DrayTek

Vigor3900

Multi-WAN Security Appliance

Providing Productivity and Security for
Small, Medium and Large Businesses

Your reliable networking solutions partner

User's Guide

V2.7

TAIWAN EXCELLENCE 2012

Vigor3900
Multi-WAN Security Appliance
User's Guide

Version: 2.7

Firmware Version: V1.4.0

(For future update, please visit DrayTek website)

Date: June 13, 2018

Intellectual Property Rights (IPR) Information

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 95, 98, Me, NT, 2000, XP, Vista, 7 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 and Approval

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

Chapter 1: Introduction 1

1.1 LED Indicators and Connectors 2

1.2 Hardware Installation 4

1.2.1 Network Connection 4
1.2.2 Rack-Mounted Installation 5

Chapter 2: Basic Setup 7

2.1 Changing Password 7

2.2 Quick Start Wizard 9

2.2.1 Step 1 - Specifying the WAN Profile 9
2.2.2 Step 2 - Configuring the Selected Protocol 11

2.3 Register Vigor Router 18

Chapter 3: Application and Tutorial 21

3.1 How to use Bandwidth Limit on Vigor3900? 21

3.2 How to use Session Limit on Vigor3900? 24

3.3 How to assign other IP as Gateway IP for LAN DHCP clients? 26

3.4 How to use Port Redirection on Vigor3900? 28

3.5 How to Configure OSPF? 30

3.6 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 36

3.7 How to run RDP service in the browser via logging in 3900's HTTPS Server? 39

3.8 How to Configure VPN Load Balance between Vigor3900 and Other Router 44

3.9 How to Setup 50 WANs on Vigor3900 53

3.10 CVM Application - How to manage the CPE (router) through Vigor3900? 58

3.11 CVM Application - How to build the VPN between remote devices and Vigor3900? 63

3.12 CVM Application - How to upgrade CPE firmware through Vigor3900? 66

3.13 How to use High Availability for Vigor routers? 72

3.14 How to Configure DNS Inbound Load Balance on Vigor 3900? 76

3.15 How to Bridge LAN networks over GRE Tunnel between two Vigor3900s? 79

Chapter 4: Advanced Web Configuration 83

4.1 WAN Setup 83

4.1.1 General Setup 84
4.1.2 Inbound Load Balance 107
4.1.3 Switch 113

4.2 LAN 118

4.2.1 General Setup 118
4.2.2 PPPoE Server 133
4.2.3 Switch 137

4.2.4 Bind IP to MAC 143
4.2.5 LAN DNS 146

4.3 Routing 149

4.3.1 Load Balance Pool 149
4.3.2 Static Route 153
4.3.3 Policy Route 159
4.3.4 Fast Route 176
4.3.5 Default Route 178
4.3.6 RIP Configuration 179
4.3.7 OSPF Configuration 180
4.3.8 BGP Configuration 183

4.4 NAT 188

4.4.1 Port Redirection 188
4.4.2 Fast NAT 192
4.4.3 Server Load Balance 196
4.4.4 DMZ Host 199
4.4.5 ALG 202
4.4.6 Connection Timeout 203

4.5 Firewall 205

4.5.1 Filter Setup 205
4.5.2 DoS Defense 228
4.5.3 MAC Block 231
4.5.4 Filter Counter 233

4.6 Objects Setting 234

4.6.1 IP Object 234
4.6.2 IP Group 236
4.6.3 IPv6 Object 238
4.6.4 MAC/Vendor Object 240
4.6.5 Country Object 242
4.6.6 Service Type Object 243
4.6.7 Service Type Group 245
4.6.8 Keyword /DNS Object 247
4.6.9 File Extension Object 251
4.6.10 APP Object 254
4.6.11 Web Category Object 257
4.6.12 QQ Object 261
4.6.13 QQ Group 262
4.6.14 Time Object 264
4.6.15 Time Group 267
4.6.16 SMS Service Object 268
4.6.17 Mail Service Object 271
4.6.18 Notification Object 273

4.7 User Management 277

4.7.1 Web Portal 277
4.7.2 User Profile 284
4.7.3 User Group 298
4.7.4 Guest Profile 301
4.7.5 RADIUS 306
4.7.6 LDAP/Active Directory 308

4.8 Application 312

4.8.1 Dynamic DNS 312
4.8.2 DNS Security 318
4.8.3 GVRP 319
4.8.4 IGMP Proxy 320

4.8.5 UPnP 321
4.8.6 High Availability 322
4.8.7 Wake on LAN 331
4.8.8 SMS / Mail Alert Service 334

4.9 VPN and Remote Access 338

4.9.1 VPN Client Wizard 338
4.9.2 VPN Server Wizard 345
4.9.3 Remote Access Control 352
4.9.4 PPP General Setup 353
4.9.5 OpenVPN General Setup 358
4.9.6 IPSec General Setup 360
4.9.7 VPN Profiles 361
4.9.8 VPN Trunk Management 376
4.9.9 Connection Management 381

4.10 Certificate Management 383

4.10.1 Local Certificate 383
4.10.2 Trusted CA Certificate 390
4.10.3 Remote Certificate 393

4.11 SSL Proxy 394

4.11.1 SSL Web Proxy 394
4.11.2 SSL Application 396
4.11.3 Online User Status 400

4.12 Bandwidth Management 401

4.12.1 Quality of Service 401
4.12.2 QoS Rule 405
4.12.3 Sessions Limit 412
4.12.4 Bandwidth Limit 416

4.13 USB Application 420

4.13.1 Disk Status 420
4.13.2 FTP Server 421
4.13.3 SAMBA Server 422
4.13.4 Printer 425
4.13.5 Temperature Sensor 426
4.13.6 Modem Support List 428

4.14 System Maintenance 429

4.14.1 TR-069 429
4.14.2 Administrator Password 432
4.14.3 Configuration Backup 433
4.14.4 Syslog / Mail Alert 437
4.14.5 Time and Date 441
4.14.6 Access Control 442
4.14.7 SNMP Setup 447
4.14.8 Reboot System 448
4.14.9 Firmware Upgrade 451
4.14.10 APP Signature Upgrade 455
4.14.11 APP Support List 457

4.15 Diagnostics 458

4.15.1 Routing Table 458
4.15.2 ARP Cache Table 461
4.15.3 DNS Cache Table 463
4.15.4 DHCP Table 464
4.15.5 Session Table 466
4.15.6 Traffic Graph 467

4.15.7 Web Console 470
4.15.8 Ping/Trace Route 470
4.15.9 Data Flow Monitor 471
4.15.10 User Status 476
4.16 Central Management (VPN) 477
4.16.1 General Setup 477
4.16.2 CPE Management 479
4.16.3 Log/Alert 488
4.17 Central Management (AP) 489
4.17.1 General Setup 491
4.17.2 Dashboard 492
4.17.3 Status 492
4.17.4 WLAN Profile 494
4.17.5 AP Maintenance 498
4.17.6 AP Map 499
4.17.7 Traffic Graph 502
4.17.8 Rogue AP 503
4.17.9 Event Log 505
4.17.10 Total Traffic 506
4.17.11 Station Number 506
4.17.12 Load Balance 507
4.17.13 Function Support List 509
4.18 Central Management (Switch) 510
4.18.1 Status 510
4.18.2 Profile 513
4.18.3 Group 517
4.18.4 Maintenance 518
4.18.5 Support List 519
4.19 External Devices 520
4.20 Product Registration 521

Chapter 5: Trouble Shooting 523

5.1 Checking If the Hardware Status Is OK or Not 523
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 524
5.3 Pinging the Router from Your Computer 527
5.4 Checking If the ISP Settings are OK or Not 528
5.5 Backing to Factory Default Setting If Necessary 529
5.6 Contacting DrayTek 530

Chapter 6: Telnet Commands 531

6.1 Accessing Telnet of Vigor Router 531
6.2 Global Commands 533
6.3 Available Configure Commands 540
6.4 WAN Configuration 542
6.4.1 Telnet Command: pf 542
6.4.2 Telnet Command: defaultroute 556
6.4.3 Telnet Command: lbpool 556
6.4.4 Telnet Command: autolb 559

6.4.5 Telnet Command: switch 560
6.4.6 Telnet Command: 3g 561

6.5 LAN Configuration 562

6.5.1 Telnet Command: ipbindmac 562
6.5.2 Telnet Command: iprouting 564
6.5.3 Telnet Command: pf 567
6.5.4 Telnet Command: route 578
6.5.5 Telnet Command: route6 580
6.5.6 Telnet Command: switch 583

6.6 NAT Configuration 584

6.6.1 Telnet Command: port_redirect 584
6.6.2 Telnet Command: dmz 589

6.7 Objects Setting Configuration 593

6.7.1 Telnet Command: fext_object 593
6.7.2 Telnet Command: ip_group 597
6.7.3 Telnet Command: ip_object 599
6.7.4 Telnet Command: keyword_object 602
6.7.5 Telnet Command: service_group 603
6.7.6 Telnet Command: service_object 605
6.7.7 Telnet Command: time_group 608
6.7.8 Telnet Command: time_object 610
6.7.9 Telnet Command: web_category 613

6.8 User Management Configuration 619

6.8.1 Telnet Command: users 619
6.8.2 Telnet Command: group 626

6.9 Applications Configuration 629

6.9.1 Telnet Command: DDNS 629
6.9.2 Telnet Command: GVRP 631
6.9.3 Telnet Command: HA 632
6.9.4 Telnet Command: ldap 632
6.9.5 Telnet Command: ospf 636
6.9.6 Telnet Command: rip 637
6.9.7 Telnet Command: SIP ALG 637
6.9.8 Telnet Command: UPnP 638

6.10 VPN Configuration 639

6.10.1 Telnet Command: lan2lan 639
6.10.2 Telnet Command: remotedialin 658
6.10.3 Telnet Command: trunk 662

6.11 Bandwidth Management Configuration 668

6.11.1 Telenet Command: access_barrier 668
6.11.2 Telenet Command: bandwidth_limit 669
6.11.3 Telenet Command: sesslimit 672

6.12 System Management Configuration 675

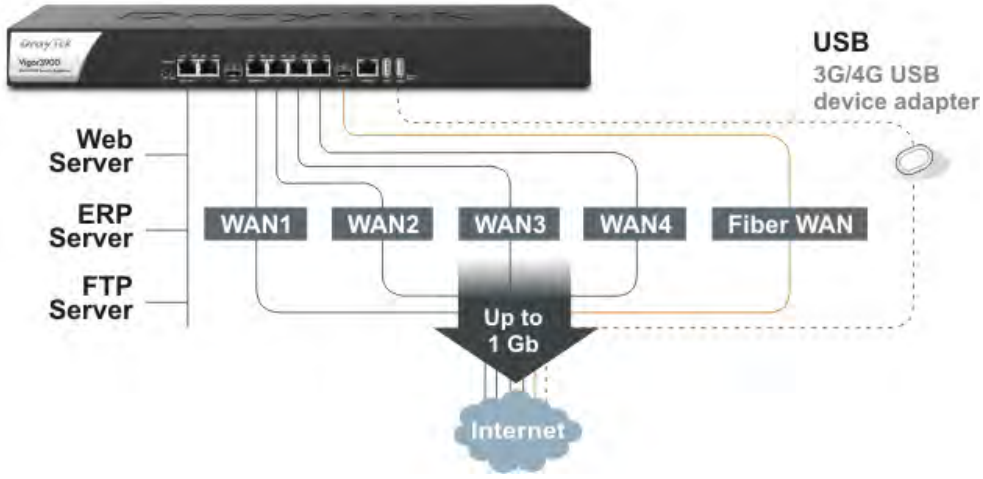
6.12.1 Telnet Command: acc_ctrl 676
6.12.2 Telnet Command: admin_passwd 679
6.12.3 Telnet Command: autodiscovery 680
6.12.4 Telnet Command: cc 680
6.12.5 Telnet Command: cmm 681
6.12.6 Telnet Command: config 681
6.12.7 Telnet Command: firmware 686
6.12.8 Telnet Command: mailalert 686
6.12.9 Telnet Command: ntpclient 688

6.12.10 Telnet Command: reboot 689
6.12.11 Telnet Command: snmpagent 689
6.12.12 Telnet Command: syslogd 691
6.12.13 Telnet Command: tr069 692

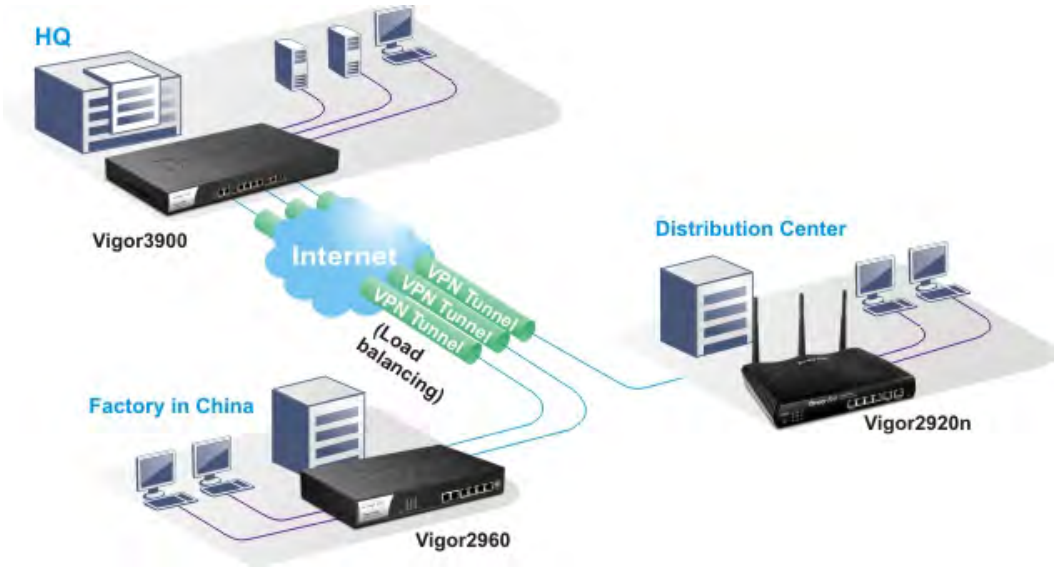
Chapter 1: Introduction

Note: 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.

The Vigor3900 Series integrates a rich suite of functions, including NAT, firewall, VPN, load balance, and bandwidth management capability. These products are very suitable for providing multi-integrated solutions to SME markets.



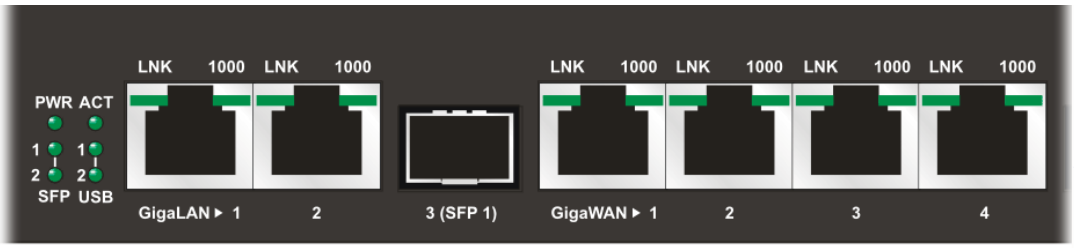
A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like an Intranet. A VPN enables you to send data between two computers across a shared public Internet network in a manner that emulates the properties of a point-to-point private link. The DrayTek Vigor3900 Series VPN router supports Internet-industry standards technology to provide customers with open, interoperable VPN solutions such as X.509, DHCP over Internet Protocol Security (IPSec) **up to 500** tunnels, and Point-to-Point Tunneling Protocol (PPTP).



1.1 LED Indicators and Connectors

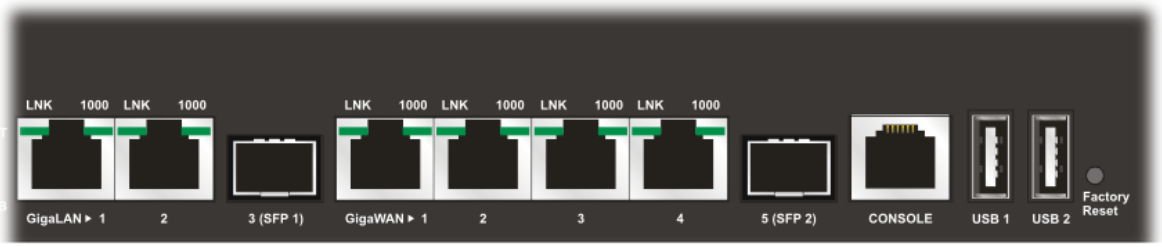
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

Description for LED



LED		Status	Explanation
PWR		On	The router is powered on.
		Off	The router is powered off.
ACT		Blinking	The system is active.
		On/Off	The system is hanged.
SFP 1/2		On	The fiber connection is established.
		Off	No fiber connection is established.
USB 1/2		On	The USB device is installed and ready.
		Off	No USB device is installed.
GigaLAN1 /LAN 2)	LNK	On	The Ethernet link is established on corresponding port.
		Blinking	The data transmission is done through the corresponding port.
		Off	No Ethernet link is established.
	1000	On	It means that a normal 1000 Mbps connection is through its corresponding port.
		Off	It means that a normal 10/100 Mbps connection is through its corresponding port.
Giga WAN1/2/3/4	LNK	On	The Ethernet link is established.
		Blinking	The data transmission is done through the corresponding port.
		Off	No Ethernet link is established.
	1000	On	It means that a normal 1000Mbps connection is through its corresponding port.
		Off	It means that a normal 10/100Mbps connection is through its corresponding port.

Connectors



Interface	Description
GigaLAN1 / 2	Connecter for local network devices.
3(SFP)	Connecter for fiber cable.
GigaWAN1/2/3/4	Connecter for remote network devices.
5(SFP)	Connecter for fiber cable.
Console	Provided for technician use.
USB1 / USB2	Connecter for the USB device.
Factory Reset	Used to restore the default settings. Press it and keep for more than 5 seconds. When you see the **ACT** LED begins to blink, release the button. Then the router will restart with the factory default configuration.
	Connecter for a power cord. ON/OFF - Power switch.

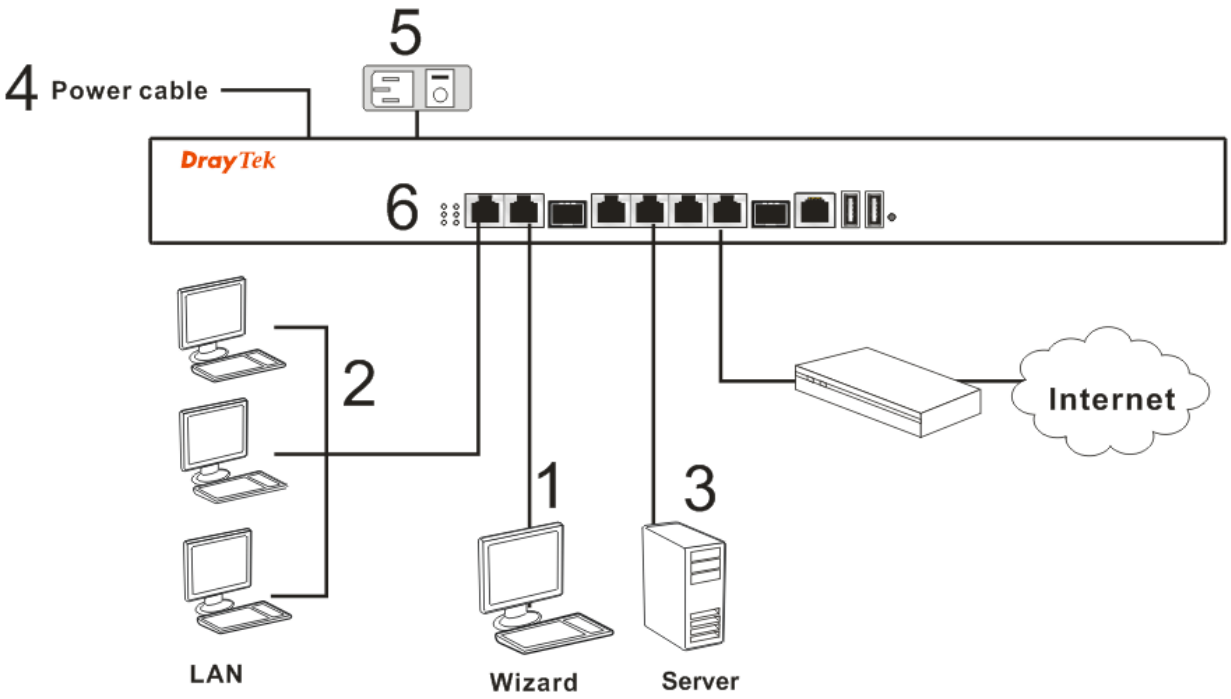
1.2 Hardware Installation

1.2.1 Network Connection

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

1. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of Vigor3900s.
2. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The **LAN** LED for that port on the front panel will light up.
3. Connect a server/modem/router (depends on your requirement) to any WAN port of Vigor3900 with Ethernet cable (RJ-45). The **WAN1 (to WAN4)** LED will light up.
4. Connect the power cord to Vigor3900's power port on the rear panel, and the other side into a wall outlet.
5. Power on the device by pressing down the power switch on the rear panel. The **PWR** LED should be **ON**.
6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

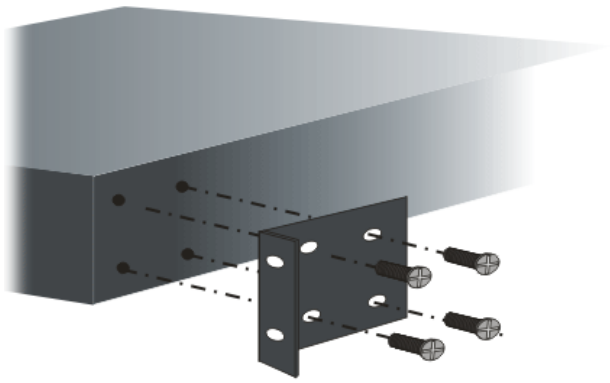
Below shows an outline of the hardware installation for your reference.



1.2.2 Rack-Mounted Installation

The Vigor3900 Series can be mounted on the wall by using standard brackets shown below.

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



After the bracket installation, the Vigor3900 Series chassis can be installed in a rack by using four screws for each side of the rack.

Desktop Type Installation

Rubber pads are included with the Vigor3900 Series. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

This page is left blank.

Chapter 2: Basic Setup

For use the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

To change the password for this device, you have to access into the web browse with default password first.

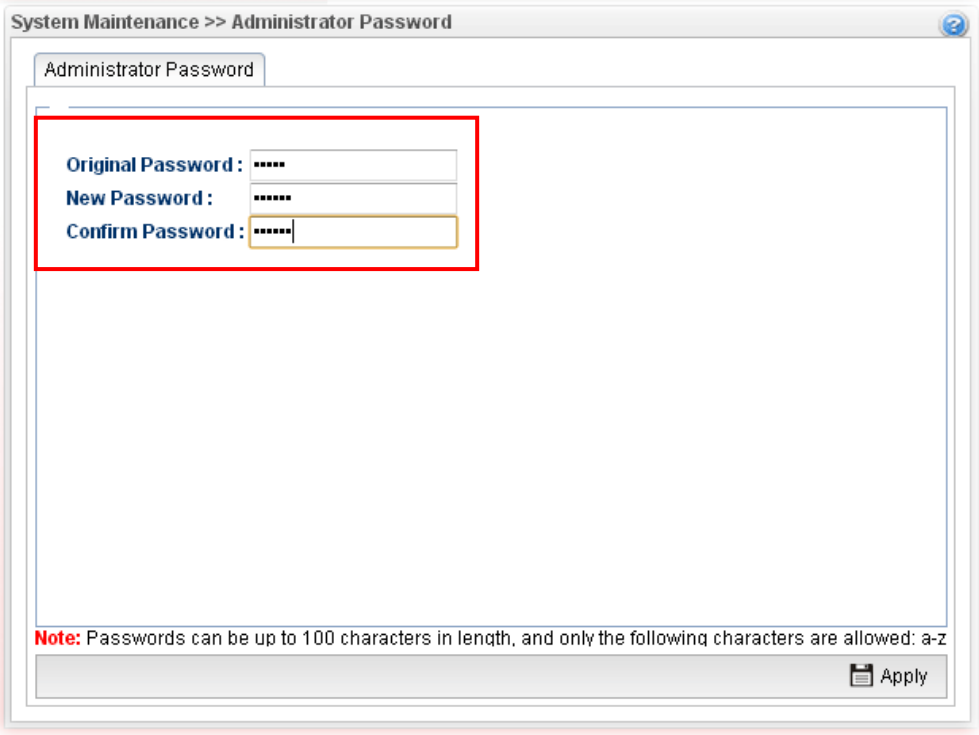
1. Make sure your computer connects to the router correctly.

> **Notice:** 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 this guide.

2. 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. Please type default values on the window for the first time accessing. The default value for user name is **admin** and the password is **admin**. Next, click **Login**.

3. Now, the **Main Screen** will pop up.

4. Go to **System Maintenance** page and choose **Administrator Password**.



5. Enter the login password (admin) on the field of **Original Password.** Type a new one in the field of **New Password** and retype it on the field of **Confirm Password**. Then click **Apply** to continue.

6. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this router.

2.2 Quick Start Wizard

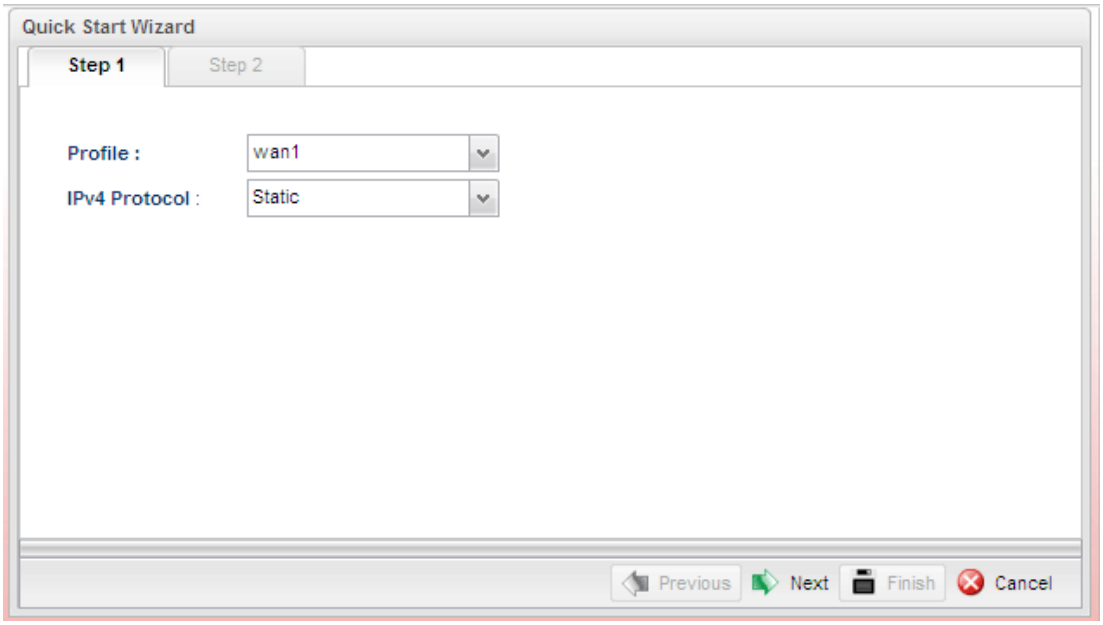
Quick Start Wizard is a wizard which is designed for configuring your router accessing Internet with simply steps. In the **Quick Start Wizard** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes.

For most users, Internet access is the primary application. The router supports the Ethernet WAN interface for Internet access.

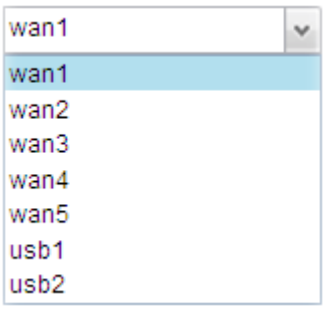
Click **Quick Start Wizard** from the home page. Quick Start Wizard will guide the user to establish LAN interface profile, WAN interface profile and select proper protocol for connection. The following will explain in more detail for the various broadband access configurations.

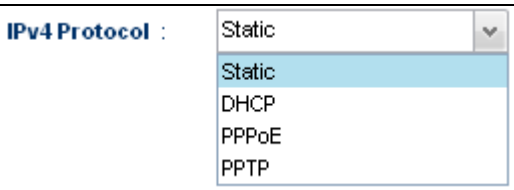
2.2.1 Step 1 - Specifying the WAN Profile

In the first page of Quick Start Wizard, please create a WAN profile.



Available settings are explained as follows:

Item	Description
Profile	Use the drop down list to choose one WAN profile. 
IPv4 Protocol	Use the drop down list to choose a connection mode for such WAN profile.

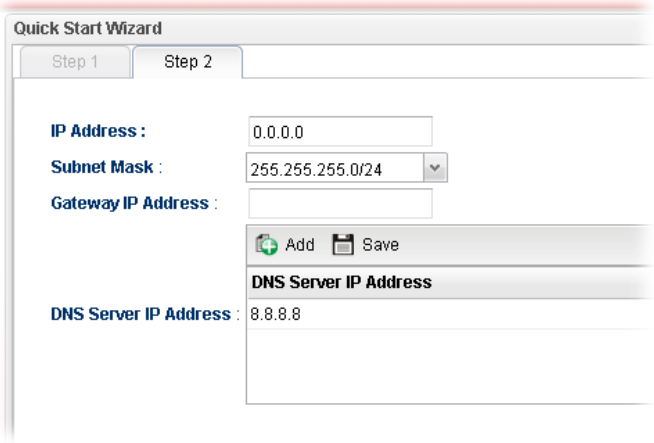
Item	Description
	 **Static** - If **Static** is selected, you can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings. **DHCP** - It allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for Vigor3900 automatically. It is not necessary for you to assign any setting. (Host Name and Domain Name are required for some ISPs). **PPTP** - This mode lets user get the IP group information by a DSL modem with PPTP service from ISP. Your service provider will give you user name, password, and authentication mode for a PPTP setting. Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol. If your ISP offers you **PPTP** (Point-to-Point Tunneling Protocol) mode, please select **PPTP** for this router. Next, enter the required information provided by your ISP on the web page. **PPPoE** - PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection. PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode. If your ISP provides you the **PPPoE** (Point-to-Point Protocol over Ethernet) connection, please select **PPPoE** for this router to get the following page. Enter the **username** and **password** provided by your ISP on the web page.

Note: After you creating the WAN profile(s) by using Quick Start Wizard, you can select the existing WAN profiles for next time. Simply use the drop down list to choose the WAN profile available for modifying.

When you finish the above settings, please click **Next** to go to next page.

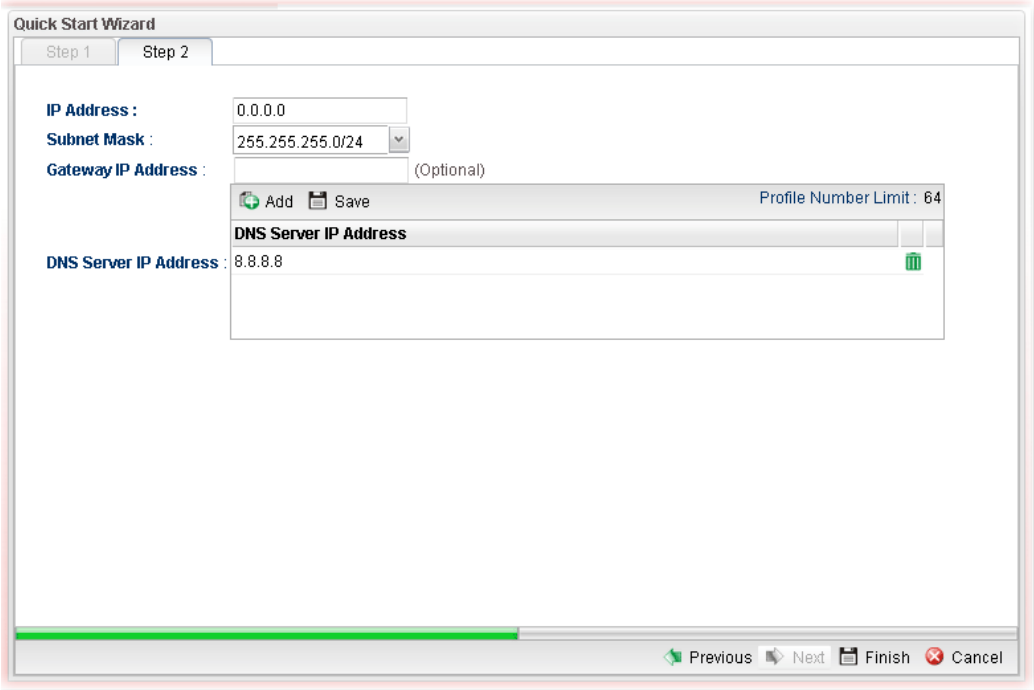
2.2.2 Step 2 - Configuring the Selected Protocol

This page will be changed according to the **IPv4 Protocol Type** selected on last page.



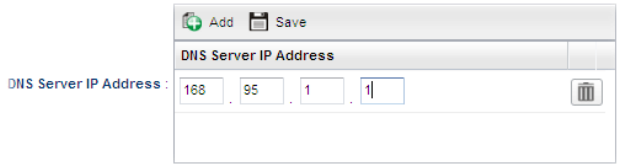
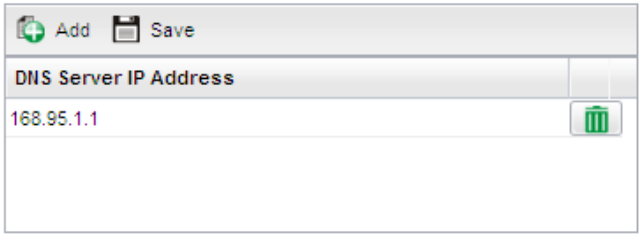
If Static is selected

If **Static** is selected, the following screen will appear. You can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings.



Available parameters are listed as follows:

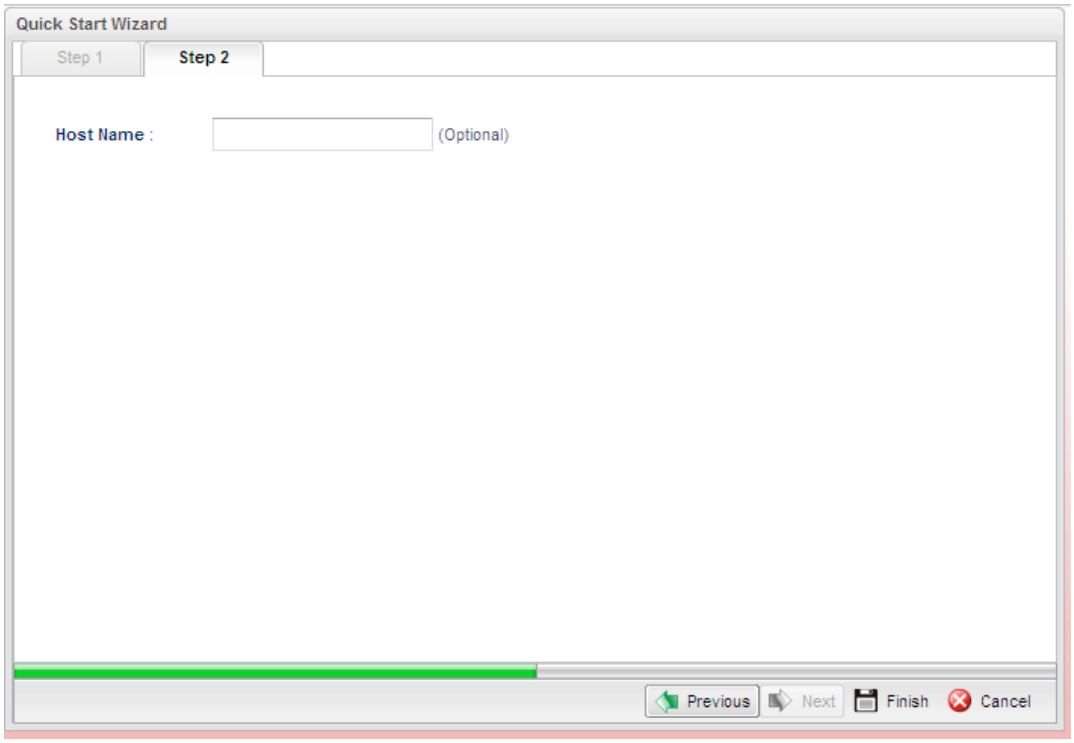
Item	Description
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile. - click it to remove the created IP address if you are not satisfied with it.

DNS Server IP Address	**Add** – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny boxes one by one.  **Save** – After finished the IP address configuration, click Save to save the setting onto the router.  – Click the icon to remove the selected entry.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

When you finished the above settings, please click **Finish**.

If DHCP is selected

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for Vigor3900 automatically. It is not necessary for you to assign any setting. (Host Name is required for some ISPs).



Available parameters are listed as follows:

Item	Description
Host Name (Optional)	Type a name as the host name for identification.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

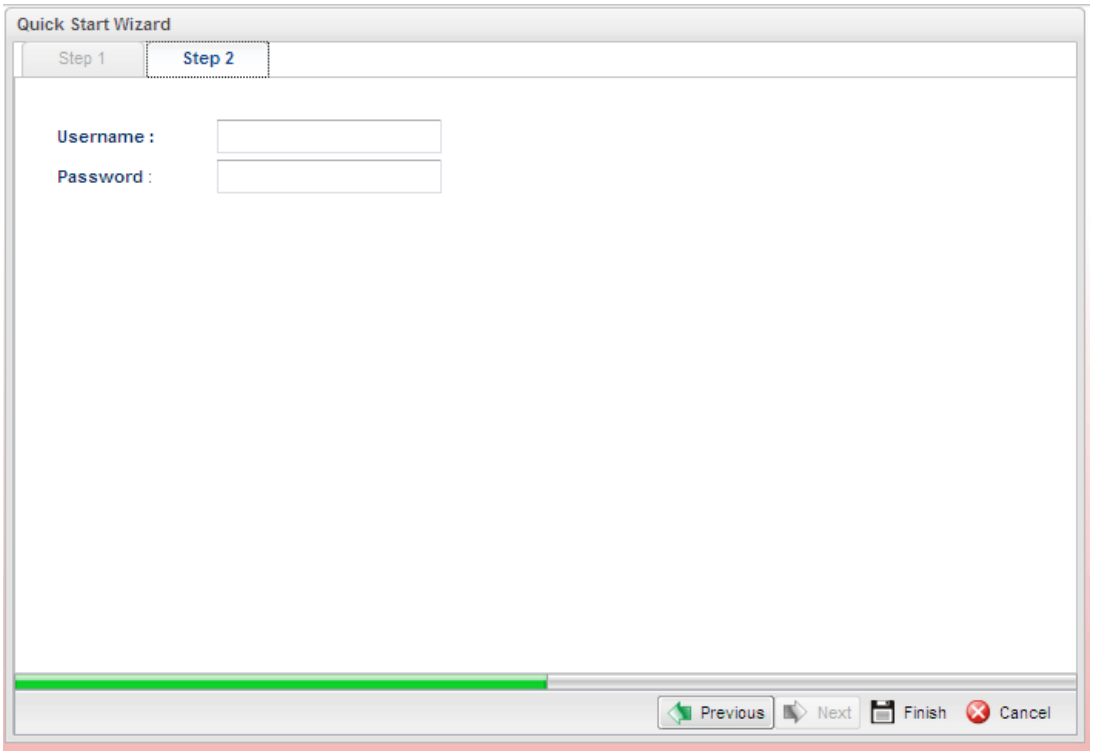
When you finished the above settings, please click **Finish**.

If PPPoE is selected

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** (Point-to-Point Protocol over Ethernet) connection, please select **PPPoE** for this router to get the following page. Enter the **username** and **password** provided by your ISP on the web page.



Available parameters are listed as follows:

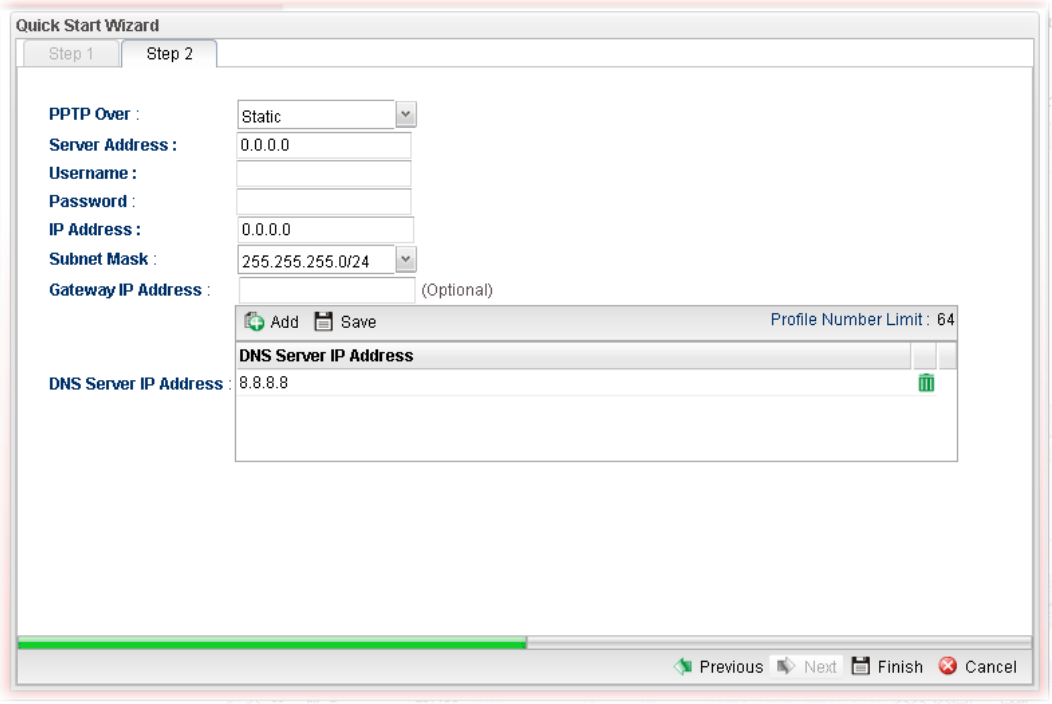
Item	Description
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

When you finished the above settings, please click **Finish**.

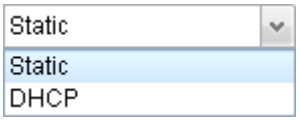
If PPTP is selected

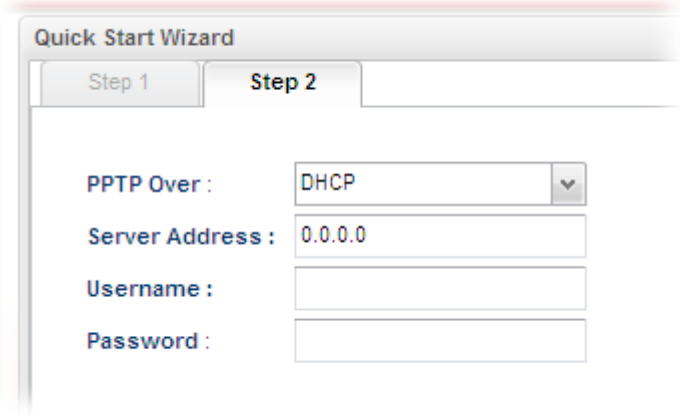
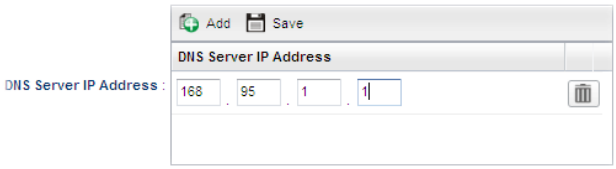
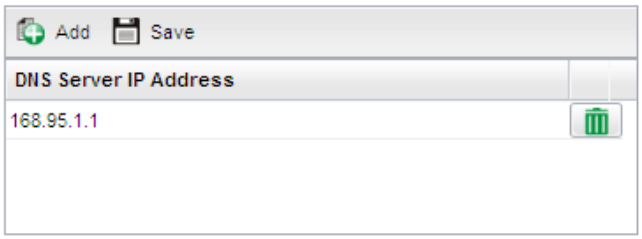
This mode lets user get the IP group information by a DSL modem with PPTP service from ISP. Your service provider will give you user name, password, and authentication mode for a PPTP setting. Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.

If your ISP offers you **PPTP** (Point-to-Point Tunneling Protocol) mode, please select **PPTP** for this router. Next, enter the settings provided by your ISP on the web page.

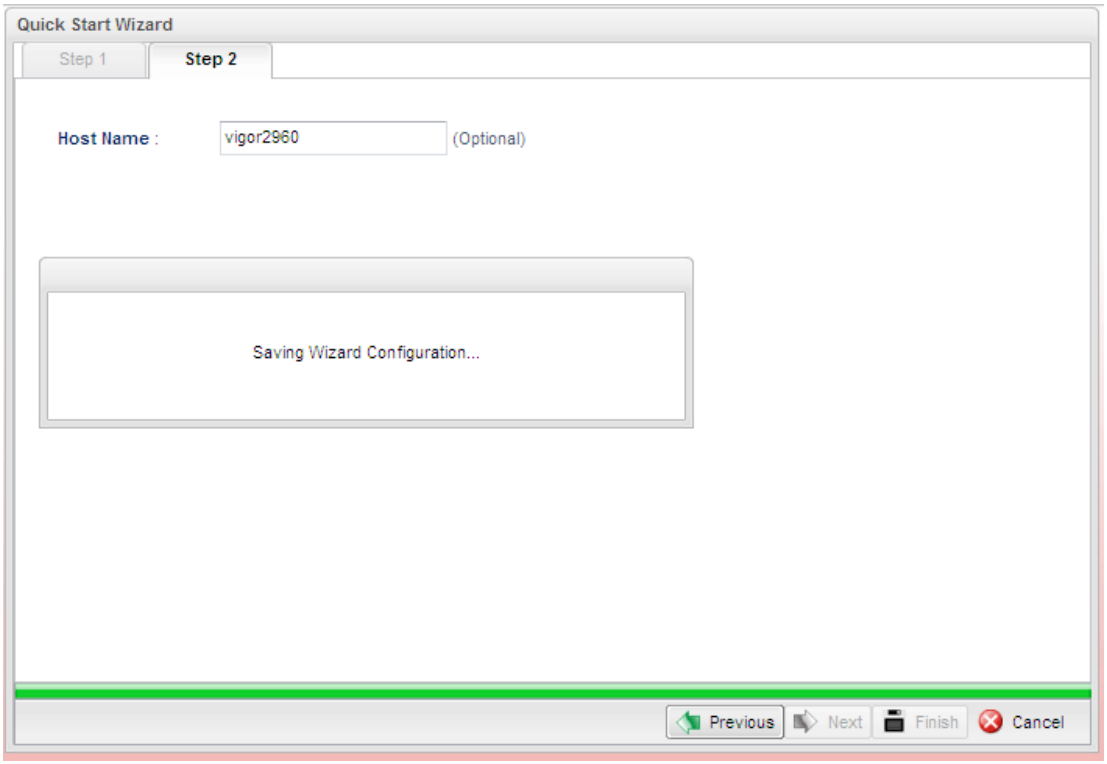


Available parameters are listed as follows:

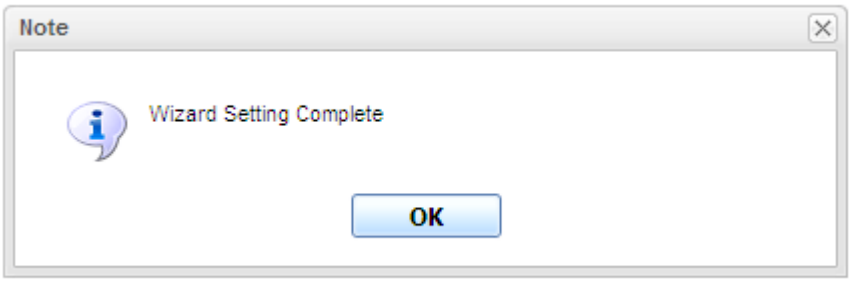
Item	Description
PPTP Over	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. **Please contact your ISP before you want to use this function.**  **Static** – specify the IP address. **DHCP** - obtain the IP address automatically.

	
Server Address	Type a remote IP address of PPTP server.
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile. - click it to remove the IP address if you are not satisfied with it.
DNS Server IP Address	To add a new IP address, simply place the mouse cursor on this filed. The following dialog will appear.  **Add** – Click this button to display the IP address field for adding a new IP address. **Save** – After finished the IP address configuration, click Save to save the setting onto the router.  – Click the icon to remove the selected entry.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

When you finished the above settings, please click **Finish**. Later, you can surf the Internet at any time.



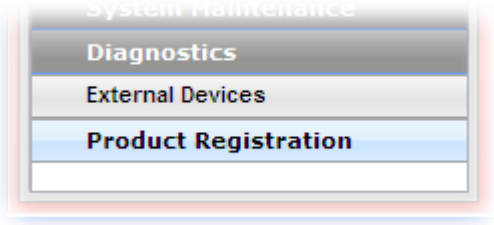
When the following screen appears, it means you have finished the Quick Start Wizard configuration.



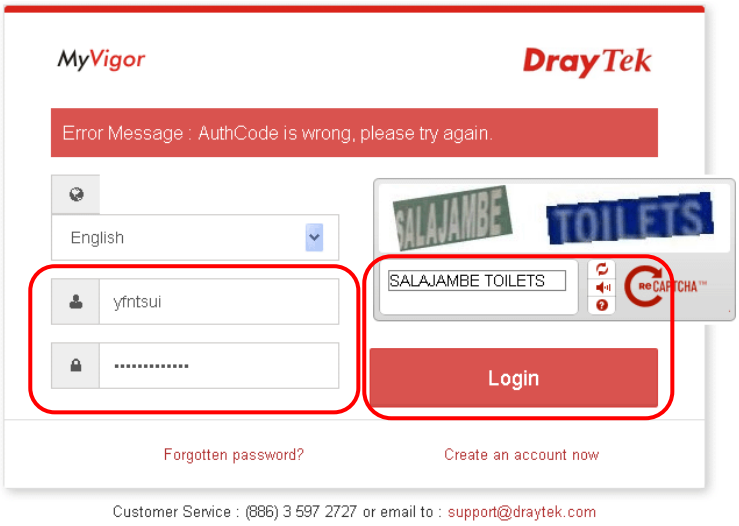
2.3 Register Vigor Router

Please follow the steps below to register the router.

1 Before using such function, please register your router online first. Log into the Web User Interface of Vigor3900 and click **Product Registration**.

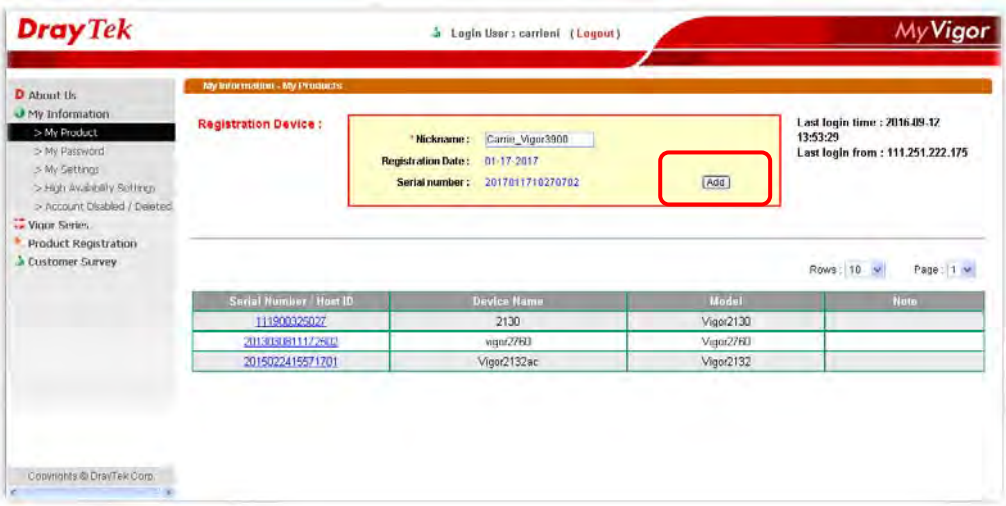


2 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



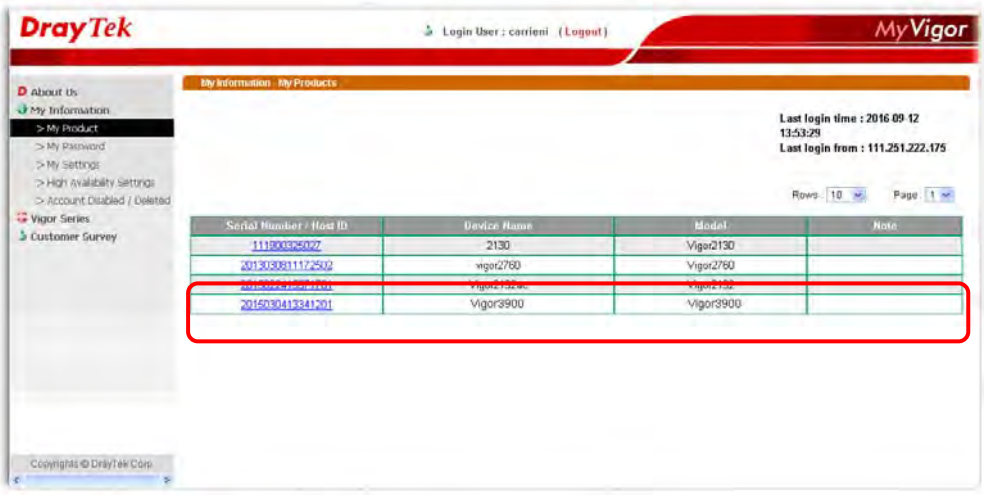
Note: If you haven't an accessing account, please create a new one first. Please **read the articles on the Agreement regarding user rights** carefully while creating a user account.

3 The following page will be displayed after you logging in MyVigor. From this page, please click **Add**.



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

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



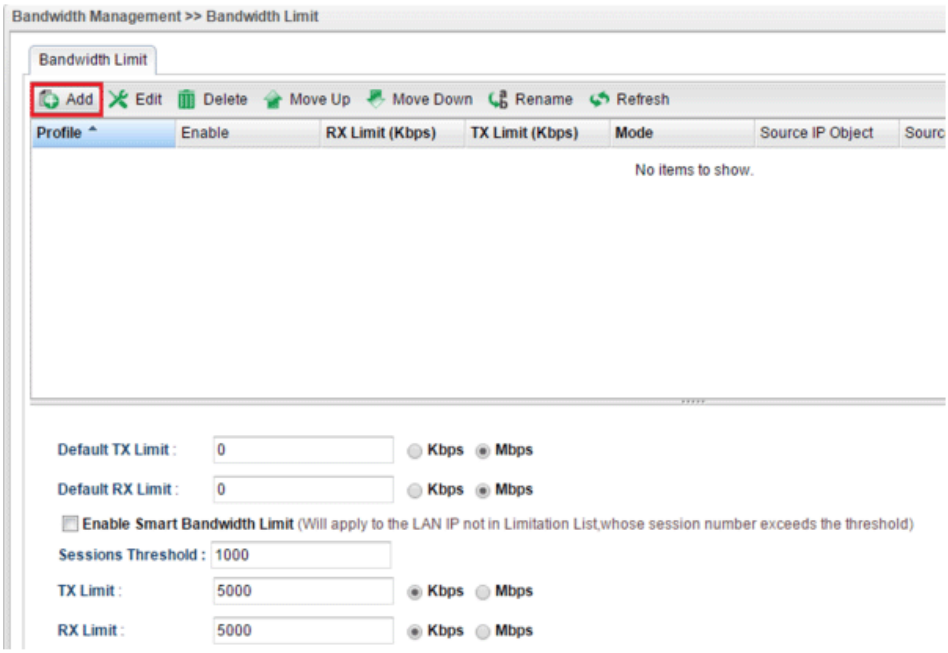
This page is left blank.

Chapter 3: Application and Tutorial

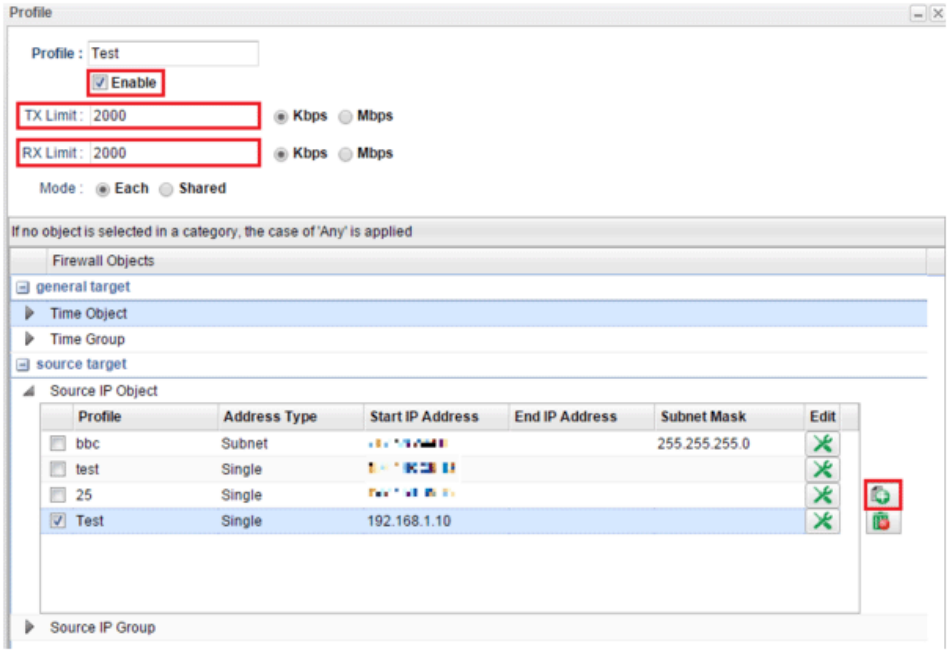
3.1 How to use Bandwidth Limit on Vigor3900?

Bandwidth Limit feature enables Network Administrator to limit the amount of data that a LAN client can transfer over a period of time. This will prevent the router's resources from being taken up by only a few LAN clients. We can also create customized Bandwidth Limit rule for each LAN client. This note demonstrates how to set up Bandwidth Limit with Vigor3900.

1. Go to **Bandwidth Management >> Bandwidth Limit** and click "**Add"** to start the configuration.

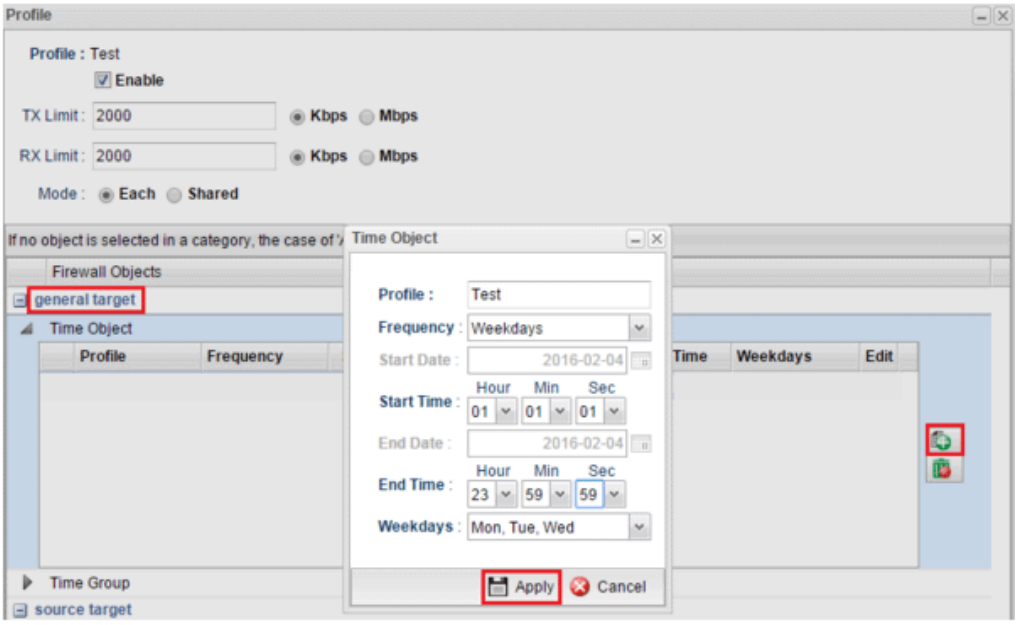


2. Then set up the details for the new rule.



- Enter the profile name.
- Enable the profile.
- Set the customized TX Limit and RX Limit for transmission rate.
- Enable Each or Shared Mode.
  - Each: Bandwidth Limit for each LAN Client
  - Shared: Bandwidth Limit for a group of LAN Clients
- Go to source target and click "+" icon to set the rule for particular IP address.
- Click **Apply** to save.

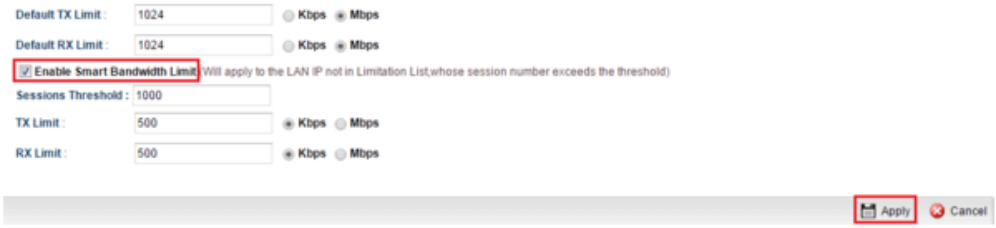
3. Bandwidth Limit can also be used with a time schedule to restrict LAN clients only at a certain time.



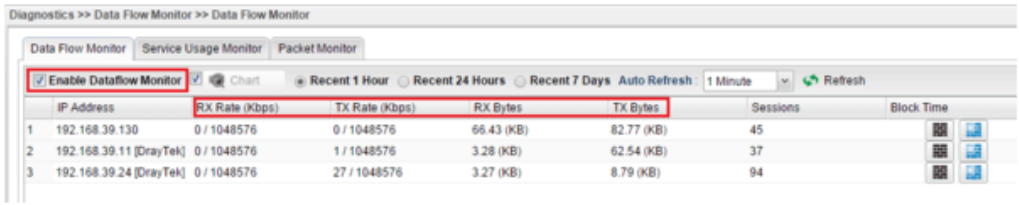
- Go to generate target >> Time Object.
- Click “+” icon to setup the time schedule.
- Set profile name, frequency, data and time.
- Click **Apply** to save.

4. Furthermore, you may enable Default Session Limit to apply session limit to all the other unspecified LAN clients.

5. We can also enable Smart Bandwidth Limit to restrict the bandwidth of unspecified LAN clients only when their session number is over the threshold.



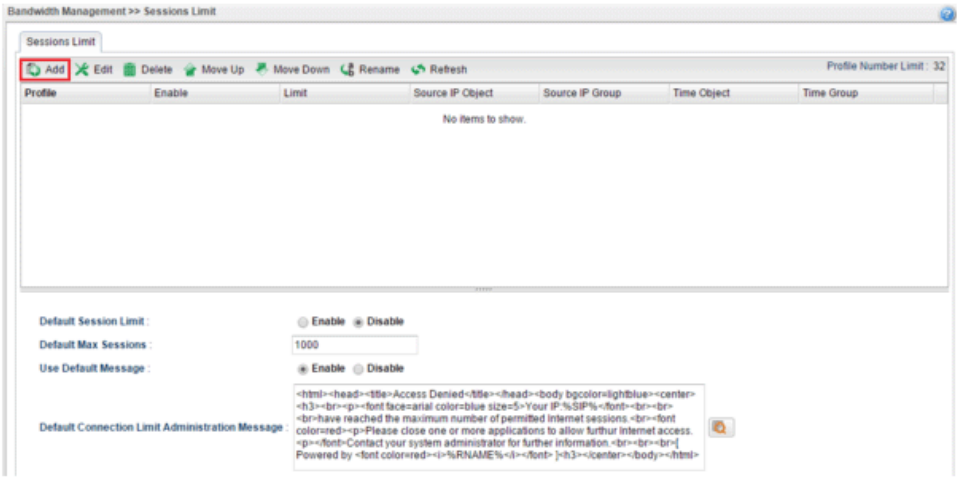
6. Data Flow Monitor can be used to check the status of Bandwidth Limit. Go to Diagnostics >> Data Flow Monitor and enable the monitor then we can check the transmission rate displayed on the screen.



3.2 How to use Session Limit on Vigor3900?

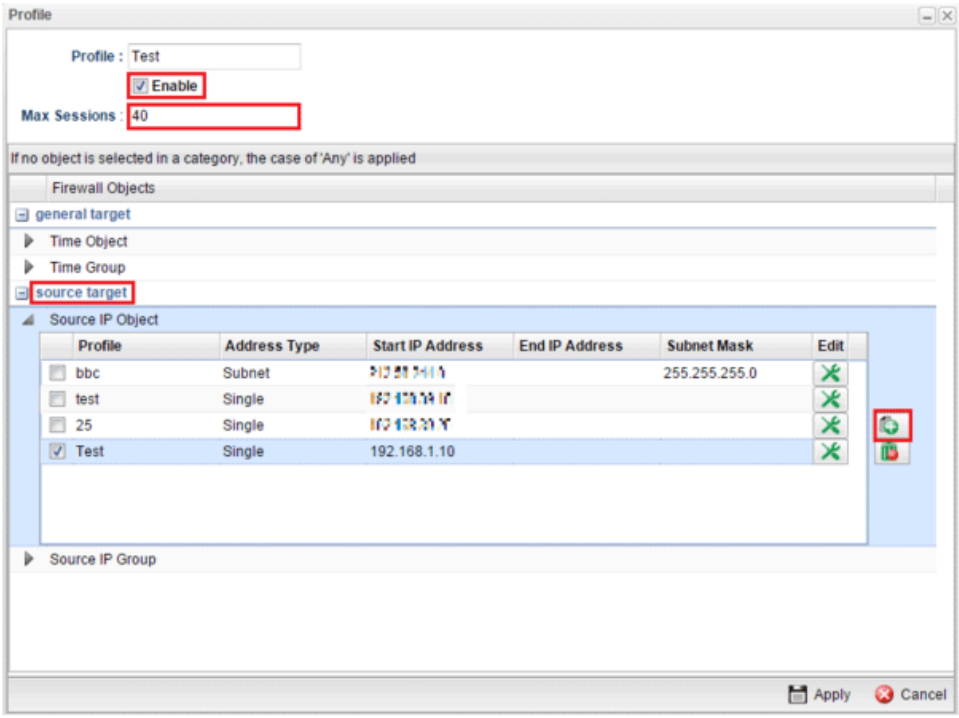
Session Limit feature enables Network Administrator to limit the number of sessions that a LAN client can use. This will prevent the router's resources from being taken up by, for example, P2P applications. We can also create customized Session Limit rule for each LAN client. This note demonstrates how to set up Session Limit with Vigor3900.

1. Go to **Bandwidth Management >> Session Limit** and click "**Add**" to create a new rule.



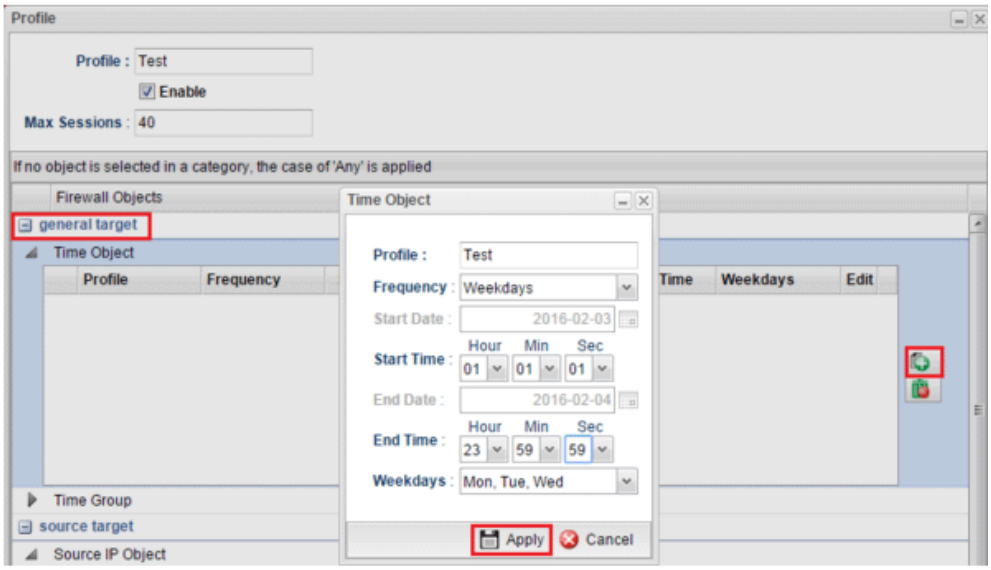
2. Then set up the details for the new rule.

- Enter the profile name.
- Enable the profile.
- Set the customized max session.
- Go source target and click the "+" icon to set the rule for particular IP address.



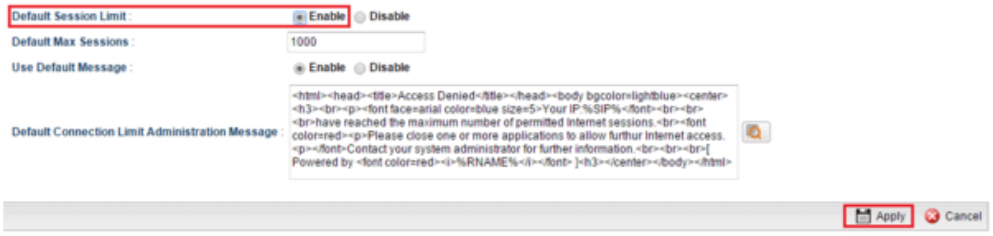
3. Session Limit can also be used with time schedule to restrict sessions only at a certain time.

- Go to generate target.
- Click “+” icon to setup the time schedule.
- Set profile name, frequency, date, and time.
- Click **Apply** to save.

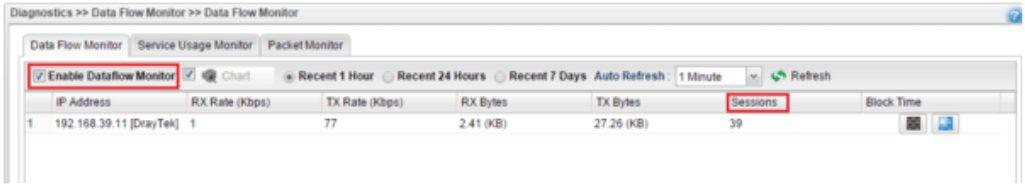


4. Furthermore, you may enable Default Session Limit to apply session limit to all other unspecified LAN clients.

- Enable Default Session Limit.
- Customize your Default Max Sessions.
- Click **Apply** to save.

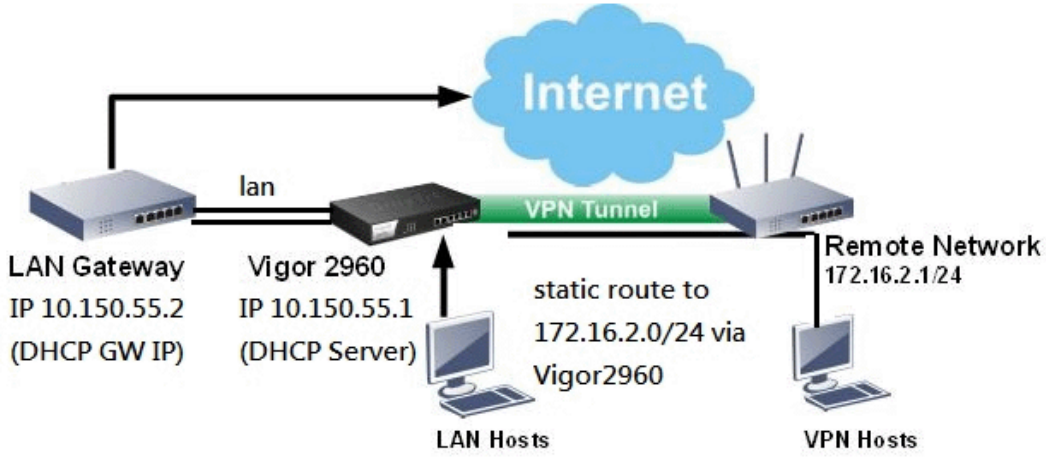


5. Go to **Diagnostics >> Data Flow Monitor** and enable the monitor then we can check how many sessions a specific LAN client use.

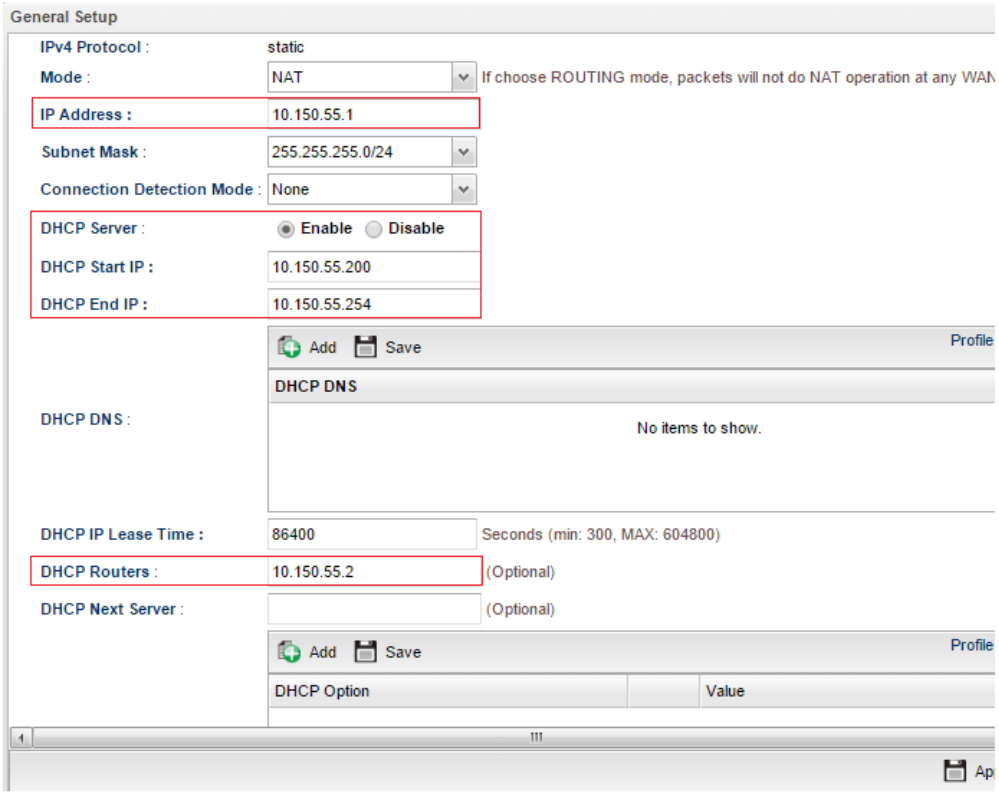


3.3 How to assign other IP as Gateway IP for LAN DHCP clients?

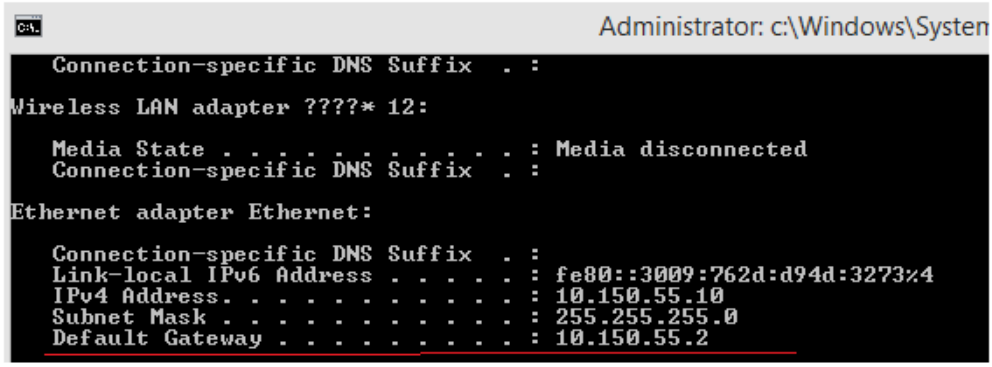
While Vigor3900 acts as DHCP Server, it will assign its LAN IP as the Gateway IP to DHCP clients by default. Then DHCP clients will use Vigor3900 as Default Gateway for accessing the Internet. However, in some cases, network administrator would like Vigor3900 to be the DHCP server but use another LAN router as Internet Gateway for LAN hosts. This document introduces how to achieve the purpose and below is the scenario:



1. Go to **LAN >> General Setup** >> lan1 click **Edit**, input the Gateway IP you'd like to assign to DHCP clients in **DHCP Routers** field and then **Apply** it.

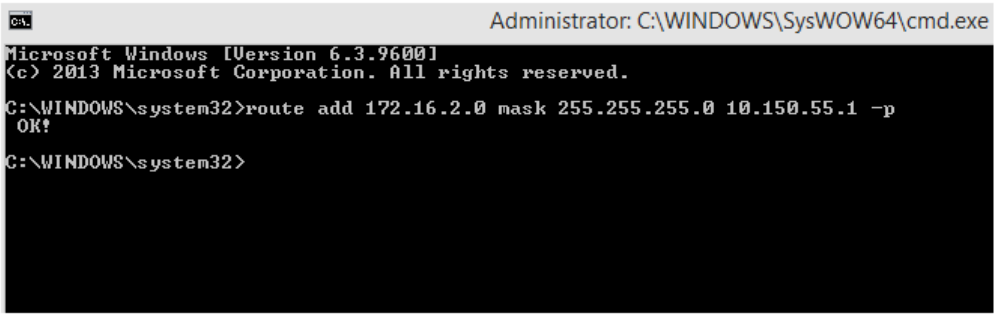


2. Then, run “cmd” to open Command Prompt on a PC (DHCP client), then use command “ipconfig/release” and “ipconfig/renew” to get an IP address again, and check if it obtains the configured Gateway IP.

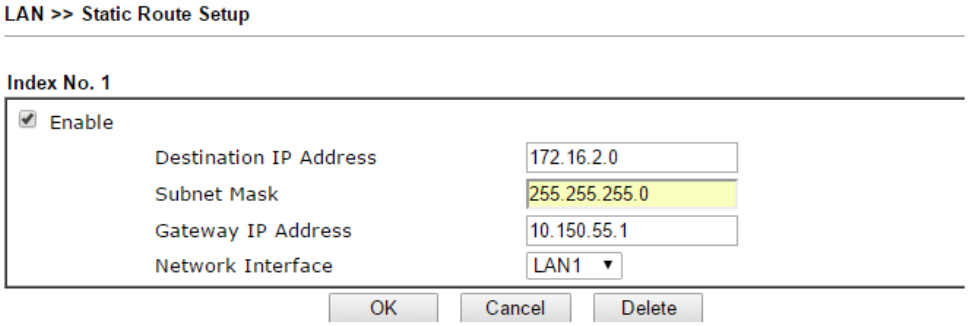


3. Now, this PC will access the Internet through Gateway IP 10.150.55.2! But what should we do if we want this PC to be able to access the remote VPN network connected through Vigor3900? It requires to specify Vigor3900's IP as the gateway to remote VPN Network, there are two ways to do this:

   a. Add Static Route on the PC by command “ip route add 172.16.2.0 mask 255.255.255.0 10.150.55.1 -p” Where 172.16.2.0 mask 255.255.255.0 is the IP address of remote VPN Network, 10.150.55.1 is the LAN IP of Vigor2960.

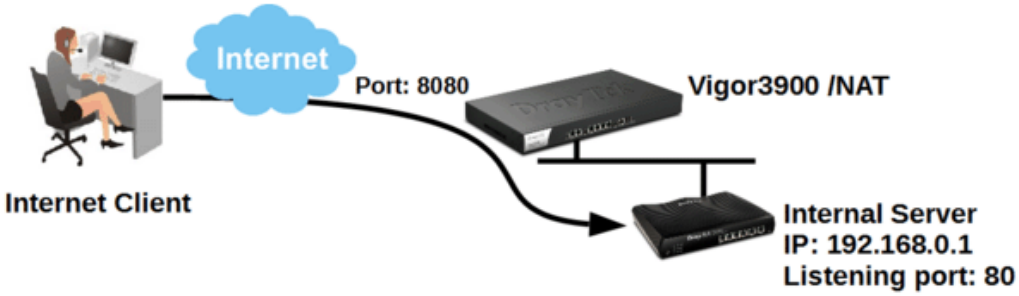


   b. Add a Static Route on the Gateway Router 10.150.55.2.

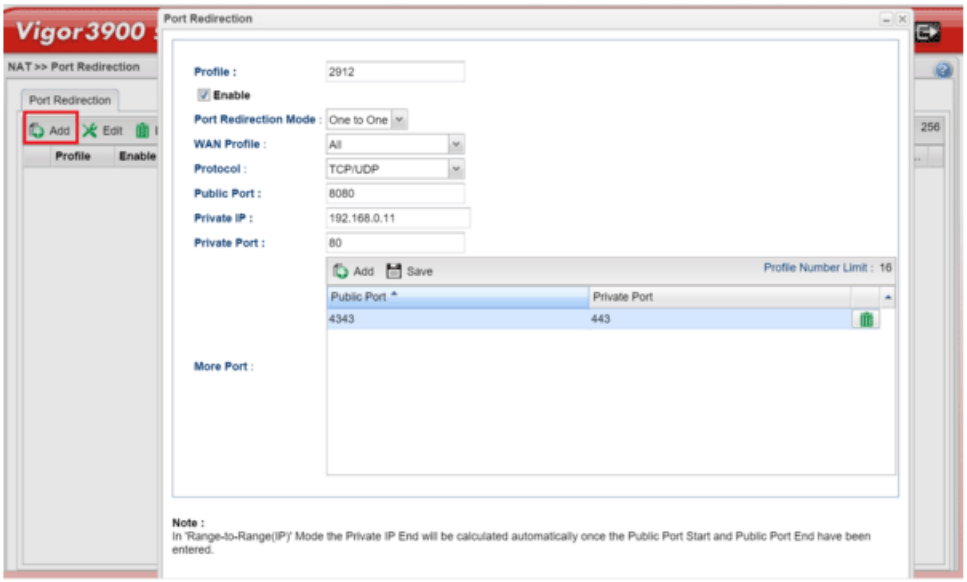


3.4 How to use Port Redirection on Vigor3900?

Port Redirection allows Internet clients to access server behind router on a certain port of router's WAN IP. This note is going to demonstrate how to use this feature with the following topology in Vigor3900.



1. Go to **NAT >> Port Redirection**, click **Add t**o create a profile.
2. Edit the profile.



- Give profile name and enable it.
- Select “One to One” as Port Redirection Mode.
- Select Protocol.
- Enter Public Port as the port to which Internet client should connect.
- Enter Private IP as the IP of the server on LAN.
- Enter Private Port as the port to which the server is listening.
- Click Add in More Port to allow more public ports to be redirected to other private ports.

3. Now, we can access the server behind NAT(Vigor3900) from Vigor3900's WAN IP with the specified port.

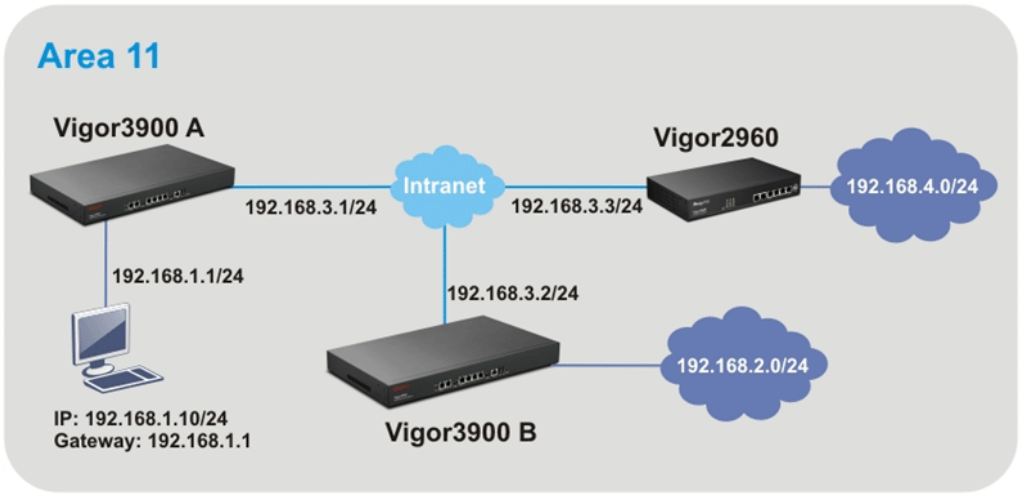
3.5 How to Configure OSPF?

OSPF (Open Shortest Path First) uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Both Vigor2960 and Vigor3900 support up to OSPF version 2(only for IPv4).

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

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

In the following example, a PC can go 192.168.2.0/24 and 192.168.4.0/24 without setting any Static Route. Refer to the OSPF topology diagram listed below.

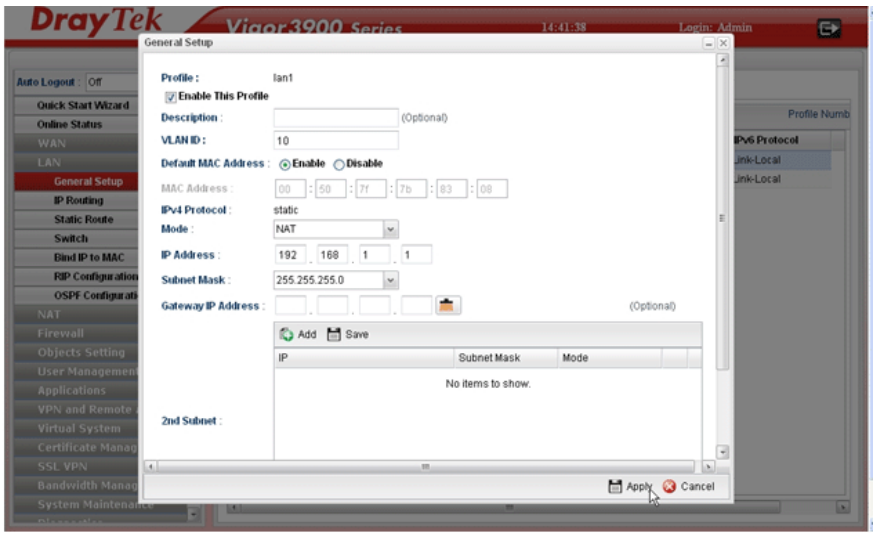


OSPF can place each router (e.g., Vigor3900A, Vigor3900B and Vigor2960 shown above) at the root of a tree and calculate the shortest path to each destination according to the cumulative cost to reach the destination.

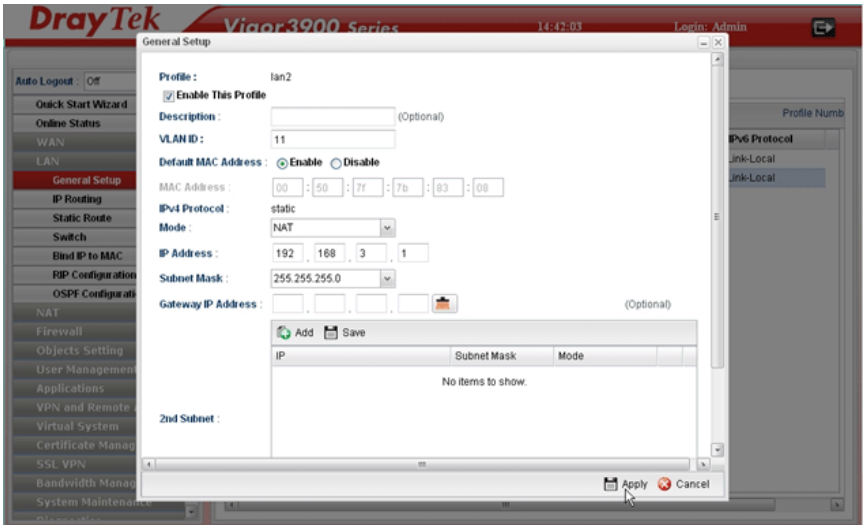
Each router has its own view of the topology and calculates its own SPF tree, even though all the routers build a shortest-path tree using the same link-state database.

Configuration for Vigor3900 A,

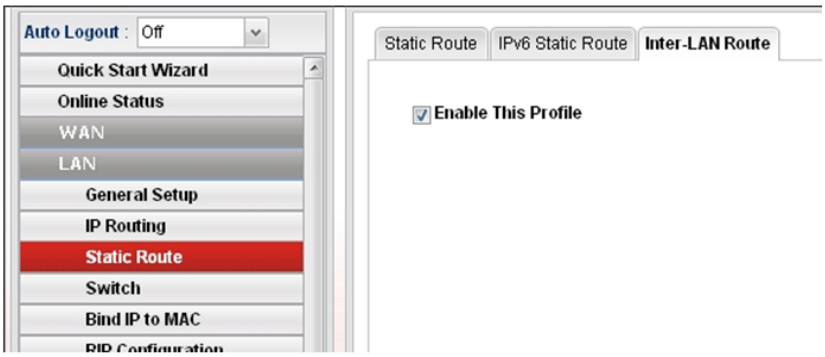
1. Open **LAN >> General Setup** to create a LAN (192.168.1.1/24) profile named lan1 with the settings shown below.



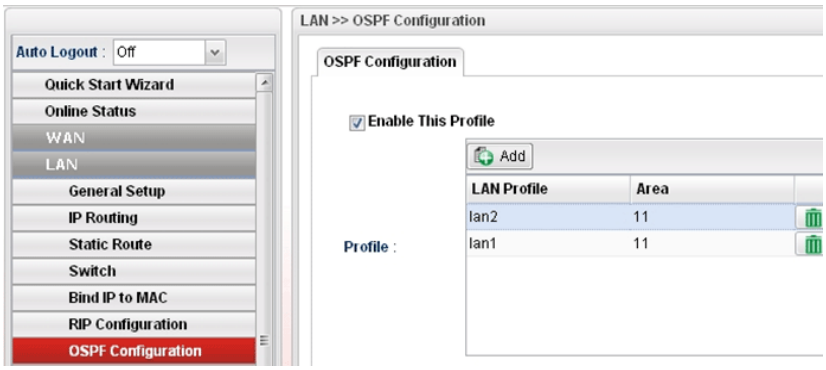
2. Next, continue to create a LAN (192.168.3.1/24) profile named lan2 with the settings shown below.



3. Open **LAN >> Static Route** and click the **Inter-LAN Route** tab to enable this profile.

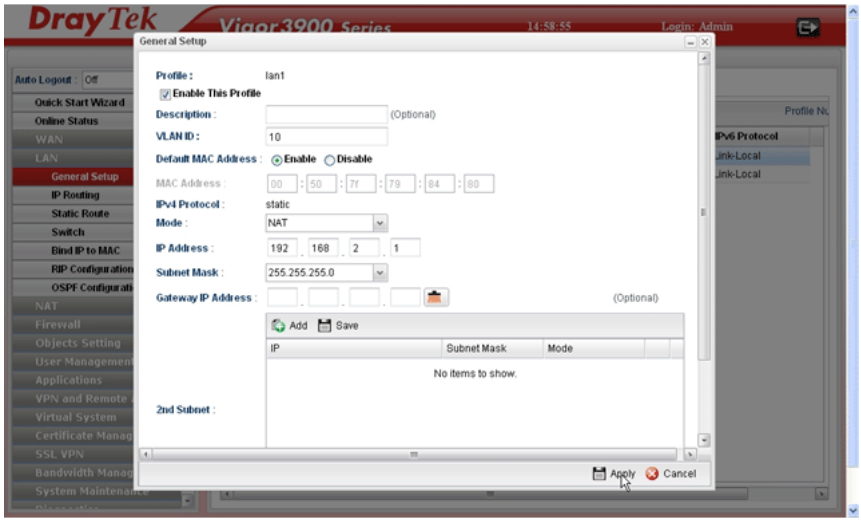


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

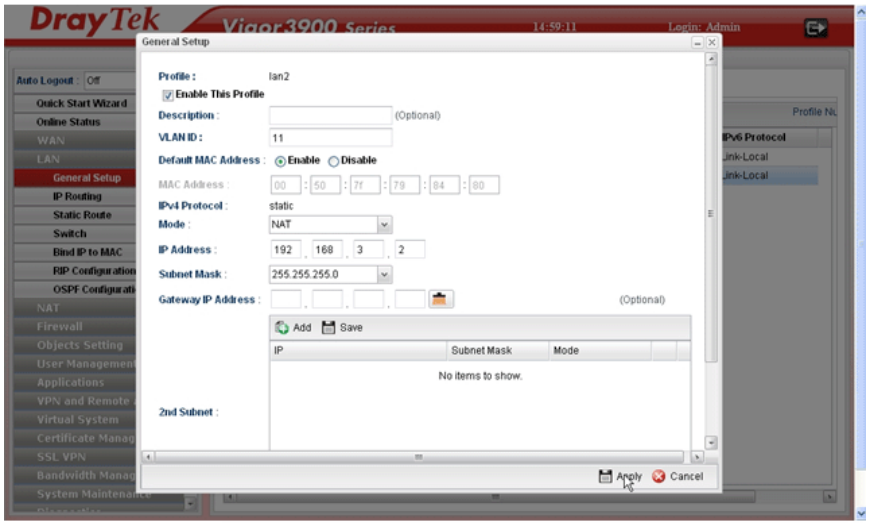


Configuration for Vigor3900 B,

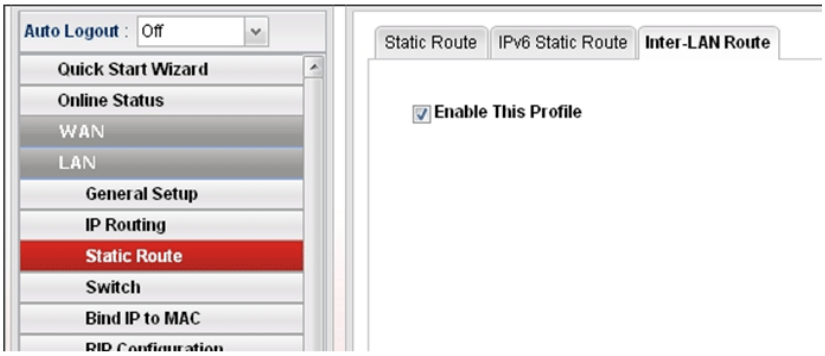
1. Open **LAN >> General Setup** to create a LAN (192.168.2.1/24) profile named lan1 with the settings shown below.



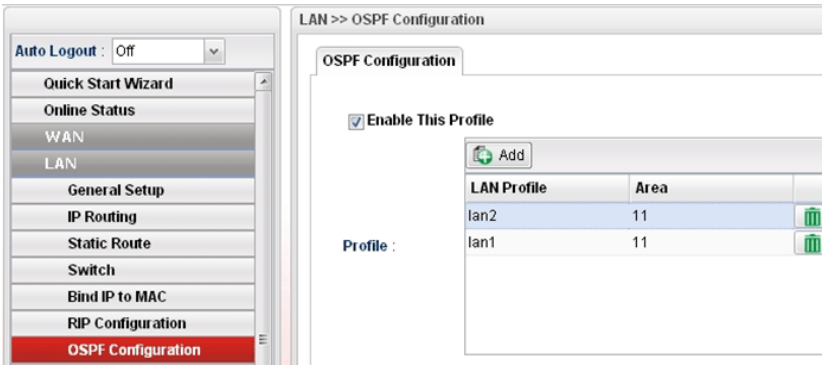
2. Next, continue to create a LAN (192.168.3.2/24) profile named lan2 with the settings shown below.



3. Open **LAN >> Static Route** and click the **Inter-LAN Route** tab to enable this profile.

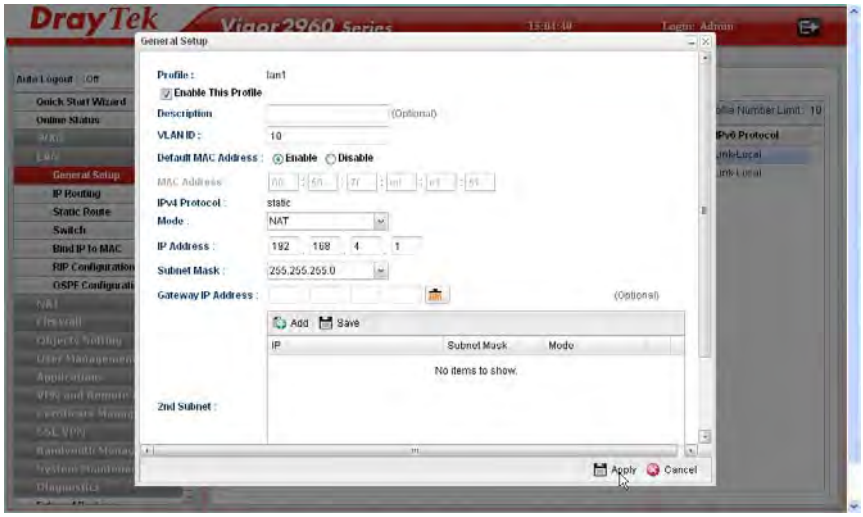


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

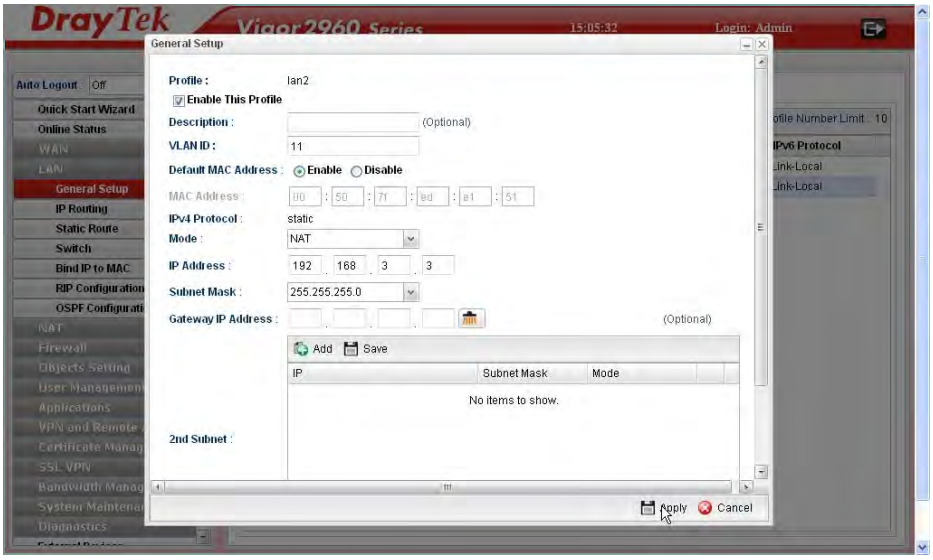


Configuration for Vigor2960,

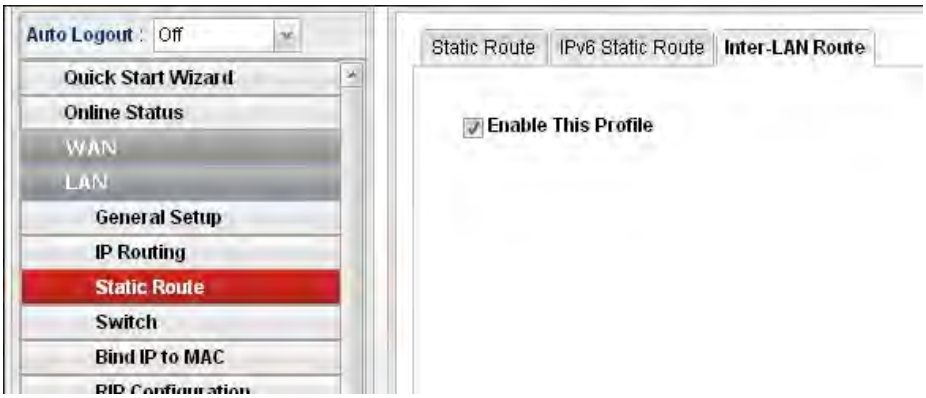
1. Open **LAN >> General Setup** to create a LAN (192.168.4.1/24) profile named lan1 with the settings shown below.



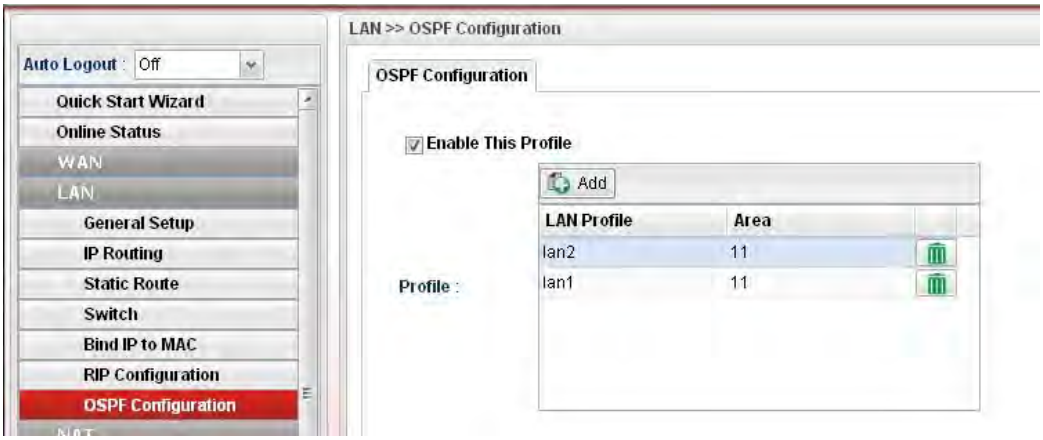
2. Next, continue to create a LAN (192.168.3.3/24) profile named lan2 with the settings shown below.



3. Open **LAN >> Static Route** and click the **Inter-LAN Route** tab to enable this profile.

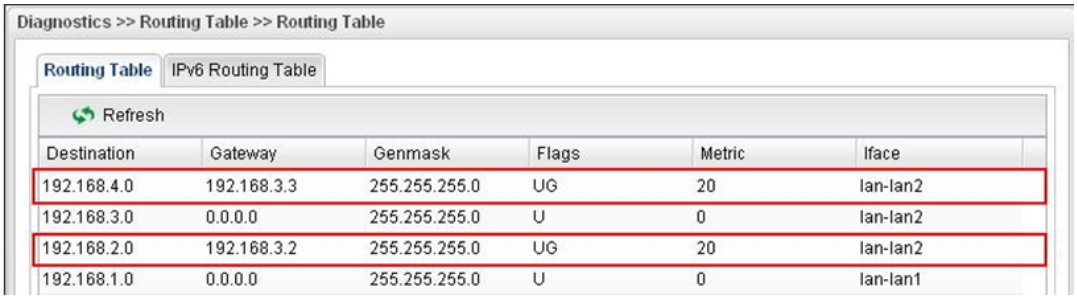


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

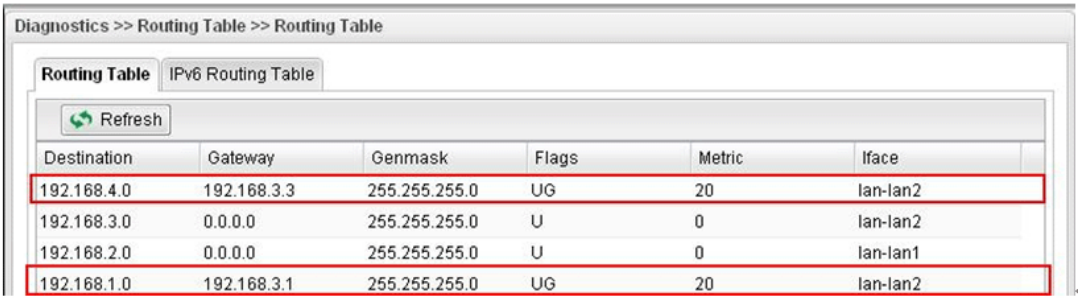


5. After setting, check the routing information (marked with red line) which is created by OSPF.

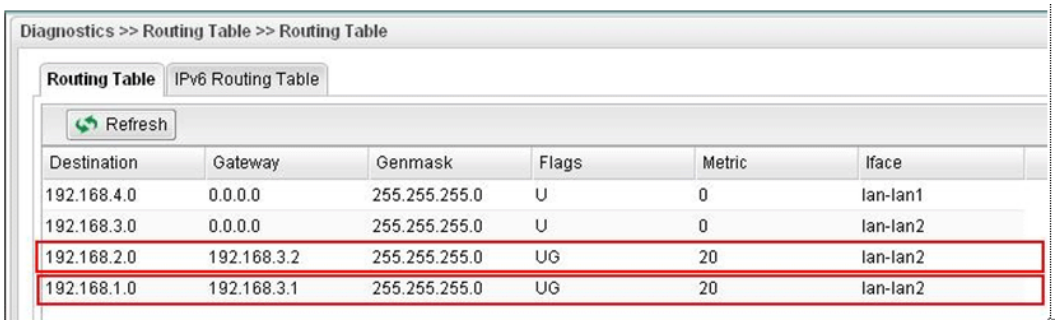
Routing information for Vigor3900 A



Routing information for Vigor3900 B

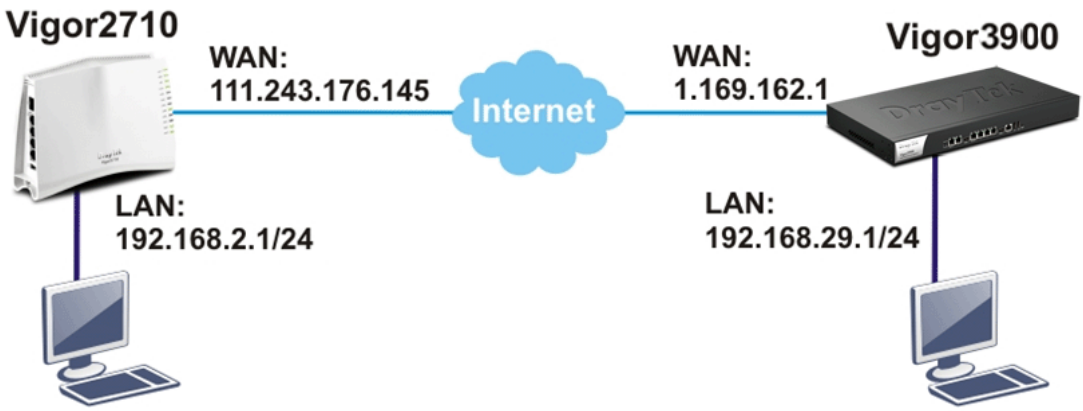


Routing information for Vigor2960



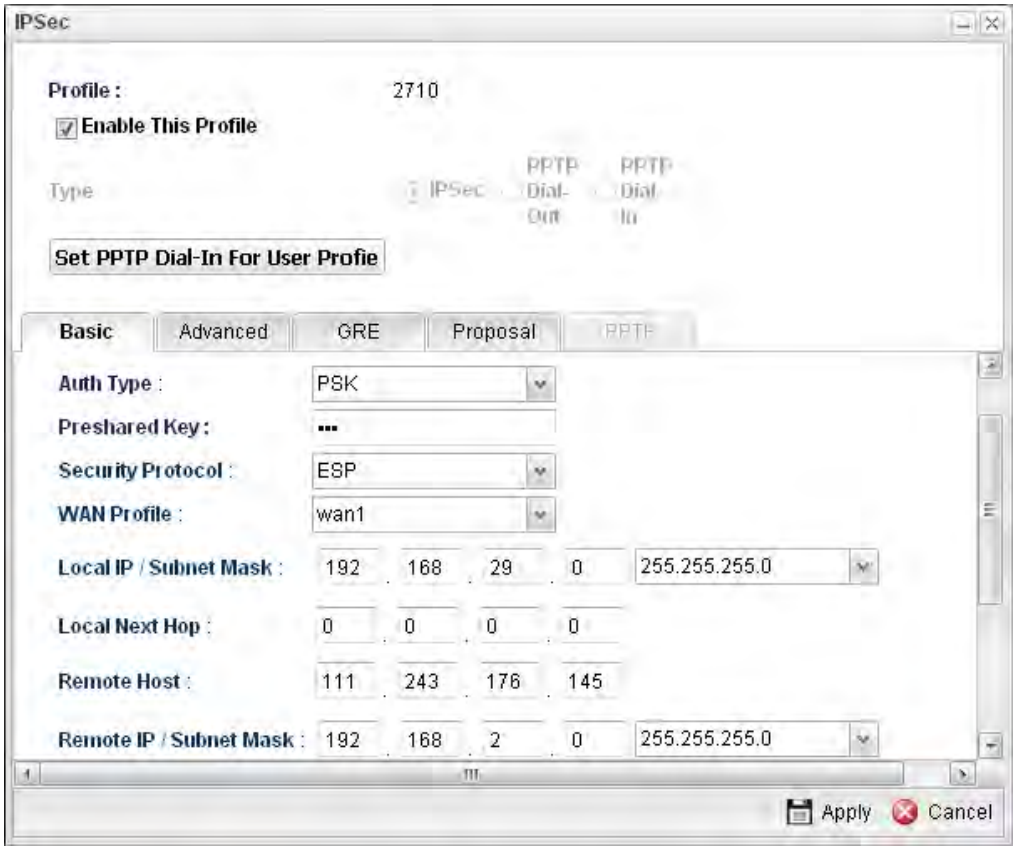
3.6 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode)

Here provides an example about LAN to LAN IPSec tunnel established between Vigor3900 and Vigor2710.



Configuring Vigor3900

1. Access into the Web User Interface of Vigor3900 and open **VPN and Remote Access >> LAN to LAN Profiles** to add a new VPN configuration.

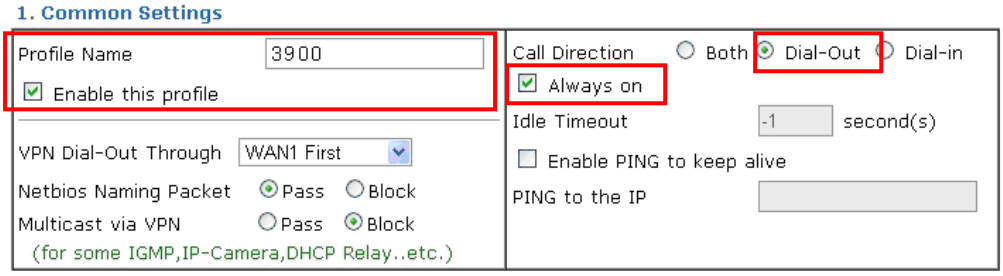


Type the Pre-shared key and choose a WAN Profile. Specify Local IP/Subnet Mask with 192.168.29.0/24. The Remote Host should be Vigor 2710's WAN IP address; and the Remote IP/Subnet Mask should be192.168.2.0/24.

2. Click **Apply** to save the settings and return to previous page.

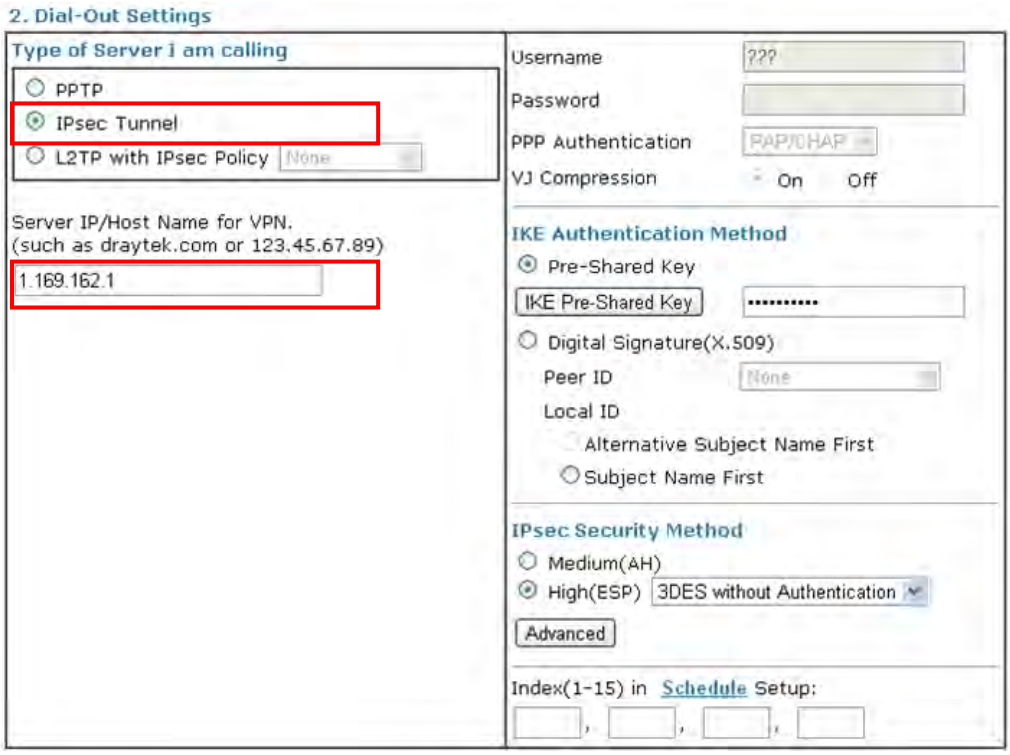
Configuring Vigor2710

1. In Vigor2710, it is necessary to build two VPN connections (for two WANs) to connect with Vigor3900. Please open the Web User Interface of Vigor2710 and open **VPN and Remote Access >> LAN to LAN**.

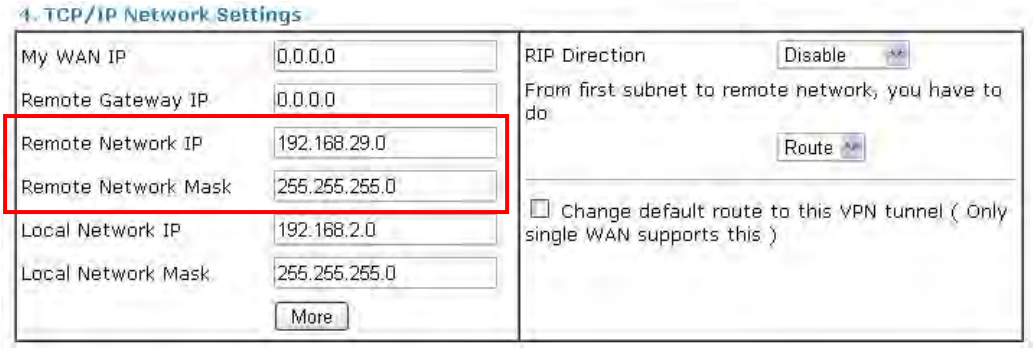


- First, please type the name of such VPN connection in the field of Profile Name (e.g., 3900).
- Check the box of **Enable this profile**.
- Choose **Dial-Out** as **Call Direction** and check the box of **Always on**.

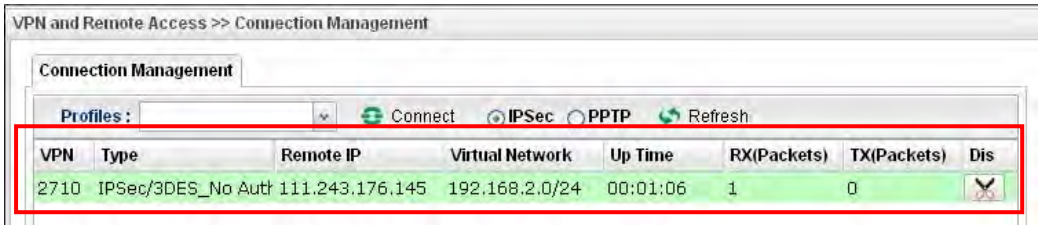
2. For **Dial-Out Settings**, please choose **IPSec Tunnel** and type WAN IP address of Vigor3900 in the field of **Server IP/Host Name for VPN** (e.g., 1.169.162.1). Type the same IKE Pre-Shared Key configured in Vigor3900.



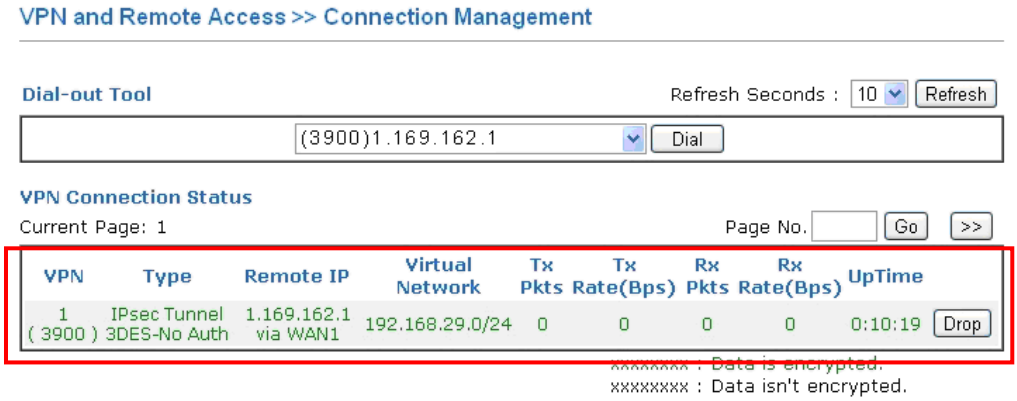
3. For the role of Vigor2710 is dialing-out, please skip Dial-In setting. Type the **Remote Network IP** and **Remote Network Mask** of Vigor3900 to complete configuration.



4. Please check if the VPN connection is built successfully in both devices respectively. For Vigor3900, open **VPN and Remote Access>>IPSec>>Status** for viewing the result.

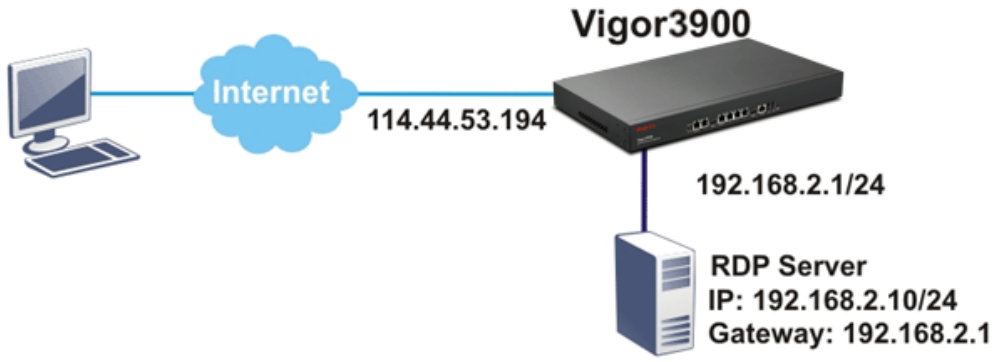


As to Vigor2710, please open **VPN and Remote Access>>Connection Management** to confirm the result.



3.7 How to run RDP service in the browser via logging in 3900's HTTPS Server?

Remote Desktop Protocol (RDP) is a protocol designed for secure communications in networks using Microsoft Terminal Services. An easy way is provided to establish connection between the router and the RDP Server via any browser.



1. Open the Web User Interface of Vigor3900.
2. Enable the HTTPS service from **System Maintenance >> Access Control** by clicking **Enable** for **HTTPS Allow** and type **443** as the value of **HTTPS Port.**

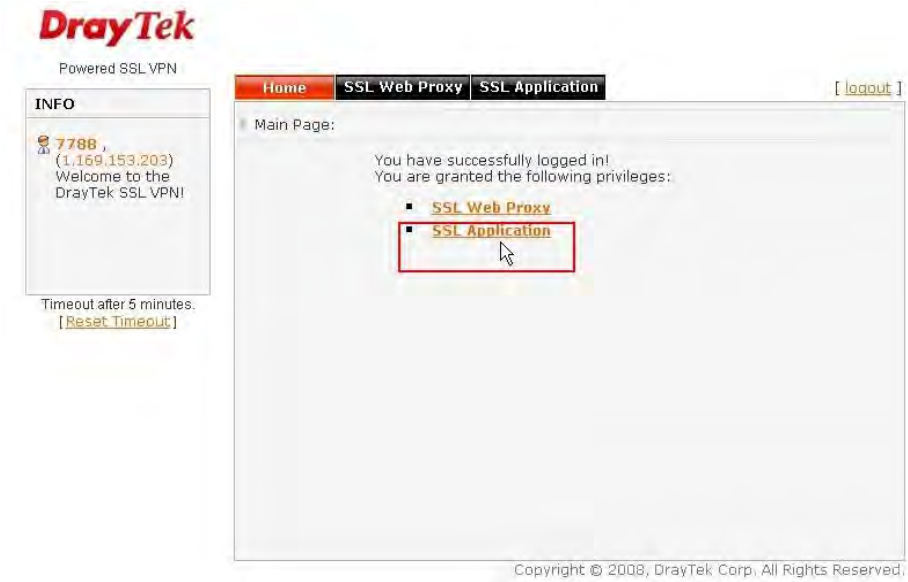
3. Open **SSL VPN >> SSL Application** and click the **RDP** tab to create a profile named "Win7". Type IP address, Port number, and Screen Size as you want, then click **Apply** to save the settings.

4. Open **User Management >> User Profile** to create a new profile named "7788". Set the **Password** as 7788 and choose the profile of **Win7** as **SSL Application (RDP)**. Click **Apply**.

5. Logout Vigor3900.

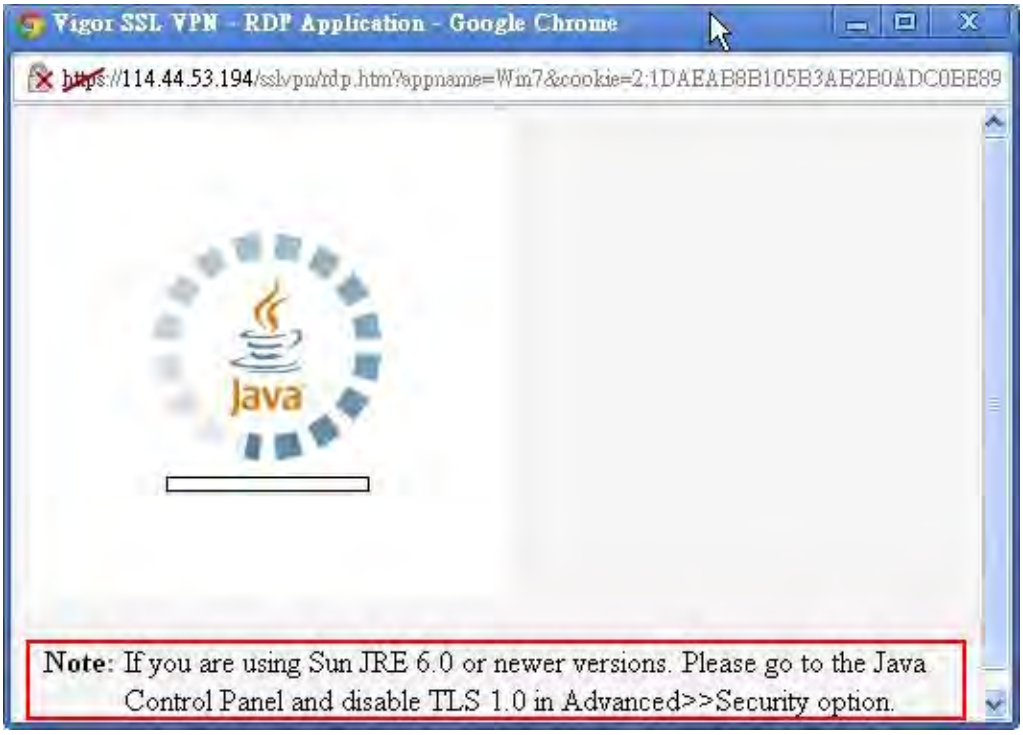
6. Login Vigor3900 HTTPS Server with 7788 for both Username and Password.

7. A screen like the following figure will appear. Simply click the **SSL Application** link.



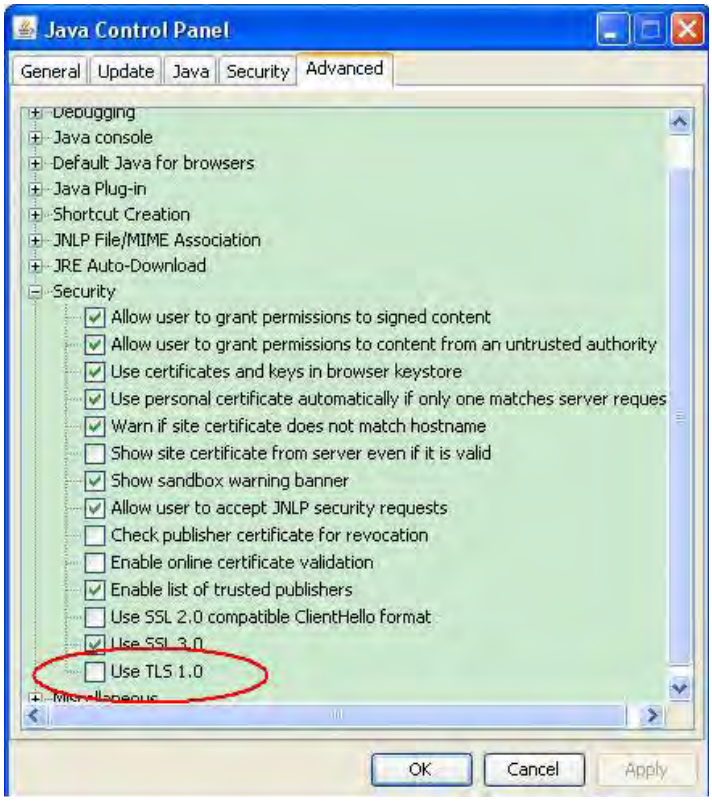
8. In the following screen, click **Connect** for connecting to Win7, the RDP server.

9. After that, you can access into Windows 7 via a browser. Note the message below the window. In which, TLS means Transport Layer Security.



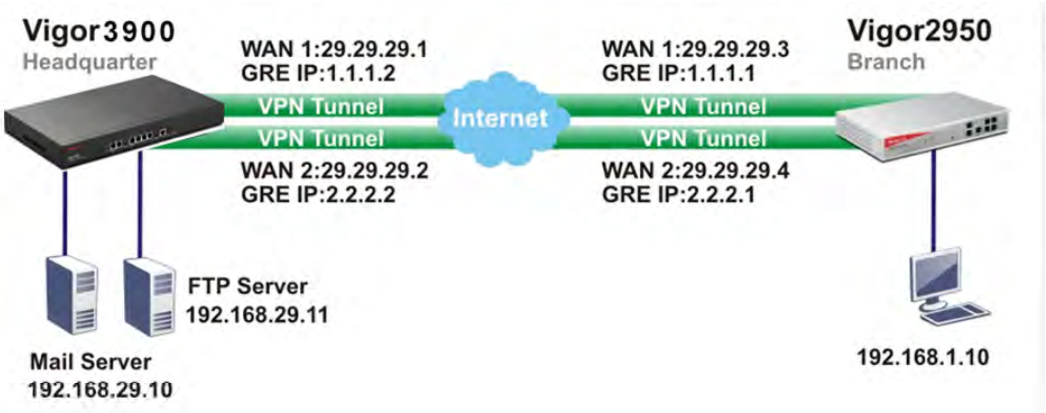
Troubleshooting

If you have installed Java Runtime Environment edition 6 but still cannot establish the connection, please make sure you have disabled "**Use TLS 1.0**" in the **Java Control Panel** as figure shown below. Then, try to connect again.



3.8 How to Configure VPN Load Balance between Vigor3900 and Other Router

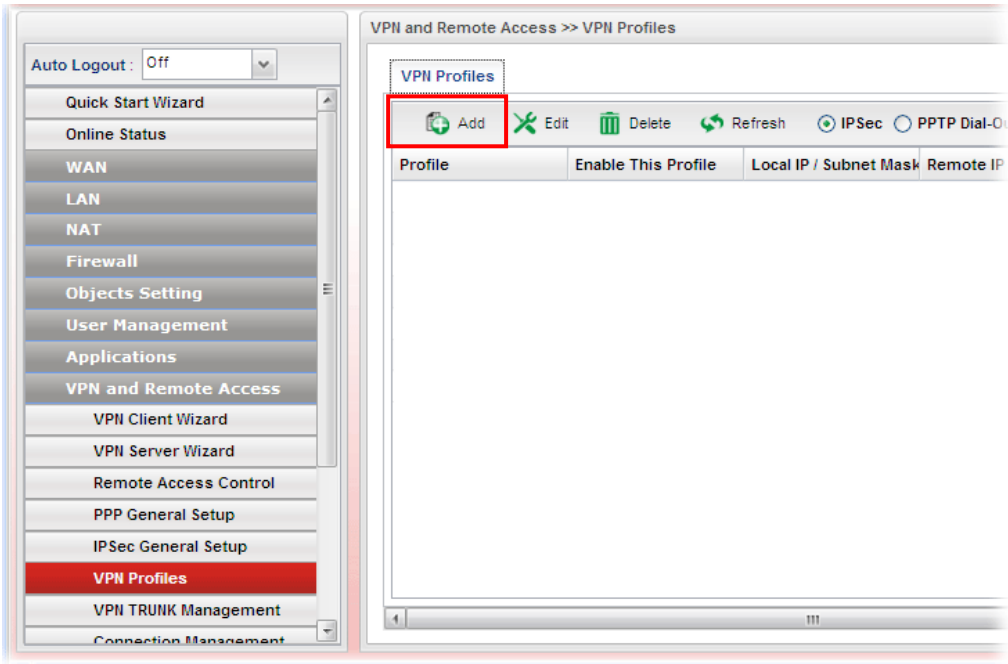
The staff in branch office can access into mail server/FTP server installed in the headquarters via VPN Load Balance tunnels. Refer to the following figure.



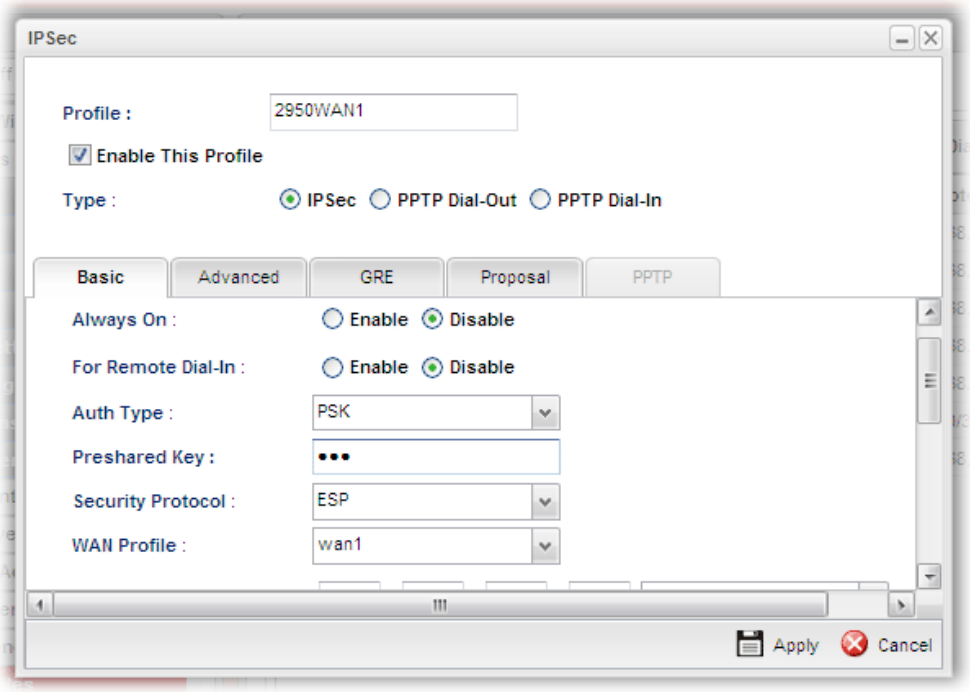
Vigor3900 allows users to build VPN load balance connection between Vigor3900 and other router. Take Vigor2950 for an example. There are two WANs on Vigor2950 and two WANs on Vigor3900. We will build VPN connection with load balance between Vigor3900 and two WANs of Vigor2950 respectively.

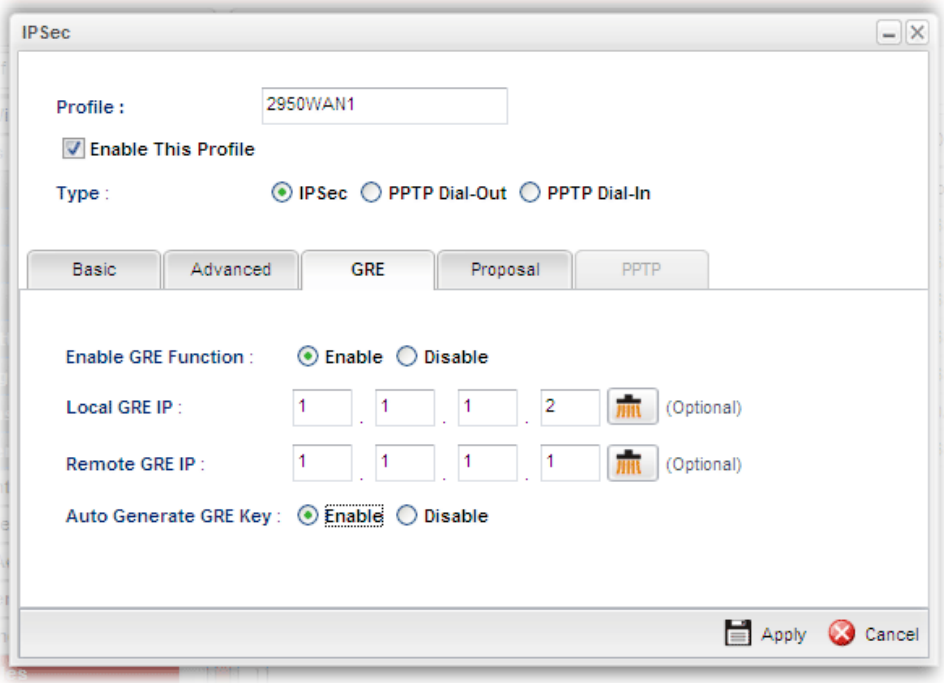
Configuring Vigor3900

1. Access into the Web User Interface of Vigor3900 and open **VPN and Remote Access >> VPN Profiles** to add new VPN profiles. Click **Add**.

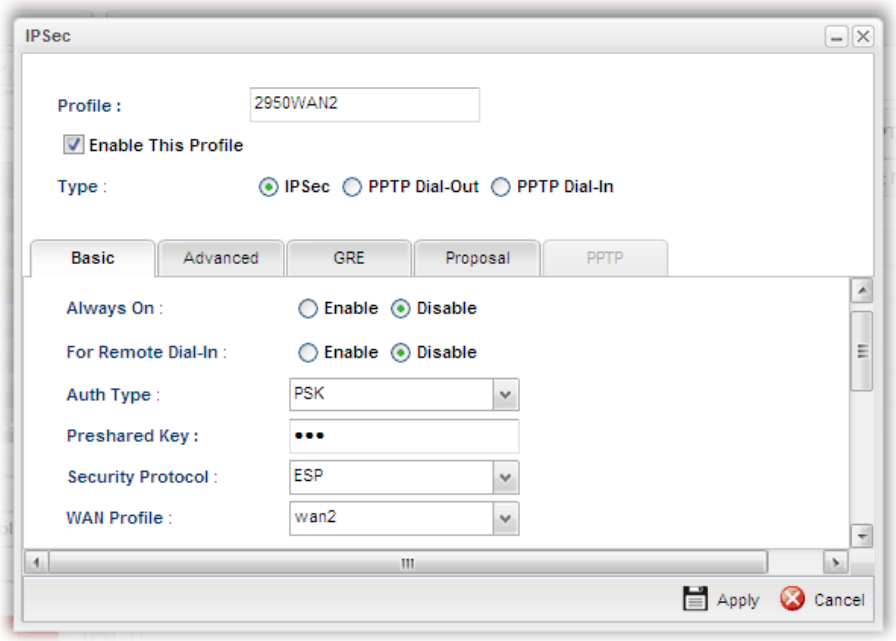


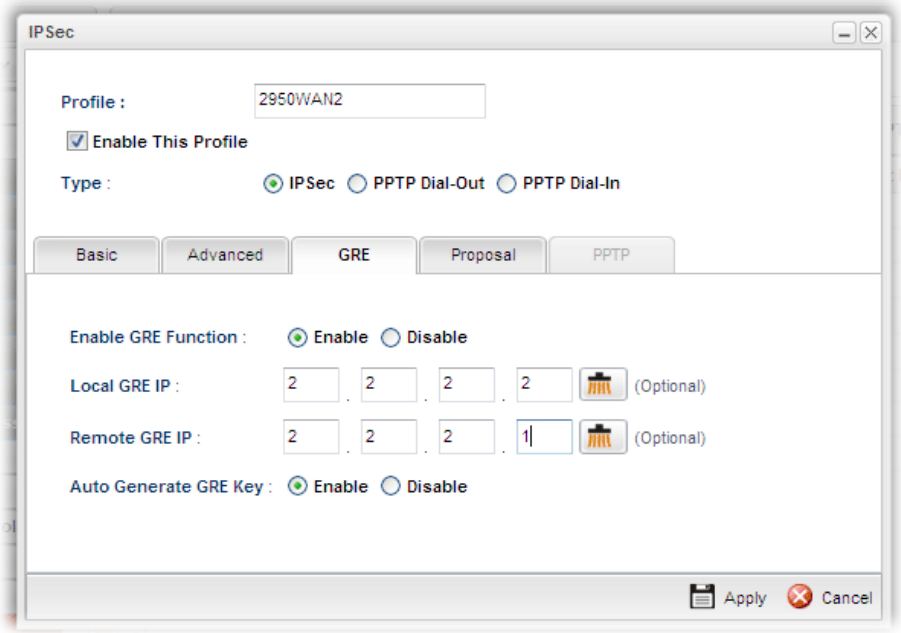
2. Create a profile for WAN 1 (named 2950WAN1). Type the settings as shown below:





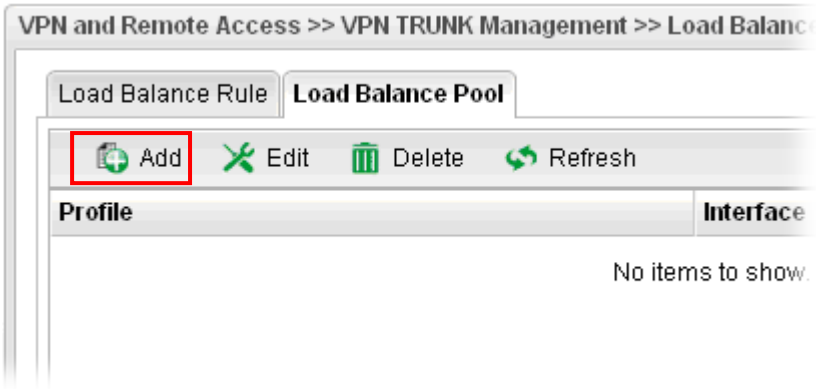
3. Click **Apply** to save the settings and exit the dialog.
4. Create a profile for WAN 2 (named 2950WAN2).



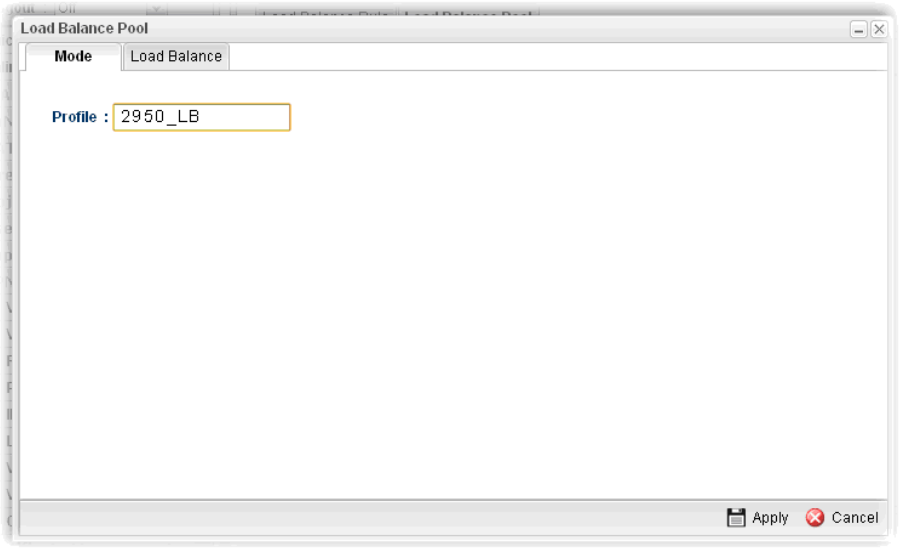


5. Click **Apply** to save the settings and exit the dialog.

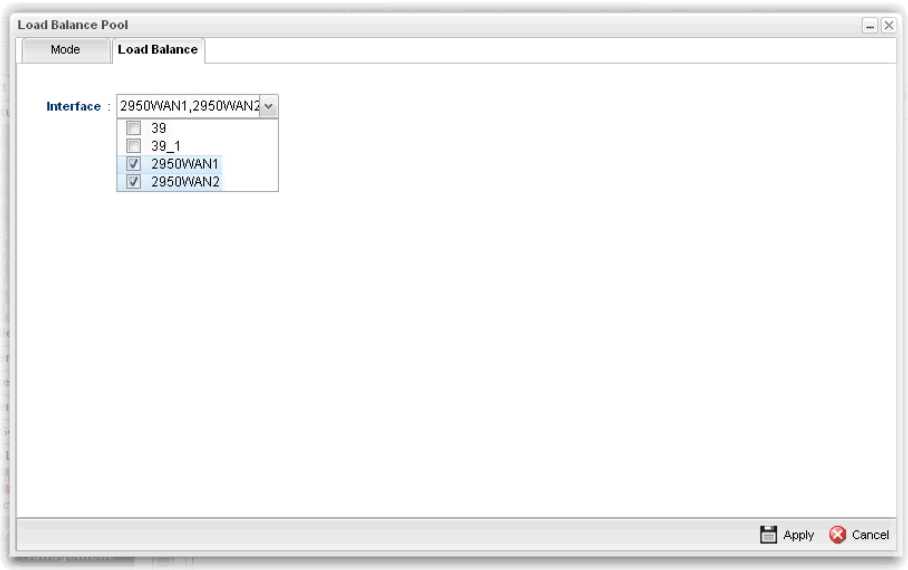
6. Open **VPN and Remove Access>>VPN Trunk Management** and click the **Load Balance Pool** tab. Click **Add** to add a Load Balance Pool profile.



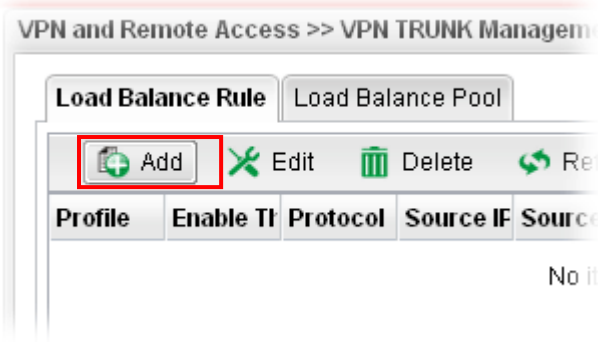
7. The following window will pop up. Give a name for the profile.



8. Click the **Load Balance** tab. Select the IPSec GRE profiles (e.g., 2950WAN1) set for Vigor2950 then click **Apply**.

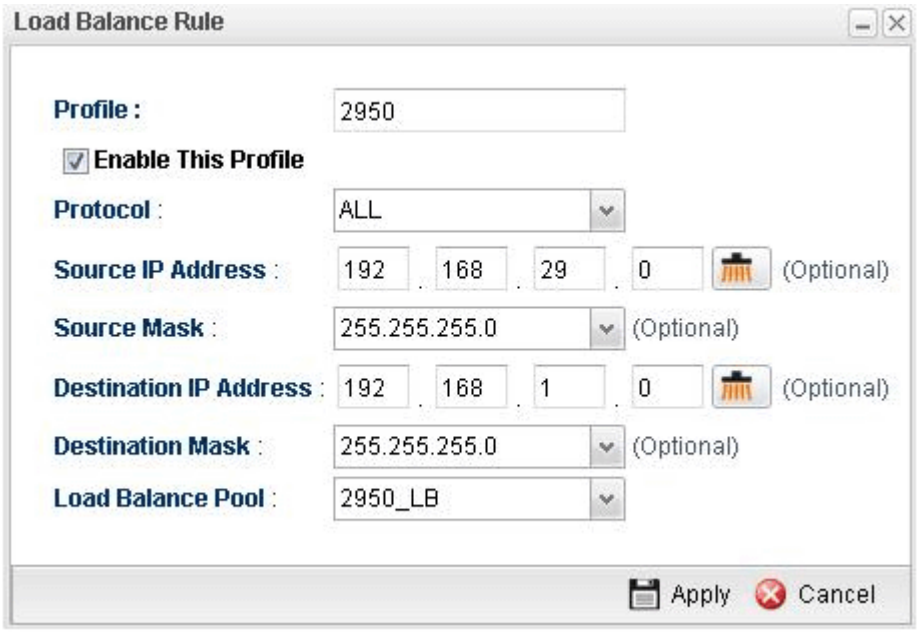


9. Click the **Load Balance Rule** tab and click **Add** to add a Load Balance rule profile.



10. Enable this profile and input the following settings then click **Apply**.

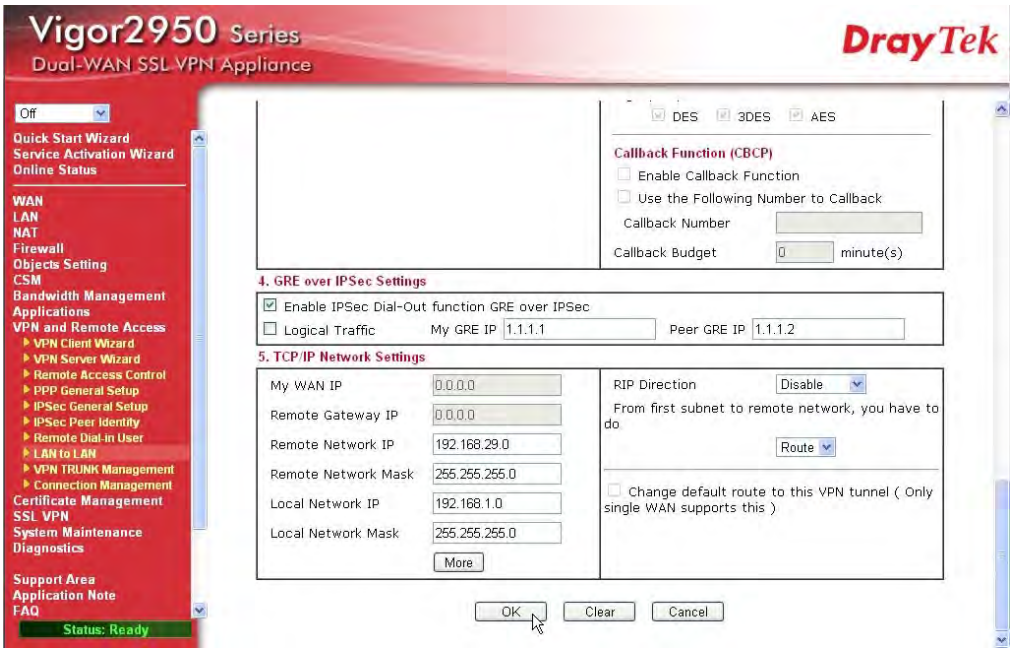
    Type the local network IP address and Mask of Vigor3900 as Source IP Address and Source Mask; type the network IP and Mask of Vigor2950 as Destination IP Address & Destination Mask. Select the Load Balance Pool profile (e.g., 2950_LB) set for Vigor2950.



Configuring Vigor2950

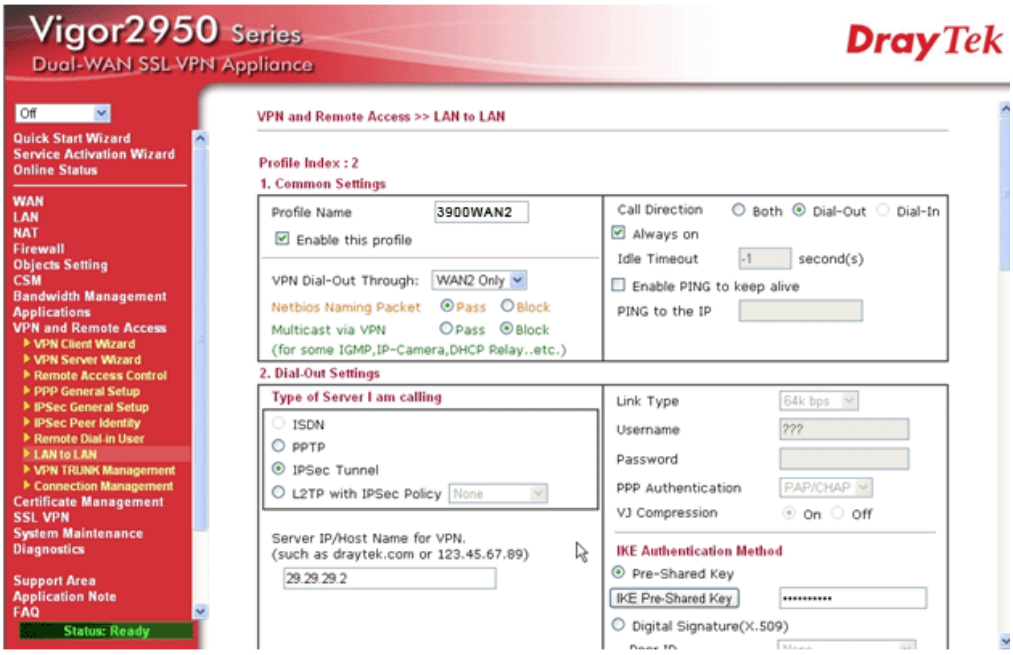
1. In Vigor2950, it is necessary to build two VPN connections (for two WANs) to connect with Vigor3900. Please open the Web User Interface of Vigor2950 and open **VPN and Remote Access >> LAN to LAN**.

- First, please type the name of such VPN connection in the field of Profile Name (e.g., 3900WAN1).
- Choose **WAN1 Only** as **VPN Dial-Out Through** setting to specify which WAN interface will be used for building VPN connection.
- Choose **Dial-Out** as **Call Direction** and check the box of **Always on**.
- For **Dial-Out Settings**, please choose **IPSec Tunnel** and type WAN IP address of Vigor3900 in the field of **Server IP/Host Name for VPN** (e.g., 29.29.29.1). Type the same IKE Pre-Shared Key configured in Vigor3900.
- For the role of Vigor2950 is dialing-out, please skip Dial-In setting. In this example, please type the 1.1.1.1 in the field of **My GRE IP**; and type the GRE IP address 1.1.1.2 in the field of **Peer GRE IP**.



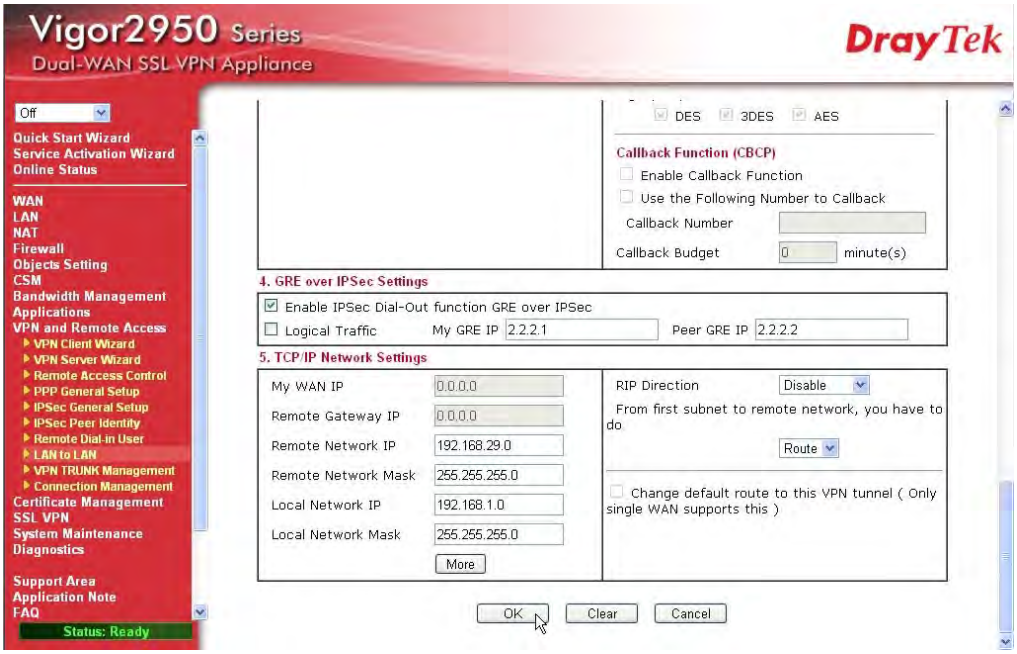
- Please type the network IP address and subnet of Vigor3900 in the field of Remote Network IP and Remote Network Mask. Type the network IP address and subnet of Vigor2950 in the field of Local Network IP and Local Network Mask.

2. Continue to set the second VPN connection (profile name is 3900WAN2). The first VPN tunnel will be used by WAN1 of Vigor2950. The second VPN tunnel will be configured for the WAN2 of Vigor2950. Therefore, please choose **WAN2 Only** for **VPN Dial-Out Through**.



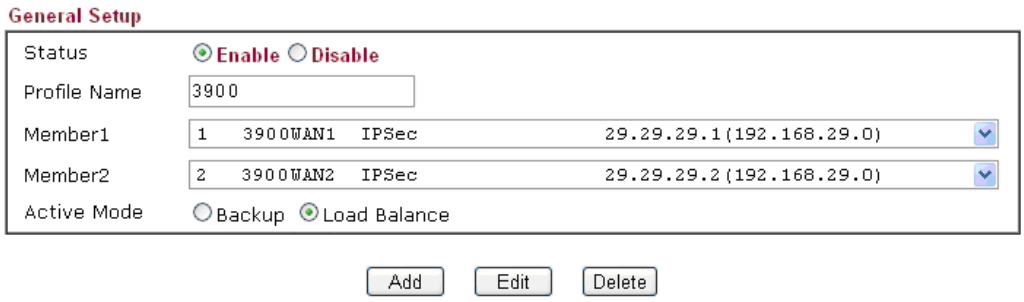
- Choose **IPSec Tunnel** and type the **Server IP** and Pre-shared Key as shown below.
- In the field of GRE over IPSec, please type the corresponding settings for Vigor3900. Refer to the following figure.In this example, please type the 2.2.2.1 in the field of **My GRE IP**; and type the GRE IP address 2.2.2.2 in the field of **Peer GRE IP**.

- Next, type the **Network IP** and **Network Mask** for both remote and local ends to complete the second VPN connection.

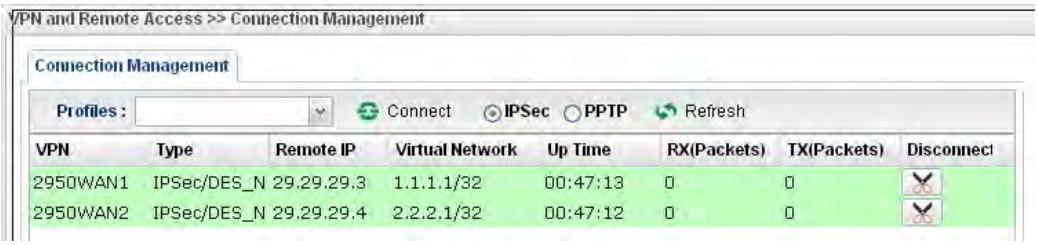


3. After finished the settings on both VPN connections, please access the Web User Interface of Vigor2950 and open **VPN and Remote Access > VPN Trunk Management** to make these two VPN connections into one **Load Balance** group.

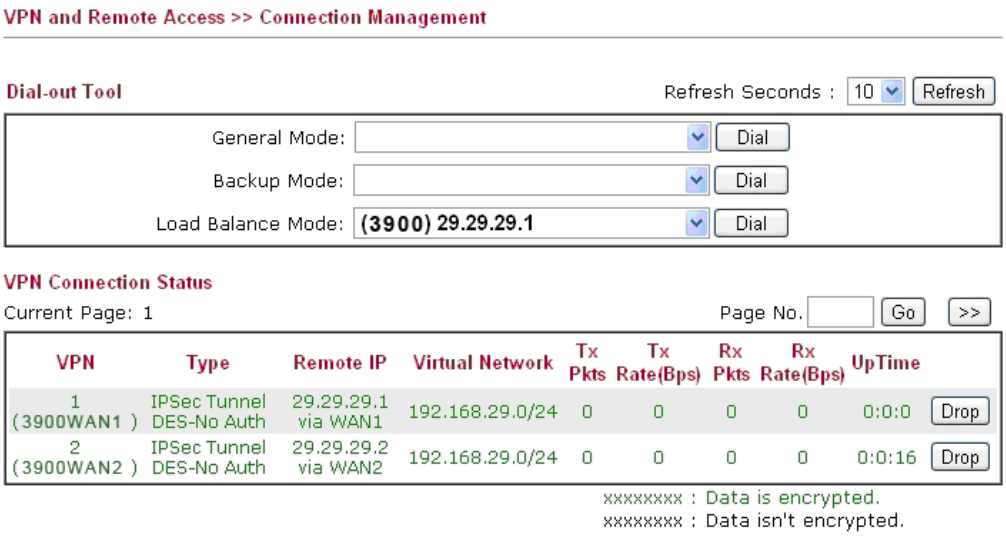
4. Type the name (e.g., 3900) of the **Load Balance** in the field of **Profile Name**. Specify the VPN profiles in Member 1 and Member 2 respectively. Then, choose **Load Balance** as the **Active Mode**.



5. Click **Add**. After finished the settings for Vigor3900 and Vigor2950, please check if the VPN connection is built successfully in both devices respectively. Take Vigor3900 for an example, open **VPN and Remote Access>> Connection Management** for viewing the result.



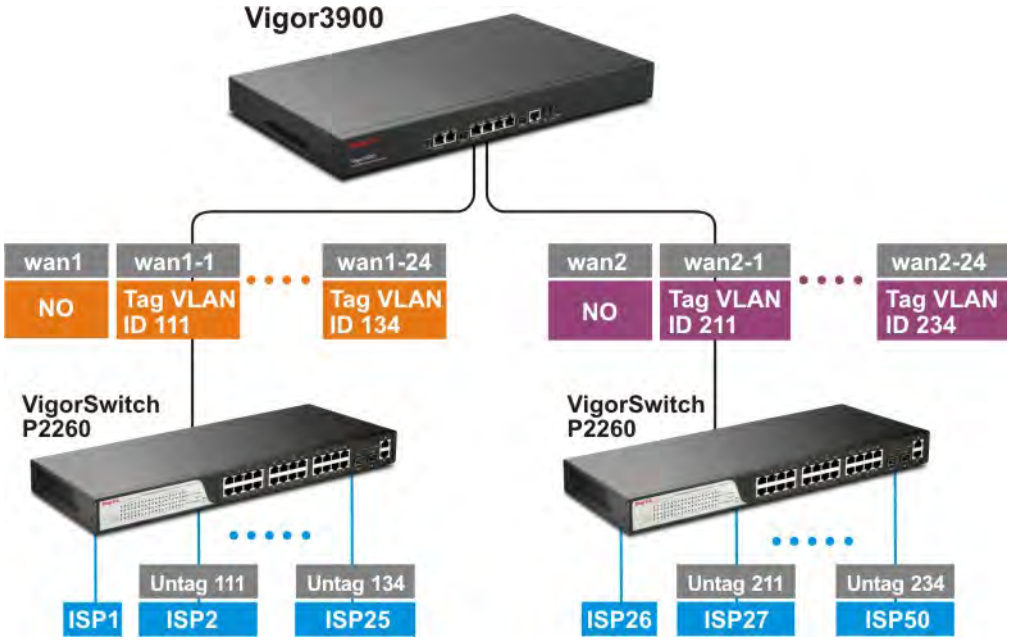
As to Vigor2950, please open **VPN and Remote Access>>Connection Management** to confirm the result.



3.9 How to Setup 50 WANs on Vigor3900

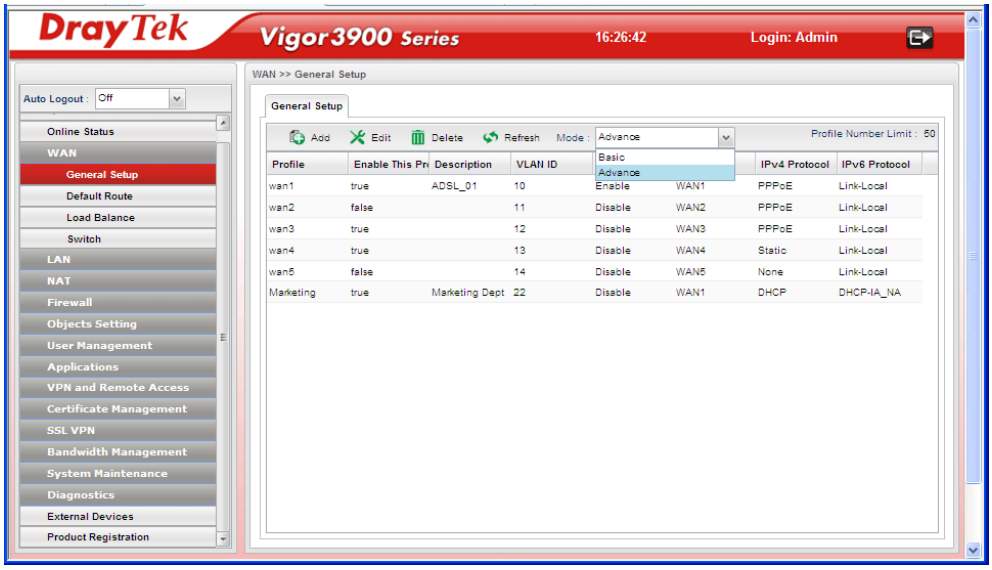
Vigor3900 has 5 physical WANs; however, it can be extended to 50 WANs at most by using VLAN Tagging technology.

Below will show how to achieve **50** WANs setup by one Vigor3900 and two VigorSwitch2260s. Refer to the following application illustration:

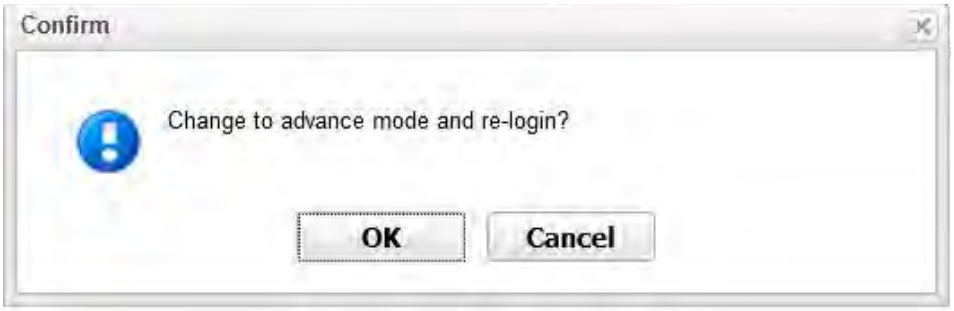


Configuring 50 WAN profiles on Vigor3900

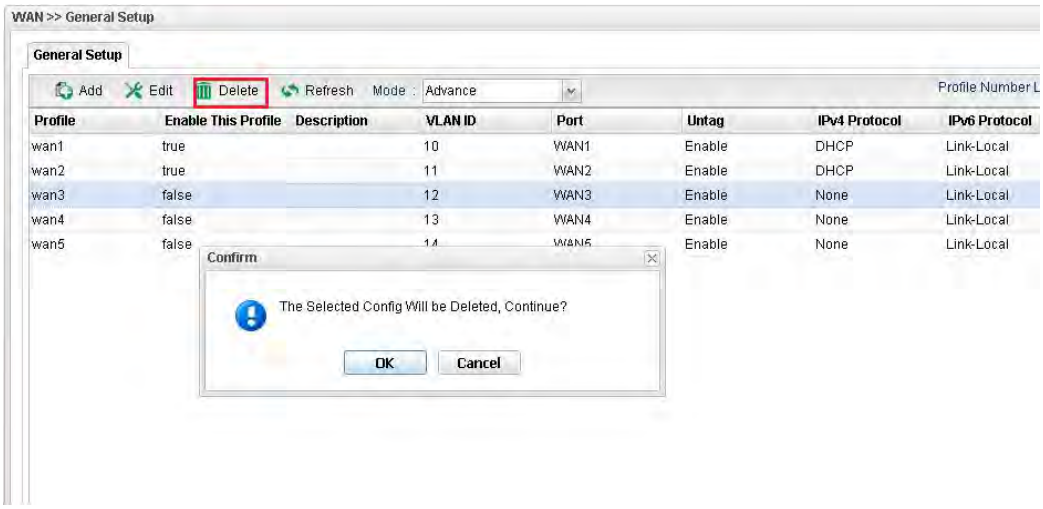
1. Change mode from **Basic** to **Advance** via **WAN>>General Setup** page.



2. Click **OK**. Vigor3900 will ask you to re-login.

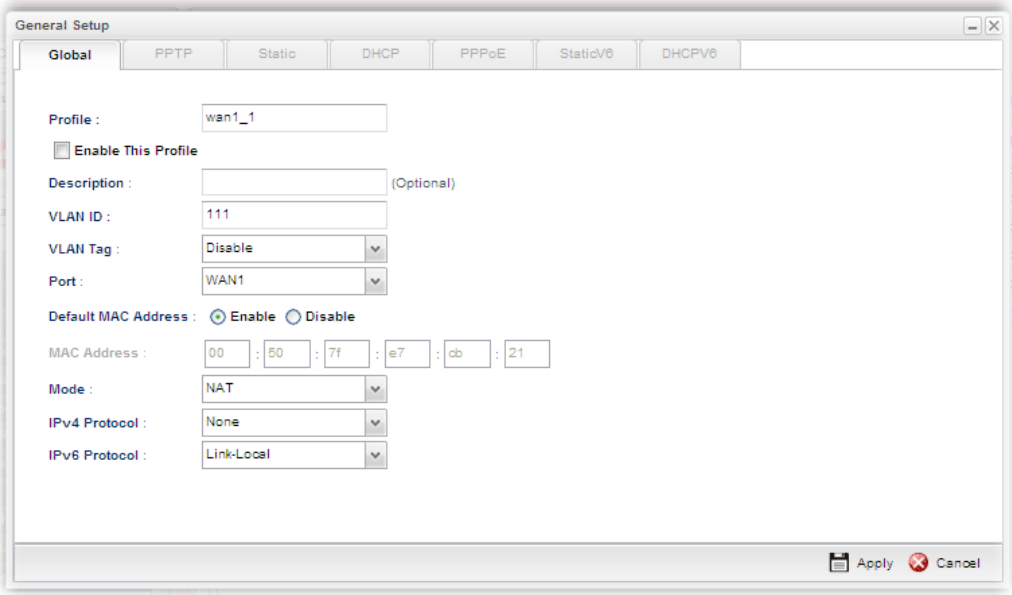


3. Delete default wan profiles for wan3, wan4 and wan5 by selecting the wan profile then click **Delete**.



4. Click **Add** to add new WANs.

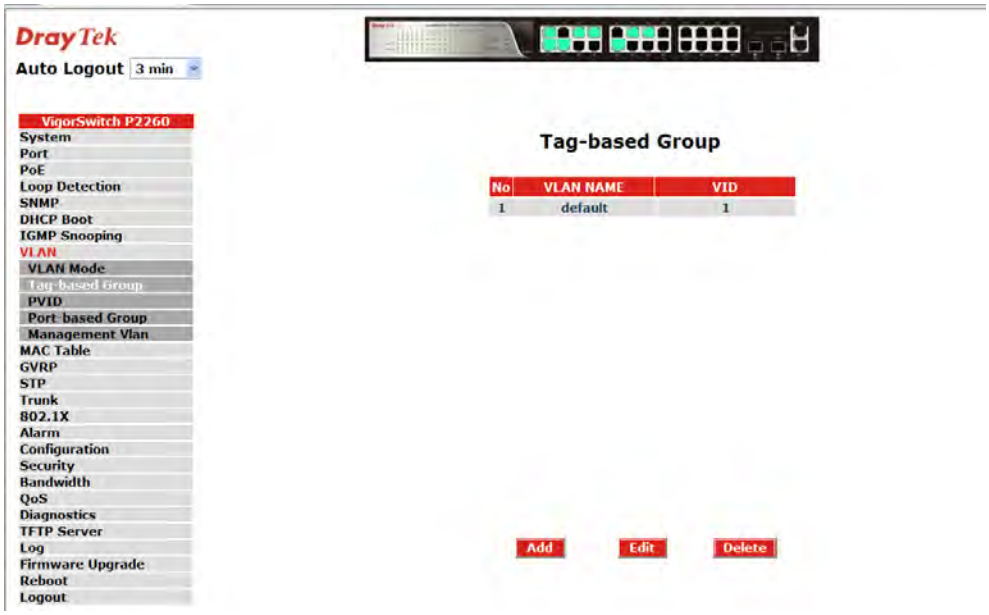
5. Create a new WAN profile named with **wan1_1,** and set VLAN ID named with **111** based on WAN Port 1(WAN1). Note that **Untag** must be set with **Disable**. It means wan1_1 can accept the packets tagged with VLAN ID 111. Next, click **Apply** to save the settings.



6. Create other WAN profiles named with **wan1_2 ~ wan1_24** (referring to the settings on the left side of the application illustration) and **wan2_1~ wan2_24** (referring to the settings on the right side of the application illustration) and set them with VLAN ID (112~ 134 and 211~ 234) by repeating step 4 ~ step 5.

Configuration on VigorSwitch2260

1. Setup **VLAN** mode as **Tag VLAN**.
2. Click **Add** to create a New VLAN GROUP via **VLAN>>TAG-based Group** page.



3. Type VLAN name and VID with **111**.

Tag-based VLAN

VLAN name	111							
VID	111							
Member	1. ☑	2. ☐	3. ☐	4. ☐	5. ☐	6. ☐	7. ☐	8. ☐
	9. ☐	10. ☐	11. ☐	12. ☐	13. ☐	14. ☐	15. ☐	16. ☐
	17. ☐	18. ☐	19. ☐	20. ☐	21. ☐	22. ☐	23. ☐	24. ☐
	25. ☐	26. ☑						
Untag	1. ☑	2. ☐	3. ☐	4. ☐	5. ☐	6. ☐	7. ☐	8. ☐
	9. ☐	10. ☐	11. ☐	12. ☐	13. ☐	14. ☐	15. ☐	16. ☐
	17. ☐	18. ☐	19. ☐	20. ☐	21. ☐	22. ☐	23. ☐	24. ☐
	25. ☐	26. ☐						

Apply

- Suppose the physical WAN1 of Vigor3900 connects to Port 26 of VigorSwitch. Port 26 will receive untagged packets (based on profile wan1) and packets tagged with 111 to 134 (based on profiles **wan1_1** to **wan1_24**). Therefore VigorSwitch Port 26 must be the member of VLAN Group ID 111 to 134.
- In **Member** field, select Port 1 and Port 26 as members of VLAN Group 111. Member setting means only the selected port number (e.g., Port 1 and Port 26) will receive packets with VLAN TAG 111 coming from Vigor3900.
- In **Untag** field, select Port 1 as Untag. Untag setting means VigorSwitch will untag the packets while sending it to Port 1. Because general PC or normal network devices do not accept VLAN packets, therefore in this example, Vigor3900 WAN1 must be connected to VigorSwitch Port 26 for receiving packets with tagged VLAN ID.
- Since ISP modem usually doesn't accept tagged packets, we have to set Untag for the Port (e.g, Port 1) used for ISP modem. Connect ISP modem for **wan1_1** to VigorSwitch Port 1.

4. Create the rest VLAN Groups (total is 24) by referring to the following figure. Please notice that Port 26 must be selected as the member for each group, for it is the channel for any packets coming from Vigor3900. As to Untag, when you check Port 2 and Port 26, you have to untag Port 2; when you check Port 3 and Port 26, you have to untag Port 3; and so forth.

Tag-based Group

No	VLAN NAME	VID
1	default	1
2	111	111
3	112	112
4	113	113
5	114	114
6	115	115
7	116	116
8	117	117
9	118	118
10	119	119
11	120	120
12	121	121
13	122	122
14	123	123
15	124	124
16	125	125
17	126	126

Add Edit Delete

5. Go to **VLAN>>PVID** page to set up PVID for each port.

PVID

Port No	PVID	Default Priority	Drop Untag
1	111	0	Disable
2	112	0	Disable
3	113	0	Disable
4	114	0	Disable
5	115	0	Disable
6	116	0	Disable
7	117	0	Disable
8	118	0	Disable
9	119	0	Disable
10	120	0	Disable
11	121	0	Disable
12	122	0	Disable
13	123	0	Disable
14	124	0	Disable
15	125	0	Disable
16	126	0	Disable
17	127	0	Disable
18	128	0	Disable
19	129	0	Disable
20	130	0	Disable
21	131	0	Disable
22	132	0	Disable
23	133	0	Disable
24	134	0	Disable
25	1	0	Disable
26	1	0	Disable

- PVID means VigorSwitch2260 will check and add VLAN tags while receiving packets from Ports.
- ISP modem 1 which connects to Port 1 doesn't support VLAN Tag.
- While the switch receives packets from Port 1, it will add VLAN Tag 111 to the packets Then Vigor3900 wan1_1 will receive the packets.

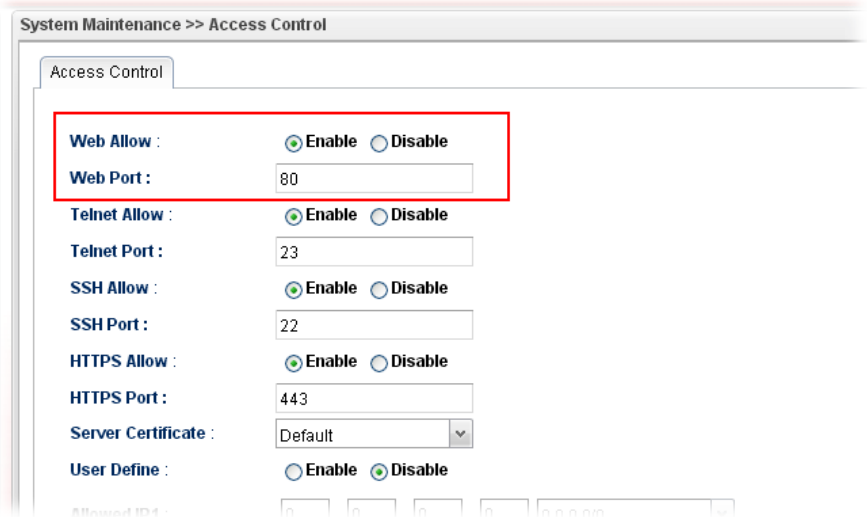
6. After finishing the configuration for one VigorSwitch, please set for another VigorSwitch with the same procedure. The file names shall be wan2_1~ wan2_24 and the VLAN ID shall be set as 211~ 234.

3.10 CVM Application - How to manage the CPE (router) through Vigor3900?

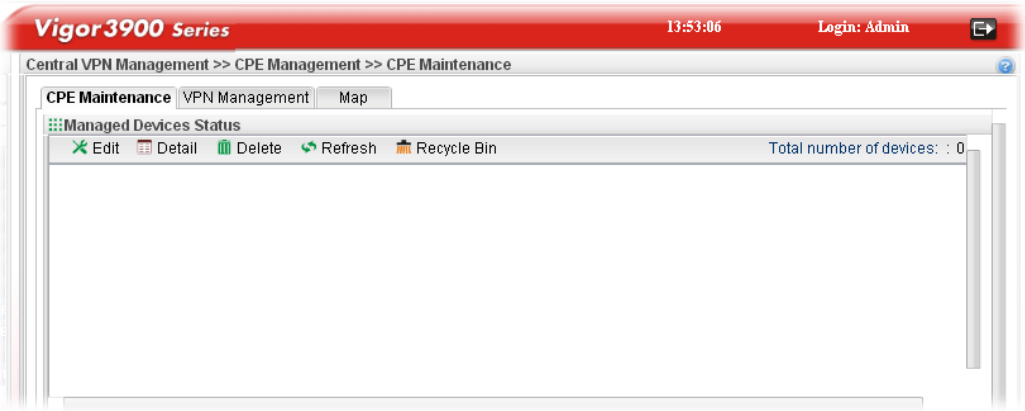
To manage CPEs through Vigor3900, you have to set URL on CPE first and set username and password for Vigor3900. For this section, we use Vigor2830 series as the example. The firmware upgrade for the CPE can be done through Vigor2830 series.

3.10.1 Configure Settings on Vigor3900

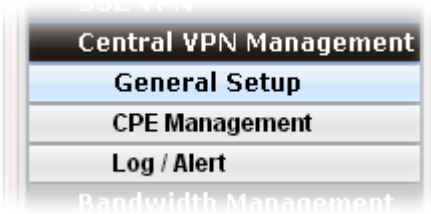
1. Access into the web user interface of Vigor3900.
2. Open **System Maintenance>>Access Control**. Check **Enable** for **Web Allow** and type the value for **Web Port**. Then click **Apply** to save the settings.



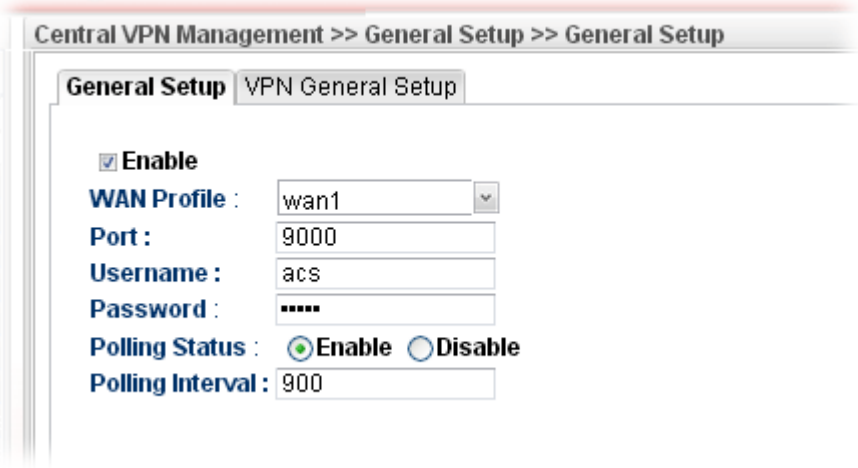
3. Open **Central VPN Management>>CPE Management**. On the page of **CPE Maintenance**, there is no CPE managed by Vigor3900.



4. Open **Central VPN Management>>General Setup.**



5. Click the **General Setup** tab. Check the **Enable** box. Specify the WAN interface from the WAN Profile drop down list. Type the values for **Port, Username**, and **Password** respectively. Remember the values configured in this page.



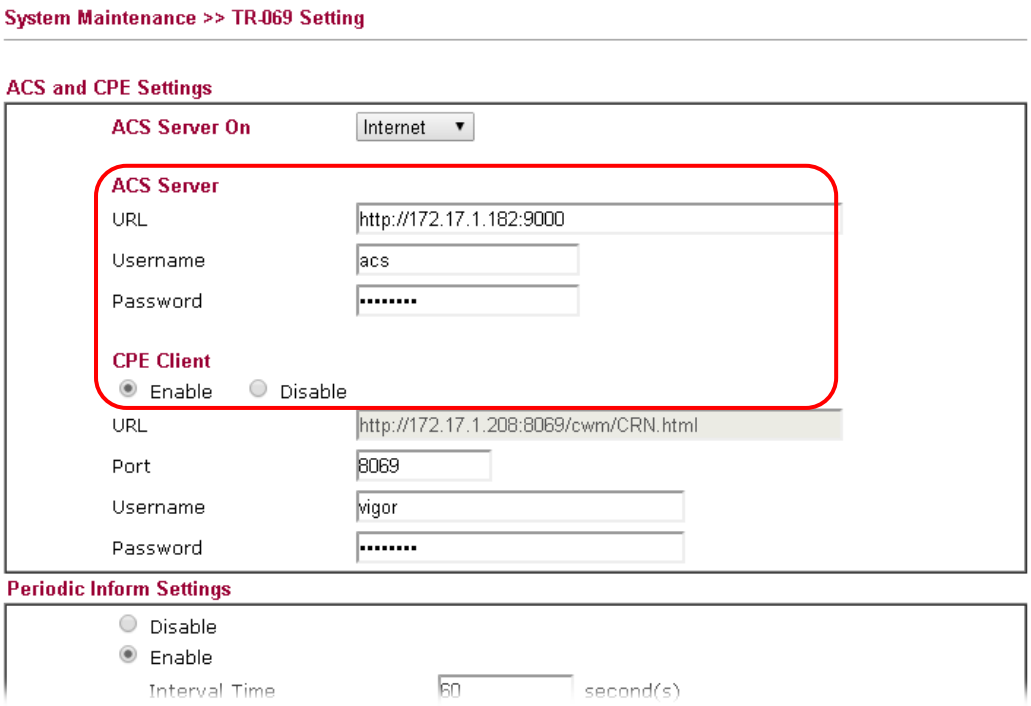
6. Click **Apply** to save the settings.

3.10.2 Configure Settings on CPE

To manage CPEs through Vigor3900, you have to set ACS URL on CPE first and set username and password for Vigor3900.

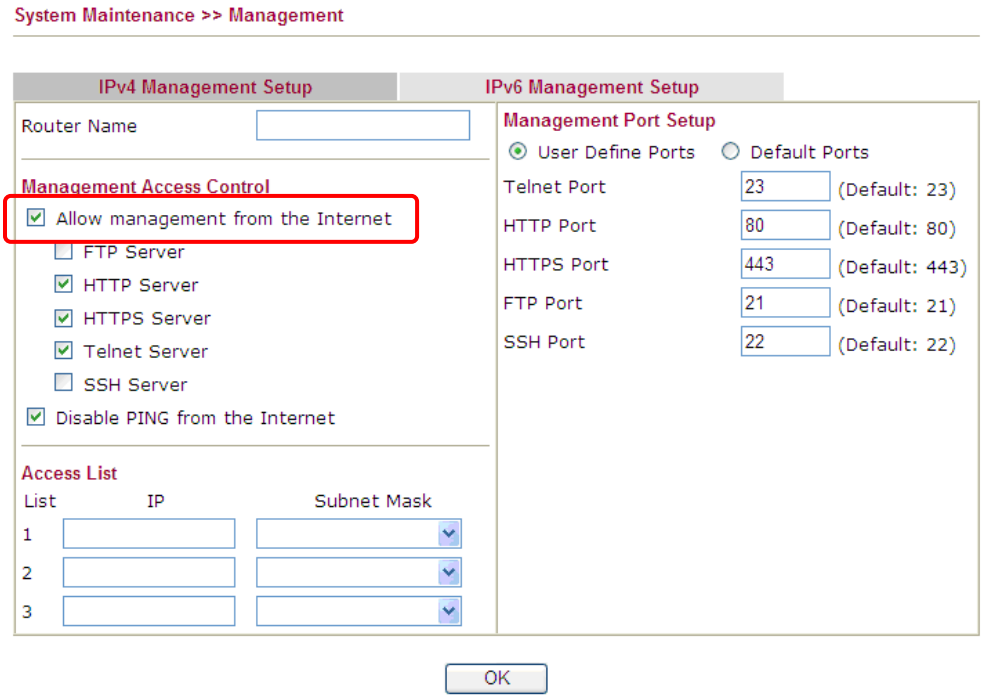
1. Connect one CPE (e.g., Vigor2830 series) and get ready to access into the web user interface of the CPE.
2. Open a web browser (for example, **IE**, **Mozilla Firefox** or **Netscape**) on your computer and type **http://192.168.1.1.**
3. Please type username and password on the window. If you don't know the correct username and password, please consult our dealer to get them.
4. Open **System Maintenance** >> **TR-069**.

5. In the field of ACS Server, type the URL (IP address with port number) of Vigor3900: "http://{IP address of Vigor3900}:{CVM port}/ACSServer/services/ACSServlet" and type the same Username and Password defined on the page of Central VPN Management>>General Setup in Vigor3900. Then, click Enable for CPE Client and then click OK to save the settings.



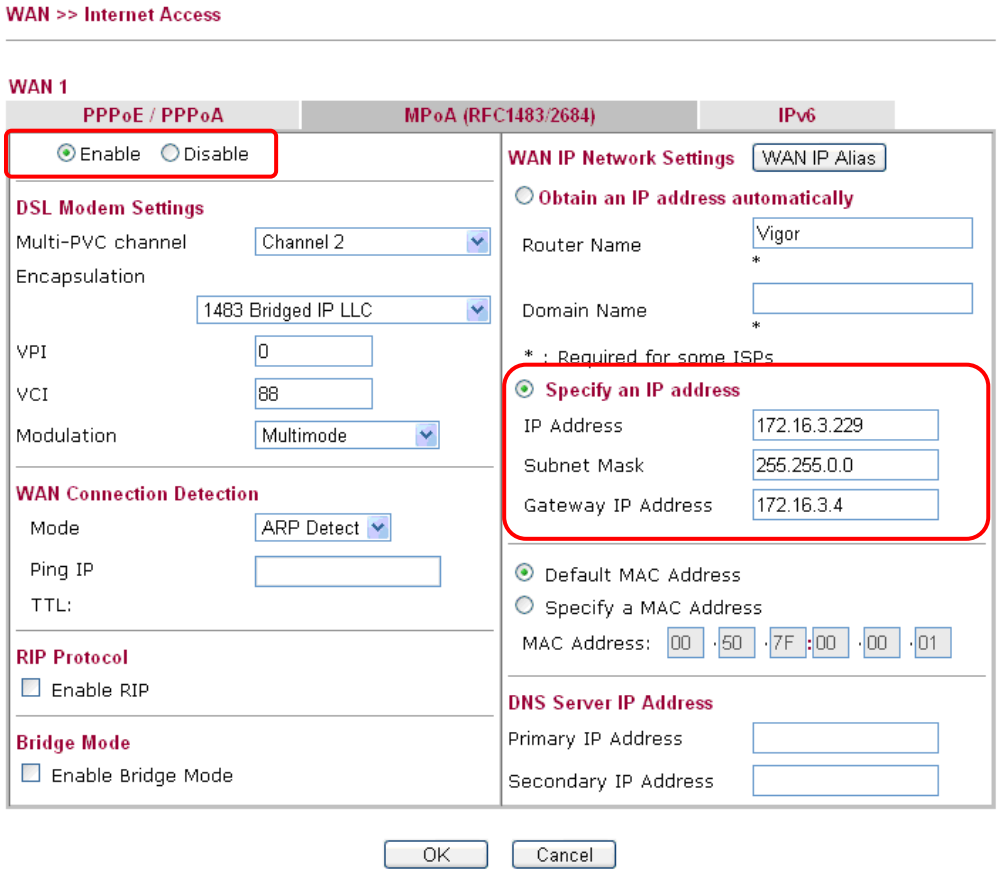
3.10.3 Invoke Remote Management for CPE

1. Login the web user interface of the CPE.
2. Open **System Maintenance>>Management Setup**.
3. Check **Allow management from the Internet** to set management access control.



3.10.4 Enable WAN Connection on CPE

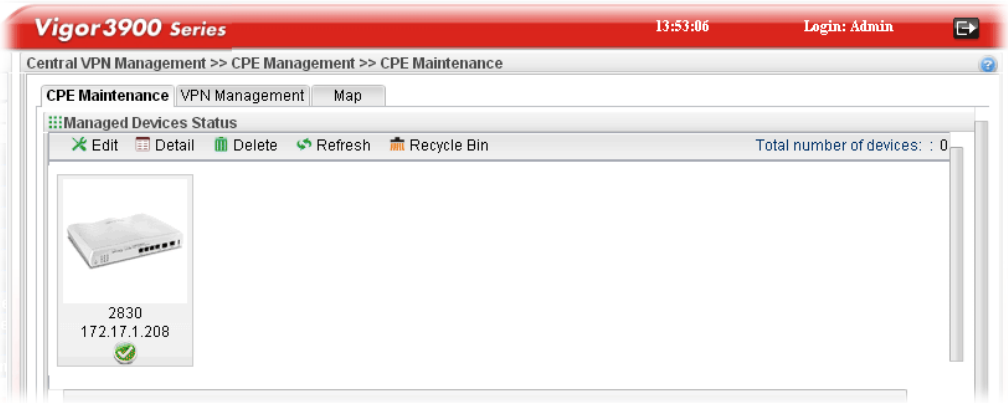
1. Login the web user interface of the CPE.
2. Open **WAN>>Internet Access.** Use the drop down list of **Access Mode** on WAN1 to select **MPoA** (RFC1483/2684). Then, click **Details Page**.
3. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.



Note: Reboot the CPE device and re-log into Vigor3900. CPE which has registered to Vigor3900 will be captured and displayed on the page of **Central VPN Management>>CPE Management**.

3.10.5 Check CPE Maintenance Page

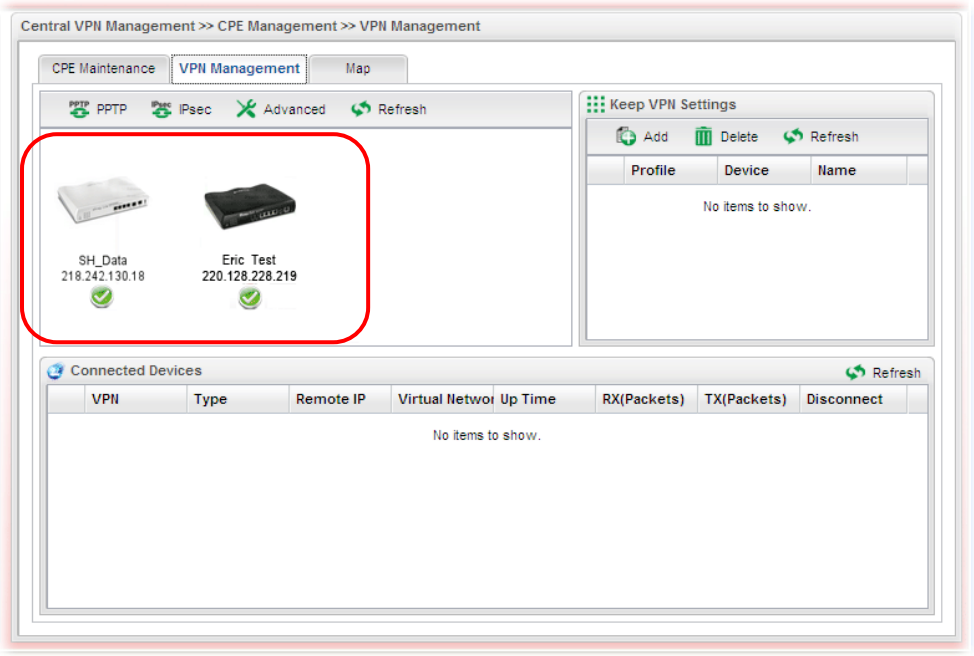
1. Return to the web user interface of Vigor3900.
2. Open **Central VPN Management>>CPE Management.**
3. Now there is one CPE managed (Vigor2830) by Vigor3900 on the page of **CPE Maintenance**.



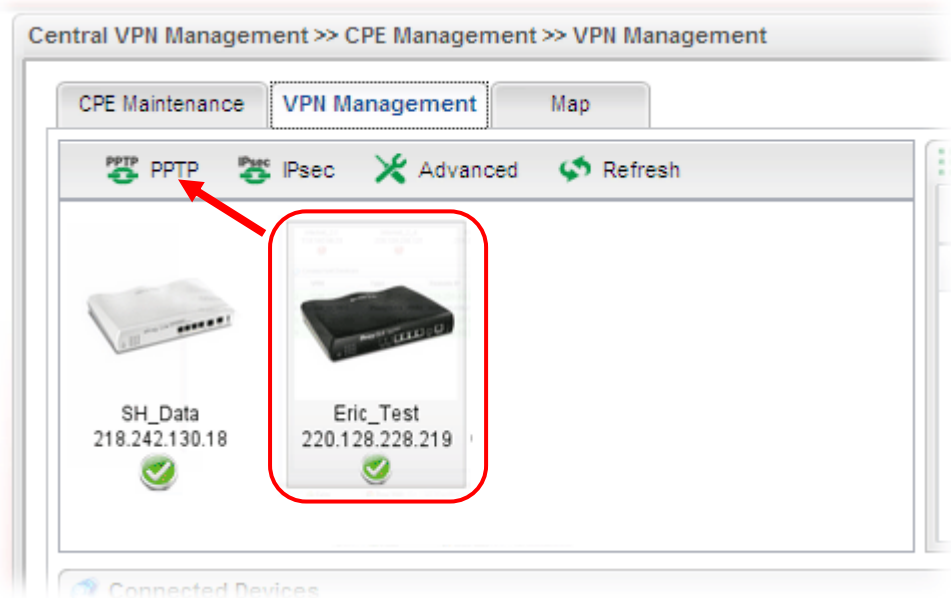
3.11 CVM Application - How to build the VPN between remote devices and Vigor3900?

When a remote device is managed by Vigor3900 series, it is easy to build VPN between these two devices.

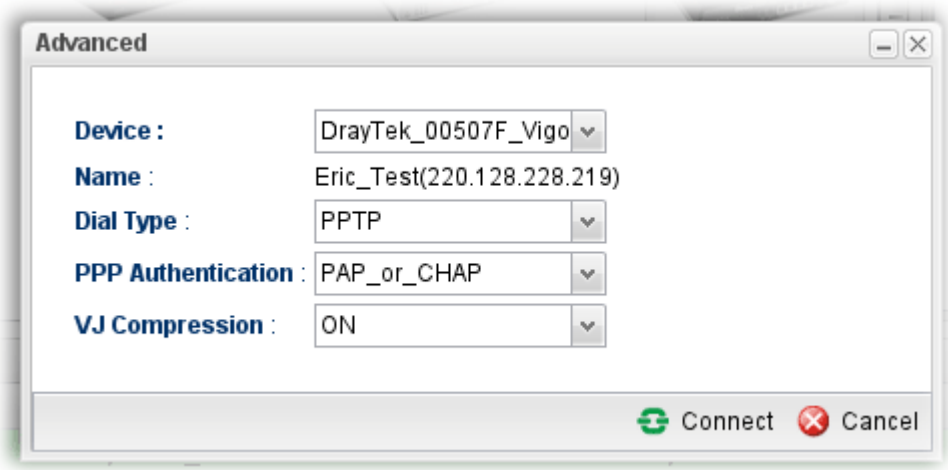
1. Access into the web user interface of Vigor3900 series.
2. Open **Central VPN Management>>CPE Management**. The icons displayed on the screen means the remote devices are ready for building VPN with Vigor3900.



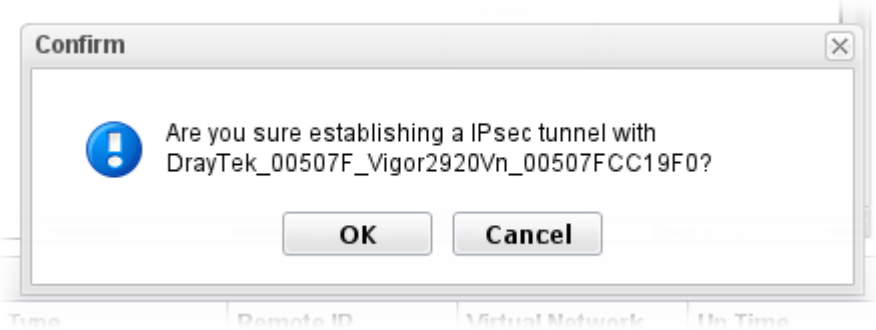
3. Click the device icon (marked with) and click the **PPTP** or **IPsec** button.



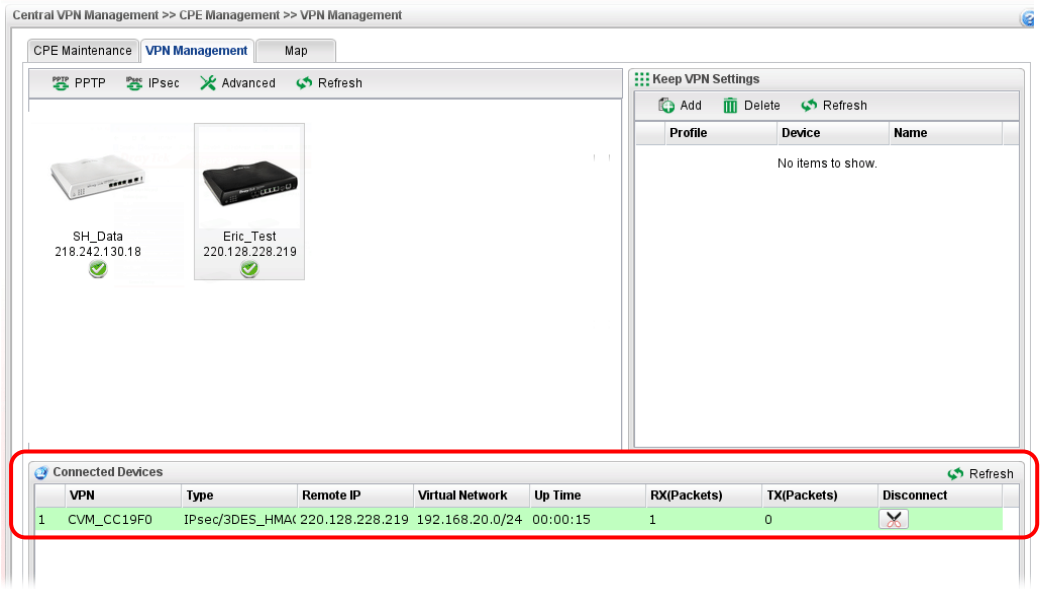
Or click **Advanced** to open the following page for specified the CPE you want. Click **Connect** after finished the settings.



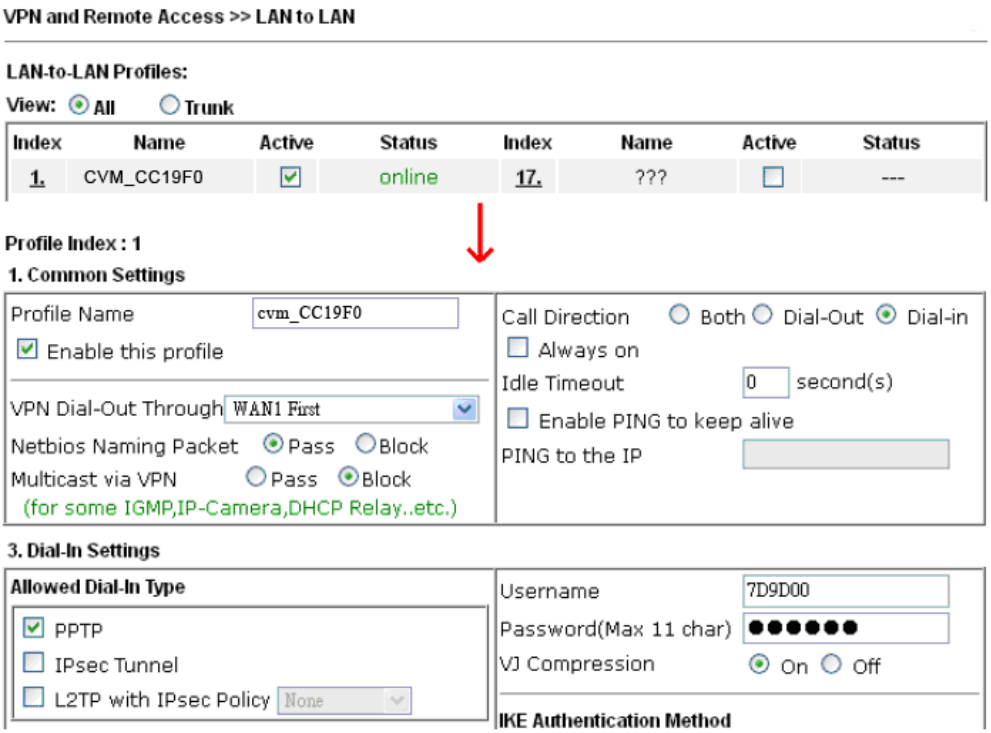
4. A confirmation dialog will appear. Click **OK** and wait for a moment.



5. If VPN is built successfully, related information will be displayed on **Connected Devices.**



6. 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.

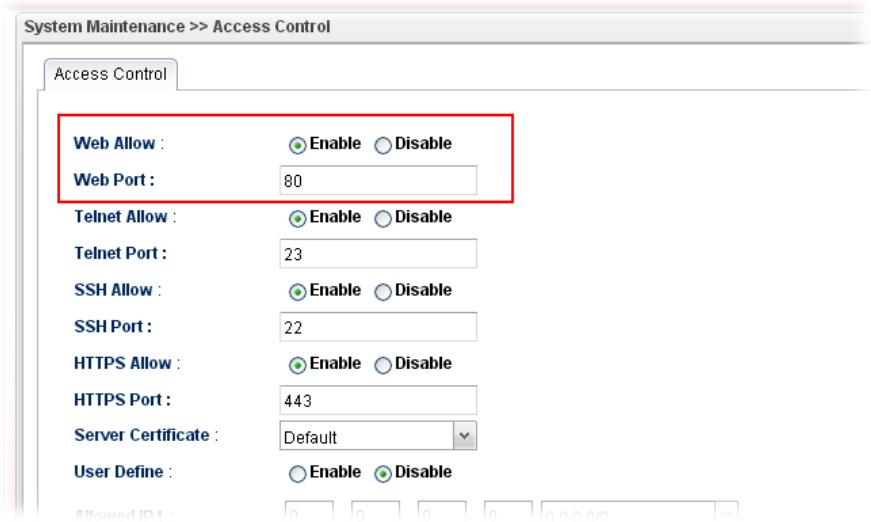


Note: The profile name is created automatically by the system. Do not modify any value in such page to avoid VPN error.

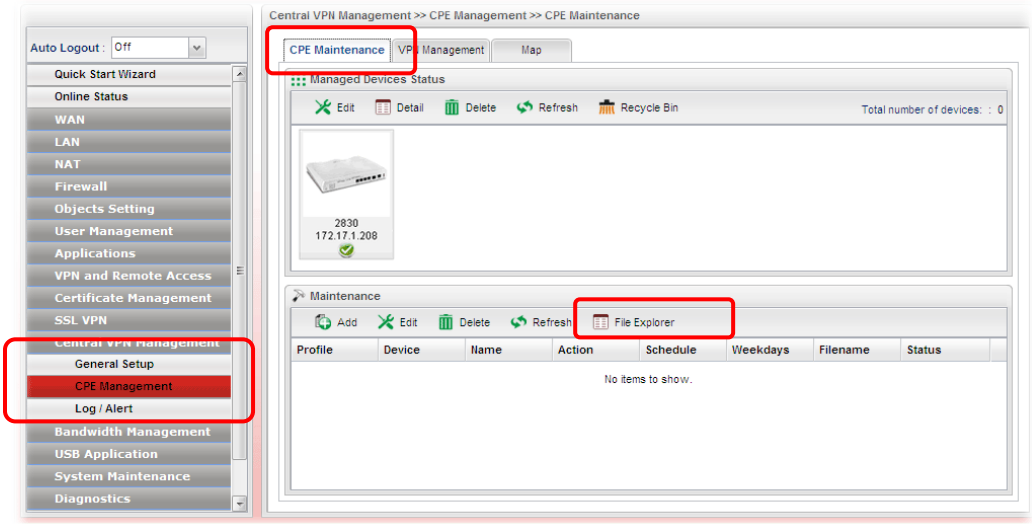
3.12 CVM Application - How to upgrade CPE firmware through Vigor3900?

3.12.1 Import firmware file from your PC to Vigor3900

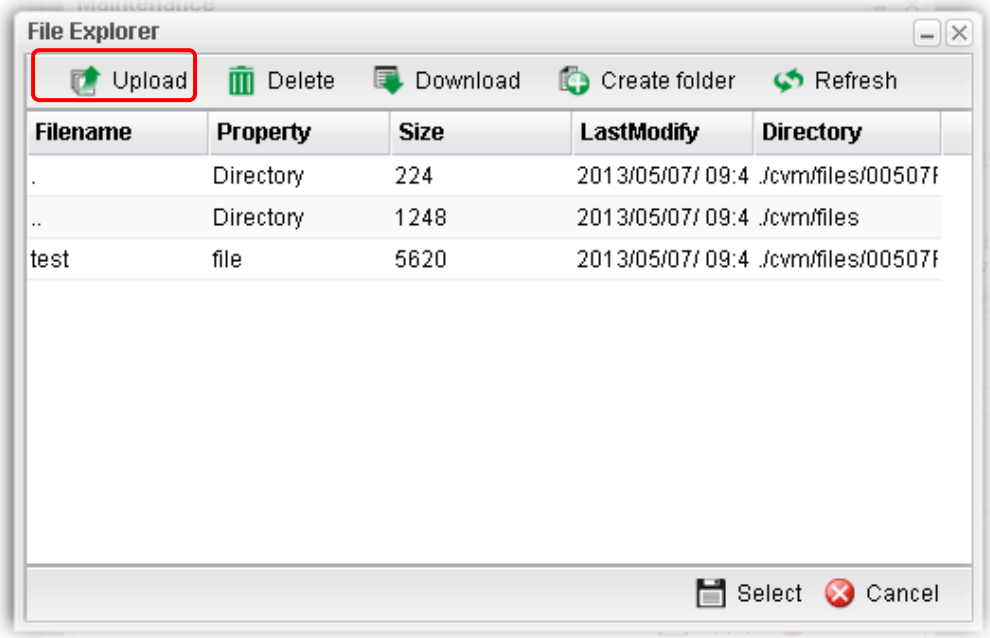
1. Suppose the newest firmware file is located on your PC. You can upload it from your PC to Vigor3900.
2. Log into the web user interface of Vigor3900.
3. Open **System Maintenance>>Access Control**. Check **Enable** for **Web Allow** and type the value for **Web Port**. Then click **Apply** to save the settings.



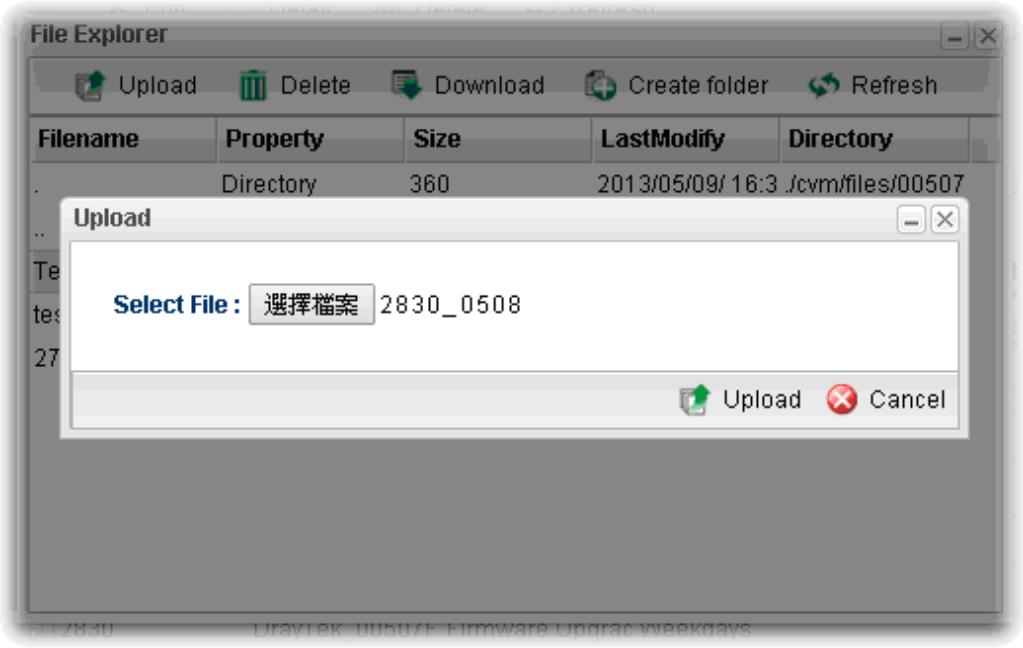
4. Open **Central VPN Management>>CPE Management.** Click **CPE Maintenance**. In the **Maintenance** area, click **File Explorer.**



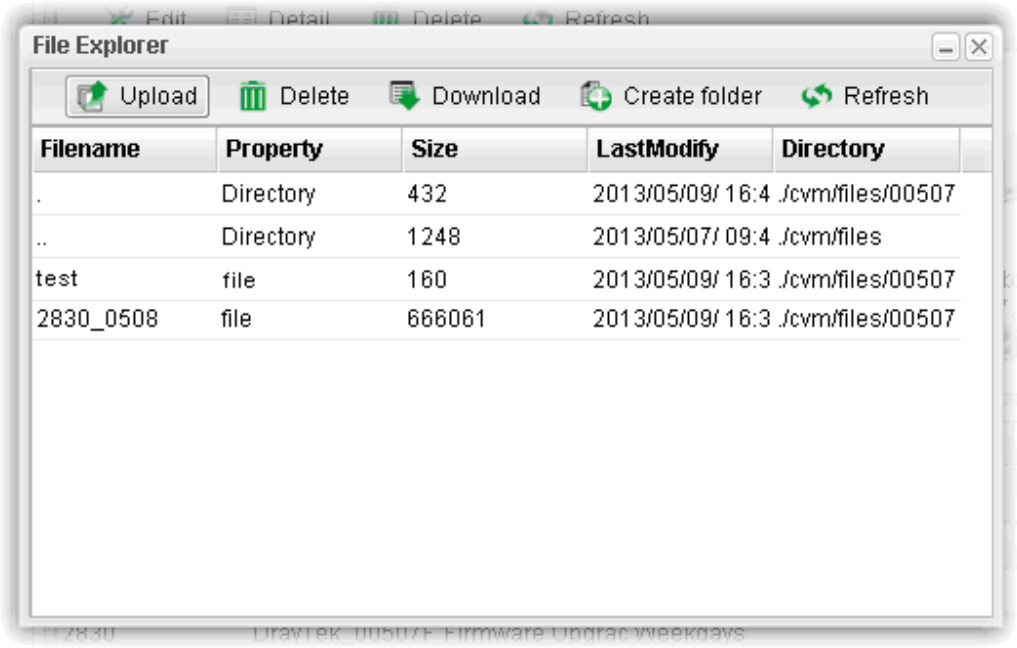
5. In the File Explorer dialog, click **Upload**.



6. In the Upload dialog, click the **Browse..** button to find out the firmware (e.g., 2830_0508 in this case) you want to upload **from PC to Vigor3900.** Then, click **Upload**.



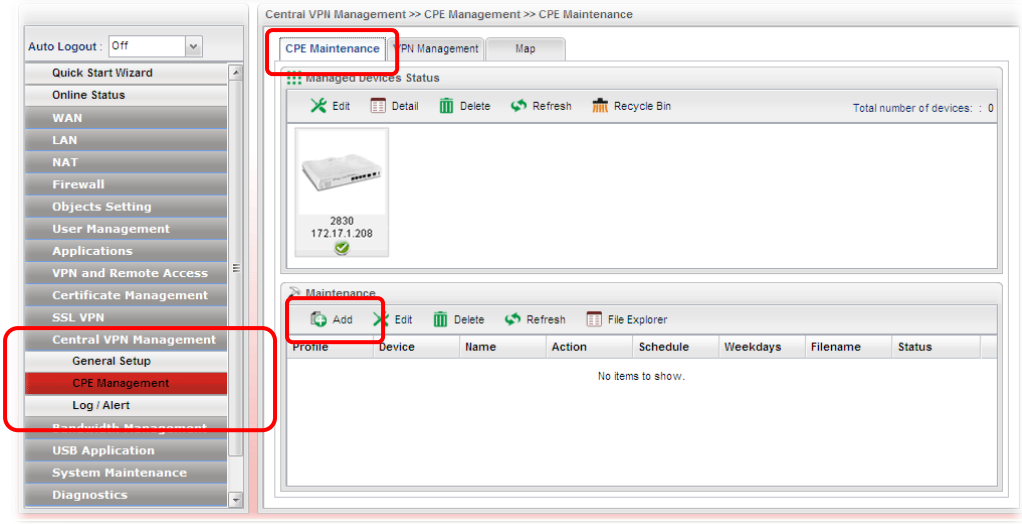
7. When the file is uploaded successfully, later you will find the one in the File Explorer dialog.



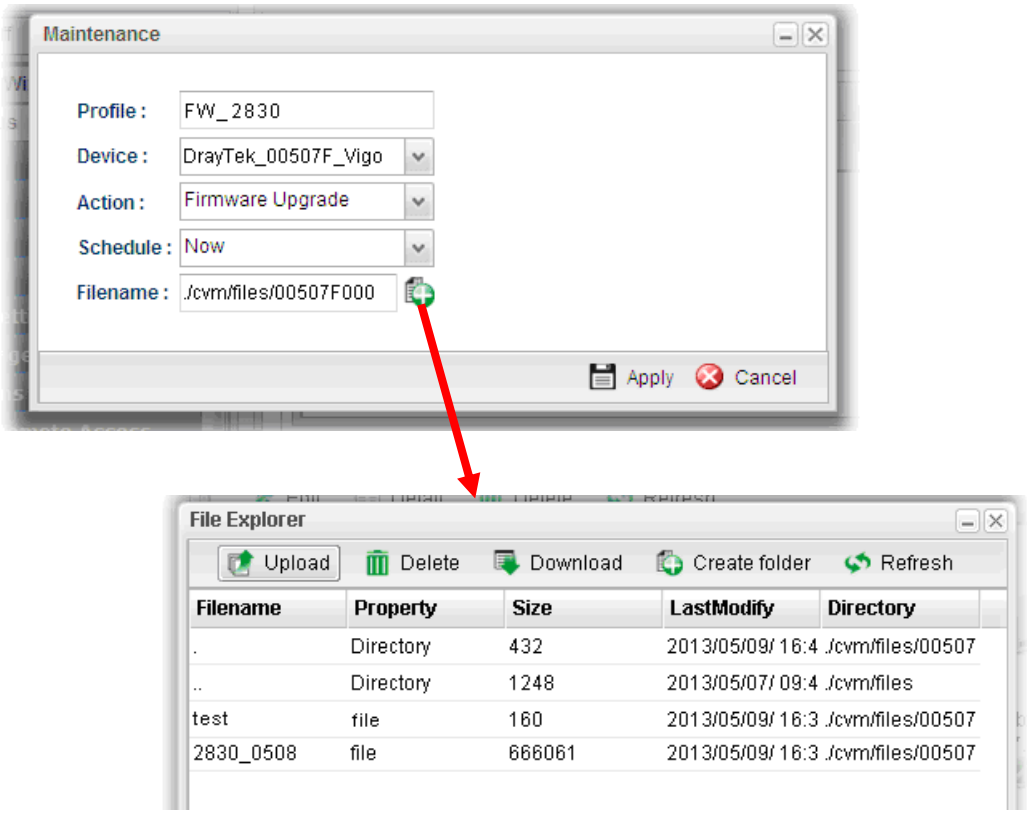
3.12.2 Set a new firmware upgrade profile

To create a new firmware upgrade profile, one CPE (e.g., 2830 in this case) must be managed by Vigor3900 at least. Otherwise, the profile cannot be created successfully.

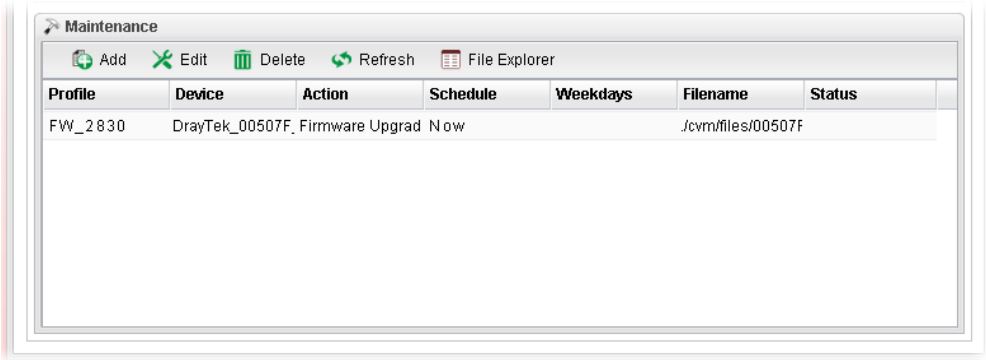
1. Open Central **VPN Management>>CPE Management.** Click **CPE Maintenance**. In the **Maintenance** area, click **Add.**



2. In the following dialog, type the name for the new profile; specify the vigor router the file will be applied to; choose **Firmware Upgrade** as the **Action**, choose **Now** as the Schedule (it means the firmware upgrade will be performed after clicking **Apply**); and type the string of the firmware filename or click to choose a correct one.

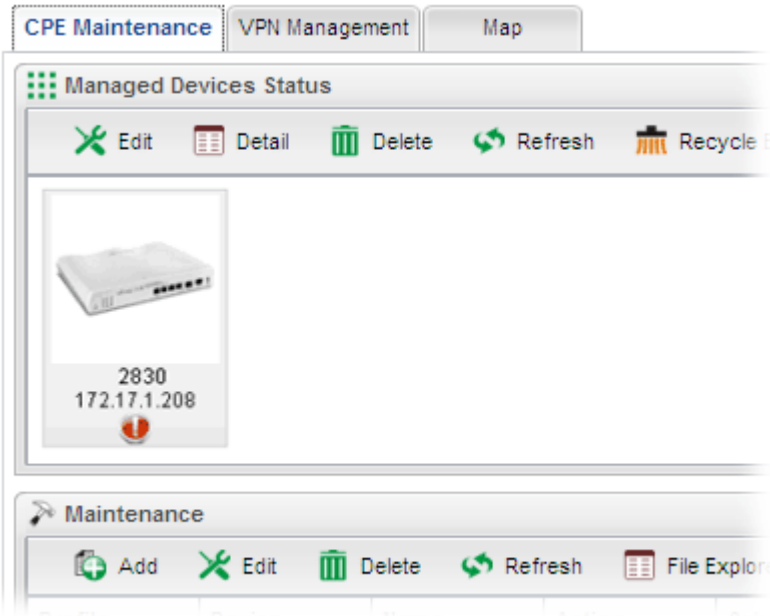


3. When you finished the above settings, click **Apply** to save them. The new maintenance profile has been created and displayed on the Maintenance area.



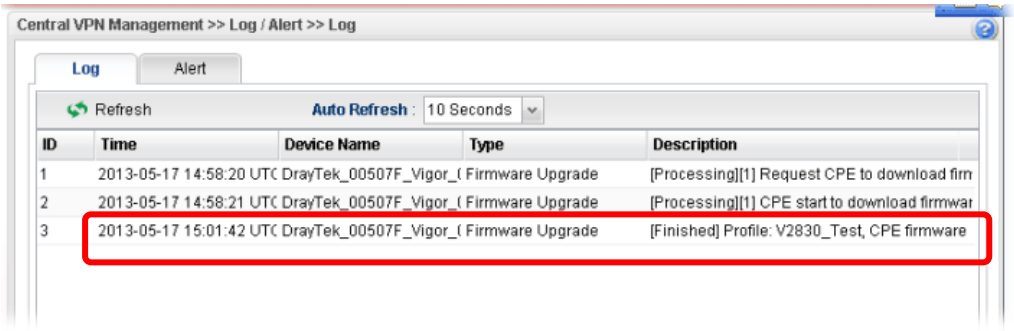
4. Now, the new firmware will be loaded into the CPE immediately (based on the schedule setting – now).

Note that a red icon, will appear during the period of firmware upgrading.



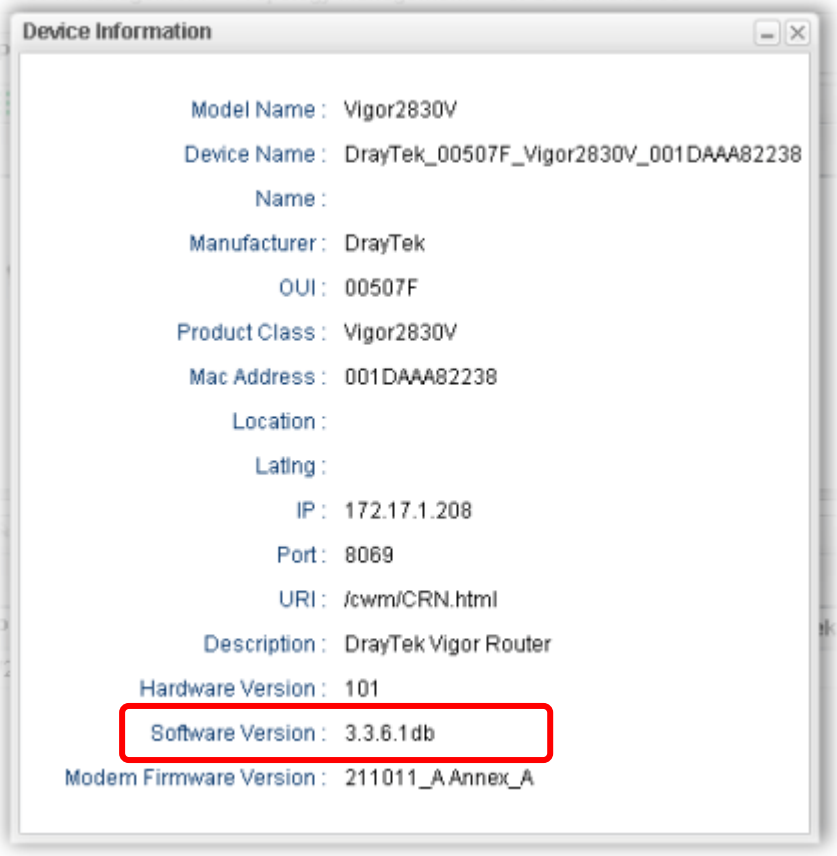
And, in the web user interface of client's CPE, the system will show you that firmware upgrade is on going.

5. Please wait for a moment. Later, open **Central VPN Management>>Log/Alert>>Log** page to check the result. If [Finished] is displayed, it means the firmware upgrade of specified CPE has completed.



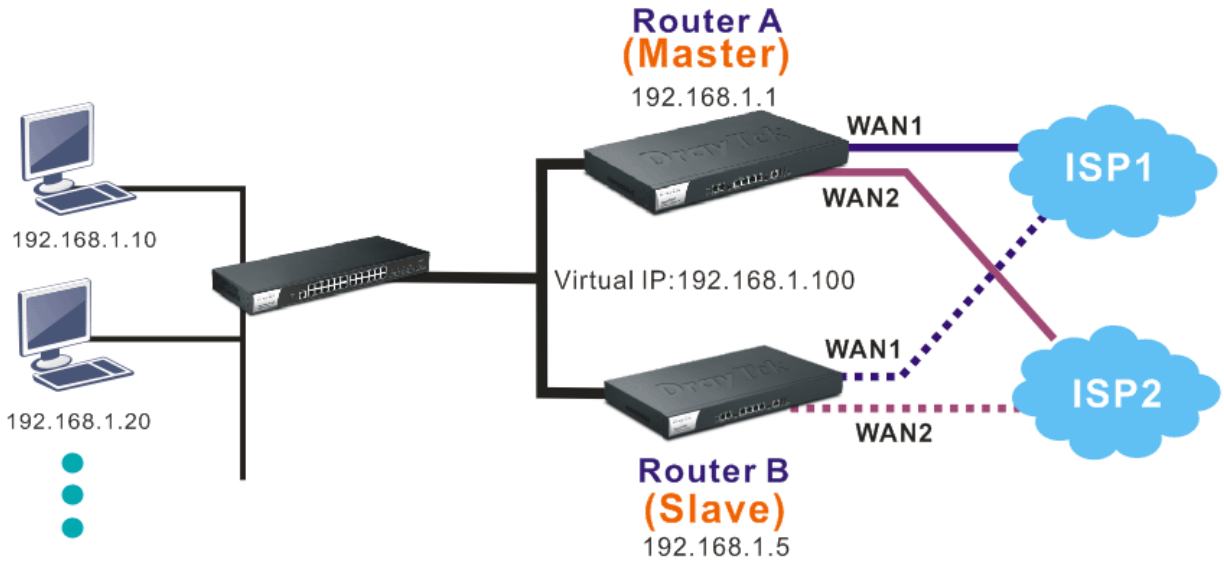
3.12.3 Check the Device Information

1. Open Central **VPN Management>>CPE Management.** In the **Managed Devices Status** area, choose the router (representing Vigor2830) and click **Detail**.
2. Check the software version field.



3.13 How to use High Availability for Vigor routers?

The High Availability (HA) feature in Vigor3900 can ensure the business continuity for your organization. IT staff can use HA as a simple solution for the disaster recovery. Vigor3900 utilizes the Common Address Redundancy Protocol (CARP) to avoid the system crashing which could stop the normal operation and then cause considerable lost of the entire organization.

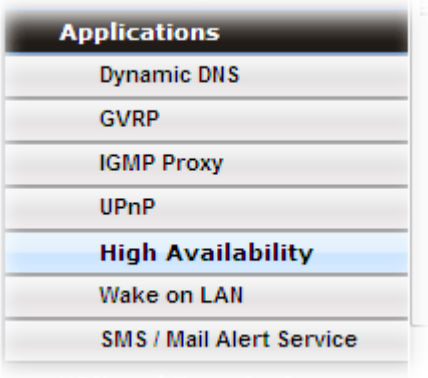


When the HA feature is enabled, the network administrator can set another Vigor3900(s) as the backup device(s) to deliver full routing services during the shutdown of the main Vigor3900. The network administrator can use a Virtual IP (e.g. 192.168.1.100) for both master device and backup device. During the system uptime, the master device (e.g. 192.168.1.1) can offer services and act as the Virtual IP. Once the master device is temporarily out-of-service, the backup device(s) (e.g. 192.168.1.5) will take over the service that the Virtual IP does and deliver all routing functions.

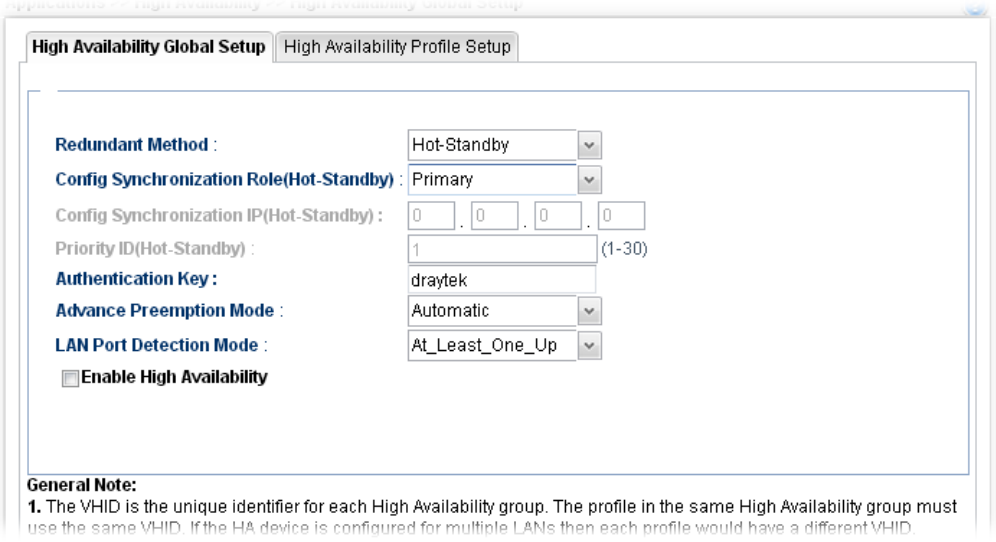
> **Note:** Make sure the WAN interfaces for both Router A and Router B are well connected. Both routers can be used to access into Internet.
>
> **Note:** For advanced applications, please refer to FAQ/Application Notes on www.draytek.com.

For router A

1. Access into the web user interface of Vigor3900.
2. Open **Applications** >>**High Availability.**

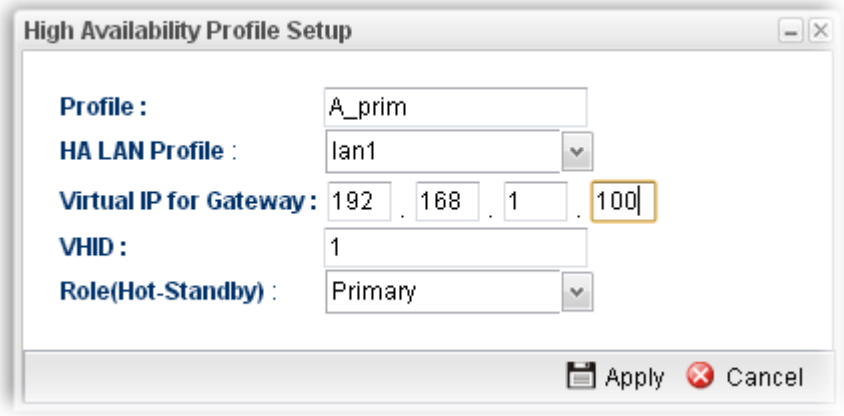


3. In the tab of **High Availability Global Setup**, choose **Hot-Standby** as Redundant Method; choose **Primary** as Config Synchronization Rule; type **draytek** as Authentication Key; choose **Automatic** as Advance Preemption Mode. Click **Apply** to save the settings.



4. Click the **High Availability Profile Setup** tab to create HA profile(s). Click **Add**.

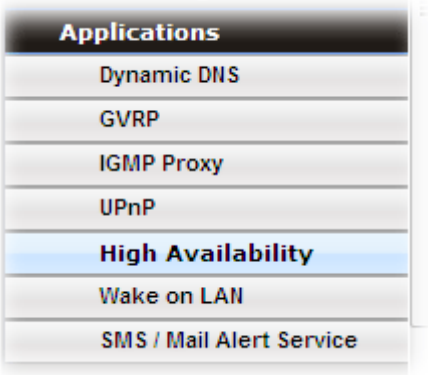
5. Create an HA profile. Refer to the following figures.



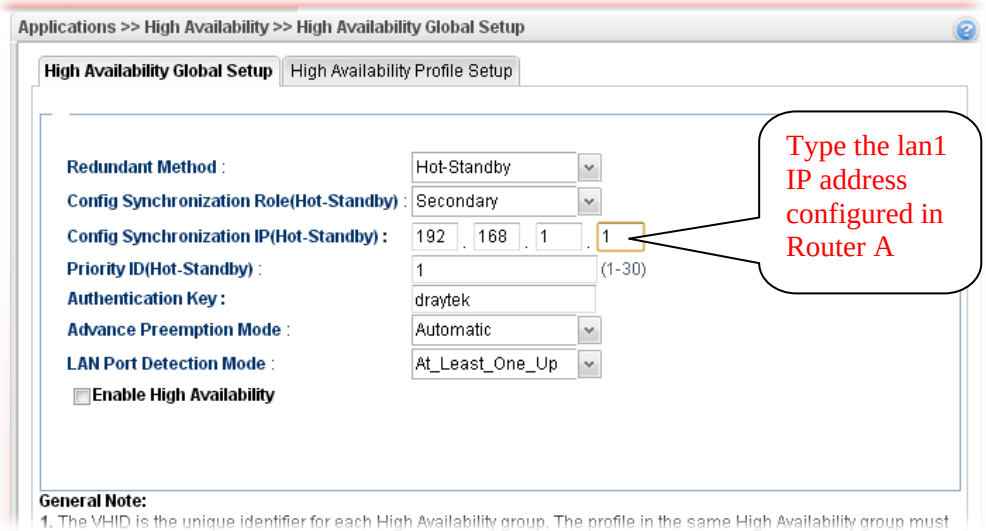
6. Now, the configuration for router A has been finished.

For router B

1. Access into the web user interface of Vigor3900.
2. Open **Applications** >>**High Availability.**

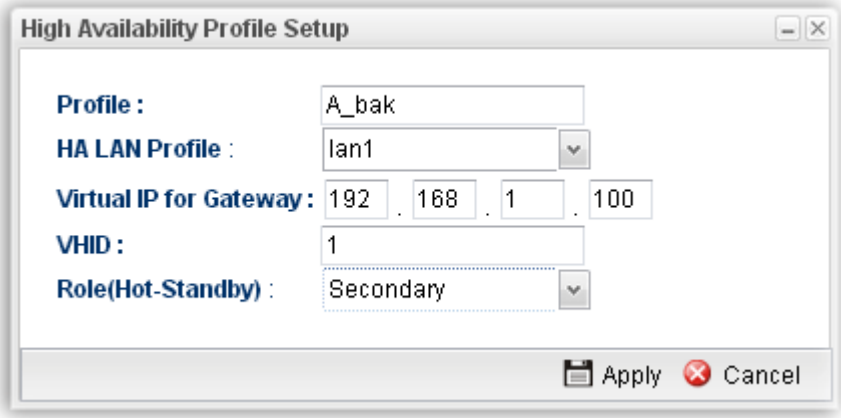


3. In the tab of **High Availability Global Setup**, choose **Hot-Standby** as Redundant Method; choose **Secondary** as Config Synchronization Rule; type the lan1 IP address configured in router A; type **draytek** as Authentication Key; choose **Automatic** as Advance Preemption Mode. Click **Apply** to save the settings.



4. Click the **High Availability Profile Setup** tab to create HA profile(s). Click **Add**.

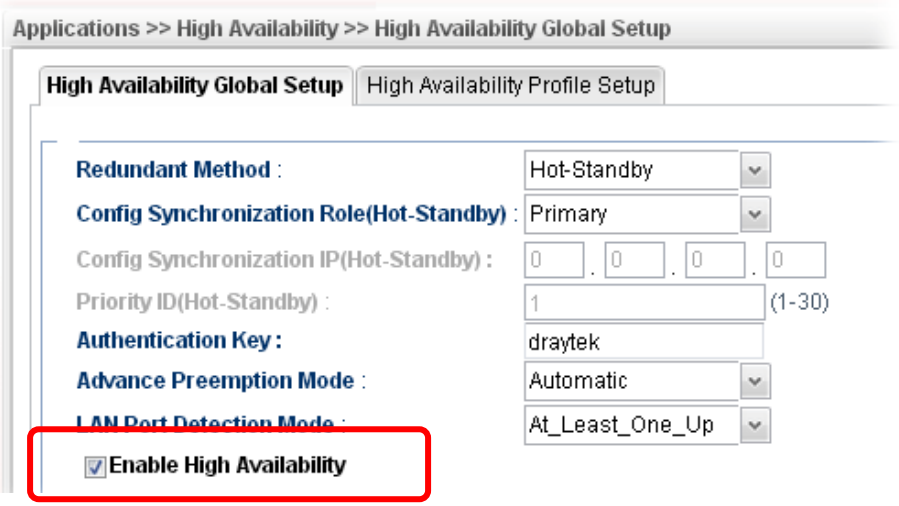
5. Create an HA profile. Refer to the following figures.



6. Now, the configuration for router B has been finished.

After finished the above settings, it is the time to activate HA function for both router A and router B. It is recommended to activate the HA for router A (Primary) before router B (Secondary).

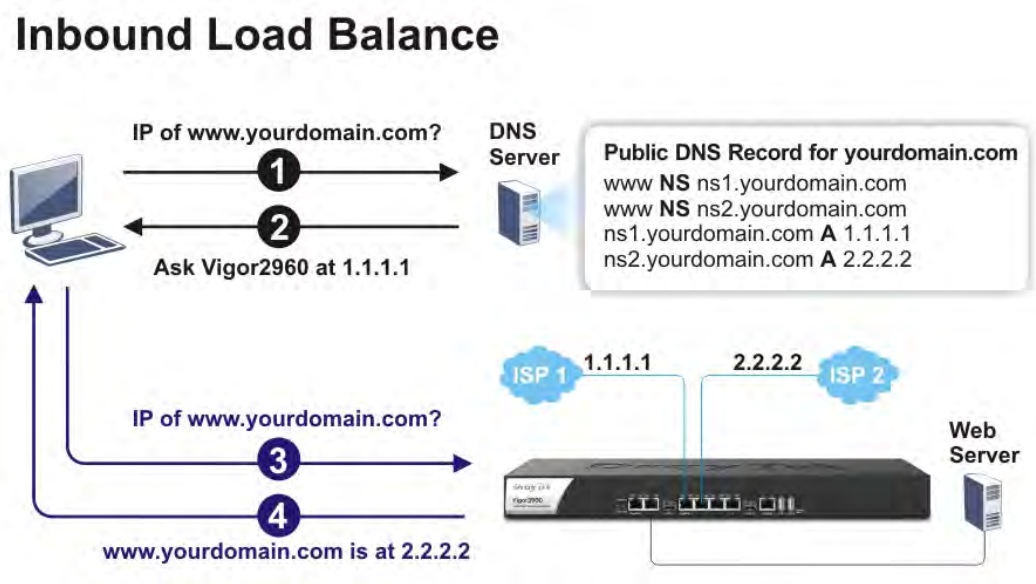
- Simply open **Applications>>High Availability** and click the **High Availability Global Setup**. Locate **Enable High Availability**. Check the box and click **Apply** to save the settings.



Under such construction, when Router A (defined as Master device) is powered off, Router B (defined as Slave device) will be up and take over all the jobs that Router A performs. Later, when Router A is powered on again, all the jobs will return to Router A.

3.14 How to Configure DNS Inbound Load Balance on Vigor 3900?

Vigor3900 can offer the mapped IP address to respond the DNS query coming from the remote end through the designate domain to reduce the loading of the network traffic.



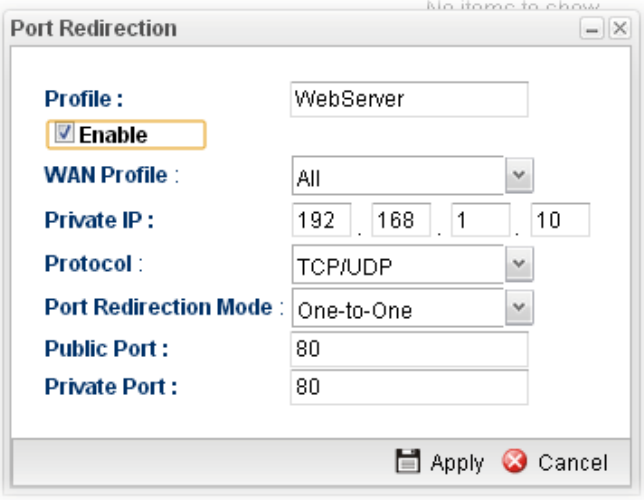
WAN1 IP Address: 1.1.1.1

WAN2 IP Address: 2.2.2.2

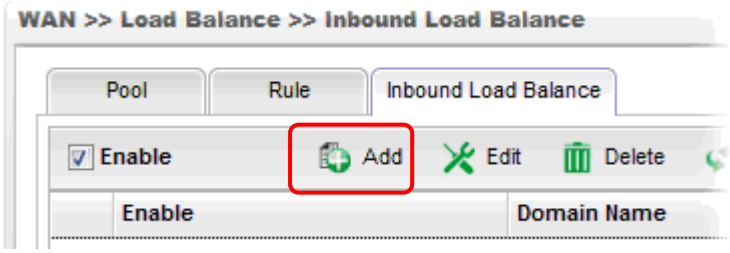
Inbound Load Balance allows Vigor3900 acting as a DNS Server to separate the traffic for each WAN interface according to the DNS query time. Follow the steps listed below to Configure DNS Inbound Load Balance.

Enabling Web service on the Router

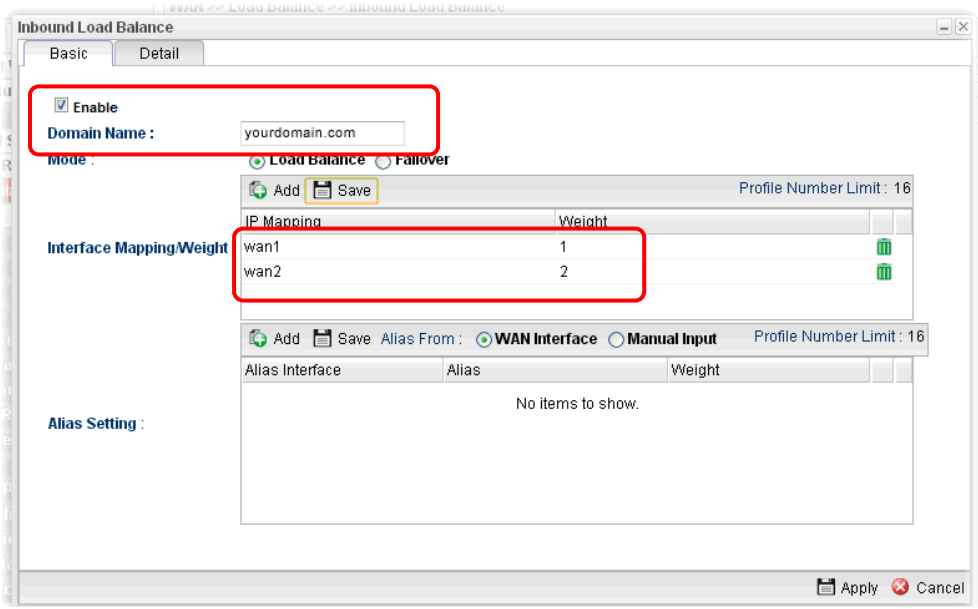
1. Open **NAT >> Port Redirection** to set up Port Redirection rules for the Web server. Click **Apply** to save the settings.



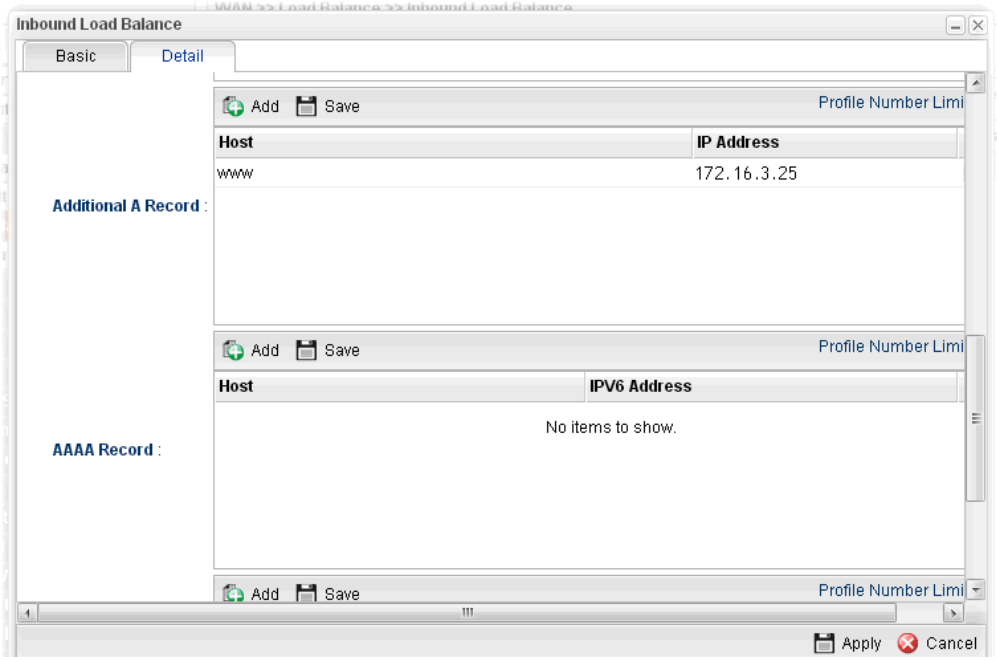
2. Open **WAN >> Load Balance** and click the tab of **Inbound Load Balance** to enable the service. Click **Add**.



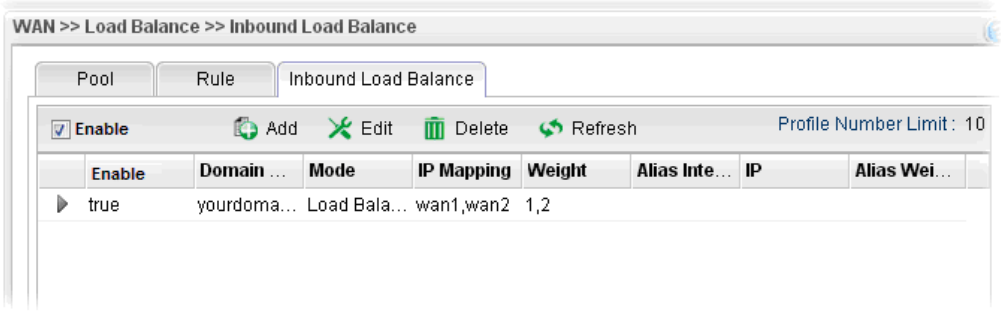
3. Add a profile named “yourdomain.com”. Define WAN1 weights 1 and WAN2 weights 2. It means the total DNS query time will be three, one will pass through WAN1; two will pass through WAN2.



4. Click the **Detail** tab and locate **Additional A Record**. Type “www” as the name of the **Host**, and type “192.168.1.10” as the **IP Address**.



5. Then click **Apply** to save the settings.



Now, make a test for inbound load balance.

Click **Start>> Run** and type **cmd**. Execute the command, nslookup, for DNS query test.

First DNS query

```
>www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
Name: www. yourdomain.com
Address: 1.1.1.1
```

Second DNS query

```
> www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
Name: www.yourdomain.com
Address: 2.2.2.2
```

Third DNS query

```
> www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
Name: www.yourdomain.com
Address: 2.2.2.2
```

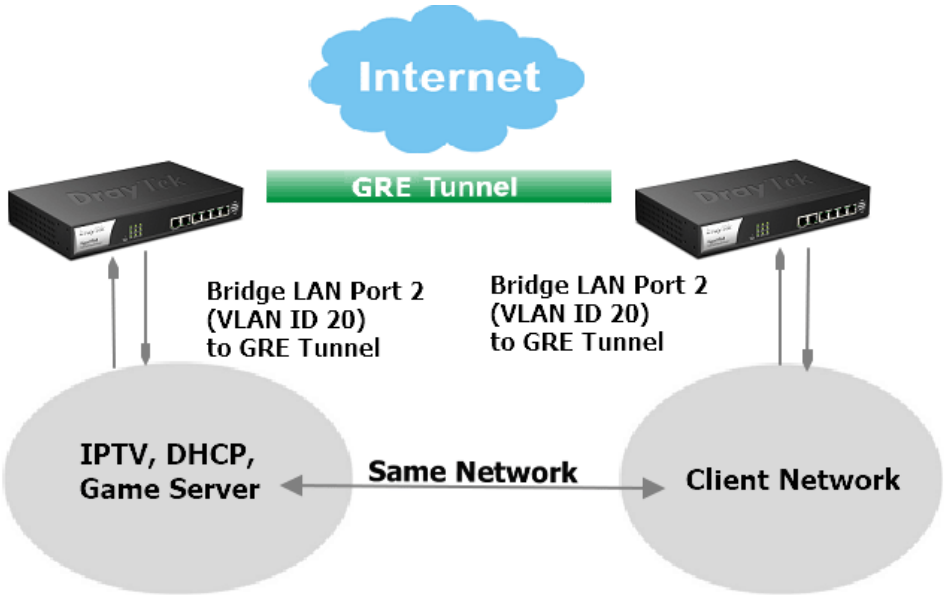
Note: It is recommended to clear cache before executing “nslookup” for DNS query.

3.15 How to Bridge LAN networks over GRE Tunnel between two Vigor3900s?

Since firmware version 1.4.0, Vigor3900 supports bridging local network to another remote network by using GRE tunnel.

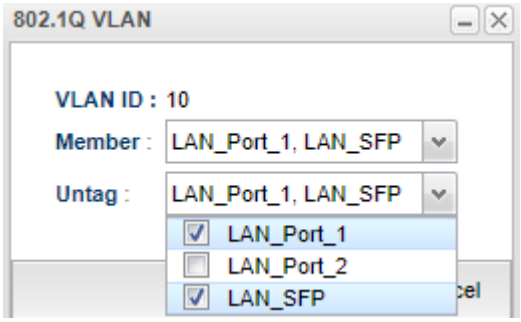
GRE tunnel is created between two Vigor3900s over the Internet. When the bridging over GRE function of the router is enabled, all Ethernet traffic, including ARP, DHCP, IGMP from the selected VLAN group will be bridged just as if there are a physical Ethernet interface and a cable between the two routers.

Take the scenario below as an example:



Below shows the configurations:

1. Go to **LAN >> Switch >> 802.1Q VLAN** page and edit the default 802.1Q VLAN ID 10 as follows:

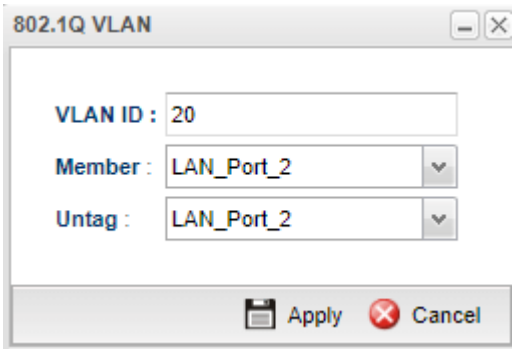


   (a) In Member, de-select LAN_Port_2,

   (b) In Untag, de-select LAN_Port_2,

   (c) Apply the setting.

2. In same page, click **Add** to add a new 802.1Q VLAN profile and edit the profile as follows:



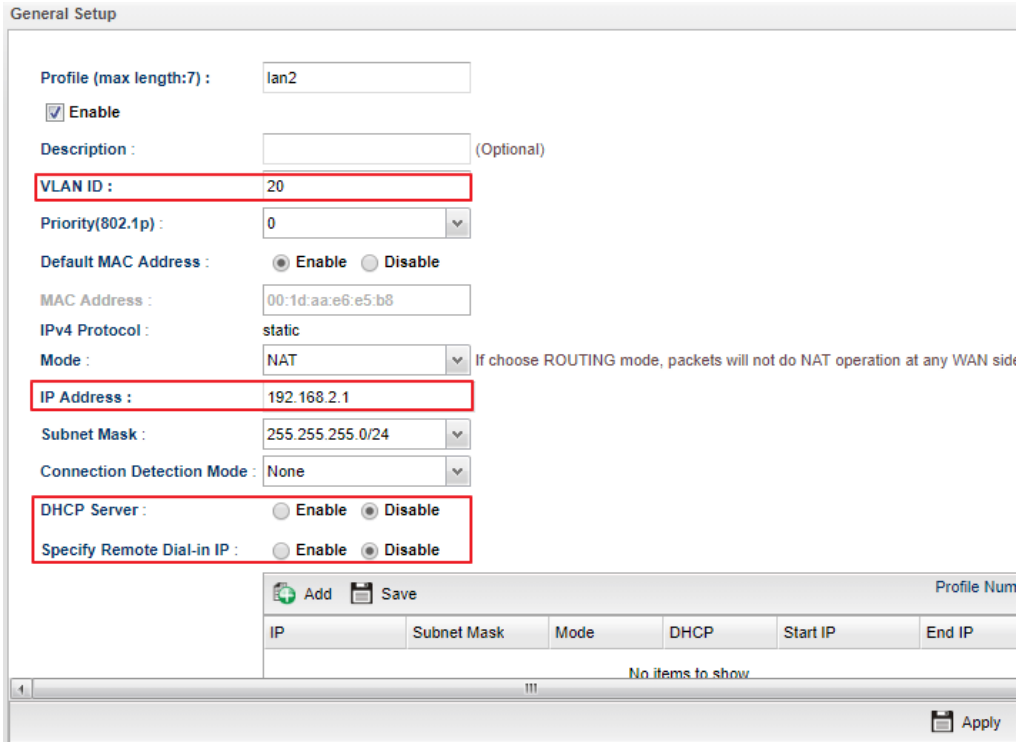
(a) Enter VLAN ID as 20.

(b) Select LAN_Port_2 as Member.

(c) Select LAN_Port_2 as Untag.

(d) Apply the settings.

3. Add a new LAN profile with VLAN ID 20 via **LAN >> General Setup** page, edit the profile as follows:



(a) Input LAN Profile Name.

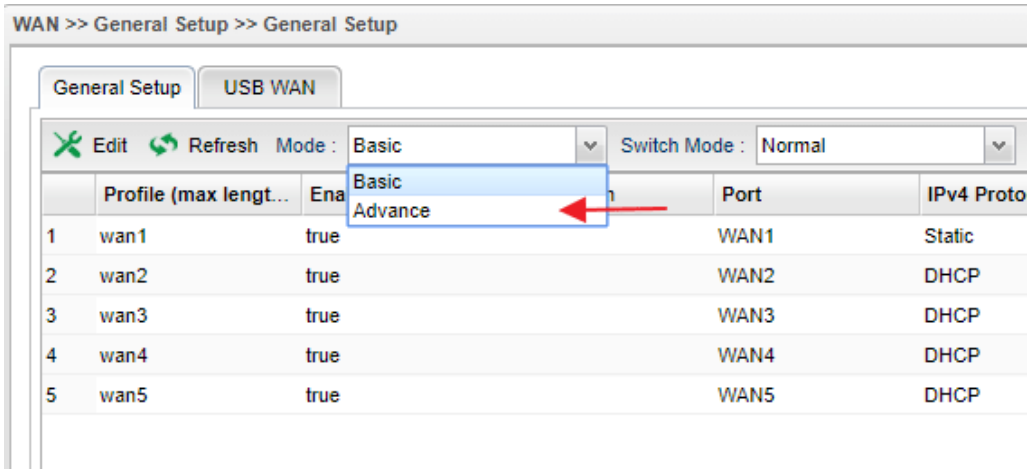
(b) Input the VLAN ID 20 (The VLAN ID must be same to the remote Vigor3900).

(c) Input the LAN IP address as 192.168.2.1 (This IP can be any IP and we just need to ensure it won't conflict with the IP in the bridge networks).

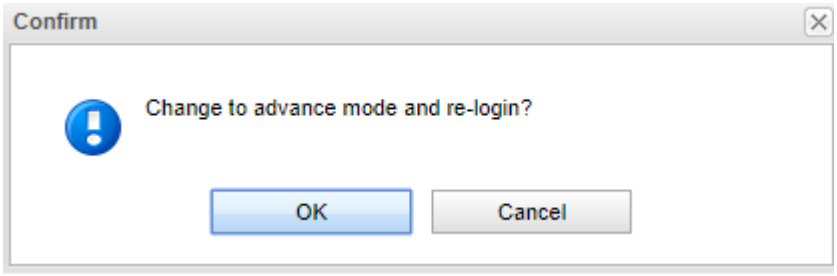
(d) Disable DHCP Server.

(e) Apply the configurations.

4. Go to **WAN >>General Setup** page. Change the Mode from **Basic** to **Advance**.

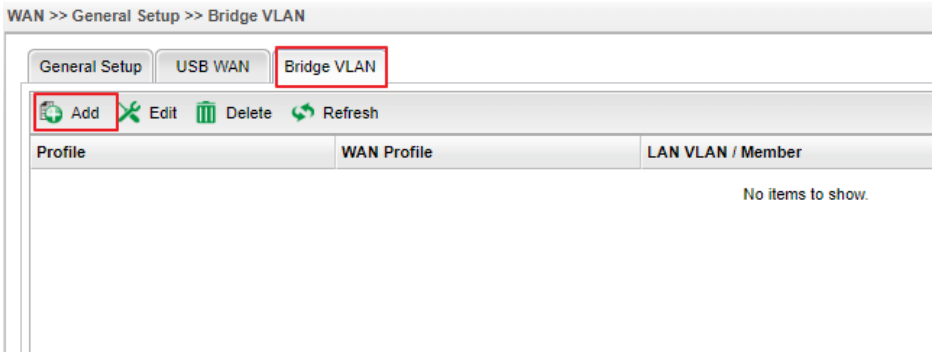


5. A Confirm window will pop up. Click **OK** to continue.

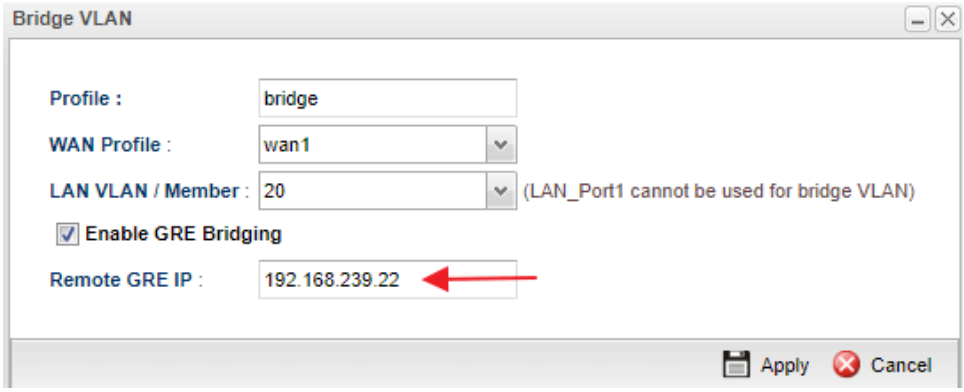


6. Login Vigor3900 again and go to **WAN >>General Setup** page.

   Bridge VLAN tab is visible in Advance mode. Click Add to create a **Bridge VLAN** profile.



7. Edit the Bridge VLAN profile as show below:



   (a) Input LAN Profile Name.

(b) Select wan1 for WAN profile.

(c) Select LAN VLAN ID 20.

(d) Tick Enable GRE Bridging option.

(e) Enter Peer Vigor3900's WAN IP or Domain Name as Remote GRE IP.

(f) Apply the settings.

8. Do similar configurations on the remote Vigor3900.

   Please note the VLAN ID Group must be same and the Remote GRE IP should be configured to Vigor3900's WAN IP or Domain Name.

9. Once we finished the above configurations on both Vigor3900s, GRE tunnel will be up.

   Vigor3900 will forward all the Ethernet Packets receiving from the specified VLAN ID Group / the LAN ports over the GRE tunnel.

   When the remote Vigor3900 receiving such packets, it will remove the GRE IP header and send the packets to the ports according to the VLAN ID.

Note:
1. GRE tunnel is up once the GRE configuration is enabled. It is not possible to check the GRE tunnel status on Vigor3900.
2. To bridge more than one VLAN IDs over the GRE tunnel is possible.
   We just need to ensure the VLAN IDs are configured well on both Vigor3900s.
3. Vigor3900 only bridges the packets from and to the GRE tunnel.
   It is not possible to let clients in site A access Internet through Vigor3900 in site B.

Chapter 4: Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to chapter 3.

4.1 WAN Setup

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **WAN** group and click the **General Setup** link.

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

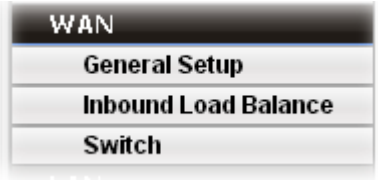
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the 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.



4.1.1 General Setup

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

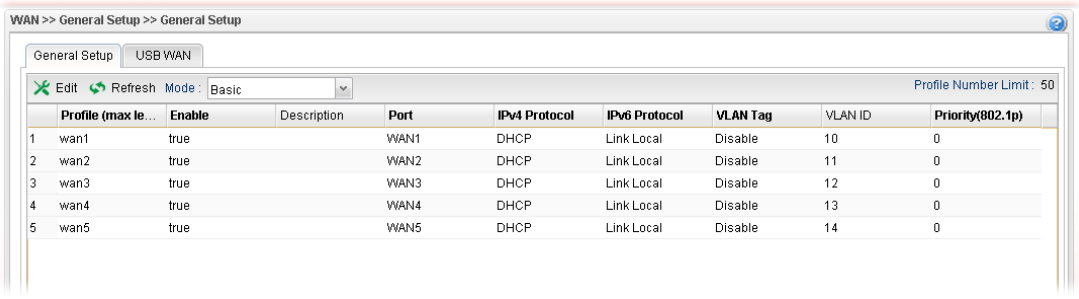
This router supports multi-WAN function. It allows users to access Internet and combine the bandwidth of the WAN profiles to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such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

There are two modes for you to choose for setting a WAN profile. **Basic** mode allows you to view and edit the existing WAN profile. However, **Advance** mode allows you to **define** new WAN profile.

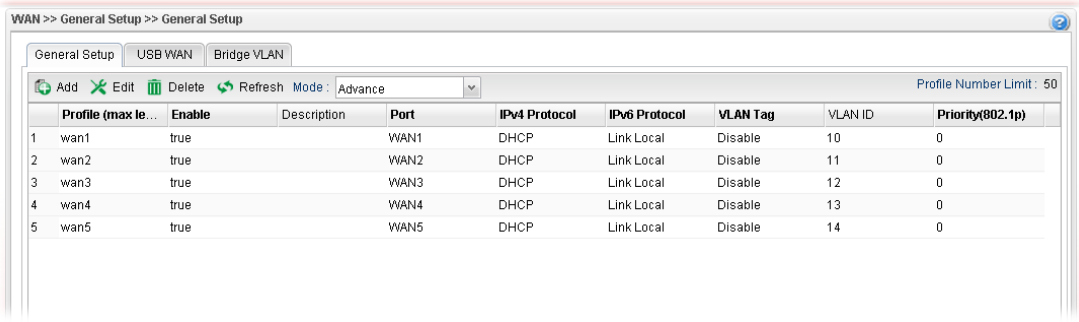
When you switch the Mode setting from Advance to Basic or from Basic to Advance, the system will ask you to re-login web configuration interface to activate some parameters.

Note: Some menu items (e.g., Bridge VLAN) are available only under Advance Mode.

Web Page in Basic Mode

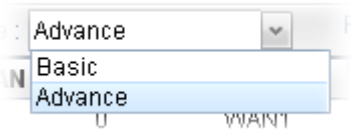


Web Page in Advance Mode



Each item will be explained as follows:

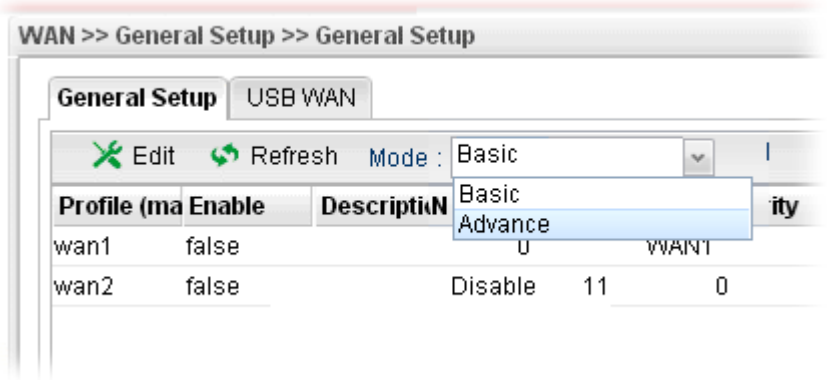
Item	Description
Add	Add a new WAN profile. Such function is available in

	Advance mode only.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected WAN profile. Such function is available in Advance mode only. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Mode	Specify the mode for adding /editing (Advance) new WAN profile or just editing (Basic) existing WAN profile. 
Profile Number Limit	Display the total number (50) of the profiles to be created.
Profile (max length:7)	Display the profile name.
Enable	Display the status of the profile. False means disabled; True means enabled.
Description	Display a brief explanation for such profile.
Port	Display the physical WAN interface for such profile.
IPv4 Protocol Type	Display the IPv4 protocol selected by the profile.
IPv6 Protocol Type	Display the IPv6 protocol selected by the profile.
VLAN Tag	Display if the function is enabled or not. If the data transmitted with tag, **Enable** will be displayed in this field. Otherwise, **Disable** will be shown instead.
VLAN ID	Display the VLAN ID of the profile.
Priority(802.1p)	Display the level of the priority for such profile.

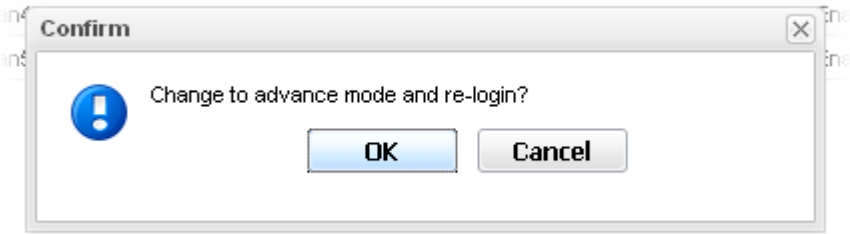
4.1.1.1 Ethernet WAN Profiles

How to add a new WAN profile:

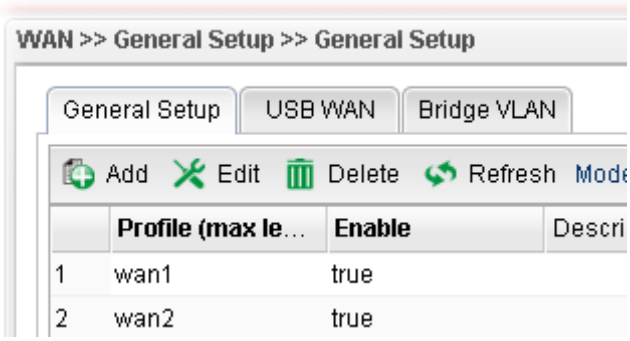
1. If the router is under **Basic** mode, you have to switch into **Advance** mode. If the router is under **Advance** mode, go to Step 4 directly.



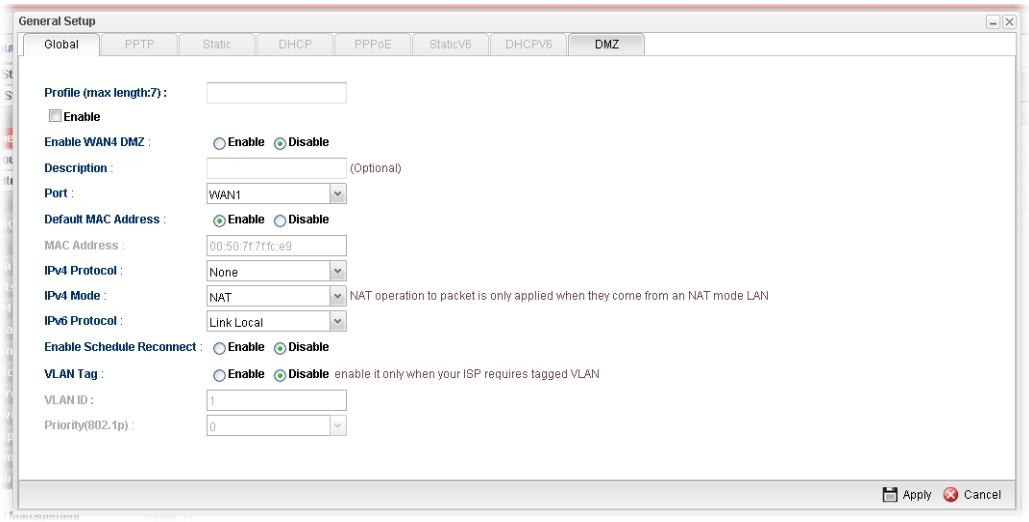
2. A confirmation dialog will appear. Click **OK** to apply the related settings for **Advance** mode.



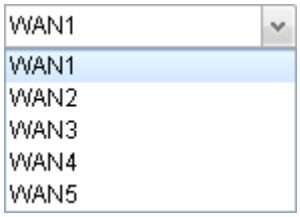
3. Re-login the system.
4. Open **WAN>>General Setup**.

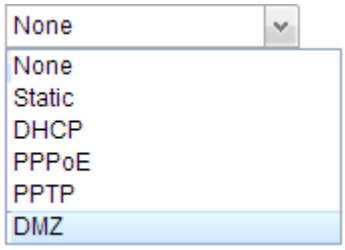
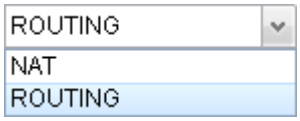
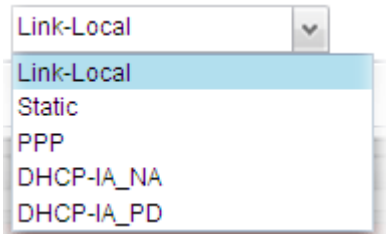


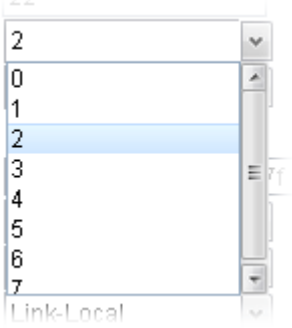
5. Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.



Available parameters are listed as follows:

Item	Description
Profile (max length:7)	Type a name (less than 7 characters) for such profile.
Enable	Check this box to enable such profile.
Enable WAN4 DMZ	WAN DMZ is the feature to use WAN Port 4 as a DMZ port. The host or server connecting to DMZ port will behave like a neutral zone between a company's private network and the outside public network. The server connecting to DMZ port can provide services from the Internet and still have the protection of Firewall. **Enabled** - DMZ is separated from company's local LAN network by default. It improves the security and can avoid the attacking events happening between LAN and DMZ networks.
Description	Give the brief description for such profile.
Port	Choose the physical WAN interface for such profile. 
Default MAC Address	**Enable** – Click it to enable the default MAC address for such profile. **Disable** – Click it to type the MAC address manually for such profile.
MAC Address	Specify the MAC address for such profile. In default, the system will determine it automatically.

IPv4 Protocol	There are several connection modes for you to specify for IPv4 protocol type. Each mode will bring up different web page.  The DMZ protocol is available for WAN4 profile only.
IPv4 Mode	Determine such profile will be used for. 
IPv6 Protocol	There are four connection modes for you to specify for IPv6 protocol type. Each mode will bring up different web page. 
Enable Schedule Reconnect	**Enable** – Click it to enable the function of reconnecting the network automatically within the time schedule. **Disable** – Click it to disable the schedule reconnect function.
Schedule Time Object	Choose the time object profile to be applied by such WAN.
VLAN Tag	**Enable** – Click it to enable the function of VLAN Tag. Data transmitted through the router will be tagged with specified number for identification. **Disable** – Click it to disable the function of VLAN Tag. Data transmitted through the router will not be tagged with any number.
VLAN ID	Type the VLAN ID number for such profile.
Priority(802.1p)	Type the packet priority number for such VLAN. The range is from 0 to 7.

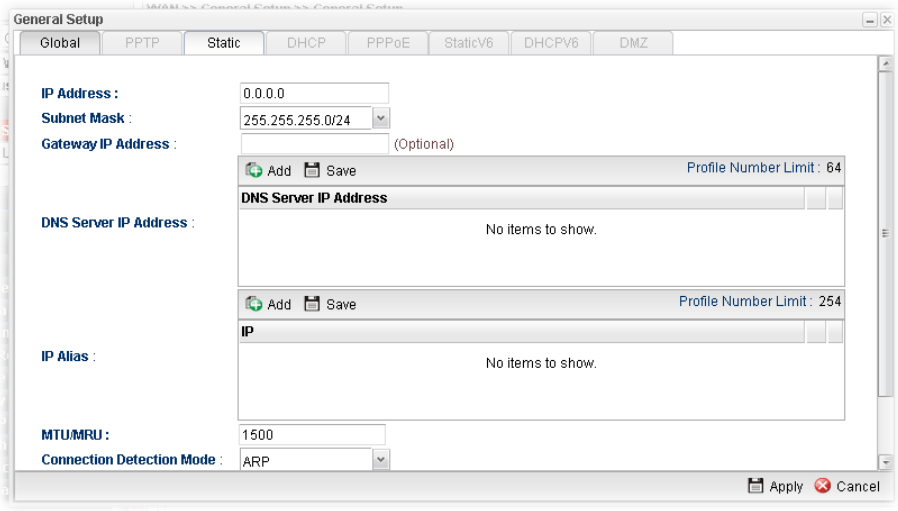
	
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

General Settings allows you to enable the profile, give a brief explanation for such profile, specify the VLAN ID, specify MAC address, choose IPv4 and IPv6 protocol, and specify the mode of the data transmission (**NAT** or **Routing**).

Note: The DMZ tab is available for WAN4 profile only.

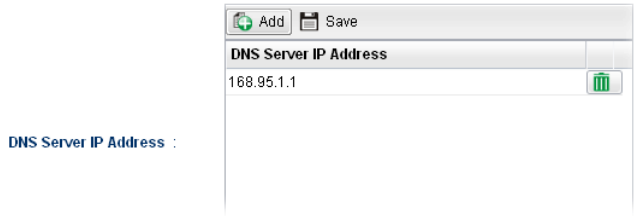
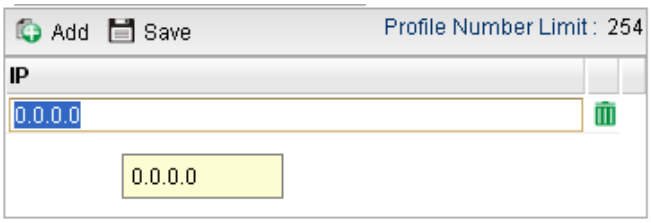
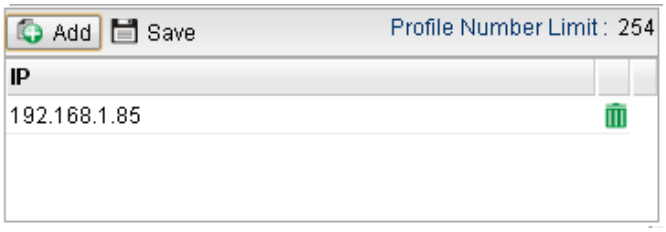
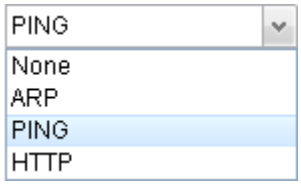
Different IPv4 and IPv6 protocol types specified will bring up different configuration web page.

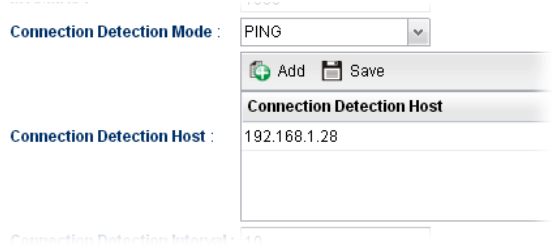
- ***If you choose Static as IPv4 protocol type, click the Static Tab to open the following page:***



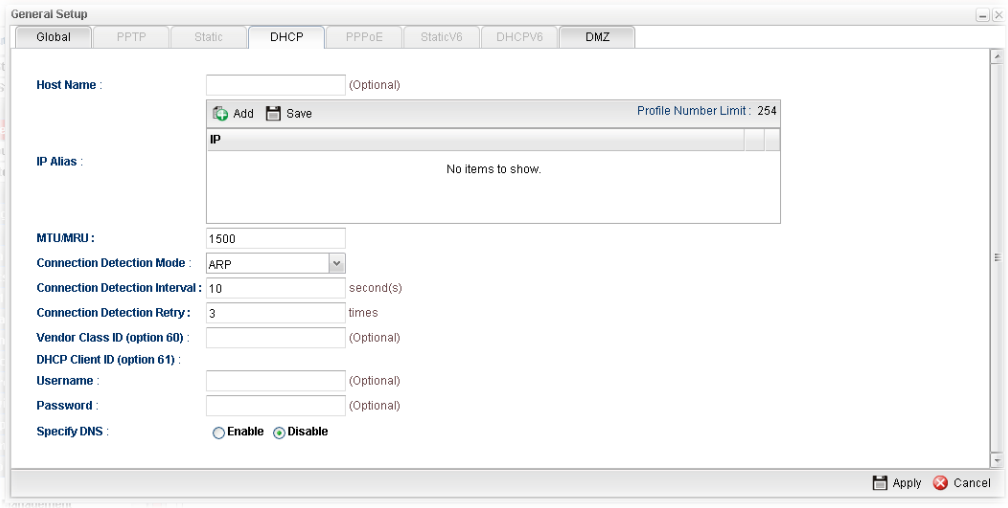
Available parameters are listed as follows:

Item	Description
IP Address	Type the IP address specified for such profile.
Subnet Mask	Use the drop down list to choose the subnet mask for such profile.
Gateway IP Address	Type the gateway address for such profile.
DNS Server IP Address	Type a public IP address as the primary DNS (Domain Name Server). To add a new IP address, simply place the mouse cursor on this filed. The following dialog will appear.

	 **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny boxes one by one.  **Save** – Click this button to save the setting.  – click the icon to remove the selected entry.
MTU/MRU	Type the value of MTU/MRU. The default value is 1500.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are three ways **ARP**, **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	**Add** – click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN

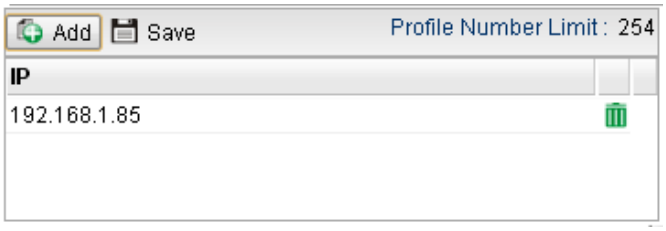
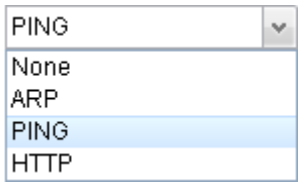
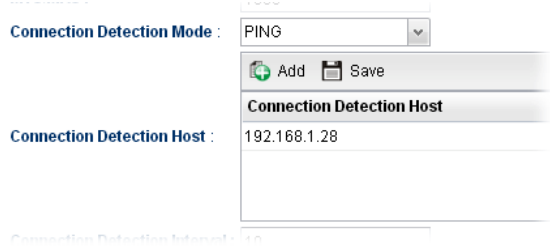
	interface will be regarded as breaking down. This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**.  **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

- ***If you choose DHCP as IPv4 protocol type, click the DHCP Tab to open the following page:***



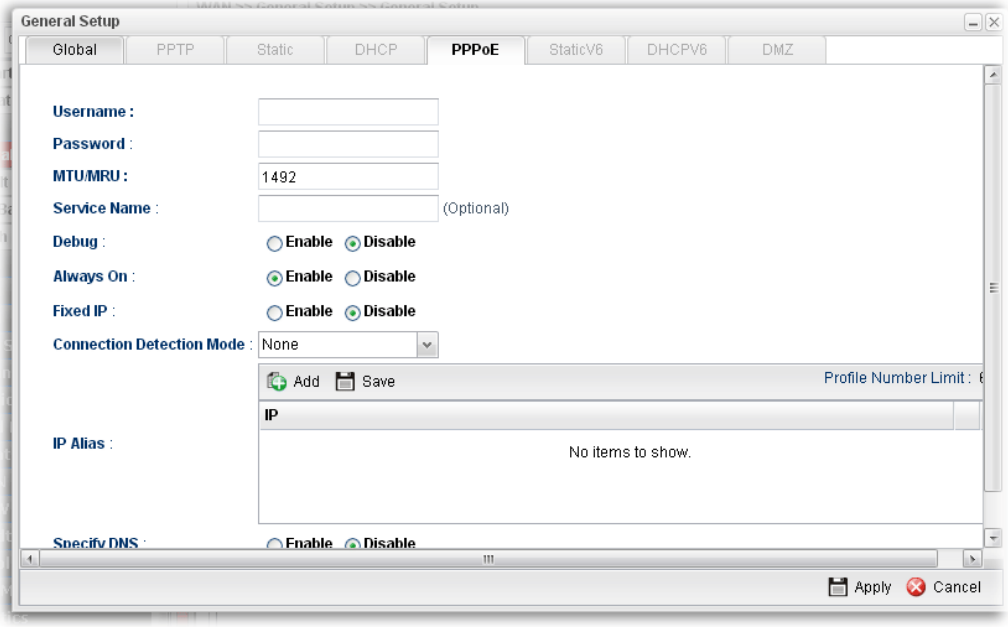
Available parameters are listed as follows:

Item	Description
Host Name (Optional)	Type a name as the host name for identification.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – To add a new IP address, click **Add.** Type the IP

	address and use the drop down list to specify the subnet mask. Next, click **Save**. The new one will be added and displayed on the field under the box.  **Save –** click this button to save the setting. – click the icon to remove the selected entry.
MTU/MRU	It means Max Transmit Unit for packet. The default setting is 1500.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are three ways **ARP**, **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	**Add** – click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**.  **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Vendor Class ID (option 60)	It is used to identify the vendor type and the configuration of a DHCP client.

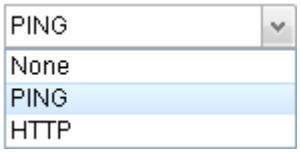
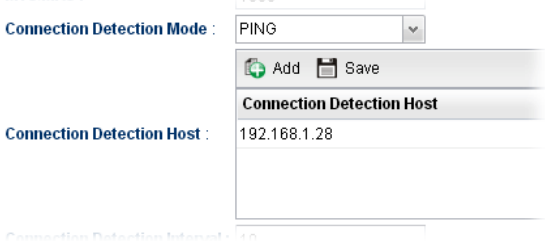
DHCP Client ID (option 61)	Type a string (in the field of Username) for identification of client. It is required for the mode, DHCP (option 61). Specify username and password as the DHCP client identifier for some ISP. **Username** – Type a name for authentication. **Password** – It is optional. If you want, simply type a password for authentication if you want.
Specify DNS	**Enable** – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. **Disable** – Click it to disable the function of DNS specified.
DNS	**Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

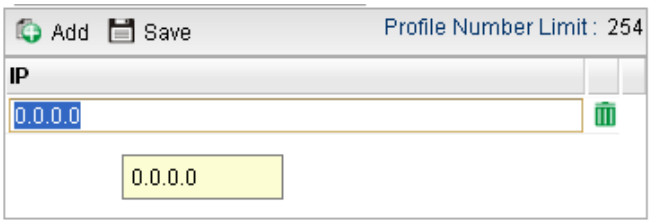
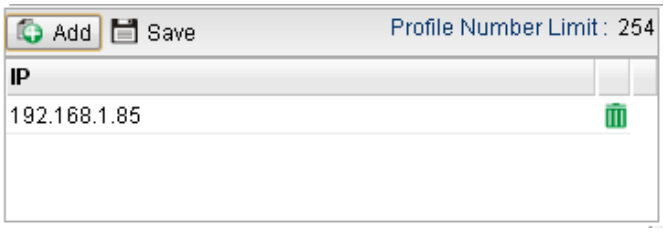
- ***If you choose PPPoE as IPv4 protocol type, click the PPPoE Tab to open the following page:***



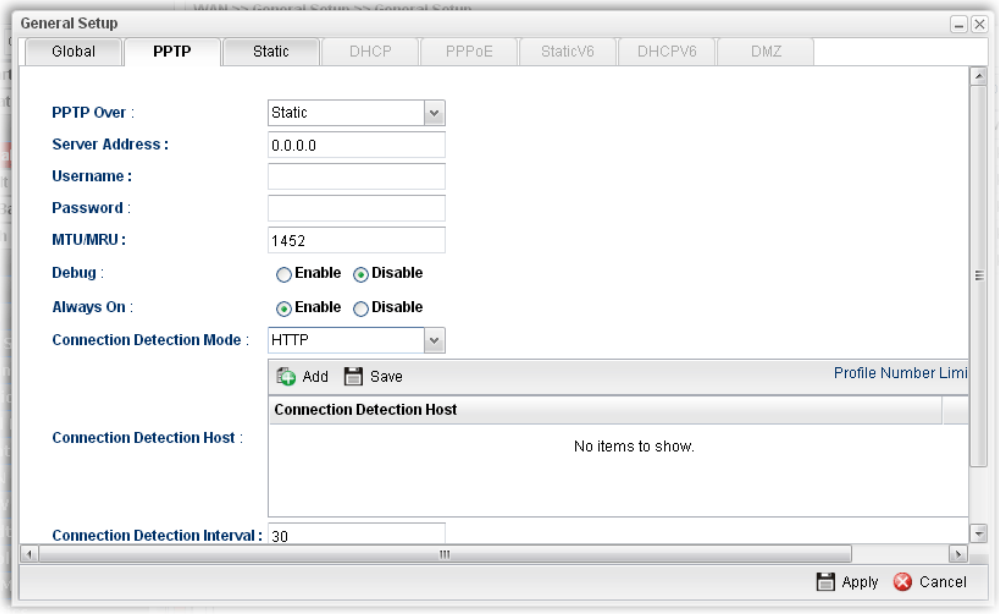
Available parameters are listed as follows:

Item	Description
Username	Type the user name offered by your ISP.
Password	Type the password offered by your ISP.
MTU/MRU	Type the value of MTU/MRU. The default value is 1492.
Service Name	This is an optional setting. Some ISP will offer such

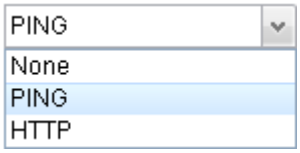
	information and ask you to type the same data on this field.
Debug	Click **Enable** to display the PPPoE debug message in Syslog. The default setting is **Disable**.
Always On	**Enable** – Click it to enable the function of Always On. The router will keep network connection all the time. **Disable** – Click it to disable the function of Always On.
Fixed IP	**Enable** – Click it to enable the function of fixed IP. **Disable** – Click it to disable the function of fixed IP.
Fixed IP Address	Type the IP address in the boxes.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field. Use the default setting. **Add** – Click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down.  **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny

	boxes one by one.  **Save** – After finished the IP address configuration, click **Save** to save the setting onto the router.  – Click the icon to remove the selected entry.
Specify DNS	**Enable** – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. **Disable** – Click it to disable the function of DNS specified.
DNS	**Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

- ***If you choose PPTP as IPv4 protocol type, click the PPTP Tab to open the following page:***



Available parameters are listed as follows:

Item	Description
PPTP Over	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.** Choose a proper protocol, **Static** or **DHCP**. After finished the settings in such page, you need to open the Static or DHCP tab for configuring the settings there.
Server Address	Type the IP address of PPTP server offered by your ISP.
Username	Type the user name offered by your ISP.
Password	Type the password offered by your ISP.
MTU/MRU	Type the value of MTU/MRU. The default value is 1452.
Debug	Click **Enable** to display the PPTP debug message in syslog. The default setting is **Disable**.
Always On	**Enable** – Click it to enable the function of Always On. The router will keep network connection all the time. **Disable** – Click it to disable the function of Always On.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field.

Detection Host	Use the default setting. **Add** – Click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Apply	After finished the PPTP configuration, please click **Static** or **DHCP** (according to the PPTP Over Protocol setting) to modify the Static/DHCP configuration for such profile. Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

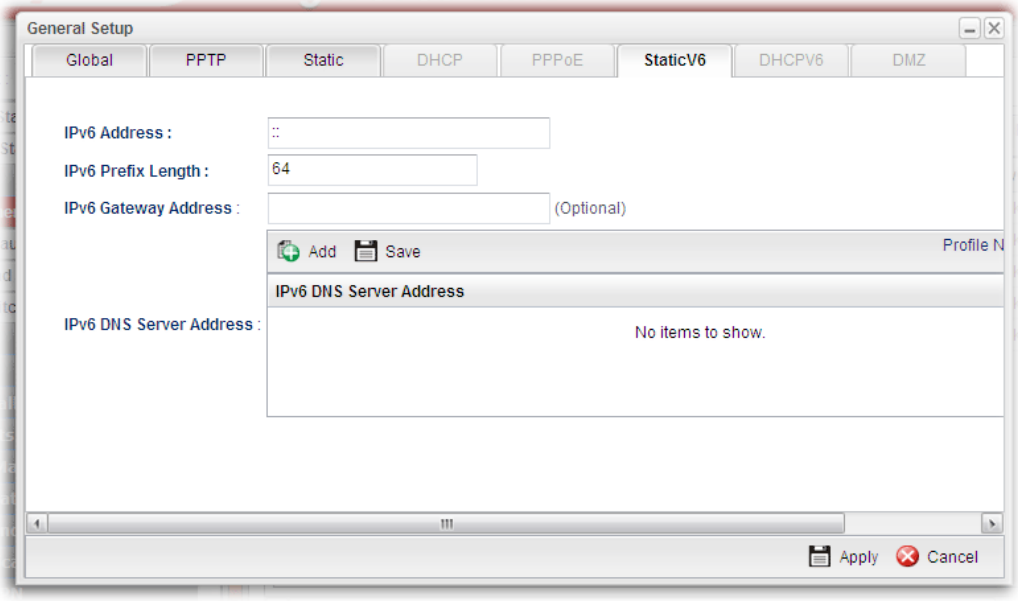
- ***If you choose Link-Local as IPv6 protocol type***

  Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/64**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.

- ***If you choose PPP as IPv6 protocol type***

  Simply refer to the section of "***If you choose PPPoE as IPv4 protocol type, click the PPPoE Tab to open the following page"*** for detailed information.

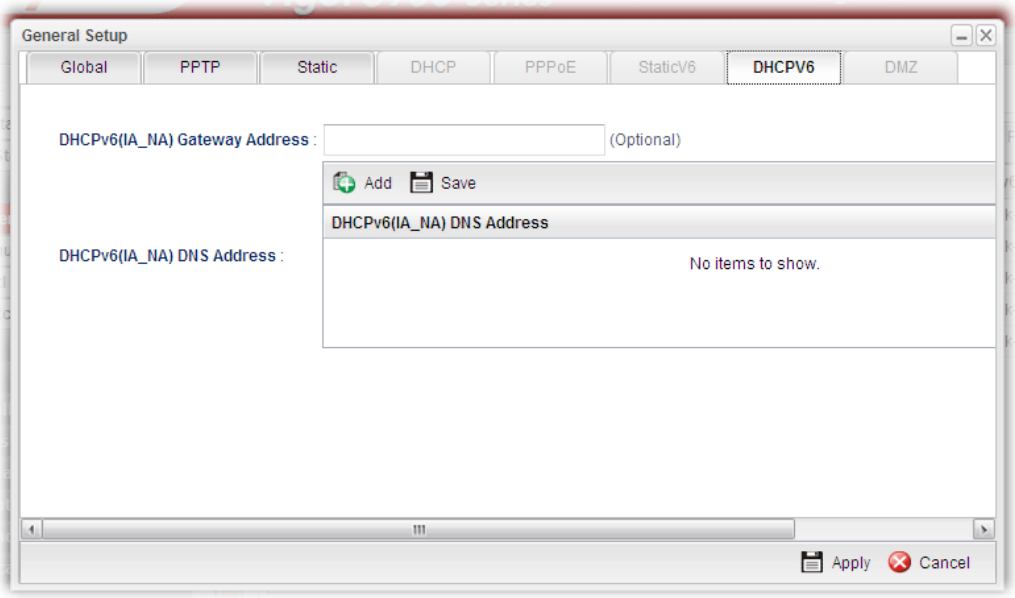
- ***If you choose Static as IPv6 protocol type, click the StaticV6 tab to open the following page:***



Available parameters are listed as follows:

Item	Description
IPv6 Address	Type the IP address for such protocol.
IPv6 Prefix Length	Type your IPv6 address prefix length.
IPv6 Gateway Address	Type your IPv6 gateway address.
IPv6 DNS Server Address	Type your IPv6 primary DNS Server address. **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

- ***If you choose DHCP-IA_NA as IPv6 protocol type, click the DHCPV6 Tab to open the following page:***



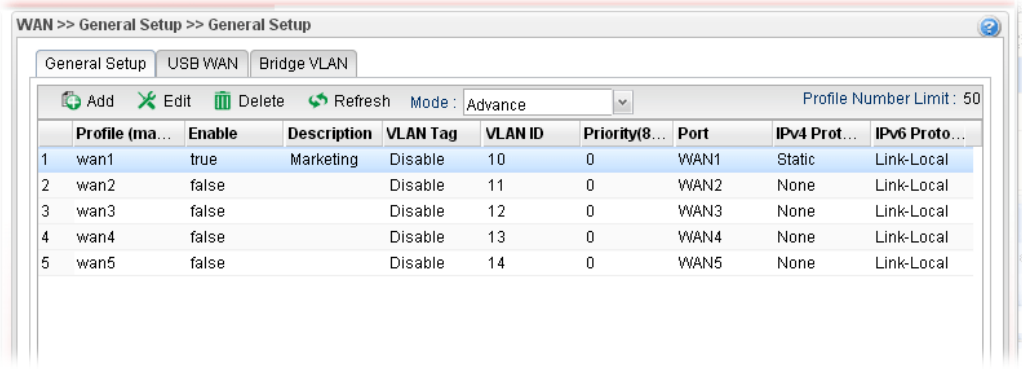
Available parameters are listed as follows:

Item	Description
DHCP (IA_NA) Gateway Address	Type the gateway IP address for IPv6 DHCP IA_NA mode.
DHCP (IA_NA) DNS Address	Type your IPv6 primary DNS Server address. **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

- ***If you choose DHCP-IA_PD as IPv6 protocol type***

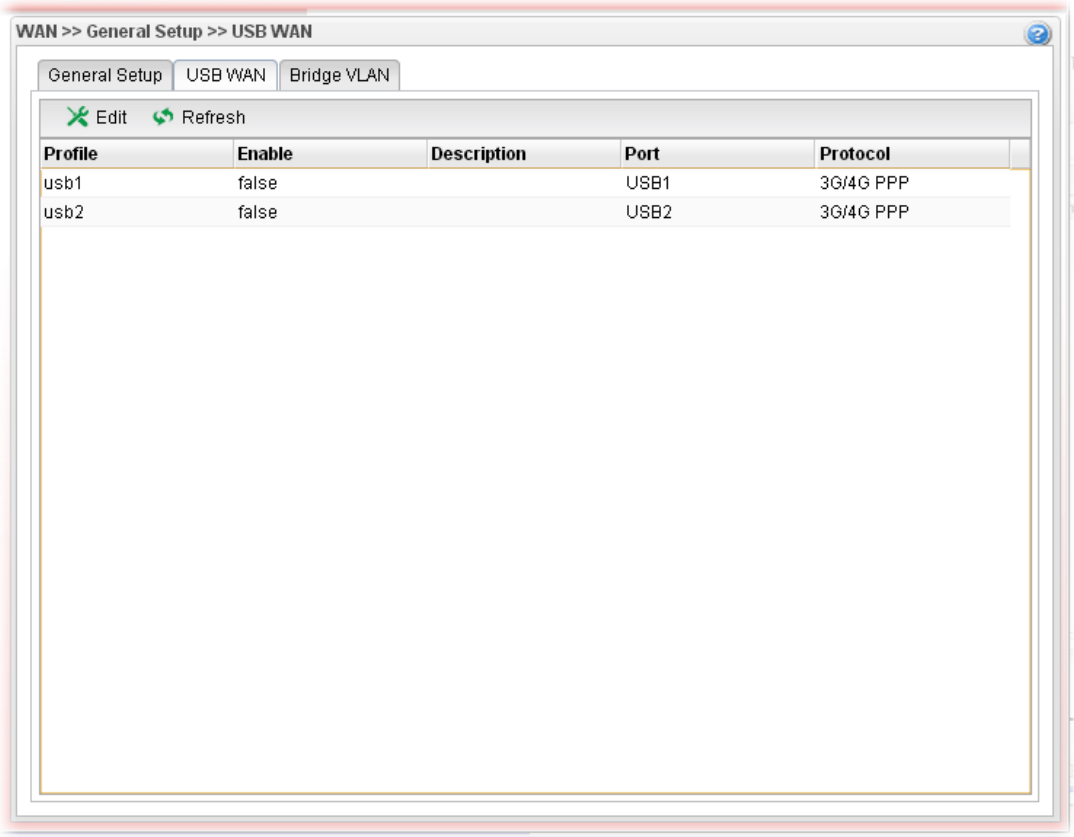
  It is not necessary for you to configure any web page.

6. Enter all the settings and click **Apply**. The new added profile will be shown as below.



4.1.1.2 USB WAN Profiles

Open **WAN>>General Setup** and click the **USB WAN** tab.

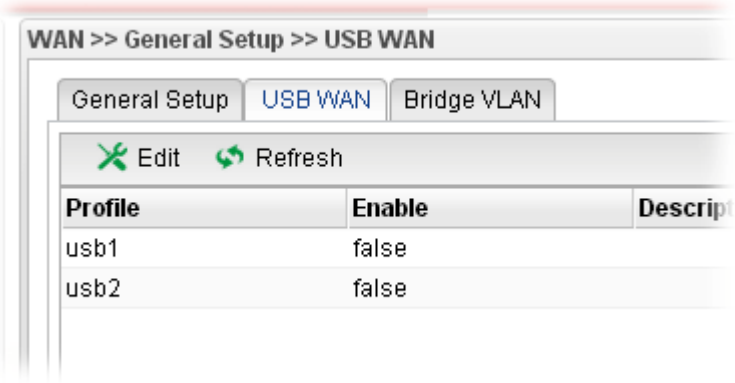


Each item will be explained as follows:

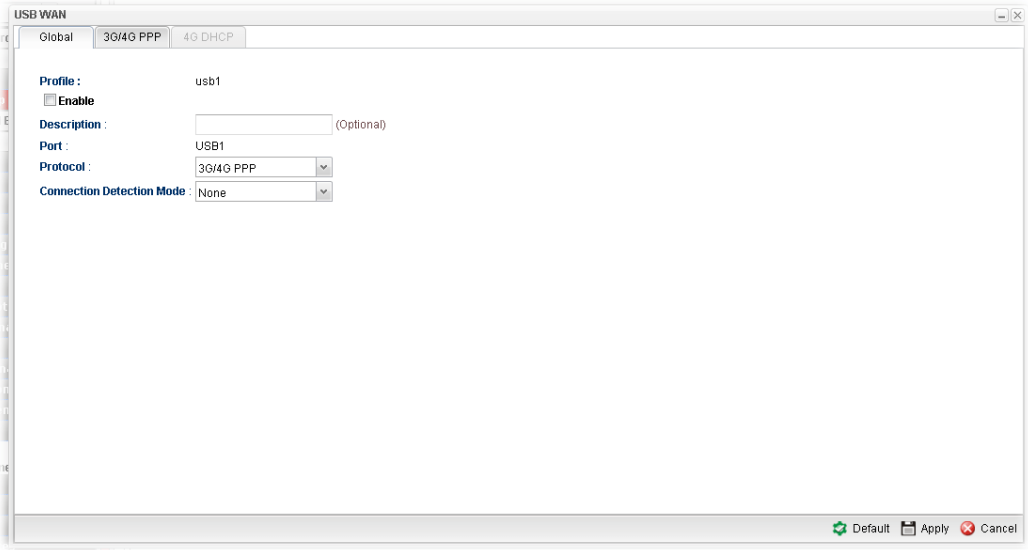
Item	Description
Edit	Modify the selected USB WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the profile name.
Enable	Display the status of the profile. False means disabled; True means enabled.
Description	Display a brief explanation for such profile.
Port	Display the physical WAN interface for such profile.
Protocol	Display the protocol selected by the profile.

How to edit a new USB WAN profile

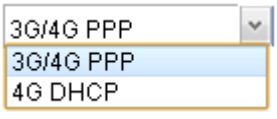
1. Choose one of the USB WAN profiles and click **Edit**.



2. The settings under **Global** tab are listed as below:

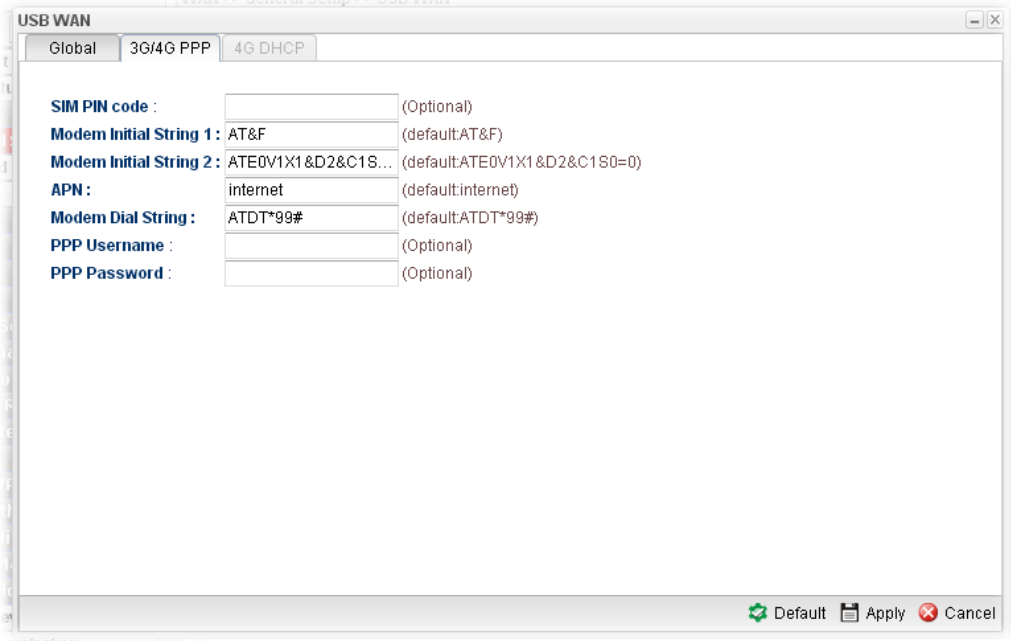


Available parameters are listed as follows:

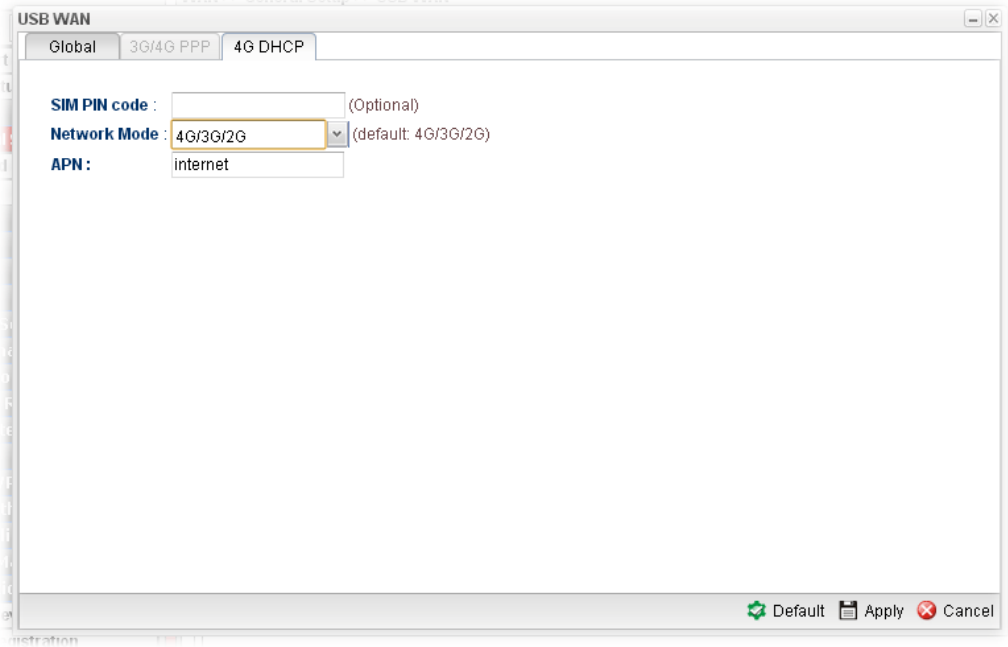
Item	Description
Profile	Display the name of the USB WAN profile.
Enable	Check it to enable the USB WAN profile.
Description	Give the brief description for such profile.
Port	Display the physical WAN interface for such profile.
Protocol	Choose the connection mode for USB WAN. 
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field.

	Use the default setting. **Add** – Click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**. **Save** – Click this button to save the setting.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. After finished the settings above, click the 3G/4G PPP or 4G DHCP tab (based on the Protocol specified) to display the following page:

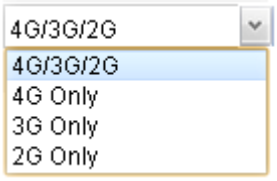


Or,

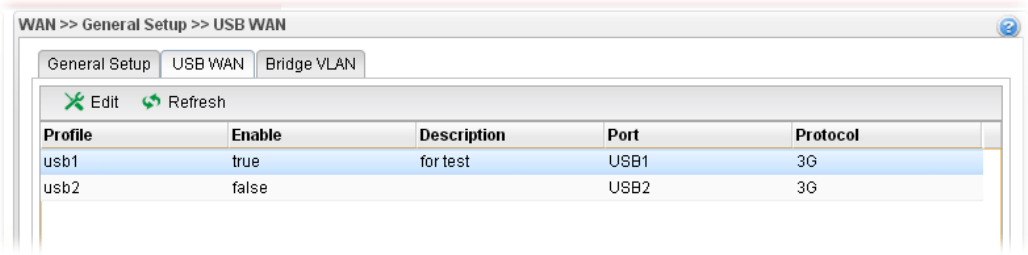


Available parameters are listed as follows:

Item	Description
3G/4G PPP	**SIM PIN code** -Type PIN code of the SIM card that will be used to access Internet. **Modem Initial String 1**-Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. **Modem Initial String 2**-The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. **APN** -APN means Access Point Name which is provided and required by some ISPs. Type the name. **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. **PPP Username** -Type the PPP username (optional). **PPP Password** -Type the PPP password (optional).
4G DHCP	**SIM Pin code** –Type PIN code of the SIM card that will be used to access Internet. **Network Mode** – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.

	 **APN Name** – APN means Access Point Name which is provided and required by some ISPs.
Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

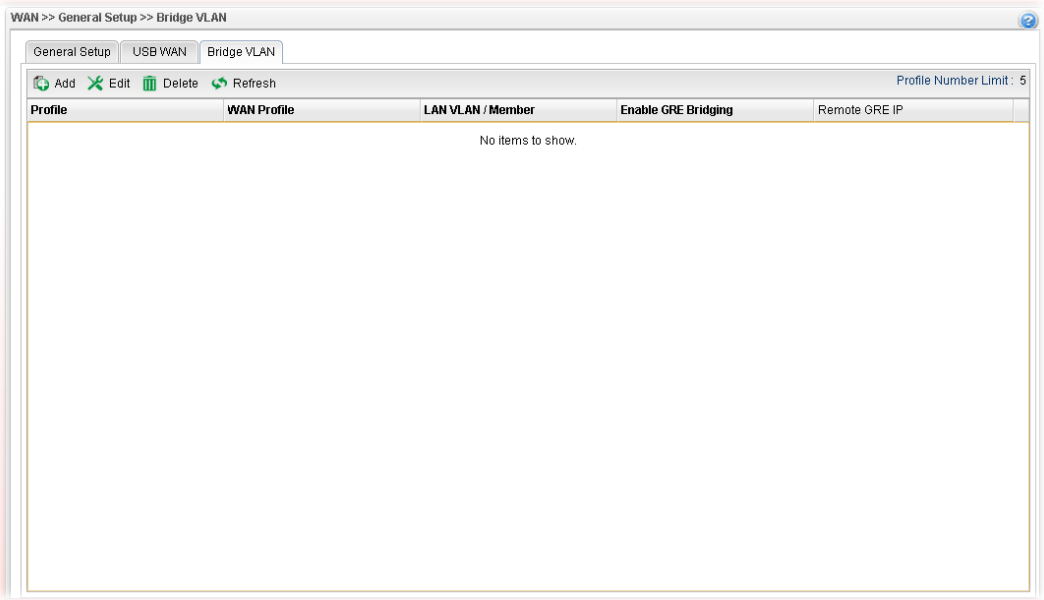
4. Enter all the settings and click **Apply**. The modified profile will be shown as below.



4.1.1.3 Bridge VLAN Profiles

Open **WAN>>General Setup** and click the **Bridge VLAN** tab.

It can specify a VLAN ID for WAN port and offers more advanced environmental application for the users through the bridge technique in WAN port and LAN port.

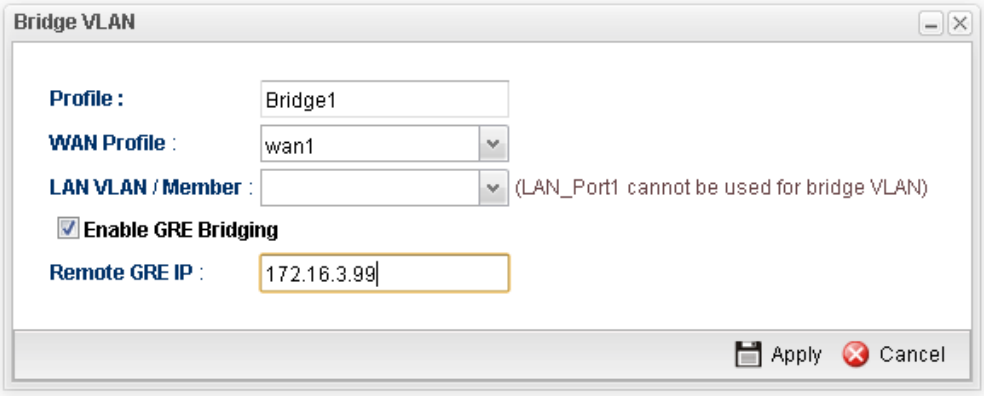


Each item will be explained as follows:

Item	Description
Add	Click to create a new profile.
Edit	Modify the selected USB WAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected WAN profile. Such function is available in Advance mode only. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the profile name.
WAN Profile	Display the WAN profile selected.
LAN VLAN/Member	Display VLAN ID number of the LAN port selected.

How to add a new bridge VLAN profile

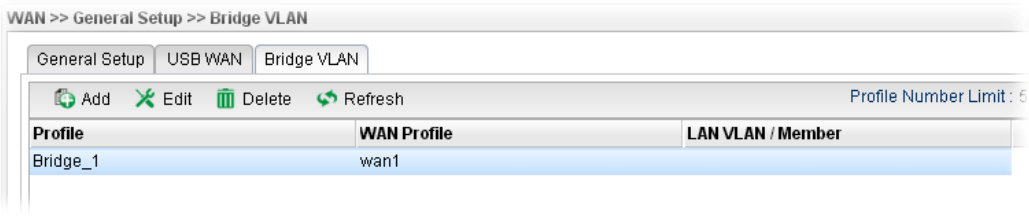
1. Click **Add.**
2. The settings under **Global** tab are listed as below:



Available parameters are listed as follows:

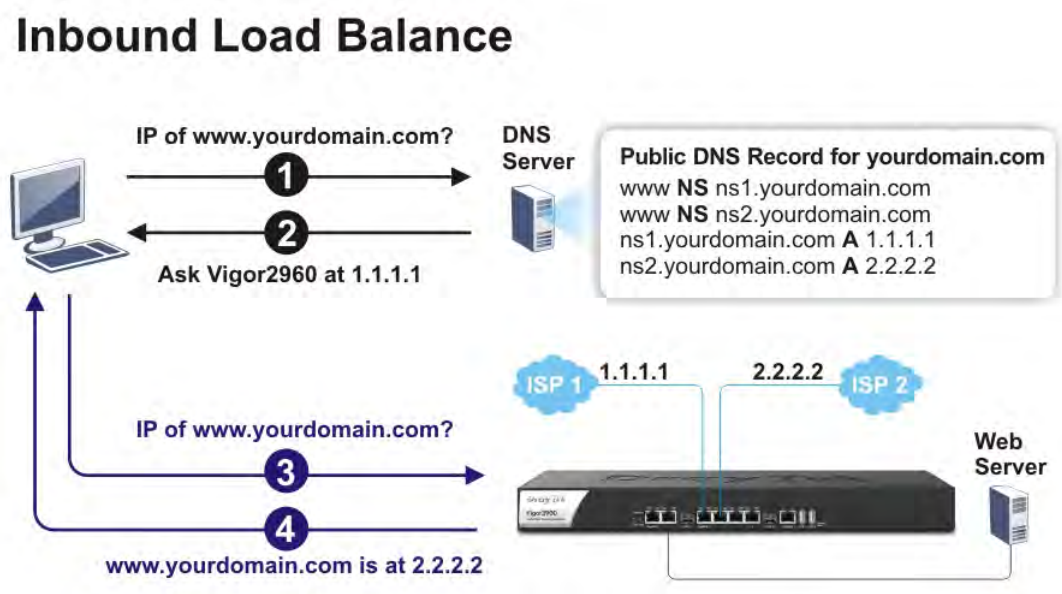
Item	Description
Profile	Type the name of the profile.
WAN Profile	Use the drop down list to choose the WAN interface.
LAN VLAN/Member	Choose a VLAN profile from the drop down list. You have to open **LAN>>Switch** page and click **802.1Q** VLAN for creating VLAN ID number bound with LAN port (802.1Q VLAN profile) first. Otherwise, no profiles will be displayed here for you to specify.
Enable GRE Bridging	Such function is used to bridge local network to remote network by using GRE tunnel to make both routers on the same network. For more detailed information, refer to *"3.15 How to Bridge LAN networks over GRE Tunnel between two Vigor3900s?"*.
Remote GRE IP	Enter the GRE IP of remote device.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. Enter all of the settings and click **Apply**. The modified profile will be shown as below.



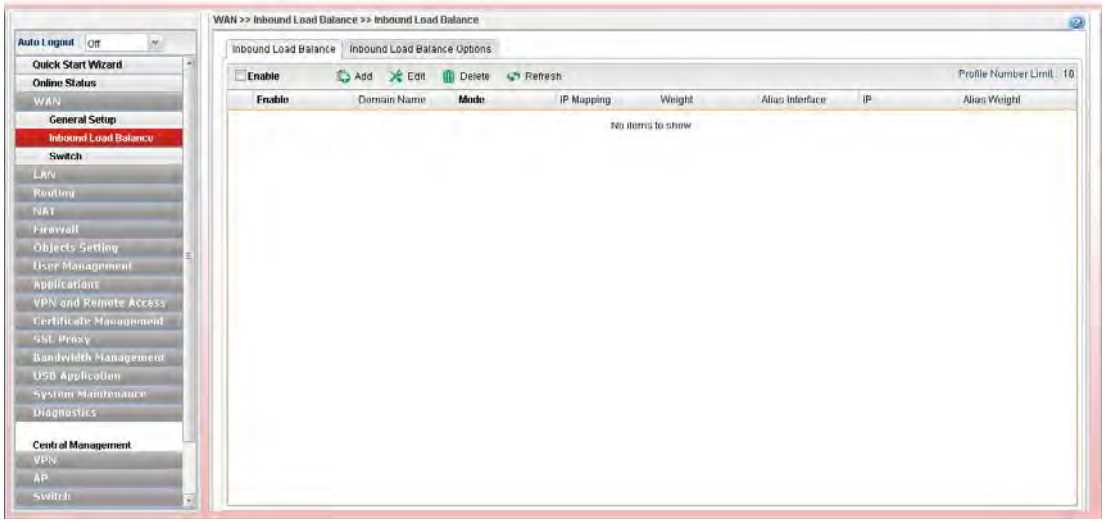
4.1.2 Inbound Load Balance

Vigor3900 can offer the mapped IP address to respond the DNS query coming from the remote end through the designate domain to reduce the loading of the network traffic.



4.1.2.1 Inbound Load Balance

Click **WAN>>Inbound Load Balance** and click the **Inbound Load Balance** tab.



Each item will be explained as follows:

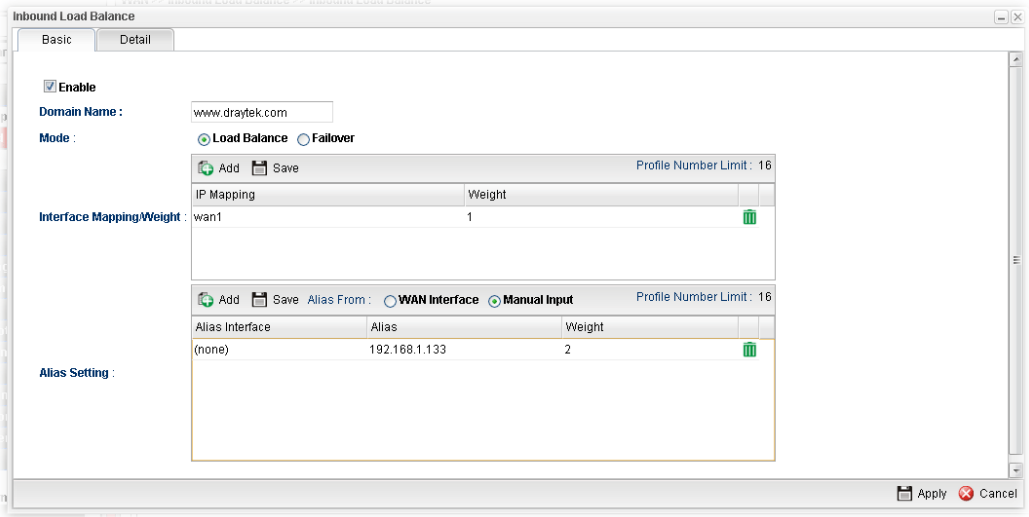
Item	Description
Enable	Check the box the enable inbound load balance function.
Add	Add a new WAN profile for inbound load balance.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.

Delete	Remove the selected WAN profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Enable	Display the status of the profile. False means disabled; True means enabled.
Domain Name	Display the domain name used by the profile.
Mode	Display the mode (failover or load balance) applied by the profile.
IP Mapping	Display the WAN interfaces used by the profile.
Weight	Display the weight(s) that WAN interface(s) used.
Alias Interface	Display the WAN interfaces used by the IP alias.
IP	Display the alias IP settings used by the profile.
Alias Weight	Display the weight that the above IP address used.

How to create a new Inbound Load Balance profile

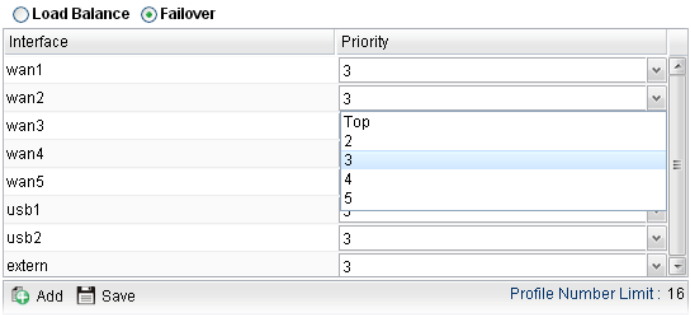
Such page allows you to create a new WAN profile for inbound load balance.

1. Open **WAN>>Inbound Load Balance**.
2. Simply click the **Add** button to open the following dialog.

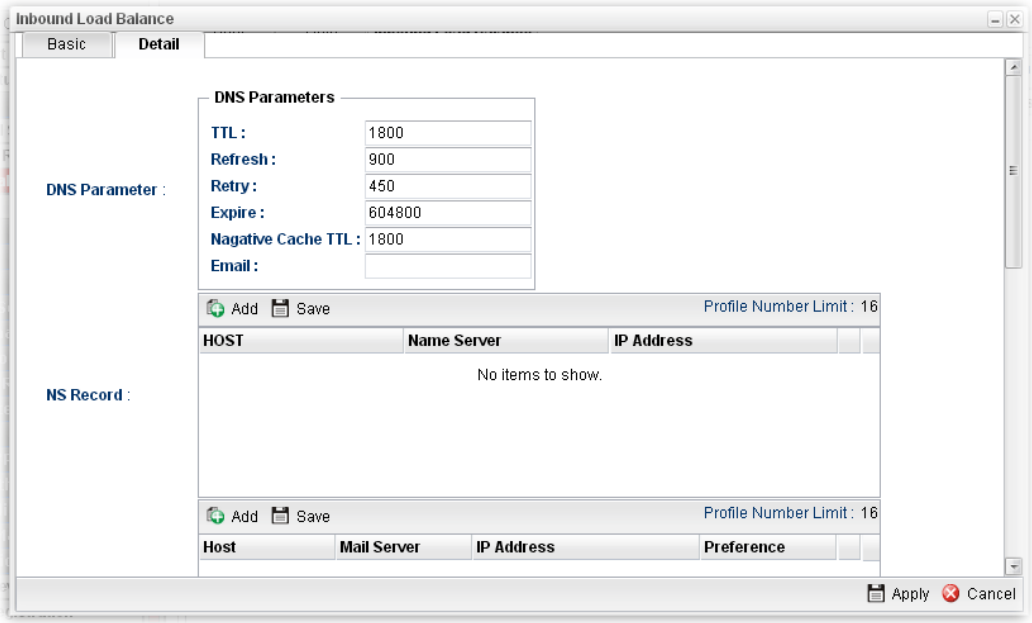


Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
Domain Name	Type an available domain name to serve the inbound load balance.
Mode	Specify the type (Load Balance or Failover) of the WAN profile for inbound load balance

Priority Setting	It is available only when **Failover** is selected as the Mode. There are five levels (Top, 2, 3, 4 and 5) which can be specified for WAN profiles (including default WAN profiles and user-defined WAN profiles). 
Interface Mapping/Weight	The domain name will inform the remote end with the IP address for DNS query asked by the remote end. The incoming query from the WAN interfaces specified in IP Mapping will be processed according to the weight value. **Add** – Click it to choose a WAN interface and weight. **Save** – Click it to save the settings. **IP Mapping** – Use the drop down list to choose a WAN interface profile which will be used by the domain. **Weight** – Use the drop down list to choose the one you want.
Alias Setting	The purpose of such setting is to specify a WAN IP address from the WAN interface or by typing it manually to respond DNS query. **Add** – Click it to add a new IP address. **Save** – Click it to save the settings. **Alias From WAN Interface** – The alias IP setting can be specified from existed WAN IP alias. **Alias From Manual Input** – The alias IP setting can be specified manually. The Alias Interface is not necessary for such method. **Alias Interface** –Use the drop down list to choose a WAN interface profile for the alias IP setting. **Alias** – Use the drop down list to choose an alias IP setting (for **Alias From WAN Interface**) or type an IP address manually (for **Alias From Manual Input**). **Weight** –Use the drop down list to choose the one you want.

3. After finished the settings on the **Basic** page, click the **Detail** Tab to open the following dialog.



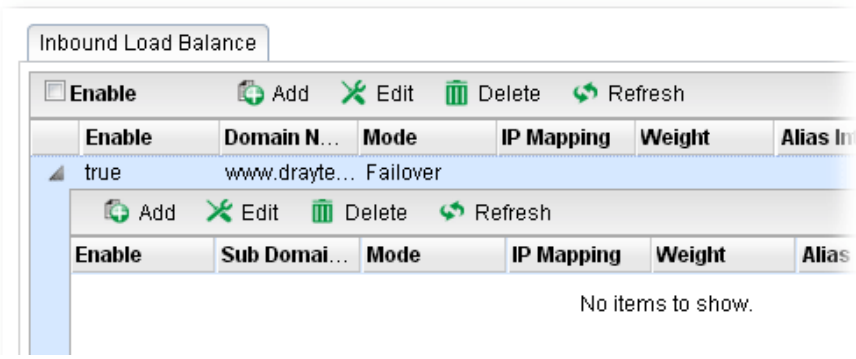
Available parameters are listed as follows:

Item	Description
DNS Parameter	To configure Vigor router as a DNS server, type the related information for applying the function of DNS. **TTL** – It means Time to live of a DNS response. Available setting range is from 0 to 2147483647. **Refresh** – Set the time for the PC in LAN to refresh the data. **Retry** – Set the times of retry if the PC fails to contact with Vigor router before the refreshing expired. **Expire** – PC stops responding to the query from Vigor router when such time setting has expired. **Negative Cache TTL** – Set the negative caching time (name error). **Email** – Type the e-mail address of the administrator.
NS Record	This page is used to specify name server which will be used as DNS server. **Add** – Click it to add a new server with specified name and IP address. **Save** – Click it to save the settings. **HOST** – Type the domain name of the server. This is optional. If no information added here, the router will use the DNS server configured in Domain Name under the Basic tab. **Name Server** –Type the URL for the name server which will be used to receive the DNS query forwarded by HOST. **IP Address** – This is optional. If required, simply type the IP address of the NS record server.
MX Record	This is used to specify the mail server with IP address. **Add** –Click it to add a new server with specified name and IP

	address. **Save** – Click it to save the settings. **Host** –Type the name (URL) of the mail server. **Mail Server** – Type the name (URL) of the mail server. **IP Address** – Type the IP address of the mail server. **Preference** – Set a number for the priority of such mail server.
Additional A Record	It is used to record the DNS query by IPv4 address. **Add** –Click it to add a new host with specified IP address. **Save** – Click it to save the settings. **Host** –Set a domain name. **IP Address** – Type the IP address of the mail server.
AAAA Record	It is used to record the DNS query by IPv6 address. **Add** –Click it to add a new host with specified IPv6 address. **Save** – Click it to save the settings. **Host** – Set a domain name. **IPv6 Address** –Type the IPv6 address of the host. Any query concerning of Host will be forwarded to the server selected in Reference for advanced process.
CNAME Record	It is used to record the DNS query for CNAME. **Add** – Click it to add a new host with specified reference. **Save** – Click it to save the settings. **Host** – Set a domain name. **Reference** – Choose a sub domain name from the drop down list. Any query concerning of Host will be forwarded to the server selected in Reference for advanced process.

4. Click **Apply**. A new profile will be added on the page.

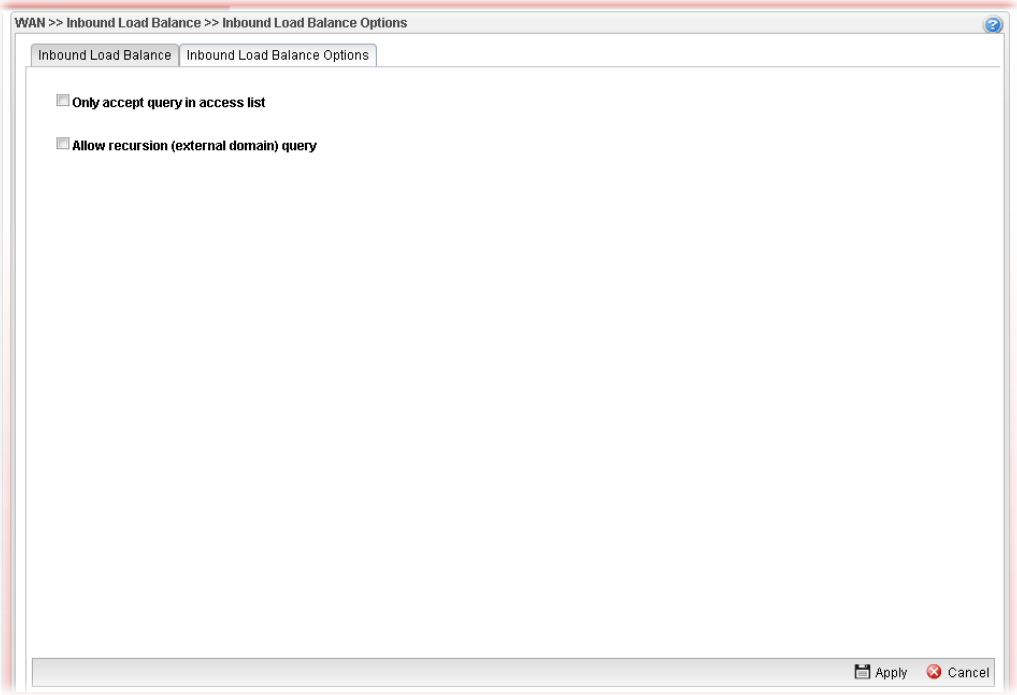
You can create sub-domain by clicking ▶ on the left side of the selected inbound load balance profile. A **sub-domain** setting page will appear for you to add new profile.



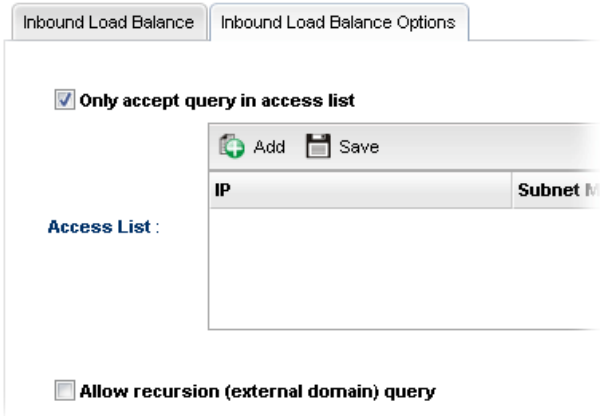
Note that the configuration is similar to the way stated on the above steps.

4.1.2.2 Inbound Load Balance Options

This page is used for configuring detailed Domain Name Server settings. Open **WAN>>Load Balance** and click the **Inbound Load Balance** Options tab.

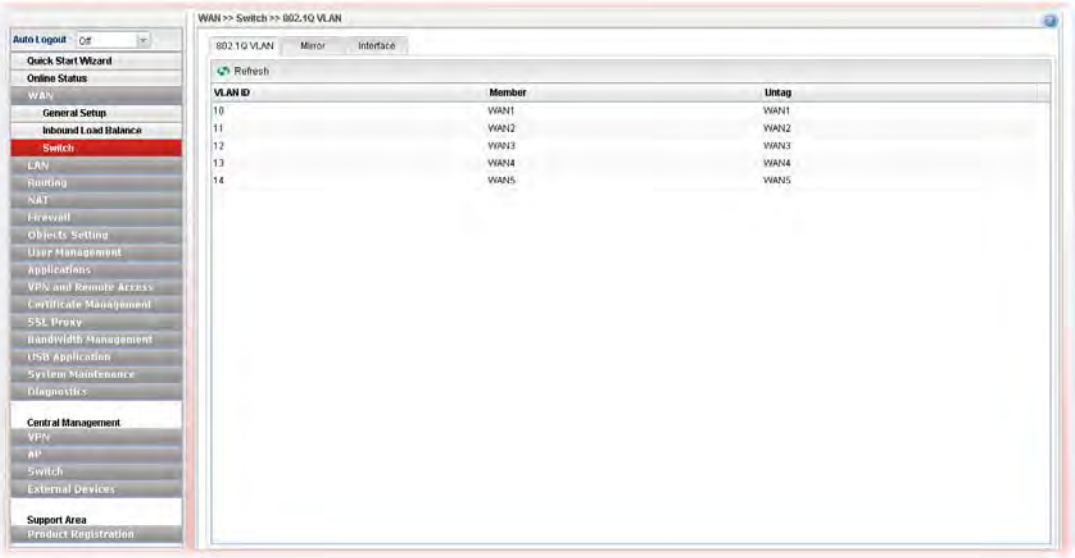


Each item will be explained as follows:

Item	Description
Only accept query in access list	If it is enabled, Vigor router only accepts DNS queries coming from the IP addresses or subnets in the Access List. **Access List** – Display a table of IP address(es) with subnet(s). **Add** – Create an IP address with subnet mask. 
Allow recursion (external domain) query	If it is enabled, Vigor router will reply all DNS queries even if querying an external domain which is NOT set in inbound load balance page.
Apply	Save and activate the settings.

4.1.3 Switch

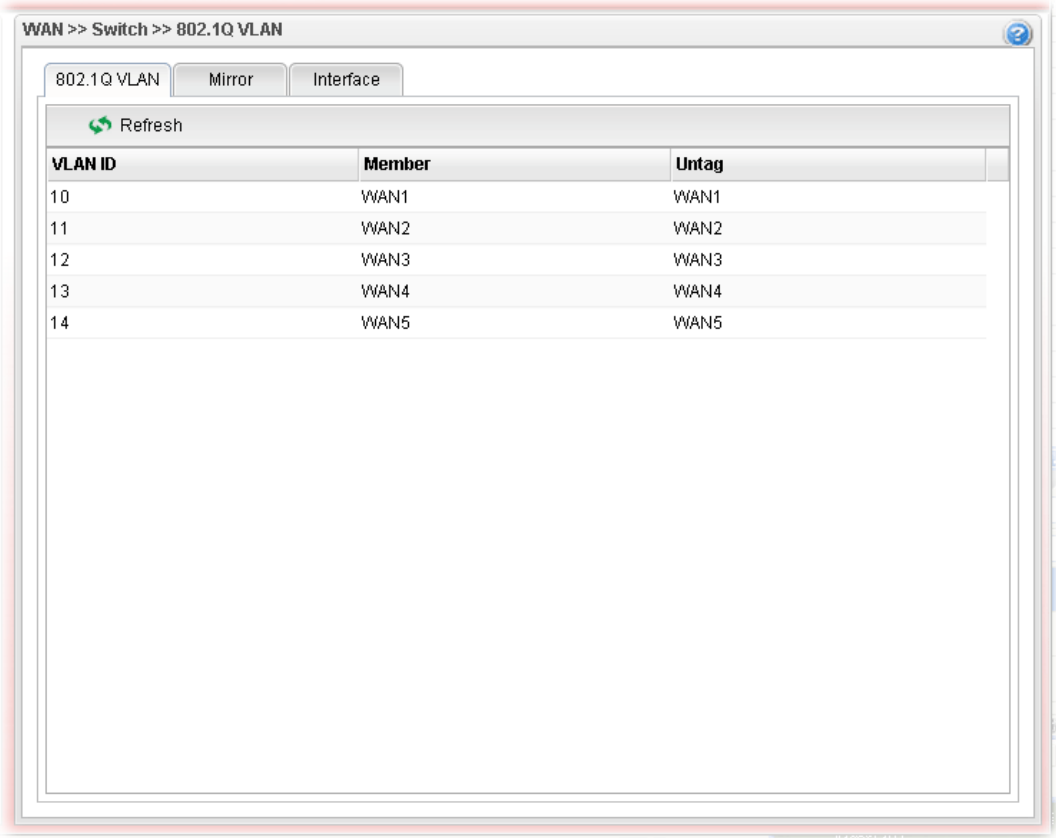
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable WAN interface, and configure 802.1Q VLAN ID for different WAN interfaces, and so on.



4.1.3.1 802.1Q VLAN

Packets passing through the WAN interface might be tagged or untagged with VLAN ID number. It depends on the setting configured in this page for VLAN ID configured in **WAN >>General Setup>>Profile** relates to the VLAN ID setting configured here.

This page simply displays current status of 802.1Q VALN setting profiles.

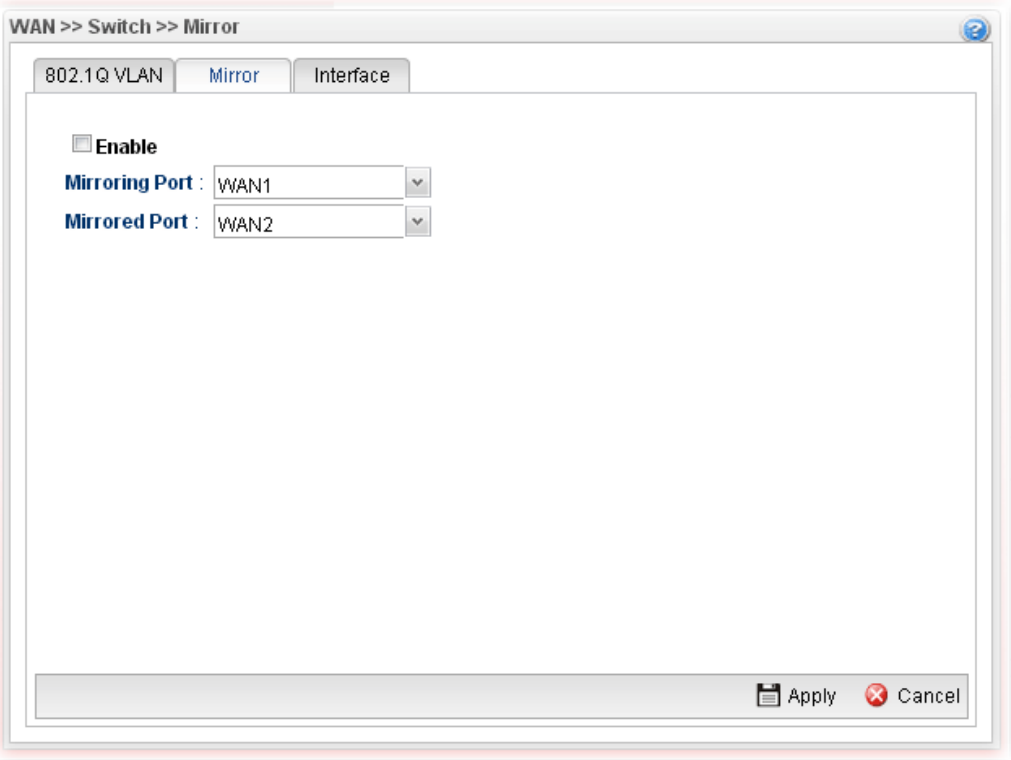


Each item will be explained as follows:

Item	Description
Refresh	Click it to reload this page.
VLAN ID	Display the VLAN ID number.
Member	Display **number** of the WAN interface for the packets tagged with such VLAN ID number to pass through.
Untag	Display **number** of the WAN interface for the VLAN ID will be untagged for packets passing through the WAN interface selected.

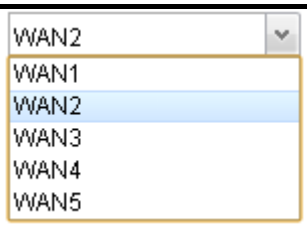
4.1.3.2 Mirror Configuration

The administrator can monitor all the packets passing through mirrored port with the mirroring port. It is useful for the administrator to analyze the troubles on Network.



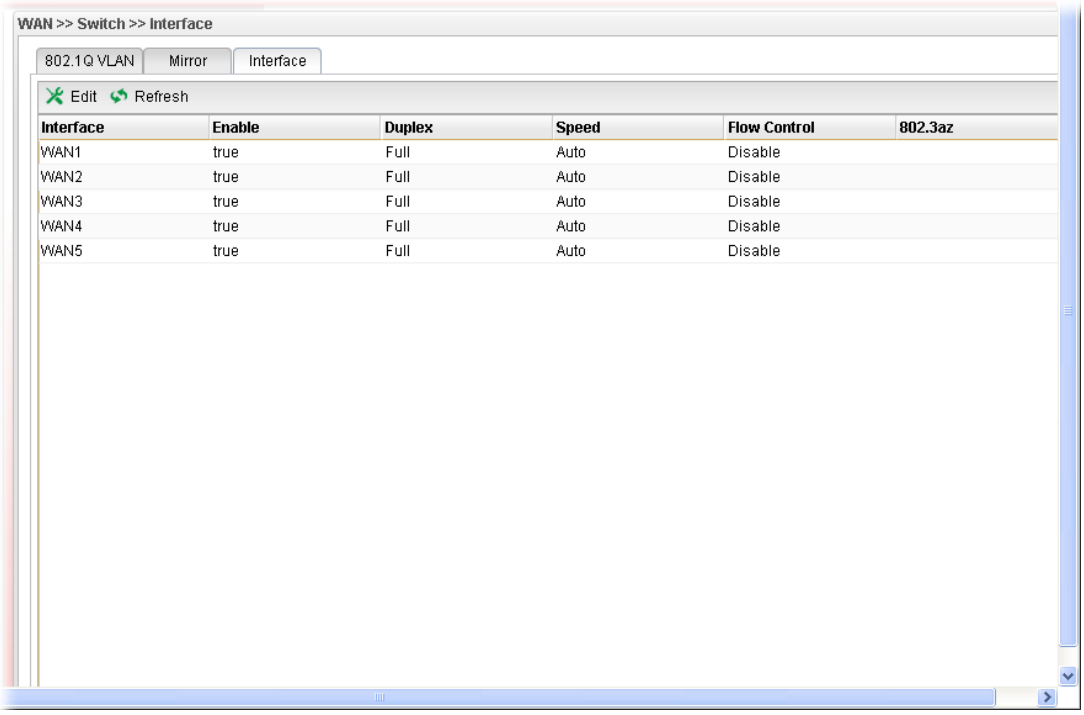
Available parameters are listed as follows:

Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Mirroring Port	Select a port for the administrator to use for viewing traffic sent from mirrored ports.

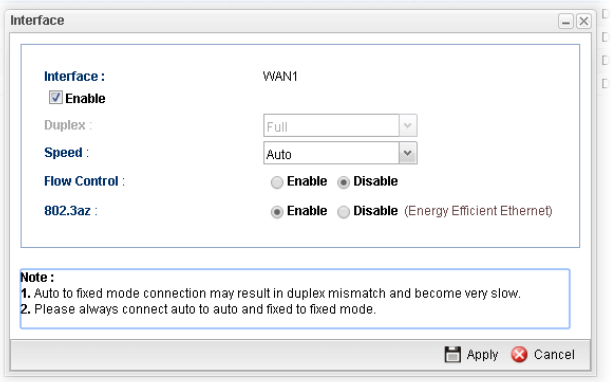
	
Mirrored Port	Select a port to make the packets passing through it monitored by the administrator.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.1.3.3 Interface Configuration

This page allows you to modify the status (enable / disable), duplex (Half/Full), speed, flow control and 802.3az for the WAN ports respectively.



Each item will be explained as follows:

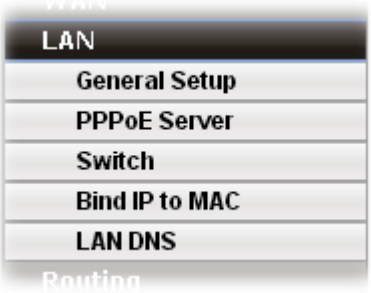
Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.  **Interface** – Display the name of WAN interface. **Enable** – Check it to enable such interface. **Speed** – Use the drop down list to specify the transmission rate (**Auto, 10M, 100M** or **1000M**) for such interface. **Flow Control** – The default setting is **Disable**. If **Enabled** is clicked, Vigor router will drop the packet if too much to handle. **802.3az –** It is a function of energy-efficient Ethernet.

	It can detect the network traffic automatically to adjust the power output and let Vigor3900 save the energy during the period of low traffic. Click **Enable** to activate the power/energy saving function if required. **Apply** – Click it to save and exit the dialog. **Cancel** – Click it to exit the dialog without saving anything.
Refresh	Renew current web page.
Interface	Display the name of the WAN port on the router.
Enable	Display the status of the profile. False means disabled; True means enabled.
Duplex	Display the duplex used (full or half) by such profile.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.
Flow Control	Display if such function is enabled or disabled.
802.3az	Display such function is enabled or disabled.

4.2 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 private IP address to public 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.



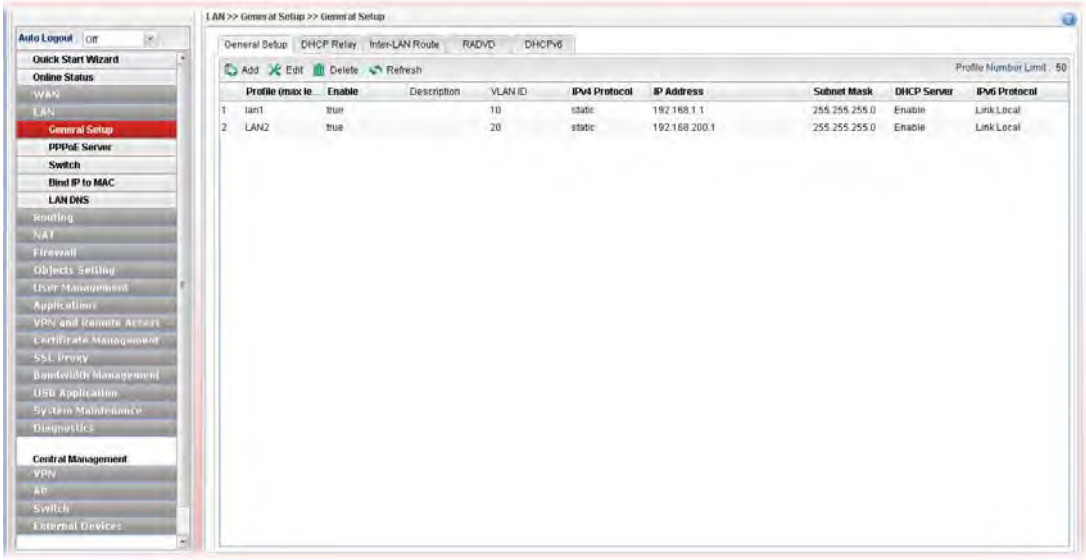
4.2.1 General Setup

This page allows you to configure general settings for PCs in LAN.

> **Note**: One LAN profile shall be enabled at least to keep the normal operation. The default LAN profile named “lan1” shall not be deleted. Otherwise, the system might be damaged. If such file is deleted due to careless, please reset your router to restore the default setting.

4.2.1.1 General Setup

This page allows you to enable the profile, give a brief explanation for such profile, specify the VLAN ID, specify MAC address, and choose protocol type for such profile.



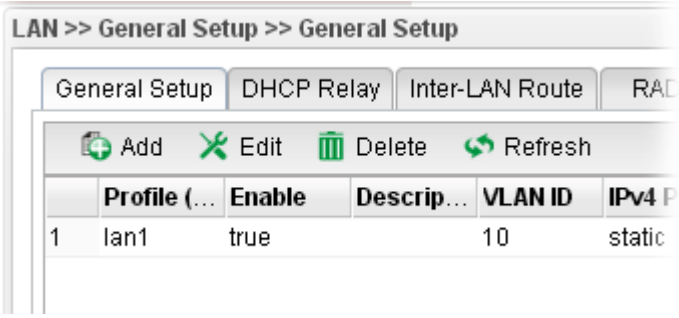
Each item will be explained as follows:

Item	Description
Add	Add a new LAN profile.

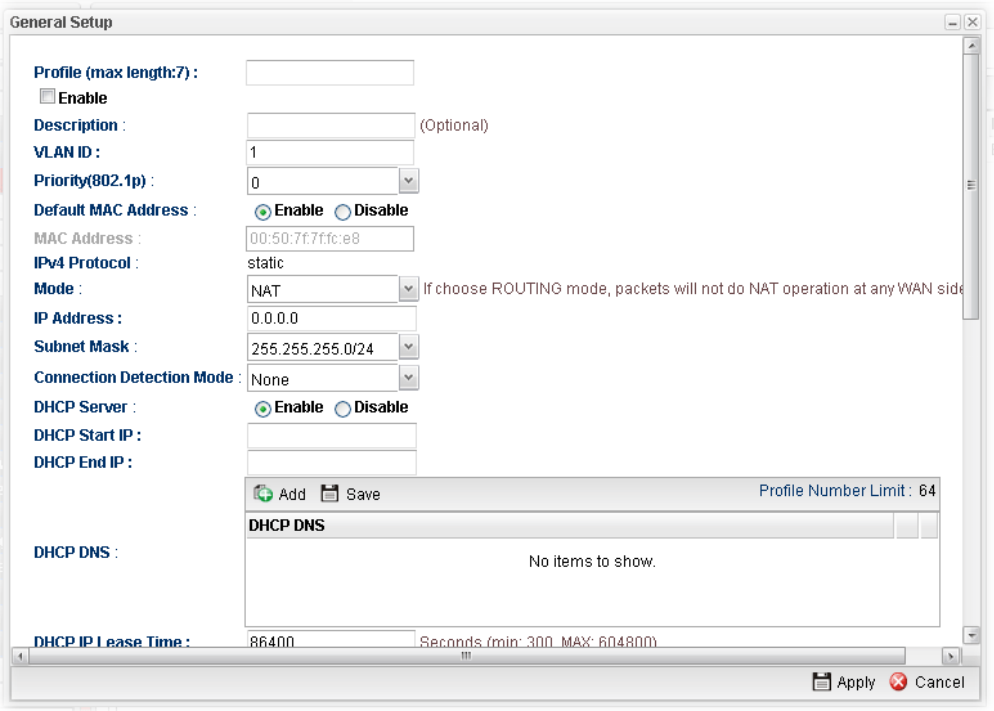
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected LAN profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page
Profile (max length:7)	Display the name of the LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Description	Display the brief explanation for the LAN profile.
VLAN ID	Display the VLAN ID configured for the LAN profile.
IPv4 Protocol	Display the IPv4 protocol type for the LAN profile.
IP Address	Display the IP address for such LAN profile.
Subnet Mask	Display the subnet mask for such LAN profile.
DHCP Server	Display the status (Enable/Disable) of the DHCP server.
IPv6 Protocol	Display the IPv6 protocol type for the LAN profile.

How to add a new LAN profile

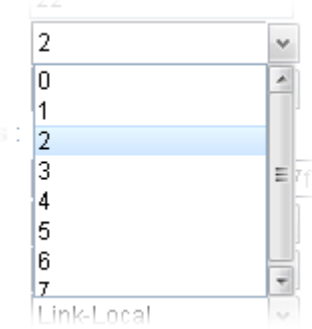
1. Open **LAN>>General Setup** and click the **General Setup** tab.

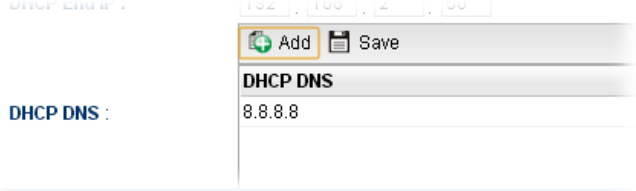


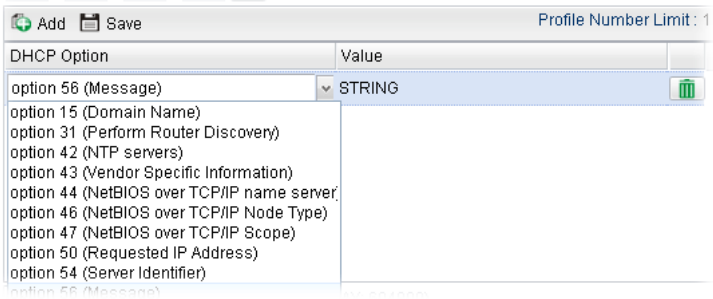
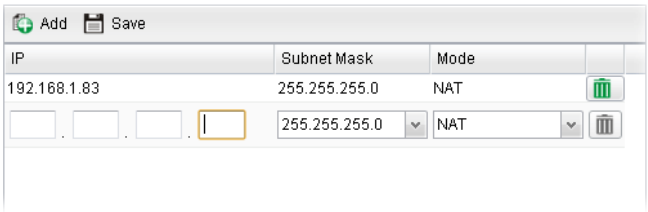
2. Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.



Available parameters are listed as follows:

Item	Description
Profile (max length:7)	Type the name of the LAN profile.
Enable	Check this box to enable such profile.
Description	Type the description for the new LAN profile.
VLAN ID	Type a number as the VLAN ID to make the data be identified while performing data transmission.
Priority(802.1q)	Type the packet priority number for such profile. The range is from 0 to 7. 
Default MAC Address	**Enable** – Click it to enable the default MAC address for such profile. **Disable** – Click it to type the MAC address manually for such profile.
MAC Address	If Default MAC address is disabled, please specify a MAC

	address manually with the format like “00:1d:aa:b2:69:80”.
IPv4 Protocol	Display the fixed type (static) for the IPv4 protocol for such profile.
Mode	Choose **NAT** or **ROUTING** as the operation mode for such profile.
IP Address	Type the IP address (with the format like 192.168.1.25) of the router for the LAN profile.
Subnet Mask	Use the drop down list to choose a suitable mask for the LAN profile.
Connection Detection Mode	Select a detecting mode for this LAN interface. This feature is used to operate in coordination with **Policy Route** profile. Vigor system can choose suitable router policy through connection detection automatically.
Gateway IP Address	It is available when **ARP** is selected as Connection Detection Mode. Type a public gateway address. Vigor router will detect the destination IP specified here automatically when such LAN profile is used. If the IP is not detected, the connection status for LAN will be shown as “down”.
Connection Detection Interval	It is available when **ARP** is selected as Connection Detection Mode. Assign an interval period of time for each detecting.
Connection Detection Retry	It is available when **ARP** is selected as Connection Detection Mode. Assign detecting times to ensure the connection of the LAN interface. After passing the times you set in this field and no reply received by the router, the connection of LAN interface will be regarded as breaking down.
DHCP Server	**Enable** – Click it to enable the DHCP server. The DHCP server will assign the IP address randomly for the LAN user. The range of the IP addresses must be defined in DHCP Start IP and DHCP End IP. **Disable** – Click it to disable the DHCP server.
DHCP Start IP	Type an IP address as the starting point for DHCP server.
DHCP End IP	Type an IP address as the ending point for DHCP server.
DHCP DNS	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting.

DHCP IP Lease Time	Set a lease time for the DHCP server. The time unit is minute.
DHCP Routers	In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user. However, if you want to use other gateway, please assign the IP address in this field.
DHCP Next Server	Type the IP address of the secondary DHCP server.
DHCP Options	DHCP packets can be processed by adding option number and data information when such function is enabled. 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.  **Add** – Click it to add a new DHCP option profile. **Save** – Click it to save the setting. **DHCP Option** – Use the drop down list to choose the one you want. **Value** – Type the content of the data to be processed by the function of DHCP option.
Specify Remote Dial-in IP	**Enable** – Check the box to enable this function. Remote clients within the range specified in the fields of **Remote Dial-in Start IP** and **Remote Dial-in End IP** can access into Vigor3900 WUI.
More Subnet	Different subnets can be created under one LAN profile. Specify other subnets which might be needed in the future.  **Add** – Click it to add a new subnet mask with IP address and specified mode. **Save** – Click it to save the settings. **IP** – Type the IP address if you click Add for adding a new entry.

	Subnet Mask – Use the drop down list to choose the one you want. **Mode** – Specify NAT or Routing as the mode. **DHCP** – Click **Enable** to activate the DHCP function on such subnet. When it is enabled, you have to specify the IP range to be assigned by the DHCP server for such subnet. **Start IP** – Type an IP address as a starting point. **End IP** – Type an IP address as an ending point.
DNS Redirection	**Enable** – It can redirect DNS queries from such LAN profile to router's DNS Server. It must work with LAN DNS function.
IPv6 Protocol	It defines the IPv6 connection types for LAN interface. Possible types contain Link-Local, Static and DHCP-SLA. Except Link-Local, each type requires different parameter settings. **Link-Local**- Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address. **Static** –This type allows you to setup static IPv6 address for LAN. **DHCP-SLA**- DHCPv6 client mode would use IA_NA option of DHCPv6 protocol to obtain IPv6 address from server.
IPv6 Address	If **Static** is chosen as IPv6 Protocol, please type the IPv6 address in this field.
IPv6 Prefix Length	Display the IPv6 prefix length.
DHCPv6 SLA WAN Interface	If **DHCP-SLA** is chosen as IPv6 Protocol, please choose one of the WAN profiles in this field.
DHCPv6 SLA ID	The ID number set here is used by an individual organization to create its own local addressing hierarchy and to identify subnets.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

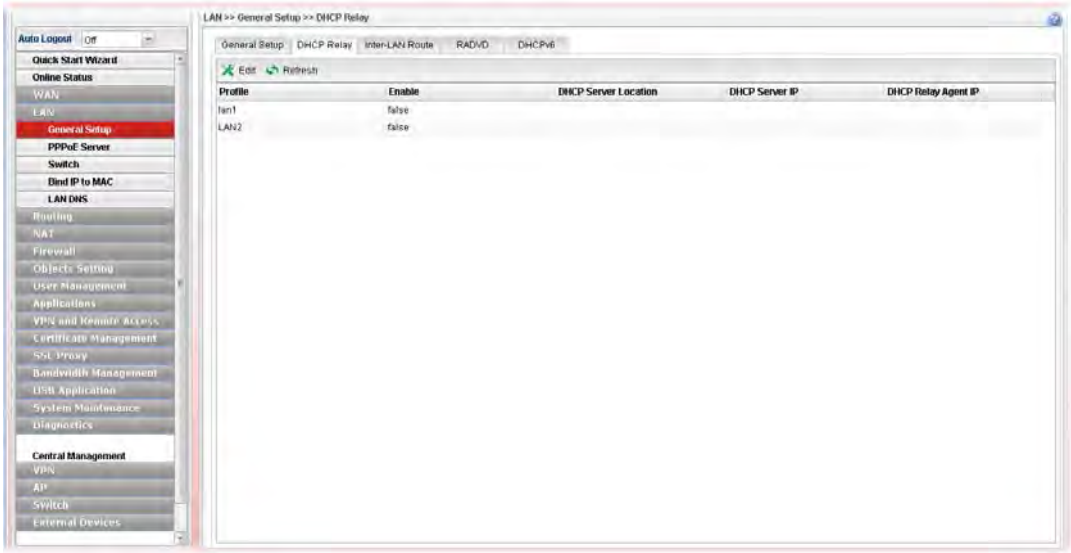
3. When you finish the above settings, please click **Appl**y to save the configuration and exit the dialog.

4.2.1.2 DHCP Relay

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let **Relay Agent** help you to redirect the DHCP request to the specified location.

This page allows users to specify which subnet that DHCP server is located that the relay agent should redirect the DHCP request to.

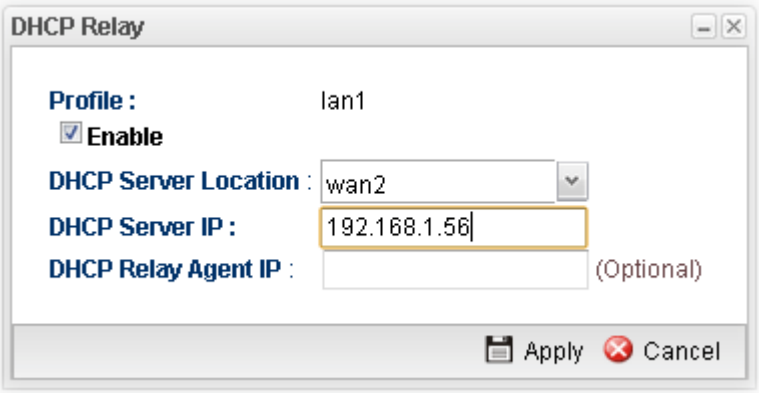


Each item will be explained as follows:

Item	Description
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the name of the LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
DHCP Server Location	Display the LAN or WAN profile for the DHCP server.
DHCP Server IP	Display the IP address of DHCP server.
DHCP Relay Agent IP	Display the IP address of DHCP relay agent server.

How to edit a LAN profile for DHCP Relay

1. Open **LAN>>General Setup** and click the **DHCP Relay** tab.
2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.



Available parameters are listed as follows:

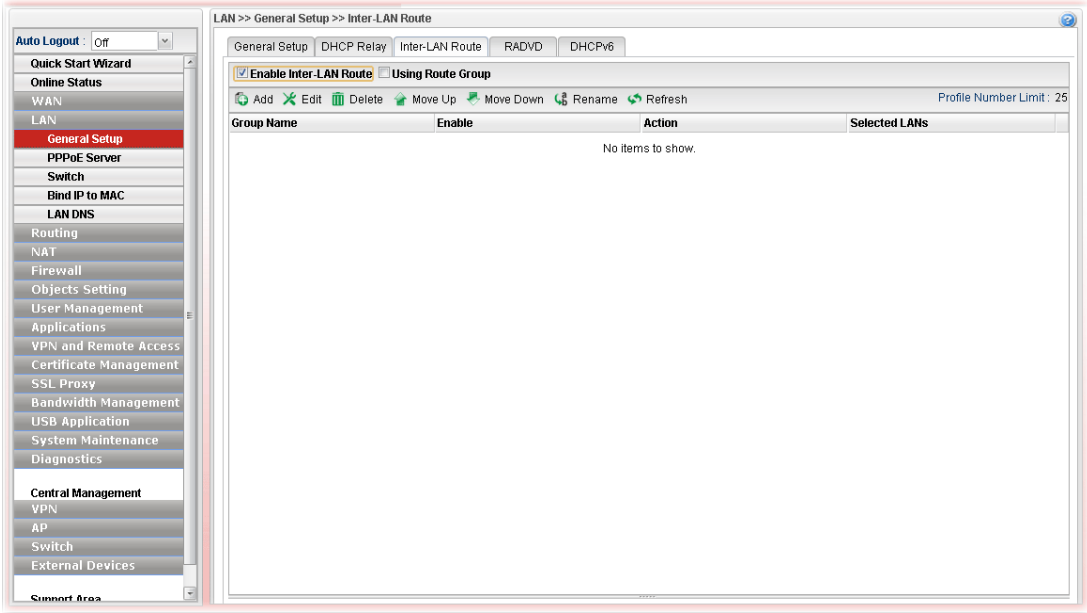
Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
DHCP Server Location	Choose the interface for the DHCP server.
DHCP Server IP	Type the IP address of DHCP Server.
DHCP Relay Agent IP	Type the IP address of DHCP Relay Agent.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.

4. The LAN profile has been edited.

4.2.1.3 Inter-LAN Route

Inter-LAN route profile is created for making the users in different LAN be able to communicate with each other.



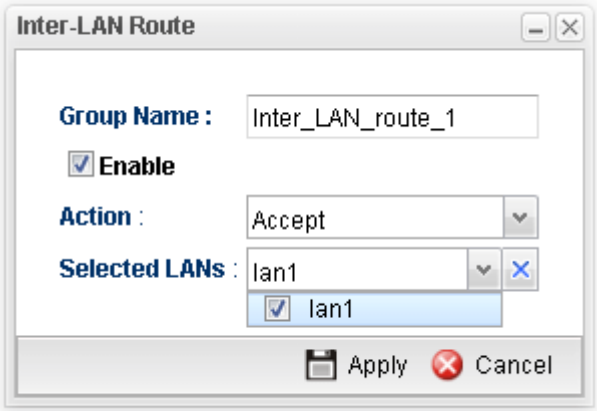
Each item will be explained as follows:

Item	Description
Enable Inter-LAN Route	In default, such function is disabled. Check the box of **Enable Inter-LAN Route** to create route profile. However, if there is no route profile created, all of LAN users can communicate with each other.
Using Route Group	After checking **Enable Inter-LAN Route**, check this box to specify which LANs are allowed to communicate with each other. For example, LAN1 and LAN2 are set as members in group1; LAN3 and LAN4 are set as members in group2. LAN1 can communicate with LAN2 but not LAN3/LAN4. LAN3 can communicate with LAN4 but not LAN1/LAN2.
Add	Add a new LAN group profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Move Up / Move Down	Move the selected profile up or down.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.

Profile Number Limit	Display the total number of the profiles to be created.
Group Profile	Display the name of the group profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Action	Display the action specified for such group profile.
Selected LANs	Display LAN profiles grouped under such group profile.

How to add an Inter-LAN profile

1. Open **LAN>>General Setup** and click the **Inter-LAN Route** tab.
2. Click the **Add** button to open the following dialog.



Available parameters are listed as follows:

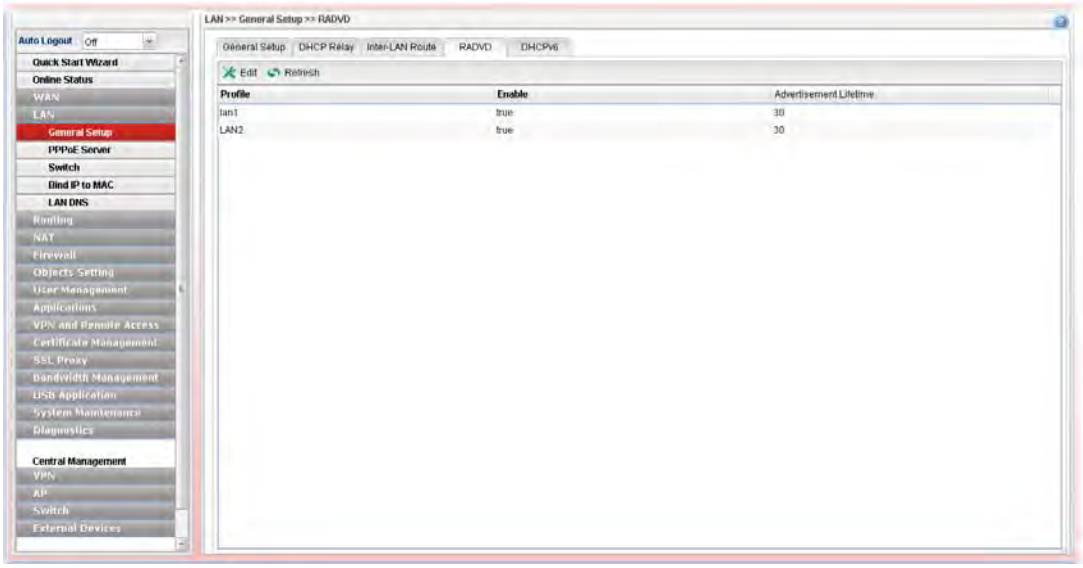
Item	Description
Group Name	Type the name for such group profile.
Enable	Check this box to enable this profile.
Action	**Accept** – Users in selected LANs can communicate with each other. **Block** – Users in selected LANs are unable to communicate with each other.
Selected LANs	Choose LAN profiles by using the drop down list. Users listed in the selected LAN will be influenced by the action defined above.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.

The inter-LAN route profile has been created.

4.2.1.4 RADVD

The router advertisement daemon (radvd) 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.



Each item will be explained as follows:

Item	Description
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the name of the LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Advertisement Lifetime	Display the lifetime value. The lifetime associated with the default router in units of minutes, ranging from 10 ~ 150. It is used to control the lifetime of the prefix. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.

How to edit a LAN profile for RADVD

1. Open **LAN>>General Setup** and click the **RADVD** tab.
2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.

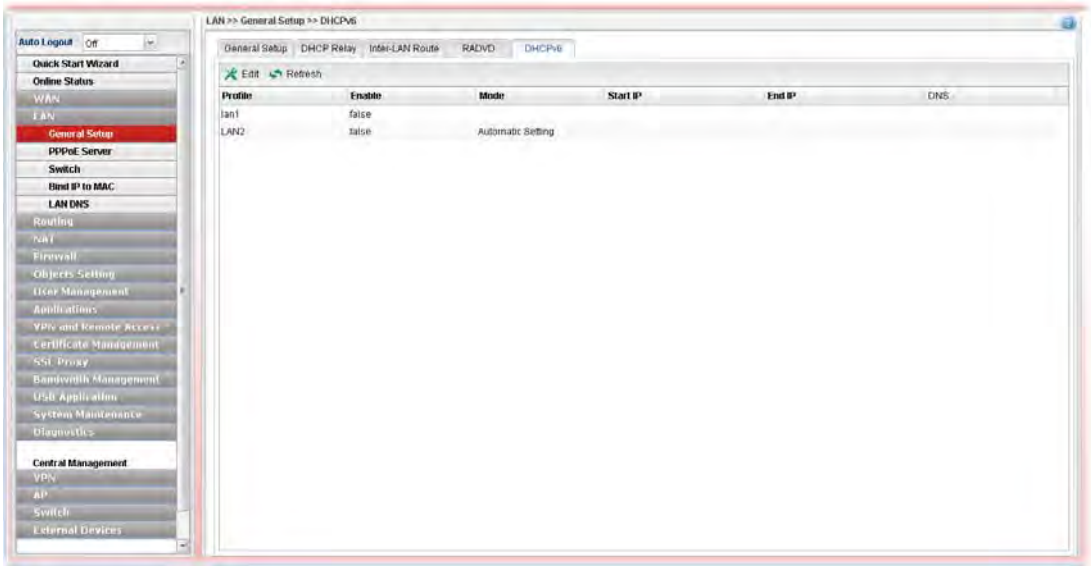
Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
Advertisement Lifetime	Type a value for advertisement lifetime. The lifetime associated with the default router in units of minutes, ranging from 10 ~ 150. It is used to control the lifetime of the prefix. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.
4. The LAN profile has been edited.

4.2.1.5 DHCP6

DHCP6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.

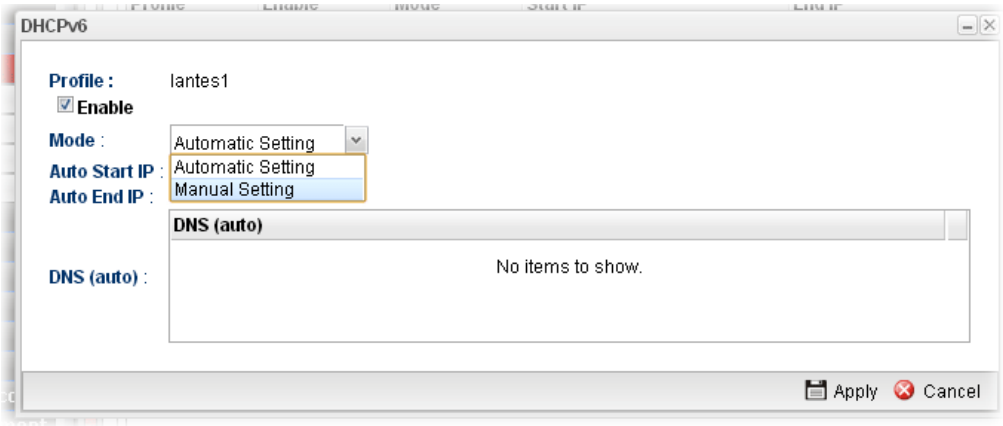


Each item will be explained as follows:

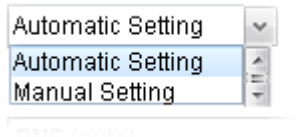
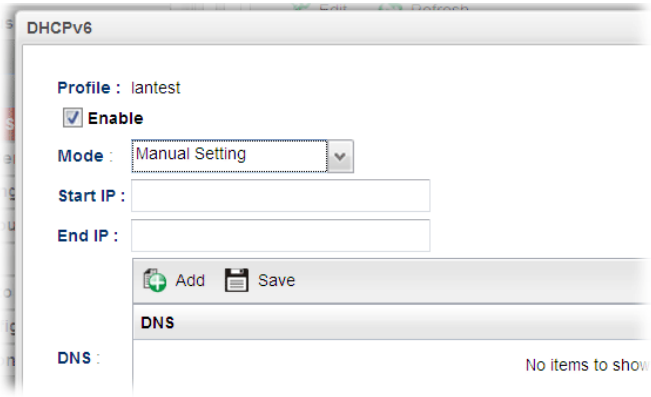
Item	Description
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the name of the LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Mode	Display the mode (automatic setting or manual setting) specified for such profile.
Start IP	Display the starting IP address of the IP address pool for DHCP server.
End IP	Display the ending IP address of the IP address pool for DHCP server.
DNS	Display the private IP address for DNS server.

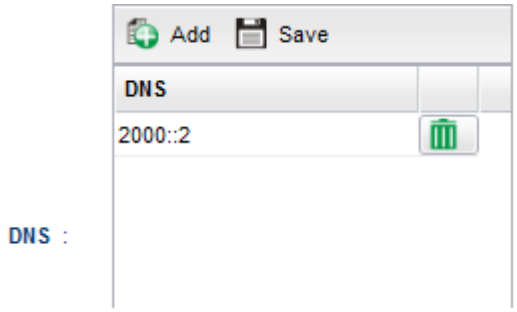
How to edit a LAN profile for DHCPv6

1. Open **LAN>>General Setup** and click the **DHCPv6** tab.
2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.



Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
Mode	Choose **Automatic Setting** or **Manual Setting**.  **Automatic Setting** – It is not necessary to configure Start IP, End IP and DNS setting. The system will assign suitable address automatically. **Manual Setting** – You should type the Start IP address and End IP address manually. 
Start IP	Set the starting IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.

End IP	Set the ending IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.
DNS	It is available when **Manual Setting** is selected as **Mode**. Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

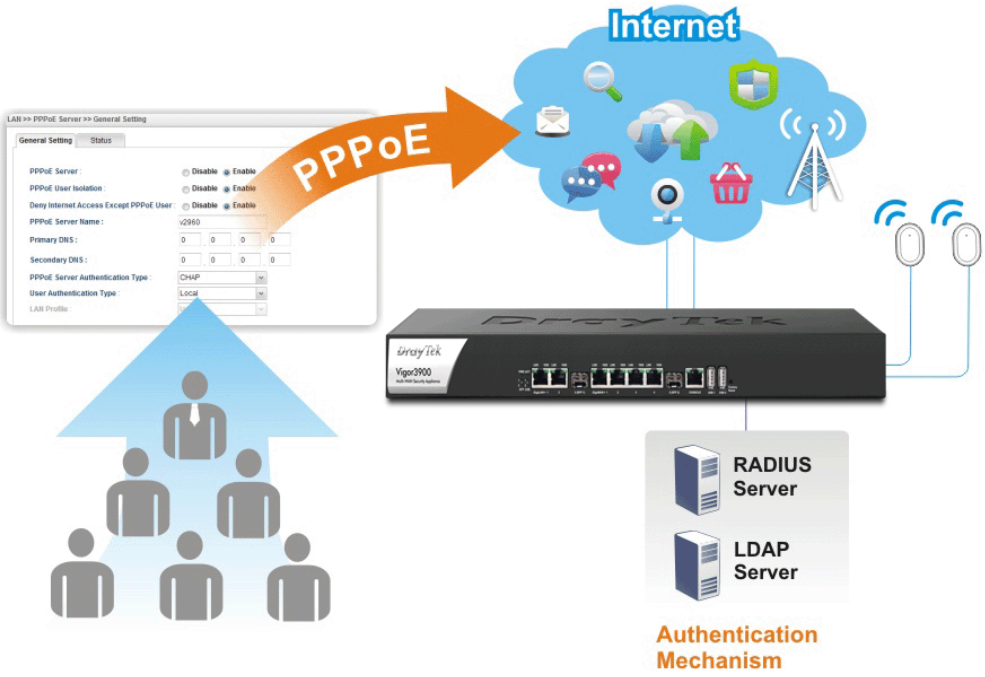
3. When you finish the above settings, please click **Appl**y to save the configuration and exit the dialog.

4. The LAN profile has been edited.

4.2.2 PPPoE Server

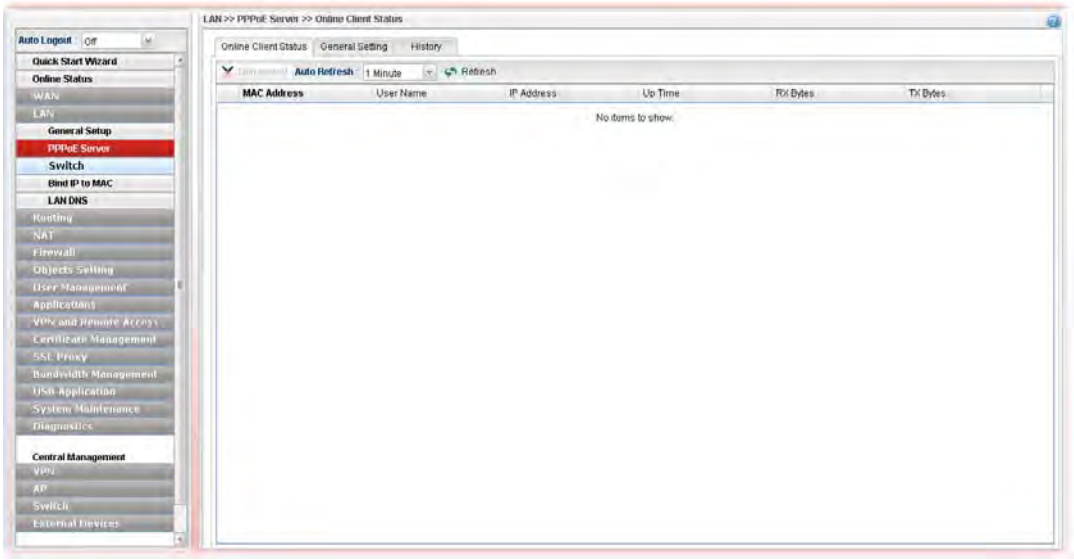
This feature makes the router working like an ISP, providing PPPoE connections to LAN PCs. The only difference is that local PCs don't need an ADSL modem.

There are several advantages of using PPPoE connections on the LAN. Firstly, the PPPoE server can secure the LAN PC connections with username/password authentication. Secondly, it can prevent ARP attack by nature. Thirdly, the system administrator can configure quota (time/traffic based) for each user as ISP does.



4.2.2.1 Online Client Status

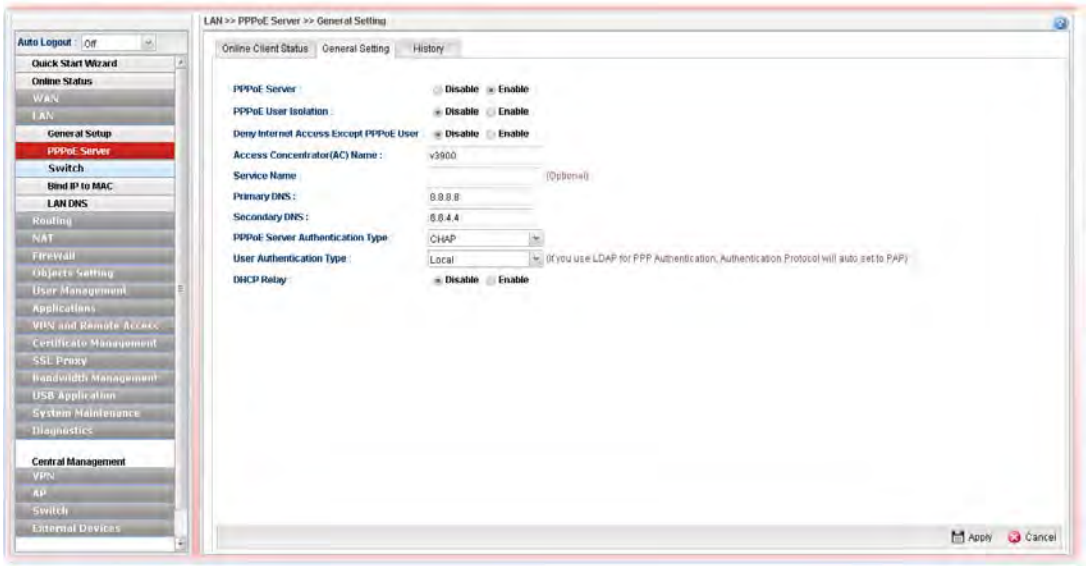
This page displays general information for PPPoE server; allows you to disconnect the network connection to PPPoE server.



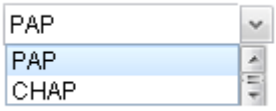
Each item will be explained as follows:

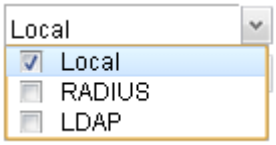
Item	Description
Refresh	Renew current web page.
Disconnect	Click it to disconnect the profile connection.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
MAC Address	Display the MAC address of the client's host.
User Name	Display the user name used to access into the PPPoE server.
IP Address	Display the IP address of the client's host.
Up Time	Display the time that the PPPoE connection built.
RX Bytes	Display the total amount of received packets.
TX Bytes	Display the total amount of transmitted packets.

4.2.2.2 General Setting



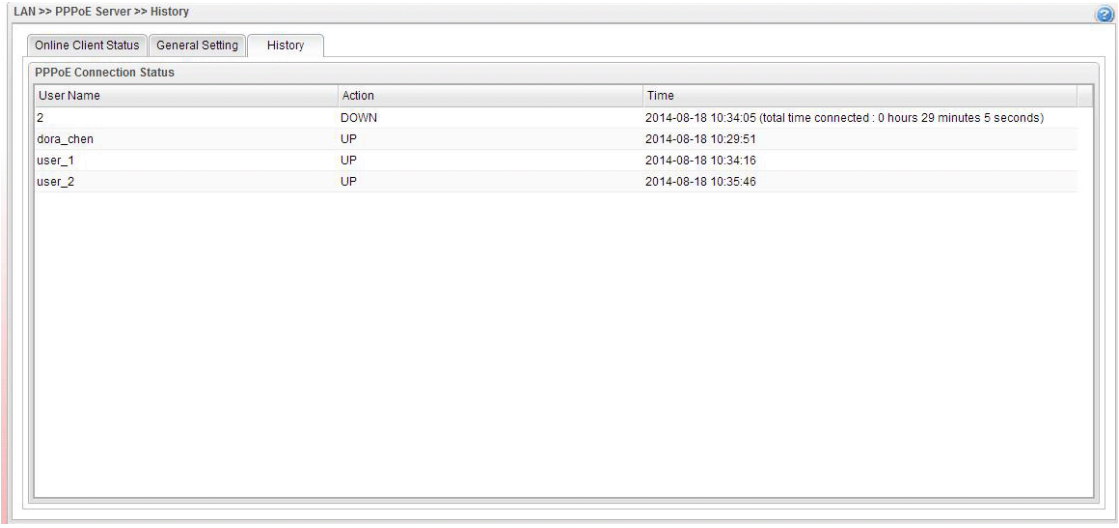
Available parameters are listed as follows:

Item	Description
PPPoE Server	**Disable** – Click it to disable this function. **Enable** – Click it to enable the function of PPPoE server.
PPPoE User Isolation	**Disable** – Click it to disable this function. **Enable** – Click it to isolate the PPPoE users who access into Internet via Vigor router..
Deny Internet Access Except PPPoE User	**Disable** –Click it to disable this function. **Enable** – If you click **Enable**, only the PPPoE user can access into Internet.
Access Concentrator (AC) Name	Type the name which will be reported as the access concentrator name.
Service Name	Type a specific string for authentication. It causes the named service to be advertised in a Service Name tagged in the PADO (PPPoE Active Discovery Offer) frame.
Primary DNS	Type an IP address as primary DNS.
Secondary DNS	Type another IP address as secondary DNS.
PPPoE Server Authentication Type	Choose the authentication type for PPPoE server.  Any PPPoE user shall pass the authentication of PPPoE server and access into Internet.
User Authentication	Users in LAN can access into Internet through Vigor router with RADIUS, LDAP or local authentication. Specify the

Type	type for the users. 
LDAP Profile	It is available when **LDAP** is selected as User Authentication Type. If you choose LDAP as the authentication type, use the drop down list to specify the LDAP profile.
DHCP From	It is available when **RADIUS** is selected as User Authentication Type.
DHCP Relay	**Enable** - 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. **DHCP Server Location** – Choose one of the interfaces for DHCP server. **DHCP Server IP Address** - Set the IP address of the DHCP server you are going to use so DHCP Relay can help to forward the DHCP request to the DHCP server.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard current page modification.

4.2.2.3 History

This page displays records of connection status (up or down) and the connection time and the name of the user who accesses into PPPoE server of such router.



Each item will be explained as follows:

Item	Description
User Name	Display the user name used to access into the PPPoE server.
Action	Display the connection status (up or down) of the user account.

Time	Display the connection time. If the action is “Down”, such field will display the total connection time. If the action is “up”, such field will display the time point that the user account access into the PPPoE server.

4.2.3 Switch

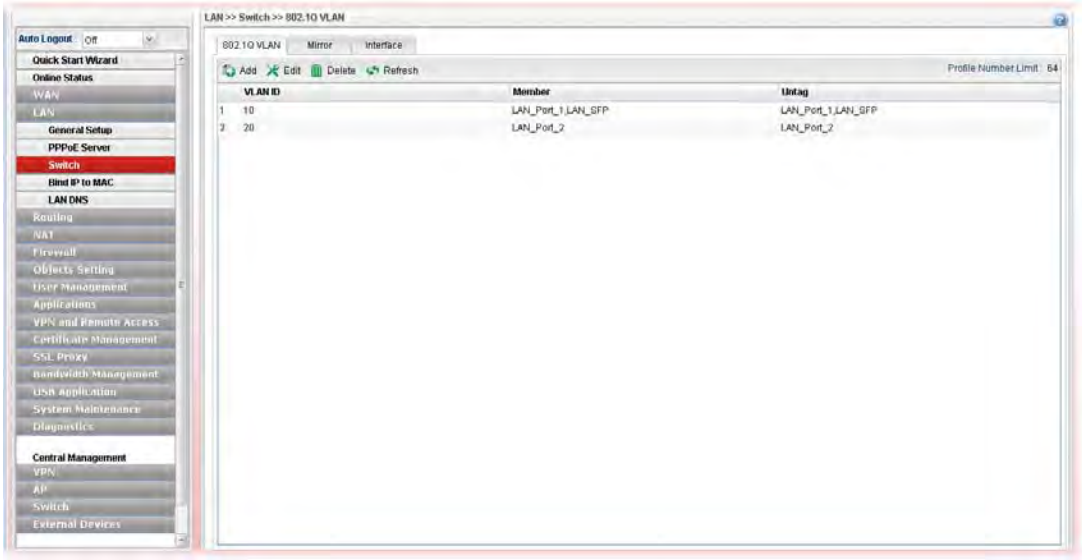
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable LAN interface, and configure 802.1Q VLAN ID for different LAN interfaces, and so on.

4.2.3.1 802.1Q VLAN

Virtual LANs (VLANs) are logical, independent workgroups within a network. These workgroups communicate as if they had a physical connection to the network. However, VLANs are not limited by the hardware constraints that physically connect traditional LAN segments to a network. As a result, VLANs allow the network manager to segment the network with a logical, hierarchical structure. VLANs can define a network by application or department. For instance, in the enterprise, a company might create one VLAN for multimedia users and another for e-mail users; or a company might have one VLAN for its Engineering Department, another for its Marketing Department, and another for its guest who can only use Internet not Intranet. VLANs can also be set up according to the organization structure within a company. For example, the company president might have his own VLAN, his executive staff might have a different VLAN, and the remaining employees might have yet a different VLAN. VLANs can also set up according to different company in the same building to save the money and reduce the device establishment.

User can select some ports to add into a VLAN group. In one VLAN group, the port number can be single one or more.

The purpose of VLAN is to isolate traffic between different users and it can provide better security application.



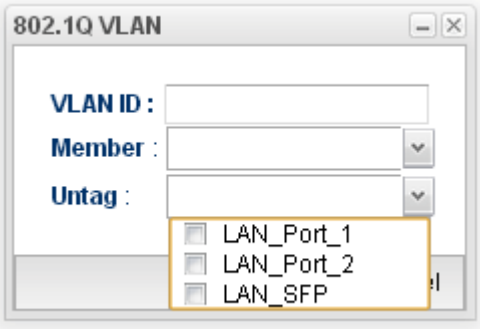
Each item will be explained as follows:

Item	Description
Add	Add a new VLAN ID setting.

Edit	Modify the selected VLAN ID setting. To edit VALN ID setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected VLAN ID setting. To delete a VLAN ID setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
VLAN ID	Display the VLAN ID number.
Member	Display the LAN interface that is used to access into Internet for such LAN profile with the VLAN ID number.
Untag	Display the LAN interface that packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or untagged.

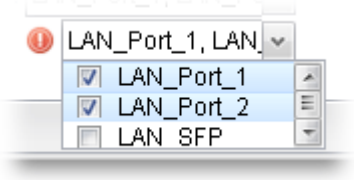
How to add a new 802.1Q VLAN profile

1. Open **LAN>>Switch** and click the **802.1Q VLAN** tab.
2. Click the **Add** button.
3. The following dialog will appear.

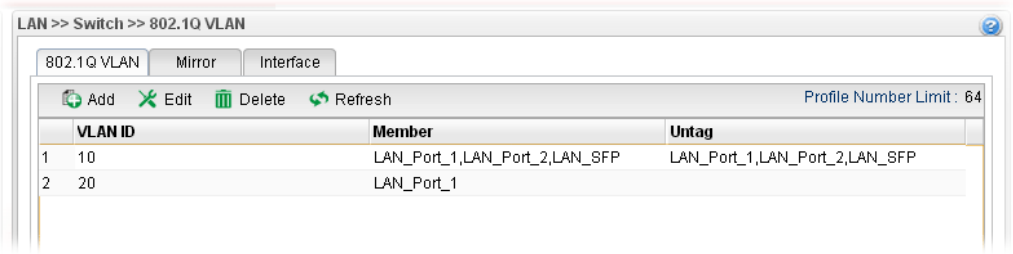


Available parameters are listed as follows:

Item	Description
VLAN ID	Type the number as the VLAN ID. Type a number used for identification on VLAN for your computer. Later, you have to type the same ID number for each PC which wants to be grouped within the same VLAN group.
Member	Determine which LAN interface can be used to access into Internet for such LAN profile with the VLAN ID number. If the icon appears in front of the drop down list, it means one of the selections has been chosen by other profile. You cannot choose it. If you want to specify that one for such profile, please exit this dialog to release that

	selection from its original VLAN profile, than return this page and make the selection again. 
Untag	Determine if the packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or not. If the icon appears in front of the drop down list, it means one of the selections has been chosen by other profile. You cannot choose it. If you want to specify that one for such profile, please exit this dialog to release that selection from its original VLAN profile, than return this page and make the selection again.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

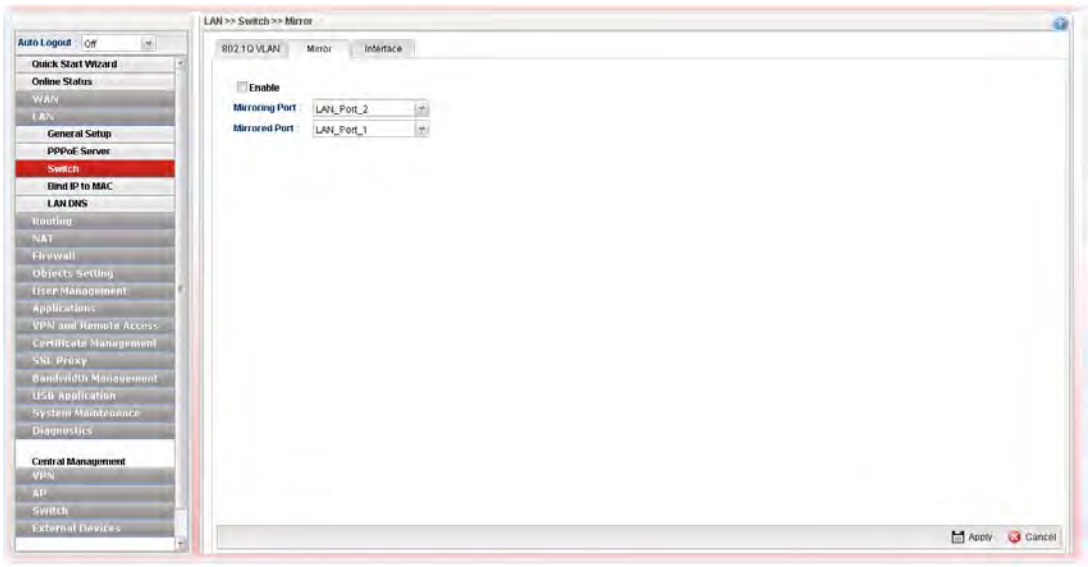
4. Enter all the settings and click **Apply**. The new profile will be added on the screen.



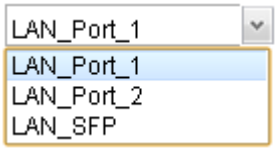
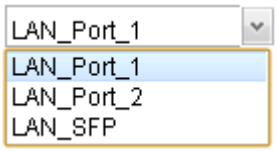
4.2.3.2 Mirror

Vigor3900 supports port mirroring function in LAN interfaces. This mechanism helps manager track the network errors or abnormal packets transmission without interrupting the flow of data access the network. By the way, user can apply this function to monitor all traffics which user needs to check.

There are some advantages supported in this feature. Firstly, it is more economical without other detecting equipments to be set up. Secondly, it may be able to view traffic on one or more ports within a VLAN at the same time. Thirdly, it can transfer all data traffics to be mirrored to one analyzer connect to the mirroring port. Last, it is more convenient and easy to configure in user's interface.

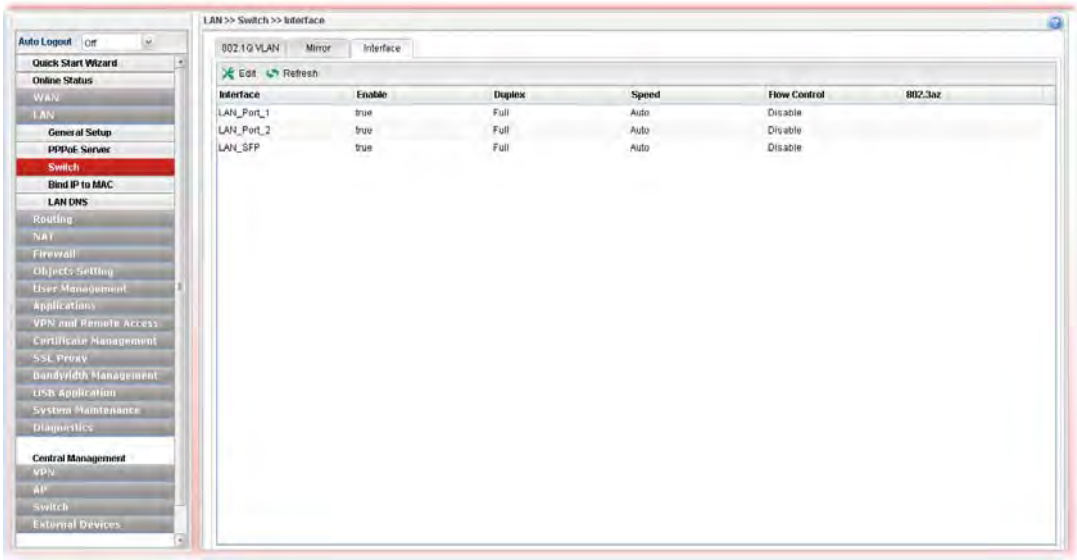


Available parameters are listed as follows:

Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Mirroring Port	Select a port to view traffic sent from mirrored ports. 
Mirrored Port	Select which port is necessary to be mirrored. 
Refresh	Renew current web page.
Apply	Click it to save the settings.

4.2.3.3 Interface

This page allows you to modify the status (enable / disable), speed(Auto,10M,100M,1000M) and duplex (Half/Full) for the LAN ports respectively.

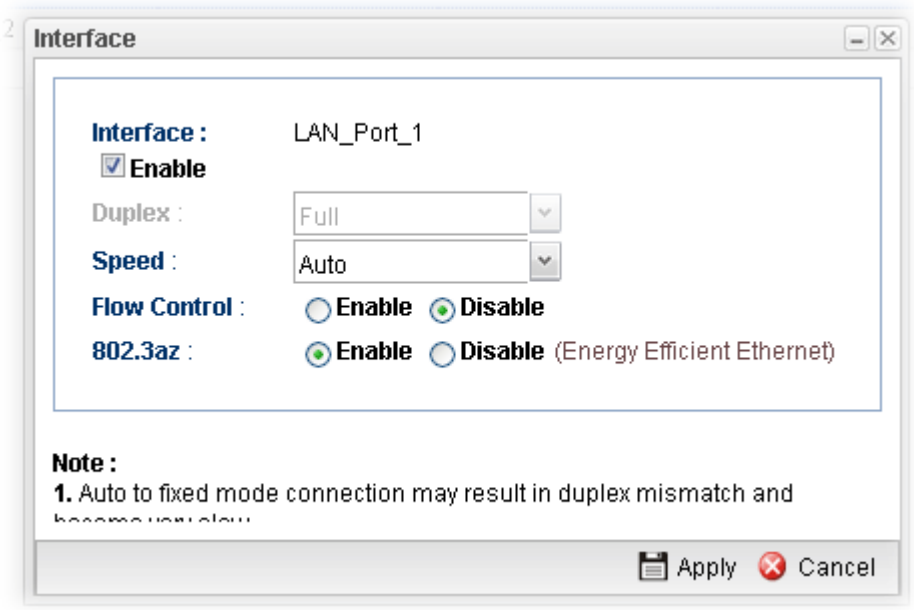


Each item will be explained as follows:

Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.
Refresh	Renew current web page.
Interface	Display the profile name of the interface.
Enable	Display the status of the profile. False means disabled; True means enabled.
Duplex	Display the duplex used (full or half) by such profile.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.
Flow Control	Display the status (enable or disable) of such function.
802.3az	Display such function is enabled or disabled.

How to edit an Interface profile

1. Open **LAN>>Switch** and click the **Interface** tab.
2. Please select a profile and click the **Edit** button.
3. The following dialog will appear.



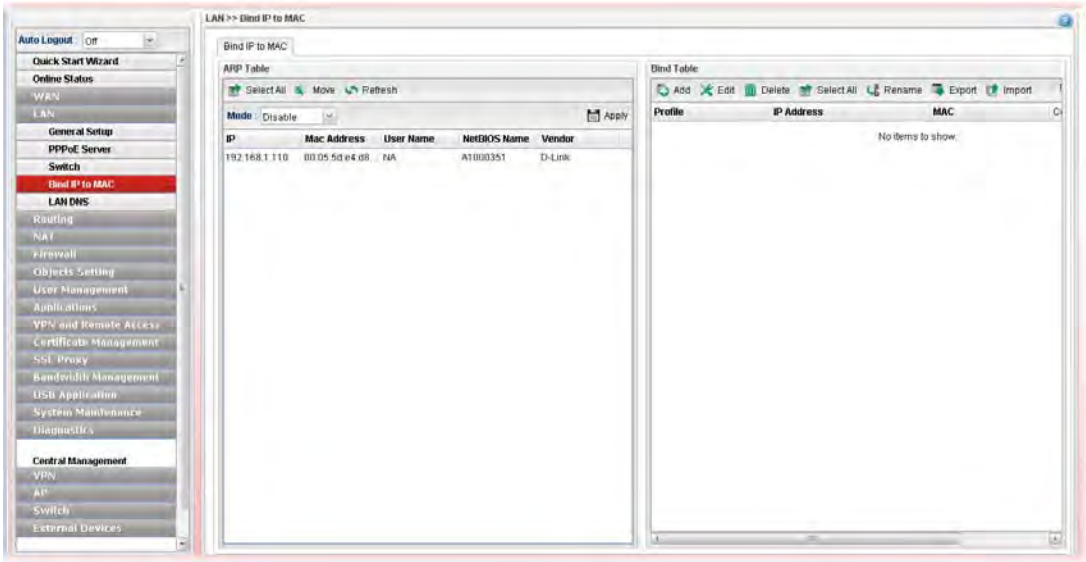
Available parameters are listed as follows:

Item	Description
Interface	Display the name of LAN interface profile.
Enable	Check the box to enable the Mirror function for the switch.
Speed	Use the drop down list to specify the transmission rate for such profile.
Flow Control	Click **Enable** to enable such function. When the data cache is approaching to full load, Vigor router will pause transmitting the packets till the system is able to accept new data again. It can avoid the network traffic congestion.
802.3az	It is a function of energy-efficient Ethernet. It can detect the network traffic automatically to adjust the power output and let Vigor3900 save the energy during the period of low traffic.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**. The profile has been edited.

4.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthen control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.



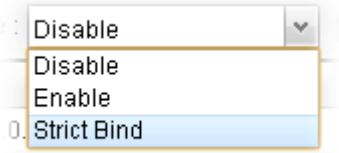
Each item will be explained as follows:

Item	Description
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 **Move** on IP Bind List. **Select All** - Allow you to choose all the items listed in ARP Table. **Move** -Move the selected item to IP Bind List. **Refresh** - It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information. **Mode** - ● **Enable** - Choose it to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet. ● **Disable** - Choose it to disable this function. All the settings on this page will be invalid. ● **Strict Bind** – Choose it to lock the connection of the IP/MAC which is not listed in IP Bind List. **Interface** – When **Strict Bind** is selected, specify an interface. The default is “lan1”. **Syslog** - When **Strict Bind/Enable** is selected, you can check the box to save records of Bind IP to MAC in Syslog.

	Apply – Click it to save the setting. **IP Address -** Display the IP address of one device. **MAC Address -** Display the MAC address of the device.
Bind Table	It displays a list for the IP bind to MAC information. **Add** -It allows you to add one pair of IP/MAC address and display on the table of **IP Bind List**. **Edit** -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**. **Select All** -Choose all of the selections at one time. **Rename** -Allow to modify the selected profile name. **Export –** The list for the IP bind to MAC information can be stored as a text file. Such file can be imported by other Vigor router. Thus, it is not necessary for that router to create Bind IP to MAC one by one. **Import –** Click it to import an IP bind to MAC information (e.g., 123.txt) obtained from other Vigor router and to be applied by Vigor3900. **Profile -** Display the name of the profile. **IP Address -** Display the IP address specified for the profile. **MAC -** Display the MAC address specified for the profile. **Comment** – Display the brief description for such profile.

How to configure Bind IP to MAC

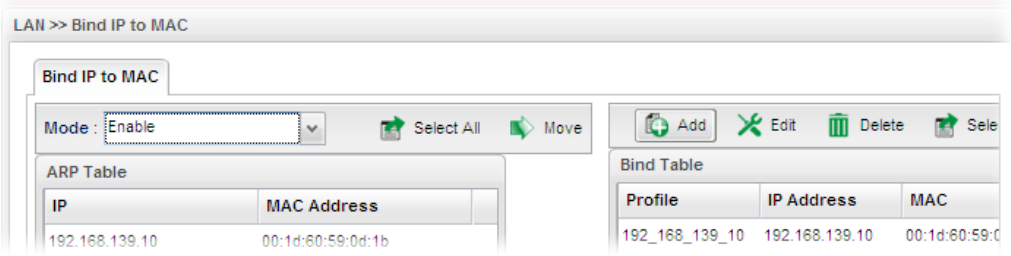
1. Open **LAN>>Bind IP to MAC**.
2. Use the drop down menu to specify a suitable mode.



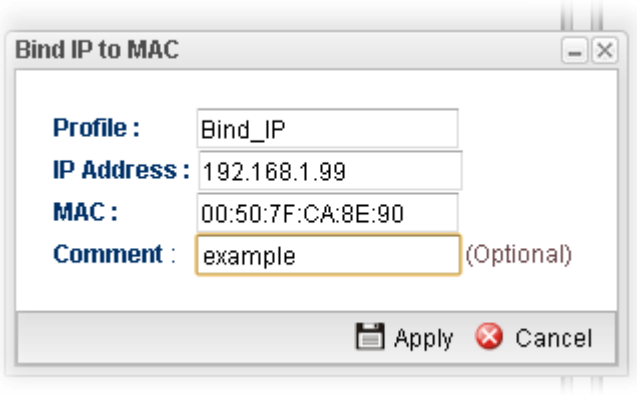
There are three modes offered for you to choose.

- **Disable** – The function of Bind IP to MAC is disabled.
- **Enable** – Specified IP addresses on the Bind Table will be reserved for the device with bind MAC address. Other devices which are not listed on the Bind Table shall still get the IP address from DHCP server.
- **Strict Bind** – Only specified IP addresses will be assigned to the device with bind MAC address. Other devices which are not listed on the Bind Table shall still **NOT** get the IP address from DHCP server.

3. Click **Add** on **Bind Table**.



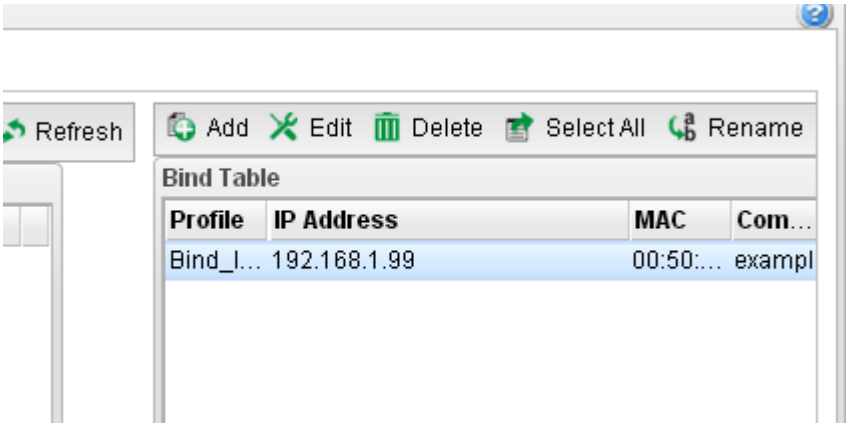
4. The following dialog appears.



Available parameters are listed as follows:

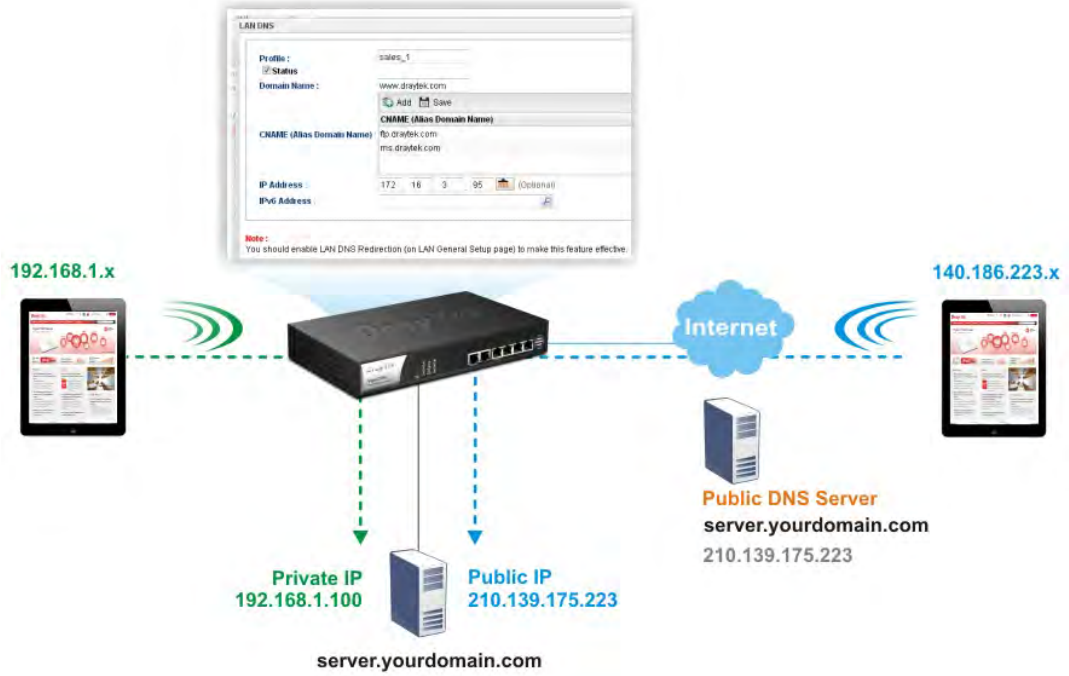
Item	Description
Profile	Type the name of the profile.
IP Address	Type the IP address that will be used for the specified MAC address.
MAC	Type the MAC address that is used to bind with the assigned IP address.
Comment	Type a brief description for such profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

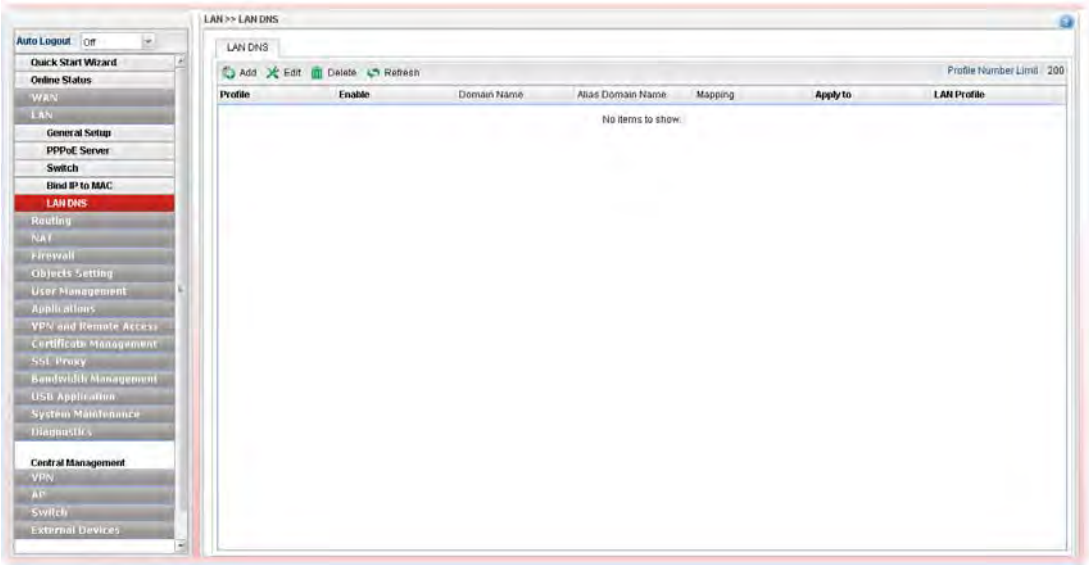
5. Enter all the settings and click **Apply**.
6. A new profile has been added onto **Bind Table**.



4.2.5 LAN DNS

LAN DNS is a simple version of DNS server. It is not necessary for the user to build another DNS server in LAN. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.





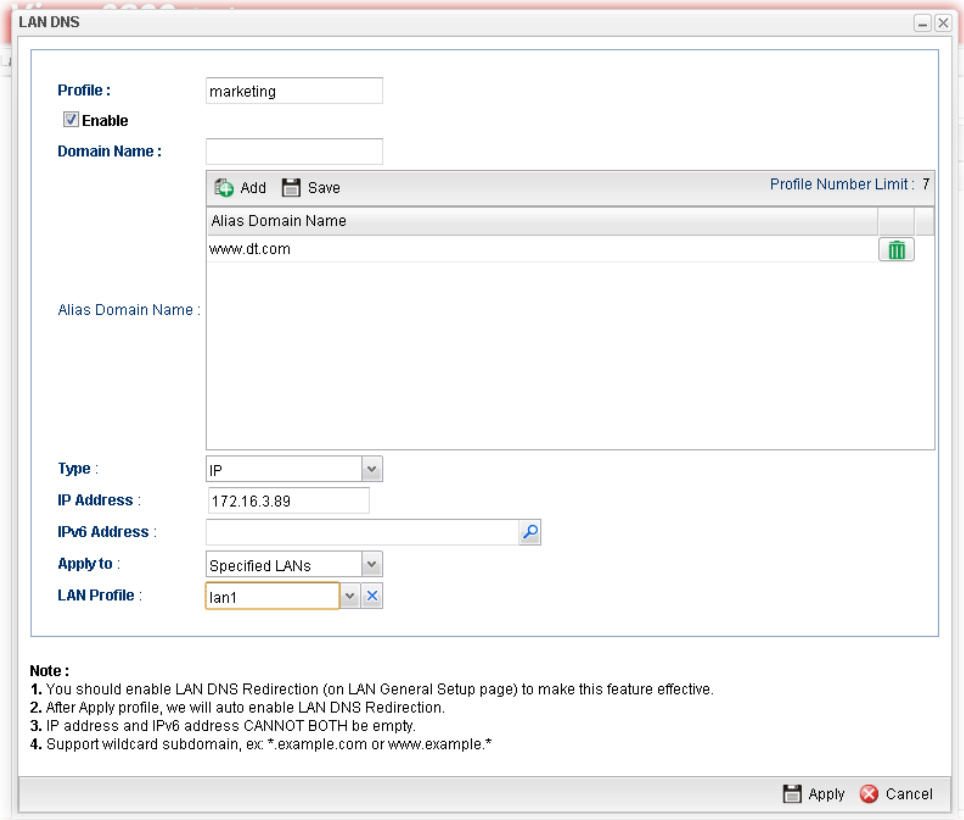
Each item will be explained as follows:

Item	Description
Add	Add a new VLAN ID setting.
Edit	Modify the selected VLAN ID setting. To edit VALN ID setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.

Delete	Remove the selected VLAN ID setting. To delete a VLAN ID setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of the profile.
Status	Display if such profile is enabled (true) or disabled (false).
Domain Name	Display the domain name configured for such profile.
Alias Domain Name	Display the alias domain name for such profile.
Mapping	Display the IP address that domain name and domain name alias will be mapped to.
Applied to	Display which type (Specified LAN or All LANs) the LAN DNS will be applied to.
LAN Profile	Display the LAN profile selected for applying LAN DNS configuration.

How to add a new LAN DNS profile

1. Open **LAN>>LAN DNS.**
2. Click the **Add** button.
3. The following dialog will appear.



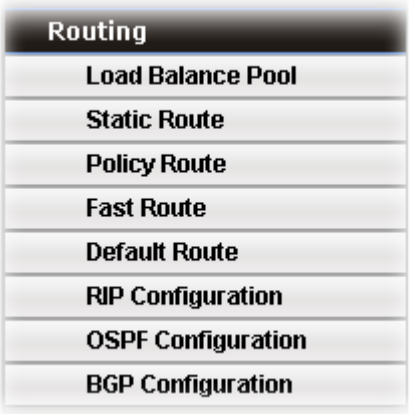
Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
Enable	Check the box to enable such profile.
Domain Name	Type the domain name for such profile.
Alias Domain Name	Type several domain names in this field. LAN DNS will redirect both Domain name and Alias Domain Name to an assigned IP. For example, Domain Name is set with "www.draytek.com", and the Alias Domain Name is set as "www.dray.com". If the IP address is set with "192.168.1.123", then both "www.draytek.com" and "www.dray.com" will be directed to "192.168.1.123".
Type	When you choose **IP**, you need to type IP address and/or IPv6 address as the mapping target. When you choose **CNAME**, you need to type the content (domain) of CNAME as the mapping target. Please choose the suitable type to determine which IP address or CNAME will be mapped by the above domain name/alias domain name. When you choose **FORWARD**, you need to type the IP address of DNS server as the mapping target.
IP Address	Type the IP address in this field. Then, the above domain and/or alias domain name will be mapped to such IP address.
IPv6 Address	Type the IPv6 address in this field. Then, the above domain and/or alias domain name will be mapped to such IPv6 address.
CNAME	Type another domain name in this field. Then, the above domain and/or alias domain name will be mapped to such specified domain.
DNS Server	Type the IP address of the DNS server.
Apply to	LAN DNS can be applied to specified LAN interfaces or all of the LAN interfaces. **LAN Profile** – When you choose **Specified LAN**s, it is necessary to specify at least one LAN profile in this field.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**. The new profile will be added on the screen.

4.3 Routing

This menu contains Static Route, RIP Configuration, OSPF Configuration and BGP Configurations.

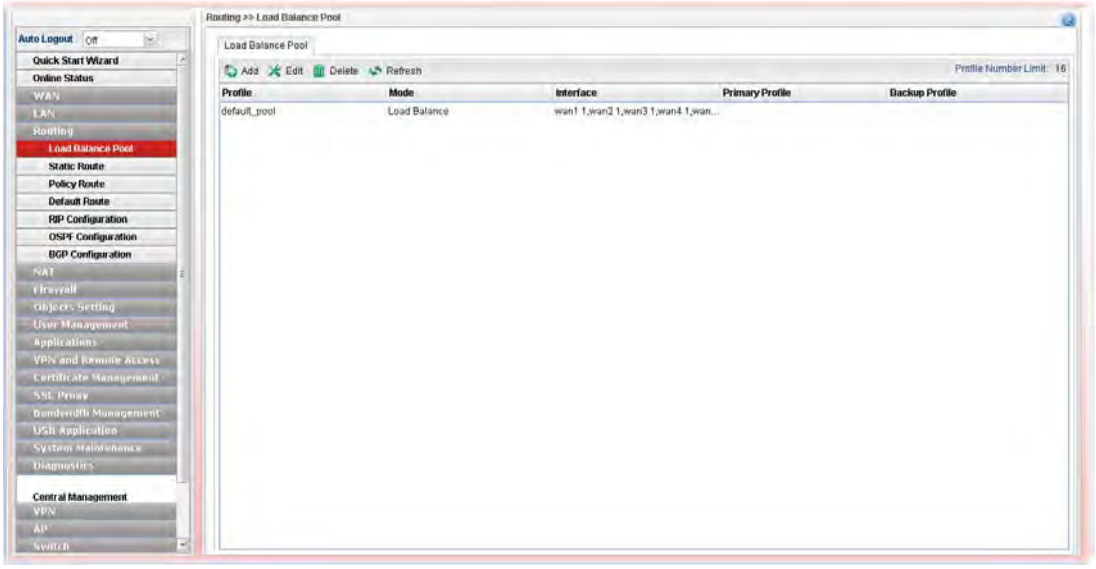


4.3.1 Load Balance Pool

Vigor3900 supports a load balancing function. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN interface. User can assign traffic category and force it to go to dedicate network interface based on the following web page setup.

In the **Routing** group, click the **Load Balance Pool** option.

This page allows the user to integrate **several** WAN profiles as a pool profile specified with the function of load balance or failover. The profiles configured here will be selected in the field of **Routing >>Default Route** page.



Each item will be explained as follows:

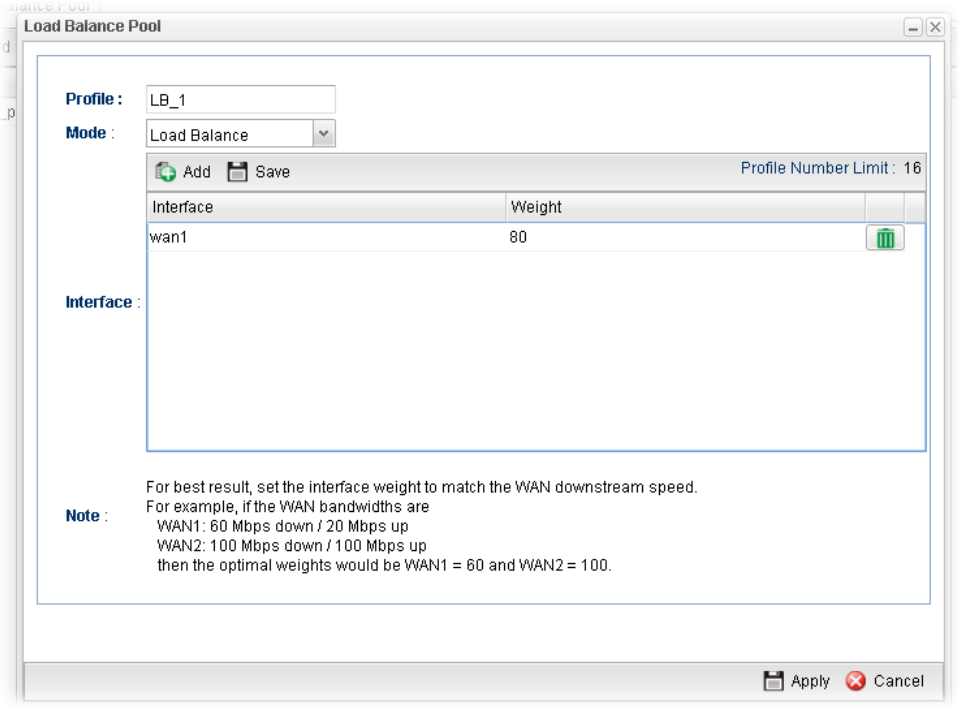
Item	Description
Add	Add a new pool profile.
Edit	Modify the selected pool profile.

	To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected rule profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the load balance profile.
Mode	Display the mode (failover or load balance) used by the pool profile.
Interface	Display the name of the WAN profiles for Load Balance rule.
Primary Profile	Display the primary profile configured in Failover page for such profile.
Backup Profile	Display the backup profile configured in Failover page for such profile.

There are two modes, **Load Balance** and **Failover**, for you to choose as the **Pool** configuration. If you choose **Load Balance**, the tab of **Load Balance** will be shown which allows you to configure for different WAN interfaces. If you choose **Failover**, the tab of **Failover** will be displayed which allows you to specify the primary profile and backup profile for such **Pool** setting.

How to add a Pool profile for Load Balance

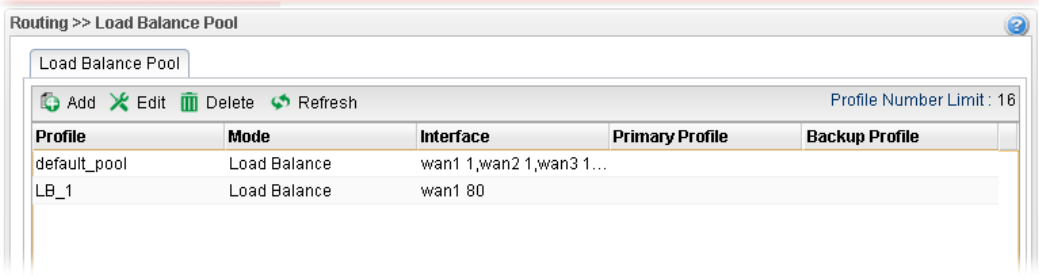
1. Open **Routing>>Load Balance Pool**.
2. Simply click the **Add** button to open the following dialog. Type a name (e.g., LB_1) for such profile.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Mode	Choose **Load Balance** as the **Mode** selection.
Interface	Click **Add**. A new line for adding new entry will appear. Use the drop down list of **Interface** to choose the WAN profiles that will be in the Load Balance Pool. Type the value for **Weight**.

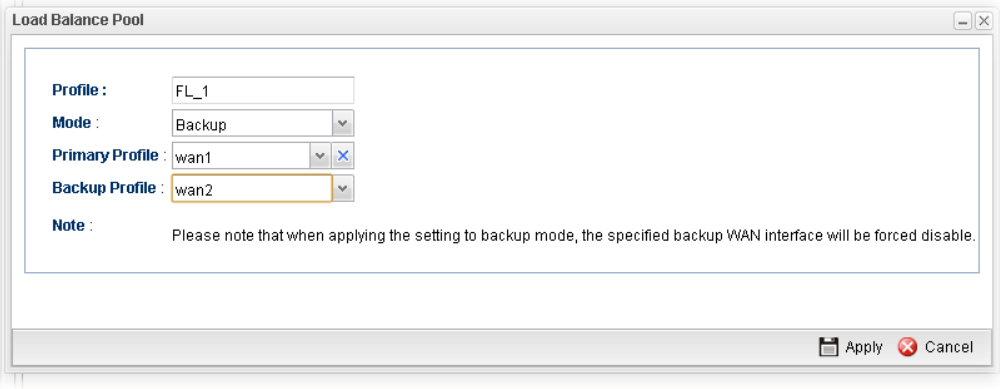
3. Click **Apply**. A new profile will be added on the page.



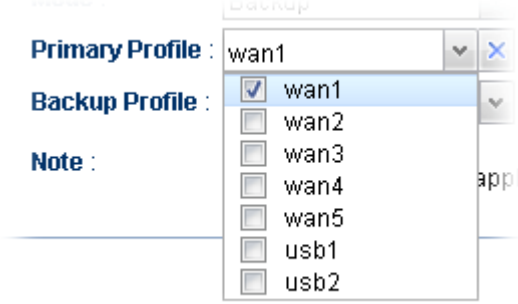
How to add a Pool profile for Backup

Such page allows you to set a backup profile which will be activated when the primary profile is invalid by any reason.

1. Open **Routing >>Load Balance Pool**.
2. Simply click the **Add** button to open the following dialog. Type a name (e.g., FL_1) for such profile. Choose **Backup** as the **Mode** selection.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Mode	Choose **Backup** as the **Mode** selection.
Primary Profile	In default, the system will apply Primary Profile. If Primary Profile cannot be used any more, the Backup Profile will be used instead. Use the drop down list to choose the one you need.
Backup Profile	Use the drop down list to choose the one you need. 

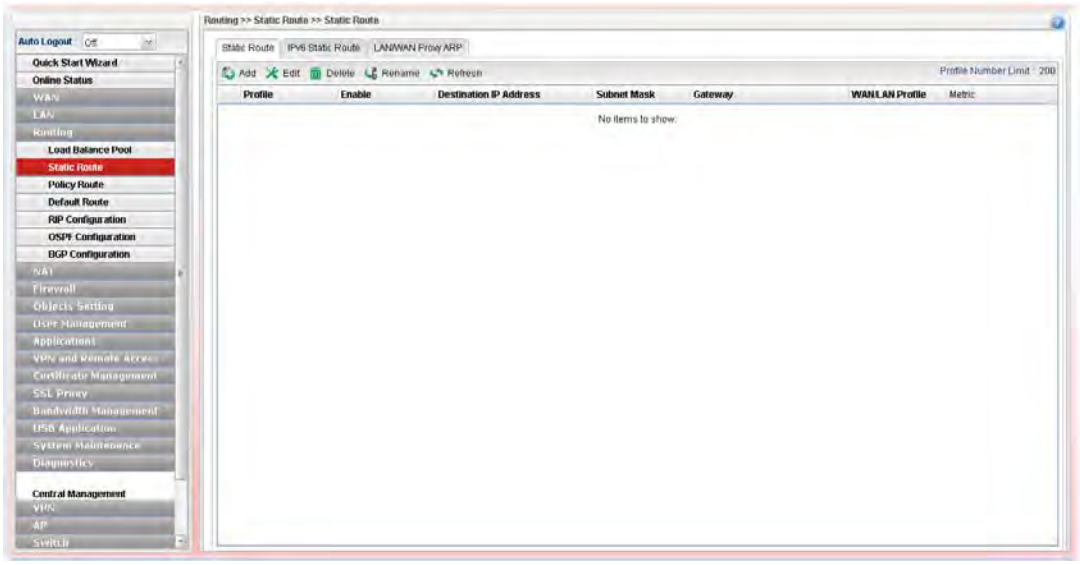
3. Click **Apply**. A new profile will be added on the page.

4.3.2 Static Route

When there are several subnets in LAN, a more effective and quicker way for connection is static route rather than other methods. Simply set rules to forward data from one specified subnet to another specified subnet.

4.3.2.1 Static Route

The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.



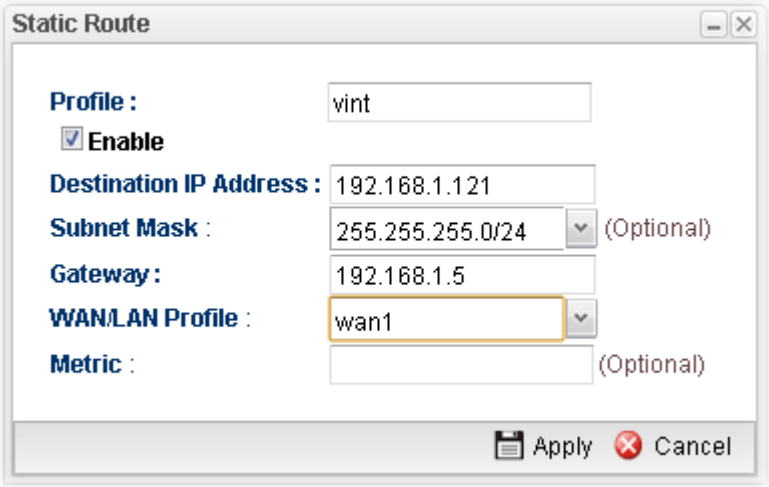
Each item will be explained as follows:

Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected static route setting. To delete a static route setting, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of such static route.
Enable	Display the status of the profile. False means disabled; True means enabled.
Destination IP Address	Display the IP address for such static route profile.
Subnet Mask	Display the subnet mask for such static route profile.
Gateway	Display the gateway address for such static route profile.

WAN/LAN Profile	Display the subnet / LAN or WAN profile of the gateway.
Metric	Display the distance to the target.

How to add a new Static Route profile

1. Open **Routing>>Static Routing** and click the **Static Route** tab.
2. Click the **Add** button.
3. The following dialog will appear.



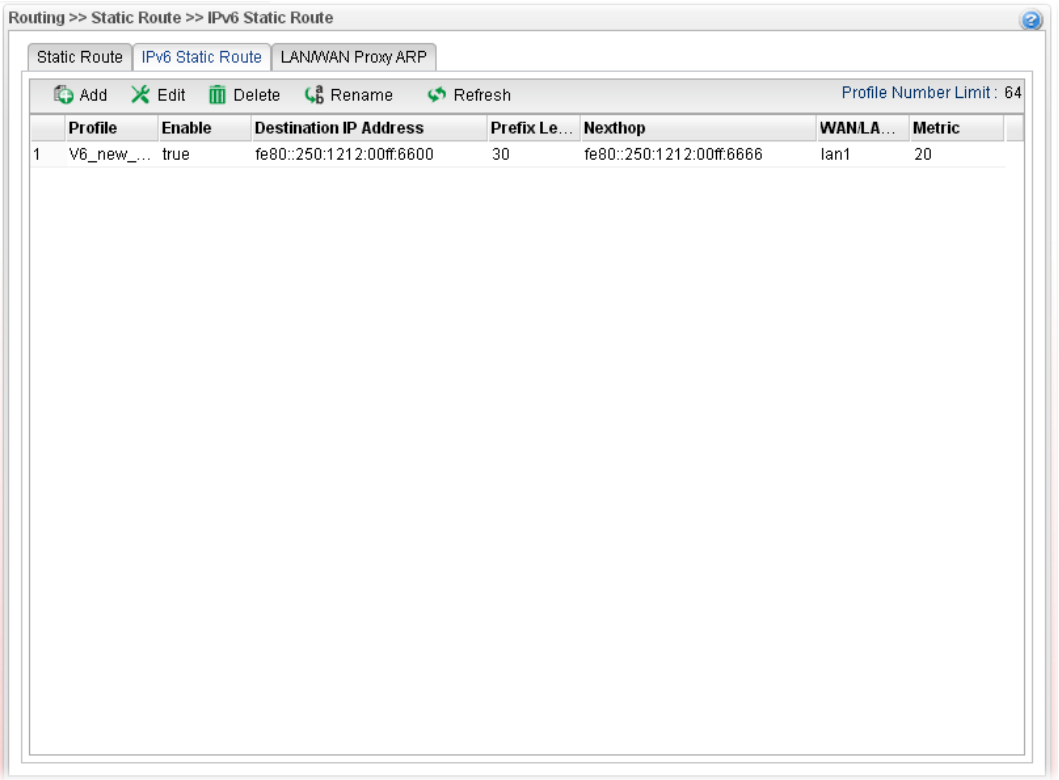
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the static route profile.
Enable	Check this box to enable such profile.
Destination IP Address	Type the IP address for such static route profile.
Subnet Mask	Use the drop down list to choose the subnet mask for such static route profile.
Gateway	Type the gateway address for such static route profile.
WAN/LAN Profile	Choose one of the LAN/WAN profiles of the gateway for such static route.
Metric	Type the distance to the target (usually counted in hops).
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

5. Enter all of the settings and click **Apply**. The new profile will be added on the screen.

4.3.2.2 IPv6 Static Route

For IPv6 protocol, click the **IPv6 Static Route** tab to configure detailed settings.



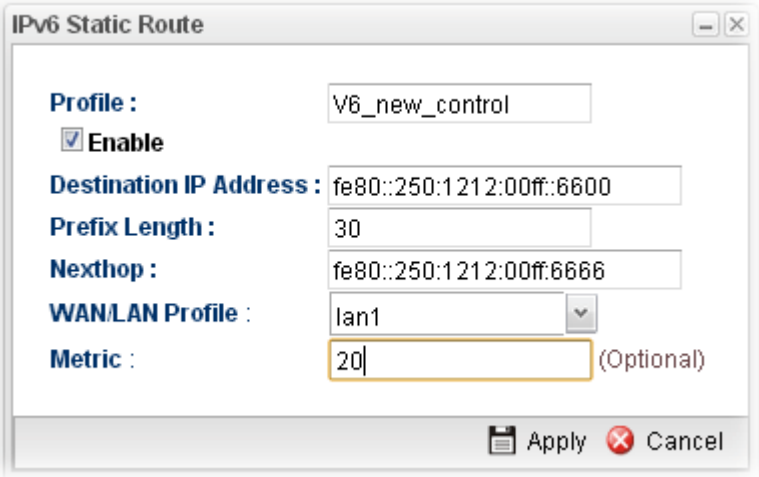
Each item will be explained as follows:

Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected static route setting. To delete a static route setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of such static route.
Enable	Display the status of the profile. False means disabled; True means enabled.
Destination IP Address	Display the IP address for such static route profile.
Prefix Length	Display the prefix length of the profile.
Nexthop	Display the nexthop address for such static route profile.

WAN / LAN Profile	Display the subnet LAN or WAN profile of the gateway.
Metric	Display the distance to the target.

How to add a new IPv6 Static Route profile

1. Open **Routing>>Static Route** and click the **IPv6 Static Route** tab.
2. Click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

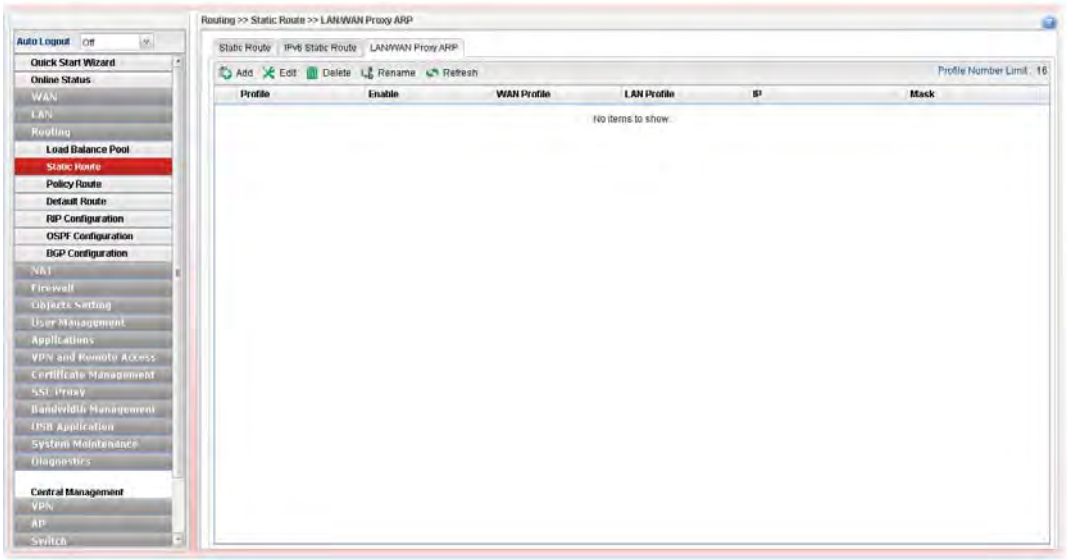
Item	Description
Profile Name	Type the name of the static route profile.
Enable	Check this box to enable such profile.
Destination IP Address	Type the IP address for such static route profile.
Prefix Length	Type the prefix length for such profile.
Nexthop	Type the nexthop address for such static route profile.
WAN/LAN Profile	Choose one of the LAN/WAN profiles of the gateway for such static route.
Metric	Type the distance to the target (usually counted in hops).
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**. The new profile will be added on the screen.

4.3.2.3 LAN/WAN Proxy ARP

To make local device in LAN accessing into external network without passing NAT or let the remote device access into the local device without passing NAT behind the router, please use IP routing function to complete the work.

Usually, the local device might be assigned with a public IP address or an IP address with the same subnet as certain WAN. When the local device tries to transmit the data packets out, Vigor3900 will send it out through that certain WAN interface without passing through NAT. Meanwhile, remote device also can access the local device directly without any difficulty.



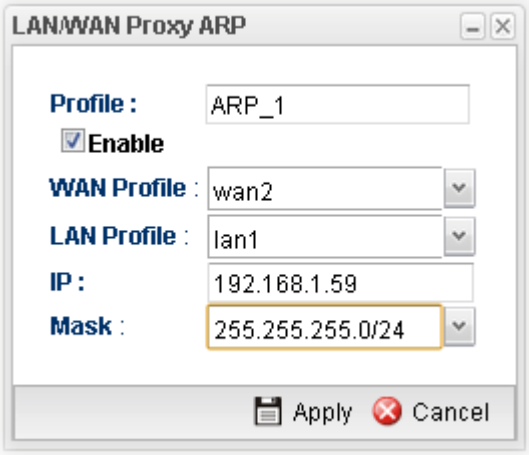
Each item will be explained as follows:

Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected static route setting. To delete a static route setting, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of such profile
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN profile used for such ARP profile.
LAN Profile	Display the LAN profile used for such ARP profile.
IP	Display the IP address used by such ARP profile.

Mask	Display the mask address used by such ARP profile.

How to add a new Proxy ARP profile

1. Open **Routing>>Static Route** and click the **LAN/WAN Proxy ARP** tab.
2. Click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the static route profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose one of the WAN/USB profiles of the gateway for such profile.
LAN Profile	Choose one of the LAN profiles for such profile.
IP	Type an IP address for such profile.
Mask	Use the drop down menu to specify mask address.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**. The new profile will be added on the screen.

4.3.3 Policy Route

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

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

- **Auto load balance to reduce the loading of the network traffic.**

  You have to manually create policy rules in order to force the traffic going to dedicate network interface.

- **Strict Bind.**

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

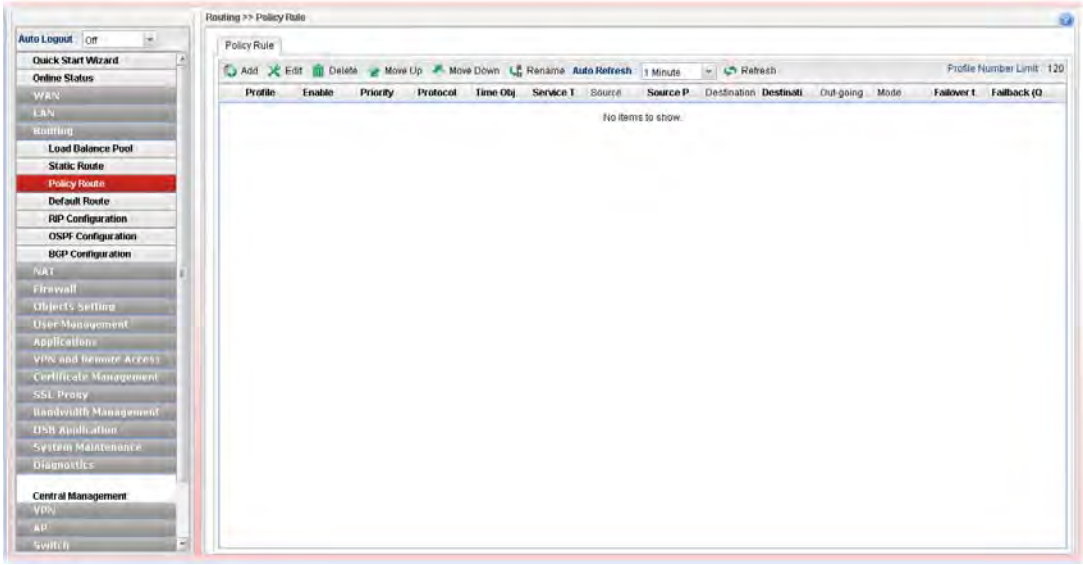
- **Address Mapping.**

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

- **Other routing.**

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

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



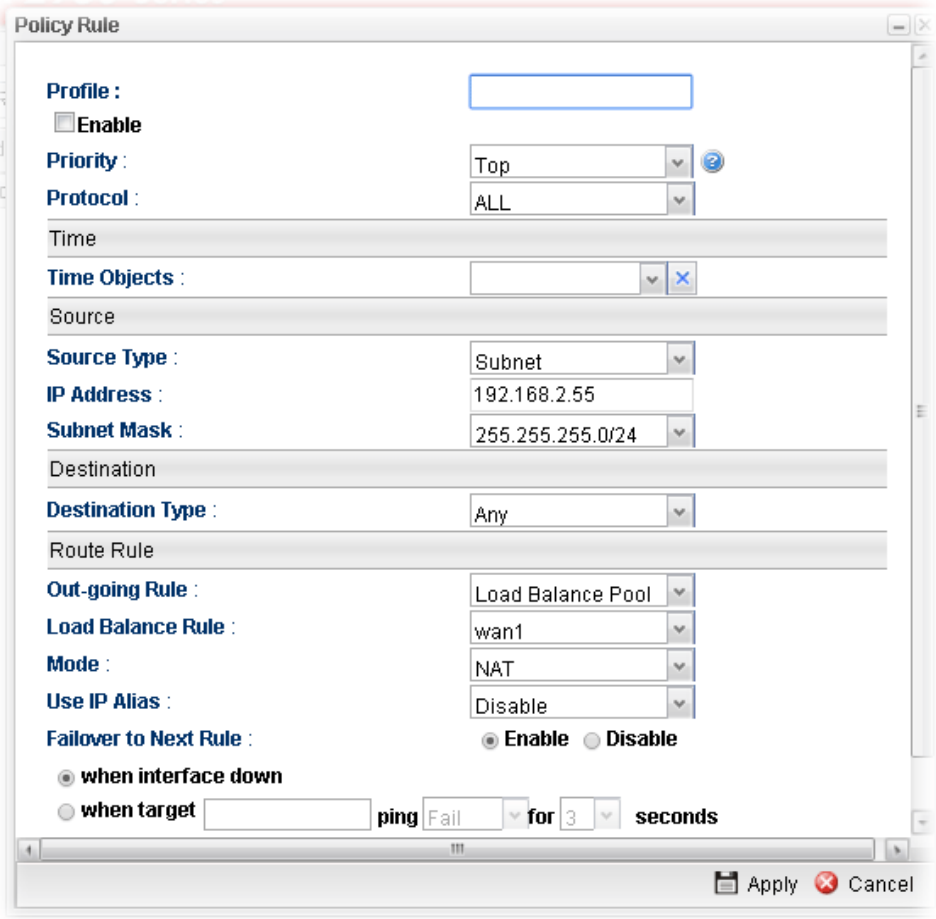
Each item will be explained as follows:

Item	Description
Add	Add a new rule profile.
Edit	Modify the selected rule profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected

	rule.
Delete	Remove the selected rule profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Move Up / Move Down	Move the selected profile up or down.
Rename	Allow to modify the selected profile name.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Refresh	Renew current web page.
Profile	Display the name of the rule.
Enable	Display the status of the profile. False means disabled; True means enabled.
Priority	Display the priority of such rule.
Protocol	Display the protocol of such rule.
Time Objects	Display the name of time object.
Service Type Objects	Display the name of service type.
Source	Display the name of the source subnet/IP object/IP group.
Source Port	Display the source port range.
Destination	Display the name of the destination subnet/IP object/IP group/DNS object.
Destination Port	Display the destination port range.
Out-going Rule	Display the route way (where the traffic forwarded) selected.
Mode	Display the route mode (NAT or Routing) used by such policy route.
Failover to Next Rule	Display the status (enabled or disabled) of the function.
Failback (Quick Recover)	Display the status (enabled or disabled) of the function.

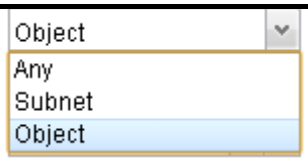
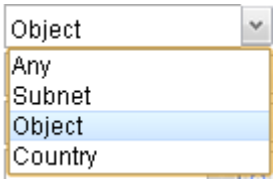
How to add a new policy rule

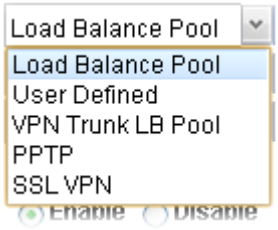
1. Open **Routing>>Policy Route**.
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the rule.
Enable	Check this box to enable such profile.
Priority	Choose the priority for such profile (top, high and normal).
Protocol	Choose a protocol (ALL, TCP, UDP, TCP/UDP and ICMP) for such rule applied to load balance. **All** is the default setting.
Time	Choose a time object to be applied by such profile.
Service Protocol	It is available when TCP/UDP is selected as protocol. Choose a profile for such rule.
Source	**Source Type** - Choose the address type (Any, Subnet or Object) for such rule.

	 Each type will bring different settings for configuration.
	When Subnet is selected as Source Type
	• **IP Address** - Type an IP address here as the source IP address for such rule. • **Subnet Mask** - Use the drop down list on the right to choose a suitable mask for the source.
	When Object is selected as Source Type
	• **IP Object –** Use the drop down list to choose the source IP object(s) for such rule profile. • **IP Group –**Use the drop down list to choose the source IP group(s) for such rule profile.
Destination	**Destination Type** - Choose the address type (Any, Subnet, Object or Country) for such rule.  Each type will bring different settings for configuration.
	When Subnet is selected as Destination Type
	• **IP Address** - Type an IP address here as the destination IP address for such rule. • **Subnet Mask** - Use the drop down list on the right to choose a suitable mask for the destination.
	When Object is selected as Destination Type
	• **IP Object –** Use the drop down list to choose the destination IP object(s) for such rule profile. • **IP Group –**Use the drop down list to choose the destination IP group(s) for such rule profile. • **DNS Object** - Use the drop down list to choose DNS object(s) for such rule profile.
	When Country is selected as Destination Type
	• **Country Object** - Use the drop down list to choose the country object(s) for such rule profile.
Route Rule	**Out-going Rule** - It determines the way (interface) that the incoming traffic will be forwarded to.



Load Balance Pool –The incoming traffic will be forwarded to specified WAN interface or load balance pool.

User Defined –The incoming traffic will be forwarded to the specified WAN or LAN interface with a user defined gateway.

VPN Trunk LB Pool –The incoming traffic will be forwarded to specified VPN trunk profile.

PPTP – The incoming traffic will be forwarded to specified PPTP VPN profile.

SSL VPN – The incoming traffic will be forwarded to specified SSLVPN profile.

When Load Balance Pool is selected as Out-going Rule

- **Load Balance Rule** - Choose one of the profiles to be used by such rule. In which, wan1 to wan2 profiles are configured in default. In addition, profiles configured in **Routing**>>**Load Balance Pool** also will be displayed here.
- **Mode** – Specify which mode (NAT or Routing) will be used for such route rule.
- **Use IP Alias** - Click **Enable** to enable such function. Or, click **Disable** to disable such function. When **Enable** is chosen, choose an alias WAN IP address to replace the default WAN IP address.
- **Failover to the Next Rule** - When the specified interface disconnects due to some reason, the router can use next matched policy route rule to perform data transmission automatically. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
  - **When interface down** - When the specified interface (selected by out-going rule) disconnects, the router will use next rule match with policy route to perform data transmission.
  - **When target …..**- When certain IP or domain connects successfully or fails to connect for several seconds, Vigor router will treat the selected interface as disconnected and activate Failover mechanism. For example, you might configure settings as:

    Out-going Rule : User Defined

	Out-going interface : wan1 **Failover : Enable** **when target [8.8.8.8] ping [Fail] for [5] seconds** Then, it means even if wan1 connects to network always, once the target cannot be detected by Vigor router for 5 seconds, Vigor router will use next matched rule to perform data transmission. ● **Failback (Quick Recover) -** When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
When User Defined is selected as Out-going Rule	
	● **Outgoing Interface** - Choose one of the profiles to be used by such rule. In which, wan1 to wan2 profiles are configured in default. ● **Out-going (Gateway)** – Type an IP address as the gateway. Notice that LAN interface does not have default gateway. You MUST specify a gateway if you choose LAN as out-going interface. ● **Mode** – Specify which mode (NAT or Routing) will be used for such route rule. ● **Use IP Alias -** Click **Enable** to enable such function. Or, click **Disable** to disable such function. When **Enable** is chosen, choose an alias WAN IP address to replace the default WAN IP address. ● **Failover to the Next Rule** - When the specified interface disconnects due to some reason, the router can use next matched policy route rule to perform data transmission automatically. Click **Enable** to enable such function. Or, click **Disable** to disable such function. ◆ **When interface down** - When the specified interface (selected by out-going rule) disconnects, the router will use next rule match with policy route to perform data transmission. ◆ **When target …..**- When certain IP or domain connects successfully or fails to connect for several seconds, Vigor router will treat the selected interface as disconnected and activate Failover mechanism. For example, you might configure settings as: **Out-going Rule : User Defined** **Out-going interface : wan1**

Failover : Enable

when target [8.8.8.8] ping [Fail] for [5] seconds

Then, it means even if wan1 connects to network always, once the target cannot be detected by Vigor router for 5 seconds, Vigor router will use next matched rule to perform data transmission.

- **Failback (Quick Recover) -** When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. Click **Enable** to enable such function. Or, click **Disable** to disable such function.

When VPN Trunk LB Pool selected as Out-going Rule

- **Load Balance Pool –** IPsec VPN trunk profile can be selected by such policy route. You should define the VPN trunk profile in **VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool** before
- **Mode** – Specify which mode (NAT or Routing) will be used for such route rule.
- **Failover to the Next Rule** - When the specified interface disconnects due to some reason, the router can use next route rule to perform data transmission automatically. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
  - **When interface down** - When the specified interface (selected by out-going rule) disconnects, the router will use next rule match with policy route to perform data transmission.
  - **When target …..**- When certain IP or domain connects successfully or fails to connect for several seconds, Vigor router will treat the selected interface as disconnected and activate Failover mechanism. For example, you might configure settings as:

    Out-going Rule : User Defined

    Out-going interface : wan1

    Failover : Enable

    when target [8.8.8.8] ping [Fail] for [5] seconds

    Then, it means even if wan1 connects to network always, once the target cannot be detected by Vigor router for 5 seconds, Vigor router will use next matched rule to perform data transmission.

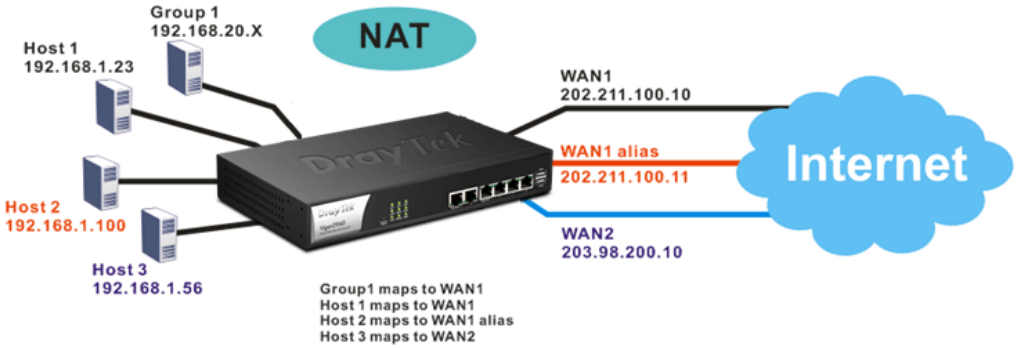
	● **Failback (Quick Recover) -** When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
	When PPTP selected as Out-going Rule
	● **PPTP Profile – VPN PPTP dial-out and VPN PPTP dial-in** profiles can be selected by such policy route. ● **Mode** – Specify which mode (NAT or Routing) will be used for such route rule. ● **Failover to the Next Rule** - When the specified interface disconnects due to some reason, the router can use next route rule to perform data transmission automatically. Click **Enable** to enable such function. Or, click **Disable** to disable such function. ◆ **When interface down** - When the specified interface (selected by out-going rule) disconnects, the router will use next rule match with policy route to perform data transmission. ◆ **When target …..**- When certain IP or domain connects successfully or fails to connect for several seconds, Vigor router will treat the selected interface as disconnected and activate Failover mechanism. For example, you might configure settings as: **Out-going Rule : User Defined** **Out-going interface : wan1** **Failover : Enable** **when target [8.8.8.8] ping [Fail] for [5] seconds** Then, it means even if wan1 connects to network always, once the target cannot be detected by Vigor router for 5 seconds, Vigor router will use next matched rule to perform data transmission. ● **Failback (Quick Recover) -** When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
	When SSL VPN selected as Out-going Rule
	● **SSL Profile – VPN SSL** profiles can be selected by such policy route. ● **Mode** – Specify which mode (NAT or Routing)

	will be used for such route rule. ● **Failover to the Next Rule** - When the specified interface disconnects due to some reason, the router can use next route rule to perform data transmission automatically. Click **Enable** to enable such function. Or, click **Disable** to disable such function. ◆ **When interface down** - When the specified interface (selected by out-going rule) disconnects, the router will use next rule match with policy route to perform data transmission. ◆ **When target …..**- When certain IP or domain connects successfully or fails to connect for several seconds, Vigor router will treat the selected interface as disconnected and activate Failover mechanism. For example, you might configure settings as: **Out-going Rule : User Defined** **Out-going interface : wan1** **Failover : Enable** **when target [8.8.8.8] ping [Fail] for [5] seconds** Then, it means even if wan1 connects to network always, once the target cannot be detected by Vigor router for 5 seconds, Vigor router will use next matched rule to perform data transmission. ● **Failback (Quick Recover)** - When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. Click **Enable** to enable such function. Or, click **Disable** to disable such function.
Apply	Click it to save the configuration.
Cancel	Click it to return to the factory setting.

4. Enter all of the settings and click **Apply**. The new rule profile will be added on the screen.

Example 1: How to Setup Address Mapping by Using Policy Route

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.



Suppose the WAN settings for a router are configured as follows:

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11

WAN2: 203.98.200.10

Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

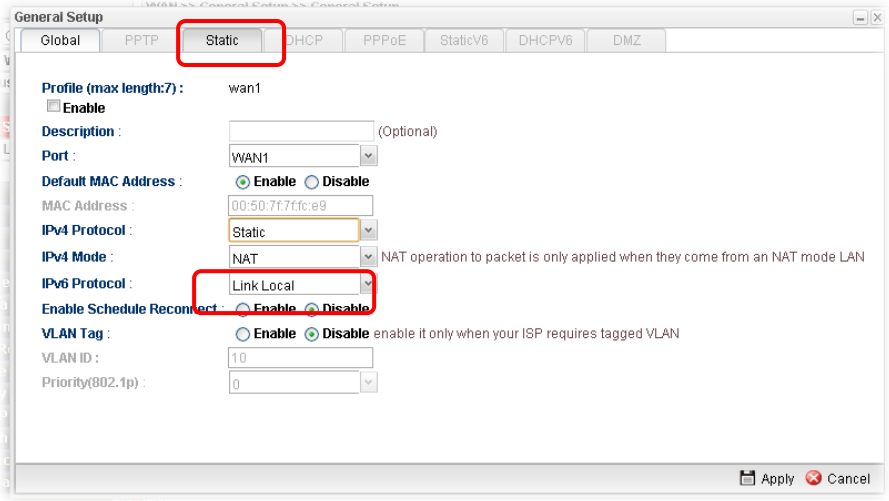
With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

NAT Address Mapping function lets you specify the outgoing IP address(es) for one internal IP address or a block of internal IP addresses.

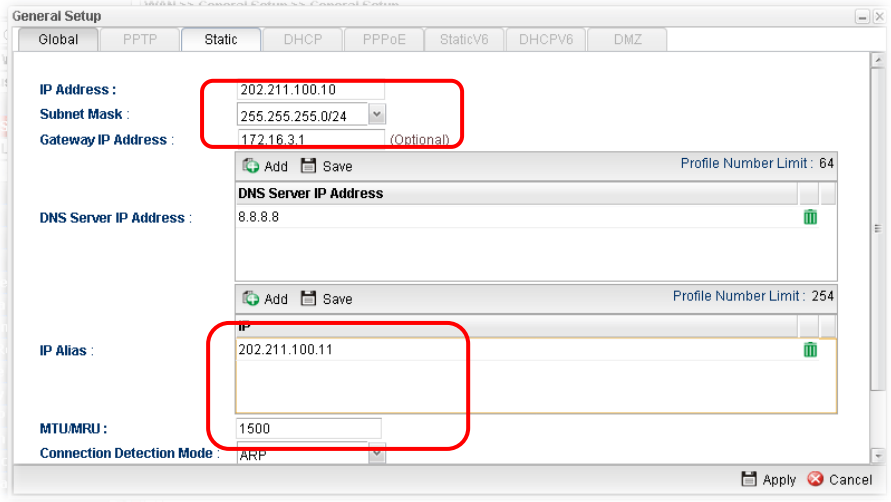
We will take an example to introduce how to make use of this feature.

1. Log into the web user interface of Vigor3900.

2. Open **WAN>>General Setup**. For WAN1, choose wan1 item and click **Edit**. Choose **Static** as the **IPv4 Protocol.**

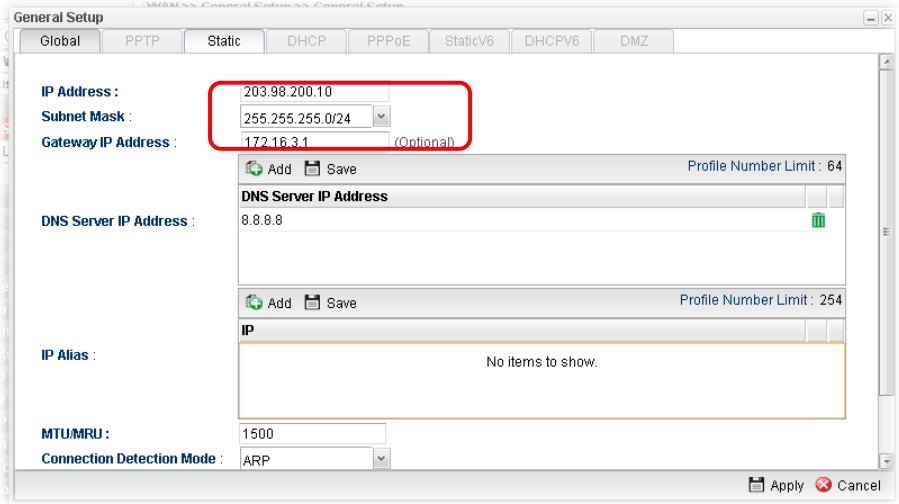


3. From the following page, set main WAN IP address as *202.211.100.10*.

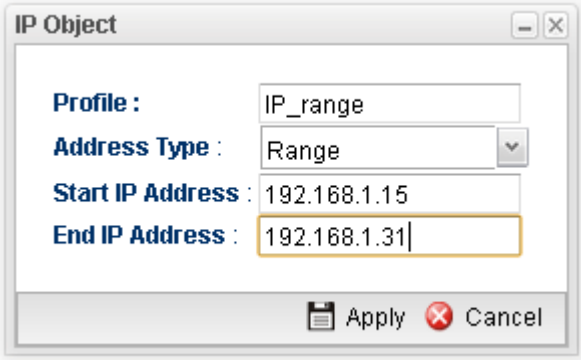


Click **Add** on IP Alias to configure the other IP address which is *202.211.100.11*.

4. After finished configuration for WAN1, continue to configure WAN2. At this time, the IP switch shall be set as "*203.98.200.10*".

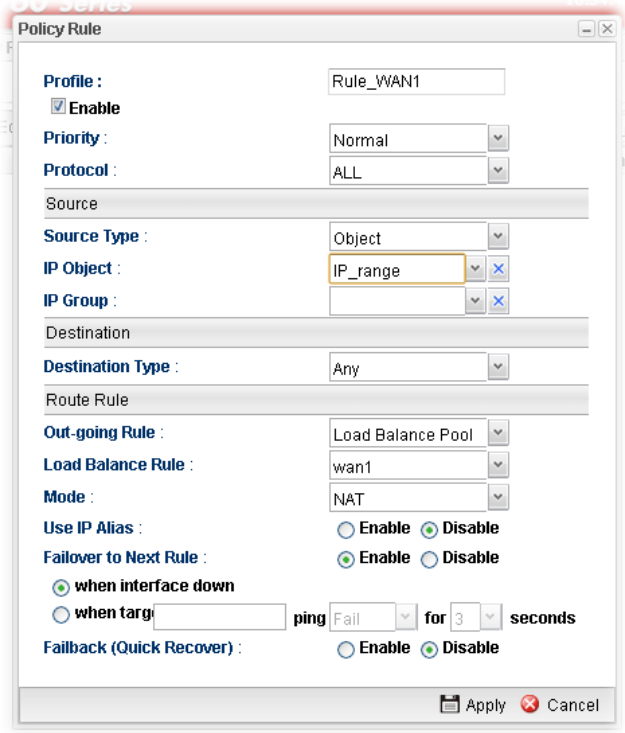


5. Open **Objects Setting>>IP Object** and click **Add** to create a new IP object profile. Type the required information as shown below. Click **Apply** to save the settings.

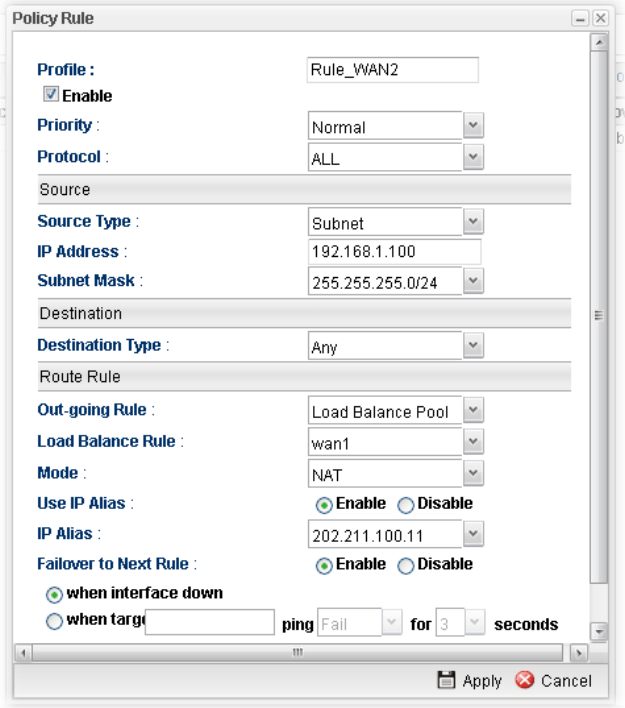


6. Open **Routing>> Policy Route** and click **Add** to create a new profile.

7. In the following page, check the box of **Enable**. Choose **Object** as the **Source Type** and choose IP range object profile from the drop down list of IP Object. Click **Apply** to save the settings.



And,

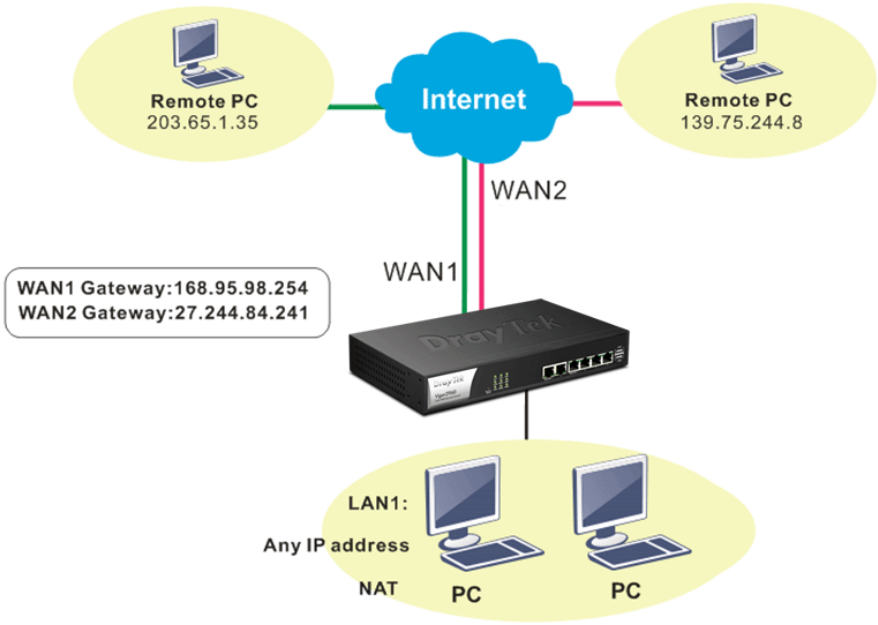


8. Upon completing the above configuration, you have specified the outgoing IP address(es) for some specific computers.

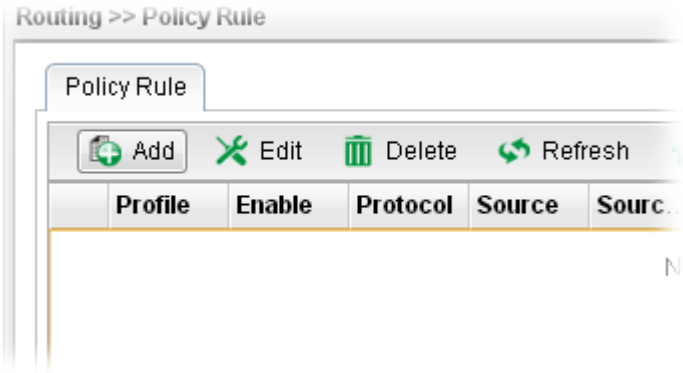
Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

Example 2: How to Setup Load Balance by Using Policy Route

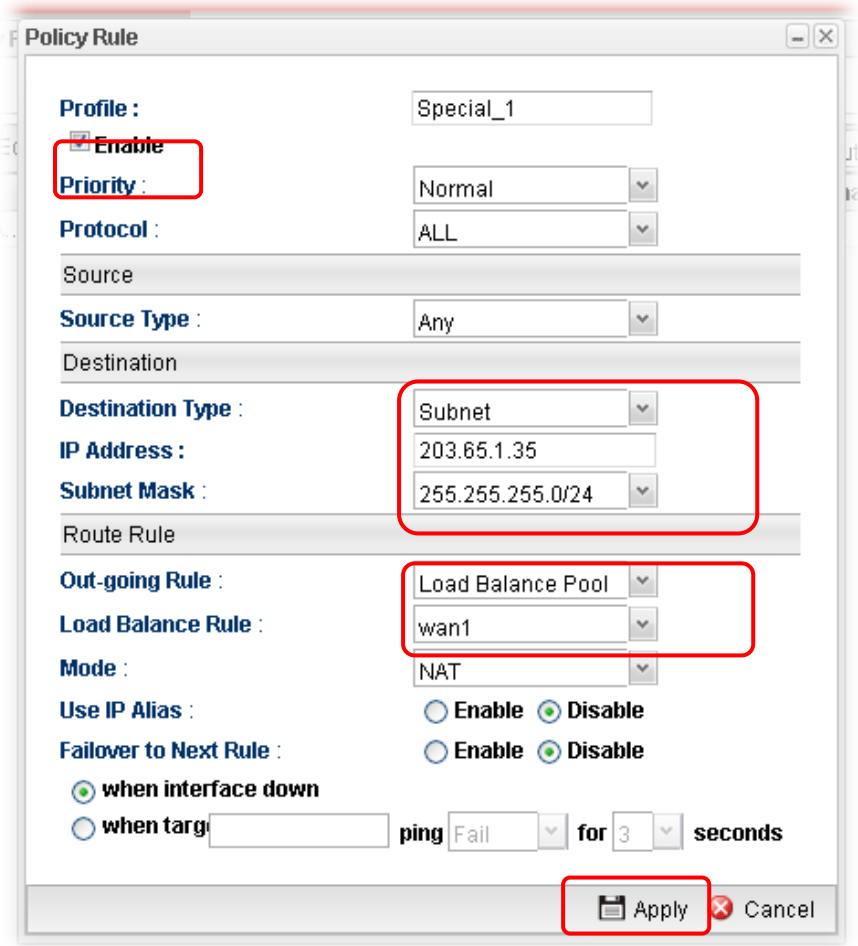
The following figure shows a simple application of load balance. WAN1 and WAN2 can be used to access into Internet. The PC in LAN1 can send the data to the remote PC through the specified WAN1.



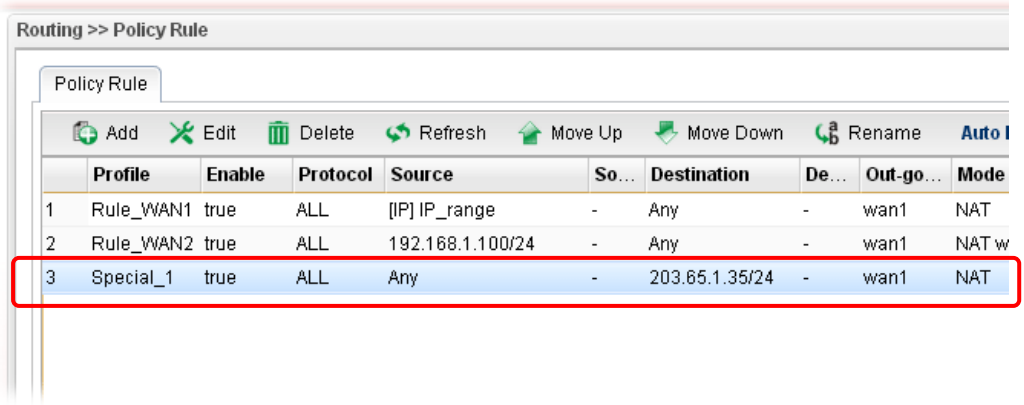
1. Access into web user interface of Vigor3900.
2. Open **Routing>> Policy Route** and click **Add** to create a new profile.



3. In the following page, type a name for such profile; check **Enable**; choose **Subnet** as **Destination Type**; type 203.65.1.35 as IP address; choose **Load Balance Pool** as **Out-going Rule**; choose WAN1 as the **Load Balance Rule**; click **Disable** for **Failover to Next Rule**.



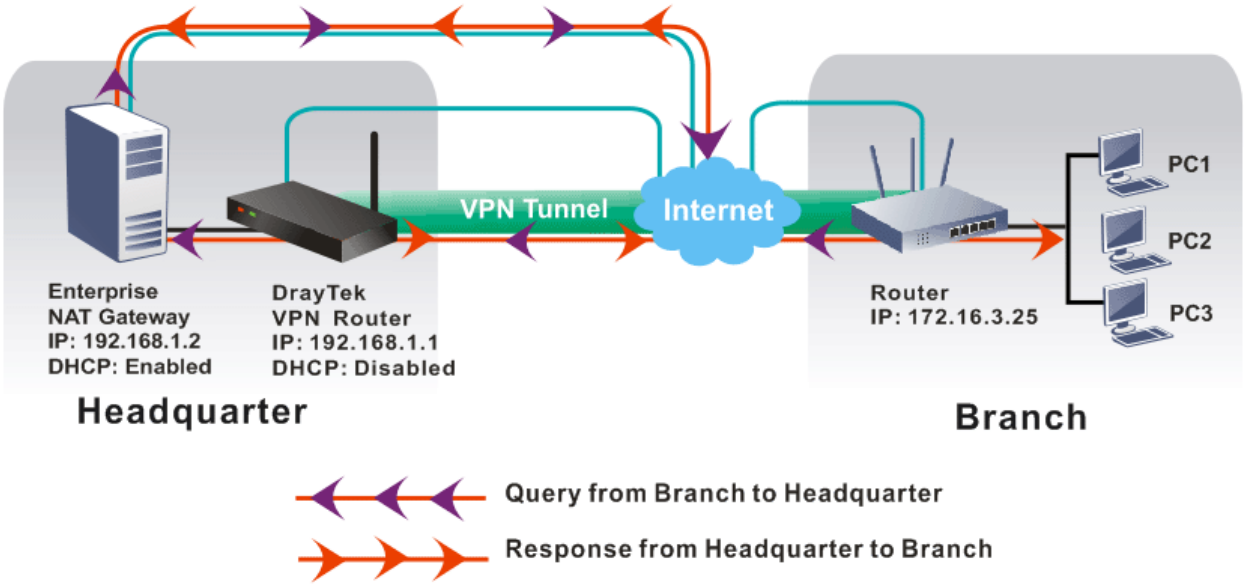
4. After finished the above settings, click **Apply** to save the configuration.



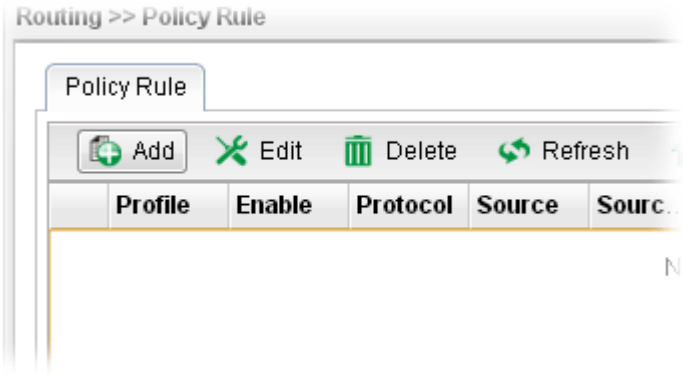
Now, any packets from LAN1 sent to the remote PC (IP address: 203.65.1.35) will be forcefully to pass through WAN1.

Example 3: How to Customize a Secure Route between Headquarter and Branch by Using Policy Route

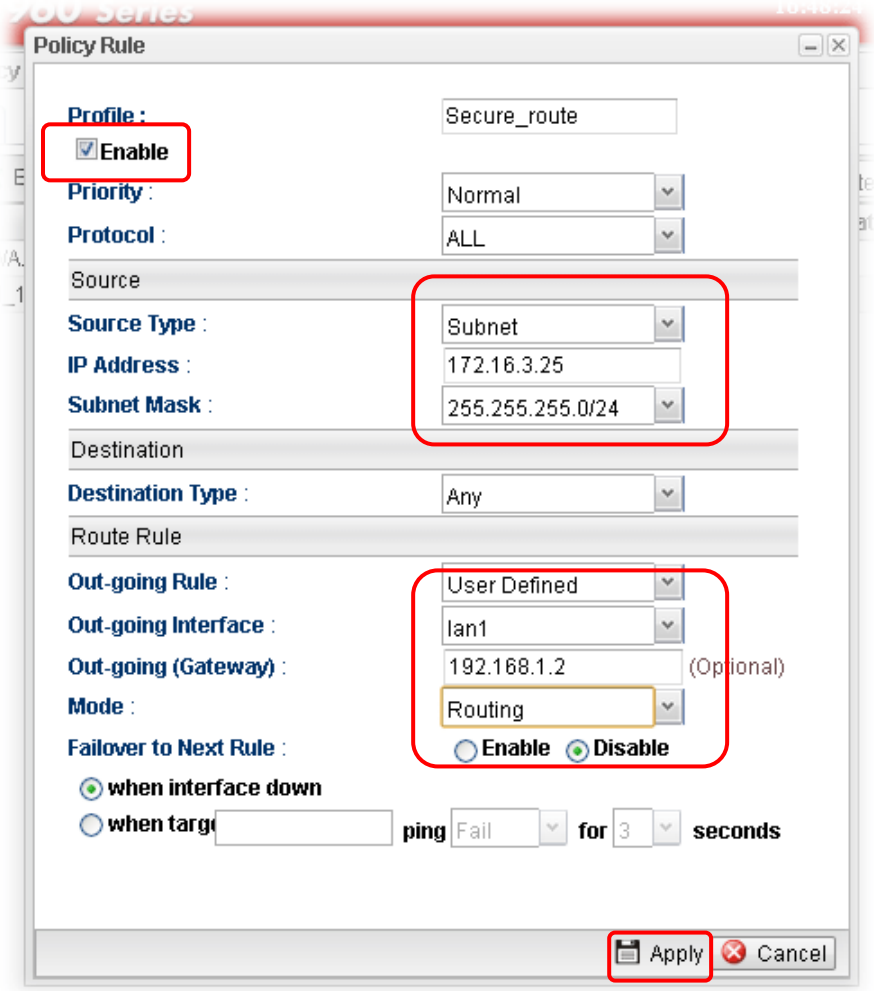
A LAN to LAN VPN tunnel is built between DrayTek VPN router (e.g., Vigor3900) and the remote router. Enterprise firewall router (in Headquarter) can control the all of the traffic coming from the remote PC (in Branch) which wants to access into Internet.



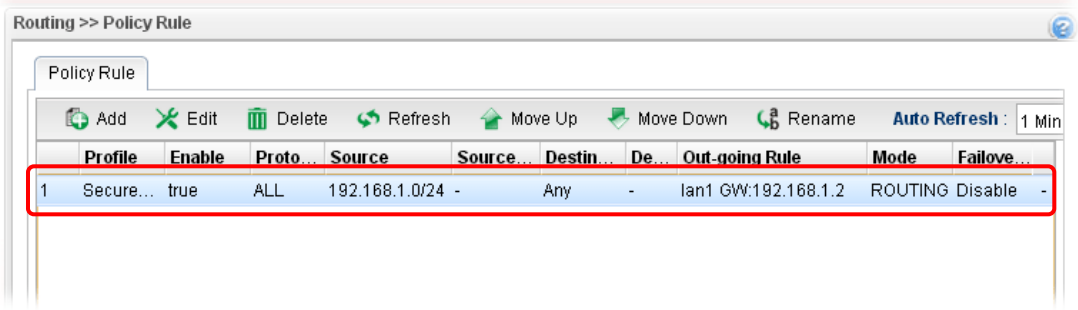
1. Access into web user interface of Vigor3900.
2. Open **Routing>> Policy Route** and click **Add** to create a new profile.



3. In the following page, type a name for such profile (e.g., Secure_route); choose **Subnet** as **Source Type** and type the source IP address with 172.16.3.25; choose **User Defined** as **Out-going Rule**; choose **lan1** as the **Out-going Interface**; type 192.168.1.2 as the **Out-going (Gateway)**; and click **Disable** for **Failover to Next Rule**.

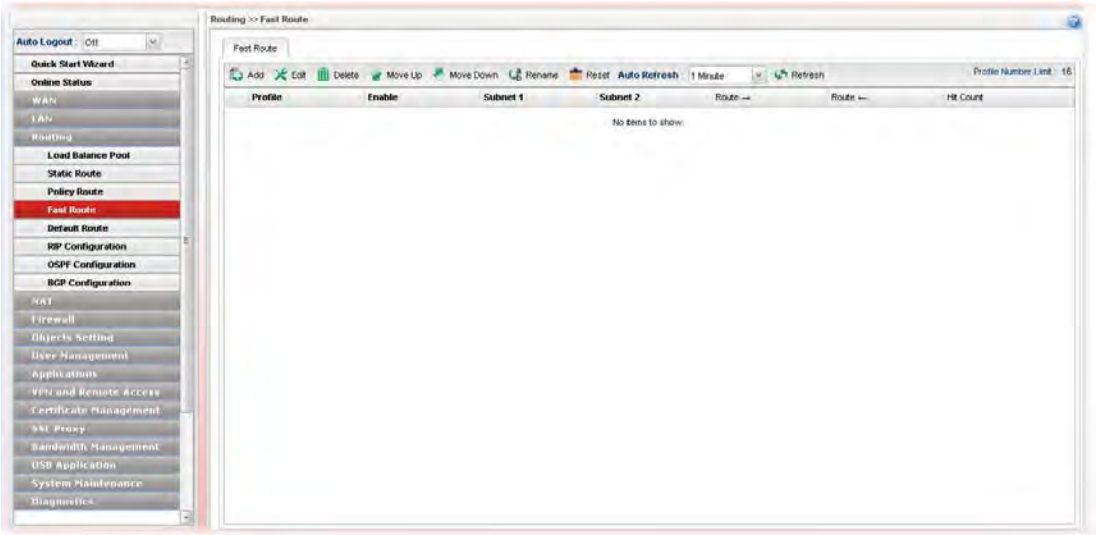


4. After finished the above settings, click **Apply** to save the configuration.



4.3.4 Fast Route

This page allows you to configure fast paths between “2” routing subnets by using hardware acceleration. The connection with fast route will ignore all firewall and portal examinations; however it will have the highest priority and the best performance, instead.



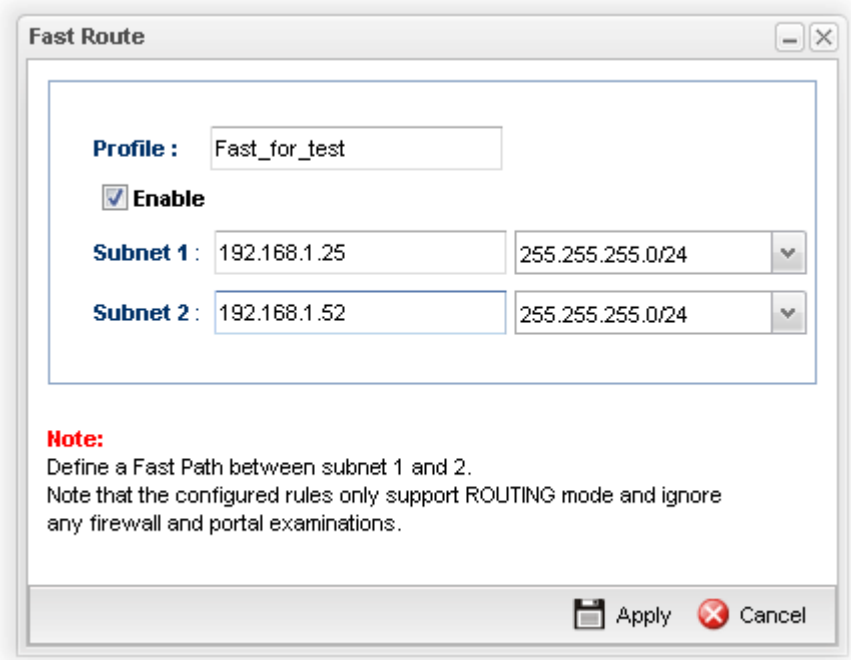
Each item will be explained as follows:

Item	Description
Add	Add a new route profile.
Edit	Modify the selected route profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected route profile.
Delete	Remove the selected route profile. To delete a route profile, simply select the one you want to delete and click the **Delete** button.
Move Up / Move Down	Move the selected profile up or down.
Rename	Allow to modify the selected profile name.
Reset	Reset the hit count.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Refresh	Renew current web page.
Profile	Display the name of the route profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Subnet 1/Subnet 2	Display the subnet mask defined in such profile.
Route →	Display the direction of the specified 2 routes -- output interface from Subnet 1 to Subnet 2.

Route ←	Display the direction of the specified 2 routes -- output interface from Subnet 2 to Subnet 1.
Hit Count	Display how many connections matched this rule (enabled).

How to add a new policy rule

1. Open **Routing>>Fast Route**.
2. Simply click the **Add** button. The following dialog will appear.



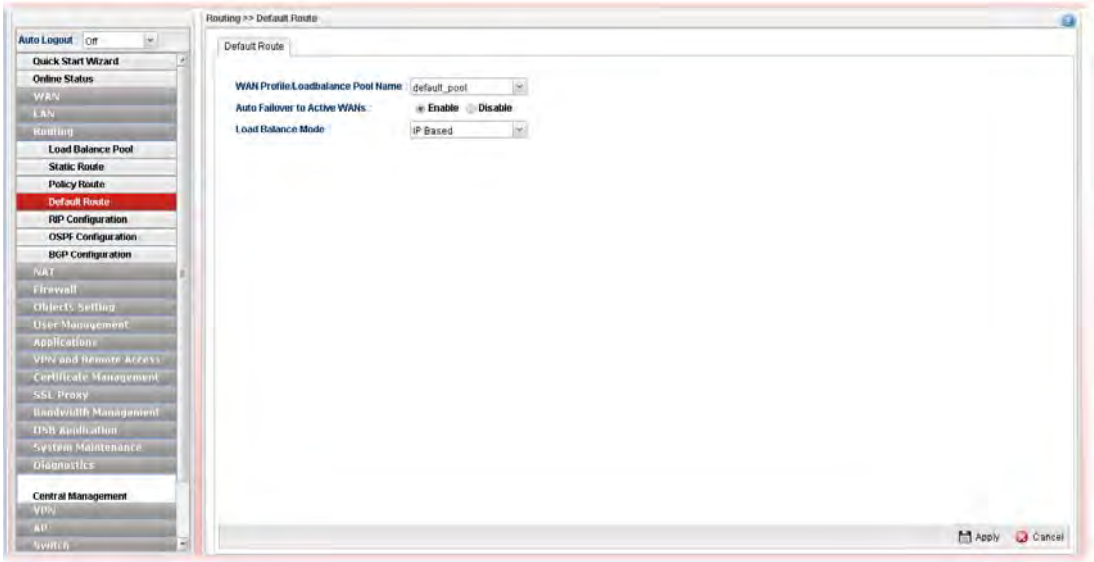
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the route profile.
Enable	Check this box to enable such profile.
Subnet 1 / 2	Enter the IP addresses for subnet 1 and subnet 2. Use the drop down list to specify subnet mask.
Apply	Click it to save the configuration.
Cancel	Click it to return to the factory setting.

3. Enter all of the settings and click **Apply**. The new rule profile will be added on the screen.

4.3.5 Default Route

This page allows you to assign a WAN profile or a Load Balance profile as the default route.



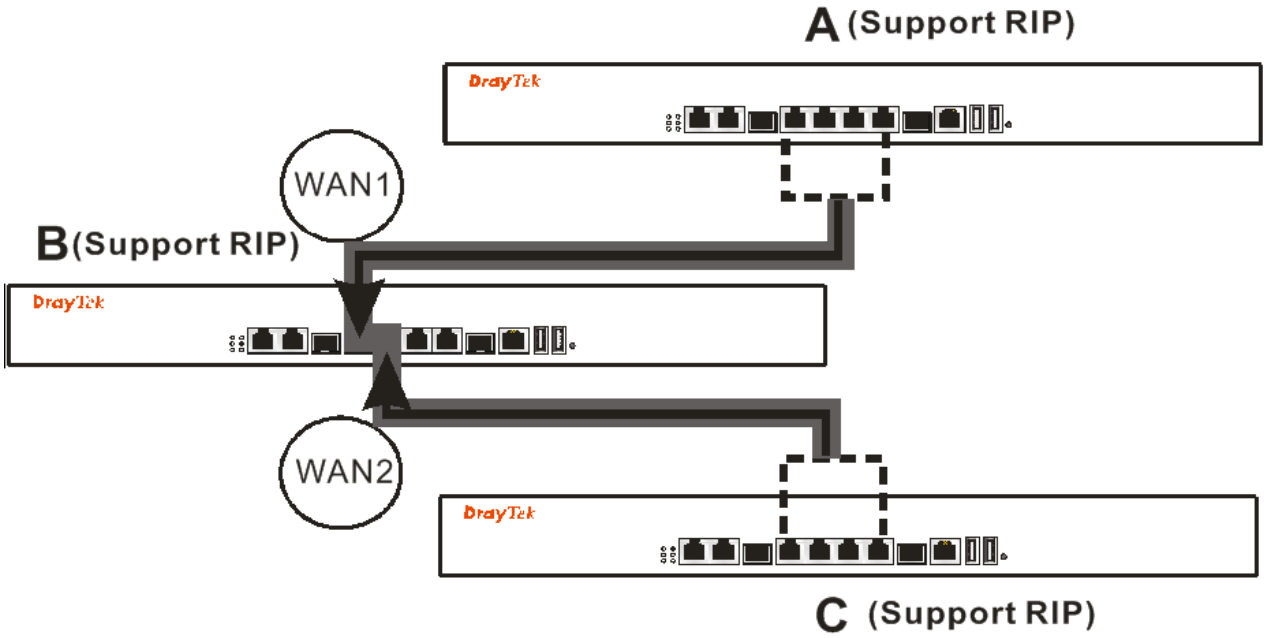
Available parameters are listed as follows:

Item	Description
WAN Profile /Load Balance Pool Name	Display the WAN profiles for user to choose as a default route. In which, wan1 to wan5 are factory default settings.
Auto Failover to Active WANs	**Enable** – Check it to let the network connection being established through any active WAN interface. **Disable** – Check it to disable the function.
Load Balance Mode	**IP Based** - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting. **Session Based**- All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP. ● **Exclude Service Type Object** – Use the drop down list to specify service type objects which can NOT perform session based routing, (performing IP based routing instead). If you have no strong demand about speed test result, keep default settings as IP based.
Apply	Click it to save the configuration.
Cancel	Discard current page modification.

4.3.6 RIP Configuration

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. The routing information packet will be sent out by web server or router periodically, and can be used to communicate with other routers. It will calculate the number of network nodes on the route to ensure there is no obstruction on the network routine. In addition, it will choose a correct route based on the method of Distance Vector Routing and use the Bellman-Ford algorithm to calculate the routing table.

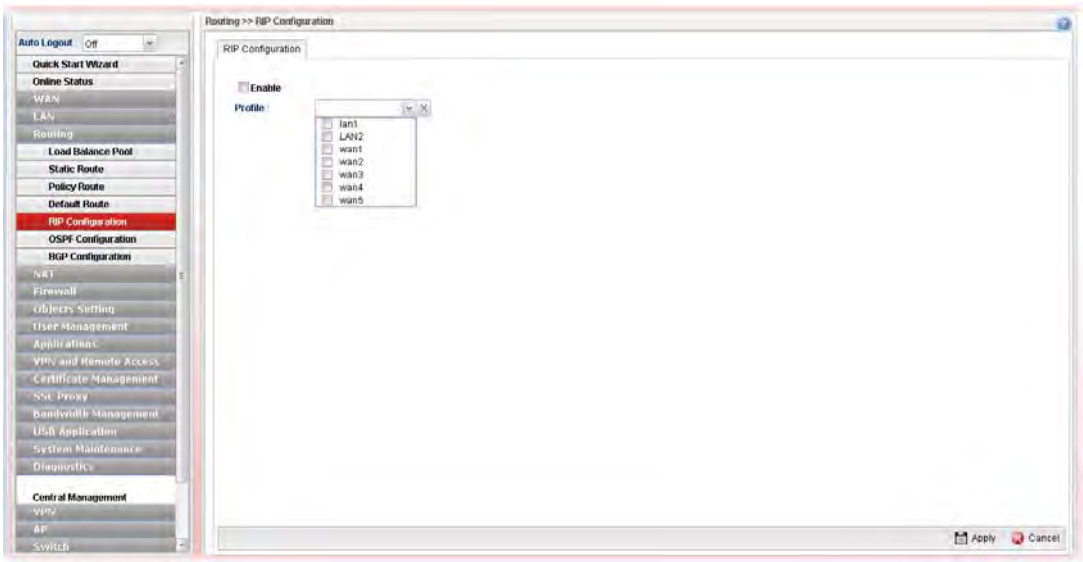
RIP can update the routing table automatically and find a route to send packet. See the following figure as an example:



Suppose A supports RIP on WAN1/WAN2/WAN3/WAN4, B supports RIP on WAN1 and WAN2, and C supports RIP on WAN1/WAN2/WAN3/WAN4.

B will tell A "if you want to send packets to C, please send it to me first", then A will create a routing rule to forward packet that destination is C to B.

In another direction, C will do the same thing.



Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable the Mirror function for the switch.
Profile	Choose the LAN/WAN profile(s).
Apply	Click it to save the settings.
Cancel	Click it to exit the dialog without saving anything.

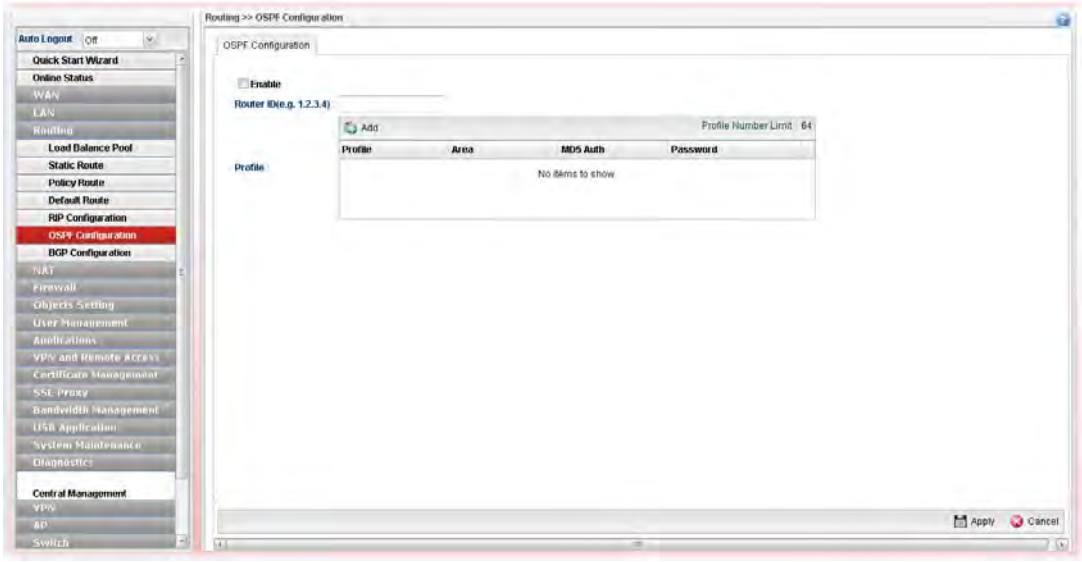
After finished the settings, click **Apply** to save them.

4.3.7 OSPF Configuration

OSPF (Open Shortest Path First) uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor 3900 supports up to OSPF version 2(only for IPv4).

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

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



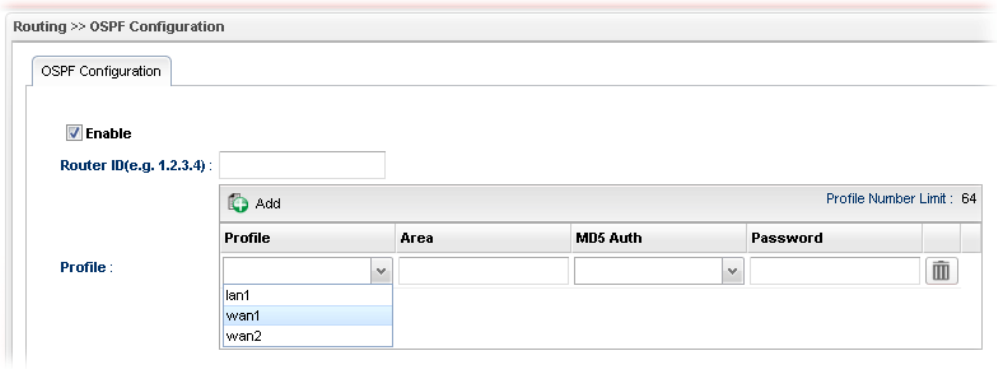
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable the Mirror function for the switch.
Router ID (e.g.1.2.3.4)	Specify the IP address of such Vigor router. Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically.
Profile	**Add**- Click it to create a new profile. **Profile -** Choose a LAN/WAN profile from the drop down list to apply for such configuration. **Area** – An AS will be divided into several areas. Each area must be assigned with a dedicated number. **MD5 Auth** – Enable/disable the MD5 authentication mechanism for such profile. **Password** – Type characters as the password for MD5 authentication. **Note**: For the detailed information of OSPF application, refer to section *"3.5 How to Configure OSPF?"*.
Apply	Click it to save the settings.
Cancel	Click it to discard the settings configured in this page.

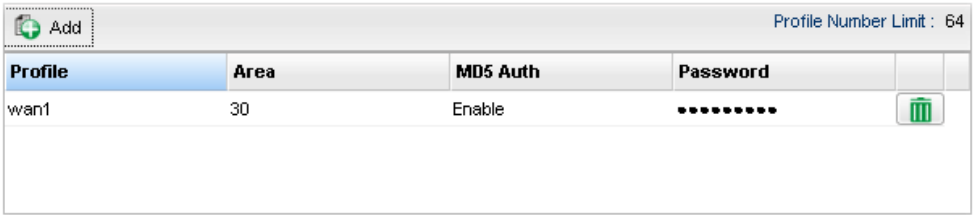
How to add a new profile

1. Open **Routing>>OSPF Configuration**.
2. Check **Enable**.
3. Enter the IP address as Router ID. Click **Add**.

4. Use the drop down list of LAN Profile to choose the one you need. And specify the value of Area (either 0.0.0.0 ~ 255.255.255.255 or 0 ~ 4294967295) for that profile. Enable/disable MD5 authentication and enter characters as the password.



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

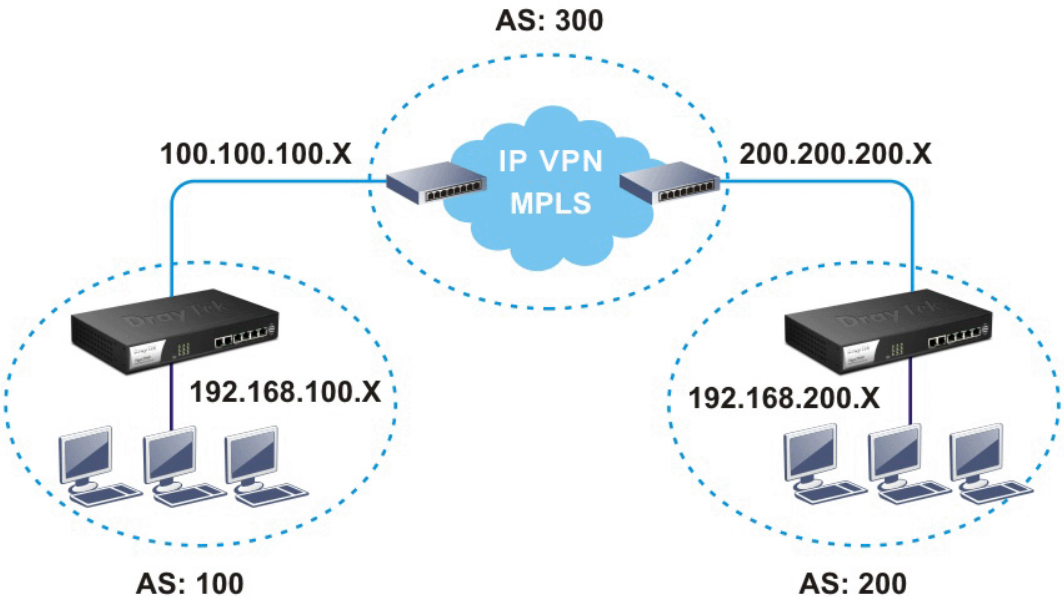


4.3.8 BGP Configuration

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

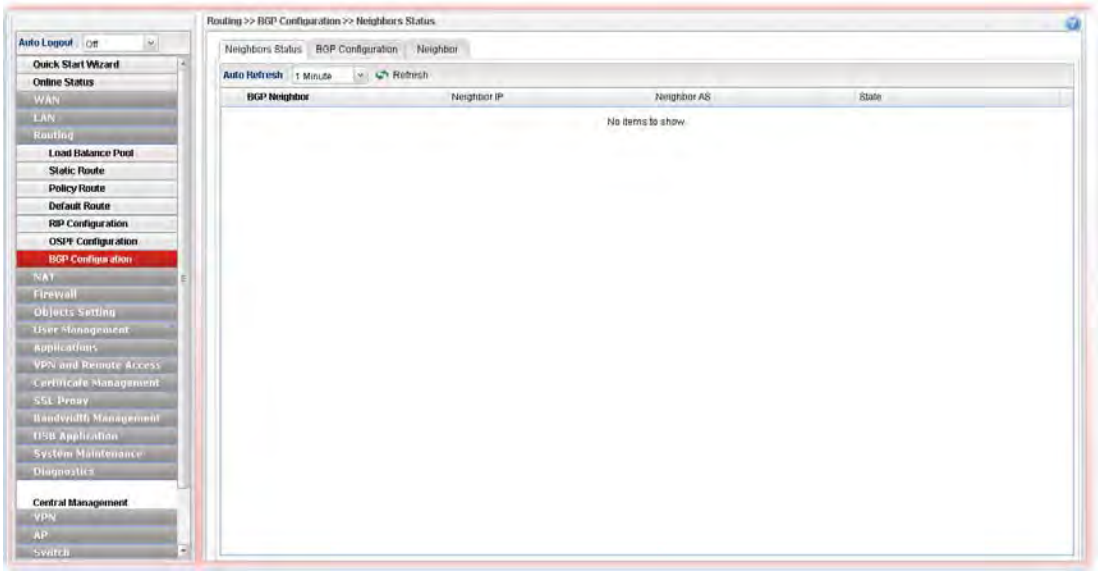
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the “neighbor” of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

AS, the abbreviation of Autonomous System, is a group interconnected with multiple IP addresses. AS numbers indicate the full paths that the route information will be taken. It can be operated by one or several ISPs and follows the routing policies made by ISP.

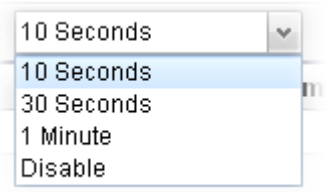


4.3.8.1 Neighbors Status

Such page displays current neighbors status in BGP routing environment.

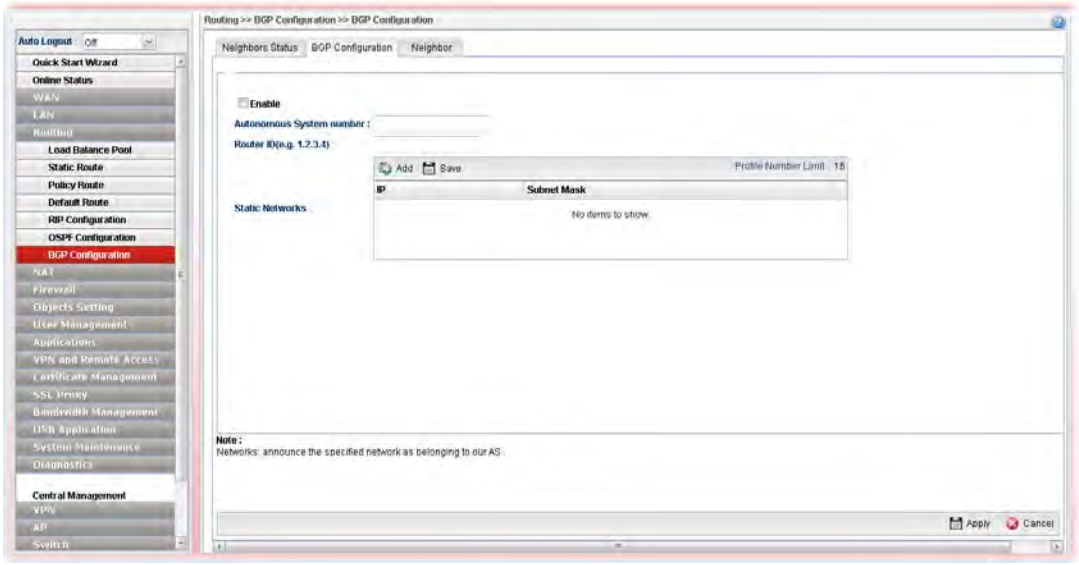


Available parameters are listed as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked. 
BGP Neighbor	Display the neighbor profile name configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
Neighbor IP	Display the neighbor IP address configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
Neighbor AS	Display the autonomous system number of the neighbor configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
State	Display the status of neighbor profile. If it is established successfully, “Established (time)” will be shown in this field.

4.3.8.2 BGP Configuration

This page is used to configure the general settings for the host which is ready for using BGP.



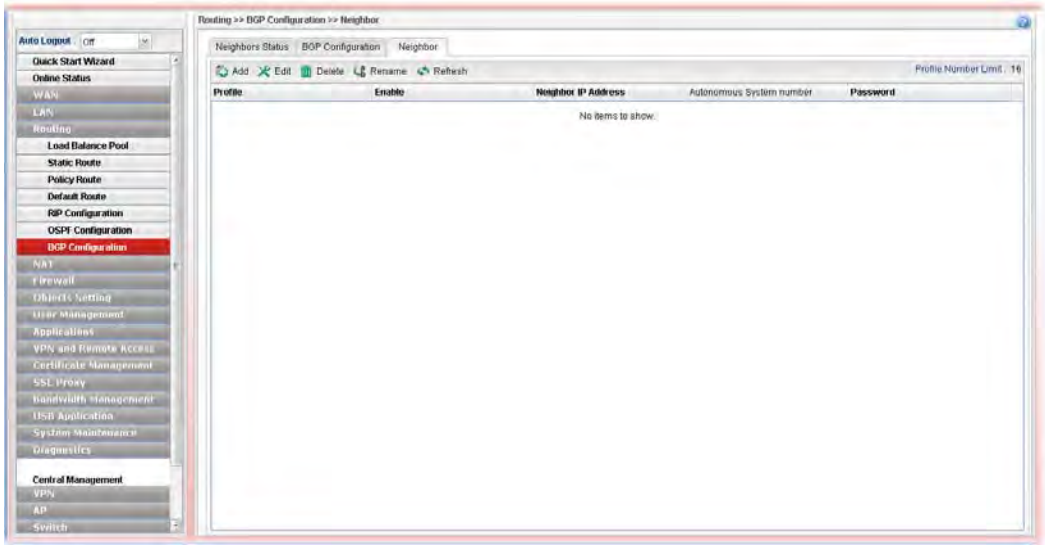
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable BGP function.
Autonomous System number	Type the autonomous system number for the host in BGP application.
Router ID (e.g.1.2.3.4)	Specify the IP address of such Vigor router. Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically.
Static Networks	Define the IP addresses (forming network range) which allow to be connected by other clients through static route. **Add** – Click it to add a specified IP address and subnet mask. **Save** – Click it to save the settings. **Profile Number Limit** - Display the total number of the profiles to be created. **IP** – Type the IP address. **Subnet Mask** – Display subnet mask for the IP address automatically.

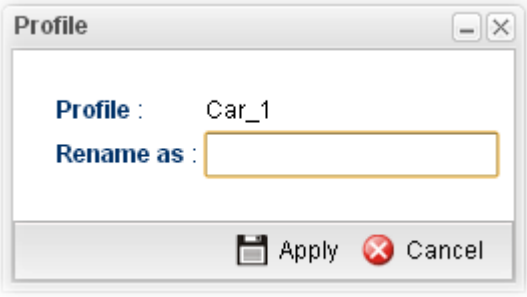
After finished the settings, click **Apply** to save the configuration.

4.3.8.3 Neighbor

This page is used to configure the IP address and AS number for the neighbor which will exchange BGP routing information with your Vigor router.



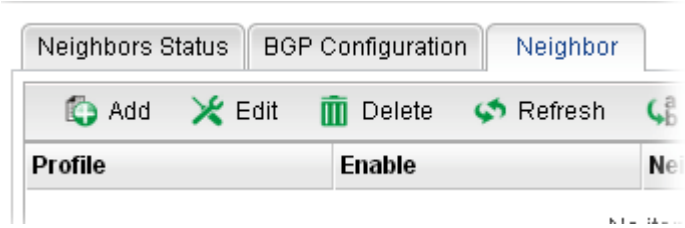
Available parameters are listed as follows:

Item	Description
Add	Add a new port redirect profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.  Before using such function, there is one profile existed at least.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.

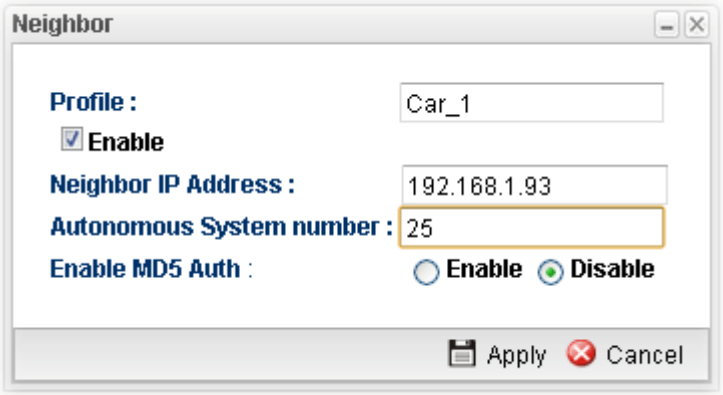
Neighbor IP Address	Display the IP address of the neighbor**.**
Autonomous System Number	Display the autonomous system number of the neighbor in BGP application.
Password	Display the password for MD5 authentication.

How to add a new BGP profile

1. Open **Routing>> BGP Configuration** and click the **Neighbor** tab.
2. Simply click the **Add** button.



3. The following dialog will appear.



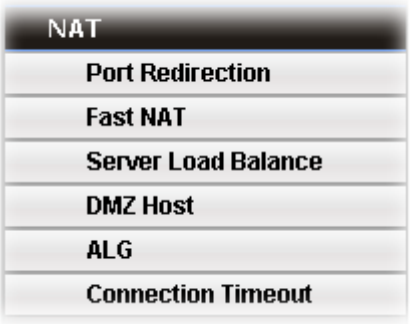
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Neighbor IP Address	Type the private IP used for this profile.
Autonomous System number	Type the autonomous system number for the neighbor in BGP application.
Enable MD5 Auth	Click **Enable** to enable MD5 authentication. **Password** – Type characters as the password for MD5 authentication.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.
5. A new profile has been added onto **Neighbor** table.

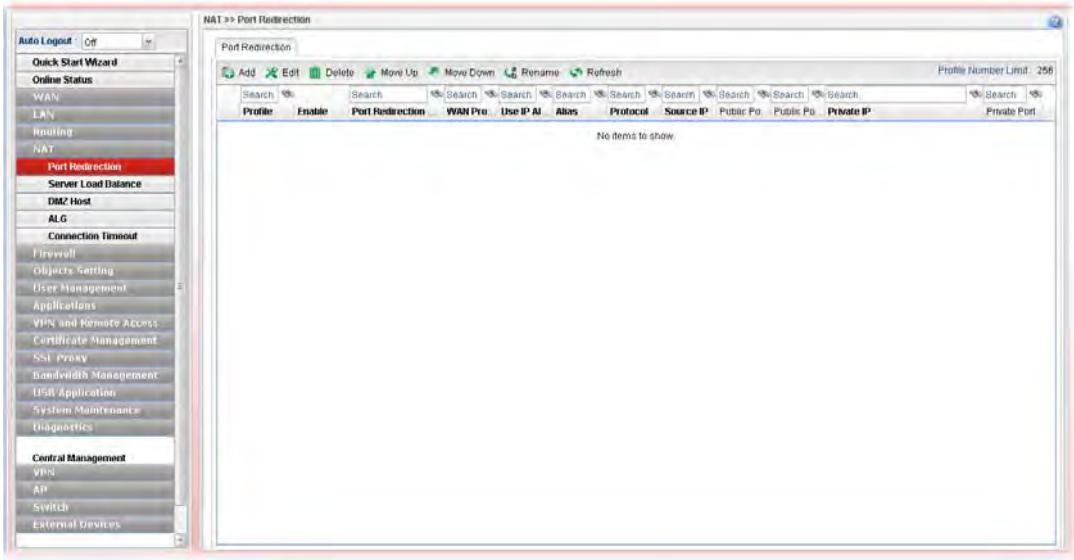
4.4 NAT

NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services. It allows the internal IP addresses of many computers on a LAN to be translated to one public address to save costs and resources of multiple public IP addresses. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. The Vigor 3900 Series is NAT-enabled by default and gets one globally routable IP addresses from the ISP by Static, PPPoE, or DHCP mechanism. The Vigor3900 Series assigns private network IP addresses according to RFC-1918 protocol and translates the private network addresses to a globally routable IP address so that local hosts can communicate with the router and access the Internet.

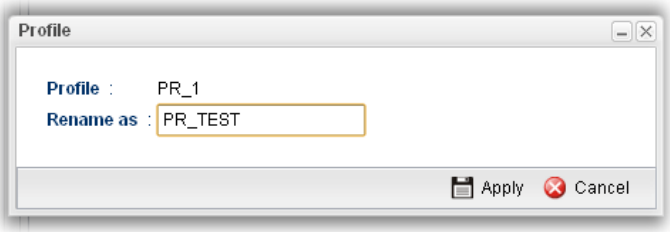


4.4.1 Port Redirection

Port Redirection means port forwarding. It may be used to expose internal servers to the public domain or open a specific port to internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW and etc. The internal FTP server is running on the local host addressed as 192.168.1.2. When other users send this type of request to your network through the Internet, the router will direct these requests to an appropriate host inside. A user can also translate the port to another port by configuration. For example, port number with 1024 can be transferred into IP address of 192.168.1.100 of LAN. The packet is forwarded to a specific local host if the port number matches that defined in the table.



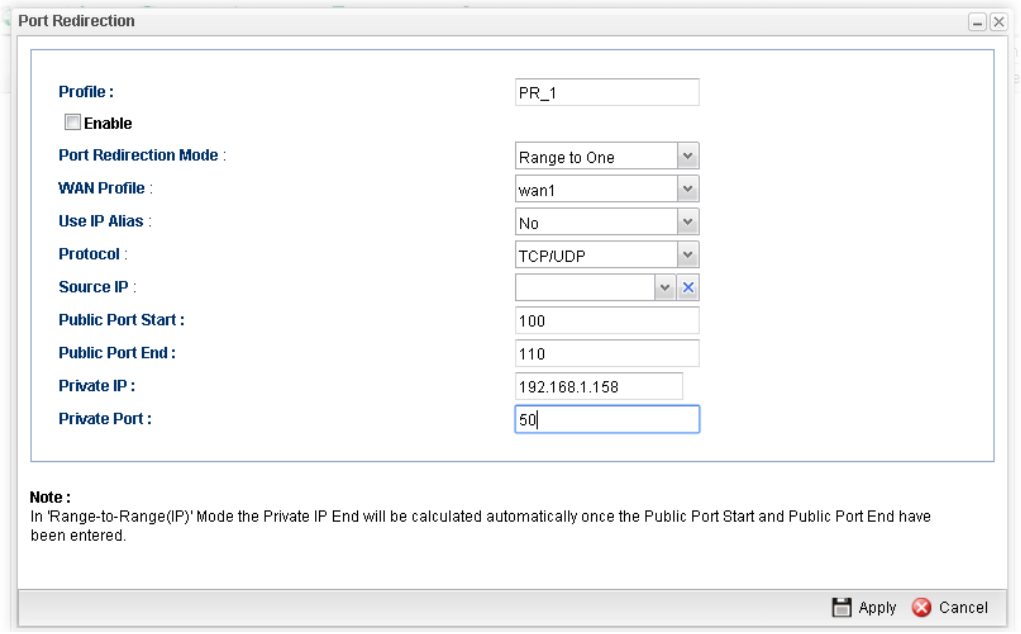
Each item will be explained as follows:

Item	Description
Add	Add a new port redirect profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name. 
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Port Redirection Mode	Display the direction for the port to be redirected.
WAN Profile	Display the WAN interface of this profile.
Use IP Alias	Display the type (no, Single_Alias, All) the IP Alias used.
Alias	Display the selected WAN IP address.
Protocol	Display the protocol used for the entry.
Source IP	Display the name of the source IP object.
Change Source IP	Display the changed source IP address.
Public Port Start	Display the starting number of the public port.
Public Port End	Display the ending number of the public port.
Private Port	Display the number of the private port.

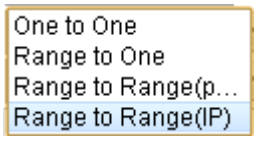
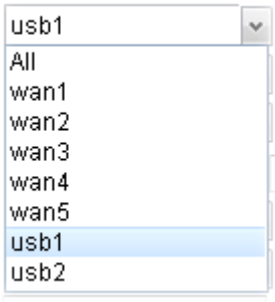
How to add a new Port Redirection profile

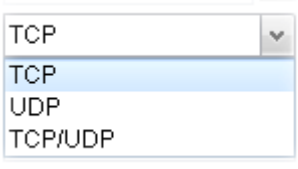
1. Open **NAT>> Port Redirection**.
2. Simply click the **Add** button.

3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Port Redirection Mode	Specify the direction for the port to be redirected. 
WAN Profile	Specify the WAN profile for such profile. 
Use IP Alias	When **All** is selected as **WAN Profile**, such feature is unavailable. Use the drop down list to select the type you want. **Single Alias** – You have to type one IP address used for IP Alias.

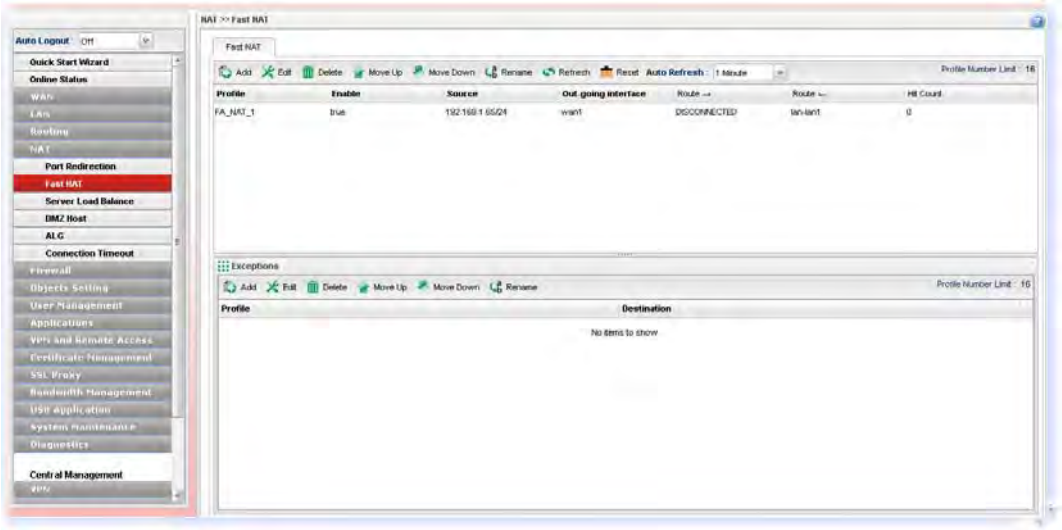
	All – All the IP address can be treated as IP Alias.
Alias	WAN IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
Protocol	Choose the protocol used for the entry. 
Source IP	Choose an IP object for port redirection.
Change Source IP	If the source IP object shall be changed due to some reason, enter a new IP address in this field.
Public Port Start/ Public Port End	It is available when **Range to One** or **Range to Range (port) or Range to Range (IP)** is selected as Port Redirection Mode. Type the starting/ending number of the public port. For Range-to-One, set both Start and End values with the same value.
Private IP	Specify the private IP address of the internal host providing the service. Simply type the private IP used for this entry.
Private IP Start / Private IP End	It is available when **Range to Range (IP)** is selected as Port Redirection Mode. Type the starting/ending IP address.
Private Port	Type a port number for such profile.
More Port	It is available when **One to One** is selected as Port Redirection Mode. Click **Add** to enter public port number and private port number.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new profile has been added onto **Port Redirection** table.

4.4.2 Fast NAT

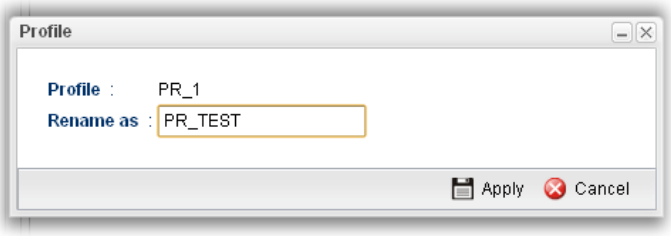
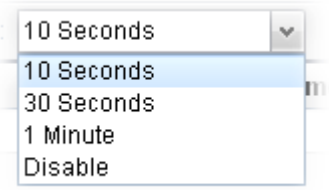
This page allows you to configure fast paths from chosen subnets to access Internet with hardware acceleration. The network connection with fast NAT will ignore all firewall and portal examinations; however it will have the higher priority and the better performance, instead.

> **Note**: **Fast Route** has the highest priority and the best performance, for network connection.



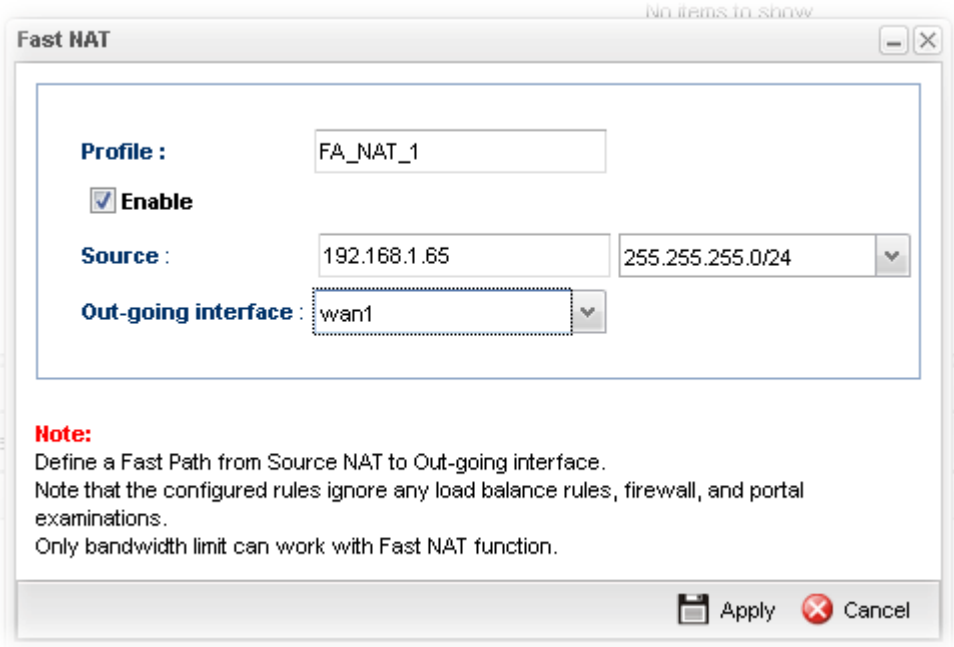
Each item will be explained as follows:

Item	Description
Add **(for Fast NAT/Exceptions)**	Add a new fast NAT / exceptions profile.
Edit **(for Fast NAT/Exceptions)**	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete **(for Fast NAT/Exceptions)**	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up / Move Down **(for Fast NAT/Exceptions)**	Change the order of selected profile by moving it up / down.
Rename **(for Fast NAT/Exceptions)**	Allow to modify the selected profile name.

	 Before using such function, there is one profile existed at least.
Refresh	Renew current web page.
Reset	Reset the hit count.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked. 
Profile	Display the name of the “Fast NAT / Exceptions” profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Source	Display the source IP address and subnet mask.
Out-going interface	Display the WAN interface for outgoing traffic.
Route →	Display the direction of the specified 2 routes -- output interface from Subnet 1 to Subnet 2.
Route←	Display the direction of the specified 2 routes -- output interface from Subnet 2 to Subnet 1.
Hit Count	Display how many connections matched this rule (enabled).
Exceptions	Destination subnets in this table do NOT perform Fast NAT. **Profile** – Display the name of exception profile. **Destination** – Display the IP address with subnet mask specified in the exception profile.

How to add a new Fast NAT profile

1. Open **NAT>> Fast NAT**.
2. Simply click the **Add** button.
3. The following dialog will appear.



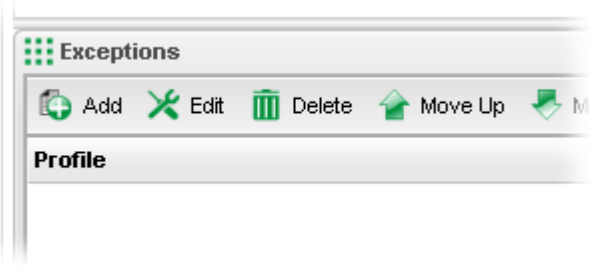
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Source	Enter the IP address as source IP. Use the drop down list to choose subnet mask.
Out-going interface	Specify an interface for outgoing traffic.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

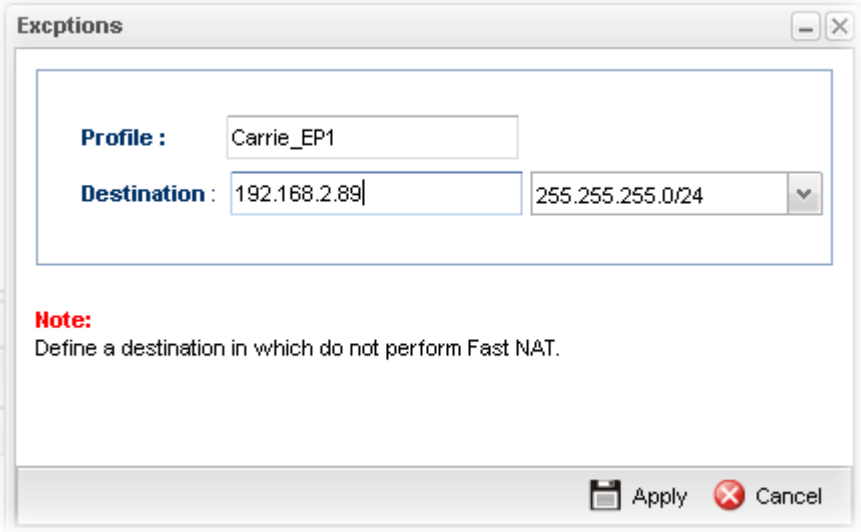
4. Enter all of the settings and click **Apply**.
5. A new profile has been added onto **Fast NAT** table.

How to add an Exception profile

1. Open **NAT>> Fast NAT**.
2. Simply click the **Add** button below **Exceptions**.



3. The following dialog will appear.



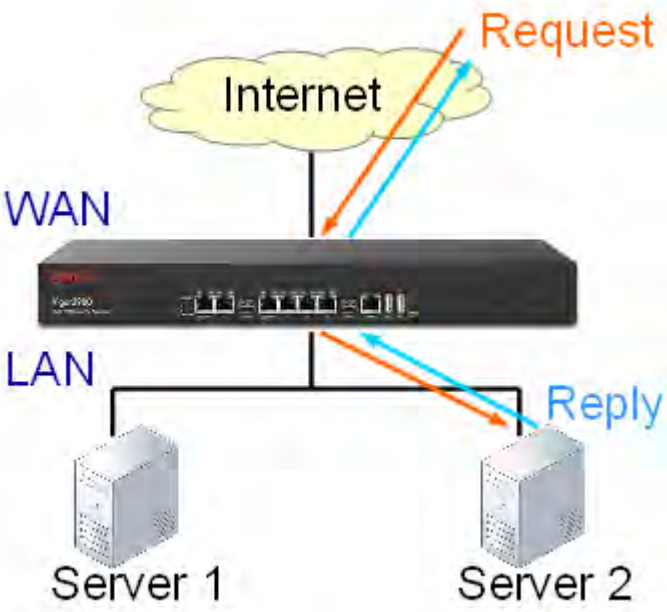
Available parameters are listed as follows:

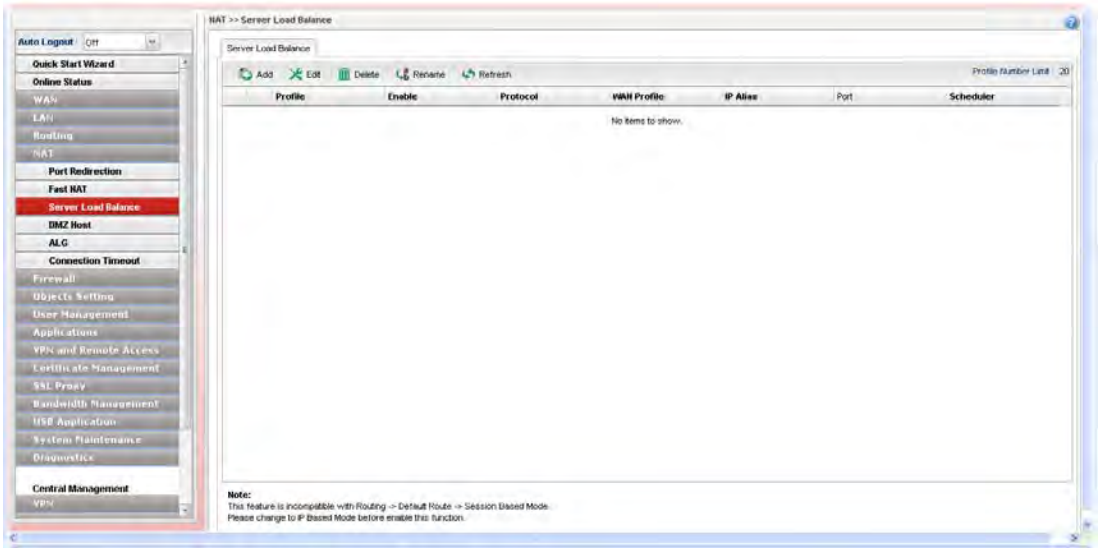
Item	Description
Profile	Type the name of the profile.
Destination	Enter the IP address as destination IP. Use the drop down list to choose subnet mask.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.
5. A new profile has been added onto **Exceptions** table.

4.4.3 Server Load Balance

When data traffic is large, Server Load Balance can distribute heavy traffic load among **different servers** equally to reach load balance. Thus, each server may keep average workload and the network will not become slowly or interrupted due to large traffic.





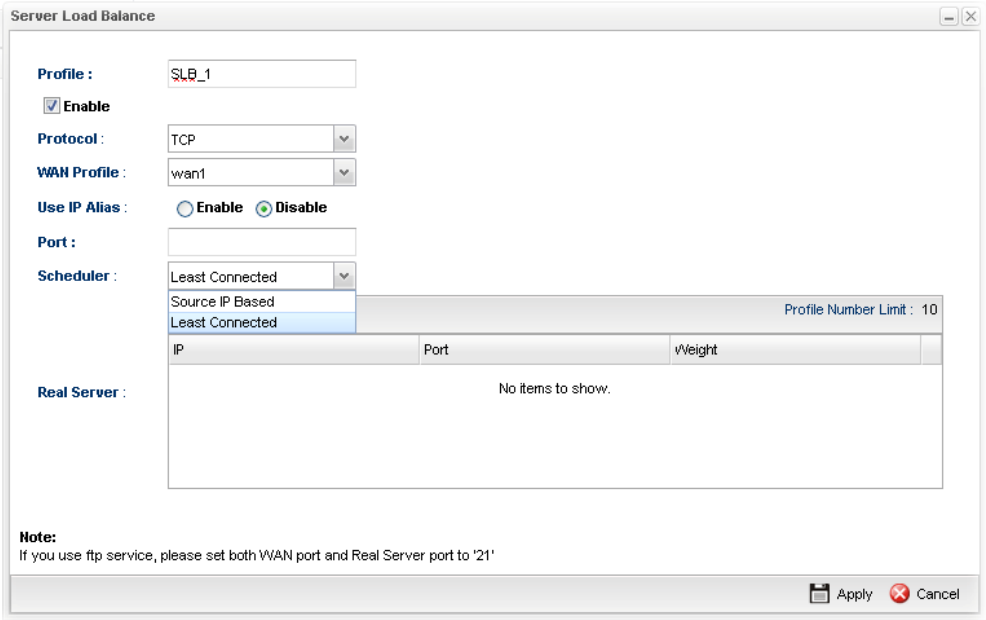
Each item will be explained as follows:

Item	Description
Add	Add a new server load balance profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.

	To delete a profile, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name. Before using such function, there is one profile existed at least.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Protocol	Display the protocol used for the entry.
WAN Profile	Display the WAN interface of this profile.
IP Alias	Display the selected WAN IP address.
Port	Display the port value used by WAN interface.
Scheduler	Display the algorithm (e.g., Source IP Based or Least Connected) of schedule.

How to add a new server load balance profile

1. Open **NAT>> Server Load Balance**.
2. Simply click the **Add** button.
3. The following dialog will appear.

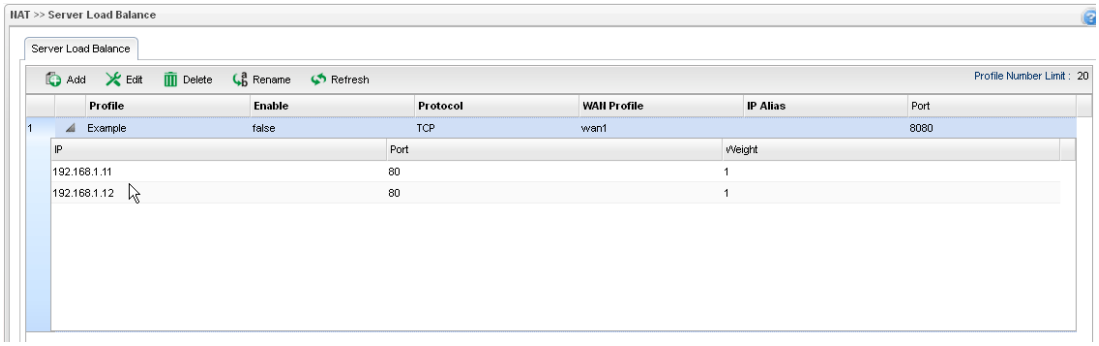


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Protocol	Choose the protocol (TCP or UDP) used for the entry.

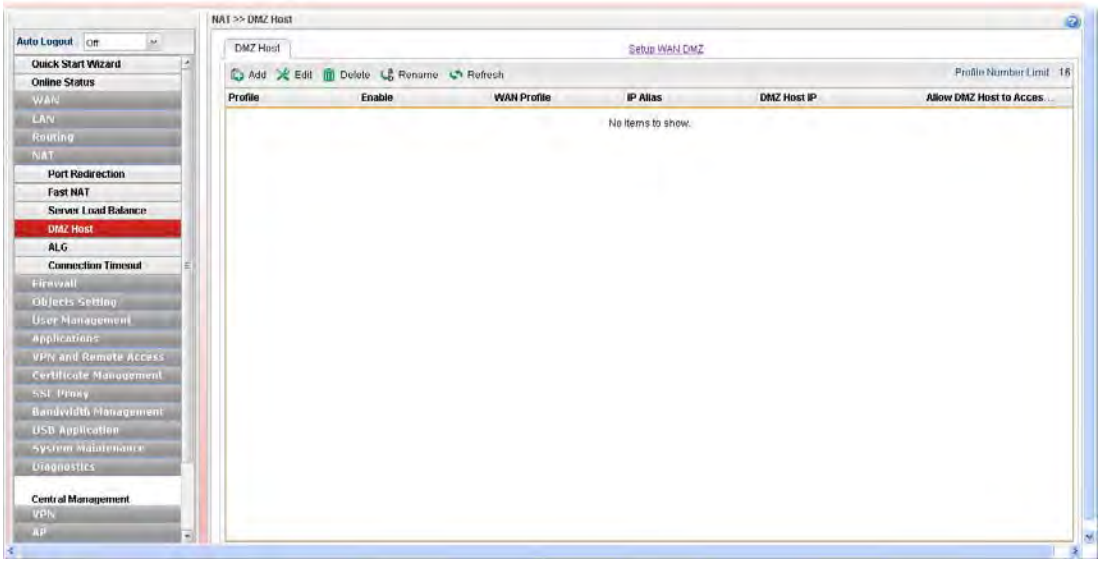
WAN Profile	Specify the WAN interface for such profile.
Use IP Alias	Click **Enable** to specify IP alias for such profile. **Alias** - WAN IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
Port	Type a public port number for WAN interface.
Scheduler	Any inquiry will be processed by the server according to the algorithm selected. **Source IP Based** – The inquiry will be assigned to the corresponding server according to the source IP address of the inquiry. **Least Connected** – The inquiry will be processed by the server with fewer sessions.
Real Server	Type the IP, port and weight values for the server(s) which is installed behind Vigor router. **IP –** Type the IP address (LAN subnet) of real server. **Port –** Type a private port number for real server. **Weight –** Greater value can be specified for a server with high process capability.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.
5. A new profile has been added onto server load balance table.



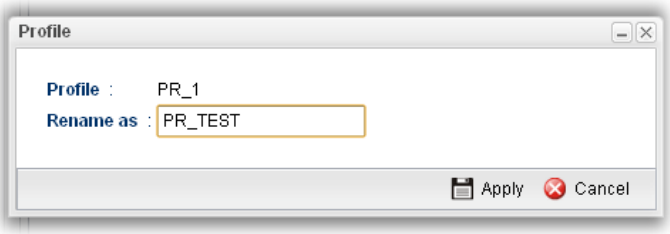
4.4.4 DMZ Host

In computer networks, a DMZ (De-Militarized Zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to company network. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well. In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initializes sessions for these requests on the public networks. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host. **The DMZ may typically also have the company's Web pages so these could be served to the outside world.** If an outside user penetrated the DMZ host's security, only the Web pages will be corrupted but other company information would not be exposed.



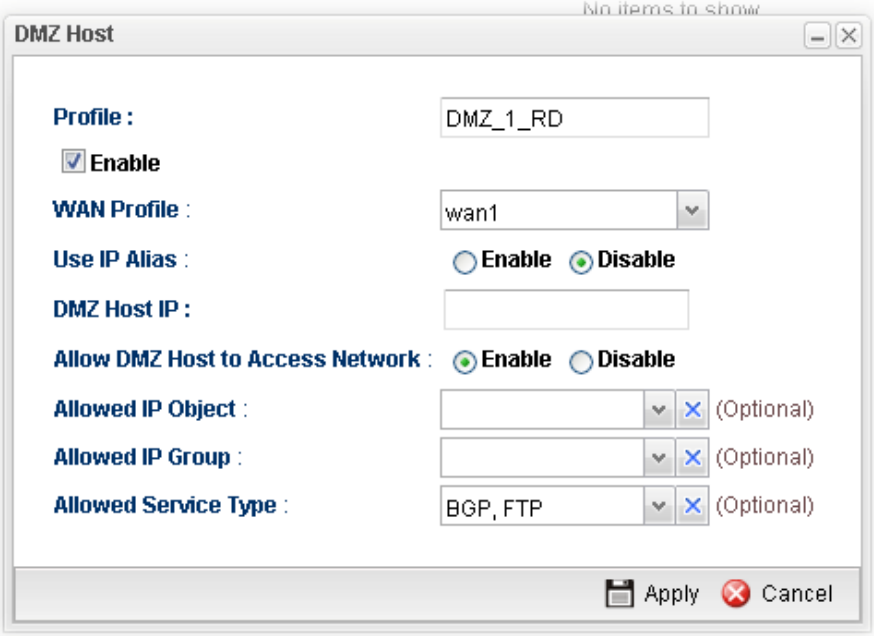
Each item will be explained as follows:

Item	Description
Add	Add a new DMZ host profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.

	
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN profile that such DMZ host profile will be applied to.
IP Alias	Display the selected WAN IP address if Use IP Alias is enabled.
DMZ Host IP	Display the IP address of the DMZ host.
Allow DMZ Host to Access Network	Display if such function is enabled or disabled.

How to add a new DMZ Host profile

1. Open **NAT>> DMZ Host**.
2. Simply click the **Add** button.
3. The following dialog will appear.

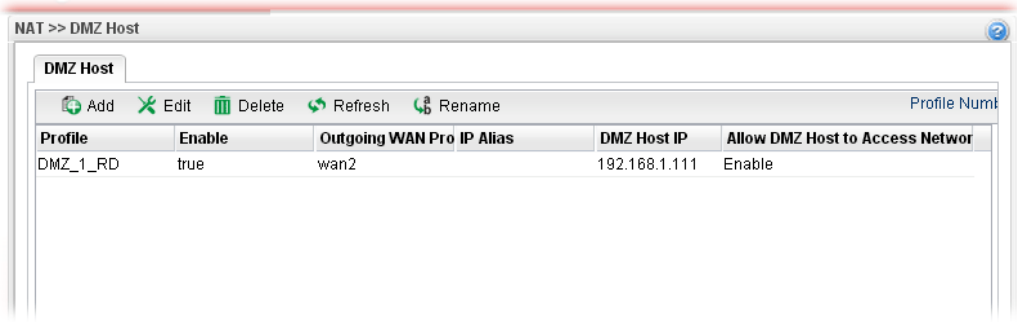


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.

Enable	Check the box to enable the DMZ Host profile.
WAN Profile	Choose a WAN profile for such entry.
Use IP Alias	Click **Enable** to invoke IP Alias function.
IP Alias	IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
DMZ Host IP	Type the IP address of the DMZ host.
Allow DMZ Host to Access Network	Click Enable to make DMZ host accessing network.
Allowed IP Object	This is an optional setting. Use the drop down list to choose the IP object profile(s) to apply to such profile.
Allowed IP Group	This is an optional setting. Use the drop down list to choose the IP group profile(s) to apply to such profile.
Allowed Service Type	This is an optional setting. Use the drop down list to choose the type(s) to apply to such profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

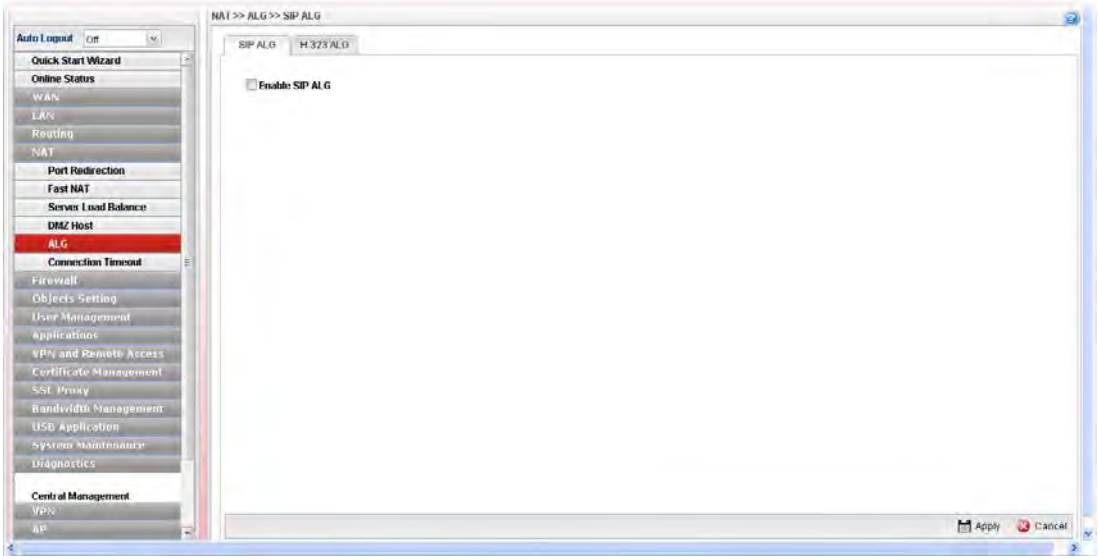
4. Enter all the settings and click **Apply**.
5. A new profile has been added onto **DMZ Host** table.



4.4.5 ALG

4.4.5.1 SIP ALG

SIP ALG means **Session Initiation Protocol, Application Layer Gateway**. This option allows Vigor router to make SIP message and RTP packets of voice being transmitting and receiving correctly via NAT.



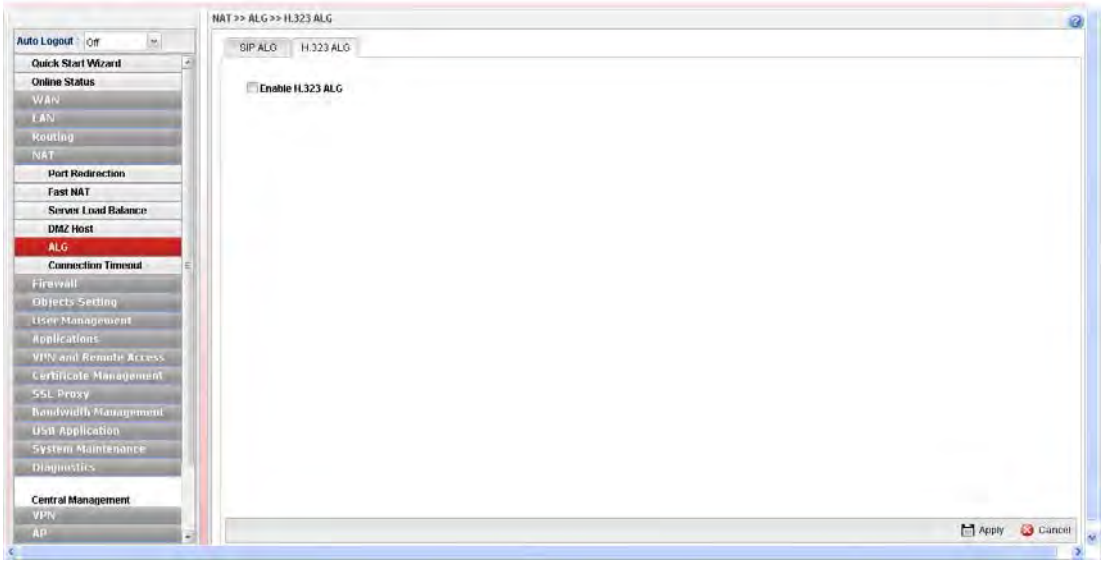
Available parameters are listed as follows:

Item	Description
Enable SIP ALG	Check the box to enable the Mirror function for the switch.
Refresh	Renew current web page.
Apply	Click it to save the settings.

Click **Apply** to save the settings.

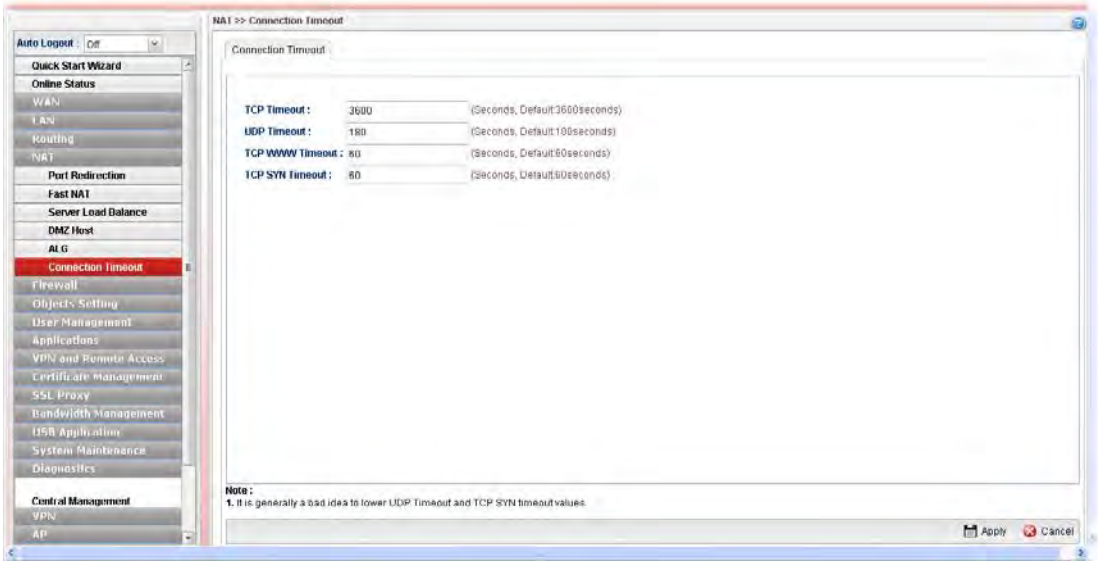
4.4.5.2 H.323 ALG

The H.323 ALG allows incoming and outgoing VoIP calls passing through NAT. If required, check the box and click **Apply** to save the settings.



4.4.6 Connection Timeout

This feature is used to configure timeout setting for sessions established by TCP/UDP. When a session is idle for a period of time, the connection will be terminated after reaching the time limit configured in such page.



Available parameters are listed as follows:

Item	Description
TCP Timeout	Set a time limit for sessions established by TCP (except Port 80 and Port 443).
UDP Timeout	Set a time limit for sessions established by UDP.
TCP WWW Timeout	Set a time limit for sessions established by TCP Port 80 and Port 443.

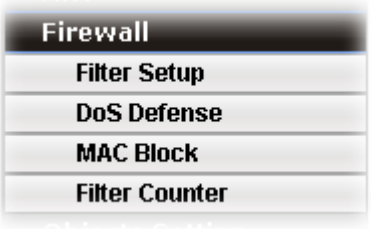
TCP SYN Timeout	Set a time limit for sessions established by TCP SYN.
Apply	Click it to save the settings.
Cancel	Click it to discard the settings configured in this page.

Click **Apply** to save the settings.

4.5 Firewall

The firewall controls the allowance and denial of packets through the router. The **Firewall Setup** in the Vigor3900 Series mainly consists of packet filtering, Denial of Service (DoS) and URL (Universal Resource Locator) content filtering facilities. These firewall filters help to protect your local network against attack from outsiders. A firewall also provides a way of restricting users on the local network from accessing inappropriate Internet content and can filter out specific packets, which may trigger unexpected outgoing connection such as a Trojan.

The following sections will explain how to configure the **Firewall**. Users can select **IP Filter**, **DoS Defense, MAC Block** and **Port Block** options from **Firewall** menu. The **DoS Defense** facility can detect and mitigate the DoS attacks.

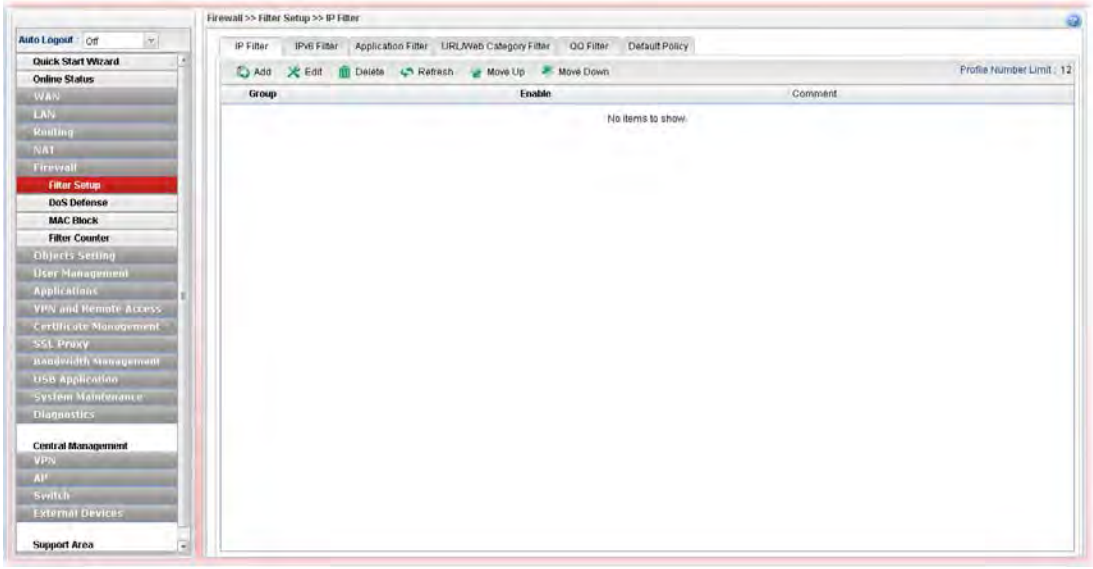


4.5.1 Filter Setup

Vigor firewall will filter the packets based on the settings, including IP Filter, Application Filter, URL/Web Filter and QQ Filter configured under **Firewall>>Filter Setup**. These filters will group certain objects (e.g., IP Object, Service Object, Keyword Object, File Extension Object, IM Object, P2P Object, P2P Object, Protocol Object, Web Category Object, QQ Object, QQ Group, Time Object, and etc.) and form a powerful firewall to protect your computer.

4.5.1.1 IP Filter

This page allows you to create new filter, group, and profile for your request.



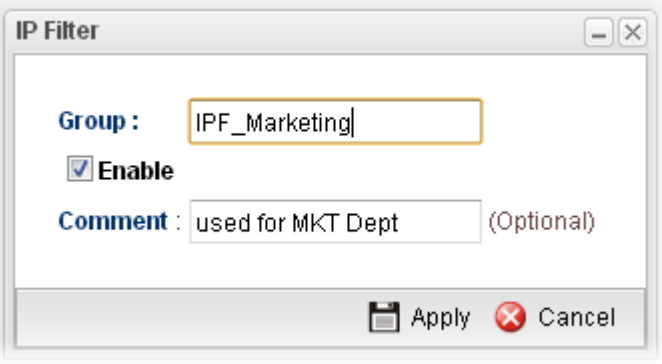
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for IP filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Profile Number Limit	Display the total number of the profiles to be created.
Group	Display the name of the **IP filter group** profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Comment	Display the description for such profile.

How to create an IP Filter group

To build an IP group containing IP filter rules, please follow the steps:

1. Open **Firewall>>Filter Setup** and click the **IP Filter** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.

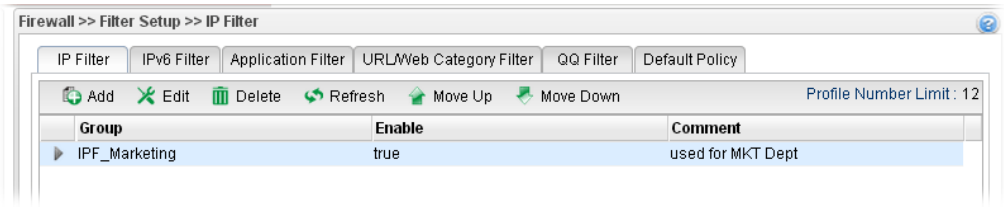


Available parameters are listed as follows:

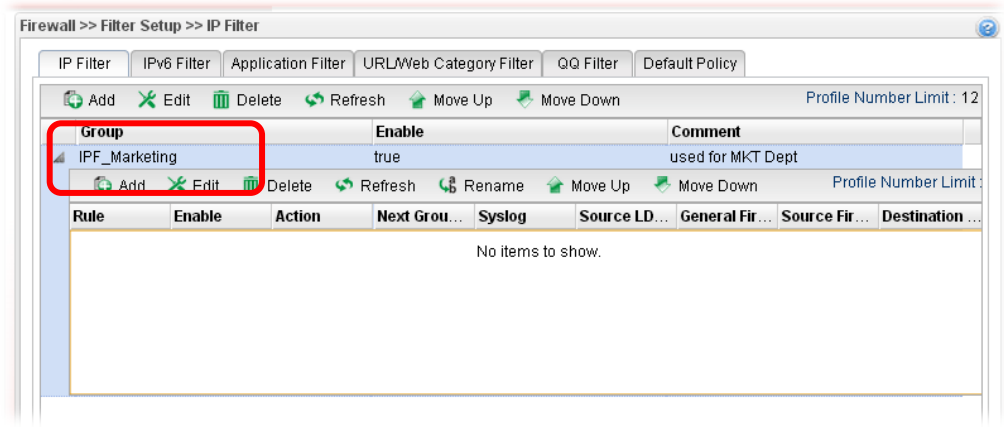
Item	Description
Group	Type the name of the IP filter group.
Enable	Check the box to enable this profile.
Comment	Give a brief description for the profile.

4. Enter all the settings and click **Apply**.

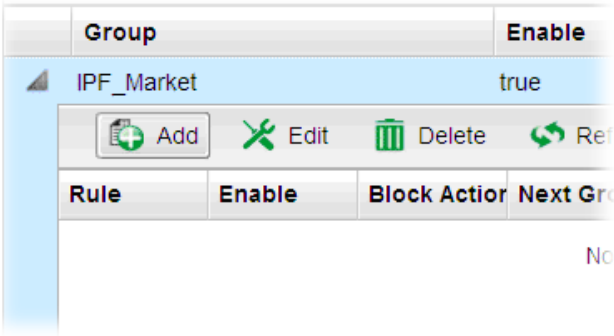
5. A new filter group has been added.



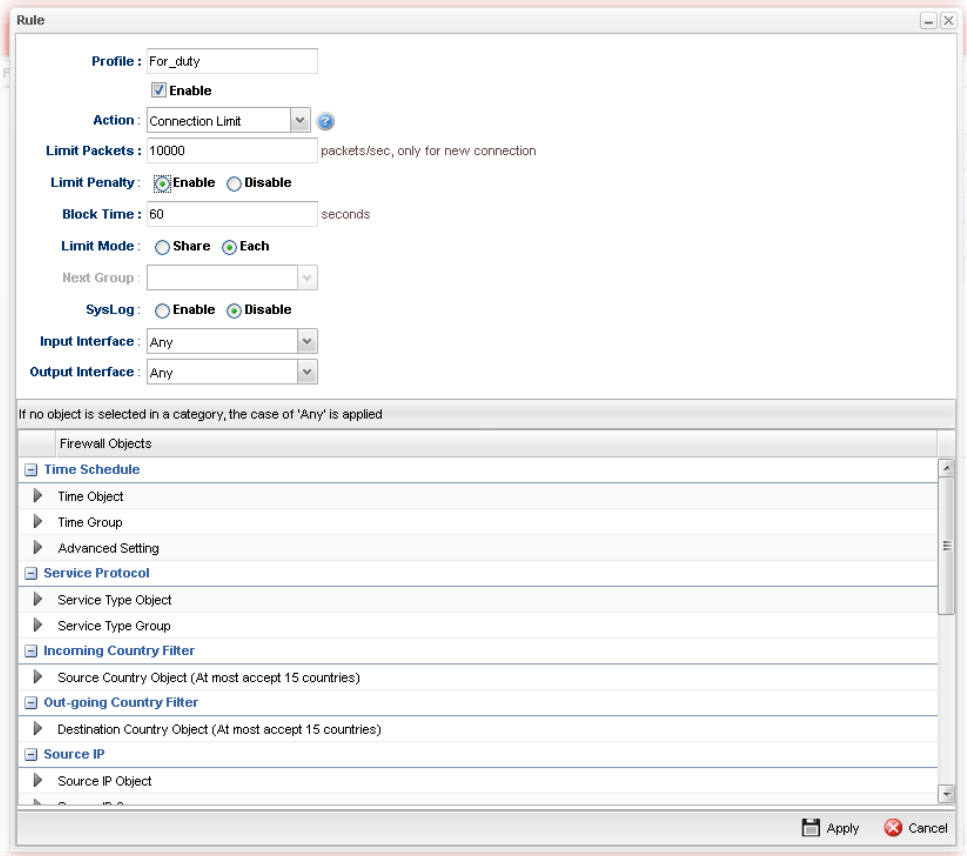
6. You can create filter rule by clicking ▶ on the left side of the selected IP filter group profile. A setting page will appear for you to add new IP filter rule profile.



7. Move your mouse to click **Add**.

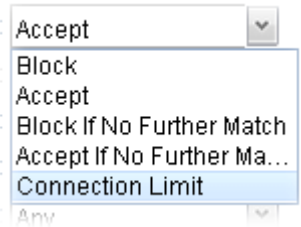
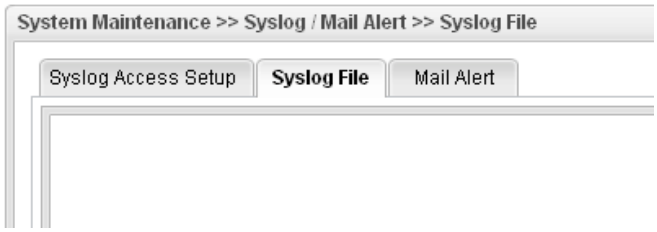


8. The following page for configuration will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Block Action	The action to be taken when packets match the rule. **Block -** Packets matching the rule will be dropped immediately **Accept**- Packets matching the rule will be passed immediately. **Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Accept If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through. **Connection Limit** –Limiting the number of packets for new connection can avoid attack driven by unknown person. For each connection session, packets number smaller than the Limit Packets setting can be passed immediately; however, packets number greater that the Limit Packets setting will be dropped. That is, packets to be passed or dropped are determined by connection rate (new session) at that time.

	
Limit Packets	When you choose **Connection Limit** as **Action,** you have to configure limit packets number to determine how many packets per second will be passed through.
Limit Penalty	**Enable** – Click it to enable the function of limit penalty. When the total packet number from source IP exceeds the value defined in Limit Packets, all packets of source IP will be blocked temporarily till the time is passed. ● **Block Time** – Enter the values (unit is second). **Disable** – In default, such function is disabled. Packets from source IP will not be blocked.
Limit Mode	When you choose **Connection Limit** as **Action,** you have to choose Share or Each in addition to the number of packets limits. **Share** – It means the total IP addresses in a segment will be limited with certain packets number per second. **Each** –It means each IP will be limited with certain packets number per second.
Next Group	When you choose **Block If No Further Match** or **Accept If No Further Match** as **Action**, you have to specify next IP filter group for further matching.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance >> Syslog/Mail Alert** >> **Syslog File**. 
Input Interface	Choose one of the LAN or WAN profiles as data receiving interface.
Output Interface	Choose one of the LAN or WAN profiles as data transmitting interface.
Time Schedule	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click to create another new time object profile. **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another

	new time group profile. **Advanced Setting –** Check the box of **Clear sessions when schedule ON** to clear the sessions when the above schedule profiles are applied.
Service Protocol	**Service Type Object** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type object profiles from the drop down list. The selected profile will be treated as service type. You can click to create another new service type object profile. **Service Type Group** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type group profiles from the drop down list. The selected profile will be treated as service type. You can click to create another new service type group profile.
Incoming Country Filter	**Source Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an incoming country filter. You can click to create another new filter profile.
Out-going Country Filter	**Destination Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an outgoing country filter. You can click to create another new filter profile.
Source IP	**Source IP Object / Source IP Group / Source User Profile / Source User Group / Source LDAP Group / Source Guest Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more object profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new object profile, or click the edit icon to modify the existed profile.
Destination IP	**Destination IP Object / Destination IP Group / Destination DNS Object / Destination User Profile / Destination User Group / Destination LDAP Group / Destination Guest Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more object profiles from the drop down list. The selected profile will be treated as destination target. You can click to create another new object profile, or click the edit icon to modify the existed profile.
Incoming MAC Filter	**Source MAC Object -** Click the triangle icon ▶ to display the profile selection box. Choose one or more MAC object profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new MAC object profile.

Out-going MAC Filter	**Destination MAC Object -** Click the triangle icon ▶ to display the profile selection box. Choose one or more MAC object profiles from the drop down list. The selected profile will be treated as destination target. You can click to create another new MAC object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

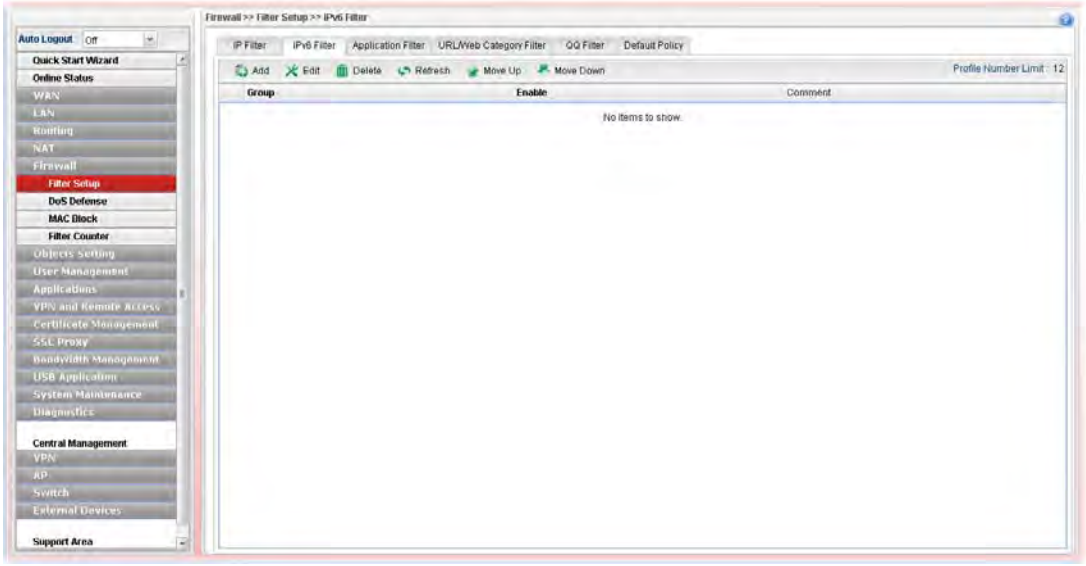
9. Enter all the settings and click **Apply**.

10. A new IP filter rule has been added under the IP Filter Group (named IPF_Market in this case).

Note: You can create multiple IP filter rules under a certain IP Filter group.

4.5.1.2 IPv6 Filter

This page allows you to create new IPv6 filter group for your request.



Each item will be explained as follows:

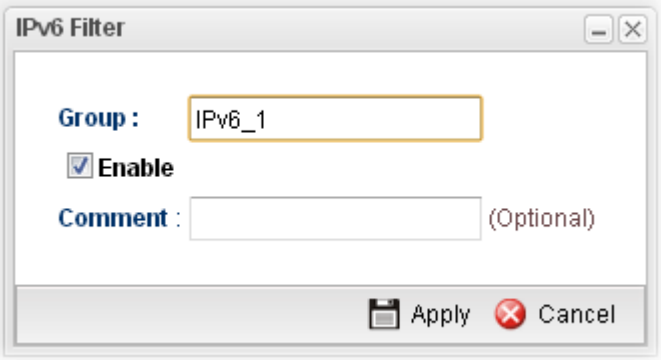
Item	Description
Add	Add a new group profile for IPv6 filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Profile Number Limit	Display the total number of the profiles to be created.
Group	Display the name of the **IP filter group** profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Comment	Display the description for such profile.

How to create an IPv6 Filter group

To build an IP group containing IP filter rules, please follow the steps:

1. Open **Firewall>>Filter Setup** and click the **IPv6 Filter** tab.
2. Simply click the **Add** button.

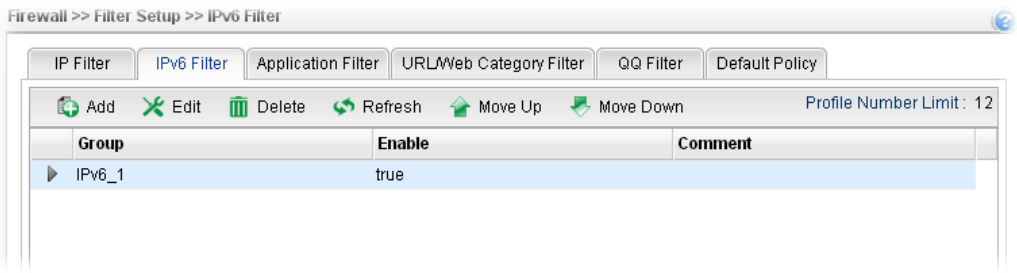
3. The following dialog will appear.



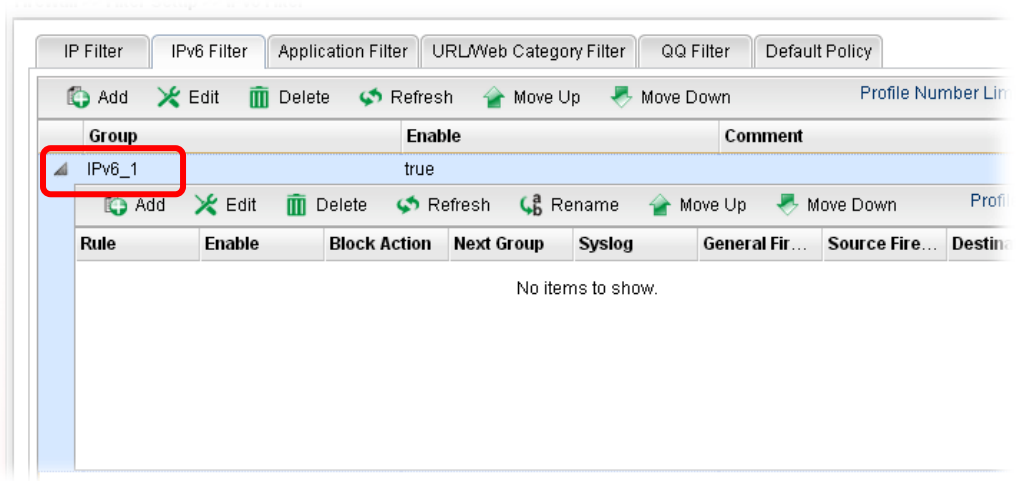
Available parameters are listed as follows:

Item	Description
Group	Type the name of the IP filter group.
Enable	Check the box to enable this profile.
Comment	Give a brief description for the profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

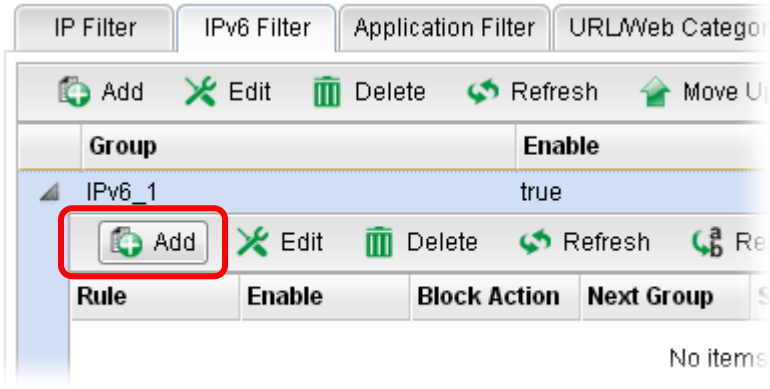
4. Enter all of the settings and click **Apply**.
5. A new filter group has been added.



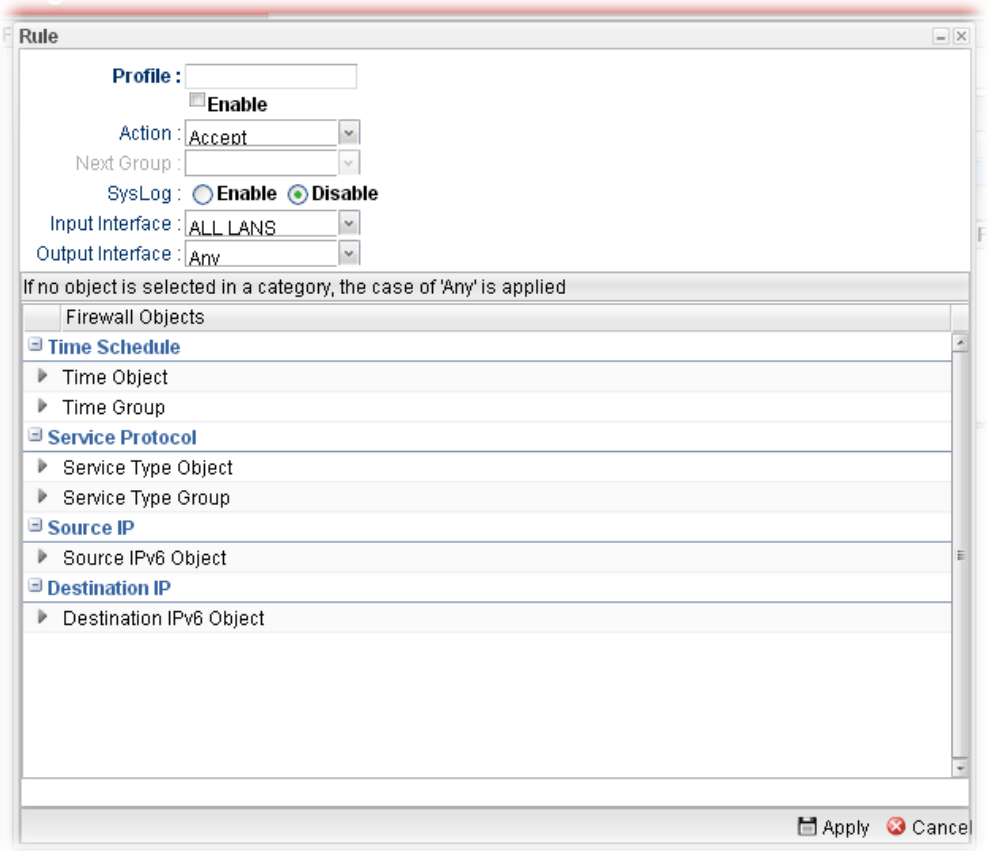
6. You can create filter rule by clicking on the left side of the selected IP filter group profile. A setting page will appear for you to add new IP filter rule profile.



7. Move your mouse to click **Add**.

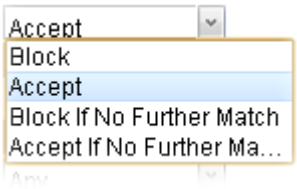
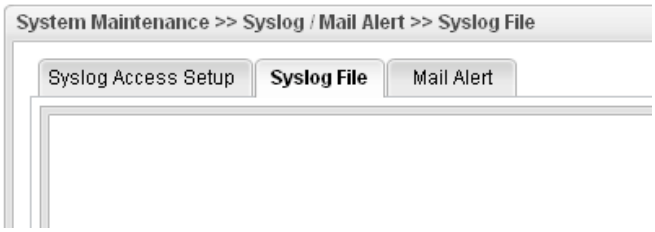


8. The following page for configuration will appear.



Available parameters are listed as follows:

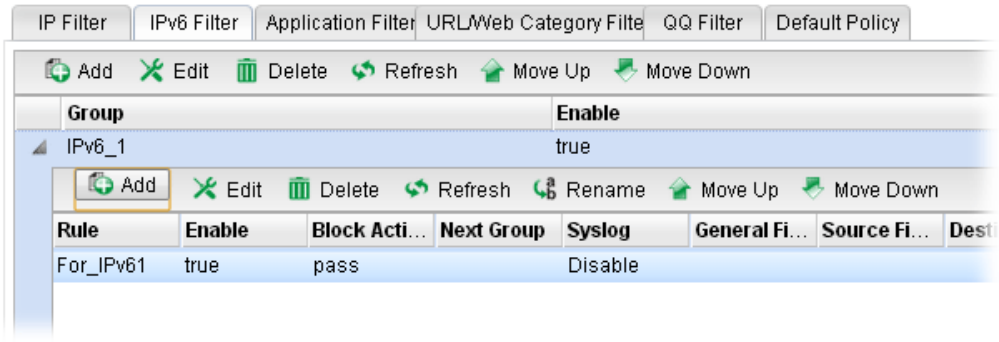
Item	Description
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Action	The action to be taken when packets match the rule. **Block** - Packets matching the rule will be dropped immediately **Accept**- Packets matching the rule will be passed immediately.

	Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. **Accept If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through. 
Next Group	When you choose **Block If No Further Match** or **Accept If No Further Match** as **Block Action**, you have to specify next IP filter group for further matching.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance >> Syslog/Mail Alert** >> **Syslog File**. 
Input Interface	Choose one of the LAN or WAN profiles as data receiving interface.
Output Interface	Choose one of the LAN or WAN profiles as data transmitting interface.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click to create another new time object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another new time group profile.
Service Protocol	**Service Type Object** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type object profiles from the drop down list. The selected profile will be treated as service type. You can click to create another new service type object profile. **Service Type Group** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type group profiles from the drop down list. The selected profile will be treated as service type. You can click to create another new service type group profile.
Source IP	**Source IPv6 Object -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source target. You can click to create another

	new IP object profile.
Destination IP	**Destination IPv6 Object-** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected profile will be treated as destination target. You can click to create another new IP object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

9. Enter all of the settings and click **Apply**.

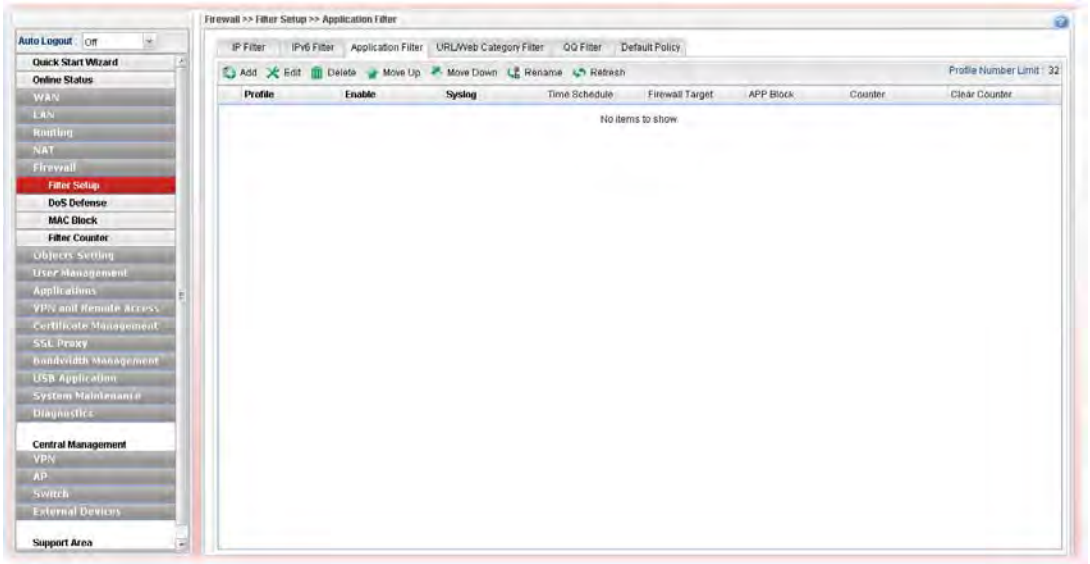
10. A new IPv6 filter rule has been added under the IPv6 Filter Group (named For_IPv61 in this case).



Note: You can create multiple IPv6 filter rules under a certain IP Filter group.

4.5.1.3 Application Filter

Application Filter can integrate several application objects within one profile for restricting the usage of application. For example, it can block people defined in IP object profile not using IM application, not using P2P for file sharing, and not downloading files via certain protocol.



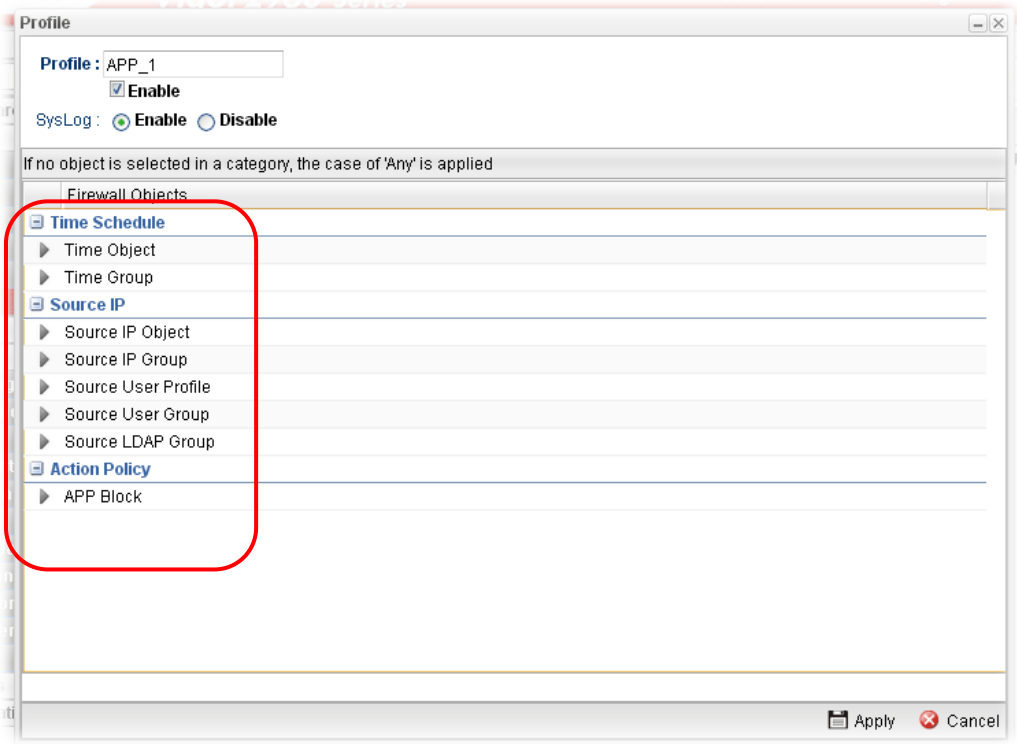
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for Application filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Syslog	Display if information for application filter will be recorded on Syslog or not (Enable/disable).
Time Schedule	If no time schedule is set, **None** will be shown in this field.
Firewall Target	Display the IP object profile selected for such application profile.

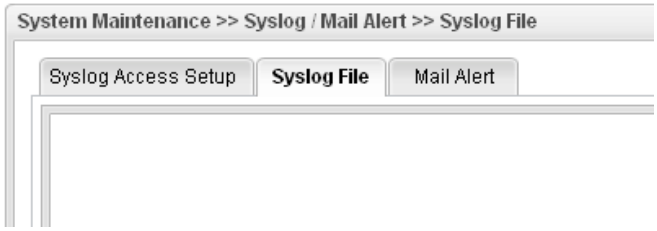
Item	Description
APP Block	Display the APP object profile selected for such application profile.
Counter	Display the number of packets matched.
Clear Counter	Click the icon to reset the counter.

How to create an Application Filter profile

1. Open **Firewall>>Filter Setup** and click the **Application Filter** tab.
2. Simply click the **Add** button.
3. The following dialog will appear. Click the triangle icon ▶ to display the profile selection box (red rectangle).

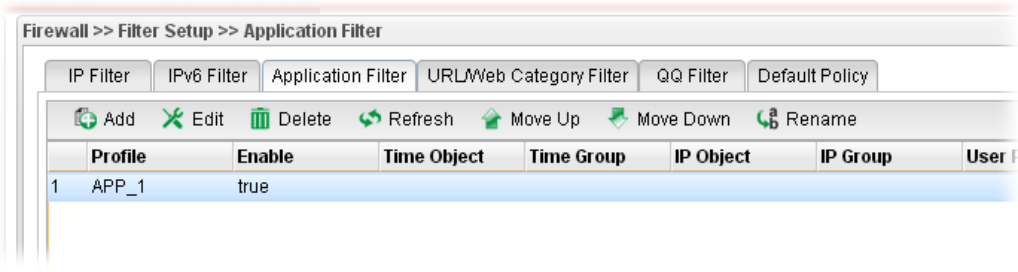


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the application filter profile.
Enable	Check the box to enable this profile.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance** >> **Syslog/Mail Alert** >> **Syslog File**. 

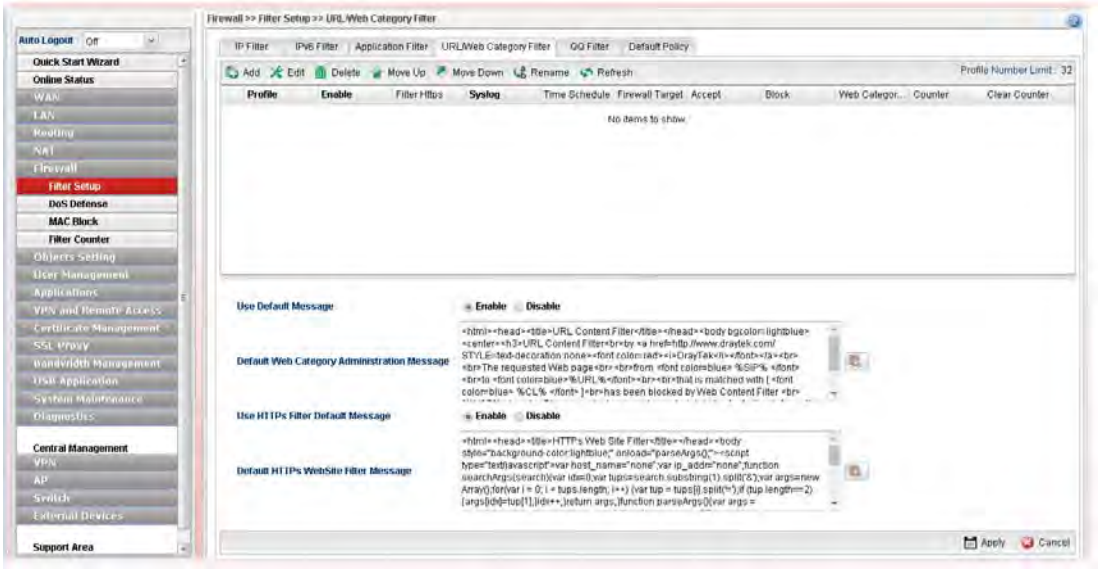
Time Schedule	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click to create another new time object profile, or you can click the edit icon to modify the existed object profile. **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another new time group profile, or you can click the edit icon to modify the existed group profile.
Source IP	**Source IP Object / Source IP Group / Source User Profile / LDAP Group/ Guest Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object / IP group / user profile / user group / LDAP group / Guest group profiles from the drop down list. The selected object will be filtered by the router when such application filter profile is applied. You can click to create another new object profile, or click the edit icon to modify the existed group profile.
Action Policy	**APP Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more APP object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click to create another new APP object profile, or you can click the edit icon to modify the existed object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new Application filter profile has been added.



4.5.1.4 URL/Web Category Filter

URL Filter can integrate URL, Keyword, File extension and WCF object profiles within one profile for restricting certain people accessing into Internet.



Each item will be explained as follows:

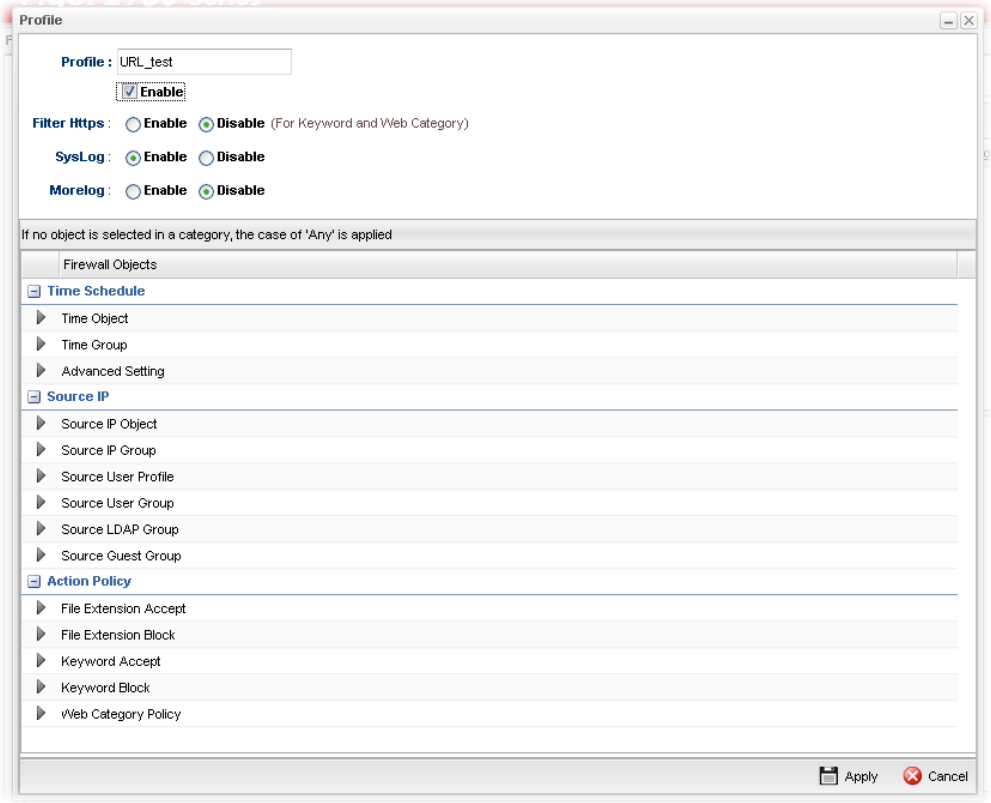
Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.

Item	Description
Rename	Allow to modify the selected profile name.
Profile Number Limit	Display the total number of the object profiles to be created.
Profile	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Filter Https	Display if the HTTPs filter is enabled or not.
Syslog	Display if information for URL/Web Category filter will be recorded on Syslog or not (Enable/disable).
Time Schedule	If no time schedule is set, **None** will be shown in this field.
Firewall Target	Display the IP object profile selected for such application profile.
Accept	Display the Keyword/File Extension object profile selected for system to accept.
Block	Display the Keyword/File Extension object profile selected for system to block.
Web Category Block	Display the web category object profile selected for each rule which is not allowed to pass through the router.
Counter	Display the number of packets matched.
Clear Counter	Click the icon to reset the counter.
Use Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Web Category Administration Message	Such field is available when you disable the function of **Use Default Message**. The message will display on the user's browser when he/she tries to access the blocked web page.
Use HTTPs Filter Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page through HTTPs. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page through HTTPs.
Default HTTPS WebSite Filter Message	The message will display on the user's browser when he/she tries to access the blocked web page through HTTPs.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

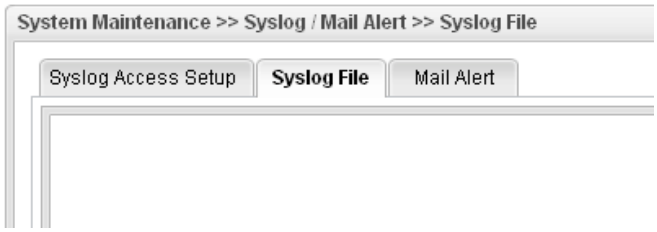
How to create a URL Filter profile

1. Open **Firewall>>Filter Setup** and click the **URL/Web Category Filter** tab.
2. Simply click the **Add** button.

3. The following dialog will appear.



Available parameters are listed as follows:

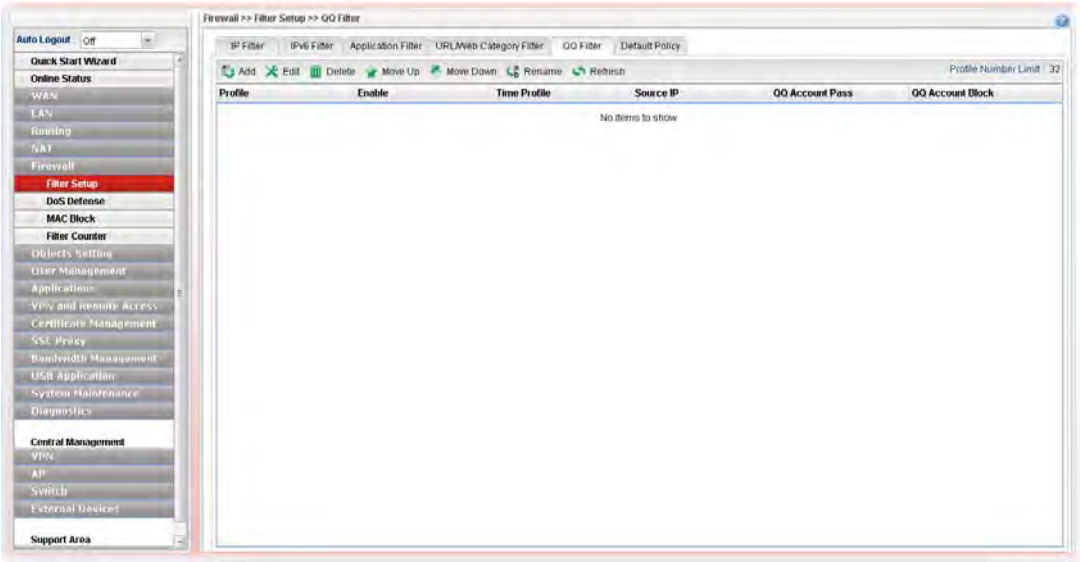
Item	Description
Profile	Type the name of the URL filter profile.
Enable	Check the box to enable this profile.
Filter https	**Enable** – Click it to enable the HTTPS filtering job. **Disable** – When only keyword and web category are selected for such rule, choose Disable.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance >> Syslog/Mail Alert** >> **Syslog File**. 
Morelog	Except the items displayed on Syslog, more items of log will be shown if it is enabled.
Time Schedule	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click to create another new time object

Item	Description
	profile, or you can click the edit icon to modify the existed object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another new time group profile, or you can click the edit icon to modify the existed group profile.
Source IP	**Source IP Object / Source IP Group / Source User Profile / Source User Group / Source LDAP Group / Source Guest Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more object profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new object profile, or click the edit icon to modify the existed profile.
Action Policy	**File Extension Accept / File Extension Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more File Extension object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click to create another new File Extension object profile, or you can click the edit icon to modify the existed object profile. **Keyword Accept / Keyword Block -** Click the triangle icon ▶ to display the profile selection box. Choose e one or more keyword object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click to create another new keyword object profile, or you can click the edit icon to modify the existed object profile. **Web Category Policy -** Click the triangle icon ▶ to display the profile selection box. Choose one or more web category object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new web category object profile, or you can click the edit icon to modify the existed object profile. **China Web Category Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more web category object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new web category object profile, or you can click the edit icon to modify the existed object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new URL filter profile has been added.

4.5.1.5 QQ Filter

This page is designed for the user in China only. For people **outside China, skip this section**.



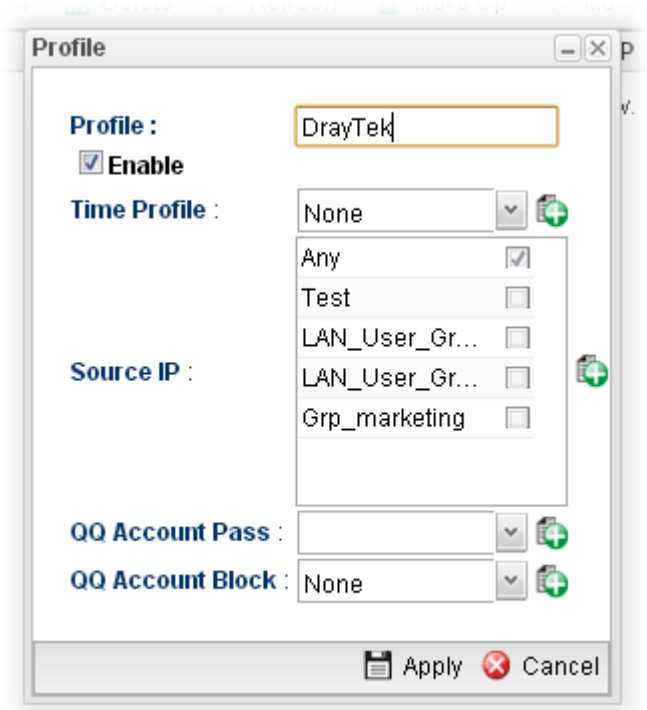
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for QQ filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Profile Number Limit	Display the total number of the object profiles to be created.
Profile	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Time Profile	If no time schedule is set, **None** will be shown in this field.
Source IP	Display the IP object profile selected for each rule.
QQ Account Pass	Display the account name which is allowed to pass if the selected QQ profile is enabled.
QQ Account Block	Display the account name which will be blocked if the

Item	Description
	selected QQ profile is enabled.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to create a QQ Filter profile

1. Open **Firewall>>Filter Setup** and click the **QQ Filter** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.

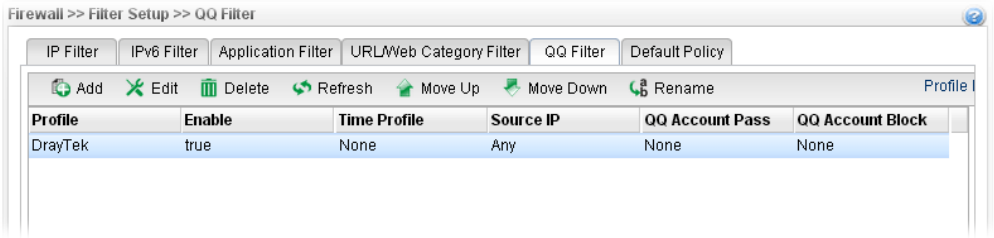


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the QQ filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Use the drop down list to specify a time profile for such profile. You can click to create another new time object profile.
Source IP	Specify user profiles for such profile. Users within the source IP will be filtered by Vigor router when such profile is applied.
QQ Account Pass	Use the drop down list to specify a QQ account profile for such profile. The select account will not be blocked by Vigor router. You can click to create another new QQ account.

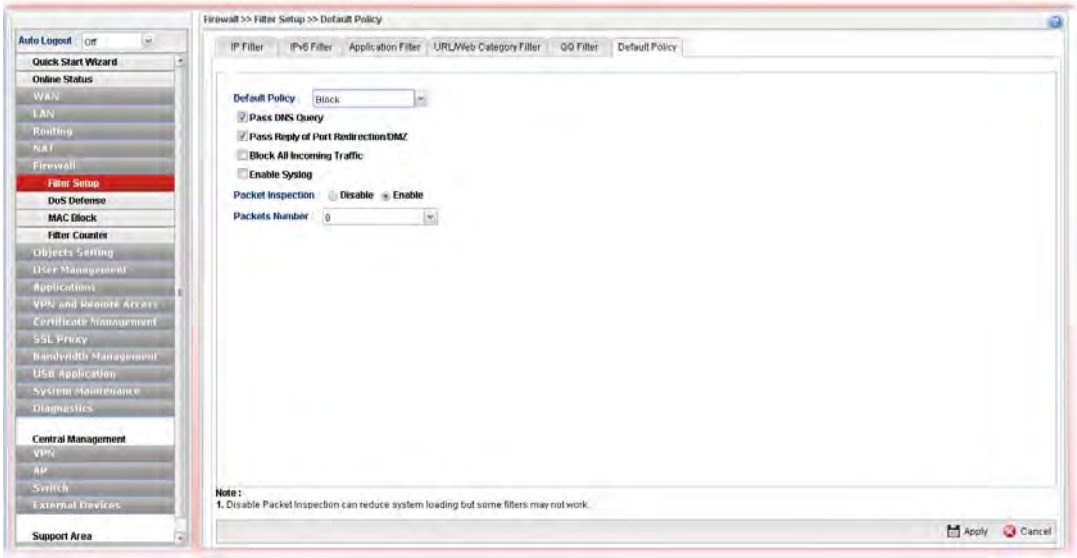
Item	Description
QQ Account Block	Use the drop down list to specify a QQ account profile for such profile. The select account will be blocked by Vigor router. You can click to create another new QQ account.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

4. Enter all the settings and click **Apply**.
5. A new QQ filter profile has been added.



4.5.1.6 Default Policy

Default policy will be applied to all of the incoming packets, if IP Filter, Application Filter, URL/Web Category Filter and QQ Filter are not suitable for the incoming packets.



Available parameters are listed as follows:

Item	Description
Default Policy	**Pass** – All of the incoming packets can pass through Vigor router without any filtering. **Block** – All of the incoming packets will be blocked except the following rules. ● **Pass DNS Query** – Check the box to make the DNS query passing through Vigor router's firewall. ● **Pass Reply of Port Redirection /DMZ** – Check the

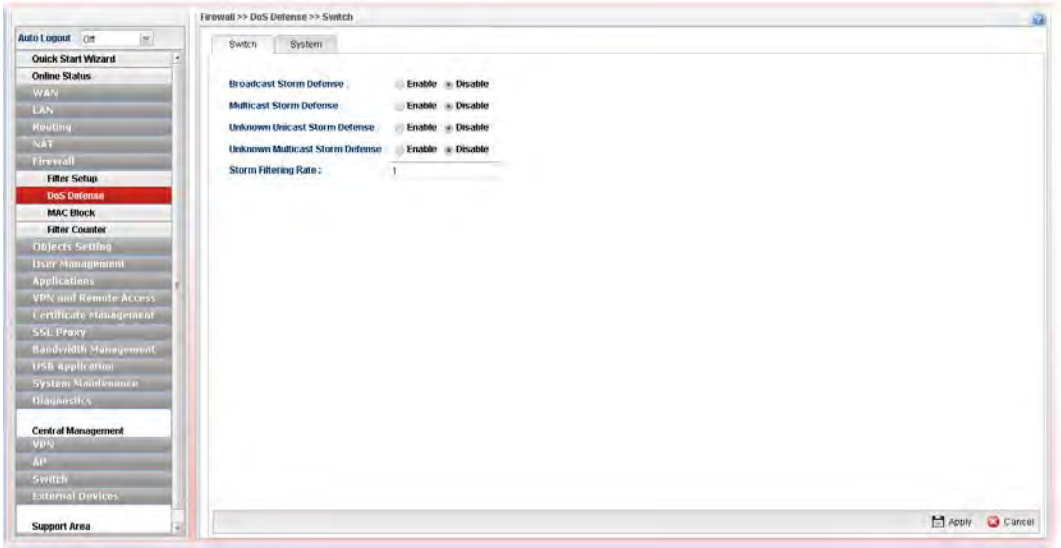
Item	Description
	box to make the **outgoing** packets processed by Port Redirection/DMZ passing through Vigor router's firewall. ● **Block All Incoming Traffic** – Check the box to block all of the incoming packets. ● **Enable Syslog** – Check the box to make related information for the blocked packets being recorded in Syslog. The above three policies also can be configured in **Firewall>>Filter Setup>>IP Filter/Application Filter.**
Packet Inspection	**Disable** – No inspection will be performed. **Enable** – Packet inspection will be performed.
Packets Number	If **Packet Inspection** is enabled, choose a packet number for filtering. Available settings are from 4 to 16. For example, "8" is selected as packet number setting. It means only the former 8 packets will be filtered and inspected by Firewall rule. Others are allowed to pass through without any inspection.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.5.2 DoS Defense

The DoS function helps to detect and mitigates DoS attacks. These include flooding-type attacks and vulnerability attacks. Flooding-type attacks attempt to use up all your system's resources while vulnerability attacks try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

4.5.2.1 Switch

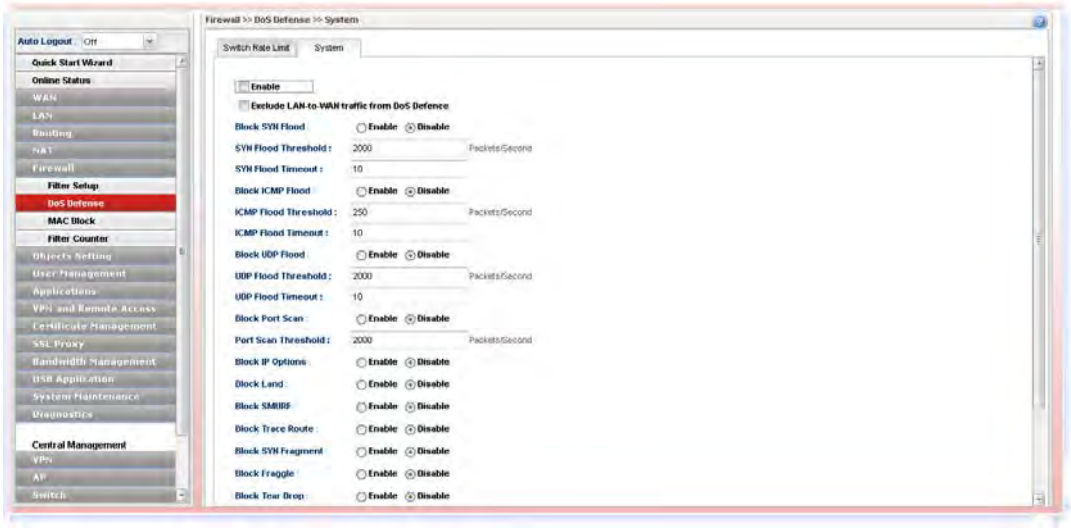


Available parameters are listed as follows:

Item	Description
Broadcast Storm Defense	Click **Enable** to block the packets attacks coming from broadcast storm.
Multicast Storm Defense	Click **Enable** to block the packets attacks coming from multicast storm.
Unknown Unicast Storm Defense	Click **Enable** to block the packets attacks coming from unknown unicast storm.
Unknown Multicast Storm Defense	Click **Enable** to block the packets attacks coming from unknown multicast storm.
Storm Filtering Rate	Type a number (1~4096, unit of 64Kpbs) as for the filtering rate. The default value for different hardware version will be varied. Default value of "-1" means no limit in filtering rate.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

4.5.2.2 System

In the **Firewall** group, click the **DOS Defense** and click the tab of **System**. You will see the following page. The DoS Defense Engine inspects each incoming packet against the attack signature database. Any packet that may paralyze the host in the security zone is blocked. The DoS Defense Engine also monitors traffic behavior. Any anomalous situation violating the DoS configuration is reported and the attack is mitigated.



Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable this profile.
Exclude LAN-to-WAN traffic from DoS Defense	Check it to exclude traffic from LAN to WAN for DoS Defense.
Block SYN Flood	Click **Enable** to activate the SYN flood defense function. If the amount of TCP SYN packets from the Internet

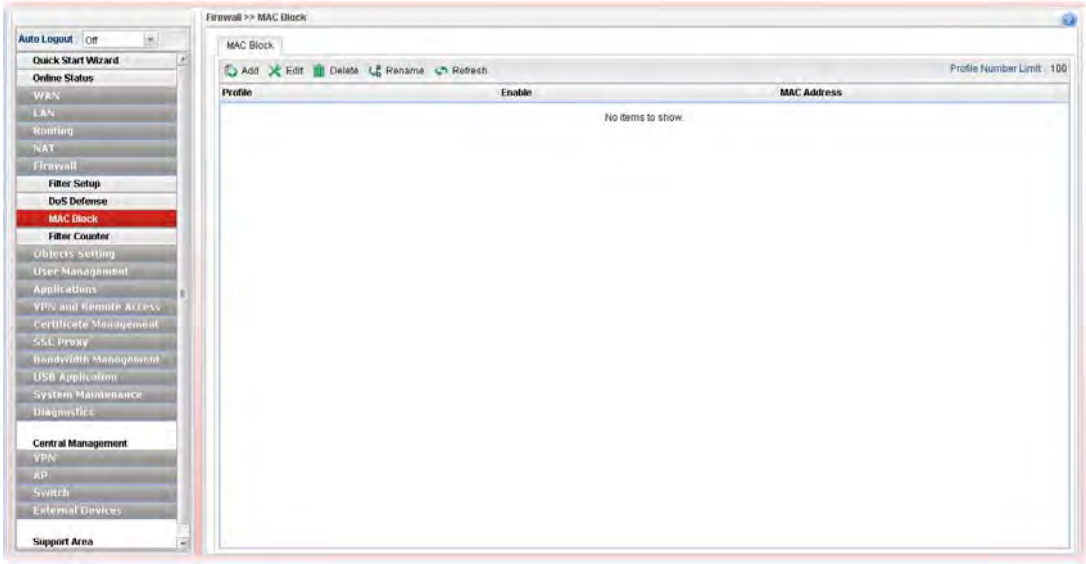
Item	Description
	exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN packets within the user-defined timeout period.
SYN Flood Threshold	The default setting for threshold is **2000** packets per second.
SYN Flood Timeout	The default setting for timeout is **10** seconds.
Block ICMP Flood	Click **Enable** to activate the ICMP flood defense function. If the amount of ICMP echo requests from the Internet exceeds the user-defined threshold value, the router will discard the subsequent echo requests within the user-defined timeout period.
ICMP Flood Threshold	The default setting for threshold is **250** packets per second.
ICMP Flood Timeout	The default setting for timeout is **10** seconds.
Block UDP Flood	Click **Enable** to activate the UDP flood defense function. If the amount of UDP packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent UDP packets within the user-defined timeout period.
UDP Flood Threshold	The default setting for threshold is **2000** packets per second.
UDP Flood Timeout	The default setting for timeout is **10** seconds.
Block Port Scan	Click **Enable** to activate the Port Scan detection function. Port scan sends packets with different port numbers to find available services, which respond. The router will identify it and report a warning message if the port scanning rate in packets per second exceeds the user-defined threshold value.
Port Scan Threshold	The default threshold is **2000** pps (packets per second).
Block IP Options	Click **Enable** to activate the Block IP options function. The router will ignore any IP packets with IP option field appearing in the datagram header.
Block Land	Click **Enable** to activate the Block Land function. A Land attack occurs when an attacker sends spoofed SYN packets with identical source address, destination addresses and port number as those of the victim.
Block SMURF	Click **Enable** to activate the Block Smurf function. The router will reject any ICMP echo request destined for the broadcast address.
Block Trace Route	Click **Enable** to activate the Block Trace Route function.
Block SYN Fragment	Click **Enable** to activate the Block SYN fragment function. Any packets having the SYN flag and fragmented bit sets will be dropped.
Block Fraggle	Click **Enable** to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet are blocked.

Item	Description
Block Tear Drop	Click **Enable** to activate the Block Tear Drop function. This attack involves the perpetrator sending overlapping packets to the target hosts so that target host will hang once they re-construct the packets. The routers will block any packets resembling this attacking activity.
Block Ping of Death	Click **Enable** to activate the Block Ping of Death function. Many machines may crash when receiving an ICMP datagram that exceeds the maximum length. The router will block any fragmented ICMP packets with a length greater than 1024 octets.
Block ICMP Fragment	Click **Enable** to activate the Block ICMP fragment function. Any ICMP packets with fragmented bit sets are dropped.
Block Unknown Protocol	Click **Enable** to activate the Block Unknown Protocol function. The router will block any packets with unknown protocol types.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.5.3 MAC Block

MAC Block allows you to set lots of proprietary MAC Address. Packets will be dropped if the source or destination MAC Address of packets is matched with these assigned MAC Addresses. The advantage of MAC Block is that it can filter some unnecessary packets or attacking packets on LAN network.



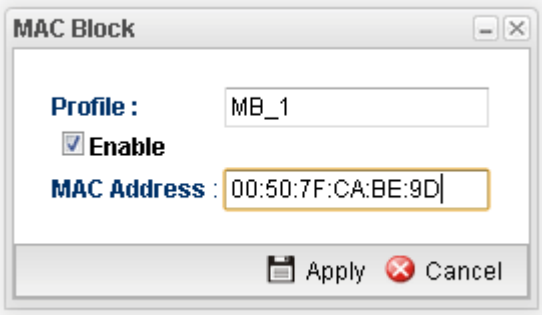
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile.

Item	Description
	To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the object profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
MAC Address	Display the MAC address for such profile.

How to create a new MAC Block profile

1. Open **Firewall>>MAC Block**.
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

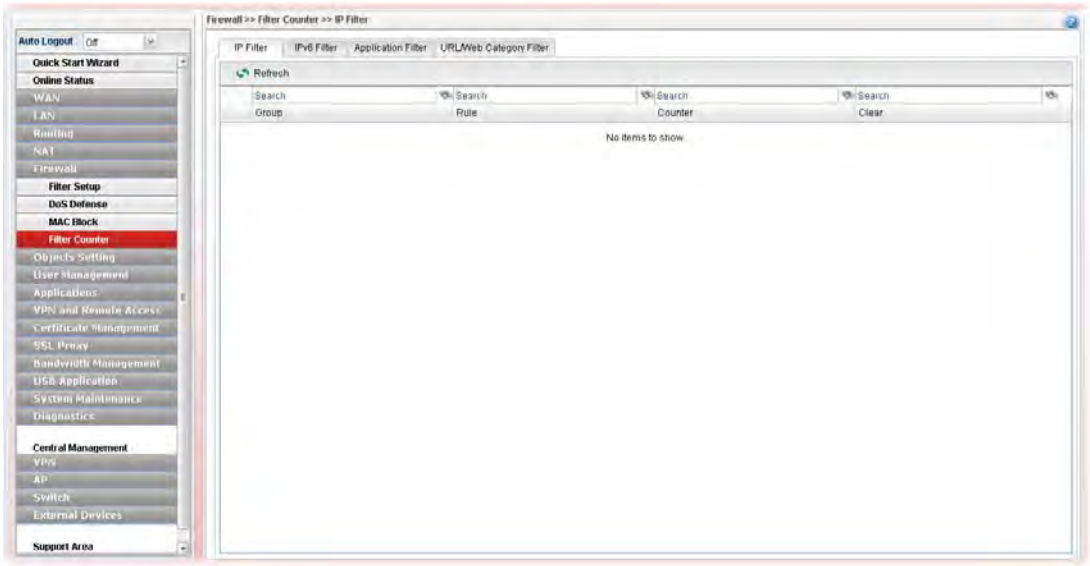
Item	Description
Profile	Type the name which can briefly describe the reason of the MAC block of such profile.
Enable	Check the box to enable this profile.
MAC Address	Type the MAC address which will be blocked by the system for such profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new MAC Block profile has been created.

4.5.4 Filter Counter

Such page will display log or status for firewall group, rule information for IP Filter, IPv6 Filter, Application Filter and URL/Web Category Filter.

Simply click the tab of IP Filter, IPv6 Filter, Application Filter or URL/Web Category Filter to get the status for each filter.



If there is no data (counter number is “0”) for certain rule displayed on such page, that means such rule might be configured wrong or blocked by other rules. Then the administrator or the user can adjust the filter to meet his request.

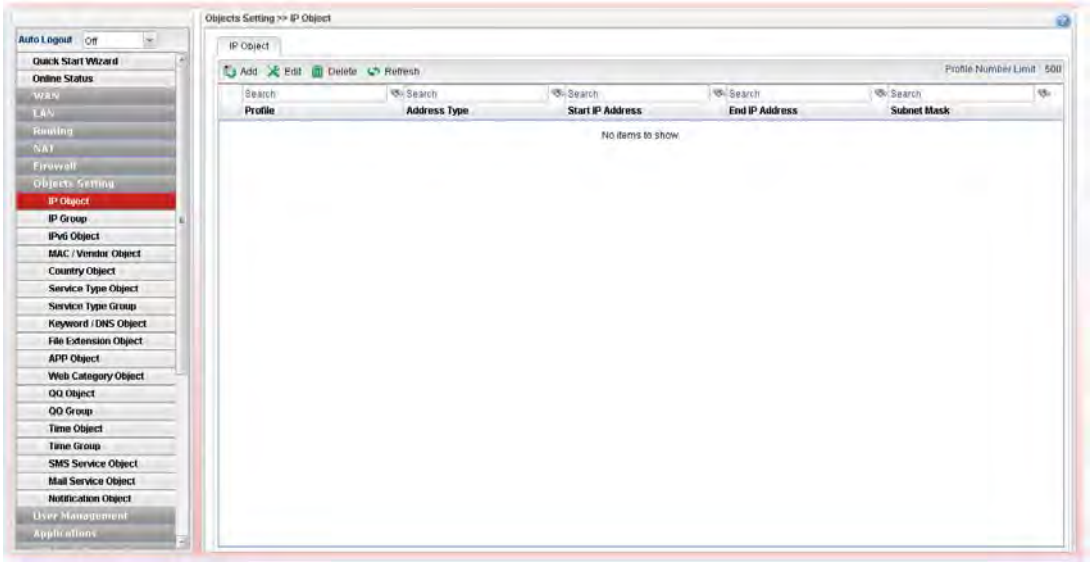
4.6 Objects Setting

Vigor3900 allows users to set different filter profiles based on IP, service type, keyword, file extension, instant message application, P2P application, protocol application, web category, QQ application, time setting, SMS service, mail service and notification. These objects setting profiles can be applied in **Firewall**.

4.6.1 IP Object

For IPs in a limited range usually will be applied in configuring router's settings, we can define them with ***objects*** and bind them with ***groups*** for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

This page allows you to specify certain IP address, range of IP addresses or subnet mask as an object which will be applied in **Firewall**.

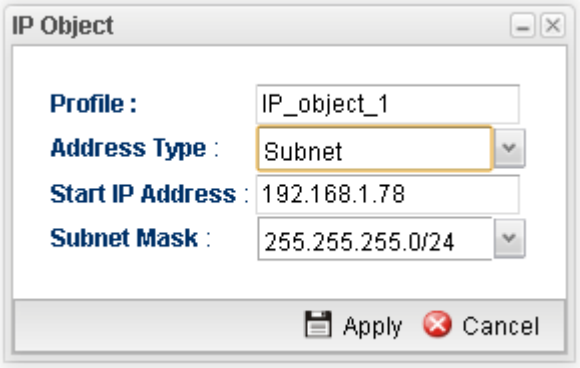


Each item will be explained as follows:

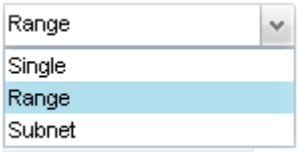
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (256) of the object profiles to be created.
Profile	Display the name of the profile.
Address Type	Display the address type (single, range or subnet) for such profile.
Start IP Address	Display the IP address of the starting point for such profile.
End IP Address	Display the IP address of the ending point for such profile. It will be joined with **Start IP Address** only when you choose **Range** as the **Address Type**.
Subnet Mask	Display the subnet mask for such profile.

How to create a new IP object profile

1. Open **Objects Setting>>IP Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



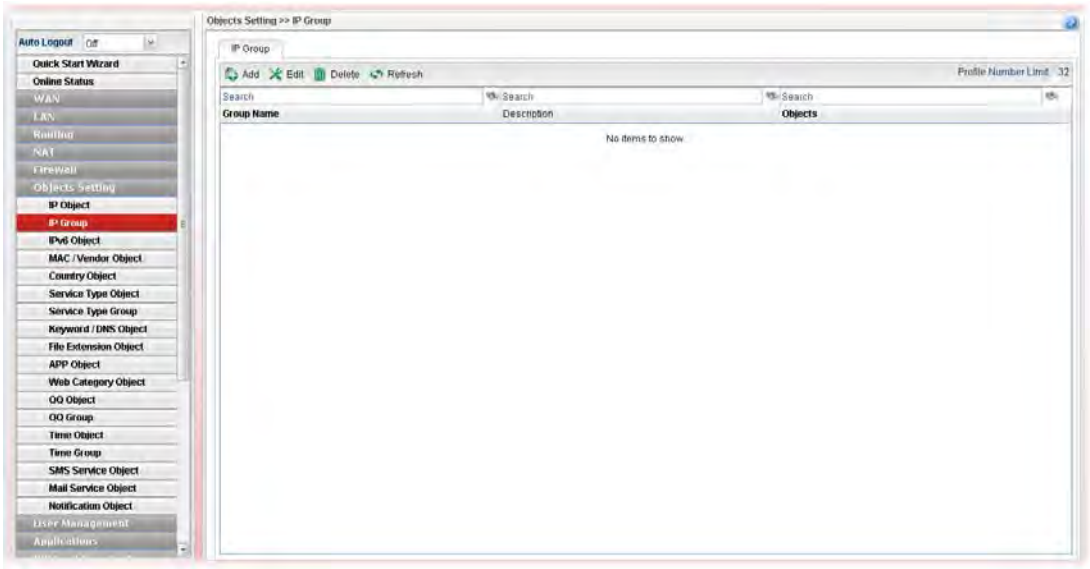
Available parameters are listed as follows:

Item	Description
Profile	Type the name of such profile.
Address Type	Choose the address type (Single / Range /Subnet) for such profile. 
Start IP Address	Type the IP address of the starting point for such profile.
End IP Address	Type the IP address of the ending point for such profile if you choose **Range** as **Address Type**.
Subnet Mask	Use the drop down list to choose the subnet mask for such profile if you choose **Subnet** as **Address Type**.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new IP object profile has been created.

4.6.2 IP Group

To manage conveniently, several IP object profiles can be grouped under a group. Different IP group can contain different IP object profiles.

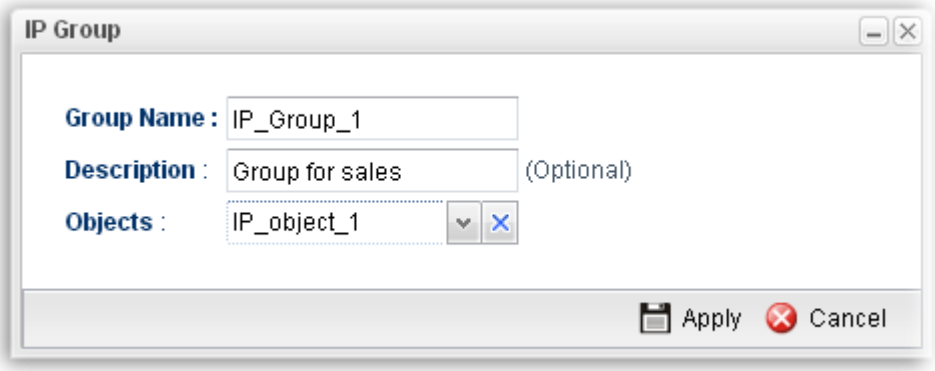


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Group Name	Display the name of the object group.
Description	Display the description for such profile.
Objects	Display the object profiles grouped under such group.

How to create a new IP group profile

1. Open **Objects Setting>>IP Group.**
2. Simply click the **Add** button.
3. The following dialog will appear.



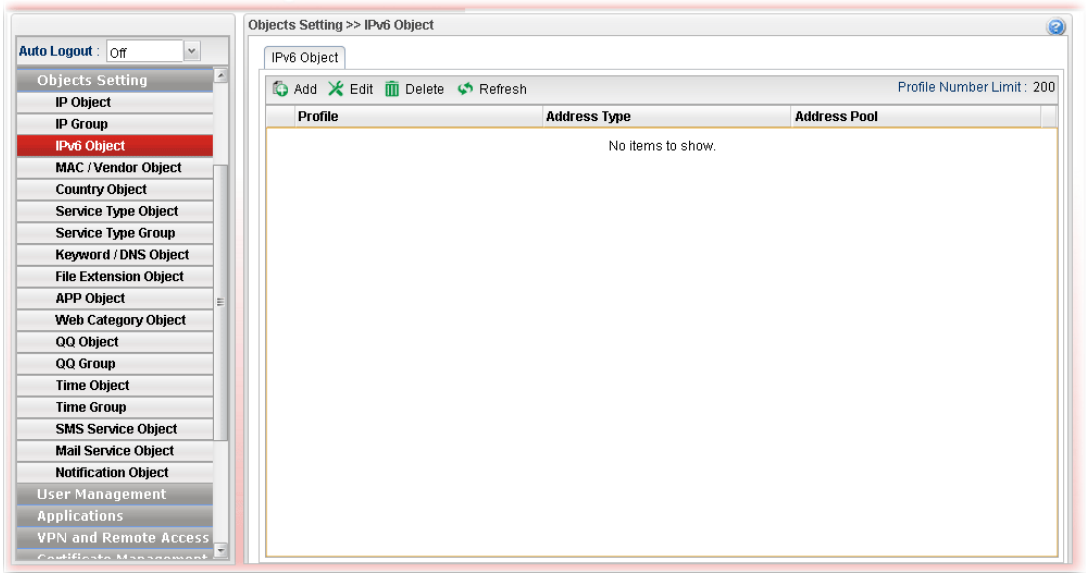
Available parameters are listed as follows:

Item	Description
Group Name	Type the name of the object group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the IP object profiles under such group. All the available IP objects that you have added on **Objects Setting>>IP Object** will be seen here. To clear the selected one, click to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all the settings and click **Apply**.
5. A new IP Group profile has been created.

4.6.3 IPv6 Object

You can set up to 200 sets of IPv6 Objects with different conditions.



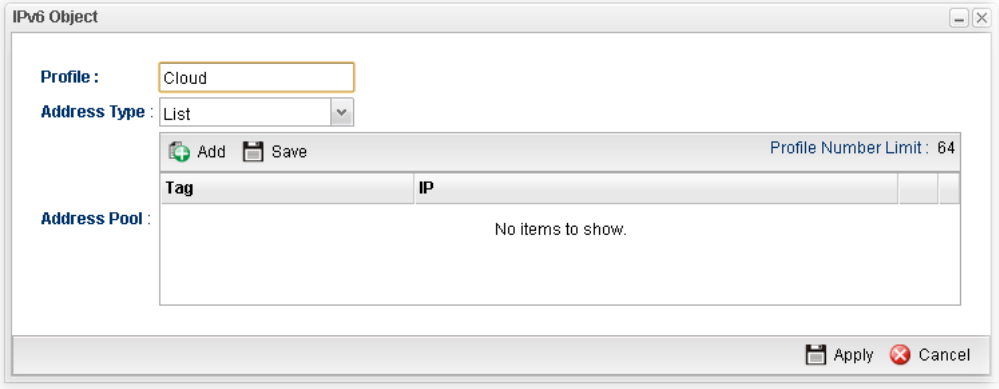
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (200) of the object profiles to be created.
Profile	Display the name of the object.
Address Type	Display the address type of the object.
Address Pool	Display the IP address/ IP range /subnet of the object.

How to create a new IPv6 Object profile

1. Open **Objects Setting>>IPv6 Object.**
2. Simply click the **Add** button.

3. The following dialog will appear.



Available parameters are listed as follows:

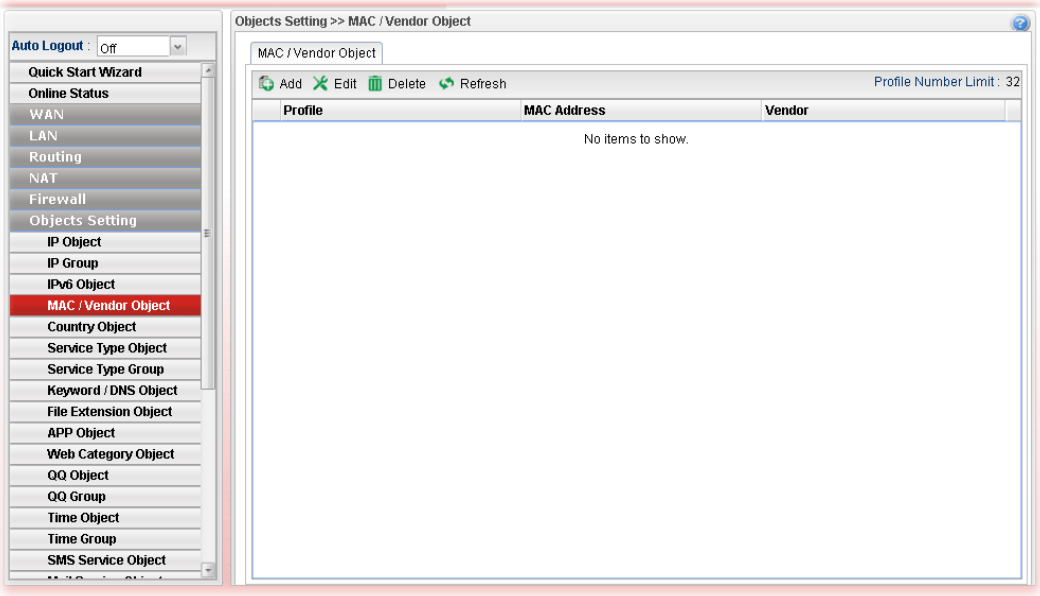
Item	Description
Profile	Type the name of the object.
Address Type	There are three types: **List** – Allow to specify IP address. **Range** – Allow to specify a range of IP addresses. **Prefix** – Allow to specify prefix for IPv6 IP address. **Suffix** – Allow to specify suffix for IPv6 IP address.
Address Pool	This field allows you to type IP address, specify Tag number and type subnet mask based on IPv6 protocol. Tag is an optional field only used for user to distinguish the name/usage of the defined address.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.

   A new IPv6 Object profile has been created.

4.6.4 MAC/Vendor Object

MAC/Vendor object profile can determine which MAC address of vendor shall be blocked by the Vigor router's Firewall.

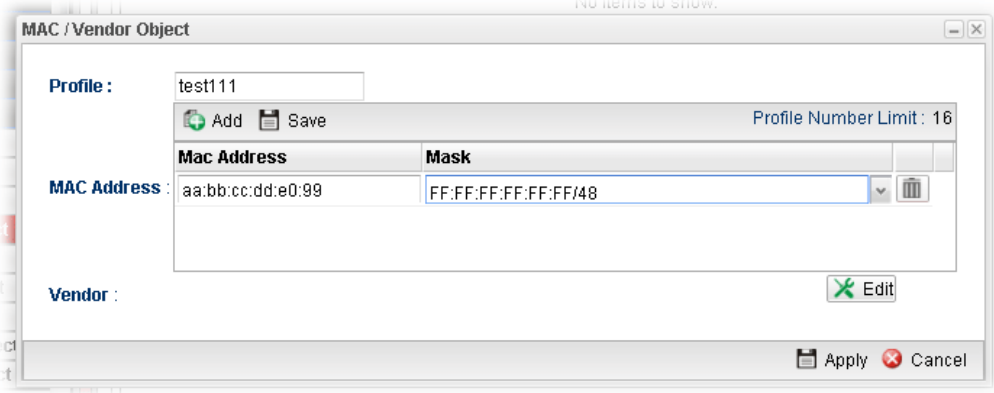


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.

How to create a new MAC / Vendor profile

1. Open **Objects Setting>> MAC / Vendor Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



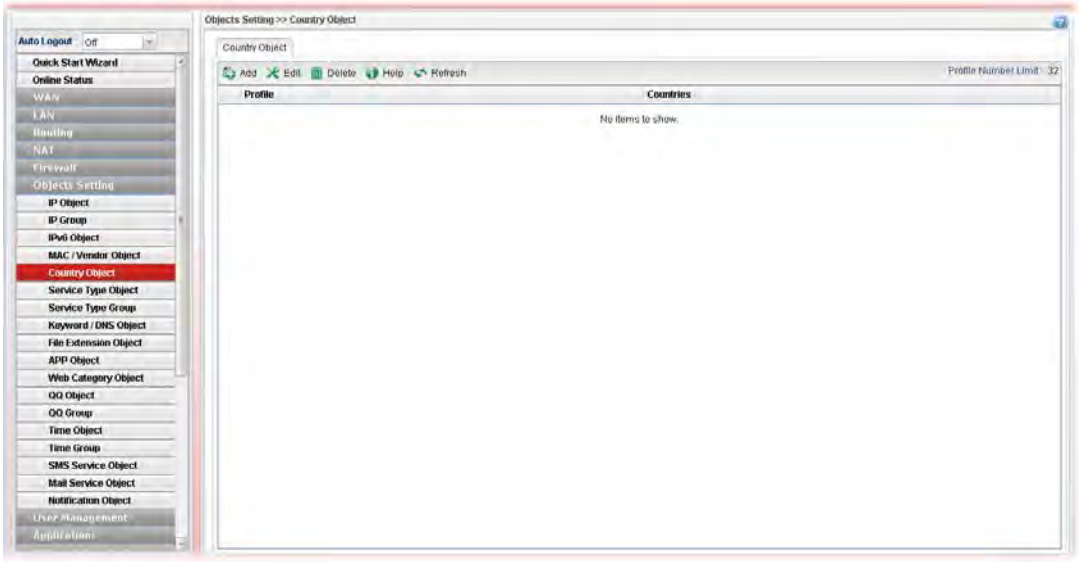
Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
MAC Address	Click Add to have the fields of MAC Address and Mask. Type the address with the correct format (will be shown automatically when the mouse cursor is on it). Choose a suitable mask selection.
Apply	Click it to save the configuration.
Vendor	**Edit** – Click it to open a table of vendor list. Check the one(s) you want. The names for selected vendors will be shown later.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.
5. A new MAC/Vendor Object profile has been created.

4.6.5 Country Object

To country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.



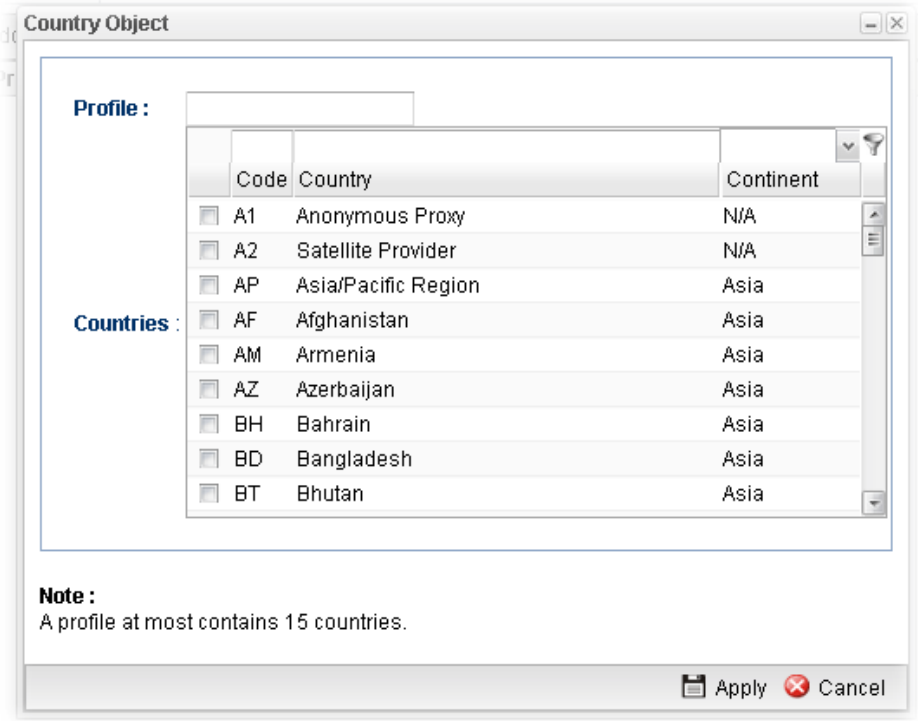
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.

Item	Description
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.

How to create a new Country Object profile

1. Open **Objects Setting>>Country Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

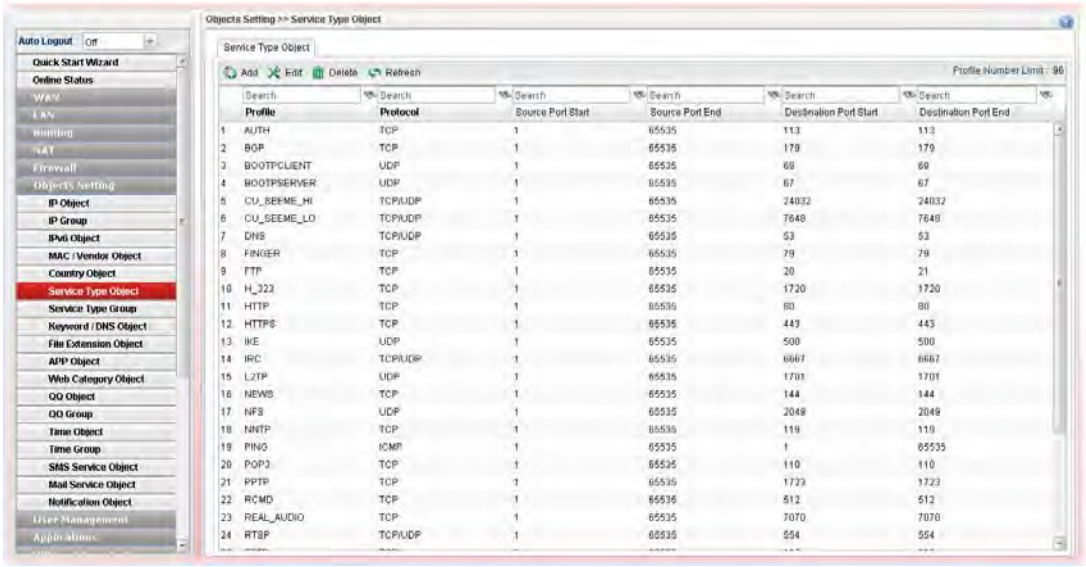
Item	Description
Profile	Type a name for such profile.
Countries	Check the box(es) for the country/countries to be blocked by Firewall.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.
5. A new Country Object profile has been created.

4.6.6 Service Type Object

TCP and UDP service with specified port range can be saved with different service type object profiles. Later, it can be applied to Firewall as a filter rule.

In default, common used service type object profiles have been created in this page.



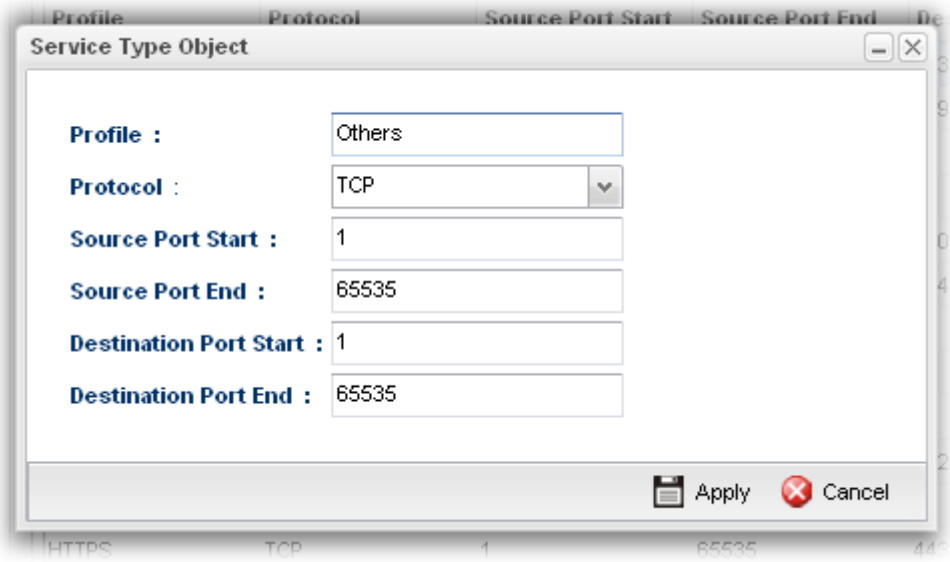
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (96) of the object profiles to be created.
Profile	Display the name of the service type object profile.
Protocol	Display the protocol selected for such profile.
Source Port Start	Display the starting source port for such profile.
Source Port End	Display the ending source port for such profile.
Destination Port Start	Display the starting destination port for such profile.
Destination Port End	Display the ending destination port for such profile.

How to create a new service type object profile

1. Open **Objects Setting>> Service Type Object.**
2. Simply click the **Add** button.

3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile. The number of the characters allowed to be typed here is 10.
Protocol	Specify one of the protocols for such profile.
Source Port Start	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the starting source port.
Source Port End	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the ending source port.
Destination Port Start	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the starting destination port.
Destination Port End	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the ending destination port.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

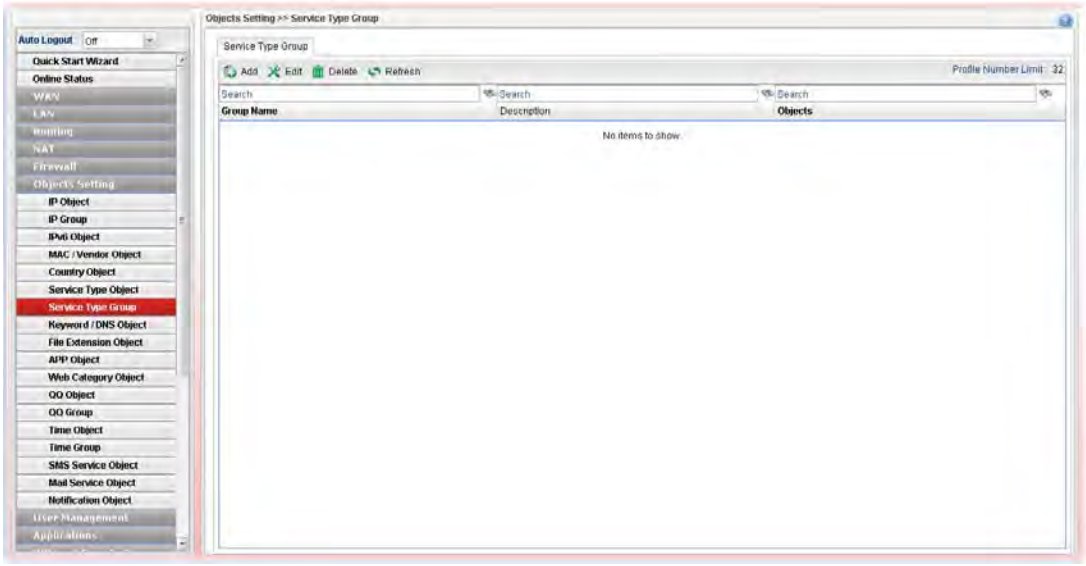
4. Enter all the settings and click **Apply**.

5. A new Service Type Object profile has been created.

4.6.7 Service Type Group

This page allows you to bind several service types into one group.

To manage conveniently, several service type profiles can be grouped under a service type group. Different service type group can contain different service type profiles.

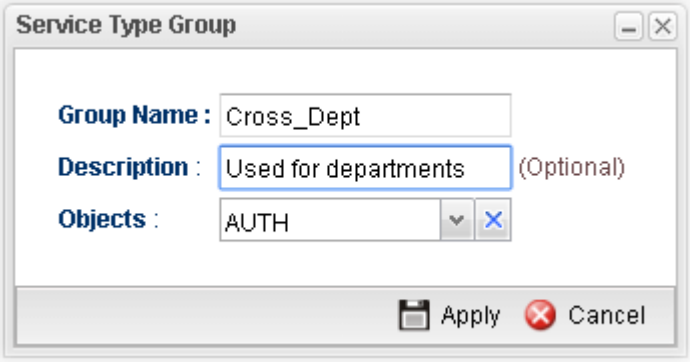


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Group Name	Display the name of the service type group.
Description	Display the description for such profile.
Objects	Display the service type object profiles grouped under such group.

How to create a new service type group profile

1. Open **Objects Setting>> Service Type Group.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

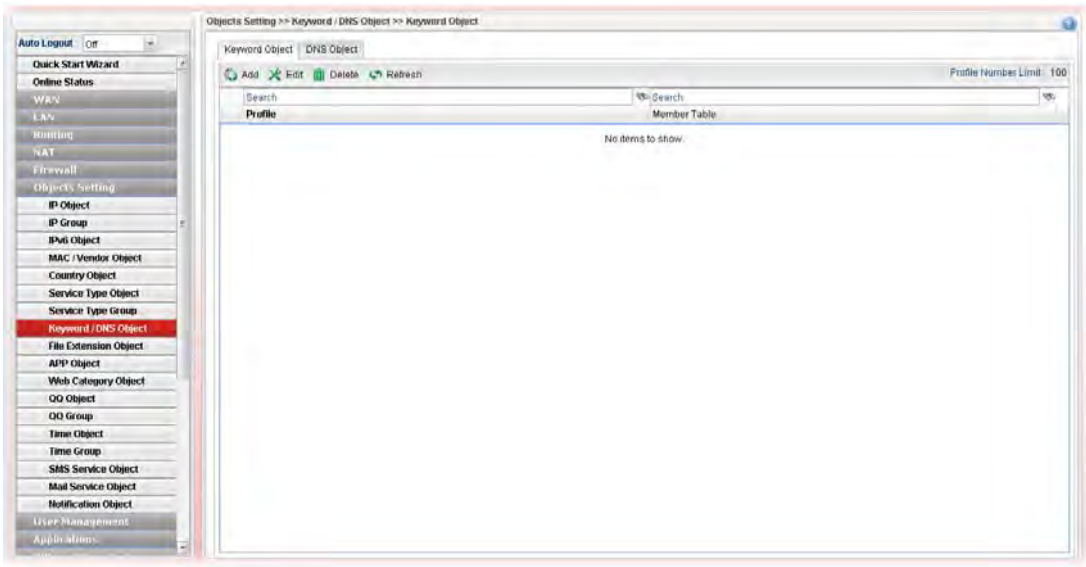
Item	Description
Group Name	Type the name of the service type object group. The number of the characters allowed to be typed here is 10.
Description	Type some words to describe such group.
Objects	Use the drop down list to check the service type object profiles under such group. All the available service type objects that you have added on **Objects Setting>>Service Type Object** will be seen here. To clear the selected one, click to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new Service Type Group profile has been created.

4.6.8 Keyword /DNS Object

4.6.8.1 Keyword Object

Keyword can be set as a filter rule to be applied in Firewall. Vigor3900 allows users to set keyword profile with several keywords. Even, it allows users to group several keyword profiles within a keyword group.

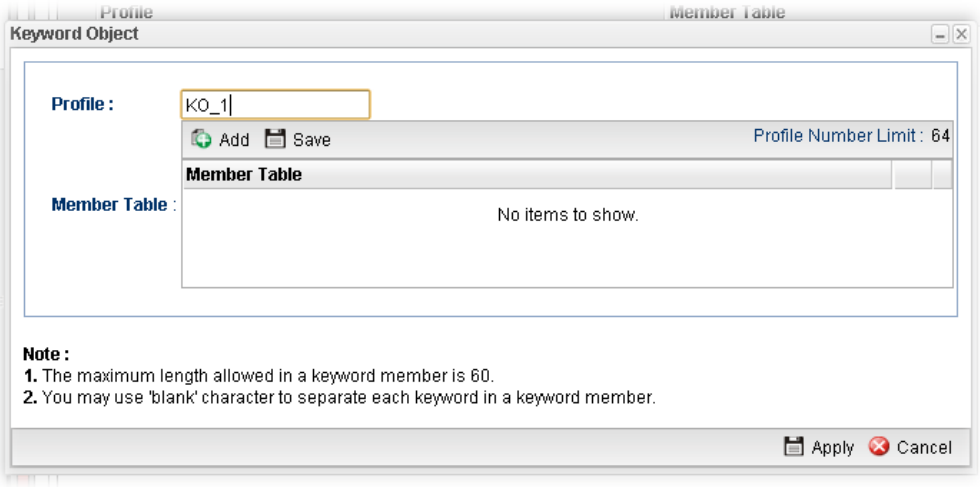


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (100) of the object profiles to be created.
Profile	Display the name of the keyword object profile.
Member Table	Display the words specified in such profile.

How to create a new keyword object profile

1. Open **Objects Setting>> Keyword /DNS Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



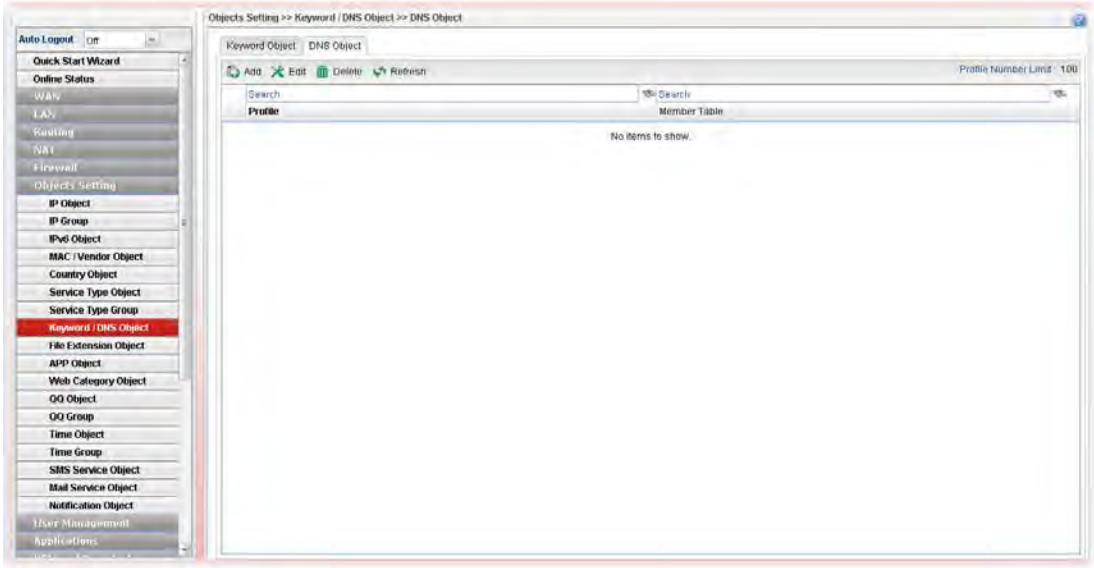
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the Keyword Object.
Member Table	Type the content for such profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings. **Add** – Type the word in the box of Member and click this button to add the new word as keyword object. **Save** – Click it to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new **Keyword Object** profile has been created.

4.6.8.2 DNS Object

DNS can be set as a filter rule to be applied in Firewall.

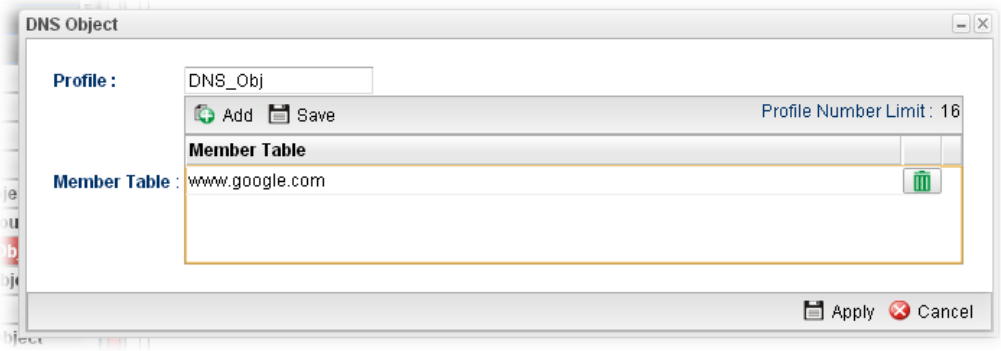


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (100) of the object profiles to be created.
Profile	Display the name of the DNS object profile.
Member Table	Display the words specified in such profile.

How to create a new DNS Object profile

1. Open **Objects Setting>>DNS Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

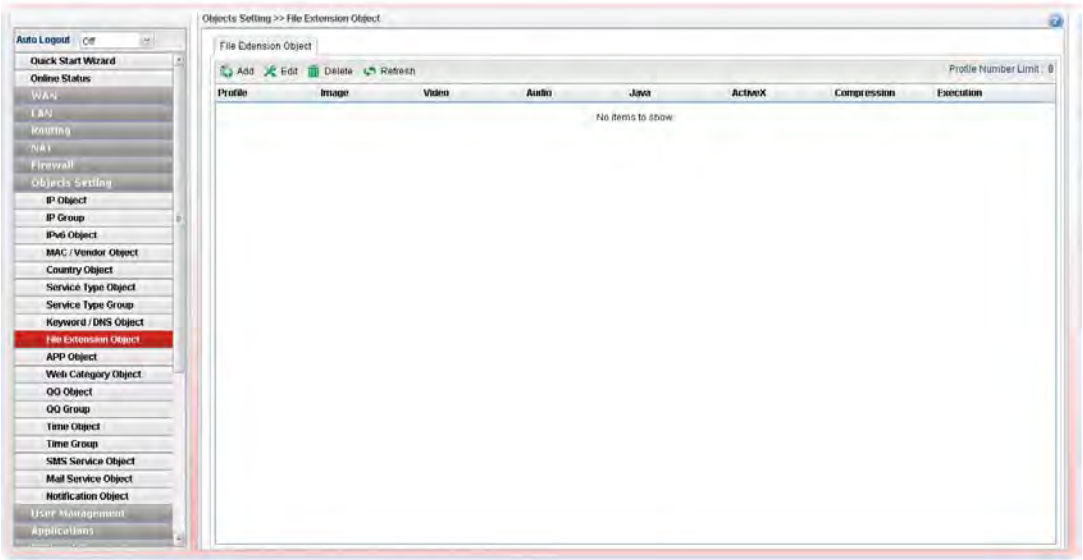
Item	Description
Profile	Type the name of the DNS object profile.
Member Table	Type the domain name of the DNS that you want to filter. **Add** – Type the word in the box of Member and click this button to add the new word as DNS object. **Save** – Click it to save the setting. – Click the icon to remove the selected entry.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all of the settings and click **Apply**.

5. A new **DNS Object** profile has been created.

4.6.9 File Extension Object

This page allows you to set file extension profiles which will be applied in **Firewall**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

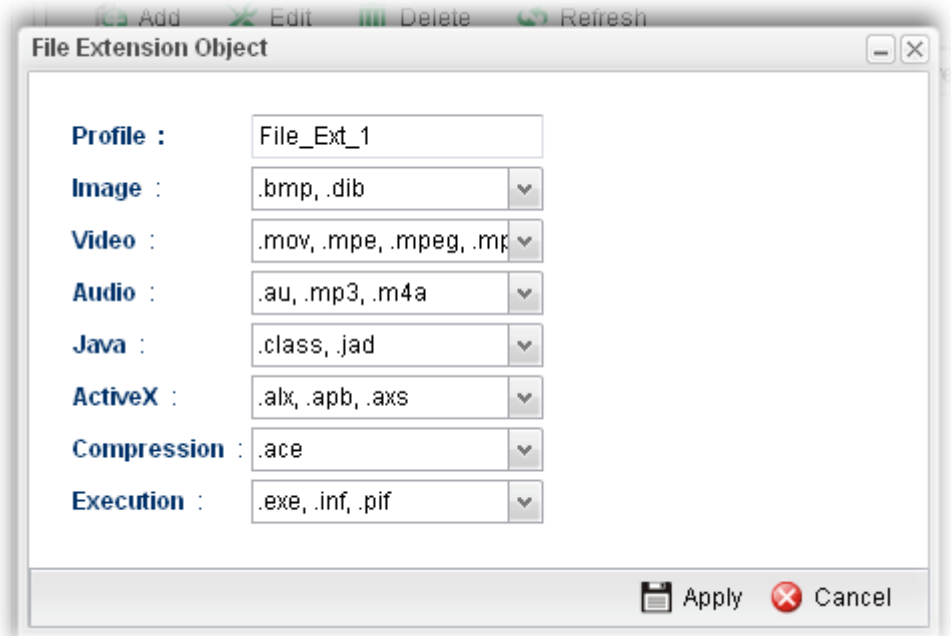


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Profile	Display the name of the profile.
Image	Display the selected file extension of image.
Video	Display the selected file extension of video.
Audio	Display the selected file extension of audio.
Java	Display the selected file extension of java.
ActiveX	Display the selected file extension of activeX.
Compression	Display the selected file extension of compression.
Execution	Display the selected file extension of execution.

How to create a new file extension object profile

1. Open **Objects Setting>>File Extension Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

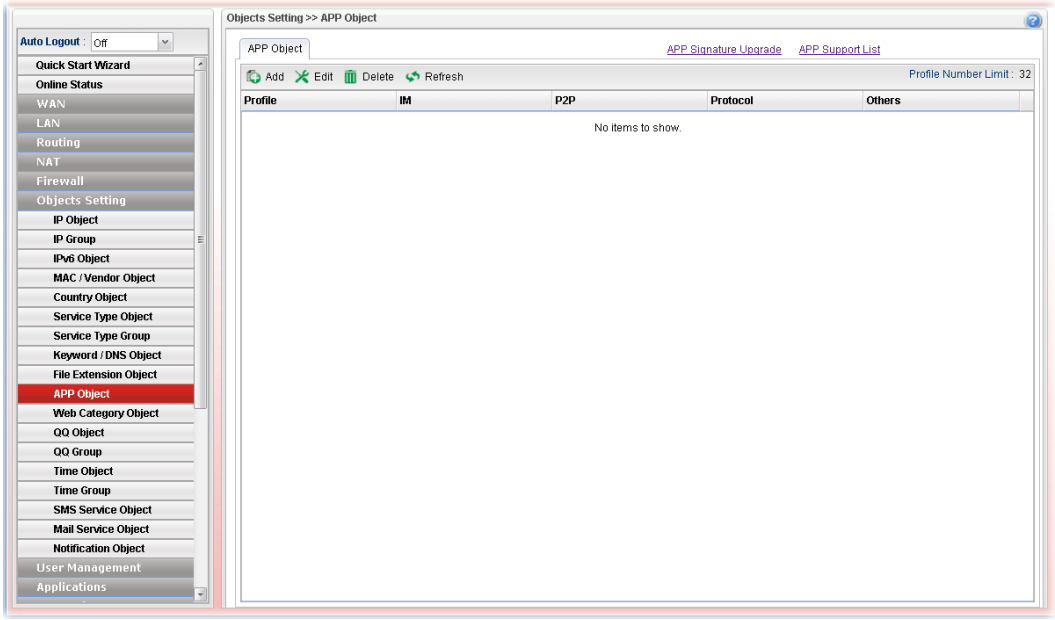
Item	Description
Profile	Type the name of the File Extension Object group..
Image	Several file extensions for Image offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Video	Several file extensions for Video offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Audio	Several file extensions for Audio offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Java	Several file extensions for Java offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
ActiveX	Several file extensions for ActiveX offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Compression	Several file extensions for compression offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Execution	Several file extensions for execution offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.

5. A new File Extension Object profile has been created.

4.6.10 APP Object

The IM, P2P, Protocol and Others types can be integrated as an APP object which can be used in Firewall to block certain applications.



Each item will be explained as follows:

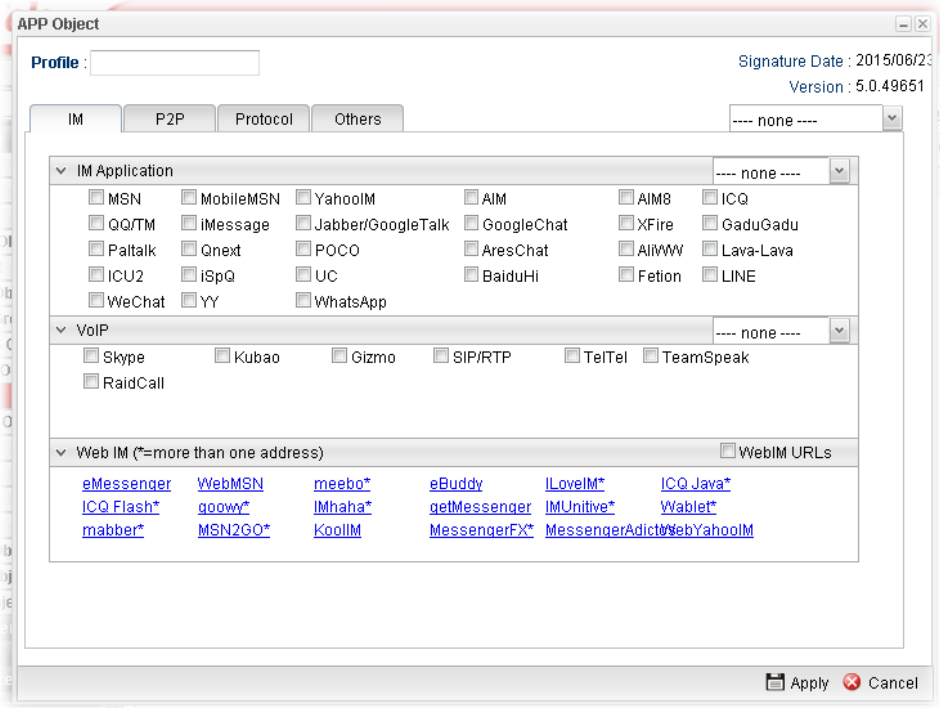
Item	Description
APP Signature Upgrade	Click it to open **System Maintenance>>APP Signature Upgrade** configuration page.
APP Support List	APP Support List will display all of the applications with versions supported by Vigor router. They are separated with types of IM, P2P, Protocol and Others. Each tab will bring out different items with supported versions. Below shows the items with versions which are categorized under **IM.**
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Profile	Display the name of the IM object profile.

IM	Display the IM application specified in such profile.
P2P	Display the P2P specified in such profile.
Protocol	Display the protocol specified in such profile.
Others	Display other types specified in such profile.

How to create a new APP Object Profile

1. Open **Objects Setting>>APP Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.

   Click **IM** to get the following page. People like to use Instant Message to communication with friends on line just for fun or just because it is easy and convenient. However, it might reduce the productivity of employees to a company. Therefore, a tool to block or limit the usage of IM application is important to a company. IM object setting lists all of the popular instant message application for you to choose to block. Choose the one(s) you want to block and save as an IM Object profile. Later, it can be applied to Firewall as a filter rule and reach the purpose of block.



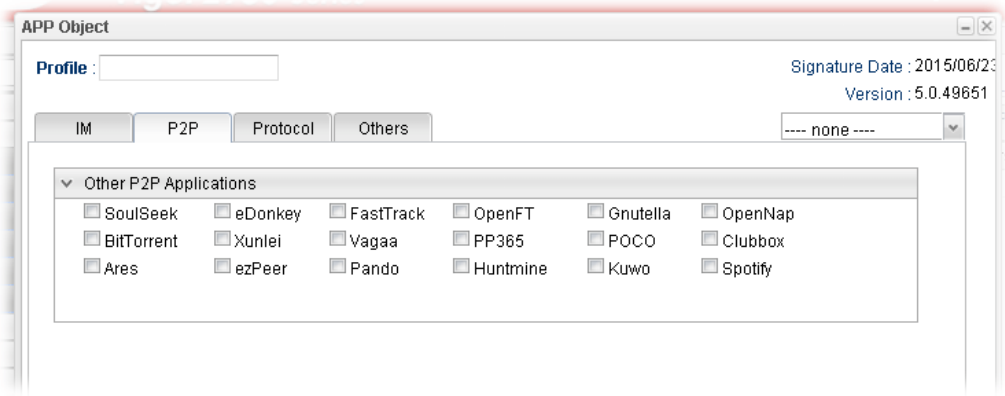
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IM object group. The number of the characters allowed to be typed here is 10.
IM Application	Several IM applications offered for you to choose. Check the one(s) you want to add for such profile.
WebIM	It lists a package of IM application based on web page. You may check the box to include all of them.

Item	Description
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

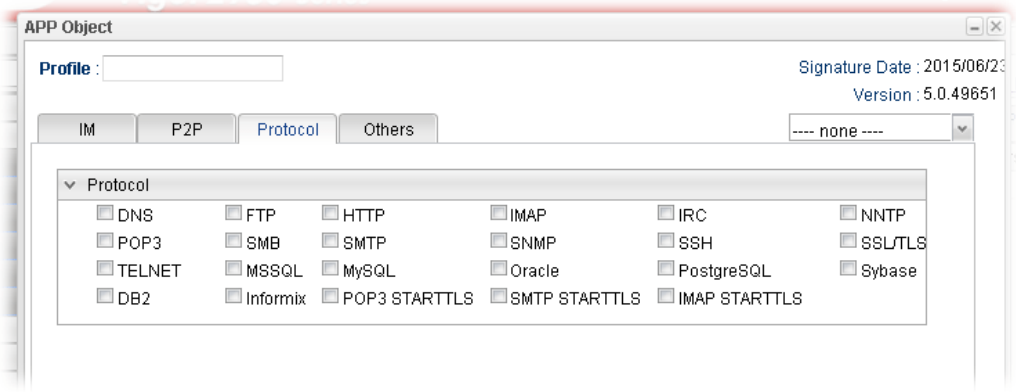
Click **P2P** to get the following page. Vigor3900 can block P2P application for users, especially for the ones who always upload or download improper files to Internet.

P2P object setting lists all of the point to point application for you to choose to block. Choose the one(s) you want to block and save as a P2P Object profile. Later, it can be applied to Firewall as a filter rule and reach the purpose of block.



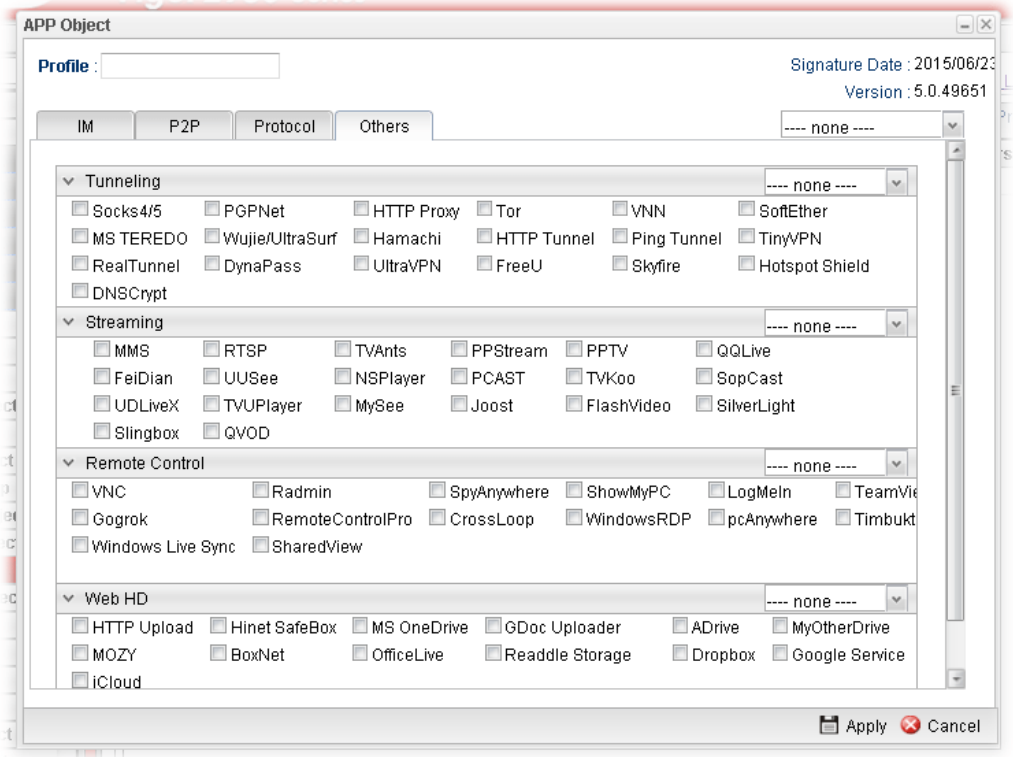
Item	Description
Other P2P Applications	Several P2P applications offered for you to choose. Check the one(s) you want to add for such profile.

Click **Protocol** to get the following page. Network services, e.g., DNS, FTP, HTTP, POP3, for LAN users can be blocked by Vigor3900. Common services will be listed in this function and can be selected to be blocked by the router.



Item	Description
Protocol	Several protocols offered for you to choose. Check the one (s) you want to add for such profile.

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



Item	Description
Tunneling/Streaming/Remote Control/Web HD	Several protocols offered for you to choose. Check the one (s) you want to add for such profile.

4. Enter all of the settings and click **Apply**.
5. A new APP Object profile has been created.

4.6.11 Web Category Object

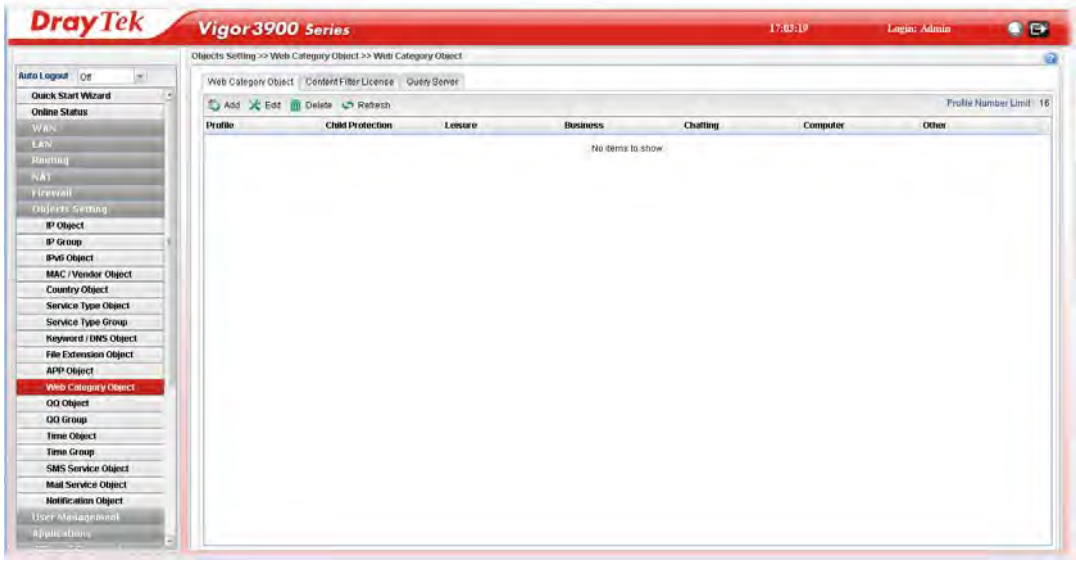
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With web category filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

WCF adopts the mechanism developed and offered by certain service provider. No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate URL** to satisfy your request. Note that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with your DrayTek dealer.

> **Note 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.

Note 2: Commtouch is merged by Cyren and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html
Note 3: fragFINN service will be terminated from 2015.

4.6.11.1 Web Category Object



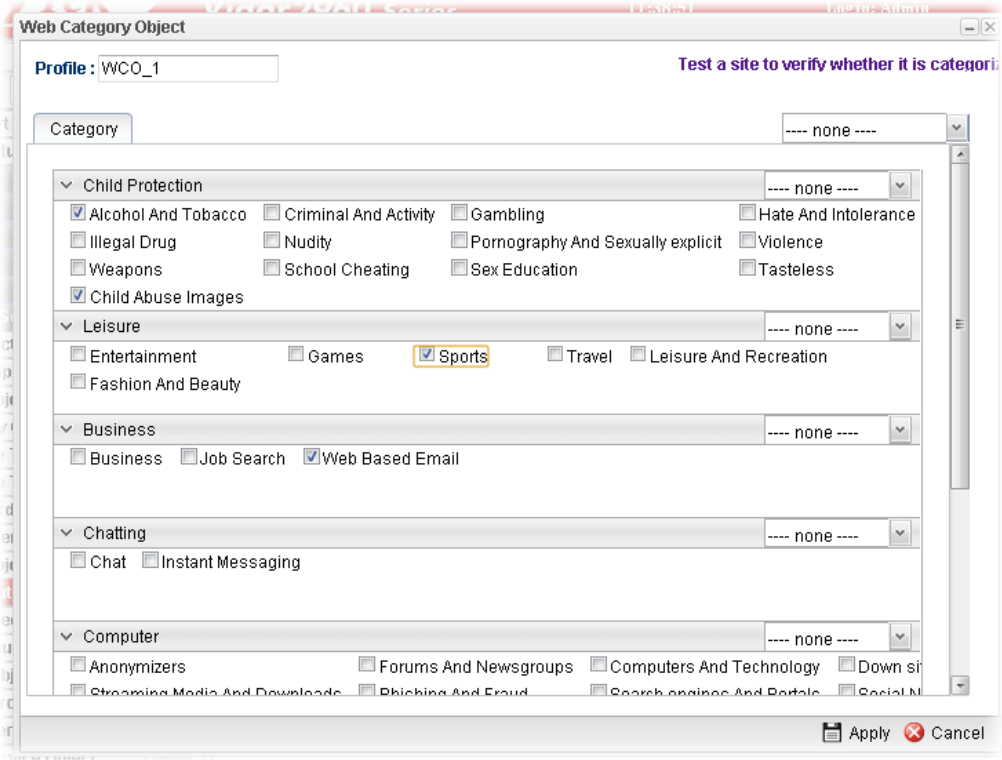
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (16) of the object profiles to be created.
Profile	Display the name of the object profile.
Child Protection	Display the items under certain category that you choose to block for protecting the children.
Leisure	Display the items under certain category that you choose to block.
Business	Display the items under certain category that you choose to block.
Chatting	Display the items under certain category that you choose to block.

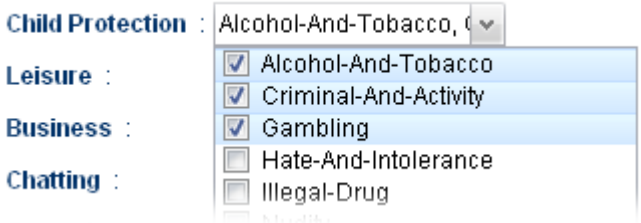
Item	Description
Computer	Display the items under certain category that you choose to block.
Other	Display the items under certain category that you choose to block.

How to create a new web category object profile

1. Open **Objects Setting>> Web Category Object** and click the **Web Category Object** tab**.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the web category object profile. The number of the characters allowed to be typed here is 10.
Child Protection	The web pages which are not suitable for children will be classified into different categories. Simply check the one(s) that you don't want the children to visit. 

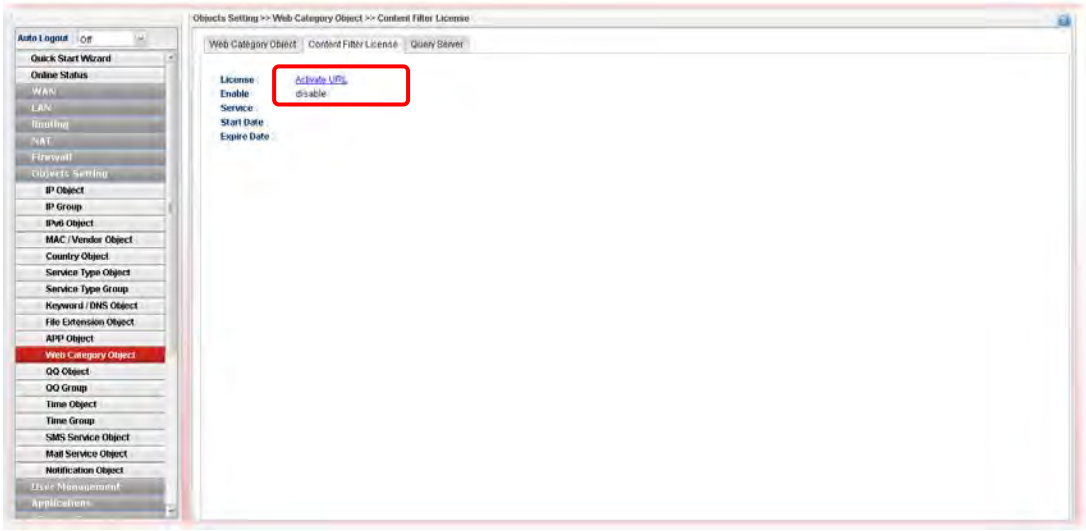
Leisure	Simply check the one(s) that you don't want the user to visit.
Business	Simply check the one(s) that you don't want the user to visit.
Chatting	Simply check the one(s) that you don't want the user to use for gossip with remote people.
Computer	Simply check the one(s) that you don't want the user to visit.
Other	Simply check the one(s) that you don't want the user to visit.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.

5. A new Web Category Object profile has been created.

4.6.11.2 Content Filter License

Move your mouse to the link of **Activate URL** and click it. The system will guide you to access into MyVigor website.

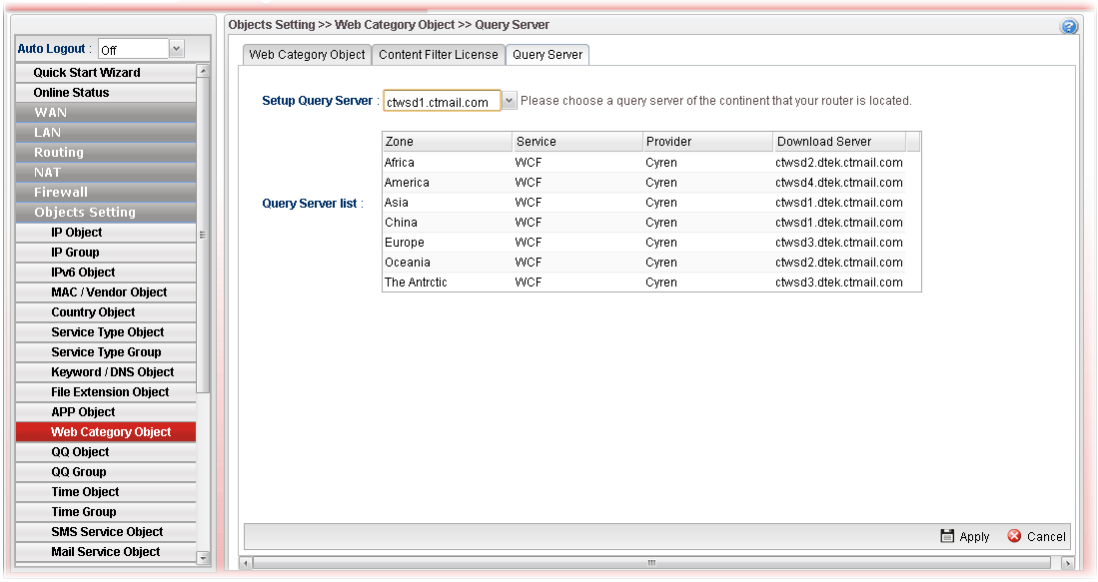


After finishing the activation for the trial version of WCF, remember to purchase "Silver Card" for WCF service from your DrayTek dealer or distributor.

4.6.11.3 Query Server

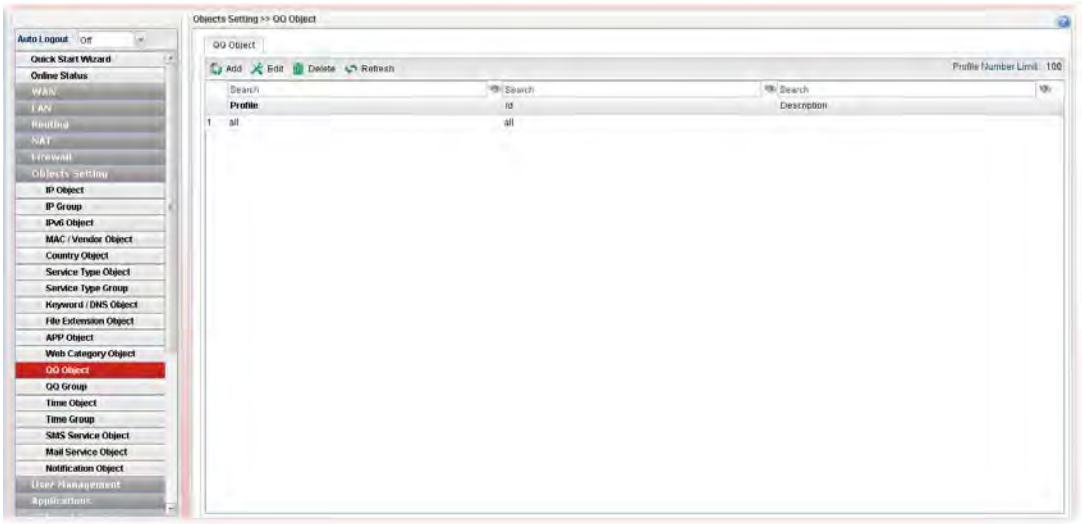
It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.

> Note: Due to the location difference, the response time for each query server will be different and influence the effect of WCF.



4.6.12 QQ Object

Note: This page is designed for Chinese IM "Tencent QQ" users (especially for China) only. For people who do not use QQ, skip this section.



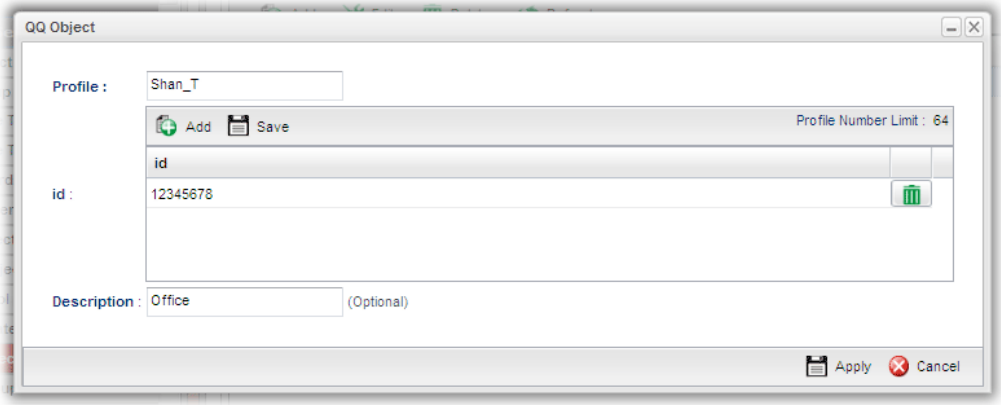
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.

Profile Number Limit	Display the total number (16) of the object profiles to be created.
Profile	Display the name of the QQ object profile.
id	Display the account name of the QQ object profile.
Description	Display a brief explanation of the QQ object profile.

How to create a new QQ object profile

1. Open **Objects Setting>> QQ Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



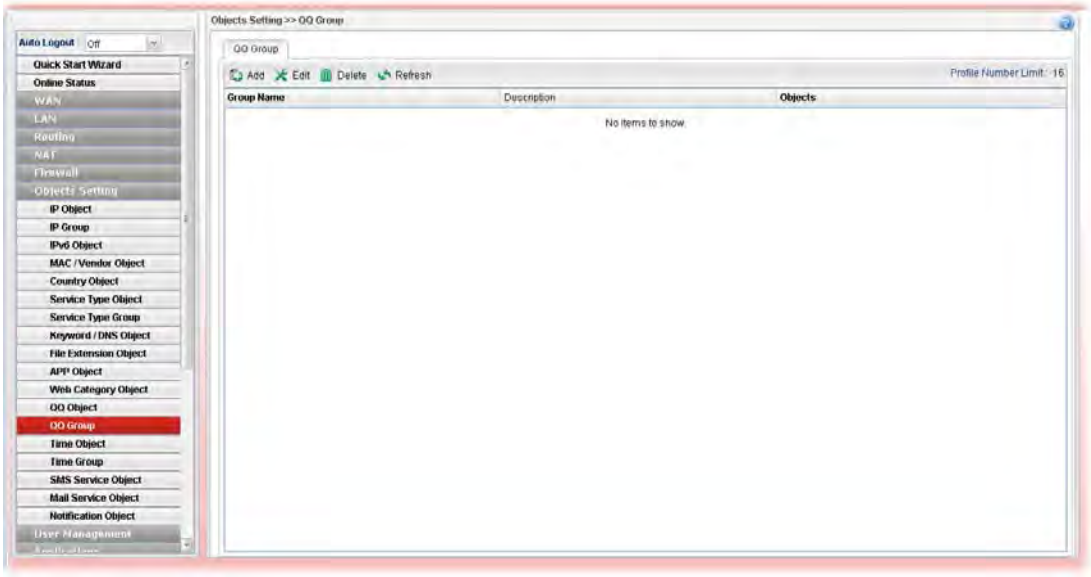
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the QQ object profile. The number of the characters allowed to be typed here is 10.
id	Create the account name for such QQ object profile. **Add** – Click this button to add a new account. **Save** – Click this button o save the new account. - Click this button to remove the selected account.
Description	Type a brief explanation for the QQ object profile.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new QQ Object profile has been created.

4.6.13 QQ Group

This page allows you to group several QQ object profiles.

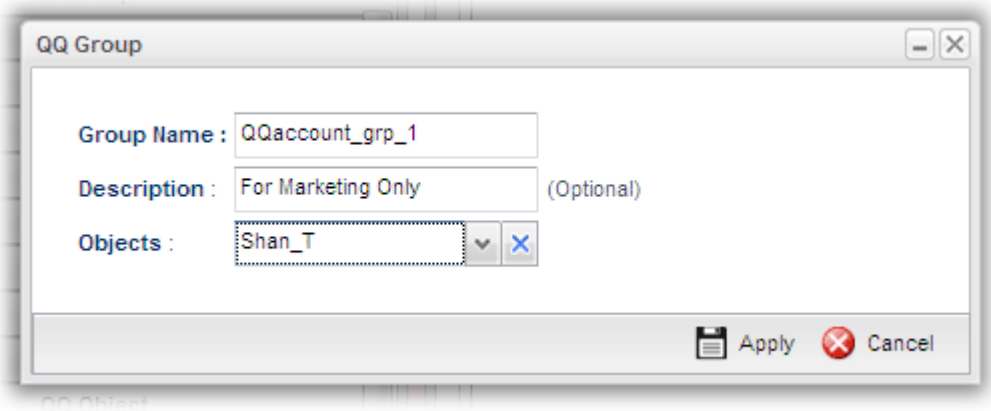


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (16) of the object profiles to be created.
Group Name	Display the name of the group.
Description	Display the brief explanation for such group.
Objects	Display the objects selected by such group.

How to create a new QQ group profile

1. Open **Objects Setting>> QQ Group.**
2. Simply click the **Add** button.
3. The following dialog will appear.



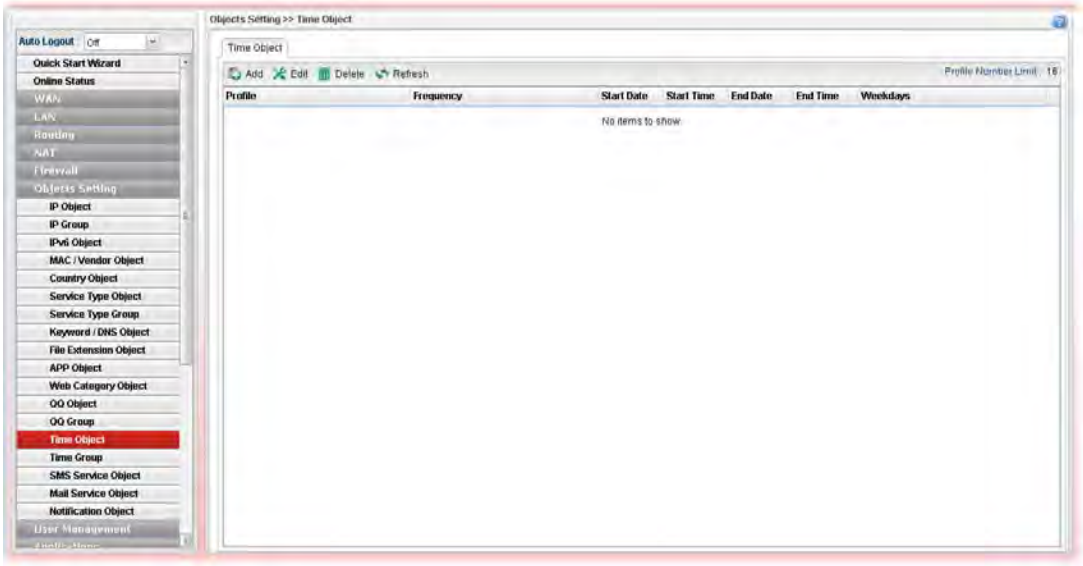
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the time group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to select the object profiles under such group. All the available objects that you have added on **Objects Setting>>QQ Object** will be seen here. To clear the selected one, click to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new QQ group profile has been created.

4.6.14 Time Object

You 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, e.g., Firewall.

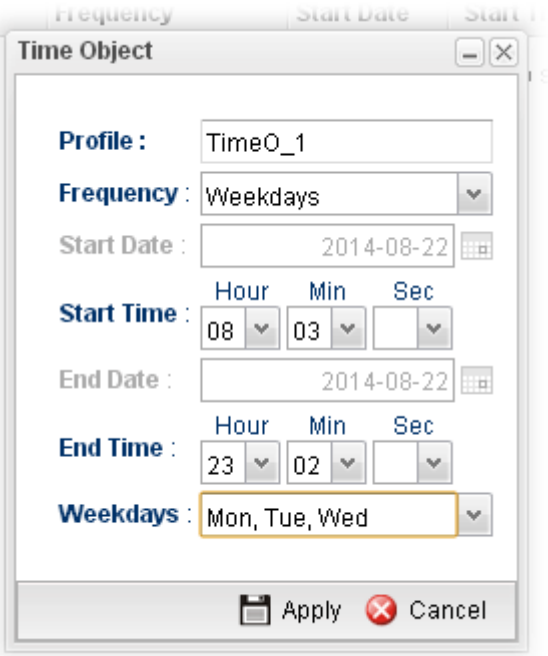


Each item will be explained as follows:

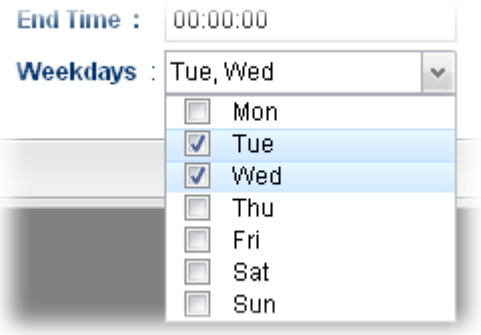
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (16) of the object profiles to be created.
Profile	Display the name of the time object profile.
Frequency	Display the duration (or period) of the time object profile.
Start Date	Display the starting date of the time object profile.
Start Time	Display the starting time of the time object profile.
End Date	Display the ending date of the time object profile.
End Time	Display the ending time of the time object profile.
Weekdays	Display the frequency of such time object profile.

How to create a new time object profile

1. Open **Objects Setting>> Time Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the time object profile. The number of the characters allowed to be typed here is 10.
Frequency	Specify how often (Weekdays or Once) the schedule will be applied.
Start Date	Specify the starting date of the time object profile.
Start Time	Specify the starting time of the time object profile.
End Date	Specify the ending date of the time object profile.
End Time	Specify the ending time of the time object profile.
Weekdays	Specify which days in one week should perform the schedule. 

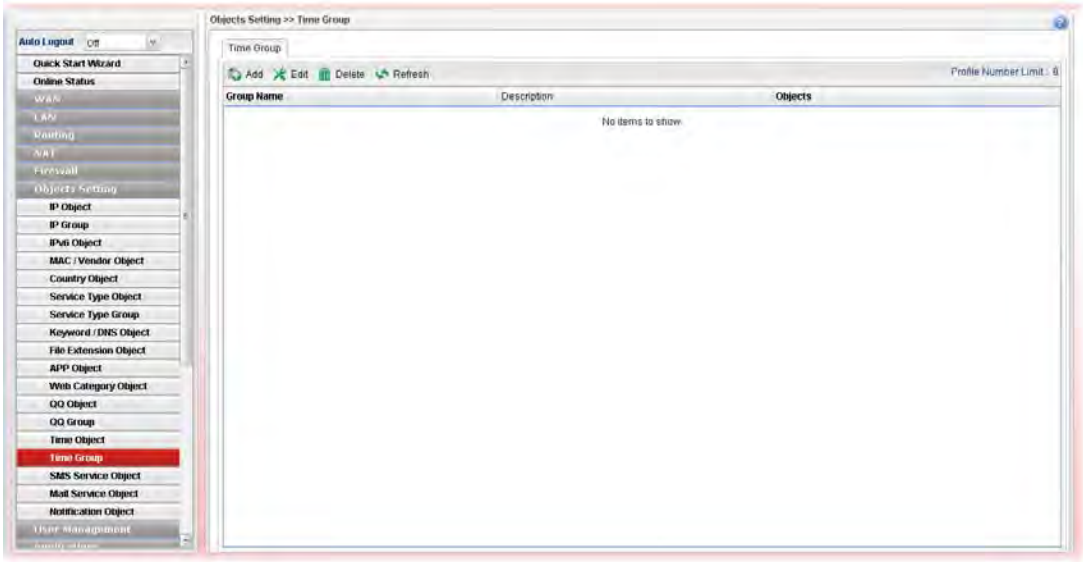
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.

5. A new Time Object profile has been created.

4.6.15 Time Group

This page allows you to group several time object profiles.

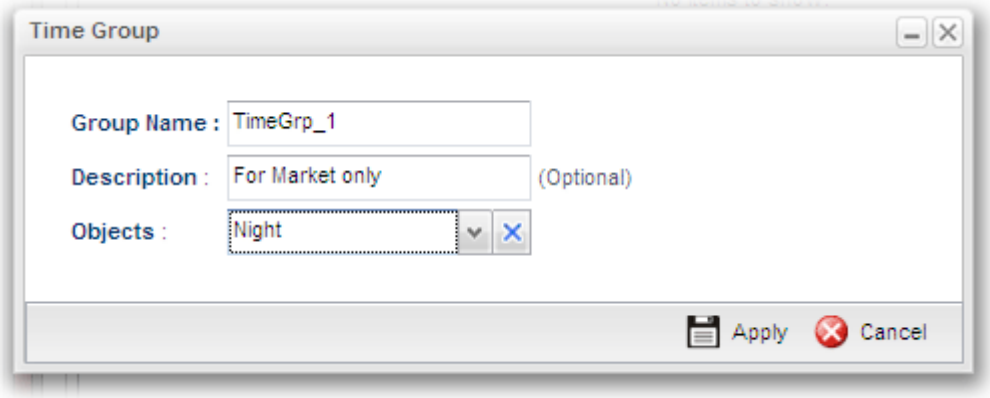


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Group Name	Display the name of the group.
Description	Display the brief explanation for such group.
Objects	Display the time objects selected by such group.

How to create a new time group profile

1. Open **Objects Setting>> Time Group.**
2. Simply click the **Add** button.
3. The following dialog will appear.



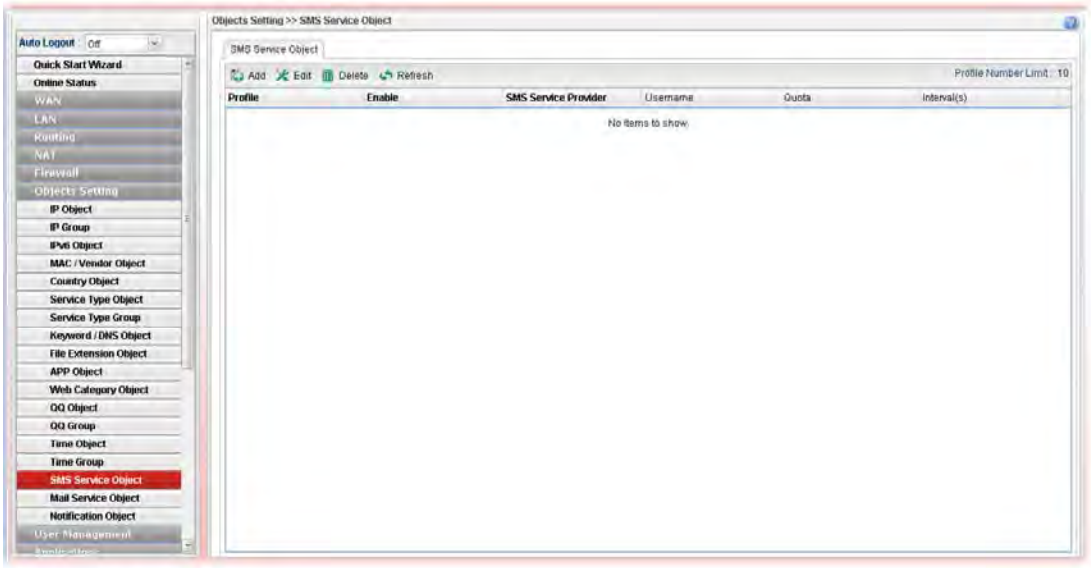
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the time group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the time object profiles under such group. All the available time objects that you have added on **Objects Setting>>Time Object** will be seen here.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new time group profile has been created.

4.6.16 SMS Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

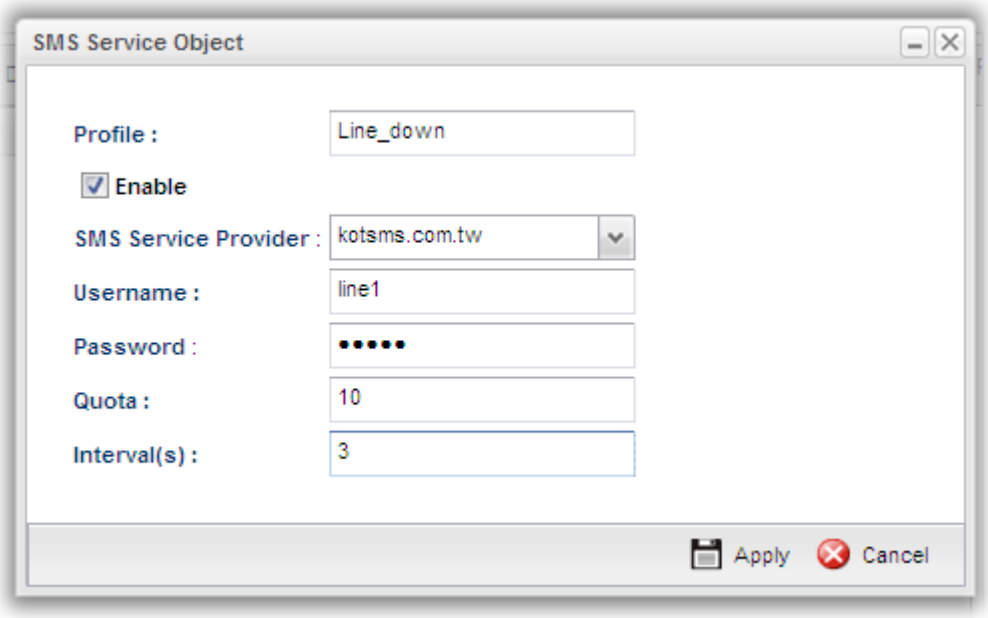


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (10) of the object profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
SMS Service Provider	Display the service provider which offers SMS service.
Username	Display the user name that the sender can use to register to selected SMS provider.
Quota	Display the number of the credit that you purchase from the service provider
Interval(s)	Display the time interval for sending the SMS.

How to create a new SMS service profile

1. Open **Objects Setting>> SMS Service Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

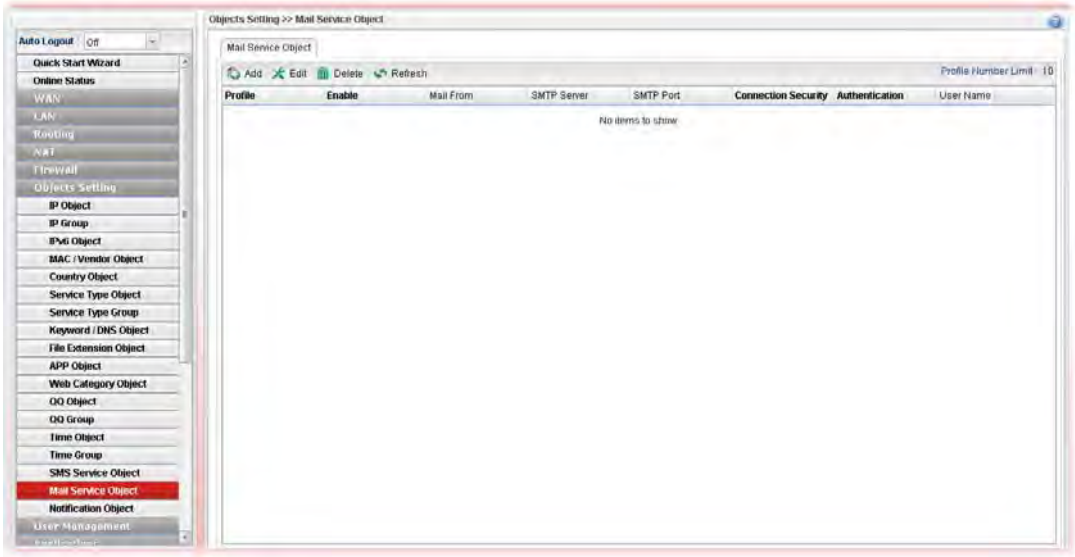
Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.
Enable	Check this box to enable such profile.
SMS Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Interval(s)	To avoid quota being exhausted soon, type time interval for sending the SMS.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.

5. A new SMS object profile has been created.

4.6.17 Mail Service Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.



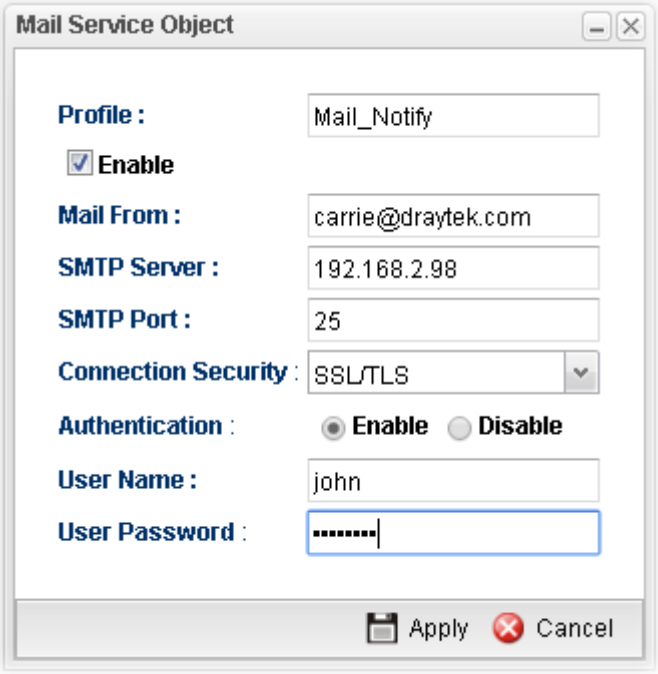
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Mail From	Display the mail address of the sender.
SMTP Port	Display the port number used for the SMTP service.
SMTP Server	Display the IP address of the SMTP Server
SSL/TLS	Display the status of SSL/TLS service.
Authentication	Enable means such profile must be authenticated by the

Item	Description
	server. Disable means such profile will not be authenticated by the server.
User Name	Display the name used for authentication.

How to create a new mail service profile

1. Open **Objects Setting>> Mail Service Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.
Enable	Check this box to enable such profile.
Mail From	Type the e-mail address of the sender.
SMTP Server	Type the IP address of the mail server.
SMTP Port	Type the port number for SMTP server.
Connection Security	Choose SSL/TLS or StartTLS to enable the service for connection security. Or, use the default setting, Disable.
SSL/TLS	Click the **Enable** button to enable service.

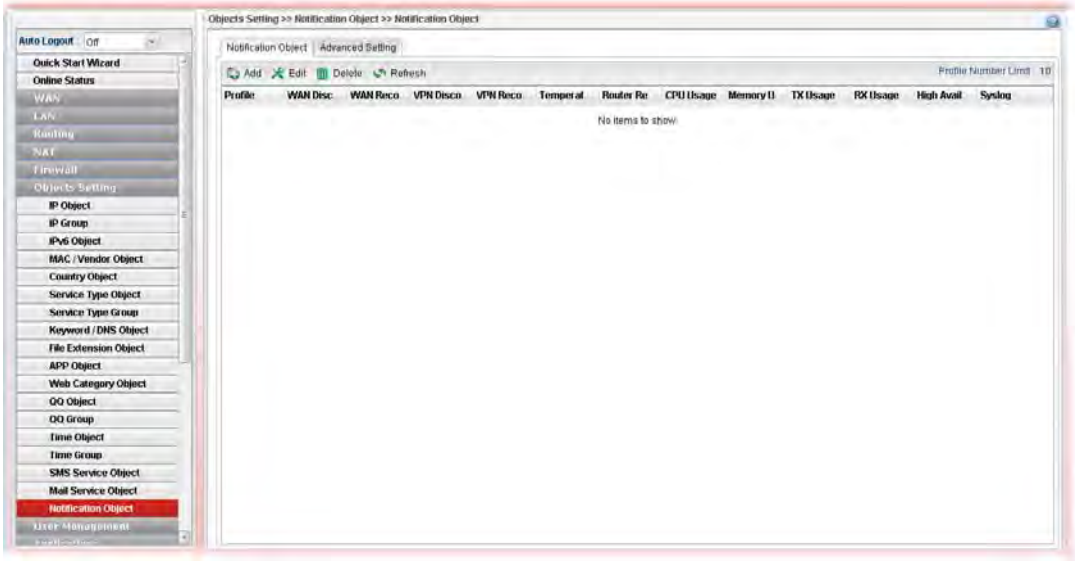
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Click the **Enable** button to enable the function. **User Name** – Type a name for authentication. The maximum length of the name you can set is 31 characters. **User Password** – Type a password for authentication. The maximum length of the password you can set is 31 characters.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new mail service object profile has been created.

4.6.18 Notification Object

This page allows you to set ten profiles which will be applied in **Application>>SMS/Mail Alert Service**.

4.6.18.1 Notification Object



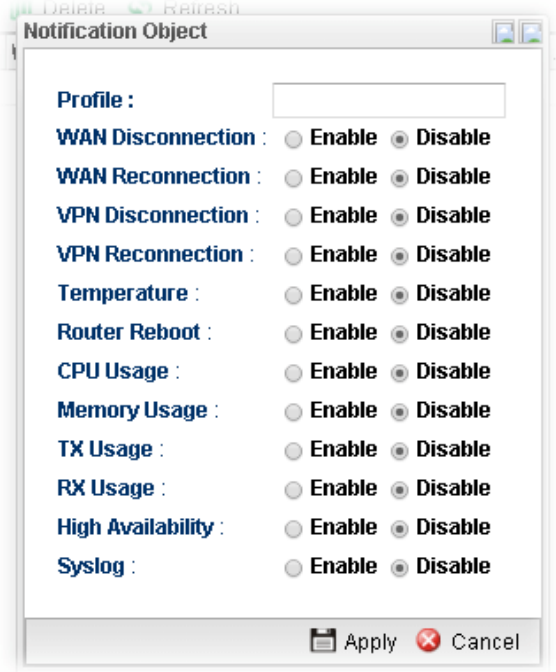
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.

Item	Description
Refresh	Renew current web page.
Profile Number Limit	Display the total number (10) of the object profiles to be created.
Profile	Display the name of the profile.
WAN Disconnection	Display if such function is enabled or disabled.
WAN Reconnection	Display if such function is enabled or disabled.
VPN Disconnection	Display if such function is enabled or disabled.
VPN Reconnection	Display if such function is enabled or disabled.
Temperature	Display if such function is enabled or disabled.
Router Reboot	Display if such function is enabled or disabled.
Syslog	Display if such function is enabled or disabled.

How to create a new notification profile

1. Open **Objects Setting>> Mail Service Object.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

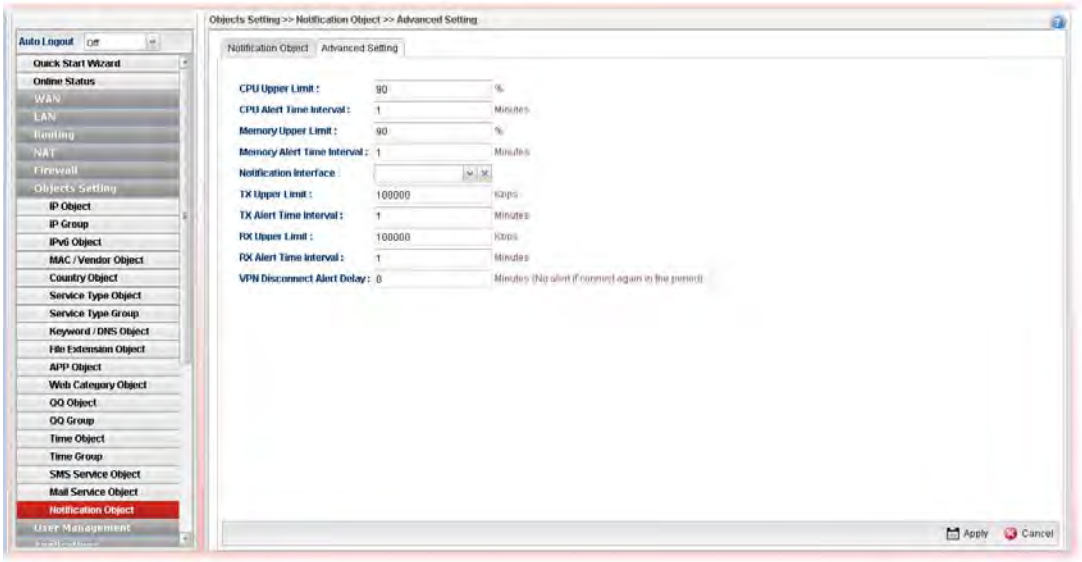
Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters. There are several situations to be monitored by such profile.

WAN Disconnection	**Enable** – When disconnection happened to WAN interface, the router system will send the alert message to the recipient.
WAN Reconnection	**Enable** - When reconnection happened to WAN interface, the router system will send the alert message to the recipient.
VPN Disconnection	**Enable** – When disconnection happened to a VPN tunnel, the router system will send the alert message to the recipient.
VPN Reconnection	**Enable** - When reconnection happened to a VPN tunnel, the router system will send the alert message to the recipient.
Temperature	**Enable** - When the temperature is out of range, the router system will send the alert message to the recipient.
Router Reboot	**Enable** - When the router reboots, the router system will send the alert message to the recipient.
CPU Usage	**Enable** – When the CPU usage reaches a certain value, the router system will send the alert message to the recipient.
Memory Usage	**Enable** – When the memory usage reaches a certain value, the router system will send the alert message to the recipient.
TX Usage/RX Usage	**Enable** – When TX/RX usage reaches a certain value, the router system will send the alert message to the recipient.
High Availability	**Enable** – When such Vigor router becomes the “Master” device in the application of HA, the router system will send the alert message to the recipient.
Syslog	**Enable** – Such notification will be recorded in Syslog.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new notification object profile has been created.

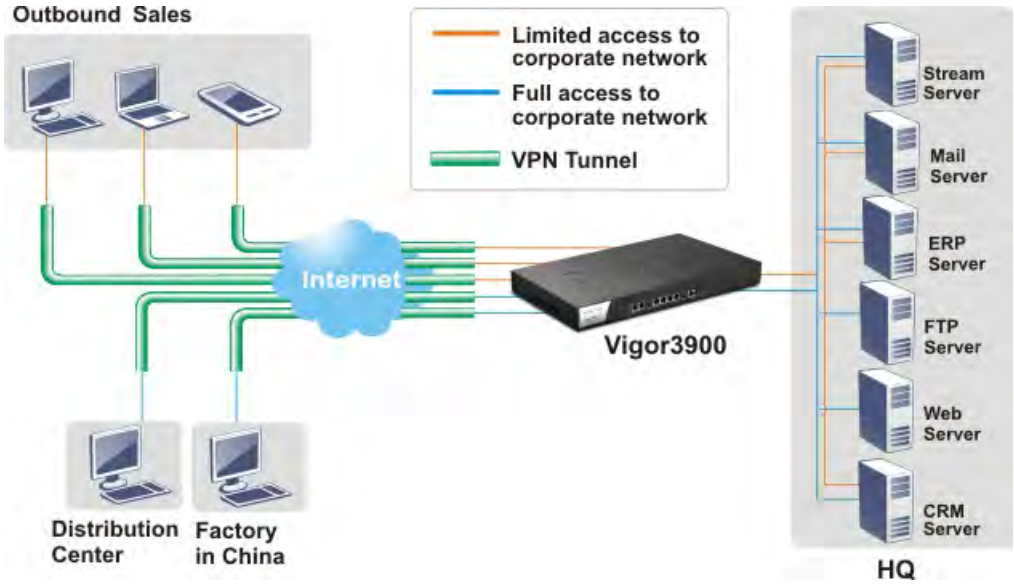
4.6.18.2 Advanced Setting

Such page is used to set the limit value for CPU, Memory, TX / RX. When CPU, Memory, TX / RX usage reaches the threshold, the router system will send the alert message to the recipient.

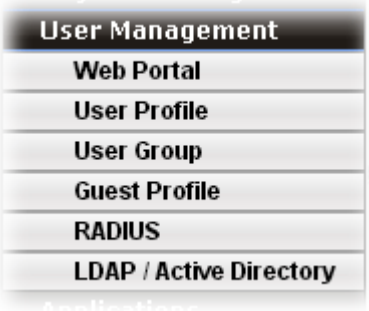


4.7 User Management

User Management can manage all the accounts (user profiles) to connect to Internet via different protocols.



Below shows the menu items for User Management:



4.7.1 Web Portal

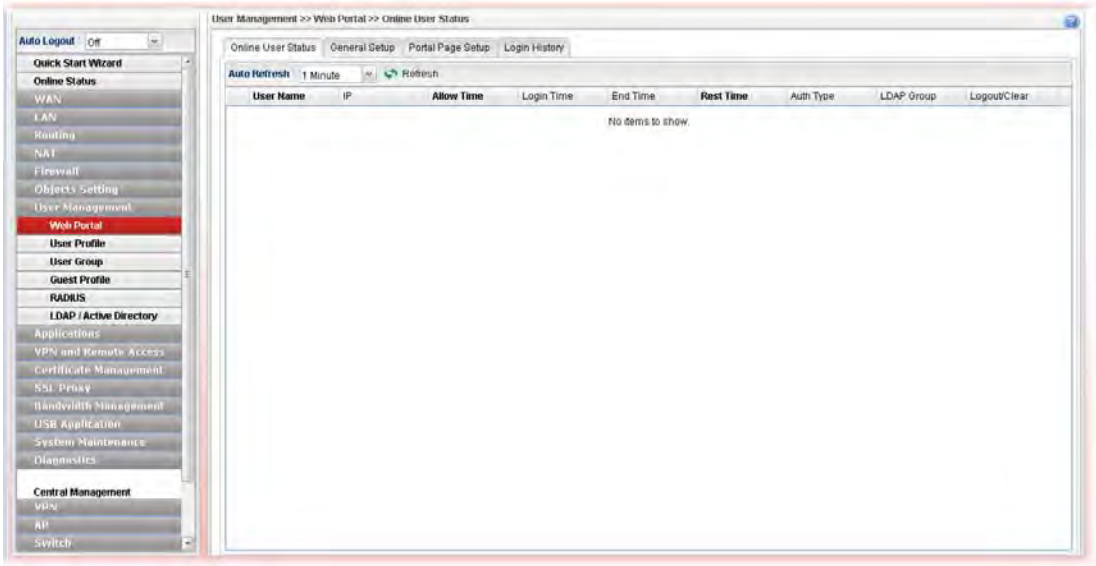
Web Portal is a gateway which organizes the network access of LAN hosts. The identity of LAN host can be recognized by web portal mechanism and then be managed for functions like firewall or load balance.

This page can determine the general rule for the users controlled by User Management. The mode selected in this page will influence the contents of the filter rule(s) applied to every user.

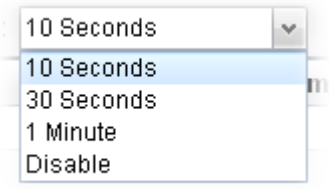
4.7.1.1 Online User Status

The **Online User Status** is a monitoring tool which only works after you choose **HTTP** or **HTTPS** as the **Mode** setting on **General Setup** page of **User Management>>Web Portal**.

Refer to section 4.7.1.2 General Setup to get more detailed information of setting web portal.

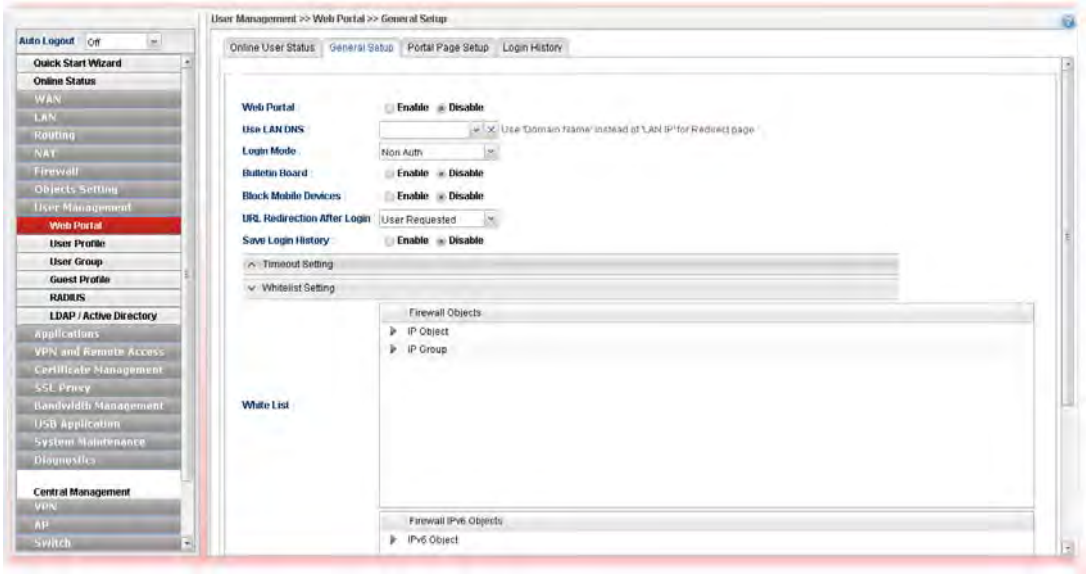


Available parameters will be explained as follows:

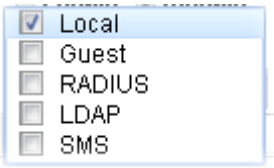
Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked. 
User Name	Display the name information for the user who logs into the WUI of Vigor3900.
IP	Display the IP address of the user who logs into the WUI of Vigor3900.
Allow Time	Display the total network connection time allowed for the log-in user.
Login Time	Display the starting time of the network connection.
End Time	Display the ending time of the network connection.
Rest Time	Display the rest time of the network connection.
Auth Type	Display the authentication type (local, RADIUS, LDAP, Login Disable, Guest) used by such user.
LDAP Group	Display the LDAP group used by such user.
Logout/Clear	It is a button which is used to disconnect the connection manually.

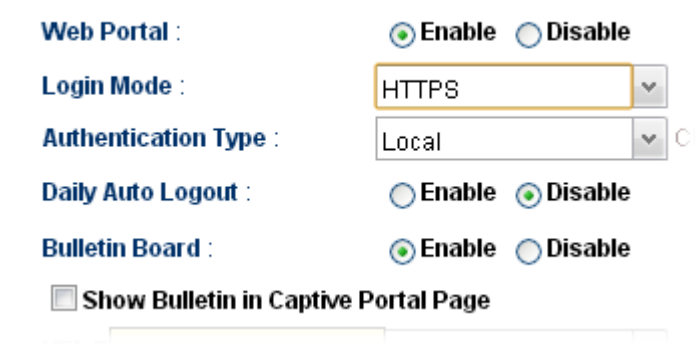
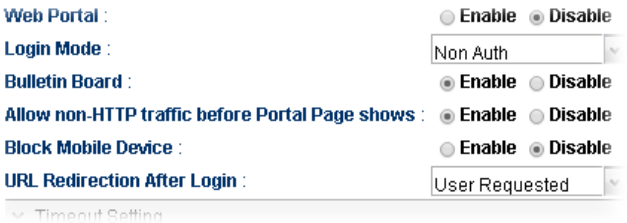
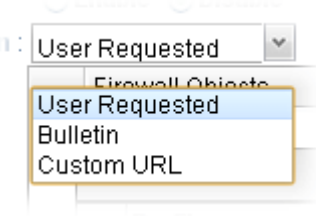
4.7.1.2 General Setup

This page configures the main settings of web portal function**.**



Available parameters will be explained as follows:

Item	Description
Web Portal	Click **Enable** to enable such function.
Use LAN DNS	Choose one of the LAN DNS profile
Login Mode	There are several login modes offered here for you to choose. **Non Auth** – Authentication is not required. **HTTP/HTTPS**- If you choose such mode, the user can access into Vigor router by HTTP or HTTPS.
HTTPS Redirect	This option is available when the Login Mode is set as **HTTP** or **HTTPS**. **Enable** – Only HTTPS sessions will be processed by Vigor router when multiple users access into Vigor router via the web portal.
Authentication Type	This option is available when the **Login Mode** is set as **HTTP** or **HTTPS**. Note that the authentication sequence adopted by the system will be Local first, Guest second, RADIUS third and LDAP the last. However, if you check SMS, the router will authenticate the user with SMS rules and the others (Local, Guest, RADIUS, LDAP) at the same time.  **LDAP Profiles -** It is available when **LDAP** is selected as **Authentication Type**. You have to specify one profile (defined in User Management>>LDAP/Active Directory) from the drop down list for LDAP authentication.

Bulletin Board	**Disable –** The function of Bulletin Board is disabled. **Enable –** The function of Bulleting Board is enabled. The message on the Bulleting Board will be displayed on the screen when the user logs into the web user interface of Vigor router. ● **Show Bulletin in Captive Portal Page –** It is available when **Bulletin Board** is enabled and **HTTP/HTTPS** is selected as **Login Mode**. It is used to determine showing bulletin in web portal login page or not.  ● **Allow non-HTTP traffic before Portal Page shows –** It is available when **Bulletin Board** is enabled and **Non Auth** is selected as **Login Mode**. When it is enabled, non-HTTP traffic is allowed before the portal page appears. 
Block Mobile Device	**Enable –** Vigor router will detect and block if there is any mobile device trying to access into Internet via Vigor router. **Alert Message** – If a mobile device is detected, a warning message (typed in this field) will be displayed on the screen of mobile device. The default content is “Mobile Device Detected”.
URL Redirection After Login	 **User Requested –** After passed the authentication made by Vigor router, the user will be redirected to original requested web page. **Bulletin** – If it is selected, users will be forced to see the information displayed on bulletin after passing through web portal.

	Custom URL - Any user who wants to access into Internet through this router will be forcefully redirected to the URL specified here first no matter what URL he types. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit. ● **Custom URL** – Type the URL of specified web page for redirection if **Custom URL** is selected as **URL Redirection After Login**.
SMS Setting – It is available when **SMS** is selected as the **Authentication Type**. When a user wants to log into Internet, he/she will be asked for passing the authentication process by using the applied validation code. The following settings are used to specify will be sent to specified users through SMS.	
SMS Provider	Use the drop down list to specify the service provider which offers SMS service.
SMS Button Name	It is a button with short message which will appear to remind the user that SMS is allowed to get username and password for accessing into Vigor router.
SMS resend interval	Type a time interval in this field. The advantage of such feature is that SMS will not be sent frequently within a short time and cost too much.
SMS Content	Type the content of the SMS. The default URL encode format for SMS is “UTF-8”. Before typing the content, make sure the encode format that the SMS server offers. If it does not support “UTF-8”, transcoding shall be done first. If you have any question, contact the SMS service provider.
Customized Field 1/2/3	The administrator can collect data (such as name, e-mail, address, age, job and etc.) offered by users who ask for validation code to access into Internet. There are three fields allowed for acquiring data coming from mobile user. Each field can be enabled / disabled separately. **Enable** – Make the title (defined in Customized Field 1/2/3 Label) be seen on the mobile phone. When the field is enabled, the mobile user must offer the data related to the defined label to get the validation code. **Disable** – The title (defined in Customized Field 1/2/3 Label) will not be shown on the mobile phone. The mobile user can get the validation code after typing the phone number and click the confirmation button (which is defined in SMS Button Name). **Enable and Required** - The mobile user **MUST** type the phone number and fill in all the required information on the screen and click the confirmation button (which is defined in SMS Button Name). Then Vigor router will send SMS of validation code to the mobile user.
Customized Field 1/2/3 Label	Type a brief text as the title for the above customized field.
Log File Limit	Information collected from mobile users (through the

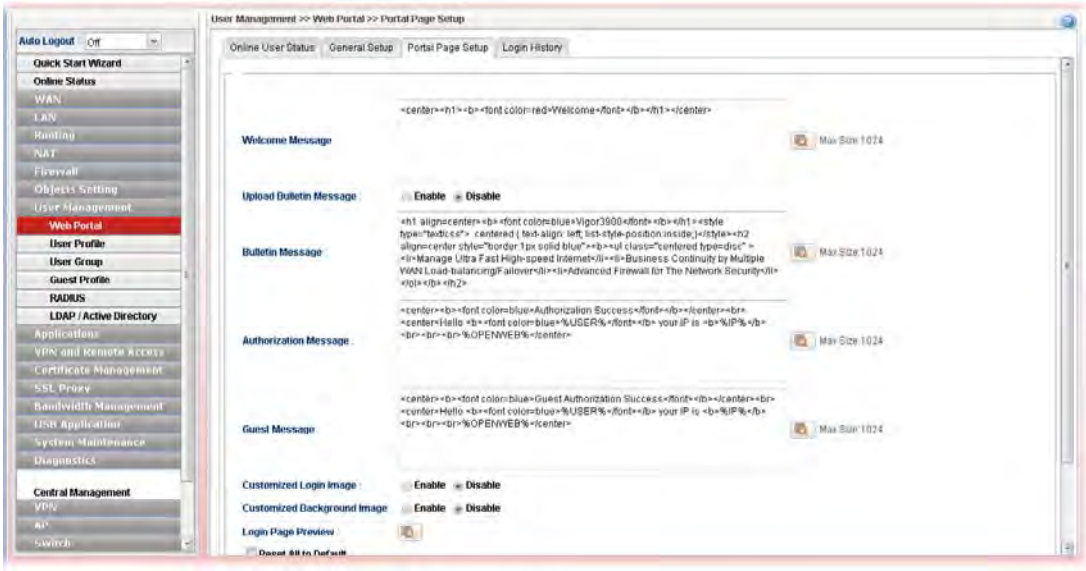
	request of validation code) will be stored in a log file. It is used to restrict the maximum size of the log file.
Export Log File	The log of SMS can be exported as a file with the file format of ".csv".
Timeout Setting	
Daily Logout	**Enable** - Force the online user logging out the web user interface of Vigor router everyday. ● **Daily Time to Logout** - It is available when **Daily Logout** is enabled. Type that time setting (HH:MM) for the router to force online user leaving Vigor router. ● **Fully Recharge Time Quota After….** - It is available when **Daily Logout** is enabled. The time quota of all local users will be recharged whenever Daily Logout is executed.
Period Logout	**Enable** - Force the online user logging out the web user interface of Vigor router after passing a period of time. ● **Period Time to Logout** - It is available when **Period Logout** is enabled.
Idle Logout	**Enable** - Force the online user logging out the web user interface of Vigor router when the router is idle. Enable such feature if time quota is used. ● **Idle Time(min)** – Set a time period. When the time is up, Vigor router will terminate the network connection for the online user.
Whitelist Setting	
White List	Select the source IP objects/groups that are ignored by web portal function.
White List IPv6	Select the source IP objects/groups that are ignored by web portal function.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

Note: To turn off the web portal function, disable Login Mode and Bulletin Board at the same time.

4.7.1.3 Portal Page Setup

This page allows you to configure specified messages (HTML-supported) in web portal pages, and shows them to users accessing into Internet via web portal.

No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal



Available parameters will be explained as follows:

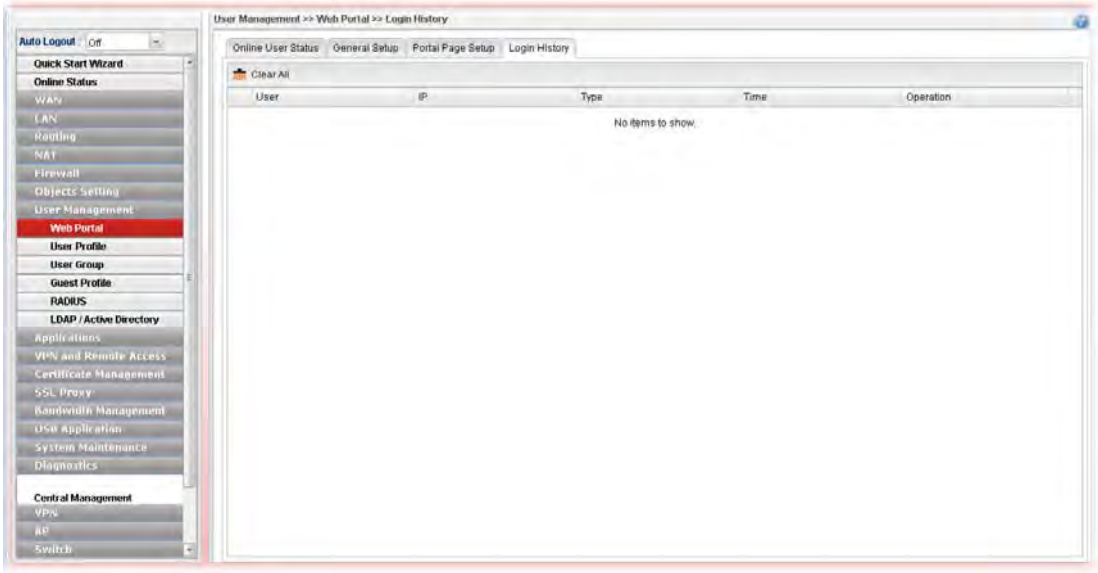
Item	Description
Welcome Message	Type words or sentences here. The message will be displayed on the top of the login page.
Upload Bulletin Message	**Upload Selected File** - It is available when **Enable** is selected in **Upload Bulletin Message**. Choose a file to upload to Vigor3900.
Bulletin Message	It is available when **Disable** is selected in **Upload Bulletin Message**. The bulletin message is shown on login page or authorization page. In login page, it can be disabled by Show Bulletin In Login Page.
Authorization Message	The welcome message is shown in authorization page which is the page after a user passing the authentication successfully.
Guest Message	A welcome message is shown on the screen after the guest passing the authentication successfully.
Customized Login Image	Specify an image file which will be displayed on the login page when a user or guest tries to access into Internet. **Upload Login Image** – Choose a file to upload to Vigor3900. It is useful for advertisement.
Customized Background Image	Specify an image file which will be display on the login page as a background. It is useful for advertisement. **Upload Background Image** – Choose a file to upload to Vigor3900.
Login Page Preview	Click it to have a preview of login page (including welcome message, and bulletin message).
Reset All to Default	Reset the above message fields to default settings. Check the box and then press **Apply**.
Apply	Click it to save the configuration.

Item	Description
Cancel	Click it to discard the settings configured in this page.

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

4.7.1.4 Login History

This page shows the history that wireless client(s) access into Vigor3900.



4.7.2 User Profile

This function allows to configure all accounts (user profiles) in Vigor3900, including PPTP/L2TP/SSL/PPPoE, System user, and so on.

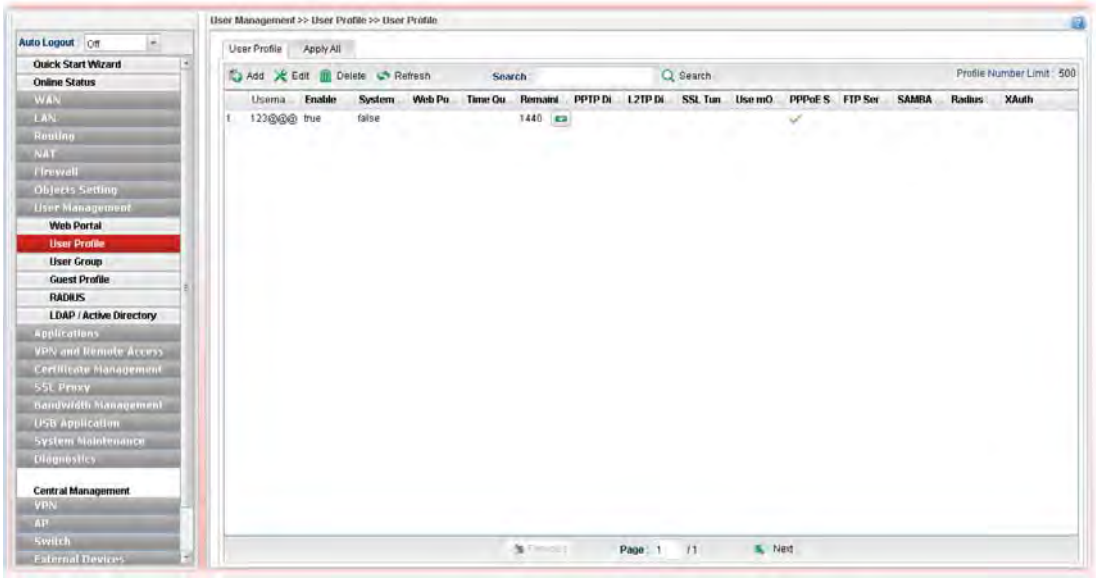
4.7.2.1 User Profile

User profile is used to configure different authorities, including web portal, VPN dial-in, PPTP/L2TP/SSL/PPPoE server, system administration, etc., for different users.

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

There are two benefits that SSL VPN provides:

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



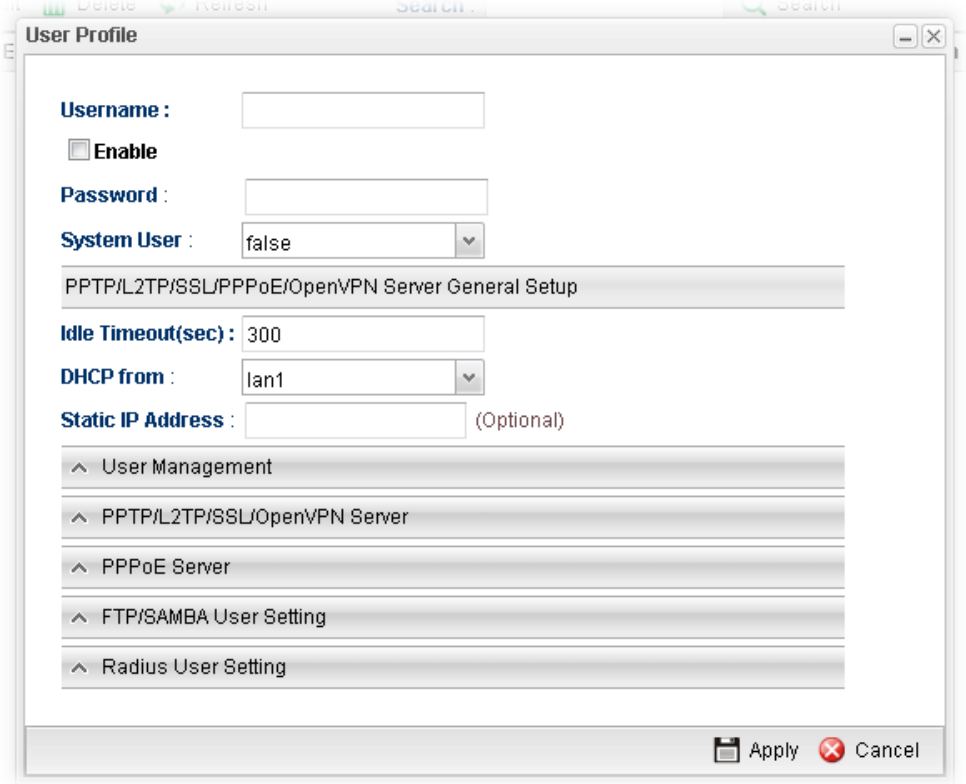
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the user profiles to be created.
Username	Display the name of the user.
Enable	Display the status of the profile. False means disabled; True means enabled.
System User	Display the status of the System User. False means disabled; True means enabled.
Allow Web Portal Login	Display the status (Enable/Disable) of the account usage for web portal login.
Time Quota	Display the status (Enable/Disable) of time quota mechanism for web portal use.
Remaining Time	Display the remaining time for the user profile. **Recharge** – It can recharge the remaining time quota of the user on-the-fly (will not log out online users)**.**
PPTP Dial-in	Display the status of PPTP connection for such user profile.
L2TP Dial-in	Display the status of L2TP connection for such user profile.
SSL Tunnel	Display if SSL Tunnel is activated (enable or disable) or

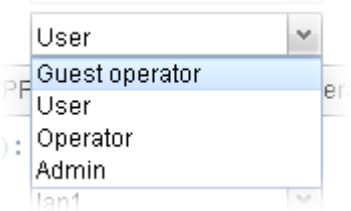
Item	Description
	not.
Use mOTP	Display if mOTP is activated (enable or disable) or not.
Allow PPPoE Server Login	Display the status of PPPoE connection for such user profile. (enable or disable)
PPPoE Time Quota(min)	Display the current PPPoE time quota usage portion for such user.
PPPoE Traffic Quota(MB)	Display the current PPPoE traffic quota usage portion for such user.
Allow FTP Server Login	Display if FTP Server Login is activated (enable or disable) or not.
Allow SMABA Server Login	Display if **SMABA** Server Login is activated (enable or disable) or not.
Allow Radius Server Login	Display if **Radius** Server Login is activated (enable or disable) or not.

How to create a new User Profile

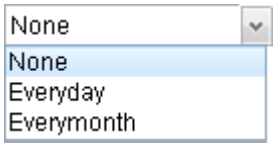
1. Open **User Management>>User Profile.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Username	Type a name for such user profile (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the Username specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Enable	Check this box to enable such profile.
Password	Type a password for such profile (e.g., *lug123*, *wug123*,*wug456*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.
System User	Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router. **False –** Choose it to disable the function of System User. Such user profile does not have the right to operate the router's function. **True –** Choose it to enable the function of System User. **Privilege Level –** If true is selected for **System User**, you have to specify the privilege level (Guest operator/ User/Operator/Admin) for such profile.  **Admin** has the greatest authority for router operation; **Guest operator** has the smallest authority for router operation.
PPTP/L2TP/SSL/PPPoE/OpenVPN Server General Setup	
Idle Timeout (sec)	If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.
DHCP from	Choose a LAN profile for DHCP server IP dispatching. Remote clients using this profile to do PPTP/L2TP dial-in will be assigned IP addresses according to this DHCP pool.
Static IP Address	Type an IP address for such user profile which accesses Internet with PPTP/L2TP connection.
User Management	

Web Portal Login	**Enable** – Click it to enable web portal login with such profile. **Disable** – Click it to disable the option.
Time Quota	**Enable** – Click it to enable time quota function. ● **Set Time Quota (min)** – Type the time value. ● **Remaining Time** – Display the remaining time for the user profile. **Disable** – Click it to disable the function. **Note**: The range of Time Quota is 1~14400 minutes.
Max Simultaneous Login	It means the maximum online number of clients logging with this profile. The range is from 1 to 255. -1 means not limit; 0 means No access.
Logout Earliest User	Force the earliest user to logout when exceeded the maximum number of online user setting. **Enable** – Click it to enable such function. **Disable** – Click it to disable such function.
PPTP/L2TP/SSL/OpenVPN Server	
PPTP Dial-in / L2TP Dial-in / SSL Tunnel	Click **Enable** to make network connection through PPTP/L2TP/SSL Tunnel protocol for users who access into Internet via such profile.
OpenVPN Dial-in	OpenPVN is a mechanism which is easy for users to build safe and reliable virtual network, even if the brand or model of router used by both ends are totally different. **Enable** – Click it to enable such function. **Disable** – Click it to disable such function.
XAuth / EAP	Click **Enable** to allow the remote user accessing into Internet via IPsec authentication. **Enable** – Click it to enable such function. **Disable** – Click it to disable such function.
Use mOTP	Click **Enable** to make the authentication with mOTP function. ● **mOTP PIN Code -** Type the code for authentication (e.g, 1234). ● **mOTP Secret -** Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Time Objects	Choose a time object or time objects for such user profile. Users in this profile can access into Vigor router within the time period defined by the selected time object.
SSL Proxy	It is available when **System User** is set with **false**. The web proxy over SSL will be applied for VPN. To clear the selected one, click to remove current object selections.

SSL Application (VNC)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (VNC) for applying into this profile. To clear the selected one, click to remove current object selections.
SSL Application (RDP)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (RDP) for applying into this profile. To clear the selected one, click to remove current object selections.
IP Address/Domain Name	Specify an IP address for remote dial-in VPN client. Client with such user profile can only use such IP or host name to access into such Vigor router. If not, the VPN connection is not allowed.
PPPoE Server	
PPPoE Server Login	Click **Enable** to activate related PPPoE configuration.
Quota Reset Frequency	It is used to configure the cycle time for PPPoE quota. Note that each time when the quota is reset, the value of Current Time Used/Current Traffic Quota will be reset to initial situation (0). **Everyday** – The quota for PPPoE will be reset every day. **Everymonth** – The quota for PPPoE will be reset every month. 
Time Quota (min)	Type a time quota for PPPoE connection. **Note**: The range of Time Quota is 1~14400 minutes.
Current Time Used (min)	Display the cumulative amount of time that the user used. **Reset -** Click it to reset the setting to default value (0).
Traffic Quota(MB)	It is used to set the maximum traffic (MB) for such user profile.
Current Traffic Quota (MB)	Display the cumulative amount of data traffic that the user used. **Reset -** Click it to reset the setting to default value (0).
MAC Binding	Specify a MAC address which is limited and used for such PPPoE account. **Enable –** Click it to enable the function. **MAC Address** – If MAC Binding is enabled, simply type the MAC address of the router in this field.
FTP/SAMBA User Setting	
FTP/SAMBA	Click **Enable** to allow the remote user accessing into

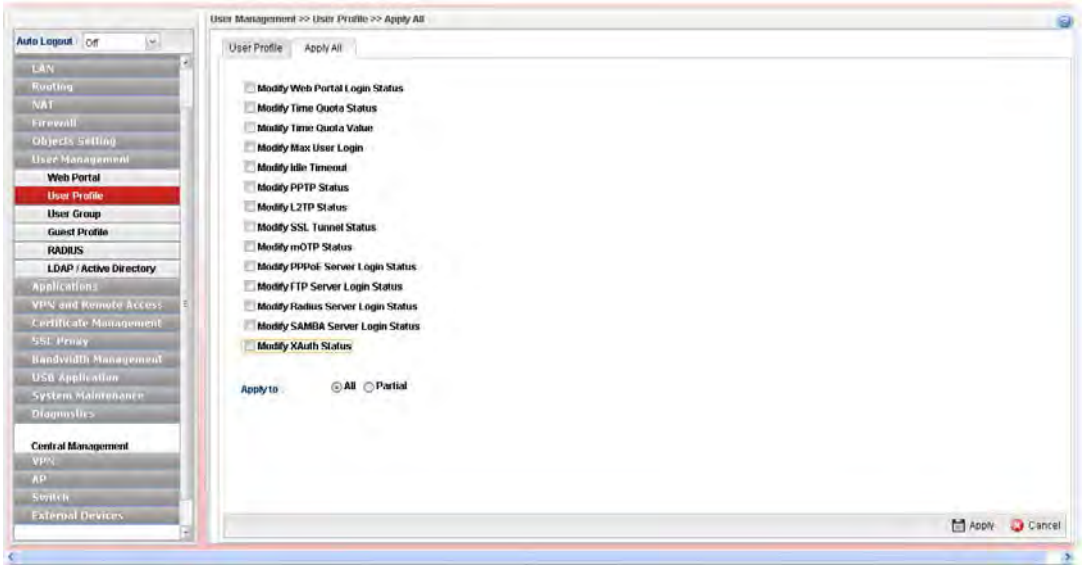
Server Login	Internet via FTP/SAMBA server.
Radius User Setting	
Radius Server Login	Click **Enable** to allow the remote user accessing into Internet via **Radius** server.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new User Profile has been created.

4.7.2.2 Apply All

This page allows you to modify many options for **ALL** user profiles in one apply operation. It is useful for administrator to edit the options of all users without opening profile one by one.

You can click **Apply** to save the settings and apply all of the modifications to all user profiles.



Available parameters are listed as follows:

Item	Description
Modify Web Portal Login Status	Check the box to configure detailed setting. **Enable –** Click it to enable the web portal login function for remote client.
Modify Time Quota Status	Check the box to configure detailed setting. **Enable –** Click it to enable the time quota function for all user profiles.
Modify Time Quota Value	Check the box to configure detailed setting. You have to check this box and type the time quota value in **Time Quota Value(min)**.
Modify Max User Login	-1 means not limit; 0 means No access.
Modify Idle Timeout	If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.
Modify PPTP Status /Modify L2TP Status /Modify SSL Tunnel Status	Check the box to configure detailed setting. **Enable –** Click it to enable the PPTP/L2TP/SSL tunnel network connection all user profiles.
Modify mOTP Status	Check the box to configure detailed setting. **Enable –** Click it to enable the mOTP function all user profiles.
Modify	Check the box to configure detailed setting.

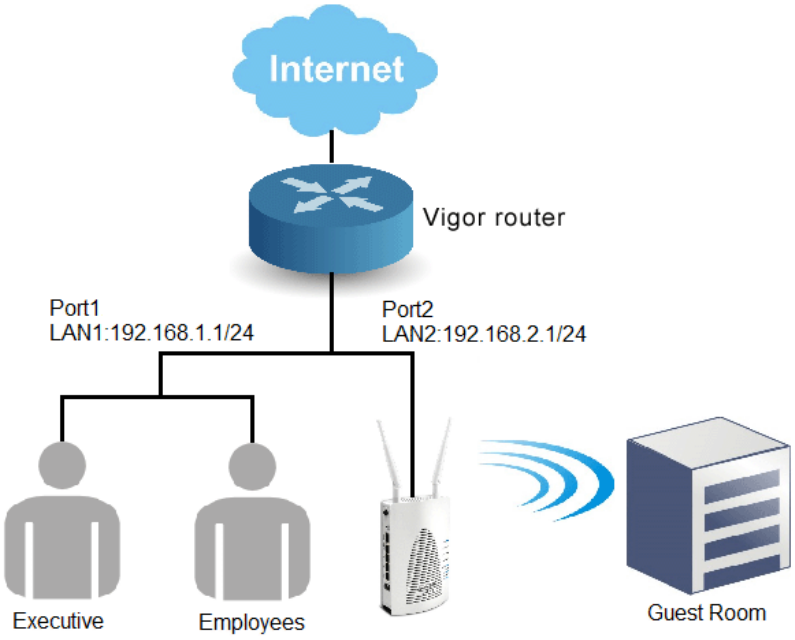
PPPoE/FTP/Radius Server Login	**Enable –** Click it to enable the PPPoE/FTP/Radius authentication function all user profiles.
Modify SAMBA Server Login Status	Check the box to configure detailed setting. **Enable –** Click it to enable the SAMBA server authentication function all user profiles.
Modify XAuth Status	Check the box to configure detailed setting. **XAuth -** Click **Enable** to enable the XAuth authentication function all user profiles.
Apply to	**All** – Apply all of the modifications to all user profiles. **Partial** – Apply all of the modifications to specified user profile.

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

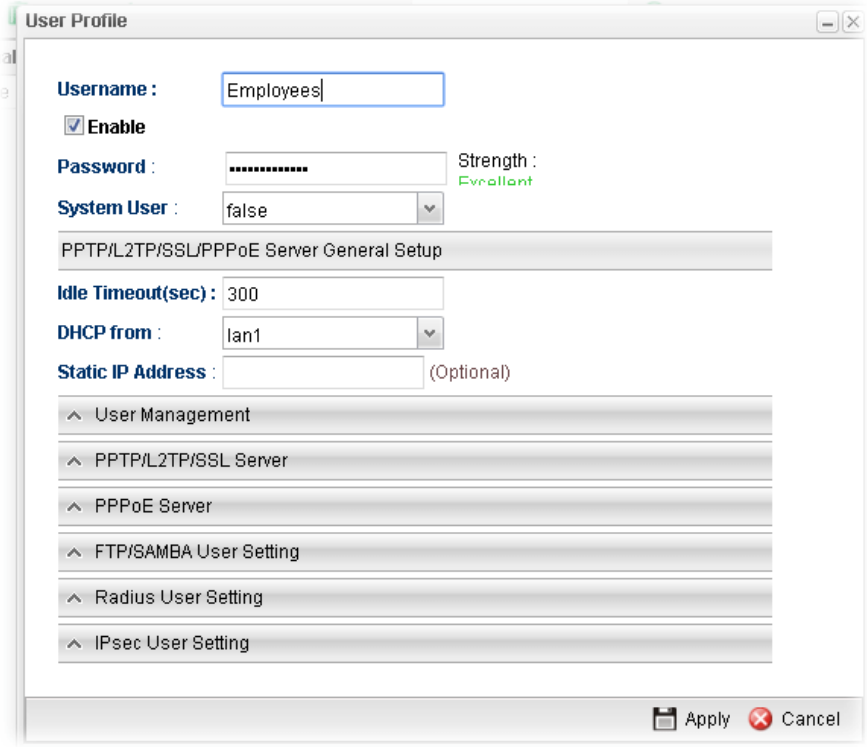
Example: How to Generate Mass LAN Clients with User Management on Vigor2960/Vigor3900

The following table shows the function differences between User Profile and Guest Profile (created by using Mass Guest Generator):

	User Profile	Mass User Generator
Number of Account	Create at most 500 user accounts at a time	Create at most 255 user accounts at a time
Account	Manually	Auto-generated with regularity
Password	Distinct password created by Administrator	Randomly generated, and the length is defined by Administrator
Max Simultaneous users per account	1~255 or unlimited (-1)	Not support
Privilege	Internet Access, VPN, PPPOE client…	Internet Access only
Usage Restriction /Expired Time	Time Quota (1~14400 minutes)	Time Quota (1~14400 minutes) Validity Period (days)
Authentication	YES	YES
Max Simultaneous user	YES	NO
Bind IP	YES	NO

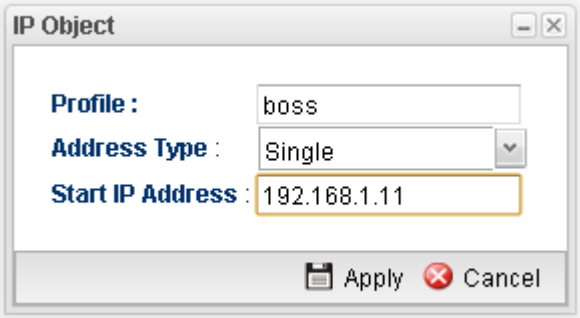


1. Open **User Management** >> **User Profile**, and click **Add**.
2. Set up user profile as shown below. Type **Username;** check **Enable** and type **Password**. Then, type **Max User Login**. Click **Apply** to save the settings.

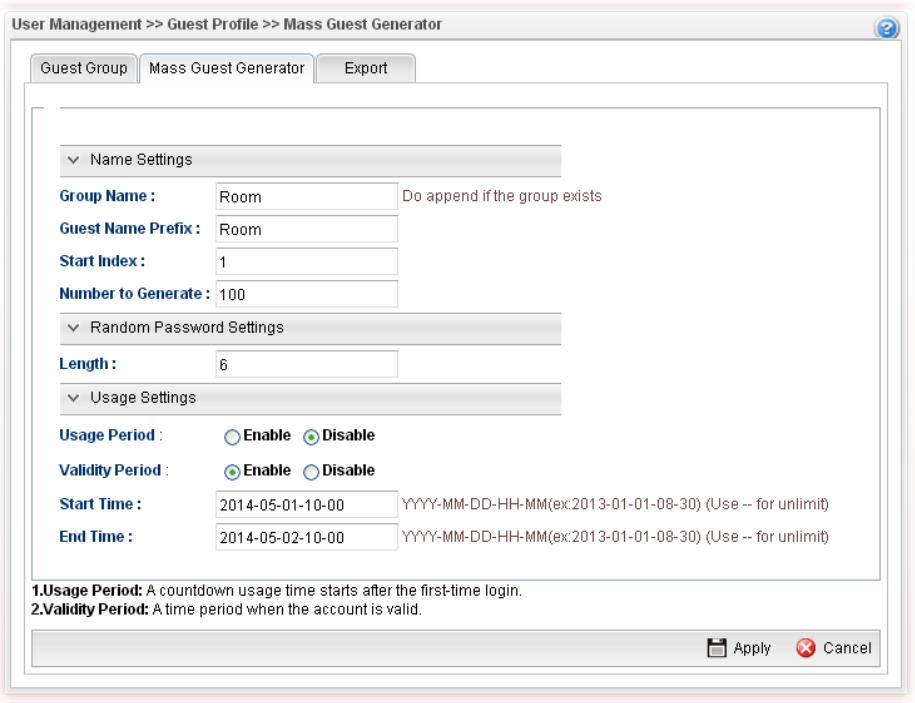


3. Open **Objects Setting** >> **IP Object**, and click **Add**.

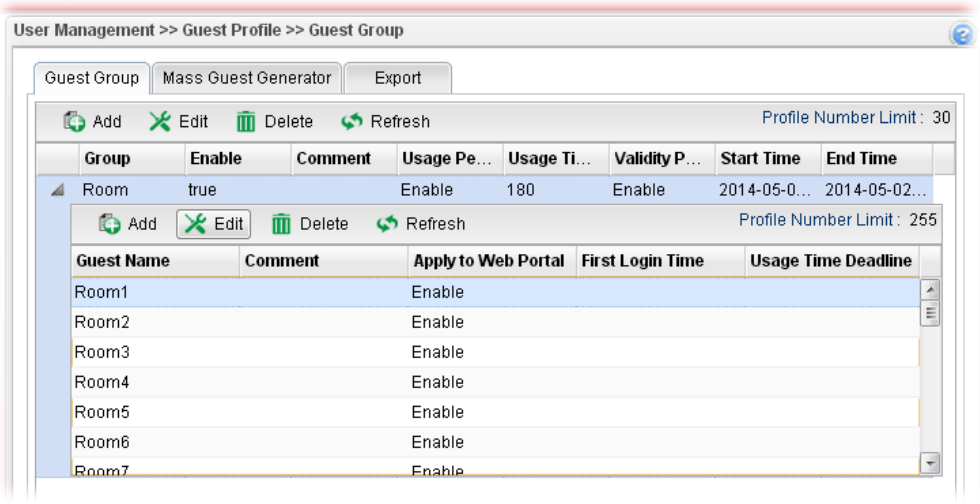
4. Set up **IP Object** for Executive. Type the name of the **Profile** (e.g., boss in this case); choose Single as the **Address Type**; and type 192.168.1.11 as **Start IP Address**. Click **Apply** to save the settings.



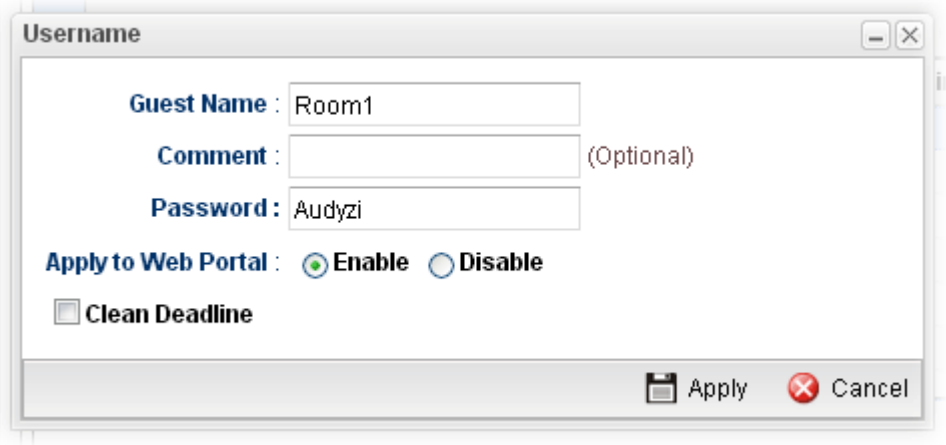
5. Open **User Management** >> **Guest Profile** and click the **Mass Guest Generator** tab to open the following page. Type the **Group Name** (in this case, Room); **Guest Name Prefix**, and **Number of Generate** (in this case, 100); click **Enable** for **Validity Period** to type the **Start Time** and **End time**, and click **Apply** to save the settings.



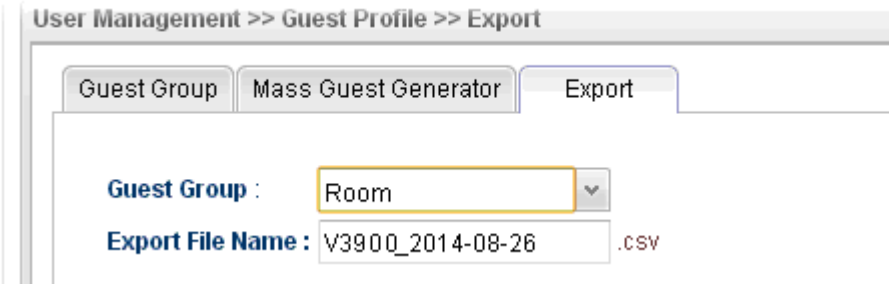
6. Open **User Management >> Guest Profile** and click **Guest Group** to check the **Mass User account Group**.

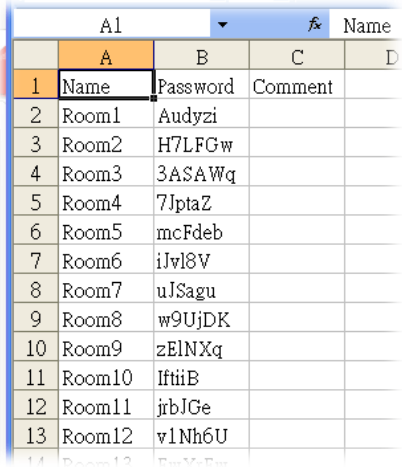


By clicking each account (e.g., choose **1001** and click **Edit**), we can check the information for this account, and we may also modify the account name and password manually.



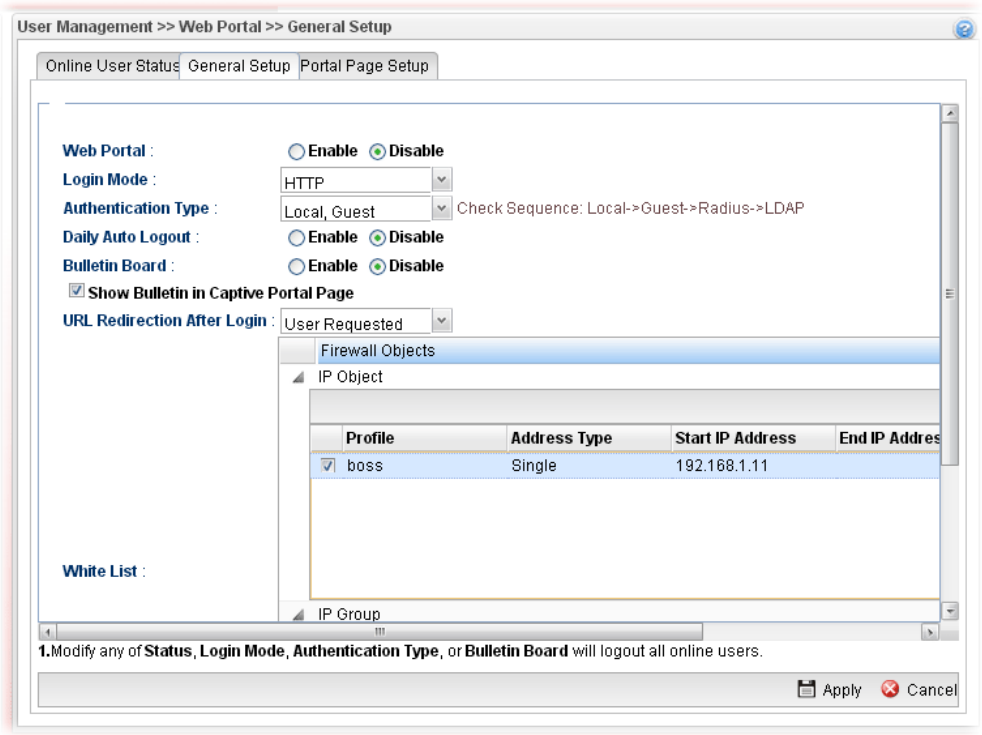
Note that Administrator is able to **Export** the information for the whole group to a *.csv* file, which is useful to **redistribute** the account and password combinations to guests.





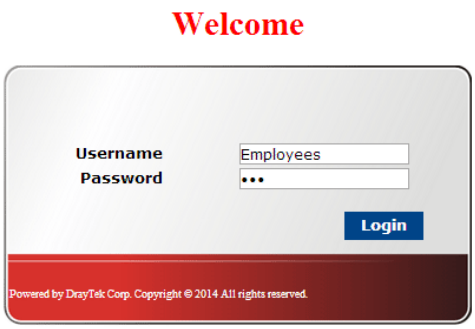
	A	B	C	D
1	Name	Password	Comment	
2	Room1	Audyzi		
3	Room2	H7LFGw		
4	Room3	3ASAWq		
5	Room4	7JptaZ		
6	Room5	mcFdeb		
7	Room6	iJvl8V		
8	Room7	uJSagu		
9	Room8	w9UjDK		
10	Room9	zElNXq		
11	Room10	IftiiB		
12	Room11	jrbJGe		
13	Room12	v1Nh6U		

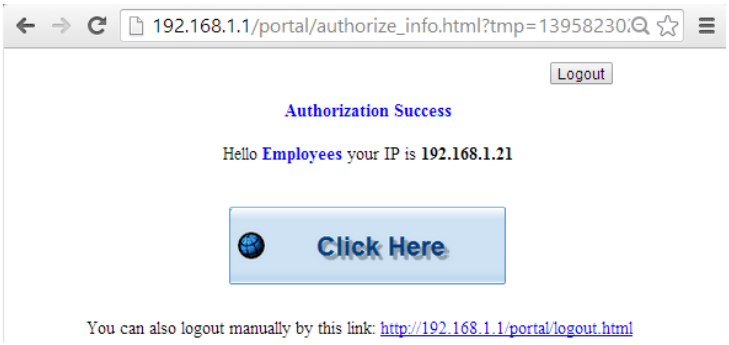
7. Open **User Management >> Web Portal** and click the **General Setup** tab to open the following page. Check **Local** and **Guest** as **Authentication Type**. Check IP object named of **Boss** to put it into the white list, and this will allow this IP address to access to the Internet without authentication.



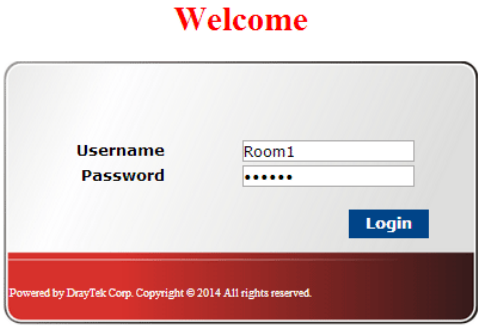
8. After finishing configuration, Vigor3900 will redirect users to the authentication page when they try accessing to the Internet.

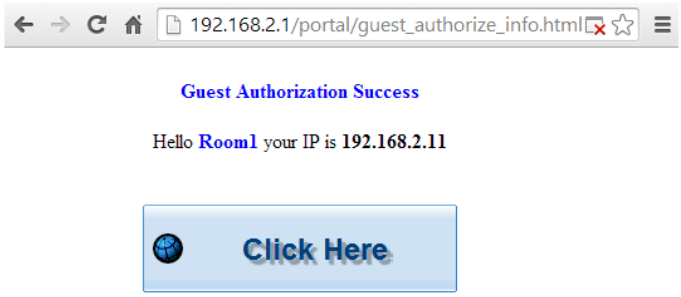
For Employees to access into Internet:





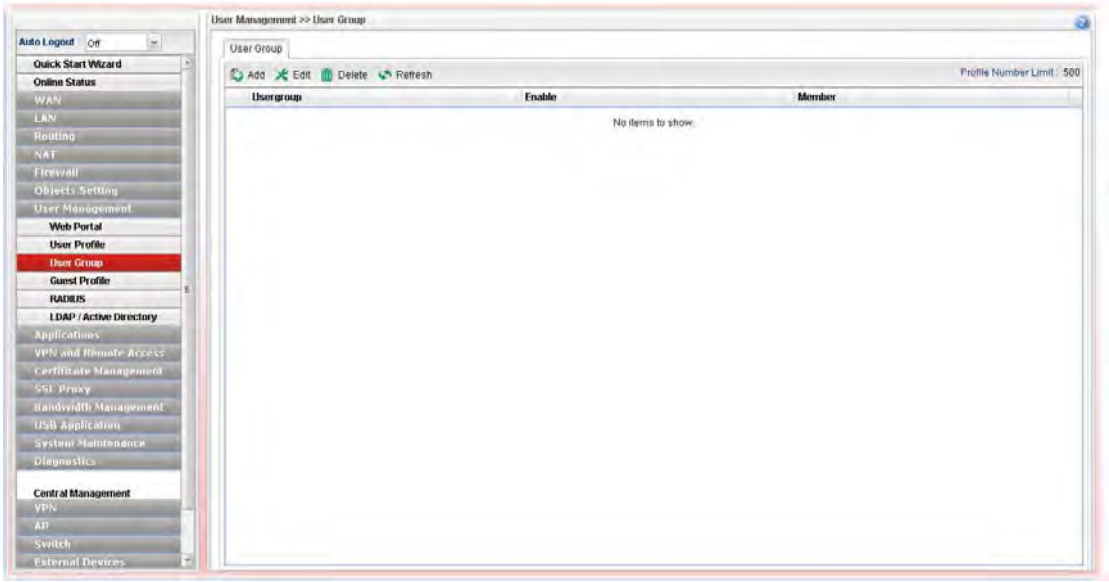
For Room guest to access into Internet:





4.7.3 User Group

The **User Group** can consist of several user profiles, which help the administrator to manage a large number of users conveniently.



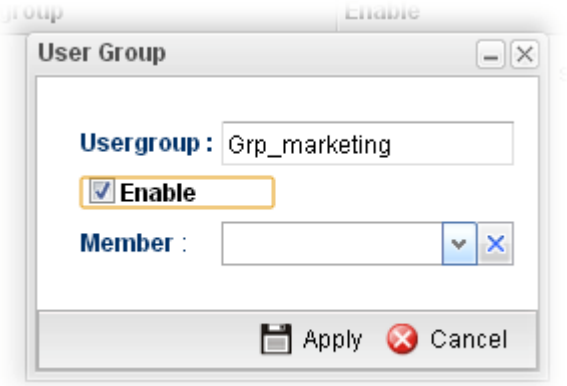
Each item will be explained as follows:

Item	Description

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (30) of the object profiles to be created.
Usergroup	Display the name of the user group.
Enable	Display the status of the profile. False means disabled; True means enabled.
Member	Display the user profiles under such group.

How to create a new User Group Profile

1. Open **User Management>>User Group.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

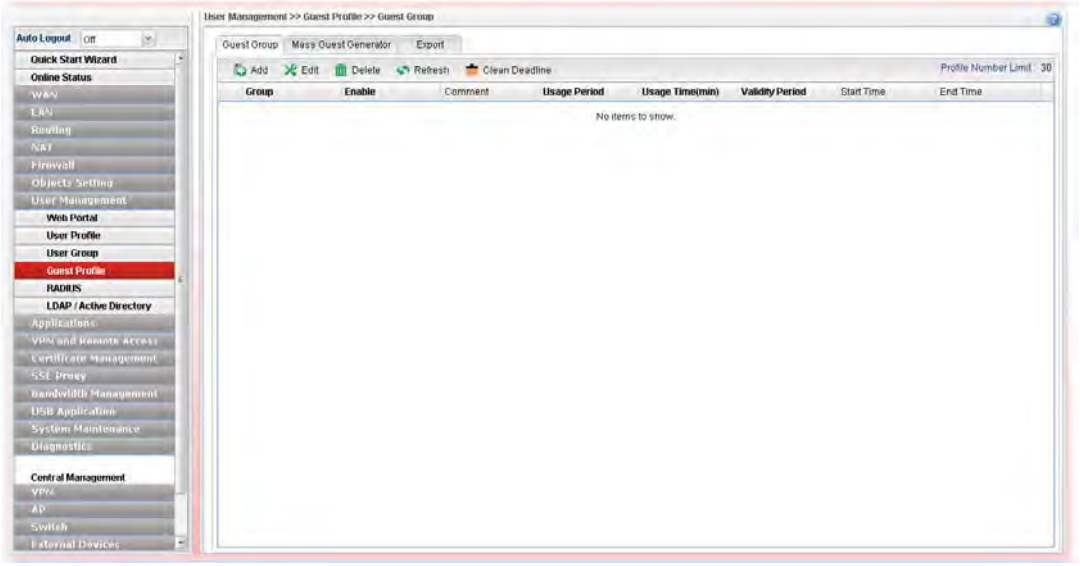
Item	Description
Usergroup	Type the name of such profile.
Enable	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group. To clear the selected one, click to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new User Group Profile has been created.

4.7.4 Guest Profile

Guest Profile allows the users to access Internet within validity period and limit the user accessing into the specified URL configured by web portal.

4.7.4.1 Guest Group



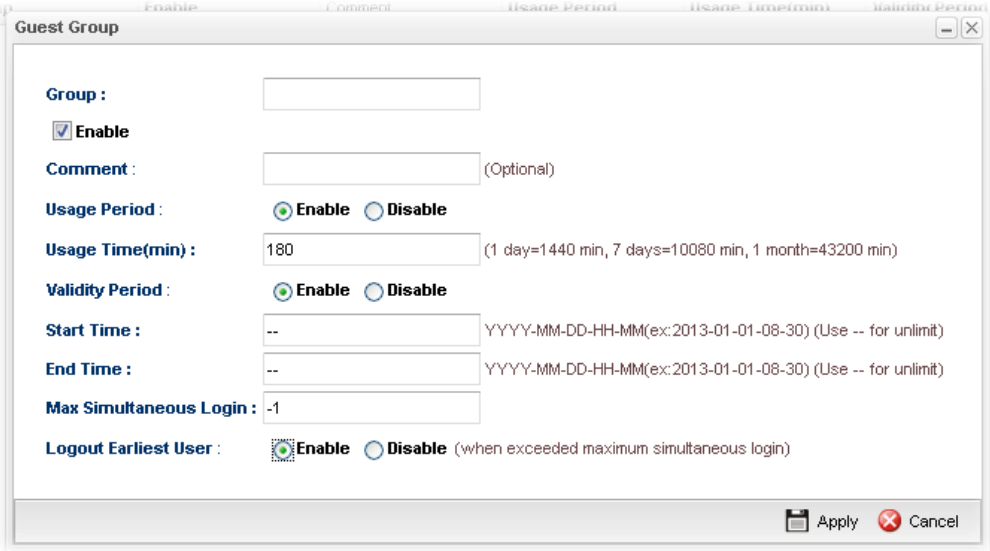
Available parameters are listed as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Clean Deadline	Renew the usage time designated for such profile.
Profile Number Limit	Display the total number (30) of the profiles to be created.
Group	Display the name of the guest group.
Enable	Display the status of the profile. False means disabled; True means enabled.
Comment	Display the description for the profile.
Usage Period	Display the status (Enable/Disable) for the function of usage time.
Usage Time(min)	Display the usage time for the guest accessing into Internet each time.

Item	Description
Validity Period	Display the valid period for the guest accessing into Internet.
Start Time/ End Time	Display the detailed time setting (starting and ending).

How to create a new Guest Group Profile

1. Open **User Management>>Guest Group.** Click the **Guest Group** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.

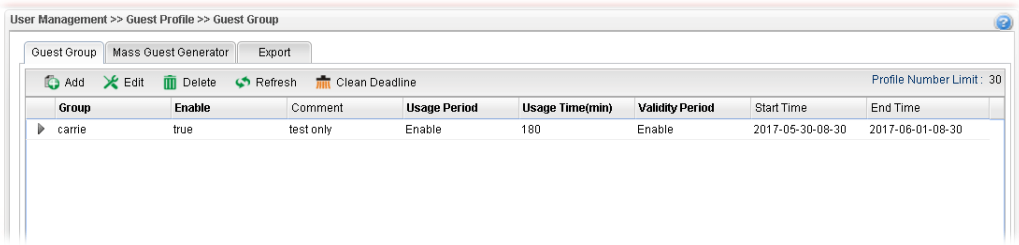


Available parameters are listed as follows:

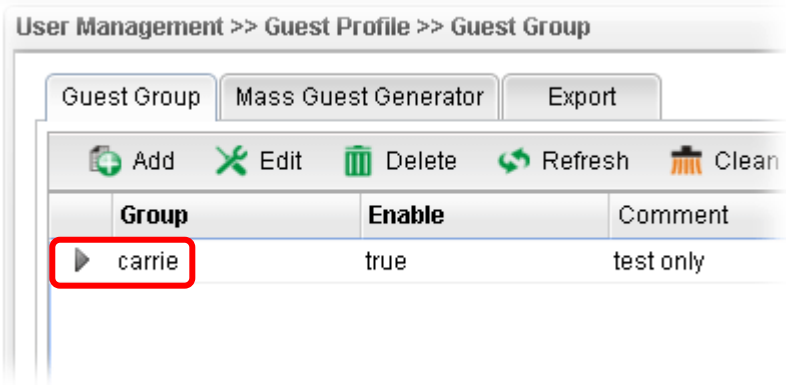
Item	Description
Group	Type the name of such profile.
Enable	Check this box to enable such profile.
Comment	Give a brief description for the profile.
Usage Period	It determines the usage time for the guest accessing into Internet each time. Click **Enable** to enable such option. **Usage Time(min)**- Determines the connection time allowed for accessing Internet every time. The default setting is 180 minutes. When the time is up, the user will be forced to exit Internet.
Validity Period	Validity Period determines the effective time for the user account/guest. Within the period of the validity, the user/guest can access into Internet whenever he wants. **Start Time/End Time** – Specify the valid period by typing the time with the format of YYYY-MM-DD-HH-MM. When it is set with "--", that means such time setting is no limit.
Max Simultaneous Login	It means the maximum online number of clients logging with this profile. The range is from 1 to 255. -1 means no limit; 0 means No

	access.
Logout Earliest User	Force the earliest user to logout when exceeded the maximum number of online user setting. (The number is defined in Max Simultaneous Login). **Enable** – Click it to enable such function. **Disable** – Click it to disable such function.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

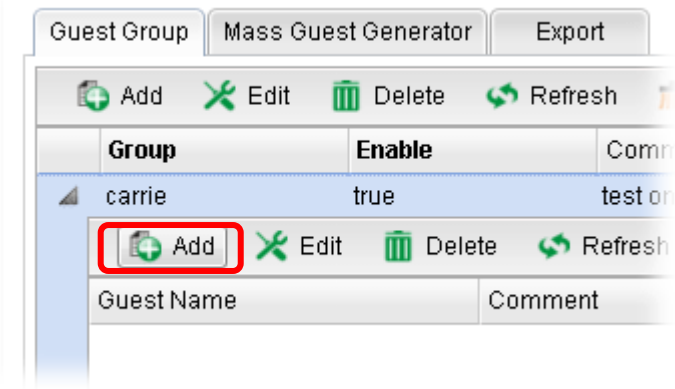
4. Enter all of the settings and click **Apply**.
5. A new guest group profile has been created.



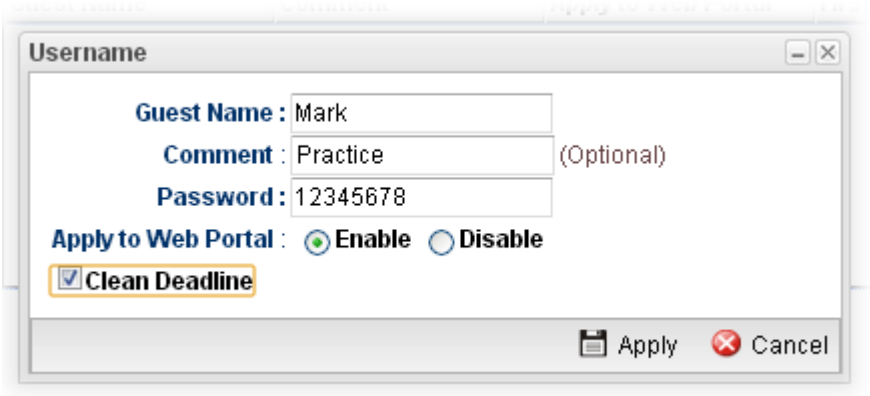
6. You can create several guest names by clicking ▶ on the left side of the selected guest group profile. A setting page will appear for you to add new guest list.



7. Move your mouse to click **Add**.



8. The following page for configuration will appear.

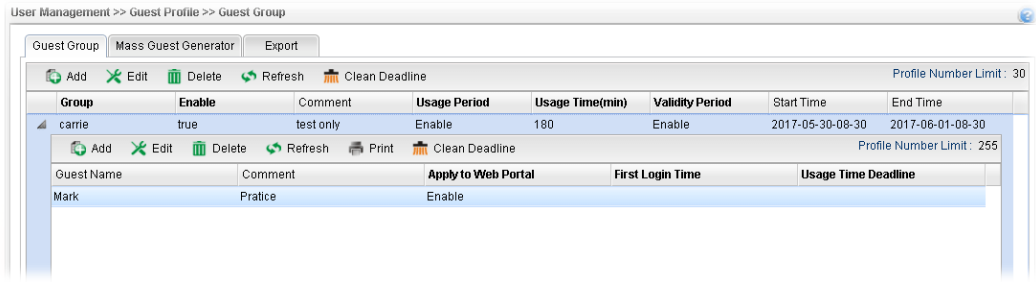


Available parameters are listed as follows:

Item	Description
Guest Name	Type the name of the guest under the guest group.
Comment	Give a brief description for the guest.
Apply to Web Portal	**Enable** – Click it to make such profile being applied to web portal. Disable – Click it to disable the option.
Clean Deadline	The guest profile can be unlocked to be used by other users.

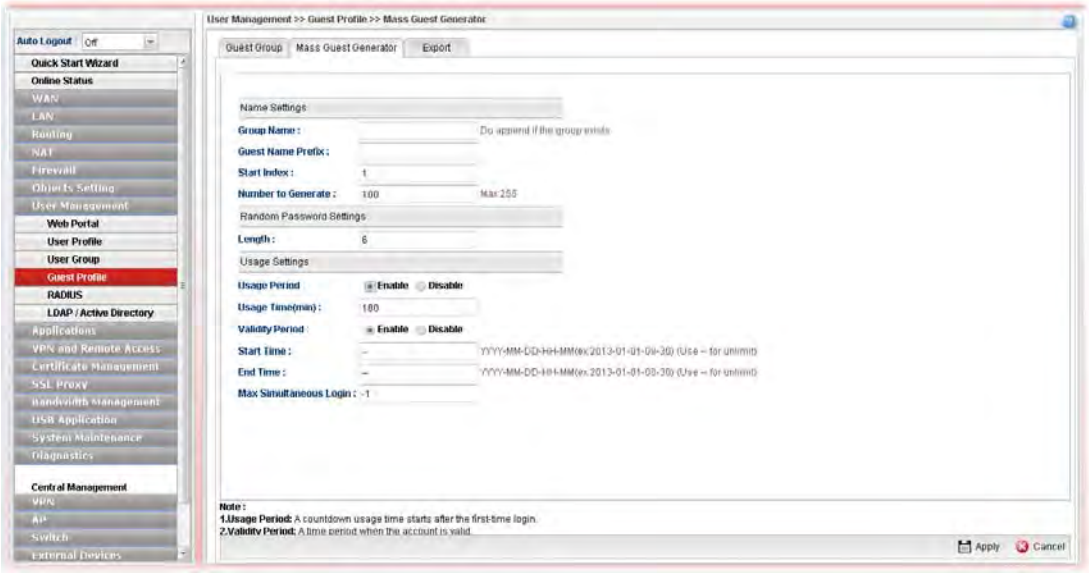
9. Enter all of the settings and click **Apply**.

10. A new guest has been added under the Guest Group (named Carrie in this case).



4.7.4.2 Mass Guest Generator

This option is useful to create **a lot of** guest profiles with the most expeditious manner.



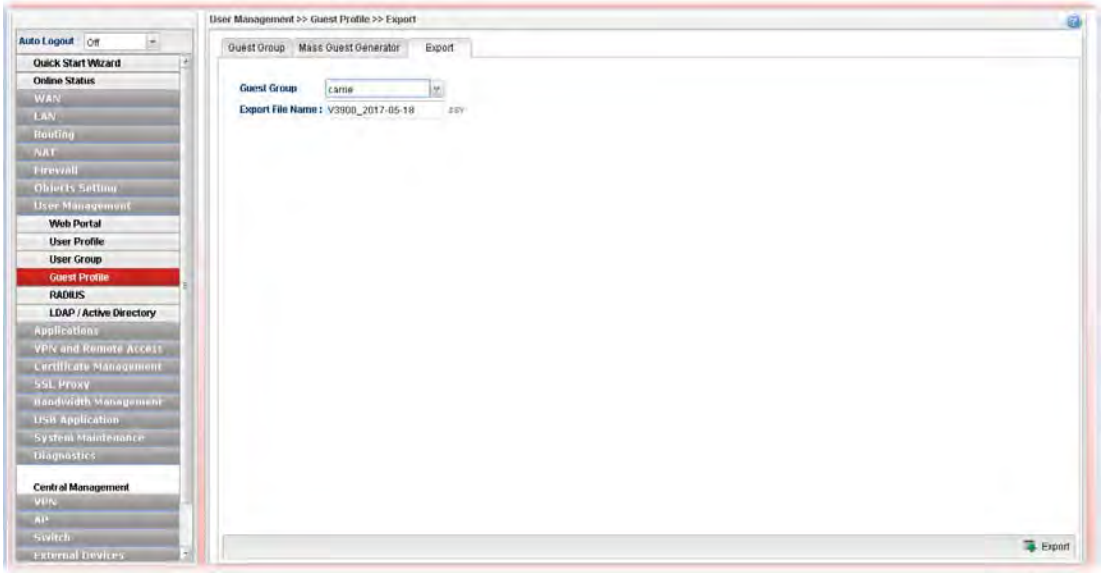
Available parameters are listed as follows:

Item	Description
Name Settings	**Group Name** – Type the name of the guest group. **Guest Name Prefix** – The guest names created with such manner requires a prefix as the basis of name input. **Note:** Guest Name Prefix disallows these 6 characters "^?$%.&". **Start Index** – Type a number which will be treated as the starting number for generating mass guest profiles. **Note:** The range of Start index is 1~10000. **Number to Generate** – Type the total number of guests to be generated at one time. The guest name will be named by combining "Guest Name Prefix" + "Start Index", for example: Guest Name Prefix => teashop_ Start Index => 100 Number to Generate => 50 Then, the guests names generated will be: teashop_100 (starting) teashop_101 teashop_102 ... teashop_150 (ending)
Random Password Settings	**Length** – Type a number to determine the length of the random passwords which will be assigned to the mass guest profiles by the system. The range of Password Length is 6~12.

Item	Description
Usage Settings	**Usage Period** –It determines the usage time for the guest accessing into Internet each time. Click **Enable** to enable such option. ● **Usage Time(min)**-The default setting is 180 minutes. **Validity Period** –It determines the valid period for the guest accessing into Internet. That is, the guest cannot access into the Internet anytime outside the valid period. Click **Enable** to enable such option. ● **Start Time/End Time** – Specify the valid period by typing the time with the format of HH-MM-SS.
Max Simultaneous Login	It means the maximum online number of clients logging with this profile. The range is from 1 to 255. -1 means no limit; 0 means No access.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.7.4.3 Export

This function is used to export the guest profile names and random passwords.



Available parameters are listed as follows:

Item	Description
Guest Group	Choose a group that you want to export the settings, including guest profile names and random passwords as a file for reference.

4.7.5 RADIUS

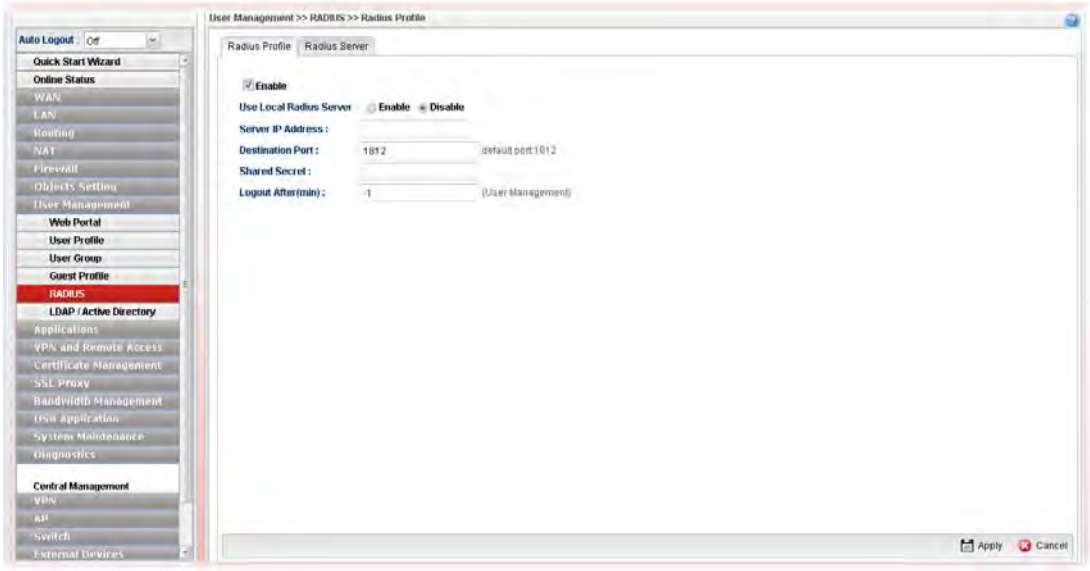
Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is

widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

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

4.7.5.1 External Radius Server

Vigor router can specify external RADIUS server for performing security authentication.



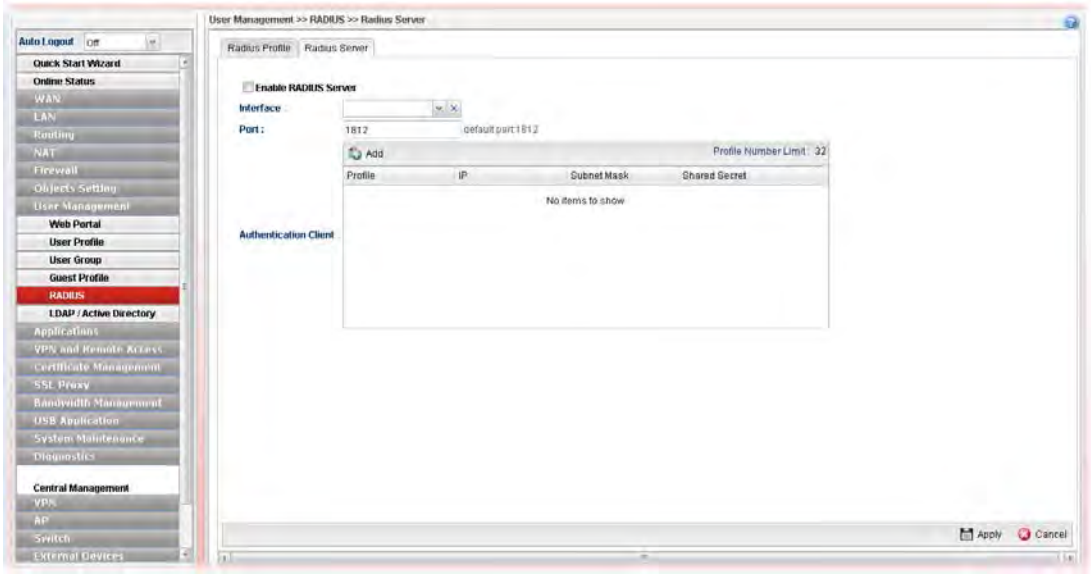
Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
Use Local Radius Server	**Enable**- Choose it to use local RADIUS server for user authentication. **Disable** – Choose it to specify another server for user authentication.
Server IP Address	Enter the IP address of RADIUS server.
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared 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.
Logout After(min)	It means the maximum usage duration for RADIUS authentication.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.7.5.2 Radius Server

In addition to specifying an external RADIUS server for security authentication, Vigor router also can be treated as a RADIUS server for performing security authentication and offer the RADIUS service for wireless clients.



Available parameters are listed as follows:

Item	Description
Enable RADIUS Server	Check this box to make Vigor router as a RADIUS server.
Interface	Only the clients from the selected interface can be authenticated by Vigor RADIUS server.
Port	Clients can use the specified port number to exchange RADIUS information.
Authentication Client	Only the clients specified in this field can be authenticated by Vigor RADIUS server.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

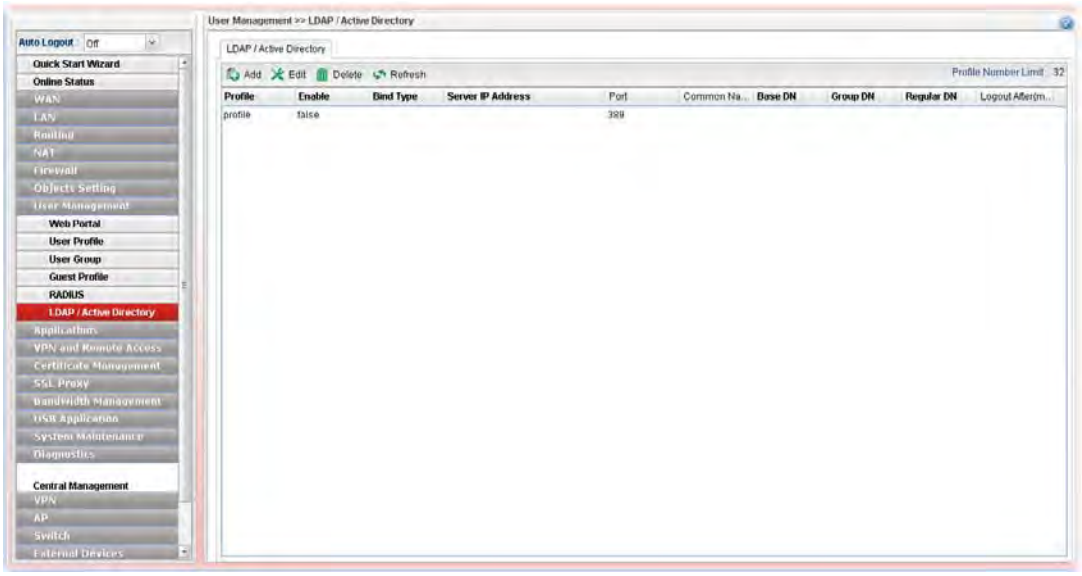
After finished the above settings, click **Apply** to save the configuration.

Note: "**Allow Radius Server Login**" can be enabled from the configuration page in **User Management>>User Profile**. It allows the clients to be authenticated by internal RADIUS server of Vigor router.

4.7.6 LDAP/Active Directory

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.



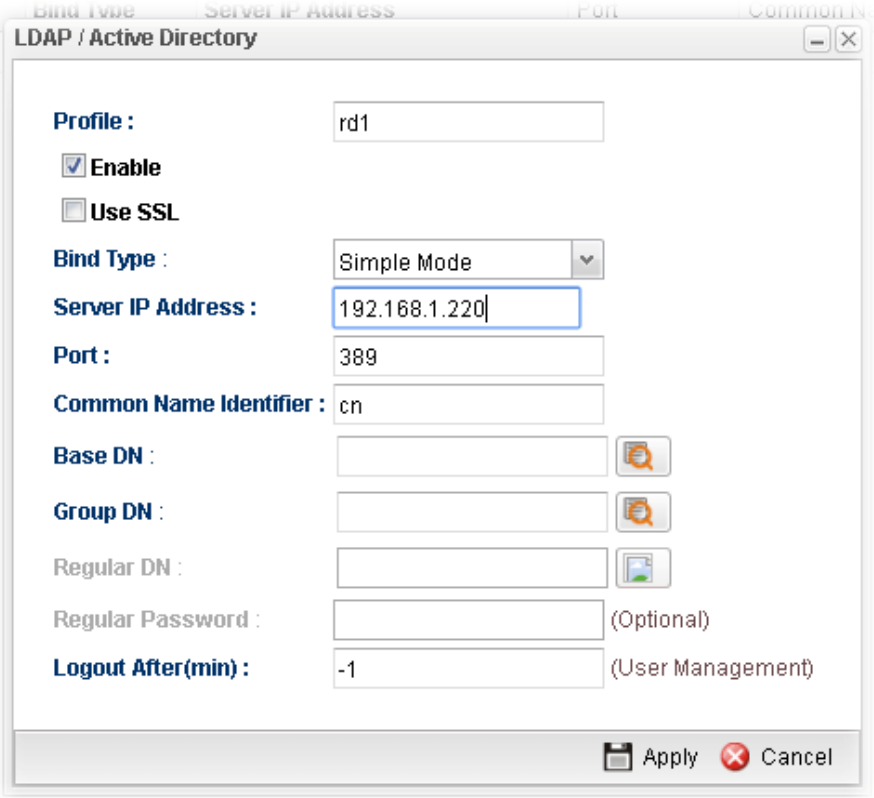
Available parameters are listed as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Bind Type	Display the type setting selected for such profile.
Server IP Address	Display the IP address of the LDAP server.
Port	Display the port number set for such profile.
Common Name Identifier	Display the name for identification.
Base DN	Display the configured Base DN if Bind Type is set with Simple Mode.
Group DN	Display the configured Group DN if Bind Type is set with Simple Mode.
Regular DN	Display the configured regular DN if Bind Type is set with Regular Mode.

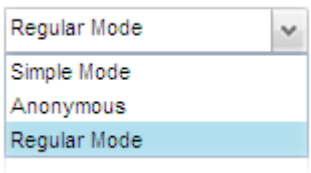
Item	Description
Logout After(min)	Display the maximum usage duration for RADIUS authentication.

How to create a new LDAP/Active Directory Profile

1. Open **User Management>>LDAP/Active Directory.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
Enable	Check this box to enable such profile.
Use SSL	Check this box to enable SSL tunnel for such profile.
Bind Type	There are three types of bind type supported.  **Simple Mode** – Just simply do the bind authentication without any search action. **Anonymous** – Perform a search action first with

	Anonymous account then do the bind authentication. **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
Server IP Address	Enter the IP address of LDAP server.
Port	Type a port number as the destination port for LDAP server.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn"
Base DN	It means "**Base Distinguished Name**". Type the distinguished name used to look up entries on the LDAP server.
Group DN	It means "**Group Distinguished Name**". Type the distinguished name used to look up entries on the LDAP server.
Regular DN	Type this setting if **Regular Mode** is selected as **Bind Type.**
Regular Password	Specify a password if **Regular Mode** is selected as **Bind Type.**
Logout After(min)	It means the maximum usage duration for RADIUS authentication.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new LADP/Active Directory Profile has been created.

4.8 Application

Below shows the menu items for Applications.

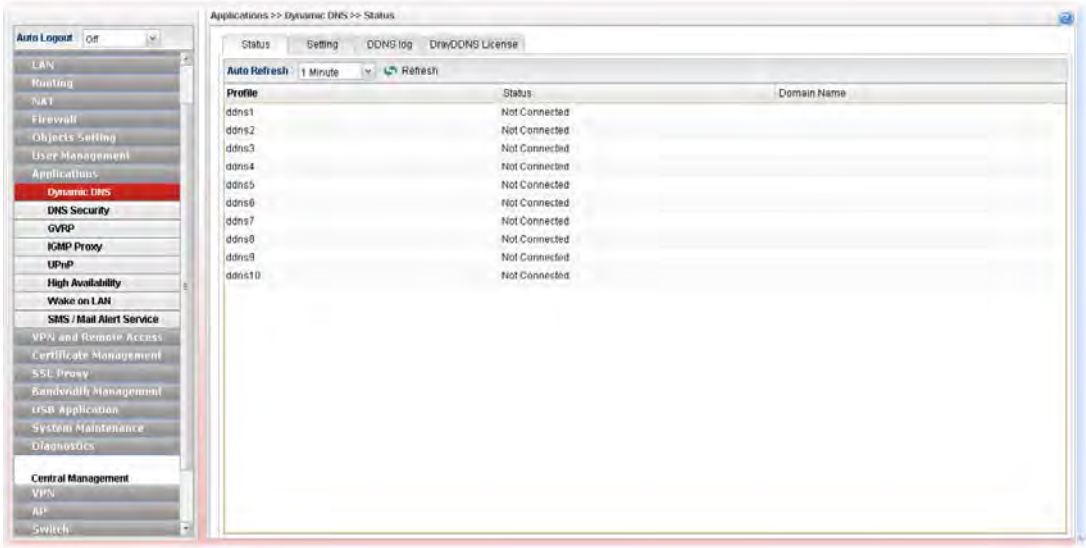
4.8.1 Dynamic DNS

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

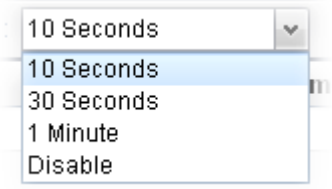
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to ten accounts from eight different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers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

4.8.1.1 Status

This page displays the status for all the available DDNS profiles.

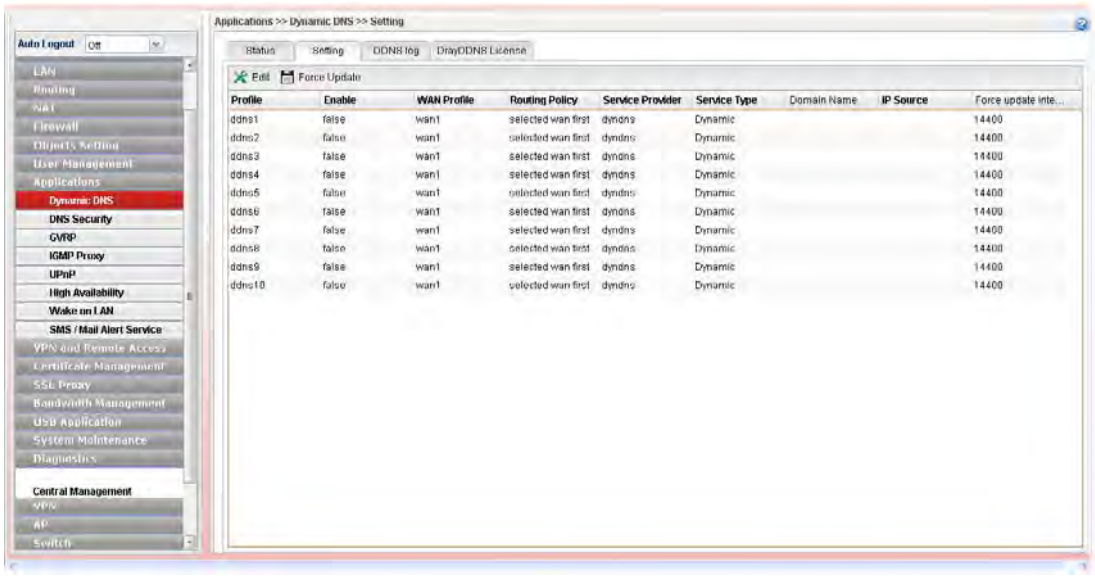


Each item will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked. 
Profile	Display the name of the DDNS.
Status	Display the connection status for the DDNS sever.
Domain Name	Display the domain name for the DDNS server.

4.8.1.2 Setting

This page allows you to configure DDNS profiles for your request.



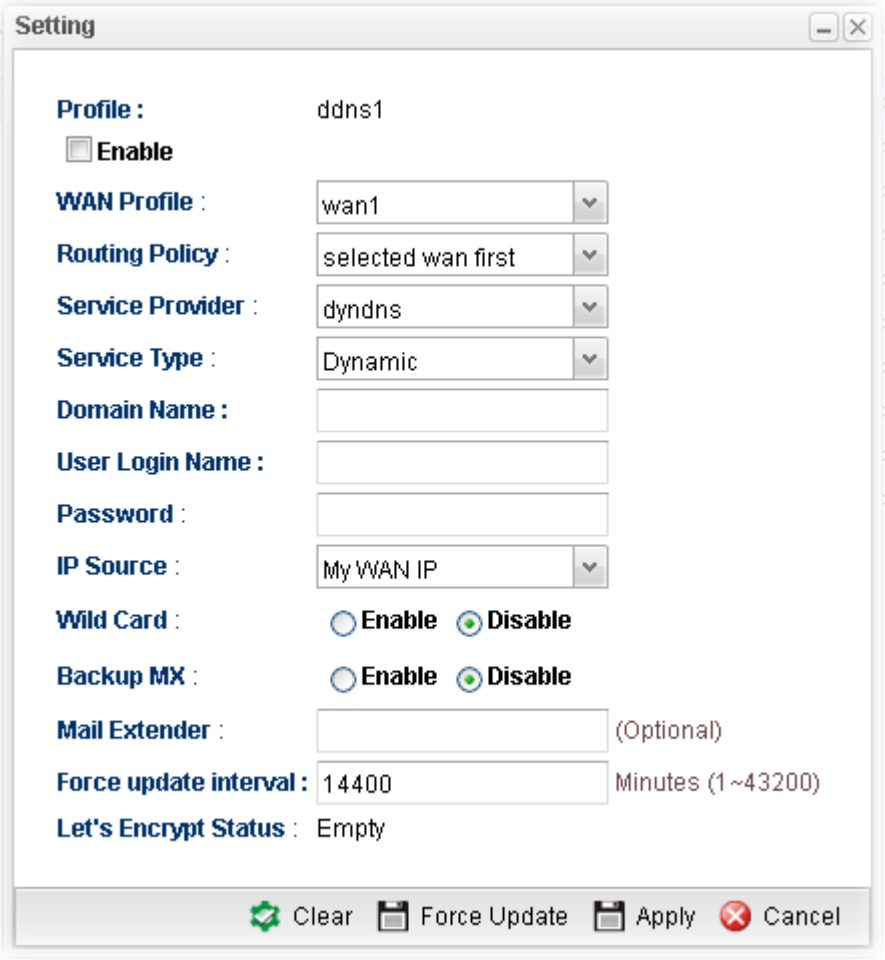
Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Force Update	Force the router updates its information to DDNS server immediately.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display current WAN profile used by such DDNS profile.
Routing Policy	Display the routing policy used by such DDNS profile.
Service Provider	Display the name of service provider used by such profile.
Service Type	Display the type for such profile.
Domain Name	Display the domain name of such profile.
IP Source	Display the interface (My WAN IP or My Internet IP) selected by such DDNS profile.
Force update interval	Display the interval setting to refresh the data for such profile.

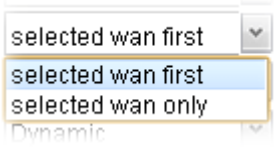
How to edit a DDNS Profile

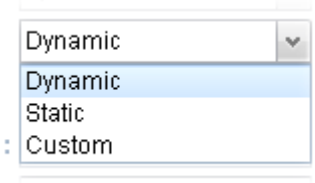
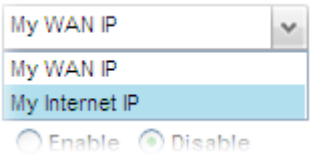
There are 10 sets of DDNS server offered for you to modify and configure. Please choose any one of them and click **Edit** to open the following page for modification.

1. Open **Applications>>Dynamic DNS** and click the **Setting** tab.
2. Choose one of the DDNS profiles and click the **Edit** button.

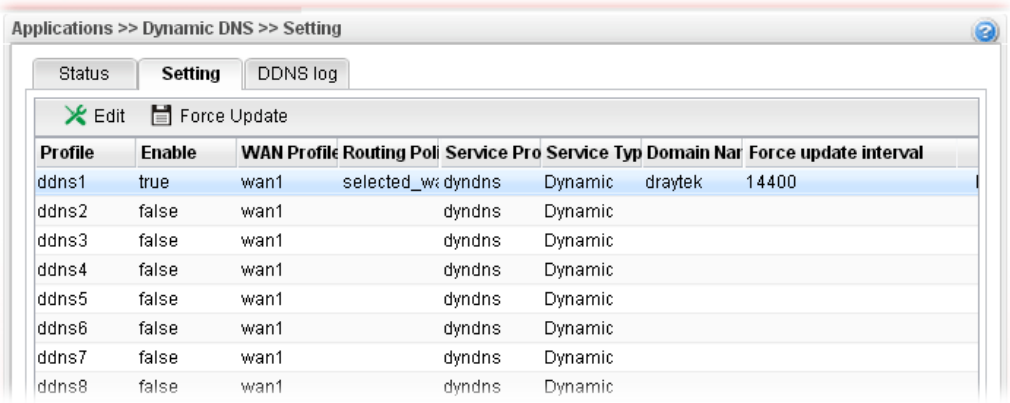


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose a WAN interface that such profile will apply to.
Routing Policy	Choose a routing policy applied to the DDNS profile.  **selected wan first** – The DDNS profile will be applied to the traffic via WAN interface first, then applied to other interface. **selected wan only** – The DDNS profile will be applied to the traffic via WAN interface only. No other interface will be used.
Service Provider	Select the service provider for the DDNS account.

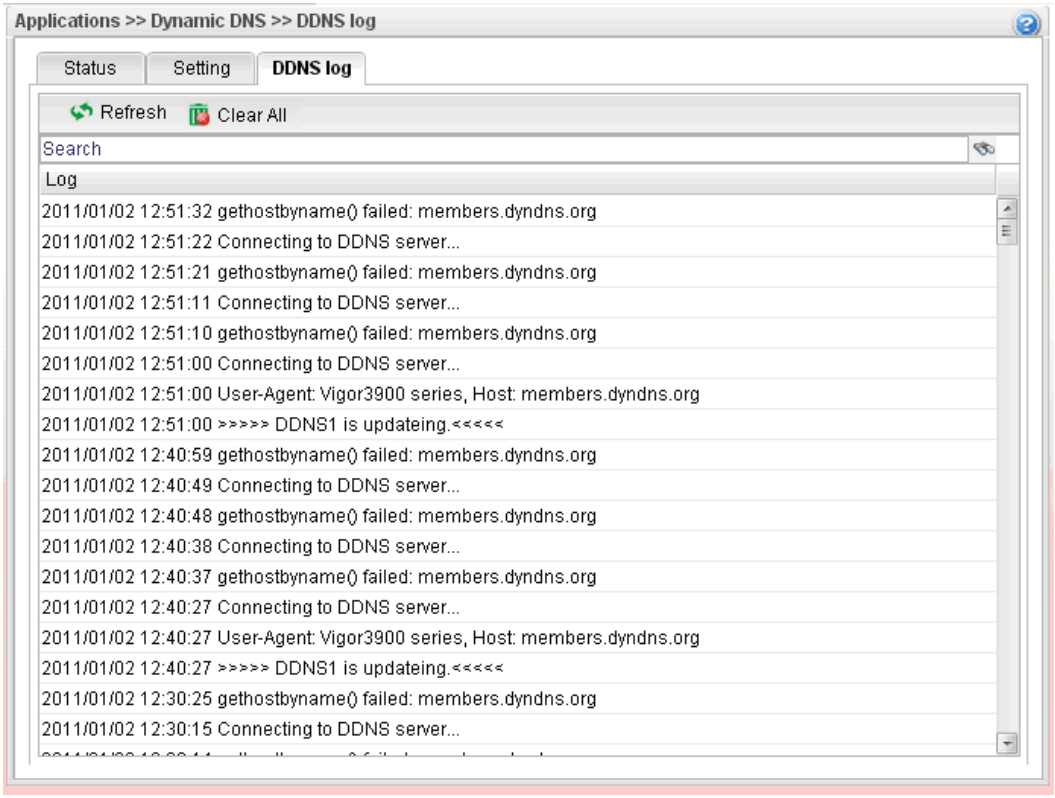
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. 
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
User Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
IP Source	Choose My WAN IP or My Internet IP as the source for the DDNS profile. 
Wildcard and Backup MX	The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	Type the IP/Domain name of the mail server.
Force update interval	Set the time for the router to perform auto update for DDNS service.
Clear	Click it to restore the default settings for such profile.
Force Update	Click it to force update the profile.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

3. Enter all the settings and click **Apply**.
4. The DDNS Profile has been modified.



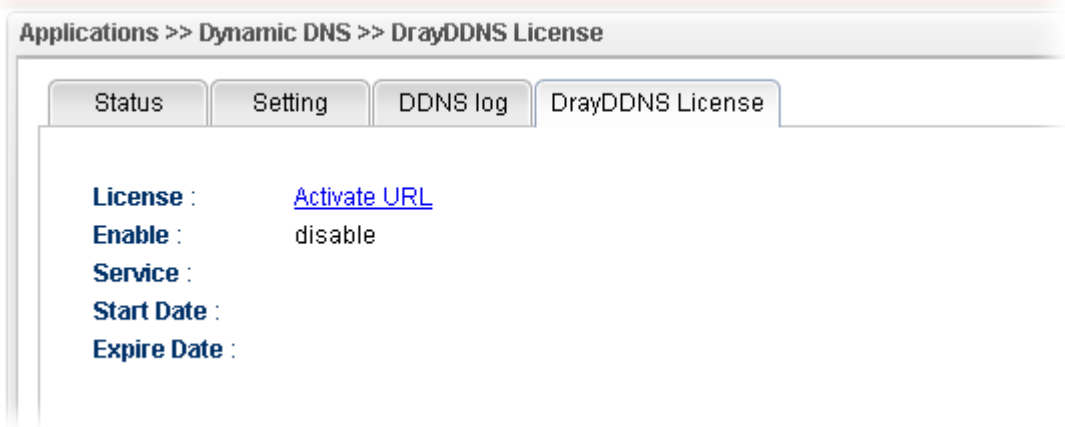
4.8.1.3 DDNS Log

This page displays the information related to all DDNS.



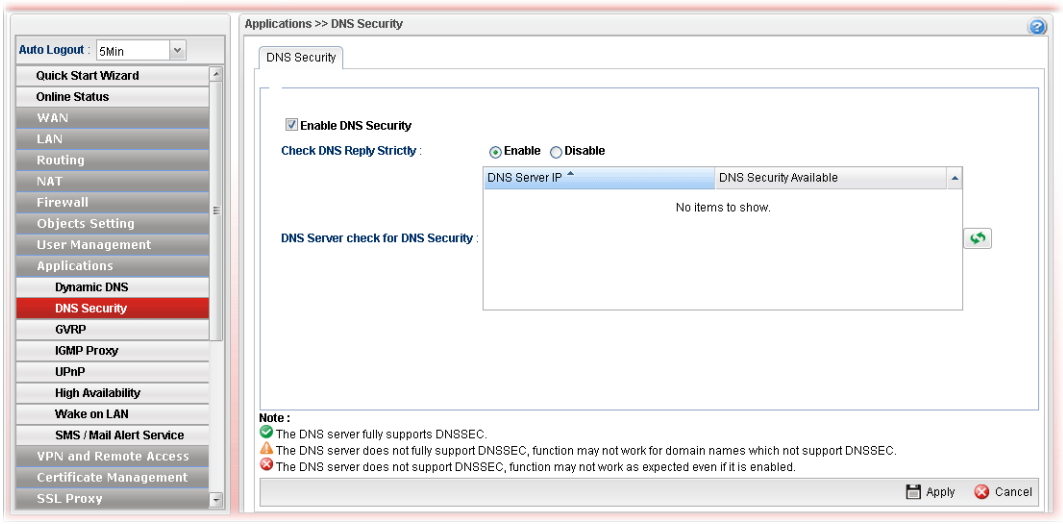
4.8.1.4 DrayDDNS License

Such page displays license information for DrayDDNS service.



4.8.2 DNS Security

DNS security is able to ensure that the incoming data is not falsified and the source of the data is secure and correct to prevent from DNS attack by someone.

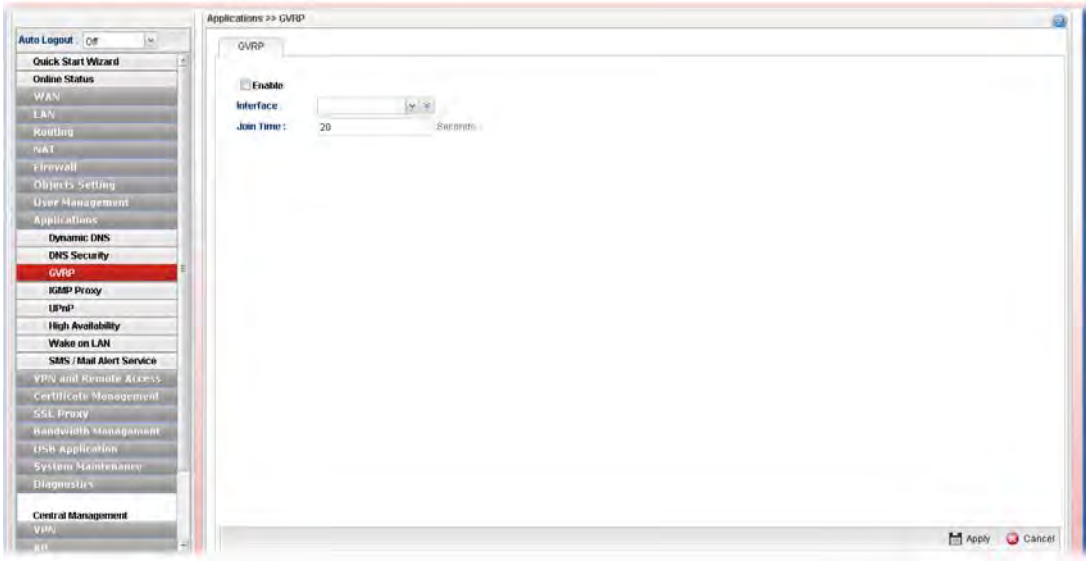


Available parameters are listed as follows:

Item	Description
Enable DNS Security	Check the box to enable the DNS security management.
Check DNS Reply Strictly	In default, Vigor router does not check that unsigned DNS replies are legal or not: they are assumed to be valid and passed on. This does not protect against an attacker forging unsigned replies for signed DNS zones, but it is fast. If this option is enabled, Vigor router will check the zones of unsigned replies to ensure that unsigned replies are allowed in those zones. The cost of this is more upstream queries and slower performance. **Enable** – It will check if the unsigned DNS replies are unsigned or not. **Disable** – The unsigned DNS replies will be regarded as "legal". It is default setting.
DNS Server check for DNS Security	Vigor router will check and display if the DNS servers listed in WAN profiles supporting DNS security or not.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.3 GVRP

This function can define the method for the changing the VLAN information among devices. With supporting GVRP, the device can receive the VLAN information coming from other devices.

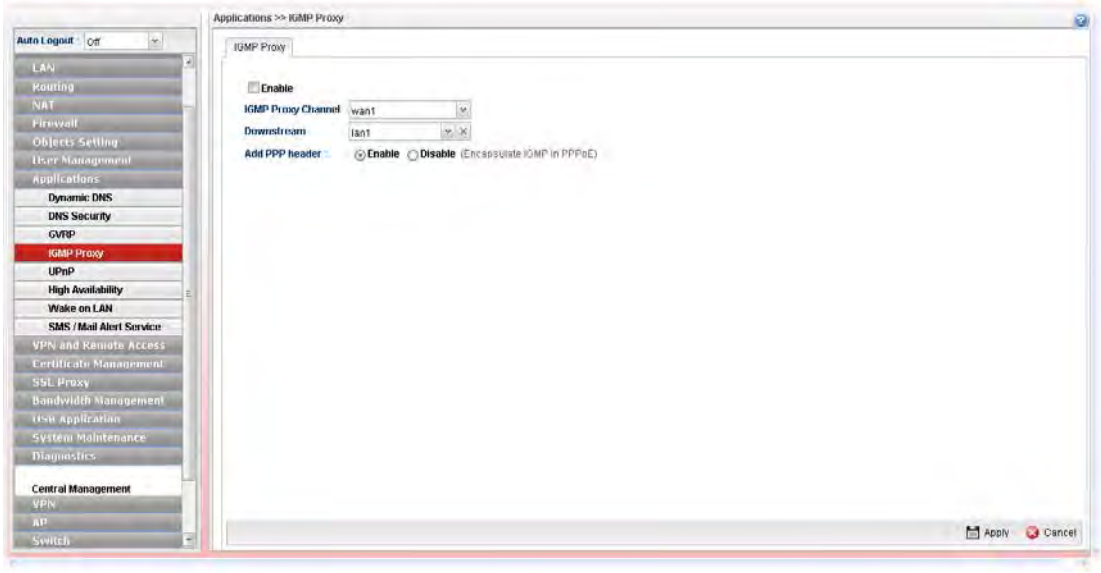


Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable GVRP function.
Interface	Choose LAN and/or WAN profiles. To clear the selected one, click to remove current object selections.
Join Time	Define the time for the system to send GVRP packet to other device. The unit is second.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.4 IGMP Proxy

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

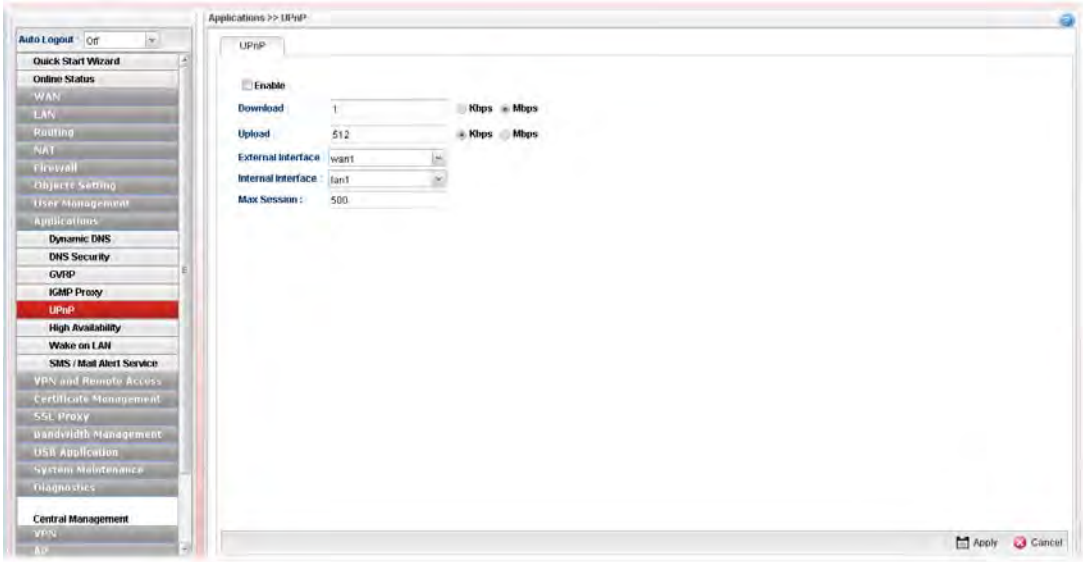


Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable IGMP proxy function.
IGMP Proxy Channel	The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.
Downstream	Use the drop down list to specify the LAN profile as the destination of data coming from WAN interface (defined in IGMP Proxy Channel).
Add PPP header	**Enable** – For PPPoE WAN connection, the IGMP packets will be sent with PPP header and WAN IP address. **Disable** – For PPPoE WAN connection, the IGMP packets will be sent without PPP header. IGMP interface IP will be used as source IP address. ● **IGMP Interface IP** – Type the IP address of IGMP server.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.5 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.



Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable UPnP function.
Download	Enter the maximum sustained WAN download speed in kilobits/second. Such information can be requested by UPnP clients.
Upload	Enter the maximum sustained WAN upload speed in kilobits/second. Such information can be requested by UPnP clients.
External Interface	Select a WAN profile for UPnP protocol.
Internal Interface	Select a LAN profile for UPnP protocol.
Max Session	Determine the maximum session number for UPnP function.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

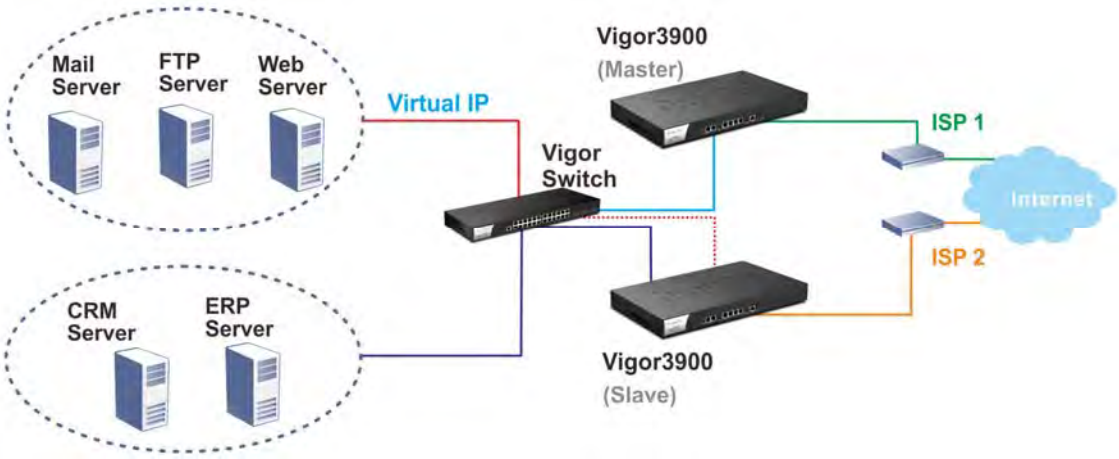
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.8.6 High Availability

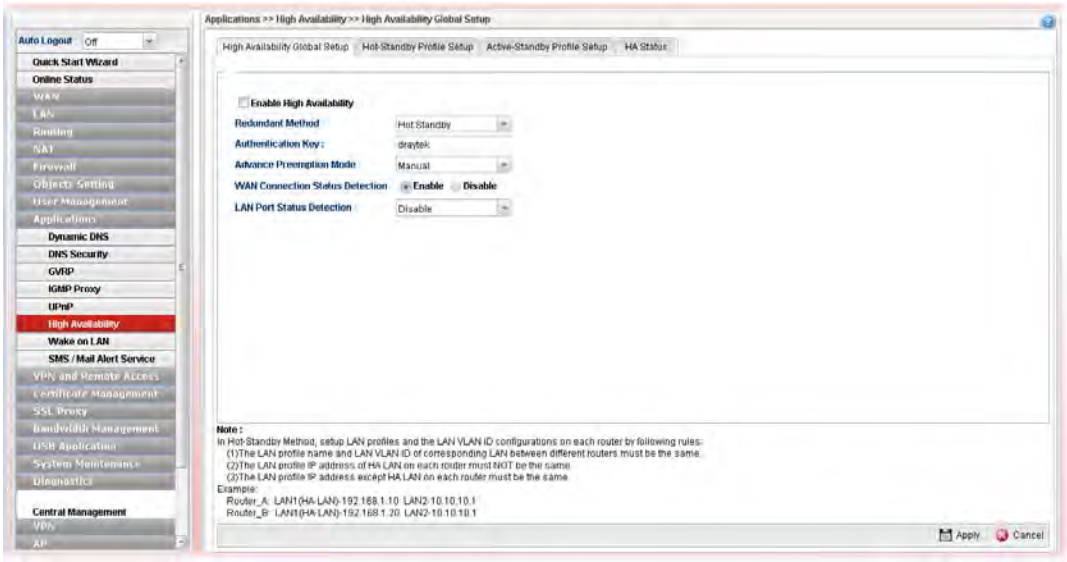
The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, provide nearly full-time availability, typically have redundant hardware and software that make the system available despite failures.

The high availability of the V3900 Series is designed to avoid single points-of-failure. When failures occur, the failover process moves processing performed by the failed component (the "Master") to the backup component (the "Slave"). This process remains system-wide resources, recovers partial of failed transactions, and restores the system to normal within a matter of microseconds.

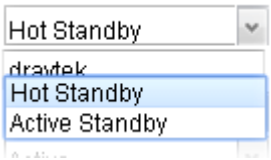
Take the following picture as an example. The left V3900 Series is regarded as Master device, the right V3900 Series is regarded as Slave device. When Master V3900 Series is broken down, the Slave (backup) device could replace the Master role to take over all jobs as soon as possible. However, once the original Master is working again, the Slave would be changed to original role to stand by.

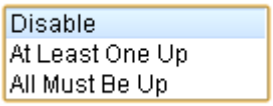


4.8.6.1 High Availability Global Setup



Available parameters are listed as follows:

Item	Description
Enable High Availability	Check this box to enable HA function.
Redundant Method	Choose Hot Standby or Active Standby as the method for HA.  **Hot Standby** –Hot Standby is a redundant method of having several secondary service nodes running standby with another identical primary service node. Upon failure of the primary node, the system immediately elects one from all secondary nodes to replace the failure one and take over the service. While in the standby status, the secondary nodes are still mirrored the configuration of primary in real time, thus the whole systems are assured of having identical configuration. **Active Standby** –Active Standby is a redundant method of having the access points configured independently by participating in HA session with individual LAN interface. As an active gateway LAN, it routes user's traffic while others stay in standby status.
Settings under Hot Standby	**Authentication Key** – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack. **Advance Preemption Mode** – Specify a mode for changing the Config Synchronization Role.

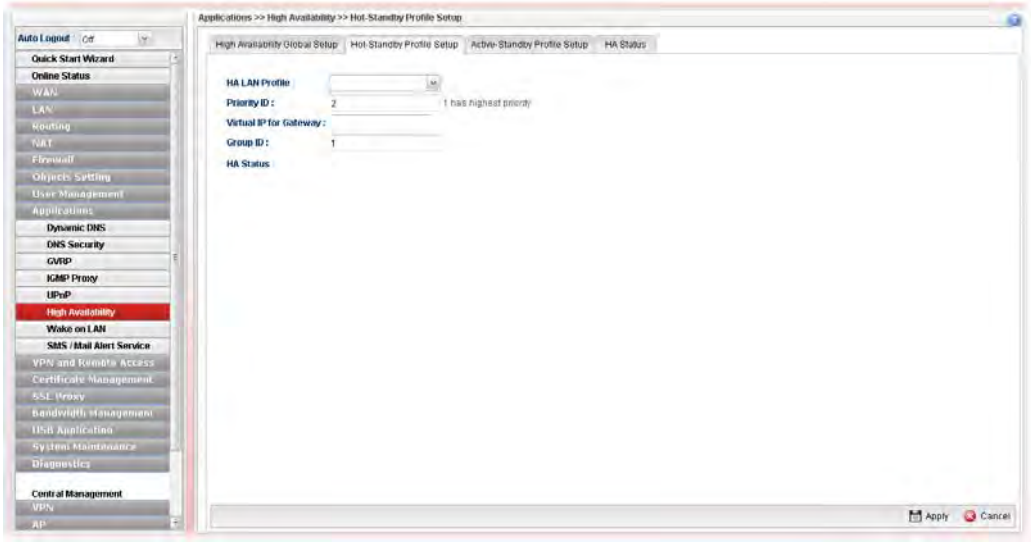
Item	Description
	 ● **Immediate** – The router will be restored to primary (master) router once the service is restored. ● **Delayed** – The router must wait for a period of time to restore to primary (master) router when the service is restored. **Delayed Interval:** Specify the time for waiting. ● **Manual** – Restoring must be done according to the setting of **Manual Preemption Status**. **Manual Preemption Status** – Click Active or Inactive. **Manual Mode Threshold** – Set a period of time for the system to determine the master router when there is no master router detected. If the router is set as Master router, and you change the Manual Preemption Status from Active to Inactive. Once the router detects that it is in Inactive state, it will not take preemption. However, if there is no secondary router taking over the service, all the data traffic would be terminated. To solve the problem, two methods can be executed: 1. Simply reset Manual Preemption Status from Inactive to Active and then click **Apply** to save the settings. 2. Set the value for Manual Mode Threshold. After passing the time configured in Manual Mode Threshold, if the system detects no master router existing, then Manual Preemption Status will be reset to Active to locate the master router. **WAN Connection Status Detection –**Click **Enable** to make the router detecting WAN connection status. It is similar to "LAN Port Detection Mode" but will detect connection status of all enabled WAN profiles. If connection status of all enabled WAN profiles are **down**, the master router hands off its position. **LAN Port Detection Mode –** The router (with the role of Primary - Master) will detect if there is malfunction on LANs automatically. This function will force the master router to failover to other backups if any failure of LAN is detected. There are two schemes to determine the failure of LAN ports:  ● **At Least One Up** - The master router can own its position only if one LAN port is connecting. ● **All Must Be Up** - The master router can own its position only when all of LAN ports are connecting.
Settings under Active	**Authentication Key** – Type a string as the authentication key.

Item	Description
Standby	It is used for encrypting the HA session communication to prevent malicious attack. **WAN Connection Status Detection –** Click **Enable** to make the router detecting WAN connection status**.** It is similar to "LAN Port Detection Mode" but will detect connection status of all enabled WAN profiles. If connection status of all enabled WAN profiles are **down**, the master router hands off its position.

4.8.6.2 Hot Standby Profile Setup

The Hot Standby mechanism is that the router with highest priority to be Master device. And other lower priority router will be a backup device for the highest router.

When the Master device fails, one of the backup devices will be chosen by priority as the Master device to offer the network service for the connected PCs.



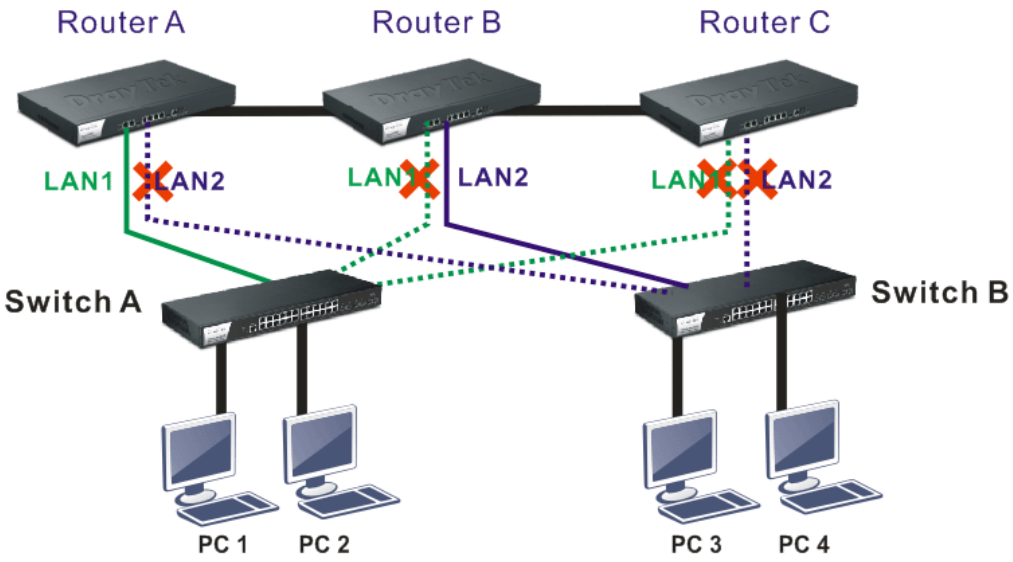
Available parameters are listed as follows:

Item	Description
HA LAN Profile	Choose one of the LAN profiles for communication in HA application.
Priority ID	“1” has the highest priority. For example, Vigor router with the priority of “1” shall play the role of Master device.
Virtual IP for Gateway	Assign an IP address as a virtual IP.
Group ID	Type a value as Group ID for identification in HA application. All of the routers under a certain HA application must be configured with the same group ID. Different HA applications shall have different group ID.
HA Status	It will display the HA status (Master or Backup) for such router.
Apply	Click it to save the configuration.

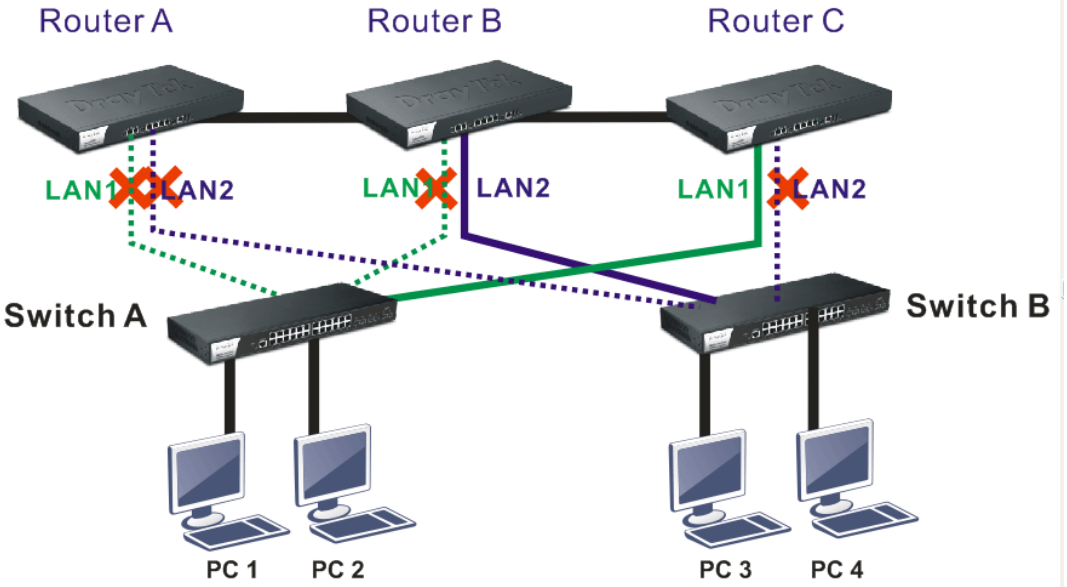
Cancel	Click it to discard the settings configured in this page.

4.8.6.3 Active-Standby Mechanism

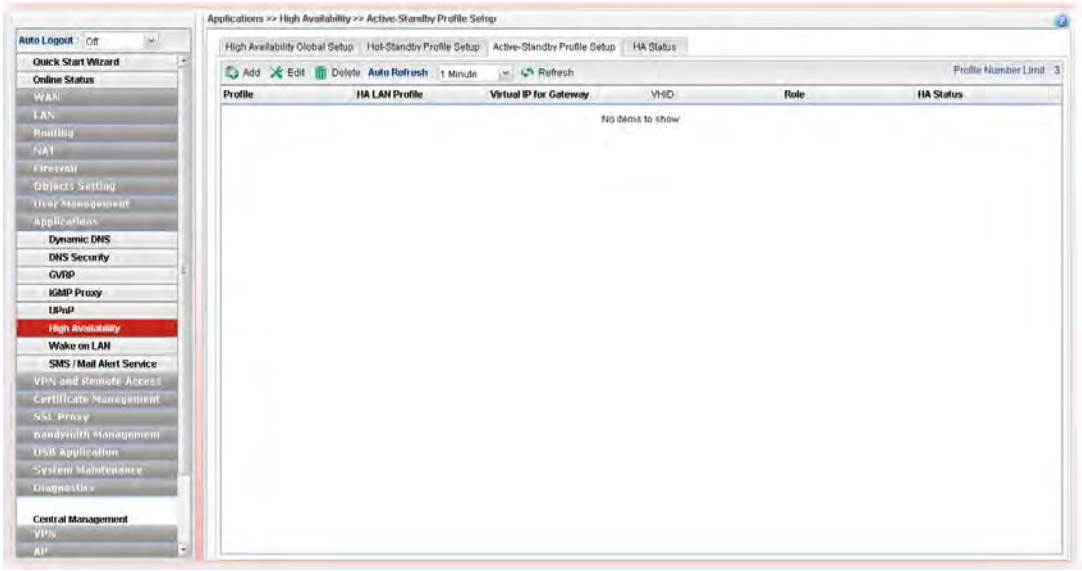
The active-standby Mechanism is that each access point in LAN will participate in different high availability sessions. All the WAN interfaces can be active which provide more flexible utilization of network service.



When LAN1 in Router A fails, one of the available line connections (e.g., LAN1 in Router C) will be selected to offer the network service for all the connected PCs.



The following page is used to create Active-Standby profiles.



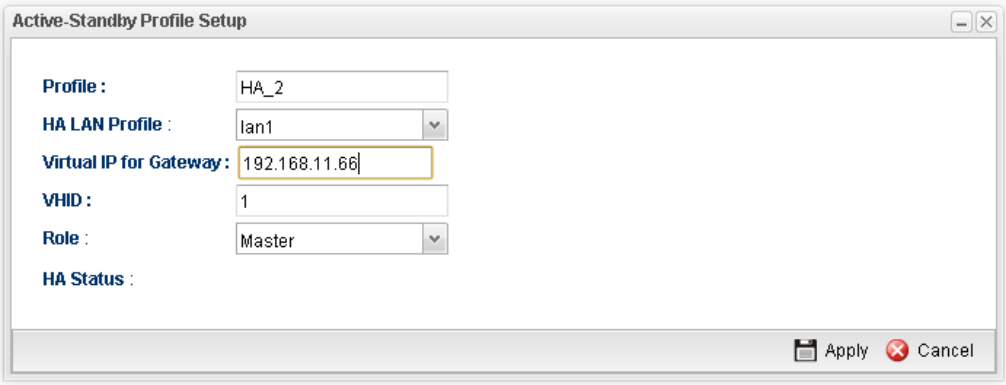
Available parameters are listed as follows:

Item	Description
Add	Add a new HA profile.
Edit	Modify the selected HA profile. To edit the profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected HA profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Profile Number Limit	Display the total number (3) of the object profiles to be created.
Profile	Display the name of the HA profile.
HA LAN Profile	Display the LAN profile used by such HA.
Virtual IP for Gateway	Display the IP address of the gateway.
VHID	Display the virtual host ID number of the profile.
Role	Display the role of this profile in the corresponding HA group.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.

How to create a new Active-Standby Profile

1. Open **Applications>>High Availability** and click the **Active Standby Profile Setup** tab.

2. Simply click the **Add** button.
3. The following dialog will appear.



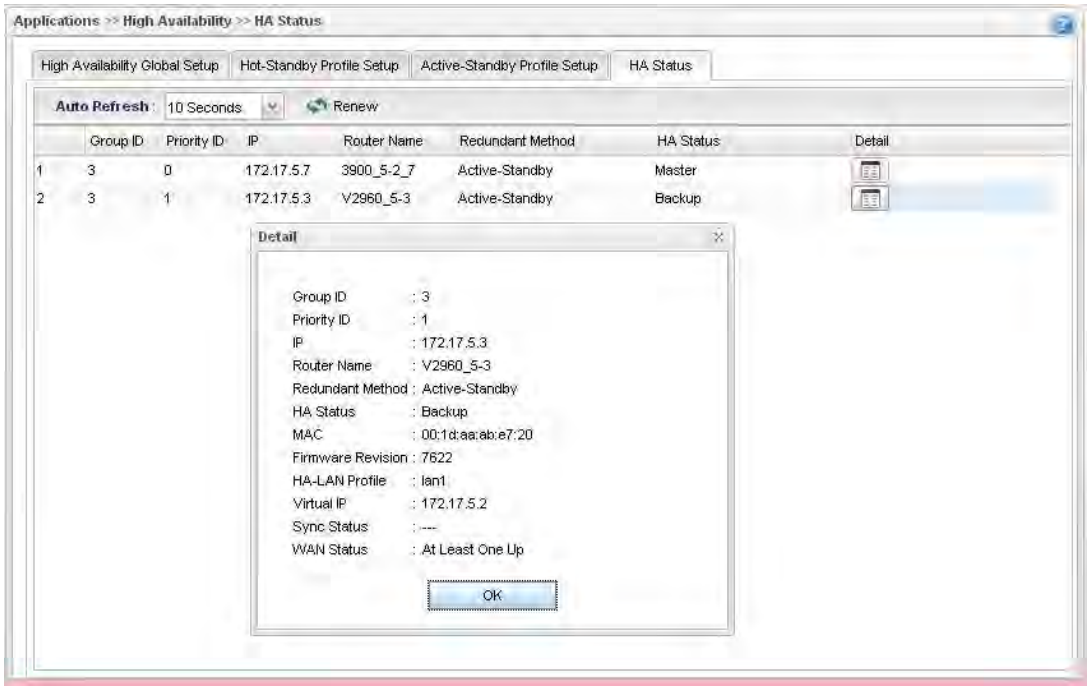
Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
HA LAN Profile	Choose one of the LAN profiles that such function will be applied to.
Virtual IP for Gateway	Assign an IP address as a virtual IP.
VHID	It means Virtual Host ID. Type a number as VHID for such function. VHID is used for Backup router to identify which Master will be backed up.
Role	LAN profiles configured for HA application can run independently and will not interfere with each other. Therefore, LAN1 (Backup) of router A can be the backup of LAN1 (Master) of router B; LAN2 (Backup) of router B can the backup of LAN2 of router A(Master). Each HA LAN profile (configured under the same router) must be specified a role as Master or Backup.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4. Enter all of the settings and click **Apply**.

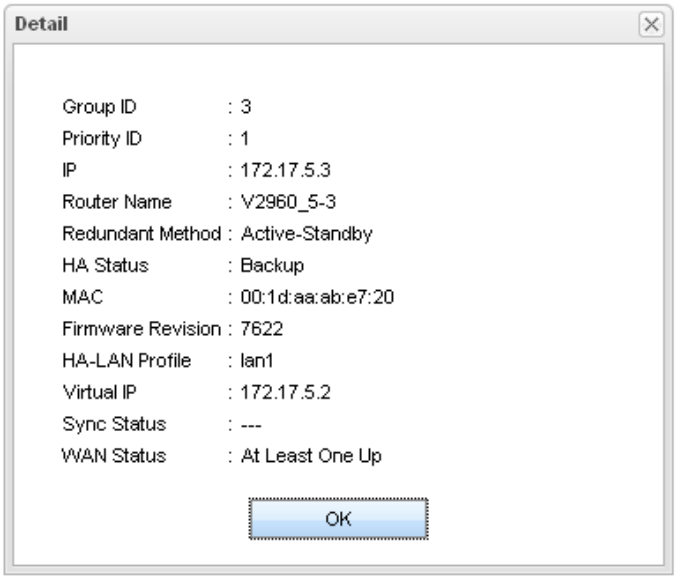
4.8.6.4 HA Status

This page displays status information of High Availability.



Each item is explained as follows:

Item	Description
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Renew	Renew current web page.
Group ID	Display the group ID number of such router.
Priority ID	Display the number which represents the priority of Vigor router in HA application. The less the number is; the higher the priority shall be. The router with the highest priority will be treated as the Master device in HA application.
IP	Display the IP address of Vigor router.
Router Name	Display the name of Vigor router.
Redundant Method	Display the method (Hot-Standby or Active-Standby) used for HA.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.

Detail	An icon displayed here allows opening a detailed settings page for HA configuration. 

4.8.7 Wake on LAN

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

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

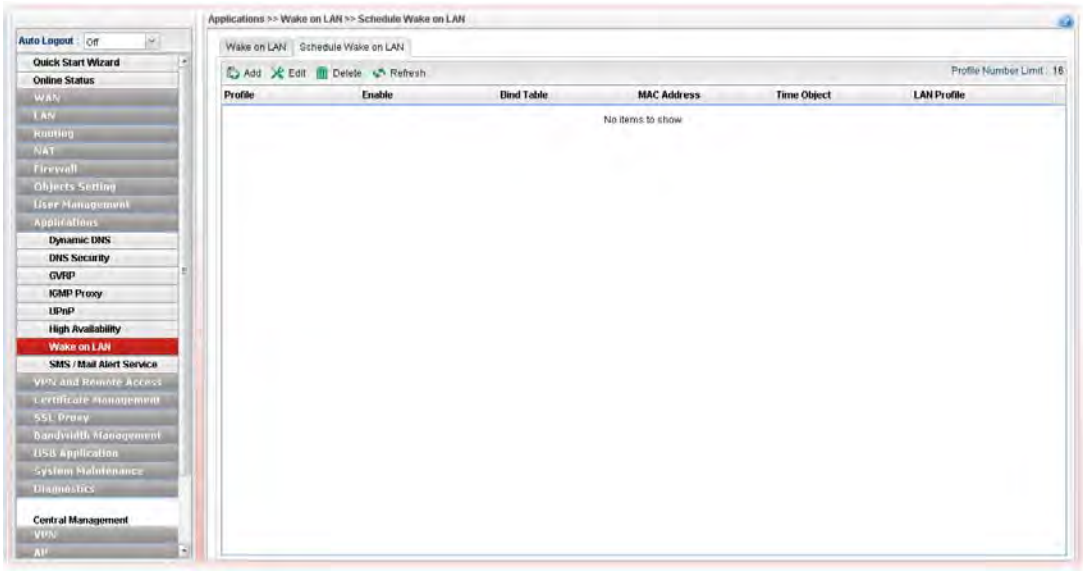
4.8.7.1 Wake on LAN

Available parameters are listed as follows:

Item	Description
Configure Bind IP to MAC	Click it to open the setting page of Bind IP to MAC.
Wake by	Three types provide for you to wake up the bound IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address. **Profile Name** – Choose a profile (created by **LAN>>Bind IP to MAC**) from the drop down list. **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 bind PCs. **LAN Profile** – Use the drop down list to choose one of the LAN profiles.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.
Delete	Click this button to remove all the settings.

4.8.7.2 Schedule Wake on LAN

This page is used to set profiles which will perform WOL based on the conditions specified by Bind Table profile, MAC address, LAN profile and time profile.

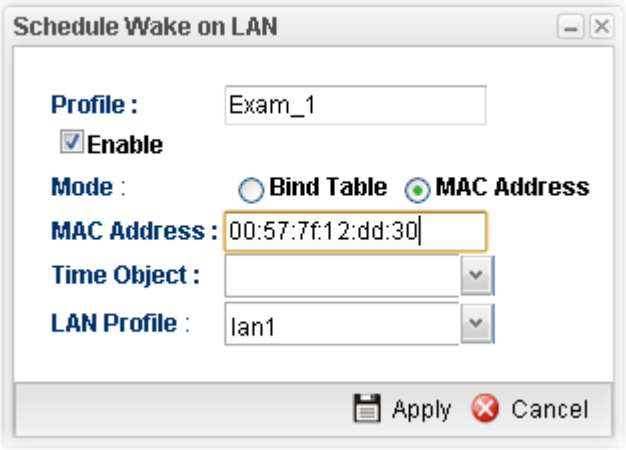


Available parameters are listed as follows:

Item	Description
Add	Add a new schedule profile.
Edit	Modify the selected schedule profile. To edit the profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected schedule profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of profile (true means Enable/ false means Disable).
Bind Table	Display the profile name from Bind Table.
MAC Address	Display the MAC address of the computer to be woke on LAN.
Time Object	Display the name of the time object selected for WOL.
LAN Profile	Display the name of LAN profile.

How to create a new schedule profile for WOL

1. Open **Applications>>Wake on LAN** and click the **Schedule Wake on LAN** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
Enable	Check the box to enable such profile.
Mode	Choose the type for data input, **Bind Table** or **MAC Address**.
Bind Table	It is available when **Bind Table** is selected as **Mode**. Choose one of the profiles listed in Bind Table.
MAC Address	It is available when **MAC Address** is selected as **Mode**. If MAC Address is selected as Mode, you have to type MAC address in this field. Then only the PC with such address will be waken up remotely.
Time Object	Choose time object profile for waking up the computer in specified time. Time object profiles can be configured in **Object Settings>>Time Object** previously.
LAN Profile	Choose one of the LAN profiles. The computers specified in the selected LAN profile will be waken up remotely.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all of the settings and click **Apply**.

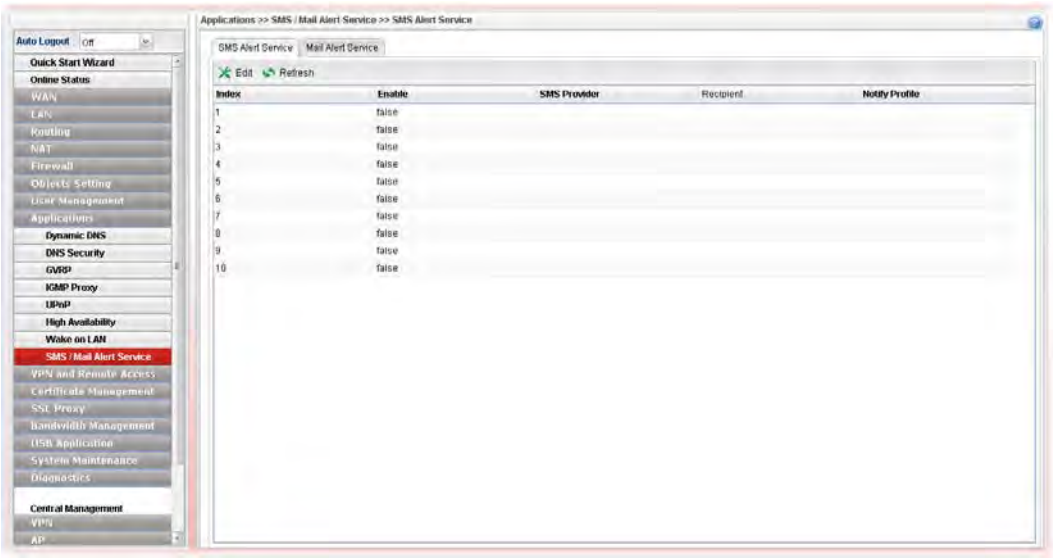
4.8.8 SMS / Mail Alert Service

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.

4.8.8.1 SMS Alert Service

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

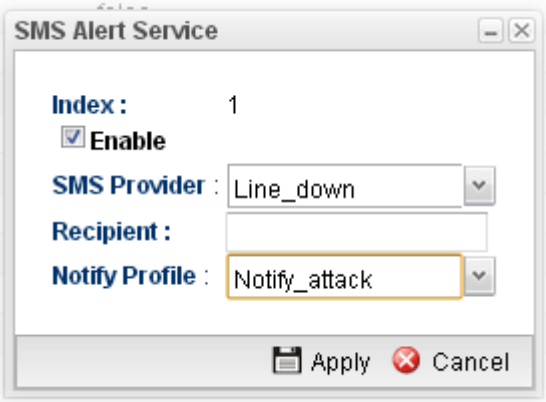


Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
SMS Provider	Display the name of the SMS provider.
Recipient	Display the one who will receive the SMS.
Notify Profile	Display the name of the notify profile.

How to edit the SMS alert service profile

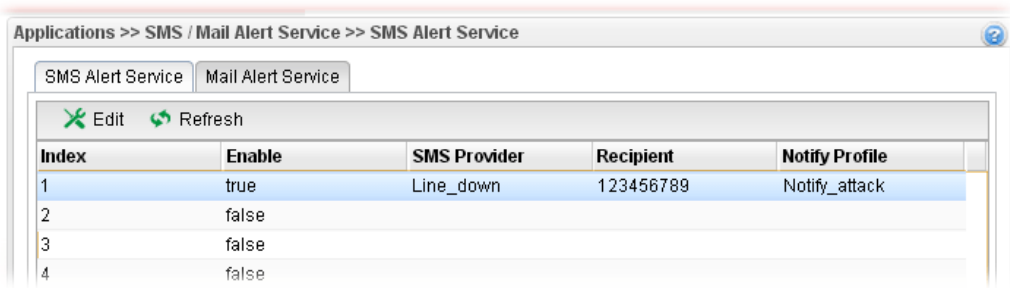
1. Open **Applications>> SMS/Mail Alert Service** and click the **SMS Alert Service** tab**.**
2. Choose one of the index numbers and click the **Edit** button.
3. The following dialog will appear.



Available parameters are listed as follows:

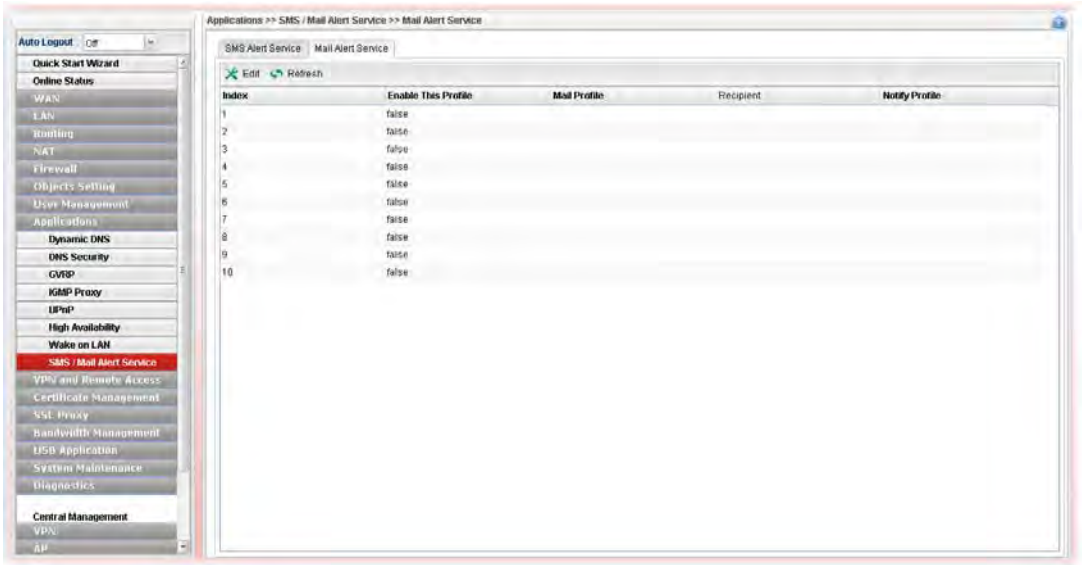
Item	Description
Enable	Check this box to enable such profile.
SMS Provider	Choose the SMS provider object profile from the drop down list. Such profiles can be created from **Object Setting>>SMS Service Object**.
Recipient	Type the cell phone number to receive the SMS.
Notify Profile	Choose a profile (specify the timing for sending SMS) from the drop down list. Such profiles can be created from **Object Setting>>Notification Object**.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all the settings and click **Apply**.
5. The SMS alert service profile has been modified.



4.8.8.2 Mail Alert Service

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.

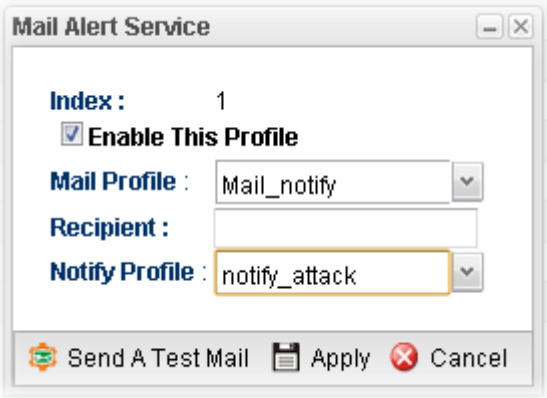


Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Mail Profile	Display the name of the mail profile.
Recipient	Display the one who will receive the mail alert.
Notify Profile	Display the name of the notify profile.

How to edit the mail alert service profile

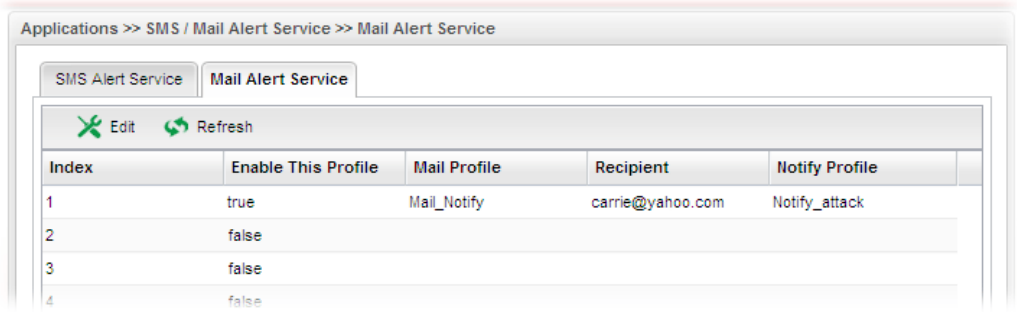
1. Open **Applications>> SMS/Mail Alert Service** and click the **Mail Alert Service** tab**.**
2. Choose one of the index numbers and click the **Edit** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Enable This Profile	Check this box to enable such profile.
Mail Profile	Choose the mail service object profile from the drop down list. Such profiles can be created from **Object Setting>>Mail Service Object**.
Recipient	Type the e-mail address for receiving the mail.
Notify Profile	Choose a profile (specify the timing for sending SMS) from the drop down list. Such profiles can be created from **Object Setting>>Notification Object**.
Send A Test Mail	Click it to send a test mail.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

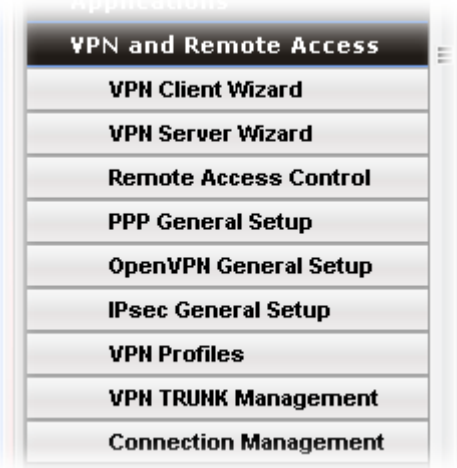
4. Enter all the settings and click **Apply**.
5. The mail alert service profile has been modified.



4.9 VPN and Remote Access

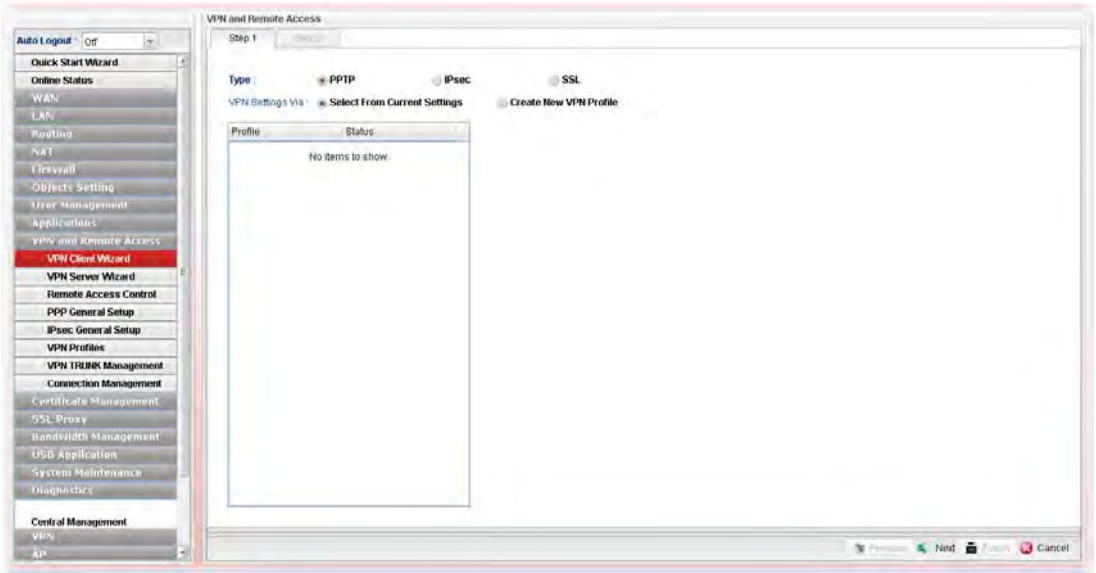
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



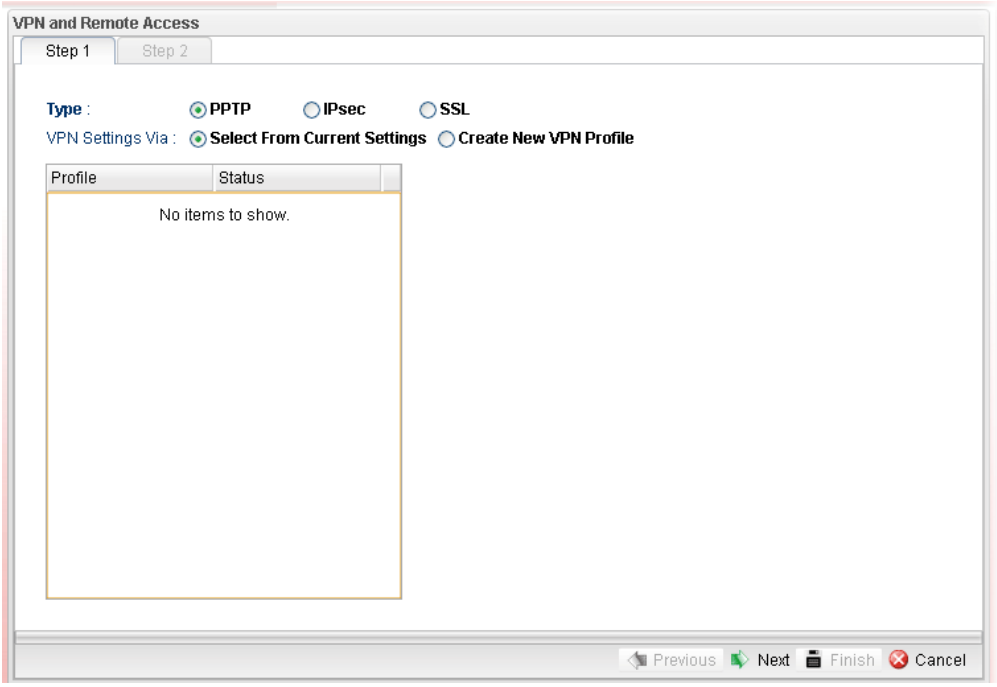
4.9.1 VPN Client Wizard

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



How to create LAN-to-LAN profile for VPN client (dial-out)

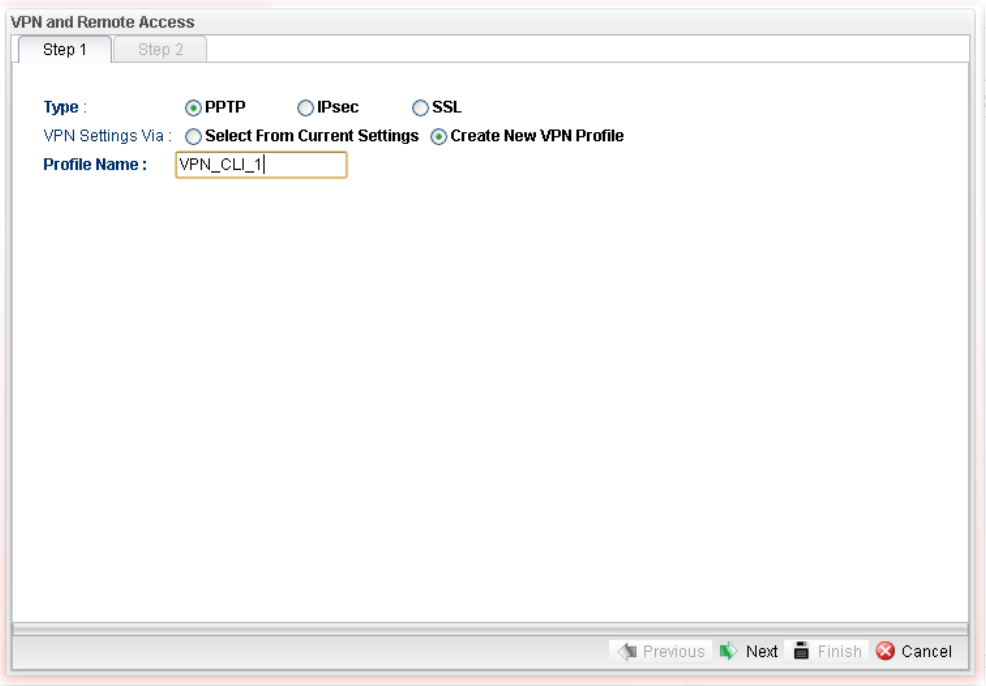
1. Open **VPN and Remote Access >> VPN Client Wizard.**
2. The following dialog will appear.



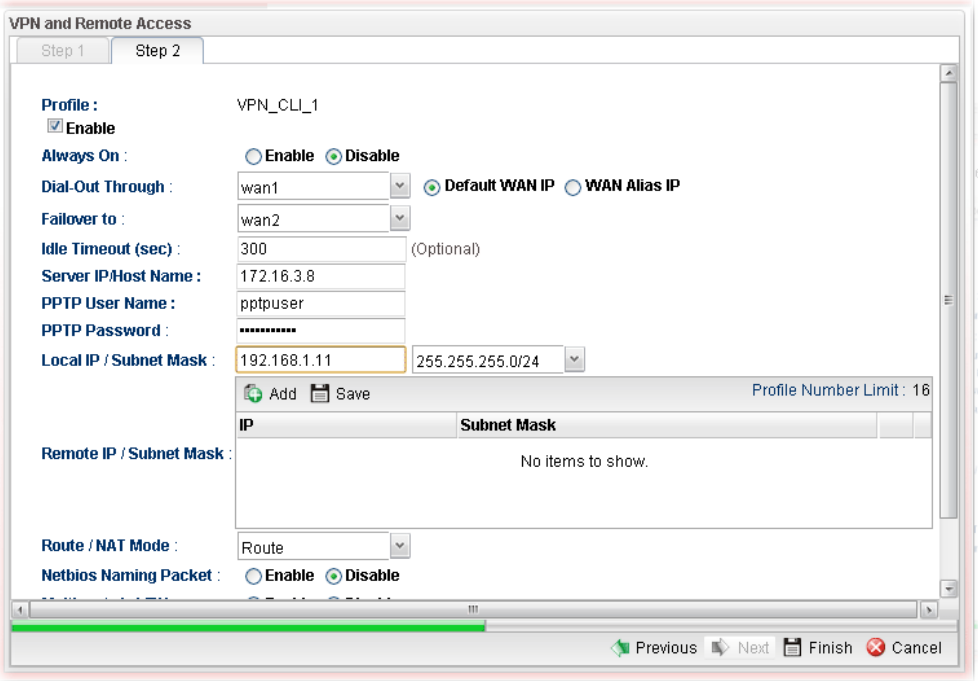
Available parameters are listed as follows:

Item	Description
Type	Specify which protocol (**PPTP**/**IPsec**/**SSL**) will be used for such VPN profile.
VPN Settings Via	**Select From Current Settings** – Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need. **Create New VPN Profile** – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of **Profile Name**. The field of Profile Name is available only when you click this setting.

3. Specify the type. Click **Create New VPN Profile** and type the name of the profile. Then, click **Next**.



4. If you choose **PPTP** as the Type, you will get the following screen:

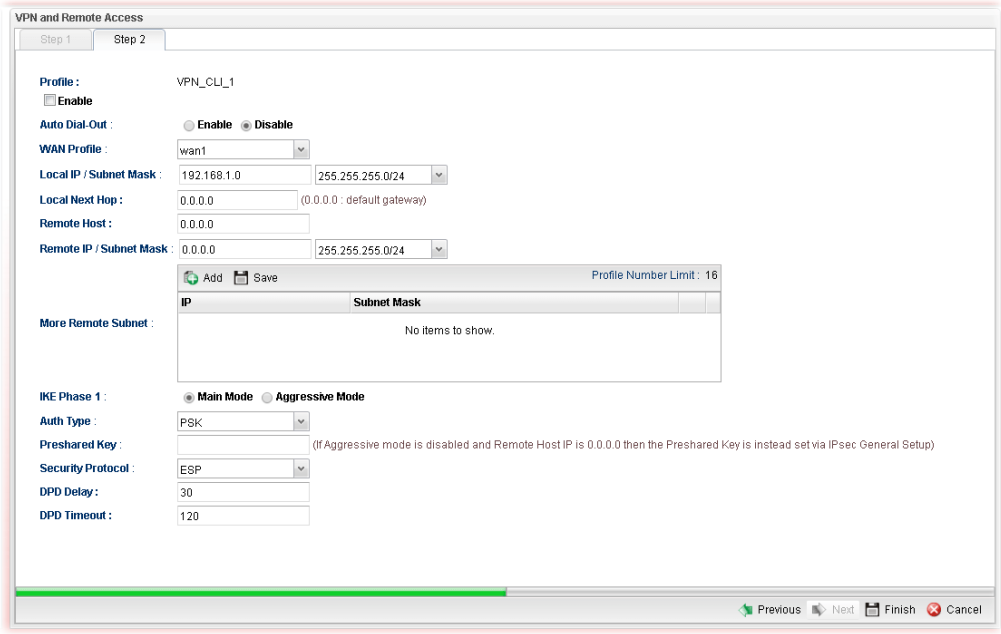


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.
Enable This Profile	Check this box to enable such profile.
Always On	Click **Enable** to make the profile being always on.

Dial-Out Through	Choose a wan profile to be used by such profile. Then, use the **default WAN IP** or specify a **WAN Alias IP** for VPN tunnel.
Failover to	Choose a wan profile which will lead the data passing through other WAN automatically when the selected WAN interface (in **Dial-Out Through**) is failover.
Idle Timeout	When Always On is disabled, you have to type the value for terminating the network connection.
Server IP/Host Name	Type the IP address or host name of PPTP server.
PPTP User Name	Type a user name for authentication in PPTP connection.
PPTP Password	Type a password for authentication in PPTP connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP/Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Route/NAT Mode	Specify the purpose for such profile.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information protocol packets via VPN connection. ● **Disable –** Disable such function. This is default setting.

If you choose **IPSec** as the Type, you will get the following screen:

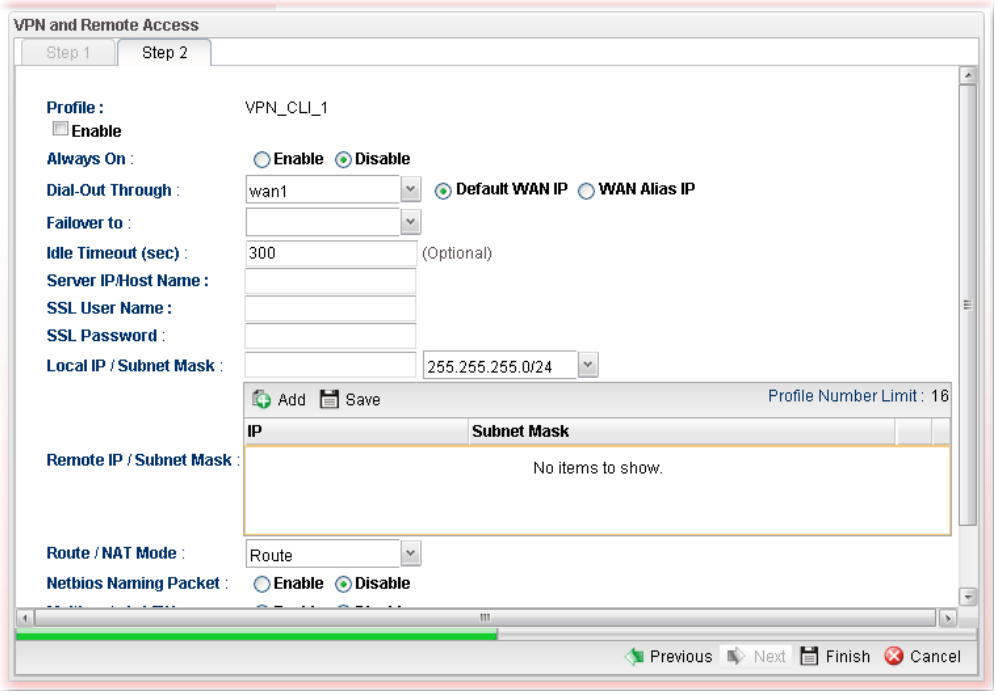


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.
Enable	Check this box to enable such profile.
Auto Dial-Out	Click Enable to enable the function of auto dial-out. **Auto Dial-Out Backup** – Specify the condition from the drop down list to activate backup dial-out.
WAN Profile	Choose a WAN profile to be used by such profile.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
More Remote Subnet	Add more remote subnet in this field if required.
IKE Phase 1	The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode. **Local ID** – Type the ID for Vigor router which can be configured by the remote end. It is available only when Aggressive Mode is enabled.

	Remote ID – It is on behalf of the IP address while identity authentication with remote VPN server. The length of ID is limited to 47 characters. It is available only when Aggressive Mode is enabled.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list if RSA is selected as Auth Type.
Preshared Key	Type a pre-shared key for authentication if PSK is selected as Auth Type.
Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
DPD Delay	DPD means dead peer detection. It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

If you choose **SSL** as the Type, you will get the following screen:

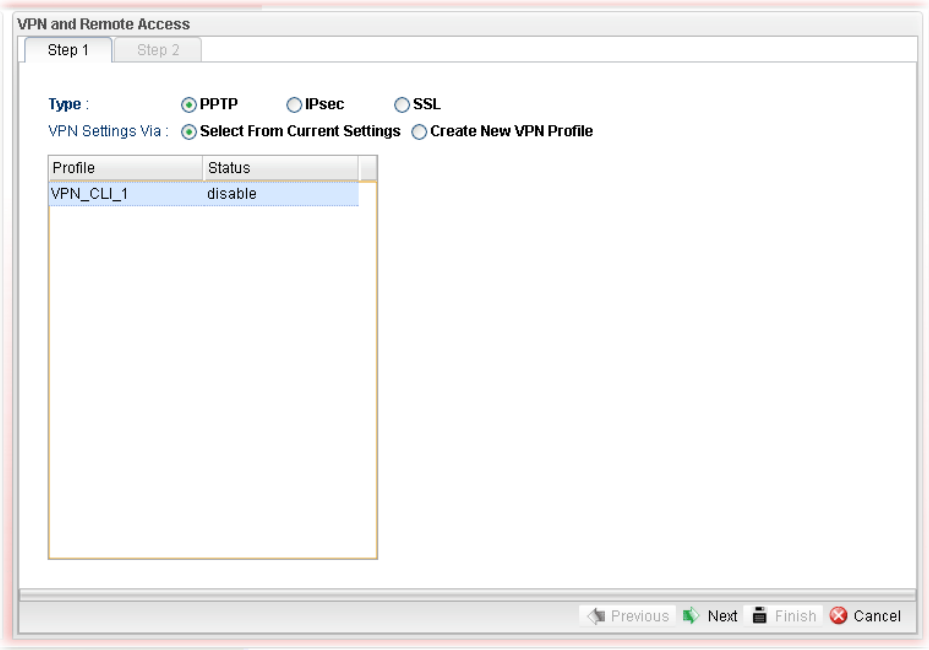


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.

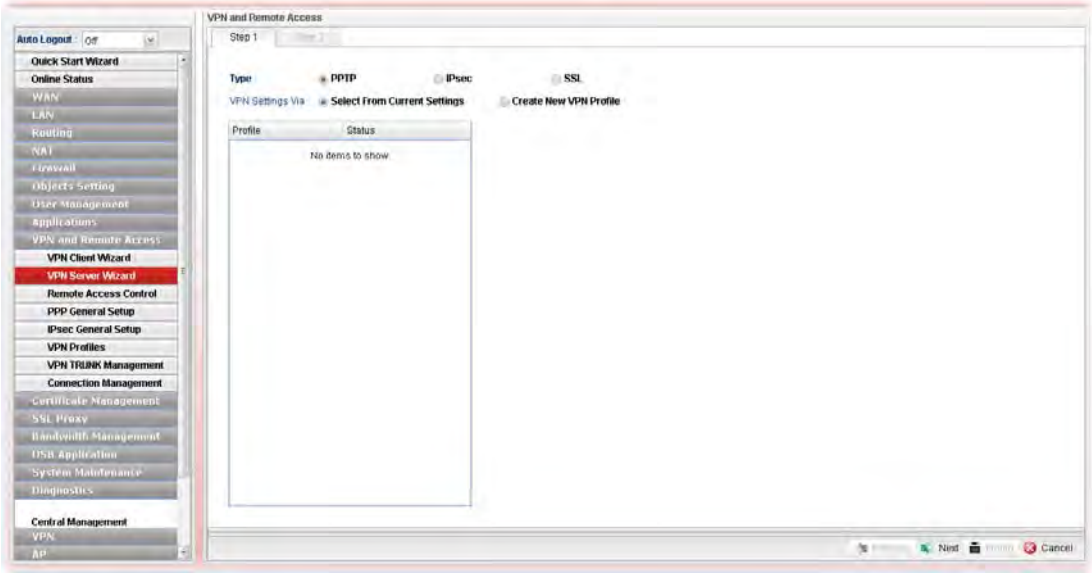
Enable	Check this box to enable such profile.
Always On	Click **Enable** to make the profile being always on.
Dial-Out Through	Choose a wan profile to be used by such profile. Then, use the **default WAN IP** or specify a **WAN Alias IP** for VPN tunnel.
Failover to	Choose a wan profile which will lead the data passing through other WAN automatically when the selected WAN interface (in **Dial-Out Through**) is failover.
Idle Timeout	When Always On is disabled, you have to type the value for terminating the network connection.
Server IP/Host Name	Type the IP address or host name of SSL VPN server.
SSL User Name	Type a user name for authentication in SSL VPN connection.
SSL Password	Type a password for authentication in SSL VPN connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP/Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Route/NAT Mode	Specify the purpose for such profile.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information packets via VPN connection. ● **Disable –** Disable such function.

5. Fill in the required information on this page and click **Finish**. A new profile has been created.



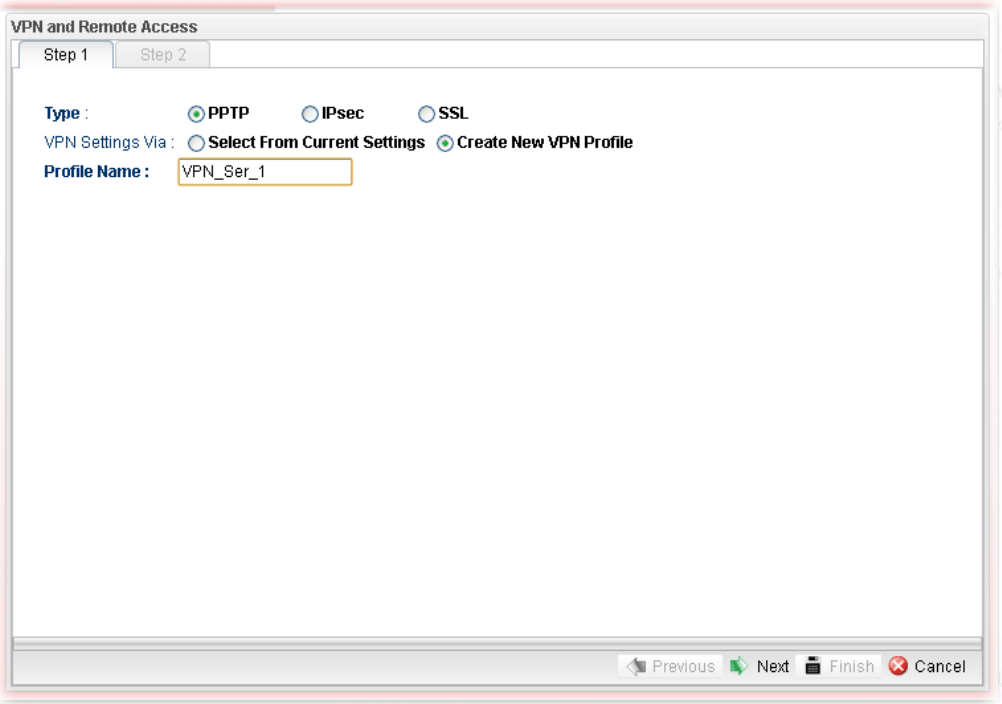
4.9.2 VPN Server Wizard

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



How to create LAN-to-LAN profile for VPN server

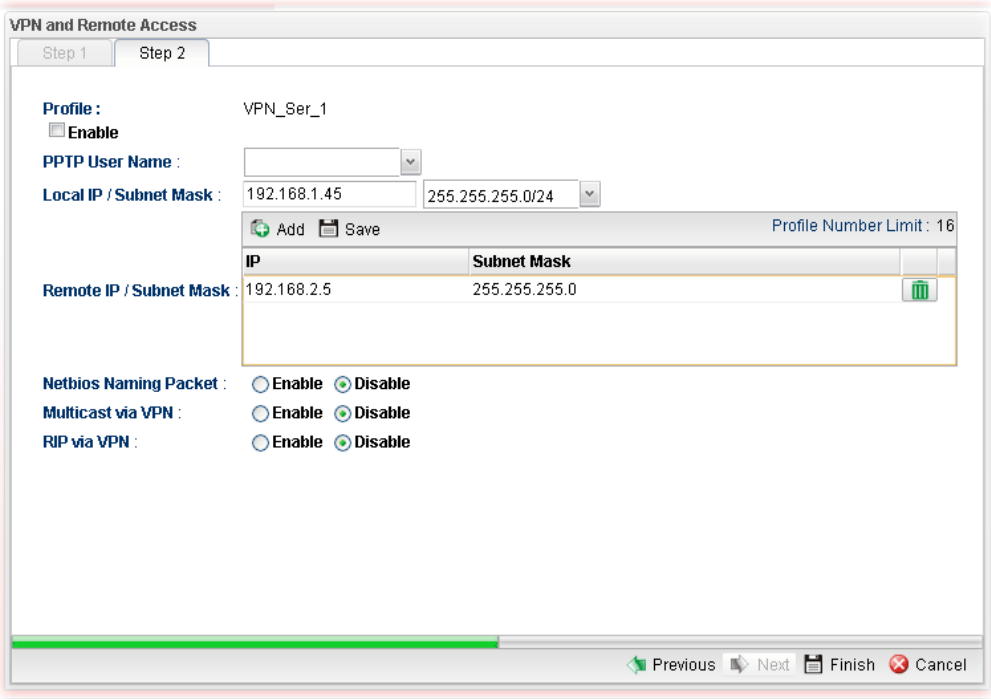
1. Open **VPN and Remote Access >> VPN Server Wizard.**
2. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Type	Specify which protocol (**PPTP/IPsec/SSL**) will be used for such VPN profile.
VPN Settings Via	**Select From Current Settings** - Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need. **Create New VPN Profile** – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of **Profile Name**. The field of Profile Name is available only when you click this setting.
Profile Name	Type a new name for such profile**.**
Next	Go to next page.
Cancel	Cancel the configuration and return to the home page of such function.

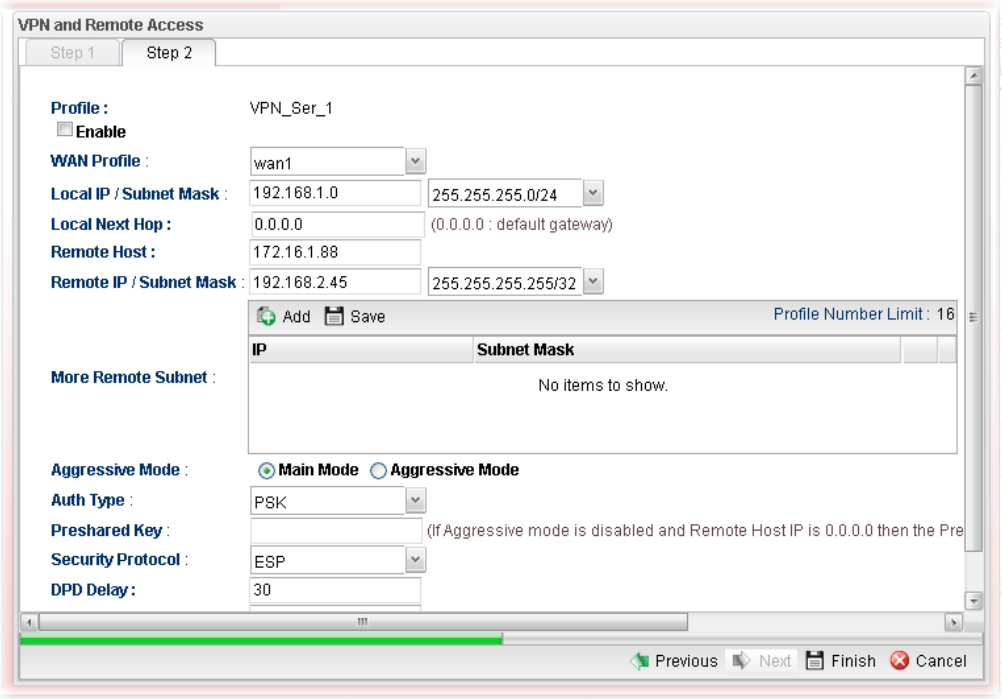
3. Click **Create New VPN Profile** and type the name of the profile. Click **Next** to get into next page. Note that if you choose **PPTP** as the **Type** in Step 2, you will see the page as below:



Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable such profile.
PPTP User Name	Choose a user for authentication in PPTP connection. Such profile shall be created in **User Management>>User Profile** previously. Otherwise, there are no selections displayed here.
Local IP / Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.

RIP via VPN	● **Enable** – Click it to exchange routing information packets via VPN connection. ● **Disable –** Disable such function. This is default setting.

If you choose **IPSec** as the **Type** in Step 1, you will get the following page:

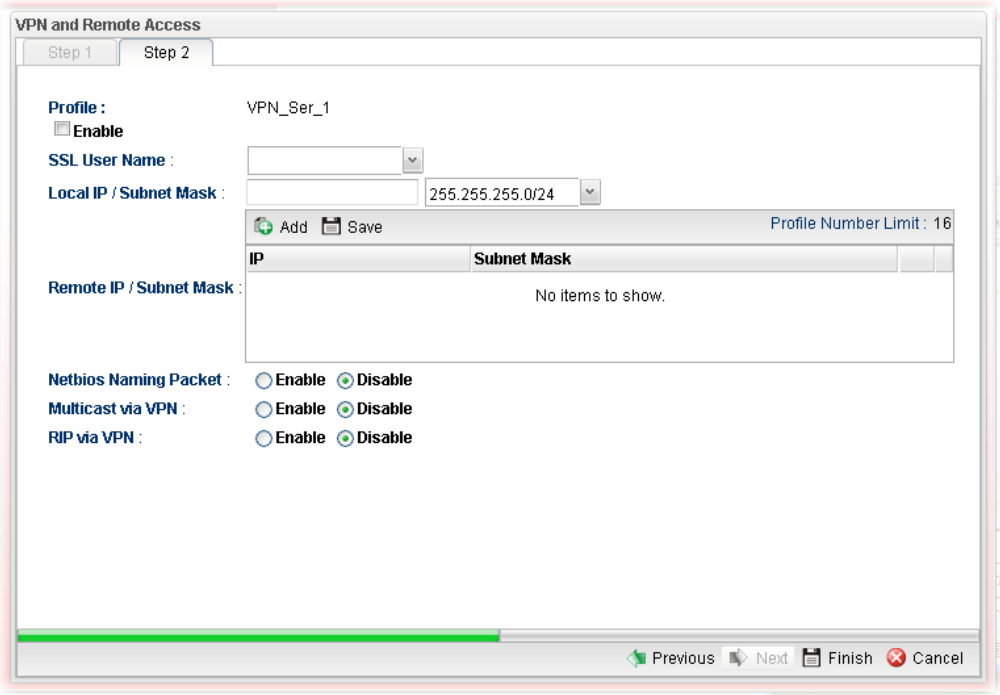


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose a WAN profile to be used by such profile.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
More Remote Subnet	Add more remote subnet in this field if required.
IKE Phase 1	The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode. **Local ID** – Type the ID for Vigor router which can be

	configured by the remote end. It is available only when Aggressive Mode is enabled. **Remote ID** – It is on behalf of the IP address while identity authentication with remote VPN server. The length of ID is limited to 47 characters. It is available only when Aggressive Mode is enabled.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list if RSA is selected as Auth Type.
Preshared Key	Type a pre-shared key for authentication if PSK is selected as Auth Type.
Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
DPD Delay	DPD means dead peer detection. It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

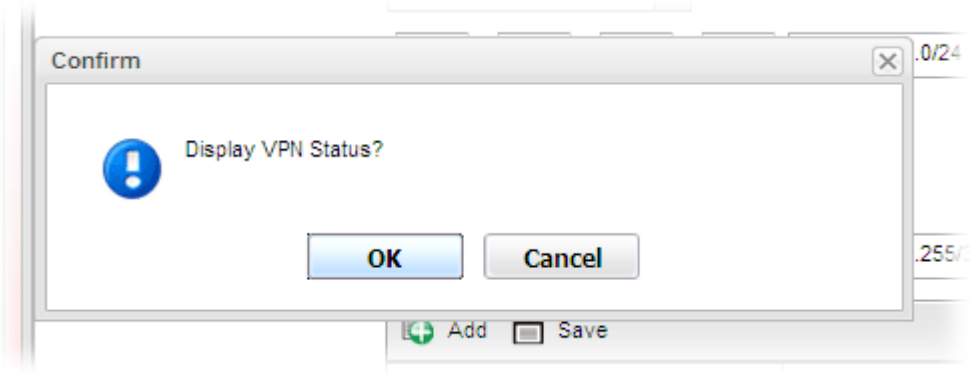
If you choose **SSL** as the **Type** in Step 1, you will get the following page:



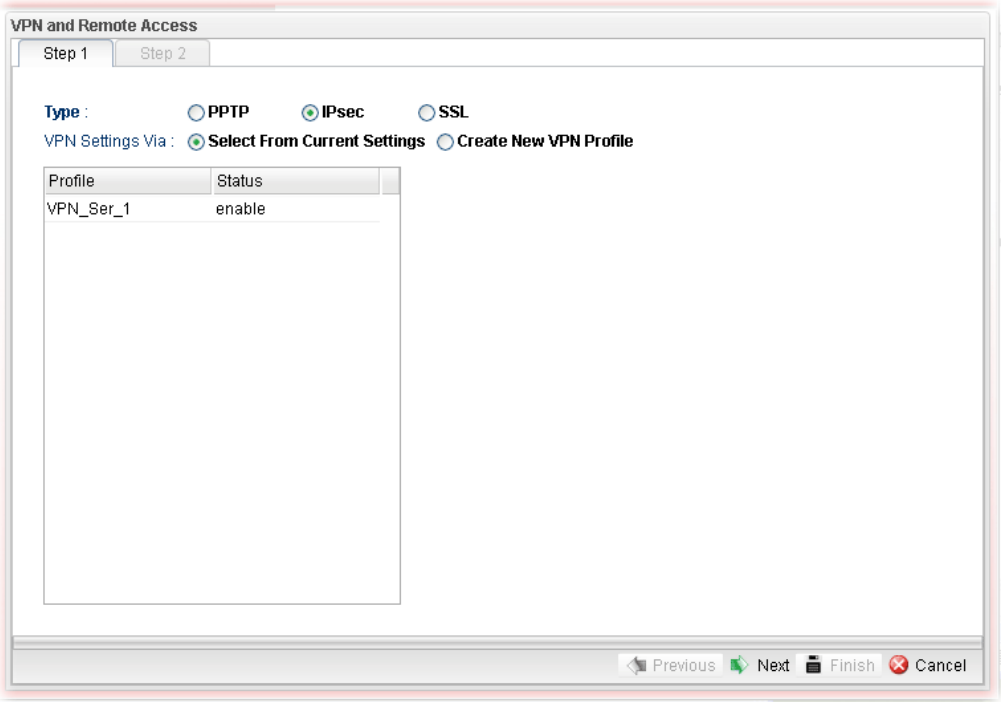
Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable such profile.
SSL User Name	Choose a user for authentication in SSL connection. Such profile shall be created in **User Management>>User Profile** previously. Otherwise, there are no selections displayed here.
Local IP / Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information

	packets via VPN connection. ● **Disable –** Disable such function. It is default setting.

4. Fill in the required information on this page and click **Finish**. A pop-up window will appear.

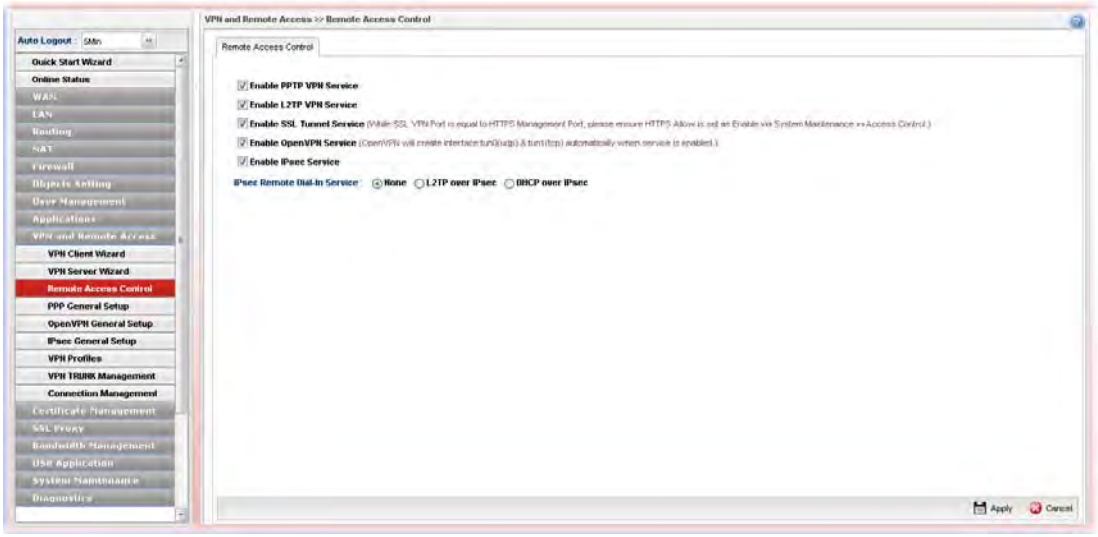


5. Click **OK.** Then, return to **VPN and Remote Access>>VPN Server Wizard.** The new added VPN server profile will be displayed on the screen.



4.9.3 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service (e.g., PPTP VPN, L2TP VPN, SSL VPN, OpenVPN, IPsec etc.) of Vigor Router to allow VPN tunnel pass through.



Available parameters are listed as follows:

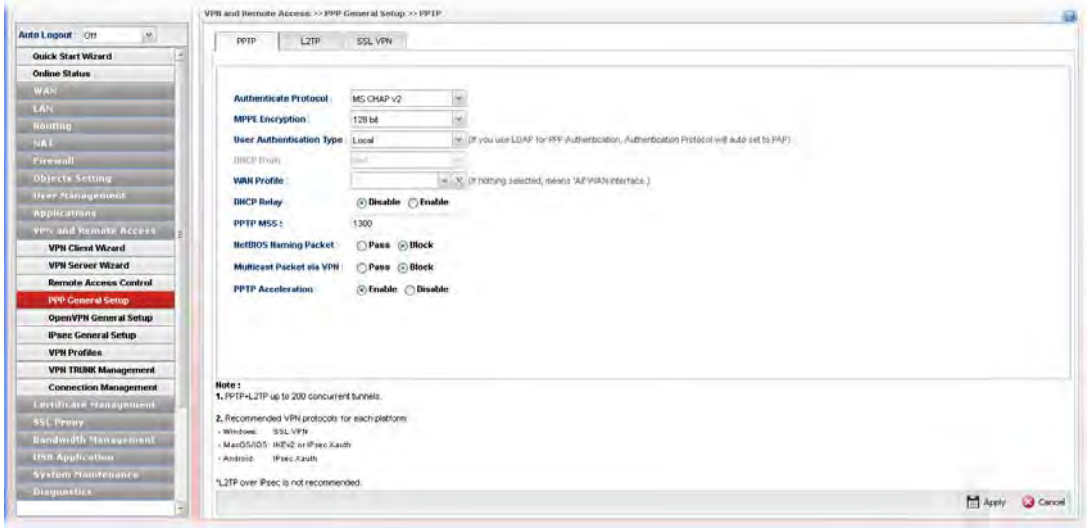
Item	Description
Enable PPTP/L2TP VPN Service / SSL Tunnel / OpenVPN Service / IPsec Service	Check the box(es) to enable the service.
IPSec Remote Dial-In Service	Choose one of the services by clicking on the radio button.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.9.4 PPP General Setup

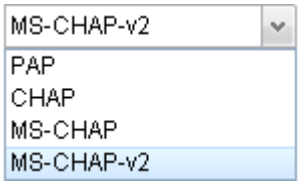
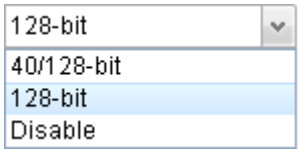
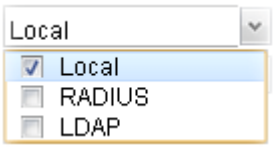
Remote users can connect to the site, host, server and etc. via VPN connection built between the router and the users by authentication procedure.

4.9.4.1 PPTP

This page display current status for VPN tunnel built with PPTP protocol.



Available parameters are listed as follows:

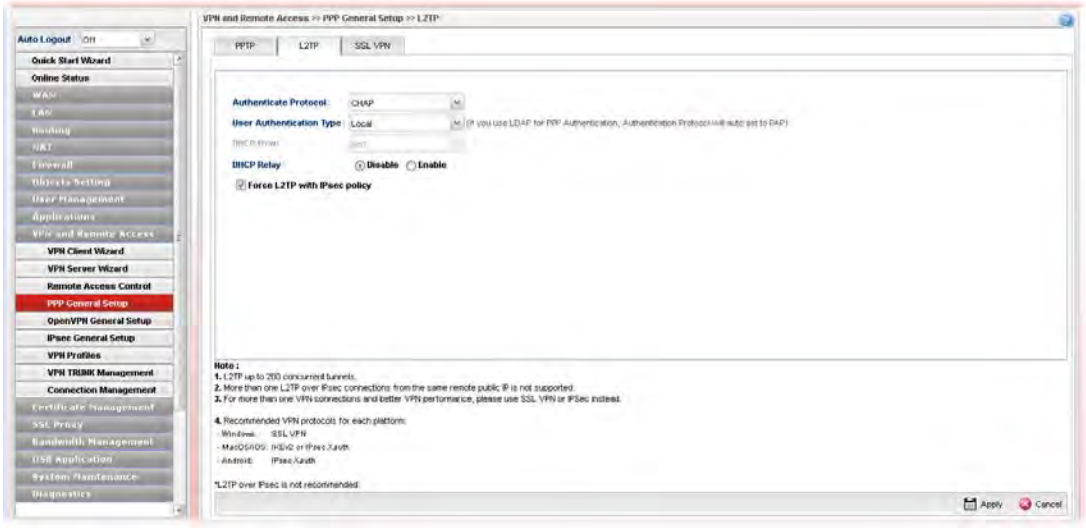
Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
MPPE Encryption	Specify one of the encryptions for such server. It is available only when MS-CHAP or MS-CHAP_v2 is selected. 
User Authentication Type	Set user authentication to **Local** server, **RADIUS** server or **LDAP** server. 

LDAP profiles	Choose a LDAP profile for PPTP Server if **LDAP** is selected as user authentication type. To clear the selected one, click to remove current object selections.
DHCP from	Choose a LAN profile for PPTP Server if **RADIUS** is selected as user authentication type.
WAN Profile	Choose an interface (e.g., wan1, usb1) profile.
DHCP Relay	**Enable** - Let the router assign IP address to every host in the LAN. ● **DHCP Server Location** - It is available when **DHCP Relay** is enabled. Choose the WAN/LAN interface for the DHCP server. ● **DHCP Server IP Address** - It is available when **DHCP Relay** is enabled. 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. **Disable** - Let you manually assign IP address to every host in the LAN.
PPTP MSS	Type the maximum segment size (MSS) for PPTP VPN tunnel.
NetBIOS Naming Packet	**Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast Packet via VPN	Some programs might send multicast packets via VPN connection. ● **Pass** – Click this button to let multicast packets pass through the router. ● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
PPTP Acceleration	**Enable –** Click it to make PPTP acceleration for VPN.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

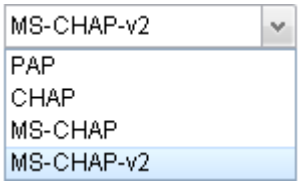
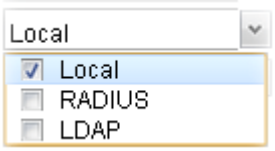
Enter all the settings and click **Apply**.

4.9.4.2 L2TP

This page display current status for VPN tunnel built with L2TP protocol.



Available parameters are listed as follows:

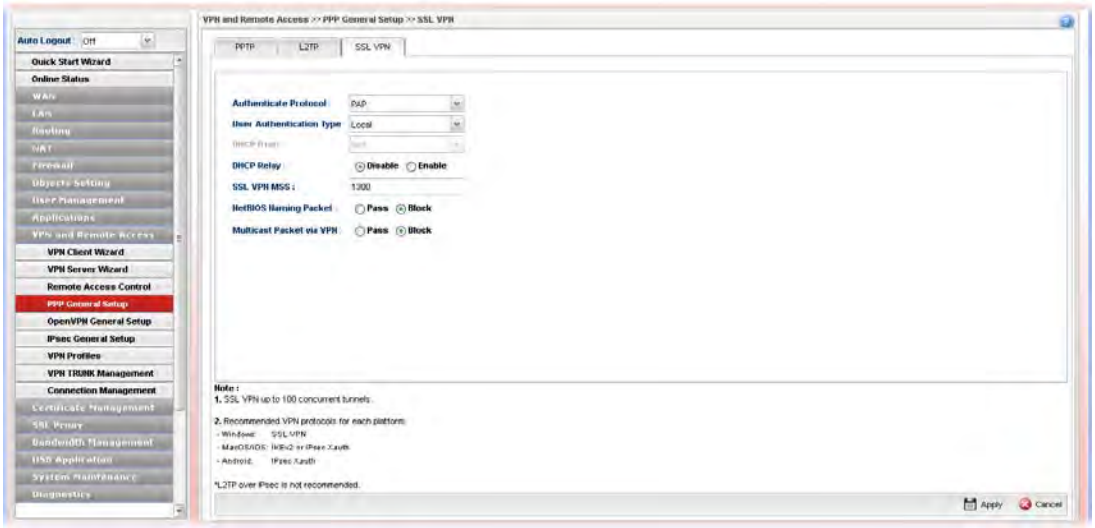
Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
User Authentication Type	Set user authentication to **Local** server or **RADIUS** server. 
LDAP profiles	Choose a LDAP profile for PPTP Server if **LDAP** is selected as user authentication type. To clear the selected one, click to remove current object selections.
DHCP from	Choose a LAN profile for L2TP Server if **RADIUS** is selected as user authentication type.
DHCP Relay	**Enable** - Let the router assign IP address to every host in the LAN. ● **DHCP Server Location** - It is available when **DHCP Relay** is enabled. Choose the WAN/LAN interface for

	the DHCP server. ● **DHCP Server IP Address** - It is available when **DHCP Relay** is enabled. 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. **Disable** - Let you manually assign IP address to every host in the LAN.
Force L2TP with IPsec policy	If it is checked, the router will use L2TP with IPsec policy for VPN connection.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

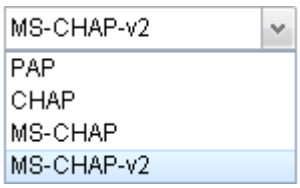
Enter all the settings and click **Apply**.

4.9.4.3 SSL VPN

This page display current status for VPN tunnel built with SSL protocol.



Available parameters are listed as follows:

Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
User Authentication	Set user authentication to **Local** server or **RADIUS** server.

Type	
LDAP profiles	Choose a LDAP profile for PPTP Server if **LDAP** is selected as user authentication type. To clear the selected one, click to remove current object selections.
DHCP from	Choose a LAN profile for L2TP Server if **RADIUS** is selected as user authentication type.
DHCP Relay	**Enable** - Let the router assign IP address to every host in the LAN. ● **DHCP Server Location** - It is available when **DHCP Relay** is enabled. Choose the WAN/LAN interface for the DHCP server. ● **DHCP Server IP Address** - It is available when **DHCP Relay** is enabled. 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. **Disable** - Let you manually assign IP address to every host in the LAN.
SSL VPN MSS	Type the maximum segment size (MSS) for SSL VPN tunnel.
NetBIOS Naming Packet	**Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast Packet via VPN	Some programs might send multicast packets via VPN connection. **Pass** – Click this button to let multicast packets pass through the router. **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.9.5 OpenVPN General Setup

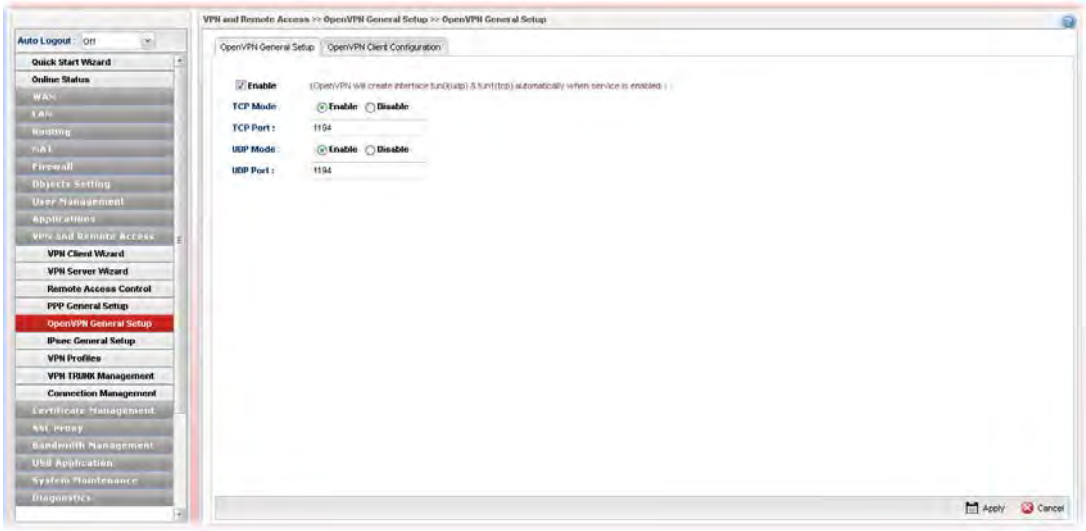
In general, both server and client must use routers with the same model to make a successful VPN. If not, a problem would be caused due to wrong brands of models. Main advantage for OpenPVN is that it is a mechanism which is easy for users to build safe and reliable virtual network, even if the brand or model of router used by both ends are totally different.

OpenVPN allows Vigor router to establish an instant VPN connection across the Internet with any router (e.g., non-Vigor router) by using simple and easy configuration.

With integration of OpenVPN, Vigor2960 can help users to achieve a more robust, reliable and secure private connections for business needs.

4.9.5.1 OpenVPN General Setup

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

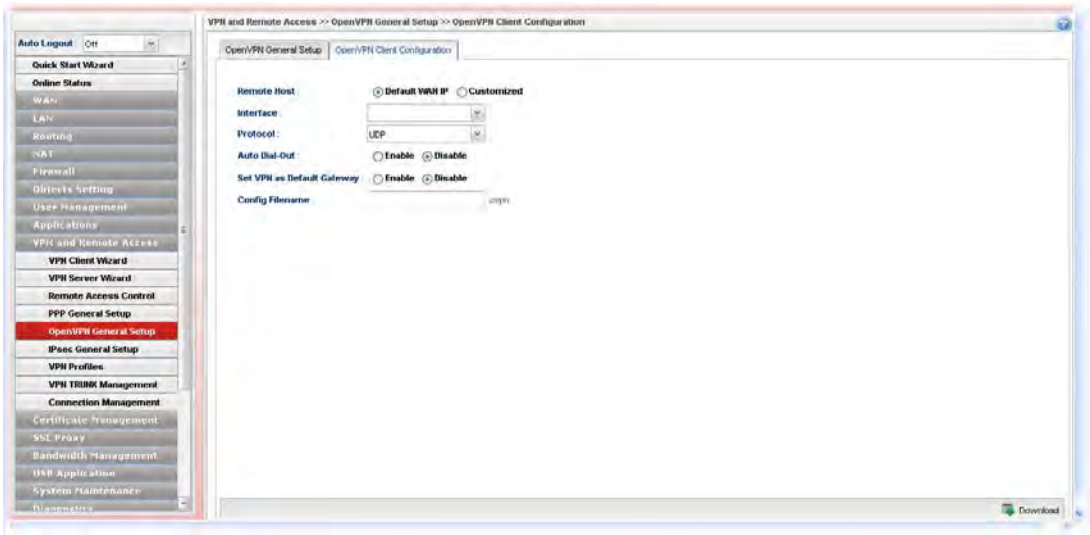


Available parameters are listed as follows:

Item	Description
Enable	Click it to enable the function of OpenVPN between VPN client and VPN server.
TCP Mode	**Enable** – Click it for entering TCP port number.
TCP Port	Enter a number for TCP protocol.
UDP Mode	**Enable** – Click if for entering UDP port number.
UDP Port	Enter a number for UDP protocol.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.9.5.2 OpenVPN Client Configuration

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



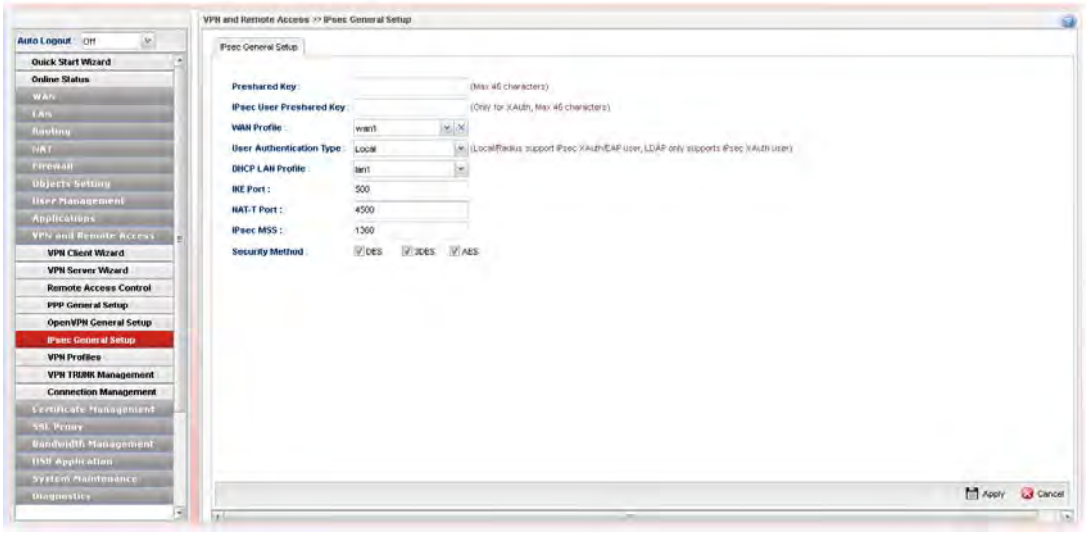
Available parameters are listed as follows:

Item	Description
Remote Host	Specify the type used for remote host. **Default WAN IP –** Click it to use default WAN IP of remote host. You need to choose an interface for such VPN. **Customized –** Click it to specify URL for the remote host. You need to enter the URL content in the field of **Host.**
Interface	It is available when **Default WAN IP** is selected as Remote Host. Specify a WAN interface (e.g., WAN1/2) for setting up VPN connection. If there is any IP alias setting created for the selected WAN interface, you can choose one of the IP alias for the remote client to connect to.
Host	It is available when **Customized** is selected as Remote Host.
Protocol	Simply choose UDP or TCP as protocol for building OpenVPN connection between the server and the remote client.
Auto Dial-Out	**Enable** – Once the OpenVPN tunnel is disconnected, Vigor router will dial out for rebuilding the VPN automatically. **Disable** – When the OpenVPN tunnel is disconnected, Vigor router will not dial out for rebuilding the VPN automatically.
Set VPN as Default Gateway	After importing the configuration file to remote CPE's device, all the data can be transmitted through the original gateway or such OpenVPN tunnel. **Enable** – All the data traffic will be processed through such OpenVPN tunnel. **Disable** – All the data traffic will be processed through original gateway.
Config Finename	Type a name for the configuration file.
Download	The settings in this page can be saved as a file after clicking such button. Later, the downloaded file can be imported to

	the VPN client for building OpenVPN connection.

4.9.6 IPSec General Setup

The IPSec services can provide access control, connectionless integrity, data origin authentication, rejection of replayed packets that is a form of partial sequence integrity, and confidentiality by encryption. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.



Available parameters are listed as follows:

Item	Description
Preshared Key	Specify a key for IKE authentication.
IPsec User Preshared Key	Specify a key for IPsec XAuth/EAP user authentication.
WAN Profile	Choose a WAN interface profile to be used. To clear the selected one, click to remove current profile selections.
User Authentication Type	Set IPsec user authentication to **Local** server, **LDAP** server or **RADIUS** server.
DHCP LAN Profile	Choose one of the LAN profiles for VPN.
IKE Port	Type the UDP port number for Internet Key Exchange (IKE) traffic to the VPN server.
NAT-Port	Type the UDP port number for IPSec network address translator traversal (NAT-T) traffic.
IPsec MSS	Type the port number for IPSec MSS.
Security Method	Select the encryption method (DES, 3DES, AES) for the security of data transmission.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

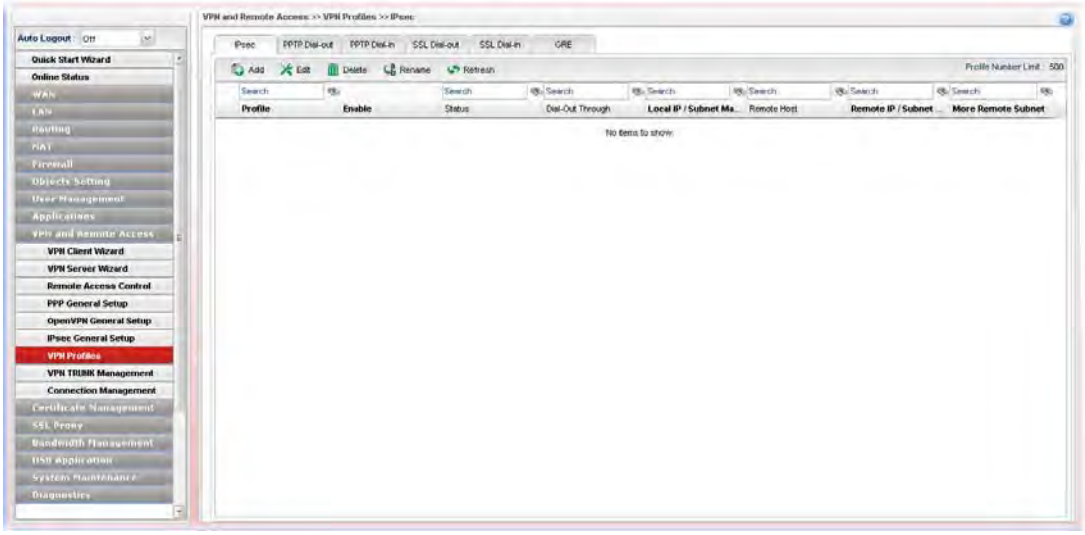
Enter all the settings and click **Apply**.

4.9.7 VPN Profiles

The router allows you to create VPN profiles via the protocol of IPSec or PPTP (dial-in or dial-out).

The router supports up to **500** VPN (tunnels or profiles) simultaneously. The following figure shows the summary table.

4.9.7.1 IPsec Tunnel



Each item will be explained as follows:

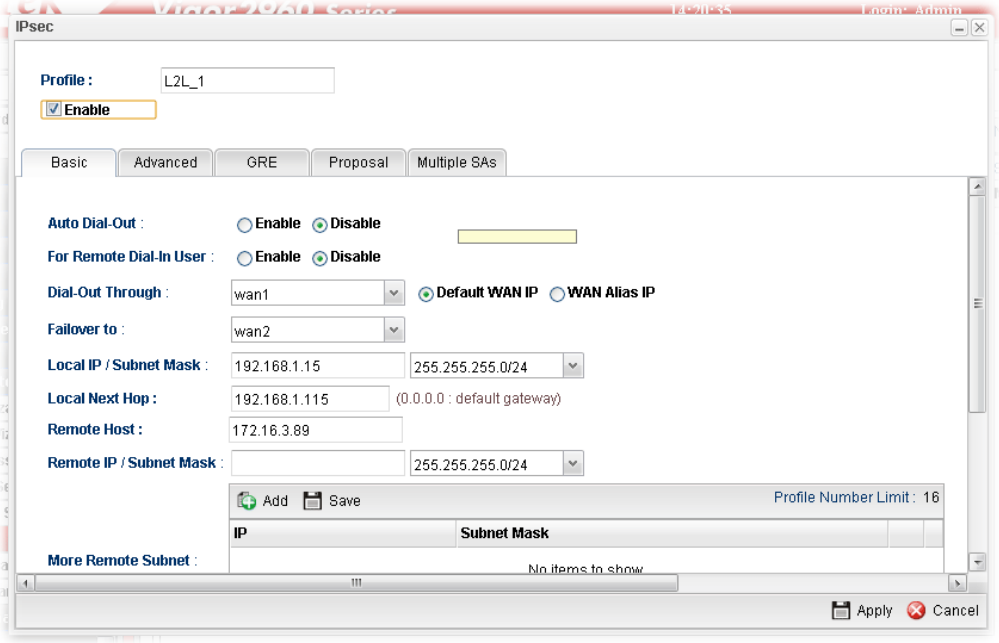
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (500) of the object profiles to be created.
Profile	Display the name of LAN to LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Dial-Out Through	Display the WAN interface selected for the profile.
Local IP / Subnet Mask	Display the LAN IP address with subnet mask of this profile.

Remote Host	Display the name of the remote host of this profile.
Remote IP / Subnet Mask	Display the WAN IP address with subnet mask of this profile.
More Remote Subnet	Display other LAN IP addresses with subnet mask which can be used of this profile.

How to create an IPSec VPN profile

The IPSec services can provide access control, connectionless integrity, data origin authentication, rejection of replayed packets that is a form of partial sequence integrity, and confidentiality by encryption. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

1. Open **VPN and Remote Access >>VPN Profiles.**
2. Simply click the **Add** button.
3. The following dialog will appear. Click the **Basic** tab to configure the settings.

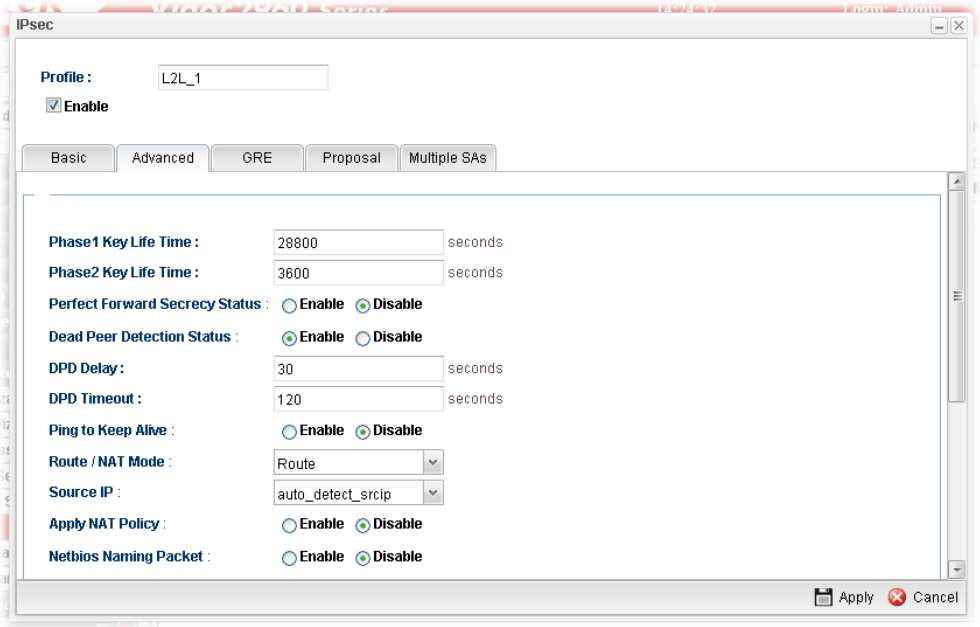


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **IPSec** for this case.
Basic	**Always On** – Click **Enable** to make router always keeping connection. **For Remote Dial-In User**- Click **Enable** to allow the connection via IPSec remote dial-in host. **Dial-Out Through-** Choose a wan profile to be used by

	such profile. **Failover to** – Choose a wan profile which will lead the data passing through other WAN automatically when the selected WAN interface (in **Dial-Out Through**) is failover. **Local IP/Subnet -** Type the IP address and subnet mask of local host. **Local Next Hop -** Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank). **Remote Host -** Type the WAN IP address for the remote host. **Remote IP / Subnet Mask -** Type the LAN IP address and LAN subnet mask for the remote host. **More Remote Subnet** – Add more remote subnet in this field if required. **IKE Protocol** – Choose IKEv1 or IKEv2. **IKE Phase 1** - Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode. **Auth Type -** The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile. **Local Certificate -** Choose a local certificate from the drop down list if RSA is selected as Auth Type. **Local Peer ID** –Type the ID for Vigor3900 which can be configured by the remote end. It is available for Aggressive Mode enabled only. **Remote Peer ID –** Peer ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters. It is available for Aggressive Mode enabled only. **Preshared Key** – Specify a key for IKE authentication if PSK is selected as Auth Type. **Security Protocol –** Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

The **Advanced** tab provides more parameters of IPsec tunnel, change setting if needed.

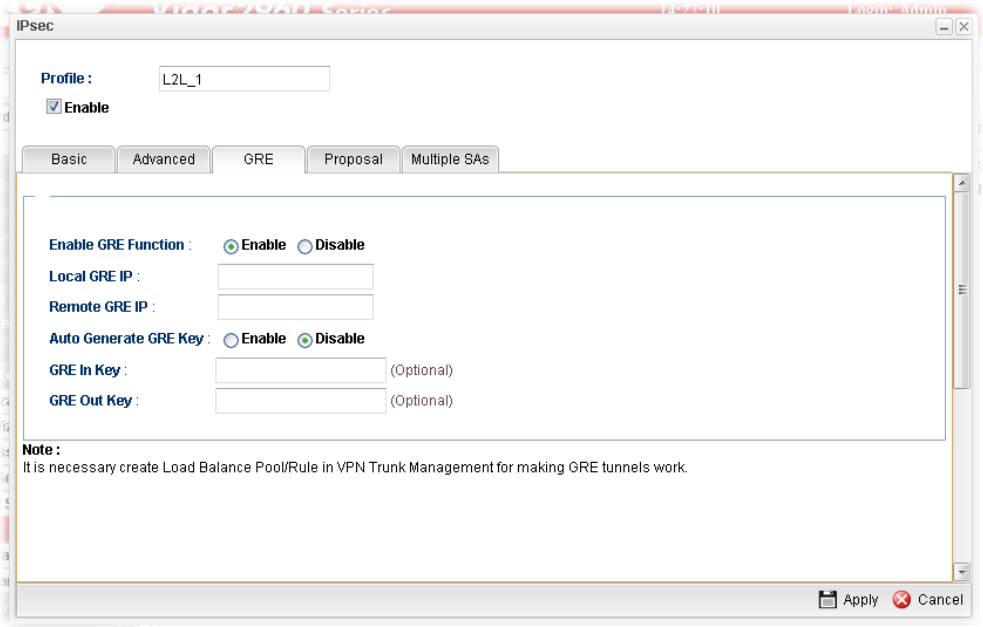


Available parameters are listed as follows:

Item	Description
Phase 1 Key Life Time	The rekey-renegotiated period of the IKE Phase1 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).
Phase 2 Key Life Time	The rekey-renegotiated period of the IKE Phase 2 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).
Perfect Forward Secrecy Status	Enables the PFS function. A new Diffie-Hellman Key Exchange is included every time an encryption and/or authentication key are computed on PFS.
Dead Peer Detection Status	**Enable** – Click it to enable DPD. When there is no traffic through the IPSec tunnel, both server and the client will send the DPD packet to each other to ensure the IPSec tunnel connection is active still. **Disable** – Click it to disable DPD.
DPD Delay	The keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	The timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.
Ping to Keep Alive	**Enable** – Click it to enable such function. **Ping to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.
Route/NAT Mode	If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route

	Mode.
Source IP	Choose one of the LAN profiles as a source IP.
Apply NAT Policy	**Enable** – This option allows for performing one-to-one NAT for all traffic flowing across the VPN. **Translated Local Network** – Specify the IP address with subnet mask of the network that all traffic will be translated into.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information protocol packets via VPN connection. ● **Disable –** Disable such function. This is default setting.
Packet-Triggered	● **Enable** – Click it to establish on-demand IPsec VPN. The IPsec negotiation will be triggered by packets sent to remote IP/subnet. This is default setting. ● **Disable –** Disable such function.
Force UDP Encapsulation	● **Enable** – Click it to encapsulate all ISAKMP packets with NAT-T encapsulation. ● **Disable –**This is default setting.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

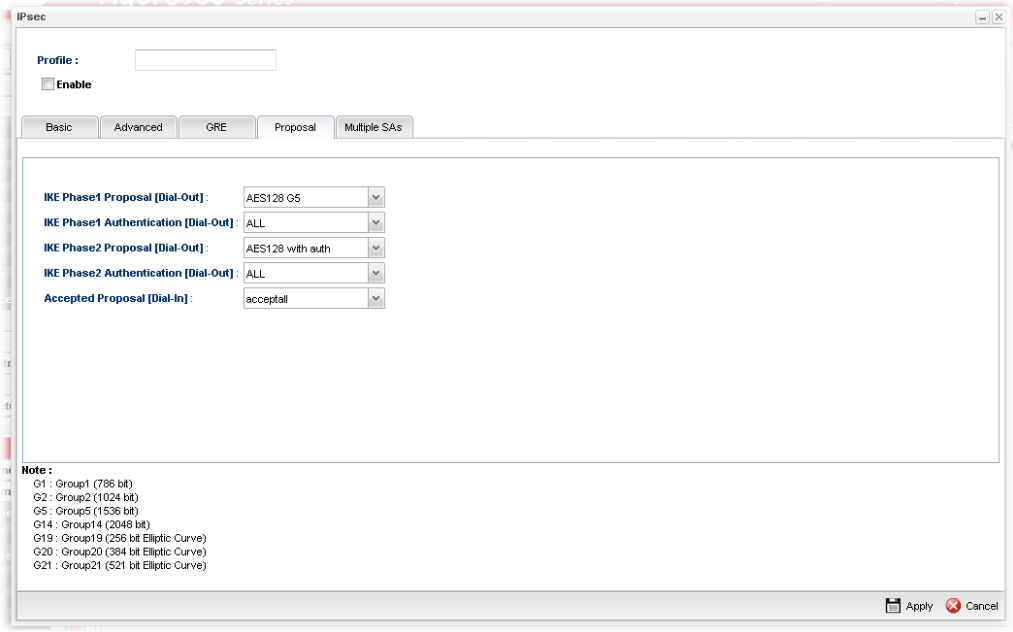
For GRE over IPsec Tunnel, please enable **GRE** function and enter your GRE IP for both sides.



Available parameters are listed as follows:

Item	Description
Enable GRE Function	Check the box to enable the function.
Local GRE IP	The virtual IP address of the router, specified for this tunnel.
Remote GRE IP	The virtual IP address of the remote client, specified for this tunnel.
Auto Generate GRE Key	Click **Enable** to generate the GRE key by the system automatically. If you click **Disable**, you need to type GRE key manually.
GRE In Key	Type the hexadecimal number as GRE In Key. This value is used for the router to authenticate the source of the packet. The length is 4 bytes.
GRE Out Key	Type the hexadecimal number as GRE Out Key. This value is used for the remote client to authenticate the source of the packet. The length is 4 bytes.

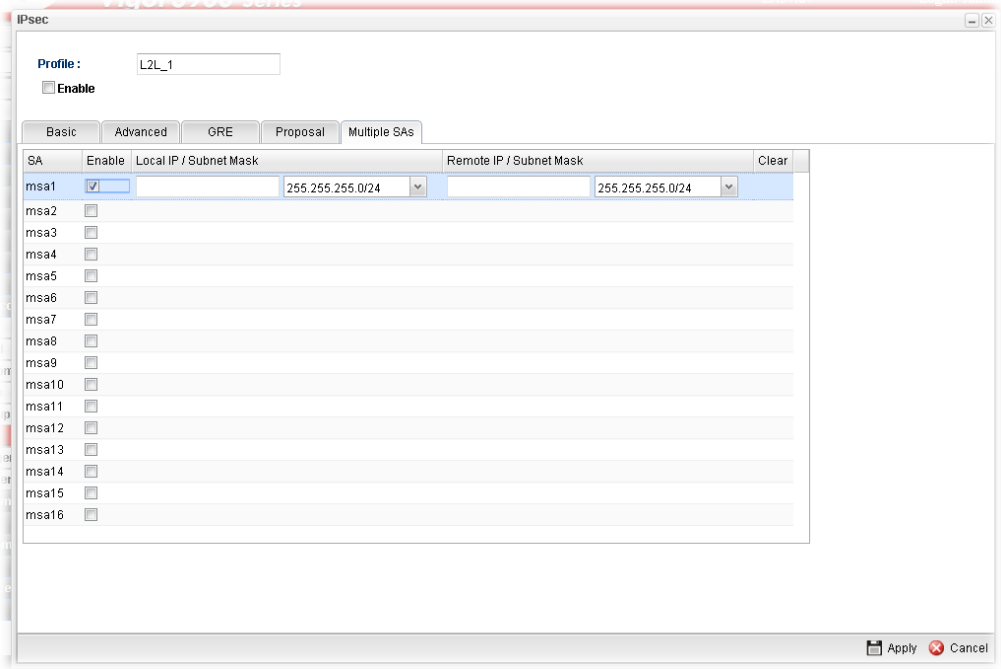
The **Proposal** tab lists encryption and authentication algorithms to be negotiated with the remote IPsec peer. Change settings to meet the security requirement.



Available parameters are listed as follows:

Item	Description
IKE Phase1 Proposal (Dial-Out)	Propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase1 Authentication (Dial-Out)	Propose the local available algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase2 Proposal (Dial-Out)	Propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase2 Authentication (Dial-Out)	Propose the local available algorithms to the VPN peers, and get its feedback to find a match.
Accepted Proposal (Dial-In)	For the dial-in VPN user, please specify the limitation of the proposal. **acceptall** - When the VPN tunnel is established, all the proposals supported by this device will be accepted and applied. **acceptabove** - When the VPN tunnel is established, only the selected proposal will be accepted and applied by this device.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving configuration.

Multiple SAs will negotiate IPSec SAs in IKE phase 2 to establish multiple IPSec tunnels for each subnet routing. Configure if required.



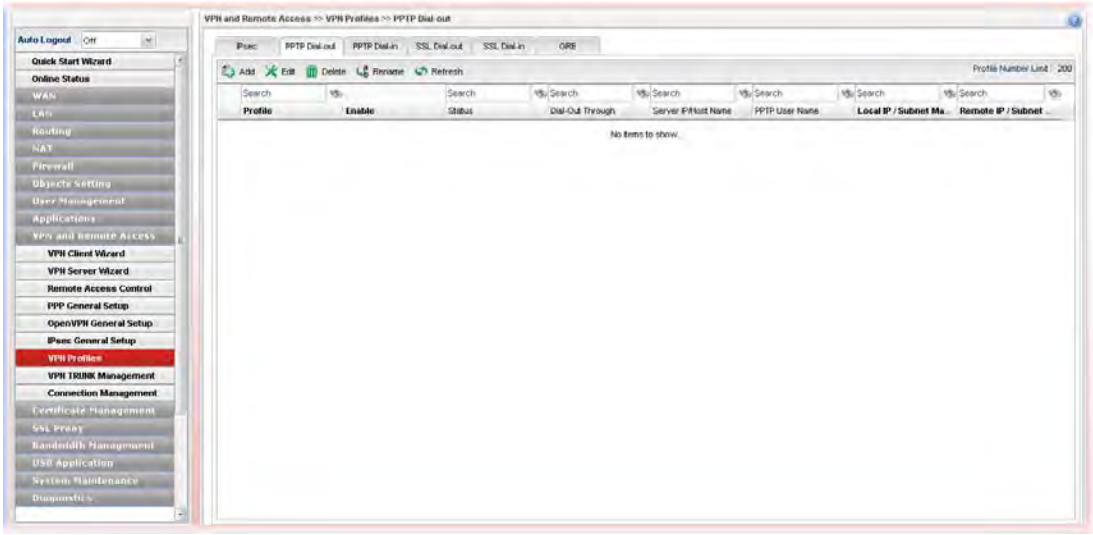
Available parameters are listed as follows:

Item	Description
Enable	An IPsec VPN profile can support 1 up to 16 multiple SAs (security association). Check the one you want to enable it.
Local IP /Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP /Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.

4. After filling the required information, click **Apply** and a new IPsec LAN-to-LAN profile will be created.

4.9.7.2 PPTP Dial-out/SSL Dial-out Tunnel

Display the name of LAN to LAN profile with PPTP dial-out/SSL dial-out tunnel.



Each item will be explained as follows:

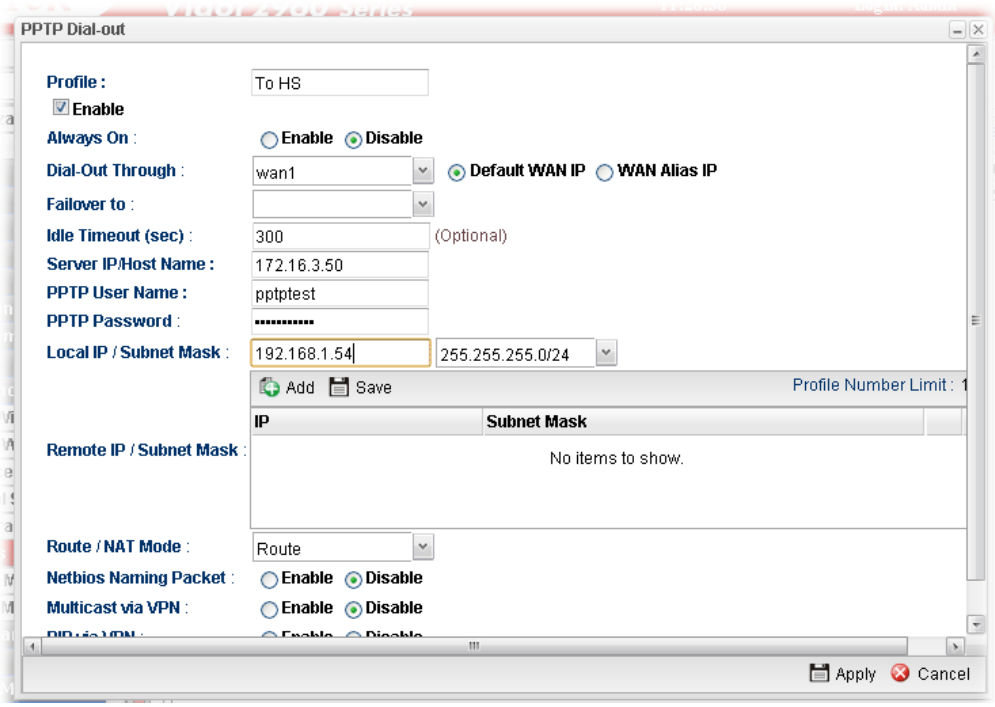
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (200) of the object profiles to be created.
Profile	Display the name of LAN to LAN profile with PPTP/SSL dial-out policy.
Enable	Display the status of the profile. False means disabled; True means enabled.
Dial-Out Through	Display the WAN interface selected for the profile.
Server IP/Host	Display the IP address or the host name of PPTP/SSL server.
PPTP User Name/ SSL User Name	Display the user name for authentication in PPTP/SSL connection.
Local IP / Subnet Mask	Display the LAN IP address with subnet mask of this profile.
Remote IP / Subnet Mask	Display the WAN IP address with subnet mask of this profile.

How to create a PPTP Dial-Out/SSL Dial-out LAN to LAN profile

Below will guide you to create a PPTP/SSL dial-out profile for VPN connection:

1. Open **VPN and Remote Access >> VPN Profiles** and click **PPTP Dial-out.**
2. Simply click the **Add** button.

3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Always On	Click **Enable** to make the profile being always on.
Dial-Out Through	Choose a wan interface to be used by such profile. Then, use the default WAN IP or specify a WAN Alias IP for VPN tunnel.
Failover to	Choose a wan profile which will lead the data passing through other WAN automatically when the selected WAN interface (in **Dial-Out Through**) is failover.
Idle Timeout (sec)	If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.
Server IP/Host Name	Type the IP address or the host name of PPTP/SSL server.
PPTP User Name/ SSL User Name	Type a user name for authentication in PPTP/SSL connection.
PPTP Password/ SSL Password	Type a password for authentication in PPTP/SSL connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.

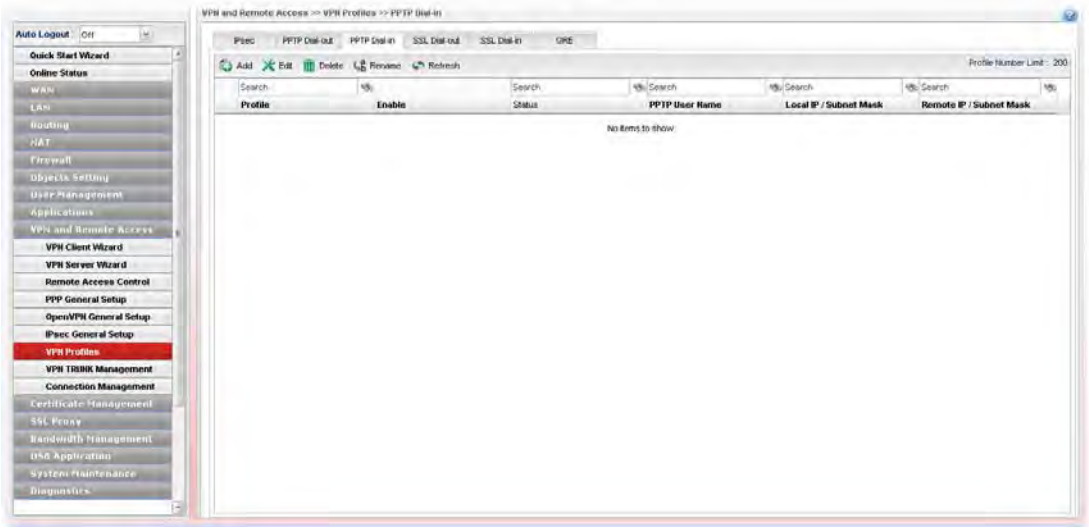
Route / NAT Mode	Specify the purpose for such profile.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information protocol packets via VPN connection. ● **Disable –** Disable such function. This is default setting.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.

5. A new PPTP/SSL Dial-Out profile has been created.

4.9.7.3 PPTP Dial-in/SSL Dial-in Tunnel

Display the name of LAN to LAN profile with PPTP dial-in/SSL dial-in tunnel.



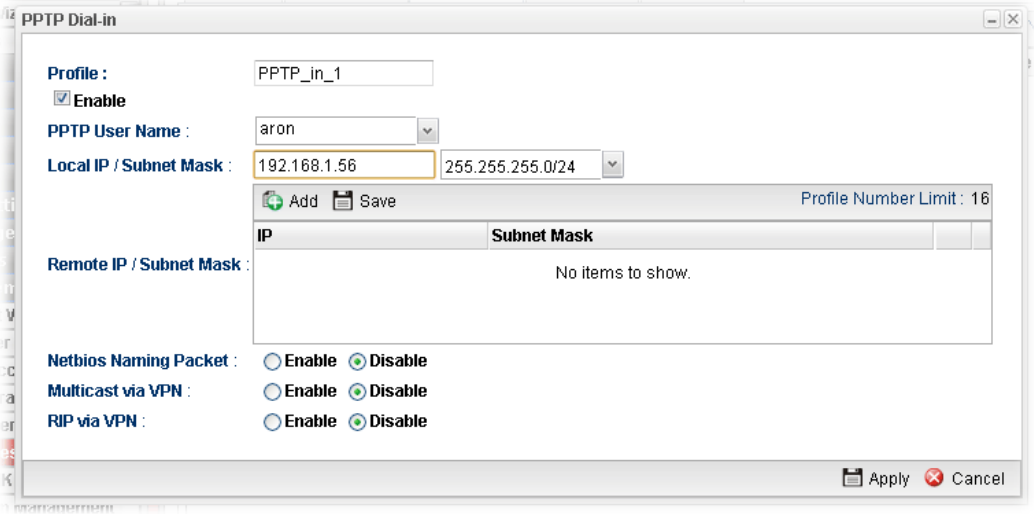
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (200 for PPTP, 50 for SSL) of the object profiles to be created.
Profile	Display the name of LAN to LAN profile with PPTP/SSL dial-in policy.
Enable	Display the status of the profile. False means disabled; True means enabled.
PPTP User Name / SSL User Name	Display the user name for authentication in PPTP/SSL connection.
Local IP / Subnet Mask	Display the LAN IP address with subnet mask of this profile.
Remote IP / Subnet Mask	Display the WAN IP address with subnet mask of this profile.

How to create a PPTP Dial-In/SSL Dial-In LAN to LAN profile

Below will guide you to create a PPTP dial-in profile for VPN connection:

1. Open **VPN and Remote Access >>VPN Profiles.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

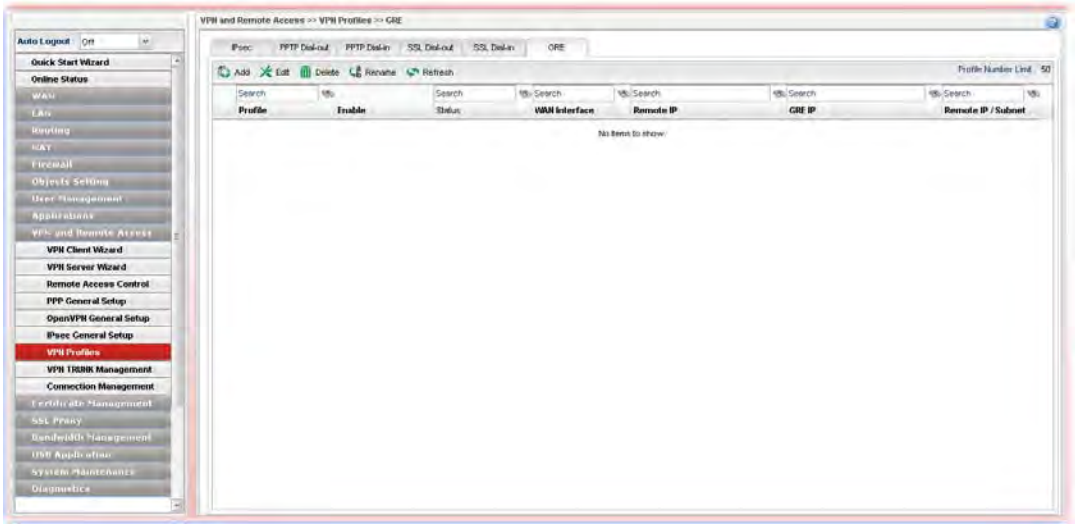
Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable this profile.
PPTP User Name / SSL User Name	Choose a PPTP/SSL user profile for authentication in PPTP/SSL connection. Such profile shall be created in **User Management>>User Profile** previously.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Netbios Naming Packet	**Enable** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Disable** –When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. ● **Enable** – Click this button to let multicast packets pass through the router. ● **Disable** – This is default setting. Click this button to let

	multicast packets be blocked by the router.
RIP via VPN	● **Enable** – Click it to exchange routing information protocol packets via VPN connection. ● **Disable –** Disable such function. This is default setting.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new PPTP/SSL Dial-In profile has been created.

4.9.7.4 GRE Tunnel

Display the name of LAN to LAN profile with GRE tunnel.



Each item will be explained as follows:

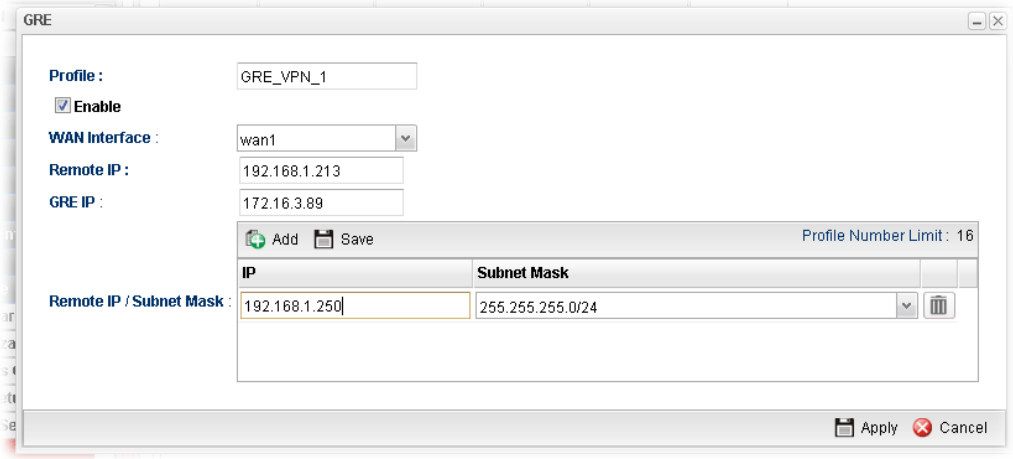
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the object profiles to be created.
Profile	Display the name of LAN to LAN profile with GRE policy.
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Interface	Display the WAN interface used for GRE tunnel.

Remote IP	Display the WAN IP address with subnet mask of this profile.
GRE IP	Display the GRE interface IP address for local host.
Remote IP / Subnet Mask	Display the IP address and subnet mask of remote client.

How to create a GRE VPN profile

Below will guide you to create a GRE profile for VPN connection:

1. Open **VPN and Remote Access >> VPN Profiles.**
2. Switch to the tab of GRE. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable this profile.
WAN Interface	Specify a WAN interface used for GRE tunnel.
Remote IP	Type the LAN IP address for the remote host.
GRE IP	Type the GRE interface IP address for local host.
Remote IP/Subnet Mask	Type the IP address and subnet mask of remote client.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

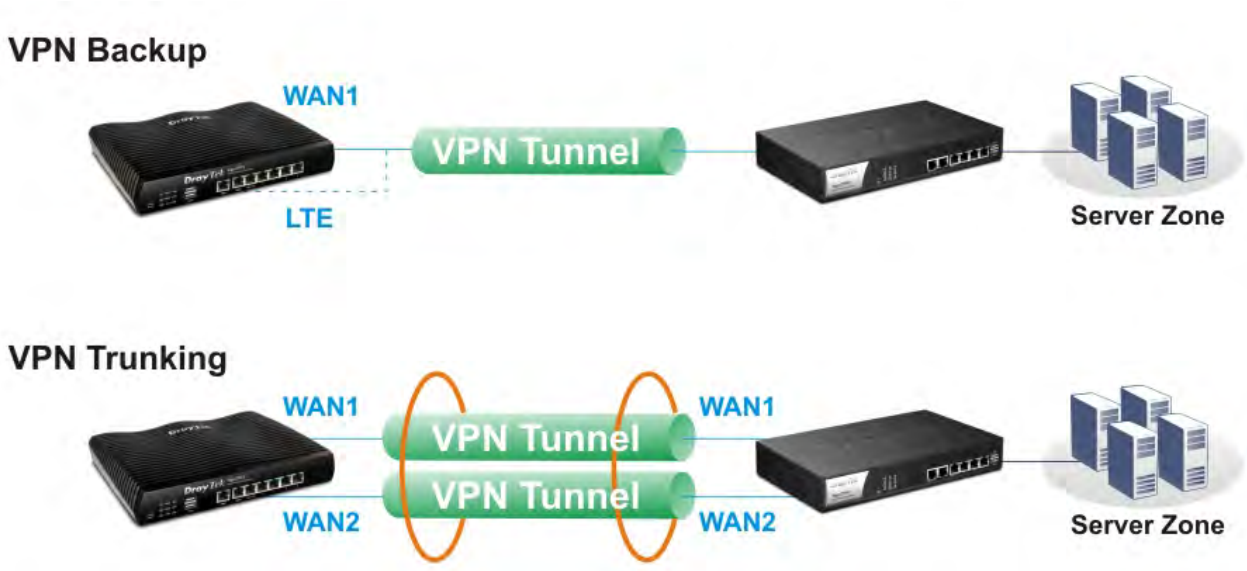
4. Enter all of the settings and click **Apply**.
5. A new GRE LAN-to-LAN profile has been created.

4.9.8 VPN Trunk Management

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism to let the administrator manage the network more flexibly.

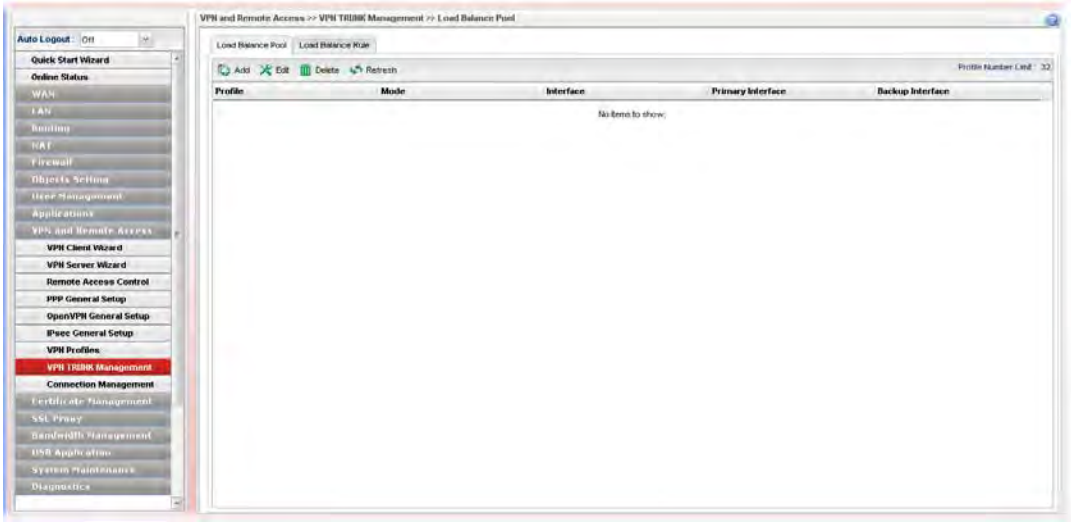
- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management
- Dial-out connection types contain IPsec, PPTP, L2TP, L2TP over IPsec and GRE over IPsec
- The web page is simple to understand and easy to configure

The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably.



4.9.8.1 Load Balance Pool

This page allows the user to integrate **several** WAN profiles as a pool profile specified with the function of load balance or failover.

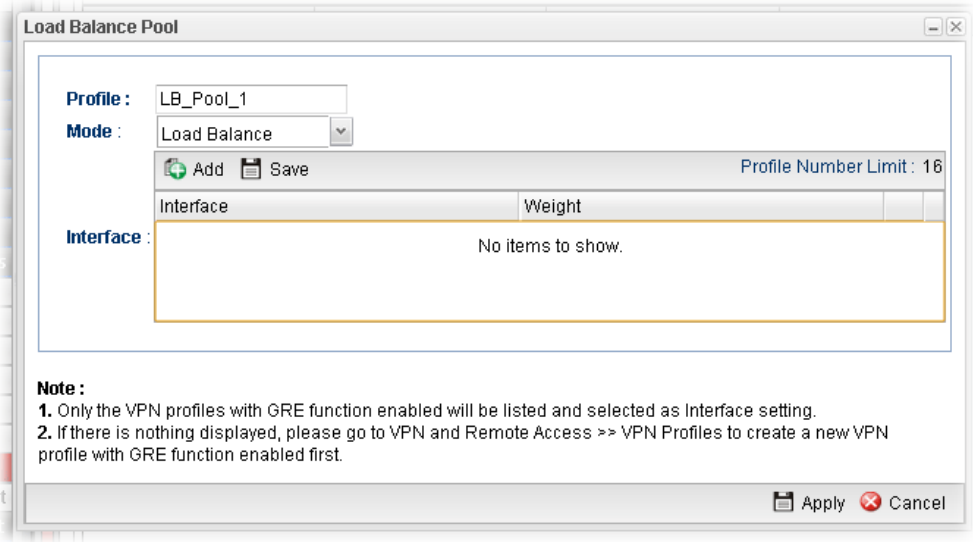


Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile.
Mode	Display which mode (load balance or failover) is selected.
Interface	Display the name of the Load Balance profile grouped under such pool profile.
Primary Interface	Display the primary interface for failover.
Backup Interface	Display the backup interface for failover.

How to add a Load Balance Pool Profile

1. Open **VPN and Remote Access >>VPN TRUNK Management** and click the **Load Balance Pool** tab.
2. Simply click the **Add** button.
3. The following dialog will appear. Type the name of the profile (e.g., LB_Pool_1, within 10 characters including digit, letter, and underline) under the **Mode** tab.



Available settings are listed below:

Item	Description
Profile	Type the name of the profile (e.g., LB_Pool_1, within 10 characters including digit, letter, and underline).
Mode	Choose Load Balance or Failover. **Load Balance** ● **Interface** – Choose VPN profile(s) as the interface. **Note:** Only the VPN profiles with GRE function enabled will be listed and selected as Interface setting. If there is nothing displayed, please go to VPN and Remote Access>>VPN Profiles to create a new VPN profile with GRE function enabled first. ● **Weight** – Type a value in such field. **Failover** ● **Primary Interface / Backup Interface** - Use the drop down list to specify the VPN profiles for Primary Interface and Backup Interface respectively.

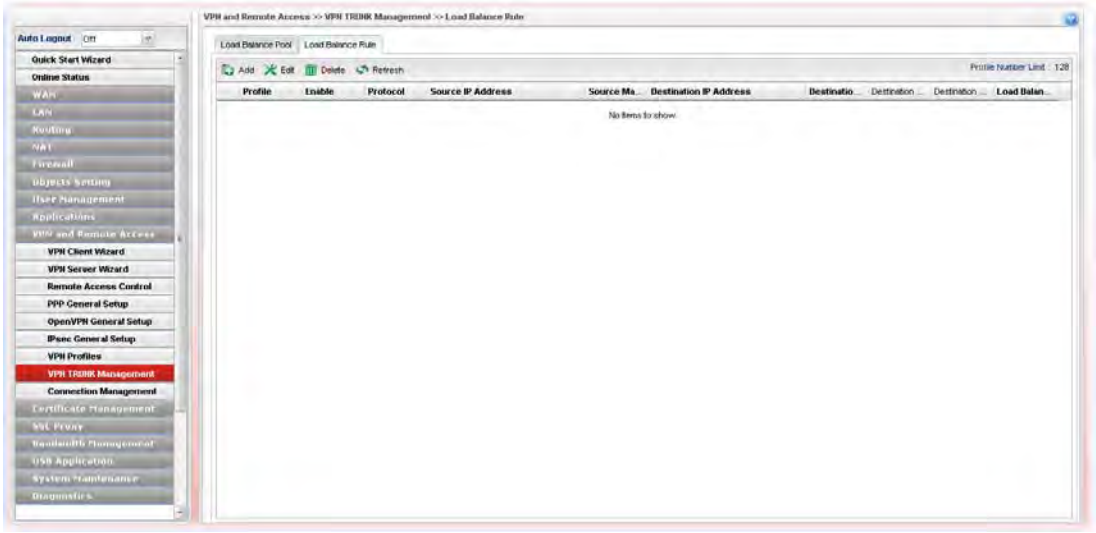
Important!!! If there is no selection for Interface option, please go to **VPN and Remote Access>>VPN Profiles** to create a new IPSec LAN to LAN profile with **enabled GRE** setting. Then, return to this page to specify the Interface option.

4. Enter all the settings and click **Apply**.
5. A new profile has been created.

Refer to Chapter 3, *How to Configure VPN Load Balance between Vigor3900 and Other Router* for getting more detailed information about Load Balance application.

4.9.8.2 Load Balance Rule

To build VPN load balance connection with other router, you can define the load balance rule in this page.



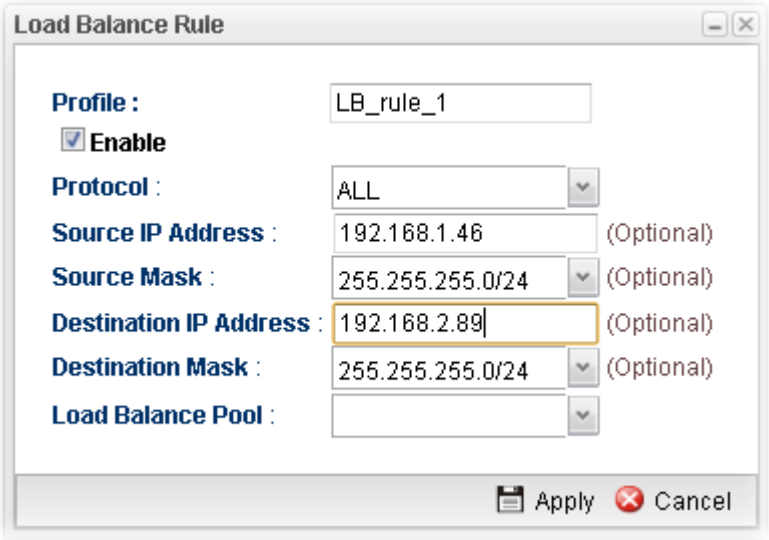
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (128) of the profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Protocol	Display the protocol configured by such profile.
Source IP Address	Display the source IP address specified for this profile.
Source Mask	Display the subnet mask address specified for the source IP of this entry.
Destination IP Address	Display the destination IP address specified for this entry.
Destination Mask	Display the subnet mask address specified for the destination IP of this entry.
Destination Port Start	Display the start point specified in the **Dest Port Range** for this entry.

Destination Port End	Display the end point specified in the **Dest Port Range** for this entry.
Load Balance Pool	Display the selection of load balance pool.

How to add a Load Balance Rule profile

1. Open **VPN and Remote Access >>VPN TRUNK Management** and click the **Load Balance Rule** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
Protocol	Choose the protocol for such profile.
Source IP Address	Type the source IP address specified for this profile.
Source Mask	Type the subnet mask address specified for the source IP.
Destination IP Address	Type the destination IP address specified for this entry.
Destination Mask	Type the subnet mask address specified for the destination IP.
Destination Port Start	Type the start point.
Destination Port End	Type the end point.
Load Balance Pool	Use the drop down list to choose one profile configured in load balance pool. Then, such rule will be applied by the pool.

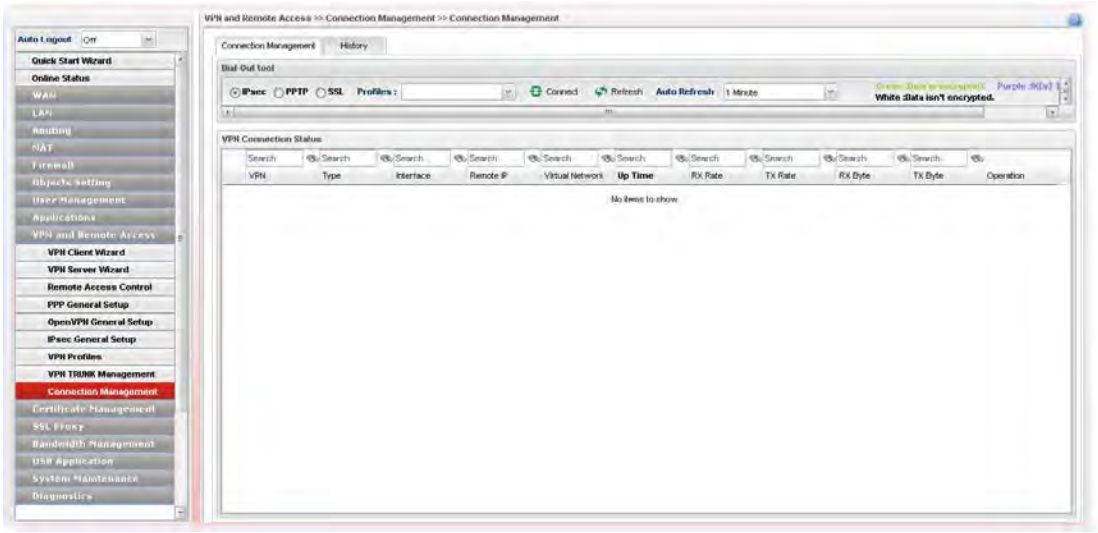
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new profile has been created.

4.9.9 Connection Management

4.9.9.1 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Disconnect** button.



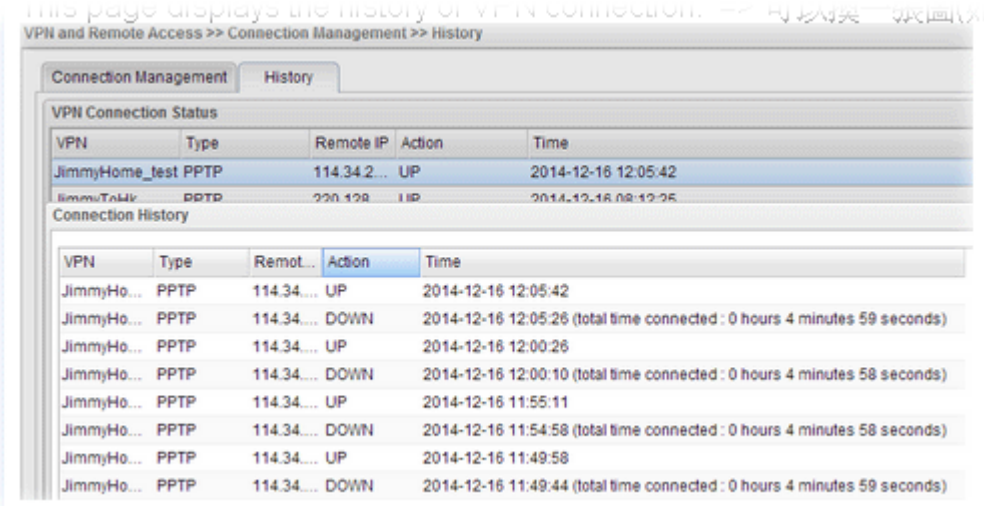
Each item will be explained as follows:

Item	Description
IPsec/PPTP/SSL	Click it to perform IPsec VPN/PPTP/SSL connection.
PPTP	Click it to perform PPTP VPN connection.
Profiles	This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.
Connect	Click this button to execute dial out function.
Refresh	Renew current web page.
VPN	Display the name of VPN profile.
Type	Display the connection type (PPTP or IPSec) for such VPN profile.
Interface	Display the WAN interface for such VPN profile.
Remote IP	Display the remote IP configure by VPN profile.
Virtual Network	Display the virtual network established by such VPN profile.

Up Time	Display the connection time of this VPN tunnel.
RX (Packets)	Display the total received packets through this VPN.
TX (Packets)	Display the total transmitted packets through this VPN.
Disconnect	Terminate the VPN connection.
Operation	Display the icons to terminate / view the VPN profile.

4.9.9.2 History

This page displays the history of VPN connection.



Each item will be explained as follows:

Item	Description
VPN	Display the name of VPN profile.
Type	Display the connection type used of such VPN.
Remote IP	Display the IP address of the remote end.
Action	Display the connection status (UP or DOWN) of VPN profile.
Time	Display the time the VPN profile connects/disconnects.

4.10 Certificate Management

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

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

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

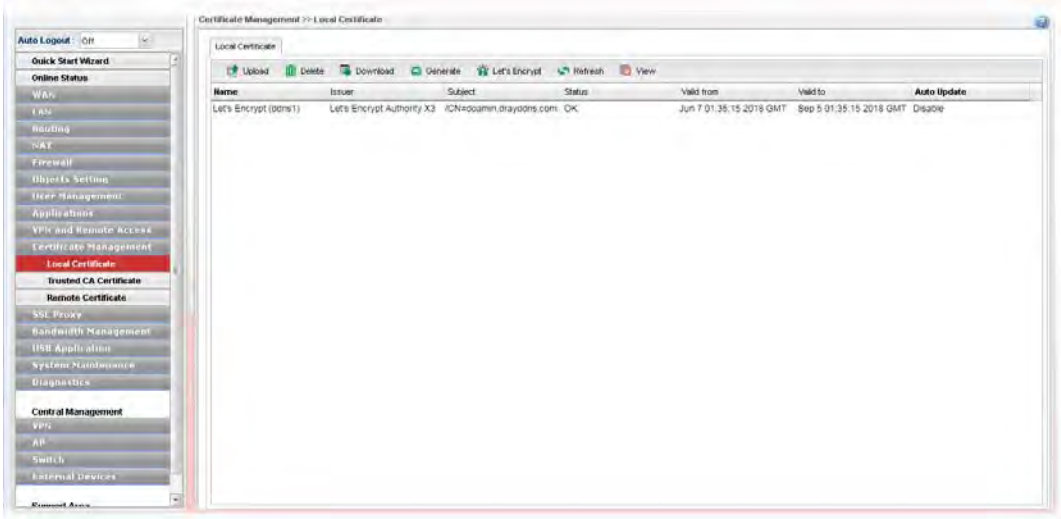
Below shows the menu items for Certificate Management.

Local certificate is created by the end user and must be signed by a trusted CA center. Vigor3900 can serve as a trusted CA and is called with “Root CA”. Therefore, any user can ask for certificate signed by Vigor3900.

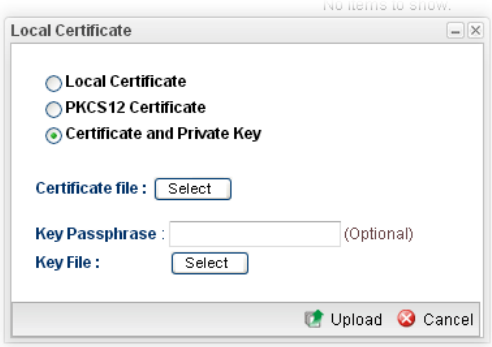
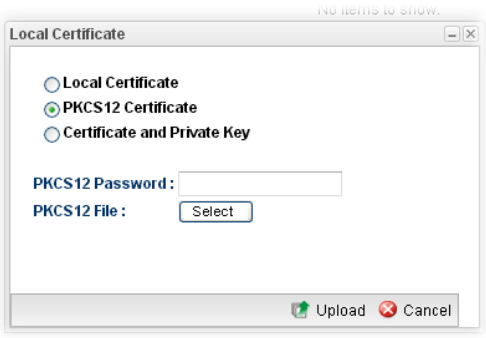
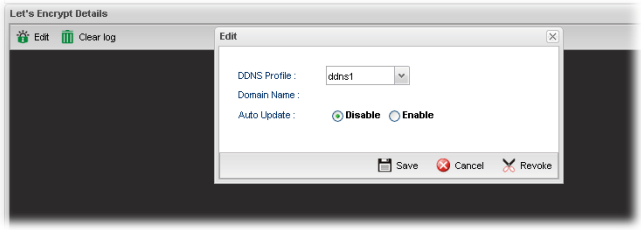
When Vigor3900 serves as a Root CA, it can sign the certificates coming from the users. First, building a Root CA for Vigor3900 by clicking **Trusted CA Certificate**. Later, certificate coming from other users can be uploaded to Root CA (Vigor3900) and be signed by Vigor3900.

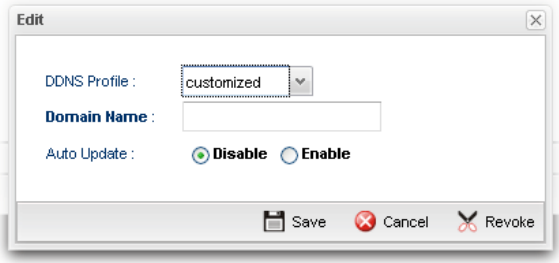
4.10.1 Local Certificate

This page allows users to generate certificate based on different work requests. Local certificate can be signed by itself or signed by a root CA (e.g., root CA on Vigor3900).



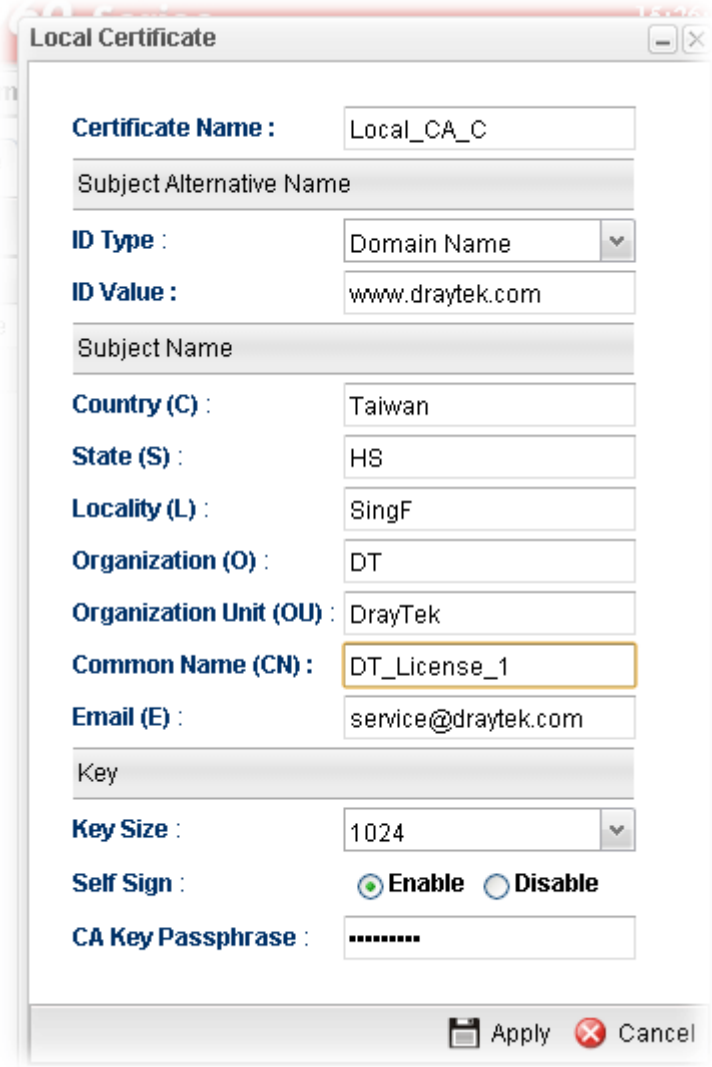
Each item will be explained as follows:

Item	Description
Upload	Click this button to open the following dialog to upload selected certificate onto the router.   After choosing the certificate file type, type the required information and choose the required file (e.g., Key Passphrase, Key File, PKCS12 Password and PKCS12 File). Later, click **Upload** on the dialog to upload the file onto Vigor router.
Delete	Remove the selected item of Trusted CA listed below.
Download	Allow you to download an existing CA certificate to the router.
Generate	Open another web page for generating the local certificate.
Let's Encrypt	You can apply for a certificate from "Let's Encrypt" Certificate Authority, based on the built-in DDNS profile or customized DDNS profile. Click it to open the **Let's Encrypt Details** window. Next, click **Edit.** A dialog will be shown as below:  **DDNS Profile** – Select one of the DDNS profiles. **Domain Name** – Display the domain name specified for the selected DDNS profile. **Auto Update** – The valid time for a certificate is three

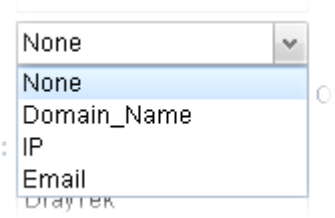
	months. If selecting **Enable**, Vigor router will automatically apply a new certificate one month before the expiration date. **Save –** Click it to open the confirmation dialog of creating a certificate. ● **Yes –** Save the configuration and start the application process for the certificate. ● **No –** Simply save the configuration. **Revoke –** Click it to revoke the selected DDNS profile with the certificate been applied before. Sometimes, the user might not use the built-in DDNS service by Vigor router but want to apply a certificate issued by Let's Encrypt with a user-defined domain name. For such case, select "**customized**" as DDNS profile and enter the desired domain name. Next, click **Save** to perform the process. 
Name	Display the name of trusted CA built.
Subject	Display the subject of the trusted CA built.
Issuer	Display the issuer of the trusted CA built.
Status	Display the status of the trusted CA built.
Valid From	Display the starting point of the valid time of trusted CA.
Valid To	Display the end point of the valid time of trusted CA.
Auto Update	Display the status (enabled/disabled) of the function. This field will be blank if the certificate is not issued by Let's Encrypt.

How to build a local certificate

1. Open **Certificate Management>> Local Certificate.**
2. Simply click the **Generate** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Certificate Name	Type the name of the local certificate.
ID Type	The ID type for such certificate. There are four types: **Domain Name**: Certificated by domain name. **IP**: Certificated by IP address. **Email**: Certificated by email address. **None**: Do not enter an ID value. 
ID Value	The ID value is determined by the **ID Type** selected for such certificate. For example, if you choose **Domain Name** as the ID Type,

	please type the domain name in this field.
Organization Unit	Type a description for the organization unit.
Organization	Type the name of the organization.
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state /province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
Country	Type the name of the country that such certificate located.
Key Size	Choose one of the key sizes for such certificate.
Self Sign	Click **Enable** to enable the self sign function. If the certificated has been signed by it self, it can not be approved or signed by other Root CA server any more. Click **Disable** to disable the self sign function. A certificate without self sign can be approved or signed by a Root CA server, e.g., Vigor3900.
CA Key Passphrase	Such string will be used for confirmation while signing remote CA. It is similar to a password but generally it is longer for security.
Apply	Click it to create a new local certificate based on the configuration here.
Cancel	Click it to exit the web page without saving the configuration.

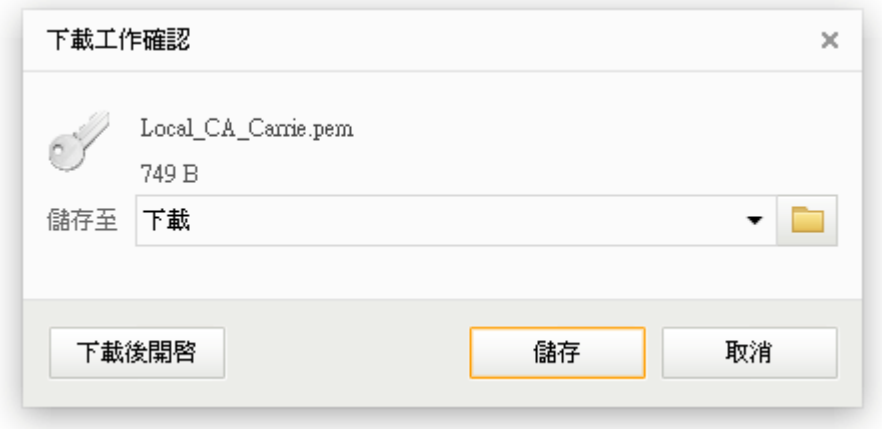
4. Enter all the settings and click **Apply**.
5. A new generated Local Certificate has been created.

How to download a local certificate into specified location

Vigor router allows you to generate a certificate request and submit it the CA server. After generating a local certificate, you can download it as a file into any place you want.

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.

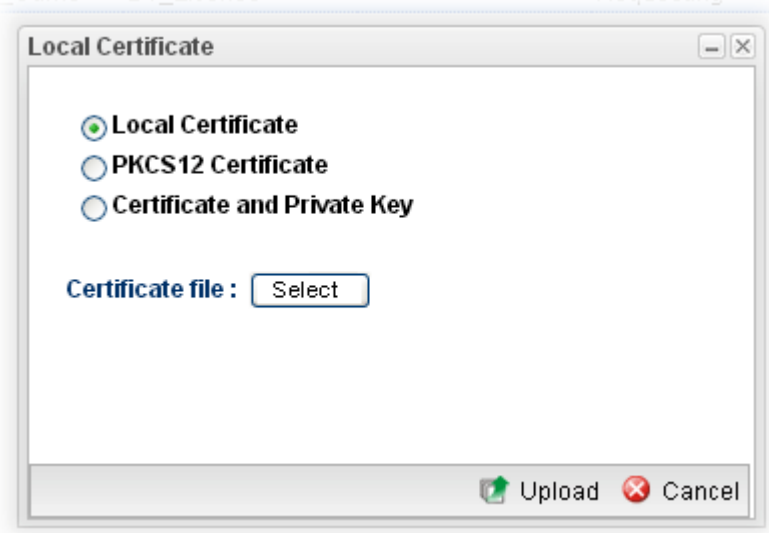
1. Open **Certificate Management>> Local Certificate.**
2. Specify a certificate and click the **Download** button.



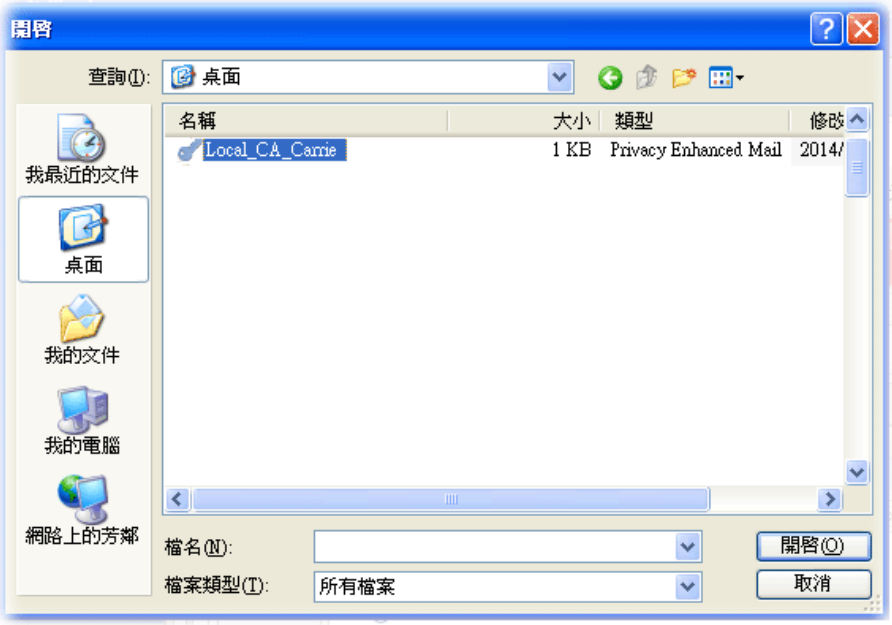
3. Click **Save**. The file will be stored under the folder you specified above.

How to upload a local certificate

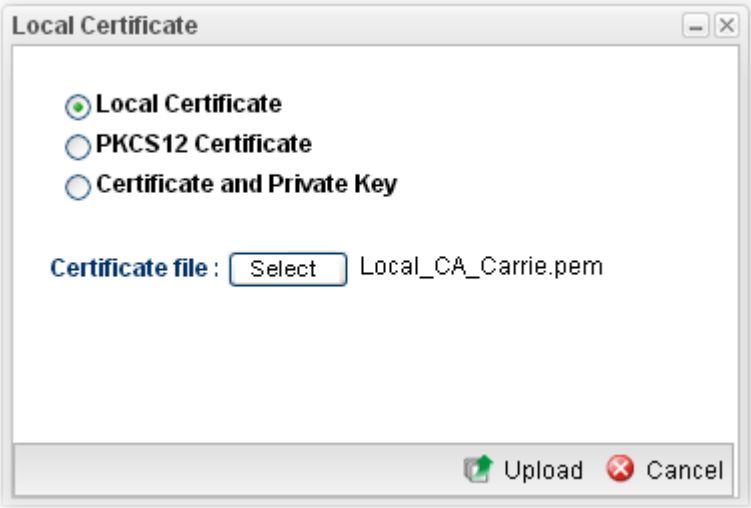
1. Open **Certificate Management>> Local Certificate.**
2. Click **Upload** to open the following dialog.



3. Choose **Local Certificate** and click the **Select** button to open the follwoing dialog.



4. From the above dialog, choose the certificate you want and click **Open**. The dialog box with the selected certificate file name will be shown as follows.

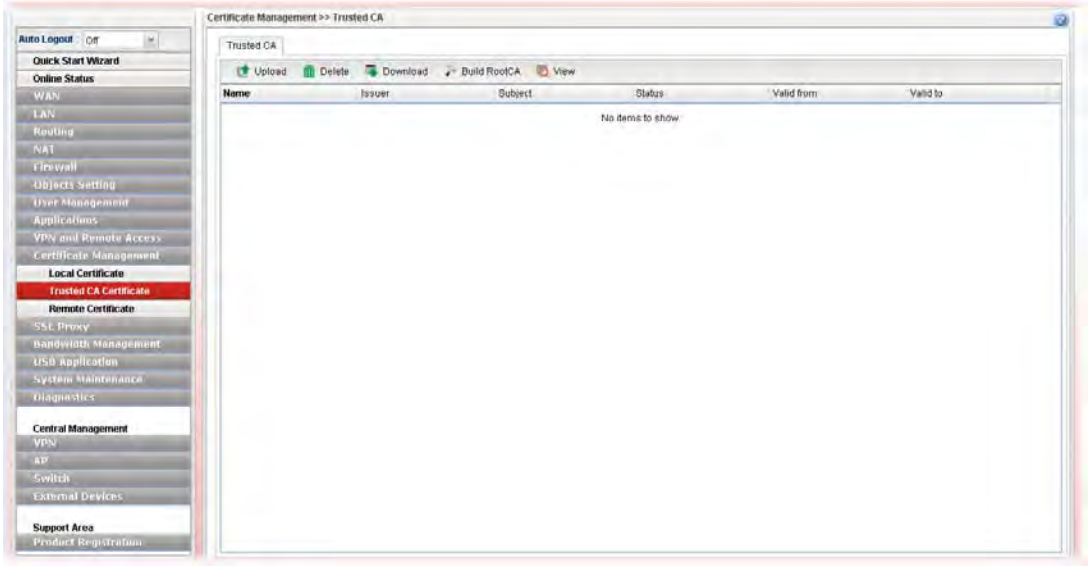


5. Click **Upload**. The system will start to upload the selected file.

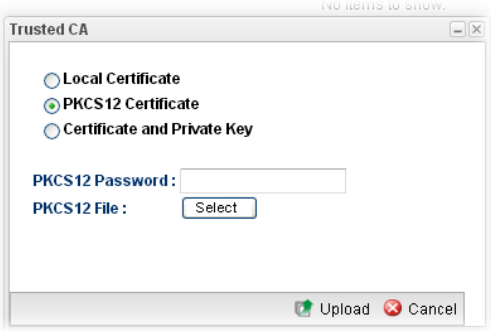
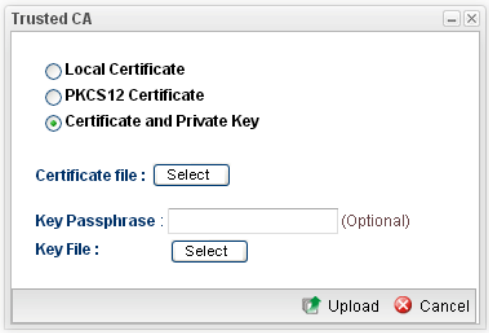
4.10.2 Trusted CA Certificate

This page allows you to build a RootCA certificate for Vigor3900.

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



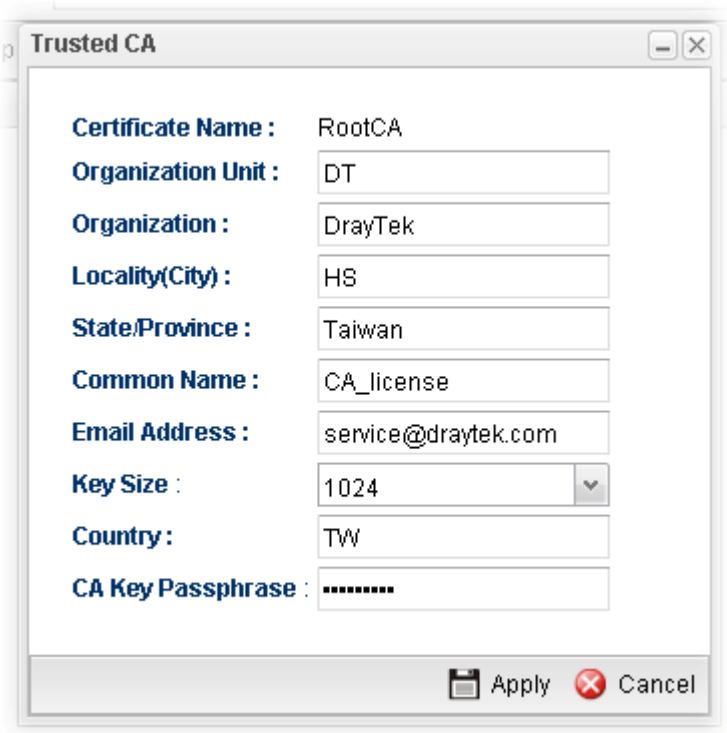
Each item will be explained as follows:

Item	Description
Upload	Click this button to open the following dialog to upload selected certificate onto the router.   After choosing the trusted CA mode, type the required information and choose the required file (e.g., Key Passphrase, Key File, PKCS12 Password and PKCS12 File). Later, click **Upload** on the dialog to upload the file onto

	Vigor router.
Delete	Remove the selected item of trusted CA listed below.
Download	Allow you to download an existing trusted CA certificate to the router.
Build RootCA	Allow to create a new CA certificate as Root CA.
Name	Display the name of trusted certificate built.
Subject	Display the subject of trusted certificate built.
Issuer	Display the issuer of trusted certificate built.
Status	Display the status of trusted certificate built.
Valid From	Display the starting point of the valid time of trusted certificate.
Valid To	Display the end point of the valid time of trusted certificate.

How to build a trusted CA certificate

1. Open **Certificate Management>>Trusted CA Certificate.**
2. Simply click the **Build RootCA** button.
3. The following dialog will appear.

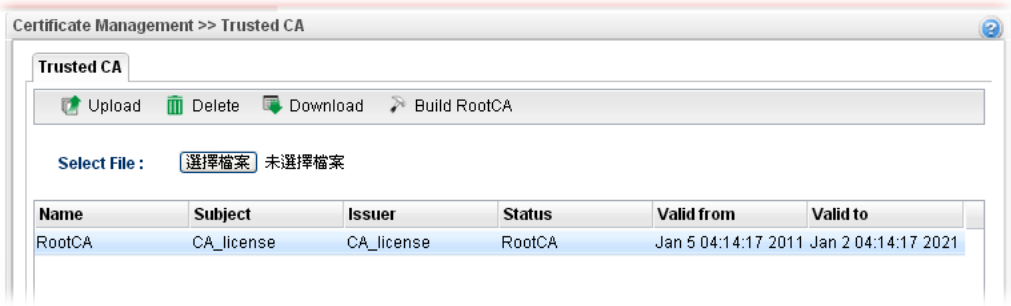


Available parameters are listed as follows:

Item	Description
Certificate Name	Display the name of the trusted CA certificate.
Organization Unit	Type a description for the organization unit.

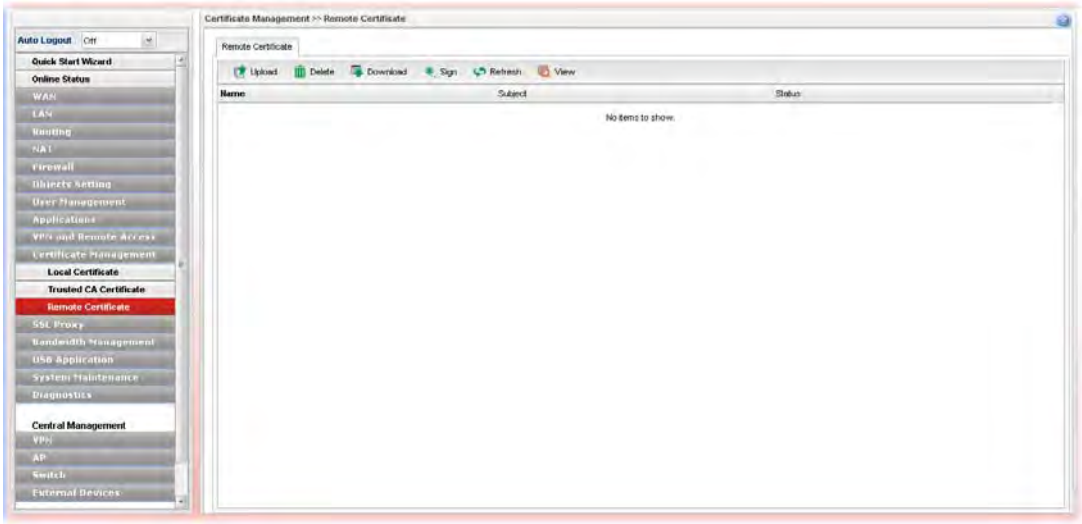
Organization	Type the name of the organization.
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state / province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
Key Size	Choose one of the key sizes for such certificate.
Country	Type the name of the country that such certificate located.
CA Key Passphrase	Type the string for the new certificate.
Apply	Click it to create a new local certificate based on the configuration here.
Cancel	Click it to exit the web page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new RootCA Certificate has been created.



4.10.3 Remote Certificate

Vigor3900, as a Root CA, can sign any certificate coming from end users locally or remotely. The selected user-defined certificate must be uploaded to Root CA. Also, the processing result will be displayed on this page.



Each item will be explained as follows:

Item	Description
Upload	Allow you to upload current configuration to the host as a remote certificate.
Delete	Remove the selected item of remote certificate listed below.
Download	Allow you to download an existing certificate to the router.
Sign	Allow you to sign a requested certificate.
Refresh	Renew current web page.
Name	Display the name of remote certificate built.
Subject	Display the subject of remote certificate built.
Status	Display the status of remote certificate built.

4.11 SSL Proxy

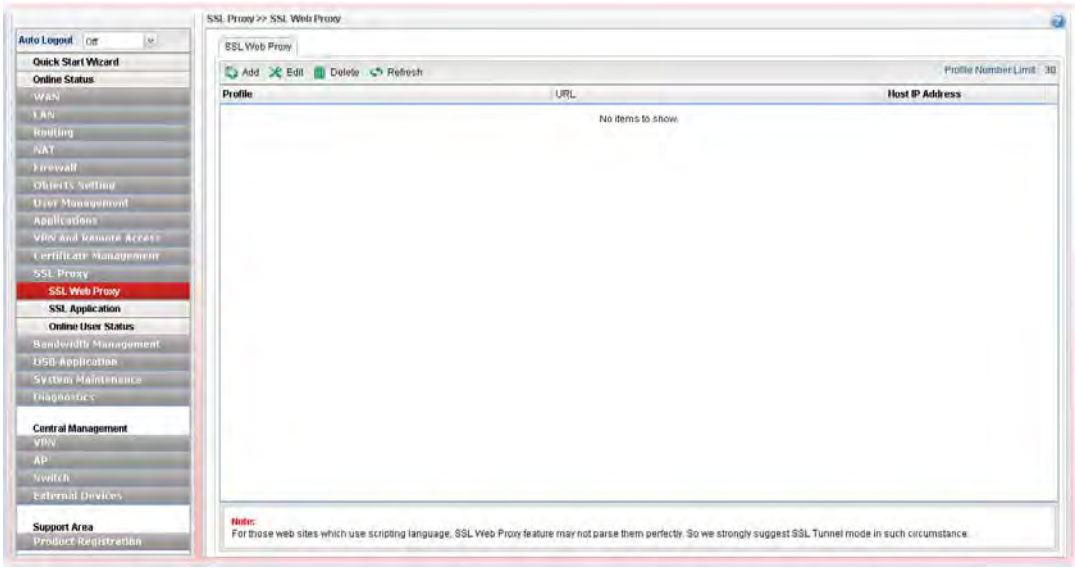
The profiles configured under such menu will be applied by **User Management>>User Profiles** for performing SSL VPN.

There are two benefits that SSL VPN provides:

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

4.11.1 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.



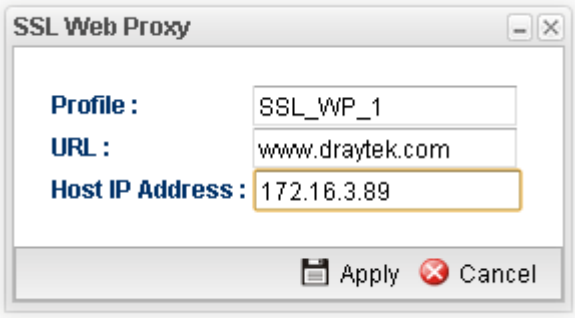
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.

Refresh	Renew current web page.
Profile Number Limit	Display the total number (30) of the profiles to be created.
Profile	Display the name of the profile that you create.
URL	Display the URL.
Host IP Address	Display the IP address for the Host.

How to create a new SSL Web Proxy

1. Open **SSL Proxy >> SSL Web Proxy.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type name of the profile.
URL	Type the address (function variation or IP address) or path of the proxy server.
Host IP Address	If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

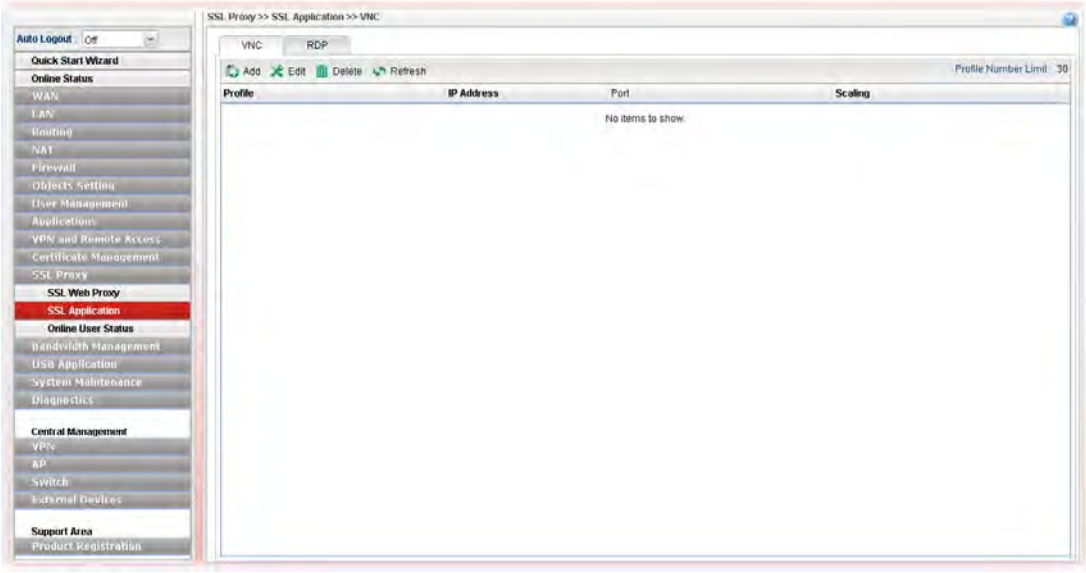
4. Enter all the settings and click **Apply**.
5. A new SSL Web Proxy profile has been created.

4.11.2 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol), to any remote user with access to Internet and a web browser.

4.11.2.1 VNC

VNC stands for **Virtual Network Computing.** It allows you to access and control a remote PC through VNC protocol.



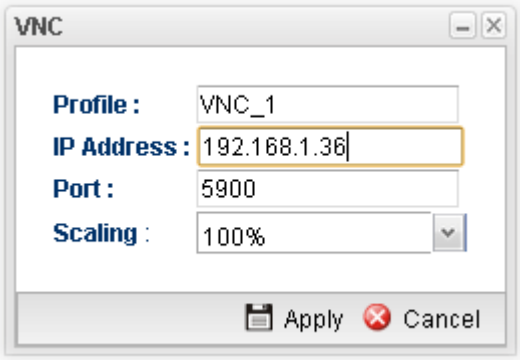
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (30) of the profiles to be created.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.
Port	Display the port used for this protocol.
Scaling	Display the percentage for such application.

How to create a new SSL Application with VNC protocol

1. Open **SSL Proxy >> SSL Application** and click the **VNC** tab.

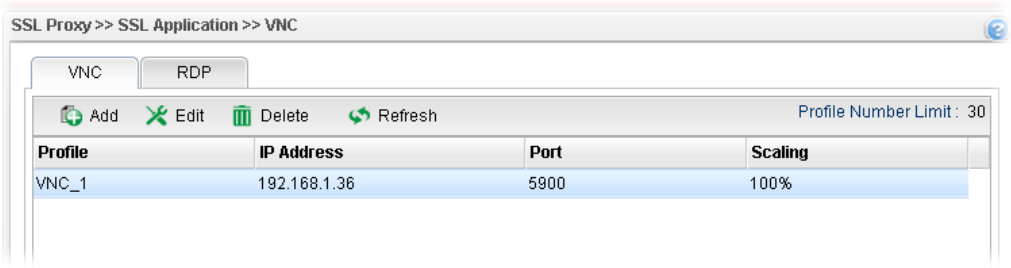
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

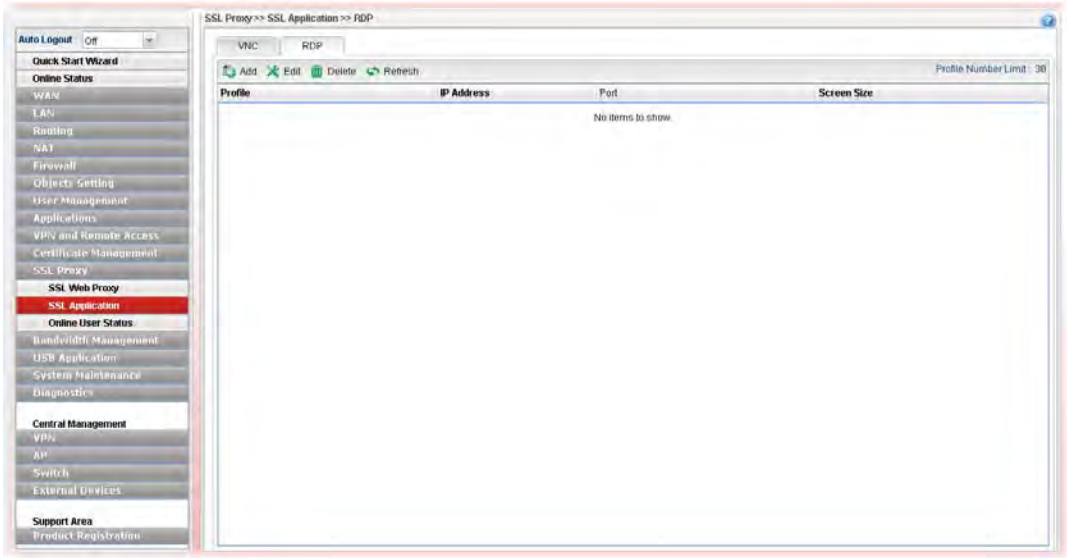
Item	Description
Profile	Type the name of the profile that you create.
IP Address	Type the IP address for this protocol.
Port	Specify the port used for this protocol. The default setting is 5900.
Scaling	Chose the percentage (100%, 80%, 60) for such application.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new SSL Application profile has been created.



4.11.2.2 RDP

RDP stands for **Remote Desktop Protocol.** It allows you to access and control a remote PC through RDP protocol.

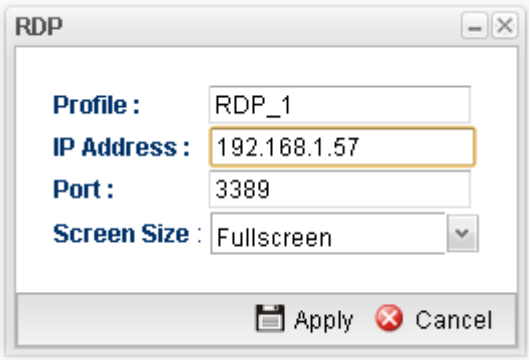


Each item will be explained as follows:

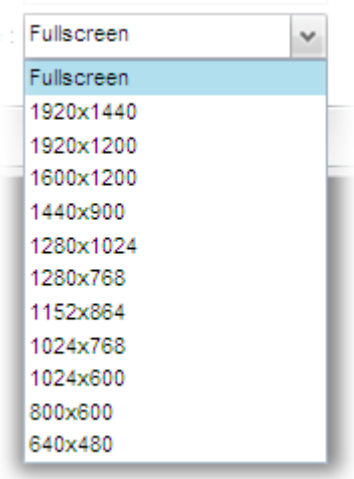
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (30) of the profiles to be created.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.
Port	Display the port used for this protocol.
Screen Size	Display the screen size for such application.

How to create a new SSL Application with RDP protocol

1. Open **SSL Proxy>> SSL Application** and click the **RDP** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.



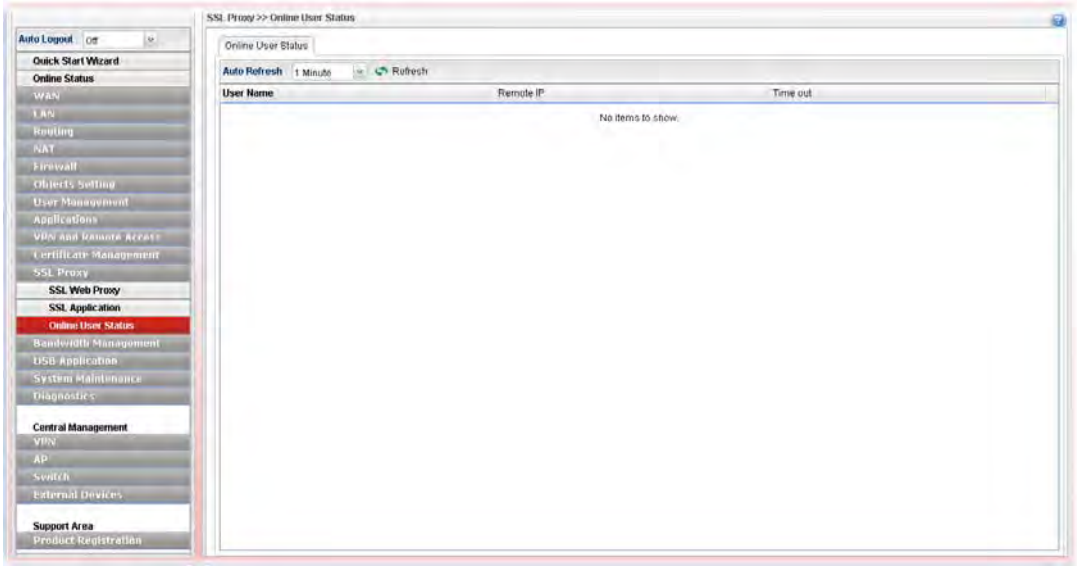
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile that you create.
IP Address	Type the IP address for this protocol.
Port	Specify the port used for this protocol.
Screen Size	Chose the screen size for such application. 
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A new SSL Application profile has been created.

4.11.3 Online User Status

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



Each item will be explained as follows:

Item	Description
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Refresh	Renew current web page.
User Name	Display current user who visit SSL VPN server.
Remote IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.

4.12 Bandwidth Management

Below shows the menu items for Bandwidth Management.

The QoS (Quality of Service) guaranteed technology in the Vigor router allows the network administrator to monitor, analyze, and allocate bandwidth for various types of network traffic in real-time and/or for business-critical traffic. Thus, timing-sensitive applications will not be impacted by web surfing traffic or other non-critical applications, such as file transfer. Without QoS-guaranteed control, there would be virtually no way to prioritize users/services or guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications.

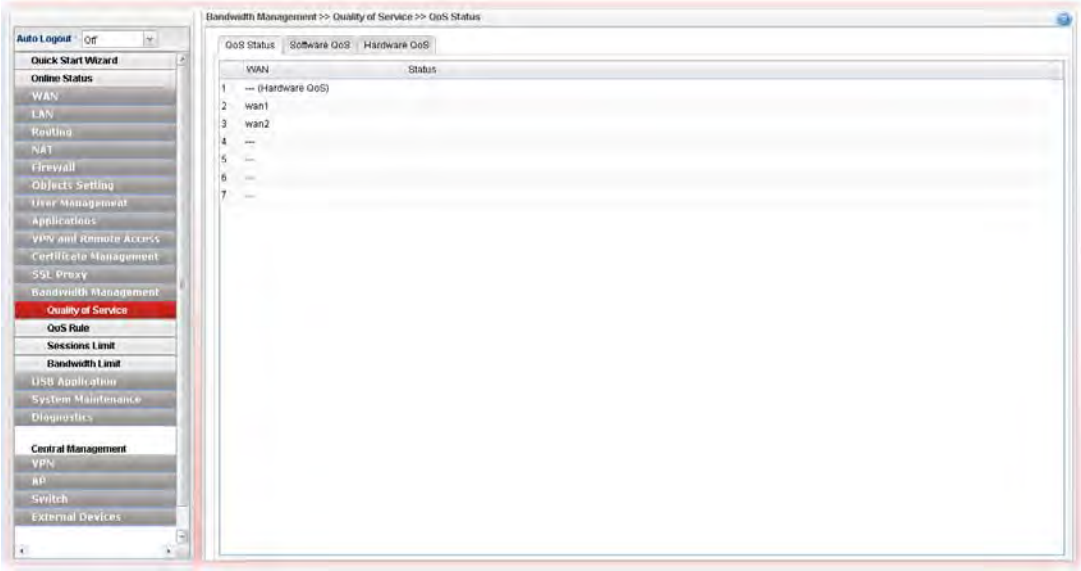
Differentiated quality of service is therefore one of the most important issues over the Internet infrastructure. In Vigor router, DSCP (Differentiated Service Code Point) support is also taken into consideration in the design of the QoS-guaranteed control module.

4.12.1 Quality of Service

The QoS function handles incoming and outgoing classes independently. Users can configure incoming or outgoing separately without any impact on the other.

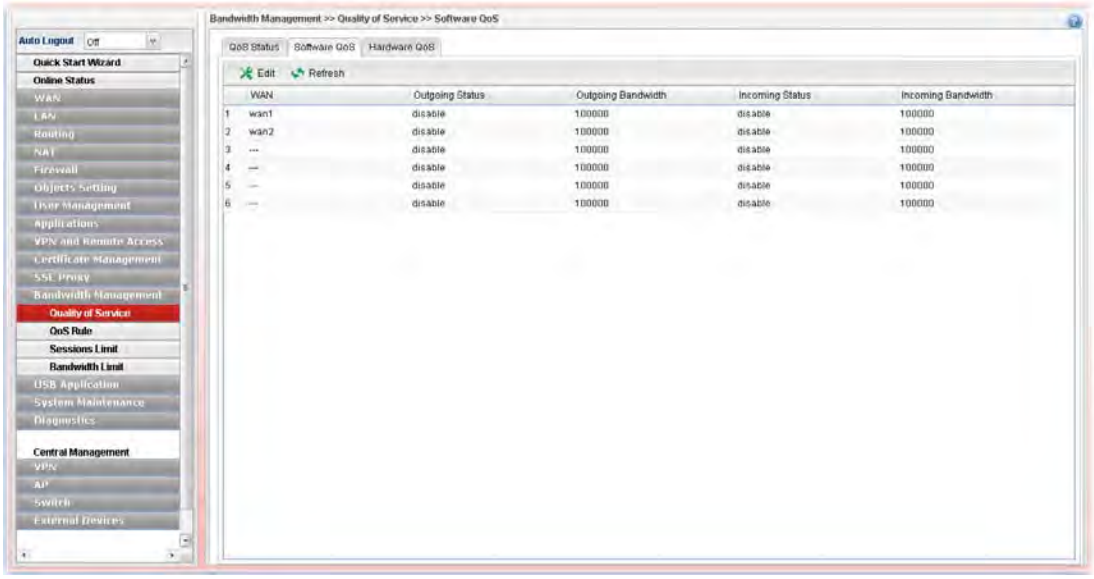
4.12.1.1 QoS Status

This page displays current QoS Status.



4.12.1.2 Software QoS

This page displays current software QoS status and allows you to edit related settings, including bandwidth, queue (high, medium, normal and low) for each QoS WAN.



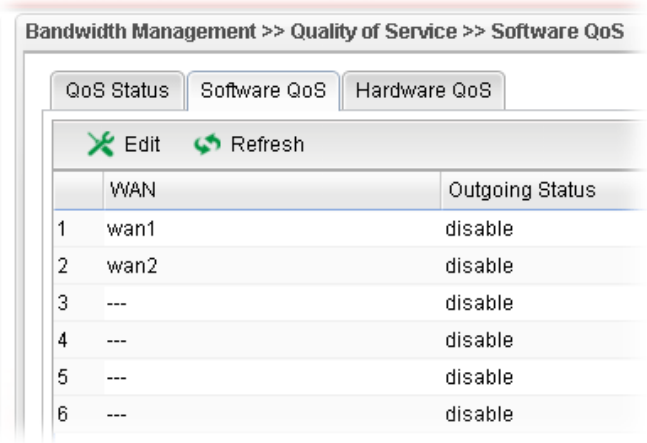
Available parameters are listed as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
WAN	Display the WAN interface used for QoS.
Outgoing Status	Display bandwidth for the outgoing data is enabled or disabled.
Outgoing Bandwidth	Display the total number of transmission rate for the outgoing data.
Incoming Status	Display the total number of transmission rate for the incoming data.
Incoming Bandwidth	Display bandwidth for the incoming data is enabled or disabled.

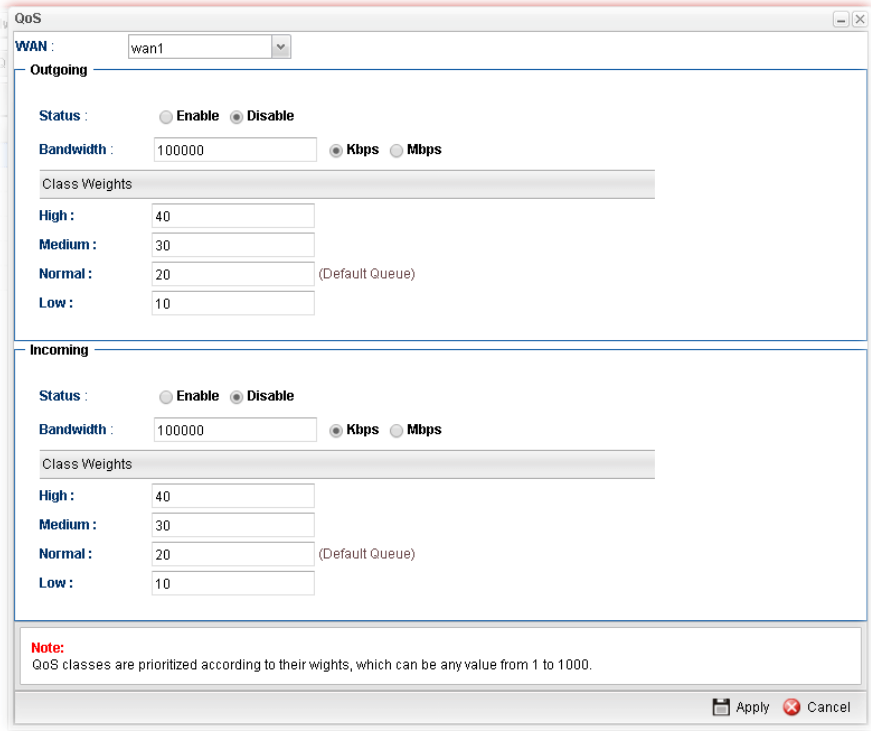
How to edit a QoS Profile

Follow the steps below to create a new maintenance profile.

1. Click one of the QoS WAN profiles to select the one you want to edit.
2. Click **Edit**.



3. The QoS settings page appears.



Available parameters are listed as follows:

Item	Description
WAN	Use the drop down list to set WAN interface for QoS by choosing one of the WAN interfaces.
Status	Enable – Click it to enable such profile. Disable – Click it to disable the QoS profile.
Bandwidth	Type the number as the total transmission rate for the outgoing /incoming data. The range can be set from 64000 to 10000000. Click the unit (Kbps or Mbps) for such rate.
High/Medium/ Normal/Low	There are several available outgoing queues. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism

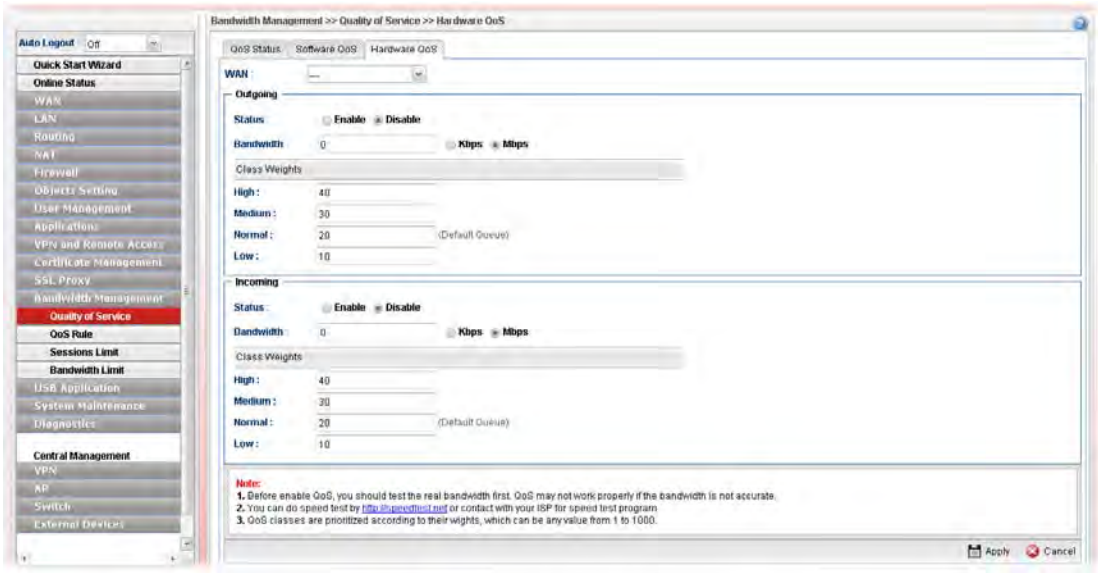
	across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

4. Enter all of the settings and click **Apply**.

4.12.1.3 Hardware QoS

This page allows you to configure bandwidth of data and voice signals transmission for outgoing data and incoming data through hardware interface.

Note: The difference between Hardware QoS and Software QoS is that only one WAN interface is supported by Hardware QoS. However, there are six WAN interfaces supported by Software QoS.



Available parameters are listed as follows:

Item	Description
WAN	Use the drop down list to choose the WAN interface to apply hardware QoS.
Status	**Enable** – Click it to enable QoS for outgoing/incoming traffic. **Disable** – Click it to disable QoS for outgoing/incoming traffic.
Bandwidth	Type the number as the total transmission rate for the outgoing /incoming data. The range can be set from 64 to 1000000 kbps. Click the unit (Kbps or Mbps) for such rate.
High/Medium/ Normal/Low	It determines the weight for each queue. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to

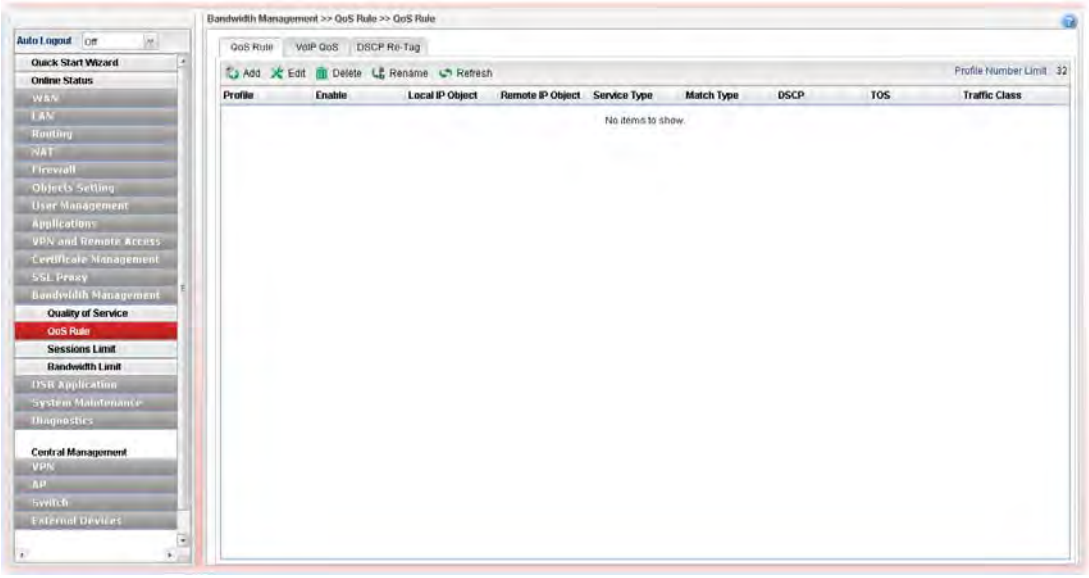
	1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

Enter all of the settings and click **Apply**.

4.12.2 QoS Rule

There are 32 filter rules that can be configured in such page for incoming and outgoing data.

4.12.2.1 QoS Rule



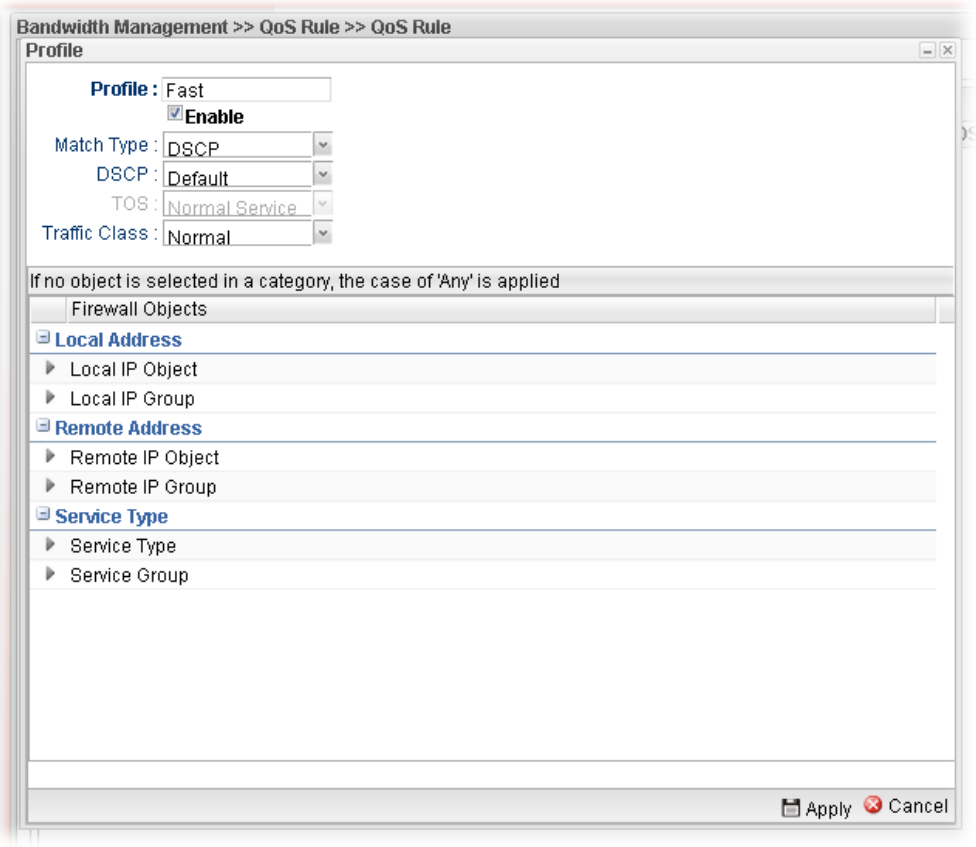
Available parameters are listed as follows:

Item	Description
Add	Add a new rule profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile for the filter.
Enable	Display the status of the profile. False means disabled; True means enabled.
Local IP Object	Display the source IP address for the filter.

Remote IP Object	Display the destination IP address for the filter.
Service Type	Display the service type (e.g., IKE, HTTP, AUTH and etc) for the filter.
Match Type	Display the match type (e.g., TOS or DSCP) for the filter.
DSCP	Display the setting of DSCP.
TOS	Display the setting of TOS.
Traffic Class	Display the queue number that such filter is categorized.

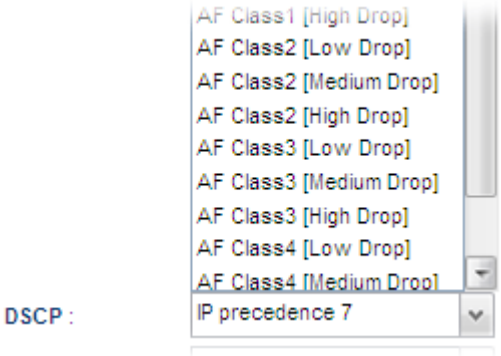
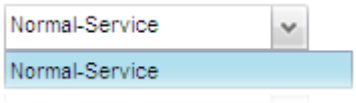
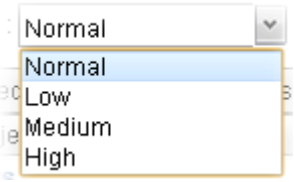
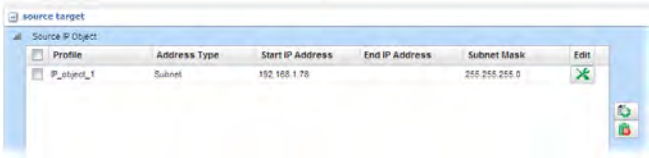
How to add a QoS rule profile

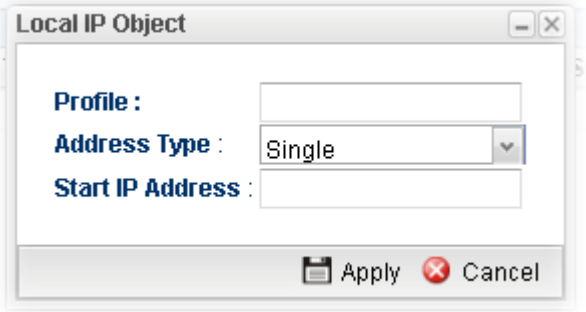
1. Open **Bandwidth Management>> QoS Rule.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the filter profile.
Enable	Check this box to enable such profile.
Match Type	Use the drop down list to specify a suitable match type.

DSCP	It is available when DSCP is selected as the Match type. 
TOS	It is available when TOS is selected as the Match type. 
Traffic Class	Choose the traffic class to category the packets matching with the condition configured as above. High is the highest; Normal is the lowest. 
Local Address	Click ▶ on the left side of the **Source IP Object/Source IP Group** profile. Check the object profile(s) as the source target.  **Local IP Object –** Use the drop down list to choose one of the IP objects for such rule profile. **Local IP Group –** Use the drop down list to choose one of the IP group for such rule profile. If you want to create a new IP object, simply click to open the following dialog.



- **Profile** – type a new name for such IP object.
- **Address Type** –Choose the address type (**Single** or **Range**) for such rule. Each type will bring different settings for configuration.
- **Start IP Address** - Type the IP address of the starting point for such profile.
- **End IP Address** - Type the IP address of the ending point for such profile if you choose **Range** as **Address Type**.
- **Subnet Mask** – Choose the subnet mask from the drop down list if you choose **Subnet** as **Address Type**.

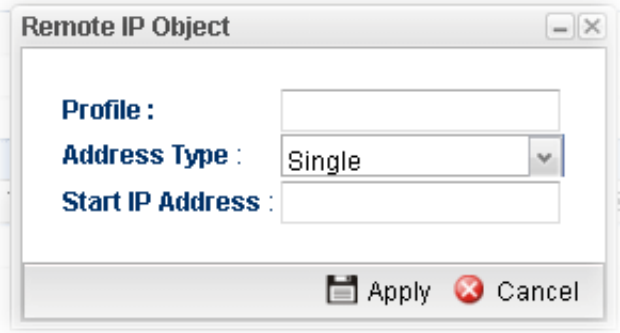
Remote Address

Click ▶ on the left side of the **Remote IP Object/ Remote IP Group** profile. Check the object profile(s) as the destination target.

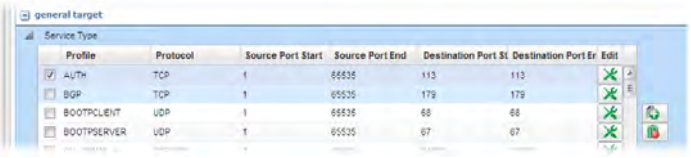
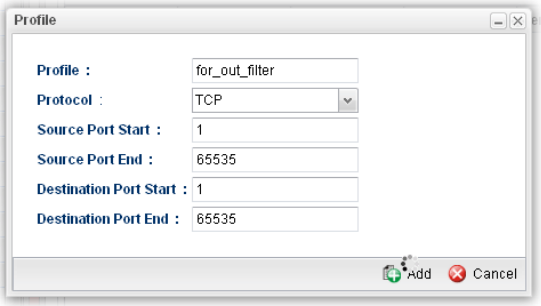
Remote IP Object – Use the drop down list to choose one of the destination IP objects for such rule profile.

Remote IP Group – Use the drop down list to choose one of the destination IP group for such rule profile.

If you want to create a new IP object, simply click to open the following dialog.



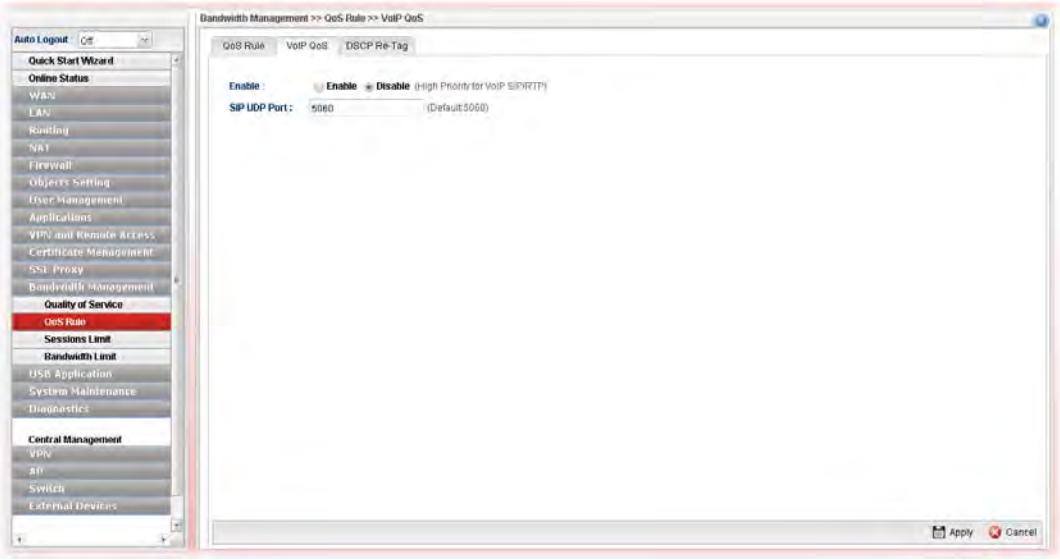
- **Profile** – Type a new name for such IP object.
- **Address Type** – Choose the address type (Single or Range) for such rule. Each type will bring different settings for configuration.
- **Start IP Address** - Type the IP address of the starting point for such profile.
- **End IP Address** - Type the IP address of the ending point for such profile if you choose **Range** as **Address**

	Type. ● **Subnet Mask** – Choose the subnet mask from the drop down list if you choose **Subnet** as **Address Type**.
Service Type	**Service Type** - Choose one of the service types from the drop down list.  If you want to create a new service type, simply click to open the following dialog.  ● **Profile** – type a new name for such service type. ● **Protocol** –There are two options: **TCP**, **UDP** and **TCP/UDP**. Select the protocol that you want to use. ● **Source Port Start /End** - Type the start /end number for the port range of the source port for such filter. ● **Destination Port Start / End** - Type the start /end number for the port range of the destination port for such filter.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. A QoS rule profiler has been created.

4.12.2.2 VoIP QoS

When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority during the process of data transmission.

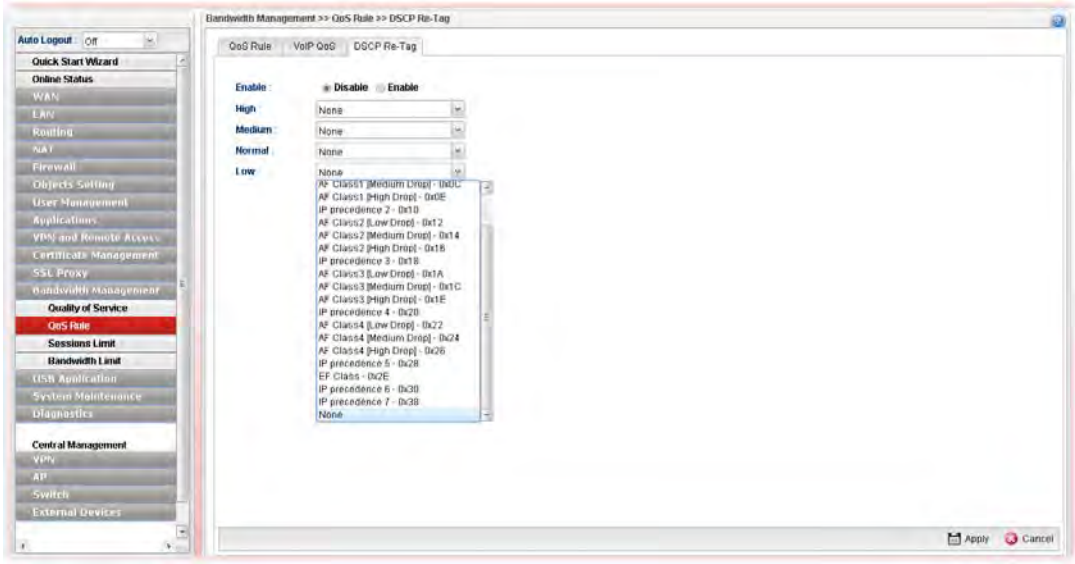


Each item will be explained as follows:

Item	Description
Enable	**Enable** - Click it to enable VoIP QoS function.
SIP UDP Port	Set a port number used for SIP.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

4.12.2.3 DSCP Re-Tag

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.



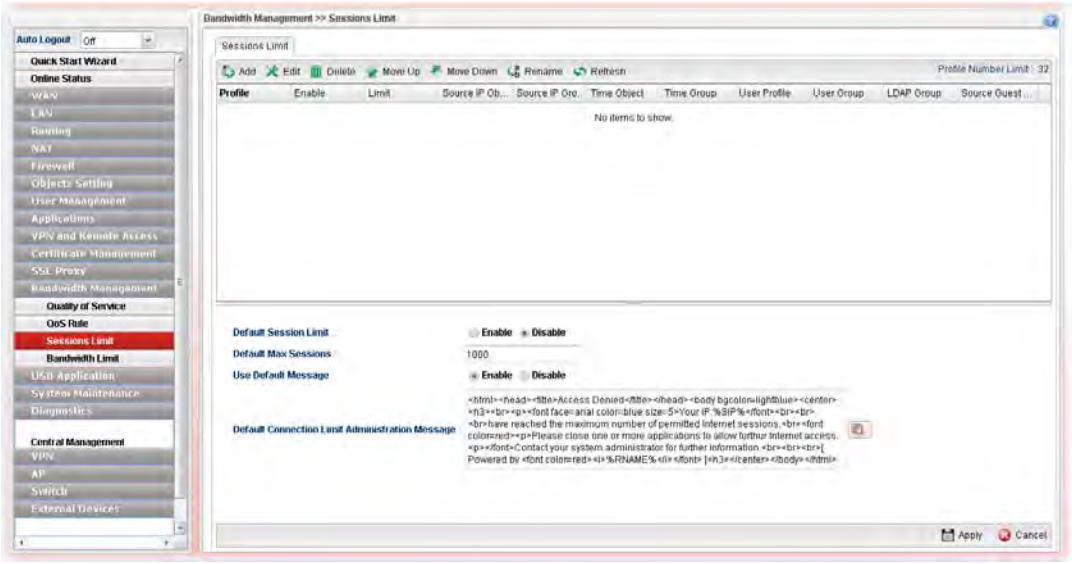
Each item will be explained as follows:

Item	Description
Enable	Enable – Click it to enable DSCP Re-Tag function.
High / Medium / Normal / Low	There are four queues allowed for QoS control. Use the drop down list to specify the heading for each queue which will be applied to the packets tagged.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

4.12.3 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



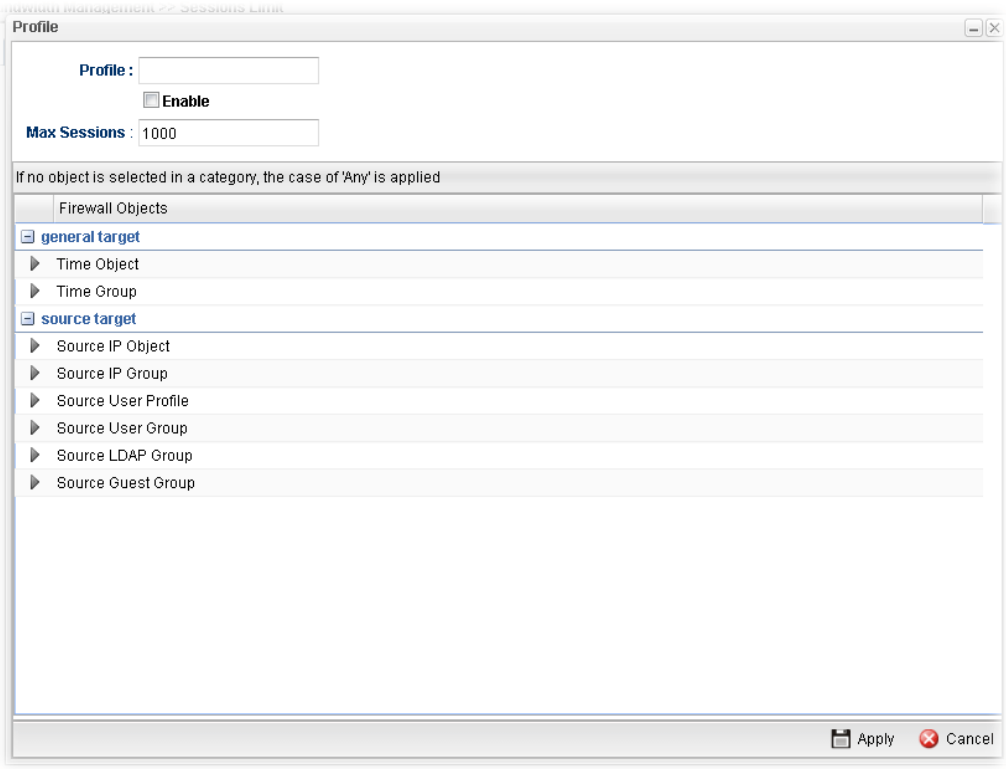
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Limit	Display the maximum session number allowed for the profile.

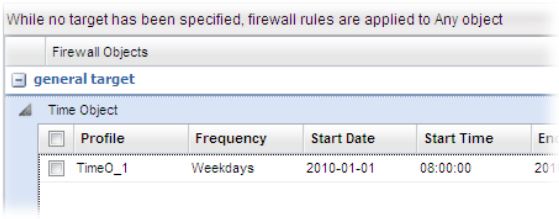
Source IP Object	Display the source IP object profile name.
Source IP Group	Display the source IP group profile name.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application profile.
Default Session Limit	Display the default session number used for each computer in LAN.
Default Max Sessions	Display the default maximum session number used for each computer in LAN.
Use Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page.. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Connection Limit Administration Message	Such field is available when you disable the function of **Use Default Message**. The message will display on the user's browser when he/she tries to access the blocked web page.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to add a session limit profile

1. Open **Bandwidth Management>> Sessions Limit.**
2. Simply click the **Add** button.
3. The following dialog will appear.

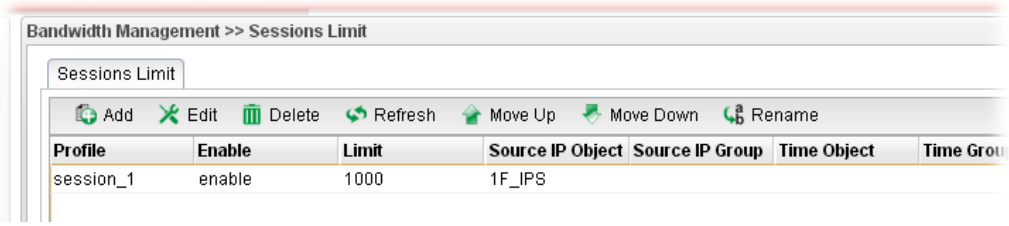


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
Max Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index. This field cannot be typed with “0”, otherwise the profile cannot be saved.
general target	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click to create another new time object profile.  **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another new time group profile.
source target	Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object/IP group/User

	Profile/User Group/LDAP Group/Guest Group profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new object profile.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

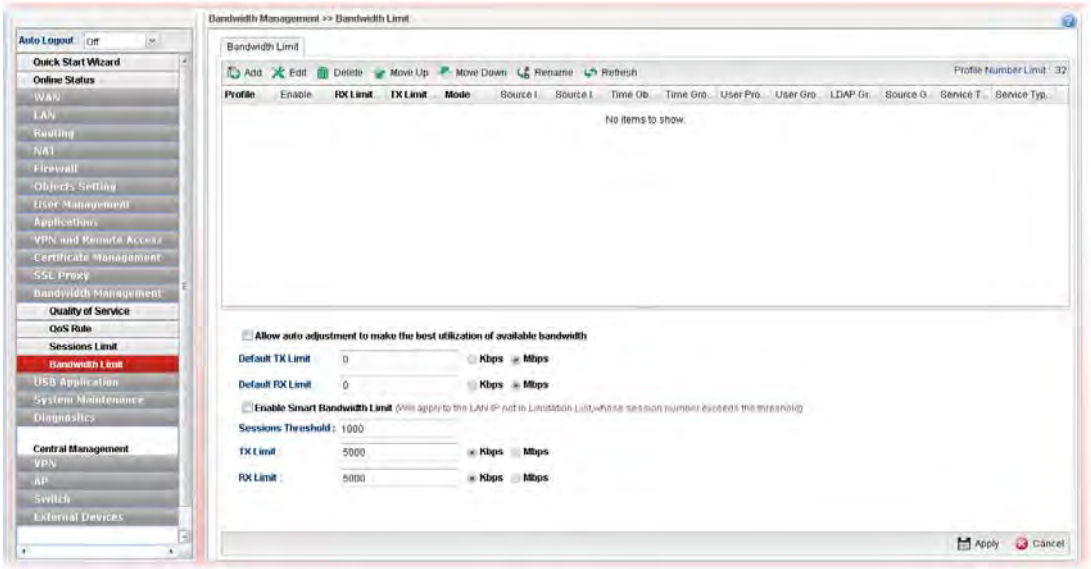
4. Enter all the settings and click **Apply**.
5. A session limit profile has been created.



4.12.4 Bandwidth Limit

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

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



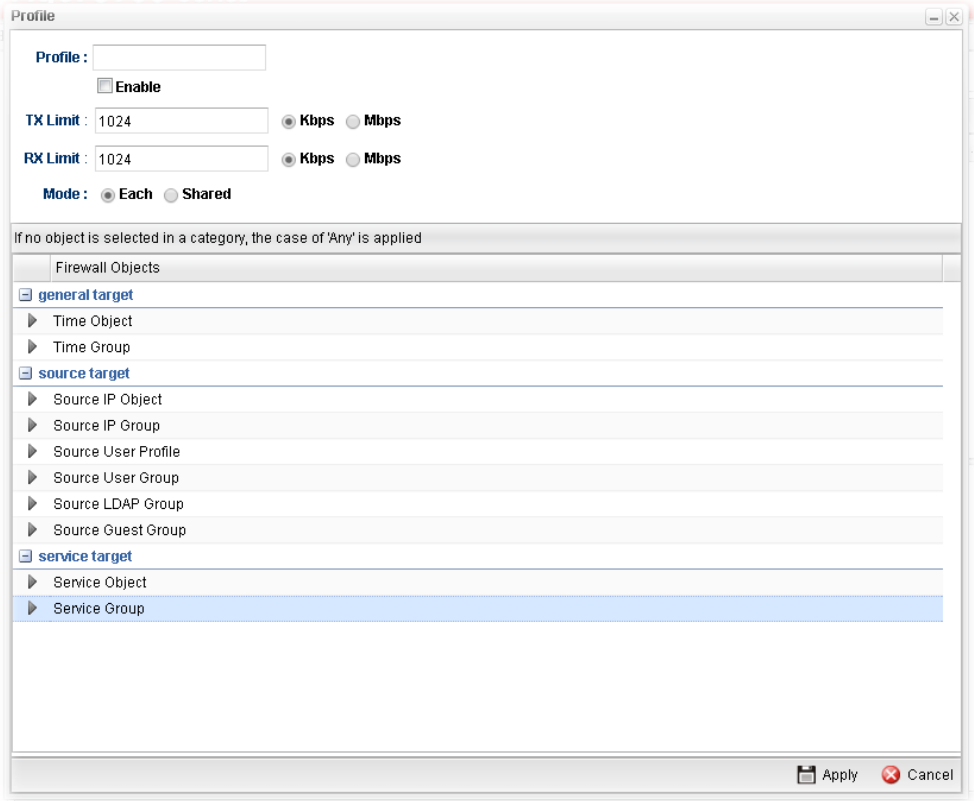
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile	Display the name of the bandwidth limitation profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
RX Limit	Display the limitation for the speed of the downstream.
TX Limit	Display the limitation for the speed of the upstream.
Mode	Display the mode selection (Each/Shared) of the selected profile.

Source IP Object	Display the source IP object profile name.
Source IP Group	Display the source IP group profile name.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application profile.
Allow auto adjustment…	Check this box to make the best utilization of available bandwidth.
Default TX/RX Limit	The default limit will apply to LAN IP(s) not in the above configuration profiles **Default TX Limit** – Define the limitation for the speed of the upstream. **Default RX Limit** –Define the limitation for the speed of the downstream.
Enable Smart Bandwidth Limit	Check this radio button to configure the default limitation for bandwidth for any LAN IP not included in the Limitation List.
Session Threshold	When session number exceeds the set threshold, Smart Bandwidth limit will work.
TX Limit	Define the speed of the upstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission.
RX Limit	Define the speed of the downstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

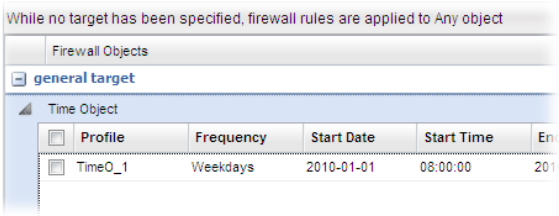
How to add a bandwidth limit profile

1. Open **Bandwidth Management>>Bandwidth Limit.**
2. Simply click the **Add** button.
3. The following dialog will appear.

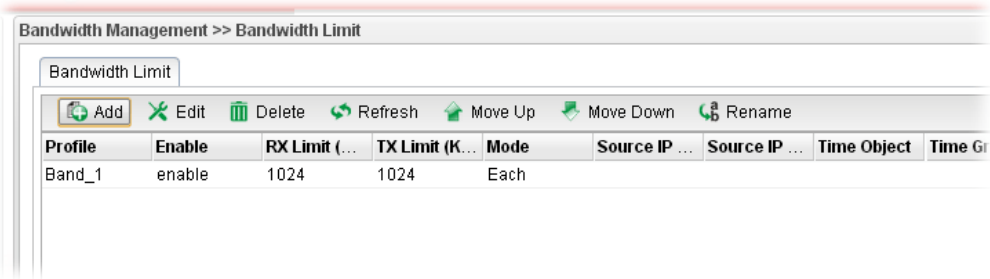


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
TX Limit(Kbps)	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
RX Limit(Kbps)	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
Mode	Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.

general target	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click to create another new time object profile.  **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click to create another new time group profile.
source target	Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object/IP group/User Profile/User Group/LDAP Group/Guest Group profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new object profile.
service target	Click the triangle icon ▶ to display the profile selection box. Choose one or more Service object/Service Group profiles from the drop down list. The selected profile will be treated as source target. You can click to create another new object profile.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

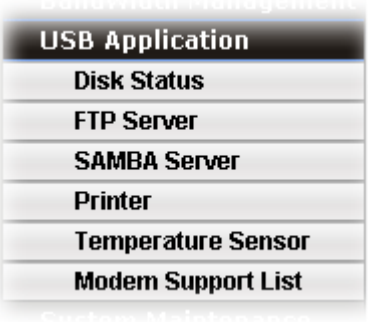
4. Enter all the settings and click **Apply**.
5. A bandwidth limit profile has been created.



4.13 USB Application

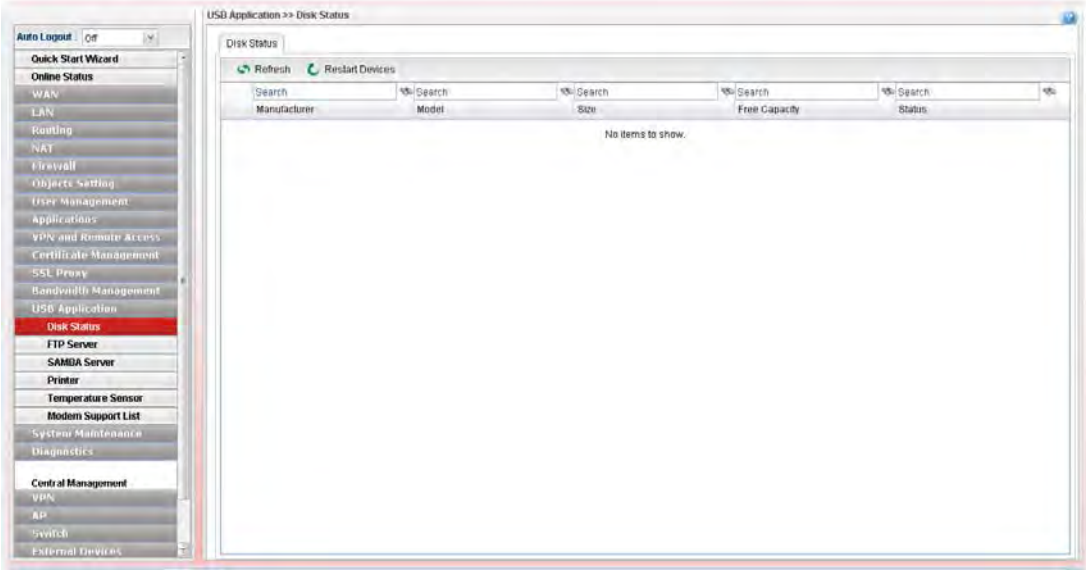
By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **User Management>>User Profile** on the client software. Then, the client can use the FTP site (USB storage disk) through Vigor router.

> **Note**: USB ports on Vigor router are allowed to connect to USB modem. Models of the modems supported by Vigor router can be seen from **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>General Setup** for detailed information.



4.13.1 Disk Status

This page is to monitor the status for the users who accessing into FTP server (USB storage disk) via the Vigor router. In addition, the status of the USB modem or USB printer connecting to Vigor router can be checked from such page.



Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh current USB connection status. The result will be shown on the screen immediately.
Restart Devices	Click it to restart the USB device.
Manufacturer	Display the manufacturer of the USB device.

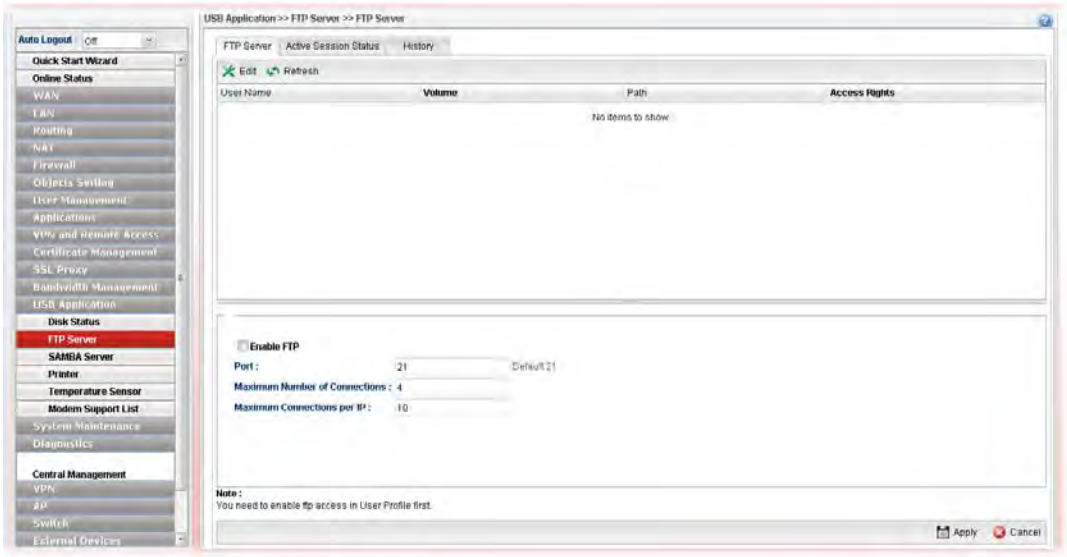
Model	Display the type of the USB device.
Size	Display the total disk capacity of the USB device.
Free Capacity	Display the remaining disk space of the USB device.
Status	Display the status of the USB device.
(Remove Icon)	At present, FAT, EXT2, EXT3 USB format can be supported by Vigor router. If such USB is inserted into the USB slot, the Status field will display “In Use” and the remove icon will appear on the screen. If you want to remove the USB disk, simply click this icon.

4.13.2 FTP Server

This page allows you to edit FTP user setting for FTP users. Any user who wants to access into the USB storage disk must type the same username and password configured for the user profile. Before adding or modifying settings in this page, please insert a USB storage disk first.

At present, the Vigor router can support USB storage disk with versions of FAT16/32 and EXT2/3 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16/32 or EXT2/3.

All of the profiles displayed here are created by **User Management>>User Profile,** with **Allow FTP Server Login** enabled. The **History** tab displays FTP connection status.



Available settings are explained as follows:

Item	Description
Edit	Click it to edit the selected USB device.
Refresh	Click it to refresh current USB connection status.
User Name	It displays the username that user uses to login to the FTP server. If there is nothing displayed here, it means there is no FTP user profile created. Just open **User Management>>User Profile,** create a new user profile with **Allow FTP Server Login** enabled.

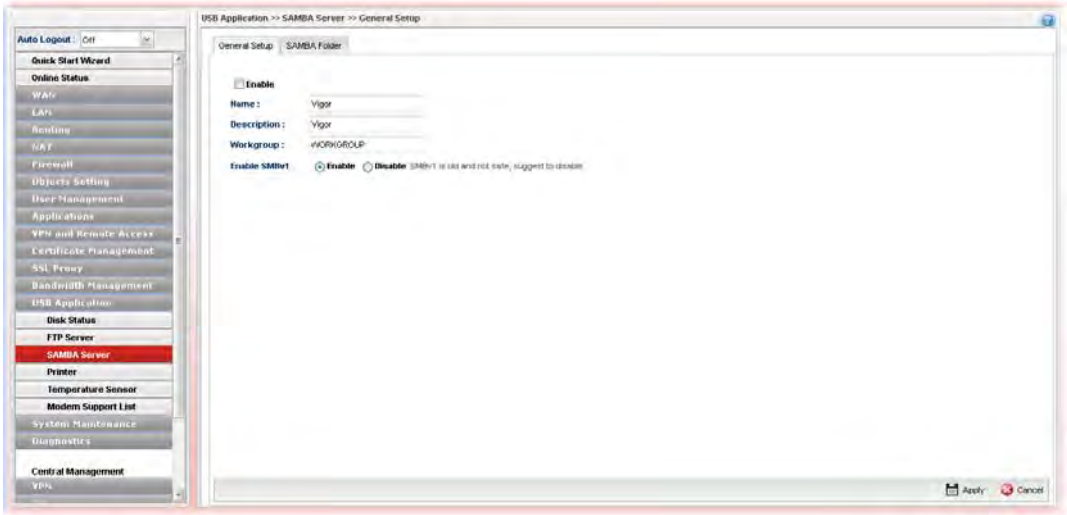
Volume	It displays the proper volume for the connected USB disk.
Path	It displays the directory name for the connected USB disk.
Access Rights	It displays the access right for the connected USB disk.
Enable FTP	Check the box to enable FTP server.
Port	Type required port number for FTP server. Or, use the default value.
Maximum Number of Connections	It means the maximum session limit for the FTP server. The default setting is “4” for downloading, uploading and keeping network connection.
Maximum Connection per IP	It means the maximum session limit for the FTP server per each IP address. For example, an IP address is used by two FTP users for connecting network. That means there are two sessions used for the IP and the FTP server. The default setting is “10”.

4.13.3 SAMBA Server

SAMBA server offers the file sharing service for users through a specified file folder. Any user who wants to access into the USB storage disk must type the same name and use the same workgroup. Before adding or modifying settings in this page, please insert a USB storage disk first.

4.13.3.1 General Setup

This page allows you to configure settings for SAMBA server.



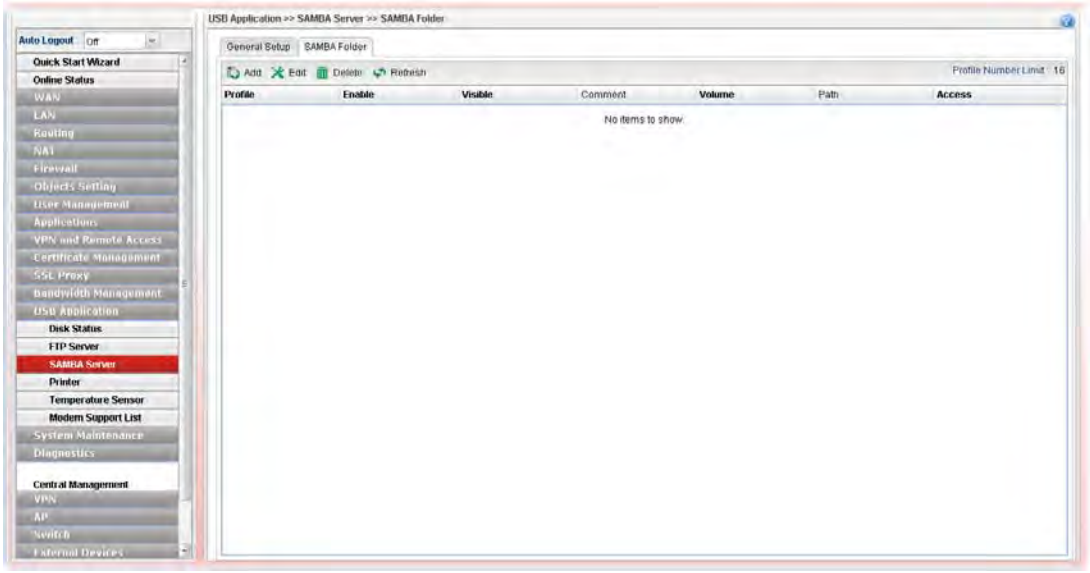
Available settings are explained as follows:

Item	Description
Enable	Check the box to enable SAMBA server.
Name	Type the NetBios name of the SAMBA Server.
Description	Type any text to describe SMABA server.
Workgroup	Type the name of the workgroup for the SAMBA server

	to be located by Windows system. Default name will be offered for Windows XP user.
Enable SMBv1	For the system security, use the default setting (Disable). SMBv1 is used for the computer with old operation system which does not support SMBv2 or SMBv3.

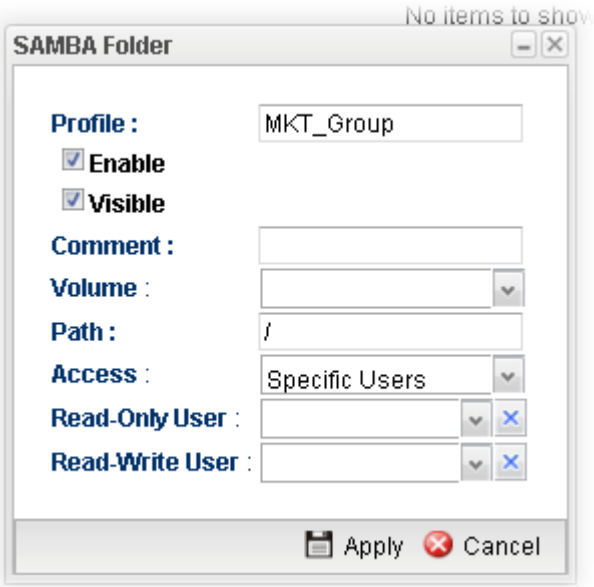
4.14.3.2 SAMBA Folder

Due to the file sharing feature of SAMBA server, this page allows you to create any profile which can be shared by clients on the network.

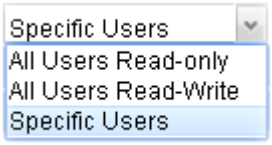


How to add/edit a SMABA folder profile

1. Open **USB Application>>SMABA Server** and click **SAMBA Folder** tab.
2. Click the **Add** button. For an existed profile, simply choose that profile and click the **Edit** button.
3. The following dialog will appear.



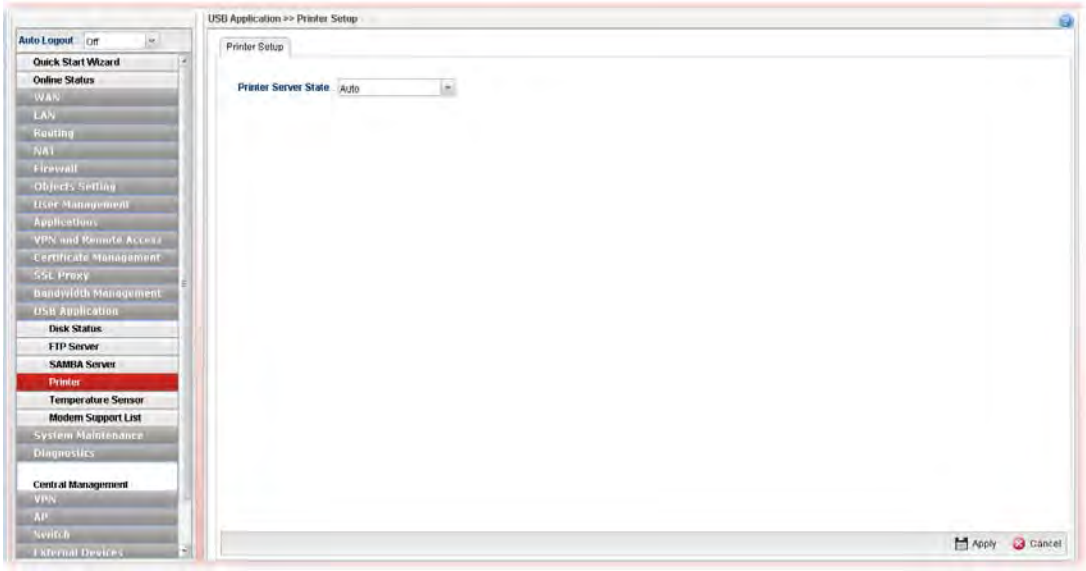
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile to be shared.
Enable	Check this box to enable such profile.
Visible	Check this box to make such profile be seen by users. If not, the user must know and type the path of the folder name to access into that folder.
Comment	Type any text to describe such profile if required.
Volume	Use the drop down list to specify the proper volume for the connected USB disk.
Path	It indicates the directory name for the connected USB disk. The default setting is "/".
Access	There are three options for you to specify.  **All Users Read-only** – Such option allows all of the users sharing the SAMBA service to read the file stored under the sharing folder. **All Users Read-Write** – Such option allows all of the users sharing the SAMBA service to read and write the file stored under the sharing folder. If **Specific Users** is selected, you have to additionally specify Read-Only User and Read-Write User. ● **Read-Only User** – User profiles (with **Allow SAMBA Server Login** Enabled) created under **User Management>>User Profile** will be displayed here. Choose the one to have the right to read the file on SAMBA folder. ● **Read-Write User** - User profiles (with **Allow SAMBA Server Login** Enabled) created under **User Management>>User Profile** will be displayed here. Choose the one to have the right to read and write the file on SAMBA folder.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

4. Enter all of the settings and click **Apply**.
5. A folder profile has been created.

4.13.4 Printer

This page is used to enable the printer server state when a printer device is connected via USB port.



Available settings are explained as follows:

Item	Description
Printer Server State	**Auto**- It's the default setting. Vigor router will detect if the connected device is printer or not. If yes, the printer server will be enabled automatically to activate the printer. **Enable** – The printer server will be enabled. **Disable** – The printer server will be disabled.
Apply	Click it to save the configuration.
Cancel	Click it to return to factory default setting.

4.13.5 Temperature Sensor

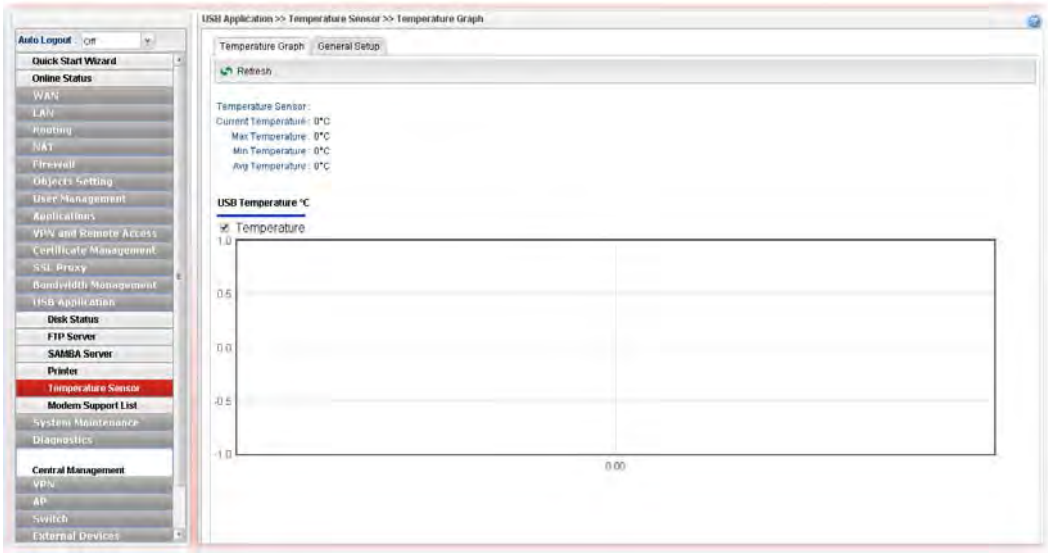
A USB Thermometer is now available that complements your installed DrayTek router installations that will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

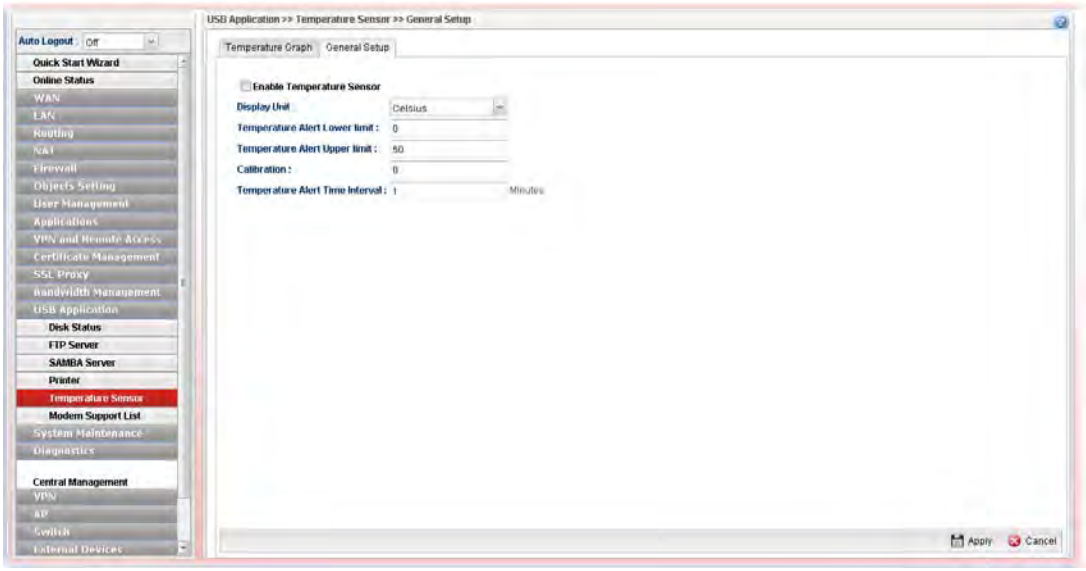
The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

4.13.5.1 Temperature Graph

Below shows an example of temperature graph:



4.13.5.2 General Setup



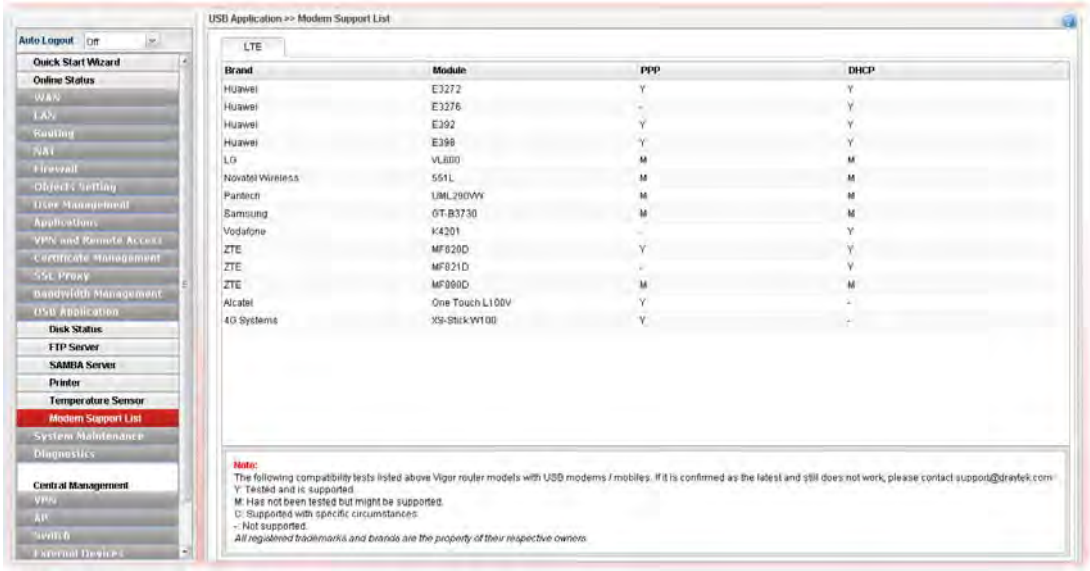
Available settings are explained as follows:

Item	Description
Enable Temperature Sensor	Check this box to enable such function.
Display Unit	Choose **Celsius** or **Fahrenheit** as the display unit.
Temperature Alert Lower limit / Temperature Alert Upper limit	Type the upper limit and lower limit for the system to send out temperature alert.
Calibration	Type a value used for correcting the temperature error.
Temperature Alert Time Interval	The default setting is one minute. That means, the temperature alert will be sent per minute.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

Enter all of the settings and click **Apply**.

4.13.6 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.



4.14 System Maintenance

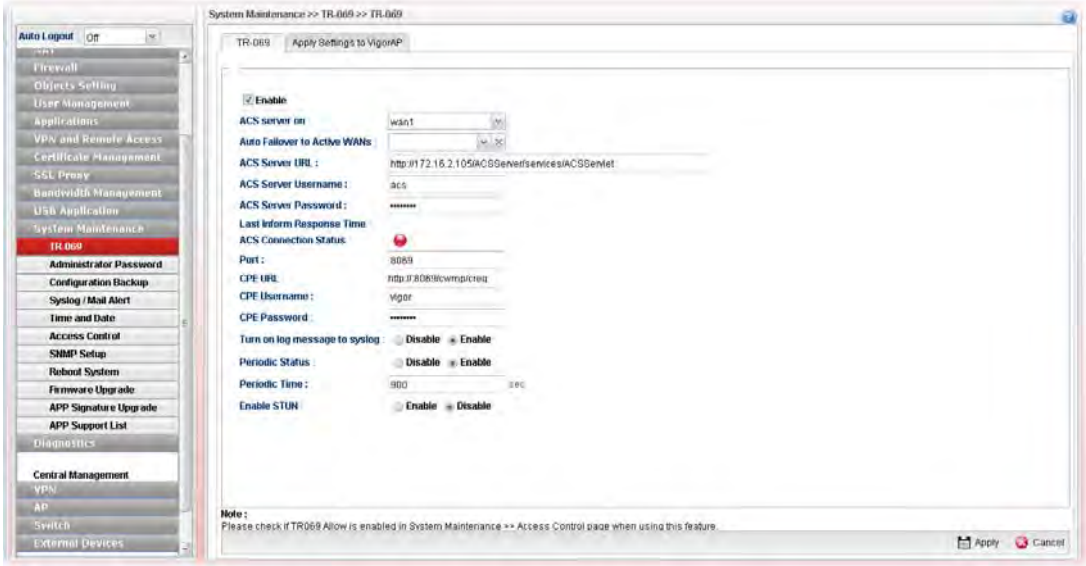
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Access Control, SNMP Setup, Reboot System, Firmware Upgrade, APP Signature Upgrade and APP Support List.

Below shows the menu items for System Maintenance.

4.14.1 TR-069

4.14.1.1 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



Each item will be explained as follows:

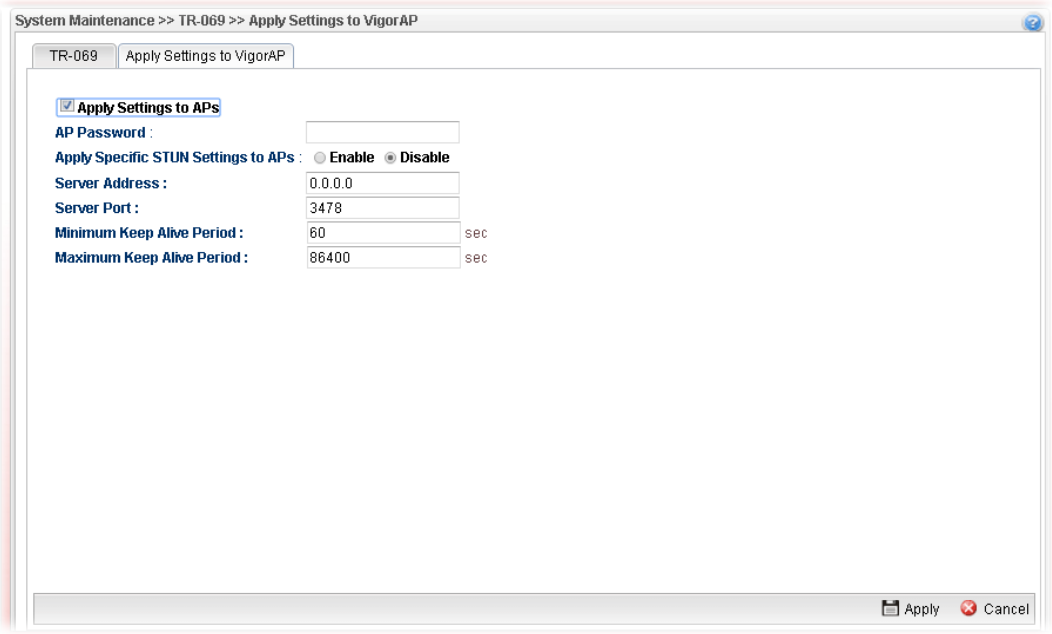
Item	Description
Enable	Check this box to enable such profile.

ACS server on	Choose one of the WAN/LAN profiles which will be recognized by VigorACS.
Auto Failover to Active WANs	Specify the WAN interface to take over the job of network connection when the original WAN interface fails.
ACS Server URL/ ACS Server Username / ACS Server Password	Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
Last Inform Response Time	Display the response time informed by VigorACS.
ACS Connection Status	When it lights in green, it means the router has been detected and can be managed by VigorACS.
CPE Protocol	Select HTTP or HTTPs for the router to communicate with VigorACS.
Port	Type the port number for Vigor3900 which will be recognized by VigorACS.
CPE URL	Display the URL of such CPE.
CPE Username	Type the user name for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
CPE Password	Type the password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
Turn on log message to syslog	The default setting **Disable**. Click **Enable** to make the log message being recorded by Syslog.
Periodic Status	The default setting is **Enable**. Please set periodic time for VigorACS to send notification to CPE. Or click **Disable** to close the mechanism of notification.
Periodic Time	Set the time for VigorACS to send notification to CPE.
Enable STUN	**Enable/Disable** - The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server Address –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.14.1.2 Apply Settings to VigorAP

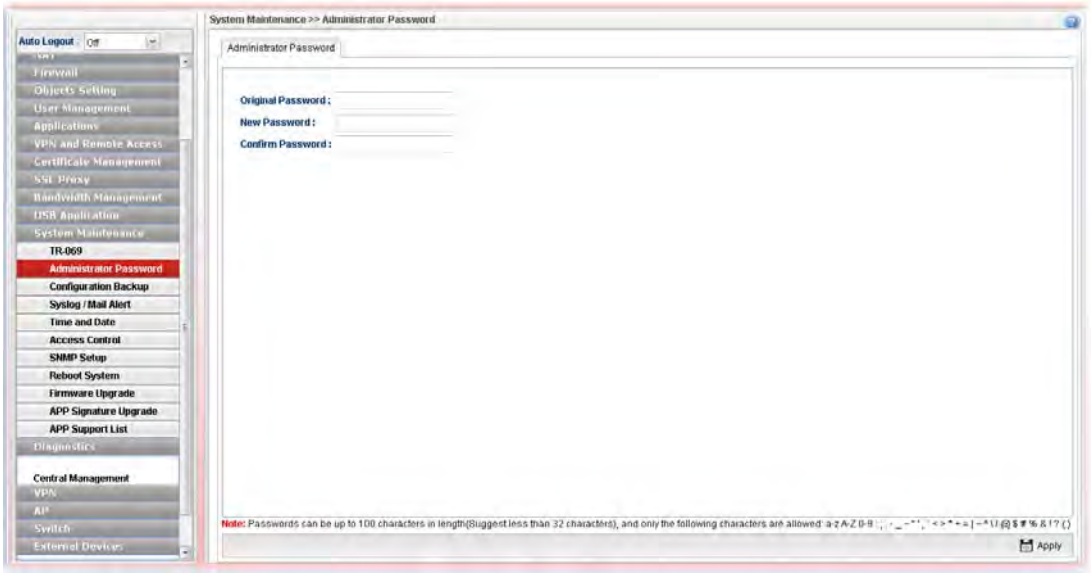
This feature is able to apply TR-069 settings (including STUN and ACS server settings) to all of APs managed by Vigor3900 at the same time.



Item	Description
Apply Settings to APs	Check this box to make the settings in this page apply to VigorAP.
AP Password	Type the password of the VigorAP that you want to apply Vigor3900's TR-069 settings.
Apply Specific STUN Settings to APs	After clicking the **Enable** radio button for **Apply Settings to APs**, if you want to apply specific STUN settings (not the STUN Settings configured for Vigor3900) to VigorAPs to meet specific requirements, simply check this box. Then, type the server IP address, server port, minimum keep alive period and maximum keep alive period respectively.
Server Address	Type the IP address of the STUN server.
Server Port	Type the port number of the STUN server.
Minimum Keep Alive Period	If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
Maximum Keep Alive Period	If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.14.2 Administrator Password

This page allows you to set new password for accessing into the web user interface of the router.



Each item will be explained as follows:

Item	Description
Original Password	Type the old password.
New Password	Type the new password.
Confirm Password	Re-type the new password for confirmation.
Apply	Click this button to save the configuration and exit the web page.

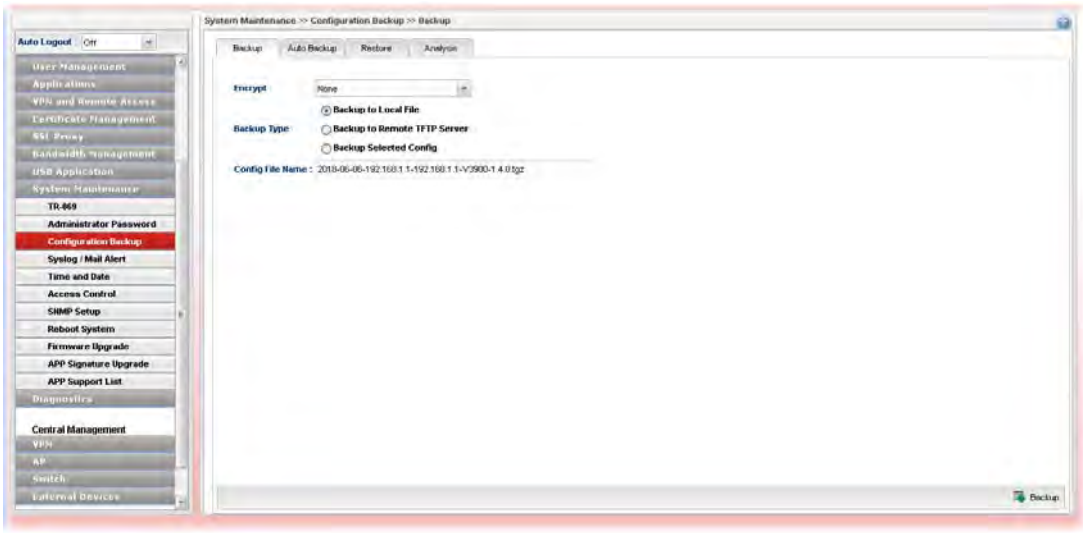
Enter all of the settings and click **Apply**.

4.14.3 Configuration Backup

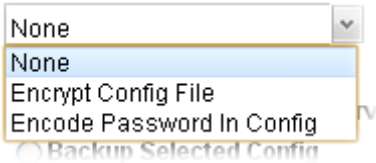
Most of the settings can be saved locally as a configuration file, and can be applied to another router. The router supports functions of **restore and backup** for the configuration file.

4.14.3.1 Backup

This page allows you to set general settings (e.g., encryption mode, backup type, config file name) for configuration backup.



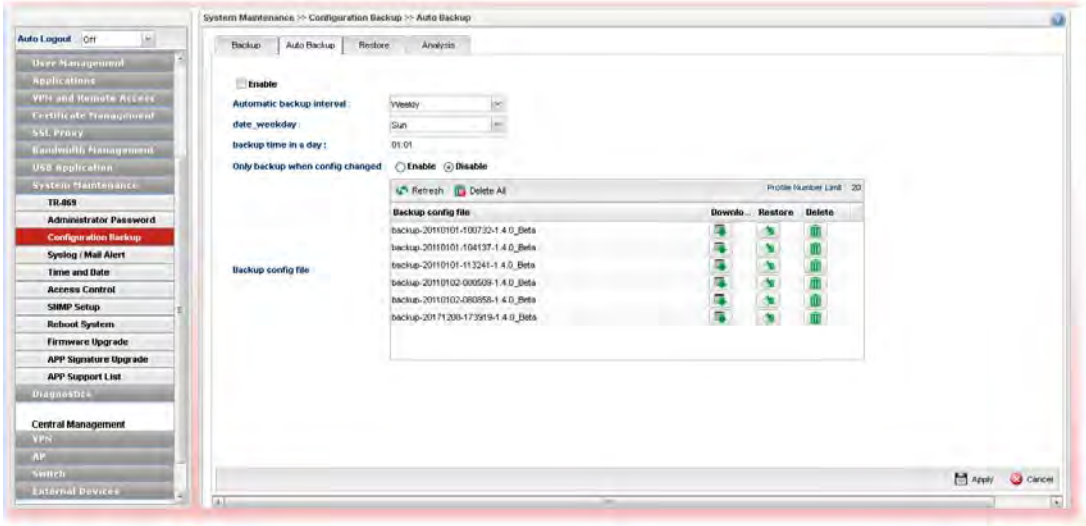
Each item will be explained as follows:

Item	Description
Encrypt	**None** – No encryption will be used. **Encrypt Config File** – Choose it to encrypt the whole configuration file. ● **Password** – Type a password for encrypting the file. ● **Confirm Password –** Retype the password for confirmation.  **Encode Password in Config** – Choose it to encrypt the password information in configuration file.
Backup Type	Choose one of the types to determine where the file will be stored. **Backup to Local File** – The configuration file will be stored in local host. **Backup to Remote TFTP Server** – The configuration file will be stored in the remote TFTP server specified. ● **Remote Server IP** – Type the IP address of the remote server. **Backup Selected Config** – The configuration file will be

	stored with an existing file in local host. You must select which file you want to store. ● **Select Config File** – Choose and check which type(s) of configuration will be saved. ● **Select Lang File** – Choose and check which language(s) to be saved.
Config File Name	Display the default configuration file name. You can change the name if required.
Backup	Execute the file downloading job to the computer.

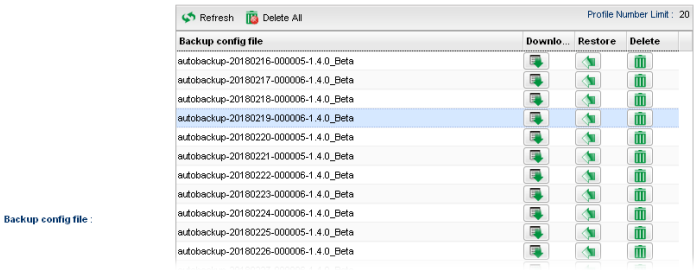
4.14.3.2 Auto Backup

The configuration can be stored to Vigor router as a backup file. Such page can set conditions for Vigor router to perform configuration backup automatically.

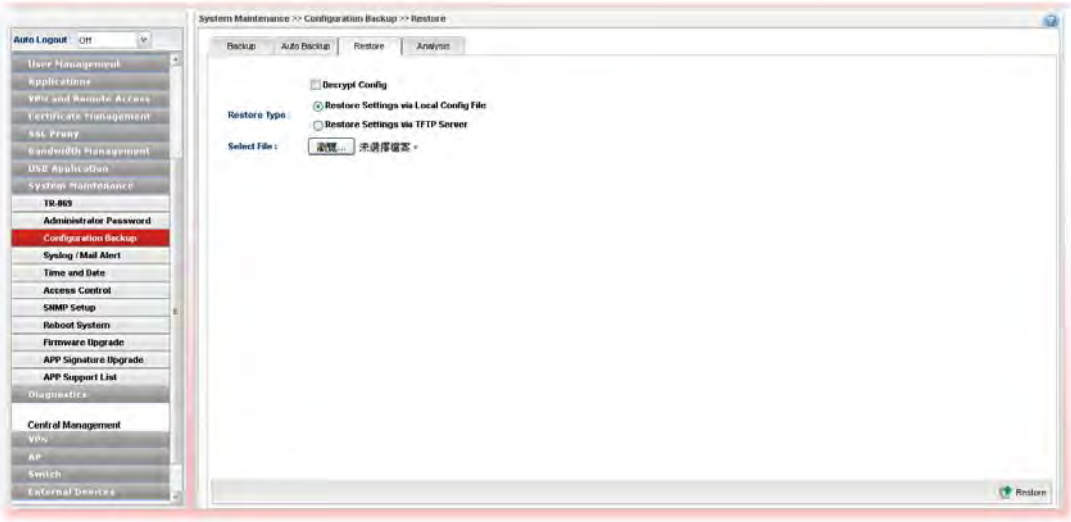


Each item will be explained as follows:

Item	Description
Enable	Check it to enable **Auto Backup** function.
Automatic backup interval	Specify the type of backup interval for the system to perform configuration backup automatically. **Daily –** Configuration backup will be performed everday. **Weekly –** Configuration backup will be performed per week. **Monthly –** Configuration backup will be performed per month.
date_weekday	It is available when **Weekly** is selected as Automatic backup interval. Use the drop down list to choose one day.
date_day	It is available when **Monthly** is selected as Automatic backup interval. Enter a number (1 to 31) to represent the day within a month.
backup time in a day	It is available when **Weekly / Daily** is selected as Automatic backup interval.

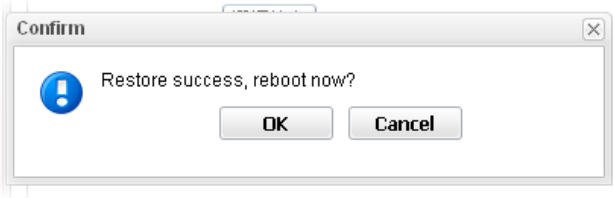
	Set the time interval by entering “hh:mm” (hours:minutes).
Only backup when config changed	**Enable** – Click it to enable such function. Then, backup will be executed whenever the configuration is changed. **Disable** – The backup will be executed periodically based on the conditions set above.
Backup config file	The records of configuration backup files will be shown in this table**.** 
Apply	Click this button to save the settings configured in this page.
Cancel	Click this button to discard the settings configured in this page.

4.14.3.3 Restore



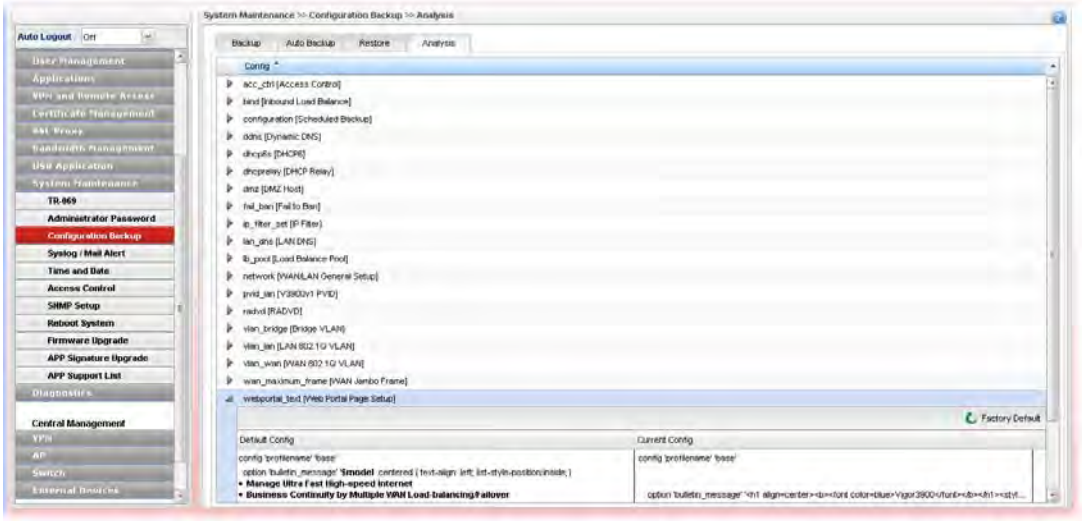
Each item will be explained as follows:

Item	Description
Decrypt Config	Check this box to decrypt an encrypted configuration file. You can specify a password for decrypting the file for restoring it for use next time. **Password** – Type a password for encrypting the file. **Confirm Password –** Retype the password for confirmation.
Restore Type	Choose one of the types to determine where the file will be downloaded from. **Restore Settings via Local Config File** – Click it to restore the configuration settings through a configuration file stored

	locally. **Restore Settings via TFTP Server** – Click it to restore the configuration settings through TFTP server. ● **Remote Server IP** – Type the IP address of the TFTP server. ● **Config File Name** – Type the configuration file name to be restored.
Select File	Use the **Select** button to locate the file for uploading to the router.
Restore	Click it to upload the selected file to the router. After finishing the restoration, the system will ask you to reboot the router. 

4.14.3.4 Analysis

Such analysis page will show user defined settings result. In comparing the default settings with information displayed in this page, it will be convenient for administrator, user or RD member for debug possible error.

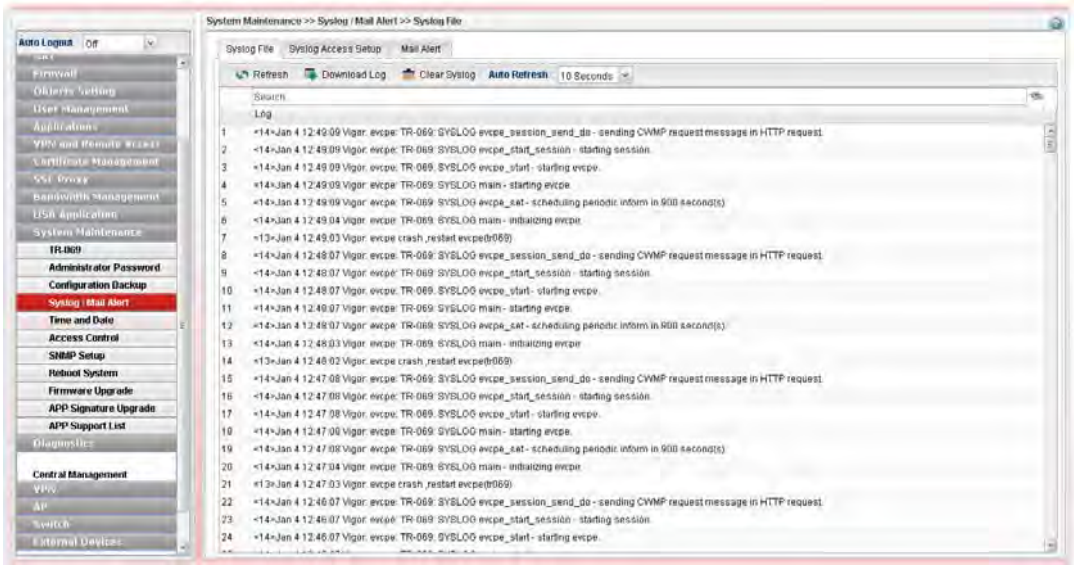


4.14.4 Syslog / Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web User Interface of the router or borrow debug equipments.

4.14.4.1 SysLog File

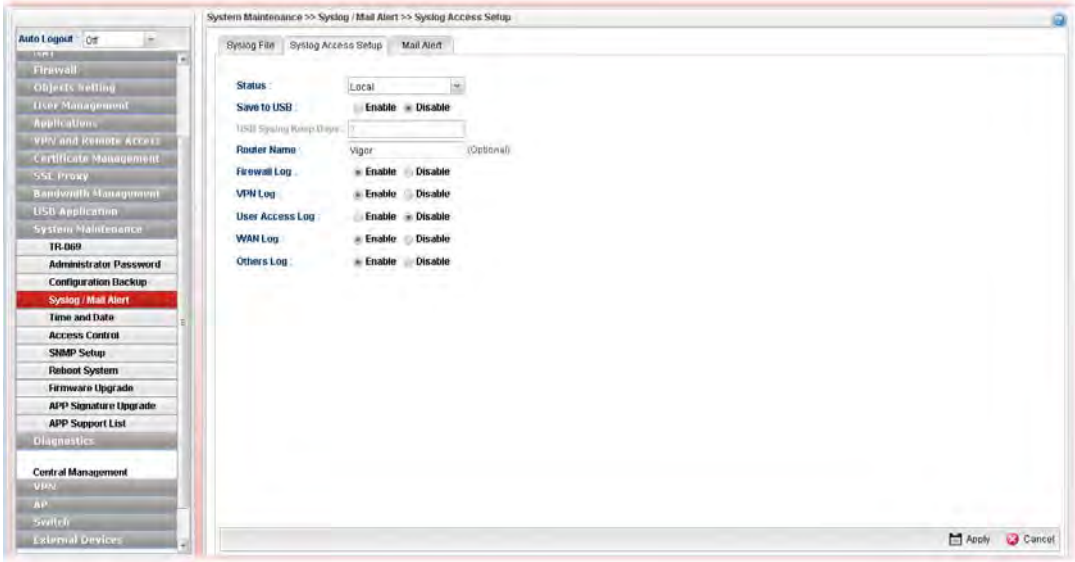
This page displays all the operation logs for the router.



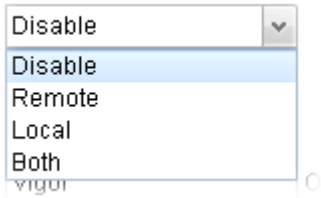
Available parameters are listed as follows:

Item	Description
Refresh	Renew the web page.
Download Log	Save or open the Syslog file.
Clear Syslog	Remove all of the records.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.

4.14.4.2 Syslog Access Setup



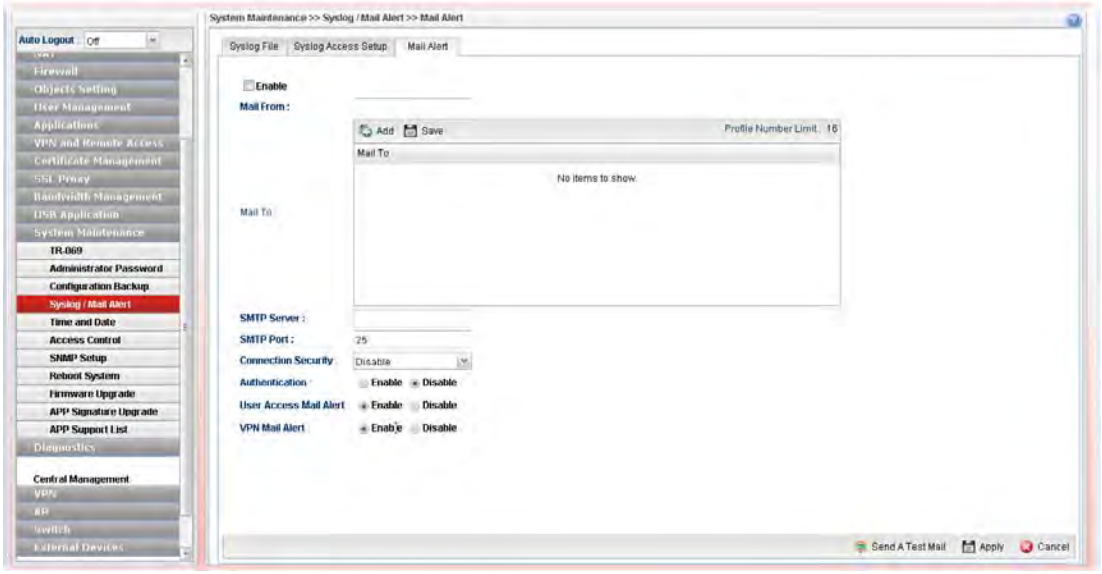
Available parameters are listed as follows:

Item	Description
Status	Choose one of the selections to determine current status for Syslog access. If you choose **Local** as Status, you don't need to type any server IP and port. Just give a name for the router. 
Save to USB	Such option is available when **Remote/Local/Both** is selected in **Status**. **Enable** – Click it to save the log onto USB disk. **Disable** – Click it to disable the function of log to USB. **USB Syslog Keep Days** – Type the days that USB disk will keep the log without deleting.
Router Name	Type the name of the router. The default name is ***Vigor.***
Server IP/Host Name	Such option is available when **Remote/Both** is selected in **Status**. Type the IP address or host name of the Syslog server. It is available when **Remote** or **Both** is selected as **Status**.
Server Port	Such option is available when **Remote/Both** is selected in **Status**. Type the port number for the Syslog server. It is available when **Remote** or **Both** is selected as **Status**.
Firewall Log	Click **Enable** to make the firewall log recorded in the Syslog.

VPN Log	Click **Enable** to make the VPN log recorded in the Syslog.
User Access Log	Click **Enable** to make the user access log recorded in the Syslog.
WAN Log	Click **Enable** to make the WAN log recorded in the Syslog.
Others Log	Click **Enable** to make other logs recorded in the Syslog.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.14.4.3 Mail Alert



Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable such profile.
Mail From	Type a mail address for the mail sender.
Mail To	Assign a mail address for the mail receiver. **Add** – Click this button to display a field for adding e-mail address. **Save** – After finished the address configuration, click Save to save the setting onto the router.
SMTP Server	Type the IP address for SMTP server.
SMTP Port	Type the port number for SMTP server.
Connection Security	Choose **SSL/TLS** or **StartTLS** to activate corresponding server.
Authentication	Click **Enable** to make any user logging into the mail server. If you click **Enable**, you have to type user name and user password on the below fields.

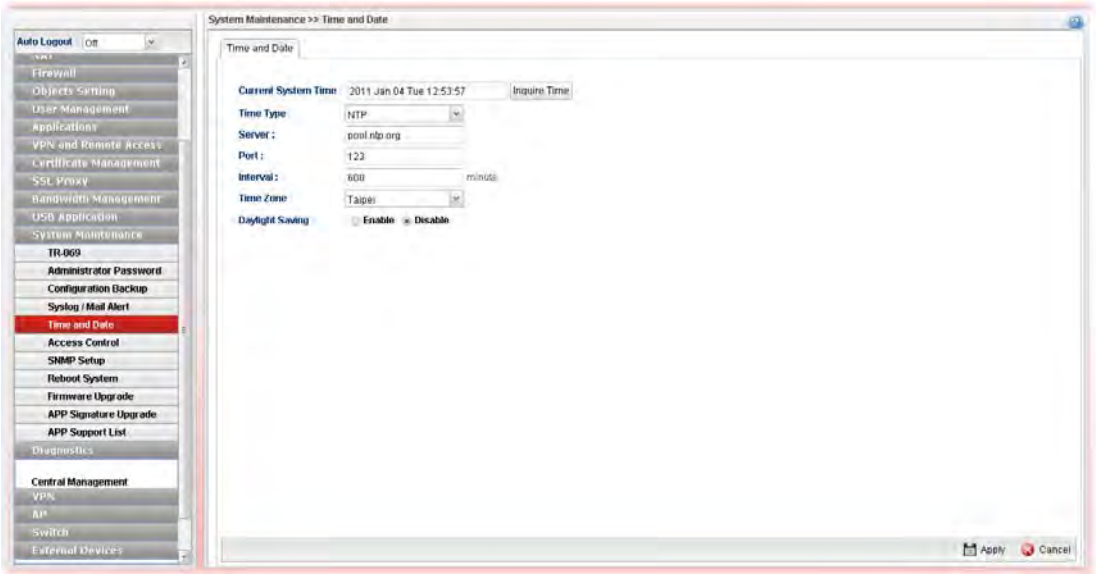
	User Name - Type the user name for authentication. **User Password -** Type the password for authentication.
User Access Mail Alert	**Enable -** Vigor router sends a mail as an alert if it detects any user access event. **Disable** – Vigor router does not send any mail to inform the user login event.
VPN Mail Alert	**Enable -** Vigor router sends a mail as an alert to inform VPN connection. **Disable** – Vigor router does not send any mail to inform VPN connection.
Send A Test Mail	Click it to send a test mail to the specified address.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.14.5 Time and Date

This page allows you to specify where the time of the router should be inquired from.

As an NTP (Network Time Protocol) client, the router gets standard time from the time server. Some time-based functions cannot work properly until the system time functions run successfully. Typically, NTP achieves high accuracy and reliability with multiple redundant servers and diverse network paths.



Available parameters are listed as follows:

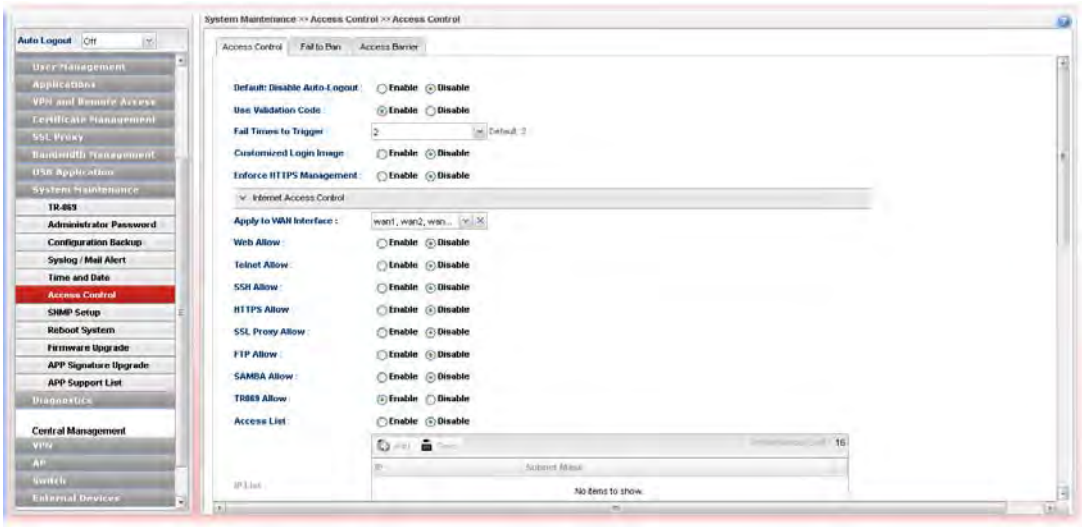
Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Time Type	**NTP** – Select to inquire time information from Time Server on the Internet using assigned protocol. **Browser** - Select this option to use the browser time from the remote administrator PC host as router's system time.
Server	Type the domain name of the server.
Port	Type the port number for the time server.
Interval	Select a time interval for updating from the NTP server.
Time Zone	Select the time zone where the router is located.
Daylight Saving	Click **Enable** to enable the daylight saving. Such feature is available for certain area.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.14.6 Access Control

4.14.6.1 Access Control

This page allows you to open or close the Web User Interface of Vigor3900 by using Telnet, SSH, HTTP, HTTPS… and etc…



Available parameters are listed as follows:

Item	Description
Default: Disable Auto-Logout	**Enable** – Vigor router will auto logout based on the specified time setting (e.g., 1, 3, 5 and 10 minutes). **Disable** – Default setting. The function of Auto-Logout will be disabled.
Use Validation Code	**Disable –** No validation will be done when a user tries to log into the web user interface of Vigor router. **Enable –** While accessing into the web user interface of Vigor router, a validation code will appear to authenticate the user trying to log into web user interface. ● **Fail Times to Trigger -** It is available when **Use Validation Code** is enabled. The number selected here means the times for login failure that will trigger Validation Code for authentication. The default setting is "0". That means no failure of login is allowed.
Customized Login Image	Specify an image file which will be displayed on the login page when a user or guest tries to access into Internet. **Upload Login Image** – Choose a file to upload to Vigor3900. It is useful for advertisement.
Enforce HTTPS Management	Click **Enable** to force the user accessing into web user interface of Vigor router by HTTPS.
Internet Access Control	
Apply to WAN Interface	Choose the WAN interface(s) to apply such feature.

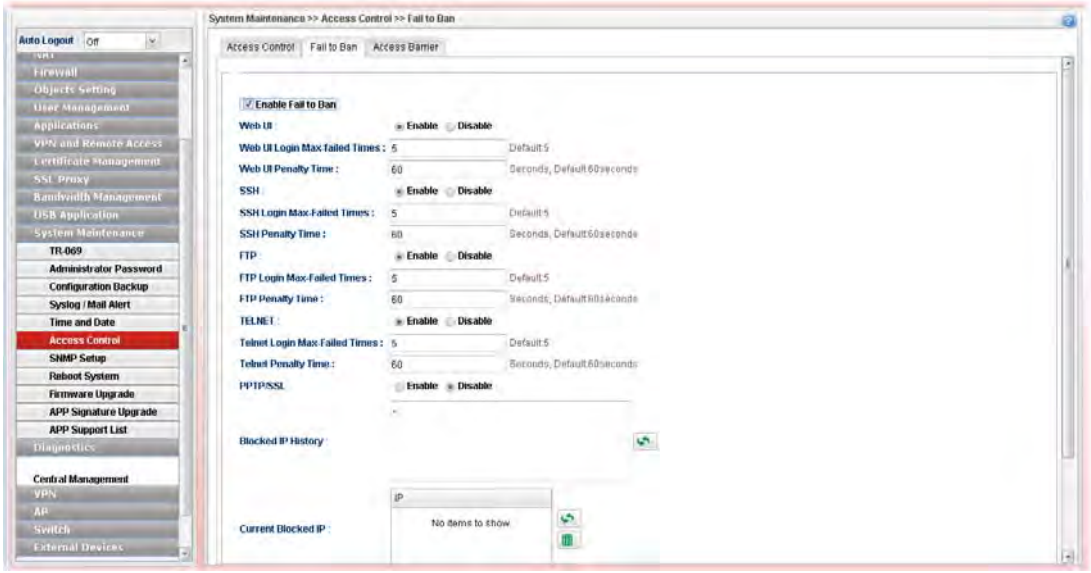
Web Allow	Click **Enable** to allow system administrator to login from the Internet and management the web page of the router.
Telnet Allow	Click **Enable** to allow system administrator to login from the telnet and management the web page of the router.
SSH Allow	Click **Enable** to allow system administrator to login from the SSH server and management the web page of the router.
HTTPS Allow	Click **Enable** to allow system administrator to login from the HTTPS server and management the web page of the router.
SSL Proxy Allow	Click **Enable** to allow SSL Proxy user to login SSL Proxy Service.
FTP Allow	Click **Enable** to allow system administrator to login from the FTP server and management the web page of the router.
SAMBA Allow	Click **Enable** to allow the users (with SAMBA function enabled) login into the SAMBA server through Vigor router.
TR069 Allow	Click **Enable** to allow Vigor router to be managed by VigorACS via WAN connection.
Server Certificate	Use the default setting.
Access List	Click **Enable** to allow system administrator to login from the user defined IP address and management the web page of the router. If you enable such function, the system can be managed by these three IP addresses via WAN.
IP List	Type the first IP address for the system administrator to login. The former boxes indicate the IP address allowed to login to the router, and the later box indicates a subnet mask allowed to login to the router.
Apply to LAN	Choose the LAN profile(s) that the IPs controlled under such profile are allowed to access into the web user interface of Vigor3900.
Allow Ping from WAN	Click **Enable** to allow system administrator to ping the router from WAN interface. **WAN Profile** – Specify the WAN interface to perform the "Ping" job.
LAN Access Control	
Allow management from LAN	Click **Enable** to control such router from LAN.
Apply to LAN Subnet	Choose the LAN profile(s) that the IPs controlled under such profile are allowed to access into the web user interface of Vigor3900.
Web Allow	Click **Enable** to allow system administrator to login from the Internet and management the web page of the router.
Telnet Allow	Click **Enable** to allow system administrator to login from the telnet and management the web page of the router.

SSH Allow	Click **Enable** to allow system administrator to login from the SSH server and management the web page of the router.
HTTPS Allow	Click **Enable** to allow system administrator to login from the HTTPS server and management the web page of the router.
FTP Allow	Click **Enable** to allow system administrator to login from the FTP server and management the web page of the router.
SAMBA Allow	Click **Enable** to allow system administrator to login from the SAMBA server and management the web page of the router.
TR069 Allow	Click **Enable** to allow Vigor router to be managed by VigorACS via WAN connection.
Allow Ping form the LAN	Click **Enable** to allow system administrator to ping the router from LAN interface.
Https Security	
Server Certificate	To ensure the network security via HTTPs, you can select a certificate for authenticating HTTPS server from the drop down list (which displays all the available certificates). If you want to add other certificate, go to **Certificate Management>>Local Certificate** to create more certificates.
Allow TLS 1.0/1.1	**Enable TLS 1.0/1.1 –** Check the box to enable the function of TLS 1.0/1.1 if required. Due to security consideration, the built-in HTTPS server of the router had upgraded to TLS1.x protocol.
Management Port Setup	
Web Port	Type the port number for the management through web page.
Telnet Port	Type the port number for the management through telnet page.
SSH Port	Type the port number for the management through SSH server.
HTTPS Port	Type the port number for the management through HTTPS server.
SSL VPN Port	Type the port number for the management through SSL VPN server.
FTP Port	Type the port number for the management through FTP server.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

4.14.6.2 Fail to Ban

When someone tries/fails to login the router many times, Vigor router system will block the network connection for a while to protect system. At present, five protocols (Web User Interface, SSH, FTP, Telnet, PPTP/SSL) are available for configuration to avoid malicious attacks.

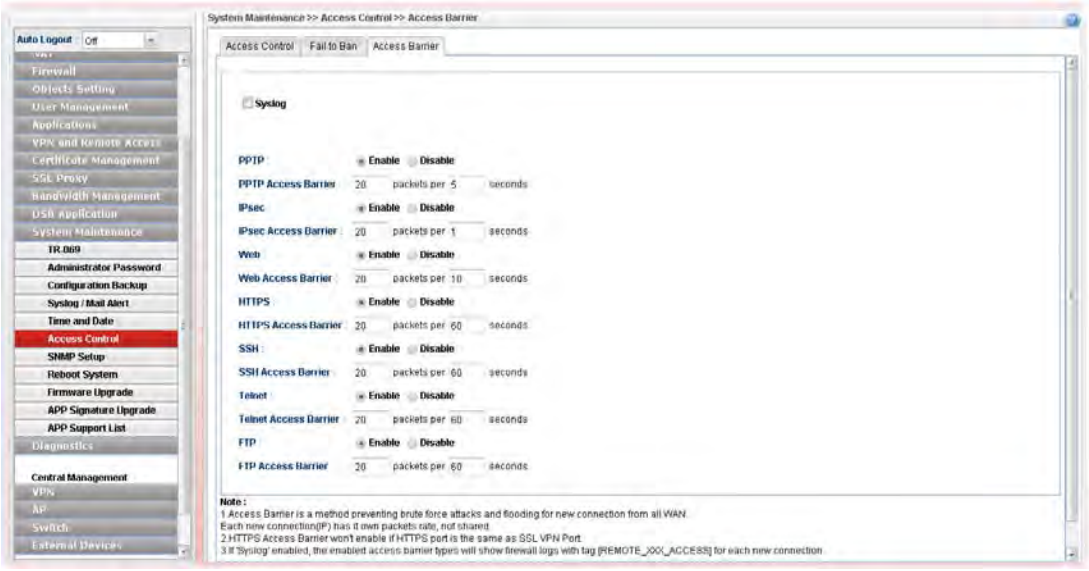


Available parameters are listed as follows:

Item	Description
Enable Fail to Ban	Enable the function to protect Vigor system while being attacked by malicious accounts and passwords.
Web UI/SSH/FTP/ TELNET/PPTP/SSL	**Enable –** Enable the function of Fail to Ban via different protocols (Web UI/SSH/FTP/TELNET/PPTP/SSL)**.** ● **Login Max-failed Times –** The number typed here means the maximum logging times allowed for a group of user account and password trying to login Vigor router. ● **Penalty Time –** This field is used to configure the blocking time. The default setting is 60 seconds. It means, when a user tries to login Vigor router with a user account for many times (defined in Login Max-failed Times) but fails, he/she will be prohibited to login for a period of time. When the penalty time limit is up, he/she is allowed to login into Vigor router again. **Disable -** Disable the function of Fail to Ban for Web UI/SSH/FTP/TELNET/PPTP/SSL.
Blocked IP History	Display the history of the IP address blocked.
Current Blocked IP	Display the IP address(es) blocked currently.
Reset Blocked Records	Click this button to reset the record for IP blocked.
Apply	Click this button to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.14.6.3 Access Barrier

This page is used to configure the access barrier to protect the system from brute-force attack and flooding attack, and ensure following protocols can run properly.



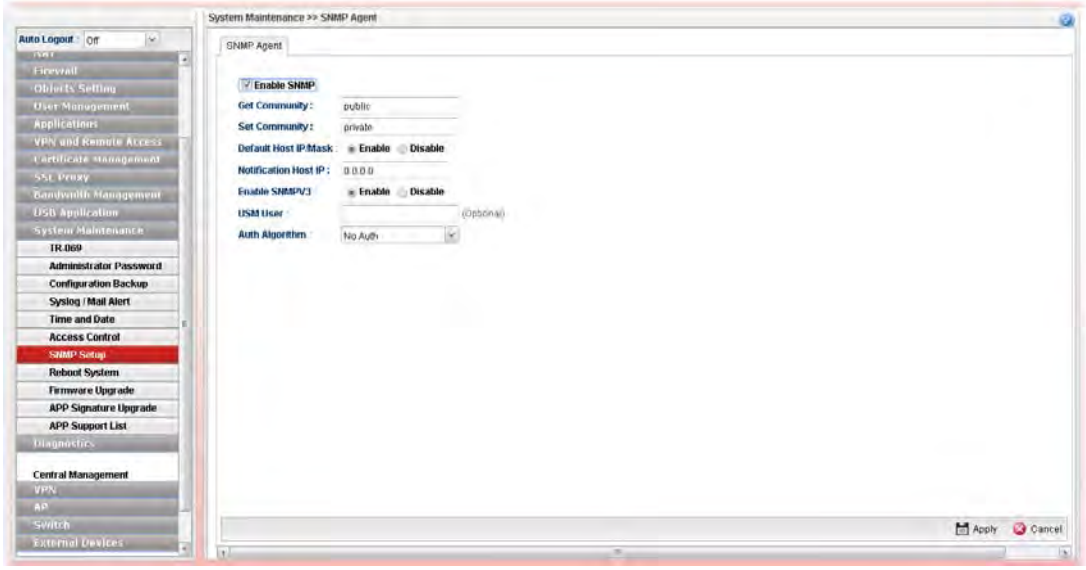
Available parameters are listed as follows:

Item	Description
Syslog	Check the box to make information related to access control recorded on Syslog.
PPTP/IPsec/Web/HTTPS SSH/Telnet/FTP Access Barrier	The port number used by these protocols always became the target attacked by hacker. Therefore, the settings for packet reception rate for certain protocol can be configured to avoid attack from unknown people.
Apply	Click this button to save the configuration.
Cancel	Click it to discard the settings configured in this page.

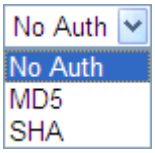
4.14.7 SNMP Setup

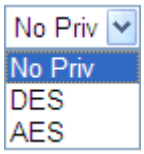
This page allows you to manage the settings for SNMP setup.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.



Available parameters are listed as follows:

Item	Description
Enable SNMP	Check the box to enable the function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**
Set Community	Set community by typing a proper name. The default setting is **private.**
Default Host IP/Mask	Click **Enable** to use the default IP and mask of the host as the SNMP agent. If you click **Disable,** you need to type the IP address and choose the mask manually in related fields.
Notification Host IP	Type the IP address of the host for notification.
Enable SNMPV3	Click **Enable** to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm (Min. Length:8)	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password (Min. Length:8)	Type a password for authentication. The maximum length of the text is limited to 23 characters.

Privacy Algorithm (Min. Length:8)	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password (Min. Length:8)	Type a password for privacy. The maximum length of the text is limited to 23 characters.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

Enter all of the settings and click **Apply**.

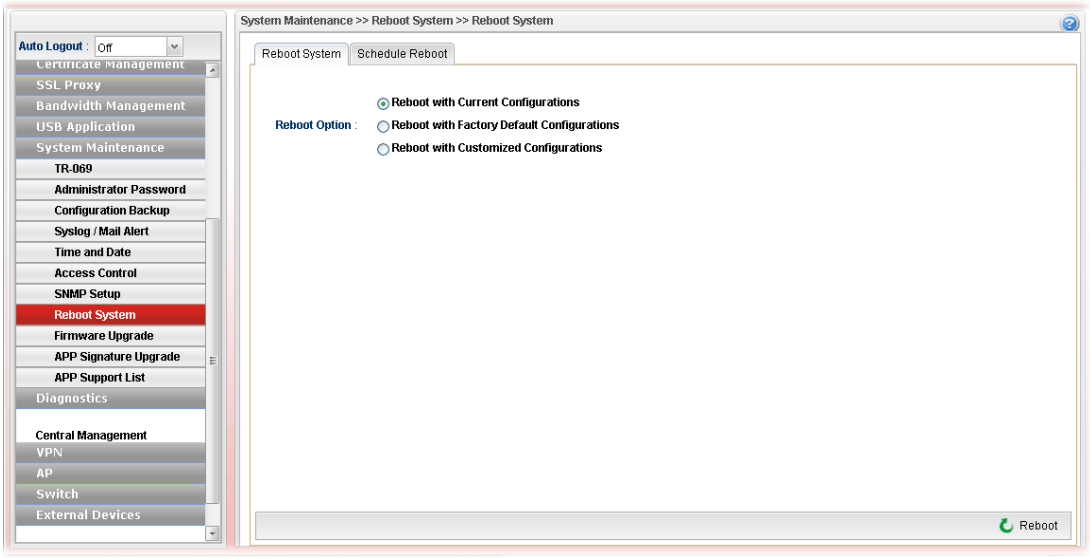
4.14.8 Reboot System

The Vigor router system can be restarted from a Web browser. You have to reboot the router to invoke the configured settings that you made before.

If you want to reboot the router using the current configuration, choose **Reboot with Current Configurations** and click **Reboot**. To reset the router settings to default values, click **Reboot with Factory Default Configurations** and click **Reboot**. The router will take a period of time to reboot the system.

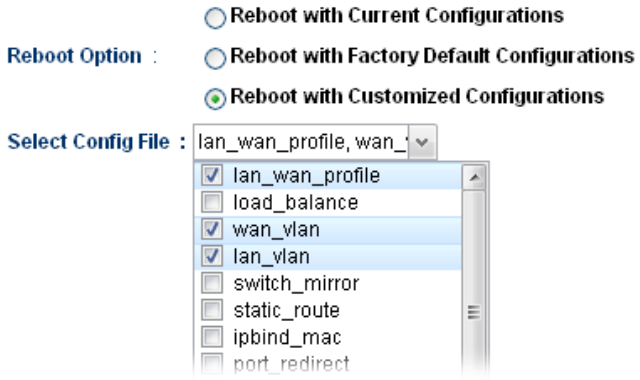
4.14.8.1 Reboot System

Open **System Maintenance>> Reboot System**.



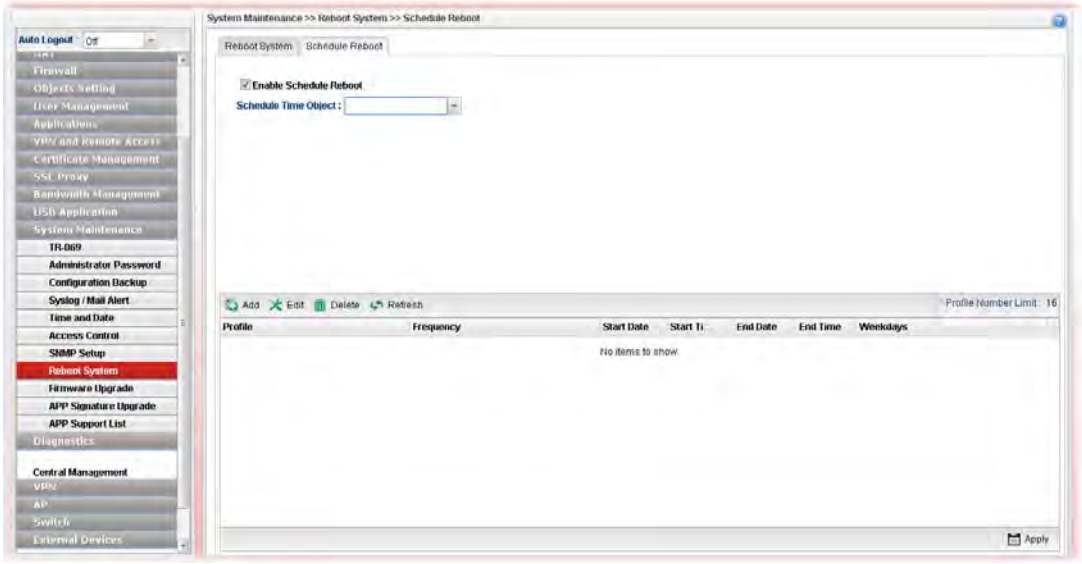
Available parameters are listed as follows:

Item	Description
Reboot with Current Configurations	Click it to reboot the router using the current configuration. Then, click **Reboot**.
Reboot with Factory Default Configurations	Click it to reset the router settings to default values. Then, click **Reboot**.

	Clear All Certificate Files – In general, the factory default configurations for Vigor router do not include certificate files. Therefore, even if the router reboots with default settings, all of the certificate files will be kept unless such option is enabled.
Reboot with Customized Configurations	Click it to reboot the router using the current configuration (only the configuration settings listed and selected below). If you choose this option, **Select Config File** will be available for you to select.  After choosing the configuration files, click **Reboot**.
Reboot	Click this button to execute the rebooting job.

4.14.8.2 Schedule Reboot

Vigor router can be rebooted based on schedule setting. Check the box of **Enable Schedule Reboot** and choose a time object from the drop down list of **Schedule Time Object.** After clicking **Apply**, Vigor router will reboot at the specified time.



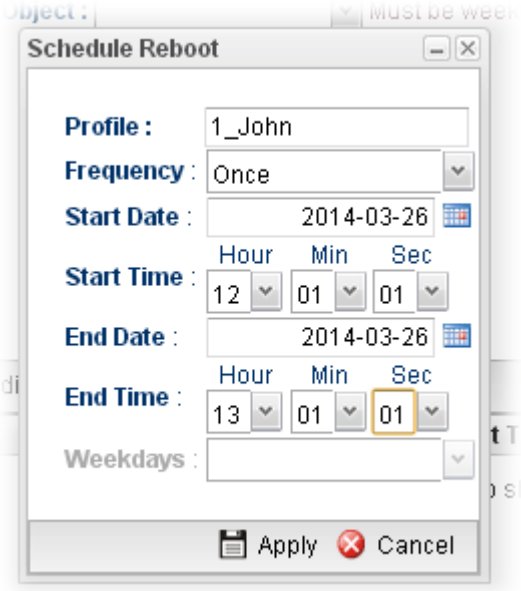
Available parameters are listed as follows:

Item	Description
Enable Schedule Reboot	Check the box to enable such option.

Schedule Time Object	Use the drop down list to choose one of the time objects to perform the schedule reboot.
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the schedule profile.
Frequency	Display the type (Once or Weekdays) of frequency selected for the profile.
Start Date	Display the starting date of the profile.
Start Time	Display the starting time of the profile.
End Date	Display the ending date of the profile.
End Time	Display the ending time of the profile.
Weekdays	Display which day in a week shall perform the reboot job.

How to add a schedule profile

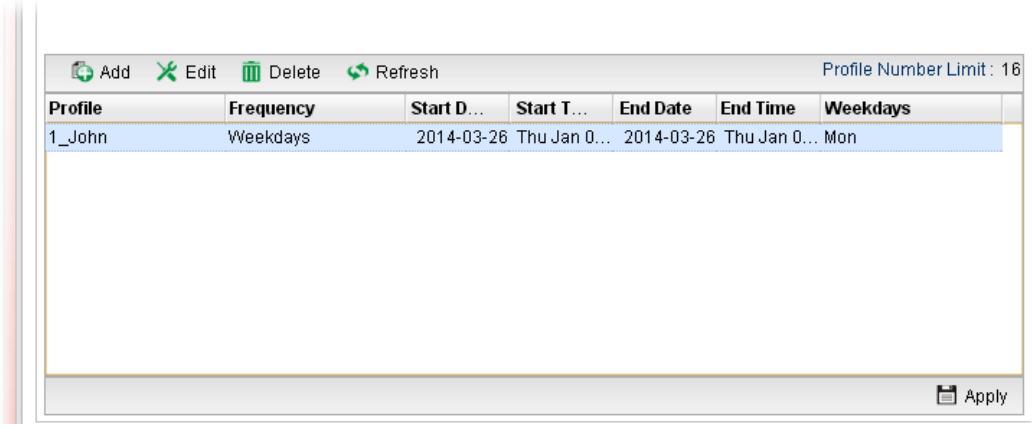
1. Open **System Maintenance>>Schedule Reboot.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Frequency	Specify how often the schedule will be applied. **Once** -The schedule will be applied just once **Weekdays** -Specify which days in one week should perform the schedule.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
End Date	Specify the ending date of the schedule.
End Time	Specify the ending time of the schedule.

4. Enter all the settings and click **Apply**.
5. A schedule profile has been created.



4.14.9 Firmware Upgrade

The following web page will guide you to upgrade firmware by using such page.

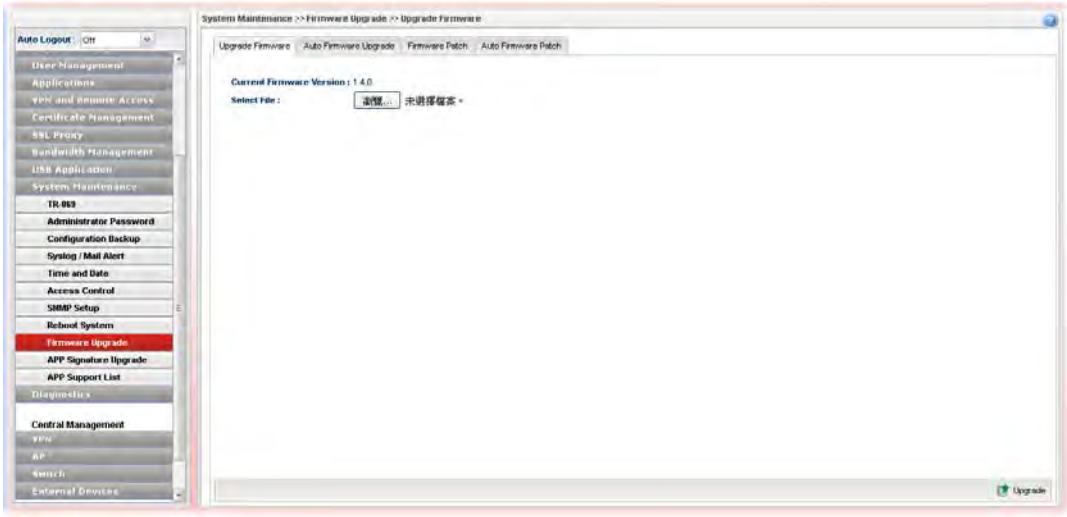
Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and the FTP site is ftp.DrayTek.com.

Click **System Maintenance>> Firmware Upgrade**.

4.14.9.1 Upgrade Firmware

This page display current firmware version used in Vigor router. In addition, it allows you to select the newest firmware version manually and update to such Vigor router immediately.

A user must connect to website (http://www.draytek.com.tw/ftp) previously to download the newest firmware to the computer.

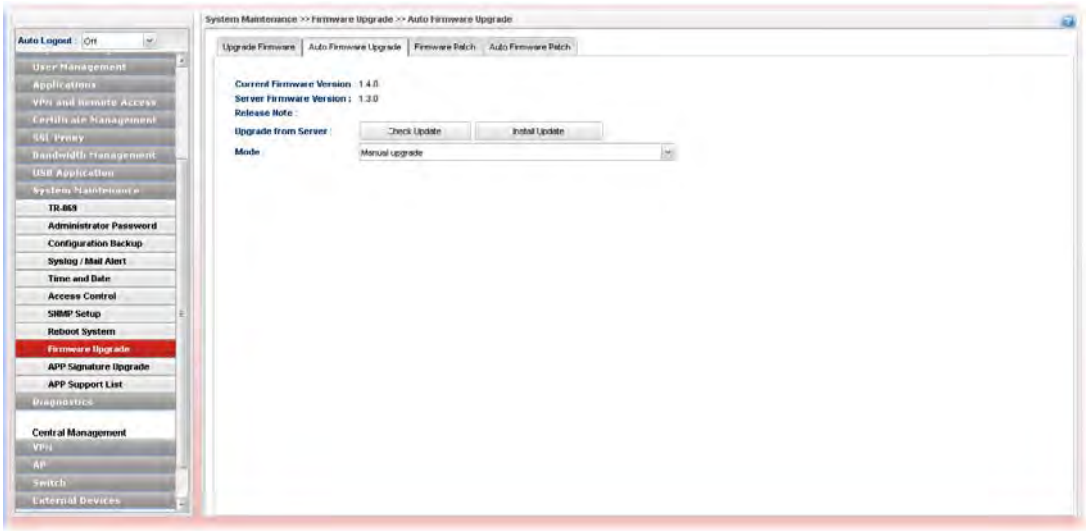


Available parameters are listed as follows:

Item	Description
Current Firmware Version	Display current version of the firmware.
Select File	Use the **Select** button to locate and select the new firmware.
Upgrade	Click it to perform the firmware upgrade.

4.14.9.2 Auto Firmware Upgrade

By clicking **Check Update/Install Update**, Vigor router can download/upgrade firmware directly from website (http://www.draytek.com.tw/ftp) automatically.



Available parameters are listed as follows:

Item	Description
Current Firmware Version	Display current firmware version of Vigor router.
Server Firmware Version	Display the firmware version shown on website (http://www.draytek.com.tw/ftp).

Upgrade from Server	**Check Update** –Vigor router will inquire to website (http://www.draytek.com.tw/ftp) if there is any newest firmware available for use. If yes, Vigor router will download the newest firmware from the website to the host (Vigor router) automatically. **Install Update** –If the firmware version stored on the website (http://www.draytek.com.tw/ftp) is newer than the version used by the host (Vigor router), then Vigor router will download and install the newest firmware version automatically.
Mode	**Manual Upgrade –** If it is selected, check and installation for firmware will be executed only when **Check Update/Install Update** is pressed. **Notify me when new firmware is available** – If it is enabled, after detecting the newest firmware from the website, Vigor router's system will automatically download (but not install) the firmware and store on the host. Later, when the user logs into the router's web user interface, the system will give a hint to notify the user in the logging window. **Auto upgrade when new firmware is available** – If it is enabled, Vigor router's system will automatically download and upgrade the firmware when detecting newest firmware from the website.

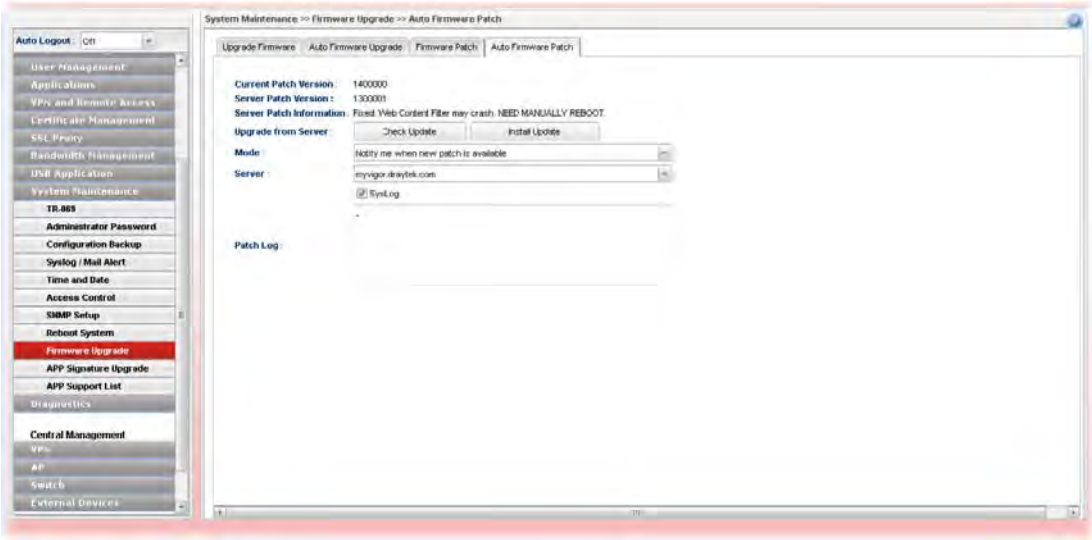
4.14.9.3 Firmware Patch

Vigor router administrator/user can manually select file (.pat) to fix/modify the mistakes, bugs or error occurred on current firmware. Usually, such firmware with instant modifications can be obtained from DrayTek MyVigor Patch Server.

4.14.9.4 Auto Firmware Patch

A firmware contains hundreds of files, and a firmware patch could be a single file or several files of a firmware. Since firmware 1.2.0, Vigor3900 supports Firmware Patch feature which allows upgrading a specific firmware patch only, but not the whole firmware. The benefit is Vigor3900 doesn't need to reboot the system after updating the firmware patch.

Auto Firmware Patch is similar to Auto Firmware Upgrade. While configuring Mode as "Notify me when a new patch is available", Vigor3900 will check if there is a new patch available on DrayTek server daily. When a new patch is available, Vigor3900 will pop-up notification window when Administrator logs in.



Available parameters are listed as follows:

Item	Description
Current Patch Version	Display the installed patch version on local system
Server Patch Version	Display the latest patch version on DrayTek MyVigor server.
Server Patch Information	Display detailed patch information.
Upgrade from Server	**Check Update** – Click the button to let the system check and get server patch version. **Install Update** – Click it to install the server patch version onto Vigor router.
Mode	There are three modes available for you to choose. **Manual upgrad**e – If it is selected, check and installation for patch will be executed only when **Check Update/Install Update** is pressed. **Notify me when new patch is available** - If it is specified, after detecting the newest patch from MyVigor server, Vigor router's system will automatically download the patch information and store on the host. Later, when the user logs into the router's web user interface, the system will give a hint to notify the user in the logging window. **Auto upgrade when new patch is available** - If the patch information stored on MyVigor server is newer than information stored in the host (Vigor router), then Vigor

	router will download and upgrade the newest information automatically.
Server	Use the drop down list to specify a suitable server.
Syslog	Check the box to store the patch log into Syslog.
Patch Log	This area will show log related to firmware patch automatically if firmware patch is executed.

When the router is doing daily firmware patch check, Syslog will have the logs below:

<13>Dec 18 13:59:18 Vigor: [patupgrade_auto][1] Check latest patch version from server ...

<13>Dec 18 13:59:18 Vigor: [patupgrade_auto][0] Try get version from http://myvigor.draytek.com/sig/APPE/dlm/c1k/latver.txt

<13>Dec 18 13:59:19 Vigor: [patupgrade_auto][0] Get version: 1200000 (latest=1200000)

<13>Dec 18 13:59:19 Vigor: [patupgrade_auto][1] Success: Your firmware is up-to-date and need not to patch.

4.14.10 APP Signature Upgrade

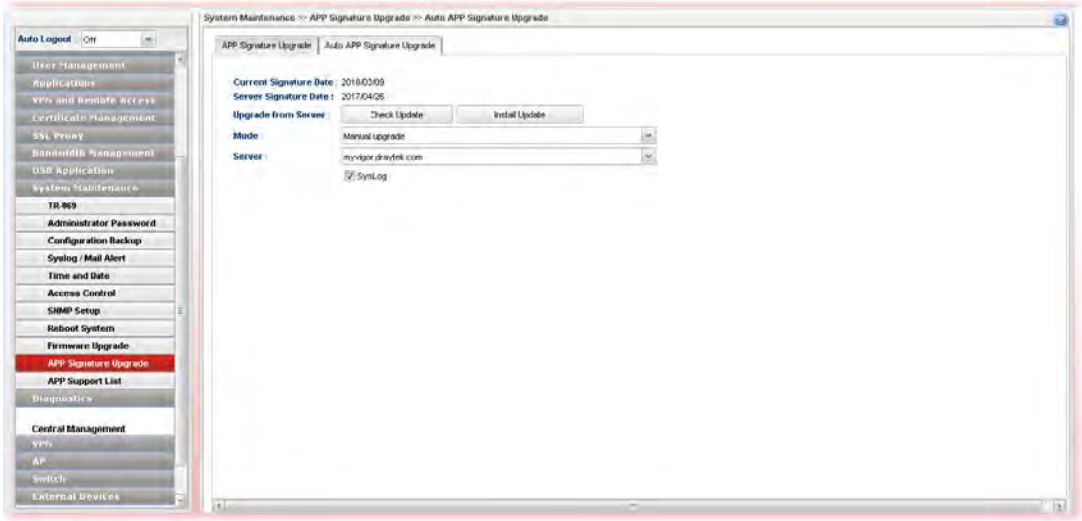
The APP object profile adopted by Vigor router will be treated as the APP signature. DrayTek will periodically upgrade versions for all of the APPs supported by Vigor router. However, it might be inconvenient for users to upgrade the APP version one by one. This feature is specially designed to offer a quick method to execute APP version upgrade. Users can perform the APP signature upgrade manually or configure the settings on this page to make Vigor router performing the APP signature automatically.

4.14.10.1 APP Signature Upgrade

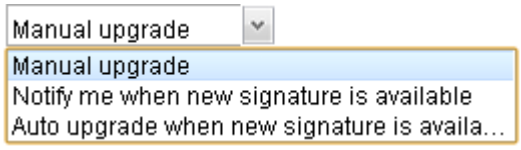
Before upgrading APP signature to Vigor3900, open this page and specify a signature file by clicking **Select**. Later, click **Upgrade** to execute signature upgrade.

4.14.10.2 Auto APP Signature Upgrade

This page allows Vigor router to execute signature upgrade automatically.



Available parameters are listed as follows:

Item	Description
Current Signature Date	Display the date of current signature installed on Vigor3900.
Server Signature Date	Display the newest signature version recorded on server (myvigor.draytek.com or myvigoreu.draytek.com).
Upgrade from Server	Get the newest signature from MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com). **Check Update** –Vigor router will inquire to MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com) if there is any newest signature available for use. If yes, Vigor router will download the newest signature from the website to the host (Vigor router) automatically. **Install Update** –If the signature information stored on MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com) is newer than the version used by the host (Vigor router), then the system will install the newest signature version information automatically.
Mode	Choose the condition to execute APP signature upgrade or send a notification.  **Manual upgrade** – If it is selected, check and installation for signature will be executed only when **Check Update/Install Update** is pressed. **Notify me when new signature is available** - If it is specified, after detecting the newest signature from MyVigor server, Vigor router's system will automatically download the signature information and store on the host. Later, when the user logs into the router's web user interface, the system

	will give a hint to notify the user in the logging window. **Auto upgrade when new signature is available -** If the signature information stored on MyVigor server is newer than information stored in the host (Vigor router), then Vigor router will download and upgrade the newest information automatically.
Server	Choose a proper server for signature upgrade from the drop down list. At present, only two servers (myvigor.draytek.com or myvigoreu.draytek.com) are supported.
Syslog	Check the box to record related information on Syslog.

4.14.11 APP Support List

APP Support List displays all of the applications with versions supported by Vigor router. They are separated with types of IM, P2P, Protocol and Others. Each tab will bring out different items with supported versions.

4.15 Diagnostics

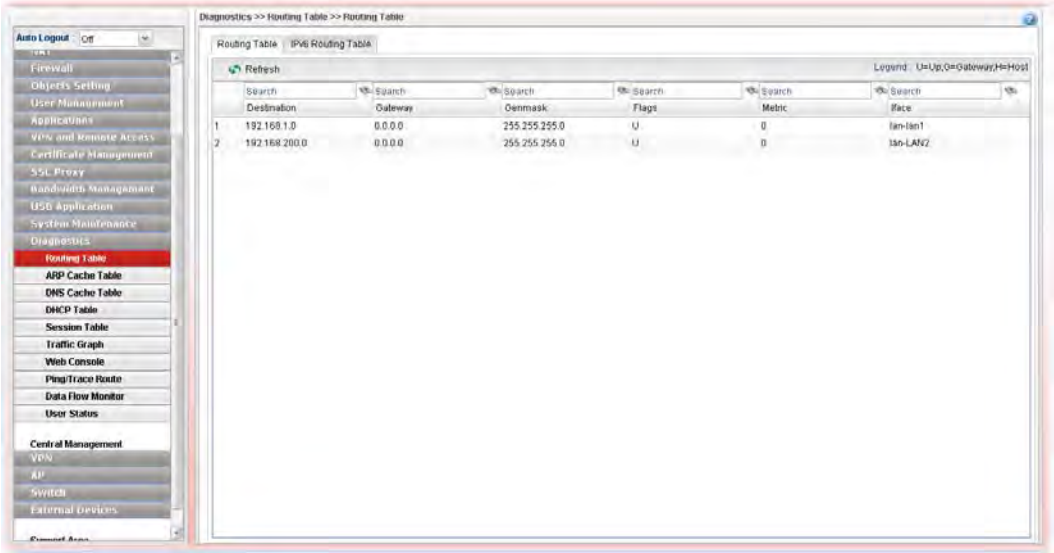
In some cases, a user may need to know some information about the router, such as static or dynamic databases, or other routing information. The Vigor3900 supports five functions, **Routing Table**, **ARP Cache Table**, **DHCP Assignment Table**, **Sessions Table**, **Traffic Graph…..** for the user to review related information.

4.15.1 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

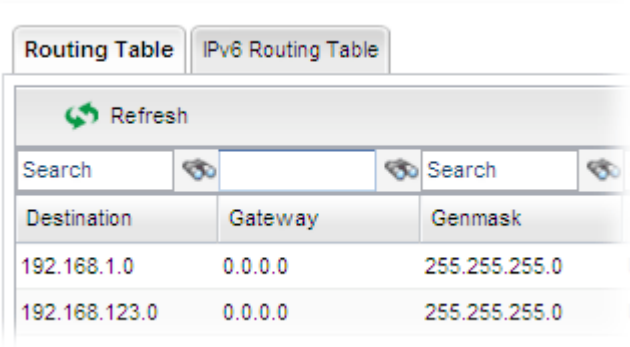
4.15.1.1 Routing Table

Display the information for each route.



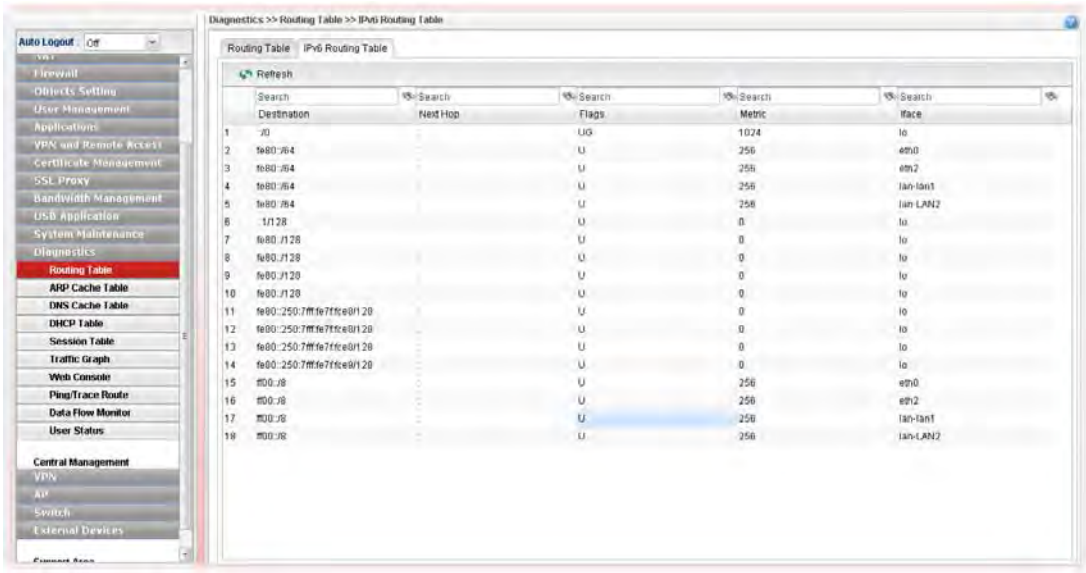
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The

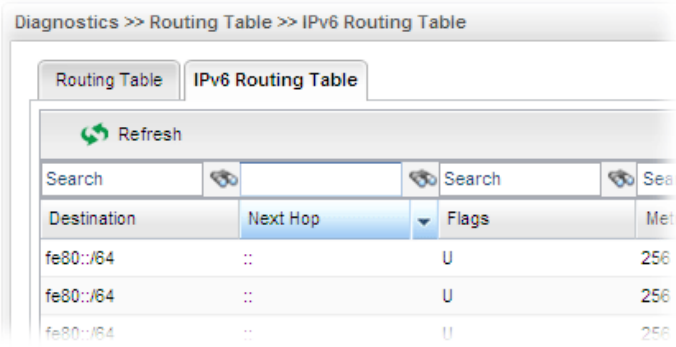
	system will display the records relating to the keyword. 
Destination	Display the destination IP address for various routings.
Gateway	Display the default gateway.
Genmask	Display the subnet mask for various routings.
Flags	Display the flag of the routing entry. Possible flags include: U (route is up) H (target is a host) G (use gateway) R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by *addrconf*) C (cache entry) ! (reject route)
Metric	Display the distance to the target (usually counted in hops). It may be needed by routing daemons.
Iface	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).

4.15.1.2 IPv6 Routing Table

Display the information for each route with IPv6 protocol.



Each item will be explained as follows:

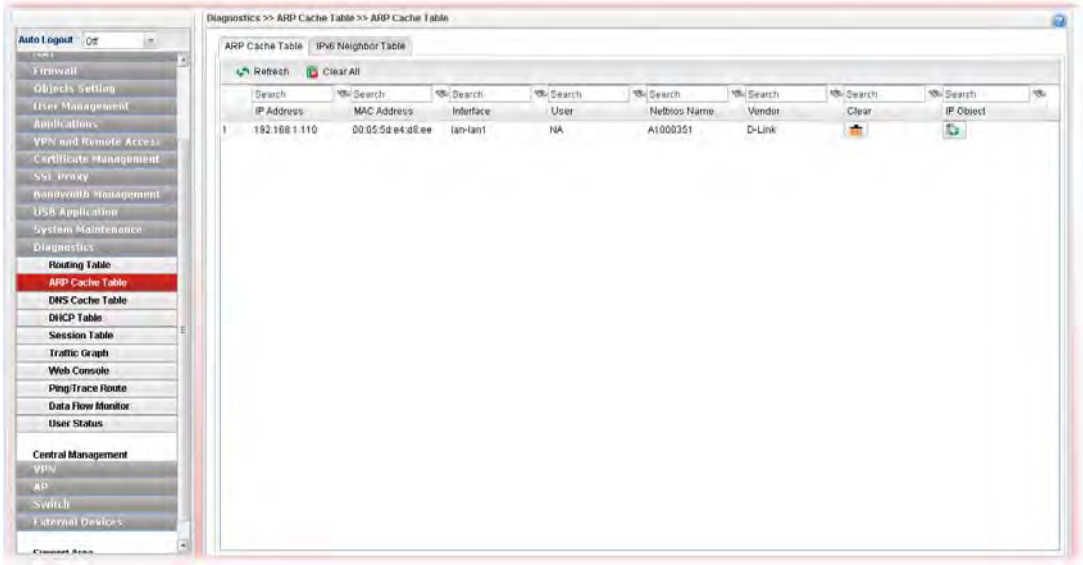
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
Destination	Display the destination IP address for various routings.
Next Hop	Display the next hop address for such route。
Flags	Display the flag of the routing entry. Possible flags include: U (route is up) H (target is a host) G (use gateway) R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by *addrconf*) C (cache entry) ! (reject route)

Metric	Display the distance to the target (usually counted in hops). It may be needed by routing daemons.
Iface	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).

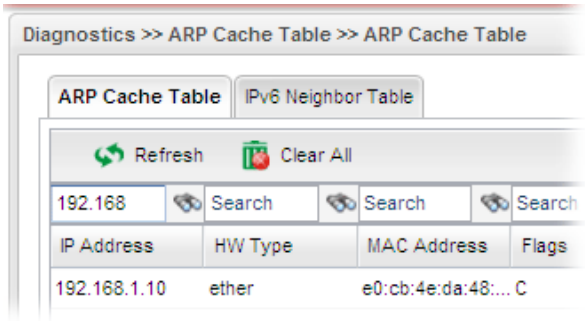
4.15.2 ARP Cache Table

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.

4.15.2.1 ARP Cache Table

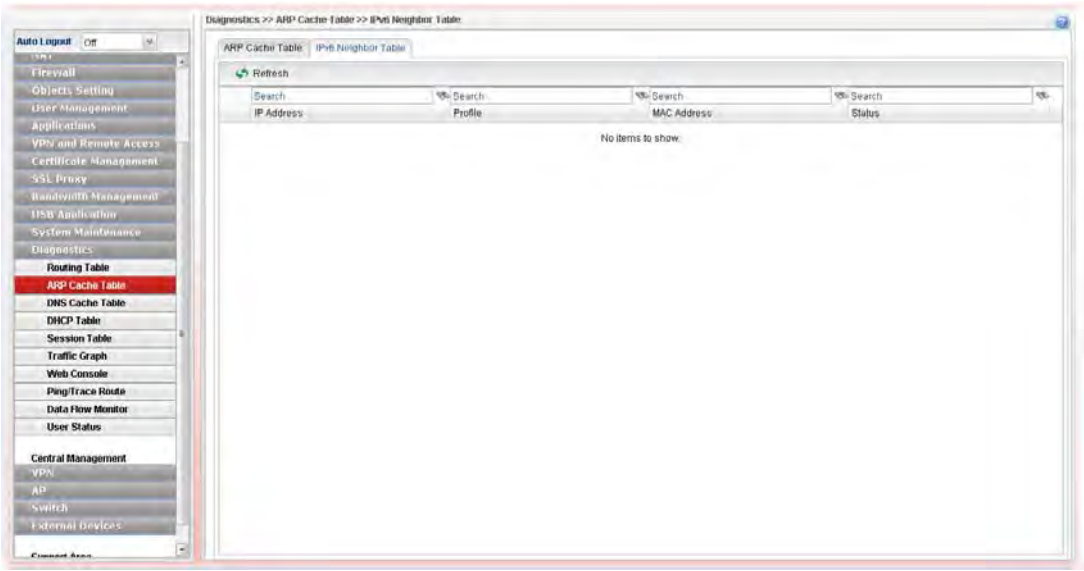


Each item will be explained as follows:

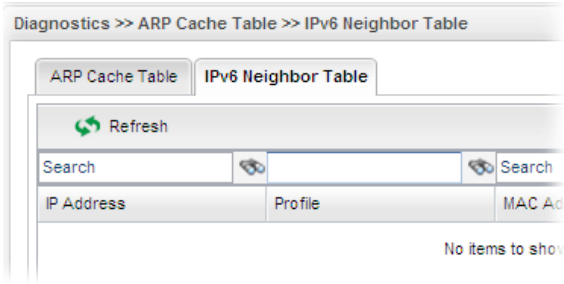
Item	Description
Refresh	Renew the web page.
Clear All	Remove all of the information from this page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
IP Address	Display the IP address for different ARP cache.

Item	Description
MAC Address	Display the MAC address for different ARP cache.
User	Display the user name of the client.
Vendor	Display the vendor of the device.
Clear	Delete the selected profile.
IP Object	Click the **Add** button to add a new IP object for such

4.15.2.2 IPv6 Neighbor Table



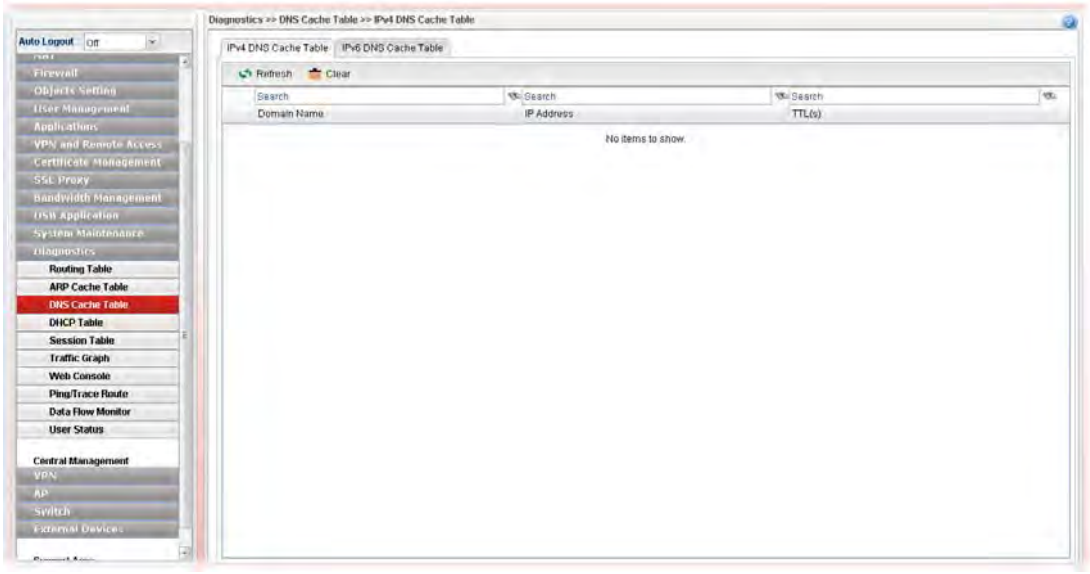
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
IP Address	Display the IPv6 address of the neighbor.
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.
Status	Display the status for such neighbor. **INCOMPLETE** - Address resolution is in progress and the link-layer address of the neighbor has not yet been

Item	Description
	determined. **REACHABLE** - The neighbor is reachable recently (within tens of seconds ago). **STALE**-The neighbor is no longer to be reachable. Yet, until traffic is sent to the neighbor, no attempt should be made to verify its reachability. **DELAY** - The neighbor is no longer to be reachable, and the traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, delay sending probes for a short while in order to give upper layer protocols a chance to provide reachability confirmation. **PROBE** - The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

4.15.3 DNS Cache Table

The record of domain name and the mapping IPv4 or IPv6 address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily.

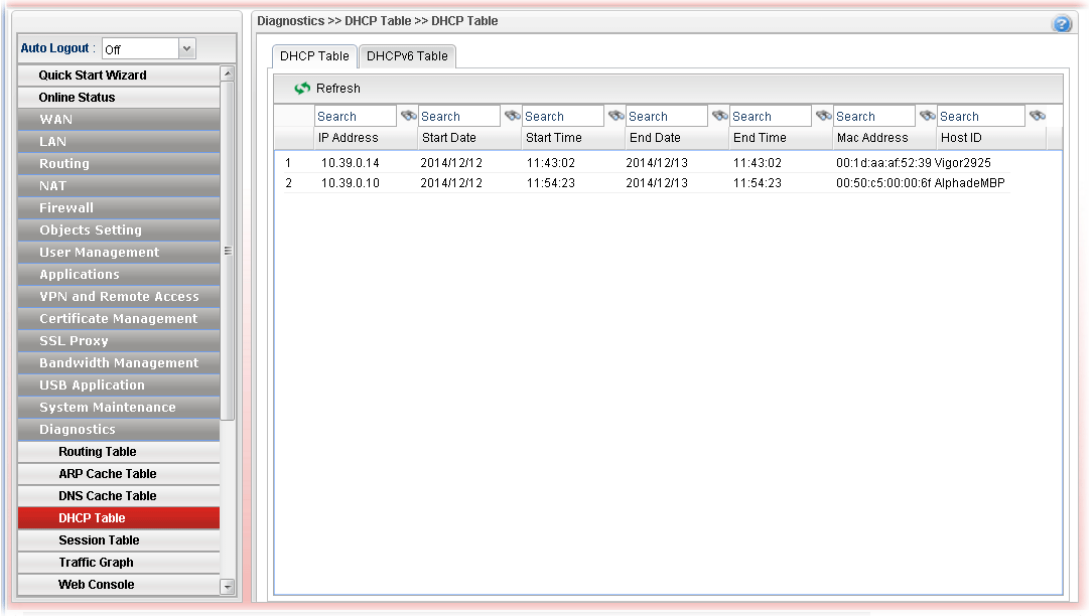


4.15.4 DHCP Table

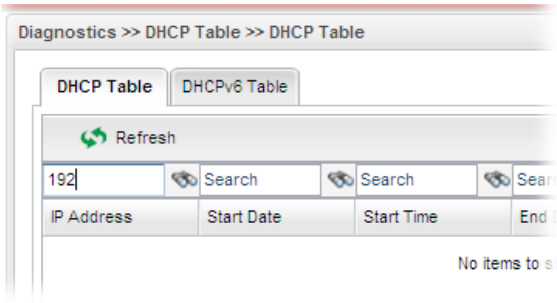
The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

4.15.4.1 DHCP Table

Click **Diagnostics** and click **DHCP Table** to open the web page.



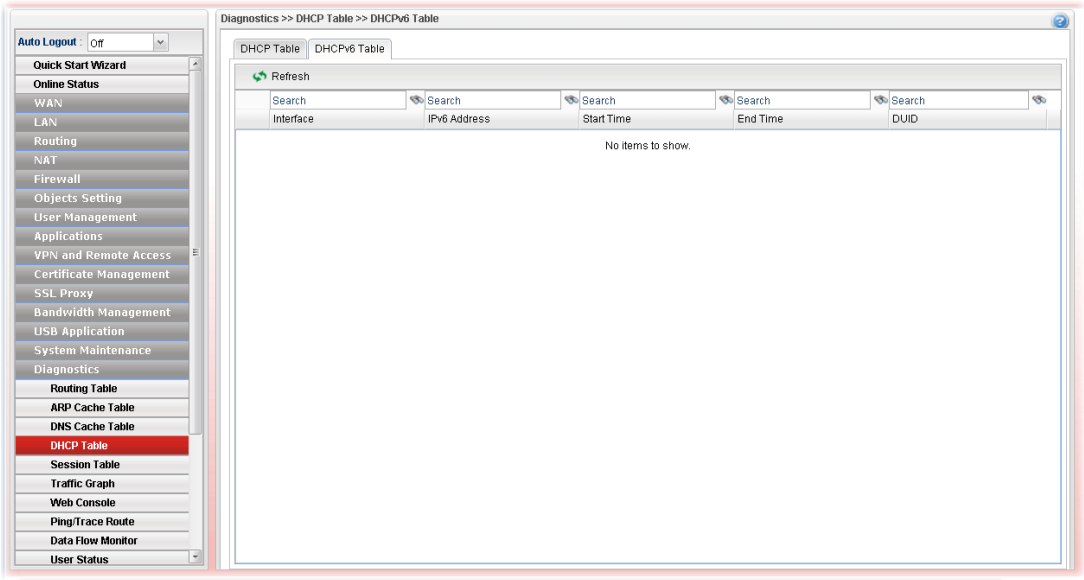
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
IP Address	Display the IP address of the static DHCP server.
Start Date	Display the starting date that DHCP server is activated.
Start Time	Display the starting time that DHCP server is activated.
End Date	Display the end date that DHCP server is closed.
End Time	Display the end time that DHCP server is closed.

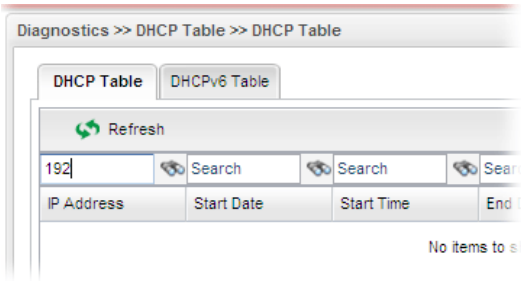
Item	Description
Mac Address	Display the MAC address of the static DHCP server.
Host ID	Display the IP address or name of the host.

4.15.4.2 DHCPv6 Table

Click **DHCPv6 Table** to open the web page.

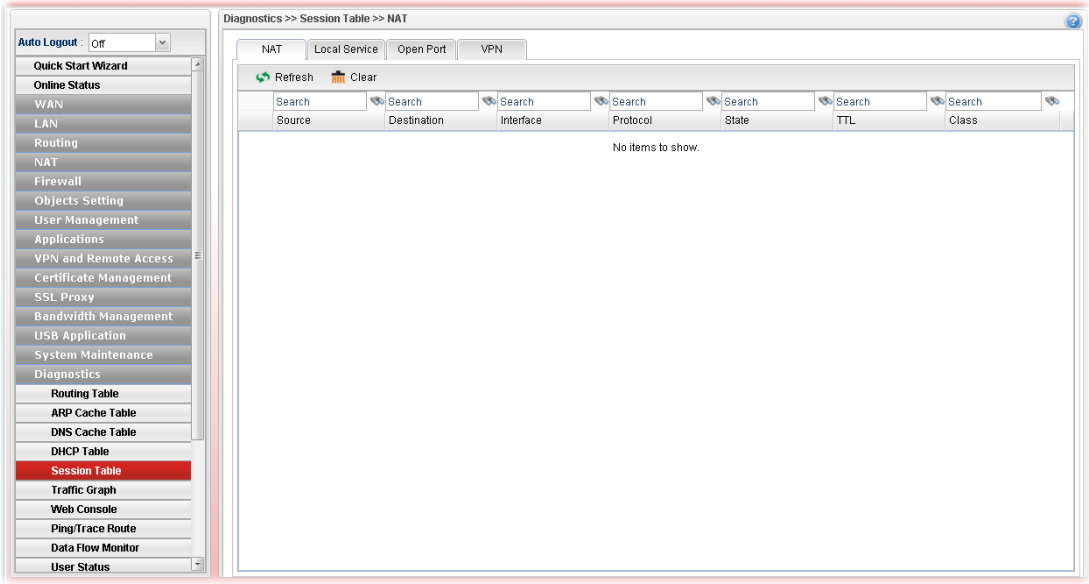


Each item will be explained as follows:

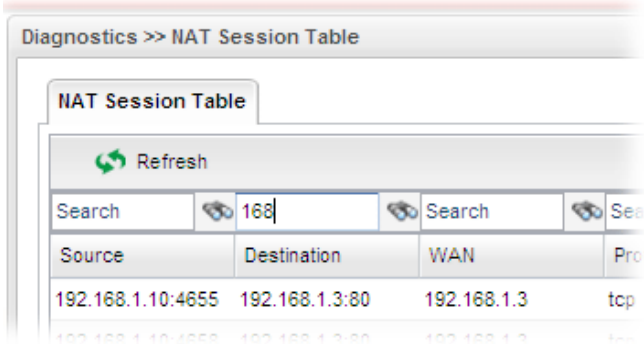
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
Interface	Display the interface used by the DHCP server.
IPv6 Address	Display the IPv6 address of the static DHCP server.
Start Time	Display the starting time that DHCP server is activated.
End Time	Display the end time that DHCP server is closed.
DUID	Display the detailed information for DUID.

4.15.5 Session Table

This table can display about 30000 sessions with 20 pages.

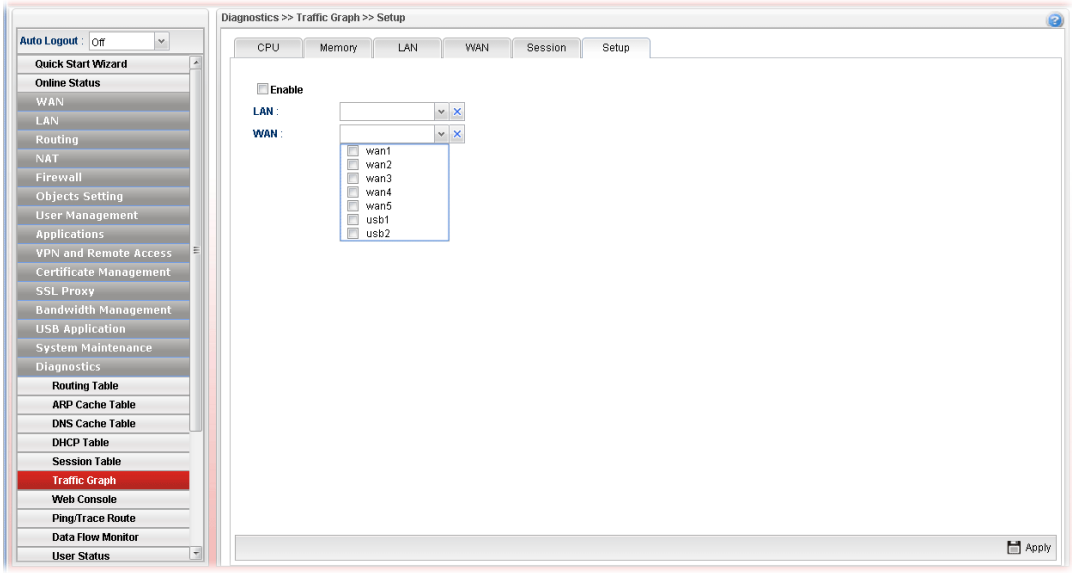


Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
Source	Display the source IP address and port of local PC.
Destination	Display the destination IP address and port of remote host.
Interface	Display the WAN IP address of the router.
Protocol	Display the protocol of such NAT session used.
State	Display the actual state of the TCP connection.
TTL	Display how long the conntrack entry has to live.

4.15.6 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose the **Setup** tab to specify LAN and WAN profiles to display corresponding graphs for CPU, Memory, LAN, WAN configurations and session. Click **Refresh** to renew the graph at any time.

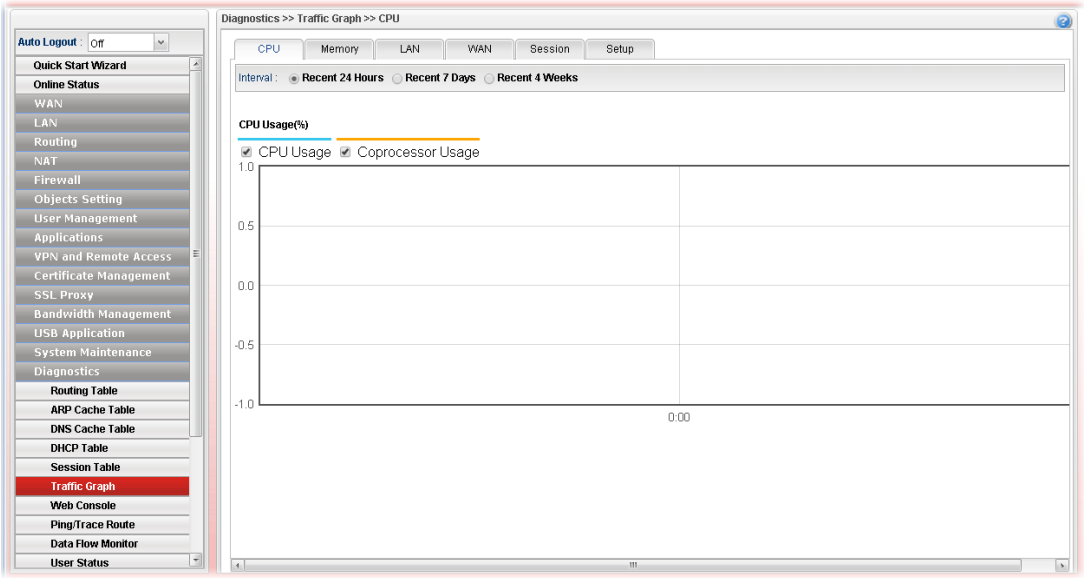


Each item will be explained as follows:

Item	Description
Setup	In this page, simply specify which LAN profile and WAN profile will be applied. The traffic graph will be drawn based on the profiles selected. **Enable** – Check this box to enable such profile. **LAN** – Use the drop down menu to choose a LAN profile. **WAN** –Use the drop down menu to choose a WAN profile. **Apply** - Click it to save the configuration configured under the Setup tab.
CPU	Click the CPU tab. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of CPU operation about recent 24 hours. **Recent 7 Days** – Display the information of CPU operation about recent 7 days. **Recent 4 Weeks** – Display the information of CPU operation about recent 4 weeks.
Memory	Click the Memory tab. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of memory operation about recent 24 hours. **Recent 7 Days** – Display the information of memory operation about recent 7 days. **Recent 4 Weeks** – Display the information of memory

Item	Description
	operation about recent 4 weeks.
LAN	Click the LAN tab. **Network Interface** – Display the information of LAN operation. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of LAN operation about recent 24 hours. **Recent 7 Days** – Display the information of LAN operation about recent 7 days. **Recent 4 Weeks** – Display the information of LAN operation about recent 4 weeks.
WAN	Click the WAN tab. **Network Interface** – Display the information of WAN operation. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of WAN operation about recent 24 hours. **Recent 7 Days** – Display the information of WAN operation about recent 7 days. **Recent 4 Weeks** – Display the information of WAN operation about recent 4 weeks.
Session	Click the Session tab. There are three selections provided for you to specify. **Recent 24 Hours** – Display the session information about recent 24 hours. **Recent 7 Days** –Display the session information about about recent 7 days. **Recent 4 Weeks** – Display the session information about about recent 4 weeks.

Below show a graphic for CPU:

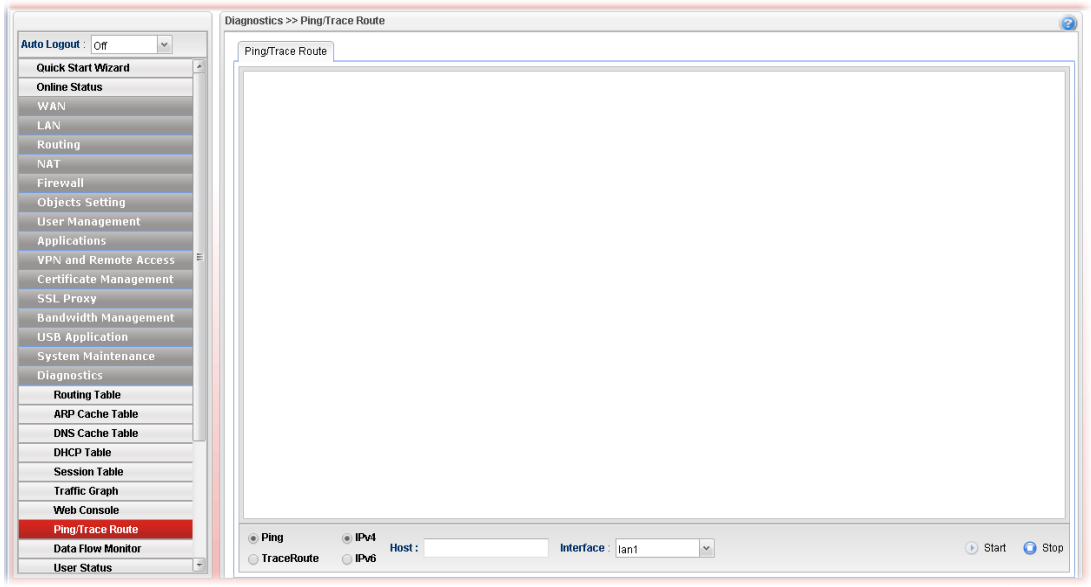


4.15.7 Web Console

Click **Diagnostics** and click **Web Console** to pen the web page for typing commands used in console connection. A remote user can operate Vigor3900 from this web page without installing and opening other connection utility.

4.15.8 Ping/Trace Route

This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Start**. The result of route trace will be shown on the screen.



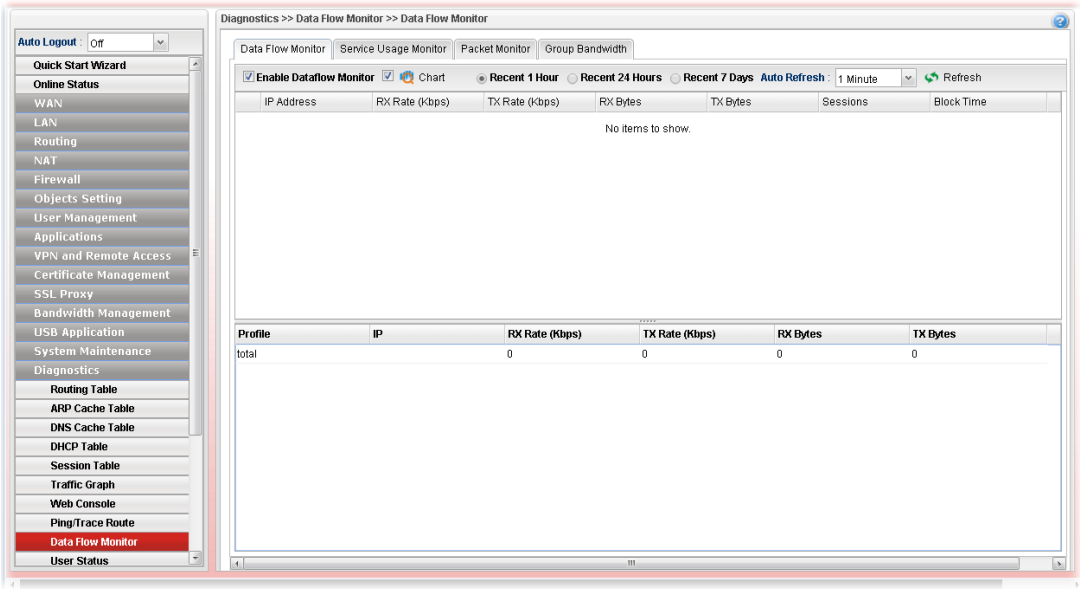
Each item will be explained as follows:

Item	Description
Ping / TraceRoute	Click **Ping** to perform ping function. Click **TraceRoute** to invoke trace router function.
IPv4 / IPv6	Click IPv4 /IPv6 to determine the format of the IP address that you can type.
Host	Type the IP address of the host.
Interface	Choose one of the LAN or WAN profile to be applied by such function.
Start	Click it to start the action of Ping or TraceRoute.
Stop	Click it to terminate the action of Ping or TraceRoute.

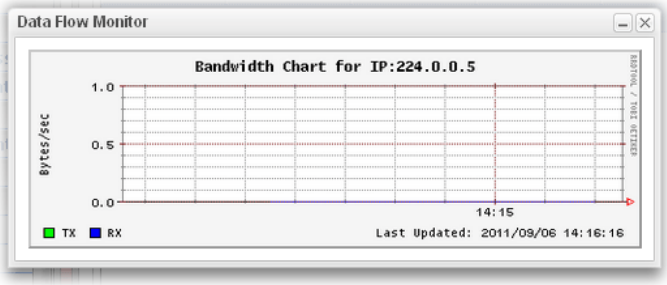
4.15.9 Data Flow Monitor

This page displays the running procedure (such as IP address, session number, transmission rate, receiving rate, and duration of the time block) by list or by chart for the IP address monitored and refreshes the data in an interval of several seconds.

4.15.9.1 Data Flow Monitor



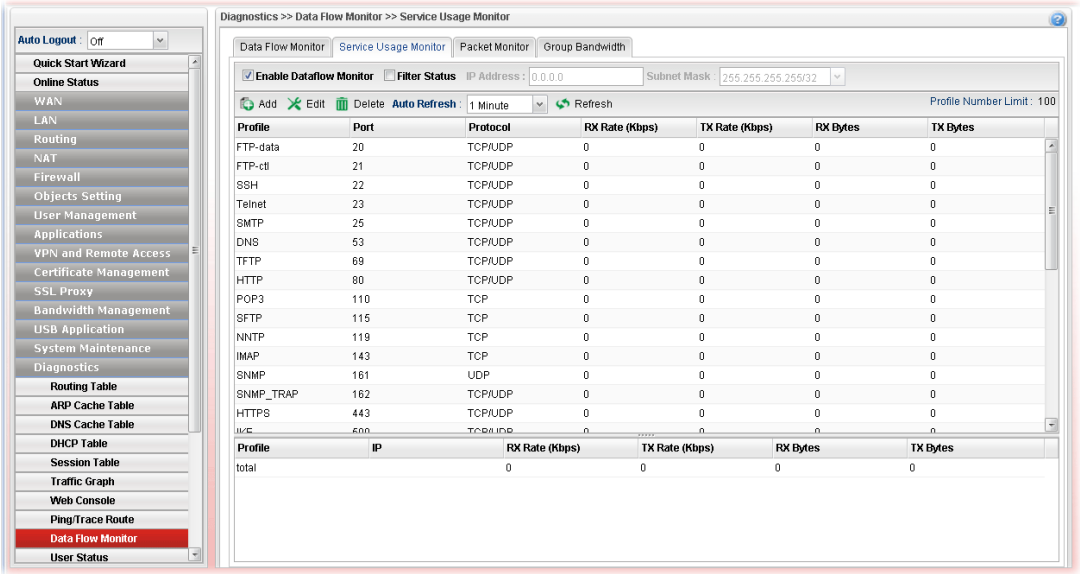
Each item will be explained as follows:

Item	Description
Enable Dataflow Monitor	Check this box to enable dataflow monitor performed by the router.
Refresh	Click it to renew the web page.
Chart	Click this button to illustrate data chart. Refer to the following figure as an example. 
Block	Prevent the specified PC accessing into Internet within 5 minutes.
UnBlock	Allow the specified PC accessing into Internet within 5 minutes.
Recent 1 Hour/ Recent 24 Hours / Recent 7 Days	Display the records with 1 hour/24 hours/7 days recently.

Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
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.
Block Time	Display the time for the duration of the block.
Profile	Display the WAN interface.
IP	Display the IP address of the WAN interface.
RX Rate	Display the rate of data received.
TX Rate	Display the rate of data transmitted.
RX byte	Display the file size of data received.
TX byte	Display the file size of data transmitted.

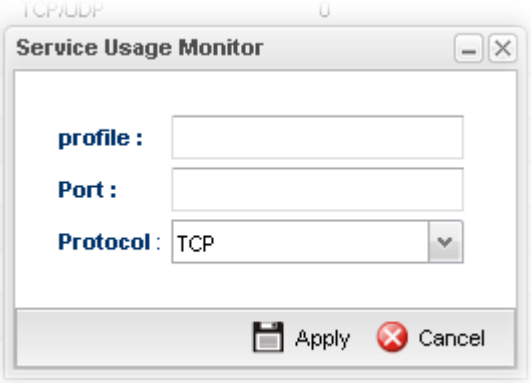
4.15.9.2 Service Usage Monitor

This page displays bandwidth usage and data traffic based on service type (port).



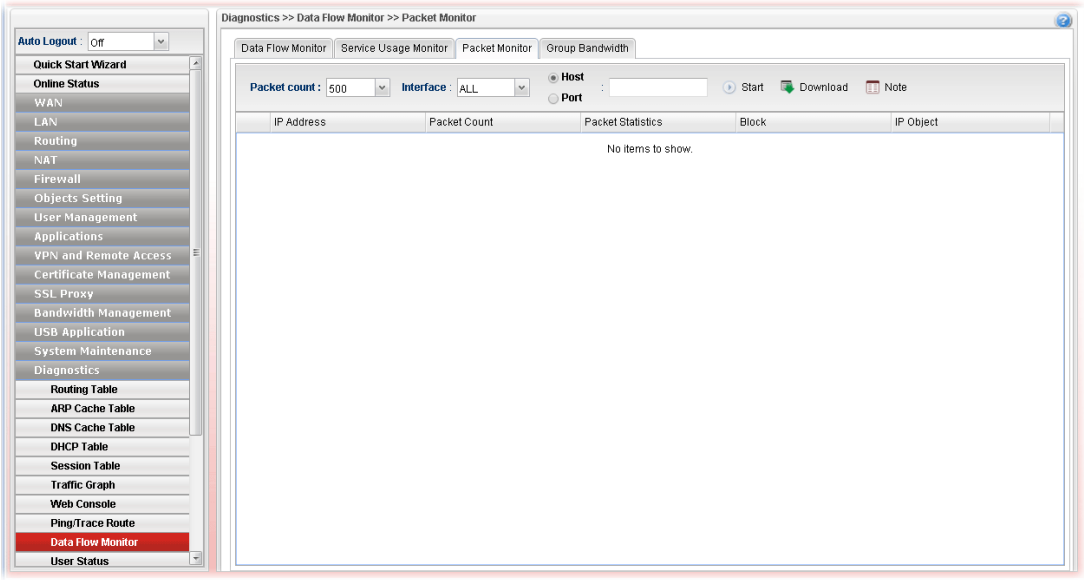
Each item will be explained as follows:

Item	Description
Enable Dataflow Monitor	Check this box to enable such function.
Filter Status	If enabled, the router will monitor the service usage for the specified IP address only. **IP Address** – Enter the IP address for monitoring. **Subnet Mask** – Enter the subnet mask for the selected IP address.

Item	Description
Add	Create a new service type (port) profile to monitor. 
Edit	Modify the selected profile. To edit the profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Auto Refresh	The system will refresh the web after specified time automatically.
Refresh	Click it to refresh the web page immediately.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of profile.
Port	Display the port number specified for the profile.
Protocol	Display the protocol specified for the profile.
RX Rate (Kbps) / TX Rate (Kbps)	Display the rate of data received / transmitted.
RX Bytes / TX Bytes	Display the file size of data received / transmitted.

4.15.9.3 Packet Monitor

This function can be used to capture the packets for analysis in the future. Moreover, the traffic data (obtaining from data flow monitor) also can be downloaded from Vigor router and stored in the host for future use.

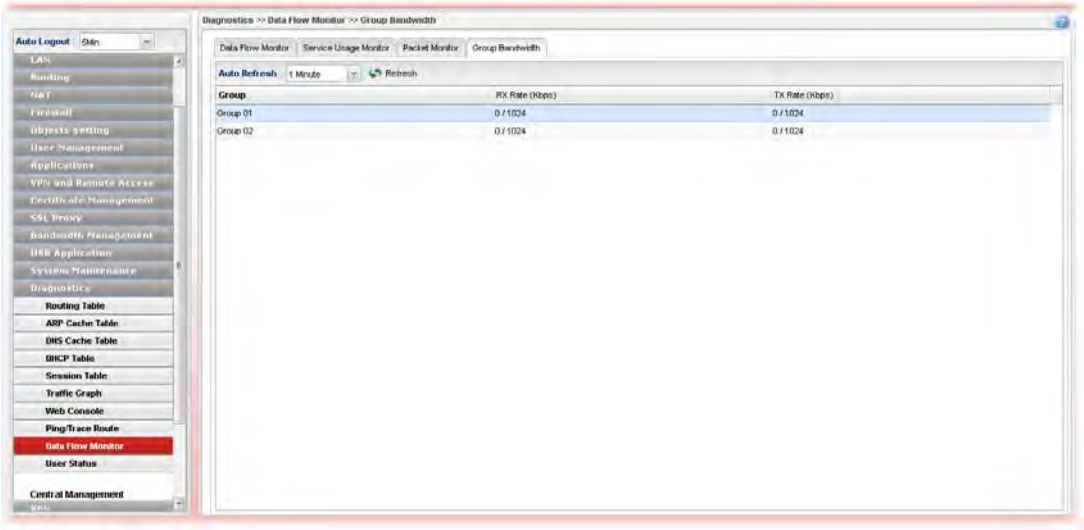


Each item will be explained as follows:

Item	Description
Packet count	Specify the threshold value of the packets to be captured by Vigor router. If the packet captured reaches the threshold value, Vigor router will cease the packet capturing.
Interface	Specify an interface which will be used to capture the packets. The default setting is “All”.
Host / Port	Type the IP address of the host or the post number that you want to monitor.
Start	Click it to capturing the packets and display the results on this page.
Download	The packets captured by Vigor router will be stored in router as “packetmonitor.pcap”. Download the file and store on your host.
Note	A pop up window appears to show special notices for such function.

4.15.9.4 Group Bandwidth

This page displays bandwidth usage or data traffic for each shared mode profile.

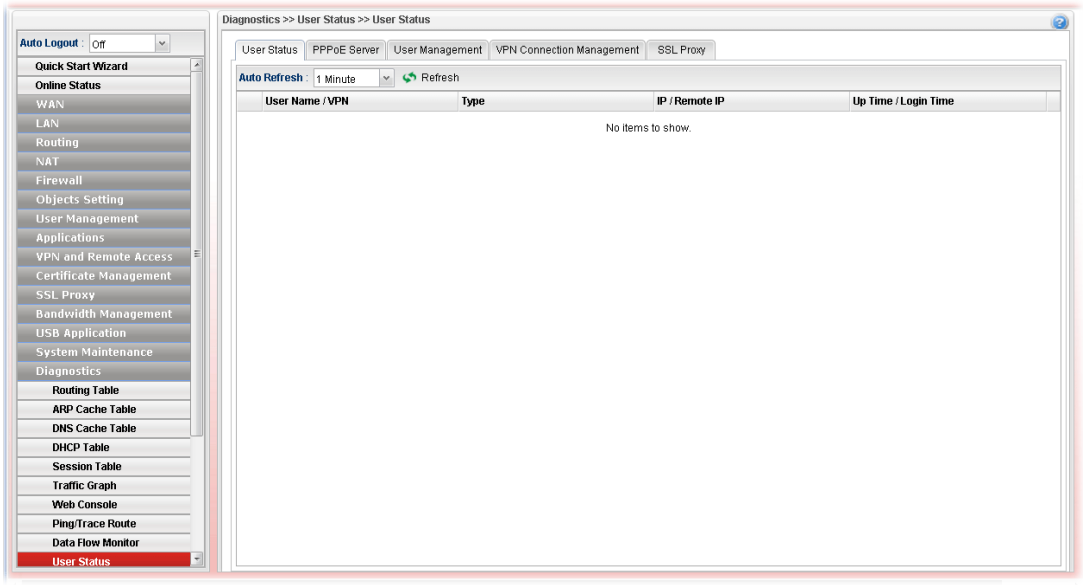


Each item will be explained as follows:

Item	Description
Auto Refresh	The system will refresh the web after specified time automatically.
Refresh	Click it to refresh the web page immediately.
Group	Display the shared mode profiles listed in **Bandwidth Management>>Bandwidth Limit**.
RX Rate (Kbps)	Display the rate of data received / transmitted.
TX Rate (Kbps)	Display the file size of data received / transmitted.

4.15.10 User Status

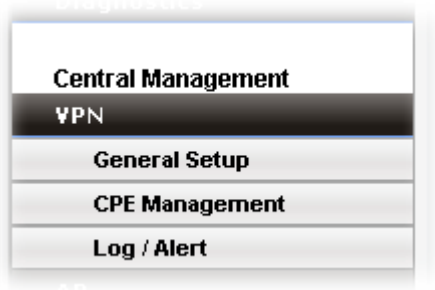
This page displays connection information of user account /VPN profile, PPPoE Server, User Management, VPN Connection Management and SSL Proxy for reference.



4.16 Central Management (VPN)

Vigor3900 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.

Below shows the menu items under CVM:



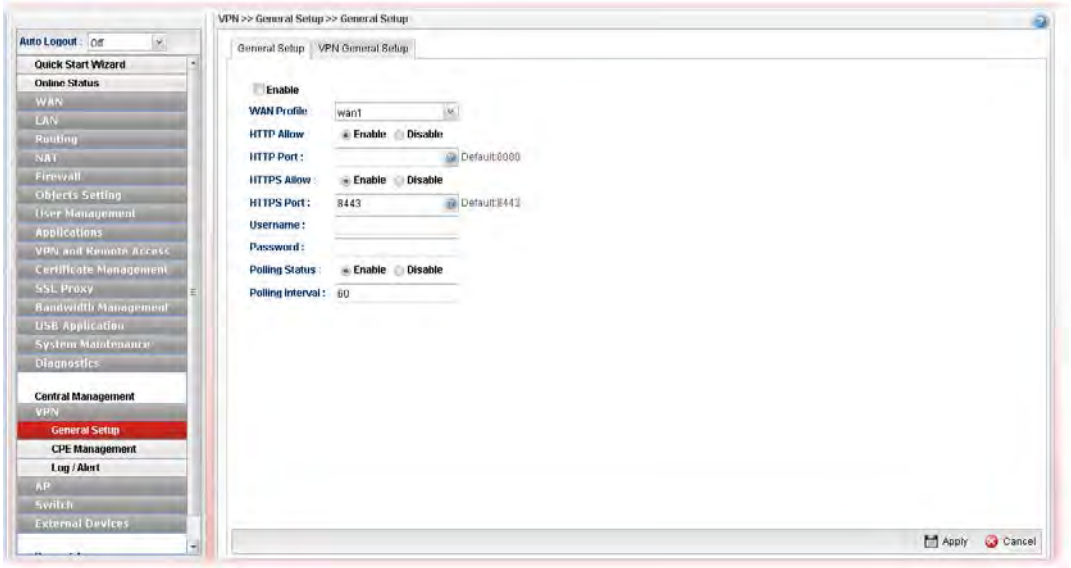
Note: 1. Such menu can manage the CPE connected through WAN only.
2. Up to 16 devices can be managed.

4.16.1 General Setup

General Setup is used to configure settings which will be used by the clients to register to such Vigor router. Under **Cental Management**, Open **VPN>>General Setup>>General Setup** to configure the basic settings for central management VPN mechanism.

4.16.1.1 General Setup

To enable the Central Management VPN feature, the first thing you have to do is enabling port settings.



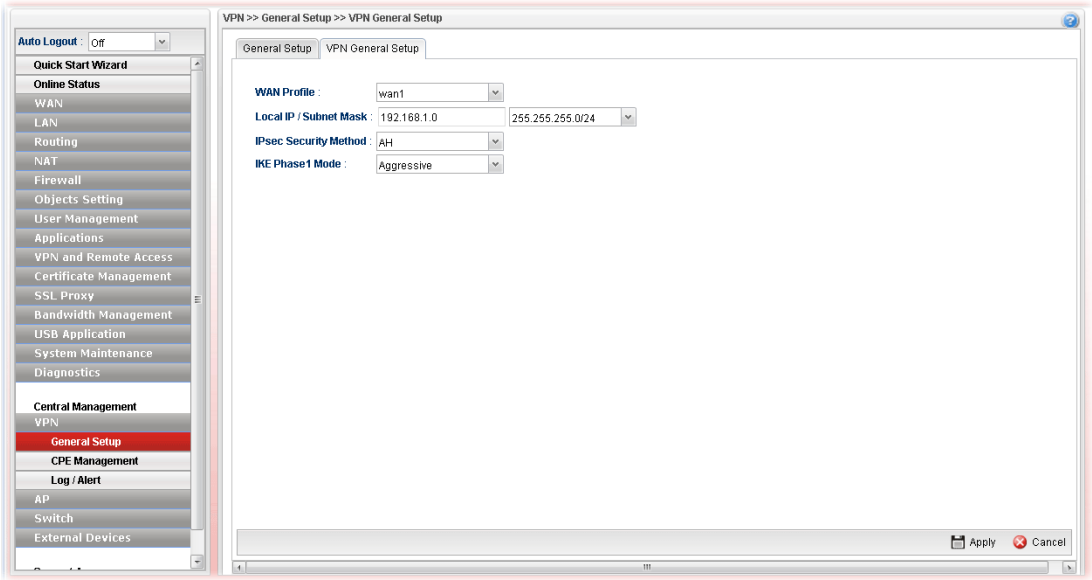
Available parameters are listed as follows:

Item	Description
Enable	Check it to enable the settings.
WAN Profile	Specify an interface for VPN management.

HTTP Allow	Click Enable to active the HTTP setting.
HTTP Port	Type a port number for HTTP. The default value is 8080.
HTTPS Allow	Click Enable to activate the HTTPS setting.
HTTPS Port	Type a port number for HTTPS. The default value is 8443.
Port	Type a port number for Vigor3900.
Username	Type a username which will be used by any CPE tried to connect to Vigor router.
Password	Type a password which will be used by any CPE tried to connect to Vigor router.
Polling Status	**Enable** – Click it to enable the polling function. **Disable** – Click it to disable the polling function.
Polling Interval	Type the time value (unit is second). The range is from 60 ~ 86400.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

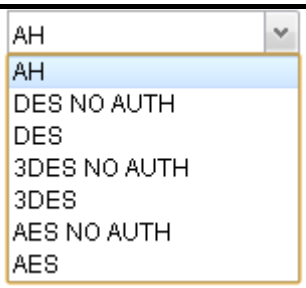
4.16.1.2 VPN General Setup

This page allows you to configure the basic settings for the VPN tunnel of Vigor3900.



Available parameters are listed as follows:

Item	Description
WAN Profile	Choose a WAN interface profile to be used.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
IPsec Security Method	Choose one of the following methods 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.

	
IKE Phase1 Mode	Choose **Aggressive** or **Main** as the IKE Phase1 Mode.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

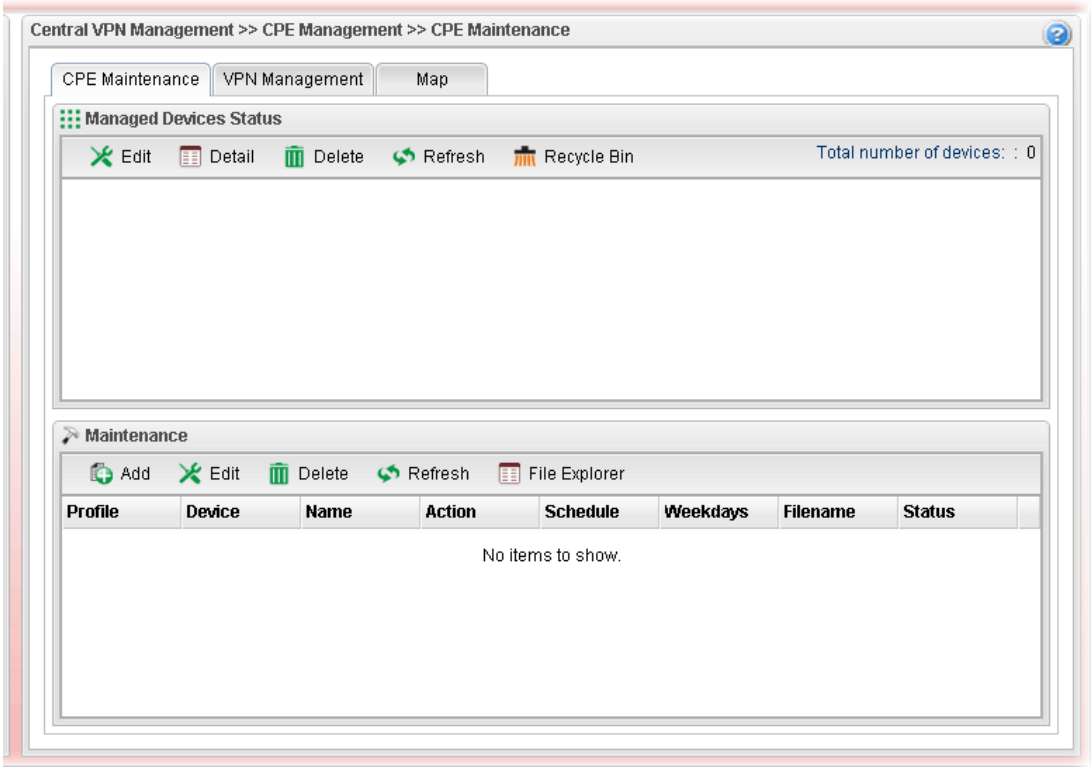
4.16.2 CPE Management

All the CPEs managed by Vigor3900 can be seen with icons from this page.

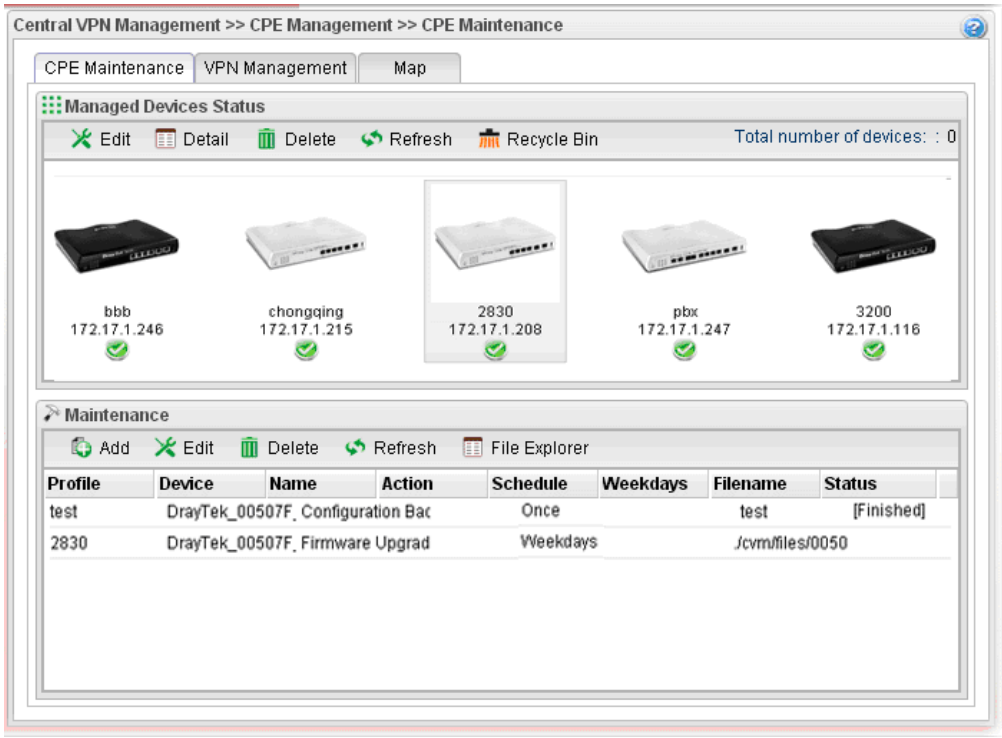
4.16.2.1 CPE Maintenance

This page allows you to manage the CPEs connected to Vigor3900.

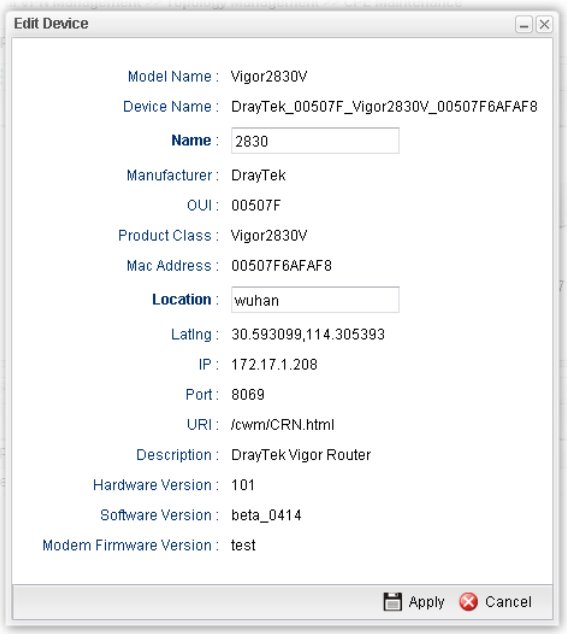
- Page without CPE connected

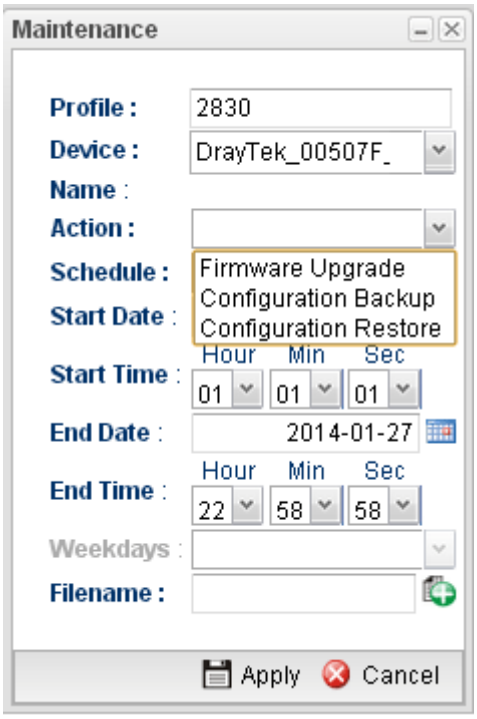


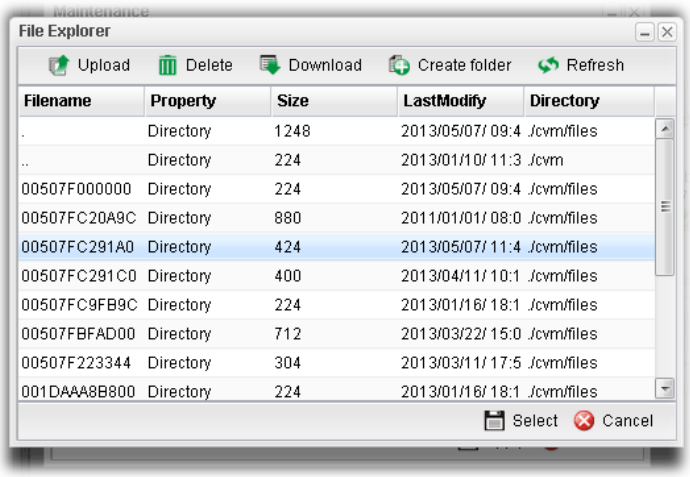
- Page with CPE connected



Available parameters are listed as follows:

Item	Description
Managed Devices Status	This area displays icons for the CPE managed by Vigor3900. **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 (for identification) and/or location manually.  **Detail** – It displays the same content as the Edit button.

	However, it cannot be used to modify name or location. **Delete** – To disconnect the management of any CPE, click the CPE icon you want and click the Delete button. **Refresh** – Click it to refresh current page. **Recycle Bin** – All the deleted CPEs will be stored in a temporary place for the administrator to retrieve. It is useful especially for the CPEs deleted carelessly. If you want to retrieve some CPE, click it to open another window. Deleted CPEs containing related information will be displayed on the window. Choose the one you want to retrieve and click Restore. Later, the selected one will appear on the **Managed Devices Status** area again.
Maintenance	This area displays all the profiles which are created for applying to the managed device. **Add** – To add a new profile, simply click it to open a pop up window.  **Edit** – To modify existed profile, choose the one you want to change and click this button to open the pop up window. **Delete** – To discard any existed profile, simply choose one you want and click this button to delete the profile. **Refresh** – Click it to refresh current page. **File Explorer** – Click it to open a file explorer. The available firmware will be displayed in such page.



Profile – Display the name of the profile.

Device – Display the name (named by Vigor3900) of the devices selected by such profile.

Name – Display the name (can be modified by the administrator) of the device.

Action – Display the action specified for such profile.

Schedule – Display the frequency of for such profile which will be performed by Vigor router.

Weekdays – Display the day(s) chosen for such profile.

Filename – Display the filename of the firmware.

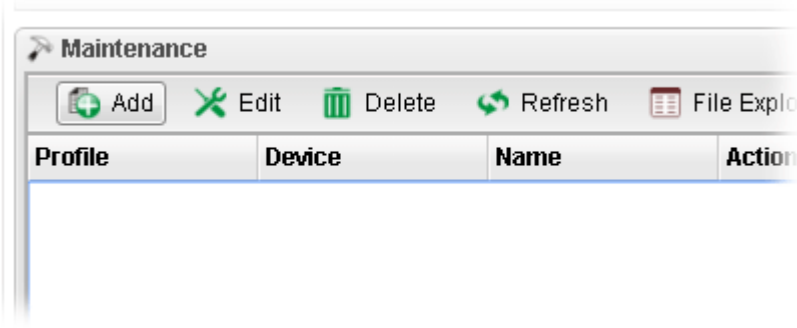
Status – Display current status of the profile has been finished or not.

Refer to sections **"How to manage the CPE (router) through Vigor3900?"** and **"How to upgrade CPE firmware through Vigor3900?"** for more detailed information.

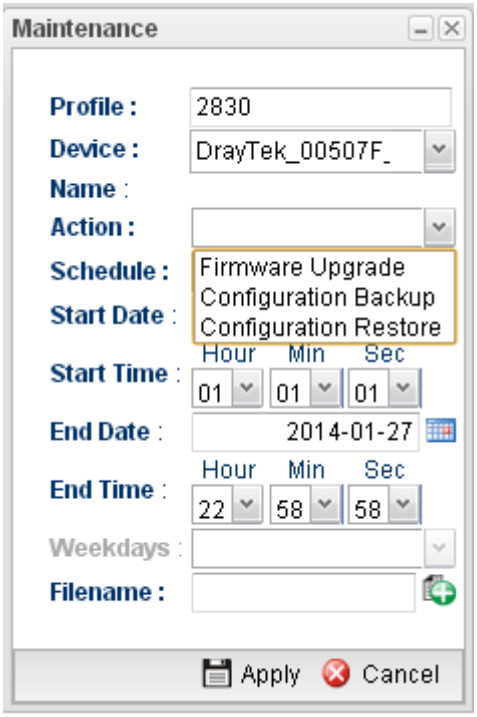
How to add a new Maintenance Profile

Follow the steps below to create a new maintenance profile.

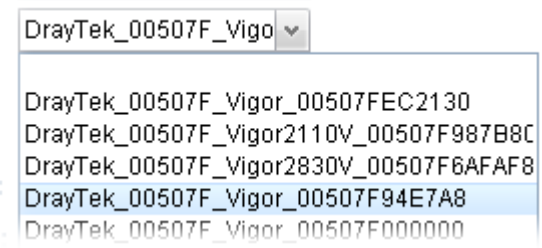
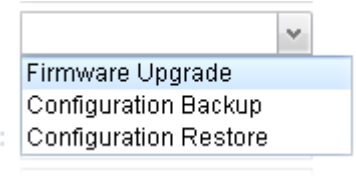
1. Click **Add** from the **Maintenance** area.

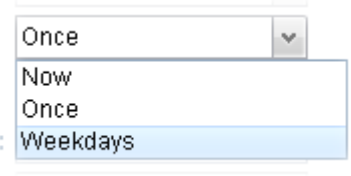
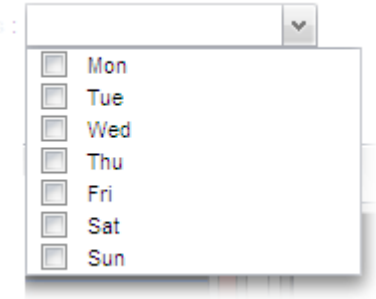


2. The Maintenance dialog appears.



Available parameters are listed as follows:

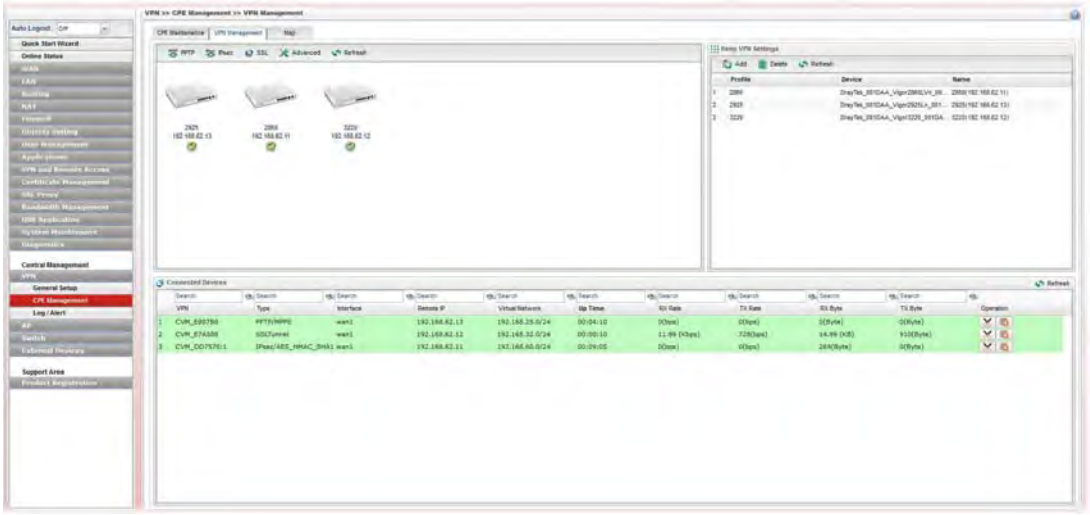
Item	Description
Profile	Type the name of the maintenance profile.
Device	The drop down list will display all the devices detected by Vigor3900. Choose the one which will be applied with such new created profile.  Usually, the name of the device will be assigned by Vigor3900 automatically. If you want to give a name easy for easy recognition, refer to 4.11.2.1 CPE Maintenance to specify another name for the device additionally.
Name	Display the name (can be modified by the administrator) of the device.
Action	There are three actions for you to choose for such profile.  **Firmware Upgrade** – It means such profile will be used for

	firmware upgrade. **Configuration Backup** – It means such profile will be used for configuration backup of the selected CPE. **Configuration Restore** – It means such profile will be used for restoring the configuration of the selected CPE.
Schedule	The new created profile can be applied to the selected CPE based on the schedule configured here.  **Now** – The action will be performed for the selected CPE immediately. **Once** – The action will be performed for the selected CPE at the specified time, and will be done for once. **Weekdays** – The action will be performed for the selected CPE at the time and date specified below every week.
Start Date / **End Date**	It is available only when **Once** is selected as **Schedule**. Specify the starting date /ending date with the format YYYY-MM-DD.
Start Time / **End Time**	It is available only when **Once** is selected as **Schedule**. Specify the starting time /ending time with the format YYYY-MM-DD.
Weekdays	It is available only when **Weekdays** is selected as **Schedule**. Simply check the day you want. 
Filename	Type the name string of the file which will be used for firmware upgrade, configuration backup or configuration restore.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

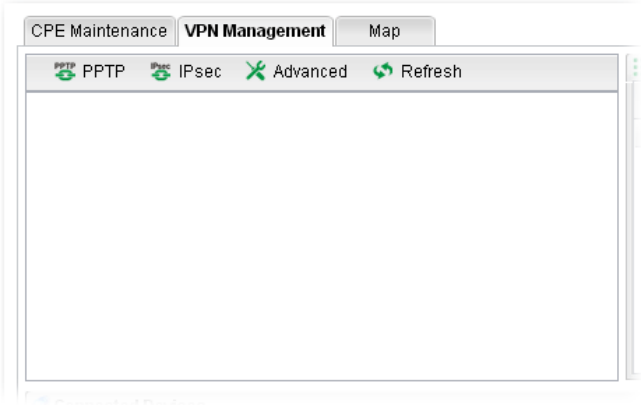
3. Enter all the settings and click **Apply**.
4. A new maintenance profile has been created.

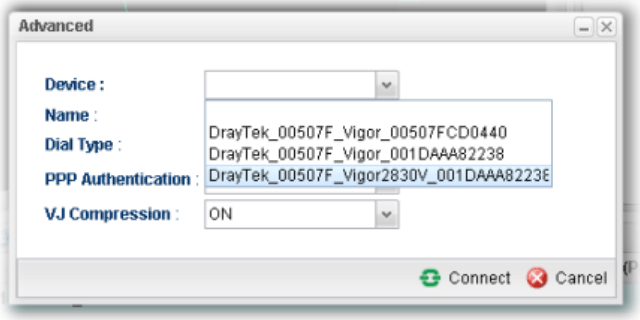
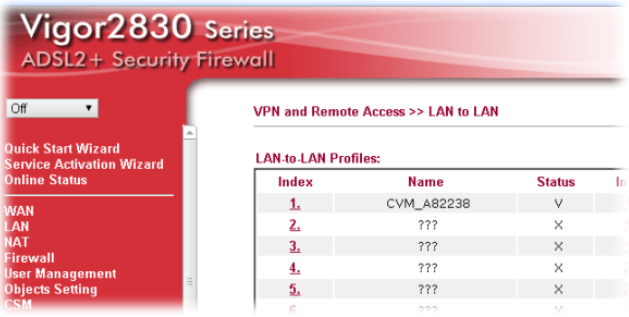
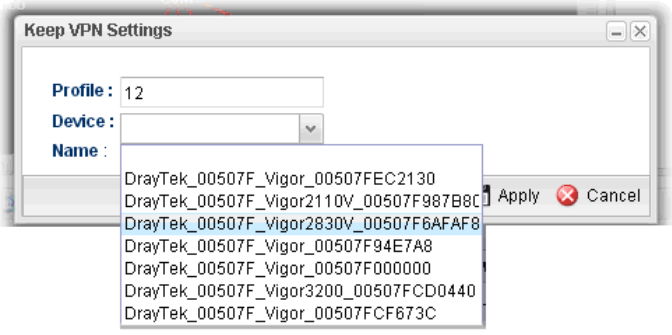
4.16.2.2 VPN Management

An easy method is offered to configure VPN settings for building VPN connection between Vigor3900 (treated as VPN server) and other Vigor router (treated as CPE device, i.e., VPN client).



Available parameters are listed as follows:

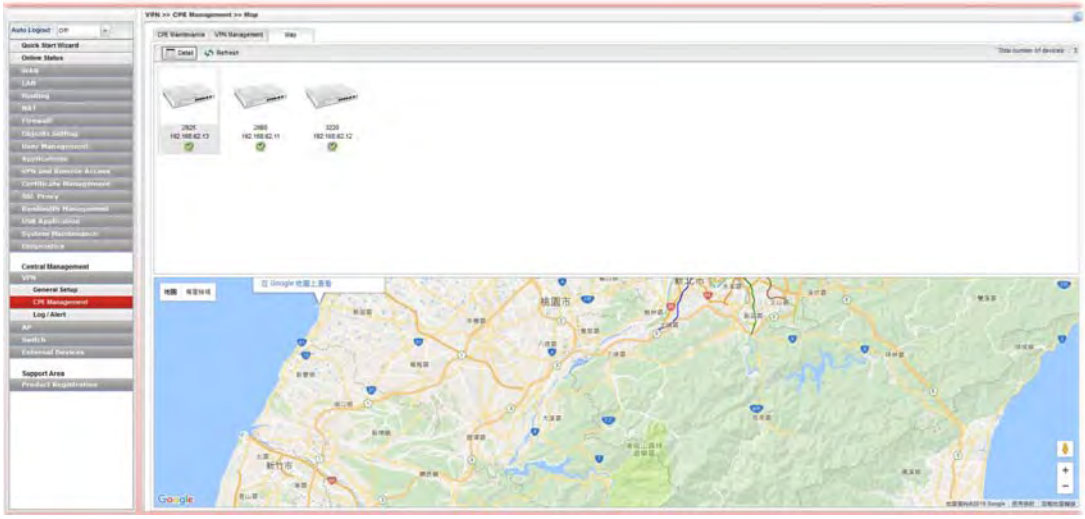
Item	Description
Display Screen	Once the device is managed (controlled) by Vigor3900, it will be displayed on such screen automatically. If not, refer to sections **"3.7 How to manage the CPE (router) through Vigor3900?"** for more detailed information. If the VPN isn't established successfully, a red line will appear instead. 
PPTP	To build a quick VPN connection with **PPTP**, simply click the remote CPE (waiting for the icon to be bigger) first and then click it. If the connection is built successfully, a green line will appear.
IPsec	To build a quick VPN connection with **IPsec**, simply click the remote CPE (waiting for the icon to be bigger) first and then click it. If the connection is built successfully, a blue line will appear.
SSL	To build a quick VPN connection with **SSL**, simply click the remote CPE (waiting for the icon to be bigger) first and

	then click it. If the connection is built successfully, a blue line will appear.
Advanced	To build a VPN connection with detailed configuration (such as PPP authentication and VJ compression), click **Advanced** tool.  Specify the CPE from the Device drop down list; choose the name of the CPE; select PPTP or IPsec as the Dial Type; choose PAP_only or PAP_or_CHAP as PPP authentication; enable or disable VJ Compression; then click **Connect** to build the VPN connection. **Note:** If the VPN connection has been established successfully, a new ***LAN to LAN profile*** will be created for the CPE automatically. See the following example. 
Keep VPN Settings	To avoid the VPN be disconnected due to the settings changed by the client, the connection status can be kept by specified by such feature. **Add** – Click it to open the following dialog. Type the name of the profile and choose the CPE from the Device drop down list. Then, click Apply to save the settings. Such profile will be applied to the device connecting to Vigor3900 with VPN.  **Delete** – Click it to delete the profile. The VPN between the

	router and the client might not be guaranteed. **Refresh** – Click it to refresh current page. **Profile** – Display of the profile used now. **Device** – Display the name of the CPE connected to Vigor router via VPN. **Name** – Display the name (can be modified by the administrator) of the device. Refer to 4.11.2.1 CPE Maintenance for detailed information.
Connected Devices	Once the VPN is established successfully, the basic information such as the connection type, IP address, RX/RX will be displayed on this field. **Refresh** – Click it to refresh current page. **VPN –** Display the name of the VPN. **Type –** Display the type of the connection mode. **Interface** – Display the WAN interface. **Remote IP –** Display the IP address of the remote end. **Virtual Network –** Display the IP address of Vigor3900. **Up Time –**Display the connection time of such VPN. **RX(Packets) /TX(Packets) –**Display the number of the packets exchanged in such VPN. **Disconnect –** Click it to disconnect the VPN.

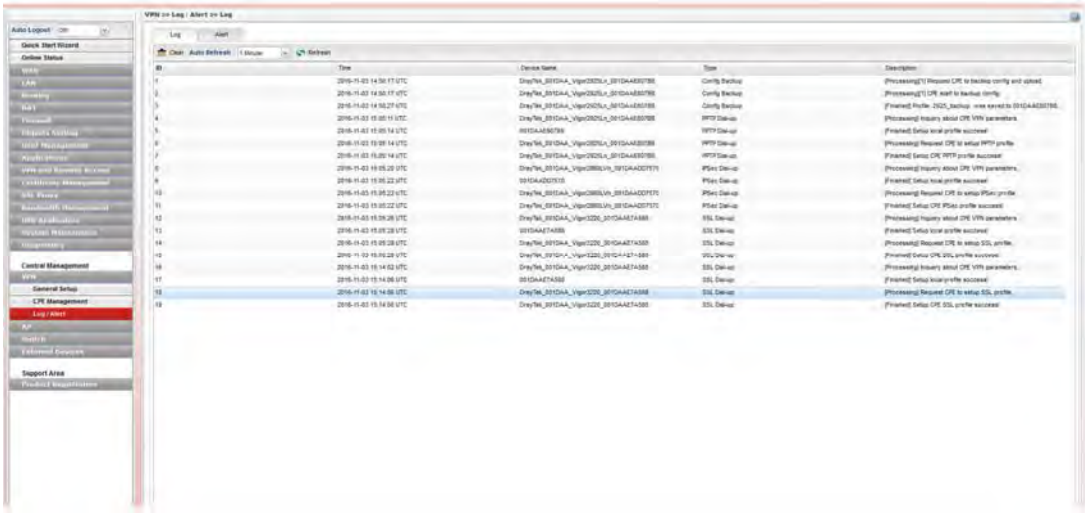
4.16.2.3 Map

To display the **location** of the selected CPE with a bird's eye view, open **Central Management>>VPN>>CPE Management** and click the tab of **Map**.



4.16.3 Log/Alert

The Log page offers brief information to identify the CPE connected to Vigor3900.



The Alert page offers brief information to identify the CPE connected to Vigor3900.

4.17 Central Management (AP)

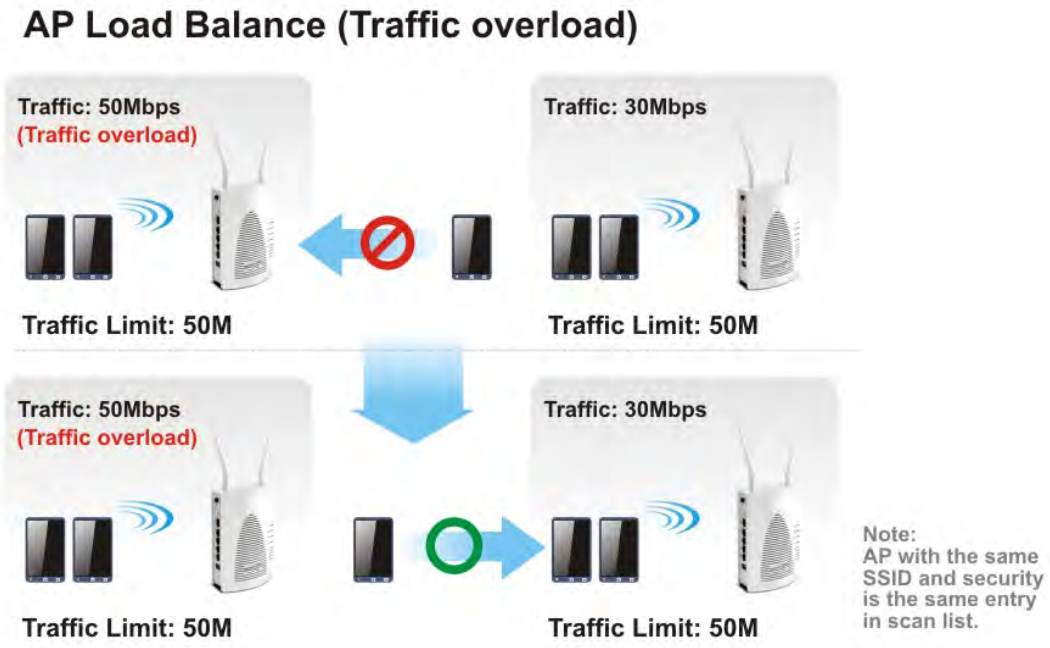
Vigor3900 can manage the access points supporting AP management via Central AP Management.

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

Load Balance for AP

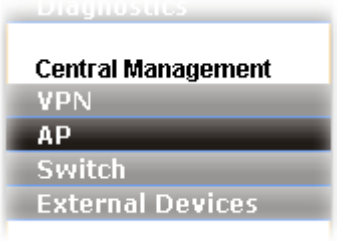
The parameters configured for Load Balance can help to distribute the traffic for all of the access points registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.



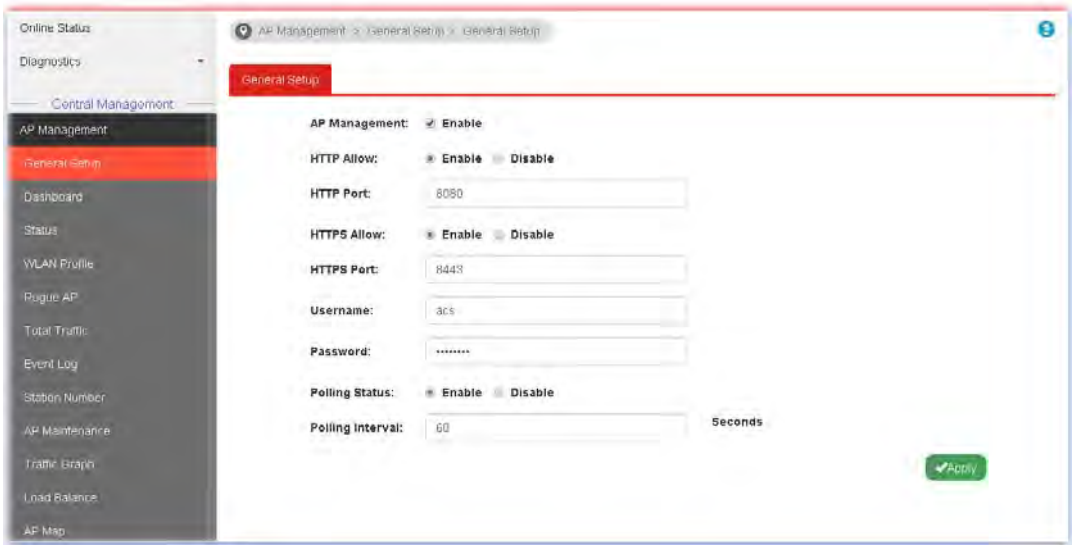
AP Maintenance

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.

Click **Central Management>>AP.**



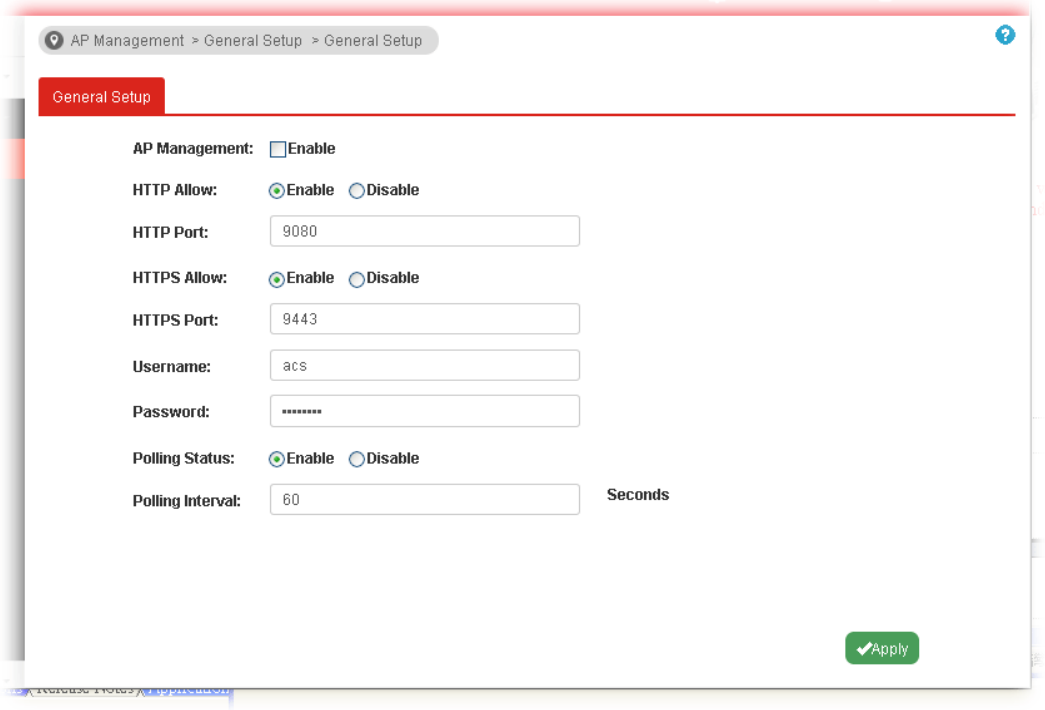
Configuration pages with new designed web pages will be shown as follows. They are suitable and easy to browse on network for PC users and mobile users.



Menu items related to AP are General Setup, Dashboard, Status, WLAN Profile, Rogue AP, Total Traffic, Event Log, Station Number, AP Maintenance, Traffic Graph, Load Balance, AP Map, and Function Support List.

4.17.1 General Setup

To enable the Central Management AP feature, the first thing you have to do is enabling port settings. Click **AP Management>>General Setup** to get the following page.



Available parameters are listed as follows:

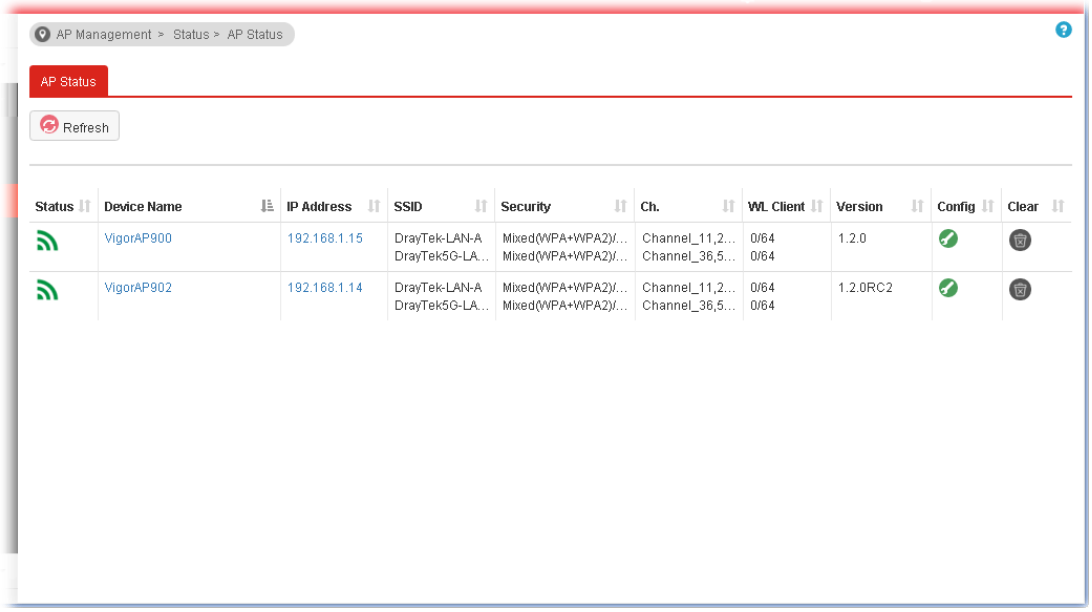
Item	Description
AP Management	Check **Enable** to enable the settings configured in this page.
HTTP Allow	Click **Enable** to active the HTTP setting.
HTTP Port	Type a port number for HTTP. The default value is 9080.
HTTPS Allow	Click **Enable** to activate the HTTPS setting.
HTTPS Port	Type a port number for HTTPS. The default value is 9443.
Username	Type a username which will be used by any Access Point trying to connect to Vigor router.
Password	Type a password which will be used by any Access Point tried to connect to Vigor router.
Polling Status	Click **Enable** to activate polling interval setting.
Polling Interval	Type the time value (unit is second). The range is from 60 ~ 86400.
Apply	Click it to save the configuration.

4.17.2 Dashboard

This page shows VigorAP's information about **Event Log, Total Traffic** or **Station Number** by displaying text and histogram.

4.17.3 Status

This page displays general information for the VigorAP managed by Vigor3900.



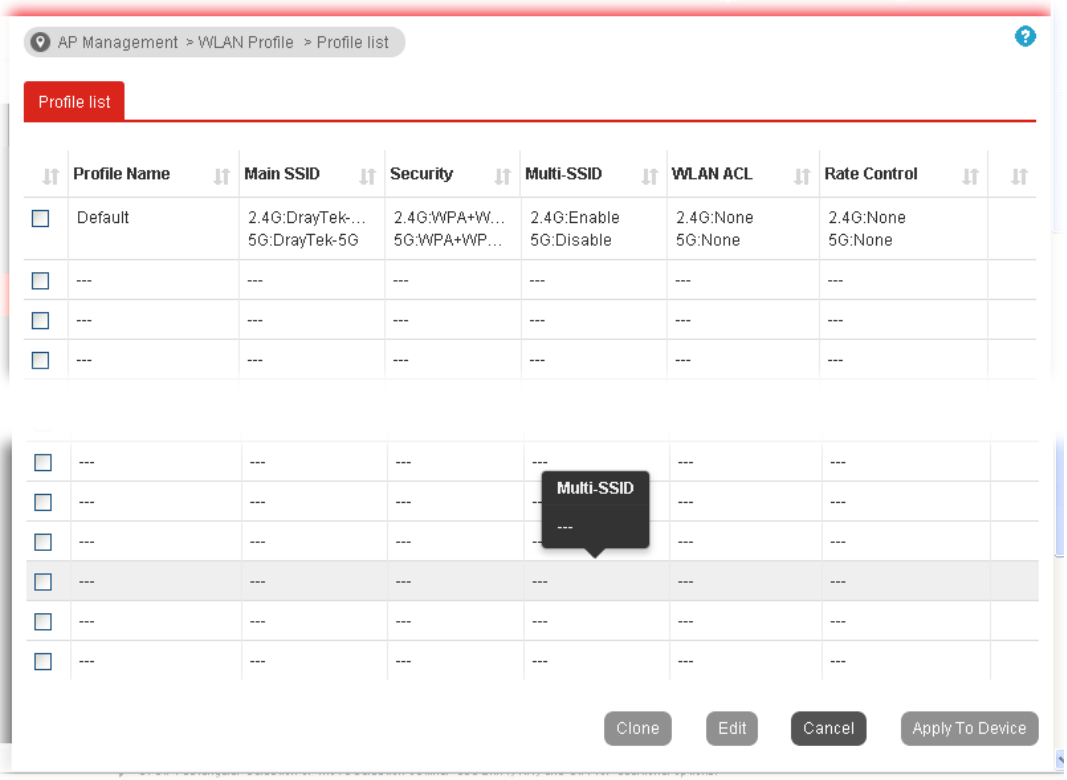
Available parameters are listed as follows:

Item	Description
Status	Display current status (connected or disconnected) of the managed AP.
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 Vigor3900.
Security	Display the security mode used by the access point.
Ch.	Display the channel used by the access point.
WL Client	Display current number/maximum number (ex: 0/64) of clients connecting to the selected wireless access point.
Version	Display the firmware version used by the access point.
Config	Click it to open the configuration page of the selected VigorAP. The device name, Login username and Login password can be modified if required.
Clear	Such button allows you to remove the selected VigorAP.

4.17.4 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.



Check the box on the left side of the selected profile to modify the content of the profile. The **Clone**, **Edit** and **Apply To Device** buttons will be available then.

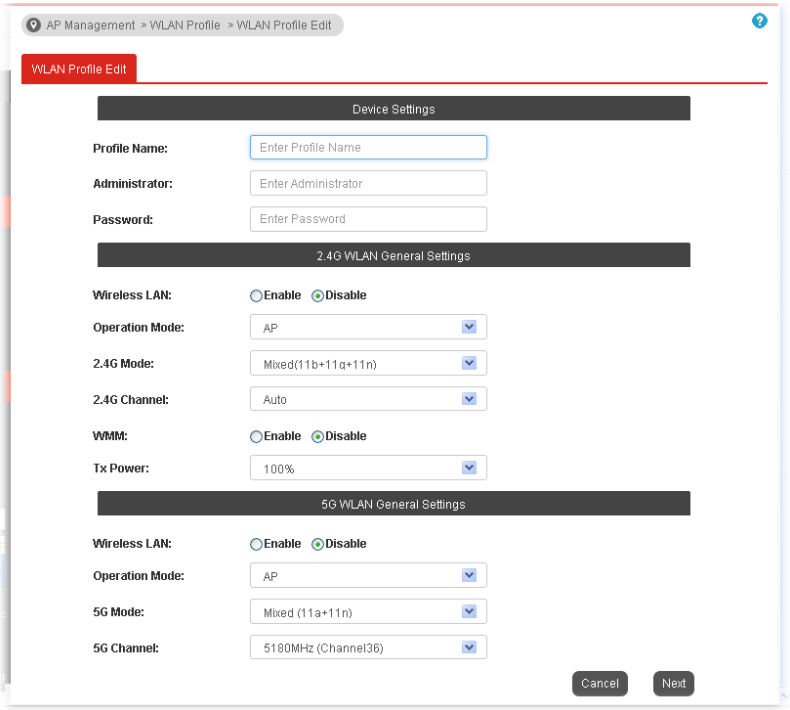
Available settings are explained as follows:

Item	Description
Profile Name	Display the name of the profile. The default profile cannot be renamed.
Main SSID	Display the SSID configured by such wireless profile.
Security	Display the security mode selected by such wireless profile.
Multi-SSID	Enable means multiple SSIDs (more than one) are active. Disable means only SSID1 is active.
WLAN ACL	Display the mode of the access control list.
Rate Control	Display the upload and/or download transmission rate.
Clone	It can copy settings from an existing WLAN profile to another WLAN profile. First, you have to check the box of the existing profile as the original profile. Second, click **Clone**. The following dialog will appear.

	 Third, choose the profile index to accept the settings from the original profile. Forth, type a new name in the field of **Renamed as**. Last, click **Apply** to save the settings on this dialog. The new profile has been created with the settings coming from the original profile.
Edit / Add	It allows you to modify an existing / add a new wireless profile or create a new wireless profile.
Apply to Device	Click it to apply the selected wireless profile to the specified Access Point. Simply choose the device you want from **Existing Device** field. Click >> to move the device to **Selected Device** field. Then, click **OK**. The selected WLAN profile will be applied to the selected access point immediately. Later the access point will reboot.

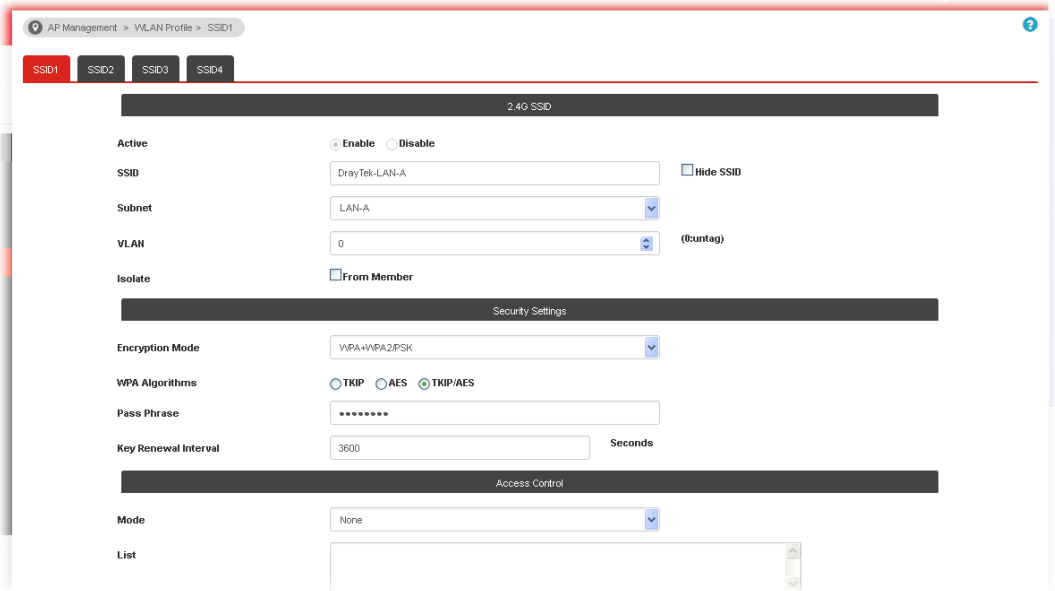
How to edit the wireless LAN profile?

1. Check the box on the left side of the selected profile.
2. Click the **Edit / Add** button to display the following page.

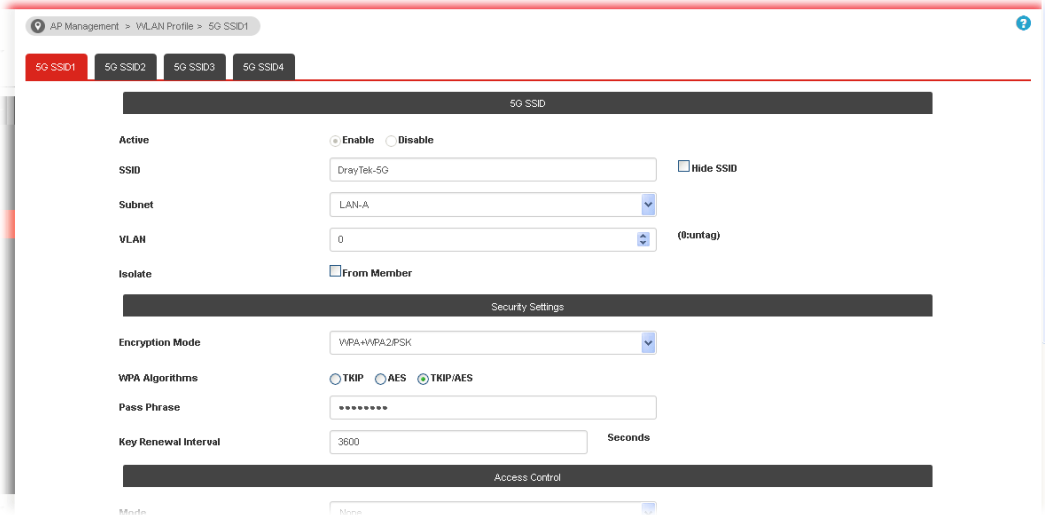


Note: The function of Auto Provision is available for the default WLAN profile.

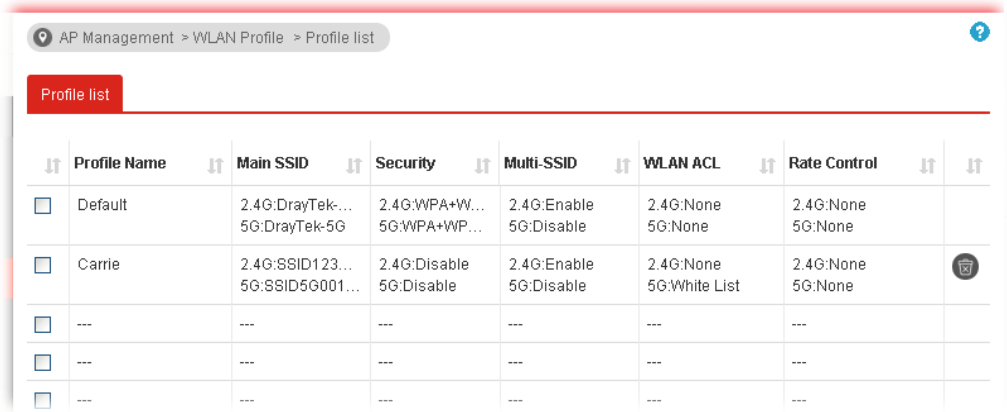
3. After finished the general settings configuration, click **Next** to open the following page for 2.4G wireless security settings.



4. After finished the above web page configuration, click **Next** to open the following page for 5G wireless security settings.



5. When you finished the above web page configuration, click **Finish** to exit and return to the first page. The modified WLAN profile will be shown on the web page.

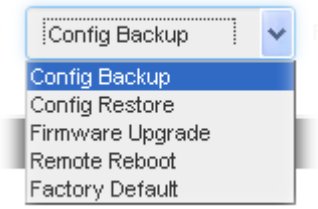


4.17.5 AP Maintenance

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.

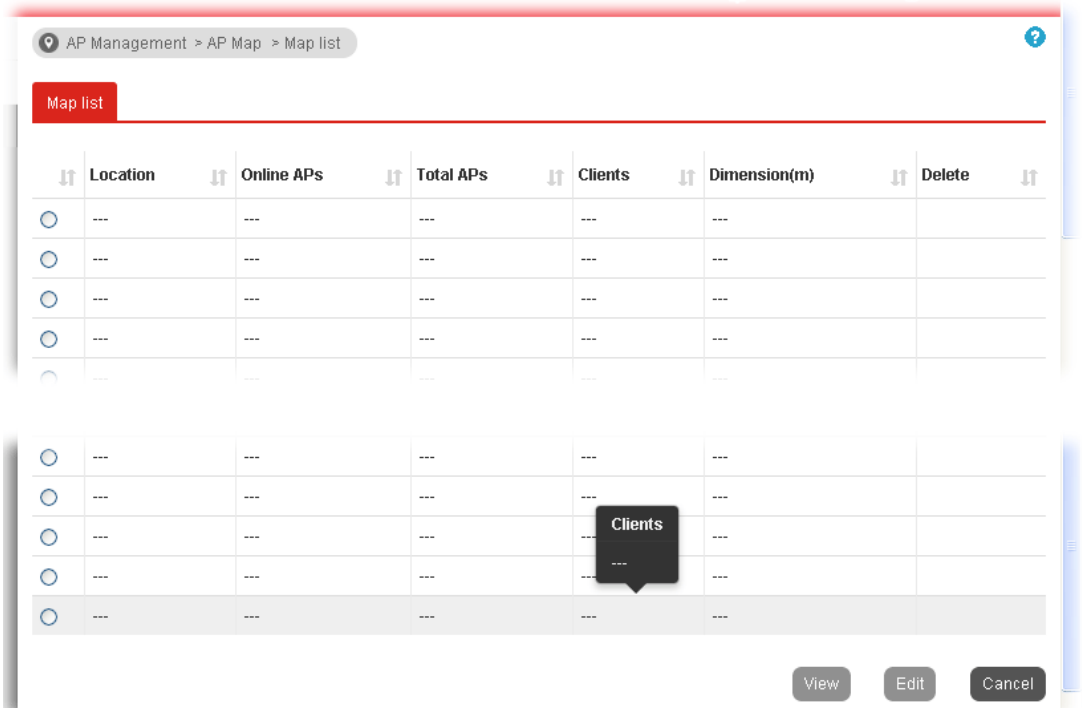
Config Backup can be performed to one AP at one time. Others functions (e.g., Config Restore, Firmware Upgrade, Remote Reboot) can be performed to more than one AP at one time by using Vigor3900.

Available settings are explained as follows:

Item	Description
Action Type	There are four actions provided by Vigor router to manage the access points.  Vigor router can **backup** the configuration of the selected AP, **restore** the configuration for the selected AP, perform the **firmware upgrade** of the selected AP, **reboot** the selected AP remotely and perform the **factory default** for the selected AP.
File/Path	Specify the file and the path which will be used to perform **Config Restore** or **Firmware Upgrade**.
Available Device	**Model** – Display the model name connected to Vigor3900. **Device name** – Display the device name of AP connected to Vigor3900.
Apply	Click it to apply the action to the selected AP.

4.17.6 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.



Each item will be explained as follows:

Item	Description
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.
Edit	Click it to modify AP map.

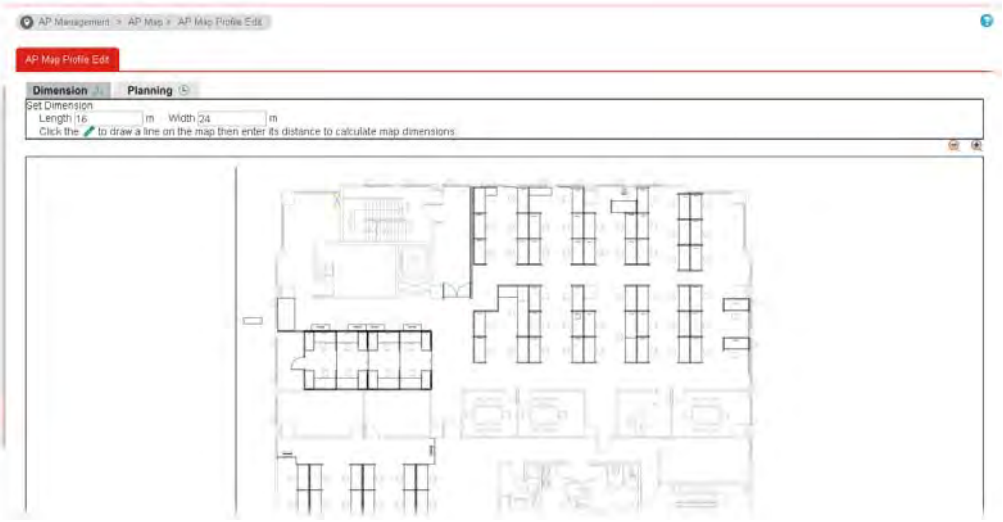
Creating /Editing the AP Map Profile

1. Select a radio button and click **Edit** to open the following web page.

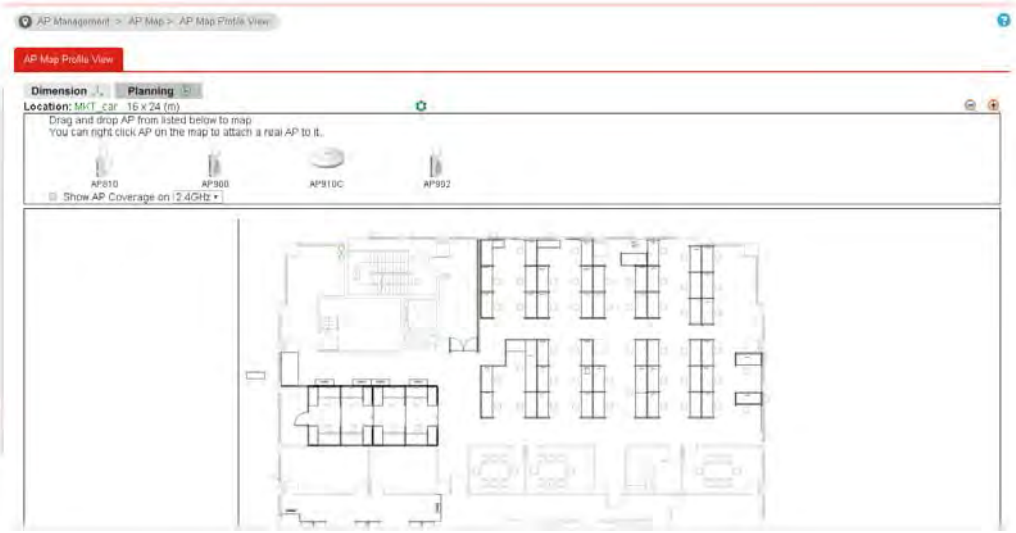
Available settings are explained as follows:

Item	Description
Location (Profile Name)	Type a name (e.g., MKT_car) 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.
Next	Click it to go to the next configuration page.
Cancel	Click it to cancel the configuration.

2. Click **Next**. The configuration page with floor plan will be shown on the web page. Set the dimensions by typing suitable numbers (unit: meter) for the length and width. Or use the ruler icon to draw a line on the map to calculate the dimensions.

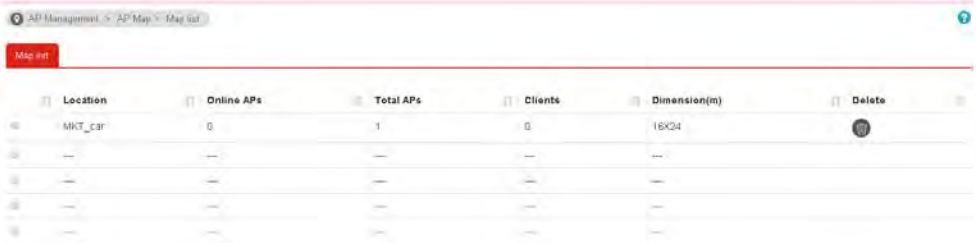


3. Click the **Planning** tab. Drag and drop an AP icon from **Compatible AP List** to the map on the left side.



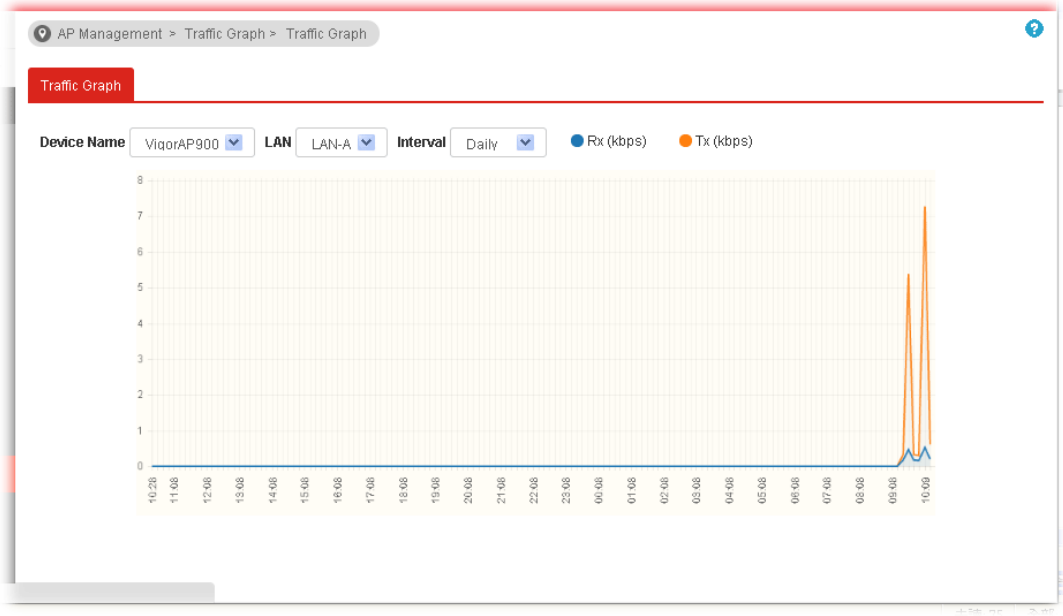
4. Check the box of **Show AP Coverage on** 5GHz/2.4 to display the signal coverage area.

5. Adjust the AP on the map to find out which place can have the best wireless coverage. At last, click **Save**.



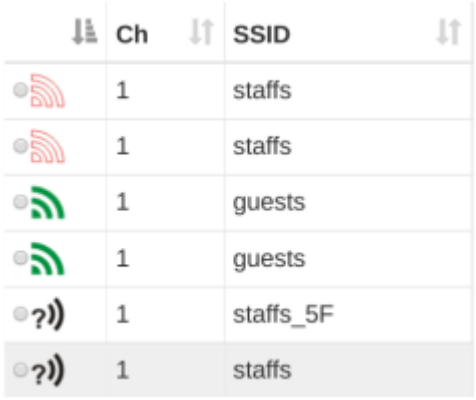
4.17.7 Traffic Graph

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.



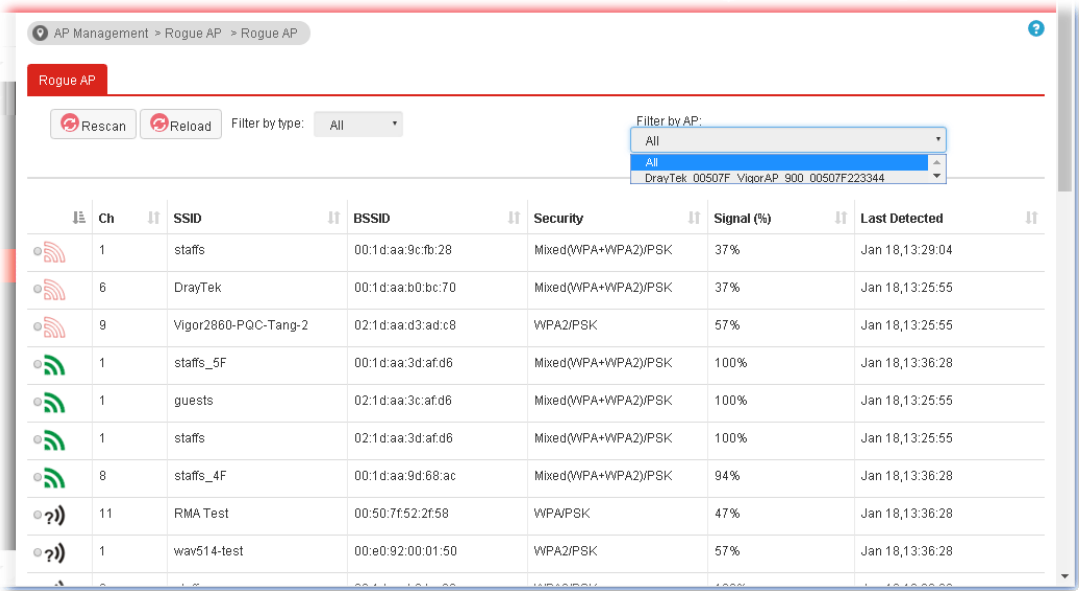
4.17.8 Rogue AP

Access Points can be classified with friendly (green) APs, rogue APs (red) and unknown (black) APs in different colors.



	Ch	SSID
	1	staffs
	1	staffs
	1	guests
	1	guests
	1	staffs_5F
	1	staffs

This page displays the access point scanned by Vigor router.



Ch	SSID	BSSID	Security	Signal (%)	Last Detected
1	staffs	00:1d:aa:9c:fb:28	Mixed(WPA+WPA2)/PSK	37%	Jan 18,13:29:04
6	DrayTek	00:1d:aa:b0:bc:70	Mixed(WPA+WPA2)/PSK	37%	Jan 18,13:25:55
9	Vigor2860-PQC-Tang-2	02:1d:aa:d3:ad:c8	WPA2/PSK	57%	Jan 18,13:25:55
1	staffs_5F	00:1d:aa:3d:af:d6	Mixed(WPA+WPA2)/PSK	100%	Jan 18,13:36:28
1	guests	02:1d:aa:3c:af:d6	Mixed(WPA+WPA2)/PSK	100%	Jan 18,13:25:55
1	staffs	02:1d:aa:3d:af:d6	Mixed(WPA+WPA2)/PSK	100%	Jan 18,13:25:55
8	staffs_4F	00:1d:aa:9d:68:ac	Mixed(WPA+WPA2)/PSK	94%	Jan 18,13:36:28
11	RMA Test	00:50:7f:52:2f:58	WPA/PSK	47%	Jan 18,13:36:28
1	wav514-test	00:e0:92:00:01:50	WPA2/PSK	57%	Jan 18,13:36:28

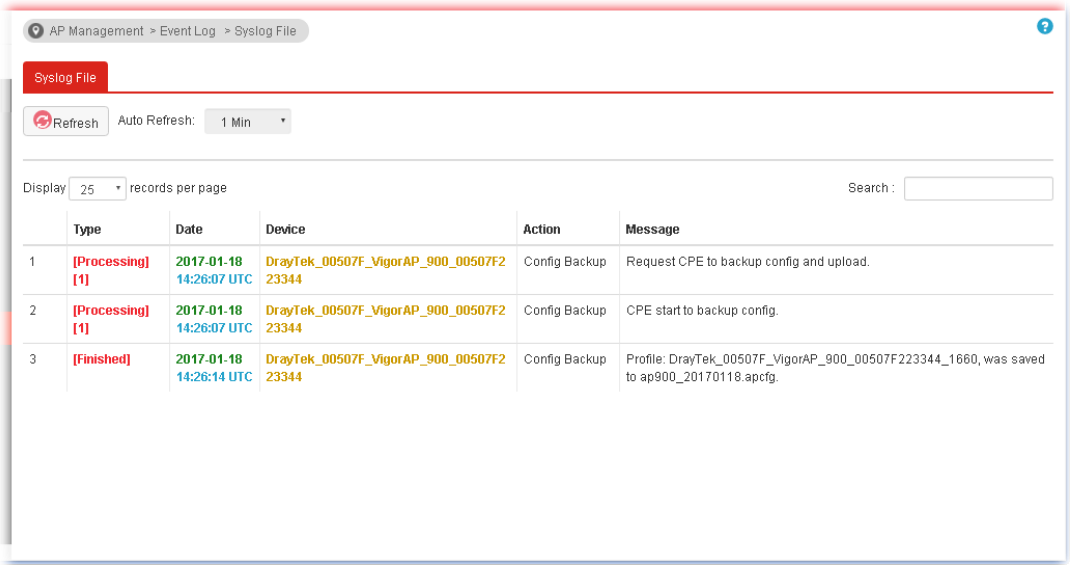
Each item will be explained as follows:

Item	Description
Rescan	Click to scan the access points again.
Reload	Click it to refresh the web page immediately.
Filter by type	AP status page will be displayed based on the type (Friendly, Rogue, Unknown) of access points. That is, only the selected type (Friendly, Rogue, Unknow) will be shown on this page. However, if unknown is selected, Vigor router will let you to classify the selected AP as a Rogue or Friendly AP.
Filter by AP	AP status page will be displayed based on the model of the access points. That is, only the selected AP model will be shown on this page.
AP's MAC Address	When an AP is selected, the MAC address related to that AP

Item	Description
	will be displayed automatically.
AP's SSID	When an AP is selected, the SSID of the selected AP will be displayed automatically.
Add to Friendly APs	**Add** - Click it to make the selected AP be classified as friendly AP.
Rogue APS	**Add** - Click it to make the selected AP be classified as rogue AP.
Delete from Friendly / Rogue APs	Click it to make the selected AP be classified as unknown AP.
Ch	Display the channel used by the detected access point.
SSID	Display the SSID specified for the detected access point.
BSSID	Display the MAC address of the detected access point.
Security	Display the security mode (e.g., WPA/PSK, Mixed (WPA+WPA2)) used by the selected access point.
Signal	Display the wireless signal strength of the access point.
Last Detected	Display the date and time that such access point was detected by Vigor router.

4.17.9 Event Log

Time and event log for all of the APs managed by Vigor router will be shown on this page. It is useful for troubleshooting if required.

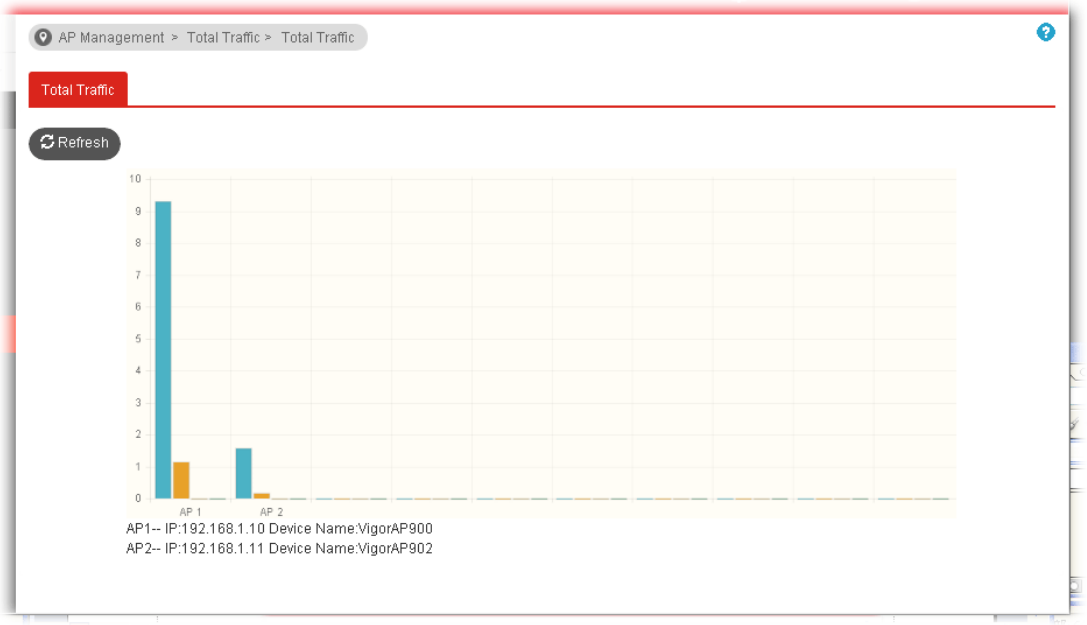


Each item will be explained as follows:

Item	Description
Refresh	Click it to refresh the web page immediately.
Auto Refresh	The system will refresh the web after specified time automatically.
Display	Specify how many records will be displayed in this page.
Type	Display the type (processing or finished) of the event.
Date	Display the date and time of the event occurred.
Device	Display the name of the access point.
Action	Display the action executed for the access point.
Message	Display the detailed execution process.

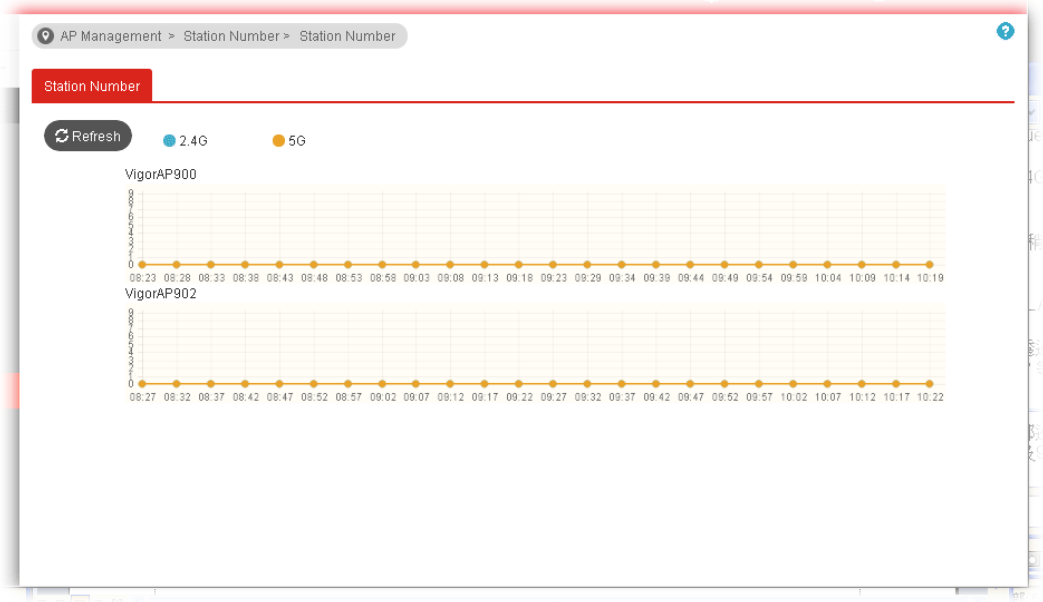
4.17.10 Total Traffic

Such page will display the total traffic of data receiving and data transmitting for VigorAPs managed by Vigor router.



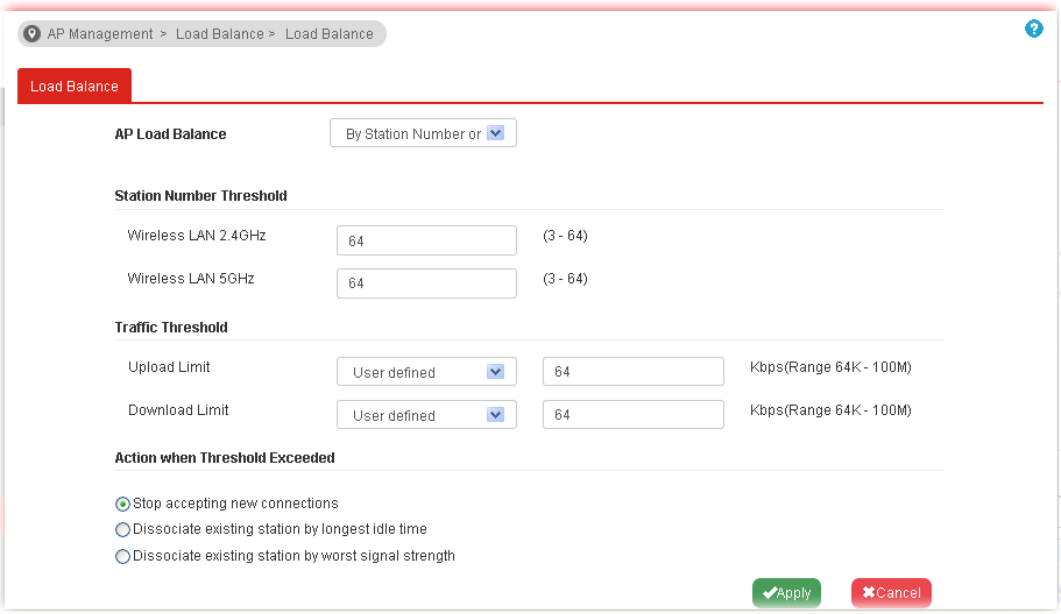
4.17.11 Station Number

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.



4.17.12 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:

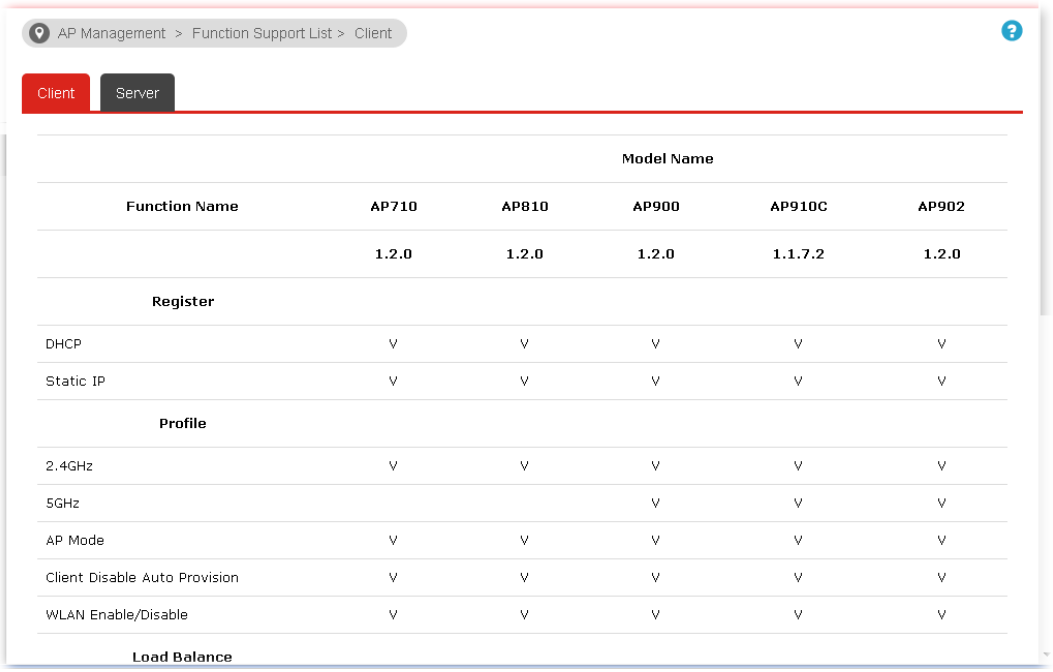
Item	Description
AP Load Balance	It is used to determine the operation mode when the system detects overload between access points. **By Station Number** –The operation of load balance will be executed based on the station number configured in this page. It is used to limit the allowed number for the 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. **By Traffics** – The operation of load balance will be executed according to the traffic configuration in this page. **By Station Numbers or Traffics** - The operation of load balance will be executed by station number or traffic by the system automatically.
Station Number Threshold	Please define the required station number for WLAN (2.4GHz) and WLAN (5GHz) separately.
Traffic Threshold	**Upload Limit** –Use the drop down list to specify the traffic limit for uploading. **Download Limit** – Use the drop down list to specify the traffic limit for downloading.
Action when Threshold Exceeded	**Stop accepting new connections –** When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate any new connection

Item	Description
	requested by client's station. **Dissociate existing station by longest idle time** - When the access point is overload (e.g., reaching the limit of station number or limit of network traffic), it will terminate the network connection of the client's station which is idle for a longest time. **Dissociate existing station by worst signal strength** - 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.
Apply	Click it to save the configuration.

4.17.13 Function Support List

Click the **Client** tab to list the AP management functions that the Access Points support under different firmware versions.

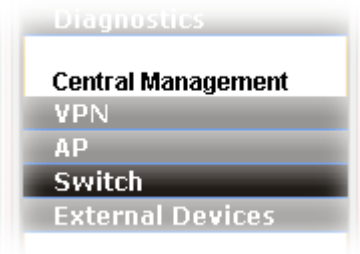
Click the **Server** tab to list the AP management functions that Vigor router supports under different firmware versions.



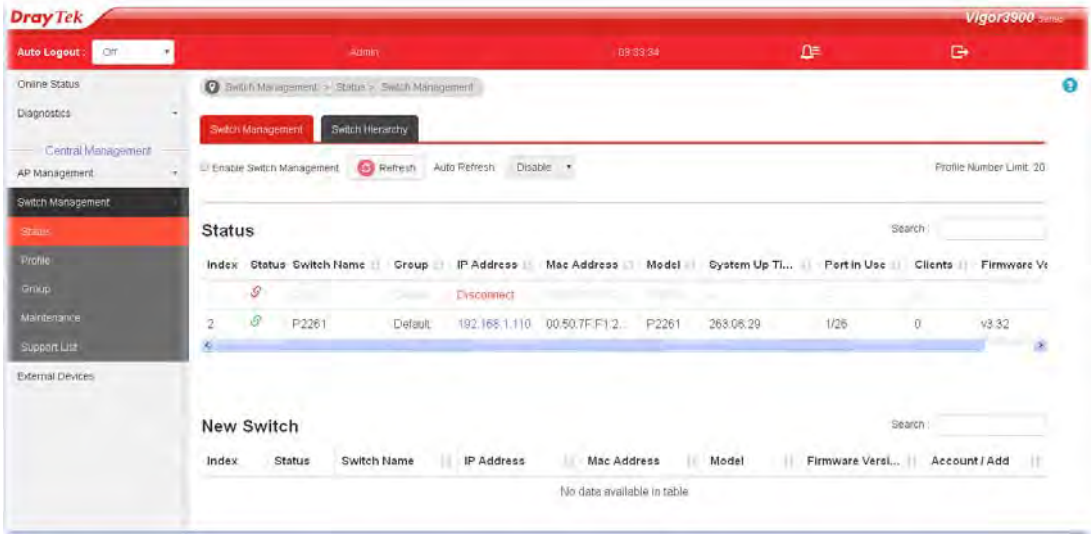
	Model Name				
Function Name	**AP710**	**AP810**	**AP900**	**AP910C**	**AP902**
	1.2.0	**1.2.0**	**1.2.0**	**1.1.7.2**	**1.2.0**
Register					
DHCP	V	V	V	V	V
Static IP	V	V	V	V	V
Profile					
2.4GHz	V	V	V	V	V
5GHz			V	V	V
AP Mode	V	V	V	V	V
Client Disable Auto Provision	V	V	V	V	V
WLAN Enable/Disable	V	V	V	V	V
Load Balance					

4.18 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. Before using such menu, please enable **External Devices Auto Discovery on External Devices** first.



Click **Central Management>>Switch** to open configuration pages in new designed web pages. They are suitable and easy to browse on network for PC users and mobile users.



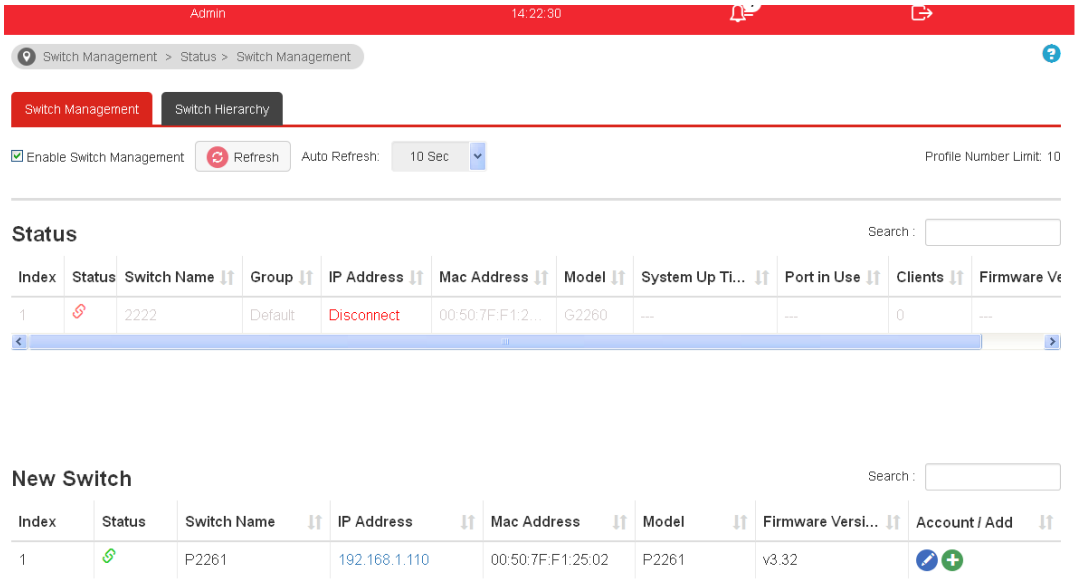
Menu items related to **Switch** are Status, Profile, Group, Maintenance and Support List.

4.18.1 Status

4.18.1.1 Switch Management

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** Vigor3900 series.

VigorSwitch listed below **Status** means the switch is managed by Viogr3900; a VigorSwitch listed below **New Switch** means it is not managed by Vigor3900 yet.



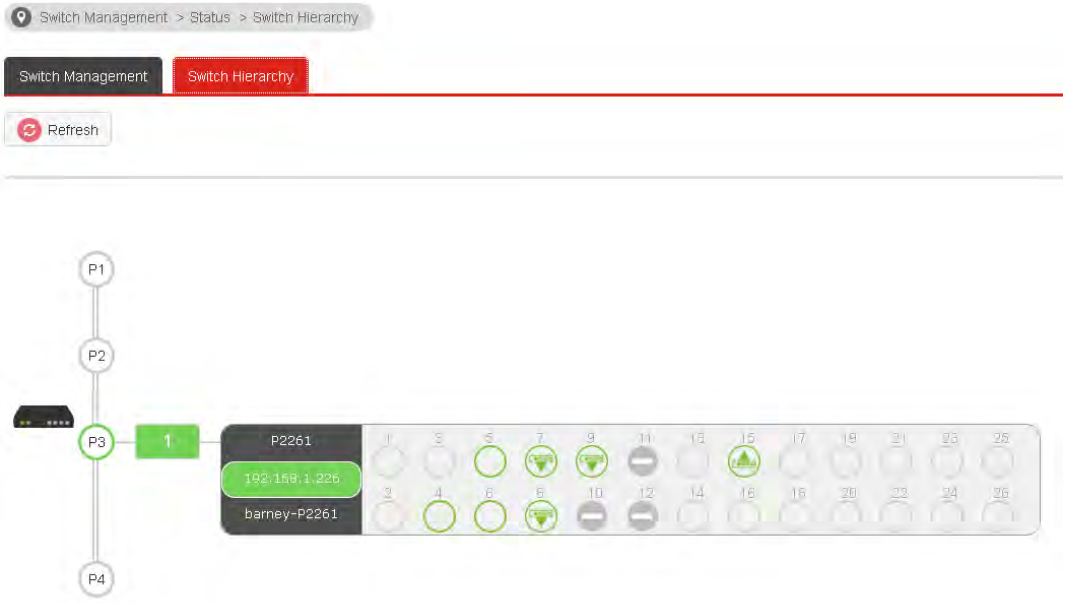
Each item will be explained as follows:

Item	Description
Enable Switch Management	Check the box to enable switch management.
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Status	**Status –** Green icon means the VigorSwitch does connect to Vigor3900 and is managed by Vigor3900. Grey icon means Vigor3900 is detecting such VigorSwitch still. Red icon means Vigor3900 cannot access it to get status information for accessing password configuration of VigorSwitch is wrong or Telnet service is disabled. **Switch Name –** Display the name of VigorSwitch. **Group –** Display the name of the group. **IP Address –** Display the IP address link of VigorSwitch. You can click the link to access into the web user interface of VigorSwitch. **Mac Address –** Display the MAC 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 the number of LAN ports used in VigorSwitch. **Clients –**Display how many devices connected to VigorSwitch. **Firmware Version** - Display the firmware version that VigorSwitch current used.

New Switch	**Status –**Green icon means the VigorSwitch does connect to Vigor3900 and is managed by Vigor3900. Grey icon means Vigor3900 is detecting such VigorSwitch still. Red icon means Vigor3900 cannot access it to get status information for accessing password configuration of VigorSwitch is wrong or Telnet service is disabled. **Switch Name –** Display the name of VigorSwitch. **IP Address –** Display the IP address link of VigorSwitch. You can click the link to access into the web user interface of VigorSwitch. **Mac Address –** Display the MAC address of VigorSwitch. **Model –** Display the model name of VigorSwitch. **Firmware Version –** Display the firmware version that VigorSwitch current used. **Account -** It is used to change the password for accessing into VigorSwitch. **Add –** Click it to make the selected VigorSwitch be managed by Vigor3900.

4.18.1.1 Switch Hierarchy

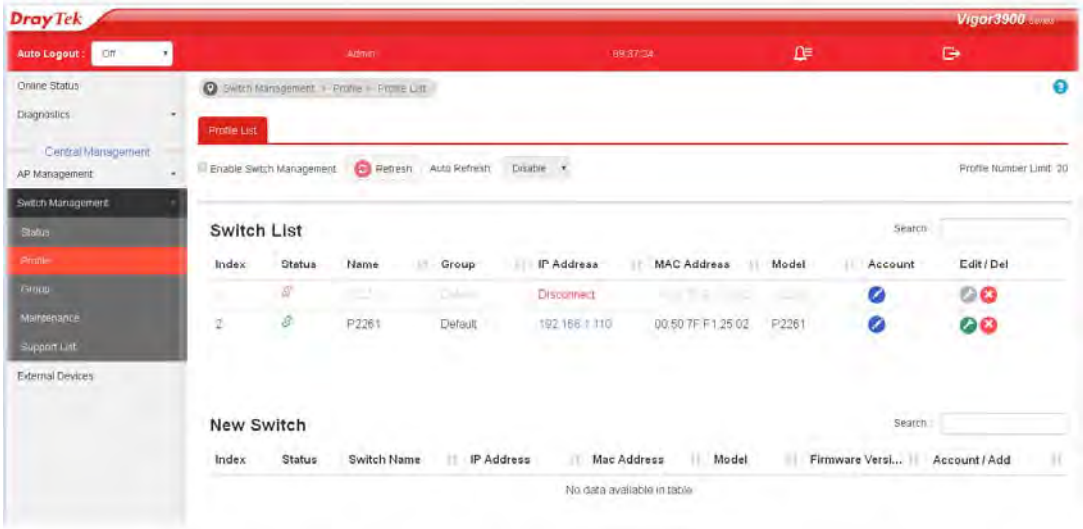
Such page displays the hierarchy of VigorSwitch(es) managed under Vigor3900.



Note: If the hierarchy display is incorrect, please access into the web user interface of VigorSwitch and enable the function of LLDP (e.g., Configuration >>DDLP>>LLDP General Setup in VigorSwitch 2261). The interval for LLDP shall be less than 3 minutes (the default setting, 30 seconds).

4.18.2 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 Vigor3900 series. By clicking the edit button, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.



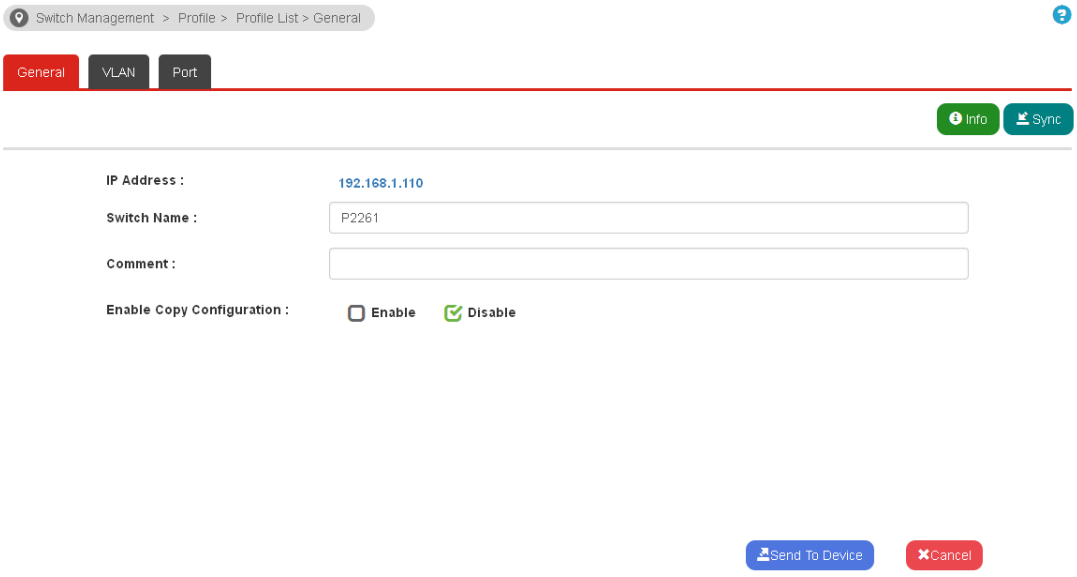
Each item will be explained as follows:

Item	Description
Enable Switch Management	Check the box to enable switch management.
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Switch List	**Status –** Green icon means the VigorSwitch does connect to Vigor3900 and is managed by Vigor3900. Grey icon means Vigor3900 is detecting such VigorSwitch still. Red icon means Vigor3900 cannot access it to get status information for accessing password configuration of VigorSwitch is wrong or Telnet service is disabled. **Switch Name –** Display the name of VigorSwitch. **Group –** Display the name of the group. **IP Address –** Display the IP address link of VigorSwitch. You can click the link to access into the web user interface of VigorSwitch. **Mac Address –** Display the MAC address of VigorSwitch. **Model –** Display the model name of VigorSwitch. **Account -** It is used to change the password for accessing into VigorSwitch. **Edit –** It is used to change general settings for the selected VigorSwitch. **Del –** It is used to remove the profiles for the selected

	VigorSwitch.
New Switch	**Status –**Green icon means the VigorSwitch does connect to Vigor3900 and is managed by Vigor3900. Grey icon means Vigor3900 is detecting such VigorSwitch still. Red icon means Vigor3900 cannot access it to get status information for accessing password configuration of VigorSwitch is wrong or Telnet service is disabled. **Switch Name –** Display the name of VigorSwitch. **IP Address –** Display the IP address link of VigorSwitch. You can click the link to access into the web user interface of VigorSwitch. **Mac Address –** Display the MAC address of VigorSwitch. **Model –** Display the model name of VigorSwitch. **Firmware Version –** Display the firmware version that VigorSwitch current used. **Account -** It is used to change the password for accessing into VigorSwitch. **Add -** The one under New Switch List is allowed to be managed under current used group.

How to Edit the VigorSwitch Profile

From the Switch List, choose the one you want to edit and then click the **Edit** icon to open the following page. The original settings configured in VigorSwitch will be displayed as follows:

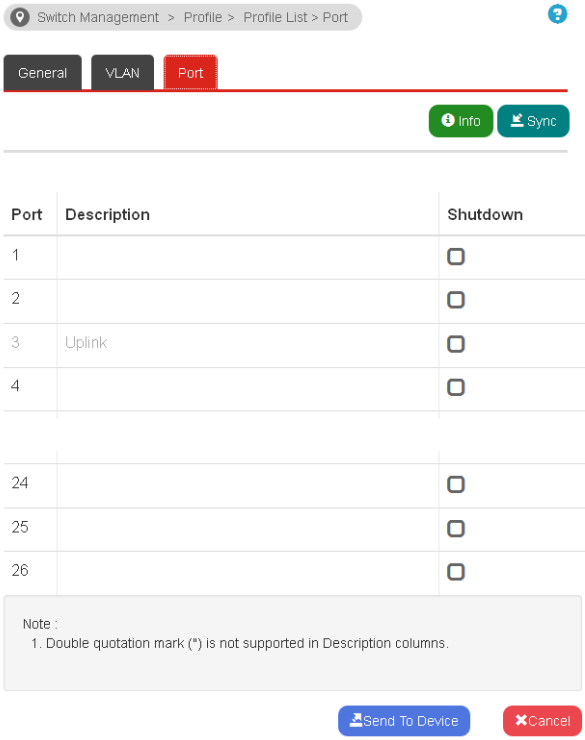


Item	Description
Info	Display the basic information of selected VigorSwitch.
sync	Click the button to download configuration settings of VigorSwitch to be used by Switch Management.
IP Address	The IP address of VigorSwitch will be displayed automatically.

Switch Name	Name of VigorSwitch will be displayed here automatically.
Comment	Type any description for such switch if required.
Enable Copy Configuration	Check Enable to activate such function.
Send to Device	Current setting will be saved. Meanwhile, the configuration in VigorSwitch also will be rewritten immediately.

Type new values and click **Send to Device** for saving the configurations.

Then, click the **Port** tab to change the port setting if required.



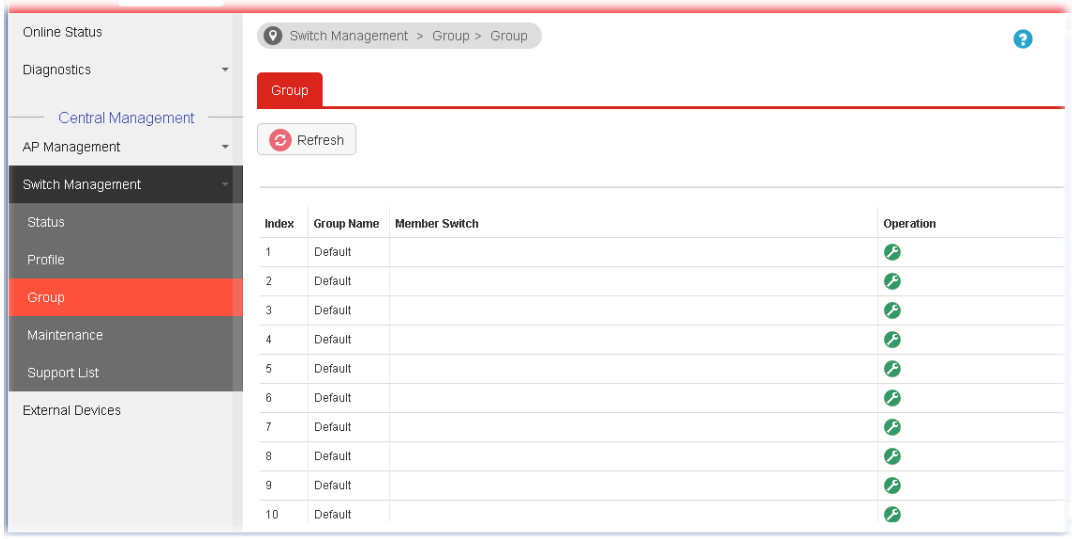
After finished the port configuration, click the VLAN tab to modify settings relevant to VLAN.

General
VLAN
Port
Info
Sync
port
Remove Tag (PVID)
vid : 1
vid : 10
un-tag
Note
1. The router configuration will be updated when getting profile settings from external switch.
2. Switch management is currently support up to 9 Vlan id(vid).
Send To Device
Cancel

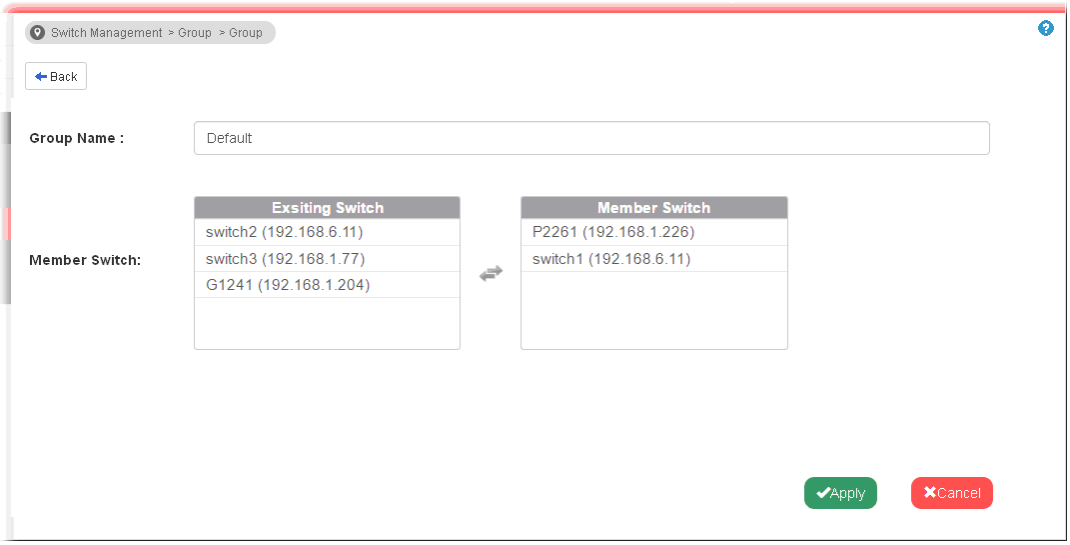
4.18.3 Group

Different switches can be classified into different group(s).

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 the icon under **Operation** to create/edit a switch group.



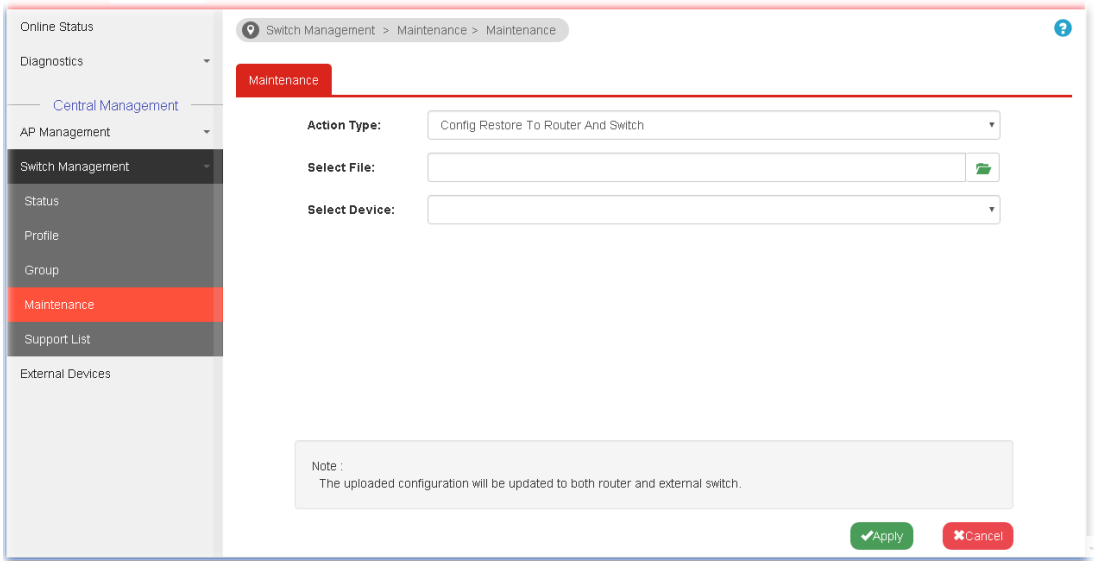
Available settings are explained as follows:

Item	Description
Group Name	Type a name as the group name. Different switches can be classified within a group.
Existing Switch	Display all of the VigorSwitch devices connecting to Vigor3900.
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.

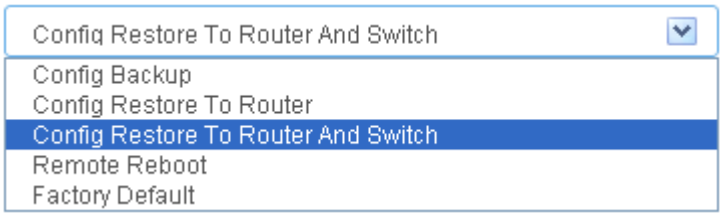
Apply	Click it to save the configuration.
Cancel	Click it to exit the setting page without saving any change.

4.18.4 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.

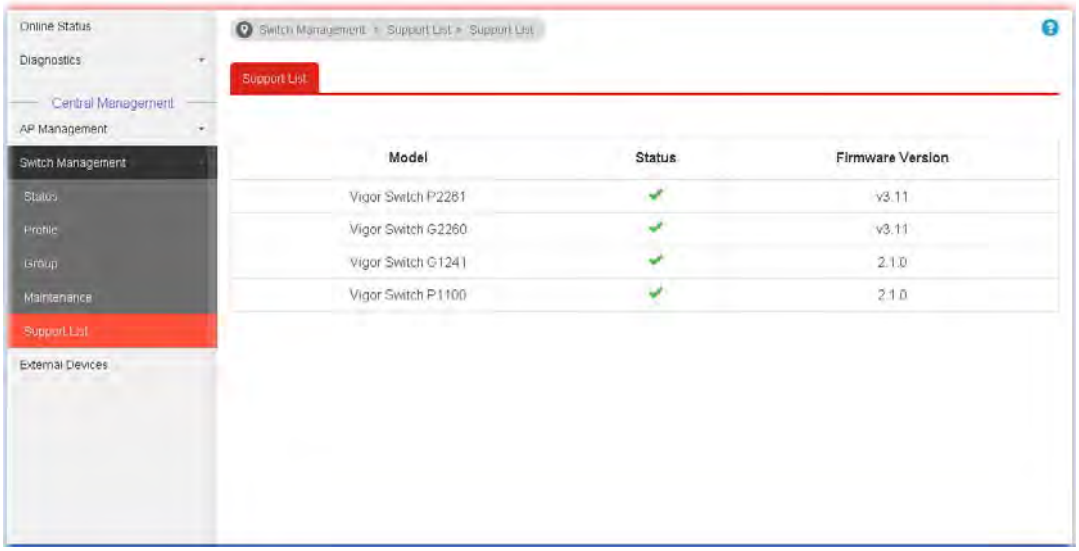


Available settings are explained as follows:

Item	Description
Action Type	Five actions including configuration backup, configuration restore, configuration restore to router and switch, remote reboot and factory reset are offered by Vigor3900 to perform on VigorSwitch. 
Select File	Click to find out the required file. Such option is available when **Config Restore To Router / Config Restore To Router And Switch** is selected as Action Type.
Select Device	Choose the switch to be applied with the action
Apply	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.

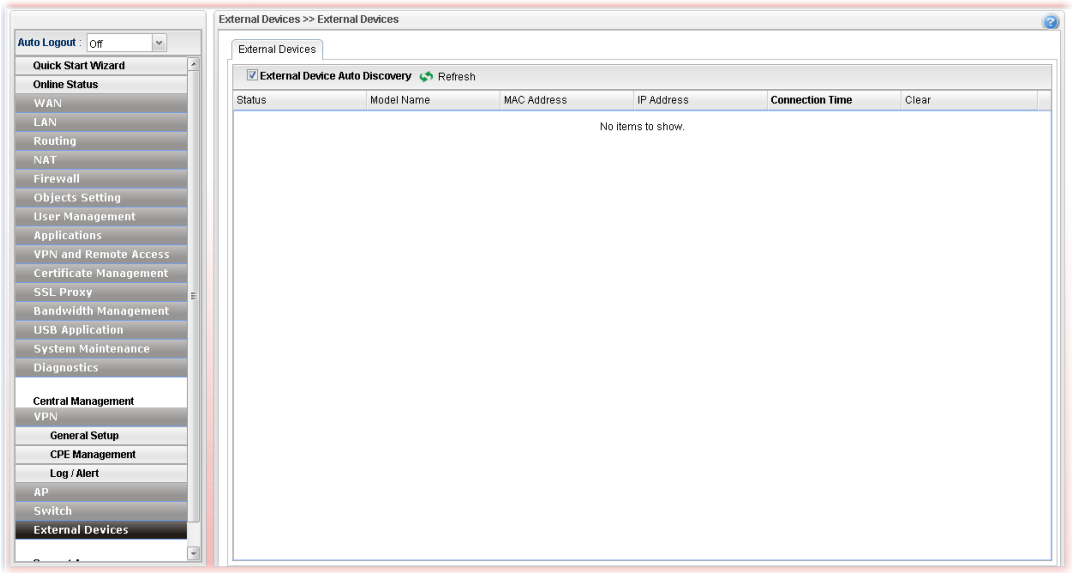
4.18.5 Support List

This page lists all models of VigorSwitch which can be managed by Vigor3900 via Switch Management.



4.19 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.



Each item will be explained as follows:

Item	Description
Enable External Devices	Check the box to detect the external device connected to Vigor3900.
Refresh	Click it to renew the web page.
Model Name	Display the model name of the external product.
MAC Address	Display the MAC address of the external product.
IP Address	Display the IP address of the external product.
Connection Time	Display the connection time that the external product connecting to Vigor3900.
Clear	Allow to delete the selected profile. Click the icon to remove the record of the device when it is offline.

From this web page, check the box of **Enable External Devices**. 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.

> **Note**: Only DrayTek products can be detected by this function.

4.20 Product Registration

Please refer to section **2.3 Register Vigor Router** for more detailed information.

This page is left blank.

Chapter 5: Trouble Shooting

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.

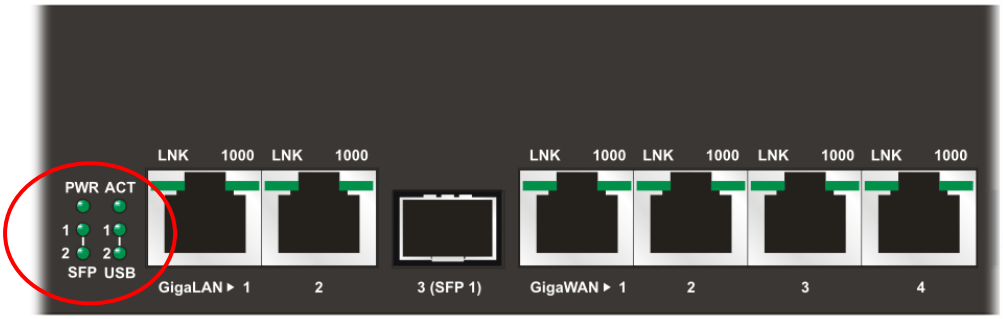
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check if the power line and WLAN/LAN cable connections is OK.
   If not, refer to "**1.3 Hardware Installation"** for reconnection.
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 **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

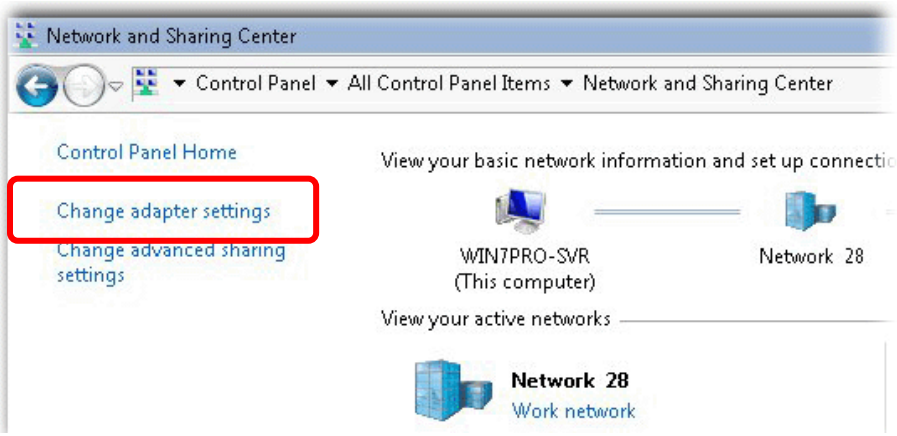
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

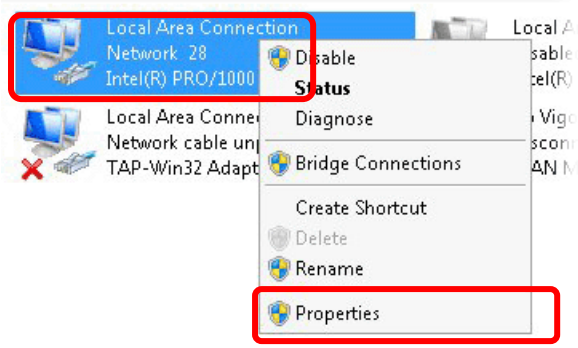
> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**

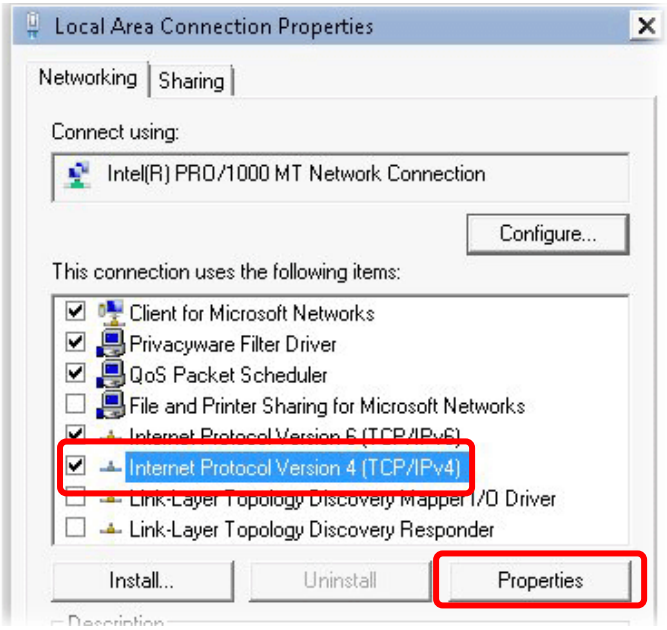
2. In the following window, click **Change adapter settings**.



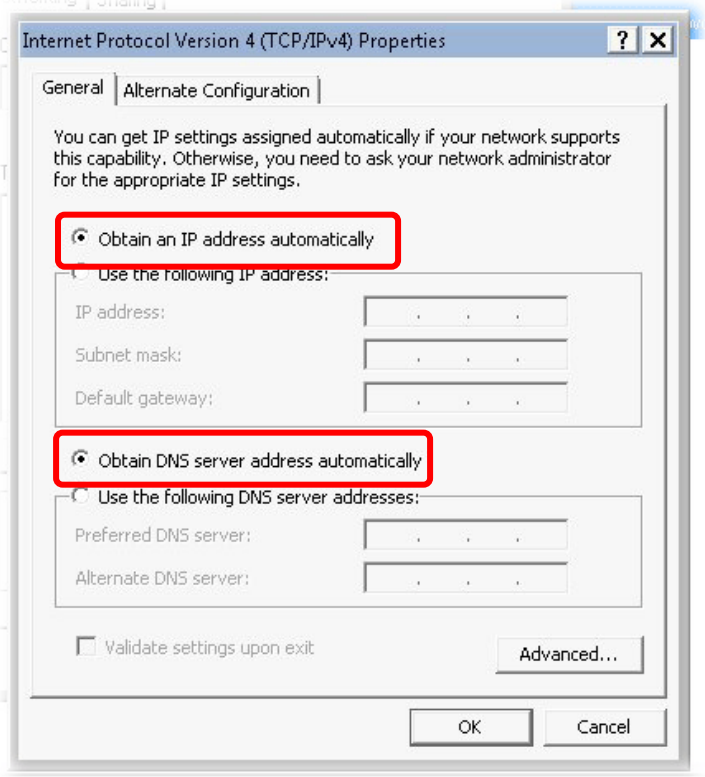
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

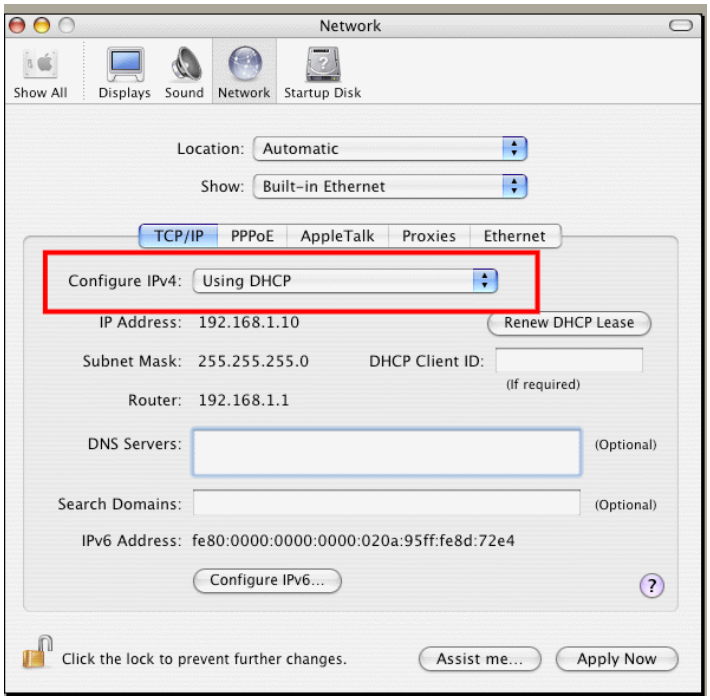


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



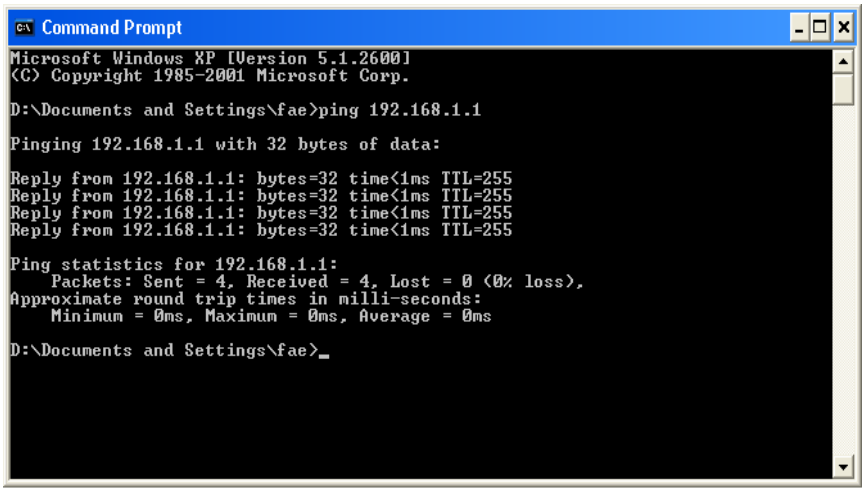
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

For Windows

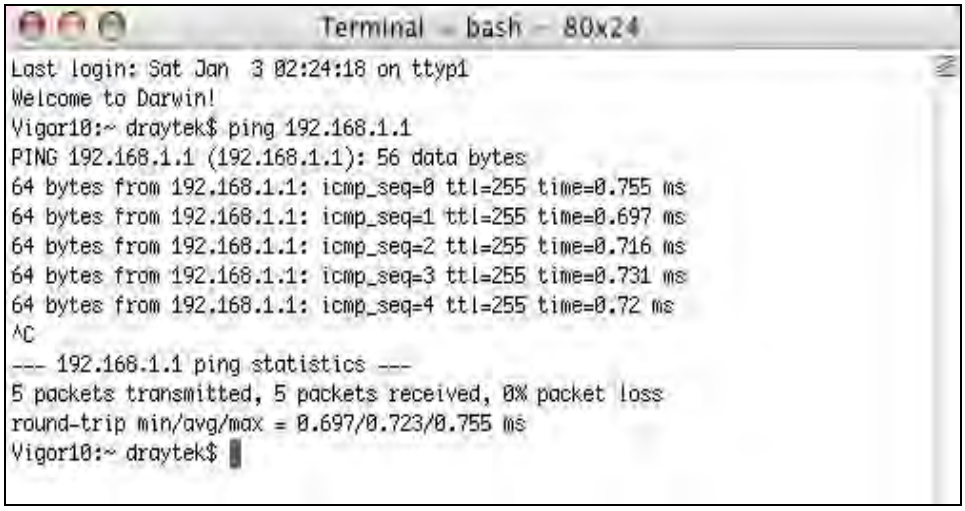
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista/7). The DOS command dialog will appear.



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.

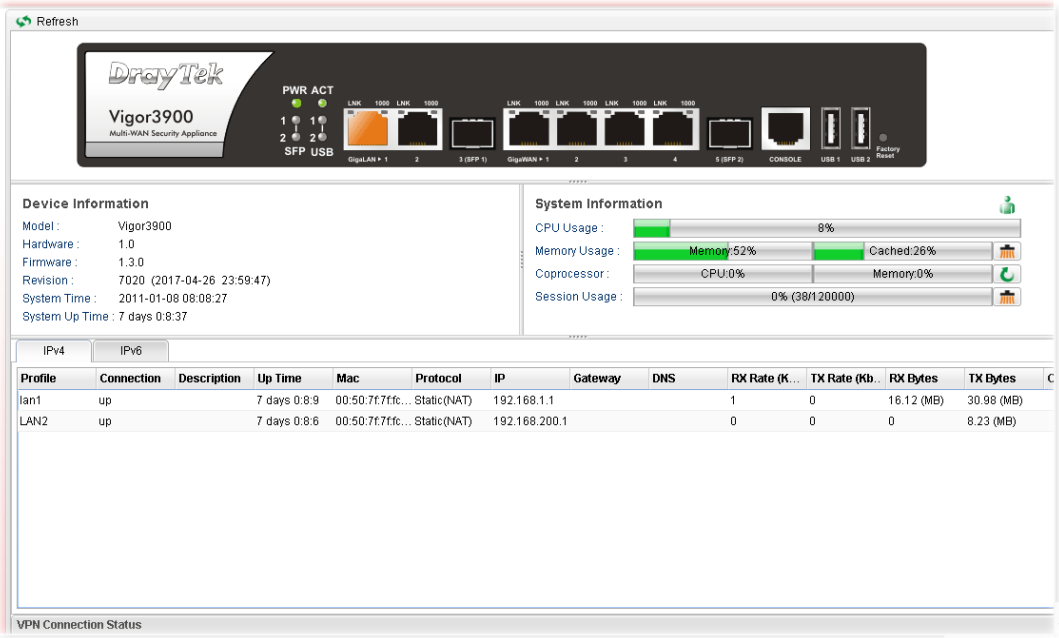
For Mac OS (Terminal)

1. Double click on the current used Mac OS 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.

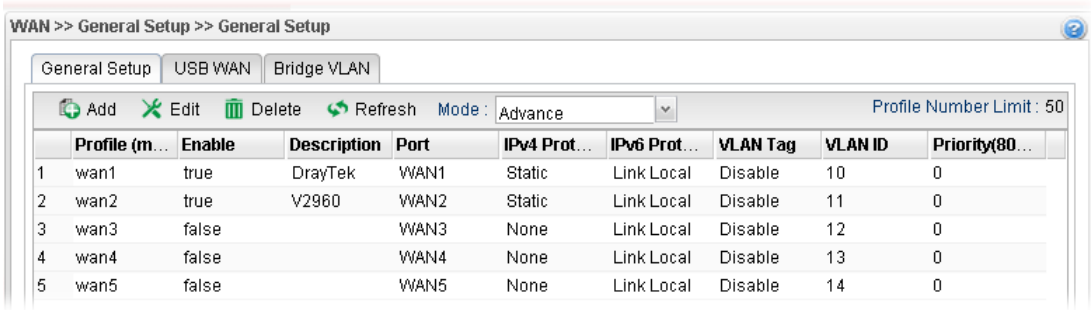


5.4 Checking If the ISP Settings are OK or Not

Open Online Status to check current network status. Be careful to check if the settings coming from your ISP have been typed correctly or not.



If there is something wrong with the configuration, please go to **WAN** page and choose **General Setup** again to modify the WAN connection.



5.5 Backing to Factory Default Setting If Necessary

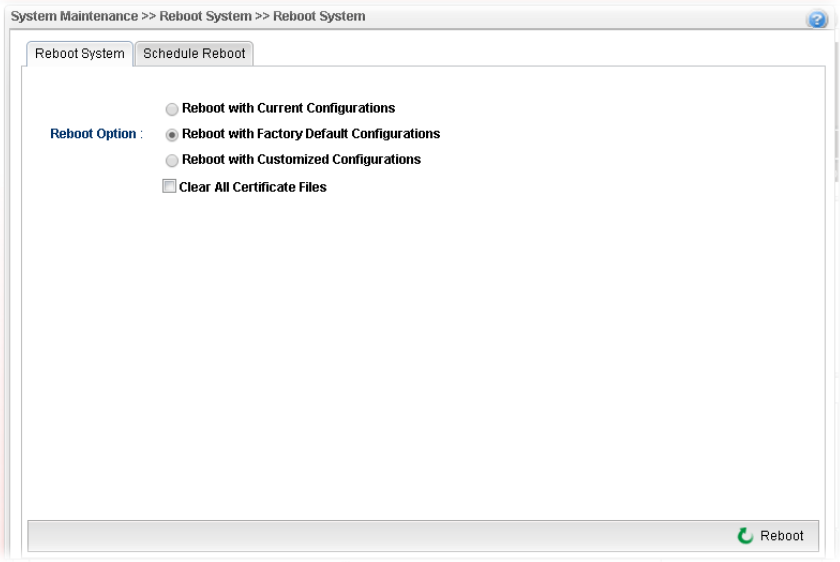
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of the factory default is null.

Software Reset

You can reset router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Reboot with Factory Default Configuration** and click **Reboot**. 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.

5.6 Contacting DrayTek

If the router settings are correct at all, and the router still does not connect to internet, please contact your ISP technical support representative to help you for configuration.

Also, if the router still cannot work correctly, please contact your dealer for help. For any further questions, please send e-mail to **support@draytek.com.**

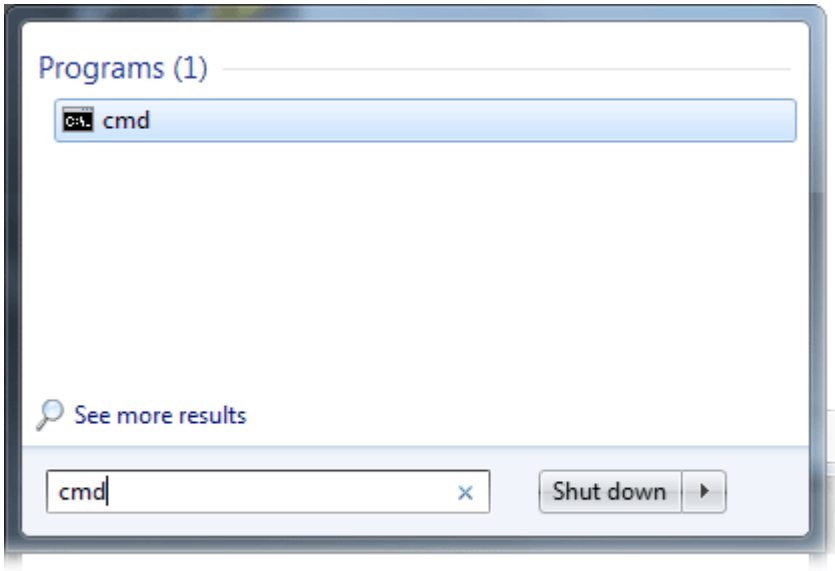
Chapter 6: Telnet Commands

6.1 Accessing Telnet of Vigor Router

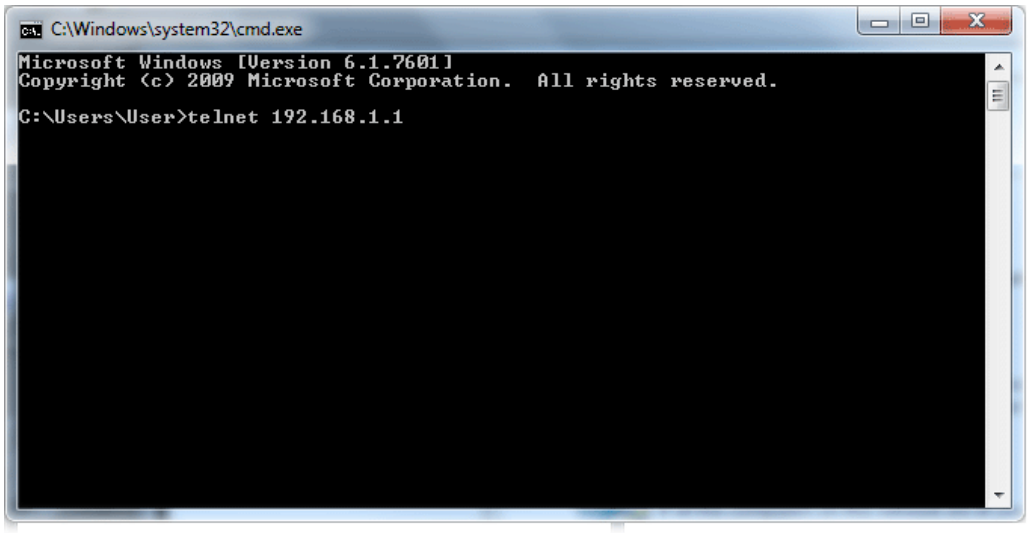
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

Info	For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under **Control Panel>>Programs**.

Type **cmd** and press Enter. The Telnet terminal will be open later.

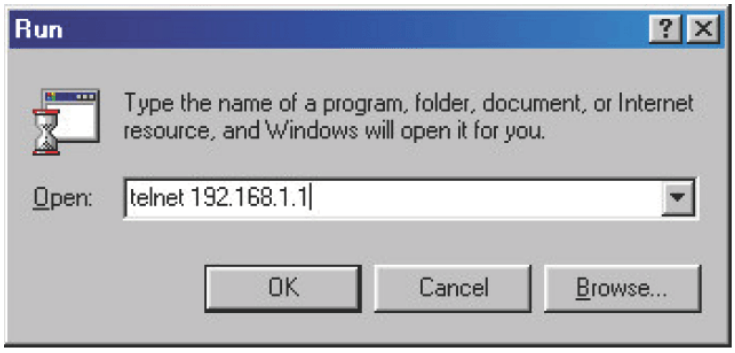


In the following window, type **Telnet 192.168.1.1** as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.

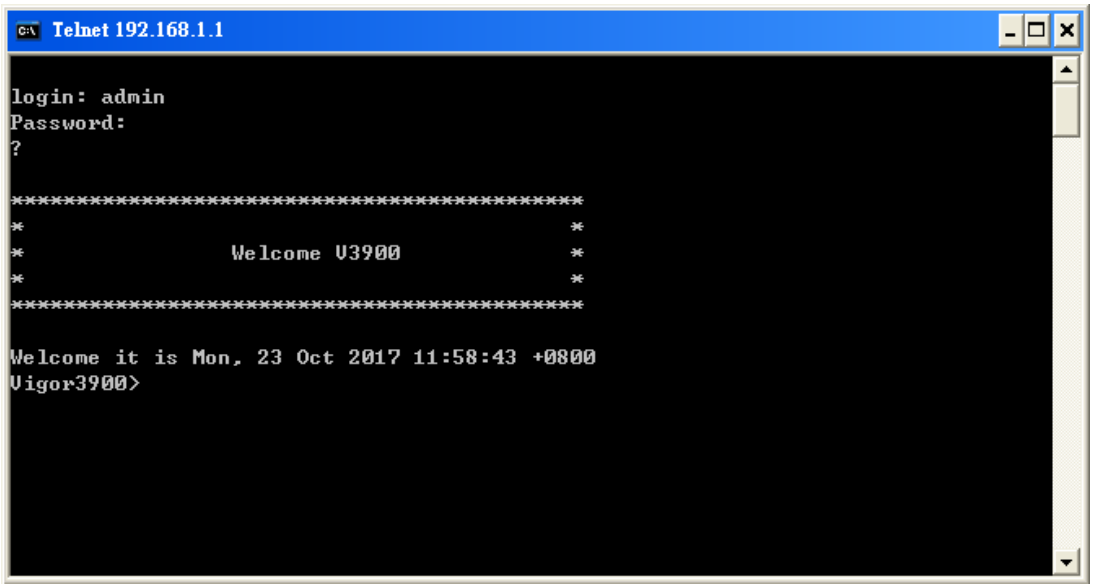


Next, type admin/admin for Account/Password.

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.

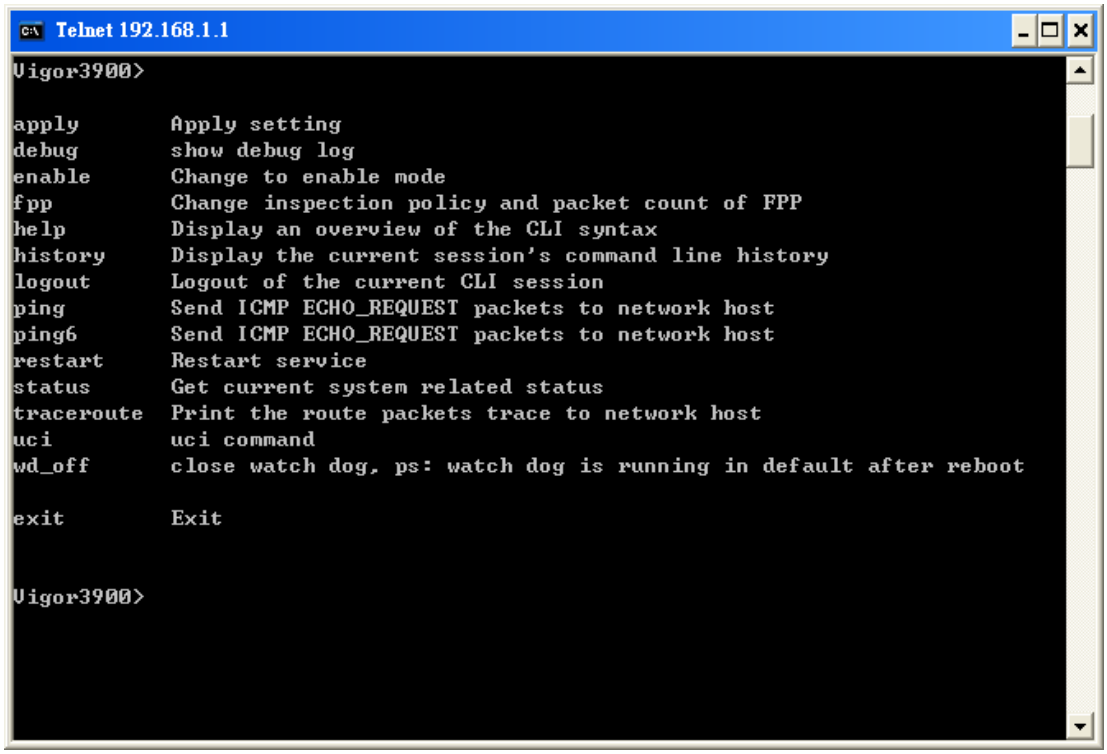


Next, type admin/admin for Account/Password.



6.2 Global Commands

Type **?** to get a list of global commands.



Global Commands contains - apply, enable, fpp, help, history, logout, ping, ping6, restart, status, traceroute, uci, wd_off and exit. Each command will be explained as follows.

Telnet Command: apply

This command is used for applying settings/modifications onto Vigor router. To configure, create, delete, or edit any command, type this command to activate the configuration.

Syntax

Vigor3900>apply *[config]*

Vigor3900>apply *[config name]*

Command	Description
[config / config name]	Type the name of the configuration, e.g., "appuser" (means application user profile).

Example

```
Vigor3900> apply appuser
```

Telnet Command: enable

This command is used for changing current status into "enable" mode. Next, the configuration commands (including applications, bandwidth, fw, nat, object_setting, system terminal, user, vpn and etc.,) can be seen and used only when the enable command is used first.

To leave "enable" mode, simply type "exit".

Syntax

Vigor3900>enable

Example

```
Vigor3900> enable
Entering enable mode...
Vigor3900# exit
Leaving enable mode...
Vigor3900>
```

Telnet Command: fpp

This command can change inspection policy and packet count for default policy.

Syntax

Vigor3900>fpp *[inspection] [packets]*

Command	Description
[inspection]	Set 1 to enable inspection based on user-defined packet number. Set 0 to make inspection based on default packet number.
[packets]	Set the number of packets needed to be inspected.

Example

```
Vigor3900> fpp
fpp [inspection] [packets]
Vigor3900> fpp 1 1000
Set inspection : 1
Set packets    : 1000
```

Telnet Command: help

This command is used for displaying an overview of CLI syntax.

Syntax

Vigor3900>help

Example

```
Vigor3900> help
CONTEXT SENSITIVE HELP
[?] - Display context sensitive help. This is either a list of possible
      command completions with summaries, or the full syntax of the
      current command. A subsequent repeat of this key, when a command
      has been resolved, will display a detailed reference.

AUTO-COMPLETION
The following keys both perform auto-completion for the current command
line.
If the command prefix is not unique then the bell will ring and a
subsequent repeat of the key will display possible completions.
```

```
[enter] - Auto-completes, syntax-checks then executes a command. If
there is a syntax error then offending part of the command line will
be highlighted and explained.
.
.
.
.
```

Telnet Command: history

This command can display current session command line history.

Syntax

Vigor3900>history

Example

```
Vigor3900> history
   1  status
   2  status conn_num
   4  status dhcp host ID
   5  status dhcp
   6  status firewall
   7  status interface
   8  status lan
   9  status wan
  10  status vpn
  11  status system
  12  status switch
  13  status switch lan
  14  status switch wan
  15  status route
  16  status route6
Vigor3900>
```

Telnet Command: logout

This command is used for logout of current CLI session.

Syntax

Vigor3900>logout

Example

```
Vigor3900> logout
login: admin
Password:
Vigor3900>
```

Telnet Command: ping

This command can send ICMP ECHO_REQUEST packets to network host (with IPv4 address).

Syntax

Vigor3900>ping *[host] [src_if]*

Command	Description
[host]	Type the IP address of the host for pinging.
[src_if]	Specify the interface (wan1 or wan2) to execute pinging. This is optional setting.

Example

```
Vigor3900> ping 6
PING 6 (0.0.0.6): 56 data bytes
ping: sendto: Network is unreachable
Send ICMP ECHO_REQUEST packets done.
Vigor3900> ping 8.8.8.8 wan2
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=56 time=11.3 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=10.6 ms
```

Telnet Command: ping6

This command can send ICMP ECHO_REQUEST packets to network host (with IPv6 address).

Syntax

Vigor3900>ping6 *[host] [src_if] [count] [ping_size] [quiet]*

Command	Description
[host]	Type the IPv6 address of the host for pinging.
[src_if]	Specify the interface (wan1 or wan2) to execute pinging. This is optional setting.
[count]	Set the number of the packets for pinging.
[ping_size]	Set the packet size for pinging.
[quiet]	Type “true” to display the pinging result only for all packets. If this parameter is not used, the pinging result for each packet will be displayed completely.

Example

```
Vigor3900>ping6
ping6 [host] [src_if] [count] [ping_size] [quiet]
Vigor3900> ping6 2001:b000:168::1 wan2 3
PING 2001:b000:168::1(2001:b000:168::1) from
2001:b011:700a:1a62:940:1a4d:7eb:1e3a : 56 data bytes
64 bytes from 2001:b000:168::1: icmp_seq=1 ttl=248 time=9.32 ms
64 bytes from 2001:b000:168::1: icmp_seq=2 ttl=248 time=5.50 ms
64 bytes from 2001:b000:168::1: icmp_seq=3 ttl=248 time=5.46 ms

--- 2001:b000:168::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.467/6.766/9.328/1.811 ms
```

```
Send ICMP ECHO_REQUEST packets done.
Vigor3900>
Vigor3900>
Vigor3900> ping6 2001:b000:168::1 wan2 3 50 true
PING 2001:b000:168::1(2001:b000:168::1) from
2001:b011:700a:1a62:940:1a4d:7eb:1e3a : 50 data bytes

--- 2001:b000:168::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 5.467/5.534/5.588/0.050 ms
Send ICMP ECHO_REQUEST packets done.
Vigor3900>
```

Telnet Command: restart

This command can activate service of DDNS, DHCP, DHCP6, DNS Proxy, FPP, HTTP, IPsec, PPTPD, SSH and xl2tpd by restarting Vigor router.

Syntax

Vigor3900>restart *[service]*

Command	Description
[service]	Type the following string to represent different services: ddns, dhcp, dhcp6, dns_proxy, fpp, http, ipsec, pptpd, ssh, xl2tpd

Example

```
Vigor3900> restart
Restart [service]
```

Telnet Command: status

This command can get current system status related to ARP, conn, conn_num, conntract, dhcp, firewall, interface, lan, neighbor6, process, route, route6, switch, system, vpn, and wan.

Syntax

Vigor3900>status arp / conn / conn_num /contract / dhcp / firewall / interface / lan / neighbor6 / process / route / route6 / switch / system / vpn / wan

Command	Description
Arp	Display ARP status.
conn	Display conntrack (connection tracking session) for specified source/destination IP.
conn_num	Display the total session number.
conntract	Display real-time session status. You can type “ctrl+c” to exit the dialog.
dhcp	Display DHCP active session situation including IP address, start time, end time, MAC address and Host ID.
firewall	Display current firewall status.

interface	Display information about interface (e.g., eth0, eth2, lan-lan1 and local loopback).
lan	Display status information for LAN.
neighbor6	Display information about current IPv6 neighbor table.
process	Display process information that Vigor router is performing.
route	Display route information (IPv4).
route6	Display route information (IPv6).
switch	Switch lan – Display current status for switch in LAN port. Switch wan – Display current status for switch in WAN port.
system	Display basic system status information.
vpn	Display information for VPN connection status.
wan	Display status information for WAN.

Example

```
Vigor3900> status arp
IP Address     HW Type MAC Address      Flags           Profile
User
    Netbios Name Vendor
192.168.1.10    ether   00:05:5d:e4:d8:ee C              lan-lan1
NA
    NA          D-Link
Vigor3900>status contract
IPTState - IPTables State Top
Version: 2.2.3 Sort: SrcIP b: change sorting h: help
Total States: 176 -- TCP: 116 UDP: 31 ICMP: 3 Other: 1 (Filtered: 25)
Source Destination Interface Protocol State TTL Class
10.10.1.11:43665 108.177.125.188:5228 wan-wan2 tcp ESTABLISHED
0:00:43 Normal
10.10.1.11:43724 216.58.200.232:443 wan-wan2 tcp ESTABLISHED 0:00:46
Normal
10.10.1.11:46635 111.13.142.2:5222 wan-wan2 tcp ESTABLISHED 21:51:50
Normal
10.10.1.11:48702 120.92.96.2:5222 wan-wan2 tcp ESTABLISHED 0:05:55
Normal
10.10.1.11:42280 64.233.188.188:5228 wan-wan2 tcp ESTABLISHED 0:09:08
Normal
10.10.1.11:40372 203.205.151.233:443 wan-wan2 tcp ESTABLISHED 0:09:44
Normal
10.10.1.11:49130 122.248.234.207:8080 wan-wan2 tcp ESTABLISHED
21:34:20 Normal
10.10.1.11:45699 111.13.142.2:5222 wan-wan2 tcp ESTABLISHED 21:09:54
Normal
.
.
Vigor3900> status vpn

VPN Name : ipsec2_out
Remote IP : 1.169.175.175
Virtual Network : 11.11.2.0/24
Algorithm : IPsec/3DES_HMAC_MD5
```

```
Up Time : 0 days 6 hours 0 minutes 42 seconds
Transmitted : 2540480 packets
Received : 1568532 packets
```

Telnet Command: traceroute

This command can print the route packets trace to network host.

Syntax

Vigor3900> traceroute *[host][src_if]*

Command	Description
[host]	Type the IPv6 address of the host for pinging.
[src_if]	Specify the interface (wan1 or wan2) to execute pinging. This is optional setting.

Example

```
Vigor3900> traceroute 8.8.8.8 wan2
traceroute to 8.8.8.8 (8.8.8.8) from 172.17.5.194, 30 hops max, 38 byte
packets
 1  172.17.5.5 (172.17.5.5)  1.614 ms  1.553 ms  1.374 ms
 2  h254.s98.ts.hinet.net (168.95.98.254)  6.257 ms  5.992 ms  5.980
ms
 3  sczs-3312.hinet.net (168.95.25.210)  6.103 ms  6.004 ms  245.245
ms
 4  sczs-3201.hinet.net (220.128.8.246)  6.294 ms
sczs-3202.hinet.net (220.128.8.254)  6.302 ms sczs-3201.hinet.net
(220.128.8.246)  17.018
ms
 5  TPDT-3012.hinet.net (220.128.2.30)  8.072 ms TPDT-3011.hinet.net
(220.128.1.30)  10.666 ms TPDT-3012.hinet.net (220.128.2.150)
11.229 m
s
 6  220-128-25-182.hinet-ip.hinet.net (220.128.25.182)  8.257 ms
417.435 ms  10.486 ms
 7  220-128-3-34.hinet-ip.hinet.net (220.128.3.34)  9.224 ms
pcpd-3212.hinet.net (220.128.27.77)  8.684 ms pcpd-3211.hinet.net
(220.128.26.7
7)  7.675 ms
 8  72.14.202.178 (72.14.202.178)  7.998 ms 72.14.202.34
(72.14.202.34)  9.311 ms pcpd-3211.hinet.net (220.128.26.77)  8.774
ms
 9  72.14.202.178 (72.14.202.178)  404.354 ms 72.14.202.34
(72.14.202.34)  8.214 ms  8.213 ms
10  72.14.238.125 (72.14.238.125)  8.662 ms 72.14.238.97
(72.14.238.97)  8.362 ms 108.170.244.129 (108.170.244.129)  13.026 ms
11  216.239.63.75 (216.239.63.75)  8.485 ms
google-public-dns-a.google.com (8.8.8.8)  10.766 ms  339.871 ms
Traceroute done.
Vigor3900#
```

Telnet Command: uci

This command is used for RD debug.

Telnet Command: wd_off

This command can close watch dog (which is running in default after reboot).

Syntax

Vigor3900>wd_off

Example

```
Vigor3900> wd_off
Watch Dog Closed
Vigor3900>
```

Telnet Command: exit

This command can exit telnet command dialog or return to previous command layer.

Syntax

Vigor3900>exit

Example

```
Vigor3900> enable
Entering enable mode...
Vigor3900# exit
Leaving enable mode...
Vigor3900>
```

6.3 Available Configure Commands

Main parameter settings can be configured only "**enable**" mode is set first.

Command	Description

applications	Settings for DDNS, GVRP, HA (High availability), LDAP, OSPF, RIP, SAMBA service, SIP ALG, and UPnP can be configure with this command.
	`Vigor3900>enable`
	`Vigor3900# configure applications`
	`Vigor3900@config-app#`

bandwidth	Settings for access barrier, bandwidth limit profile, sessions limit profile can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure bandwidth`
	`Vigor3900@config-bandwidth#`

nat	Settings for address mapping, DMZ, and port redirection can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure nat`
	`Vigor3900@config-nat#`

object_setting	Settings for File Extension Object, IP Group, IP Object, Keyword Object, Service Group, Service Object, Time Group, Time Object and Web Category Object can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure object`
	`Vigor3900@config-object#`

system	Settings for Access Control, Administrator Password, Auto Discovery, Country Code, Fast Forward Conntrack module monitor, Configuration Backup and Restore, firmware management, Mail Alert, NTP client , System Reboot, SNMP agent, Syslog Server, and TR-069 can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure system`
	`Vigor3900@config-sys#`

terminal	Settings for LAN and WAN can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure terminal`
	`Vigor3900@config-t#`
	Refer to **section 6.4 (WAN) and section 6.5 (LAN)** for more detailed information.

user	Settings for user accounts and user groups can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure user`
	`Vigor3900@config-user#`

vpn	Settings for LAN to LAN, Remote Dial-In, and Trunk can be configured with such command.
	`Vigor3900>enable`
	`Vigor3900# configure vpn`
	`Vigor3900@config-vpn#`

6.4 WAN Configuration

To make WAN configuration, you have to type "*configure terminal*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#
..          Go back to upper layer menu
exit        Go back to main menu
lan         Configure lan profile
wan         Configure wan profile
Vigor3900@config-t# wan
Vigor3900@config-t-wan# ?
.
.
.
```

There are four functions for WAN – General Setup (command "pf"), Default Route, Load Balance (including load balancer pool, rule and auto load balance for china) and Switch.

Available sub-commands under WAN include:

- pf (refer to 6.4.1)

- defaultroute (refer to 6.4.2)

- lbpool (refer to 6.4.3)

- autolb (refer to 6.4.4)

- switch (refer to 6.4.5)

- 3g (refer to 6.4.6)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.4.1 Telnet Command: pf

It is used to configure WAN Profile to add or delete the profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#
Vigor3900@config-t# wan
Vigor3900@config-t-wan# pf add <SectionName>
Vigor3900@config-t-wan# pf delete <SectionName>
Vigor3900@config-t-wan# pf show
Vigor3900@config-t-wan# pf <SectionName>
```

Command	Description

pf add <SectionName>	Create a new WAN profile (without detailed settings) <SectionName> - Enter a name (e.g., wan_carrie) for creating a new WAN profile.
pf delete <SectionName>	Delete a WAN profile. <SectionName> - Enter a name (e.g., wan_carrie) to be removed.
pf show	Display configuration on WAN profile.
pf <SectionName>	Modify a selected WAN profile. <SectionName> - Enter the name of WAN profile to be modified.

Example

In this example, we create a WAN profile named with "wan_carrie".

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
```

6.4.1.1 Telnet Command: pf add ?

To configure detailed settings for a WAN profile, users could use [pf add] to create a new WAN profile **with detailed settings** in one line.

Syntax

```
Vigor3900@config-t-wan# pf add [status status] [wan4_dmz_status
wan4_dmz_status] [desc description] [port port] [default_mac
default_mac] [mac macaddr] [proto proto] [mode mode] [proto6 proto6]
[schedule_reconnect schedule_reconnect] [timeobj timeobj] [tag tag]
[vid vid] [pvid pvid] <SectionName>
```

Command	Description
[status status]<SectionName>	Enable or disable the specified WAN profile. [status] - Enter Enable or Disable. <SectionName>- Enter the name of WAN profile.
[wan4_dmz_status wan4_dmz_status]	Enable or disable the function of DMZ for the WAN profile. [wan4_dmz_status] - Enter Enable or Disable.
[desc description]	Make a brief explanation for the WAN profile. [description] - Enter any words to describe such WAN profile.
[port port]	Specify the interface for the WAN profile. [port] - Set WAN1 / WAN2 / WAN3 / WAN4 / WAN5 as the interface for network connection.
[default_mac default_mac]	Enable / disable the function of specifying the MAC address as default setting. [default_mac] - Enter Enable or Disable.
[mac macaddr]	Enter the MAC address. [macaddr] - Enter the MAC address with the format of "xx-xx-xx-xx-xx-xx"

[proto proto]	Specify the protocol type for IPv4 connection. [proto] - Available types contain None / Static / DHCP / PPoE / PPTP.
[mode mode]	Specify NAT or ROUTE mode on this interface [mode] - Enter NAT or ROUTING.
[proto6 proto6]	Specify protocol type for IPv6 connection. [proto6] - Available types contain: ● Link_Local ● Static ● PPP ● DHCP_IA_NA ● DHCP_IA_PD
[schedule_reconnect schedule_reconnect]	Enable or disable the function of WAN schedule reconnection. [schedule_reconnect] - Enter Enable or Disable.
[timeobj timeobj]	Specify a time period for schedule reconnection. [imeobj] - Specify the time object. Enter the name of the object profile.
[tag tag]	Enable or disable the function of packet tagging. [tag] - Specify a VLAN tag for the incoming packet.
[vid vid]	Specify the name of the VLAN ID. [vid] - Set a number (1 ~ 4095) as VLAN ID.
[pvid pvid]	Specify the priority (0/1/2/3/4/5/6/7) for this VLAN profile. [pvid] – Available settings include 0/1/2/3/4/5/6/7.

Example

In this example, we create a WAN profile named with “wan_test”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add status enable wan_test vid 6 pvid 2 proto
none
Vigor3900@config-t-wan-pf-wan_test#
Vigor3900@config-t-wan-pf-wan_test#exit
Vigor3900@config-t-wan#
```

6.4.1.2 Telnet Command: cdhost

Users could use [cdhost] command to configure **connection detection hosts** of a WAN profile. Choose the [dhcp] or [static] item and then use [add] or [remove] to set the profile.

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># cdhost hdcp add <SectionName>
Vigor3900@config-t-wan-pf-<SectionName># cdhost dhcp remove
<SectionName>
Vigor3900@config-t-wan-pf-<SectionName># cdhost static add
<SectionName>
```

```
Vigor3900@config-t-wan-pf-<SectionName># cdhost static remove
<SectionName>
```

Command	Description
cdhost hdcp add <SectionName>	Add DHCP connection detection host to this profile. <SectionName>- Enter the name of WAN profile.
cdhost dhcp remove <SectionName>	Remove DHCP connection detection host from this profile. <SectionName>- Enter the name of WAN profile.
cdhost static add <SectionName>	Add a static connection detection host to this profile. <SectionName>- Enter the name of WAN profile.
cdhost static remove <SectionName>	Remove a static connection detection host from this profile. <SectionName>- Enter the name of WAN profile.

6.4.1.3 Telnet Command: connect / disconnect

Users could use [connect] or [disconnect] command to connect or disconnect DHCP/PPPoE/PPTP network connection for the selected WAN profile.

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># connect
Vigor3900@config-t-wan-pf-<SectionName># disconnect
```

Command	Description
connect	Set the DHCP/PPPoE/PPTP connect ion.
disconnect	Set the DHCP/PPPoE/PPTP disconnection

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# connect
Vigor3900@config-t-wan-pf-wan_carrie# disconnect
```

6.4.1.4 Telnet Command: dns

Users could use this command to configure the DNS server to add or remove DNS server (based on IPv4).

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># dns add <dns>
Vigor3900@config-t-wan-pf-<SectionName># dns remove <dns>
```

Command	Description
dns add <dns>	Add an IPv4 address for the DNS server. <dns> - Enter an IPv4 address for DNS server.

dns remove <dns>	Delete the IP address setting for the DNS server. <dns> - Enter an IPv4 address for DNS server.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# dns add 192.168.1.89
Vigor3900@config-t-wan-pf-wan_carrie# dns remove 192.168.1.89
```

6.4.1.5 Telnet Command: dns6

Users could use this command to configure the DNS server to add or remove DNS server (based on IPv6).

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># dns6 dhcp6-ia_na add <IPv6 address>
Vigor3900@config-t-wan-pf-<SectionName># dns6 dhcp6-ia_na remove <IPv6 address>
Vigor3900@config-t-wan-pf-<SectionName># dns6 static6 add <IPv6 address>
Vigor3900@config-t-wan-pf-<SectionName># dns6 static6 remove <IPv6 address>
```

Command	Description
dns6 dhcp6-ia_na add <IPv6 address>	Add an IPv6 address for the DNS server based on IA-NA type. <IPv6 address> - Enter an IPv6 address for DNS server.
dns6 dhcp6-ia_na remove <IPv6 address>	Delete the IPv6 address setting for the DNS server based on IA-NA type. <IPv6 address> - Enter an IPv6 address for DNS server.
dns6 static6 add <IPv6 address>	Add an IPv6 address for the DNS server based on static6 type. <IPv6 address> - Enter an IPv6 address for DNS server.
dns6 static6 remove <IPv6 address>	Delete the IPv6 address setting for the DNS server based on static6 type. <IPv6 address> - Enter an IPv6 address for DNS server.

6.4.1.6 Telnet Command: exit

Users could use this command to go back to upper level.

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># exit
```

Command	Description
exit	Go back to upper level (e.g., config-t-wan menu).

6.4.1.7 Telnet Command: get

Users could use this command to display the detailed configuration (including DHCP, IPv6 DHCP IA_NA, global, PPPoE, PPTP, Static, IPv6 Static and so on) information of the selected profile

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># get
Vigor3900@config-t-wan-pf-<SectionName>#get dhcp
Vigor3900@config-t-wan-pf-<SectionName>#get dhcp6_ia_na
Vigor3900@config-t-wan-pf-<SectionName>#get dmz
Vigor3900@config-t-wan-pf-<SectionName>#get global
Vigor3900@config-t-wan-pf-<SectionName>#get pppoe
Vigor3900@config-t-wan-pf-<SectionName>#get static
Vigor3900@config-t-wan-pf-<SectionName>#get static6
```

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# get dhcp

hostname            :
ipalias             :
mtu                 : 1500
cdmode              : arp
cdhost              :
cdint               : 10
cdretry             : 3
dhcp_vendor_class_id:
dhcp_client_id_label:
dhcp_client_id      :
dhcp_client_id_pass :
user_dns_status     : disable
user_dns            :

Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# get global

status              : Disable
wan4_dmz_status     : Disable
desc                :
port                :
default_mac         : Enable
mac                 : 00:50:7f:7b:83:01
proto               : None
mode                : NAT
proto6              : Link_Local
schedule_reconnect  : Disable
timeobj             :
tag                 : Disable
vid                 : 1
pvid                : 0
Vigor3900@config-t-wan-pf-wan_carrie#
```

6.4.1.8 Telnet Command: ipalias

Use this command to configure the IP alias address. Choose the [dhcp] or [static] item and use [add] or [remove] to set this profile.

Syntax

```
Vigor3900@config-t-wan-pf-<SectionName># ipalias dhcp add <IP
address>/<mask>
Vigor3900@config-t-wan-pf-<SectionName># ipalias dhcp remove <IP
address>
Vigor3900@config-t-wan-pf-<SectionName># ipalias static add <IP
address>
Vigor3900@config-t-wan-pf-<SectionName># ipalias static remove <IP
address>
```

Command	Description
<SecionName>	Display the name of the profile.
ipalias dhcp add <IP address>/<mask>	Add an IP alias, based on DHCP type, to the selected profile. <IP address>/<mask> - Enter an IPv4 address for the WAN profile. In which, the format for IP address is "AAA.BBB.CCC.DDD" where each part is in the range 0-255. Mask number ranges from 0 to 32.
ipalias dhcp remove <IP address>	Remove an IP alias to/from the selected profile. <IP address> - Specify an IPv4 address for the WAN profile.
ipalias static add <IP address>	Add an IP alias, based on static IP type, to the selected profile. <IP address> - Specify an IPv4 address for the WAN profile.
ipalias static remove <IP address>	Remove an IP alias, based on static IP type, to the selected profile. <IP address> - Specify an IPv4 address for the WAN profile.

Example

In this example, we create a WAN profile named with "wan_carrie".

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# ipalias dhcp add
192.168.1.56/32
Vigor3900@config-t-wan-pf-wan_carrie#
```

6.4.1.9 Telnet Command: set

It is used for reviewing the detailed settings (including DHCP, IPv6 DHCP IA_NA, DMZ, global, PPPoE, Static, IPv6 Static and so on) or modifying settings for the selected profile.

Syntax for set DHCP profile

Use [set dhcp] command to configure the DHCP WAN profile in details.

```
Vigor3900@config-t-wan-pf-<SectionName># set dhcp [hostname
dhcp_hostname] [ipalias dhcp_ipalias] [mtu dhcp_mtu]
[cdmodedhcp_cd_mode] [cdhost dhcp_cd_host] [cdint dhcp_cd_interval]
[cdretry dhcp_cd_retry] [dhcp_vendor_class_id dhcp_vendor_class_id]
[dhcp_client_id dhcp_client_id] [dhcp_client_id_pass
dhcp_client_id_pass] [user_dns_status user_dns_status] [user_dns
user_dns]
```

Command	Description
<SectionName>	Display the name of the WAN profile.
[hostname dhcp_hostname]	Specify an IP address for DHCP server. [dhcp_hostname] - Enter a name for DHCP server.
[ipalias dhcp_ipalias]	Specify an IP alias address for DHCP server. [dhcp_ipalias] - Enter the IP alias address with mask number as the DHCP server (e.g., 192.168.1.56/32). In which, the format for IP address is “AAA.BBB.CCC.DDD” where each part is in the range 0-255. Mask number ranges from 0 to 32.
[mtu dhcp_mtu]	Set MTU/MRU value (max. 1500) for DHCP server. [dhcp_mtu] - Ranges from 1~ 1500.
[cdmodedhcp_cd_mode]	Set connection detection mode (None/ARP/PING/HTTP) for DHCP server. [dhcp_cd_mode] - Available modes include None, ARP, PING, and HTTP.
[cdhost dhcp_cd_host]	Set connection detection host for DHCP server. [dhcp_cd_host]- Enter a name for the host.
[cdint dhcp_cd_interval]	Set connection detection interval for DHCP server. [dhcp_cd_interval]- Ranges from 0 to 65535.
[cdretry dhcp_cd_retry]	Set connection detection retry for DHCP server. [dhcp_cd_retry]- Enter any number**.**
[dhcp_vendor_class_id dhcp_vendor_class_id]	Set vendor class ID for DHCP server. [dhcp_vendor_class_id] - Enter a string.
[dhcp_client_id dhcp_client_id]	Set the user name for DHCP client. [dhcp_client_id] - Enter username for DHCP client.
[dhcp_client_id_pass dhcp_client_id_pass]	Set a password for DHCP client. [dhcp_client_id_pass] - Enter a password for DHCP client.
[user_dns_status user_dns_status]	Enable / disable the function of DNS settings configuration. [user_dns_status] - Enter Enable or Disable.
[user_dns user_dns]	Specify DNS Settings.

	[user_dns] - Enter the IP address of DNS server.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie# set dhcp cdmode ARP

set done

Vigor3900@config-t-wan-pf-wan_carrie# set dhcp mtu 1500

set done
Vigor3900@config-t-wan-pf-wan_carrie# set dhcp cdint 10

set done

Vigor3900@config-t-wan-pf-wan_carrie# set dhcp dhcp_vendor_class_id
draytek

set done

Vigor3900@config-t-wan-pf-wan_carrie# set dhcp user_dns_status
enable

set done


Vigor3900@config-t-wan-pf-wan_carrie# set dhcp ipalias
192.168.1.56/32
set done
Vigor3900@config-t-wan-pf-wan_carrie# ipalias dhcp add
192.168.1.100/32
Vigor3900@config-t-wan-pf-wan_carrie# ipalias dhcp add
192.168.1.200/32
Vigor3900@config-t-wan-pf-wan_carrie# ipalias dhcp add
192.168.1.155/32
Vigor3900@config-t-wan-pf-wan_carrie# get dhcp

hostname            :
ipalias             : 192.168.1.10/32, 192.168.1.100/32,
192.168.1.200/32, 192.
168.1.155/32
mtu                 : 1500
cdmode              : ARP
cdhost              :
cdint               : 10
cdretry             : 3
dhcp_vendor_class_id: draytek
dhcp_client_id_label:
dhcp_client_id      :
dhcp_client_id_pass :
user_dns_status     : Enable
user_dns            : 123

Vigor3900@config-t-wan-pf-wan_carrie# set dhcp ipalias
192.168.1.250/32
```

```
set done

Vigor3900@config-t-wan-pf-wan_carrie# get dhcp

hostname            :
ipalias             : 192.168.1.250/32
mtu                 : 1500
cdmode              : ARP
cdhost              :
cdint               : 10
cdretry             : 3
dhcp_vendor_class_id: draytek
dhcp_client_id_label:
dhcp_client_id      :
dhcp_client_id_pass :
user_dns_status     : Enable
user_dns            : 123

Vigor3900@config-t-wan-pf-wan_carrie#
```

Syntax for set global profile

Use [set global] command to configure the global profile in details.

```
Vigor3900@config-t-wan-pf-<SectionName># set global [status status]
[wan4_dmz_status wan4_dmz_status][desc description][port port]
[default_mac default_mac] [mac macaddr] [proto proto] [mode mode] [proto6
proto6] [schedule_reconnect schedule_reconnect] [timeobj timeobj] [tag
tag] [vid vid] [pvid pvid]
```

Command	Description
<SectionName>	Display the name of the WAN profile.
[status status]	Enable or disable the WAN profile. [status] - Enter Enable or Disable.
[wan4_dmz_status wan4_dmz_status]	Enable or disable the function of DMZ for the WAN profile. [wan4_dmz_status] - Enter Enable or Disable.
[desc description]	Give a brief description for WAN profile. [description] - Type the description in this field.
[port port]	Specify the physical port. [port] – Available settings include WAN1, WAN2, WAN3, WAN4 and WAN5.
[default_mac default_mac]	Enable or disable the default MAC setting. [default_mac] - Enter Enable or Disable.
[mac macaddr]	Specify a MAC address for WAN profile. [macaddr] - Enter the MAC address in this field.
[proto proto]	Specify an IPv4 protocol type for WAN profile. [proto] - Available types include None, Static, DHCP, PPPoE, PPTP.
[mode mode]	Specify NAT or Routing mode for the interface. [mode] – Available modes include NAT, Routing.

[proto6 proto6]	Specify an IPv6 protocol type for WAN profile. [proto6] - Available types include Static, DHCP-IA NA, DHCP-IA PD.
[schedule_reconnect schedule_reconnect]	Enable / disable the function of WAN reconnection based on schedule. [schedule_reconnect]- Enter Enable or Disable.
[timeobj timeobj]	If [schedule_reconnect] is enabled, specify a time object profile. [timeobj] – Enter the name of the time object.
[tag tag]	Enable /disable the function to bring VLAN tag when egress. [tag] - Enter Enable or Disable.
[vid vid]	Specify a VLAN ID for WAN profile. [vid] - Ranges from 1 to 4095.
[pvid pvid]	Specify the priority for the VLAN ID. [vid] - Ranges from 0 to 7.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# set global status enable

set done

Vigor3900@config-t-wan-pf-wan_carrie# set global desc
global_test_file

set done

Vigor3900@config-t-wan-pf-wan_carrie# set global vid 20

set done

Vigor3900@config-t-wan-pf-wan_carrie# set global default_mac enable

set done

Vigor3900@config-t-wan-pf-wan_carrie# set global proto DHCP

set done

Vigor3900@config-t-wan-pf-wan_carrie#
```

Syntax for set PPPoE profile

Use [set pppoe] command to configure the PPPoE WAN profile in details.

```
Vigor3900@config-t-wan-pf-<SectionName># set pppoe [username
pppoe_username] [password pppoe_password] [mtu pppoe_mtu] [service_name
service_name] [debug pppoe_debug] [always_on pppoe_always_on] [fixed_ip
pppoe_fixed_ip] [fixed_ip_address pppoe_fixed_ip_address] [cdmode
```

```
pppoe_cd_mode] [cdhost pppoe_cd_host] [cdint pppoe_cd_interval]
[cdretry pppoe_cd_retry] [ipalias pppoe_ipalias] [user_dns_status
user_dns_status] [user_dns user_dns]
```

Command	Description
<SectionName>	Display the name of the WAN profile.
[username pppoe_username]	Specify a username for PPPoE connection. [pppoe_username] - Define a name in this field.
[password pppoe_password]	Specify a password for the PPPoE connection. [pppoe_password] - Define the password in this field.
[mtu pppoe_mtu]	Set MTU/MRU value for PPPoE connection. [pppoe_mtu] - Ranges from 1 to 1500.
[service_name service_name]	It is optional setting. [service_name] – Enter the name of the service.
[debug pppoe_debug]	Enable / disable the PPPoE debug action. [pppoe_debug] - Enter Enable or Disable.
[always_on pppoe_always_on]	Enable /disable the function of “always on” for PPPoE connection. [pppoe_always_on] - Enter Enable or Disable.
[fixed_ip pppoe_fixed_ip]	Enable /disable the function of Fixed IP for PPPoE connection. [pppoe_fixed_ip] - Enter Enable or Disable.
[fixed_ip_address pppoe_fixed_ip_address]	Specify a fixed IP. [pppoe_fixed_ip_address] – Enter the IP address.
[cdmode pppoe_cd_mode]	Specify the detection mode for PPPoE connection. [pppoe_cd_mode] – Available settings include ● None ● PING ● HTTP
[cdhost pppoe_cd_host]	Specify the IP address as connection detection host. [pppoe_cd_host] – Enter the IP address.
[cdint pppoe_cd_interval]	Set connection detection interval for PPPoE connection. [pppoe_cd_interval] - Ranges from 0 to 65535.
[cdretry pppoe_cd_retry]	Set connection detection retry for PPPoE connection. [pppoe_cd_retry] - Enter a number.
[ipalias pppoe_ipalias]	Set an IP alias address for PPPoE connection. [pppoe_ipalias] - Enter an IP address.
[user_dns_status user_dns_status]	Enable / disable the function of defining a DNS server. [user_dns_status] – Enter Enable or Disable.
[user_dns user_dns]	Specify an IP address as DNS server. [user_dns]- Enter an IP address.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# set pppoe username
marketing_test

set done

Vigor3900@config-t-wan-pf-wan_carrie# set pppoe password
marketing_123

set done
```

Syntax for set Static profile

Use [set static] command to configure the static IP profile in details.

```
Vigor3900@config-t-wan-pf-<SectionName># set static [ipaddr
static_ipaddress] [mask static_mask] [gateway static_gateway] [dns
static_dns] [ipalias static_ipalias] [mtu static_mtu] [cdmode
static_cd_mode] [cdhost static_cd_host] [cdint static_cd_interval]
[cdretry static_cd_retry]
```

Command	Description
[ipaddr static_ipaddress]	Specify an IP address. [static_ipaddress] - Define an IPv4 address in this field.
[mask static_mask]	Specify the net mask address. [static_mask] - Define the net mask address for such profile.
[gateway static_gateway]	Specify the IPv4 address as the gateway. [static_gateway] - Define an IPv4 address as the gateway.
[dns static_dns]	Specify an IP address as DNS server. [static_dns] - Define an IPv4 address for the DNS server.
[ipalias static_ipalias]	Set an IP alias address for static connection. [static_ipalias] - Enter an IP address.
[mtu static_mtu]	Set MTU/MRU value for static connection. [static_mtu] - Ranges from 1 to 1500.
[cdmode static_cd_mode]	Set connection detection mode (ARP/PING/HTTP). static_cd_mode] - Available modes include ARP, PING, and HTTP.
[cdhost static_cd_host]	Set a static connection detection host. [static_cd_host]- Type a name for the host.
[cdint static_cd_interval]	Set connection detection interval for static connection. [static_cd_interval] - Ranges from 0 to 65535.
[cdretry static_cd_retry]	Set connection detection retry for static connection. [static_cd_retry] - Enter a number.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# set static ipaddr
192.168.1.126

set done

Vigor3900@config-t-wan-pf-wan_carrie# set static cdint 65535

set done

Vigor3900@config-t-wan-pf-wan_carrie#
```

Syntax for set Static6 profile

Use [set static6] command to configure the static IPv6 profile in details.

```
Vigor3900@config-t-wan-pf-<SectionName># set static6 [ip6addr
static_ip6address] [ip6length static_ip6length] [gateway6
static_gateway6] [dns6 static_dns6]
```

Command	Description
[ip6addr static_ip6address]	Specify an IPv6 address. [static_ipaddress] - Define an IPv4 address in this field.
[ip6length static_ip6length]	Specify the prefix length for the IPv6 address. [static_ip6length] - Define the prefix length for IPv6 address.
[gateway6 static_gateway6]	Specify the IPv6 address as the gateway. [static_gateway6] - Define an IPv6 address as the gateway.
[dns6 static_dns6]	Specify an IPv6 address as DNS server. [static_dns6] - Define an IPv6 address for the DNS server.

Example

In this example, we create a WAN profile named with “wan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# pf add wan_carrie
Vigor3900@config-t-wan-pf-wan_carrie#
Vigor3900@config-t-wan-pf-wan_carrie# set static6 ip6addr
FE80::0202:B3FF:FE1E:8329

set done

Vigor3900@config-t-wan-pf-wan_carrie#
```

6.4.2 Telnet Command: defaultroute

It is used to configure default route profile. Use “set” to configure detailed settings for default route. Then use “get” to get the profile list in the directory.

Syntax

```
Vigor3900@config-t-wan# defaultroute get
Vigor3900@config-t-wan# defaultroute set [pool lb_pool] [auto_lb
auto_lb] [ct_rt ct_rt] [session_rt_excp session_rt_excp]
```

Command	Description
get	Get the configuration of default route.
set	Modify the settings of default route.
[pool lb_pool]	Set the load balance pool for a wan profile. [lb_pool] - Enter the name of the WAN profile (e.g., wan_carrie) / WAN interface (e.g., WAN1/USB1).
[auto_lb auto_lb]	Enable or disable the Auto Failover to Active WANs. [auto_lb] - Enter Enable or Disable.
[ct_rt ct_rt]	Specify the load balance mode. [cr_rt] - Enter IP Based or Session Based.
[session_rt_excp session_rt_excp]	Specify the service type object profile to be excluded. [session_rt_excp] – Enter the name of the service type object.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# defaultroute get
pool                : default_pool
auto_lb             : Enable
ct_rt               : 0
session_rt_excp     : HTTPS, IKE, IPSecNAT

Vigor3900@config-t-wan# defaultroute set pool wan1

set done
```

6.4.3 Telnet Command: lbpool

Use this command to add or delete **Load Balance Pool** profile or use “get” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-t-wan# lbpool add <SectionName>
Vigor3900@config-t-wan# lbpool delete <SectionName>
Vigor3900@config-t-wan# lbpool show
Vigor3900@config-t-wan# lbpool <SectionName>
```

Command	Description

lbpool add <SectionName>	Add a new load balance pool profile. <SectionName> - Enter the name (e.g., lb_carrie) of the balance pool profile.
lbpool delete <SectionName>	Delete a selected balance pool profile. <SectionName> - Enter the name of the load balance pool profile.
lbpool show	Display the setting status of the load balance pool profile.
lbpool <SectionName>	Modify settings for the selected profile. <SectionName> - Enter the name of the load balance pool profile.

Example

In this example, we create a load balance profile named with “lb_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# lbpool add lb_carrie
Vigor3900@config-t-wan# lbpool show
```

6.4.3.1 Telnet Command: lbpool add ?

To configure detailed settings for a load balance pool profile, users could use [lbpool add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-wan# lbpool add [mode mode] [lbif lb_iface] [primary
primary_pf] [backup backup_pf] <SectionName>
```

Command	Description
[mode mode]	Set a load balance mode for such profile. [mode] – Available settings include: ● Load_Balance ● Backup
[lbif lb_iface]	Specify an interface for such load balance profile. [lb_iface] - Name of the WAN profile (e.g., wan1, wan4, wan_carrie).
[primary primary_pf]	Specify a primary profile from existed WAN profile (e.g., wan_carrie). [primary_pf] - Enter the name for the load balance pool profile which is going to be as the primary profile.
[backup backup_pf]	Specify a backup profile from existed WAN profile (e.g., wan_david). [backup_pf] - Enter the name for the load balance pool profile which is going to be as the backup profile.
<SectionName>	<SectionName> - Enter the name (e.g., lb_carrie) of the balance pool profile.

Example

In this example, we create a load balance profile named with “lb_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# lbpool add mode backup lb_carrie
Vigor3900@config-t-wan-lb-pool-lb_carrie# lbpool show lb_carrie
Vigor3900@config-t-wan-lb-pool-lb_carrie# get

mode              : Backup
lbif              :
primary           :
backup            :

Vigor3900@config-t-wan-lb-pool-lb_carrie#
```

6.4.3.2 Telnet Command: set, get, add, remove

It is used for reviewing the detailed settings or modifying settings for the selected load balance pool profile (e.g., lb_carrie).

Syntax

```
Vigor3900@config-t-wan-lbpool-<SectionName># get
Vigor3900@config-t-wan-lbpool-<SectionName># set [mode mode] [lbif
lb_iface] [primary primary_pf] [backup backup_pf]
Vigor3900@config-t-wan-lbpool-<SectionName># add <lb_iface>
<lb_iface_weight>
Vigor3900@config-t-wan-lbpool-<SectionName># remove bif <lb_iface>
<lb_iface_weight>
```

Command	Description
<SectionName>	Display the name of the profile.
get	Get the configuration of load balance pool.
set	Modify the settings of load balance pool.
[mode mode]	Set a load balance mode for such profile. [mode] – Available settings include: ● Load_Balance ● Backup
[lbif lb_iface]	Specify an interface for such load balance profile. [lb_iface] - Name of the WAN profile (e.g., wan1, wan4, wan_carrie).
[primary primary_pf]	Specify a primary profile from existed WAN profile (e.g., wan_carrie). [primary_pf] - Enter the name for the load balance pool profile which is going to be as the primary profile.
[backup backup_pf]	Specify a backup profile from existed WAN profile (e.g., wan_david). [backup_pf] - Enter the name for the load balance pool profile which is going to be as the backup profile.
add <lb_iface>	Specify an interface for such load balance profile.

	<lb_iface> - Name of the WAN profile (e.g., wan1, wan4, wan_carrie).
add <lb_iface_weight>	Specify the weight value for the selected load balance interface. <lb_iface_weight> - Ranges from 1 to 5.
remove bif <lb_iface>	Delete an interface for such load balance profile. <lb_iface> - Name of the WAN profile (e.g., wan1, wan4, wan_carrie).
remove <lb_iface_weight>	Delete the weight value for the selected load balance interface. <lb_iface_weight> - Ranges from 1 to 5.

Example

In this example, we create a load balance profile named with “lb_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# lbpool add lb_carrie
Vigor3900@config-t-wan# lbpool show
lb-pool           mode          lbif          primary       backup
default_pool       loadbalance    wan1 1 wan2 1 wan3 1 wan4 1 wan5 1
usb1 1 usb
2 1
lb_carrie          loadbalance
Vigor3900@config-t-wan# lbpool lb_carrie
Vigor3900@config-t-wan-lb-pool-lb_carrie# set mode Load_Balance lbif
wan1 primary wan_carrie

Set done

Vigor3900@config-t-wan-lb-pool-lb_carrie# set backup wan_david

Set done

Vigor3900@config-t-wan-lb-pool-lb_carrie# add wan2 400
Vigor3900@config-t-wan-lb-pool-lb_carrie#
Vigor3900@config-t-wan-lb-pool-lb_carrie# get

mode                 : Load_Balance
lbif                 : wan1, wan2 400
primary              : wan_carrie
backup               : wan_david
Vigor3900@config-t-wan-lb-pool-lb_carrie#
```

6.4.4 Telnet Command: autolb

Use this command to set **Auto Load Balance** profile or use “get” to get the profile list in the directory.

Syntax

```
Vigor3900@config-t-wan# autolb get
Vigor3900@config-t-wan# autolb set [status status] [telecom
telecom_pool] [cnc cnc_pool] [default default_pool]
```

Command	Description
get	Get the configuration of auto load balance.
set	Modify the settings of auto load balance.
[status status]	Enable or disable the function of auto load balance. [status] - Type Enable or Disable.
[telecom telecom_pool]	Specify a WAN profile / load balance pool for China telecom. [telecom_pool] - Name of the WAN profile (e.g., wan1, wan4, wan_carrie) or profile name defined in load balance pool.
[cnc cnc_pool]	Specify a WAN profile / load balance pool for China CNC. [cnc_pool]- Name of the WAN profile (e.g., wan1, wan4, wan_carrie) or profile name defined in load balance pool.
[default default_pool]	Specify a WAN profile / load balance pool as default setting for China.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan#
Vigor3900@config-t-wan# autolb get

status          : Disable
telecom         : wan1
cnc             : wan1
default         : wan1

Vigor3900@config-t-wan#
```

6.4.5 Telnet Command: switch

Use this command to set **switch** profile, then type [interface], [mirror] commands to configure the details.

Syntax

```
Vigor3900@config-t-wan-switch# interface show
Vigor3900@config-t-wan-switch# interface <WAN1/WAN2/WAN3/WAN4/WAN5>
Vigor3900@config-t-wan-switch# mirror get
Vigor3900@config-t-wan-switch# mirror set [status status] [mirroring
mirroring] [mirrored mirrored]
```

Command	Description
interface show	Display current setting status.
interface <WAN1/WAN2/WAN3/WAN4/WAN5>	Specify an interface for switch profile.
mirror get	Display current settings status for mirroring function.
mirror set	Modify the settings for mirror function.

[status status]	Enable or disable the function of interface mirroring. [status] - Type Enable or Disable.
[mirroring mirroring]	Specify an interface as mirroring port. [mirroring] - Available settings include WAN1 to WAN5.
[mirrored mirrored]	Specify an interface as mirrored port. [mirroring] - Available settings include WAN1 to WAN5. The interface specified here shall not be the same as the interface defined in <mirroring>.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# switch
Vigor3900@config-t-wan-switch#
Vigor3900@config-t-wan-switch# interface show
switch_wan        status       duplex       speed
flow_control
energy_efficient_ethernet
WAN1              enable       full         auto         disable
enable
WAN2              enable       full         auto         disable
enable
WAN3              enable       full         auto         disable
enable
WAN4              enable       full         auto         disable
enable
WAN5              enable       full         auto         disable
Enable
Vigor3900@config-t-wan-switch# mirror get

status             : Disable
mirroring          : WAN1
mirrored           : WAN2
Vigor3900@config-t-wan-switch# interface WAN1
Vigor3900@config-t-wan-switch-WAN1#
```

6.4.6 Telnet Command: 3g

Use this command to display the status of 3G USB connection.

Syntax

```
Vigor3900@config-t-wan# 3g show
```

Command	Description
3g show	Display the status for 3G USB.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#wan
Vigor3900@config-t-wan# 3g show
Vigor3900@config-t-wan# usb1
```

6.5 LAN Configuration

LAN (Local Area Network) 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. Vigor3900 provides many functions in LAN – users could use the commands below to set up the details.

To make LAN configuration, you have to type "*configure terminal*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#
..          Go back to upper layer menu
exit        Go back to main menu
lan         Configure lan profile
wan         Configure wan profile
Vigor3900@config-t# lan
Vigor3900@config-t-lan# ?
.
.
.
```

There are four functions for WAN – General Setup (command "pf"), Inter-LAN Route, IP Bind MAC, IP Routing, Route/Route 6 and Switch.

Available sub-commands under LAN include:

- ipbindmac (refer to 6.5.1)

- iprouting (refer to 6.5.2)

- pf (refer to 6.5.3)

- route (refer to 6.5.4)

- route6 (refer to 6.5.5)

- switch (refer to 6.5.6)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.
<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.5.1 Telnet Command: ipbindmac

Users could use [ipbindmac] command to configure IP Bind MAC. Before using such command, create a LAN profile (e.g., bind_carrie) first.

Syntax

```
Vigor3900@config-t-lan#ipbindmac add <ProfileName>
Vigor3900@config-t-lan#ipbindmac delete <ProfileName>
Vigor3900@config-t-lan#ipbindmac show
Vigor3900@config-t-lan#ipbindmac show <ProfileName>
Vigor3900@config-t-lan#ipbindmac <Profile>
Vigor3900@config-t-lan#ipbindmac get
```

Command	Description
ipbindmac add <ProfileName>	Add a new IP Bind MAC profile. <ProfileName> - Enter the name of IP Bind MAC profile.
ipbindmac delete <ProfileName>	Remove a selected IP Bind MAC profile. <ProfileName> - Enter the name (e.g., bind_carrie) of IP Bind MAC profile to be deleted.
Ipbindmac show	Display the status for all IP Bind MAC profiles.
ipbindmac show <ProfileName>	Display the status of selected IP Bind MAC profile. <ProfileName> - Enter the name (e.g., bind_carrie) of IP Bind MAC profile.
ipbindmac <ProfileName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., bind_carrie) of s IP Bind MAC profile to be modified.
ipbindmac get	Display the address (IP/MAC) information for the profiles.

6.5.1.1 Telenet Command: ipbindmac add ?

To configure detailed settings for an IP bind MAC profile, users could use [ipbindmac add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-lan#ipbindmac add [ip ip] [macaddr macaddr] [comment comment] <ProfileName>
```

Command	Description
add	Add a new IP Bind MAC profile.
[ip ip]	[IP] - Define an IPv4 address in this field.
[macaddr macaddr]	[MAC address] - Enter the MAC address.
[comment comment]	[comment] - Enter a brief description for such profile.
<ProfileName>	<ProfileName> - Enter the name (e.g., Bind_carrie) of IP Bind MAC profile.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#
Vigor3900@config-t-lan#ipbindmac add ip 192.168.1.89 Bind_carrie
Vigor3900@config-t-lan-ipbindmac-Bind_carrie#
```

6.5.1.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected IP bind MAC profile (e.g., bind_carrie).

Syntax

```
Vigor3900@config-t-lan#ipbindmac get
Vigor3900@config-t-lan#ipbindmac set [ip ip] [macaddr macaddr] [comment
comment]
```

Command	Description
get	Get the configuration of IP bind MAC.
set	Modify the settings of IP bind MAC.
[ip ip]	[IP] - Define an IPv4 address in this field.
[macaddr macaddr]	[MAC address] - Enter the MAC address.
[comment comment]	[comment] - Enter a brief description for such profile.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#
Vigor3900@config-t-lan#ipbindmac Bind_carrie
Vigor3900@config-t-lan-ipbindmac-Bind_carrie#
Vigor3900@config-t-lan-ipbindmac-bind_carrie# set ip 192.168.1.86

set done

Vigor3900@config-t-lan-ipbindmac-bind_carrie# get

ip                : 192.168.1.86
macaddr            :
comment            :
```

6.5.2 Telnet Command: iprouting

Users could use [iprouting] command to configure IP Routing (LAN/WAN Proxy ARP) to add or delete the profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-t-lan#iprouting add <SectionName>
Vigor3900@config-t-lan#iprouting delete <SectionName>
Vigor3900@config-t-lan#iprouting show
Vigor3900@config-t-lan#iprouting show <SectionName>
Vigor3900@config-t-lan#iprouting <SectionName>
```

Command	Description
iprouting add <SectionName>	Add a new IP routing profile. <SectionName> - Enter the name of IP routing profile.
iprouting delete <SectionName>	Remove a selected IP routing profile. <SectionName> - Enter the name (e.g., iprouting_carrie) of routing profile to be deleted.
iprouting show	Display a summary for all IP routing profiles.
iprouting show	Display the status of selected IP routing profile.

<SectionName>	<SectionName> - Enter the name (e.g., iprouting_carrie) of IP routing profile.
iprouting <SectionName>	Modify detailed settings for the selected IP routing profile. < SectionName > - Enter the name (e.g., iprouting_carrie) of routing profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#iprouting iprouting_carrie
Vigor3900@config-t-lan-iprouting-iprouting_carrie#
```

6.5.2.1 Telenet Command: iprouting add ?

To configure detailed settings for a session limit profile, users could use [iprouting add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-lan# iprouting add [status status] [wan_pf
wan_profile] [lan_pf lan_profile] [ipaddr ipaddr] [mask mask]
<SectionName>
```

Command	Description
add	Add a new IP routing profile.
[status status]	[status] - Enter Enable or Disable.
[wan_pf wan_profile]	[wan_profile] - Enter the name (e.g., wan_carrie) of WAN profile.
[lan_pf lan_profile]	[lan_profile] - Enter the name (e.g., lan_carrie) of LAN profile.
[ipaddr ipaddr]	[ipaddr] - Enter the IP address for such profile.
[mask mask]	Enter the network mask for such profile. [mask] - Available options include: 255.255.255.252/30 255.255.255.248/29 255.255.255.240/28 255.255.255.224/27 255.255.255.192/26 255.255.255.128/25 255.255.255.0/24
<SectionName>	Enter the name (e.g., iprouting_carrie) of routing profile.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#
```

```
Vigor3900@config-t-lan#iprouting add status enable wan_pf wan_carrie
lan_pf lan_david ipaddr 192.168.1.53 mask 255.255.255.252/30
iprouting_david
Vigor3900@config-t-lan-iprouting-iprouting_david#
```

6.5.2.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected IP routing profile (e.g., iprouting_carrie).

Syntax

```
Vigor3900@config-t-lan-iprouting-<SectionName>#get
Vigor3900@config-t-lan-iprouting-<SectionName>#set [status status]
[wan_pf wan_profile] [lan_pf lan_profile] [ipaddr ipaddr] [mask mask]
```

Command	Description
get	Display current settings of the selected IP routing profile.
set	Change or modify the settings for a selected profile.
[status status]	[status] - Enter Enable or Disable.
[wan_pf wan_profile]	[wan_profile] - Enter the name (e.g., wan_carrie) of WAN profile.
[lan_pf lan_profile]	[lan_profile] - Enter the name (e.g., lan_carrie) of LAN profile.
[ipaddr ipaddr]	[ipaddr] - Enter the IP address for such profile.
[mask mask]	Enter the network mask for such profile. [mask] - Available options include: 255.255.255.252/30 255.255.255.248/29 255.255.255.240/28 255.255.255.224/27 255.255.255.192/26 255.255.255.128/25 255.255.255.0/24

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#iprouting iprouting_carrie
Vigor3900@config-t-lan-iprouting-iprouting_carrie#
Vigor3900@config-t-lan-iprouting-iprouting_carrie# set wan_pf
wan_carrie

set done

Vigor3900@config-t-lan-iprouting-iprouting_carrie# set lan_pf
lan_carrie

set done
```

6.5.3 Telnet Command: pf

It is used to configure LAN Profile to add or delete the profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-t-lan#pf add <SectionName>
Vigor3900@config-t-lan#pf delete <SectionName>
Vigor3900@config-t-lan#pf show
Vigor3900@config-t-lan#pf show <SectionName>
Vigor3900@config-t-lan#pf <SectionName>
```

Command	Description
`pf add <SectionName>`	Add a new LAN profile. <SectionName> - Enter the name (e.g., lan_carrie) of new LAN profile.
`pf delete <SectionName>`	Remove a selected IP routing profile. <SectionName> - Enter the name (e.g., lan_carrie) of routing profile to be deleted.
`pf show`	Display a summary for all LAN profiles.
`pf show <SectionName>`	Display detailed settings for the specified LAN profile.
`pf <SectionName>`	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., lan_carrie) of LAN profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#
Vigor3900@config-t-lan#pf show
interface          status        desc          vid           proto
ipaddr        mask          dhcp_status    proto6
lan1              enable                      10            static
192.168.1.1    255.255.255.0  enable        link-local
lan_carrie         disable                     1            static
0.0.0.0       255.255.255.0  enable        link-local
Vigor3900@config-t-lan#pf show lan_carrie

status               : Disable
desc                 :
vid                  : 1
pvid                 : 0
default_mac          : Enable
mac                  : 00:50:7f:7b:83:00
proto                : static
mode                 : NAT
ipaddr               : 0.0.0.0
mask                 : 255.255.255.0
cdmode               : None
```

```
gateway              :
cdint                : 5
cdretry              : 3
dhcp_status          : Enable
start                :
end                  :
dns                  :
lease                : 86400
.....................
```

6.5.3.1 Telnet Command: pf add ?

To configure detailed settings for a LAN profile, users could use [pf add] to create a new LAN profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-lan# pf add [status status] [desc description] [vid
vid] [pvid pvid] [default_mac default_mac] [mac macaddr] [mode mode]
[ipaddr ipaddress] [mask mask] [cdmode static_cd_mode] [gateway
static_gateway] [cdint static_cd_interval] [cdretry static_cd_retry]
[dhcp_status dhcp_status] [start dhcp_start] [end dhcp_end] [dns
dhcp_dns] [lease lease] [router router] [dhcp_next_server
dhcp_next_server] [dhcp_options dhcp_options] [rdi_pool rdi_pool]
[rdi_start rdi_start] [rdi_end rdi_end] [2nd_subnet 2nd_subnet]
[lan_dns_redirect lan_dns_redirect] [proto6 proto6] [ip6addr
static_ip6address] [ip6length static_ip6length] [sla_wan dhcp6_sla_wan]
[sla_id dhcp6_sla_id] <SectionName>
```

Command	Description
[status status]	Enable or disable the specified LAN profile. [status] - Enter Enable or Disable.
[desc description]	Make a brief explanation for the LAN profile. [description] - Enter any words to describe such LAN profile.
[vid vid]	Specify the name of the VLAN ID. [vid] - Set a number (1 ~ 4095) as VLAN ID.
[pvid pvid]	Specify the priority (0/1/2/3/4/5/6/7) for this LAN profile. [pvid] - Set the priority by entering the number of 0/1/2/3/4/5/6/7.
[default_mac default_mac]	Enable / disable the function of specifying the MAC address as default setting. [default_mac] - Enter Enable or Disable.
[mac macaddr]	Enter the MAC address if default MAC address is disabled. [macaddr] - Enter the MAC address with the format of "xx-xx-xx-xx-xx-xx"
[mode mode]	From this subnet to remote network, you have to do NAT or ROUTING (NAT/ROUTING) [mode] - Enter NAT or ROUTING.
[ipaddr ipaddress]	Set a private IP address of this router for LAN profile. [ipaddress] - Enter a private IP address.
[mask mask]	Set a subnet mask for LAN profile. [mask]- Enter the subnet mask with the format of

	“xxx.xxx.xxx.xxx/0-32”.
[cdmode static_cd_mode]	Select a detecting mode for this profile. [static_cd_mode] - Enter None or ARP.
[gateway static_gateway]	If ARP is selected as cdmode, set this IP address. [static_gateway] - Enter a public IP address as gateway.
[cdint static_cd_interval]	If ARP is selected as cdmode, set connection detection interval. [static_cd_interval] - Enter an interval period of time for each detecting.
[cdretry static_cd_retry]	If ARP is selected as cdmode, set connection detection retry. [static_cd_retry] - Enter detecting times to ensure the connection of the LAN interface
[dhcp_status dhcp_status]	Enable or disable the function of the DHCP server. [dhcp_status] - Enter Enable or Disable.
[start dhcp_start]	Set an IP address as the starting point for DHCP server. [dhcp_start] - Enter an IP address.
[end dhcp_end]	Set an IP address as the ending point for DHCP server. [dhcp_end] - Enter an IP address.
[dns dhcp_dns]	Set an IP address for the DHCP DNS server. [dhcp_dns] - Enter an IP address.
[lease lease]	Set a lease time for the DHCP server. The time unit is minute. [lease] - Enter any number.
[router router]	Vigor router will be treated as gateway in default. If you want to assign other device as gateway, please enter the IP address in this field. [router] - Enter the IP address of the other gateway.
[dhcp_next_server dhcp_next_server]	Set next server for DHCP server. [dhcp_next_server] - Enter the IP address of the secondary DHCP server.
[dhcp_options dhcp_options]	Set DHCP option number for DHCP sever. [dhcp_options] - Set the option number.
[rdi_pool rdi_pool]	Enable or disable the function of remote dial-in IP. [rdi_pool]- Enter Enable / Disable.
[rdi_start rdi_start]	Set the starting IP address for remote dial-in IP range. [rdi_start] - Enter an IP address.
[rdi_end rdi_end]	Set the ending IP address for remote dial-in IP range. [rdi_end] - Enter an IP address.
[2nd_subnet 2nd_subnet]	Specify the second subnet. <2nd_subnet> - Enter the IP address.
[lan_dns_redirect lan_dns_redirect]	Enable or disable the function of redirecting DNS queries from such LAN profile to router's DNS Server. [lan_dns_redirect]- Enter Enable or Disable.
[proto6 proto6]	Defines the IPv6 connection types for LAN interface. [proto6]- Available IPv6 protocols contain:

	● Link_Local ● Static ● DHCP_SLA
[ip6addr static_ip6address]	If **Static** is set as IPv6 Protocol, please enter the IPv6 address in this field. [static_ip6address] - Enter the IPv6 address for LAN profile.
[ip6length static_ip6length]	Set prefix length for Static IPv6. [static_ip6length] - Enter the value.
[sla_wan dhcp6_sla_wan]	If **DHCP-SLA** is chosen as IPv6 Protocol, set one of the WAN profiles in this field. [dhcp6_sla_wan] - Enter the name of WAN profile.
[sla_id dhcp6_sla_id]	Set SLA_ID number for DHCPv6 server. [dhcp6_sla_id] - Enter number as SLA ID number.
<SectionName>	[SectionName]- Enter the name of LAN profile.

Example

In this example, we create a LAN profile named with “lan_test”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t# lan
Vigor3900@config-t-lan # pf add status enable lan _test vid 6 pvid 2
proto none
Vigor3900@config-t-lan-pf-lan_test#
Vigor3900@config-t-lan-pf-lan_test#exit
Vigor3900@config-t-lan#
```

6.5.3.2 Telnet Command: 2nd_subnet

Users could use [2nd_subnet] command to modify second subnet of a specified LAN profile (e.g., lan_carrie).

Syntax

`Vigor3900@config-t-LAN-pf-<SectionName>`#2nd_subnet add <ipaddr> <netmsk> <mode>
`Vigor3900@config-t-LAN-pf-<SectionName>`#2nd_subnet remove <ipaddr> <netmsk> <mode>

Command	Description
2nd_subnet add <ipaddr> <netmask> <mode>	Specify settings as second subnet. <ipaddr> - Enter an IP address. <netmask> - Enter subnet mask. <mode> - Enter NAT or ROUTING.
2nd_subnet remove	Delete settings for the second subnet. <ipaddr> - Enter the IP address of the second subnet. <netmask> - Enter subnet mask of the second subnet. <mode> - Enter NAT or ROUTING of the second subnet.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie# 2nd_subnet add 192.168.1.201
255.255.255.255/24 NAT
```

6.5.3.3 Telnet Command: dhcp

Users could use [dhcp/dhcp6] command to modify DHCP server settings (such as DNS server, DHCP server) for an existing LAN profile. Use the [get] or [set] command to configure the information.

Syntax

```
Vigor3900@config-t-lan-pf-<SectionName># dhcp
Vigor3900@config-t-lan-pf-<SectionName>_dhcp# dns add <dns>
Vigor3900@config-t-lan-pf-<SectionName>_dhcp# dns remove <dns>
Vigor3900@config-t-lan-pf-<SectionName>_dhcp# get
Vigor3900@config-t-lan-pf-<SectionName>_dhcp# set [status status]
[start start] [end end] [dns dns] [router router] [lease lease] [rdi_pool
status] [rdi_start rdi_start] [rdi_end rdi_end]
```

Command	Description
dns add <dns>	Add an IP address as DNS server. <dns> - Enter IP address for DNS server.
dns remove <dns>	Remove the IP address of the DNS server. <dns> - Enter IP address for DNS server to be removed.
get	Display current DHCP status of the selected LAN profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the profile. [status] - Enter Enable or Disable.
[start start]	Enter an IP address as starting point. [start] – Enter an IP address.
[end end]	Enter an IP address as ending point. [end] – Enter an IP address.
[dns dns]	Enter an IP address as DNS server. [dns] – Enter the IP address.
[router router]	Enter the IP address of the other gateway. [router] – Enter an IP address.
[lease lease]	Enter any number as lease time for DHCP server. [lease] – Enter a number.
[rdi_pool status]	Enable / Disable to the function of remote dial-in IP. [status] – Enter Enable or Disable.

[rdi_start rdi_start]	Enter an IP address as the starting IP address for remote dial-in IP range. [rdi_start] – Enter the IP address.
[rdi_end rdi_end]	Enter an IP address as the ending IP address for remote dial-in IP range. [rdi_end]- Enter the IP address.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#dhcp
Vigor3900@config-t-lan-pf-lan_carrie_dhcp#
```

6.5.3.4 Telnet Command: dhcp6

Users could use [dhcp6] command to modify DHCPv6 server settings (such as DHCPv6 server) for an existing LAN profile. Use the [get] or [set] command to configure the information.

Syntax

```
Vigor3900@config-t-lan-pf-<SectionName># dhcp6
Vigor3900@config-t-lan-pf-<SectionName>-dhcp6# get
Vigor3900@config-t-lan-pf-<SectionName>-dhcp6# set [status status]
[mode mode] [dns_auto dns_auto] [start start] [end end] [dns dns]
```

Command	Description
get	Display current DHCPv6 status of the selected LAN profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the profile. [status] - Enter Enable or Disable.
[mode mode]	Obtain IP address automatically or define the IPv6 address(es) manually. [mode] - Enter Automatic_Setting or Manual_Setting.
[dns_auto dns_auto]	If Manual_Setting is specified as mode, enter Enable to make Vigor3900 as DNS server automatically. [dns_auto] – Enter Enable or Disable.
[start start]	If Manual_Setting is specified as mode, enter an IPv6 address as the starting IP. [start] – Enter an IPv6 address.
[end end]	If Manual_Setting is specified as mode, enter an IPv6 address as the ending IP. [end] – Enter an IPv6 address.
[dns dns]	If Manual_Setting is specified as mode, enter the IPv6 address of DNS server.

	[dns] – Enter an IPv6 address.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#dhcp6
Vigor3900@config-t-lan-pf-lan_carrie-dhcp6#get

status              : Disable
mode                : Automatic_Setting
start_auto          :
end_auto            :
dns_auto            :
start               :
end                 :
dns                 :
```

6.5.3.5 Telnet Command: dhcprelay

Users use [dhcprelay] command to modify / configure DHCP Relay agent, then type the [get] or [set] command to configure the details information.

Syntax

```
Vigor3900@config-t-lan-pf-<SectionName>># dhcprelay
Vigor3900@config-t-lan-pf-<SectionName>>-dhcprelay>#get
Vigor3900@config-t-lan-pf-<SectionName>>-dhcprelay>#set [status status]
[wan wan_profile] [server server_ip] [agent_ip agent_ip]
```

Command	Description
get	Get the configuration of DHCP relay profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the profile. [status] – Enter Enable or Disable.
[wan wan_profile]	Specify the interface (WAN profile name) for the DHCP server. [wan_profile] – Enter the name of WAN profile.
[server server_ip]	Specify the IP address of DHCP Server. [server_ip] – Enter an IP address.
[agent_ip agent_ip]	Enter the IP address of DHCP Relay Agent. [agent_ip]- Enter the IP address.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
```

```
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#
Vigor3900@config-t-lan-pf-lan_carrie#dhcprelay
Vigor3900@config-t-lan-pf-lan_carrie-dhcprelay#get
status              : Disable
wan                 :
server              :
agent_ip            :
```

6.5.3.6 Telnet Command: exit

Users could use this command to go back to upper level.

Syntax

```
Vigor3900@config-t-LAN-pf-<SectionName># exit
```

Command	Description
exit	Go back to upper level (e.g., config-t-LAN menu).

6.5.3.7 Telnet Command: get

Users could use this command to display the detailed configuration information of the selected LAN profile

Syntax

```
Vigor3900@config-t-LAN-pf-<SectionName># get
```

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#
Vigor3900@config-t-lan-pf-lan_carrie# get
status              : Disable
desc                :
vid                 : 1
pvid                : 0
default_mac         : Enable
mac                 : 00:50:7f:7b:83:00
proto               : static
mode                : NAT
ipaddr              : 0.0.0.0
mask                : 255.255.255.0
cdmode              : None
gateway             :
cdint               : 5
cdretry             : 3
dhcp_status         : Enable
start               :
end                 :
dns                 :
lease               : 86400
```

```
router                :
dhcp_next_server      :
.....
.....
```

6.5.3.8 Telnet Command: radvd

Uses can use [radvd] command to configure / modify RADVD settings for an existing LAN profile.

Syntax

```
Vigor3900@config-t-lan-pf-<SectionName>#
Vigor3900@config-t-lan-pf-<SectionName># radvd
Vigor3900@config-t-lan-pf-<SectionName>-radvd# get
Vigor3900@config-t-lan-pf-<SectionName>-radvd# set status [status
status] [lifetime lifetime]
```

Command	Description
get	Display current RADVD of the selected LAN profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the RADVD function. [status] – Enter Enable or Disable.
[lifetime lifetime]	Enter a value (ranging from 10 ~ 150 minutes) for advertisement lifetime. [lifetime] – Enter a value.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#radvd
Vigor3900@config-t-lan-pf-lan_carrie_radvd#
Vigor3900@config-t-lan-pf-lan_carrie-radvd#get
status             : Enable
lifetime           : 30
```

6.5.3.9 Telnet Command: set

It is used for reviewing the detailed settings or modifying settings for the selected profile (e.g., lan_carrie).

Syntax

```
Vigor3900@config-t-lan-pf-<SectionName># set [status status] [desc
description] [vid vid] [pvid pvid] [default_mac default_mac] [mac macaddr]
[mode mode] [ipaddr ipaddress] [mask mask] [cdmode static_cd_mode]
[gateway static_gateway] [cdint static_cd_interval] [cdretry
static_cd_retry] [dhcp_status dhcp_status] [start dhcp_start] [end
dhcp_end] [dns dhcp_dns] [lease lease] [router router] [dhcp_next_server
dhcp_next_server] [dhcp_options dhcp_options] [rdi_pool rdi_pool]
```

```
[rdi_start rdi_start] [rdi_end rdi_end] [2nd_subnet 2nd_subnet]
[lan_dns_redirect lan_dns_redirect] [proto6 proto6]
[ip6addrstatic_ip6address] [ip6length static_ip6length] [sla_wan
dhcp6_sla_wan] [sla_iddhcp6_sla_id]
```

Command	Description
<SectionName>	Display the name of the profile.
[status status]	Enable or disable the specified LAN profile. [status] - Enter Enable or Disable.
[desc description]	Make a brief explanation for the LAN profile. [description] - Enter any words to describe such LAN profile.
[vid vid]	Specify the name of the VLAN ID. [vid] - Set a number (1 ~ 4095) as VLAN ID.
[pvid pvid]	Specify the priority (0/1/2/3/4/5/6/7) for this LAN profile. [pvid] - Set the priority by entering the number of 0/1/2/3/4/5/6/7.
[default_mac default_mac]	Enable / disable the function of specifying the MAC address as default setting. [default_mac] - Enter Enable or Disable.
[mac macaddr]	Enter the MAC address if default MAC address is disabled. [macaddr] - Enter the MAC address with the format of "xx-xx-xx-xx-xx-xx"
[mode mode]	From this subnet to remote network, you have to do NAT or ROUTING (NAT/ROUTING) [mode] - Enter NAT or ROUTING.
[ipaddr ipaddress]	Set a private IP address of this router for LAN profile. [ipaddress] - Enter a private IP address.
[mask mask]	Set a subnet mask for LAN profile. [mask]- Enter the subnet mask with the format of "xxx.xxx.xxx.xxx/0-32".
[cdmode static_cd_mode]	Select a detecting mode for this profile. [static_cd_mode] - Enter None or ARP.
[gateway static_gateway]	If ARP is selected as cdmode, set this IP address. [static_gateway] - Enter a public IP address as gateway.
[cdint static_cd_interval]	If ARP is selected as cdmode, set connection detection interval. [static_cd_interval] - Enter an interval period of time for each detecting.
[cdretry static_cd_retry]	If ARP is selected as cdmode, set connection detection retry. [static_cd_retry] - Enter detecting times to ensure the connection of the LAN interface
[dhcp_status dhcp_status]	Enable or disable the function of the DHCP server. [dhcp_status] - Enter Enable or Disable.
[start dhcp_start]	Set an IP address as the starting point for DHCP server. [dhcp_start] - Enter an IP address.
[end dhcp_end]	Set an IP address as the ending point for DHCP server. [dhcp_end] - Enter an IP address.

[dns dhcp_dns]	Set an IP address for the DHCP DNS server. [dhcp_dns] - Enter an IP address.
[lease lease]	Set a lease time for the DHCP server. The time unit is minute. [lease] - Enter any number (between 300 and 604800).
[router router]	Vigor router will be treated as gateway in default. If you want to assign other device as gateway, please enter the IP address in this field. [router] - Enter the IP address of the other gateway.
[dhcp_next_server dhcp_next_server]	Set next server for DHCP server. [dhcp_next_server] - Enter the IP address of the secondary DHCP server.
[dhcp_options dhcp_options]	Set DHCP option number for DHCP sever. [dhcp_options] - Set the option number.
[rdi_pool rdi_pool]	Enable or disable the function of remote dial-in IP. [rdi_pool]- Enter Enable / Disable.
[rdi_start rdi_start]	Set the starting IP address for remote dial-in IP range. [rdi_start] - Enter an IP address.
[rdi_end rdi_end]	Set the ending IP address for remote dial-in IP range. [rdi_end] - Enter an IP address.
[2nd_subnet 2nd_subnet]	Specify the second subnet. <2nd_subnet> - Enter the IP address.
[lan_dns_redirect lan_dns_redirect]	Enable or disable the function of redirecting DNS queries from such LAN profile to router's DNS Server. [lan_dns_redirect]- Enter Enable or Disable.
[proto6 proto6]	Defines the IPv6 connection types for LAN interface. [proto6]- Available IPv6 protocols contain: ● Link_Local ● Static ● DHCP_SLA
[ip6addr static_ip6address]	If **Static** is set as IPv6 Protocol, please enter the IPv6 address in this field. [static_ip6address] - Enter the IPv6 address for LAN profile.
[ip6length static_ip6length]	Set prefix length for Static IPv6. [static_ip6length] - Enter the value.
[sla_wan dhcp6_sla_wan]	If **DHCP-SLA** is chosen as IPv6 Protocol, set one of the WAN profiles in this field. [dhcp6_sla_wan] - Enter the name of WAN profile.
[sla_id dhcp6_sla_id]	Set SLA_ID number for DHCPv6 server. [dhcp6_sla_id] - Enter number as SLA ID number.

Example

In this example, we create a LAN profile named with “lan_carrie”.

```
Vigor3900>enable
Vigor3900# configure terminal
```

```
Vigor3900@config-t#lan
Vigor3900@config-t-lan# pf add lan_carrie
Vigor3900@config-t-lan-pf-lan_carrie#set status enable desc
for_study default_mac enable mode NAT ipaddr 192.168.1.78 mask
255.255.255.0/24 cdmode none dhcp_status disable dns 192.168.1.100
lease 350 rdi_pool disable
set done
Vigor3900@config-t-lan-pf-lan_carrie#
```

6.5.4 Telnet Command: route

Users could use [route] command to add or delete the static route profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-t-lan#route add <SecitonName>
Vigor3900@config-t-lan#route delete <SectionName>
Vigor3900@config-t-lan#route show
Vigor3900@config-t-lan#route show <SecitonName>
Vigor3900@config-t-lan#route <SecitonName>
```

Command	Description
route add <SectionName>	Add a new route profile. <SectionName> - Enter the name of route profile.
route delete <SectionName>	Remove a selected route profile. <SectionName> - Enter the name (e.g., route_carrie) of route profile to be deleted.
route show	Display the status for all route profiles.
route show <SectionName>	Display the status of selected route profile. <SectionName> - Enter the name (e.g., route_carrie) of route profile.
route <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., route_carrie) of route profile to be modified.

6.5.4.1 Telenet Command: route add ?

To configure detailed settings for a routing profile, users could use [route add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-lan#route add [status status] [dest dest] [mask mask]
[gateway gateway] [pf profile] [metric metric] <SectionName>
```

Command	Description
add	Add a new route profile based on IPv4.
[status status]	Enable or disable the route profile. [status] – Enter Enable or Disable.

[dest dest]	Specify an IP address as the destination. [dest] – Enter an IP address.
[mask mask]	Enter the network mask for the destination. [mask] - Available options include: 255.255.255.252/30 255.255.255.248/29 255.255.255.240/28 255.255.255.224/27 255.255.255.192/26 255.255.255.128/25 255.255.255.0/24
[gateway gateway]	Enter an IP address as the gateway for the route profile. [gateway] – Enter the IP address.
[pf profile]	Specify the interface (LAN or WAN profile) for this static route. [profile] – Enter the name of the profile.
[metric metric]	Enter the distance to the target (usually counted in hops). [metric] – Enter the value.
<SectionName>	Enter the name (e.g., rout_marketing) of static route profile.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#route add status enable dest 192.168.1.100
route_david
Vigor3900@config-t-lan-route-route_david#
```

6.5.4.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected routing profile (e.g., route_david).

Syntax

```
Vigor3900@config-t-lan-route-<SectionName># get
Vigor3900@config-t-lan-route-<SectionName># set set [status status]
[dest dest] [mask mask] [gateway gateway] [pf profile] [metric metric]
```

Command	Description
<SectionName>	Display the name of the profile.
get	Get the configuration of route profile.
set	Modify settings for the selected profile.
[status status]	Enable or disable the route profile. [status] – Enter Enable or Disable.
[dest dest]	Specify an IP address as the destination. [dest] – Enter an IP address.

[mask mask]	Enter the network mask for the destination. [mask] - Available options include: 255.255.255.252/30 255.255.255.248/29 255.255.255.240/28 255.255.255.224/27 255.255.255.192/26 255.255.255.128/25 255.255.255.0/24
[gateway gateway]	Enter an IP address as the gateway for the route profile. [gateway] – Enter the IP address.
[pf profile]	Specify the interface (LAN or WAN profile) for this static route. [profile] – Enter the name of the profile.
[metric metric]	Enter the distance to the target (usually counted in hops). [metric] – Enter the value.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#route add status enable dest 192.168.1.100
route_marketing
Vigor3900@config-t-lan-route-route_marketing#
Vigor3900@config-t-lan-route-route_marketing# get

status          : Enable
dest            : 192.168.1.100
mask            :
gateway         :
pf              :
metric          :

Vigor3900@config-t-lan-route-route_marketing#
Vigor3900@config-t-lan-route-route_marketing# set status enable dest
192.168.10
120 mask 255.255.252/30 gateway 192.168.10.210 pf lan_carrie metric
150

set done

Vigor3900@config-t-lan-route-route_marketing#
```

6.5.5 Telnet Command: route6

Users could use [route] command to add or delete the static profile based on IPv6 address or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-t-lan#route6 add <SecitonName>
Vigor3900@config-t-lan#route6 delete <SectionName>
```

```
Vigor3900@config-t-lan#route6 show
Vigor3900@config-t-lan#route6 show <SecitonName>
Vigor3900@config-t-lan#route6 <SecitonName>
```

Command	Description
route6 add <SectionName>	Add a new route profile. <SectionName> - Enter the name of route profile.
route6 delete <SectionName>	Remove a selected route profile. <SectionName> - Enter the name (e.g., route6_production) of route profile to be deleted.
route6 show	Display the status for all route profiles.
route6 show <SectionName>	Display the status of selected route profile. <SectionName> - Enter the name (e.g., route6_production) of route profile.
route6 <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., route6_production) of route profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#route6 add route6_production
Vigor3900@config-t-lan-route6-route6_production#
```

6.5.5.1 Telenet Command: route6 add ?

To configure detailed settings for a route profile (based on IPv6), users could use [route6 add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-t-lan# route6 add [status status] [dest dest]
[prefix_len prefix_len] [nexthop nexthop] [pf profile] [metric metric]
<SectionName>
```

Command	Description
add	Add a new route profile based on IPv6.
[status status]	Enable or Disable the route profile. [status] – Enter Enable or Disable.
[dest dest]	Specify an IP address as the destination. [dest] – Enter an IP address.
[prefix_len prefix_len]	Specify the length of prefix. [prefix_len] – Enter the length.
[nexthop nexthop]	Specify an IP address as the nexthop for the route profile. [nexthop]- Enter the IP address.
[pf profile]	Specify the interface (LAN or WAN profile) for this static route.

	[profile] – Enter the name of the profile.
[metric metric]	Specify the distance to the target (usually counted in hops). [metric] – Enter the value.
<SectionName>	Enter the name (e.g., route6_production) of route profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#route6 add status enable route6_production
Vigor3900@config-t-lan-route6-route6_production#
```

6.5.5.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected profile (e.g., route6_production).

Syntax

```
Vigor3900@config-t-lan-route6-<SectionName># get
Vigor3900@config-t-lan-route6-<SectionName># set [status status] [dest dest] [prefix_len prefix_len] [nexthop nexthop] [pf profile] [metric metric]
```

Command	Description
<SectionName>	Display the name of the profile.
get	Get the configuration of route6 profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the route profile. [status] – Enter Enable or Disable.
[dest dest]	Specify an IP address as the destination. [dest] – Enter an IP address.
[prefix_len prefix_len]	Specify the length of prefix. [prefix_len] – Enter the length.
[nexthop nexthop]	Specify an IP address as the nexthop for the route profile. [nexthop]- Enter the IP address.
[pf profile]	Specify the interface (LAN or WAN profile) for this static route. [profile] – Enter the name of the profile.
[metric metric]	Specify the distance to the target (usually counted in hops). [metric] – Enter the value.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
```

```
Vigor3900@config-t-lan#route6 add status enable route6_production
Vigor3900@config-t-lan-route6-route6_production#
Vigor3900@config-t-lan-route6-route6_production# get

status          : Enable
dest            :
prefix_len      :
nexthop         :
pf              :
metric          :
```

6.5.6 Telnet Command: switch

Use [switch] command to configure Switch of the LAN profile, then use the [interface], [mirror], and [vlan] commands to configure the details information.

Syntax

```
Vigor3900@config-t-lan-switch#interface show
Vigor3900@config-t-lan-switch#interface <intf_num>
Vigor3900@config-t-lan-switch#mirror get
Vigor3900@config-t-lan-switch#mirror set status [status status]
[mirroring mirroring] [mirrored mirrored]
```

Command	Description
interface show	Display current settings on the Switch managed by Vigor router.
interface <intf_num>	Specify a LAN interface. <intf_num> - Specify one LAN profile as interface. Available settings are LAN_Port_1 / LAN_Port_2 /LAN_SFP.
mirror get	Display current mirror configuration.
mirror set	Modify settings mirror function.
[status status]	Enable or Disable the mirror function. [status] – Enter Enable or Disable.
[mirroring mirroring]	Specify a LAN port for mirroring. [mirroring] - Available settings are LAN_Port_1 / LAN_Port_2 /LAN_SFP.
[mirrored mirrored]	Specify a LAN port to be mirrored. [mirrored] - Available settings are LAN_Port_1 / LAN_Port_2 /LAN_SFP.

Example

```
Vigor3900>enable
Vigor3900# configure terminal
Vigor3900@config-t#lan
Vigor3900@config-t-lan#switch
Vigor3900@config-t-lan-switch#
Vigor3900@config-t-lan-switch# interface show
switch_lan      status    duplex    speed     flow_control energy_efficient_ethernet
LAN_Port_1      enable    full      auto      disable      enable
LAN_Port_2      enable    full      auto      disable      enable
LAN_SFP         enable    full      auto      disable      enable
```

```
Vigor3900@config-t-lan-switch# mirror get

status          : Disable
mirroring       : LAN_Port_2
mirrored        : LAN_Port_1
Vigor3900@config-t-lan-switch# mirror set mirrored LAN_SFP
set done
Vigor3900@config-t-lan-switch# mirror get
status          : Enable
mirroring       : LAN_Port_1
mirrored        : LAN_SFP
Vigor3900@config-t-lan-switch# interface show
switch_lan      status    duplex    speed     flow_control  energy_efficient_ethernet
LAN_Port_1      enable    full      auto      disable       enable
LAN_Port_2      enable    full      auto      disable       enable
LAN_SFP         enable    full      auto      disable       enable
Vigor3900@config-t-lan-switch#
Vigor3900@config-t-lan-switch# interface LAN_Port_1
Vigor3900@config-t-lan-switch-LAN_Port_1#
Vigor3900@config-t-lan-switch-LAN_Port_1# get

status          : Enable
duplex          : Full
speed           : Auto
flow_control    : Disable
energy_efficient_ethernet : Enable

Vigor3900@config-t-lan-switch-LAN_Port_1#
```

6.6 NAT Configuration

NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services.Vigor3900 provides three functions in NAT – Port Redirection and DMZ Host. Users could use the commands below to set up the details.

To make NAT configuration, you have to type "*configure nat*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# ?
.
```

There are three functions for NAT – Port Redirection, DMZ.

Available sub-commands under NAT include:

- port_redirect (refer to 6.6.1)

- dmz (refer to 6.6.2)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.6.1 Telnet Command: port_redirect

Users could use [port_redirect] command to add or delete the Port Redirection profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile detail configuration directly.

Syntax

```
Vigor3900@config-nat#port_redirect add <ProfileName>
Vigor3900@config-nat#port_redirect delete <ProfileName>
Vigor3900@config-nat#port_redirect show
Vigor3900@config-nat#port_redirect show <ProfileName>
Vigor3900@config-nat#port_redirect <ProfileName>
```

Command	Description
port_redirect add <ProfileName>	Add a new port redirection profile. <ProfileName> - Enter the name of port redirection profile.
port_redirect delete <ProfileName>	Remove a selected port redirection profile. <ProfileName> - Enter the name (e.g., port_r_carrie) of port redirection profile to be deleted.
port_redirect show	Display the status for all Port Redirection profiles.
port_redirect show <ProfileName>	Display the status of selected port redirection profile. <ProfileName> - Enter the name (e.g., port_r_carrie) of port redirection profile
port_redirect <ProfilenName>	Modify detailed settings for the selected profile. < ProfileName > - Enter the name (e.g., port_r_carrie) of profile to be modified.

Example

In this example, we create a port redirection profile named with "port_r_carrie".

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# ?
Vigor3900@config-nat# port_redirect add status enable port_r_carrie
Vigor3900@config-nat-pr-port_r_carrie#
```

6.6.1.1 Telnet Command: port_redirct add ?

To configure detailed settings for a port redirect profile, users could use [port redirect add] to create a new port redirect profile **with detailed settings**.

Syntax

```
Vigor3900@config-nat# port_redirect add [status status] [redirect_mode
redirect_mode] [public_prof public_prof] [useipalias useipalias]
[ipalias ipalias] [proto proto] [obj src_ip_obj] [snat_ip snat_ip]
[public_port_start public_port_start] [public_port_end public_port_end]
[private_ip private_ip] [private_ip_end private_ip_end]
[private_port_start private_port_start] [private_port_end
private_port_end] [more_1to1_port more_1to1_port] <ProfileName>
```

Command	Description

[status status]	Enable or Disable the port redirection profile. [status] – Enter Enable or Disable.
[redirect_mode redirect_mode]	Specify the direction for the port to be redirected. Available options include: ● One_to_One ● Range_to_One ● Range_to_Range_port ● Range_to_Range_IP
[public_prof public_prof]	Specify the WAN profile for such profile. [public_prof] - Enter the name of the WAN profile (e.g., wan_carrie)
[useipalias useipalias]	Determine to use IP alias or not. [useipalias] - Available options include ● No – No IP alias will be used. ● Single_Alias – Only one IP Alias will be used. ● All – All of the IP address(es) will be used as IP Alias.
[ipalias ipalias]	Enter the IP alias address if Single Alias is selected. [ipalias] - Enter the IP address.
[proto proto]	Specify one protocol for such profile. [proto] - Enter TCP, UDP, or TCP/UDP.
[obj src_ip_obj]	Specify source IP address(es). [src_ip_obj] – Enter the name of IP object profile.
[snat_ip snat_ip]	Change the source IP as the new IP address specified here. [snat_ip] – Enter an IP address.
[public_port_start public_port_start]	It is available when Range to One or Range to Range (port) or Range to Range (IP) is selected as Port Redirection Mode. [public_port_start] - Enter starting number of the public port.
[public_port_end public_port_end]	It is available when Range to One or Range to Range (port) or Range to Range (IP) is selected as Port Redirection Mode. <public_port_end> - Enter ending number of the public port.
[private_ip private_ip]	Specify the private IP address of the internal host providing the service. [private_ip]- Enter a private IP address.
[private_ip_end private_ip_end]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_ip_end]- Enter a private IP address.
[private_port_start private_port_start]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_port_start] - Enter a starting number of the private port.
[private_port_end private_port_end]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_port_end]- Enter the number of the private port.

[more_1to1_port more_1to1_port]	It is available when One to One is selected as Port Redirection Mode. It allows to configure more port numbers. [more_ltol_port]- Enter a number.
<ProfileName>	[ProfileName] - Enter the name of the profile.

Example

In this example, we create a port redirection profile named with “port_r_david”.

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# ?
Vigor3900@config-nat# port_redirect add status enable redirect_mode
One_to_One public_prof wan_carrie proto TCP port_r_david
Vigor3900@config-nat-pr-port_r_david#
```

6.6.1.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected profile (e.g., port_r_david).

Syntax

```
Vigor3900@config-nat-pr-<ProfileName>#set [status status]
[redirect_mode redirect_mode] [public_prof public_prof] [useipalias
useipalias] [ipalias ipalias] [proto proto] [obj src_ip_obj] [snat_ip
snat_ip] [public_port_start public_port_start] [public_port_end
public_port_end] [private_ip private_ip] [private_ip_end
private_ip_end] [private_port_start private_port_start]
[private_port_end private_port_end] [more_1to1_port more_1to1_port]
Vigor3900@config-nat-pr-<ProfileName># get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of port redirection profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the port redirection profile. [status] – Enter Enable or Disable.
[redirect_mode redirect_mode]	Specify the direction for the port to be redirected. Available options include: ● One_to_One ● Range_to_One ● Range_to_Range_port ● Range_to_Range_IP
[public_prof public_prof]	Specify the WAN profile for such profile. [public_prof] - Enter the name of the WAN profile (e.g., wan_carrie)
[useipalias useipalias]	Determine to use IP alias or not. [useipalias] - Available options include

	● No – No IP alias will be used. ● Single_Alias – Only one IP Alias will be used. ● All – All of the IP address(es) will be used as IP Alias.
[ipalias ipalias]	Enter the IP alias address if Single Alias is selected. [ipalias] - Enter the IP address.
[proto proto]	Specify one protocol for such profile. [proto] - Enter TCP, UDP, or TCP/UDP.
[obj src_ip_obj]	Specify source IP address(es). [src_ip_obj] – Enter the name of IP object profile.
[snat_ip snat_ip]	Change the source IP as the new IP address specified here. [snat_ip] – Enter an IP address.
[public_port_start public_port_start]	It is available when Range to One or Range to Range (port) or Range to Range (IP) is selected as Port Redirection Mode. [public_port_start] - Enter starting number of the public port.
[public_port_end public_port_end]	It is available when Range to One or Range to Range (port) or Range to Range (IP) is selected as Port Redirection Mode. <public_port_end> - Enter ending number of the public port.
[private_ip private_ip]	Specify the private IP address of the internal host providing the service. [private_ip]- Enter a private IP address.
[private_ip_end private_ip_end]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_ip_end]- Enter a private IP address.
[private_port_start private_port_start]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_port_start] - Enter a starting number of the private port.
[private_port_end private_port_end]	It is available when Range to Range (IP) is selected as Port Redirection Mode. [private_port_end]- Enter the number of the private port.
[more_1to1_port more_1to1_port]	It is available when One to One is selected as Port Redirection Mode. It allows to configure more port numbers. [more_ltol_port]- Enter a number.

Example

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# ?
Vigor3900@config-nat# port_redirect add status enable port_r_david
Vigor3900@config-nat-pr-port_r_david# set status enable
more_1to1_port 10

set done

Vigor3900@config-nat-pr-port_r_david#
```

6.6.2 Telnet Command: dmz

Users could use [dmz] command to configure DMZ Host to add or delete the profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-nat#dmz add <ProfileName>
Vigor3900@config-nat#dmz delete <ProfileName>
Vigor3900@config-nat#dmz show
Vigor3900@config-nat#dmz show <ProfileName>
Vigor3900@config-nat#dmz <ProfileName>
```

Command	Description
dmz add <ProfileName>	Add a new DMZ profile. <ProfileName> - Enter the name of DMZ profile.
dmz delete <ProfileName>	Remove a selected DMZ profile. <ProfileName> - Enter the name (e.g., dmz_carrie) of DMZ profile to be deleted.
dmz show	Display the status for all DMZ profiles.
dmz show <ProfileName>	Display the status of selected DMZ profile. <ProfileName> - Enter the name (e.g., dmz_carrie) of DMZ profile.
dmz <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., dmz_carrie) of DMZ profile to be modified.

Example

In this example, we create a DMZ profile named with "dmz_carrie".

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# dmz add dmz_carrie
Vigor3900@config-nat-dmz-dmz_carrie#
```

6.6.2.1 Telnet Command: dmz add ?

To configure detailed settings for a DMZ host profile, users could use [dmz add] to create a new DMZ host profile **with detailed settings**.

Syntax

```
Vigor3900@config-nat#dmz add [status status] [prof prof] [useipalias
useipalias] [ipalias ipalias] [ip private_ip] [allow_access
allow_access] [dst_ip_obj dst_ip_obj] [dst_ip_grp dst_ip_grp]
[servicetype servicetype] <ProfileName>
```

Command	Description
[status status]	Enable or Disable the DMZ profile. [status] – Enter Enable or Disable.

[prof prof]	Specify a WAN profile for data outgoing. [prof] - Enter the name of WAN profile (e.g., wan_carrie).
[useipalias useipalias]	Enable or disable the IP Alias function. [useipalias] - Enter Enable or Disable.
[ipalias ipalias]	If IP Alias is enabled, specify an IP alias for such profile. [ipalias] - Enter the IP address you want.
[ip private_ip]	Set the IP address of the DMZ host. [private_ip] - Enter the IP address.
[allow_access allow_access]	Make DMZ host access into the network. [allow_access] - Enter Enable or disable.
[dst_ip_obj dst_ip_obj]	Specify an IP object to apply such profile. [dst_ip_obj] - Enter the name of the object profile.
[dst_ip_grp dst_ip_grp]	Specify an IP group to apply such profile. [dst_ip_grp] - Enter the name of the object group profile.
[servicetype servicetype]	Specify a user defined service type to apply such profile. [servicetype] - Enter the name of the service type.
<ProfileName>	< ProfileName > - Enter the name (e.g., dmz_david) of DMZ profile.

Example

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# dmz add status enable prof wan_carrie useipalias
disable ip 192.168.2.65 allow_access enable dmz_david
Vigor3900@config-nat-dmz-dmz_david#
Vigor3900@config-nat-dmz-dmz_david# get

status              : Enable
prof                : wan_carrie
useipalias          : Disable
ipalias             : 0.0.0.0
ip                  : 192.168.2.65
allow_access        : Enable
dst_ip_obj          :
dst_ip_grp          :
servicetype         :
```

6.6.2.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected DMZ profile (e.g., dmz_david).

Syntax

```
Vigor3900@config-nat-dmz-<ProfileName>#set status <status> prof <prof>
useipalias <useipalias> ipalias <ipalias> ip <private_ip> allow_access
```

```
<allow_access> dst_ip_obj <dst_ip_obj> dst_ip_grp <dst_ip_grp>
servicetype <servicetype>
```

```
Vigor3900@config-nat-dmz-<ProfileName>#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of DMZ profile.
set	Modify settings for the selected profile.
[status status]	Enable or Disable the DMZ profile. [status] – Enter Enableor Disable.
[prof prof]	Specify a WAN profile for data outgoing. [prof] - Enter the name of WAN profile (e.g., wan_carrie).
[useipalias useipalias]	Enable or disable the IP Alias function. [useipalias] - Enter Enable or Disable.
[ipalias ipalias]	If IP Alias is enabled, specify an IP alias for such profile. [ipalias] - Enter the IP address you want.
[ip private_ip]	Set the IP address of the DMZ host. [private_ip] - Enter the IP address.
[allow_access allow_access]	Make DMZ host access into the network. [allow_access] - Enter Enable or disable.
[dst_ip_obj dst_ip_obj]	Specify an IP object to apply such profile. [dst_ip_obj] - Enter the name of the object profile.
[dst_ip_grp dst_ip_grp]	Specify an IP group to apply such profile. [dst_ip_grp] - Enter the name of the object group profile.
[servicetype servicetype]	Specify a user defined service type to apply such profile. [servicetype] - Enter the name of the service type.

Example

In this example, we create a DMZ profile named with “dmz_david”.

```
Vigor3900>enable
Vigor3900# configure nat
Vigor3900@config-nat# dmz dmz_david
Vigor3900@config-nat-dmz-dmz_david#set prof wan1
Set done
Vigor3900@config-nat-dmz-dmz_david# get

status              : Enable
prof                : wan1
useipalias          : Disable
ipalias             : 0.0.0.0
ip                  : 192.168.2.65
allow_access        : Enable
dst_ip_obj          :
```

```
dst_ip_grp          :
servicetype         :
```

6.7 Objects Setting Configuration

Vigor3900 provides many functions in Objects Setting.Users could use the commands below to set up the details.

To make object setting configuration, you have to type "*configure object_setting*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
.
```

There are several functions for object settings. Available sub-commands under Object Setting include:

- fext_object (refer to 6.7.1)
- ip_group (refer to 6.7.2)
- ip_object (refer to 6.7.3)
- keyword_object (refer to 6.7.4)
- service_group (refer to 6.7.5)
- service_object (refer to 6.7.6)
- time_group (refer to 6.7.7)
- time_object (refer to 6.7.8)
- web_category (refer to 6.7.9)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.7.1 Telnet Command: fext_object

Users could use [fext_object] command to add or delete the File Extension Object profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#fext_object add <ProfileName>
Vigor3900@config-object#fext_object delete <ProfileName>
Vigor3900@config-object#fext_object show
Vigor3900@config-object#fext_object show <ProfileName>
Vigor3900@config-object#fext_object <ProfileName>
```

Command	Description
fext_object add <ProfileName>	Add a new File Extension Object profile. <ProfileName> - Enter the name of File Extension Object profile.
fext_object delete <ProfileName>	Remove a selected File Extension Object profile. <ProfileName> - Enter the name (e.g., fex_obj_carrie) of File

	Extension Object profile to be deleted.
fext_object show	Display the status for all File Extension Object profiles.
fext_object show <ProfileName>	Display the status of selected File Extension Object profile. <ProfileName> - Enter the name (e.g., fex_obj_carrie) of File Extension Object profile.
fext_object <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., fex_obj_carrie) of File Extension Object profile to be modified.

Example

In this example, we create an object profile named with “fex_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#fext_object add fex_obj_carrie
Vigor3900@config-object-fext-fex_obj_carrie#
```

6.7.1.1 Telnet Command: fext_object add ?

To configure detailed settings for a File Extension Object profile, users could use [fext_object add] to create a new File Extension Object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object# fext_object add [image image] [video video]
[audio audio] [java java] [activex activex] [zip zip] [exe exe]
<ProfileName>
```

Command	Description
`[image image]`	Specify the image file extension. [image] - Available settings include: .bmp/.dib/.gif/.jpeg/.jpg/.jpg2/.jp2/.pct/.pcx/.pic/.pict/.png/.tif/.tiff
`[video video]`	Specify the video file extension. [video] - Available settings include: .asf/.avi/.mov/.mpe/.mpeg/.mpg/.mp4/.qt/.rm/.wmv/.3gp/.3gpp/.3gpp2/.3g2
`[audio audio]`	Specify the audio file extension. [audio] - Available settings include: .aac/.aiff/.au/.mp3/.m4a/.m4p/.ogg/.ra/.ram/.vox/.wav/.wma
`[java java]`	Specify the JAVA file extension. [java] - Available settings include: .class/.jad/.jar/.jav/.java/.jcm/.js/.jse/.jsp/.jtk
`[activex activex]`	Specify the ActiveX file extension. [activx] - Available settings include: .alx/.apb/.axs/.ocx/.olb/.ole/.tlb/.viv/.vrm
`[zip zip]`	Specify the ZIP file extension. [zip] - Available settings include:

	.ace/.arj/.bzip2/.bz2/.cab/.gz/.gzip/.rar/.sit/.zip
[exe exe]	Specify the execution file extension. [exe] - Available settings include: .bas/.bat/.com/.exe/.inf/.pif/.reg/.scr
<ProfileName>	< ProfileName > - Enter the name (e.g., fex_obj_david) of File Extension Object profile.

Example

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# fext_object add image .bmp java .class
exe .bat fex_obj_david
Vigor3900@config-object-fext-fex_obj_david#
```

6.7.1.2 Telnet Command: add, remove, get

It is used for reviewing the detailed settings or modifying settings for the selected File Extension Object profile (e.g., fex_obj_david).

Syntax

```
Vigor3900@config-object-<ProfileName>#get
```

```
Vigor3900@config-object-<ProfileName>#activex add <activex_ext>
Vigor3900@config-object-<ProfileName>#activex remove <activex_ext>
Vigor3900@config-object-<ProfileName>#audio add <audio_ext>
Vigor3900@config-object-<ProfileName>#audio remove <audio_ext>
Vigor3900@config-object-<ProfileName>#compression add
<compression_ext>
Vigor3900@config-object-<ProfileName>#compression remove
<compression_ext>
Vigor3900@config-object-<ProfileName>#execution add <execution_ext>
Vigor3900@config-object-<ProfileName>#execution remove <execution
_ext>
Vigor3900@config-object-<ProfileName>#image add <image_ext>
Vigor3900@config-object-<ProfileName>#image remove <image_ext>
Vigor3900@config-object-<ProfileName>#java add <java_ext>
Vigor3900@config-object-<ProfileName>#java remove <java_ext>
Vigor3900@config-object-<ProfileName>#video add <video_ext>
Vigor3900@config-object-<ProfileName>#video remove <video_ext>
```

Command	Description
get	Display current setting status of the selected profile.
activex add <activex_ext>	Add a new type to such profile. Specify a type for adding onto ActiveX file extension. <activex_ext> - Specify ActiveX file extension. Available settings include: .alx/.apb/.axs/.ocx/.olb/.ole/.tlb/.viv/.vrm
activex remove <activex_ext>	Remove a type from the profile. <activex_ext> - Available settings include:

	.alx/.apb/.axs/.ocx/.olb/.ole/.tlb/.viv/.vrm
audio add <audio_ext>	Add a new type to such profile. <audio_ext> - Specify the audio file extension. Available settings include: .aac/.aiff/.au/.mp3/.m4a/.m4p/.ogg/.ra/.ram/.vox/.wav/.wma
audio remove <audio_ext>	Remove a type from the profile. <audio_ext> - Specify the audio file extension. Available settings include: .aac/.aiff/.au/.mp3/.m4a/.m4p/.ogg/.ra/.ram/.vox/.wav/.wma
compression add <compression_ext>	Add a new type to such profile. <compression_ext> - Specify the compression file extension. Available settings include: .ace/.arj/.bzip2/.bz2/.cab/.gz/.gzip/.rar/.sit/.zip
compression remove <compression_ext>	Remove a type from the profile. <compression_ext> - Specify the compression file extension. Available settings include: .ace/.arj/.bzip2/.bz2/.cab/.gz/.gzip/.rar/.sit/.zip
execution add <execution_ext>	Add a new type to such profile. <execution_ext> - Specify the compression file extension. Available settings include: .bas/.bat/.com/.exe/.inf/.pif/.reg/.scr
execution remove <execution_ext>	Remove a type from the profile. <execution_ext> - Specify the compression file extension. Available settings include: .bas/.bat/.com/.exe/.inf/.pif/.reg/.scr
image add <image_ext>	Add a new type to such profile. <image_ext> - Specify the image file extension. Available settings include: .bmp/.dib/.gif/.jpeg/.jpg/.jpg2/.jp2/.pct/.pcx/.pic/.pict/.png/.tif/.tiff
image remove <image_ext>	Remove a type from the profile. <image_ext> - Specify the image file extension. Available settings include: .bmp/.dib/.gif/.jpeg/.jpg/.jpg2/.jp2/.pct/.pcx/.pic/.pict/.png/.tif/.tiff
java add <java_ext>	Add a new type to such profile. <java_ext> - Specify the JAVA file extension. Available settings include: .class/.jad/.jar/.jav/.java/.jcm/.js/.jse/.jsp/.jtk
java remove <java_ext>	Remove a type from the profile. <java_ext> - Specify the JAVA file extension. Available settings include: .class/.jad/.jar/.jav/.java/.jcm/.js/.jse/.jsp/.jtk
video add <video_ext>	Add a new type to such profile. <video_ext> - Specify the video file extension. Available settings

	include: .asf/.avi/.mov/.mpe/.mpeg/.mpg/.mp4/.qt/.rm/.wmv/.3gp/.3gpp/.3gpp2/.3g2
video remove <video_ext>	Remove a type from the profile. <video_ext> - Specify the video file extension. Available settings include: .asf/.avi/.mov/.mpe/.mpeg/.mpg/.mp4/.qt/.rm/.wmv/.3gp/.3gpp/.3gpp2/.3g2

Example

In this example, we create a file extension profile named with “fex_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object# fext_object fex_obj_david
Vigor3900@config-object-fext-fex_obj_david#get
Vigor3900@config-object-fext-fex_obj_david# image add .gif
Vigor3900@config-object-fext-fex_obj_david# get
image       : .bmp, .gif
video       :
audio       :
java        : .class
activex     :
zip         :
exe         : .bat

Vigor3900@config-object-fext-fex_obj_david# image remove .gif
Vigor3900@config-object-fext-fex_obj_david# get

image       : .bmp
video       :
audio       :
java        : .class
activex     :
zip         :
exe         : .bat

Vigor3900@config-object-fext-fex_obj_david#
```

6.7.2 Telnet Command: ip_group

Users could use [ip_group] command to configure IP Group to add or delete the profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#ip_group add <ProfileName>
Vigor3900@config-object#ip_group delete <ProfileName>
Vigor3900@config-object#ip_group show
Vigor3900@config-object#ip_group show <ProfileName>
Vigor3900@config-object#ip_group <ProfileName>
```

Command	Description
ip_group add <ProfileName>	Add a new IP group profile. <ProfileName> - Enter the name of IP group profile.
ip_group delete <ProfileName>	Remove a selected IP group profile. <ProfileName> - Enter the name (e.g., ip_grp_carrie) of IP group profile to be deleted.
ip_group show	Display the status for all IP group profiles.
ip_group show <ProfileName>	Display the status of selected IP group profile. <ProfileName> - Enter the name (e.g., ip_grp_carrie) of IP group profile.
ip_group <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., ip_grp_carrie) of IP group profile to be modified.

Example

In this example, we create an IP group profile named with “ip_grp_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_group add ip_grp_carrie
Vigor3900@config-object-ipgrp-ip_grp_carrie#
```

6.7.2.1 Telnet Command: ip_group add ?

To configure detailed settings for an IP group profile, users could use [ip_group add] to create a new IP group profile **with detailed settings**.

Syntax

```
Vigor3900@config-object#ip_group add [desc description] <ProfileName>
```

Command	Description
[desc description]	[description] - Enter a brief description for this profile.
<ProfileName>	< ProfileName > - Enter the name (e.g., ip_grp_david) of IP Object profile.

Example

In this example, we create an IP group profile named with “ip_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_group add desc testing ip_grp_david
Vigor3900@config-object-ipgrp-ip_grp_david# get
desc            : testing
obj             :
Vigor3900@config-object-ipgrp-ip_grp_david#
```

6.7.2.2 Telnet Command: set, objects, get

It is used for reviewing the detailed settings or modifying settings for the selected IP group profile (e.g., ip_grp_david).

Syntax

```
Vigor3900@config-object-ipgrp-<ProfileName>#set [desc description]
Vigor3900@config-object-ipgrp-<ProfileName>#objects add <member>
Vigor3900@config-object-ipgrp-<ProfileName>#objects remove <member>
Vigor3900@config-object-ipgrp-<ProfileName>#get
```

Command	Description
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[desc description]	Enter a brief description for this profile. [description] – Enter the description.
objects add <member>	Add a new IP object profile to such group profile. [member] – Enter the name of the IP object.
objects remove <member>	Remove an IP object profile from the selected group profile. [member] – Enter the name of the IP object.

Example

In this example, we create an IP group profile named with “ip_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_group add desc testing ip_grp_david
Vigor3900@config-object# ip_group add desc testing ip_grp_david
Vigor3900@config-object-ipgrp-ip_grp_david# get
desc            : testing
obj             :
Vigor3900@config-object-ipgrp-ip_grp_david#
Vigor3900@config-object-ipgrp-ip_grp_david# objects add IP_carrieg
Vigor3900@config-object-ipgrp-ip_grp_david# get

desc              : testing
obj               : IP_carrie

Vigor3900@config-object-ipgrp-ip_grp_david#
```

6.7.3 Telnet Command: ip_object

Users could use [ip_object] command to add or delete the IP Object profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#ip_object add <ProfileName>
Vigor3900@config-object#ip_object delete <ProfileName>
Vigor3900@config-object#ip_object show
Vigor3900@config-object#ip_object show <ProfileName>
Vigor3900@config-object#ip_object <ProfileName>
```

Command	Description
ip_object add <ProfileName>	Add a new IP Object profile. <ProfileName> - Enter the name of IP Object profile.
ip_object delete <ProfileName>	Remove a selected IP Object profile. <ProfileName> - Enter the name (e.g., ip_obj_carrie) of IM Object profile to be deleted.
ip_object show	Display the status for all IP Object profiles.
ip_object show <ProfileName>	Display the status of selected IP Object profile. <ProfileName> - Enter the name (e.g., ip_obj_carrie) of IP Object profile.
ip_object <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., ip_obj_carrie) of IP Object profile to be modified.

Example

In this example, we create an IP object profile named with “ip_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_object add ip_obj_carrie
Vigor3900@config-object-ipobj-ip_obj_carrie#
```

6.7.3.1 Telnet Command: ip_object add ?

To configure detailed settings for an IP Object profile, users could use [ip_object add] to create a new IP Object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object#ip_object add [type type] [sip start_ip] [eip
end_ip] [mask mask] <ProfileName>
```

Command	Description
[type type]	Specify the address type for the IP object. [type] – Available settings include: ● Single – If it is selected, please set [sip start_ip]. ● Range – If it is selected, please set [sip start_ip] and eip [eip end_ip]. ● Subnet – If it is selected, please set [mask mask].
[sip start_ip]	Specify an IP address as the starting point. [start_ip] – Enter an IP address.
[eip end_ip]	Specify an IP address as the ending point. [end_ip]- Enter an IP address.
[mask mask]	Specify an IP address as Subnet Mask. [mask] – Enter the subnet mask.
<ProfileName>	< ProfileName > - Enter the name (e.g., ip_obj_david) of IP

	Object profile.

Example

In this example, we create an IP object profile named with “ip_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_object add type single sip 192.168.1.72
ip_obj_david
Vigor3900@config-object-ipobj-ip_obj_david#
```

6.7.3.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected profile (e.g., ip_obj_david).

Syntax

```
Vigor3900@config-object-ipobj-<ProfileName>#set [type type] [sip
start_ip] [eip end_ip] [mask mask]
Vigor3900@config-object-ipobj-<ProfileName>#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[type type]	Specify the address type for the IP object. [type] - Available settings include: ● Single – If it is selected, please set [sip start_ip]. ● Range – If it is selected, please set [sip start_ip] and eip [eip end_ip]. ● Subnet – If it is selected, please set [mask mask].
[sip start_ip]	Specify an IP address as the starting point. [start_ip] – Enter an IP address.
[eip end_ip]	Specify an IP address as the ending point. [end_ip]- Enter an IP address.
[mask mask]	Specify an IP address as Subnet Mask. [mask] – Enter the subnet mask.

Example

In this example, we create an IP object profile named with “ip_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#ip_object add type single sip 192.168.1.72
ip_obj_david  Vigor3900@config-object-ipobj-ip_obj_david#
Vigor3900@config-object-ipobj-ip_obj_david# get

type               : Single
```

```
sip               : 192.168.1.72
eip               :
mask              :
```

6.7.4 Telnet Command: keyword_object

Users could use [keyword_object] command to add or delete keyword object profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#
```

```
Vigor3900@config-object#keyword_object add <ProfileName>
Vigor3900@config-object#keyword_object delete <ProfileName>
Vigor3900@config-object#keyword_object show
Vigor3900@config-object#keyword_object show <ProfileName>
Vigor3900@config-object#keyword_object <ProfileName>
```

Command	Description
keyword_object add <ProfileName>	Add a new keyword object profile. <ProfileName> - Enter the name of keyword object profile.
keyword_object delete <ProfileName>	Remove a selected keyword object profile. <ProfileName> - Enter the name (e.g., key_obj_carrie) of keyword object profile to be deleted.
keyword_object show	Display the status for all keyword object profiles.
keyword_object show <ProfileName>	Display the status of selected keyword object profile. <ProfileName> - Enter the name (e.g., key_obj_carrie) of keyword object profile.
keyword_object <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., key_obj_carrie) of keyword object profile to be modified.

Example

In this example, we create a keyword object profile named with "key_obj_carrie".

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#keyword_object add key_obj_carrie
Vigor3900@config-object-kwobj-key_obj_carrie#
```

6.7.4.1 Telnet Command: keyword_object add ?

To configure detailed settings for a keyword object profile, users could use [keyword_object add] to create a new keyword object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object#keyword_object add [member member]
<ProfileName>
```

Command	Description
[member member]	The object is used to match the keywords in the whole URL. [member]- Enter the string for a keyword.
<ProfileName>	< ProfileName > **-** Enter the name (e.g., key_obj_david) of keyword object profile.

Example

In this example, we create a keyword object profile named with “key_obj_teacher”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object# keyword_object add member great
key_obj_teacher
Vigor3900@config-object-kwobj-key_obj_teacher# get

member             : great

Vigor3900@config-object-kwobj-key_obj_teacher#
```

6.7.4.2 Telnet Command: member, get

It is used for reviewing the detailed settings or modifying settings for the selected keyword object profile (e.g., key_obj_david).

Syntax

```
Vigor3900@config-object-kwobj-<ProfileName>#member add <member>
Vigor3900@config-object-kwobj-<ProfileName>#member remove <member>

Vigor3900@config-object-kwobj-<ProfileName>#get
```

Command	Description
get	Get the configuration of object profile.
member add <member>	Add a string as a keyword and add onto such profile. <member> - Enter a string.
member remove <member>	Remove a keyword from such profile. <member> - Enter a string.

Example

In this example, we create a keyword object profile named with “key_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#keyword_object add key_obj_david
Vigor3900@config-object-kwobj-key_obj_david# member add test
Vigor3900@config-object-kwobj-key_obj_david# get
member             : test
Vigor3900@config-object-kwobj-key_obj_david#
```

6.7.5 Telnet Command: service_group

Users could use [service_group] command to add or delete the Service Group profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#service_group add <ProfileName>
Vigor3900@config-object#service_group delete <ProfileName>
Vigor3900@config-object#service_group show
Vigor3900@config-object#service_group show <ProfileName>
Vigor3900@config-object#service_group <ProfileName>
```

Command	Description
service_group add <ProfileName>	Add a new service group profile. <ProfileName> - Enter the name of service group profile.
service_group delete <ProfileName>	Remove a selected ervice group profile. <ProfileName> - Enter the name (e.g., ser_grp_carrie) of service group profile to be deleted.
service_group show	Display the status for all service group profiles.
service_group show <ProfileName>	Display the status of selected service group profile. <ProfileName> - Enter the name (e.g., ser_grp_carrie) of service group profile.
service_group <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., ser_grp_carrie) of service group profile to be modified.

Example

In this example, we create a service group profile named with "ser_grp_carrie".

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#service_group add ser_grp_carrie
Vigor3900@config-object-srvgrp-ser_grp_carrie#
```

6.7.5.1 Telnet Command: service_group add ?

To configure detailed settings for a service group profile, users could use [service_group add] to create a new service group profile **with detailed settings**.

Syntax

```
Vigor3900@config-object# service_group add [desc description]
<ProfileName>
```

Command	Description
[desc description]	Set a brief description for such service group. [description] – Enter the description.
<ProfileName>	< ProfileName > - Enter the name (e.g., ser_grp_david) of service group profile.

Example

In this example, we create a service group profile named with “ser_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object# service_group add desc combine_all
ser_grp_david
Vigor3900@config-object-srvgrp-ser_grp_david#
```

6.7.5.2 Telnet Command: set, objects, get

It is used for reviewing the detailed settings or modifying settings for the selected service group profile (e.g., ser_grp_david).

Syntax

```
Vigor3900@config-object-srvgrp-<ProfileName>#set [desc description]
Vigor3900@config-object-srvgrp-<ProfileName>#objects add <member>
Vigor3900@config-object-srvgrp-<ProfileName>#objects remove <member>
Vigor3900@config-object-srvgrp-<ProfileName>#get
```

Command	Description
get	Get the configuration of object profile.
[desc description]	Enter a brief description for such group.
objects add <member>	Add a new service object profile (e.g., ser_obj_carrie) to such group profile. <member> - Enter the name of service object profile.
objects remove <member>	Remove a service object profile from the selected group profile. <member> - Enter the name of service object profile.

Example

In this example, we create a service group profile named with “ser_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object# service_group add desc combine_all
ser_grp_david
Vigor3900@config-object-srvgrp-ser_grp_david# objects add
ser_obj_carrie
Vigor3900@config-object-srvgrp-ser_grp_david# get

desc              : combine_all
obj               : ser_obj_carrie

Vigor3900@config-object-srvgrp-ser_grp_david#
```

6.7.6 Telnet Command: service_object

Users could use [service_object] command to add or delete the Service Type Object profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#service_object add <ProfileName>
Vigor3900@config-object#service_object delete <ProfileName>
Vigor3900@config-object#service_object show
Vigor3900@config-object#service_object show <ProfileName>
Vigor3900@config-object#service_object <ProfileName>
```

Command	Description
service_object add <ProfileName>	Add a new service object profile. <ProfileName> - Enter the name of service object profile.
service_object delete <ProfileName>	Remove a selected service object profile. <ProfileName> - Enter the name (e.g., ser_obj_carrie) of service object profile to be deleted.
service_object show	Display the status for all service object profiles.
service_object show <ProfileName>	Display the status of selected service object profile. <ProfileName> - Enter the name (e.g., ser_obj_carrie) of service object profile.
service_object <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., ser_obj_carrie) of service object profile to be modified.

Example

In this example, we create a service object profile named with “ser_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# service_object add ser_obj_carrie
Vigor3900@config-object-srvobj-ser_obj_carrie#
```

6.7.6.1 Telnet Command: service_object add ?

To configure detailed settings for a service object profile, users could use [service_object add] to create a new service object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object#service_object add [proto protocol] [spt_start
src_port_start] [spt_end src_port_end] [dpt_start dest_port_start]
[dpt_end dest_port_end] <ProfileName>
```

Command	Description
[proto protocol]	Speicify a protocol for such object. [protocol] - Available settings include: ● TCP/UDP ● TCP ● UDP ● ICMP
[spt_start src_port_start]	Enter a value as starting point for source port. [src_port_start] - Enter a number (range from 0 – 65535)
[spt_end	Enter a value as the ending point for source port.

src_port_end]	[src_port_end] - Enter a number (range from 0 – 65535)
[dpt_start dest_port_start]	Enter a value as starting point for destination port. [dest_port_start] - Enter a number (range from 0 – 65535)
[dpt_end dest_port_end]	Enter a value as ending point for destination port. [dest_port_end] - Enter a number (range from 0 – 65535)
<ProfileName>	< ProfileName > - Enter the name (e.g., pro_obj_david) of service object profile.

Example

In this example, we create a protocol object profile named with “ser_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#service_object add proto TCP/UDP
ser_obj_david
Vigor3900@config-object-srvobj-ser_obj_david#
```

6.7.6.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected service object profile (e.g., ser_obj_david).

Syntax

```
Vigor3900@config-object-srvobj-<ProfileName>#proto [proto protocol]
[spt_start src_port_start] [spt_end src_port_end] [dpt_start
dest_port_start] [dpt_end dest_port_end]
Vigor3900@config-object-srvobj-<ProfileName>#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[proto protocol]	Speicify a protocol for such object. [protocol] - Available settings include: ● TCP/UDP ● TCP ● UDP ● ICMP
[spt_start src_port_start]	Enter a value as starting point for source port. [src_port_start] - Enter a number (range from 0 – 65535)
[spt_end src_port_end]	Enter a value as the ending point for source port. [src_port_end] - Enter a number (range from 0 – 65535)
[dpt_start dest_port_start]	Enter a value as starting point for destination port. [dest_port_start] - Enter a number (range from 0 – 65535)
[dpt_end dest_port_end]	Enter a value as ending point for destination port. [dest_port_end] - Enter a number (range from 0 – 65535)

Example

In this example, we create a service object profile named with “ser_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#service_object add proto TCP/UDP
ser_obj_david
Vigor3900@config-object-srvobj-ser_obj_david# get
proto           : TCP/UDP
spt_start       : 1
spt_end         : 65535
dpt_start       : 1
dpt_end         : 65535
Vigor3900@config-object-srvobj-ser_obj_david#set proto TCP/UDP
spt_start 50
set done
Vigor3900@config-object-srvobj-ser_obj_david# get
proto           : TCP/UDP
spt_start       : 50
spt_end         : 65535
dpt_start       : 1
dpt_end         : 65535
```

6.7.7 Telnet Command: time_group

Users could use [time_group] command to add or delete the Time Group profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#time_group add <ProfileName>
Vigor3900@config-object#time_group delete <ProfileName>
Vigor3900@config-object#time_group show
Vigor3900@config-object#time_group show <ProfileName>
Vigor3900@config-object#time_group <ProfileName>
```

Command	Description
time_group add <ProfileName>	Add a new time group profile. <ProfileName> - Enter the name of time group profile.
time_group delete <ProfileName>	Remove a selected time group profile. <ProfileName> - Enter the name (e.g., time_grp_carrie) of time group profile to be deleted.
time_group show	Display the status for all time group profiles.
time_group show <ProfileName>	Display the status of selected time group profile. <ProfileName> - Enter the name (e.g., time_grp_carrie) of time group profile.
time_group <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., time_grp_carrie) of time group profile to be modified.

Example

In this example, we create a time group profile named with “time_grp_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object# time_group add time_grp_carrie
Vigor3900@config-object-timegrp-time_grp_carrie#
```

6.7.7.1 Telnet Command: time_group add ?

To configure detailed settings for a time group profile, users could use [time_group add] to create a new time group profile **with detailed settings**.

Syntax

```
Vigor3900@config-object#time_group [desc description] <ProfileName>
```

Command	Description
[desc description]	Enter a brief description for such group.
<ProfileName>	< ProfileName > - Enter the name (e.g., time_grp_david) of time group profile.

Example

In this example, we create a time group profile named with “time_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#time_group add desc gameplay time_grp_david
Vigor3900@config-object-timegrp-time_grp_david#
```

6.7.7.2 Telnet Command: set, objects, get

It is used for reviewing the detailed settings or modifying settings for the selected time group profile (e.g., time_grp_david).

Syntax

```
Vigor3900@config-object-timegrp-<ProfileName>#set [desc description]
Vigor3900@config-object-timegrp-<ProfileName>#objects add <member>
Vigor3900@config-object-timegrp-<ProfileName>#objects remove <member>
Vigor3900@config-object-timegrp-<ProfileName>#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[desc description]	Enter a brief description for such group.
objects add <member>	Add a new time object profile (e.g., time_obj_carrie) to such group profile. <member> - Enter the name of the object profile.
objects remove <member>	Remove a time object profile from the selected group profile. <member> - Enter the name of the object profile.

Example

In this example, we create a service object profile named with “time_grp_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#time_group add desc gameplay time_grp_david
Vigor3900@config-object-timegrp-time_grp_david#objects add
time_obj_carrie
Vigor3900@config-object-timegrp-time_grp_david#objects add
time_obj_david
Vigor3900@config-object-timegrp-time_grp_david#get
desc            : gameplay_time
obj             : time_obj_carrie, time_obj_david
Vigor3900@config-object-timegrp-time_grp_david#
```

6.7.8 Telnet Command: time_object

Users could use [time_object] command to add or delete the Time Object profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#time_object add <ProfileName>
Vigor3900@config-object#time_object delete <ProfileName>
Vigor3900@config-object#time_object show
Vigor3900@config-object#time_object show <ProfileName>
Vigor3900@config-object#time_object <ProfileName>
```

Command	Description
time_object add <ProfileName>	Add a new time object profile. <ProfileName> - Enter the name of time object profile.
time_object delete <ProfileName>	Remove a selected time object profile. <ProfileName> - Enter the name (e.g., time_obj_carrie) of time object profile to be deleted.
time_object show	Display the status for all time object profiles.
time_object show <ProfileName>	Display the status of selected time object profile. <ProfileName> - Enter the name (e.g., time_obj_carrie) of time object profile.
time_object <ProfilenName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., time_obj_carrie) of time object profile to be modified.

Example

In this example, we create a time object profile named with “time_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# time_object add time_obj_carrie
Vigor3900@config-object-timeobj-time_obj_carrie#
```

6.7.8.1 Telnet Command: time_object add ?

To configure detailed settings for a time object profile, users could use [time_object add] to create a new time object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object# time_object add [freq frequency] [sdate
startdate] [stime starttime] [edate enddate] [etime endtime]
<ProfileName>
```

Command	Description
[freq frequency]	Define the work frequency. [frequency] - Available settings include: ● Once ● Weekdays
[sdate startdate]	Define the starting date for such time object. [startdate] - Enter the data with the format of "YYYY-MM-DD", e.g. 1979-01-01
[stime starttime]	Define the starting time for such time object. [starttime] - Enter the time with the format of "HH:MM:MM", e.g. 23:59:59
[edate enddate]	Define the ending date for such time object. [enddate] - Enter the data with the format of "YYYY-MM-DD", e.g. 1979-01-01
[etime endtime]	Define the ending time for such time object. [endtime] - Enter the time with the format of "HH:MM:MM", e.g. 23:59:59
<ProfileName>	< ProfileName > - Enter the name (e.g., time_obj_david) of time object profile.

Example

In this example, we create a time object profile named with "time_obj_david".

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# time_object add freq once time_obj_david
Vigor3900@config-object-timeobj-time_obj_david#
```

6.7.8.2 Telnet Command: set, weekdays, get

It is used for reviewing the detailed settings or modifying settings for the selected time object profile (e.g., time_obj_david).

Syntax

```
Vigor3900@config-object-timeobj-<ProfileName>#set [freq frequency]
[sdate startdate] [stime starttime] [edate enddate] [etime endtime]
Vigor3900@config-object-timeobj-<ProfileName>#weekdays add <weekdays>
Vigor3900@config-object-timeobj-<ProfileName>#weekdays remove
<weekdays>
```

`Vigor3900@config-object-timeobj-<ProfileName>#get`

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[freq frequency]	Define the work frequency. [frequency] - Available settings include: ● Once ● Weekdays
[sdate startdate]	Define the starting date for such time object. [startdate] - Enter the data with the format of "YYYY-MM-DD", e.g. 1979-01-01
[stime starttime]	Define the starting time for such time object. [starttime] - Enter the time with the format of "HH:MM:MM", e.g. 23:59:59
[edate enddate]	Define the ending date for such time object. [enddate] - Enter the data with the format of "YYYY-MM-DD", e.g. 1979-01-01
[etime endtime]	Define the ending time for such time object. [endtime] - Enter the time with the format of "HH:MM:MM", e.g. 23:59:59
weekdays add <weekdays>	Specify which day shall be included in such profile. <weekdays> - Available settings include: ● Mon ● Tue ● Wed ● Thu ● Fri ● Sat ● Sun
weekdays remove <weekdays>	Specify which day shall be removed in such profile. <weekdays> - Available settings include: ● Mon ● Tue ● Wed ● Thu ● Fri ● Sat ● Sun

Example

In this example, we create a service object profile named with "ser_obj_david".

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# time_object add freq once time_obj_david
Vigor3900@config-object-timeobj-time_obj_david#
Vigor3900@config-object-timeobj-time_obj_david# get
freq                : Once
sdate               : 2010-01-01
stime               : 00:00:00
edate               : 2010-01-01
etime               : 00:00:00
weekdays            :
Vigor3900@config-object-timeobj-time_obj_david#set sdate 2017-11-28
stime 12:00:00
set done
Vigor3900@config-object-timeobj-time_obj_david#weekdays add mon
Vigor3900@config-object-timeobj-time_obj_david#get
freq                : Once
sdate               : 2017-11-28
stime               : 12:00:00
edate               : 2010-01-01
etime               : 00:00:00
weekdays            : Mon
Vigor3900@config-object-timeobj-time_obj_david#
```

6.7.9 Telnet Command: web_category

Users could use [web_category] command to add or delete the Web Category Object profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-object#web_category add <ProfileName>
Vigor3900@config-object#web_category delete <ProfileName>
Vigor3900@config-object#web_category show
Vigor3900@config-object#web_category show <ProfileName>
Vigor3900@config-object#web_category <ProfileName>
```

Command	Description
web_categroy add <ProfileName>	Add a new web category object profile. <ProfileName> - Enter the name of web category profile.
web_categroy delete <ProfileName>	Remove a selected web category profile. <ProfileName> - Enter the name (e.g., web_obj_carrie) of web category profile to be deleted.
web_categroy show	Display the status for all web category profiles.
web_categroy show <ProfileName>	Display the status of selected web category profile. <ProfileName> - Enter the name (e.g., web_obj_carrie) of web category profile.
web_categroy	Modify detailed settings for the selected profile.

<ProfilenName>	<ProfileName> - Enter the name (e.g., web_obj_carrie) of web category profile to be modified.

Example

In this example, we create a web category object profile named with “web_obj_carrie”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#web_category add web_obj_carrie
Vigor3900@config-object-webcate-web_obj_carrie#
```

6.7.9.1 Telnet Command: web_category add ?

To configure detailed settings for a web category object profile, users could use [web_category add] to create a new object profile **with detailed settings**.

Syntax

```
Vigor3900@config-object# web_category add [childp child_protect]
[leisure leisure] [business business] [chat chat] [computer computer]
[other other] <ProfileName>
```

Command	Description
[childp child_protect]	Select category to filter the web page for children protection. Available setting include: Alcohol_And_Tobacco/Criminal_And_Activity/Gambling/Hate_And_Intolerance/Illegal_Drug/Nudity/Pornography_And_Sexually_explicit/Violence/Weapons/School_Cheating/Sex_Education/Tasteless/Child_Abuse_Images
[leisure leisure]	Select category to filter the web page related to leisure matters. Available setting include: ● Entertainment ● Games ● Sports ● Travel ● Leisure_And_Recreation ● Fashion_And_Beauty
[business business]	Select category to filter the web page related to business. Available setting include: ● Business ● Job_Search ● Web_Based_Email
[chat chat]	Select category to filter the web page related to chatting tool. Available setting include: ● Chat ● Instant_Messaging
[computer computer]	Select category to filter the web page related to computer. Available setting include: Anonymizers/Forums_And_Newsgroups/Computers_And_Techn

	ology/Down_sites/Streaming_Media_And_Downloads/Phishing_And_Fraud/Search_engines_And_Portals/Social_Networking/Spam_sites/Malware/Botnets/Hacking/Illegal_Softwares/Information_Security/Peer_to_Peer
[other other]	Select category to filter the web page for special purpose. Available setting include: Advertisement_And_Pop_Ups/Arts/Transportation/Compromised/Dating_And_Personals/Education/Finance/Government/Health_And_Medicine/News/Non_profits_And_NGOs/Persional_Sites/Politics/Real_Estate/Religion/Restaurants_And_Dining/Shopping/Translators/General/Cults/Greeting_Cards/Image_Sharing/Network_Errors/Parked_Domains/Private_IP_Address/Uncategorised_Sites
<ProfileName>	< ProfileName > - Enter the name (e.g., web_obj_david) of web category object profile.

Example

In this example, we create a web category object profile named with “web_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# web_category add childp Alcohol_And_Tobacco
web_obj_david
Vigor3900@config-object-webcate-web_obj_david#
```

6.7.9.2 Telnet Command: business, chat, child_protect, computer, leisure, other, get

It is used for reviewing the detailed settings or modifying settings for the selected web category object profile (e.g., web_obj_david).

Syntax

```
Vigor3900@config-object-webcate-<ProfileName>#business add
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#business remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#chat add
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#chat remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#child_protect add
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#child_protect remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#computer add
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#computer remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#leisure add
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#leisure remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#other add
<category_type>
```

```
Vigor3900@config-object-webcate-<ProfileName>#other remove
<category_type>
Vigor3900@config-object-webcate-<ProfileName>#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of object profile.
business add <category_type>	Add a category to such profile. <category_type> - Select a category to filter the web page related to business. Available setting include: ● Business ● Job_Search ● Web_Based_Email
business remove <category_type>	Remove a category from such profile. <category_type> - Select a category to filter the web page related to business. Available setting include: ● Business ● Job_Search ● Web_Based_Email
chat add <category_type>	Add a category to such profile. <category_type> - Select a category to filter the web page related to chatting tool. Available setting include: ● Chat ● Instant_Messaging
chat remove <category_type>	Remove a category from such profile. <category_type> - Select a category to filter the web page related to chatting tool. Available setting include: ● Chat ● Instant_Messaging
child_protect add <category_type>	Add a category to such profile. <category_type> - Select category to filter the web page for children protection. Available setting include: Alcohol_And_Tobacco/Criminal_And_Activity/Gambling/Hate_And_Intolerance/Illegal_Drug/Nudity/Pornography_And_Sexually_explicit/Violence/Weapons/School_Cheating/Sex_Education/Tasteless/Child_Abuse_Images
child_protect remove <category_type>	Remove a category from such profile. <category_type> - Select category to filter the web page for children protection. Available setting include: Alcohol_And_Tobacco/Criminal_And_Activity/Gambling/Hate_And_Intolerance/Illegal_Drug/Nudity/Pornography_And_Sexually_explicit/Violence/Weapons/School_Cheating/Sex_Education/Tasteless/Child_Abuse_Images
computer add <category_type>	Add a category to such profile. <category_type> - Select category to filter the web page related to

	computer. Available setting include: Anonymizers/Forums_And_Newsgroups/Computers_And_Technology/Down_sites/Streaming_Media_And_Downloads/Phishing_And_Fraud/Search_engines_And_Portals/Social_Networking/Spam_sites/Malware/Botnets/Hacking/Illegal_Softwares/Information_Security/Peer_to_Peer
computer remove <category_type>	Remove a category from such profile. <category_type> - Select category to filter the web page related to computer. Available setting include: Anonymizers/Forums_And_Newsgroups/Computers_And_Technology/Down_sites/Streaming_Media_And_Downloads/Phishing_And_Fraud/Search_engines_And_Portals/Social_Networking/Spam_sites/Malware/Botnets/Hacking/Illegal_Softwares/Information_Security/Peer_to_Peer
leisure add <category_type>	Add a category to such profile. <category_type> - Select category to filter the web page related to leisure matters. Available setting include: ● Entertainment ● Games ● Sports ● Travel ● Leisure_And_Recreation ● Fashion_And_Beauty
leisure remove <category_type>	Remove a category from such profile. <category_type> - Select category to filter the web page related to leisure matters. Available setting include: ● Entertainment ● Games ● Sports ● Travel ● Leisure_And_Recreation ● Fashion_And_Beauty
other add <category_type>	Add a category to such profile. <category_type> - Select category to filter the web page for special purpose. Available setting include: Advertisement_And_Pop_Ups/Arts/Transportation/Compromised/Dating_And_Personals/Education/Finance/Government/Health_And_Medicine/News/Non_profits_And_NGOs/Persional_Sites/Politics/Real_Estate/Religion/Restaurants_And_Dining/Shopping/Translators/General/Cults/Greeting_Cards/Image_Sharing/Network_Errors/Parked_Domains/Private_IP_Address/Uncategorised_Sites
other remove <category_type>	Remove a category from such profile. <category_type> - Select category to filter the web page for special purpose. Available setting include: Advertisement_And_Pop_Ups/Arts/Transportation/Compromised/Dating_And_Personals/Education/Finance/Government/Health_A

	nd_Medicine/News/Non_profits_And_NGOs/Persional_Sites/Politics/Real_Estate/Religion/Restaurants_And_Dining/Shopping/Translators/General/Cults/Greeting_Cards/Image_Sharing/Network_Errors/Parked_Domains/Private_IP_Address/Uncategorised_Sites

Example

In this example, we create a web category bject profile named with “web_obj_david”.

```
Vigor3900>enable
Vigor3900# configure object_setting
Vigor3900@config-object#
Vigor3900@config-object# web_category add childp Alcohol_And_Tobacco
web_obj_david
Vigor3900@config-object-webcate-web_obj_david#business add
Web_Based_Email
Vigor3900@config-object-webcate-web_obj_david#computer add
Peer_to_Peer
Vigor3900@config-object-webcate-web_obj_david#leisure add
Leisure_And_Recreation
Vigor3900@config-object-webcate-web_obj_david#get
childp          : Alcohol_And_Tobacco
leisure         : Leisure_And_Recreation
business        : Web_Based_Email
chat            :
computer        : Peer_to_Peer
other           :

Vigor3900@config-object-webcate-web_obj_david#
```

6.8 User Management Configuration

User Management can manage all the accounts (user profiles) to connect to Internet via different protocols.

To make user management configuration, you have to type "*configure user*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user#
.
```

There are several functions for user management – users, group.

Available sub-commands under User include:

- users (refer to 6.8.1)

- group (refer to 6.8.2)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.8.1 Telnet Command: users

Users could use [users] command to add or delete the User Account Profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-user#users add <ProfileName>
Vigor3900@config-user#users delete <ProfileName>
Vigor3900@config-user#users show
Vigor3900@config-user#users show <ProfileName>
Vigor3900@config-user#users <ProfileName>
```

Command	Description
users add <ProfileName>	Add a new user account profile. <ProfileName> - Enter the name of user account profile.
users delete <ProfileName>	Remove a selected user account profile. <ProfileName> - Enter the name (e.g., user_carrie) of user account profile to be deleted.
users show	Display the status for all user account profiles.
users show <ProfileName>	Display the status of selected user account profile. <ProfileName> - Enter the name (e.g., user_carrie) of user account profile.
users <ProfileName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., user_carrie) of user

	account profile to be modified.

Example

In this example, we create a user account profile named with “user_carrie”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user# users add user_carrie
Vigor3900@config-usr-user_carrie#
```

6.8.1.1 Telnet Command: users add ?

To configure detailed settings for a user account profile, users could use [user add] to create a new users account profile **with detailed settings**.

Syntax

```
Vigor3900@config-user# users add [status status] [pass password]
[sysuser sysuser] [group group] [guest_op guest_op] [timeout timeout]
[if pptpif] [fixip fixip] [user_mnt_status user_mnt_status]
[user_enable_time_quota user_enable_time_quota] [user_set_time_quota
user_set_time_quota] [login_quota login_quota] [forced_logout
forced_logout] [pptp pptp] [l2tp l2tp] [ssltunnel ssltunnel] [openvpn
openvpn] [ipsec ipsec] [motp en_motp] [pin motp_pin] [secret motp_secret]
[time_obj time_obj] [sslproxy ssl_proxy] [ssl_vnc ssl_vnc] [ssl_rdp
ssl_rdp] [remote_ip remote_ip] [pppoe pppoe][quota_rst_freq
quota_rst_freq] [quota_time quota_time] [quota_traffic quota_traffic]
[en_bindmac en_bindmac] [bind_mac bind_mac] [vsftpd_status
vsftpd_status][smb smb] [radiusd_status radiusd_status] <ProfileName>
```

Command	Description
[status status]	Enable the user account profile. [status] - Enter Enable or Disable.
[pass password]	Enter a password for such profile to pass the authentication. [password] - Enter characters (number, letter) for a password.
[sysuser sysuser]	Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router. [sysuser] - Enter true (enable the function of System User) or false.
[group group]	If true is selected for sysuser (System User), you have to specify the privilege level (User/Operator/Admin) for such profile. [group] - Enter User / Operator / Admin.
[guest_op guest_op]	If Operator is set as privilege level, set this command as true; otherwise, set false. Set Guest Operator as priviledge level. [guest_op] – Enter True or False.
[timeout timeout]	If the user is idle over the limitation of the timer, the network connection will be stopped for such user. [timeout] - By default, the Idle Timeout is set to 300 seconds.

[if pptpif]	Specify a LAN profile for DHCP server IP dispatching. [pptpif] – Enter the name of the LAN profile.
[fixip fixip]	Assign the fixed IP address when user login via PPTP or L2TP. [fixip] - Enter IP address.
[user_mnt_status user_mnt_status]	Enable web portal login with such profile. [user_mnt_status] - Enter Enable or Disable.
[user_enable_time_quota user_enable_time_quota]	Enable the time quota mechanism for this user account. [user_enable_time_quota] - Enter Enable or Disable.
[user_set_time_quota user_set_time_quota]	Set time quota for this account. [user_set_time_quota] - Enter the time value.
[login_quota login_quota]	Set the maximum number of online user for this account [login_quota] - The range is from 1 to 255. -1 means not limit; 0 means No access.
[forced_logout forced_logout]	Force the earliest user to logout when exceeded the maximum number of online user setting. [forced_logout] – Enter Enable or Disable.
[pptp pptp]	Enable PPTP dial-in function for PPTP server. [pptp] - Enter Enable or Disable.
[l2tp l2tp]	Enable L2TP dial-in function for L2TP server. [l2tp] - Enter Enable or Disable.
[ssltunnel ssltunnel]	Enable SSL Tunnel for SSL server. [ssltunnel] - Enter Enable or Disable.
[openvpn openvpn]	Enable / disable the function of OpenVPN. [openvpn] – Enter Enable or Disable.
[ipsec ipsec]	Enable / disable the function of “XAuth/EAP”. [ipsec] – Enter Enable or Disable.
[motp en_motp]	Enable mOTP function to make the authentication with mOTP. If enabled, mOTP pin and secret shall be specified. [en_motp] - Enter Enable or Disable.
[pin motp_pin]	Specify PIN code for authentication. [motp_pin] - Enter the code for authentication (e.g, 1234).
[secret motp_secret]	Specify initial secret. [motp_secret] - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
[time_obj time_obj]	Specify time objects for the server. [time_obj] - Enter the name of time object profile.
[sslproxy ssl_proxy]	It is available when sysuser **(System User)** is set with **false**. The web proxy over SSL will be applied for VPN.

	[ssl_proxy]- Specify one of the SSL proxy profile.
[ssl_vnc ssl_vnc]	It is available when sysuser **(System User)** is set with **false**. [ssl_vnc] - Specify one of the SSL Application profiles (VNC) for applying into this profile.
[ssl_rdp ssl_rdp]	It is available when sysuser **(System User)** is set with **false**. [ssl_rdp] - Specify one of the SSL Application profiles (RDP) for applying into this profile.
[remote_ip remote_ip]	Specify Remote IP Address/Domain Name for remote dial-in VPN client. [remote_ip] - Enter IP address or domain name.
[pppoe pppoe]	Activate related PPPoE configuration for such profile. [pppoe] - Enter Enable or Disable.
[quota_rst_freq quota_rst_freq]	Specify the cycle time for PPPoE quota. [quota_rst_freq] - Enter None / Everyday / Everymonth.
[quota_time quota_time]	Set a time quota for PPPoE connection. [quota_time] - Enter a time quota (-1~50000, -1 means “unlimit”) for PPPoE connection.
[quota_traffic quota_traffic]	Set the maximum traffic (MB) for such user profile for PPPoE Connection. [quota_traffic] - Enter a number.
[en_bindmac en_bindmac]	Enable the function of PPPoE MAC Binding. [en_bindmac] - Enter Enable or Disable.
[bind_mac bind_mac]	Specify a MAC Address for PPPoE MAC Binding. [bind_mac] - Enter a MAC address.
[vsftpd_status vsftpd_status]	Allow This Account for FTP Server. [vsftpd_status] - Enter Enable or Disable.
[smb smb]	Allow the remote user accessing into Internet via SAMBA server. [smb] - Enter Enable or Disable.
[radiusd_status radiusd_status]	Allow This Account for Radius Server [radiusd_status] - Enter Enable or Disable.
<SectionName>	Enter the name (e.g., user_carrie) of user account profile to be modified.

Example

In this example, we create a user account profile named with “user_david”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user# users add shown_name enable status enable pass
num0123456 sysuser true group user user_david
Vigor3900@config-usr-user_david#
```

6.8.1.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected user account profile (e.g., user_david).

Syntax

```
Vigor3900@config-user-<SectionName># set [status status] [pass password]
[sysuser sysuser] [group group] [guest_op guest_op] [timeout timeout]
[if pptpif] [fixip fixip] [user_mnt_status user_mnt_status]
[user_enable_time_quota user_enable_time_quota] [user_set_time_quota
user_set_time_quota] [login_quota login_quota] [forced_logout
forced_logout] [pptp pptp] [l2tp l2tp] [ssltunnel ssltunnel] [openvpn
openvpn] [ipsec ipsec] [motp en_motp] [pin motp_pin] [secret motp_secret]
[time_obj time_obj] [sslproxy ssl_proxy] [ssl_vnc ssl_vnc] [ssl_rdp
ssl_rdp] [remote_ip remote_ip] [pppoe pppoe] [quota_rst_freq
quota_rst_freq] [quota_time quota_time] [quota_traffic
quota_traffic][en_bindmac en_bindmac] [bind_mac bind_mac]
[vsftpd_status vsftpd_status] [smb smb] [radiusd_status radiusd_status]

Vigor3900@config-user-<SectionNmae># users get
```

Command	Description
<**ProfileName**>	Display the name of the profile.
get	Get the configuration of object profile.
set	Modify settings for the selected profile.
[status status]	Enable the user account profile. [status] - Enter Enable or Disable.
[pass password]	Enter a password for such profile to pass the authentication. [password] - Enter characters (number, letter) for a password.
[sysuser sysuser]	Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router. [sysuser] - Enter true (enable the function of System User) or false.
[group group]	If true is selected for sysuser (System User), you have to specify the privilege level (User/Operator/Admin) for such profile. [group] - Enter User / Operator / Admin.
[guest_op guest_op]	If Operator is set as privilege level, set this command as true; otherwise, set false. Set Guest Operator as priviledge level. [guest_op] – Enter True or False.
[timeout timeout]	If the user is idle over the limitation of the timer, the network connection will be stopped for such user. [timeout] - By default, the Idle Timeout is set to 300 seconds.
[if pptpif]	Specify a LAN profile for DHCP server IP dispatching. [pptpif] – Enter the name of the LAN profile.
[fixip fixip]	Assign the fixed IP address when user login via PPTP or L2TP. [fixip] - Enter IP address.
[user_mnt_status user_mnt_status]	Enable web portal login with such profile. [user_mnt_status] - Enter Enable or Disable.

[user_enable_time_quota user_enable_time_quota]	Enable the time quota mechanism for this user account. [user_enable_time_quota] - Enter Enable or Disable.
[user_set_time_quota user_set_time_quota]	Set time quota for this account. [user_set_time_quota] - Enter the time value.
[login_quota login_quota]	Set the maximum number of online user for this account [login_quota] - The range is from 1 to 255. -1 means not limit; 0 means No access.
[forced_logout forced_logout]	Force the earliest user to logout when exceeded the maximum number of online user setting. [forced_logout] – Enter Enable or Disable.
[pptp pptp]	Enable PPTP dial-in function for PPTP server. [pptp] - Enter Enable or Disable.
[l2tp l2tp]	Enable L2TP dial-in function for L2TP server. [l2tp] - Enter Enable or Disable.
[ssltunnel ssltunnel]	Enable SSL Tunnel for SSL server. [ssltunnel] - Enter Enable or Disable.
[openvpn openvpn]	Enable / disable the function of OpenVPN. [openvpn] – Enter Enable or Disable.
[ipsec ipsec]	Enable / disable the function of “XAuth/EAP”. [ipsec] – Enter Enable or Disable.
[motp en_motp]	Enable mOTP function to make the authentication with mOTP. If enabled, mOTP pin and secret shall be specified. [en_motp] - Enter Enable or Disable.
[pin motp_pin]	Specify PIN code for authentication. [motp_pin] - Enter the code for authentication (e.g, 1234).
[secret motp_secret]	Specify initial secret. [motp_secret] - Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
[time_obj time_obj]	Specify time objects for the server. [time_obj] - Enter the name of time object profile.
[sslproxy ssl_proxy]	It is available when sysuser **(System User)** is set with **false**. The web proxy over SSL will be applied for VPN. [ssl_proxy]- Specify one of the SSL proxy profile.
[ssl_vnc ssl_vnc]	It is available when sysuser **(System User)** is set with **false**. [ssl_vnc] - Specify one of the SSL Application profiles (VNC) for applying into this profile.
[ssl_rdp ssl_rdp]	It is available when sysuser **(System User)** is set with **false**. [ssl_rdp] - Specify one of the SSL Application profiles (RDP) for applying into this profile.

[remote_ip remote_ip]	Specify Remote IP Address/Domain Name for remote dial-in VPN client. [remote_ip] - Enter IP address or domain name.
[pppoe pppoe]	Activate related PPPoE configuration for such profile. [pppoe] - Enter Enable or Disable.
[quota_rst_freq quota_rst_freq]	Specify the cycle time for PPPoE quota. [quota_rst_freq] - Enter None / Everyday / Everymonth.
[quota_time quota_time]	Set a time quota for PPPoE connection. [quota_time] - Enter a time quota (-1~50000, -1 means “unlimit”) for PPPoE connection.
[quota_traffic quota_traffic]	Set the maximum traffic (MB) for such user profile for PPPoE Connection. [quota_traffic] - Enter a number.
[en_bindmac en_bindmac]	Enable the function of PPPoE MAC Binding. [en_bindmac] - Enter Enable or Disable.
[bind_mac bind_mac]	Specify a MAC Address for PPPoE MAC Binding. [bind_mac] - Enter a MAC address.
[vsftpd_status vsftpd_status]	Allow This Account for FTP Server. [vsftpd_status] - Enter Enable or Disable.
[smb smb]	Allow the remote user accessing into Internet via SAMBA server. [smb] - Enter Enable or Disable.
[radiusd_status radiusd_status]	Allow This Account for Radius Server [radiusd_status] - Enter Enable or Disable.

Example

In this example, we create a user account profile named with “user_david”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user# users user_david
Vigor3900@config-usr-user_david#get
shown_name                  : user_tets
status                      : Disable
pass                        : num0123456
sysuser                     : true
group                       : User
timeout                     : 300
if                          : lan1
fixip                       :
user_mnt_status             : Disable
user_enable_time_quota      : Disable
user_set_time_quota         : 1440
login_quota                 : -1
forced_logout               : Disable
pptp                        : Disable
```

```
l2tp                          : Disable
ssltunnel                     : Disable
openvpn                       : Disable
ipsec                         : Disable
motp                          : Disable
pin                           :
secret                        :
time_obj                      :
sslproxy                      :
ssl_vnc                       :
ssl_rdp                       :
remote_ip                     :
pppoe                         : Disable
quota_rst_freq                : None
quota_time                    : -1
time_used                     : 0
quota_traffic                 : -1
traffic_used                  : 0
en_bindmac                    : Disable
bind_mac                      : 00:00:00:00:00:00
vsftpd_status                 : Disable
smb                           : Disable
radiusd_status                : Disable
```

6.8.2 Telnet Command: group

Users could use [group] command to add or delete the User Group Profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-user#group add <ProfileName>
Vigor3900@config-user#group delete <ProfileName>
Vigor3900@config-user#group show
Vigor3900@config-user#group show <ProfileName>
Vigor3900@config-user#group <ProfileName>
```

Command	Description
group add <ProfileName>	Add a new user group profile. <ProfileName> - Enter the name of user group profile.
group delete <ProfileName>	Remove a selected user group profile. <ProfileName> - Enter the name (e.g., user_carrie) of user group profile to be deleted.
group show	Display the status for all user group profiles.
group show <ProfileName>	Display the status of selected user group profile. <ProfileName> - Enter the name (e.g., user_carrie) of user group profile.
group <ProfileName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., user_carrie) of user group

	profile to be modified.

Example

In this example, we create a web category bject profile named with “user_grp_carrie”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user#group add user_grp_carrie
Vigor3900@config-usr-group-user_grp_carrie#
```

6.8.2.1 Telnet Command: group add ?

To configure detailed settings for a user group profile, users could use [gropu add] to create a new time object profile **with detailed settings**.

Syntax

```
Vigor3900@config-user#group add [status status] <ProfileName>
```

Command	Description
[status status]	Enable the user group profile. [status] - Enter Enable or Disable.
<SectionName>	Enter the name (e.g., user_grp_david) of user group profile to be modified.

Example

In this example, we create a user groupprofile named with “user_grp_david”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user# group add status enable user_grp_david
Vigor3900@config-usr-group-user_grp_david#
```

6.8.2.2 Telnet Command: set, get, member

It is used for reviewing the detailed settings or modifying settings for the selected user group profile (e.g., user_grp_david).

Syntax

```
Vigor3900@config-usr-group-<SectionName>#set [status status]
Vigor3900@config-usr-group-<SectionName>#member add <member>
Vigor3900@config-usr-group-<SectionName>#member remove <member>
Vigor3900@config-usr-group-<SectionName>get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of user group profile.
set	Modify settings for the selected profile.
[status status]	Enable the user group profile. [status] - Enter Enable or Disable.

member add <member>	Add a user profile to such group profile. [member] - Enter the name of the user profile.
member remove <member>	Remove a user profile from such group. [member] - Enter the name of the user profile.

Example

In this example, we create a user group profile named with “user_grp_carrie”.

```
Vigor3900>enable
Vigor3900# configure user
Vigor3900@config-user#
Vigor3900@config-user# group user_grp_carrie
Vigor3900@config-usr-group-user_grp_carrie# member add user_carrie
Vigor3900@config-usr-group-user_grp_carrie# get

status             : Disable
member             : user_carrie

Vigor3900@config-usr-group-user_grp_carrie#
```

6.9 Applications Configuration

To make applications configuration, you have to type "*configure applications*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#
.
```

There are several functions for application – DDNS, GVRP, HA, LDAP, OSPF, RIP, SIP ALG, and UPnP.

Available sub-commands under Application include:

- DDNS (refer to 6.9.1)
- GVRP (refer to 6.9.2)
- HA (refer to 6.9.3)
- LDAP (refer to 6.9.4)
- OSPF (refer to 6.9.5)
- RIP (refer to 6.9.6)
- SIP ALG (refer to 6.9.7)
- UPnP (refer to 6.9.8)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.9.1 Telnet Command: DDNS

Users could use [ddns] command to configure Dynamic DNS. Use "show" to get the profile list in the directory, or select the profile, then use the [get] or [set] command to configure the Dynamic DNS details information.

Syntax

```
Vigor3900@config-apps-ddns# set [status status] [if if-name] [policy
if-policy] [provider provider] [stype server_type] [domain domain-name]
[login login-name] [pw password] [ip_source ip_source] [wildcard
wildcard] [backup_mx backup-mx] [mx mail-extender] [time_interval
time_interval] <ProfileName>
Vigor3900@config-apps-ddns# get <profile name>
Vigor3900@config-apps-ddns# show
```

Command	Description
[status status]	Enable the DDNS profile. [status] - Enter Enable or Disable.
[if if-name]	Speicfy the interface that such profile will apply to. [if-name] - Specify WAN profile.

[policy if-policy]	Specify a routing policy applied to DDNS profile. [if-policy] - Available settings include ● selected_wan_first ● selected_wan_only.
[provider provider]	Specify DDNS server provider. [provider] - Available settings include: User-Defined/DrayTek_Global/3322/afraid/changeip/dns4biz/dns dynamic/dnsexit/dnsmax/dnsomatic/dtdns/dy-name-server/dynami /dyndns/editdns/Google_Domains/he.net/huagai/namecheap/no-ip /OpenDNS/ovh/selfhost/strato/thatip/twoddns/tzo/ubddns.org/vigo rddns/zoneedit
[stype server_type]	Specify service type for such DDNS profile. [server_type] - Dynamic / Static / Custom
[domain domain-name]	Specify a domain name for such DDNS profile. It is available when Custom is selected as service type. [domain-name] - Enter the domain name.
[login login-name]	Specify the name for user to login. [login-name]- Enter a name for user to login.
[pw password]	Specify a password for user to login. [password] - Enter a password for user to login.
[ip_source ip_source]	Specify the IP source for the DDNS profile. [ip_source] - Available settings include: ● my_wan_ip ● my_internet_ip
[wildcard wildcard]	Enable or disable the function of wild card. [wildcard] - Enter Enable or Disable.
[backup_mx backup-mx]	Enable or disable the function of Backup MX. [backup-mx] - Enter Enable or Disable.
[mx mail-extender]	Specify the mail extender. [mail-extender] - Enter the IP or domain name of the mail server.
[time_interval time_interval]	Set the time for the router to perform auto update for DDNS service. [time_interval] - Range from 1 ~ 43200. The unit is minute.
<ProfileName>	Specify a DNS profile (ddns1 to ddns10).
get <profile name>	Display current setting status of the selected profile. <profile name> – Range from “ddns1” to “ddns0”.
show	Display current setting status for all of the DDNS profiles.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#ddns
```

```
Vigor3900@config-apps-ddns#
Vigor3900@config-apps-ddns# set status enable ddns1
set done
Vigor3900@config-apps-ddns# get ddns1

status              : Disable
if                  : wan1
policy              : selected_wan_first
provider            : dyndns
stype               : Dynamic
domain              :
login               :
pw                  :
ip_source           : 0
wildcard            : Disable
backup_mx           : Disable
mx                  :
time_interval       : 14400
status              : 0
Vigor3900@config-apps-ddns#
```

6.9.2 Telnet Command: GVRP

Users could use [gvrp] command to define a method for changing the VLAN information among device.

Syntax

```
Vigor3900@config-app#gvrp set [status status] [interface interface]
[join_time join_time]
Vigor3900@config-app#gvrp get
```

Command	Description
get	Get the configuration of GVRP.
set	Modify settings for the GVRP.
[status status]	Enable the function of GVRP. [status] - Enter Enable or Disable.
[interface interface]	Speicfy the interface for sending GVRP packet. [interface] - Specify LAN or WAN profile.
[join_time join_time]	Set the time for the system to send GVRP packet to other device. [join_time] - Any value (e.g., 20). The unit is “second”.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#
Vigor3900@config-app# gvrp set status enable

set done
```

```
Vigor3900@config-app# gvrp set interface lan_carrie

set done

Vigor3900@config-app# gvrp set join_time 20

set done

Vigor3900@config-app#
```

6.9.3 Telnet Command: HA

Users could use [ha] command to configure High Availability, then use the [get] or [set] command to configure the High Availability information.

Syntax

`Vigor3900@config-app#ha set [lan lan] [HS_priority HS_priority] [vip vip] [vhid vhid]>`

`Vigor3900@config-app#ha get`

Command	Description
get	Get the configuration of HA.
set	Modify settings for HA.
[lan lan]	Specify a LAN profile
[HS_priority HS_priority]	Specify the priority of such HA. [HS_priority] - "1" has the highest priority. For example, Vigor router with the priority of "1" shall play the role of Master device.
[vip vip]	Speicfy the virtual IP for such HA. [vip] - Enter an IP address as virtual IP.
[vhid vhid]>	Speicy the virtual host ID for such HA. [vhid] - Enter a number as VHID. VHID is used for Backup router to identify which Master will be backed up.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#
Vigor3900@config-app# ha set lan lan_carrie HS_priority 2
Vigor3900@config-app# ha get
lan                 :
HS_priority         : 2
vip                 :
vhid                : 1
ha_profile_status   :
Vigor3900@config-app#
```

6.9.4 Telnet Command: ldap

Users could use [ldap] command to configure LDAP profile.

Syntax

```
Vigor3900@config-app#ldap add <ProfileName>
Vigor3900@config-app#ldap delete <ProfileName>
Vigor3900@config-app#ldap show
Vigor3900@config-app#ldap show <ProfileName>
Vigor3900@config-app#ldap <ProfileName>
```

Command	Description
ldap add <ProfileName>	Add a new profile. <ProfileName> - Enter the name of LDAP profile.
ldap delete <ProfileName>	Remove a selected profile. <ProfileName> - Enter the name (e.g., ldap_carrie) of LDAP profile to be deleted.
ldap show	Display the status for all profiles.
ldap show <ProfileName>	Display the status of selected profile. <ProfileName> - Enter the name (e.g., ldap_carrie) of LDAP profile.
ldap <ProfileName>	Modify detailed settings for the selected profile. <ProfileName> - Enter the name (e.g., ldap_carrie) of LDAP profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#
Vigor3900@config-app# ldap add ldap_carrie
Vigor3900@config-app-ldap-ldap_carrie#
```

6.9.4.1 Telnet Command: ldap add ?

To configure detailed settings for an LDAP profile, users could use [ldap add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-app# ldap add [status status] [status status]
[bind_type bind_type] [server_ip server_ip][port port] [cid cid]
[base_dn base_dn] [group_dn group_dn] [regular_dn regulardn]
[regular_pwd regular_pwd] [usage_time usage_time] <ProfileName>
```

Command	Description
[status status]	The first [status status] command is used to enable/disable LDAP function. [status]- Enter Enable or Disable.
[status status]	The second [status status] command is used to enable/disable LDAP with TLS.

	[status]- Enter Enable or Disable.
[bind_type bind_type]	Specify the Bind Type. [bind_type] – Available settings include: ● Simple_Mode ● Anonymous ● Regular_Mode
[server_ip server_ip]	Specify the IP address of LDAP server. [server_ip] – Enter the IPv4 address.
[port port]	Specify a port number for LDAP server. [port] – Enter a port number.
[cid cid]	Define common name identifier. [cid]- Enter a name. The common name identifier for most LDAP server is “cn”.
[base_dn base_dn]	Define base distinguished name. [base_dn] – Enter a name.
[group_dn group_dn]	Define group distinguished name. [group_dn] – Enter a name.
[regular_dn regulardn]	Define regular distinguished name. [regular_dn] – Enter this setting if Regular Mode is selected as Bind Type.
[regular_pwd regular_pwd]	Define regular password. [regular_pwd] – Enter a string as password if Regular Mode is selected as Bind Type.
[usage_time usage_time]	Define a value as default usage time. [usage_time] – Enter a time value. The unit is minute.
<ProfileName>	Set a new name for LDAP profile.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app# ldap add status enable bind_type simple_mode
port 5601 ladp_carrie
Vigor2960@config-app-ldap-ladp_carrie#
```

6.9.4.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected LDAP profile (e.g., ldap_david).

Syntax

```
Vigor3900@config-app-ldap-<ProfileName>#set [status status] [status
status] [bind_type bind_type] [server_ip server_ip][port port] [cid cid]
[base_dn base_dn] [group_dn group_dn] [regular_dn regulardn]
[regular_pwd regular_pwd] [usage_time usage_time]
Vigor3900@config-app-ldap#get
```

Command	Description
<ProfileName>	Display the name of the profile.
get	Get the configuration of profile.
set	Modify settings for the profile.
[status status]	The first [status status] command is used to enable/disable LDAP function. [status]- Enter Enable or Disable.
[status status]	The second [status status] command is used to enable/disable LDAP with TLS. [status]- Enter Enable or Disable.
[bind_type bind_type]	Specify the Bind Type. [bind_type] - Available settings include: ● Simple_Mode ● Anonymous ● Regular_Mode
[server_ip server_ip]	Specify the IP address of LDAP server. [server_ip] - Enter the IPv4 address.
[port port]	Specify a port number for LDAP server. [port] - Enter a port number.
[cid cid]	Define common name identifier. [cid]- Enter a name. The common name identifier for most LDAP server is “cn”.
[base_dn base_dn]	Define base distinguished name. [base_dn] - Enter a name.
[group_dn group_dn]	Define group distinguished name. [group_dn] - Enter a name.
[regular_dn regulardn]	Define regular distinguished name. [regular_dn] - Enter this setting if Regular Mode is selected as Bind Type.
[regular_pwd regular_pwd]	Define regular password. [regular_pwd] - Enter a string as password if Regular Mode is selected as Bind Type.
[usage_time usage_time]	Define a value as default usage time. [usage_time] - Enter a time value. The unit is minute.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#ldap
Vigor3900@config-app-ldap#get
status              : Disable
status              : disable
```

```
bind_type           : 0
server_ip           :
port                : 389
cid                 : cn
base_dn             :
group_dn            :
regular_dn          :
regular_pwd         :
usage_time          : -1
Vigor3900@config-app-ldap#ldap ldap_carrie
Vigor3900@config-app-ldap-ldap_carrie# set status enable bind_type
Simple_Mode
set done

Vigor3900@config-app-ldap-ldap_carrie# get

status              : Enable
status              : Enable
bind_type           : Simple_Mode
server_ip           : 0.0.0.0
port                : 389
cid                 : cn
base_dn             :
group_dn            :
regular_dn          :
regular_pwd         :
usage_time          : -1
```

6.9.5 Telnet Command: ospf

Users could use [ospf] command to configure OSPF setting.

Syntax

```
Vigor3900@config-app-ospf#pf add <profile> <area>
Vigor3900@config-app-ospf#set [status status] [router_id router_id] [pf
profile]
Vigor3900@config-app-ospf#get
```

Command	Description
add	Add a profile to support OSPF.
get	Get the configuration of profile.
set	Modify settings for the profile.
<profile>	Create a new profile. <profile> - Enter a name of WAN/LAN profile.
<area>	<area> - An AS will be divided into several areas. Each area must be assigned with a dedicated number.
[status status]	Enable the OSPF function. [status] - Enter Enable or Disable.

[router_id router_id]	Specify an IP address for Vigor router which will be recognized in an autonomous system. [router_id] - Enter an IP address (e.g., 192.168.1.56).
[pf profile]	[profile] - Enter the name of LAN/WAN profile.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#ospf
Vigor3900@config-app-ospf#pf add wan1
Vigor3900@config-app-ospf#pf add wan2 11
Vigor3900@config-app-ospf#get
status              : Disable
router_id           :
pf                  : wan2 11
```

6.9.6 Telnet Command: rip

Users could use [rip] command to configure RIP setting.

Syntax

```
Vigor3900@config-app-rip#pf add <profile>
Vigor3900@config-app-rip#set [status status] [pf profile]
Vigor3900@config-app-rip#get
```

Command	Description
pf add	Add a profile to support add RIP.
get	Get the configuration for RIP.
set	Modify settings for RIP.
<profile>	<profile> - Enter a name for WAN/LAN profile to support RIP function.
[status status]	Enable the RIP function. [status] - Enter Enable or Disable.
[pf profile]	[profile] - Enter the name of LAN/WAN profile.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#rip
Vigor3900@config-app-rip#pf add wan1
Vigor3900@config-app-rip#get
status          : Disable
pf              : wan1
Vigor3900@config-app-rip#set status enable pf wan1
```

6.9.7 Telnet Command: SIP ALG

Users could use [sipalg] command to configure SIP ALG setting.

Syntax

```
Vigor3900@config-app-sipalg#set [status status] [sip_port sip_port]
Vigor3900@config-app-sipalg#get
```

Command	Description
get	Get the configuration for SIP ALG.
set	Modify settings for for SIP ALG.
[status status]	Enable the function of UPnP. [status] - Enter Enable or Disable.
[sip_port sip_port]	Set a port number for SIP ALG. [sip_port] - Enter a value (ranging from 1 to 65535). Default value is 5060.

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#sipalg
Vigor3900@config-app-sipalg#get
status             : Disable
sip_port           : 5060
```

6.9.8 Telnet Command: UPnP

Users could use [upnp] command to configure UPnP.User could use the [get] or [set] command to configure the UPnP details information.

Syntax

```
Vigor3900@config-app-upnp# set [status status] [download download]
[upload upload] [external external] [inernal internal] [max_session
max_session]
Vigor3900@config-app-upnp#get
```

Command	Description
get	Get the configuration for UPnP.
set	Modify settings for for UPnP.
[status status]	Enable the function of UPnP. [status] - Enter Enable or Disable.
[download download]	Enter the maximum sustained WAN download speed in kilobits/second. [download] - Enter the speed rate (in kpbs).
[upload upload]	Enter the maximum sustained WAN upload speed in kilobits/second. [download] - Enter the speed rate (in kpbs).
[external external]	Select a WAN profile for UPnP protocol.

	[external] - Enter the name of the WAN profile.
[inernal internal]	Select a LAN profile for UPnP protocol. [internal] - Enter the name of LAN profile.
[max_session max_session]	Determine the maximum session number for UPnP function. [max_session] - Enter the number for maximum session (20 – 1000).

Example

```
Vigor3900>enable
Vigor3900# configure applications
Vigor3900@config-app#upnp
Vigor3900@config-app-upnp#set status enable download 1000 upload 100
external wan1 internal lan1 max_session 1000
Set done
Vigor3900@config-app-upnp#get
status              : Enable
download            : 1000
upload              : 100
external            : wan1
internal            : lan1
max_session         : 1000
```

6.10 VPN Configuration

VPN (Virtual Private Network) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, user 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.

Vigor3900 provides three functions in VPN – LAN-to-LAN, remote dial-in and VPN trunk.Users could use the commands below to set up the details.

To make VPN configuration, you have to type "*configure vpn*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
```

There are several functions for VPN configuration – LAN to LAN, Remote Dial In, Trunk and Virtual System.

- lan2lan (refer to 6.10.1)
- remotedialin (refer to 6.10.2)
- trunk (refer to 6.10.3)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.10.1 Telnet Command: lan2lan

Users could use [lan2lan] command to configure LAN to LAN, then use [ipsecpolicy], [ipsecsetup], [pptpdialin], [pptpdialout] commands to set the details.

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#
```

6.10.1.1 Telnet Command: ipsecpolicy

Users could use [ipsecpolicy] command to add or delete the IPSec Policy profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-vpn-l2l# ipsecpolicy add <SectionName>
Vigor3900@config-vpn-l2l# ipsecpolicy delete <SectionName>
Vigor3900@config-vpn-l2l# ipsecpolicy show
Vigor3900@config-vpn-l2l# ipsecpolicy show <SectionName>
Vigor3900@config-vpn-l2l# ipsecpolicy <SectionName>
```

Command	Description
ipsecpolicy add <SectionName>	Add a new LAN to LAN profile. <SectionName>- Enter the name of LAN to LAN profile.
ipsecpolicy delete <SectionName>	Remove a selected LAN to LAN profile. <SectionName> - Enter the name (e.g., l2l_carrie) of LAN to LAN profile to be deleted.
ipsecpolicy show	Display the status for all LAN to LAN profiles.
ipsecpolicy show <SectionName>	Display the status of selected LAN to LAN profile. <SectionName>> - Enter the name (e.g., l2l_carrie) of LAN to LAN profile.
ipsecpolicy <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., l2l_carrie) of LAN to LAN profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l# ipsecpolicy add l2l_carrie
Vigor3900@config-vpn-l2l# ipsecpolicy l2l_carrie
Vigor3900@config-vpn-l2l-ipsecpolicy-l2l_carrie#
```

Telnet Command: ipsecpolicy add ?

To configure detailed settings for a LAN to LAN profile, users could use [ipsecpolicy add] to create a new profile with detailed settings.

Syntax

```
Vigor3900@config-vpn-l2l# ipsecpolicy add [status status] [always_on
always_on][always_on_agent always_on_agent] [always_on_bk
always_on_bk][for_remote_dialin for_remote_dialin] [dummy_wan_alias
dummy_wan_alias][lefthost_if_alias_ip
lefthost_if_alias_ip][lefthost_if_alias lefthost_if_alias]
[lefthost_if lefthost_if][lefthost_if_bk lefthost_if_bk][localsubnet
localsubnet] [localnext localnext] [remotehostremotehost][remotesubnet
remotesubnet] [more_remotesubnet more_remotesubnet][ike_mode
ike_mode][aggrmode aggrmode][auth auth][leftpem leftpem][localid_type
localid][peerid_type remoteid][peerid_value remoteid]
[peerid_value_cert cert][psk psk][leftid localid] [rightid remoteid]
[secret_type secret_type][phase1keylifetime phase1keylifetime]
[phase2keylifetime phase2keylifetime][pfs pfs][dpd dpd] [dpddelay
dpddelay][dpdtimeout dpdtimeout][ping ping][pinghost pinghost][natmode
natmode][srcip srcip] [enable_netmap enable_netmap] [leftclient_nat
leftclient_nat][enable_def_route enable_def_route] [nbns_pass
nbns_pass][mcast_pass mcast_pass][rip_pass rip_pass] [pkt_trigger
pkt_trigger] [forceencaps forceencaps] [gre gre][localgreip
localgreip][remotegreip remotegreip] [autogrekey autogrekey][grekeyin
grekeyin] [grekeyout grekeyout] [ikephase1proposal ikephase1proposal]
[ikephase1authproposal ikephase1authproposal][ikephase2proposal
ikephase2proposal][ikephase2authproposal ikephase2authproposal]
[acceptall acceptall] <SectionName>
```

Command	Description
add	Create a new LAN to LAN profile based on IPsec policy.
[status status]	Enable the LAN to LAN profile. [status] - Enter Enable or Disable.
[always_on always_on]	Enable the function of Always On. If it is disabled, [always_on_bk] will be invalid. [status] - Enter Enable or Disable.
[always_on_agent always_on_agent]	Enable the function of Always On. [status] - Enter Enable or Disable.
[always_on_bk always_on_bk]	When the select WAN profile is down, such LAN to LAN profile be used for dialing-out. [status] – Available settings include: ● Empty ● Any WAN profile (e.g., wan1, wan_carrie, wan_david)
[for_remote_dialin for_remote_dialin]	Enable / disable to set remote dial-in for such profile. [status] - Enter Enable or Disable.
[lefthost_if_alias_ip lefthost_if_alias_ip]	Specify one WAN Alias IP. [lefthost_if_alias_ip] – Enter the IP address (configured as WAN Alias IP).
[lefthost_if_alias lefthost_if_alias]	Enable / disable the function of WAN Alias IP. [lefthost_if_alias] – Enter Enable or Disable.
[lefthost_if lefthost_if]	Specify the WAN interface for dialing out. [lefthost] – Enter the name of WAN profile.
[lefthost_if _bk lefthost_if_bk]	Specify WAN interface as backup WAN (failover WAN). [lefthost_if_bk]- Enter WAN interface profile.

[localsubnet localsubnet]	Specify subnet for local host. [localsubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[localnext localnext]	Specify the gateway for WAN interface. [localnext] – Enter the IP address.
[remotehost remotehost]	Specify an IP address for remote host. [remotehost] – Enter the IP address.
[remotesubnet remotesubnet]	Specify the subnet mask for the remote host. [remotesubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[more_remotesubnet more_remotesubnet]	Add more subnets for remotel host. [localsubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[ike_mode ike_mode]	Specify IKE Phase 1 protocol. [ike_mode] – Available settings are: ● IKEv1 ● IKEv2
[aggrmode aggrmode]	Specify the aggressive mode for IKEv1 Phase 1. [aggrmode] – Available settings are: ● Main_Mode ● Aggressive_Mode
[auth auth]	Specify the authentication type for Pre-Shared Key or RSA Signature. [auth]- Available settings are: ● PSK ● RSA
[leftpem leftpem]	Specify local certificate. It should be specified when RSA is selected as “auth” type. [leftpem] – Enter the name of local certificate.
[localid_type localid]	Specify local peer ID. [localid] – Available settings are: ● SubjectName ● SubjectAlternativeName
[peerid_type remoteid]	Specify peer ID type for remote end by entering the required string. [remoteid] – Available settings are: ● AcceptAny ● SubjectAlterName:IP ● SubjectAlterName:DomainName ● SubjectAlterName:Email ● Certificate
[peerid_value	Set the value for the remote client, if “2”, “3” or “4” is set as peer

remoteid]	ID type. [remoteid] – Enter the IP address, Domain name or Email of remote client (based on the ID type selected for peer side).
[peerid_value_cert cert]	Set the value for the remote client, if “5” is set as peer ID type. [cert] – Enter the name of certificate.
[psk psk]	Specify a key for IKE authentication if PSK is selected as Auth Type. [psk] – Enter the key.
[leftid localid]	Set a string as local ID if “PSK” is set as authentication type and “Aggressive_Mode” is set as Aggressive mode. [localid] – Enter a string.
[rightid remoteid]	Set a string as remote ID if “PSK” is set as authentication type and “Aggressive_Mode” is set as Aggressive mode. [remoteid] – Enter a string.
[secret_type secret_type]	Specify the security protocol. [secret_type] – Available settings are: ● ESP ● AH
[phase1keylifetime phase1keylifetime]	Specify the life time for IKE Phase 1 key. [phase1keylifetime] – Enter a number (from 3600 to 86400 sec.).
[phase2keylifetime phase2keylifetime]	Specify the life time for IKE Phase 2 key. [phase2keylifetime] –Enter a number (from 3600 to 86400 sec.).
[pfs pfs]	Enable / disable the perfect forward secrecy status [pfs] – Enter Enable or Disable.
[dpd dpd]	Enable / disable the dead peer detection (DPD) status. [dpd] – Enter Enable or Disable.
[dpddelay dpddelay]	Set keep-alive timer for the DPD delay. [dpddelay] – Enter a number. Default is 30 (sec.).
[dpdtimeout dpdtimeout]	Specify the timeout timer for DPD. [dpdtimeout] - Enter a number. Default is 120 (sec.).
[ping ping]	Enable / disable the function of Ping to Keeep Alive. [ping] – Enter Enable or Disable.
[pinghost pinghost]	Specify the IP address for the system to PING it for keeping alive. [pinghost] – Enter the IPv4 address.
[natmode natmode]	Specify NAT mode for LAN subnet to remote network. [natmode] – Available settings are: ● Route ● NAT
[srcip srcip]	Specify the source IP address for the router to use when transmitting a packet to the remote IPsec gatway. [srcip] – Available settings include:

	● Enter “auto_detect_srcip”. ● Enter the name of a LAN profile.
[enable_netmap enable_netmap]	Enable NAT mapping function. [enable_netmap] – Enter Enable or Disable.
[leftclient_nat leftclient_nat]	Specify an IP address with subnet mask of the network that all traffic will be translated into. [leftclient_nat] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[enable_def_route enable_def_route]	Change the default route to such tunnel (LAN to LAN profile). [enable_def_route] - Enter Enable or Disable.
[nbns_pass nbns_pass]	Enable / disable the function of passing NetBios Naming Packet. [nbns_pass] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of passing RIP packet via VPN. [rip_pass] - Enter Enable or Disable.
[pkt_trigger pkt_trigger]	Enable / disable the function of Packet-Triggered. [pkt_trigger] - Enter Enable or Disable
[forceencaps forceencaps]	Enable / disable the function of Force UDP Encapsulation with 4500 port. [forceencaps] - Enter Enable or Disable.
[gre gre]	Enable / disable the GRE function. [gre] - Enter Enable or Disable.
[localgreip localgreip]	Specify local GRE IP address. [localgreip] – Enter the IPv4 address.
[remotegreip remotegreip]	Specify remote GRE IP address. [remotegreip] – Enter the IPv4 address.
[autogrekey autogrekey]	Enable / disable the function of generating GRE key automatically. [autogrekey] - Enter Enable or Disable.
[grekeyin grekeyin]	Specify the GRE in key. [grekeyin] – Enter the key.
[grekeyout grekeyout]	Specify the GRE out key. [grekeyout] – Enter the key.
[ikephase1proposal ikephase1proposal]	Specify the IKE phase1 proposal. [ikephase1proposal] – Availale settings are: ● DES_G1 ● DES_G2 ● DES_G5 ● DES_G14 ● 3DES_G1

	● 3DES_G2 ● 3DES_G5 ● 3DES_G14 ● AES128_G1 ● AES128_G2 ● AES128_G5 ● AES128_G14 ● AES192_G1 ● AES192_G2 ● AES192_G5 ● AES192_G14 ● AES256_G1 ● AES256_G2 ● AES256_G5 ● AES256_G14
[ikephase1authproposal ikephase1authproposal]	Specify the authentication mofe for IKE phase1. [ikephase1authproposal] – Available settings are: ● ALL ● MD5 ● SHA1 ● SHA2_256
[ikephase2proposal ikephase2proposal]	Specify the proposal mofe for IKE phase2. [ikephase2proposal] – Available settings are: ● DES_without_Auth ● DES_with_auth ● 3DES_without_auth ● 3DES_with_auth ● AES128_without_auth ● AES128_with_auth ● AES192_without_auth ● AES192_with_auth ● AES256_without_auth ● AES256_with_auth
[ikephase2authproposal ikephase2authproposal]	Specify the authentication mofe for IKE phase2. [ikephase2authproposal] – Available settings are: ● ALL ● MD5 ● SHA1 ● SHA2_256
[acceptall acceptall]	Specify the proposal for dial-in. [acceptall]- Available settings are: ● acceptall

	● acceptabove
<SectionName>	Specify a name for LAN to LAN profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l# ipsecpolicy add status enable always_on
enable vpn_l2l_carrie
Vigor3900@config-vpn-l2l#
```

Telnet Command: set, get, connect, disconnect

It is used for reviewing the detailed settings or modifying settings for the selected LAN to LAN profile (e.g., l2l_carrie).

Syntax

```
Vigor3900@config-vpn-l2l-ipsecpolicy-<SectionName>#connect
Vigor3900@config-vpn-l2l-ipsecpolicy-<SectionName>#disconnect
Vigor3900@config-vpn-l2l-ipsecpolicy-<SectionName>#get
Vigor3900@config-vpn-l2l-ipsecpolicy-<SectionName>#set [status status]
[always_on always_on][always_on_agent always_on_agent] [always_on_bk
always_on_bk][for_remote_dialin for_remote_dialin] [dummy_wan_alias
dummy_wan_alias] [lefthost_if_alias_ip
lefthost_if_alias_ip][lefthost_if_alias lefthost_if_alias]
[lefthost_if lefthost_if][lefthost_if_bk lefthost_if_bk][localsubnet
localsubnet] [localnext localnext] [remotehostremotehost][remotesubnet
remotesubnet] [more_remotesubnet more_remotesubnet][ike_mode
ike_mode][aggrmode aggrmode][auth auth][leftpem leftpem][localid_type
localid][peerid_type remoteid][peerid_value remoteid]
[peerid_value_cert cert][psk psk][leftid localid] [rightid
remoteid][secret_type secret_type] [phase1keylifetime
phase1keylifetime] [phase2keylifetime phase2keylifetime][pfs pfs][dpd
dpd] [dpddelay dpddelay][dpdtimeout dpdtimeout][ping ping][pinghost
pinghost][natmode natmode][srcip srcip] [enable_netmap enable_netmap]
[leftclient_nat leftclient_nat] [enable_def_route enable_def_route]
[nbns_pass nbns_pass][mcast_pass mcast_pass][rip_pass rip_pass]
[pkt_trigger pkt_trigger] [forceencaps forceencaps] [gre
gre][localgreip localgreip][remotegreip remotegreip] [autogrekey
autogrekey][grekeyin grekeyin] [grekeyout grekeyout]
[ikephase1proposal ikephase1proposal] [ikephase1authproposal
ikephase1authproposal][ikephase2proposal ikephase2proposal]
[ikephase2authproposal ikephase2authproposal] [acceptall acceptall]
```

Command	Description
<SectionName>	Display the name of the profile.
connect	Initiate the LAN to LAN profile based on IPsec policy.
disconnect	Terminate the LAN to LAN profile based on IPsec policy.
get	Get the configuration of LAN to LAN profile.
set	Modify settings for the selected LAN to LAN profile.
[status status]	Enable the LAN to LAN profile.

	[status] - Enter Enable or Disable.
[always_on always_on]	Enable the function of Always On. If it is disabled, [always_on_bk] will be invalid. [status] - Enter Enable or Disable.
[always_on_agent always_on_agent]	Enable the function of Always On. [status] - Enter Enable or Disable.
[always_on_bk always_on_bk]	When the select WAN profile is down, such LAN to LAN profile be used for dialing-out. [status] – Available settings include: ● Empty ● Any WAN profile (e.g., wan1, wan_carrie, wan_david)
[for_remote_dialin for_remote_dialin]	Enable / disable to set remote dial-in for such profile. [status] - Enter Enable or Disable.
[lefthost_if_alias_ip lefthost_if_alias_ip]	Specify one WAN Alias IP. [lefthost_if_alias_ip] – Enter the IP address (configured as WAN Alias IP).
[lefthost_if_alias lefthost_if_alias]	Enable / disable the function of WAN Alias IP. [lefthost_if_alias] – Enter Enable or Disable.
[lefthost_if lefthost_if]	Specify the WAN interface for dialing out. [lefthost_if] – Enter the name of WAN profile.
[lefthost_if _bk lefthost_if_bk]	Specify WAN interface as backup WAN (failover WAN). [lefthost_if_bk]- Enter WAN interface profile.
[localsubnet localsubnet]	Specify subnet for local host. [localsubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[localnext localnext]	Specify the gateway for WAN interface. [localnext] – Enter the IP address.
[remotehost remotehost]	Specify an IP address for remote host. [remotehost] – Enter the IP address.
[remotesubnet remotesubnet]	Specify the subnet mask for the remote host. [remotesubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[more_remotesubnet more_remotesubnet]	Add more subnets for remotel host. [localsubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[ike_mode ike_mode]	Specify IKE Phase 1 protocol. [ike_mode] – Available settings are: ● IKEv1 ● IKEv2
[aggrmode aggrmode]	Specify the aggressive mode for IKEv1 Phase 1. [aggrmode] – Available settings are:

	● Main_Mode ● Aggressive_Mode
[auth auth]	Specify the authentication type for Pre-Shared Key or RSA Signature. [auth]- Available settings are: ● PSK ● RSA
[leftpem leftpem]	Specify local certificate. It should be specified when RSA is selected as “auth” type. [leftpem] – Enter the name of local certificate.
[localid_type localid]	Specify local peer ID. [localid] – Available settings are: ● SubjectName ● SubjectAlternativeName
[peerid_type remoteid]	Specify peer ID type for remote end by entering the required string. [remoteid] – Available settings are: ● AcceptAny ● SubjectAlterName:IP ● SubjectAlterName:DomainName ● SubjectAlterName:Email ● Certificate
[peerid_value remoteid]	Set the value for the remote client, if “2”, “3” or “4” is set as peer ID type. [remoteid] – Enter the IP address, Domain name or Email of remote client (based on the ID type selected for peer side).
[peerid_value_cert cert]	Set the value for the remote client, if “5” is set as peer ID type. [cert] – Enter the name of certificate.
[psk psk]	Specify a key for IKE authentication if PSK is selected as Auth Type. [psk] – Enter the key.
[leftid localid]	Set a string as local ID if “PSK” is set as authentication type and “Aggressive_Mode” is set as Aggressive mode. [localid] – Enter a string.
[rightid remoteid]	Set a string as remote ID if “PSK” is set as authentication type and “Aggressive_Mode” is set as Aggressive mode. [remoteid] – Enter a string.
[secret_type secret_type]	Specify the security protocol. [secret_type] – Available settings are: ● ESP ● AH
[phase1keylifetime phase1keylifetime]	Specify the life time for IKE Phase 1 key.

	[phase1keylifetime] – Enter a number (from 3600 to 86400 sec.).
[phase2keylifetime phase2keylifetime]	Specify the life time for IKE Phase 2 key. [phase2keylifetime] –Enter a number (from 3600 to 86400 sec.).
[pfs pfs]	Enable / disable the perfect forward secrecy status [pfs] – Enter Enable or Disable.
[dpd dpd]	Enable / disable the dead peer detection (DPD) status. [dpd] – Enter Enable or Disable.
[dpddelay dpddelay]	Set keep-alive timer for the DPD delay. [dpddelay] – Enter a number. Default is 30 (sec.).
[dpdtimeout dpdtimeout]	Specify the timeout timer for DPD. [dpdtimeout] - Enter a number. Default is 120 (sec.).
[ping ping]	Enable / disable the function of Ping to Keeep Alive. [ping] – Enter Enable or Disable.
[pinghost pinghost]	Specify the IP address for the system to PING it for keeping alive. [pinghost] – Enter the IPv4 address.
[natmode natmode]	Specify NAT mode for LAN subnet to remote network. [natmode] – Available settings are: ● Route ● NAT
[srcip srcip]	Specify the source IP address for the router to use when transmitting a packet to the remote IPsec gatway. [srcip] – Available settings include: ● Enter “auto_detect_srcip”. ● Enter the name of a LAN profile.
[enable_netmap enable_netmap]	Enable NAT mapping function. [enable_netmap] – Enter Enable or Disable.
[leftclient_nat leftclient_nat]	Specify an IP address with subnet mask of the network that all traffic will be translated into. [leftclient_nat] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[enable_def_route enable_def_route]	Change the default route to such tunnel (LAN to LAN profile). [enable_def_route] - Enter Enable or Disable.
[nbns_pass nbns_pass]	Enable / disable the function of passing NetBios Naming Packet. [nbns_pass] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of passing RIP packet via VPN. [rip_pass] - Enter Enable or Disable.
[pkt_trigger pkt_trigger]	Enable / disable the function of Packet-Triggered. [pkt_trigger] - Enter Enable or Disable

[forceencaps forceencaps]	Enable / disable the function of Force UDP Encapsulation with 4500 port. [forceencaps] - Enter Enable or Disable.
[gre gre]	Enable / disable the GRE function. [gre] - Enter Enable or Disable.
[localgreip localgreip]	Specify local GRE IP address. [localgreip] – Enter the IPv4 address.
[remotegreip remotegreip]	Specify remote GRE IP address. [remotegreip] – Enter the IPv4 address.
[autogrekey autogrekey]	Enable / disable the function of generating GRE key automatically. [autogrekey] - Enter Enable or Disable.
[grekeyin grekeyin]	Specify the GRE in key. [grekeyin] – Enter the key.
[grekeyout grekeyout]	Specify the GRE out key. [grekeyout] – Enter the key.
[ikephase1proposal ikephase1proposal]	Specify the IKE phase1 proposal. [ikephase1proposal] – Availale settings are: ● DES_G1 ● DES_G2 ● DES_G5 ● DES_G14 ● 3DES_G1 ● 3DES_G2 ● 3DES_G5 ● 3DES_G14 ● AES128_G1 ● AES128_G2 ● AES128_G5 ● AES128_G14 ● AES192_G1 ● AES192_G2 ● AES192_G5 ● AES192_G14 ● AES256_G1 ● AES256_G2 ● AES256_G5 ● AES256_G14
[ikephase1authproposal ikephase1authproposal]	Specify the authentication mofe for IKE phase1. [ikephase1authproposal] – Available settings are: ● ALL

	● MD5 ● SHA1 ● SHA2_256
[ikephase2proposal ikephase2proposal]	Specify the proposal mofe for IKE phase2. [ikephase2proposal] – Available settings are: ● DES_without_Auth ● DES_with_auth ● 3DES_without_auth ● 3DES_with_auth ● AES128_without_auth ● AES128_with_auth ● AES192_without_auth ● AES192_with_auth ● AES256_without_auth ● AES256_with_auth
[ikephase2authproposal ikephase2authproposal]	Specify the authentication mofe for IKE phase2. [ikephase2authproposal] – Available settings are: ● ALL ● MD5 ● SHA1 ● SHA2_256
[acceptall acceptall]	Specify the proposal for dial-in. [acceptall]- Available settings are: ● acceptall ● acceptabove

Example

```
Vigor3900> enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#
Vigor3900@config-vpn-l2l# ipsecpolicy add status enable always_on
enable vpn_l2l_carrie
Vigor3900@config-vpn-l2l# ipsecpolicy vpn_l2l_carrie
Vigor3900@config-vpn-l2l-ipsecpolicy-vpn_l2l_carrie#set gre enable
set done

Vigor3900@config-vpn-l2l-ipsecpolicy-vpn_l2l_carrie#
```

6.10.1.2 Telnet Command: pptpdialin

Users could use [pptpdialin] command to add or delete the PPTP dail-in profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-vpn-l2l# pptpdialin add <SectionName>
Vigor3900@config-vpn-l2l# pptpdialin delete <SectionName>
Vigor3900@config-vpn-l2l# pptpdialin show
Vigor3900@config-vpn-l2l# pptpdialin show <SectionName>
Vigor3900@config-vpn-l2l# pptpdialin <SectionName>
```

Command	Description
pptpdialin add <SectionName>	Add a new LAN to LAN profile. <SectionName>- Enter the name of LAN to LAN profile.
pptpdialin delete <SectionName>	Remove a selected LAN to LAN profile. <SectionName> - Enter the name (e.g., dialin_carrie) of LAN to LAN profile to be deleted.
pptpdialin show	Display the status for all LAN to LAN profiles.
pptpdialin show <SectionName>	Display the status of selected LAN to LAN profile. <SectionName>> - Enter the name (e.g., dialin_carrie) of LAN to LAN profile.
pptpdialin <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., dialin_carrie) of LAN to LAN profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#
Vigor3900@config-vpn-l2l# pptpdialin add pptp_carrie status enable
Vigor3900@config-vpn-l2l# pptpdialin show
pptp-l2l-din       status        status        username
localsubnet
remotesubnet
pptp_carrie        enable
```

Telnet Command: pptpdialin add ?

To configure detailed settings for a PPTP dial-in profile, users could use [pptpdialin add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-vpn-l2l# pptpdialin add [status status][username
username][localsubnet localsubnet][remotesubnet remotesubnet]
[nbns_pass nbns_pass][mcast_pass mcast_pass][rip_pass rip_pass]
<SectionName>
```

Command	Description
add	Create a new dial-in profile based on PPTP.
[status status]	Enable the LAN to LAN profile. [status] - Enter Enable or Disable.

[username username]	Specify a user name for such profile. [username] – Enter a string as username.
[localsubnet localsubnet]	Specify the local subnet. [localsubnet] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[remotesubnet remotesubnet]	Specify remote subnet. [remotesubnet] – Enter the subnet with mask (e.g., 192.168.1.0 /24).
[nbns_pass nbns_pass]	Enable / disable the function of NetBios Naming Packet. [nbns] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN for passing the packets. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of RIP via VPN for passing the packets. Enter Enable or Disable.
<SectionName>	Enter the name of LAN to LAN profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#
Vigor3900@config-vpn-l2l# pptpdialin add dialin_carrie
Vigor3900@config-vpn-l2l#
```

Telnet Command: set, get, disconnect

It is used for reviewing the detailed settings or modifying settings for the selected profile.

Syntax

```
Vigor3900@config-vpn-l2l-pptpdialin-<SectionName># get
Vigor3900@config-vpn-l2l-pptpdialin-<SectionName># set [status status]
[username username] [localsubnet localsubnet] [remotesubnet
remotesubnet] [nbns_pass nbns_pass] [mcast_pass mcast_pass] [rip_pass
rip_pass]
```

Command	Description
disconnect	Terminate the LAN to LAN profile based on PPTP.
get	Get the configuration of LAN to LAN profile.
set	Modify settings for the selected LAN to LAN profile.
[status status]	Enable the LAN to LAN profile. [status] - Enter Enable or Disable.
[username username]	Specify a user profile (user account with PPTP dial-in enabled) for such VPN LAN to LAN profile.

	[username] – Enter the name of user profile (e.g., user_david).
[localsubnet localsubnet]	Specify the local subnet. [localsubnet] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[remotesubnet remotesubnet]	Specify remote subnet. [remotesubnet] – Enter the subnet with mask (e.g., 192.168.1.0 /24).
[nbns_pass nbns_pass]	Enable / disable the function of NetBios Naming Packet. [nbns] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN for passing the packets. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of RIP via VPN for passing the packets. Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#
Vigor3900@config-vpn-l2l# pptpdialin add dialin_carrie
Vigor3900@config-vpn-l2l# pptpdialin dialin_carrie
Vigor3900@config-vpn-l2l-pptpdialin-dialin_carrie# set status enable
username user_david
set done
Vigor3900@config-vpn-l2l-pptpdialin-dialin_carrie# set rip_pass
enable
set done
Vigor3900@config-vpn-l2l-pptpdialin-dialin_carrie# get
status              : Enable
username            : user_david
localsubnet         :
remotesubnet        :
nbns_pass           : Disable
mcast_pass          : Disable
rip_pass            : Enable
```

6.10.1.3 Telnet Command: pptpdialout

Users could use [pptpdialout] command to add or delete the PPTP dail-out profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-vpn-l2l# pptpdialout add <SectionName>
Vigor3900@config-vpn-l2l# pptpdialout delete <SectionName>
Vigor3900@config-vpn-l2l# pptpdialout show
Vigor3900@config-vpn-l2l# pptpdialout show <SectionName>
```

```
Vigor3900@config-vpn-l2l# pptpdialout <SectionName>
```

Command	Description
pptpdialout add <SectionName>	Add a new LAN to LAN profile. <SectionName>- Enter the name of LAN to LAN profile.
pptpdialout delete <SectionName>	Remove a selected LAN to LAN profile. <SectionName> - Enter the name (e.g., dialout_carrie) of LAN to LAN profile to be deleted.
pptpdialout show	Display the status for all LAN to LAN profiles.
pptpdialout show <SectionName>	Display the status of selected LAN to LAN profile. <SectionName>> - Enter the name (e.g., dialout_carrie) of LAN to LAN profile.
pptpdialout <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., dialout_carrie) of LAN to LAN profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l# pptpdialout add dial_out_carrie
Vigor3900@config-vpn-l2l# pptpdialout show dial_out_carrie
status                  : Disable
alwayson                : disable
dummy_wan_alias         :
lefthost_if_alias_ip    :
localhost               :
idle                    : 300
serverip                :
username                :
password                :
localsubnet             :
remotesubnet            :
natmode                 : 0
nbns_pass               : disable
mcast_pass              : disable
rip_pass                : disable
```

Telnet Command: pptpdialout add ?

To configure detailed settings for a PPTP dial-out profile, users could use [pptpdialout add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-vpn-l2l# pptpdialout add [status status] [alwayson
alwayson] [lefthost_if_alias_ip lefthost_if_alias_ip]
[lefthost_if_alias lefthost_if_alias] [lefthost_if lefthost_if]
[lefthost_if_bk lefthost_if_bk] [idle idle] [serverip serverip]
```

```
[username username] [password password] [localsubnet localsubnet]
[remotesubnet remotesubnet] [natmode natmode] [nbns_pass nbns_pass]
[mcast_pass mcast_pass] [rip_pass rip_pass] <SectionName>
```

Command	Description
add	Create a new LAN to LAN profile.
[status status]	Enable the LAN to LAN profile. [status] - Enter Enable or Disable.
[alwayson alwayson]	Enable the function of Always On. [status] - Enter Enable or Disable.
[lefthost_if_alias_ip lefthost_if_alias_ip]	Specify one WAN Alias IP. [lefthost_if_alias_ip] – Enter the IP address (configured as WAN Alias IP).
[lefthost_if_alias lefthost_if_alias]	Enable / disable the function of WAN Alias IP. [lefthost_if_alias] – Enter Enable or Disable.
[lefthost_if lefthost_if]	Specify the WAN interface for dialing out. [lefthost_if] – Enter the name of WAN profile.
[lefthost_if_bk lefthost_if_bk]	Specify WAN interface as backup WAN (failover WAN). [lefthost_if_bk]- Enter WAN interface profile.
[idle idle]	Set a timeout for idle period. [idle] – Enter the value. Default is 300 (sec.).
[serverip serverip]	Specify the IP address of PPTP server. [serverip] – Enter the IP address.
[username username]	Specify a string as username. [username] – Enter a string.
[password password]	Specify a password. [password] – Enter a set of characters.
[localsubnet localsubnet]	Specify subnet for local host. [localsubnet] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[remotesubnet remotesubnet]	Specify the subnet mask for the remote host. [remotesubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[natmode natmode]	Specify NAT mode for LAN subnet to remote network. [natmode] – Available settings are: ● Route ● NAT
[nbns_pass nbns_pass]	Enable / disable the function of passing NetBios Naming Packet. [nbns_pass] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of passing RIP packet via VPN.

	[rip_pass] - Enter Enable or Disable.
<SectionName>	Enter the name of the profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l#pptpdialout add status enable alwayson
enable dial_out_david
Vigor3900@config-vpn-l2l#
```

Telnet Command: set, get, connect, disconnect

It is used for reviewing the detailed settings or modifying settings for the selected dial-out profile.

Syntax

```
Vigor3900@config-vpn-l2l-pptpdialout-<SectionName>#connect
Vigor3900@config-vpn-l2l-pptpdialout-<SectionName>#disconnect
Vigor3900@config-vpn-l2l-pptpdialout-<SectionName>#get
Vigor3900@config-vpn-l2l-pptpdialout-<SectionName>#set [status status]
[alwayson alwayson] [lefthost_if_alias_ip lefthost_if_alias_ip]
[lefthost_if_alias lefthost_if_alias] [lefthost_if lefthost_if]
[lefthost_if_bk lefthost_if_bk] [idle idle] [serverip serverip]
[username username] [password password] [localsubnet localsubnet]
[remotesubnet remotesubnet] [natmode natmode] [nbns_pass nbns_pass]
[mcast_pass mcast_pass] [rip_pass rip_pass]
```

Command	Description
<SectionName>	Display the name of the profile.
connect	Initiate the LAN to LAN profile based on IPsec policy.
disconnect	Terminate the LAN to LAN profile based on IPsec policy.
get	Get the configuration of LAN to LAN profile.
set	Modify settings for the selected LAN to LAN profile.
[status status]	Enable the LAN to LAN profile. [status] - Enter Enable or Disable.
[alwayson alwayson]	Enable the function of Always On. [status] - Enter Enable or Disable.
[lefthost_if_alias_ip lefthost_if_alias_ip]	Specify one WAN Alias IP. [lefthost_if_alias_ip] – Enter the IP address (configured as WAN Alias IP).
[lefthost_if_alias lefthost_if_alias]	Enable / disable the function of WAN Alias IP. [lefthost_if_alias] – Enter Enable or Disable.
[lefthost_if lefthost_if]	Specify the WAN interface for dialing out. [lefthost_if] – Enter the name of WAN profile.

[lefthost_if_bk lefthost_if_bk]	Specify WAN interface as backup WAN (failover WAN). [lefthost_if_bk]- Enter WAN interface profile.
[idle idle]	Set a timeout for idle period. [idle] – Enter the value. Default is 300 (sec.).
[serverip serverip]	Specify the IP address of PPTP server. [serverip] – Enter the IP address.
[username username]	Specify a string as username. [username] – Enter a string.
[password password]	Specify a password. [password] – Enter a set of characters.
[localsubnet localsubnet]	Specify subnet for local host. [localsubnet] – Enter the subnet with mask (e.g., 192.168.1.0/24).
[remotesubnet remotesubnet]	Specify the subnet mask for the remote host. [remotesubnet] –Enter the subnet with mask (e.g., 192.168.1.0/24).
[natmode natmode]	Specify NAT mode for LAN subnet to remote network. [natmode] – Available settings are: ● Route ● NAT
[nbns_pass nbns_pass]	Enable / disable the function of passing NetBios Naming Packet. [nbns_pass] - Enter Enable or Disable.
[mcast_pass mcast_pass]	Enable / disable the function of Multicast via VPN. [mcast_pass] - Enter Enable or Disable.
[rip_pass rip_pass]	Enable / disable the function of passing RIP packet via VPN. [rip_pass] - Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# lan2lan
Vigor3900@config-vpn-l2l# pptpdialout add dial_out_carrie
Vigor3900@config-vpn-l2l# pptpdialout dial_out_carrie
Vigor3900@config-vpn-l2l-pptpdialout-dial_out_carrie#set rip_pass
enable
```

6.10.2 Telnet Command: remotedialin

Users could use [remotedialin] command to configure remote dial-in profiles, then use [ipsecremotedialin], [l2tpserver], [pptpserver] commands to set the details. Refer to the following chapters for descriptions of commonly used commands.

```
Vigor3900> enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
```

```
Vigor3900@config-vpn# remotedialin
Vigor3900@config-vpn-remotedialin#
```

6.10.2.1 Telnet Command: l2tpserver

Users could use [l2tpserver] command to configure L2TP Server, then use the [get] or [set] command to configure the L2TP Server details information.

Syntax

```
Vigor3900@config-vpn-remotedialin-l2tpserver#get
Vigor3900@config-vpn-remotedialin-l2tpserver#set[auth authentication]
[user_auth user_authentication] [ldap_profile ldap_profile] [lanpf
lan_profile] [dhcp_relay dhcp_relay] [dhcp_loc dhcp_loc] [relay_ip
relay_ip] [force_ipsec status]
```

Command	Description
get	Get the configuration of L2TP server profile.
set	Modify settings for the selected L2TP server profile.
[auth authentication]	Specify a protocol for L2TP server authentication. [authentication] – Available settings include: ● PAP ● CHAP ● MS_CHAP ● MS_CHAP_v2
[user_auth user_authentication]	Specify a type for user authentication. [user_authentication] – Available settings include: ● Local ● RADIUS ● LDAP
[ldap_profile ldap_profile]	Choose a LDAP profile. [ldap_profile] – Enter the name of LDAP profile.
[lanpf lan_profile]	Specify a LAN interface for local IP address. [lan_profile] – Enter the name of LAN interface.
[dhcp_relay dhcp_relay]	Enable / disable the function of DHCP relay. [dhcp_relay] - Enter Enable or Disable.
[dhcp_loc dhcp_loc]	Specify an interface for DHCP server. [dhcp_loc]- Enter the name of WAN/LAN profile.
[relay_ip relay_ip]	Specify an IP address as DHCP relay. [relay_ip]- Enter an IP address.
[force_ipsec status]	Enable / disable the function of Force L2TP with IPsec Policy. [status] - Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
```

```
Vigor3900@config-vpn#
Vigor3900@config-vpn# remotedialin
Vigor3900@config-vpn-remotedialin# l2tpserver
Vigor3900@config-vpn-remotedialin-l2tpserver# get
auth                : CHAP
user_auth           : Local
ldap_profile        :
lanpf               : lan1
dhcp_relay          : 0
dhcp_loc            : wan1
relay_ip            :
force_ipsec         : enable
Vigor3900@config-vpn-remotedialin-l2tpserver#set auth MS_CHAP
dhcp_loc lan1
set done
```

6.10.2.2 Telnet Command: pptpserver

Users could use [pptpserver] command to configure pptp server, then use the [get] or [set] command to configure the PPTP server details information.

Syntax

```
Vigor3900@config-vpn-remotedialin-pptpserver#get
Vigor3900@config-vpn-remotedialin-pptpserver#set [auth authentication]
[encp encryption] [user_auth user_authentication] [ldap_profile
ldap_profile] [lanpf lan_profile] [localhost localhost] [dhcp_relay
dhcp_relay] [dhcp_loc dhcp_loc] [relay_ip relay_ip] [mss pptp_mss]
[disable_nbns dummy] [disable_mcast disable_mcast] [disable_pptp_fpp
dummy]
```

Command	Description
get	Get the configuration of PPTP server profile.
set	Modify settings for the selected PPTP server profile.
[auth authentication]	Specify a protocol for PPTP server authentication. [authentication] – Available settings include: ● PAP ● CHAP ● MS_CHAP ● MS_CHAP_v2
[encp encryption]	Set the encryption length for PPTP server. [encryption] – Availalbel settings include: ● 40/128_bit ● 128_bit ● Disable
[user_auth user_authentication]	Specify a type for user authentication. [user_authentication] – Available settings include: ● Local

	● RADIUS ● LDAP
[ldap_profile ldap_profile]	Choose a LDAP profile. [ldap_profile] – Enter the name of LDAP profile.
[lanpf lan_profile]	Specify a LAN interface for local IP address. [lan_profile] – Enter the name of LAN interface.
[localhost localhost]	Specify a WAN interface. [localhost] – Enter the name of WAN profile.
[dhcp_relay dhcp_relay]	Enable / disable the function of DHCP relay. [dhcp_relay] - Enter Enable or Disable.
[dhcp_loc dhcp_loc]	Specify an interface for DHCP server. [dhcp_loc]- Enter the name of WAN/LAN profile.
[relay_ip relay_ip]	Specify an IP address as DHCP relay. [relay_ip]- Enter an IP address.
[mss pptp_mss]	Specify MSS value for PPTP server. [pptp_mss]- Enter a number for MTU/MRU. (Maximum is 1500).
[disable_nbns dummy]	Let the NetBios Naming Packet pass through or be blocked. [dummy] - Enter Pass or Block.
[disable_mcast disable_mcast]	Let the Multicast Packet pass through or be blocked. [disable_mcast]- Enter Pass or Block.
[disable_pptp_fpp dummy]	Enable (Pass) / disable (Block) the function of PPTP acceleration. [dummy] - Enter Pass or Block.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# remotedialin
Vigor3900@config-vpn-remotedialin#
Vigor3900@config-vpn-remotedialin# pptpserver
Vigor3900@config-vpn-remotedialin-pptpserver#
Vigor3900@config-vpn-remotedialin-pptpserver# get
auth                : MS_CHAP_v2
encp                : 128_bit
user_auth           : Local
ldap_profile        :
lanpf               : lan1
localhost           :
dhcp_relay          : 0
dhcp_loc            : wan1
relay_ip            :
mss                 : 1300
dummy               : 1
disable_mcast       : 1
```

```
dummy                 : Enable
Vigor3900@config-vpn-remotedialin-pptpserver#set encp 40/128_bit lanpf lan_carrie
set done
set dummy pass dummy block
```

6.10.3 Telnet Command: trunk

Users could use [trunk] command to configure VPN TRUNK Manager, then use [ipseclbpool], [ipseclbrule] commands to set the details. Refer to the following sections for descriptions of commonly used commands.

```
Vigor3900> enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk#
```

6.10.3.1 Telnet Command: ipseclbrule

Users could use [ipseclbrule] command to add or delete the Load Balance Rule profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-vpn-trunk# ipseclbrule add <SectionName>
Vigor3900@config-vpn-trunk# ipseclbrule delete <SectionName>
Vigor3900@config-vpn-trunk# ipseclbrule show
Vigor3900@config-vpn-trunk# ipseclbrule show <SectionName>
Vigor3900@config-vpn-trunk# ipseclbrule <SectionName>
```

Command	Description
ipseclbrule add <SectionName>	Add a new load balance profile. <SectionName> - Enter the name of load balance profile.
ipseclbrule delete <SectionName>	Remove a selected load balance profile. <SectionName> - Enter the name (e.g., lbrule_carrie) of load balance profile to be deleted.
ipseclbrule show	Display the status for all load balance profiles.
ipseclbrule show <SectionName>	Display the status of selected load balance profile. <SectionName> - Enter the name (e.g., lbrule_carrie) of load balance profile.
ipseclbrule <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., lbrule_carrie) of load balance profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
```

```
Vigor3900@config-vpn-trunk# ipseclbrule add lbrule_carrie
Vigor3900@config-vpn-ipsec-trunk-lb-rule-lbrule_carrie#
```

Telnet Command: ipseclbrule add ?

To configure detailed settings for a profile, users could use [ipseclbrule add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-vpn-trunk# ipseclbrule add [status status] [proto
protocol] [sip src_ip] [smask src_mask] [dip dest_ip] [dmask dest_mask]
[dport dest_port] [dport_end dest_port_end] [pool lb_pool]
<SectionName>
```

Command	Description
[status status]	Enable the load balance profile. [status] - Enter Enable or Disable.
[proto protocol]	Specify a protocol for load balance profile. [protocol] – Available settings include: ● ALL ● TCP/UDP ● TCP ● UDP ● ICMP ● FTP ● TFTP ● HTTP ● SMTP ● POP3
[sip src_ip]	Specify an IP address as source IP. [src_ip]- Enter an IP address.
[smask src_mask]	Specify subnet mask for source IP. [src_mask] – Enter a subnet mask.
[dip dest_ip]	Specify an IP address as destination IP. [dest_ip]- Enter an IP address.
[dmask dest_mask]	Specify subnet mask for destination IP. [dest_mask] – Enter a subnet mask.
[dport dest_port]	Specify a port number as destination port. [dest_port] – Enter a value.
[dport_end dest_port_end]	Specify the ending port number. [dest_port_end] – Enter a value.
[pool lb_pool]	Specify a load balance pool profile. [lb_pool] – Enter the name of the load balance pool profile.
<SectionName>	Enter the name (e.g., lbrule_carrie) of IPsec load balance profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk#ipseclbrule add status enable proto ALL
sip 192.168.1.59 ibrule_david
Vigor3900@config-vpn-ipsec-trunk-lb-rule-ibrule_david#
```

Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected load balance profile (e.g., lbrule_david).

Syntax

```
Vigor3900@config-vpn-ipsec-trunk-lb-rule-<SectionName>#get
Vigor3900@config-vpn-ipsec-trunk-lb-rule-<SectionName>#set [status
status] [proto protocol] [sip src_ip] [smask src_mask] [dip dest_ip]
[dmask dest_mask] [dport dest_port] [dport_end dest_port_end] [pool
lb_pool]
```

Command	Description
get	Get the configuration of load balance rule profile.
set	Modify settings for the selected load balance rule profile.
[status status]	Enable the load balance profile. [status] - Enter Enable or Disable.
[proto protocol]	Specify a protocol for load balance profile. [protocol] – Available settings include: ● ALL ● TCP/UDP ● TCP ● UDP ● ICMP ● FTP ● TFTP ● HTTP ● SMTP ● POP3
[sip src_ip]	Specify an IP address as source IP. [src_ip]- Enter an IP address.
[smask src_mask]	Specify subnet mask for source IP. [src_mask] – Enter a subnet mask.
[dip dest_ip]	Specify an IP address as destination IP. [dest_ip]- Enter an IP address.
[dmask dest_mask]	Specify subnet mask for destination IP.

	[dest_mask] – Enter a subnet mask.
[dport dest_port]	Specify a port number as destination port. [dest_port] – Enter a value.
[dport_end dest_port_end]	Specify the ending port number. [dest_port_end] – Enter a value.
[pool lb_pool]	Specify a load balance pool profile. [lb_pool] – Enter the name of the load balance pool profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk#
Vigor3900@config-vpn-trunk# ipseclbrule ibrule_david
Vigor3900@config-vpn-ipsec-trunk-lb-rule-ibrule_david# get
status              : Enable
proto               : ALL
sip                 : 192.168.1.59
smask               :
dip                 :
dmask               :
dport               :
dport_end           :
pool                :
```

6.10.3.2 Telnet Command: ipseclbpool

Users could use [ipseclbpool] command to add or delete the Load Balance pool profile or use "show" to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-vpn-trunk# ipseclbpool add <SectionName>
Vigor3900@config-vpn-trunk# ipseclbpool delete <SectionName>
Vigor3900@config-vpn-trunk# ipseclbpool show
Vigor3900@config-vpn-trunk# ipseclbpool show <SectionName>
Vigor3900@config-vpn-trunk# ipseclbpool <SectionName>
```

Command	Description
ipseclbpool add <SectionName>	Add a new load balance pool profile. <SectionName> - Enter the name of load balance pool profile.
ipseclbpool delete <SectionName>	Remove a selected load balance pool profile. <SectionName> - Enter the name (e.g., lbpool_carrie) of load balance pool profile to be deleted.
ipseclbpool show	Display the status for all load balance pool profiles.
ipseclbpool show <SectionName>	Display the status of selected load balance pool profile. <SectionName> - Enter the name (e.g., lbpool_carrie) of load

	balance pool profile.
ipseclbpool <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., lbpool_carrie) of load balance pool profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk# ipseclbpool add lbpool_carrie
Vigor3900@config-vpn-trunk-ipsec-lb-pool-lbpool_carrie#..
Vigor3900@config-vpn-trunk# ipseclbpool show lbpool_carrie

mode                : Load_Balance
lbif                :
primary             :
backup              :
```

Telnet Command: ipseclbpool add ?

To configure detailed settings for a profile, users could use [ipseclpool add] to create a new profile **with detailed settings**.

Syntax

```
Vigor3900@config-vpn-trunk# ipseclbpool add [mode mode] [lbif lb_iface]
<SectionName>
```

Command	Description
[mode mode]	Specify load balance mode. [mode] – Available settings include: ● Load_Balance ● Backup
[lbif lb_iface]	Specify an interface for applying load balance pool. [lb_iface] – Enter the name of LAN/WAN profile.
<SectionName>	Enter the name (e.g., lbpool_david) of load balance pool profile.

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk#ipseclbpool add mode load_balance
ibpool_david
Vigor3900@config-vpn-ipsec-trunk-lb-pool-ibpool_david#
```

Telnet Command: set, get, add, remove

It is used for reviewing the detailed settings or modifying settings for the selected load balance profile (e.g., lbpool_david).

Syntax

```
Vigor3900@config-vpn-ipsec-trunk-lb-pool-<SectionName>#add <lb_iface>
Vigor3900@config-vpn-ipsec-trunk-lb-pool-<SectionName>#get
Vigor3900@config-vpn-ipsec-trunk-lb-pool-<SectionName>#set [mode mode]
[lbif lb_iface]
Vigor3900@config-vpn-ipsec-trunk-lb-pool-<SectionName>#remove [lbif
lb_iface]
```

Command	Description
<SectionName>	Display the name of load balance pool profile.
add <lb_iface>	Add the interface setting for load balance pool profile. <lb_iface> - Enter the name of VPN profile with GRE enabled (e.g., vpn_l2l_carrie).
get	Get the configuration of load balance pool profile.
set	Modify settings for the selected load balance pool profile.
[mode mode]	Specify load balance mode. [mode] – Available settings include: ● Load_Balance ● Backup
[lbif lb_iface]	Specify an interface for applying load balance pool. [lb_iface] – Enter the name of LAN/WAN profile.
remove [lbif lb_iface]	Remove the load balance interface setting. [lb_iface] - Enter the name of VPN profile with GRE enabled (e.g., vpn_l2l_carrie).

Example

```
Vigor3900>enable
Vigor3900# configure vpn
Vigor3900@config-vpn#
Vigor3900@config-vpn# trunk
Vigor3900@config-vpn-trunk#
Vigor3900@config-vpn-trunk# ipseclbpool ibpool_david
Vigor3900@config-vpn-ipsec-trunk-lb-pool-ibpool_david# set lbif
vpn_l2l_carrie
Vigor3900@config-vpn-trunk-ipsec-lb-pool-ibpool_david# set lbif
vpn_l2l_carrie

set done

Vigor3900@config-vpn-trunk-ipsec-lb-pool-ibpool_david# get
mode                : Load_Balance
lbif                : vpn_l2l_carrie
primary             :
backup              :
```

6.11 Bandwidth Management Configuration

Vigor3900 provides three functions in Bandwidth Managemant – bandwidth limit and sessions limit .Users could use the commands below to set up the details.

To make bandwidth management configuration, you have to type "*configure bandwidth*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth#
```

There are several functions for Bandwidth Managemant – Access Barrier, Bandwidth Limit and Session Limit.

Available sub-commands under Bandwidth include:

- access_barrier (refer to 6.11.1)
- bandwidth_limit (refer to 6.11.2)
- sesslimit (refer to 6.11.3)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.11.1 Telenet Command: access_barrier

Users could use [access_barrier] command configure the access barrier to protect the system from brute-force attack and flooding attack

Syntax

```
Vigor3900@config-bandwidth# access_barrier [option] [action]
```

Command	Description
access_barrier [option] [action]	Specify the type of access barrier. [option] – Available settings include: ● pptp ● Ipsec ● Web ● telnet ● https ● ssh ● ftp [action] – Enable or disable the access barrier function. ● on ● off

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth#
Vigor3900@config-bandwidth# access_barrier pptp on
Success !!
Vigor3900@config-bandwidth#
```

6.11.2 Telenet Command: bandwidth_limit

Users could use [bandwidth_limit] command to add or delete the bandwidth limit profile or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-bandwidth# bandwidth_limit add <SectionName>
Vigor3900@config-bandwidth# bandwidth_limit delete <SectionName>
Vigor3900@config-bandwidth# bandwidth_limit show
Vigor3900@config-bandwidth# bandwidth_limit show <SectionName>
Vigor3900@config-bandwidth# bandwidth_limit <SectionName>
```

Command	Description
bandwidth_limit add <SectionName>	Add a new bandwidth limit profile. <SectionName> - Enter the name of bandwidth limit profile.
bandwidth_limit delete <SectionName>	Remove a selected bandwidth limit profile. <SectionName> - Enter the name (e.g., bandli_carrie) of bandwidth limit profile to be deleted.
bandwidth_limit show	Display the status for all bandwidth limit profiles.
bandwidth_limit show <SectionName>	Display the status of selected bandwidth limit profile. <SectionName> - Enter the name (e.g., bandli_carrie) of bandwidth limit profile.
bandwidth_limit <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., bandli_carrie) of bandwidth limit profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# bandwidth_limit add bandli_carrie
Vigor3900@config-bw-limit-bandli_carrie#
```

6.11.2.1 Telenet Command: bandwidth_limit add ?

To configure detailed settings for a bandwidth limit profile, users could use [bandwidth_limit add] to create a new bandwidth limit profile **with detailed settings**.

Syntax

```
Vigor3900@config-bandwidth# bandwidth_limit add [status status]
[rx_limit rx_limit] [tx_limit tx_limit] [mode mode] [ip_obj ip_obj]
[ip_grp ip_grp] [time_objs time_objs] [time_grps time_grps] [usr_obj
usr_obj] [usr_grp usr_grp] [ldap_grp ldap_grp] [user_obj user_obj]
[usr_grp usr_grp] [guest_grp guest_grp] [srv_obj srv_obj] [srv_grp
srv_grp] <SectionName>
```

Command	Description
[status status]	Enable / disable the bandwidth limit profile. [status] - Enter Enable or Disable the bandwidth limit profile.
[rx_limit rx_limit]	Define the limitation for the speed of the downstream. [rx_limit] - Enter a number (0 is not allowed).
[tx_limit tx_limit]	Define the limitation for the speed of the upstream. [tx-limit] - Enter a number (0 is not allowed).
[mode mode]	Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields. [mode] - Available modes include: ● Each ● Shared
[ip_obj ip_obj]	Specify an IP object to apply such profile. [ip_obj] - Enter a name of the IP object profile.
[ip_grp ip_grp]	Specify an IP group to apply such profile. [ip_grp] - Enter a name of the IP group profile.
[time_objs time_objs]	Specify a time object to apply such profile. [time_objs] - Enter a name of the time object profile.
[time_grps time_grps]	Specify a time group to apply such profile. [time_grps] - Enter a name of the time group profile.
[usr_obj usr_obj]	Specify a user account object to apply such profile. [usr_obj] - Enter a name of the user account object profile.
[usr_grp usr_grp]	Specify a user group to apply such profile. [usr_grp] - Enter a name of the user group profile.
[ldap_grp ldap_grp]	Specify a LDAP group to apply such profile. [ldap_grp] - Enter a name of the LDAP group profile.
[guest_grp guest_grp]	Specify a guest group to apply such profile. [guest_grp] - Enter a name of the guest group profile.
[srv_obj srv_obj]	Specify a service object to apply such profile. [usr_obj] - Enter a name of the service object profile.
[srv_grp srv_grp]	Specify a service group to apply such profile. [usr_grp] - Enter a name of the service group profile.
<SectionName>	<SectionName> - Enter the name (e.g., bandli_david) of bandwidth limit profile.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# bandwidth_limit add status enable ip_grp
ip_grp_david  bandli_david
Vigor3900@config-bw-limit-bandli_david#
```

6.11.2.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected bandwidth limit profile (e.g., bandli_david).

Syntax

```
Vigor3900@config-bw-limit-<SectionName># get
Vigor3900@config-bw-limit-<SectionName># set [status status] [rx_limit
rx_limit] [tx_limit tx_limit] [mode mode] [ip_obj ip_obj] [ip_grp ip_grp]
[time_objs time_objs] [time_grps time_grps] [usr_obj usr_obj] [usr_grp
usr_grp] [ldap_grp ldap_grp] [guest_grp guest_grp] [srv_obj srv_obj]
[srv_grp srv_grp]
```

Command	Description
<SectionName>	Display the name of bandwidth limit profile.
get	Get the configuration of bandwidth limit profile.
set	Modify settings for the selected bandwidth limit profile.
[status status]	Enable / disable the bandwidth limit profile. [status] - Enter Enable or Disable the bandwidth limit profile.
[rx_limit rx_limit]	Define the limitation for the speed of the downstream. [rx_limit] - Enter a number (0 is not allowed).
[tx_limit tx_limit]	Define the limitation for the speed of the upstream. [tx-limit] - Enter a number (0 is not allowed).
[mode mode]	Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields. [mode] - Available modes include: ● Each ● Shared
[ip_obj ip_obj]	Specify an IP object to apply such profile. [ip_obj] - Enter a name of the IP object profile.
[ip_grp ip_grp]	Specify an IP group to apply such profile. [ip_grp] - Enter a name of the IP group profile.
[time_objs time_objs]	Specify a time object to apply such profile. [time_objs] - Enter a name of the time object profile.
[time_grps time_grps]	Specify a time group to apply such profile. [time_grps] - Enter a name of the time group profile.

[usr_obj usr_obj]	Specify a user account object to apply such profile. [usr_obj] - Enter a name of the user account object profile.
[usr_grp usr_grp]	Specify a user group to apply such profile. [usr_grp] - Enter a name of the user group profile.
[ldap_grp ldap_grp]	Specify a LDAP group to apply such profile. [ldap_grp] - Enter a name of the LDAP group profile.
[guest_grp guest_grp]	Specify a guest group to apply such profile. [guest_grp] - Enter a name of the guest group profile.
[srv_obj srv_obj]	Specify a service object to apply such profile. [usr_obj] - Enter a name of the service object profile.
[srv_grp srv_grp]	Specify a service group to apply such profile. [usr_grp] - Enter a name of the service group profile.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# bandwidth_limit add bandli_david
Vigor3900@config-bw-limit-bandli_david# set status enable
set done
Vigor3900@config-bw-limit-bandli_david# set rx_limit 1000 ip_obj
ip_david
set done
Vigor3900@config-bw-limit-bandli_david# get

status              : enable
rx_limit            : 1000
tx_limit            :
mode                :
ip_obj              : ip_david
ip_grp              :
time_objs           :
time_grps           :
usr_obj             :
usr_grp             :
ldap_grp            :
guest_grp           :
srv_obj             :
srv_grp             :
Vigor3900@config-bw-limit-bandli_david#
```

6.11.3 Telenet Command: sesslimit

Users could use [sesslimit] command to add or delete the sessions limit profiles or use “show” to get the profile list in the directory. Enter the profile name to open it and modify the profile directly.

Syntax

```
Vigor3900@config-bandwidth# sesslimit add <SectionName>
Vigor3900@config-bandwidth# sesslimit delete <SectionName>
Vigor3900@config-bandwidth# sesslimit show
```

```
Vigor3900@config-bandwidth# sesslimit show <SectionName>
Vigor3900@config-bandwidth# sesslimit <SectionName>
```

Command	Description
sesslimit add <SectionName>	Add a new session limit profile. <SectionName> - Enter the name of session limit profile.
sesslimit delete <SectionName>	Remove a selected session limit profile. <SectionName> - Enter the name (e.g., sess_carrie) of session limit profile to be deleted.
sesslimit show	Display the status for all session limit profiles.
sesslimit show <SectionName>	Display the status of selected session limit profile. <SectionName> - Enter the name (e.g., sess_carrie) of session limit profile.
sesslimit <SectionName>	Modify detailed settings for the selected profile. <SectionName> - Enter the name (e.g., sess_carrie) of session limit profile to be modified.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# sesslimit add sess_carrie
Vigor3900@config-bw-sesslimit-sess_carrie#
```

6.11.3.1 Telenet Command: sesslimit add ?

To configure detailed settings for a session limit profile, users could use [sesslimit add] to create a new session limit profile **with detailed settings**.

Syntax

```
Vigor3900@config-bandwidth# sesslimit add [status status] [session
session] [ip_obj ip_obj] [ip_grp ip_grp] [time_objs time_objs]
[time_grps time_grps] [usr_obj usr_obj] [usr_grp usr_grp] [ldap_grp
ldap_grp] [guest_grp guest_grp] <SectionName>
```

Command	Description
[status status]	Enable / disable the session limit profile. [status] - Enter Enable or Disable the session limit profile.
[session session]	Define the maximum sessions for such profile. [session] – Enter a number ranging from 20 to 1000.
[ip_obj ip_obj]	Specify an IP object to apply such profile. [ip_obj] - Enter a name of the IP object profile.
[ip_grp ip_grp]	Specify an IP group to apply such profile. [ip_grp] - Enter a name of the IP group profile.
[time_objs time_objs]	Specify a time object to apply such profile. [time_objs] - Enter a name of the time object profile.

[time_grps time_grps]	Specify a time group to apply such profile. [time_grps] - Enter a name of the time group profile.
[usr_obj usr_obj]	Specify a user account object to apply such profile. [usr_obj] - Enter a name of the user account object profile.
[usr_grp usr_grp]	Specify a user group to apply such profile. [usr_grp] - Enter a name of the user group profile.
[ldap_grp ldap_grp]	Specify a LDAP group to apply such profile. [ldap_grp] - Enter a name of the LDAP group profile.
[guest_grp guest_grp]	Specify a guest group to apply such profile. [guest_grp] - Enter a name of the guest group profile.
<SectionName>	< SectionName > - Enter the name (e.g., session_david) of session limit profile.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# sesslimit add status enable ip_obj
ip_obj_david session_david
Vigor3900@config-bw-sesslimit-session_david#
```

6.11.3.2 Telnet Command: set, get

It is used for reviewing the detailed settings or modifying settings for the selected session limit profile (e.g., session_david).

Syntax

```
Vigor3900@config-bw-sesslimit-<SectionName># get
Vigor3900@config-bw-sesslimit-<SectionName># set [status status]
[session session] [ip_obj ip_obj] [ip_grp ip_grp] [time_objs time_objs]
[time_grps time_grps] [usr_obj usr_obj] [usr_grp usr_grp][ldap_grp
ldap_grp] [guest_grp guest_grp]
```

Command	Description
<SectionName>	Display the name of session limit profile.
get	Get the configuration of session limit profile.
set	Modify settings for the selected session limit profile.
[status status]	Enable / disable the session limit profile. [status] - Enter Enable or Disable the session limit profile.
[session session]	Define the maximum sessions for such profile. [session] – Enter a number ranging from 20 to 1000.
[ip_obj ip_obj]	Specify an IP object to apply such profile. [ip_obj] - Enter a name of the IP object profile.
[ip_grp ip_grp]	Specify an IP group to apply such profile. [ip_grp] - Enter a name of the IP group profile.

[time_objs time_objs]	Specify a time object to apply such profile. [time_objs] - Enter a name of the time object profile.
[time_grps time_grps]	Specify a time group to apply such profile. [time_grps] - Enter a name of the time group profile.
[usr_obj usr_obj]	Specify a user account object to apply such profile. [usr_obj] - Enter a name of the user account object profile.
[usr_grp usr_grp]	Specify a user group to apply such profile. [usr_grp] - Enter a name of the user group profile.
[ldap_grp ldap_grp]	Specify a LDAP group to apply such profile. [ldap_grp] - Enter a name of the LDAP group profile.
[guest_grp guest_grp]	Specify a guest group to apply such profile. [guest_grp] - Enter a name of the guest group profile.

Example

```
Vigor3900>enable
Vigor3900# configure bandwidth
Vigor3900@config-bandwidth# sesslimit add status enable ip_obj
ip_obj_david session_david
Vigor3900@config-bw-sesslimit-session_david# set ip_grp ip_grp_david
usr_obj usr_david
set done
Vigor3900@config-bw-sesslimit-session_david# get
status              : enable
session             : 1000
ip_obj              : ip_obj_david
ip_grp              : ip_grp_david
time_objs           :
time_grps           :
usr_obj             : usr_david
usr_grp             :
ldap_grp            :
guest_grp           :
```

6.12 System Management Configuration

Vigor3900 provides many functions in system management .Users could use the commands below to set up the details.

To make system management configuration, you have to type "*configure system*" to access into next phase.

```
Vigor3900>enable
Vigor3900# configure system
Vigor3900@config-sys#
```

There are several functions for System Managemant – acc_ctrl, admin_passwd, autodiscovery, cc, cmm, config, firmware, mailalert, ntpclient, reboot, snmpagent, syslogd and tr069.

Available sub-commands under System include:

- acc_ctrl (refer to 6.12.1)
- admin_passwd (refer to 6.12.2)
- autodiscovery (refer to 6.12.3)
- cc (refer to 6.12.4)
- cmm (refer to 6.12.5)
- config (refer to 6.12.6)
- firmware (refer to 6.12.7)
- mailalert (refer to 6.12.8)
- ntpclient (refer to 6.12.9)
- reboot (refer to 6.12.10)
- snmpagent (refer to 6.12.11)
- syslogd (refer to 6.12.12)
- tr069 (refer to 6.12.13)

Note:

[XXX XXX] - [ ] means such command is optional. The former is command itself; the latter is value/selection for such command.

<XXX XXX> - < > means such command is required. The former is command itself; the latter is value/selection for such command.

6.12.1 Telnet Command: acc_ctrl

Users could use the [acc_ctrl] command to configure Access control and type the [get], [set] command to configure the details information.

Syntax

```
Vigor3900@config-sys# acc_ctrl get
Vigor3900@config-sys# acc_ctrl set [disable_auto_logout
disable_auto_logout] [validation_code validation_code] [fail_times
fail_times] [upload_login_image_status upload_login_image_status]
[enforce_https enforce_https] [apply_to_wan_interface apply_to_wan_if]
[web_allow web_allow] [telnet_allow telnet_allow] [ssh_allow ssh_allow]
[https_allow https_allow] [sslproxy_allow sslproxy_allow] [ftp_allow
ftp_allow] [samba_allow samba_allow] [tr069_allow tr069_allow]
[server_cert server_cert] [user_define_ip user_define_ip] [allow_ip
allow_ip] [wan_ping_allow wan_ping_allow] [allow_to_lan allow_to_lan]
[apply_to_lan_subnet apply_to_lan_subnet] [web_lan_allow web_lan_allow]
[telnet_lan_allow telnet_lan_allow] [ssh_lan_allow ssh_lan_allow]
[https_lan_allow https_lan_allow] [sslproxy_lan_allow
sslproxy_lan_allow] [ftp_lan_allow ftp_lan_allow] [samba_lan_allow
samba_lan_allow] [tr069_lan_allow tr069_lan_allow] [lan_ping_allow
lan_ping_allow] [web_port web_port] [telnet_port telnet_port] [ssh_port
ssh_port] [https_port https_port] [sslproxy_port sslproxy_port]
[sslvpn_port sslvpn_port] [ftp_port ftp_port] [mngt_wan mngt_wan]
```

Command	Description
get	Get the configuration of access control.

set	Configure settings for access control.
[disable_auto_logout disable_auto_logout]	Enable / disable the function of Auto-Logout. [disable_auto_logout] - Enter Enable or Disable.
[validation_code validation_code]	Enable / disable the function of Validation Code. [validation_code] - Enter Enable or Disable.
[fail_times fail_times]	It is available when **Use Validation Code** is enabled. The number selected here means the times for login failure that will trigger Validation Code for authentication. [fail_times] – Available settings include: 0, 1, 2, 3, 4 and 5.
[upload_login_image_status upload_login_image_status]	Enable / disable the function of specifying an image file which will be displayed on the login page when a user or guest tries to access into Internet. [upload_login_image_status] - Enter Enable or Disable.
[enforce_https enforce_https]	Force the user accessing into web user interface of Vigor router by HTTPS. [enforce_https] - Enter Enable or Disable.
[apply_to_wan_interface apply_to_wan_if]	Specify the WAN interface(s) to apply such feature. [apply_to_wan_if] – Enter the name for one WAN interace (e.g., wan1, wan2, wan3, wan4, wan5, usb1, usb2).
[web_allow web_allow]	Enable or disable the permission of web access. [web_allow] - Enter Enable or Disable.
[telnet_allow telnet_allow]	Enable or disable the permission of telnet access. [telnet_allow] - Enter Enable or Disable.
[ssh_allow ssh_allow]	Enable or disable the permission of SSH access. [ssh_allow] - Enter Enable or Disable.
[https_allow https_allow]	Enable or disable the permission of HTTPS access. [https_allow] - Enter Enable or Disable.
[sslproxy_allow sslproxy_allow]	Enable or disable the permission of SSL Proxy access. [sslproxy_allow] - Enter Enable or Disable.
[ftp_allow ftp_allow]	Enable or disable the permission of FTP access. [ftp_allow] - Enter Enable or Disable.
[samba_allow samba_allow]	Enable or disable the permission of SAMBA access. [samba_allow] - Enter Enable or Disable.
[tr069_allow tr069_allow]	Enable or disable the permission of TR069 access. [tr069_allow] - Enter Enable or Disable.
[server_cert server_cert]	Specify a server certificate. [server_cert] – Enter ‘Default” to use the default sever certificate.
[user_define_ip user_define_ip]	Enable or disable the function of user defined IP address. [user_define_ip] - Enter Enable or Disable.

[allow_ip allow_ip]	System administrator can login from the IP address defined here. [allow_ip] – Enter IP address with subnet mask (ex, 192.168.1.11/24).
[wan_ping_allow wan_ping_allow]	Enable / disable the function of Allow Ping from WAN. [wan_ping_allow] - Enter Enable or Disable.
[allow_to_lan allow_to_lan]	Enable / disable the function of Allow management from LAN. [allow_to_lan]- Enter Enable or Disable.
[apply_to_lan_subnet apply_to_lan_subnet]	Specify which LAN interface shall be applied to. [apply_to_lan_subnet] – Enter the name of LAN profile (e.g., lan1).
[web_lan_allow web_lan_allow]	Enable or disable the permission of web access. [web_lan_allow] - Enter Enable or Disable.
[telnet_lan_allow telnet_lan_allow]	Enable or disable the permission of telnet access. [telnet_lan_allow] - Enter Enable or Disable.
[ssh_lan_allow ssh_lan_allow]	Enable or disable the permission of SSH access. [ssh_lan_allow] - Enter Enable or Disable.
[https_lan_allow https_lan_allow]	Enable or disable the permission of HTTPS access. [https_lan_allow] - Enter Enable or Disable.
[sslproxy_lan_allow sslproxy_lan_allow]	Enable or disable the permission of SSL Proxy access. [sslproxy_lan_allow] - Enter Enable or Disable.
[ftp_lan_allow ftp_lan_allow]	Enable or disable the permission of FTP access. [ftp_lan_allow]- Enter Enable or Disable.
[samba_lan_allow samba_lan_allow]	Enable or disable the permission of SAMBA access. [samba_lan_allow] - Enter Enable or Disable.
[tr069_lan_allow tr069_lan_allow]	Enable or disable the permission of TR069 access. [tr069_lan_allow]- Enter Enable or Disable.
[lan_ping_allow lan_ping_allow]	Enable or disable the function of Allow ping from the LAN. [lan_ping_allow] – Enter Enable or Disable.
[web_port web_port]	Specify a number as web service port. [web_port] – Enter a number. (The default value is 80)
[telnet_port telnet_port]	Specify a number as telnet service port. [telnet_port] – Enter a number. (The default value is 23)
[ssh_port ssh_port]	Specify a number as SSH service port. [ssh_port] - Enter a number. (The default value is 22)
[https_port https_port]	Specify a number as HTTPS service port. [https_port] - Enter a number. (The default value is 443)
[sslproxy_port sslproxy_port]	Specify a number as SSL Proxy service port. [sslproxy_port] –Enter a number. (The default value is 44300)
[sslvpn_ports	Specify a number as SSL VPN port.

slvpn_port]	[slvpn_port] - Enter a number. (The default value is 443)
[ftp_port ftp_port]	Specify a number as FTP service port. [ftp_port] - Enter a number. (The default value is 21)
[mngt_wan mngt_wan]	Specify a WAN profile for accessing Vigor router. [mngt_wan] – Enter the name of WAN proifle.

Example

```
Vigor3900>enable
Vigor3900# configure system#acc_ctrl set web_allow enable
set done
Vigor3900@config-sys# acc_ctrl get

disable_auto_logout     : disable
validation_code         : Enable
fail_times              : 2
upload_login_image_status : disable
upload_login_image      :
enforce_https           : disable
wan_access_control      : Internet Access Control
apply_to_wan_interface  : wan1, wan2, wan3, wan4, wan5, usb1, usb2
web_allow               : Disable
telnet_allow            : Disable
ssh_allow               : Disable
https_allow             : Disable
sslproxy_allow          : disable
ftp_allow               : Disable
samba_allow             : Disable
.
.
.
```

6.12.2 Telnet Command: admin_passwd

Users could use the [admin_passwd] command to configure administrator password by entering new password, and confirm password.

Syntax

```
Vigor3900@config-sys# admin_passwd
```

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys# admin_passwd
Vigor3900@config-sys# admin_passwd
Changing password for admin
New password:
Bad password: similar to username
Retype password:
```

```
Password for admin changed by root
Vigor3900@config-sys#
```

6.12.3 Telnet Command: autodiscovery

Users could use the [autodiscovery] command to enable auto discovery mode.

Syntax

```
Vigor3900@config-sys# autodiscovery get
Vigor3900@config-sys# autodiscovery set [mode mode]
```

Command	Description
get	Get the configuration of auto discovery mode.
set	Configure settings for auto discovery mode.
[mode mode]	Enable / disable the function of auto discovery mode. [mode] - Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys#
Vigor3900@config-sys# autodiscovery set mode enable
set done
Vigor3900@config-sys# autodiscovery get
mode              : Enable
Vigor3900@config-sys#
```

6.12.4 Telnet Command: cc

Users could use the [cc] command to configure country code settings.

Syntax

```
Vigor3900@config-sys# cc get
Vigor3900@config-sys# cc set [value]
```

Command	Description
get	Get the configuration of country code.
set	Configure settings for country code.
[value]	Enter the number which can represent a country.

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys#
Vigor3900@config-sys# cc set 23
Set country code success.
Vigor3900@config-sys# cc get
```

```
Country code=23
```

6.12.5 Telnet Command: cmm

Users can use the [cmm] command to configure Connect to Fast Forward Conntrack; then the screen will Entering character mode.

Syntax

```
Vigor3900@config-sys# cmm
```

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys#
Vigor3900@config-sys# cmm

Entering character mode
Escape character is '^]'.

Welcome to the Fast Forward Contrack module monitor CLI
cmm> ?
  help              Show available commands
  quit              Disconnect
  logout            Disconnect
  exit              Exit from current mode
  history           Show a list of previously run commands
  enable            Turn on privileged commands
  show
  query
  set
  ipv4
  ipv6
  prf
  mspmem
  vlan
  gre               GRE settings
```

6.12.6 Telnet Command: config

Users could use [config] command to configure Configuration Backup.

6.12.6.1 Telnet Command: automatic get, automatic set

It is used for reviewing the detailed settings or modifying settings for automatic backup configuration.

Syntax

```
Vigor3900@config-sys# config automatic get
Vigor3900@config-sys# config automatic set [status status] [interval
interval] [date_day date_day] [date_weekday date_weekday] [date_time
date_time] [only_change only_change]
```

Command	Description
get	Get the configuration of automatic backup configuration.
set	Modify settings for automatic backup configuration.
[status status]	Enable / disable the function of automatic backup configuration. [status] – Enter Enable or Disable.
[interval interval]	Specify an interval for automatic backup. [interval]- Available settings include: ● Daily ● Weekly ● Monthly
[date_day date_day]	Specify a date. [date_day] – Enter 1 to 31 to reprensent different date in a month.
[date_weekday date_weekday]	Specify which day (in one week) to perform the automatic backup. [date_weekday] – Available settings include: ● Mon ● Tue ● Wed ● Thu ● Fri ● Sat ● Sun
[date_time date_time]	Specify the backup time in a day. [date_time] – Enter the hour and the minute (e.g., 00:00)
[only_change only_change]	Enable / disable the function of Only backup when config changed. [only_change] – Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys#
Vigor3900@config-sys# config automatic set date_time 01:01
only_change enable
set done
Vigor3900@config-sys# config automatic set status enable
Vigor3900@config-sys# config automatic get
status              : Enable
interval            : Weekly
date_day            : 1
date_weekday        : Sun
date_time           : 01:01
only_change         : Enable
```

```
cfg_files           : backup-20110102-080509-1.4.0_Beta,
backup-20110102-080858-1.4.0_Beta
Vigor3900@config-sys#
```

6.12.6.2 Telnet Command: backup

It is used for backup configuration to remote TFTP server.

Syntax

```
Vigor3900@config-sys# config backup [serverip][filename]
```

Command	Description
[serverip]	Specify the IP address of TFTP server. [serverip] – Enter the IP address (e.g., 192.168.1.130) of TFTP server.
[filename]	Specify the filename on server (e.g., cfg.tar.gz).

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys#
Vigor3900@config-sys# config backup 192.168.1.130 cfg.tar.gz
Configuration backup... tar: removing leading '/' from member names
done
Vigor3900@config-sys#
```

6.12.6.3 Telnet Command: default_set

It is used for customizing default configuration.

Syntax

```
Vigor3900@config-sys# config default_set enable [filename]
Vigor3900@config-sys# config default_set disable
Vigor3900@config-sys# config default_set get
```

Command	Description
default_set enable [filename]	Enable the function of customized default configuration. [filename] – Enter the name of configuration backup file (created by using *config local backup, refer to 6.12.6.4*).
default_set disable	Disable the function of customized default configuration.
default_set get	Get the information for customized default configuration.

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys# config default_set
Vigor3900@config-sys# config default_set enable
backup-20171208-173919-1.4.0_Beta
Vigor3900@config-sys#
```

```
Vigor3900@config-sys# config default_set get
Customized default configuration enabled. configuration name:
Name: backup-20171208-173919-1.4.0_Beta
Model: Vigor3900
Created time: 2017-12-08 17:39:19
Firmware version: 1.4.0_Beta
Comment: test_for_carrie
Vigor3900@config-sys#
```

6.12.6.4 Telnet Command: local

It is used for creating or deleting configuration backup file in ***local storage***. Before using the commands of "backup", "restore" or "default_set", perform such command first.

Syntax

```
Vigor3900@config-sys# config local backup [comment]
Vigor3900@config-sys# config local delete [conf_name]
Vigor3900@config-sys# config local download [serverip][filename]
Vigor3900@config-sys# config local list
Vigor3900@config-sys# config local restore [filename]
Vigor3900@config-sys# config local upload [serverip] [filename]
```

Command	Description
backup [comment]	[comment] – Enter a name for configuration backup.
delete [conf_name]	Delete backup configuration file in local storage. [conf_name] – Enter the name of backup configuration file.
download [serverip] [filename]	Download backup configuration file from local storage to TFTP server. [serverip] – Enter the IP address (e.g., 192.168.1.130) of TFTP server for storing the configuration file. [filename] – Enter the name (e.g., e.g., backup-20180105-150537-1.4.0_Beta) of the backup configuration file.
list	Display the backup configuration with detailed settings.
restore [filename]	Restore backup configuration from the local storage. [filename] – Enter the name (e.g., backup-20180105-150537-1.4.0_Beta) of the backup configuration file.
Upload [serverip] [filename]	Upload backup configuration file from TFTP server to local storage. [serverip] – Enter the IP address (e.g., 192.168.1.130) of TFTP server for storing the configuration file. [filename] – Enter the name of the backup configuration file (e.g., backup-20180105-150537-1.4.0_Beta).

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys# config local backup test_for_carrie
```

```
Starting backup ...
Backup created.
Vigor3900@config-sys#
Vigor3900@config-sys# config local list
Total 1 backup configuration(s).
List of local backup configuration(s):
Name: backup-20171208-173919-1.4.0_Beta
Model: Vigor3900
Created time: 2017-12-08 17:39:19
Firmware version: 1.4.0_Beta
Comment: test_for_carrie
Vigor3900@config-sys#config local download 192.168.1.130
backup-20110102-080858-1.4.0_Beta
download
Vigor3900@config-sys#config local restore
backup-20180105-150537-1.4.0_Beta
Start restoring configuration ...
Restore OK ,reboot
Vigor3900@config-sys#
```

遺失與主機的連線。

6.12.6.5 Telnet Command: restore

It is used for restoring configuration from ***remote TFTP*** server.

Syntax

```
Vigor3900@config-sys# config restore [serverip][filename]
```

Command	Description
[serverip][filename]	[serverip] – Enter the IP address (e.g, 192.168.1.130) of TFTP server. [filename] – Enter the name of TFTP server (e.g., cfg.tar.gz).

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys# config restore
Vigor3900@config-sys# config restore 192.168.1.130 cfg.tar.gz
Configuration restore... tar: removing leading '/' from member names
etc/persistence/config/
etc/persistence/config/vs
etc/persistence/config/dmz
etc/persistence/config/lpd
etc/persistence/config/nat
etc/persistence/config/qos
etc/persistence/config/rrd
etc/persistence/config/swm
…….
etc/persistence/data/ipsec.d/private/private_key_Local_CA.pem
```

```
cp: cannot stat '/tmp/config': No such file or directory
rm: cannot remove '/tmp/config': No such file or directory
done
Vigor3900@config-sys#
```

6.12.7 Telnet Command: firmware

Users could use [firmware] command to perform firmware upgrade.

Syntax

```
Vigor3900@config-sys# firmware upgrade [serverip] [filename] [default]
```

Command	Description
[serverip]	[serverip] – Enter the IP address of TFTP server.
[filename]	[filename] – Enter the name of the firmware (e.g., V3K9.all) of Vigor router stored in TFTP server. Such file shall be stored in the database of Vigor router beforehand.
[default]	Reboot Vigor router with default setting. [default] – Enter “true” or “false”.

Example

```
Vigor3900>enable
Vigor3900# configure system#
Vigor3900@config-sys# firmware upgrade
Vigor3900@config-sys# firmware upgrade 192.168.1.130 V3K9.all
Firmware Update: Downloading image file from server.
Firmware Update: Download OK
Firmware Update: Checking if the firmware is valid
Firmware Update: Checksum passed. from tmp
Firmware Update: Shutting down applications
Firmware Update: Writing image to flash. Do not turn off or reboot the
machine. from
Firmware Update: Upgrade success. from
Firmware Update: Rebooting...
```

6.12.8 Telnet Command: mailalert

Users could use [mailalert] command to configure Mail Alert settings and use the [get], [set], [mailto] command to configure the details information.

Syntax

```
Vigor3900@config-sys# mailalert get
Vigor3900@config-sys# mailalert set [status status] [mailfrom mailfrom]
[smtpserver smtpserver] [smtpport smtpport] [ssl_tls ssl_tls]
[user_login user_login] [user_name user_name] [user_password
user_password] [usermail usermail] [vpnmail vpnmail]
Vigor3900@config-sys# mailalert mailto add <member>
Vigor3900@config-sys# mailalert mailto remove <member>
```

Command	Description
get	Get the configuration of mail alert configuration.
set	Modify settings for mail alert configuration.
[status status]	Enable / disable the function of Mail Alert. [status] – Enter Enable or Disable.
[mailfrom mailfrom]	Specify an e-mail address of sender. [mailfrom] – Enter the e-mail address.
[smtpserver smtpserver]	Specify an IP address for SMTP server. [smtpserver] – Enter the IP address.
[smtpport smtpport]	Specify a port number for SMTP server. [smtpport] – Enter a number (ranging from 1 ~ 65535).
[ssl_tls ssl_tls]	Specify communications privacy over the Internet. [ssl_tls] – Available settings include: ● Disable ● StartTLS ● SSL ● TLS
[user_login user_login	Enable / disable the function of login by SMTP server. [user_login] - Enter Enable or Disable.
[user_name user_name]	Specify a login name for SMTP server. [user_name] – Enter a string as login name.
[user_password user_password]	Specify a password for SMTP server. [user_password] – Enter a string as password.
[usermail usermail]	Enable / disable the function of User Access Mail Alert. [usermail] - Enter Enable or Disable.
[vpnmail vpnmail]	Enable / disable the function of VPN Mail Alert. [vpnmail] – Enter Enable or Disable.
mailto add <member>	Add a destination e-mail address. <member> - Enter an e-mail address.
mailto remove <member>	Remove an existed e-mail address. <member> - Enter an e-mail address.

Example

```
Vigor3900>enable
Entering enable mode...
Vigor3900# configure system
Vigor3900@config-sys# mailalert get
status              : Disable
mailfrom            :
mailto              :
smtpserver          :
```

```
smtpport            : 25
ssl_tls             : disable
user_login          : Disable
user_name           :
usermail            : enable
vpnmail             : Disable
Vigor3900@config-sys# mailalert set status enable vpnmail enable

set done

Vigor3900@config-sys#
```

6.12.9 Telnet Command: ntpclient

It is used for configuring time and date of Vigor router.

Syntax

```
Vigor3900@config-sys# ntpclient get
Vigor3900@config-sys# ntpclient set [status status] [server server]
[port port] [interval interval] [zone zone] [daylight daylight]
Vigor3900@config-sys# ntpclient manual <date>
```

Command	Description
get	Get the time configuration.
set	Modify the time settings.
[status status]	Specify which time type will be used. [status] – Enter NTP or Browser.
[server server]	Specify the IP address / domain name of NTP server. [server]- Enter the IP address or the domain name.
[port port]	Specify a port number for NTP server. [port] – Enter a port number.
[interval interval]	Specify the request interval. [interval] - Enter
[zone zone]	Specify the time zone for Vigor router. [zone] – Available settings include: Eniwetok/MidwayIslands/Samoa/Hawaii/Alaska/PacificTime/Tijuana/Arizona/MountainTime/CentralTime/MexicoCity/Saskatchewan/Tegucigalpa/Bogota/EasternTime/Indiana/Lima/Quito/Caracas/AtlanticTime/Georgetown/LaPaz/Santiago/Newfoundland/Brasilia/BuenosAires/Mid-Atlantic/Azores/Casablanca/Greenwich/Lisbon/London/Monrovia/Amsterdam/Belgrade/Berlin/Bern/Bratislava/Brussels/Budapest/Copenhagen/Edinburgh/Ljubljana/Madrid/Oslo/Paris/Prague/Rome/Sarajevo/Skopje/Stockholm/Vienna/Warsaw/Zagreb/Windhoek/Athens/Bucharest/Cairo/Harare/Helsinki/Istanbul/Jerusalem/Pretoria/Riga/Sofia/Tallinn/Vilnius/Baghdad/Kuwait/Moscow/Nairobi/Riyadh/Tehran/AbuDhabi/Baku/Muscat/SaintPetersburg/Tbilisi/Volgograd/Kabul/Ekaterinburg/Islamabad/Karachi/Mumbai/Kolkata/Colombo/Madras/NewDelhi/Kathmandu/Alma

	ty/Astana/Dhaka/Rangoon/Bangkok/Hanoi/Jakarta/Beijing/Chongqing/HongKong/Perth/Singapore/Taipei/Urumqi/Osaka/Sapporo/Seoul/Tokyo/Yakutsk/Adelaide/Darwin/Brisbane/Canberra/Guam/Hobart/Magadan/Melbourne/PortMoresby/Sydney/Vladivostok/NewCaledonia/SolomonIslands/Auckland/Fiji/Kamchatka/Kwajalein/MarshallIslands/Wellington
[daylight daylight]	Enable / disable the function of daylight saving. [daylight] – Enter Enable or Disable.
manual <date>	Manually set current time and date. <date> - Enter the date and time with the format of "MMDDhhmmYYYY" (e.g., manual 120812102017).

Example

```
Vigor3900>enable
Vigor3900@config-sys# ntpclient get

Current System Time  :
status               : NTP
server               : pool.ntp.org
port                 : 123
interval             : 600
zone                 : Taipei
daylight             : Disable
Vigor3900@config-sys# ntpclient set status Browser

set done

Vigor3900@config-sys# ntpclient manual 120812102017
Vigor3900@config-sys# ntpclient get

Current System Time  :
status               : Browser
server               : pool.ntp.org
port                 : 123
interval             : 600
zone                 : Taipei
daylight             : Disable

Vigor3900@config-sys#
```

6.12.10 Telnet Command: reboot

Users can use the [reboot] command to reboot Vigor router and type the [reboot default] command to reboot with factory by default.

Syntax

```
Vigor3900@config-sys# reboot
Vigor3900@config-sys# reboot default
```

6.12.11 Telnet Command: snmpagent

Users can use the [snmpagent] command to configure SNMP and then use the [get], [set] command to configure the the details information.

Syntax

```
Vigor3900@config-sys# snmpagent get
Vigor3900@config-sys# snmpagent set [status status] [getcommunity
getcommunity] [setcommunity setcommunity] [dfl dfl_host] [mgnip mgnip]
[notification_host notification_host] [snmpv3_status snmpv3_status]
[usm usm] [auth auth_algorithm] [auth_password auth_password] [privacy
privacy_algorithm] [privacy_password privacy_password]
```

Command	Description
get	Get the configuration of SNMP agent.
set	Modify the settings of SNMP agent.
[status status]	Enable / disable the function of SNMP. [status] – Enter Enable or Disable.
[getcommunity getcommunity]	Set the get community. [getcommunity] – Enter a string. The default is “public”.
[setcommunity setcommunity]	Set the set community. [setcommunity] – Enter a string. The default is “private”.
[dfl dfl_host]	Enable / disable the function of Default Host IP/Mask. [dfl_host] - Enter Enable or Disable.
[mgnip mgnip]	Set an IP range to manage. [mgnip]- Enter an IP address with subnet mask (e.g., 192.168.1.1/24).
[notification_host notification_host]	Specify an IP address for notification host. [notification_host] – Enter an IP address.
[snmpv3_status snmpv3_status]	Enable / disable the SNMPV3 agent. [snmpv3_status] - Enter Enable or Disable.
[usm usm]	It means “user-based security mode”. [usm]- Enter a user name which will be used for authentication. The maximum length of the text is limited to 23 characters.
[auth auth_algorithm]	Specify the authentication algorithm. [auth_algorithm] – Available settings include: ● No_Auth ● MD5 ● SHA
[auth_password auth_password]	Set a password for authentication. [auth_password] – Enter a string as password.
[privacy privacy_algorithm]	Specify the privacy algorithm. [privacy_algorithm] – Available settings include: ● No_Priv ● DES ● AES
[privacy_password privacy_password]	Set a password for privacy. [privacy_password] – Enter a string as password.

Example

```
Vigor3900>enable
Vigor3900@config-sys# snmpagent get
status               : Disable
getcommunity         : public
setcommunity         : private
dfl                  : enable
mgnip                : default
notification_host    : 0.0.0.0
snmpv3_status        : Disable
usm                  :
auth                 : No_Auth
auth_password        :
privacy              : No_Priv
privacy_password     :
```

6.12.12 Telnet Command: syslogd

Users can use the [syslogd] command to configure syslog and use [get] or [set] command to configure the details information.

Syntax

```
Vigor3900@config-sys# syslogd get
Vigor3900@config-sys# syslogd set [status status] [ip remotehost] [port
remoteport] [log_to_usb log_to_usb] [reposit_days reposit_days]
[routername routername] [firewall firewall] [vpn vpn] [useraccess
useraccess] [ua_high_priority ua_high_priority] [wan wanlog] [others
others]
```

Command	Description
get	Get the configuration of SNMP agent.
set	Modify the settings of SNMP agent.
[status status]	Specify a method to determine current status for Syslog access. [status] – Available settings include: ● Disable ● Remote ● Local ● Both
[ip remotehost]	Such option is available when Remote / Both is selected in Status. Set the IP address of host name of Syslog server. [remotehost] – Enter the IP address or host name.
[port remoteport]	Set the port number for the Syslog server. Such option is available when Remote / Both is selected in Status. [remoteport] – Enter a port number.
[log_to_usb log_to_usb]	Enable / disable the function of storing syslog in USB disk. [log_to_usb] – Enter Enable or Disable.
[reposit_days	Specify the period of keeping record of Syslog in USB.

reposit_days]	[reposit_days]- Enter a number (ranging from 1 to 9999).
[routername routername]	Set a name for such router. [routername] – Enter a string.
[firewall firewall]	Enable / disable the function of recording Firewall log onto Syslog. [firewall] – Enter Enable or Disable.
[vpn vpn]	Enable / disable the function of recording VPN log onto Syslog. [vpn] – Enter Enable or Disable.
[useraccess useraccess]	Enable / disable the function of recording user access log onto Syslog. [useraccess] – Enter Enable or Disable.
[ua_high_priority ua_high_priority]	Enable / disable the function of User Access Log High Priority which can reduce the loss of user access log. [ua_high_priority] – Enter Enable or Disable.
[wan wanlog]	Enable / disable the function of recording WAN log onto Syslog. [wanlog] – Enter Enable or Disable.
[others others]	Enable / disable the function of recording all other log onto Syslog. [others] – Enter Enable or Disable.

Example

```
Vigor3900>enable
Vigor3900@config-sys# syslogd set reposit_days 6 vpn disable
set done

Vigor3900@config-sys# syslogd get
status              : Local
ip                  : 127.0.0.1
port                : 514
log_to_usb          : Disable
reposit_days        : 6
routername          : Vigor
firewall            : Enable
vpn                 : Disable
useraccess          : Disable
ua_high_priority    : Disable
wan                 : Enable
others              : Enable
```

6.12.13 Telnet Command: tr069

Users can use the [tr069] command to configure TR-069 settings and use [get] or [set] command to configure the details information.

Syntax

```
Vigor3900@config-sys# tr069 get
```

```
Vigor3900@config-sys# tr069 set [status status] [wan_profile
wan_profile] [wan_failover wan_failover][acs_server acs_server]
[acs_username acs_username] [acs_password acs_password][cpe_proto
cpe_proto] [port port] [cpe_username cpe_username] [cpe_password
cpe_password] [tr069_log tr069_log] [period_status period_status]
[period period] [stun_status stun_status] [stun_host stun_ip]
[stun_port stun_port] [stun_min_period stun_min_keepalive]
[stun_max_period stun_max_keepalive]
```

Command	Description
get	Get the configuration of SNMP agent.
set	Modify the settings of SNMP agent.
[status status]	Enable / disable the configuration of TR-069. [status] – Enter Enable or Disable.
[wan_profile wan_profile]	Specify WAN/LAN profile to be recognized by VigorACS. [wan_profile] – Enter the name of WAN interface (e.g., wan1).
[wan_failover wan_failover]	Specify the WAN interface to take over the job of network connection when the original WAN interface fails. [wan_failover] – Enter the name of WAN/USB WAN interface (e.g., wan2).
[acs_server acs_server]	Specify the IP address of VigorACS server. [acs_server] – Enter the IP address.
[acs_username acs_username]	Specify a username for VigorACS server. [acs_username] – Enter a string.
[acs_password acs_password]	Specify a password for VigorACS server. [acs_password] – Enter a string.
[cpe_proto cpe_proto]	Specify CPE protocol. [cpe_proto] – Available settings include: ● http ● https
[port port]	Specify a port number for Vigor router. [port] – Enter a port number (ranging from 0 – 65535).
[cpe_username cpe_username]	Specify user name for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900. [cpe_username] – Enter a string as username.
[cpe_password cpe_password]	Specify password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900. [cpe_password] – Enter a string as password.
[tr069_log tr069_log]	Record log related to TR-069 configuration. [tr069_log] – Enter Enable or Disable.
[period_status period_status]	Enable / disable the function of Periodic Status. [period_status] – Enter Enable or Disable.
[period period]	Specify a time period as Periodic Time. [period] – Enter a number (ranging from 60 ~ 86400). Unit is

	second.
[stun_status stun_status]	Enable / disable the STUN server. [stun_status] – Enter Enable or Disable.
[stun_host stun_ip]	Specify the IP address of STUN server. [stun_ip]- Enter the IP address.
[stun_port stun_port]	Specify a port number for STUN server. [stun_port] – Enter a port number (ranging from 1 – 65535).
[stun_min_period stun_min_keepalive]	If STUN server is enabled, specify a time period (minimum) for maintaining the binding in the Gateway. The default setting is “60 seconds”. [stun_min_keepalive] – Enter a number (ranging from 60 ~ 86400). Unit is second.
[stun_max_period stun_max_keepalive]	If STUN server is enabled, specify a time period (maximum) for maintaining the binding in the Gateway. A value of “-1” indicates that no maximum period is specified. [stun_max_keepalive] – Enter a number (ranging from 60 ~ 86400). Unit is second.

Example

```
Vigor3900>enable
Vigor3900@config-sys# tr069 set status enable wan_failover wan2
tr069_log enable period 1000
set done
Vigor3900@config-sys# tr069 get
status              : Enable
wan_profile         : wan1
wan_failover        : wan2
acs_server          :
acs_username        : acs
acs_password        : **********
cpe_time            :
connect_acs_status  : OFF
cpe_proto           : http
port                : 8069
cpe_url             : http://:8069/cwmp/creq
cpe_username        : vigor
cpe_password        : **********
tr069_log           : Enable
period_status       : Enable
period              : 1000
stun_status         : Disable
stun_host           : 0.0.0.0
stun_port           : 3478
stun_min_period     : 60
stun_max_period     : 90
```