2/3/4/5/6] [TFTP server name]*

### Syntax Description

| Parameter | Description |
|---|---|
| *2/3/4/5/6* | It means LAN interface.<br>2=LAN2<br>3=LAN3<br>4=LAN4<br>5=LAN5<br>6=LAN6 |
| *TFTP server name* | Type a name to indicate the TFTP server. |

### Example

```
> msubnet tftp ?
% msubnet tftp <2/3/4/5/6> <TFTP server name>
% Now: LAN2
      LAN3
      LAN4
      LAN5
      LAN6

> msubnet tftp 2 publish
% Set LAN2 TFTP Server Name done !!!

> msubnet tftp ?
% msubnet tftp <2/3/4/5/6> <TFTP server name>
% Now: LAN2 publish
      LAN3
      LAN4
```

```
LAN5
LAN6
```

## 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~LAN6, IP_Routed_Subnet, and DMZ. |
| *value* | 1000 ~ 1508 (Bytes), default: 1500 (Bytes) |

### Example

```
> msubnet mtu LAN1 1492
> msubnet mtu ?
Usage:

  >msubnet mtu <interface> <value>

  <interface>: LAN1~LAN6,IP_Routed_Subnet,DMZ
  <value>:    1000 ~ 1508 (Bytes), default: 1500 (Bytes)

  e.x: >msubnet mtu LAN1 1492

Current Settings:

   LAN1 MTU:           1492 (Bytes)
   LAN2 MTU:           1500 (Bytes)
   LAN3 MTU:           1500 (Bytes)
   LAN4 MTU:           1500 (Bytes)
   LAN5 MTU:           1500 (Bytes)
   LAN6 MTU:           1500 (Bytes)
   DMZ MTU:            1500 (Bytes)
   IP Routed Subnet MTU: 1500 (Bytes)
```

## 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.<br>Example: *object ip obj 1 -v* |
| *-n NAME* | It means to define a name for the IP object.<br>NAME: Type a name with less than 15 characters.<br>Example: *object ip obj 9 -n bruce* |
| *-i INTERFACE* | It means to define an interface for the IP object.<br>INTERFACE=0, means any<br>INTERFACE=1, means LAN<br>INTERFACE=3, means WAN<br>Example: *object ip obj 8 -i 0* |
| *-s INVERT* | It means to set invert seletion for the object profile.<br>INVERT=0, means disableing the function.<br>INVERT=1, means enabling the function.<br>Example: *object ip obj 3 -s 1* |
| *-a TYPE* | It means to set the address type and IP for the IP object profile.<br>TYPE=0, means Mask<br>TYPE=1, means Single<br>TYPE=2, means Any<br>TYPE=3, means Rang<br>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.<br>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.<br>Example: *object ip grp 1 -v* |
| *-n NAME* | It means to define a name for the IP group.<br>NAME: Type a name with less than 15 characters.<br>Example: *object ip grp 8 -n bruce* |
| *-i INTERFACE* | It means to define an interface for the IP group.<br>INTERFACE=0, means any<br>INTERFACE=1, means LAN<br>INTERFACE=2, means WAN<br>Example: *object ip grp 3 -i 0* |
| *-a IP_OBJ_INDEX* | It means to specify IP object profiles for the group profile.<br>Example: *:object ip grp 3 -a 1 2 3 4 5*<br>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*

**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.<br>Example: *object ip obj 1 -v* |
| *-n NAME* | It means to define a name for the IP object.<br>NAME: Type a name with less than 15 characters.<br>Example: *object ip obj 9 -n bruce* |
| *-i INTERFACE* | It means to define an interface for the IP object.<br>INTERFACE=0, means any<br>INTERFACE=1, means LAN<br>INTERFACE=3, means WAN<br>Example: *object ip obj 8 -i 0* |
| *-s INVERT* | It means to set invert seletion for the object profile.<br>INVERT=0, means disableing the function.<br>INVERT=1, means enabling the function.<br>Example: *object ip obj 3 -s 1* |
| *-a TYPE* | It means to set the address type and IP for the IP object profile.<br>TYPE=0, means Mask<br>TYPE=1, means Single<br>TYPE=2, means Any<br>TYPE=3, means Rang<br>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 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.<br>Example: *object ip grp 1 -v* |
| *-n NAME* | It means to define a name for the IP group.<br>NAME: Type a name with less than 15 characters.<br>Example: *object ip grp 8 -n bruce* |
| *-i INTERFACE* | It means to define an interface for the IP group.<br>INTERFACE=0, means any<br>INTERFACE=1, means LAN<br>INTERFACE=2, means WAN<br>Example: *object ip grp 3 -i 0* |

| | |
|---|---|
| *-a IP_OBJ_INDEX* | It means to specify IP object profiles for the group profile.<br>Example: *:object ip grp 3 -a 1 2 3 4 5*<br>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 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.<br>Example: *object service obj 1 -v* |
| *-n NAME* | It means to define a name for the IP object.<br>NAME: Type a name with less than 15 characters.<br>Example: *object service obj 9 -n bruce* |
| *-i PROTOCOL* | It means to define a PROTOCOL for the service object profile.<br>PROTOCOL =0, means any<br>PROTOCOL =1, means ICMP<br>PROTOCOL =2, means IGMP<br>PROTOCOL =6, means TCP<br>PROTOCOL =17, means UDP<br>PROTOCOL =255, means TCP/UDP<br>Other values mean other protocols.<br>Example: *object service obj 8 -i 0* |
| *CHK* | It means the check action for the port setting.<br>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.<br>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.<br>2=larger**(>)**, the port number greater than this value is available..<br>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.<br>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.<br>END_P, type a port number to indicate destination port.<br>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.<br>Example: *object service grp 1 -v* |
| *-n NAME* | It means to define a name for the service group.<br>NAME: Type a name with less than 15 characters.<br>Example: *object service grp 8 -n bruce* |

| | |
|---|---|
| *-a SER_OBJ_INDEX* | It means to specify service object profiles for the group profile.<br>Example: *:object service grp 3 -a 1 2 3 4 5*<br>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.<br>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.<br>NAME: Type a name with less than 15 characters. |
| *-a CONTENTS* | It means to set the contents for the keyword profile.<br>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.<br>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:<br>Image, Video, Audio, Java, ActiveX, Compression, Executation<br>Example: *object fe obj 1 -e Image*<br>FILE_EXTENSION:<br>".bmp", ".dib", ".gif", ".jpeg", ".jpg", ".jpg2", ".jp2", ".pct", ".pcx", ".pic", ".pict", ".png", ".tif", ".tiff", ".asf", ".avi", ".mov", ".mpe", ".mpeg", ".mpg", ".mp4", ".qt", ".rm", ".wmv", ".3gp", ".3gpp", ".3gpp2", ".3g2", ".aac", ".aiff", ".au", ".mp3", ".m4a", ".m4p", ".ogg", ".ra", ".ram", ".vox", ".wav", ".wma", ".class", ".jad", ".jar", ".jav", ".java", ".jcm", ".js", ".jse", ".jsp", ".jtk", ".alx", ".apb", ".axs", ".ocx", ".olb", ".ole", ".tlb", ".viv", ".vrm", ".ace", ".arj", ".bzip2", ".bz2", ".cab", ".gz", ".gzip", ".rar", ".sit", ".zip", ".bas", ".bat", ".com", ".exe", ".inf", ".pif", ".reg", ".scr"<br>Example: *object fe obj 1 -e .bmp* |

## Example

```
> object fe obj 1 -n music
> object fe obj 1 -e Audio
> object fe obj 1 -v
Profile Index: 1
Profile Name:[music]


------------------------------------------------------------------------
------
```

```
Image category:
 [ ].bmp   [ ].dib   [ ].gif   [ ].jpeg  [ ].jpg   [ ].jpg2  [ ].jp2   [ ].pct
 [ ].pcx   [ ].pic   [ ].pict  [ ].png   [ ].tif   [ ].tiff
--------------------------------------------------------------------------
------
Video category:
 [ ].asf   [ ].avi   [ ].mov   [ ].mpe   [ ].mpeg  [ ].mpg   [v].mp4   [ ].qt
 [ ].rm    [v].wmv   [ ].3gp   [ ].3gpp  [ ].3gpp2 [ ].3g2
--------------------------------------------------------------------------
------
Audio category:
 [v].aac   [v].aiff  [v].au    [v].mp3   [v].m4a   [v].m4p   [v].ogg   [v].ra
 [v].ram   [v].vox   [v].wav   [v].wma
--------------------------------------------------------------------------
------
Java category:
 [ ].class [ ].jad   [ ].jar   [ ].jav   [ ].java  [ ].jcm   [ ].js    [ ].jse
 [ ].jsp   [ ].jtk
--------------------------------------------------------------------------
------
ActiveX category:
 [ ].alx   [ ].apb   [ ].axs   [ ].ocx   [ ].olb   [ ].ole   [ ].tlb   [ ].viv
 [ ].vrm
--------------------------------------------------------------------------
------
Compression category:
 [ ].ace   [ ].arj   [ ].bzip2 [ ].bz2   [ ].cab   [ ].gz    [ ].gzip  [ ].rar
 [ ].sit   [ ].zip
--------------------------------------------------------------------------
------
Executation category:
 [ ].bas   [ ].bat   [ ].com   [ ].exe   [ ].inf   [ ].pif   [ ].reg   [ ].scr
```

## Telnet Command: port

This command allows users to set the speed for specific port of the router.

### Syntax

**port** *[1, 2, 3, 4, 5, 6, wan2, all] [AN, 100F, 100H, 10F, 10H, status]*

**port status**

**port sniff** *[on,off,port,txrx,restart,status]*

**port 802.1x***[enable,disable,status,addport,delport]*

**port jumbo**

**port wanfc**

### Syntax Description

| Parameter | Description |
|---|---|
| *1, 2, 3, 4, 5, 6, wan2, all* | It means the number of LAN port and WAN port. |
| *AN... 10H* | It means the physical type for the specific port.<br>AN: auto-negotiate.<br>100F: 100M Full Duplex.<br>100H: 100M Half Duplex.<br>10F: 10M Full Duplex.<br>10H: 10M Half Duplex. |
| *status* | It means to view the Ethernet port status. |
| *sniff [on,off,port,txrx,restart,status]* | |
| *802.1x[enable,disable,status,addport,delport]* | |
| *wanfc* | It means to set WAN flow control. |

### Example

```
> port 1 100F
%Set Port 1 Force speed 100 Full duplex OK !!!
```

## Telnet Command: portmaptime

This command allows you to set a time of keeping the session connection for specified protocol.

### Syntax

**portmaptime** *[-<command> <parameter> | ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command> <parameter>|...]* | The available commands with parameters are listed below.<br>*[...]* means that you can Enter several commands in one line. |
| *-t <sec>* | It means “TCP” protocol.<br><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.<br><sec>: Type a number to set the IGMP session timeout. |
| *-w <sec>* | It means “TCP WWW” protocol.<br><sec>: Type a number to set the TCP WWW session timeout. |
| *-s <sec>* | It means “TCP SYN” protocol.<br><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.<br>*[…]* means that you can Enter several commands in one line. |
| *-m <mode>* | Specify a mode.<br>1=auto<br>2=manual(traffic)<br>3=manual(qos)<br>4=manual(specific hosts)<br>0=disable |
| *-p <proto>* | Specify a protocol.<br>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. |
| *-S* | Show multicast table in HW accleration |
| *-v* | Show PPA_WAN_Table and PPA_LAN_Table for reference. |
| *-c* | Clean all settings. |
| -x | Show hardware acceleration information. |
| -k | Clean the PPA table. |
| **ppa n –** used in QoS or specific host | |
| -l <rule> | Specify an index number of rule profile for QoS mode. |
| -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 mode is Auto
%PPA Protocol TCP 1, UDP 0
%PPA two way enable
%PPA time  is 10
%PPA range is 8000
%PAE range is 2048
%MPE range is 5952
%PPA LAN entries 0
%PPA WAN entries 0
>
```

## Telnet Command: prn

This command allows you to view current status (interface and driver) of USB printer.

### Syntax

**prn status**

**prn debug**

### Example

```
> prn status
Interface: USB bus 2.0
Printer: NotReady

> prn debug
conn[0] :
none
conn[1] :
none
conn[2] :
none
conn[3] :
none
LPD_data_total=0

usblp_ptr=0
UsbPrintReady=0, UsbIsPrinting=0
```

## Telnet Command: qos setup

This command allows user to set general settings for QoS.

### Syntax

**qos setup** *[-<command> <parameter> | ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command> <parameter>\|...]* | The available commands with parameters are listed below.<br>*[...]* means that you can Enter several commands in one line. |
| *-h* | Type it to display the usage of this command. |
| *-m <mode>* | It means to define which traffic the QoS control settings will apply to and eable QoS control.<br>0: disable.<br>1: in, apply to incoming traffic only.<br>2: out, apply to outgoing traffic only.<br>3: both, apply to both incoming and outgoing traffic.<br>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).<br>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.<br>0: disable<br>1: enable<br>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.<br>0: disable<br>1: enable |
| *-V* | Show all the settings. |
| *-D* | Set all to factory default (for all WANs). |
| *[…]* | It means that you can Enter several commands in one line. |

### Example

```
> qos setup -m 3 -i 9500 -o 8500 -r 3:20 -u 1 -p 50 -t 1
 WAN1 QOS mode is both
 inbound bandwidth set to 9500
 outbound bandwidth set to 8500
 WAN1 class 3 ratio set to 20
 WAN1 udp bandwidth control set to enable
 WAN1 udp bandwidth limit ratio set to 50
 WAN1 Outbound TCP ACK Prioritizel set to enable
QoS WAN1 set complete; restart QoS
DrayTek>
```

## Telnet Command: qos class

This command allows user to set QoS class.

### Syntax

**qos class -c** *[no] –[a|e|d] [no][-<command> <parameter> | … ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command> <parameter>|…]* | The available commands with parameters are listed below. |

| | |
|---|---|
| | *[…]* means that you can Enter several commands in one line. |
| *-h* | Type it to display the usage of this command. |
| *-c <no>* | Specify the inde number for the class.<br>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.<br><no>: Enter the index number for the rule. |
| *-d <no>* | It means to delete specified rule.<br><no>: Enter the index number for the rule. |
| *-m <mode>* | It means to enable or disable the specified rule.<br>0: disable,<br>1: enable |
| *-I <addr>* | Set the local address.<br>*Addr1* – It means Single address. Please specify the IP address directly, for example, "*-I 172.16.3.9*".<br>*addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50*."<br>*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*<br>*any* – It means Any address. Simple type "*-I*" to specify any address for this command. |
| *-r <addr>* | Set the remote address.<br>*addr1* – It means Single address. Please specify the IP address directly, for example, "*-I 172.16.3.9*".<br>*addr1:addr2* – It means Range address. Please specify the IP addresses, for example, "*-I 172.16.3.9: 172.16.3.50*."<br>*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*<br>*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 service type by typing the number. The available types are listed as below:<br>1:ANY 2:DNS 3:FTP 4:GRE 5:H.323 |

| | |
|---|---|
| | 6:HTTP 7:HTTPS 8:IKE 9:IPSEC-AH 10:IPSEC-ESP<br>11:IRC 12:L2TP 13:NEWS 14:NFS 15:NNTP<br>16:PING 17:POP3 18:PPTP 19:REAL-AUDIO 20:RTSP<br>21:SFTP 22:SIP 23:SMTP 24:SNMP 25:SNMP-TRAPS<br>26:SQL-NET 27:SSH 28:SYSLOG 29:TELNET 30:TFTP |
| *-S <d/s>* | Show the content for specified DSCP ID/Service type. |
| *-V <1/2/3>* | Show the rule in the specified class. |
| *[…]* | It means that you can Enter several commands in one line. |

### Example

```
> qos class -c 2 -n draytek -a -m 1 -l 192.168.1.50:192.168.1.80

 Following setting will set in the class2
 class 2 name set to draytek
 Add a rule in class2
 Class2 the 1 rule enabled
 Set local address type to Range, 192.168.1.50:192.168.1.80
```

## Telnet Command: qos type

This command allows user to configure protocol type and port number for QoS.

### Syntax

**qos type** *[-a <service name> | -e <no> | -d <no>]***.**

### 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.<br>6: tcp(default)<br>17: udp<br>0: tcp/udp<br><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: 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]  192.168.2.10      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]LAN5  192.168.5.1    255.255.255.0   [V]  192.168.5.10      100
192.168.5.1
[X]LAN6  192.168.6.1    255.255.255.0   [V]  192.168.6.10      100
192.168.6.1
[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 172.16.3.221
  2    Disable 192.168.1.65
```

## Telnet Command: show dns

This command displays current status of DNS setting

### Example

```
> show dns
%%     Domain name server settings:
%            Primary DNS: [Not set]
%            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: 10000
% Maximum Session Usage: 49
% Current Session Usage: 0
% Current Session Used(include waiting for free): 0
% WAN1 Current Session Usage: 0
```

## Telnet Command: show status

This command displays current status of LAN and WAN connections.

### Example

```
> show status)

> show status
System Uptime:95:4:44
LAN Status
Primary DNS:8.8.8.8         Secondary DNS:8.8.4.4
IP Address:192.168.1.1       Tx Rate:125096    Rx Rate:41045

WAN 1 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
Mode:DHCP Client Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0

WAN 2 Status: Disconnected
Enable:Yes      Line:Ethernet    Name:
Mode:DHCP Client Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0

WAN 3 Status: Disconnected
Enable:No       Line:Ethernet    Name:
Mode:---        Up Time:0:00:00    IP:---          GW IP:---
TX Packets:0        TX Rate(bps):0   RX Packets:0        RX Rate(bps):0

WAN 4 Status: Disconnected
Enable:No       Line:Ethernet    Name:
...
```

## 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: srv dhcp dhcp2

This command is used for configuring which method (LAN interface or MAC address) that the DHCP server on IP routed LAN shall use for assigning an IP address to the IP routed LAN clients.

### Syntax

**srv dhcp dhcp2** *-l <enable>*

**srv dhcp dhcp2** *-m <enable>*

**srv dhcp dhcp2** *-e <id>*

**srv dhcp dhcp2** *-d <id>*

**srv dhcp dhcp2** *-v*

### Syntax Description

| Parameter | Description |
|---|---|
| *-l <enable>* | The DHCP server assigns the IP addresses to the clients via LAN port.<br><enable> : Enter 0 (disable) or 1 (enable). |
| *-m <enable>* | The DHCP server assigns the IP addresses to the clients via MAC address configuration.<br><enable> : Enter 0 (disable) or 1 (enable). |
| *-e <id>* | Turn on the flag of LAN 1 or LAN 2 if LAN port is enabled.<br><id>: Enter 1 or 2. |
| *-d <id>* | Turn off the flag of LAN port 1 or LAN port 2.<br><id>: Enter 1 or 2. |
| *-v* | View current status. |

### Example

```
> srv dhcp dhcp2 -l 1 -e 1,2
> srv dhcp dhcp2 -v
 2nd DHCP server flag status --
   Server works on specified MAC address: ON
   Server works on specified LAN port: ON
   Port 1 flag: ON
   Port 2 flag: ON
>
```

## Telnet Command: srv dhcp public

This command allows users to configure DHCP server for second subnet.

### Syntax

**srv dhcp public** *start [IP address]*

**srv dhcp public** *cnt [IP counts]*

**srv dhcp public** *status*

**srv dhcp public** *add [MAC Addr XX-XX-XX-XX-XX-XX]*

**srv dhcp public** *del [MAC Addr XX-XX-XX-XX-XX-XX/all/ALL]*

### Syntax Description

| Parameter | Description |
|---|---|
| *start* | It means the starting point of the IP address pool for the DHCP server. |
| *IP address* | It means to specify an IP address as the starting point in the IP address pool. |
| *cnt* | It means the IP count number. |
| *IP counts* | It means to specify the number of IP addresses in the pool. The maximum is 10. |
| *status* | It means the execution result of this command. |
| *add* | It means creating a list of hosts to be assigned. |
| *del* | It means removing the selected MAC address. |
| *MAC Addr* | It means to specify MAC Address of the host. |
| *all/ALL* | It means all of the MAC addresses. |

### Example

```
Vigor> ip route add 192.168.1.56 255.255.255.0 192.168.1.12 3 default
Vigor> 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** *[?]*

**srv dhcp dns1** *[DNS IP address]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current IP address of DNS 1 for the DHCP server. |
| *DNS IP address* | It means the IP address that you want to use as DNS1.<br>**Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS). |

### Example

```
> srv dhcp dns1 168.95.1.1
% srv dhcp dns1 <DNS IP address>
% Now: 168.95.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

## Telnet Command: srv dhcp dns2

This command allows users to set Secondary IP Address for DNS Server in LAN.

### Syntax

**srv dhcp dns2** *[?]*

**srv dhcp dns2** *[DNS IP address]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current IP address of DNS 2 for the DHCP server. |
| *DNS IP address* | It means the IP address that you want to use as DNS2.<br>**Note:** The IP Routed Subnet DNS must be the same as NAT Subnet DNS). |

### Example

```
> srv dhcp dns2 10.1.1.1
% srv dhcp dns2 <DNS IP address>
% Now: 10.1.1.1
(IP Routed Subnet dns same as NAT Subnet dns)
```

## Telnet Command: srv dhcp frcdnsmanl

This command can force the router to invoke DNS Server IP address.

### Syntax

**srv dhcp frcdnsmanl** *[on]*

**srv dhcp frcdnsmanl** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | 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** *[?]*

**srv dhcp gateway** *[Gateway IP]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current gateway that you can use. |
| *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** *[?]*

**srv dhcp ipcnt** *[IP counts]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current used IP count number. |
| *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 subnet** *[index]*

### Syntax Description

| Parameter | Description |
|---|---|
| *server ip* | It means the IP address that you want to used as DHCP server. |
| *Index* | It means subnet 1 or 2. Please type 1 or 2. The router will invoke this function according to the subnet 1 or 2 specified here. |

### Example

```
> srv dhcp relay servip 192.168.1.46
> srv dhcp relay subnet 2
> srv dhcp relay servip ?
% srv dhcp relay servip <server ip>
```

```
% Now: 192.168.1.46
```

## Telnet Command: srv dhcp startip

### Syntax

**srv dhcp startip** *[?]*

**srv dhcp startip** *[IP address]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current used start IP address. |
| *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.

### Example

```
> srv dhcp status
DHCP server: Relay Agent
Default gateway: 192.168.1.1
Index   IP Address     MAC Address           Leased Time     HOST ID
1      192.168.1.113   00-05-5D-E4-D8-EE      17:20:08       A1000351
```

## Telnet Command: srv dhcp leasetime

This command can set the lease time for the DHCP server.

### Syntax

**srv dhcp leasetime** *[?]*

**srv dhcp leasetime** *[Lease Time (sec)]*

### Syntax Description

| Parameter | Description |
|---|---|
| *?* | It means to display current leasetime used for the DHCP server. |
| *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.<br>1. B-node<br>2. P-node<br>4. M-node<br>8. H-node |

### Example

```
> srv dhcp nodetype 1
> srv dhcp nodetype ?
%% srv dhcp nodetype <count>
%% 1. B-node 2. P-node 4. M-node 8. H-node
% Now: 1
```

## Telnet Command: srv dhcp primWINS

This command can set the primary IP address for the DHCP server.

### Syntax

**srv dhcp primWINS** *[WINS IP address]*

**srv dhcp primWINS clear**

### Syntax Description

| Parameter | Description |
|---|---|
| *WINS IP address* | It means the IP address of primary WINS server. |
| *clear* | It means to remove the IP address settings of primary WINS server. |

### Example

```
> srv dhcp primWINS 192.168.1.88
> srv dhcp primWINS ?
%% srv dhcp primWINS <WINS IP address>
%% srv dhcp primWINS clear
% Now: 192.168.1.88
```

## Telnet Command: srv dhcp secWINS

This command can set the secondary IP address for the DHCP server.

### Syntax

**srv dhcp secWINS** *[WINS IP address]*

**srv dhcp secWINS clear**

### Syntax Description

| Parameter | Description |
|---|---|
| *WINS IP address* | It means the IP address of secondary WINS server. |
| *clear* | It means to remove the IP address settings of second WINS server. |

### Example

```
> srv dhcp secWINS 192.168.1.180
> srv dhcp secWINS ?
%% srv dhcp secWINS <WINS IP address>
%% srv dhcp secWINS clear
% Now: 192.168.1.180
```

## Telnet Command: srv dhcp expired_RecycleIP

This command can set the time to check if the IP address can be assigned again by DHCP server or not.

### Syntax

**srv dhcp expRecycleIP** <*sec time*>

### Syntax Description

| Parameter | Description |
|---|---|
| *sec time* | It means to set the time (5~300 seconds) for checking if the IP can be assigned again or not. |

### Example

```
Vigor> srv dhcp expRecycleIP 250
% DHCP expired_RecycleIP = 250
```

## Telnet Command: srv dhcp tftp

This command can set the TFTP server as the DHCP server.

### Syntax

**srv dhcp tftp** <*TFTP server name*>

### Syntax Description

| Parameter | Description |
|---|---|
| *TFTP server name* | It means to 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 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] -c [option number] -v [option value]*

**srv dhcp option** *-e [1 or 0] -c [option number] -a [option value]*

**srv dhcp option -***e [1 or 0] -c [option number] -x [option value]*

**srv dhcp option** *-u [idx unmber]*

## Syntax Description

| Parameter | Description |
|---|---|
| *-h* | It means to display usage of this command. |
| *-l* | It means to display all the user defined DHCP options. |
| *-d[idx]* | It means to delete the option number by specifying its index number. |
| *-e [1 or 0]* | It means to enable/disable custom option feature.<br>1:enable<br>0:disable |
| *-c* | It means to set option number. Available number ranges from 0 to 255. |
| *-v* | It means to set option number by typing string. |
| *-a* | It means to set the option value by specifying the IP address. |
| *-x* | It means to set option number with the format of Hexadecimal characters. |
| *-u* | It means to update the option value of the sepecified index. |
| *idx number* | It means 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.<br>1: wan1<br>2: wan2 |
| *m* | It means the index number of the DMZ host.<br>Default setting is "1" (WAN 1). It is only available for Static IP mode. If you use other mode, you can set 1 ~ 8 in this field. If WAN IP alias has been configured, then the number of DMZ host can be added more. |
| *[<command> <parameter>\|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-e* | It means to enable/disable such feature.<br>1:enable<br>0:disable |
| *-i* | It means to specify the private IP address of the DMZ host. |
| *-r* | It means to remove DMZ host setting. |
| *-v* | It means to display current status. |

### Example

```
> srv nat dmz 1 1 -i 192.168.1.96
> srv nat dmz -v
%     WAN1 DMZ mapping status:
 Index  Status  WAN1 aux IP    Private IP
-----------------------------------------------------
   1    Disable 0.0.0.0 192.168.1.96
```

## 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.<br>*[…]* means that you can Enter several commands in one line. |
| *-a <enable>* | It means to enable or disable the open port rule profile.<br>0: disable<br>1:enable |
| *-c <comment>* | It means to Enter the description (less than 23 characters) for the defined network service. |
| *-i <local ip>* | It means to set the IP address for local computer.<br>Local ip: Type an IP address in this field. |
| *-w <idx>* | It means to specify the public IP.<br>1: WAN1 Default,<br>2: WAN1 Alias 1,<br>…and so on. |

| | |
|---|---|
| *-p <protocol>* | Specify the transport layer protocol.<br>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.<br>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.<br>remove: Enter the index number of the profile. |
| *-f <flush>* | It means to return to factory settings for all the open ports profiles. |

### Example

```
> srv nat openport 1 1 -a 1 -c games -i 192.168.1.100 -w 1 -p TCP -s 23 -e
83
> srv nat openport -v
%% Status: Enable
%% Comment: games
%% Private IP address: 192.168.1.100
Index   Protocal       Start Port     End Port
************************************************************
  1.    TCP            23             83

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
************************************************************

%% Status: Disable
%% Comment:
%% Private IP address: 0.0.0.0
Index   Protocal       Start Port     End Port
************************************************************
>
```

## 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][pri ip][pri port][wan1/wan2]*

**srv nat portmap** *del [idx]*

**srv nat portmap** *disable [idx]*

**srv nat portmap** *enable [idx] [proto]*

**srv nat portmap** *flush*

**srv nat portmap** *table*

## Syntax Description

| Parameter | Description |
|---|---|
| *Add[idx]* | 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. |
| *pri ip* | It means to specify the private IP address of the internal host providing the service. |
| *pri port* | It means to specify the private port number of the service offered by the internal host. |
| *wan1/wan2* | It means to specify WAN interface for the port redirection. |
| *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 game tcp 80 192.168.1.11 100 wan1
> 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

D01     All     0.0.0.0                 192.168.1.96             Y

R:Port Redirection, O:Open Ports, D:DMZ
```

## 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*<br>*acc*<br>*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 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.<br>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: 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:<br>Local [0-1]<br>LDAP [0-1]<br>edit [INDEX]<br>delete [INDEX]<br>view [INDEX] |

| | |
|---|---|
| *Local [0-1]* | 0 – Disable the local user.<br>1 – Enable the local user. |
| *LDAP [0-1]* | 0 – Disable the LDAP.<br>1 – Enable the LDAP. |
| *edit [INDEX] username password* | Edit an existed user account or create a new local user account.<br>[INDEX] – 1 ~8. There are eight profiles to be added / edited.<br>Username – Type a new name for local user.<br>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 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 cmdlog
   [2] sys cmdlog ?
   [3] sys ?
   [4] sys cfg status
   [5] sys cfg ?
```

## Telnet Command: sys ftpd

This command displays current status of FTP server.

### Syntax

**sys ftpd** *on*

**sys ftpd** *off*

### Syntax Description

| Parameter | Description |
|---|---|
| *on* | It means to turn on the FTP server of the system. |

| | |
|---|---|
| *off* | It means to turn off the FTP server of the system. |

### Example

```
> sys ftpd on
% sys ftpd turn on !!!
```

## Telnet Command: sys domainname

This command can set and remove the domain name of the system when DHCP mode is selected for WAN.

### Syntax

**sys domainname** *[wan1/wan2] [Domain Name Suffix]*

**sys domainname** *[wan1/wan2] clear*

### Syntax Description

| Parameter | Description |
|---|---|
| *wan1/wan2* | It means to specify WAN interface for assigning a name for it. |
| *Domain Name Suffix* | It means the name for the domain of the system. The maximum number of characters that you can set is 40. |
| *clear* | It means to remove the domain name of the system. |

### Example

```
> sys domainname wan1 clever
> sys domainname wan2 intellegent
> sys domainname ?
% sys domainname <wan1/wan2> <Domain Name Suffix (max. 40 characters)>
% sys domainname <wan1/wan2> clear
% Now: wan1 == clever, wan2 ==intelligent
>
```

## Telnet Command: sys iface

This command displays the current interface connection status (UP or Down) with IP address, MAC address and Netmask for the router.

### Example

```
> sys iface
Interface 0 Ethernet:
Status: UP
IP Address: 192.168.1.1      Netmask: 0xFFFFFF00 (Private)
IP Address: 0.0.0.0         Netmask: 0xFFFFFFFF
```

```
MAC: 00-50-7F-00-00-00
Interface 4 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-02
Interface 5 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-03
Interface 6 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-04
Interface 7 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-05
Interface 8 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-06

Interface 9 Ethernet:
Status: DOWN
IP Address: 0.0.0.0         Netmask: 0x00000000
MAC: 00-50-7F-00-00-07
--- MORE ---   ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
>
```

## Telnet Command: sys name

This command can set and remove the name for the router when DHCP mode is selected for WAN.

### Syntax

**sys name** *[wan1] [ASCII string]*

**sys name** *[wan1]* **clear**

### Syntax Description

| Parameter | Description |
|---|---|
| *wan1* | It means to specify WAN interface for assigning a name for it. |
| *ASCII string* | It means the name for router. The maximum character that you can |

| | |
|---|---|
| | set is 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.

**sys passwd** *[ASCII string]*

### Syntax Description

| Parameter | Description |
|---|---|
| *ASCII string* | It means the password for administrator. The maximum character that you can set is 23. |

### Example

```
> sys passwd admin123
>
```

## Telnet Command: sys reboot

This command allows users to restart the router immediately.

### Example

```
> sys reboot
>
```

## Telnet Command: sys autoreboot

This command allows users to restart the router automatically within a certain time.

### Syntax

**sys autoreboot** *[on/off/hour(s)]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | On – It means to enable the function of auto-reboot.<br>Off – It means to disable the function of auto-reboot. |
| *hours* | It means to set the time schedule for router reboot.<br>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
> sys version
Router Model: Vigor2927Lac   Version: 4.2.0 English
Profile version: 4.0.0   Status: 1 (0x9de71d8f)
Router IP: 192.168.1.1   Netmask: 255.255.255.0
Firmware Build Date/Time: Jul  8 2020 11:52:59
Router Name: DrayTek
Revision: 91691 V410_2927
Router serial no: None

>
```

## Telnet Command: sys qrybuf

This command can display the system memory status and leakage list.

### Example

```
> sys qrybuf
System Memory Status and Leakage List

Buf sk_buff  ( 200B), used#: 1647, cached#:   30
Buf KMC4088  (4088B), used#:    0, cached#:    8
Buf KMC2552  (2552B), used#: 1641, cached#:   42
Buf KMC1016  (1016B), used#:    7, cached#:    1
Buf KMC504   ( 504B), used#:    8, cached#:    8
Buf KMC248   ( 248B), used#:   26, cached#:   22
Buf KMC120   ( 120B), used#:   67, cached#:   61
Buf KMC56    (  56B), used#:   20, cached#:   44
Buf KMC24    (  24B), used#:   58, cached#:   70
Dynamic memory: 13107200B; 4573168B used; 190480B/0B in level 1/2 cache.

FLOWTRACK Memory Status
# of free = 12000
# of maximum = 0
# of flowstate = 12000
# of lost by siganture = 0
# of lost by list = 0
```

## Telnet Command: sys pollbuf

This command can turn on or turn off polling buffer for the router.

### Syntax

**sys pollbuf** *[on]*

**sys pollbuf** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on* | It means to turn on pulling buffer. |
| *off* | It means to turn off pulling buffer. |

### Example

```
> sys pollbuf on
% Buffer polling is on!

> sys pollbuf off
```

```
% Buffer polling is off!
```

## Telnet Command: sys britask

This command can improve triple play quality.

### Syntax

**sys britask** *[on]*

**sys britask** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on* | It means to turn on the bridge task for improving the triple play quality. |
| *off* | It means to turn off the bridge task. |

### Example

```
> sys britask on
% bridge task is ON, now
```

## Telnet Command: sys tr069

This command can set CPE settings for applying in VigorACS.

### Syntax

**sys tr069 get** *[parm] [option]*

**sys tr069 set** *[parm] [value]*

**sys tr069 getnoti** *[parm]*

**sys tr069 setnoti** *[parm] [value]*

**sys tr069 log**

**sys tr069 debug** *[on/off]*

**sys tr069 save**

**sys tr069 inform** *[event code]*

**sys tr069 port** *[port num]*

**sys tr069 cert_auth** *[on/off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *get [parm] [option]* | It means to get parameters for tr-069.<br>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.<br>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.<br>[event code] includes:<br>0-"0 BOOTSTRAP",<br>1-"1 BOOT",<br>2-"2 PERIODIC",<br>3-"3 SCHEDULED",<br>4-"4 VALUE CHANGE",<br>5-"5 KICKED",<br>6-"6 CONNECTION REQUEST",<br>7-"7 TRANSFER COMPLETE",<br>8-"8 DIAGNOSTICS COMPLETE",<br>9-"M Reboot" |

| | |
|---|---|
| *port [port num]* | It means to change tr069 listen port number. |
| *cert_auth [on/off]* | on: turn on certificate-based authentication.<br>off: turn off certificate-based authentication. |

### Example

```
> sys tr069 get Int. nextlevel
Total number of parameter is 24
Total content length of parameter is 915
InternetGatewayDevice.LANDeviceNumberOfEntries
InternetGatewayDevice.WANDeviceNumberOfEntries
InternetGatewayDevice.DeviceInfo.
InternetGatewayDevice.ManagementServer.
InternetGatewayDevice.Time.
InternetGatewayDevice.Layer3Forwarding.
InternetGatewayDevice.LANDevice.
InternetGatewayDevice.WANDevice.
InternetGatewayDevice.Services.
InternetGatewayDevice.X_00507F_InternetAcc.
InternetGatewayDevice.X_00507F_LAN.
InternetGatewayDevice.X_00507F_NAT.
InternetGatewayDevice.X_00507F_Firewall.
InternetGatewayDevice.X_00507F_Bandwidth.
InternetGatewayDevice.X_00507F_Applications.
InternetGatewayDevice.X_00507F_VPN.
InternetGatewayDevice.X_00507F_VoIP.
InternetGatewayDevice.X_00507F_WirelessLAN.
InternetGatewayDevice.X_00507F_System.
InternetGatewayDevice.X_00507F_Status.

InternetGatewayDevice.X_00507F_Diagnostics.
--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

## Telnet Command: sys sip_alg

This command can turn on/off SIP ALG (Application Layer Gateway) for traversal.

### Syntax

**sys sip_alg** *[1]*

**sys sip_alg** *[0]*

### Syntax Description

| Parameter | Description |
|---|---|
| *1* | It means to turn on SIP ALG. |
| *0* | It means to turn off SIP ALG. |

## Example

```
> sys sip_alg ?
usage: sys sip_alg [value]
 0 - disable SIP ALG
 1 - enable SIP ALG
 current SIP ALG is disabled
```

## Telnet Command: sys license

This command can process the system license.

### Syntax

**sys license** *licmsg*

**sys license** *licauth*

**sys license** *regser*

**sys license** *licera*

**sys license** *licifno*

**sys license** *lic_wiz [set/reg/qry]*

**sys license** *dev_chg*

**sys license** *dev_key*

### Syntax Description

| Parameter | Description |
|---|---|
| *licmsg* | It means to display license message. |
| *licauth* | It means the license authentication time setting. |
| *regser* | It means the license register server setting. |
| *licera* | It means to erase license setting. |
| *licifno* | It means license and signature download interface setting. |
| *lic_wiz [set/reg/qry]* | It means the license wizard setting.<br>qry: query service support status<br>set [idx] [trial] [service type] [sp_id] [start_date] [License Key]<br>reg: register service in portal |
| *dev_chg* | It means to change the device key. |
| *dev_key* | It means to show device key. |

### Example

```
> sys license licifno

License and Signature download interface setting:
licifno [AUTO/WAN#]

Ex: licifno wan1

Download interface is "auto-selected" now.
```

## Telnet Command: sys 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.<br>w - Available value ranges from 100 to 50000. |
| *level[x]* | It determines the level of data displayed.<br>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, VoIP and EthOAM. |
| *voip_feature [on/off][vf_name]* | It means VoIP feature. Type on to enable the feature or type off to disable the feature.<br>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 Disabled.
 lineno : 10000.
 level : 3.
 Enabled feature: SYS

>
```

## Telnet Command: testmail

This command is used to display current settings for sending test mail.

### Example

```
> testmail
Send out test mail
 Mail Alert:[Disable]
 SMTP_Server:[0.0.0.0]
 Mail to:[]
 Return-Path:[]
```

## Telnet Command: upnp off

This command can close UPnP function.

### Example

```
>upnp off
UPNP say bye-bye
```

## Telnet Command: upnp on

This command can enable UPnP function.

### Example

```
>upnp on
UPNP start.
```

## Telnet Command: upnp nat

This command can display IGD NAT status.

### Example

```
> upnp nat ?
*****************  IGD NAT Status  ***************


((0))
InternalClient >>192.168.1.10<<, RemoteHost >>0.0.0.0<<
InternalPort >>21<<, ExternalPort >>21<<
PortMapProtocol >>TCP<<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
Ftp Example [MICROSOFT]
((1))
InternalClient >>0.0.0.0<<, RemoteHost >>0.0.0.0<<
InternalPort >>0<<, ExternalPort >>0<<
PortMapProtocol >><NULL><<
```

```
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
PortMapProtocol >><NULL><<
The tmpvirtual server index >>0<<
PortMapLeaseDuration >>0<<, PortMapEnabled >>0<<
0<<


--- MORE ---  ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] ---
```

## Telnet Command: upnp service

This command can display the information of the UPnP service. UPnP service must be enabled first.

### Example

```
> upnp on
UPNP start.


> upnp service
>>>>> SERVICE TABLE1 <<<<<
  serviceType urn:schemas-microsoft-com:service:OSInfo:1
  serviceId   urn:microsoft-com:serviceId:OSInfo1
  SCPDURL     /upnp/OSInfo.xml
  controlURL  /OSInfo1
  eventURL    /OSInfoEvent1
  UDN         uuid:774e9bbe-7386-4128-b627-001daa843464

>>>>> SERVICE TABLE2 <<<<<
  serviceType
urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
  serviceId   urn:upnp-org:serviceId:WANCommonIFC1
  SCPDURL     /upnp/WComIFCX.xml
  controlURL  /upnp?control=WANCommonIFC1
  eventURL    /upnp?event=WANCommonIFC1
  UDN         uuid:2608d902-03e2-46a5-9968-4a54ca499148
.
.
.
```

## Telnet Command: upnp subscribe

This command can show all UPnP services subscribed.

### Example

```
> upnp on
UPNP start.
> upnp subscribe
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.<br>n=0, it means to auto-select WAN interface.<br>n=1, WAN1<br>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
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 C331          3.5G              Y
BandRich    Bandluxe C502          3.5G              Y
Huawei     Huawei E169u            3.5G              Y
Huawei     Huawei E220             3.5G              Y
Huawei     Huawei E303D            3.5G              Y
Huawei     Huawei E392             3.5G              Y
Huawei     Huawei E398             3.5G              Y
Sony Erics  Sony Ericsson MD30     3.5G              Y
TP-LINK    TP-LINK MA180           3.5G              Y
TP-LINK    TP-LINK MA260           3.5G              Y
```

```
Vodafone    Vodafone K3765-Z        3.5G                Y
Vodafone    Vodafone K4605          3.5G                Y
ZTE         ZTE MF626               3.5G                Y
ZTE         ZTE MF627 plus          3.5G                Y
ZTE         ZTE MF633               3.5G                Y
ZTE         ZTE MF636               3.5G                Y

SpinCom     SpinCom GPRS Modem      3.5G                Y
- MORE - ['q': Quit, 'Enter': New Lines, 'Space Bar': Next Page] -
```

## Telnet Command: vigbrg on

This command can make the router to be regarded as a modem but not a router.

### Example

```
> vigbrg on
%Enable Vigor Bridge Function!
```

## Telnet Command: vigbrg off

This command can disable vigor bridge function.

### Example

```
> vigbrg off
%Disable Vigor Bridge Function!
```

## 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 wan1on

This command is used to enable the bridge WAN1 management.

### Example

```
> vigbrg wan1on
%Enable Vigor Bridge Wan1 management!
```

## Telnet Command: vigbrg wan1off

This command is used to disable the bridge WAN1 management.

### Example

```
> vigbrg wan1off
%Disable Vigor Bridge Wan1 management!
```

## Telnet Command: fullbrg

The command is used to enable Full Bridge Mode so that the router will work as a bridge modem which is able to forward incoming packets with VLAN tags.

### Syntax

**fullbrg status**

**fullbrg set -i** *[WAN index]* **-n** *[Subnet index]* **-b** *[Bridge mode]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-I [WAN index]* | WAN index: Ranges from 1 to 10. |

| | |
|---|---|
| | 1: WAN1, 2: WAN2, …etc.,<br>In which, WAN3 and WAN 4 are USB WAN. |
| *-n[Subnet index]* | Subnet index: Ranges from 1 to 8.<br>1: Subnet 1, 2: Subnet 2, …etc. |
| *-b[Bridge mode]* | It means to enable / disable Bridge mode.<br>0: OFF<br>1: ON |

### Example

```
> fullbrg status ?
Show gConfig setting of full bridge
WAN 1 full bridge to LAN 1, mode=OFF.
WAN 2 full bridge to LAN 1, mode=OFF.
WAN 5 full bridge to LAN 1, mode=OFF.
WAN 6 full bridge to LAN 1, mode=OFF.
WAN 7 full bridge to LAN 1, mode=OFF.
WAN 8 full bridge to LAN 1, mode=OFF.
WAN 9 full bridge to LAN 1, mode=OFF.
WAN10 full bridge to LAN 1, mode=OFF.
> fullbrg set -i 2 -n 5 -b 1
Configure OK! Please reboot device to make it effective.
> sys reboot
> fullbrg status
Show gConfig setting of full bridge
WAN 1 full bridge to LAN 1, mode=OFF.
WAN 2 full bridge to LAN 5, mode=ON.
WAN 5 full bridge to LAN 1, mode=OFF.
WAN 6 full bridge to LAN 1, mode=OFF.
WAN 7 full bridge to LAN 1, mode=OFF.
WAN 8 full bridge to LAN 1, mode=OFF.
WAN 9 full bridge to LAN 1, mode=OFF.
WAN10 full bridge to LAN 1, mode=OFF.
```

## Telnet Command: voip debug

This command can display debug message on the screen.

### Syntax

**voip debug** *[flush]*

**voip debug** *[showmsg]*

### Syntax Description

| Parameter | Description |
|---|---|
| *flush* | It means to clear current log. |
| *showmsg* | It means to show current log. |

### Example

```
> voip debug showmsg
-->Send Message to 192.168.1.2:5060 <02:35:16>
INVITE sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.1:5060;branch=z9hG4bK-YMa-3630;rport
From:  <sip:change_me@192.168.1.1>;tag=WLJ-11782
To: <sip:192.168.1.2>
Call-ID: PbU-25312@192.168.1.1
CSeq: 1 INVITE
Contact: <sip:change_me@192.168.1.1>
Max-Forwards: 70
supported: 100rel, replaces
User-Agent: DrayTek UA-1.2.3 DrayTek Vigor2910
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, INFO, REFER, NOTIFY, PRACK
Content-Type: application/sdp
Content-Length:   264

v=0
o=change_me 5972727 56415 IN IP4 192.168.1.1
```

## Telnet Command: voip dialplan

This command allows users to set phone book settings.

### Syntax

**voip dialplan block** *n [-<command><parameter>]*

**voip dialplan phonebook** *n [-<command><parameter>]*

**voip dialplan region** *[-<command><parameter>]*

**voip dialplan local** *[1/0]*

### Syntax Description

| Parameter | Description |
|---|---|
| **voip dialplan block** | |
| *n* | It means the index number of the VoIP settings.<br>n=1 ~ 20 |

| | |
|---|---|
| *-<command><parameter>* | The available commands with parameters are listed below. |
| *-m 0/1* | It means to enable or disable the block mode.<br>0 – Disable<br>1 - Enable |
| *-p <path>* | Determines the block path.<br>1:in_url,<br>2:in_number<br>3:out_url,<br>4:out_number<br>5:(in & out)_url,<br>6:(in & out)_number) ) |
| *-n <number>* | Determines the block number (maximum 29 characters). |
| *-d <domain>* | Block the specified domain. |
| *-i <inf>* | Block the specified interface(s) or All interfaces. |
| *-s <Schedule>* | Specify schedule profiles by indicating the index number of the schedule profile. Four schedule profiles can be used at one time. |
| *-w* | Delete the selected entry. N=null (clear all) |
| *-v* | List current settings. |
| **voip dialplan phonebook** | |
| *n* | It means the index number of the VoIP settings.<br>n=1 ~ 60 |
| *-<command><parameter>* | The available commands with parameters are listed below. |
| *-d <number>* | Specify the speed dial number. |
| *-c <url>* | Contact SIP URL l(max. 59 characters) |
| *-n <name>* | Contact name (max. 23 characters) |
| *-a <enable>* | Enable/disable the specify entry. |
| *-m <mode>* | Specify backup number mode.<br>0 – none<br>2 - PSTN |
| *-b <number>* | Spedify the backup number. |
| *-o <acc num>* | Specify the dial out account.<br>0 – default<br>1 - acc1, 2 - acc2… ~ 12:=acc12 |
| *-z <enable>* | Enable/disable ZRTP/SRTP VoIP security. |

| | |
|---|---|
| | 1 – enable<br>0 - disable |
| *-l* | Delete the specify entry. |
| *-V* | List current VoIP settings. |
| **voip dialplan region** | |
| *-e* | Dnable or disable the regional function.<br>1 – enable<br>0 - disable |
| *-m <number>* | Return the last miss call. |
| *-I <number>* | Return the last incoming call. |
| *-o <number>* | Return the last outgoing call. |
| *-F <number>* | Hotkey to enable call forwarding (all) function. |
| *-f <number>* | Hotkey to enable call forwarding (busy) function. |
| *-C <number>* | Hotkey to enable call forwarding (no answer) function. |
| *-c <number>* | Hotkey to disable call forwarding function. |
| *-W <number>* | Hotkey to enable call waiting function. |
| *-w <number>* | Hotkey to disable call waiting function. |
| *-H <number>* | Hotkey to enable hide caller ID function. |
| *-h <number>* | Hotkey to disable hide caller ID function. |
| *-D <number>* | Hotkey to enable DND function. |
| *-d <number>* | Hotkey to disable DND function. |
| *-A <number>* | Hotkey to enable block anonymous calls function. |
| *-a <number>* | Hotkey to disable block anonymous calls function. |
| *-U <number>* | Hotkey to enable block unknow domain calls function. |
| *-u <number>* | Hotkey to disable block unknow domain calls function. |
| *-P <number>* | Hotkey to disable block IP calls function. |
| *-p <number>* | Hotkey to disable block IP calls function. |
| *-I <number>* | Hotkey to block last incoming call. |
| *-v* | List current status for Regional settings. |
| **voip dialplan local** | |
| *enable/disable* | Enable or disable the local calls.<br>1 – enable |

| | |
|---|---|
| | 0 - disable |

### Example

```
> voip dialplan phonebook 1 -d 1125
> voip dialplan region -l 8
> voip dialplan region -v
 Your Setting for Regional
 Regional Function is: Enable
 Return the Last Miss Call: 20
 Return the Last Incoming Call: *12
 Return the Last Outgoing Call: 1
 Hotkey to enable call forwarding (all) function: 0
 Hotkey to enable call forwarding (busy) function: *90
 Hotkey to enable call forwarding (no answer) function: *92
 Hotkey to disable call forwarding function: 12
 Hotkey to Enable Call Waiting Function: *56
 Hotkey to Disable Call Waiting Function: *57
 Hotkey to Enable Hide Caller ID Function: *67
 Hotkey to Disable Hide Caller ID Function: *68
 Hotkey to Enable DND Function: *78
 Hotkey to Disable DND Function: *79
 Hotkey to Enable Block Anonymous Calls Function: *77
 Hotkey to Disable Block Anonymous Calls Function: *87
 Hotkey to Enable Block Unknow Domain Calls Function: *40
 Hotkey to Disable Block Unknow Domain Calls Function: *04
 Hotkey to Enable Block IP Calls Function: *50
 Hotkey to Disable Block IP Calls Function: *05
 Hotkey to Disable Block The Last Incoming Call Function: 8
```

## Telnet Command: voip dsp

### Syntax

**voip dsp countrytone** *[channel] [value]*

**voip dsp dialtonepwr** *[channel] [AbsoluteValue]*

**voip dsp EchoCanceller** *[type] [w_size] [nlp]*

**voip dsp cidtype** *[channel] [value]*

**voip dsp micgain** *[channel] [value/(1~10)]*

**voip dsp spkgain** *[channel] [value/(1~10)]*

**voip dsp jitterBuffer** *[port] [mode] [value]*

**voip dsp dtmfDetset** *[nLevel] [nTwist]*

**voip dsp dtmftonepwr** *[Level]*

**voip dsp cwtonepwr** *[ch] [value]*

**voip dsp pstnringfxs** *[1|2] [on|off]*

**voip dsp relaydbounce** *[on|off]*

**voip dsp setRingPat** *[ring_pattern_index] [patten_num]*

*voip dsp setDtmfCidlevel –l [value]*

*voip dsp setDtmfCidlevel –h [value]*

*voip dsp setDtmfCidlevel –r 0*

*voip dsp cidplusdigit [1/0] [channel] [value]*

## Syntax Description

| Parameter | Description |
|---|---|
| **voip dsp countrytone** | |
| *[channel] [value]* | This command allows users to set the region for the tone settings. Different regions usually need different tone settings.<br>Channel – 1 or 2.<br>Value – displayed as follows:<br>[2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany,<br>[7] Netherlands, [8] Portugal, [9] Sweden, [10] Australia,<br>[11] Slovenia, [12] Czech, [13] Slovakia, [14] Hungary,<br>[15] Switzerland , [16] France , [17] Malta |
| *voip dsp dialtonepwr* | |
| *channel* | This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.<br>Channel - Available channel number: 1 – 2 |
| *AbsoluteValue* | AbsoluteValue - In -1 dB increments, with 1 corresponding to 6 dBm.<br>Range - 1 to 30 |
| *voip dsp EchoCanceler* | |
| *type* | This command is used to set the type of echo reduction.<br>0 - Disable the LEC processing.<br>1 - Cancel using the fixed window.<br>2 - Cancel using the fixed and moving window.<br>3 - Cancel using fixed window + Echo Suppressor. |
| *w_size* | The Line Echo Canceller (LEC) window size is 4, 6, 8 or 16 (ms). |
| *nlp* | Nlp - Non-linear processing (NLP) for more smooth transitions.<br>1 - disable |

| | |
|---|---|
| | 0 - enable |
| *voip dsp cidtype* | |
| *channel* | Set the caller ID type for FXS 1 (Channel 1) or FXS 2 (Channel 2).<br>1 – FXS 1<br>2 – FXS 2 |
| *value* | Each number (1 to 6) represents different type.<br>1 – FSK_ETSI<br>2 - FSK_ETSI(UK)<br>3 - FSK_BELLCORE(US/AU)<br>4 - DTMF<br>5 - DTMF(Dk)<br>6 - DTMF(SE,NL,FIN)<br>For example :<br>Vigor> voip dsp cidtype 2 6<br>channel=2, current cidType: 6<br>That means the caller ID type for FXS2 (Channel2) is DTMF (SE, NL, FIN). |
| *voip dsp micgain* | |
| *channel* | Adjust the volume of microphone by entering number from 1- 10 for FXS 1 or FXS 2.<br>1 – FXS 1<br>2 – FXS 2 |
| *value/(1~10)* | The larger the number is, the louder the volume will be. |
| *voip dsp spkgain* | |
| *channel* | Adjust the volume of speaker by entering number from 1- 10 for FXS 1 or FXS 2.<br>1 – FXS 1<br>2 – FXS 2 |
| *value/(1~10)* | The larger the number is, the louder the volume will be. |
| *voip dsp jb* | |
| port | Set the size of jitter buffer.<br>Available settings are 0 (FXS1) and 1 (FXS2). |
| mode | Available settings are **Fixed** and **Adaptive** (default setting). |
| value | Available settings are 1 ~ 180 (unit: msec).<br>e.g.,<br>Vigor> voip dsp jb 1 FIXED 100 |

| *voip dsp timer* | |
|---|---|
| *[Timer]* | Set the waiting time for dialing out.<br>It means to set the timer settings. The unit is mini-second. The range is from 1 to 255. Value “1” is corresponding to 500ms. That is to say, Value “6” is corresponding 3000ms (i.e., 3 seconds)<br>Timer: 1 ~ 20.<br>Vigor> voip dsp timer 20<br>Set the timer:20 |
| *Voip dsp debugMsg* | |
| *?* | Avaible settings include:<br>clrev - clear phone hook status.<br>getev - get phone hook status.<br>clrfskcid - clear fsk data for caller-ID from PSTN line.<br>getfskcid - get fsk data for caller-ID from PSTN line.<br>clrdtmfcid - clear dtmf data for caller-ID from PSTN line.<br>getdtmfcid - get dtmf data for caller-ID from PSTN line.<br>voicebuf - get message for available voice buffer pool.<br>clrint - clear status for interrupt.<br>getint - get status for interrupt.<br>Vigor> voip dsp debugMsg getint<br>the interrupt status for ad0 = 21<br>the interrupt status for ad1 = 0<br>the interrupt status for vc = 0 |
| *voip dsp dtmfDetset* | |
| *nLevel* | Set minimal signal level in dB, for DTMF detection.<br>Range – (-96 ~ -1) |
| *nTwist* | Maximum allowed signal twist in dB, for DTMF detection.<br>Range – (0 ~ 12) |
| *voip dsp dtmftonepwr* | |
| *Level* | Set power level for DTMF frequency.<br>Level – 0 ~ 100. Power level for dtmf frequency in 0.3 dB steps.<br>0 map to 0dB<br>1 map to -0.3dB …. 100 map to -30dB |
| *voip dsp cwtonepwr* | |
| *ch* | Set the call waiting tone power level.<br>1 – FXS 1 |

| | |
|---|---|
| | 2 – FXS 2. |
| *value* | 1 ~ 30, in -1 dB increments, with 1 corresponding to 8 dBm. |
| *voip dsp pstnringfxs* | |
| *1\|2* | Enable or disable PSTN ring on FXS 1/FXS 2.<br>1 meansFXS1; 2 means FXS2. |
| *on\|off* | On means enable; off means disable. |
| *voip dsp relaydbounce* | |
| *on\|off* | on: Enable relay filter noise. But it maybe ignore the caller-id!!!<br>off: Disable relay filter noise. But the noise will cause the relay to switch to PSTN!!! |
| *voip dsp setRingPat* | |
| *ring_pattern_index* | This command can change the ring pattern at Index(2)~Index(6).<br>ring_pattern_index – Index (1) was locked for your country. |
| *patten_num* | It's the ring pattern number (1~12) for a country.<br>----------<br>*patten_num=1 Australia Ring Pattern:*<br>*cadenceOneOn=400, cadenceOneOff=200*<br>*cadenceTwoOn=400, cadenceTwoOff=2000*<br>*patten_num=2 Denmark Ring Pattern:*<br>*cadenceOneOn=1000, cadenceOneOff=4000*<br>…… |
| *voip dsp setFaxECmode -s* | |
| *ch* | Set the FAX error correction mode.<br>ch : range (0 ~ 1) |
| *mode* | mode : EC(error correction) ch(x) mode(0) : REDUNDANCY<br>EC(error correction) ch(x) mode(1) : FEC |
| *voip dsp setDtmfCidlevel –l / voip dsp setDtmfCidlevel –h [value]*<br>*voip dsp setDtmfCidlevel –r 0* | |
| *value* | "setDtmfCidLevel" is used to configure the signal strength for transferring to FXS DTMF caller ID.<br>value - 0 ~ 64<br>voip dsp setDtmfCidLevel -l [value]<br>voip dsp setDtmfCidLevel -h [value]<br>voip dsp setDtmfCidLevel -r 0/1<br>r - reset low/high DTNF level to default setting. 0 means Disable; 1 |

| | |
|---|---|
| | means Enable.<br>Note: This function is supported only by special mode. |
| *voip dsp setfxoCY* | |
| *value* | It is used to apply FXO country settings.<br>0: "use system country"<br>1: "Taiwan"<br>2: "Germany"<br>3: "Sweden"<br>4: "France"<br>5: "Switzerland"<br>6: "Holland"<br>7: "Finland"<br>8: "Denmark"<br>9: "UK"<br>10: "Australia"<br>12: "Italy"<br>14: "Red_China"<br>15: "Singapore"<br>17: "Spain"<br>18: "Portugal"<br>20: "Poland"<br>21: "Czech"<br>22: "Hungary"<br>23: "Slovenia"<br>25: "Slovakia"<br>37: "Brasil"<br>61: "US" |
| *voip dsp setfxoringl* | |
| *value* | It is used to configure detection ring voltage threshold to apply to FXO.<br>Available setting include:<br>0 : use driver default value<br>1 : Minimum voltage threshold: 25V<br>2 : Minimum voltage threshold: 35V<br>3 : Minimum voltage threshold: 45V<br>Note: This function is supported only by special mode. |
| *voip dsp setfxoCid* | |
| *value* | Set FXO detect caller ID type.<br>It is available only for the model with FXO port. |
| *voip dsp cidplusdigit* | |

| | |
|---|---|
| *[1/0] [channel] [value]* | Set the substitution (0~9) for '+' digit in caller ID.<br>1 – enable the substitution.<br>0 – disable the substitution.<br>channel – 0 (FXS 1) -1 (FXS 2)<br>value – 0 – 9 |
| *voip dsp setRingThres* | |
| *port* | Set the threshold for ring signal.<br>Port setting is "0" only. |
| *value* | Available settings 0-250. Unit is ms.<br>The time is an approximate value. |
| *voip dsp setCidDetGain* | |
| *tx\|rx gain* | Set the gain value of caller ID detected.<br>Tx gain – Available settings -24 ~ 12. Default is 0.<br>Rx gain – Available settings -24 ~ 12. Default is -6. |

## Example

```
> voip dsp countrytone ?
VoIP has been disable. Please enable VoIP first.
> voip sip misc –D 0
System reboot now!
> voip dsp countrytone ?
> Vigor> voip dsp countrytone?
usage:
 voip dsp countrytone [channel][value]
 [channel]: 1-2
 [value]: ( [2] UK, [3] USA, [4] Denmark, [5] Italy, [6] Germany, [7] Netherland
s, [8] Portugal, [9] Sweden, [10] Australia, [11] Slovenia, [12] Czech, [13]
Slovakia, [14] Hungary, [15] Switzerland , [16] France , [17] Malta)
============  Channel=1  ====================
 current country tone: user defined

----------- ( Dial tone ) --------------------
 Feq1=425, Feq2=0, OneOn=0, Off=0, TwoOn=0, TwoOff=0
----------- ( Ringing tone ) -----------------
 Feq1=425, Feq2=0, OneOn=1500, OneOff=3000, TwoOn=0, TwoOff=0
----------- ( Busy tone ) --------------------
 Feq1=425, Feq2=0, OneOn=200, OneOff=200, TwoOn=0, TwoOff=0
```

```
============  Channel=2  ===================
 current country tone: user defined
> voip dsp dialtonepwr 1 20
Current power level of dialtone:20 (-13 db), channel=1
> voip dsp setCidDetGain tx 1
 Current CID Detect Tx Gain [1], Rx Gain [-6]
> voip dsp setCidDetGain rx 3
 Current CID Detect Tx Gain [1], Rx Gain [3]
```

## Telnet Command: voip rtp

### Syntax

**voip rtp codec** *[sip acc index][type|size|vad|one][value]*

**voip rtp dtmf** *[index] [mode|payloadtype][value]*

**voip rtp port** *[start|end] [value]*

**voip rtp symmetric** *[value]*

**voip rtp tos ?**

### Syntax Description

| Parameter | Description |
|---|---|
| *voip rtp codec* | |
| *[sip acc index][type\|size\|vad\|one][value]* | Set the voice coding.<br>sip acc index –SIP account index number. Available number, 1 ~ 12.<br>type – Available settings include<br>0. G.711MU<br>1. G.711A<br>2. G.729A/B<br>3. G.723<br>4. G.726_32<br>size - Five options,<br>0 means 10ms<br>1 means 20ms<br>2 means 30ms<br>3 means 40ms<br>5 means 60ms<br>Vad - 0 means to Disable the function of Voice Active Detector (vad); 1 means to Enable the function of Voice Active Detector (vad).<br>One – 0 means to Disable the function of single codec; 1 means to |

| | |
|---|---|
| | Enable the function of single codec. |
| *voip rtp dtmf* | |
| *[index] [mode \| payloadtype][value]* | Set the DTMF mode and Payload type for DTMF.<br>Index – SIP account index number. Available number, 1 ~ 12.<br>Mode – Four options to be selected.<br>0. Inband<br>1. Outband<br>2. SIP INFO (cisco)<br>3. SIP INFO (nortel)<br>Payloadtype – Available settings 96~127.<br>Value – Type 0~3 or 96~127 based on the mode specified.<br>For example,<br>> voip rtp dtmf 1 mode 1 |
| *voip rtp port* | |
| *start\|end* | Specifies the start/end port for RTP stream. |
| *value* | The default value is 10050/15000. |
| *voip rtp symmetric* | |
| *value* | Make the data transmission going through on both ends of local router and remote router not misleading due to IP lost.<br>1 – Enable<br>0 - Disable |
| *voip rtp tos* | |
| *value* | Set the type of service (TOS) setting for RTP packets.<br>For example,<br>> voip rtp tos 0x899<br>Set TOS: 0x899 |

## Example

```
> voip rtp codec 1 type 3
> voip rtp dtmf 2 mode 3
> voip rtp port start 10070 end 14400
Set start port: 10070
> voip rtp port end 14400
Set end port: 14400
> voip rtp symmetric 1
Set symmetric rtp to Enable
```

## Telnet Command: voip sip

This command allows users to set SIP account.

### Syntax

**voip sip acc n** *[-<command> <parameter> | ... ]*

**voip sip calllog**

**voip sip ep n** *[-<command> <parameter> | ... ]*

**voip sip misc***[-<command> <parameter> | ... ]*

**voip sip nat** *[-<command> <parameter> | ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *voip sip acc* - Allows users to set SIP account. | |
| *n* | n = 1 to 12<br>It means the index number of the VoIP settings. |
| *-P [profile]* | It means the name of the account profile (maximum 11 characters). |
| *-r [reg mode]* | Set registration mode for SIP account.<br>0 – none<br>1 – auto<br>2 - wan1 only<br>3 - wan2 only<br>4 - lan/vpn<br>5 – PVC<br>6 - wan3 only<br>7 - wan4 only<br>8 - wan1 first<br>9 - wan2 first<br>10 - wan3 first<br>11 - wan4 first |
| *-o [port]* | Set the port number for sending/receiving SIP message for building a session. The default value is 5060. |
| *-d [domain]* | Set the domain name or IP address of the SIP Registrar server. The maximum is 63 characters. |
| *-y [proxy]* | Set domain name or IP address of SIP proxy server. The maximum is 63 characters. |
| *-b [enable]* | Enable / disable outbound proxy by SIP account.<br>0 – disable<br>1 - enable |
| *-s [enable]* | Enable / disable to locate SIP server (rfc 3263).<br>0 – disable |

| | |
|---|---|
| | 1 - enable |
| *-N [name]* | Set SIP account display name.<br>Name - max. 23 characters. |
| *-n [number]* | Set SIP account number.<br>Number - max. 63 characters. |
| *-a [id]* | Set SIP authentication ID.<br>Id - max. 63 characters. |
| *-A [enable]* | Enable /disable to use SIP authentication ID.<br>0 – disable<br>1 - enable |
| *-p [passwd]* | Set SIP account password (max. 63 characters). |
| *-e [sec]* | Set expiry time (default 3600) for SIP account. |
| *-w [enable]* | Enable to make phone call without registering. |
| *-m [mode]* | Set NAT traversal mode.<br>0 – disable<br>1 – stun<br>2 – manual<br>3 - nortel |
| *-F [mode]* | Set call forwarding mode.<br>0 – disable<br>1 – always<br>2 – busy<br>3 - no answer<br>4 - busy or no answer |
| *-u [url]* | Set SIP URL for call forwarding (max. 63 characters). |
| *-t [sec]* | Set call forwarding timer. For example,<br>voip sip acc 1 –t 30 |
| *-g [port]* | Set the ring port for incoming call. For example,<br>Port - r1 means FXS1; r2 means FXS2. |
| *-z [pattern]* | Set account ring pattern (1 ~ 6). |
| *-i [enable]* | Remove all bindings while they are un-registered. 0 means Disable; and 1 means Enable. |
| *-B <enable>* | Enable / disable the function of Broadsoft Call Control.<br>0 – disable<br>1 - enable |

| | |
|---|---|
| *-S [idx]* | Enable and use alias IP to register.<br>idx - 1 to 31. If 0 is used, such function will be disabled. |
| *-k [num1 num2…]* | Set backup wan list (first wan, second wan…).<br>range: 1 to 4. |
| *-v* | View current status for account settings. |
| *Voip sip calllog* | Display current status for SIP call log. |
| *voip sip ep* | |
| *n* | The index number of the VoIP settings.<br>n – 1, 2. |
| *-o [acc]* | Available dial out account (1 ~ 12). |
| *-L [url]* | Set SIP URL (max. 63 characters) for hot line. |
| *-l [enable]* | Enable / disable the function of hot line.<br>0 – disable<br>1 - enable |
| *-W [enable]* | Enable / disable the function of warm line.<br>0 – disable<br>1 - enable |
| *-w [enable]* | Enable / disable the function of call waiting enable.<br>0 – disable<br>1 - enable |
| *-E [enable]* | Enable / disable the function of call waiting enable but only remind one time.<br>0 – disable<br>1 - enable |
| *-x <enable>* | Enable / disable the function of call transfer.<br>0 – disable<br>1 - enable |
| *-d [enable]* | Enable / disable the function of DND (Do Not Disturb)<br>0 – disable<br>1 - enable |
| *-s [id]* | Indicate DND schedule.<br>Id - s1, s2, s3, s4 (max. 4 schedule) |
| *-h [enable]* | Enable / disable the function of calling line identification restriction (CLIR).<br>0 – disable |

| | |
|---|---|
| | 1 - enable |
| *-u [mode]* | Set CLIR mode.<br>0 - means “draft-ietf-sip-privacy”<br>1 – means “rfc 3323/3325)” |
| *-z [enable]* | Enable / disable playing dial tone when registered on sip server.<br>0 – disable<br>1 - enable |
| *-n [enable]* | Enable / disable session timer.<br>0 – disable<br>1 - enable |
| *-m [sec]* | Set the value for session timer (unit: sec). |
| *-R [min,max]* | Set the flash hook time range 100~2000 (unit: ms). |
| *-8 [enable]* | Enable or disable T.38 fax relay feature.<br>0 – disable<br>1 - enable |
| *-v* | View current settings. |
| *voip sip misc* - Allows users to set miscellaneous settings for the device. | |
| *-c [enable]* | Enable compact header to shorten the packet (0: disable, 1: enable). |
| *-s [enable]* | Change “#” into digit number.<br>0 - disable<br>1 - enable |
| *-e [enable]* | Enable Europe style flash hook operation mode.<br>0 - disable<br>1 - enable |
| *-h [enable]* | Enable/disable call hold mode based on protocol RFC2543 (0: disable, 1:enable). |
| *-i [enable]* | Enable CODEC change without Re-INVITE.<br>0 - disable<br>1 - enable |
| *-p [enable]* | Enable PRACK message.<br>0 – Not support PRACK.<br>1 – Support PRACK. |
| *-P [enable]* | Enable IP Call.<br>0 – Disable IP call. |

| | |
|---|---|
| | 1 – Enable IP call. |
| *-H [enable]* | SIP INFO packet will be sent out when encounting hook flash event.<br>0 - disable<br>1 - enable |
| *-t [val]* | Set the mode of User-Agent (e.g., phone, software, and device) for SIP packet.<br>0 - Hide SIP header "User-Agent".<br>1 - Show SIP header "User-Agent".<br>2 - Use default "User-Agent" value.<br>3 - Use user-defined "User-Agent" value. |
| *-u UAValue* | For every SIP user agent identifies itself with a string, this command allows you to set the value (e.g, IP address, phone number, e-mail address) of User-Agent. The length of the string must be less than 64 characters. |
| *-D [disable]* | Disable VoIP Service.<br>1 – disable VoIP service.<br>0 – enable VoIP service.<br>System will automatic reboot to activate voip service |
| *-v* | View current status for miscellaneous settings. |
| *voip sip nat* - Allows users to set NAT Traversal Setting. | |
| *-s [server]* | Set the IP address for STUN server. |
| *-t [sec]* | Set ping interval for SIP account.<br>Sec – 6 ~ 600 |
| *-i [ip]* | Indicate external IP address. |
| *-v* | View current settings for SIP NAT. |

## Example

```
> voip sip misc -t 1
includes User-Agent header

> voip sip misc -u 91704688carrie
user-defined User-Agent:91704688carrie
> voip sip acc 1 -P carrie_1 -r 1 -d 172.16.3.133
> voip sip acc 1 -t 30
> voip sip misc -h 1
> voip sip acc 1 -v
index        :  1
```

```
profile      :  carrie_1
reg mode     :  1 | reg. [No]
alias_ip_idx      :  0
backup list       :
domain       :  172.16.3.133
proxy        :   | outbound [No] | DNS-SRV [No]
noreg call   :  No
disp. Name   :
acc number   :  ---
auth. ID     :   | [disable]
expiry       :  3600
NAT mode     :  0
ring ports   :  0
ring pat.    :  1
call fwd mode     :  0
call fwd url      :
call fwd timer    :  30
Broadsoft    :  disable
Italian ITSP modification: disable
```

## Telnet Command: voip secure

This command allows users to enable or disable secure phone feature, and SAS voice prompt.

### Syntax

**voip secure general** *[-<command> <parameter> | … ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *voip secure general -e* | Enable / disable secure phone feature.<br>0 - disable<br>1 - enable |
| *voip secure general -p* | Enable /disable SAS voice prompt.<br>0 - disable<br>1 - enable |
| *voip secure general -v* | view only secure phone general settings |

### Example

```
> voip secure general -v
secure phone feature is disabled
```

```
SAS voice prompt is enabled
> voip secure general -p  0
SAS voice prompt is disabled
```

## Telnet Command: 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]* **phase***1[lifetime]*

**vpn l2lset** *[list index]* **phase2***[lifetime]*

### Syntax Description

| Parameter | Description |
|---|---|
| *list index* | It means the index number of L2L (LAN to LAN) profile. |
| *peerid* | It means the peer identity for aggressive mode. |
| *localid* | It means the local identity for aggressive mode. |
| *main* | It means to choose proposal for main mode. |
| *auto index* | It means to choose default proposals. |
| *proposal index* | It means to choose specified proposal. |
| *aggressive* | It means the chosen DH group for aggressive mode |
| *pfs* | It means “perfect forward secrete”. |
| *on/off* | It means to turn on or off the PFS function. |
| *phase1* | It means phase 1 of IKE. |
| *lifetime* | It means the lifetime value (in second) for phase 1 and phase 2. |
| *phase2* | It means phase 2 of IKE. |

### Example

```
> VPN l2lset 1 peerid 10226
```

## Telnet Command: vpn l2lDrop

This command allows users to terminate current LAN to LAN VPN connection.

### Example

```
> vpn l2lDrop
>
```

## 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*> **motp** <*on/off*>

**vpn dinset** <*list index*> **pin_secret** <*pin*> <*secret*>

### Syntax Description

| Parameter | Description |
|---|---|
| <*list index*> | It means the index number of the profile. |
| <*on/off*> | It means to enable or disable the profile.<br>on – Enable.<br>off – Disable. |
| *motp* <*on/off*> | It means to enable or disable the authentication with mOTP function.<br>on – Enable.<br>off – Disable. |
| *pin_secret*<*pin*> <*secret*> | It means to set PIN code with secret.<br><*pin*> **-** Enter the code for authentication (e.g, 1234).<br><*secret*> - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6) |

### 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] [1/2/3/4/5/6]*

### Syntax Description

| Parameter | Description |
|---|---|
| *<index>* | It means the index number of the VPN profile. |
| *<1/2/3/4/5/6>* | 1 – it means LAN1<br>2 – it means LAN2.<br>3 – it means LAN3<br>4 – it means LAN4.<br>5 – it means LAN51<br>6 – it means LAN6. |

### 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.<br>e.g.,<br>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.<br>e.g.,<br>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.<br>e.g.,,<br>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.<br>e.g.,<br>vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0 |

## Example

```
> vpn setup 1 name1 dialin 1.2.3.4 vigor 1234 abc 192.168.1.0 255.255.255.0
% Profile Change Log ...

% Profile Index : 1
% Profile Name : name1
% Username : vigor
% Password : 1234
% Pre-share Key : abc
% Call Direction : Dial-In
% Type of Server :  ISDN PPTP IPSec L2TP
% Dial from : 1.2.3.4
% Remote NEtwork IP : 192.168.1.0
% Remote NEtwork Mask : 255.255.255.0
>
```

## Telnet Command: vpn option

This command allows users to configure settings for LAN to LAN profile.

### Syntax

**vpn option** <*index*> <*cmd1*>=<*param1*> [<*cmd2*>=<*para2*> | … ]

### Syntax Description

| Parameter | Description |
|---|---|
| <*index*> | It means the index number of the profile.<br>Available index numbers:<br>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.<br>on – Enable<br>off - Disable |
| *thr* | It means the way that VPN connection passes through. Available settings are wlf, wlo, w2f, and w2o.<br>w1f – WAN1 First.<br>w1o – WAN1 Only.<br>w2f – WAN2 First.<br>w2o – WAN2 Only. |
| *nnpkt* | It means the NetBios Naming Packet.<br>on – Enable the function to pass the packet.<br>off – Disable the function to block the packet. |
| *dir* | It means the call direction. Available settings are b, o and i.<br>b – Both<br>o – Dial-Out<br>i – Dial-In. |
| *idle=[value]* | It means Always on and Idle Time out.<br>Available values include:<br>-1 – it means always on for dial-out.<br>0 – it means always on for dial-in.<br>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.<br>-1 – disable the function.<br>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”.<br>“ctype=t” means PPTP.<br>“ctype=s” means IPSec.<br>“ctype= l” means L2TP(IPSec Policy None).<br>“ctype= l1” means L2TP(IPSec Policy Nice to Have).<br>“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.<br>“ltype=0” means “Disable”.<br>“ltype=1” means “64kbps”.<br>“ltype=2” means “128kbps”.<br>“ltype=3” means “BOD”. |
| *oname* | It means Dial-Out Username.<br>“oname=admin” means to set Username = admin. |
| *opwd* | It means Dial-Out Password<br>“opwd=1234” means to set Password = 1234. |
| *pauth* | It means PPP Authentication.<br>“pauth=pc” means to set PPP Authentication = PAP&CHAP.<br>“pauth=p” means to set PPP Authentication = PAP Only |
| *ovj* | It means VJ Compression.<br>“ovj=on/off” means to enable/disable VJ Compression. |
| *okey* | It means IKE Pre-Shared Key.<br>“okey=abcd” means to set IKE Pre-Shared Key = abcd. |
| *ometh* | It means IPSec Security Method.<br>“ometh=ah/” means AH.<br>“ometh=espd/espda/” means ESP DES without/with Authentication.<br>“ometh=esp3/esp3a/” means ESP 3DES without/with Authentication.<br>“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.<br>"rcallb=on/off" means to enable/disable Set Require Remote to Callback. |
| *ikeid* | It means IKE Local ID.<br>"ikeid=vigor" means Set Local ID = vigor. |
| **For Dial-In Settings** | |
| *itype* | It means Allowed Dial-In Type. Available settings include:<br>"itype=t" means PPTP.<br>"itype=s" means IPSec.<br>"itype=L1"means L2TP (None).<br>"itype=L1" means L2TP(Nice to Have).<br>"itype=l2" means L2TP(Must). |
| *peer* | It means specify Peer VPN Server IP for Remote VPN Gateway.<br>Type "203.12.23.48" means to allow VPN dial-in with IP address of 203.12.23.48.<br>Type "off" means any remote IP is allowed to dial in. |
| *peerid* | It means the peer ID for Remote VPN Gateway.<br>Type "draytek" means the word is used as local ID. |
| *iname* | It means Dial-in Username.<br>"iname=admin" means to set username as "admin". |
| *ipwd* | It means Dial-in Password.<br>"ipwd=1234" means to set password as "1234". |
| *ivj* | It means VJ Compression.<br>"ivj=on/off" means to enable /disable VJ Compression. |
| *ikey* | It means IKE Pre-Shared Key.<br>"ikey=abcd" means to set IKE Pre-Shared Key = abcd. |
| *imeth* | It means IPSec Security Method<br>"imeth=h" means "Allow AH".<br>"imeth=d" means "Allow DES".<br>"imeth=3" means "Allow 3DES".<br>"imeth=a" means "Allow AES. |
| **For TCP/IP Settings** | |
| *mywip* | It means My WAN IP.<br>"mywip=1.2.3.4" means to set My WAN IP as "1.2.3.4". |

| | |
|---|---|
| *rgip* | It means Remote Gateway IP.<br>"rgip=1.2.3.4" means to set Remote Gateway IP as "1.2.3.4". |
| *rnip* | It means Remote Network IP.<br>"rnip=1.2.3.0" means to set Remote Network IP as "1.2.3.0". |
| *rnmask* | It means Remote Network Mask.<br>"rnmask=255.255.255.0" means to set Remote Network Mask as "255.255.255.0". |
| *rip* | It means RIP Direction.<br>"rip=d" means to set RIP Direction as "Disable".<br>"rip=t" means to set RIP Direction as "TX".<br>"rip=r" means to set RIP Direction as "RX".<br>"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".<br>"mode=r" means to set Route mode.<br>"mode=n" means to set NAT mode. |
| *droute* | It means to Change default route to this VPN tunnel ( Only single WAN supports this).<br>droute=on/off means to enable/disable the function. |

### Example

```
> vpn option 1 idle=250
% Change Log..

% Idle Timeout = 250
```

## Telnet Command: vpn mroute

This command allows users to list, add or delete static routes for a certain LAN to LAN VPN profile.

### Syntax

**vpn mroute** <*index*> **list**

**vpn mroute** <*index*> **add** <*network ip*>/<*mask*>

**vpn mroute** <*index*> **del** <*network ip*>/<*mask*>

### Syntax Description

| Parameter | Description |
|---|---|
| *list* | It means to display all of the route settings. |

| | |
|---|---|
| *add* | It means to add a new route. |
| *del* | It means to delete specified route. |
| <*index*> | It means the index number of the profile.<br>Available index numbers:<br>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.<br>Available index numbers:<br>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* VPN service.

### Syntax

**vpn remote** *[PPTP/IPSec/L2TP] [on/off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *PPTP/IPSec/L2TP* | There are four types to be selected. |
| *on/off* | on – enable VPN remote setting.<br>off – disable VPN remote setting. |

### Example

```
> vpn remote PPTP on
Set PPTP VPN Service : On

Please restart the router!!
```

## Telnet Command: vpn 2ndsubnet

This command allows users to enable second subnet IP as VPN server IP.

### Syntax

**vpn 2ndsubnet** *on*

**vpn 2ndsubnet** *off*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | It means to enable or disable second subnet. |

### Example

```
> vpn 2ndsubnet on
%Enable second subnet IP as VPN server IP!
```

## Telnet Command: vpn NetBios

This command allows users to enable or disable NetBios for Remote Access User Accounts or LAN-to-LAN Profile.

### Syntax

**vpn NetBios set** *<H2I/L2I> <index> <Block/Pass>*

### Syntax Description

| Parameter | Description |
|---|---|

| | |
|---|---|
| *<H2I/L2I>* | H2I means Remote Access User Accounts.<br>L2I means LAN-to-LAN Profile.<br>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.<br>**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.<br>1 – PPTP<br>2 – L2TP<br>3 – IPSec<br>4 – L2TP over IPSec |
| *<TCP maximum segment size range>* | Each type has different segment size range.<br>PPTP – 1 ~ 1412<br>L2TP – 1 ~ 1408 |

| | |
|---|---|
| | IPSec – 1 ~ 1381<br>L2TP over IPSec – 1 ~ 1361 |

### 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).<br>L2I means LAN-to-LAN Profile. |
| *<index>* | The index number of the profile. |
| *<Block/Pass>* | Set Block/Pass the Multicast Packets.<br>The default is Block. |

### Example

```
> vpn Multicast set L2l 1 Pass
% Lan to Lan Profile Index [1] :
% Status Block/Pass: [PASS]
```

## Telnet Command: vpn pass2nd

This command allows users to determine if the packets coming from the second subnet passing through current used VPN tunnel.

### Syntax

**vpn pass2nd***[on]*

**vpn pass2nd** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | on – the packets can pass through NAT.<br>off – the packets cannot pass through NAT. |

### Example

```
> vpn pass2nd on
% 2nd subnet is allowed to pass VPN tunnel!
```

## Telnet Command: vpn pass2nat

This command allows users to determine if the packets passing through by NAT or not when the VPN tunnel disconnects.

### Syntax

**vpn pass2nat** *[on]*

**vpn pass2nat** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | on – the packets can pass through NAT.<br>off – the packets cannot pass through NAT. |

### Example

```
> vpn pass2nat on
% Packets would go through by NAT when VPN disconnect!!
```

## 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.<br>For Static IP/DHCP, the maximum number will be 1500.<br>For PPPoE, the maximum number will be 1492.<br>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 DF_check

This command allows you to enable or disable the function of DF (Don't fragment)

### Syntax

**wan DF_check** *[on]*

**wan DF_check** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | It means to enable or disable DF. |

### Example

```
> wan DF_check on
%DF bit check enable!
> wan DF_check off
%DF bit check disable (reset DF bit)!
```

## Telnet Command: wan disable

This command allows you to disable WAN connection.

### Example

```
> wan disable WAN
%WAN disabled.
```

## Telnet Command: wan enable

This command allows you to disable wan connection.

### Example

```
> wan enable WAN

%WAN1 enabled.
```

## Telnet Command: wan forward

This command allows you to enable or disable the function of WAN forwarding. The packets are allowed to be transmitted between different WANs.

### Syntax

**wan forward** *[on]*

**wan forward** *[off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *on/off* | It means to enable or disable WAN forward. |

### Example

```
> wan forward ?

%WAN forwarding is Disable!


> wan forward on

%WAN forwarding is enable!
```

## Telnet Command: wan status

This command allows you to display the status of WAN connection, including connection mode, TX/RX packets, DNS settings and IP address.

### Example

```
> wan status

WAN1: Offline, stall=N

 Mode: ---, Up Time=00:00:00

 IP=---, GW IP=---

 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0

 Primary DNS=0.0.0.0, Secondary DNS=0.0.0.0


PVC_WAN3: Offline, stall=N

 Mode: ---, Up Time=00:00:00

 IP=---, GW IP=---

 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0


PVC_WAN4: Offline, stall=N

 Mode: ---, Up Time=00:00:00
```

```
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0


PVC_WAN5: Offline, stall=N
 Mode: ---, Up Time=00:00:00
 IP=---, GW IP=---
 TX Packets=0, TX Rate(Bps)=0, RX Packets=0, RX Rate(Bps)=0
```

## 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.<br>"0":disable |
| *paponly* | It means PAP Only. Set the PPP authentication of the USB WAN.<br>on: None.<br>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.<br>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 lte

This command allows you to configure LTE WAN (for L model only).

### Syntax

**wan lte auth** *[0/1]*

**wan lte band**

**wan lte del** *[index #/all]*

**wan lte pass** *[string]*

**wan lte quota** *[-<command><parameter>|...]*

**wan lte read** *[index #/all]*

**wan lte reboot** *[-<command><parameter>|...]*

**wan lte reply** *[-<command><parameter>|...]*

**wan lte send** *[number][message]*

**wan lte stus**

**wan lte tag** *[index #/all]*

**wan lte user** *[string]*

**wan lte wms** *[send[cdma/gwpp]/recv[cdma/gwgw]/setting]*

### Syntax Description

| Parameter | Description |
|---|---|
| *auth [0/1]* | Set PPP authentication of LTE WAN.<br>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* | Set the password of LTE WAN. |
| *quota [-<command><parameter>|...]* | Set settings of SMS Quota Limit function.<br>Available commands with parameter are listed below:<br>[...] means that you can Enter several commands in one line.<br>-a <0/1>: Set whether to send an e-mail alert when SMS quota exceeded. (0: no 1: yes)<br>-c <cycle>: Set the order of today in refresh cycle.<br>-d <day>: Set the refresh day.<br>-e <0/1>: Enable or disable SMS Quota Limit function. (0: disable 1: enable)<br>-h <hour>: Set the refresh hour.<br>-m <0/1/2>: Set SMS quota refresh mode. (0: None 1: monthly 2: periodically)<br>-n <number>: Set SMS quota. The avaible number is between 1 and 1000000.<br>-s <0/1>: Set whether to stop sending SMS after SMS quota exceeded. (0: no 1: yes) |
| *read* | 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.<br><command> <parameter> | ...<br>The available commands with parameters are listed below.<br>[...] means that you can Enter several commands in one line.<br>-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)<br>-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)<br>-p <password>: Set the Password / PIN. This setting is necessary if this function is enabled.<br>-x <number>: Set the first phone number in Access Control List.<br>-y <number>: Set the second phone number in Access Control List.<br>-z <number>: Set the third phone number in Access Control List. |
| *reply* | Set settings of Reply with Router Status Message function. |

| | |
|---|---|
| | <command> <parameter> \| ...<br>The available commands with parameters are listed below.<br>[...] means that you can Enter several commands in one line.<br>-a <0/1>: Enable or disable Access Control List. (0: disable 1: enable)<br>-c <0/1>: Set whether to reply with MAC address. (0: no 1: yes)<br>-e <0/1>: Enable or disable Reboot on SMS Message function. (0: disable 1: enable)<br>-f <0/1>: Set whether to reply with WAN1 IP address. (0: no 1: yes)<br>-g <0/1>: Set whether to reply with WAN2 IP address. (0: no 1: yes)<br>-h <0/1>: Set whether to reply with LTE WAN IP address. (0: no 1: yes)<br>-i <0/1>: Set whether to reply with WAN4 IP address. (0: no 1: yes)<br>-j <0/1>: Set whether to reply with WAN1 data usage. (0: no 1: yes)<br>-k <0/1>: Set whether to reply with WAN2 data usage. (0: no 1: yes)<br>-l <0/1>: Set whether to reply with LTE WAN data usage. (0: no 1: yes)<br>-m <0/1>: Set whether to reply with WAN4 data usage. (0: no 1: yes)<br>-n <0/1>: Set whether to reply with Router name. (0: no 1: yes)<br>-p <password>: Set the Password / PIN. This setting is necessary if this function is enabled.<br>-u <0/1>: Set whether to reply with Router system uptime. (0: no 1: yes)<br>-v <0/1>: Set whether to reply with Router firmware version. (0: no 1: yes)<br>-x <number>: Set the first phone number in Access Control List.<br>-y <number>: Set the second phone number in Access Control List.<br>-z <number>: Set the third phone number in Access Control List. |
| *send* | Send an SMS message to the specified phone number through the LTE SIM card. |
| *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/wan3/wan4][on/off/always_on]*

**wan detect** *[wan1/wan2/wan3/wan4]* **target** *[ip addr]*

**wan detect** *[wan1/wan2/wan3/wan4]* **target2***[ip addr]*

**wan detect** *[wan1/wan2/wan3/wan4]* **target_gw** *[1/0]*

**wan detect** *[wan1/wan2/wan3/wan4]* **ttl** *[value]*

**wan detect** *[wan1/wan2/wan3/wan4]* **interval** *[interval]*

**wan detect** *[wan1/wan2/wan3/wan4]* **retry** *[retry]*

**wan detect status**

### Syntax Description

| Parameter | Description |
|---|---|
| *on* | Enable ping detection. The IP address of the target shall be set. |
| *off* | Enable ARP detection (default). |
| *always_on* | Disable link detect, always connected(only support static IP) |

| | |
|---|---|
| *target* | Set the ping target. |
| *Target2* | Set the secondary ping target. |
| *Target_gw* | Set whether to use gateway as ping target. (1: yes 0: no)<br>Note that USB WAN (PPP mode) cannot support PING gateway |
| *ip addr* | It means the IP address used for detection. Type an IP address in this field. |
| *ttl* | It means to set the ping TTL value (work as trace route)<br>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.<br>*[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.<br>[retry] : Type a number. |
| *status* | It means to show the current status. |

## Example

```
> wan detect status
 WAN1: always on
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
> wan detect wan1 target 192.168.1.78
 Set OK

> wan detect wan1 on
 Set OK

> wan detect status
 WAN1: on, Target=192.168.1.78, TTL=255
 WAN2: off
 WAN3: off
 WAN4: off
 WAN5: off
>
```

## Telnet Command: wan lb

This command allows you to Enable/Disable for each WAN to join auto load balance member.

### Syntax

**wan lb** *[wan1/wan2/...] on*

**wan lb** *[wan1/wan2/...] off*

**wan lb 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
 WAN6: on
 WAN7: on
```

## Telnet Command: wan mvlan

This command allows you to configure multi-VLAN for WAN and LAN. It supports pure bridge mode (modem mode) between Ethernet WAN and LAN port 2~4.

### Syntax

**wan mvlan** *[pvc_no/status/save/enable/disable] [on/off/clear/tag tag_no] [service type/vlan priority] [px ... ]*

**wan mvlan** *keeptag[pvc_no][on/off]*

### Syntax Description

| Parameter | Description |
|---|---|
| *pvc_no* | It means index number of PVC. There are 10 PVC, 0(Channel-1) to 9(Channel-9) allowed to be configured.<br>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.<br>-1: No need to add tag number.<br>1-4095: Available setting numbers used as tagged number. |
| *service type* | It means to specify the service type for VLAN.<br>0: Normal.<br>1: IGMP. |
| *vlan priority* | It means to specify the priority for the VALN setting.<br>Range is from 0 to 7. |
| *px* | It means LAN port. Available setting number is from 2 to 4. Port number 1 is locked for NAT usage. |
| *keeptag* | It means Multi-VLAN packets will keep their VLAN headers to LAN. |

### Example

PVC 7 will map to LAN port 2/3/4 in bridge mode; service type is Normal. No tag added.

```
> > wan mvlan 7 on p2 p3 p4
PVC  Bridge  p1 p2 p3 p4 p5 p6   Service Type    Tag    Priority    Keep Tag
 ---------------------------------------------------------------------
   7  ON     0  0  1  1  0  0     Normal      0(OFF)     0       OFF
>
```

## Telnet Command: wan multifno

This command allows you to specify a channel (in Multi-PVC/VLAN) to make bridge connection to a specified WAN interface.

### Syntax

**wan multifno** *[channel #] [WAN interface #]*

**wan multifno** *status*

### Syntax Description

| Parameter | Description |
|---|---|
| *channel #* | There are 4 (?) channels including VLAN and PVC.<br>Available settings are:<br>1=Channel 1<br>3=Channel 3 |

| | |
|---|---|
| | 4=Channel 4<br>5=Channel 5 |
| *WAN interface #* | Type a number to indicate the WAN interface.<br>*1=WAN1*<br>*2=WAN2* |
| *status* | It means to display current bridge status. |

### Example

```
> wan multifno 5 1
% Configured channel 5 uplink to WAN1
> wan multifno status
% Channel 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 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.<br>Disable: Disable the function of tagging on WAN interface. |
| *stat* | Display current VLAN status. |

### Example

```
> wan vlan stat
> wan vlan stat
% Interface    Pri     Tag    Enabled
% ======================================
% WAN1         0       0
```

```
% WAN2          0       0
% WAN3          0       0
% WAN4          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** *[#]* **action** *[action bitmap]*

**wan budget status**

### Syntax Description

| Parameter | Description |
|---|---|
| *wan[#]* | Specify the WAN interface. |
| *rdate* | Specify the WAN budget refresh time.<br>day – Available settings are from 1 to 30.<br>hour – Available settings are from 1 to 23.<br>E.g., `wan budget wan 1 rdate 5 10`<br>If monthy mode is selected: WAN budget will be refreshed on 5th day at 10:00 in each month<br>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.<br>disable - Disable the function of wan budget. |
| *thres [budget limit (MB)]* | Specify the maximum value for WAN budget limit. (Unit: MB)<br>budget limit – Type a number. |
| *gthres [budget limit (GB)]* | Specify the maximum value of wan budget limit. (Unit: GB)<br>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.<br>E.g., `wan budget wan 5 psday` → It means "today" is the 5th day in the billing cycle. |

| | |
|---|---|
| *action [action bitmap]* | Determine the action to be performed when it reaches the WAN budget limit.<br>*action bitmap* – Type a total number of actions to be executed. Different numbers represent different actions.<br>1: shotdown wan<br>2: send mail alert<br>4: send sms alert<br>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 -w** *[number]* **-i** *[Host/IP address]* **-s** *[base_size]* **-d** *[decrease_size] (-c [count])*

### Syntax Description

| Parameter | Description |
|---|---|
| *-w [number]* | Specify the WAN interface.<br>Value: Enter the number of WAN interface. 1: WAN1; 2:WAN2….and etc. |
| *-I [Host/IP address]* | Specify the IPv4 target to detect. If can be an IPv4 address or domain name.<br>Host/IP address: Enter the IP address/domain name of the target. |
| *-s [base_size]* | Set the MTU size base for Discovery.<br>base_size: Available setting is 1000 ~ 1500. |
| *-d [decrease size]* | Set the MTU size to decrease between detections.<br>decrease size: Available setting is 1 ~ 100. |
| *-c [count]* | Set the maximum times of ping failure during a Discovery.<br>count: Available settings are 1 ~ 10. Default value is 3. |

### Example

```
> wan detect_mtu -w 2 -i 8.8.8.8 -s 1500 -d 30 -c 10
 detecting  mtu size:1500!!!

 mtu size:1470!!!
```

## Telnet Command: wan detect_mtu6

This command allows you to run a WAN MTU Discovery. The user can specify an IPv6 target to ping and find the suitable MTU size of the WAN interface.

### Syntax

**wan detect_mtu6 -w** *[number]* **-i** *[IPv6 address]* **-s** *[base_size]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-w [number]* | Specify the WAN interface<br>number: Enter the number of WAN interface. 1: WAN1;<br>2:WAN2….and etc. |
| *-I [IPv6 address]* | Specify the IPv6 target to detect. It must be an IPv6 IP address.<br>IPv6 address: Enter the IPv6 address of the target. |
| *-s [base_size]* | Specify the size of MTU.<br>base_size: Available setting is 1000 ~ 1500. |

### Example

```
> wan detect_mtu6 -w 2 -i 2404:6800:4008:c06::5e -s 1500
>
```

## Telnet Command: hsportal

This command is used to configure a profile (Hotspot Web Portal) with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router.

### Syntax

**hsportal setup -p** <*profile*> *[-I <lan>] [-s <ssid>] …*

**hsportal setup -p** <*profile*> *-c*

### Syntax Description

| Parameter | Description |
|---|---|
| *-p* | Indicate available profile to be configured.<br>Number of profile: 1 /2 /3 / 4. |
| *-I* | Apply to LAN interfaces. E.g., apply LAN1 and LAN2:<br>-I 1, 2. |
| *-s* | Apply to WLAN interfaces. E.g., apply SSID1 and SSID2:<br>-s 1, 2. |
| *-a* | Apply to WLAN5G interfaces. E.g., apply SSID1 and SSID2:<br>-s 1, 2. |
| *-m* | Select login mode. |

| | |
|---|---|
| | 0:skip<br>1:click<br>2:social<br>3:pin<br>4:social or pin |
| *-f* | Configure facebook login.<br>0: disable.<br>1: enable. |
| *-g* | Configure google login.<br>0: disable.<br>1: enable. |
| *-h* | Enable HTTPS redirection.<br>0: disable.<br>1: enable. |
| *-v* | Enable portal detection.<br>0: disable.<br>1: enable. |
| *-i* | Configure APP id.<br>For example, to configure facebook APP id, you can type:<br>>hsportal -p 1 -f -i this_is_app_id<br>Profile 1 set facebook login disabled … [OK] |
| *-k* | Configure app key.<br>For example, to configure google APP key, you can type:<br>> hsportal -p 1 -g -i this_is_app_key<br>Profile 1 set google login disabled … [OK] |
| *-r* | Configure landing page mode.<br>0: fixed URL.<br>1: user request.<br>2: bulletin.<br>E.g.<br>> hsportal -p 1 -r 0<br>Profile 1 set landing page mode 0 … [OK] |
| *-e* | Enable the specified profile. |
| *-d* | Disable the specified profile. |
| *-c* | Reset the specified profile.<br>Number of profile: 1 /2 /3 / 4. |

| | |
|---|---|
| *-o* | Clear profiles for all clients. |

### Example

```
> hsportal setup -p 1 -c
Reset profile 1 ... [OK]
> hsportal setup -p 1 -r 0
Profile 1 set landing page mode 0 ... [OK]
> hsportal setup -p 2 -g 1 -k app_key_google
Profile 2 set google login enabled ... [OK]
Profile 2 set API KEY   ... [OK]
>
```

## Telnet Command: 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.<br>[MAC] format: xx-xx-xx-xx-xx-xx<br>or xx:xx:xx:xx:xx:xx<br>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* | It means to set white/black list for each SSID. |

| | |
|---|---|
| *ssid4] [white/black]* | |
| *wl acl show* | It means to show access control status. |
| *wl acl showmode* | It means to show the mode for each SSID. |
| *wl acl clean* | It means to clean all access control setting. |

### Example

```
> > wl acl showmode
 ssid1: none
 ssid2: none
 ssid3: none
 ssid4: none
> wl acl add 00-50-70-ff-12-70
 Set Done !!
> 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
   0                  00:50:70:ff:12:70   ssid1 ssid2 ssid3 ssid4
   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 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]*

## Syntax Description

| Parameter | Description |
|---|---|
| *mode[value]* | It means to select connection mode for wireless connection.<br>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.<br>The available settings are 0,1,2,3,4,5,6,7,8,9,10,11,12 and 13.<br>number=0, means Auto<br>number=1, means Channel 1<br>….<br>number=13, means Channel 13. |
| *preamble [enable]* | It means to define the length of the sync field in an 802.11 packet.<br>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.<br>0: disable to use long preamble.<br>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.<br>0: disable the function.<br>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.<br>*ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*ssid_name*: Give a name for the specified SSID.<br>*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.<br>*SSID_NUMBER*: Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*mode*: Available settings are:<br>disable: No security.<br>wpa1x: WPA/802.1x Only<br>wpa21x: WPA2/802.1x Only<br>wpamix1x: Mixed (WPA+WPA2/802.1x only)<br>wep1x: WEP/802.1x Only |

| | |
|---|---|
| | wpapsk: WPA/PSK<br>wpa2psk: WPA2/PSK<br>wpamixpsk: Mixed (WPA+WPA2)/PSK<br>wep: WEP<br>*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.<br>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.<br>*ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable.<br>*upload*: It means to configure the rate control for data upload. The unit is kbps.<br>*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.<br>*lan* – It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.<br>*member* – It can make the wireless clients (stations) with the same SSID not accessing for each other. |

## Example

```
> wl config mode 11bgn
 Current mode is 11bgn
% <Note> Please restart wireless after you set the channel
> wl config channel 13
 Current channel is 13
% <Note> Please restart wireless after you set the channel.
> wl config preamble 1
 Long preamble is enabled
% <Note> Please restart wireless after you set the parameters.
> wl config ssid 1 enable dray
 SSID  Enable  Hide_SSID  Name
 1     1       0         dray
% <Note> Please restart wireless after you set the parameters.
> wl config security 1 wpa1x
%% Configured Wlan Security Setting:
```

```
% SSID1
%%  Mode: wpa1x
%% Wireless card must be reset for configurations to take effect
%% (Telnet Command: wl restart)
```

## Telnet Command: wl set

This command allows users to configure basic wireless settings.

### Syntax

**wl set** *[SSID] [CHAN[En]]*

**wl set txburst** *[enable]*

### Syntax Description

| Parameter | Description |
|---|---|
| *SSID* | It means to Enter the SSID for the router. The maximum character that you can use is 32. |
| *CHAN[En]* | It means to specify required channel for the router.<br>*CHAN:* The range for the number is between 1 ~ 13.<br>*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.<br>0: disable the function.<br>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.<br>0: diable<br>1: enable |

### Example

```
> wl act on
% Set Wlan to Enable.
```

## Telnet Command: wl scan

This command allows users to perform AP scanning.

### Syntax

**wl scan** *[start]*

**wl scan** *set [wlist/blist/stime][MAC]*

**wl scan** *del [wlist/blist] [MAC]*

**wl scan** *filter [ssid/channel/mac]*

**wl scan** *show [0/1/2/3]*

### Syntax Description

| Parameter | Description |
|---|---|
| *start* | It means to start AP scanning. |
| *set [wlist/blist/stime] [MAC]* | Set white list/block list/scan time.<br>*wlist* – It means to set white list for passing. MAC address must be added in the end.<br>e.g., *wl scan set wlist 001122aabbcc*<br>*blist* – It means to set black list for blocking. MAC address must be added in the end.<br>*stime* – It means to set scanning time. Time value (2~5 second) must be added in the end.<br>e.g., *wl scan set time 5* |
| *del* | Remove white list/block list.<br>e.g., *wl scan del wlist 001122aabbcc* |
| *filter* | Set which filter you want.<br>*ssid* – scanning the AP based on SSID setting.<br>*channel* - scanning the AP based on channel setting.<br>*mac* - scanning the AP based on MAC address setting.. |
| *show [0/1/2/3]* | It is used to show AP list.<br>0 - display white list<br>1 - display block list, |

| | |
|---|---|
| | 2 - display gray/unknown list,<br>3 - display all list |

### Example

```
> wl scan set wlist 001122aabbcc
> wl scan start
> wl scan show 3
>
```

## 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.<br>Available channel for 2.4G: 0/1/2/3<br>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.<br>1: SSID1<br>2: SSID2<br>3: SSID3<br>4: SSID4 |
| *En* | It means to enable or disable the function of VPN isolation.<br>0: disable<br>1: enable |

### Example

```
> wl iso_vpn 1 on
% ssid: 1 isolate vpn on :1
```

## Telnet Command: wl wpa

This command allows you to configure WPA wireless settings.

### Syntax

**wl wpa** *1/2/3*

### Syntax Description

| Parameter | Description |
|---|---|
| *wl wpa* | Type 1/2/3 to represent different WPA modes.<br>1 – means WPA+WPA2<br>2 – means WPA2 Only<br>3 – means WPA Only |

### Example

```
> wl wpa 1
>
```

## Telnet Command: wl wmm

This command allows users to set WMM for wireless connection. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs).

### Syntax

**wl wmm ap** *QueIdx Aifsn Cwmin Cwmax Txop ACM*

**wl wmm bss** *QueIdx Aifsn Cwmin Cwmax Txop ACM*

**wl wmm ack** *Que0_Ack Que1_Ack Que2_Ack Que3_Ack*

**wl wmm enable** *SSID0 SSID1 SSID2 SSID3*

**wl wmm apsd** *value*

**wl wmm show**

## Syntax Description

| Parameter | Description |
|---|---|
| *ap* | It means to set WMM for access point. |
| *bss* | It means to set WMM for wireless clients. |
| *ack* | It means to map to the Ack policy settings of AP WMM. |
| *enable* | It means to enable the WMM for each SSID.<br>0: disable<br>1: enable |
| *Apsd [value]* | It means to enable / disable the ASPD(automatic power-save delivery) function.<br>0: disable<br>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.<br>0: disable<br>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.<br>0: 2T3R<br>1: 2T2R<br>2: 1T2R<br>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.<br>[value]: Available settings are :<br>d: Disable<br>b: Bridge<br>r: Repeapter |
| *security [value]* | It means to configure security mode with encrypted keys for WDS.<br>*mode*: Available settings are:<br>disable: No security.<br>wep: WEP<br>wpapsk [key]: WPA/PSK<br>wpa2psk [key]: WPA2/PSK<br>*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.<br>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.<br>e.g., |

| | |
|---|---|
| | *wl dual wds security disable*<br>*wl dual wds security wep 12345*<br>*wl dual wds security wpa2psk 12345678* |
| *ap [value]* | It means to enable or disable the AP function.<br>Value: 1 – enable the function.<br>0 – disable the function. |
| *hello [value]* | It means to send hello message to remote end (peer).<br>Value: 1 – enable the function.<br>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,<br>*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.<br>1 – enable<br>0 – disable |
| *security [mode]* | There are several modes to be selected:<br>Disable – disable the security settings.<br>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.<br>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.<br>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.<br>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.<br>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* | 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<br>1: enable |

### Example

```
> wl btnctl 1
Enable wireless botton control
Current wireless botton control is on
>
```

## Telnet Command: wl iwpriv

This command is reserved for RD debug. Do not use them.

## Telnet Command: wl stalist

This command is used to display the wireless station which accessing Internet via Vigor router.

### Syntax

**wl stalist**

### 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 set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication.

### Syntax

**wl set8021x -t** *[0/1]*

**wl set8021x -v**

### Syntax Description

| Parameter | Description |
|---|---|
| *-t* | Specify the type (external or internal) of wireless authentication server.<br>0 – Indicate the external RADIUS server.<br>1- Indicate the local 802.1x server. |
| *-v* | View the settings of 802.1x. |

### Example

```
> wl set8021x -t 1
% <Note> Please restart wireless after you set the parameters.
> wl set8021x -v
 802.1X type is : Local 802.1X
>
```

## 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.<br>1 – enable<br>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.<br>*[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.<br>1 – enable<br>0 – disable |
| *Trg_num [value]* | Set a threshold when the active station number achieves this number, the airtime fairness function will be applied.<br>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.<br>0 - disable<br>1 - Strictly Minimum RSSI<br>2 - Minimum RSSI<br>rs_low – Set a value of Strictly Minimum RSSI (62~86).<br>rs_low_security – Set a value of Minimum RSSI (62~86).<br>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.<br>[MAC] format: xx-xx-xx-xx-xx-xx<br>or xx:xx:xx:xx:xx:xx<br>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<br>or xx:xx:xx:xx:xx:xx<br>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
> wl_acl add 00-50-70-ff-12-80 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
   0       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 cardmac

### Example

```
> wl_dual cardmac
Card MAC: 54:2a:a2:37:00:ef
```

## 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**

### Syntax Description

| Parameter | Description |
|---|---|
| *enable[value]* | It means to enable/disable the 5GHz wireless function.<br>1: enable<br>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.<br>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.<br>The available settings are: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 and 140.<br>number=0, means Auto |

| | |
|---|---|
| | number=36, means Channel 36<br>….<br>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.<br>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.<br>0: disable to use long preamble.<br>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.<br>*ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*ssid_name*: Give a name for the specified SSID. |
| *ssid hide [ssid_num enab le]* | It means to hide the name of the SSID if required.<br>*ssid_num:* Type 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>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.<br>*ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*enable*: It means to enable the function of the rate control for the specified SSID. 0: disable and 1:enable.<br>*upload*: It means to configure the rate control for data upload. The unit is kbps.<br>*download*: It means to configure the rate control for data download. The unit is kbps.<br>(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.<br>It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.<br>*ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*enable*: It means to enable such function.<br>0: disable and 1:enable |
| *isolate member [ssid_num enable]* | It means to isolate the wireless connection from Member.<br>It can make the wireless clients (stations) with the same SSID not |

| | |
|---|---|
| | accessing for each other.<br>*ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*enable*: It means to enable such function.<br>0: disable and 1:enable. |
| *isolate vpn [ssid_num enable]* | It means to isolate the wireless connection from VPN.<br>*ssid_num:* Choose 1, 2, 3 or 4 to specify SSID1, SSID2, SSID3 or SSID4.<br>*enable*: It means to enable such function.<br>0: disable and 1:enable. |
| *isolate show* | It means to display the status of wireless isolation. |

### 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.<br>*mode*: Available settings are:<br>disable: No security.<br>wpa1x: WPA/802.1x Only<br>wpa21x: WPA2/802.1x Only<br>wpamix1x: Mixed (WPA+WPA2/802.1x only)<br>wep1x: WEP/802.1x Only<br>wpapsk: WPA/PSK<br>wpa2psk: WPA2/PSK<br>wpamixpsk: Mixed (WPA+WPA2)/PSK<br>wep: WEP<br>*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.<br>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**

### Example

```
> wl_dual stalist
5G Wireless Station List :

Index  Status  IP Address      MAC Address       Associated with

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.
```

## Telnet Command: wl_dual wds

This command allows users to configure WDS for wireless connection (5GHz).

### Syntax

**wl_dual wds mode** *[value]*

**wl_dual wds security** *[value]*

**wl_dual wds ap** *[value]*

**wl_dual wds hello** *[value]*

**wl_dual wds status**

**wl_dual wds show**

**wl_dual wds mac add** *[index addr]*

**wl_dual wds mac clear/disable/enable** *[index/all]*

**wl_dual wds flush**

## Syntax Description

| Parameter | Description |
|---|---|
| **mode** *[value]* | It means to specify connection mode for WDS.<br>[value]: Available settings are :<br>d: Disable<br>b: Bridge<br>r: Repeapter |
| **security** *[value]* | It means to configure security mode with encrypted keys for WDS.<br>*mode*: Available settings are:<br>disable: No security.<br>wep: WEP<br>wpapsk [key]: WPA/PSK<br>wpa2psk [key]: WPA2/PSK<br>*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.<br>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.<br>e.g.,<br>*wl_dual wds security disable*<br>*wl_dual wds security wep 12345*<br>*wl_dual wds security wpa2psk 12345678* |
| **ap** *[value]* | It means to enable or disable the AP function.<br>Value: 1 – enable the function.<br>0 – disable the function. |
| **hello** *[value]* | It means to send hello message to remote end (peer).<br>Value: 1 – enable the function.<br>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,<br>*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 mode b
> wl dual wds security wep
>
> wl_dual wds show
5G Wireless WDS Setting

Mode : Bridge
Security : WEP
AP Function : Enable
Send Hello Function : Enable

Bridge :
Index  Enable  MAC Address
  1     0    00:00:00:00:00:00
  2     0    00:00:00:00:00:00
  3     0    00:00:00:00:00:00
  4     0    00:00:00:00:00:00

Repeater :
Index  Enable  MAC Address
  5     0    00:00:00:00:00:00
  6     0    00:00:00:00:00:00
  7     0    00:00:00:00:00:00
  8     0    00:00:00:00:00:00
```

```
> 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.<br>1 – enable<br>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.<br>[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 set8021x

This command allows you to configure the external or internal server used by Vigor router for wireless authentication (5GHz).

### Syntax

**wl_dual set8021x -t** *[0/1]*

**wWl_dual set8021x -v**

### Syntax Description

| Parameter | Description |
|---|---|
| *-t* | Specify the type (external or internal) of wireless authentication server. |

| | |
|---|---|
| | 0 – Indicate the external RADIUS server.<br>1- Indicate the local 802.1x server. |
| *-v* | View the settings of 802.1x. |

### Example

```
> wl_dual set8021x -t 1
% <Note> Please restart 5G wireless after you set the parameters.
> wl_dual set8021x -v
 802.1X type is : Local 802.1X
>
```

## 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.<br>1 – enable<br>0 – disable |
| *Security [mode]* | There are several modes to be selected:<br>Disable – disable the security settings.<br>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.<br>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.<br>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.<br>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.<br>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
Vigor> 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.<br>1 – enable<br>0 – disable |
| *Trg_num [value]* | Set a threshold when the active station number achieves this number, the airtime fairness function will be applied.<br>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] [rs_low_security] [delta]* | Select a mode for roaming.<br>0 - disable<br>1 - Strictly Minimum RSSI<br>2 - Minimum RSSI<br>rs_low – Set a value of Strictly Minimum RSSI (62~86).<br>rs_low_security – Set a value of Minimum RSSI (62~86).<br>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: radius

This command allows you to configure detailed settings for RADIUS server

### Syntax

**radius enable** *[0/1]*

**radius authport** *[port number]*

**radius set_auth_method** *[method idx]*

**radius client** *[add] [idx] -i [address] -m [mask] -p [prefix] -l [length] -s [secret]*

**radius client** *[del] [idx]*

**radius show**

**radius set_dot1x_phase1 -e** *[method_idx]*

**radius set_dot1x_phase1 -d** *[method_idx]*

**radius set_dot1x_phase2 -e** *[method_idx]*

**radius set_dot1x_phase2 -d** *[method_idx]*

### Syntax Description

| Parameter | Description |
|---|---|
| *enable[0/1]* | Enable (1) or disable (0) the RADIUS server. |
| *authport [port number]* | Configure the port number for authentication.<br>Port number: Available range is from 0 to 65535.<br>Default value is “1812”. |
| *set_auth_method [method idx]* | Specify which method will be used for authentication.<br>Method idx: “0” is “Only PAP”; “1” is “PAP/CHAP/MS-CHAP/MS-CHAPv2”. |
| *client add* | Specify a client to be authenticated by RADIUS server by typing required information as follows:<br>-i [address]: client IPv4 address(domain)<br>-m [mask]: client IPv4 mask<br>-p [prefix]: client IPv6 prefix<br>-l [length]: client IPv6 prefix length |

| | |
|---|---|
| | -s [secret]: shared secret<br>ex: radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123 |
| *client [del] [idx]* | *del* - Delete related settings for selected client.<br>*Idx* - Specify the index number of client profiles. |
| *show* | Display the status of RADIUS server. |
| *enable_dot1x [0/1]* | Enable (1) or disable (0) the 802.1X Authentication function of RADIUS Server. Default is disabled. |
| *set_dot1x_phase1 [method_idx]* | Set the phase1 method for 802.1X authentication of RADIUS server.<br>*method_idx* - Specify which method will be used.<br>At present, dot1x_phase1 can only support PEAP now. So only "1" can be used for it. |
| *set_dot1x_phase2 [method_idx]* | Set the phase2 method for 802.1X authentication of RADIUS server.<br>*method_idx* - Specify which method will be used.<br>Dot1x_phase2 can only support MS-CHAPv2 now. So only "1" can be used for it. |
| *-e* | Set method for dot1x_phase1 or dot1x_phase2. |
| *-d* | Delete method for dot1x_phase1 or dot1x_phase2. |

### Example

```
> radius client add 1 -i 192.168.1.1 -m 255.255.255.0 -s 123
 This setting will take effect after rebooting.
 Please use "sys reboot" command to reboot the router.
```

## Telnet Command: local_8021x

The command is used to configure general settings for Local 802.1X server built in Vigor router.

### Syntax

**local_8021x enable** *[0/1]*

**local_8021x set_localdot1x_phase1 options…**

**local_8021x set_localdot1x_phase2 options…**

**local_8021x show**

### Syntax Description

| Parameter | Description |
|---|---|
| *enable* | Enable or disable the configuration.<br>0: disable.<br>1: enable. |
| set_localdot1x_phase1 | Only support PEAP now. The method_idx for such phase1 is "1". |

| | |
|---|---|
| set_localdot1x_phase2 | Only support MS-CHAPv2 now. The method_idx for such phase2 is "1". |
| options | -e [method_idx]: set method.<br>e.g, local_8021x set_localdot1x_phase1 -e 1<br>-d: delete mehod.<br>e.g, local_8021x set_localdot1x_phase1 -d |
| show | Display current settings of local 802.1x server. |

### Example

```
> local_8021x show
% Local 802.1X enable: enable
% phase1 support method: [PEAP]
% phase2 support method: [None]
```

## 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.<br>on: enable<br>off: disable<br>any: It means any source IP address can pass through NAT and wake up the LAN client.<br>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.<br>*ip address* - It means the WAN IP address.<br>*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

**sser set** *[-e|-d|-c|-l|-o|-a|-r|-b]*

**user edit** *[PROFILE_IDX] [-e|-d|-n|-p|-t|-u|-i|-q|-r|-w|-s|-m|-x|-v]*

**user account** *[USER_NAME] [-t|-d|-q|-r|-w]*

### Syntax Description

| Parameter | Description |
|---|---|
| *set* | It means to configure general setup for the user management. |
| *edit* | It means to modify the selected user profile. |
| *account* | It means to set time and data quota for specified user account. |
| *User Set* | |
| *-e* | Enable User management function. |
| *-d* | Disable User management function. |
| *-a[Profile idx][User name][IP_Address]* | It means to pass an IP Address.<br>*Profile idx*- Enter the index number of the selected profile.<br>*User name*- Enter the user name that you want it to pass.<br>*IP_Address*- Enter the IP address that you want it to pass. |
| *-l all*<br>*-l userl*<br>*-l ip* | Show online user.<br>*all* – all of the users will be displayed on the screen.<br>*user name* – Enter the user name that you want to view on the screen.<br>*ip* – Enter the IP address that you want to view on the screen. |
| *-o* | It means to show user account information.<br>e.g.,*-o* |
| *-c[user name]*<br>*-c all* | Clear the user record.<br>*user name* – Enter the user name that you want to get clear corresponding record.<br>*all* – all of the records will be removed. |
| *-buser [user name]*<br>*-b ip [ ip address]* | Block specifies user or IP address.<br>*user name* – Enter the user name that you want to block.<br>*ip address* — Enter the IP address that you want to block. |
| *-u user [user name]*<br>*-u ip [ ip address]* | Unblock specifies user or IP address.<br>*user name* – Enter the user name that you want to unblock.<br>*ip address* — Enter the IP address that you want to unblock. |

| | |
|---|---|
| *-r [user name \| all]* | Remove the user record.<br>*user name* – Enter the name of the user profile.<br>*all* – all of the user profile settings will be removed. |
| *-q* | It means to trigger the alert tool to do authentication. |
| *-s* | It means to set login service.<br>0:HTTPS<br>1:HTTP<br>e.g.,*-s 1* |
| *User edit* | |
| *PROFILE_IDX* | Enter the index number of the profile that you want to edit. |
| *-e* | Enable User profile function. |
| *-d* | Disable User profile function. |
| *-n* | It means to set a user name for a profile.<br>e.g.,*-n fortest* |
| *-p* | It means to configure user password.<br>e.g., *-p 60fortest* |
| *-t* | It means to enable /disable time quota limitation for user profile<br>0:Disable<br>1:Enable |
| *-u* | It means to enable /disable data quota limitation for user profile<br>0:Disable<br>1:Enable |
| *-i* | It means to set idle time.<br>e.g., *-i 60* |
| *-q* | set time quota<br>It means to set time quota of the user profile.<br>e.g., *-q 200* |
| *-r* | It means to set data quota.<br>e.g., *-r 1000* |
| *-w* | It means to specify the data quota unit (MB/GB).<br>e.g., -w MB |
| *-s* | It means to set schedule index. Available settings are" sch_idx1,sch_idx2,sch_idx3, and sch_idx4. |
| *-m* | It means to set the maximum login user number.<br>e.g., *-m 200* |

| | |
|---|---|
| *-x* | It means to set external server authentication<br>0: None<br>1: LDAP<br>2: Radius<br>3: TACAS<br>e.g., *-x 2* |
| *-v* | It means to view user profile(s). |
| *User account* | |
| *USER_NAME* | It means to type a name of the user account. |
| *-d* | It means to enable /disable data quota limitation for user account.<br>0:Disable<br>1:Enable |
| *-q* | It means to set account time quota.<br>e.g., *-q 200* |
| *-r* | It means to set account data quota.<br>e.g., *-r 1000* |
| *-t* | It means to enable /disable time quota limitation for user account.<br>0:Disable<br>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.<br>Use "appqos traceable –v" to display all of the traceable APS with speficed index number.<br>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.<br>Index number: 50, 51, 52, 53, 54, 58, 60, 62, 63, 64, 65, 66, 68 are used for 13 traceabel APPs.<br>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<br>1:Class 1, 2:Class 2, 3:Class 3, 4:Other Class |
| *-d* | It means to disable QoS for application(s). |

### Example

```
> appqos enable 1

APP QoS set to Enable.
> appqos traceable -e 68 2

TELNET: ENABLED, QoS Class 2.
```

## Telnet Command: nand bad /nand usage

"NAND usage" is used to display NAND Flash usage; "nand bad" is used to display NAND Flash bad blocks.

### Syntax

**nand bad**

**nand usage**

### Example

```
>nand usage
Show NAND Flash Usage:
Partition    Total          Used           Available      Use%
cfg          4194304        7920           4186384          0%
bin_web      33554432       11869493       21684939        35%
cfg-bak      4194304        7920           4186384          0%
```

```
bin_web-bak 33554432       11869493      21684939        35%
> nand bad
Show NAND Flash Bad Blocks:
Block   Address        Partition
1020    0x07f80000     unused
1021    0x07fa0000     unused
1022    0x07fc0000     unused
1023    0x07fe0000     unused
```

## Telnet Command: apm show /clear/discover/query

The apm command(s) is use to display, remove, discover or query the information of VigorAP registered to Vigor2927.

### Syntax

**apm show**

**apm clear**

**apm discover**

**apm query**

### Syntax Description

| Parameter | Description |
|---|---|
| *show* | It displays current information of APM profile. |
| *clear* | It is used to remove all of the APM profile. |
| *discover* | It is used to search VigorAP on LAN. |
| *query* | It is used to query any VigorAP which has been registered to APM (Central AP Management) in Vigor2927. Information related to the registered AP will be send back to Vigor2927 for updating the web page of Central AP Management. |

### Example

```
> apm clear ?
Clear all clients ... done
```

## Telnet Command: apm profile

This command allows to configure wireless profiles to be used in Central AP Management.

### Syntax

**apm profile clone** *[from index][to index][[new name]*

**apm profile del** *[index]*

**apm profile reset**

**apm profile summary**

**apm profile** *[show [profile index]]*

**apm profile** *apply [profile index] [client index1 [index2 .. index5]]*

## Syntax Description

| Parameter | Description |
|---|---|
| *clone* | It is used to copy the same parameters settings from one profile to another APM profile. |
| *del* | It is used to delete a specified APM profile. The default (index #1) should not be deleted. |
| *reset* | It is used to reset to factory settings for WLAN profile. |
| *summary* | It is used to list all of the APM profiles with required information. |
| *show* | It is used to display specified APM profile. |
| *apply* | It is used to apply the selected APM profile onto specified VigorAP. |
| *from index* | Type an index number in this field. It is the original APM profile to be cloned to other APM profile. |
| *to index* | Type an index number in this file. It is the target profile which will clone the parameters settings from an existed APM profile. |
| *new name* | Type a name for a new APM profile. |
| *profile index* | Enter the index number of existed profile. |
| *client index1/2/3/4/5* | It is useful for applying the selected APM profile to the specified VigorAP. |

## Example

```
> apm profile clone 1 2 forcarrie
(Done)

> apm profile summary
# Name           SSID           Security    ACL    RateCtrl(U/D)
- ---------------- ---------------- ------------ ------- ------
0 Default       DrayTek-LAN-A    WPA+WPA2/PSK x         - /    -
                DrayTek-LAN-B    WPA+WPA2/PSK x         - /    -

1 -             -              -          -               -
2 forcarrie       DrayTek         Disable     x         - /    -

3 -             -              -          -               -
4 -             -              -          -               -
```

## Telnet Command: apm cache

This command is used to display or remove the information of registered VigorAP, including MAC address, name, and authentication. Up to 30 entries of registered information can be stored and displayed.

### Syntax

**apm cache** *[show]*

**apm cache clear**

### Syntax Description

| Parameter | Description |
|---|---|
| *show* | It means to display the information related to VigorAP registered Vigor2927. |
| *clear* | It means to remove the information related to VigorAP registered Vigor2927. |

### Example

```
> apm cache show
MAC         Name               Auth
------------ -------------------- --------------------


>
```

## Telnet Command: apm lbcfg

This command allows to set parameters related to AP management control.

### Syntax

**apm lbcfg** *[set] [value]*

**apm lbcfg***[show]*

### Syntax Description

| Parameter | Description |
|---|---|
| *set* | It means to set the load balance configuration file for APM. |
| *Show* | It shows the configuration value. |
| *[value]* | You need to type 10 numbers in this field. Each number represents different setting value.<br>[1] – The first number means the load balance function. Type<br>1 – enable load balance,<br>0 – disable load balance.<br>[2] – The second number means the station limit function. Type<br>1 –enable station limit, |

| | |
|---|---|
| | 0 – disable station limit.<br>[3] – The third number means the traffic limit function. Type<br>1 – enable traffic limit,<br>0 – disable traffic limit.<br>[4] – The forth number means the limit num of station. Available range is 3~64.<br>[5] – The fifth number means the upload limit function. Type<br>1 – enable upload limit,<br>0 – disable upload limit.<br>[6] – The sixth number means the download limit function. Type<br>1 – enable download limit,<br>0 – disable download limit.<br>[7] – The seventh number means disassociation by idle time. Type<br>1 – enable disassociation,<br>0 – disable disassociation.<br>[8] – The eighth number means to enable or disable disassociation by signal strength. Type<br>1 – enable disassociation,<br>0 – disable disassociation.<br>[9] – The ninth number means to determine the unit of traffic limit (for upload)<br>1 – Mbps<br>0 – kbps<br>[10] – The tenth number means to determine the unit of traffic limit (for download)<br>1 – Mbps<br>0 – kbps |

## Example

```
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 0
2. Enable station limit : 0
3. Enable traffic limit : 0
4. limit Number : 64
5. Upload limit : 0
6. Download limit : 0
```

```
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 0
10.Traffic limit unit (download) : 0
flag : 0
> apm lbcfg set 1 1 0 15 0 0 0 0 1 1
> apm lbcfg show
apm LoadBalance Config :
1. Enable LoadBalance : 1
2. Enable station limit : 1
3. Enable traffic limit : 0
4. limit Number : 15
5. Upload limit : 0
6. Download limit : 0
7. Enable disassociation by idle time : 0
8. Enable disassociation by Signal strength : 0
9. Traffic limit unit (upload)   : 1
10.Traffic limit unit (download) : 1
flag : 49
```

## Telnet Command: apm napdetect

This command is used to enable/disable AP detection function.

### Syntax

**apm napdetect** *[get]*

**apm napdetect** *[set] [enable/disable AP Detection 1/0][Refresh Time].*

### Syntax Description

| Parameter | Description |
|---|---|
| *get* | It is used to get AP detection data from VigorAP (e.g., AP900). |
| *set* | It allows to set detect configuration to VigorAP. |
| *enable/disable AP Detection 1/0* | It is used to enable or disable the AP detection function.<br>0 – disable the function.<br>1 – enable the function. |
| *Refresh Time* | Available values are 1, 3 or 5 (minutes). |

### Example

**Note**: To check the scanning result of AP detection, use the command of "*wl scan show*".

```
> apm napdetect set 1 1
> wl scan show 3
```

```
Sta Ch SSID          BSSID           BssType  Security Siganl(%)  Beacon
Period First Detected  Last Detected
11 DrayTek-LAN-B    02:1d:aa:4c:bd:a8  AP     Mixed      26      100
11 DrayTek-LAN-A    00:1d:aa:4f:bd:a8  AP     Mixed      42      100
Dec 09,10:35:44 Dec 09,10:35:44
```

## Telnet Command: apm apsyslog

This command is used to display the AP syslog data coming form VigorAP.

### Syntax

**apm apsyslog** *[AP_Index]*

### Syntax Description

| Parameter | Description |
|---|---|
| *AP_Index* | Specify the index number which represents VigorAP. |

### Example

```
> apm apsyslog 1
8d 02:46:09  syslog: [APM] Send Rogue AP Detection data.
8d 02:53:04  syslog: [APM] Run AP Detection / Discovery.
8d 02:56:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:00:42  kernel: 60:fa:cd:55:f5:ea had disassociated.
8d 03:03:12  syslog: [APM] Run AP Detection / Discovery.
8d 03:06:09  syslog: [APM] Send Rogue AP Detection data.
8d 03:13:21  syslog: [APM] Run AP Detection / Discovery.
8d 03:16:10  syslog: [APM] Send Rogue AP Detection data.
8d 03:16:41  kernel: 60:fa:cd:55:f5:ea had associated successfully
8d 03:16:55  kernel: 60:fa:cd:55:f5:ea had disassociated.
```

## Telnet Command: apm syslog

This command is used to display related syslog data from central AP management.

### Syntax

**apm syslog**

### Example

```
> apm syslog
"2015-11-04 12:24:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP"
2015-11-04 12:24:56", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
2015-11-04 12:34:21", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
```

```
Data from AP"
2015-11-04 12:34:57", "[APM] [VigorAP900_01daa902080] Get Rogue AP Detection
Data from AP Success"
```

## Telnet Command: apm stanum

This command is used to display the total number of the wireless clients, no matter what mode of wireless connection (2.4G WLAN or 5G WLAN) used by wireless clients to access into Internet through VigorAP.

### Syntax

**apm stanum** *[AP_Index]*

### Syntax Description

| Parameter | Description |
|---|---|
| *AP_Index* | Specify the index number which represents VigorAP. |

### Example

```
> apm stanum

% Show the APM AP Station Number data.
% apm stanum AP_Index.
%     ex : apm stanum 1
%          Idx Nearby(2.4/5G) Conn(2.4/5G)
%           1   2   5          0   0
%           2   2   5          1   0
%           3   2   5          1   0
```

## Telnet Command: ha set

This command can be used to configure HA settings for Vigor routers.

### Syntax

**ha set** *[-<command> <parameter>| ... ]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command> <parameter>\|...]* | The available commands with parameters are listed below.<br>*[...]* means that you can Enter several parameters in one line. |
| *-e <1/0>* | 1: Enable the function of High Availability (HA).<br>0: Disable the function of High Availability (HA). |
| *-l <1/0>* | 1: Enable the function of recording the operation record of HA in Syslog.<br>0: Disable the function of recording the operation record of HA in Syslog. |

| | |
|---|---|
| *-M <1/0>* | Specify the Redundancy Method for HA.<br>1: Active-Standby<br>0: Hot-Standby |
| *-v <1-255>* | Specify the group ID (VHID)<br>1- 255: Setting range. |
| *-R* | Set HA settings to Factory Default. |
| *-p <1-30>* | Specify the Priority ID.<br>1-30: Setting range. |
| *-k <key>* | Specify the Authentication Key.<br>Key: Max. 31 Characters. |
| *-u <1/0>* | Enable or disable the function of Update DDNS.<br>1: Enable. When a router changes HA status to primary, it will update DDNS automatically.<br>0: Disable. |
| *-m <interface>* | Specify the management interface.<br>Interface: LAN1 ~ LAN6, DMZ. |
| *-s* | It means to get the newest status of other router (except the local router). |
| *-y* | It means sync local config to other router. Primary can executes this command. Secondary can not execute this commad. |
| *-c <1/0>* | Enable or disable the function of Config Sync.<br>1: Enable.<br>0: Disable. |
| *-I -[M\|H\|D] <interval>* | Set the Config Sync Interval for HA. Minimum interval is 15 minutes.<br>-M: Minute. Setting range is 0/15/30/45. (e.g., ha set -I -M 30)<br>-H: Hour. Setting range is from 0 to 23. (e.g., ha set -I -H 12)<br>-D: Day. Setting range is from 0 to 30. (e.g., ha set -I -D 15) |
| *-h -<4/6><Subnet> [<Virtual IP>]* | Enable and set virtual IP to the subnet.<br>4: IPv4; 6: IPv6.<br>Subnet: LAN1 to LAN6, DMZ.<br>Virtual IP*:* The type format shall be “xxx.xxx.xxx.xxx”. (e.g, 192.168.1.0)<br>For example, to enable a virtual IP to the sunet, simply type:<br>*ha set –h LAN1 192.168.1.5* |
| *-d -<4/6><Subnet>* | Disable a virtual IP to the subnet.<br>4: IPv4; 6: IPv6.<br>Subnet: LAN1 to LAN6, DMZ. |

| | |
|---|---|
| | For example, to disable a virtual IP to the subnet, just type:<br>*ha set –h LAN1* |
| *-o <1/0>* | Run DARP protocol on IPv4 or IPv6.<br>0: IPv4<br>1: IPv6 |

### Example

```
> > ha set -h -4 LAN1 192.168.1.1
% Enable IPv4 Virtual IP on LAN1
% Virtual IP can not be same as router IP (192.168.1.1)!!!
>
```

## Telnet Command: ha show

This command can be used to show the *settings information* about config sync and general setup.

### Syntax

**ha show –c**

**ha show –g**

### Syntax Description

| Parameter | Description |
|---|---|
| *-c* | Show the settings of config sync. |
| *-g* | Show the settings of general setup. |

### Example

```
> ha show -g
%  High Availability   : Disable
%  Redundancy Method   : Active-Standby
%  Group ID           : 1
%  Priority ID        : 10
%  Preempt Mode       : Enable
%  Update DDNS        : Disable
%  Management Interface : LAN1
%  Authentication Key  : draytek
%  Syslog             : OFF
%
%  [ Index | Enable | Virtual IP ]
%    LAN1   On      192.168.1.0
%    LAN2   -       0.0.0.0
%    LAN3   -       0.0.0.0
%    LAN4   -       0.0.0.0
%    LAN5   -       0.0.0.0
%    LAN6   -       0.0.0.0
%    DMZ    -       0.0.0.0
%  [ Index | Enable | Virtual IPv6 ]
```

```
%    LAN1    On     FE80::200:5EFF:FE00:101
%    LAN2    On     FE80::200:5EFF:FE00:101
%    LAN3    On     FE80::200:5EFF:FE00:101
%    LAN4    On     FE80::200:5EFF:FE00:101
%    LAN5    On     FE80::200:5EFF:FE00:101
%    LAN6    On     FE80::200:5EFF:FE00:101
%    DMZ     On    FE80::200:5EFF:FE00:101
>
```

## Telnet Command: ha status

This command is used to display *HA status information*.

### Syntax

**ha status -a** *[Detail Level]*

**ha status -m** *[Detail Level]*

### Syntax Description

| Parameter | Description |
|---|---|
| *-a* | Show the status for all of the routers in HA group. |
| *-m* | Show the status of local router only. |
| *Detail Level* | 0: Important status.<br>1: Important status, plus some information.<br>2: Show settings |

### Example

```
> ha status -m 2
%   [Local Router] DrayTek
%   IP               : 192.168.1.1 (FE80::21D:AAFF:FEC6:4C50)
%   Status           : !
%   High Availability   : ! Disable
%   Redundancy Method   : Active-Standby
%   Group ID          : 1
%   Priority ID       : 10
%   Update DDNS       : Disable
%   Protocol          : IPv4
%   Management Interface: LAN1
%   Authentication Key  : draytek
%   Virtual IP: (Max. 7 Virtual IPs)
%     ON       LAN1  192.168.1.0
%   Virtual IPv6: (Max. 7 Virtual IPv6s)
%     ON       LAN1  FE80::200:5EFF:FE00:101
%     ON       LAN2  FE80::200:5EFF:FE00:101
%     ON       LAN3  FE80::200:5EFF:FE00:101
%     ON       LAN4  FE80::200:5EFF:FE00:101
%     ON       LAN5  FE80::200:5EFF:FE00:101
%     ON       LAN6  FE80::200:5EFF:FE00:101
%     ON       DMZ   FE80::200:5EFF:FE00:101
%   Config Sync            : Disable
```

```
%   Config Sync Interval    : 0 Day 0 Hour 15 Minute
%   Cached Time        : 0 (s)

>
```

## Telnet Command: swm show

This command is used to display general setting of of VigorSwitch which connecting to Vigor router in LAN.

### Syntax

**swm show** *[LAN_port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *LAN_port* | Specify the LAN port number (1 to 6). |

### Example

```
> swm show

** If you connected a VigorSwitch but does not display here.
** Please check the LLDP is enabled and VLAN ID is matched on VigorSwitch.
********************************************************************************
LAN Port Model Name MAC IP Address Con Port
-------- ---------------- ------------ --------------- ---------
1 G1241 00507FF105FD 192.168.1.10 23
--------------------------------------------------------------------------------
Internal VLAN is [Enable]
Only show P1 related VLAN settings here.
VLAN Subn Tag VID Pri LAN WLAN(2.4G) WLAN(5G)
---- ---- --- ---- --- ------------------ ------------ ------------
0 LAN1 Off 0 0 P1,P2,P3,P4,P5,P6 none none
1 LAN1 On 20 0 P1,P2,P3,P4,P5,P6 none none
2 LAN1 On 100 0 P1,P2,P3,P4,P5,P6 none none
```

## Telnet Command: swm get

This command is used to **get** configuration information of VigorSwitch which connecting to Vigor router in LAN. Before using such command, make sure VigorSwitch has been managed under Vigor router (refer to Telnet Command: swm profile for adding a VigorSwitch device onto Vigor router).

### Syntax

**swm get** *[LAN_port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *LAN_port* | Specify the LAN port number (1 to 6). |

### Example

```
> swm get 1

Start get cfg from LAN (1) external switch
Please wait a few seconds...
Result: [OK].
>
```

## Telnet Command: swm post

This command is used to transfer switch configuration to VigorSwitch which connecting to Vigor router in LAN.

### Syntax

**swm post** *[LAN_port]*

### Syntax Description

| Parameter | Description |
|---|---|
| *LAN_port* | Specify the LAN port number (1 to 6). |

### Example

```
> swm post 1
Start post cfg to LAN (1) external switch with currect settings.
Please wait a few seconds...
Result: [OK]
>
```

## Telnet Command: swm auth

This command is used to display or remove the authentication record for external switch.

### Syntax

**swm auth** *[show/clear]*

### Syntax Description

| Parameter | Description |
|---|---|
| *show* | Display recorded external switch MAC address list. |
| *clear* | Clear specific index of authentication record table.<br>Index range: (1 - 30) |

### Example

```
> swm auth show
===== SWM Auth Records List=====
Index Model   Mac
----- ------- ------------
================================
> swm auth clear 1

 Clear index (1) swm auth record OK
```

## Telnet Command: swm extvlan

This command is used to configure port VLAN of VigorSwitch.

### Syntax

**swm extvlan** *[LAN_Port][VLAN_idx][Port_Description]*

### Syntax Description

| Parameter | Description |
|---|---|
| *LAN_Port* | Setting range is from 1 to 6. |
| *VLAN_idx* | Index number range for VLAN is from 0 to 7. |
| *Port_Description* | Setting range is from 1 to 24. |

### Example

```
> swm extvlan 1 1 13
Set OK.
> swm post 1
Start post cfg to LAN (1) external switch with currect settings.//post cfg
Please wait a few seconds...
Result: [OK].
```

System will cover the original VLAN settings on your VigorSwitch. Please backup the configuration file before you run this function.

System also will select the physical connect port as trunk port and let it join each VLAN group.

Before using such command, please use [swm show] to check valid VLAN index firstly.

## Telnet Command: backupmode

This command is used to backup the firmware to the router. The firmware will be retrieved for rebooting Vigor router after it crashes over three times.

### Syntax

**backupmode** *[<command><parameter>|…]*

### Syntax Description

| Parameter | Description |
|---|---|
| *[<command><parameter>|…]* | The available commands with parameters are listed below.<br>*[…]* means that you can Enter several commands in one line. |
| *-t n* | Set the backup time.<br>n : 1 ~ 168 hours |
| *-m n* | Set the firmware backup mode.<br>1: Backup after timeout.<br>0: Backup after upgrade. |
| *-b* | Backup the firmware manually and immediately. |

### Example

```
> backupmode -b
 Do Firmware backup now!!!.
```

# Index


## 3

3G/4G USB Modem, 62

3G/4G USB Modem (DHCP mode), 55

3G/4G USB Modem (PPP mode), 54

## 6

6rd Mode, 100

6rd Prefix, 100

6rd Prefix Length, 100

## 8

802.1x ports, 143

## A

Access Control, 265

Access List, 436

Access Mode, 73

Access Mode-Etherenet / USB, 73

Access Tech, 251

Active Directory/LDAP, 181

Active Mode, 65, 68, 69, 71

Active-Standby, 194

Additional Filter, 183

Address Mapping, 220, 236

Advance Mode, 369

Advanced Mode, 246

Advanced Setting, 272

Aggregation MSDU, 273

Airtime Fairness, 279

ake on LAN, 187

Always On, 79, 84, 91, 93, 94, 96, 97, 99, 100, 105

Analyze, 383

Anonymous, 181

Antenna, 274

AP Discovery, 85, 278

AP Maintenance, 540, 548

AP Map, 540, 549

APN Name, 54, 87, 89

APP Enforcement, 366, 375

APP Enforcement Filter, 385

APP Enforcement Profile, 386

APP QoS, 460

APPE Module Version, 388

APPE Signature Upgrade, 388

Applications, 158

APSD Capable, 274

ARP Cache Table, 633

ARP Detect, 76, 79, 84, 87, 89

ARP Table, 140

Authentication, 179

Authentication Information, 648

Authentication Key, 195

Authentication Mode, 269

Authentication Port, 178

Authentication Type, 143

Auto Adjustment, 277

Auto Logout, 24

Auto-Update interval, 162

Aux. WAN IP, 154

## B


Backup, 140

Band Steering, 281

Bandwidth Limit, 449

Bandwidth Management, 277, 449

Base Distinguished Name, 183

Bind IP to MAC, 139

Bind to WAN, 307

Bind Type, 181

Bogus DNS Reply, 171

Bonjour, 190

Bridge mode, 107

Bridge Mode, 80, 96, 98

Bridge Subnet, 80, 96, 98

Brute Force Protection, 434


## C


Cache, 395

Call Direction, 325

Certificate Backup, 357

Change the TTL value, 77, 80

Channel, 258, 262

Channel Bandwidth, 273

Choose IP, 152

Comment, 140, 154

Common Name Identifier, 183

Config Backup, 33

Config Sync, 196

Configuration Backup, 424

Connection Management, 339

Connectivity, 61

Country Code, 275

CPE Management, 522

CSV file, 608

Current System Time, 173


## D


Dashboard, 27, 541

Data Coding Scheme, 248

Data Filter, 361

Data Flow Monitor, 639

Data Quota, 467

DataType, 73

Daylight Saving, 430

Days in a week, 173

Default Lifetime, 132

Default MAC Address, 80

Default Preference, 132

Default Rule, 365

Destination IP, 227

Details Page, 73

Details-3G/4G USB Mdem(PPP mode), 86

Details-3G/4G USB Modem(DHCP mode), 88

Details-IP Routed Subnet, 128

Details-IPv6-6in4 Static Tunnel, 98

Details-IPv6-6rd, 100

Details-IPv6-AICCU, 94

Details-IPv6-DHCPv6 Client, 95

Details-IPv6-Offline, 90

Details-IPv6-PPP, 91

Details-IPv6-Static IPv6, 97

Details-IPv6-TSPC, 92

Details-LAN IPv6, 130

Details-LAN-DMZ, 126

Details-LAN-Ethernet, 122

Details-PPPoE, 75

Details-PPTP/L2TP, 82

Details-Static IP or Dynamic IP, 78

Details-Static or Dynamic IP, 84

Determine Real WAN IP, 164

DFS Restrictions, 256

DHCP, 46

DHCP Server Configuration, 123, 126, 128

DHCP Server IP Address, 123, 126

DHCP Table, 635

DHCPv6 (Stateful), 130

DHCPv6 Server, 131

Diagnose, 172, 231

Diagnostic, 631

Dial-out Triggering, 631

Digital Signature, 321

Display Name, 67, 69, 71, 73

DMZ Host, 151

DNS Cache Table, 637

DNS Filter, 366

DNS Filter Profile, 397

DNS Security, 171

DNS Server, 172

DNS Server IP Address, 81, 124, 127

DNS Server IPv6 Address, 131

Domain, 172

Domain Diagnose, 172

Domain Name, 80, 230

DoS Defense, 361, 378, 380

DoS Flood Table, 650, 651

Download Limit, 277

DrayTek Banner, 376

Dynamic DNS, 158, 161

Dynamic DNS Account, 163, 165

Dynamic IP, 84

## E

Enable PING to keep alive, 79

End IPv6 Address, 131

End Port, 155

ESP, 308

Event Code, 414

Event Log, 555

Extension WAN, 132

External Devices, 574

External RADIUS, 176

External TACACS+, 180

## F

Failover, 68, 69, 71

Failover to/Failback, 220

File Explorer, 618

File Extension Object, 594

Filter Setup, 368

Firewall, 361

Firmware Upgrade, 445

Fixed IP, 77, 83, 105

Force NAT /Force Routing, 228

Force Update, 161

Fragment Length, 274

## G

Gateway IP Address, 80, 84, 123, 126

General Setup, 64

Google Map, 527

GRE, 328

Group ID, 186, 195

Guard Interval, 273

GUI Map, 31

## H

Hardware Acceleration, 144

Hardware Installation, 14

Hide SSID, 262

High Availability, 193

High Availability Status, 646

Host Name, 46

Hot-Standby, 194

## I

Idle Timeout, 77, 83, 105

IGMP, 185

IGMP Proxy, 185

IGMP Snooping, 185

Incoming Port, 158

Incoming Protocol, 157

Indicators and Connectors, 2, 12

Installation, i

Interface, 228

Inter-LAN Routing, 122

Internal RADIUS, 177

Internal Service User List, 447

Internet Access, 72

IP (Internet Protocol), 62

IP address, 84

IP Address, 80, 83, 122, 126, 128

IP Address Assignment Method(IPCP), 83

IP Address List, 169

IP Based, 65

IP Bind List, 140

IP Group, 581

IP Object, 578

IP Pool Counts, 123, 126, 128

IPsec General Setup, 307, 308

IPsec Peer Identity, 311

IPTV, 105

IPv4 Border Relay, 100

IPv4 Mask Length, 100

IPv6 Address, 97

IPv6 Gateway Address, 97

IPv6 Group, 585

IPv6 Neighbour Table, 634

IPv6 Object, 583

IPv6 TSPC Status, 646

Isolate, 262

ISP Access Setup, 75, 82

ISP Name, 105

## K

Keep WAN Connection, 79

Keyword Group, 593

Keyword Object, 591

## L

LAN, 118

LAN DNS / DNS Forwarding, 159, 167

LAN Port Mirror, 142

LAN to LAN, 323

Landing Page, 463

LAN-General Setup, 120

LDAP /Active Directory Setup, 159

Lease Time, 123, 126, 128

Line Speed, 64, 67, 69, 71

Load Balance, 557

Load Balance for AP, 540

Load Balance Mode, 65

Load-Balance, 226, 234

Load-Balance /Route Policy, 226

Local 802.1X, 447

Local 802.1X General Setup, 198

Local Certificate, 294, 350

Local IP Address, 154

Log, 391

Log & Alert, 530

Login, 58

Login Page Greeting, 422

Logout, 33

Long Preamble, 273

LTE, 242

LTE Status, 251

## M

Mail Alert, 189

Mail Extender, 164

Mail Service, 189

Main Screen, 24

Maintenance, 568

Management, 433

Management Interface, 195

Min/Max Interval Time, 132

Minimum Keep Alive Period, 414

Mirror Port, 142

Mode, 258, 263

Modem Code Upgrade, 446

Modem Dial String, 87

Modem Initial String, 54, 87

Modem Initial String2, 87

Modem Support List, 86, 88

MPPE, 305

MTU, 76, 79, 82, 85, 90, 132

Multiple SSID, 254

multiple-WAN, 64

Multi-PVC/VLAN, 102

MyVigor, 56

## N

Name Link, 29

NAT, 146

NAT Sessions Table, 636

Network Configuration, 122, 126, 128

Network Interface, 225

Network Mode, 89

Notification Object, 601

NS Detect, 96

## O

Objects Settings, 577

Online Statistics, 455

Open Ports, 154

Option Number, 73

## P

Packet-OVERDRIVE, 273

PAP, 305

Pass Phrase, 85

Password, 75, 80, 82, 93, 94, 105

Password Strength, 264, 419

Path MTU Discovery, 76, 79, 82, 90

Peer ID, 300, 303

Per Station Limit, 277

Physical Connection, 34

Physical Members, 105, 107

Physical Mode, 64, 67, 69, 71, 73

Physical Type, 39, 64

PinCode, 269

Ping Detect, 76, 79, 84, 87, 89, 91, 93, 94, 96, 97, 99, 100

Ping Diagnosis, 638

Ping Gateway IP, 76, 79, 84, 87, 89

Ping Interval, 76, 79, 87, 89

PING Interval, 79

Ping IP/Hostname, 91, 93, 94, 96, 97, 99, 100

Ping Retry, 76, 79, 87, 89

Port Redirection, 147

Port Triggering, 156, 158

Port-based Bridge, 103

Port-Based VLAN, 135

PPP Authentication, 77, 83, 87, 105

PPP General Setup, 305

PPP Password, 87

PPP Setup, 83

PPP Username, 87

PPPoE, 40

PPPoE Pass-through, 76

PPTP/L2TP, 42

Prefix Len, 225

Prefix Length, 97

Pre-shared Key, 271

Pre-Shared Key (PSK), 264

Primary DNS Sever, 131

Primary IP Address, 124, 127

Primary/Secondary Ping IP, 76, 79, 87, 89

Printer Server, 616

Priority, 68, 107, 136, 220, 231

Priority ID, 195

Private IP, 149

Private IP Address, 62

Private Port, 149

Production Registration, 58

Protocol, 195

Protocol Processing Engine (PPE), 144

Public IP Address, 62

Public Port, 149

Push Button, 269

## Q

Quality of Service, 449, 454

Query Server, 395

Quick Access, 30

Quick Start Wizard, 38

Quota Limit, 109

## R

RADIUS/TACACS+, 159, 176

Rate Adaptation Algorithm, 274

Rate Control, 119

Reboot System, 444

Recipient, 188

Recipient Number, 248

Redundancy Method, 194

Registering Vigor Router, 58

Regular DN, 182

Regular Mode, 181

Regular Password, 182

Relay Agent, 123, 126

Remote Access Control, 304

Remote Dial-in User, 313, 315, 319

Remote Endpoint IPv4 Address, 98

Repeater, 271

Restore, 140

RIP Protocol, 80

RIPng Protocol, 91, 96, 98, 132

Root CA, 356

Route Policy, 220

Router Advertisement Configuration, 132

Router Commands, 249

Router Name, 80, 427

Routing, 220

Routing Information Protocol, 119

Routing Table, 632

RTS Threshold, 275

## S

Scan, 278

Schedule, 87, 89, 159, 173, 262

Secondary DNS Server, 131

Secondary IP Address, 124, 127

Security, 263
Security Key, 258
Self-Signed Certificate, 359, 442
Send SMS, 248
Sensor, 620
Server Address, 82
Server Certificate, 307
Service, 157
Service Activation Wizard, 56
Service Name, 75, 87, 149
Service Provider, 163, 165, 597
Service Type Group, 589
Service Type Object, 587
Sesseion Based, 65
Sessions Control, 365
Sessions Limit, 449, 450
Set to Factory Default, 161, 173, 222
Shared Secret, 178, 180
SIM card, 242
SIM Pin code, 54
SIM PIN code, 87, 89
Simple Mode, 181, 245
SLAAC(stateless), 130
Smart Bandwidth Limit, 453
SMB, 617
SMS / Mail Alert Service, 188
SMS Alert, 188
SMS Inbox, 245
SMS Provider, 188
SMS Quota Limit, 243
SMS/Mail Service Object, 596
Source IP, 149, 155, 157, 227
SPI, 361
SSL VPN, 307
Start IP Address, 123, 126, 128
Start IPv6 Address, 131
Start Port, 155
Static IP, 44, 48, 51
Static Route, 119, 221
Static Route for IPv6, 224
Station Control, 276
Station List, 256, 285, 286
Station Number, 556
Stations (STA), 254
Status, 542
Strict Bind, 139
Strict Security Firewall, 364
String Object, 604, 605
STUN Settings, 414
Subnet, 136
Subnet Mask, 80, 83, 84, 122, 126, 128
Subnet Prefix, 94
Support List, 569, 572, 573
Switch, 559
Switch Group, 566
Switch Hierarchy, 562
Switch Status, 560
Sync User Profile, 198
Syslog Alarm, 621
Syslog Explorer, 645
Syslog/Mail Alert, 427
System Maintenance, 410
System time set, 173

## T

Tag value, 68
Tagged VLAN, 135
Temperature Sensor, 620
Time and Date, 430
Time Quota, 466
Time Schedule, 453

Time Server, 430

Time Zone, 430

Total Traffic, 556

Trace Route, 644

Traceable, 460

Traffic Graph, 554, 642

Traffic Threshold, 68, 69, 71

Triggering Port, 157

Triggering Protocol, 157

Trusted CA Certificate, 355

TSPC, 92

TTL (Time to Live), 76, 79, 84, 87, 89, 91, 93, 94, 96, 97, 99, 100

Tunnel Broker, 93, 94

Tunnel ID, 94

TX Power, 274

## U

Unique Local Address (ULA), 131

Update DDNS, 195

Upload Limit, 277

UPnP, 159, 183

URL Access Control, 391

URL Content Filter, 366, 375, 385

URL Content Filter Profile, 390

USB, 48, 54

USB General Settings, 615

USB User Management, 616

User Group, 468

User Password, 419

User Profile, 179, 198, 464

Username, 75, 80, 82, 93, 94, 105

## V

VID, 136

View SMS Outbox Cache, 248

Virtual LAN, 119

Virtual Panel, 28

Virtual WAN, 37

VLAN, 135

VLAN Applications, 663

VLAN Configuration, 137

VLAN Tag, 102, 107, 136

VLAN Tag insertion, 39, 68

VPN, 288, 519

VPN and Remote Access, 289

VPN Client Wizard, 290

VPN Dial-Out Through, 294

VPN Graph, 643

VPN Management, 529

VPN Server Wizard, 296

VPN Trunk Management, 332

## W

Wake by IP Address, 187

Wake on LAN, 160

WAN, 62

WAN Budget, 108

WAN Budget-Status, 112

WAN Connection Detection, 76, 79, 84, 87, 89, 91, 93, 94, 96, 97, 99, 100

WAN Failure, 68, 69, 71

WAN Interface, 154, 163, 165

WAN IP, 149

WAN IP Alias, 77, 80, 83

WAN IP Network Settings, 80, 83

WAN Setup, 105

WAN Type, 102, 104, 107

WAN-USB, 70

WDS, 270

Web Console, 32

Web Content Filter, 366, 375, 385

Web Content Filter Profile, 394

Web Feature, 392

Weight, 65

WEP, 85, 255, 264

Wildcard, 164

Wired 802.1x, 143

Wireless 2.4/5G, 67

Wireless LAN, 253

Wireless Wizard, 257

Wizard Mode, 369

WLAN Isolation, 255

WLAN Profile, 543

WMM Capable, 274

WPA, 255, 264

WPS, 256, 267