

DrayTek

Vigor3900

Multi-WAN Security Appliance

DrayTek

Providing Productivity and Security for
Small, Medium and Large Businesses

Your reliable networking solutions partner

User's Guide

V2.0



TAIWAN
EXCELLENCE
2012

Vigor3900

Multi-WAN Security Appliance

User's Guide

Version: 2.0

Firmware Version: V1.1.0

(For future update, please visit DrayTek website)

Date: September 1, 2015

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 by 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 to restore 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>

European Community Declarations

Manufacturer: DrayTek Corp.

Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu County, Taiwan
303

Product: Vigor3900

DrayTek Corp. declares that Vigor3900 of routers are in compliance with the following essential requirements and other relevant provisions of EC, Directive 2004/108/EC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class A and EN55024/Class A.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.



More update, please visit 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
<hr/>	
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
<hr/>	
Chapter 3: Application and Tutorial.....	21
3.1 How to Configure Load Balance with Multi-WAN on Vigor3900?	21
3.2 How to Configure OSPF?.....	27
3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode)	33
3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server?	36
3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router.....	41
3.6 How to Setup 50 WANs on Vigor3900	50
3.7 CVM Application - How to manage the CPE (router) through Vigor3900?	55
3.8 CVM Application - How to build the VPN between remote devices and Vigor3900?	60
3.9 CVM Application - How to upgrade CPE firmware through Vigor3900?	63
3.10 How to use High Availability for Vigor routers?	69
3.11 How to Configure DNS Inbound Load Balance on Vigor 3900?	73
<hr/>	
Chapter 4: Advanced Web Configuration	77
4.1 WAN Setup.....	77
4.1.1 General Setup.....	78
4.1.2 Inbound Load Balance.....	98
4.1.3 Switch	104
4.2 LAN	109
4.2.1 General Setup.....	109
4.2.2 PPPoE Server.....	123
4.2.3 Switch	127
4.2.4 Bind IP to MAC	133
4.2.5 LAN DNS	136
4.3 Routing	139
4.3.1 Load Balance Pool.....	139
4.3.2 Static Route	143

4.3.3 Policy Route.....	149
4.3.4 Default Route.....	166
4.3.5 RIP Configuration	167
4.3.6 OSPF Configuration.....	168
4.3.7 BGP Configuration.....	171
4.4 NAT.....	176
4.4.1 Port Redirection	176
4.4.2 DMZ Host.....	180
4.4.3 ALG	182
4.4.4 Connection Timeout.....	184
4.5 Firewall.....	185
4.5.1 Filter Setup	185
4.5.2 DoS Defense	210
4.5.3 MAC Block	213
4.6 Objects Setting.....	215
4.6.1 IP Object	216
4.6.2 IP Group	218
4.6.3 IPv6 Object	220
4.6.4 Country Object.....	222
4.6.5 Service Type Object	224
4.6.6 Service Type Group.....	226
4.6.7 Keyword /DNS Object.....	228
4.6.8 File Extension Object.....	232
4.6.9 APP Object	234
4.6.10 Web Category Object	238
4.6.11 QQ Object.....	242
4.6.12 QQ Group	245
4.6.13 Time Object	247
4.6.14 Time Group.....	249
4.6.15 SMS Service Object.....	251
4.6.16 Mail Service Object.....	253
4.6.17 Notification Object.....	255
4.7 User Management.....	257
4.7.1 Web Portal	258
4.7.2 User Profile	263
4.7.3 User Group	276
4.7.4 Guest Profile	278
4.7.5 RADIUS	284
4.7.6 LDAP/Active Directory	286
4.8 Application	289
4.8.1 Dynamic DNS	289
4.8.2 GVRP	294
4.8.3 IGMP Proxy	295
4.8.4 UPnP	297
4.8.5 High Availability	298
4.8.6 Wake on LAN.....	308
4.8.7 SMS / Mail Alert Service	311
4.9 VPN and Remote Access.....	315
4.9.1 VPN Client Wizard	315
4.9.2 VPN Server Wizard.....	322
4.9.3 Remote Access Control	328
4.9.4 PPP General Setup	329
4.9.5 IPSec General Setup.....	333
4.9.6 VPN Profiles	334

4.9.7 VPN Trunk Management	347
4.9.8 Connection Management	352
4.10 Certificate Management	354
4.10.1 Local Certificate	355
4.10.2 Trusted CA Certificate	360
4.10.3 Remote Certificate	363
4.11 SSL Proxy	364
4.11.1 SSL Web Proxy	364
4.11.2 SSL Application	366
4.11.3 Online User Status	370
4.12 Central VPN Management	371
4.12.1 General Setup	371
4.12.2 CPE Management	373
4.12.3 Log/Alert	381
4.13 Bandwidth Management	383
4.13.1 Quality of Service	383
4.13.2 QoS Rule	387
4.13.3 Sessions Limit	394
4.13.4 Bandwidth Limit	397
4.14 USB Application	401
4.14.1 Disk Status	401
4.14.2 FTP Server	402
4.14.3 Temperature Sensor	403
4.14.4 Modem Support List	405
4.15 System Maintenance	406
4.15.1 TR-069	406
4.15.2 Administrator Password	408
4.15.3 Configuration Backup	409
4.15.4 Syslog / Mail Alert	411
4.15.5 Time and Date	414
4.15.6 Access Control	415
4.15.7 SNMP Setup	419
4.15.8 Reboot System	420
4.15.9 Firmware Upgrade	423
4.15.10 APP Signature Upgrade	425
4.15.11 APP Support List	427
4.16 Diagnostics	428
4.16.1 Routing Table	428
4.16.2 ARP Cache Table	431
4.16.3 DHCP Table	434
4.16.4 Session Table	436
4.16.5 Traffic Graph	437
4.16.6 Web Console	439
4.16.7 Ping/Trace Route	439
4.16.8 Data Flow Monitor	440
4.16.9 User Status	441
4.17 External Devices	442
4.18 Product Registration	443

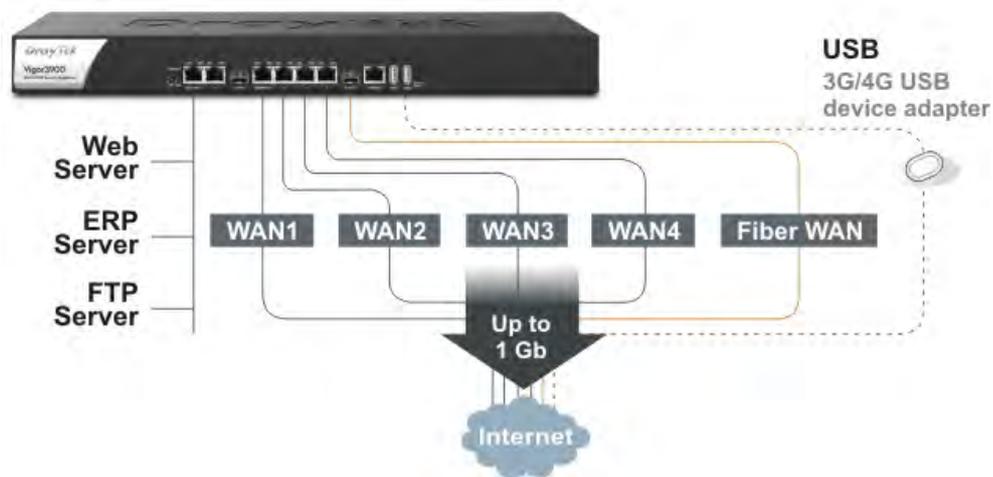
Chapter 5: Trouble Shooting.....445

5.1 Checking If the Hardware Status Is OK or Not.....	445
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	446
5.3 Pinging the Router from Your Computer	449
5.4 Checking If the ISP Settings are OK or Not	450
5.5 Backing to Factory Default Setting If Necessary.....	451
5.6 Contacting DrayTek	452

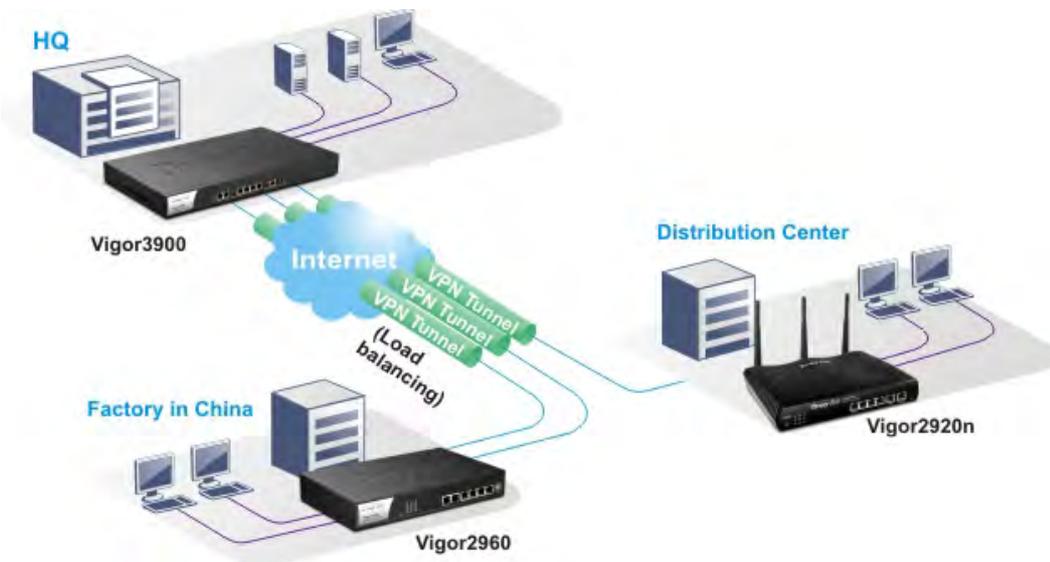
Chapter 1: Introduction

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.



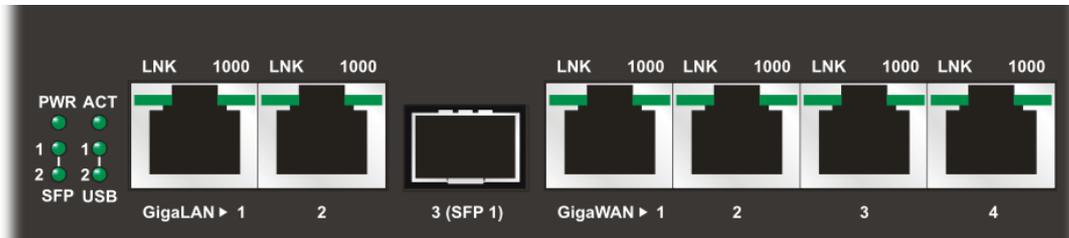
A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like an Intranet. A VPN enables you to send data between two computers across a shared public Internet network in a manner that emulates the properties of a point-to-point private 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

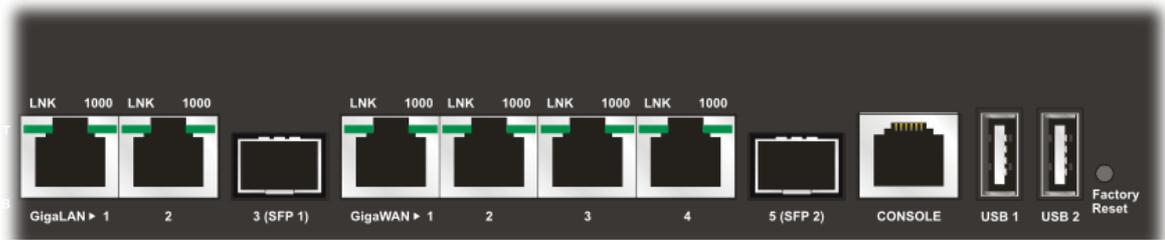
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

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	Connector for local network devices.
3(SFP)	Connector for fiber cable.
GigaWAN1/2/3/4	Connector for remote network devices.
5(SFP)	Connector for fiber cable.
Console	Provided for technician use.
USB1 / USB2	Connector 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.
	Connector for a power cord. ON/OFF - Power switch.

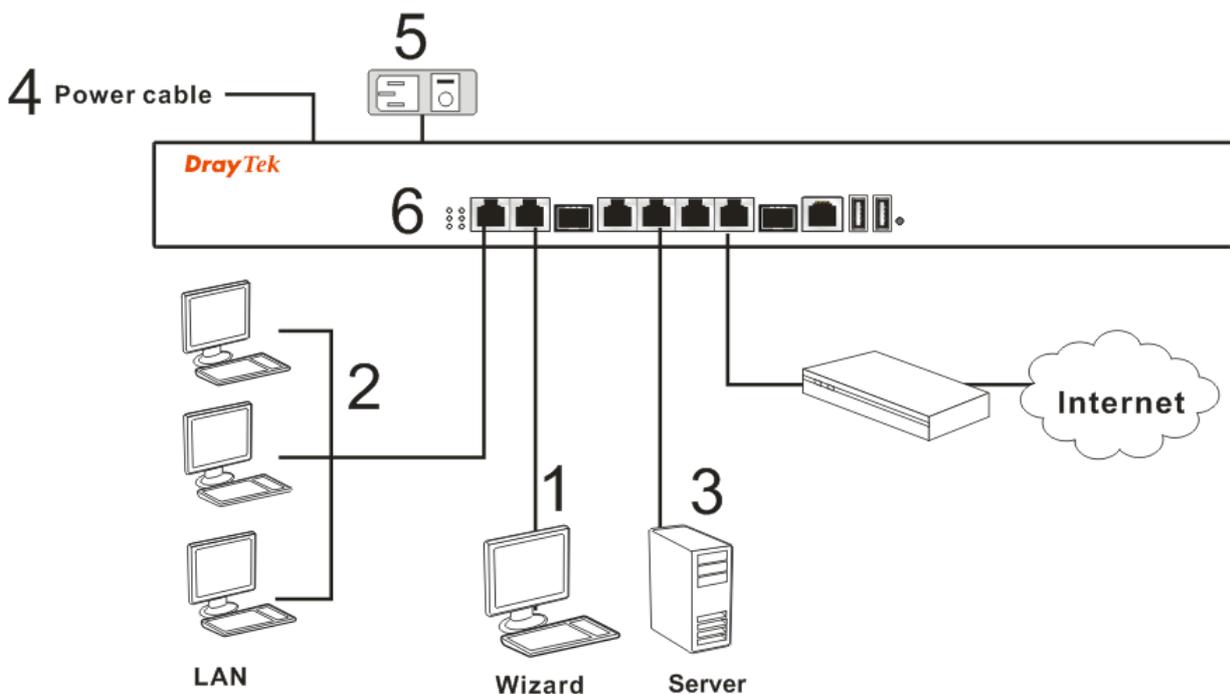
1.2 Hardware Installation

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.

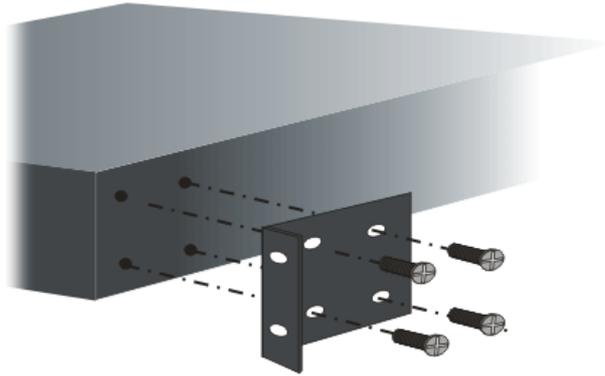


1.2.2 Rack-Mounted Installation

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**.

DrayTek **Vigor3900 Series**

Login

User :

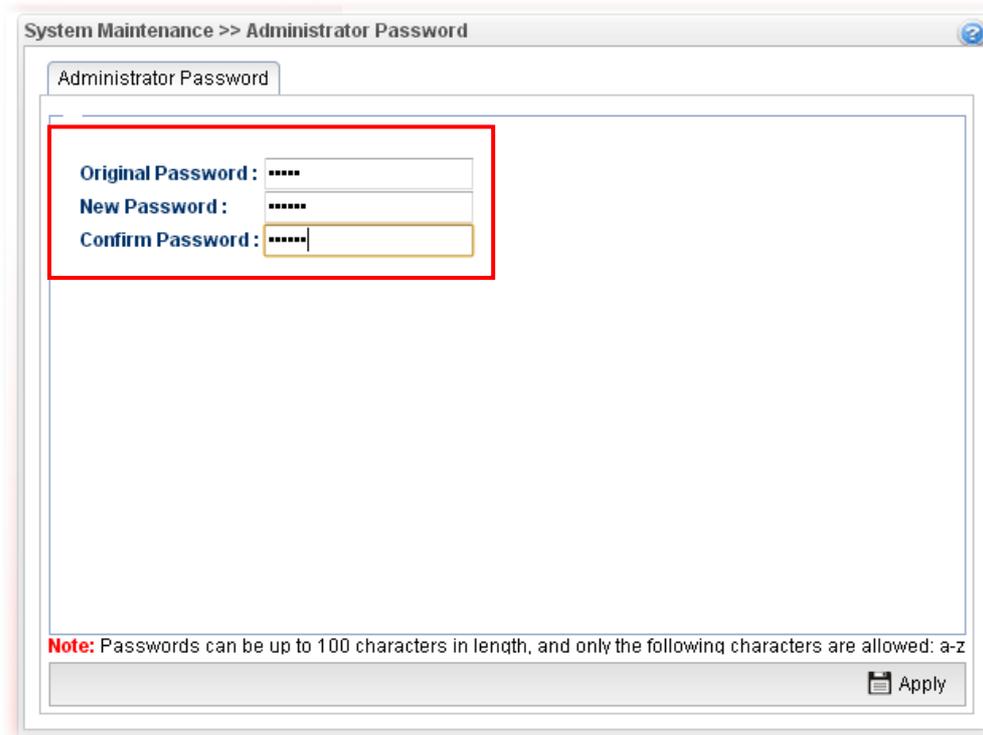
Password :

English

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



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



- 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.
- 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

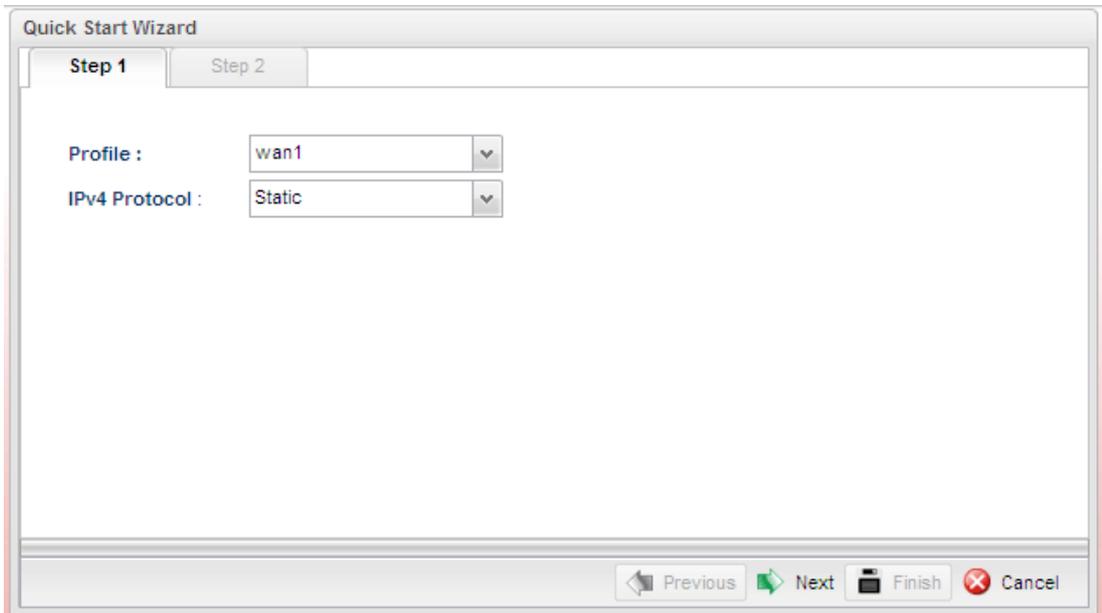
Quick Start Wizard is a wizard which is designed for configuring your router accessing Internet with simply steps. In the **Quick Start Wizard** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes.

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.

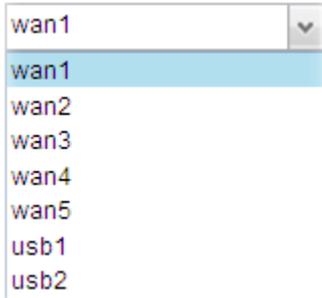
2.2.1 Step 1 - Specifying the WAN Profile

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



The screenshot shows a window titled "Quick Start Wizard" with two tabs: "Step 1" (active) and "Step 2". Under "Step 1", there are two dropdown menus. The first is labeled "Profile :" and has "wan1" selected. The second is labeled "IPv4 Protocol :" and has "Static" selected. At the bottom of the window, there are four buttons: "Previous" (disabled), "Next" (enabled), "Finish" (disabled), and "Cancel" (disabled).

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
	<p data-bbox="678 255 842 282">IPv4 Protocol :</p> <div data-bbox="890 248 1185 427" style="border: 1px solid gray; padding: 2px;"> <p data-bbox="895 255 959 282">Static</p> <p data-bbox="895 297 959 324">Static</p> <p data-bbox="895 331 959 358">DHCP</p> <p data-bbox="895 365 959 392">PPPoE</p> <p data-bbox="895 398 959 425">PPTP</p> </div> <p data-bbox="678 445 1401 544">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.</p> <p data-bbox="678 555 1410 786">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).</p> <p data-bbox="678 797 1410 996">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.</p> <p data-bbox="772 1008 1374 1140">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.</p> <p data-bbox="678 1151 1406 1382">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.</p> <p data-bbox="772 1393 1401 1559">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.</p> <p data-bbox="772 1570 1401 1736">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.</p>

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.

Quick Start Wizard

Step 1 Step 2

IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255.255.255.0

Gateway IP Address : . . .

Add Save

DNS Server IP Address

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.

Quick Start Wizard

Step 1 Step 2

IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255.255.255.0

Gateway IP Address : . . . (Optional)

Add Save

DNS Server IP Address

No items to show.

Previous Next Finish Cancel

Available parameters are listed as follows:

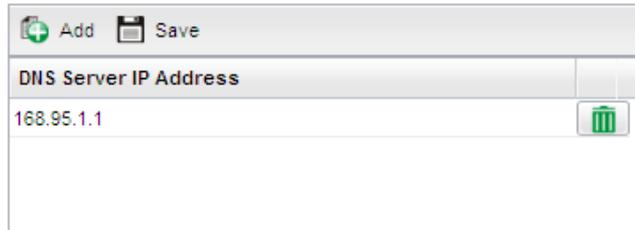
Item	Description
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile.  - click it to remove the IP address if you are not satisfied with it.

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.

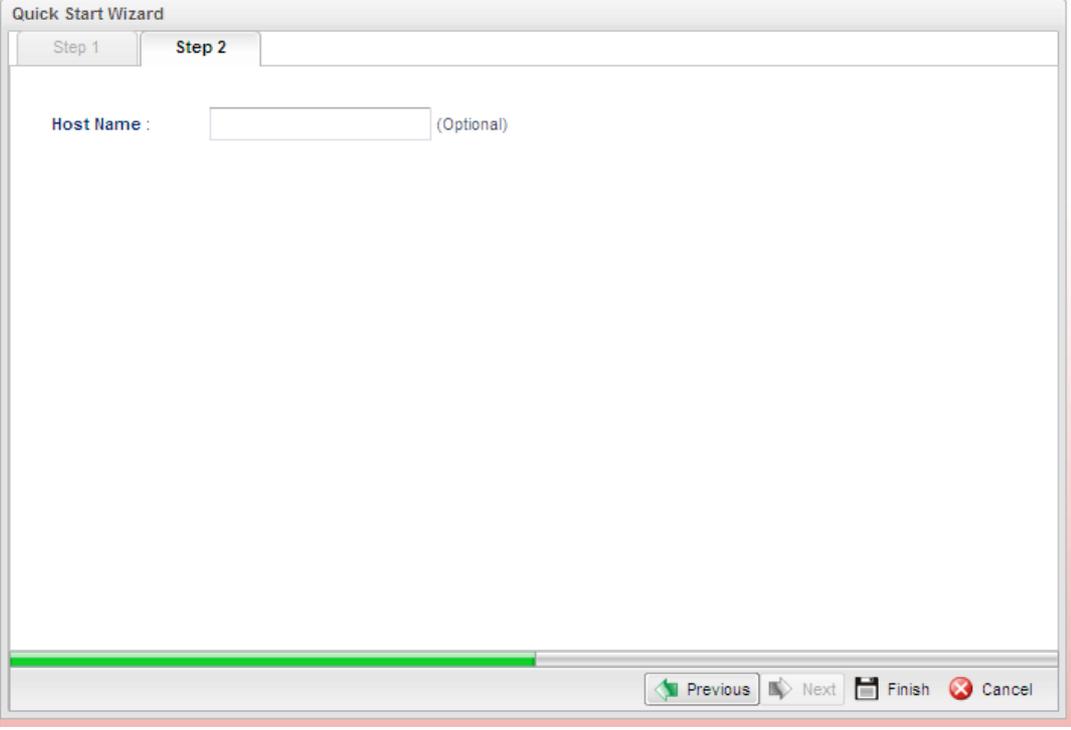
Cancel

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).



The screenshot shows a window titled "Quick Start Wizard" with two tabs: "Step 1" and "Step 2". The "Step 2" tab is active. Inside the window, there is a label "Host Name:" followed by a text input field and the text "(Optional)". At the bottom of the window, there is a progress bar and four buttons: "Previous" (with a left arrow), "Next" (with a right arrow), "Finish" (with a floppy disk icon), and "Cancel" (with a red X icon).

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.

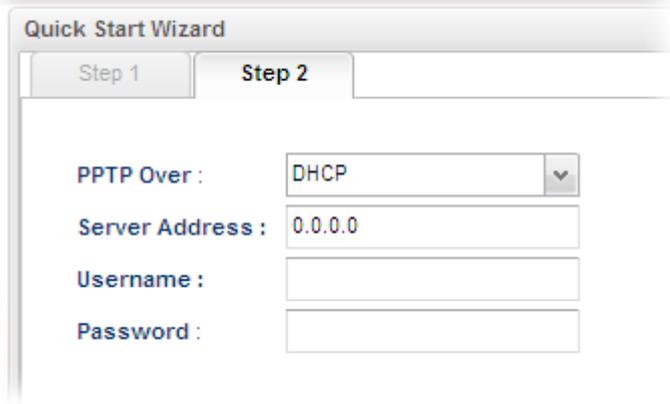
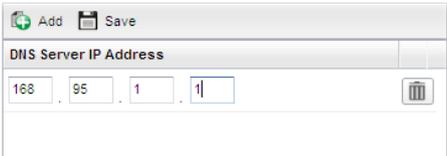
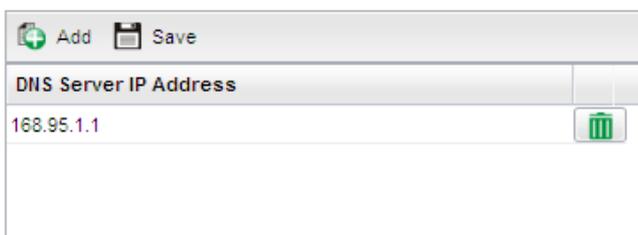
The screenshot shows the 'Quick Start Wizard' interface, specifically 'Step 2'. The configuration options are as follows:

- PPTP Over :** Static (dropdown menu)
- Server Address :** 0.0.0.0
- Username :** [Empty text box]
- Password :** [Empty text box]
- IP Address :** 0 . 0 . 0 . 0
- Subnet Mask :** 255.255.255.0 (dropdown menu)
- Gateway IP Address :** [Empty text boxes] (Optional)
- DNS Server IP Address :** A table with 'Add' and 'Save' buttons. The table contains the text 'No items to show.'

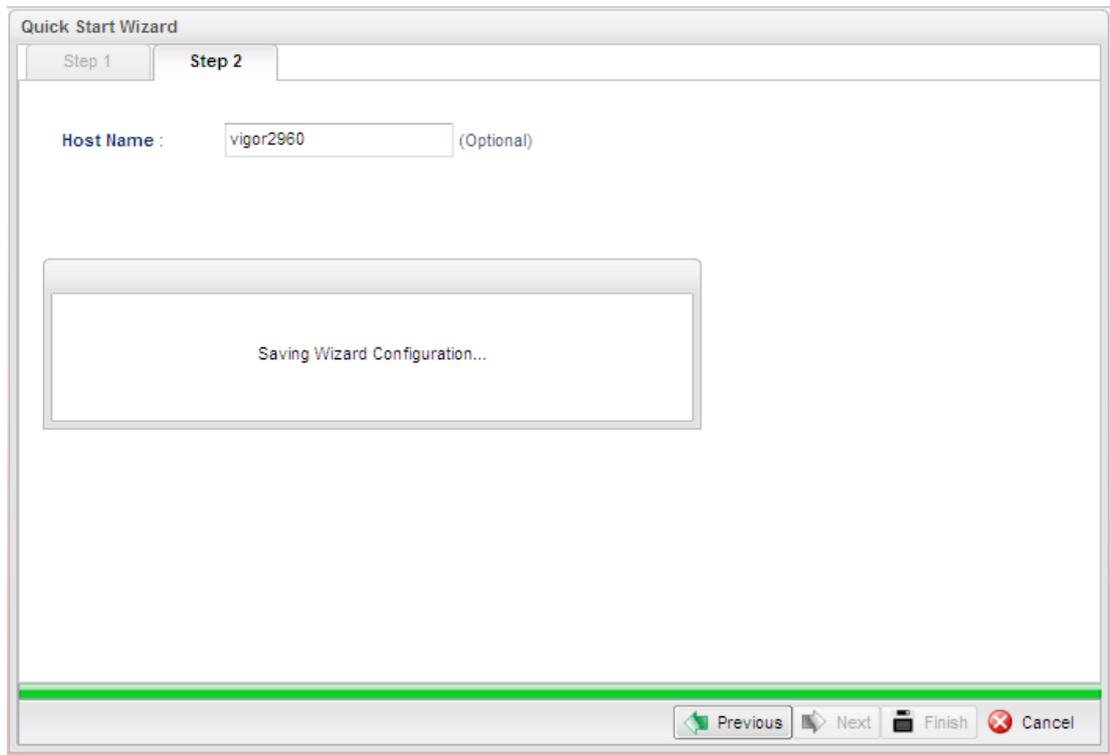
At the bottom of the wizard, there are navigation buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

Available parameters are listed as follows:

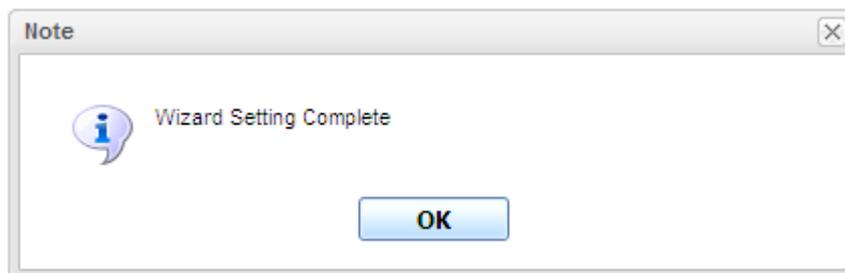
Item	Description
PPTP Over	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <div style="border: 1px solid gray; padding: 2px; width: fit-content;"> <p>Static</p> <p>Static</p> <p>DHCP</p> </div> <p>Static – specify the IP address. DHCP - obtain the IP address automatically.</p>

	
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.



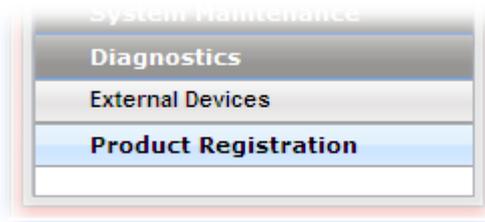
When the following screen appears, it means you have finished the Quick Start Wizard configuration.



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**.



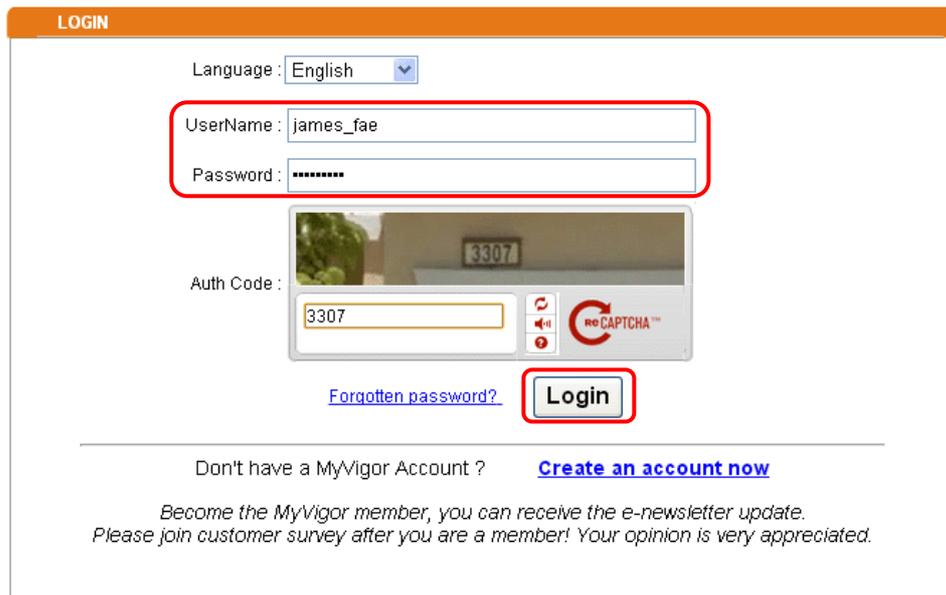
- 2 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



Please take a moment to register.

Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

A screenshot of a login page titled 'LOGIN'. It features a language dropdown menu set to 'English'. Below it are input fields for 'UserName' (containing 'james_fae') and 'Password' (masked with dots), which are enclosed in a red rectangular box. Underneath is an 'Auth Code' section with a small image of a license plate '3307' and a corresponding input field containing '3307'. To the right of the input field is a 'reCAPTCHA' logo. Below the input fields is a blue link for 'Forgotten password?' and a 'Login' button, also enclosed in a red rectangular box. At the bottom, there is a link for 'Create an account now' and a short paragraph of text.

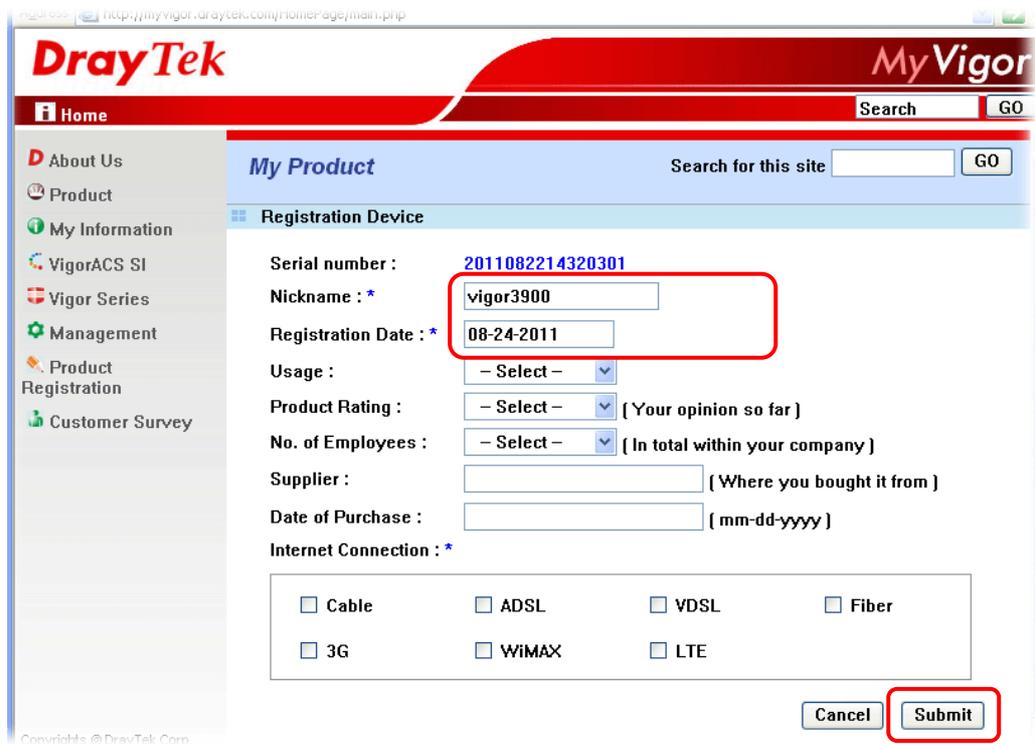
Note: If you haven't an accessing account, please create a new one first. Please **read the articles on the Agreement regarding user rights** carefully while creating a user account.

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



Note: Below the field of **Your Device List**, all the Vigor routers that you have registered to MyVigor website will be displayed in sequence.

- When the following page appears, please type in Nick Name (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.



- 5 Now, your router information has been added to the database. Click **OK** to leave this web page and return to **My Information** web page.

Your device has been successfully added to the database.



- 6 Take a look at the page of My Information, the new added Vigor3900 is listed under **Your Device List**.

The screenshot shows the MyVigor web interface. The header includes the DrayTek logo and the MyVigor title. A navigation menu on the left lists various options. The main content area is titled "My Information" and displays user login details. Below this, the "Your Device List" section contains a table with the following data:

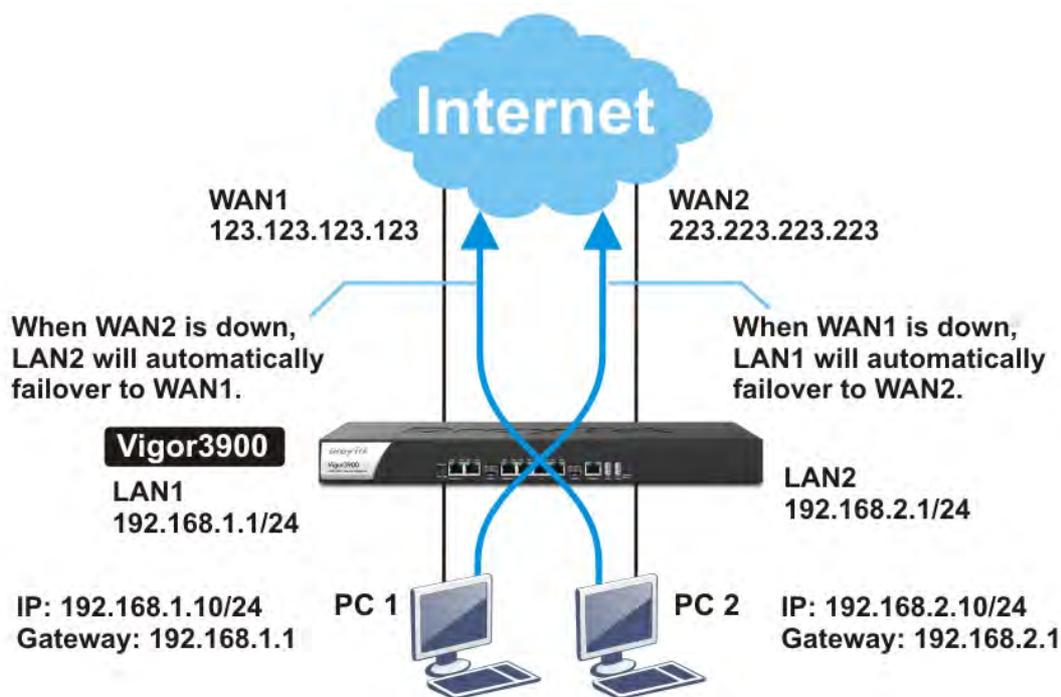
Serial Number / Host ID	Device Name	Model	Note
20100707144801	Vigor3300V	Vigor3300	-
20100708105301	Vigor2820	Vigor2820	-
20101005104801	Vigor2710vn	Vigor2710	-
2010121707335201	Vigor2920	Vigor2920	-
2011082214320301	vigor3900	Vigor3900	-

The last row of the table, representing the Vigor3900 device, is highlighted with a red border.

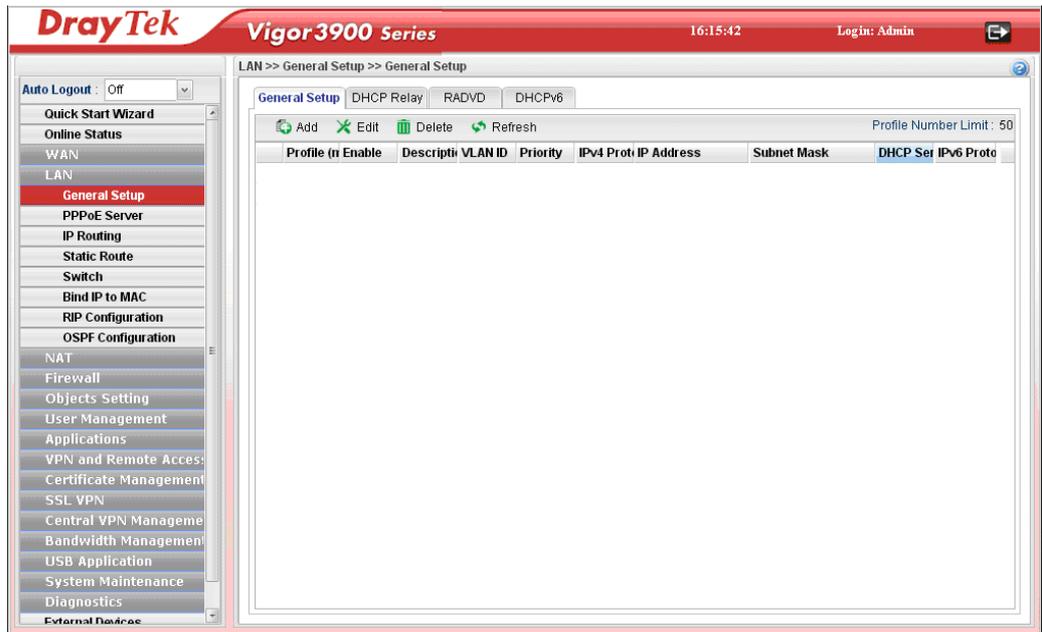
Chapter 3: Application and Tutorial

3.1 How to Configure Load Balance with Multi-WAN on Vigor3900?

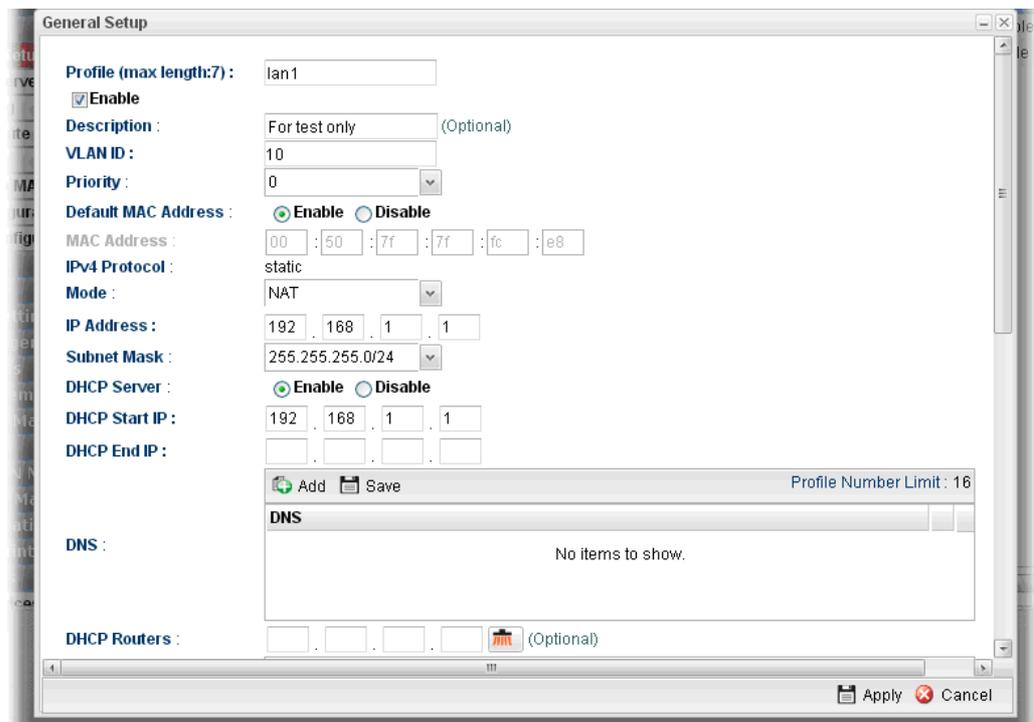
There are two different LANs configured in the following figure. One is for Sale (192.168.1.1/24) and the other is for FAE (192.168.2.1/24). Sale's LAN will be configured to go Internet always via WAN1. When WAN1 is down, Sale's LAN will automatically failover to WAN2. FAE's LAN will be configured to go Internet always via WAN2, but when WAN2 is down Sale's LAN will automatically failover to WAN1.



1. Access into the Web User Interface page of Vigor router (here, we take Vigor300B as an example).
2. Go to **LAN>>General Setup** to create a profile for LAN1 (192.168.1.1/24).

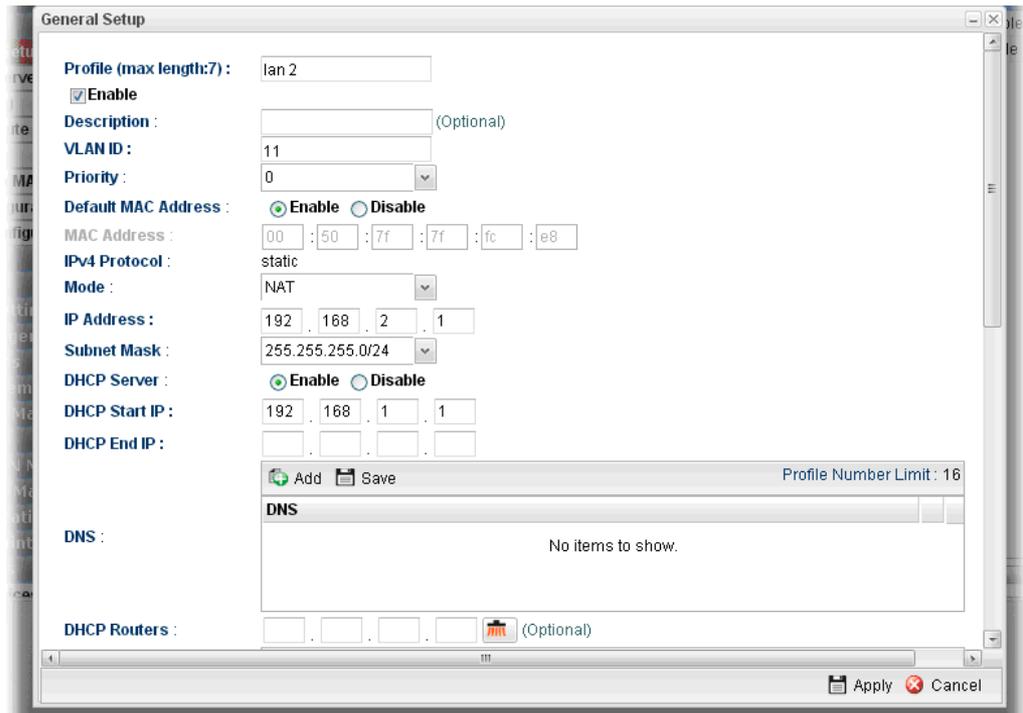


3. Click **Add** to open the following page.



Type the information specified for LAN1 profile, then click **Apply** to save the settings and exit the screen.

4. Click **Add** again to create a profile for LAN2 (192.168.2.1/24).

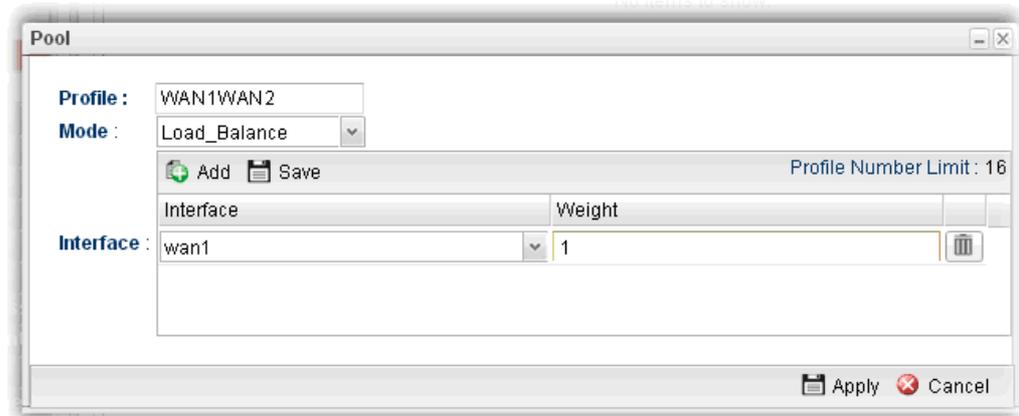


Type the information specified for LAN2 profile, then click **Apply** to save the settings and exit the screen.

5. Open **WAN >> Load Balance** and click the **Pool** tab.

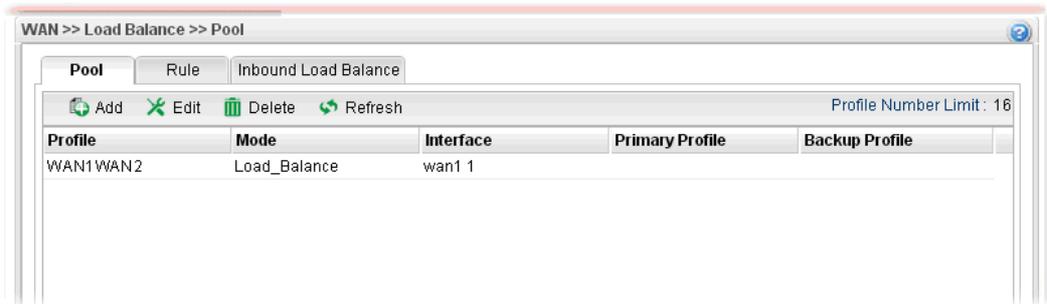


- Click **Add** under the **Pool** tab to create a profile (e.g., WAN1WAN2) for automatic Load Balance between WAN1 and WAN2. Choose **Load_Balance** as the **Mode** option.

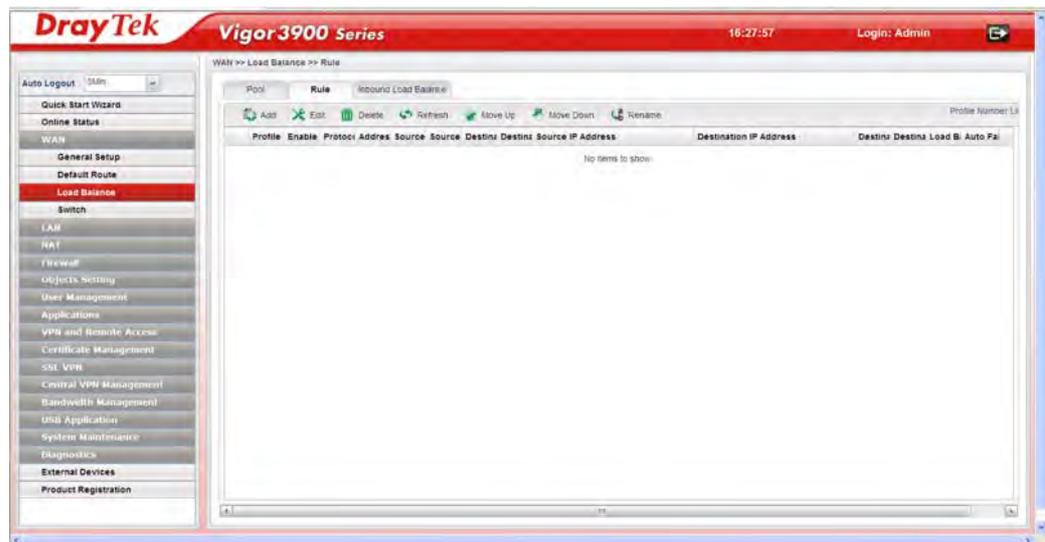


Click Add to configure the interface. Setup the Weights (e.g, “1”) of WAN1 and WAN2 respectively as you want. In this case ratio of WAN1 and WAN2 is 1:1. Also, you can type 2 and 1 for WAN1 and WAN2, then the ratio of line speed of WAN 1 and line speed of WAN 2 will be 2:1.

- After clicking **Apply**, the created profile will be shown on the screen.



- Open **WAN >> Load-Balance** and click the **Rule** tab.



- Click **Add** to create a profile for Rule1 accepting the data coming from 192.168.1.0/24 which always goes Internet via WAN1 when WAN1 is up. Type the information specified for such rule. (e.g., **Rule1** for Profile; **192.168.1.0** for **Source IP Address**;

wan1 for Load Balance Pool/WAN Profile and so on). Next, click **Apply** to save and exit.

The screenshot shows a 'Rule' configuration window with the following settings:

- Profile: Rule1
- Enable:
- Protocol: ALL
- Address Type: Subnet
- Source IP Address: 192.168.1.0 (Optional)
- Source Mask: 255.255.255.0/24 (Optional)
- Destination IP Address: (Optional)
- Destination Mask: 255.255.255.0/24 (Optional)
- Load Balance Pool/WAN Profile: wan1 (Must have value)
- Failover to the Default Route: Enable Disable
- Failback: Enable Disable

Buttons: Apply, Cancel

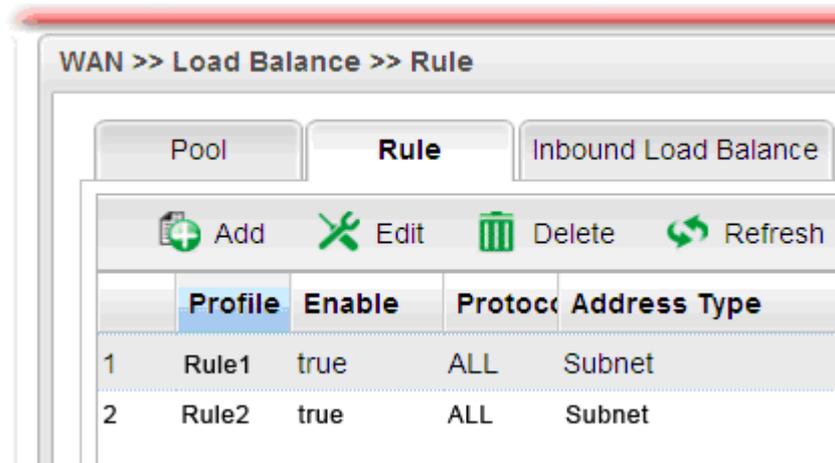
10. Click **Add** again to create a profile for Rule2 accepting 192.168.2.0/24 which always goes Internet via WAN2 when WAN2 is up.

The screenshot shows a 'Rule' configuration window with the following settings:

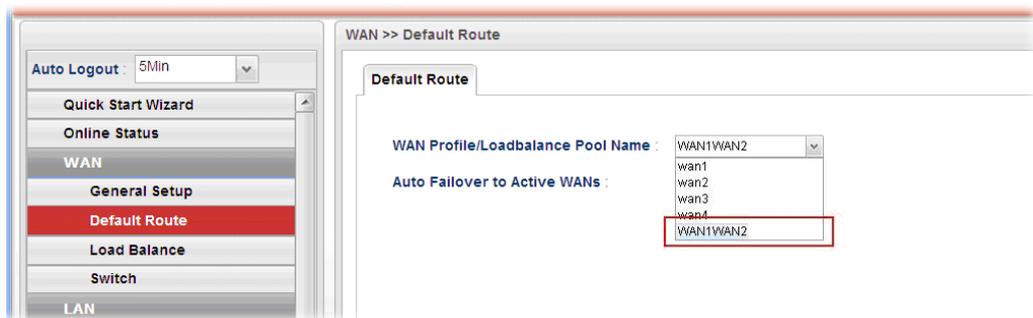
- Profile: Rule2
- Enable:
- Protocol: ALL
- Address Type: Subnet
- Source IP Address: 192.168.2.0 (Optional)
- Source Mask: 255.255.255.0/24 (Optional)
- Destination IP Address: (Optional)
- Destination Mask: 255.255.255.0/24 (Optional)
- Load Balance Pool/WAN Profile: wan2 (Must have value)
- Failover to the Default Route: Enable Disable
- Failback: Enable Disable

Buttons: Apply, Cancel

11. After clicking **Apply**, the created profiles will be shown on the screen.



- Next, open **WAN >> Default Route**. Choose the profile of “WAN1WAN2” as **WAN Profile/Loadbalance Pool Name**.



Note: The priority of **WAN >> Load Balance>>Rule** is higher than **WAN >> Default Route**.

Now, you have completed the configuration. Next time, when WAN1 is down, the connection for PCs behind Sale's LAN (192.168.1.1/24) will automatically failover to WAN2.

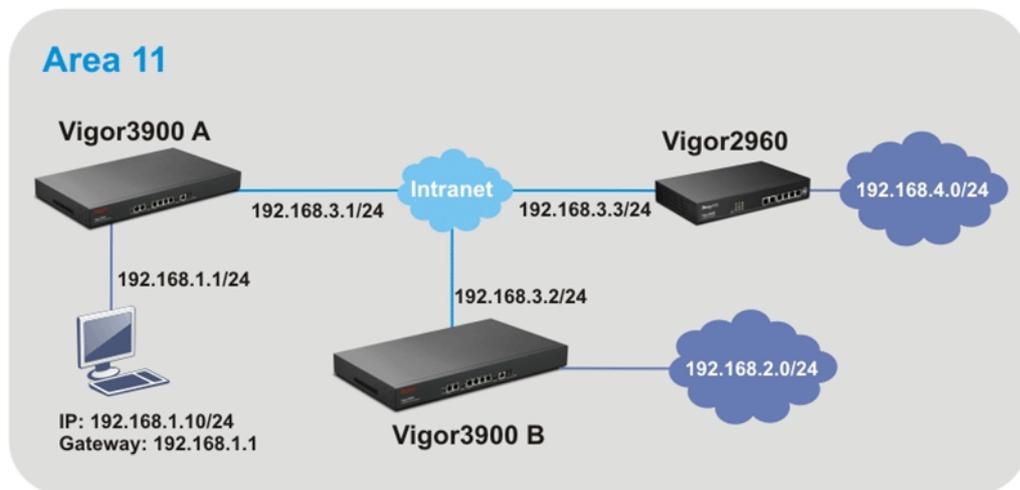
3.2 How to Configure OSPF?

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 **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.

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.

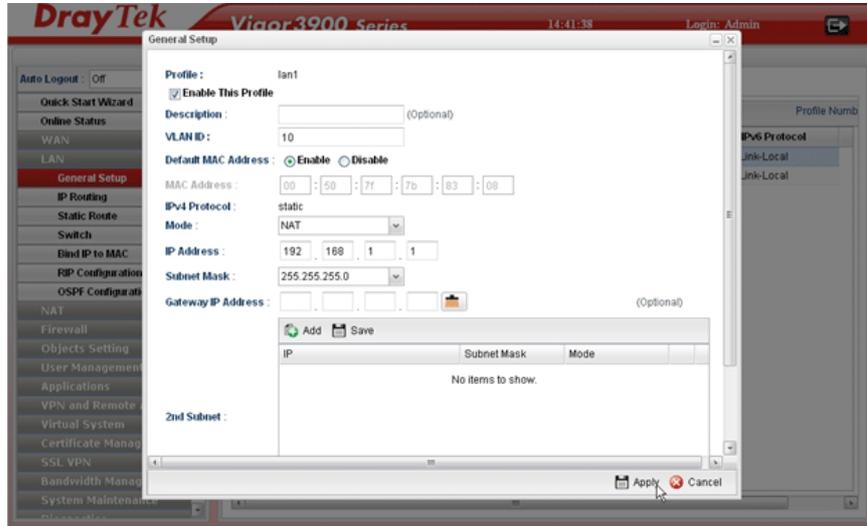


OSPF can place each router (e.g., Vigor3900A, Vigor3900B and Vigor2960 shown above) at the root of a tree and calculate the shortest path to each destination according to the cumulative cost to reach the destination.

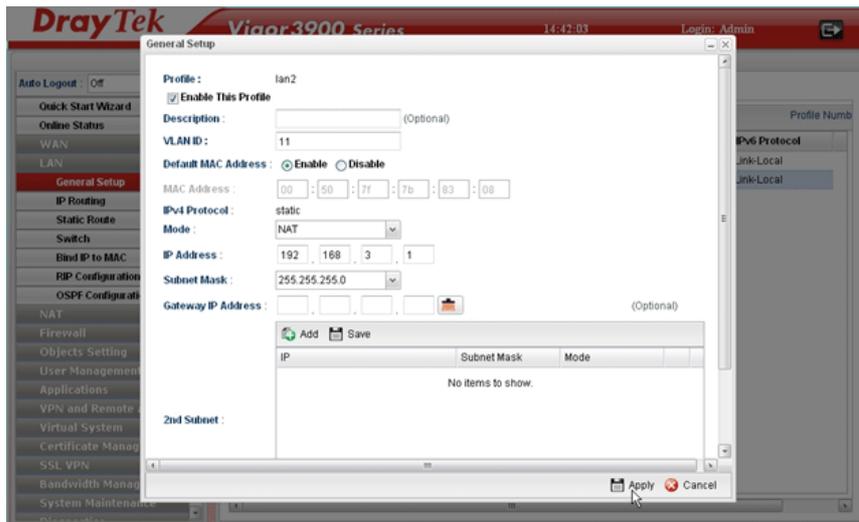
Each router has its own view of the topology and calculates its own SPF tree, even though all the routers build a shortest-path tree using the same link-state database.

Configuration for Vigor3900 A,

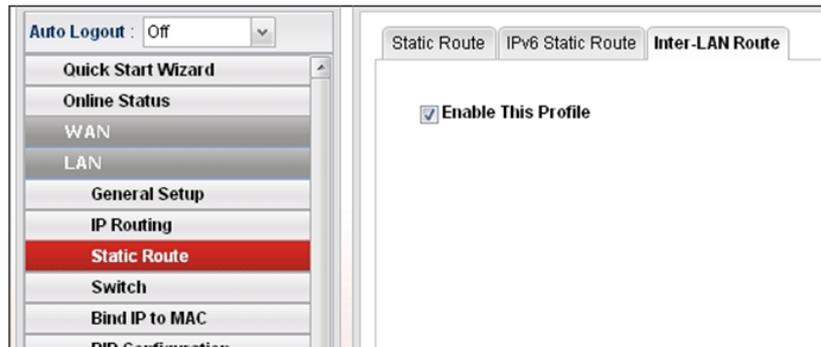
1. Open LAN >> **General Setup** to create a LAN (192.168.1.1/24) profile named lan1 with the settings shown below.



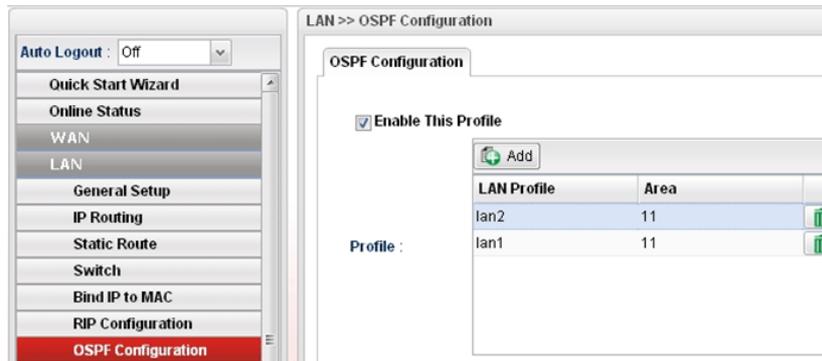
2. Next, continue to create a LAN (192.168.3.1/24) profile named lan2 with the settings shown below.



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

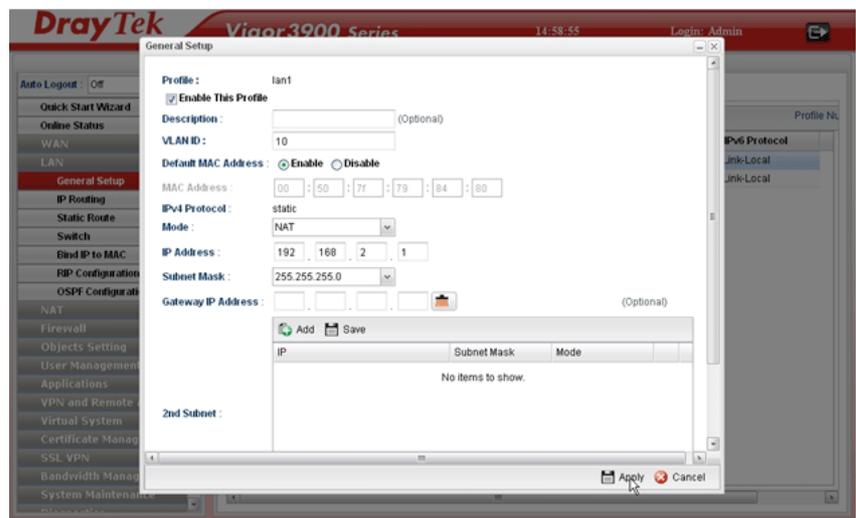


- Open LAN >> **OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

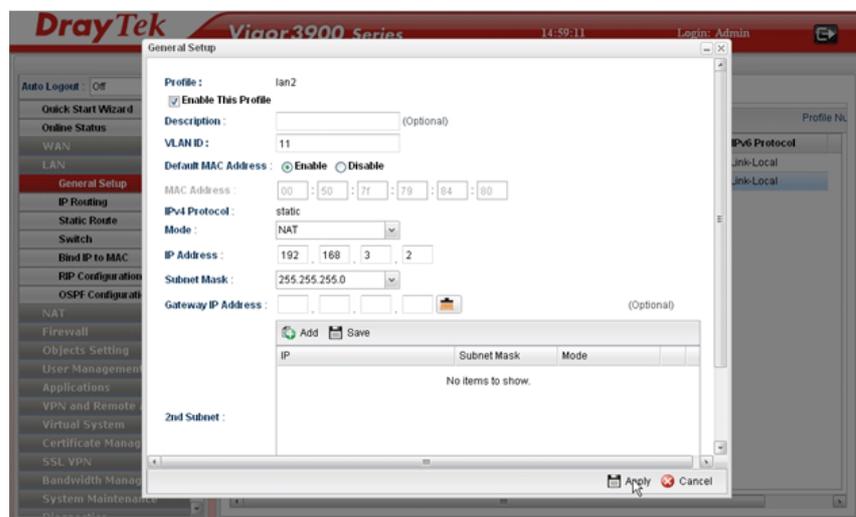


Configuration for Vigor3900 B,

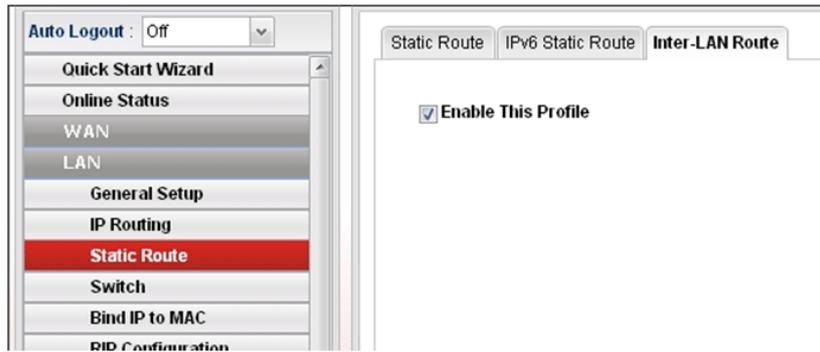
- Open LAN >> **General Setup** to create a LAN (192.168.2.1/24) profile named lan1 with the settings shown below.



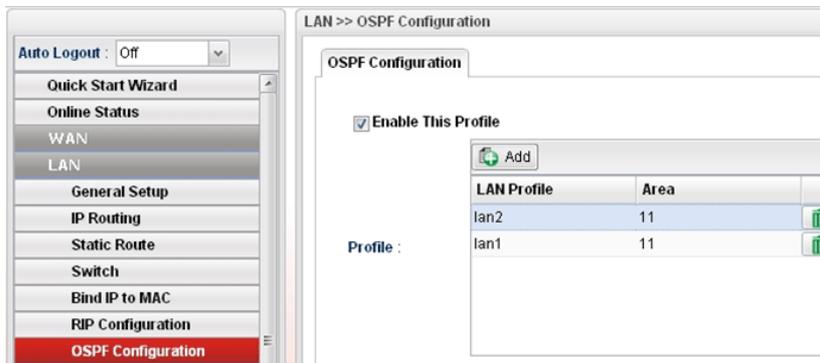
- Next, continue to create a LAN (192.168.3.2/24) profile named lan2 with the settings shown below.



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

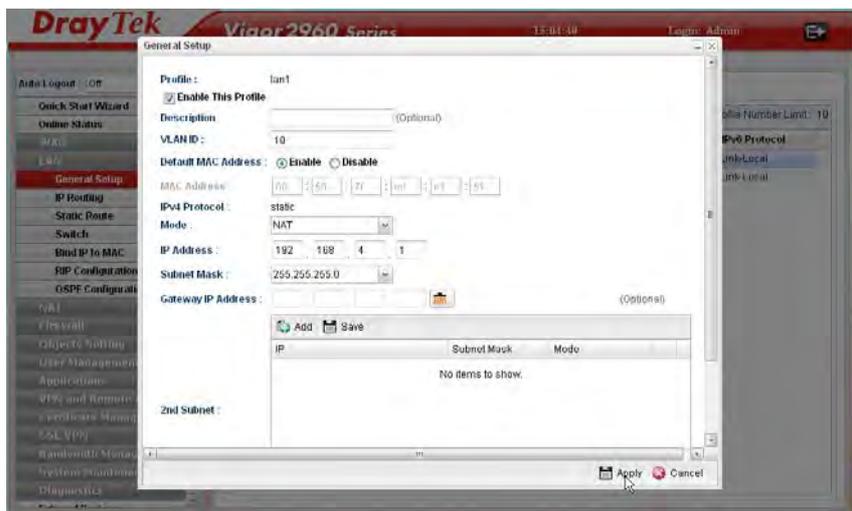


- Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

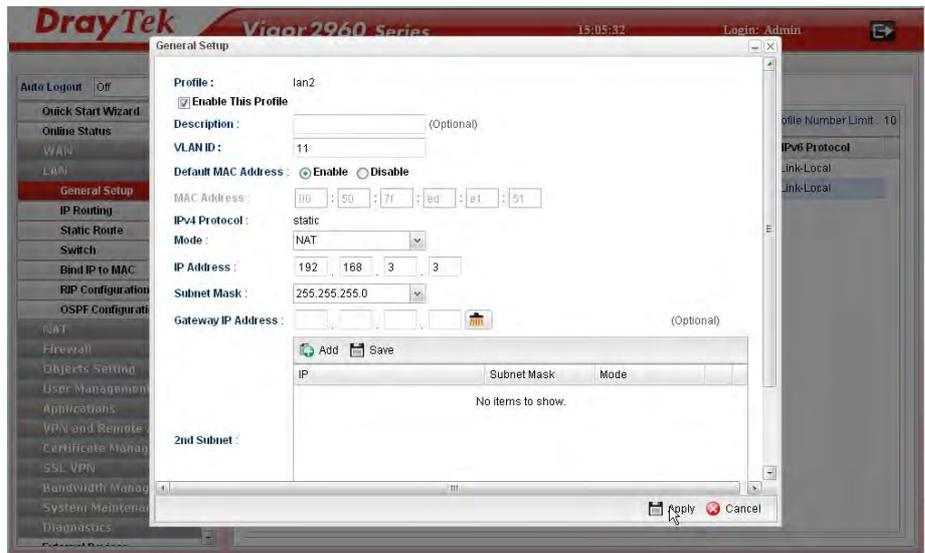


Configuration for Vigor2960,

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



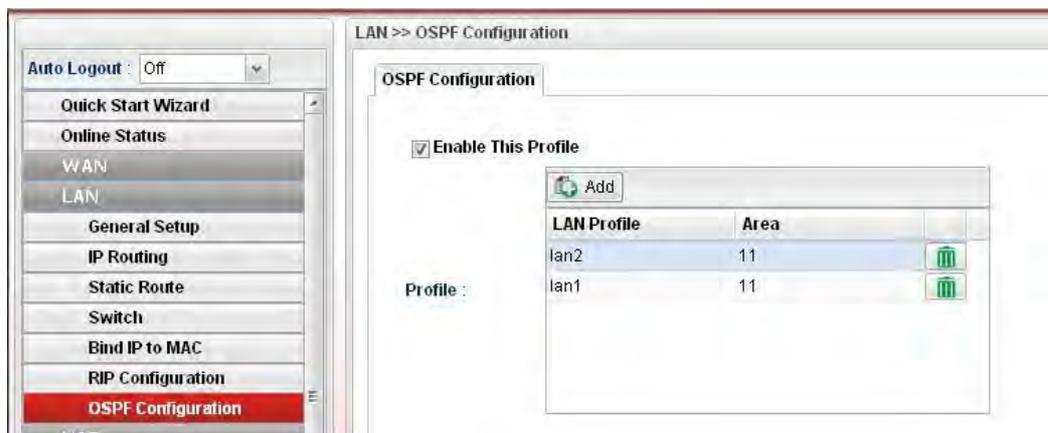
- Next, continue to create a LAN (192.168.3.3/24) profile named lan2 with the settings shown below.



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



- 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.)



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

Routing information for Vigor3900 A

Diagnostics >> Routing Table >> Routing Table

Routing Table IPv6 Routing Table

Refresh

Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1

Routing information for Vigor3900 B

Diagnostics >> Routing Table >> Routing Table

Routing Table IPv6 Routing Table

Refresh

Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
192.168.1.0	192.168.3.1	255.255.255.0	UG	20	lan-lan2

Routing information for Vigor2960

Diagnostics >> Routing Table >> Routing Table

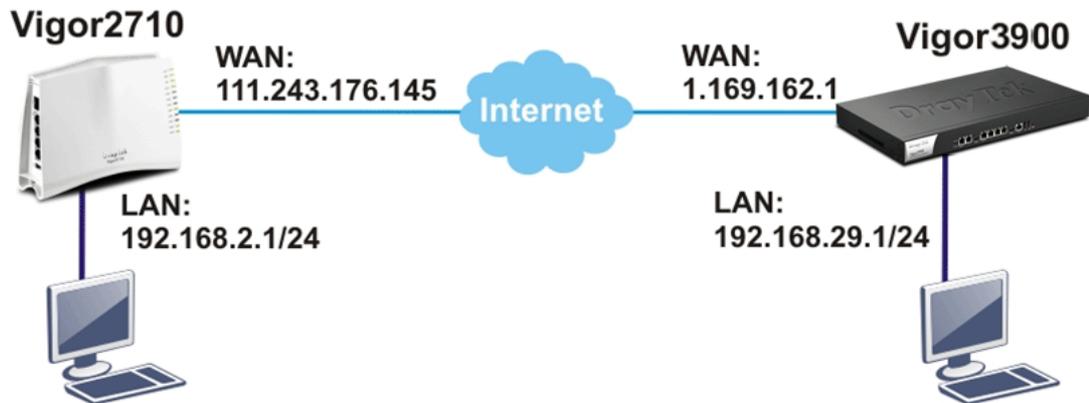
Routing Table IPv6 Routing Table

Refresh

Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	192.168.3.1	255.255.255.0	UG	20	lan-lan2

3.3 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.

The screenshot shows the 'IPSec' configuration window in the Vigor3900 Web User Interface. The window title is 'IPSec'. The 'Profile' is set to '2710'. The 'Enable This Profile' checkbox is checked. The 'Type' is set to 'IPSec'. There are buttons for 'Set PPTP Dial-In For User Profile' and 'PPTP Dial-Out'. The 'Basic' tab is selected, showing the following configuration:

Auth Type :	PSK
Preshared Key :	...
Security Protocol :	ESP
WAN Profile :	wan1
Local IP / Subnet Mask :	192 168 29 0 255.255.255.0
Local Next Hop :	0 0 0 0
Remote Host :	111 243 176 145
Remote IP / Subnet Mask :	192 168 2 0 255.255.255.0

At the bottom right, there are 'Apply' and 'Cancel' buttons.

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 be 192.168.2.0/24.

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**.

1. Common Settings

Profile Name <input type="text" value="3900"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input checked="" type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="-1"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	PING to the IP <input type="text"/>

- 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.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text" value="1.169.162.1"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="....."/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) <input type="text" value="3DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup : <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

- 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. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.29.0	Route	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network IP	192.168.2.0		
Local Network Mask	255.255.255.0		
More			

- 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.

VPN and Remote Access >> Connection Management

Connection Management

Profiles: [] Connect [IPSec] [PPTP] Refresh

VPN	Type	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Dis
2710	IPSec/3DES_No Auth	111.243.176.145	192.168.2.0/24	00:01:06	1	0	[X]

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

VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds: 10 Refresh

(3900)1.169.162.1 Dial

VPN Connection Status

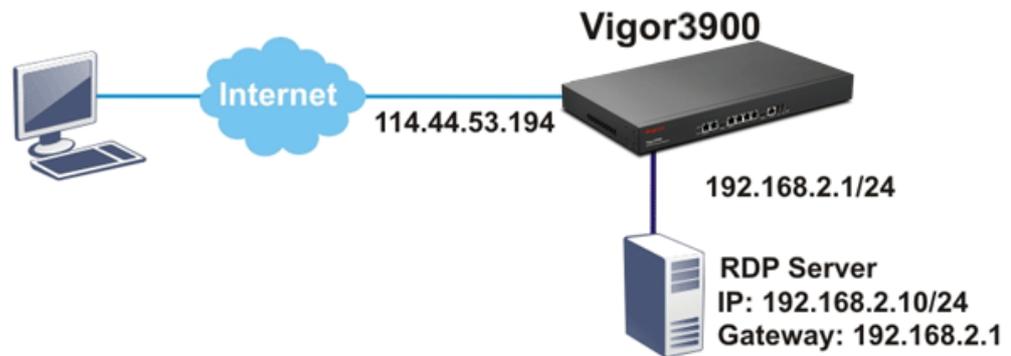
Current Page: 1 Page No. [] Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime
1 (3900)	IPsec Tunnel 3DES-No Auth	1.169.162.1 via WAN1	192.168.29.0/24	0	0	0	0	0:10:19 Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

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

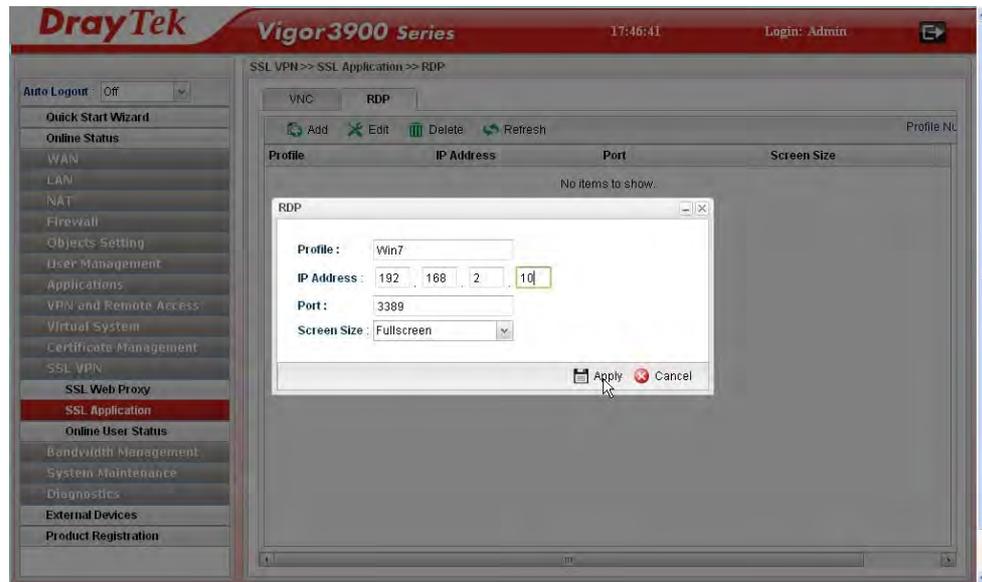
Remote Desktop Protocol (RDP) is a protocol designed for secure communications in networks using Microsoft Terminal Services. An easy way is provided to establish connection between the router and the RDP Server via any browser.



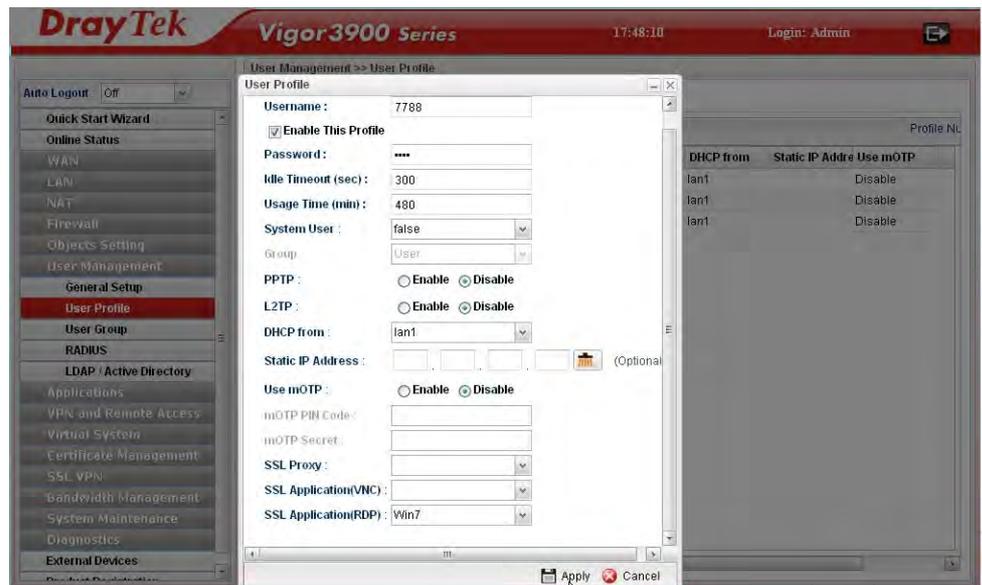
1. Open the Web User Interface of Vigor3900.
2. Enable the HTTPS service from **System Maintenance >> Access Control** by clicking **Enable** for **HTTPS Allow** and type **443** as the value of **HTTPS Port**.



- 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.



- 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**.



- Logout Vigor3900.

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



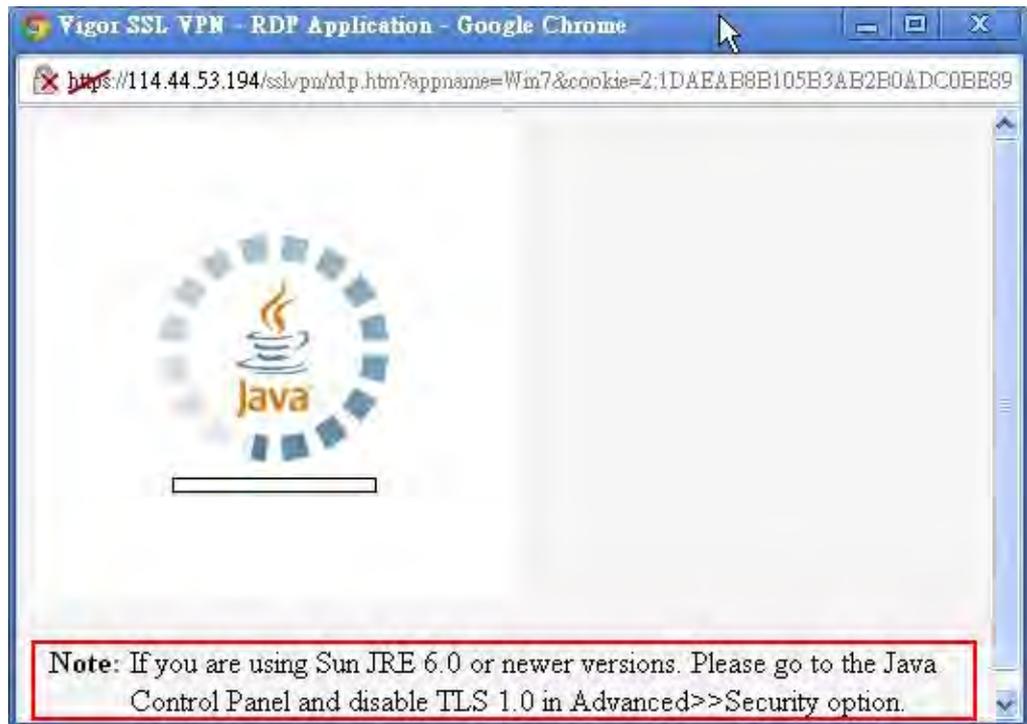
7. A screen like the following figure will appear. Simply click the **SSL Application** link.



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

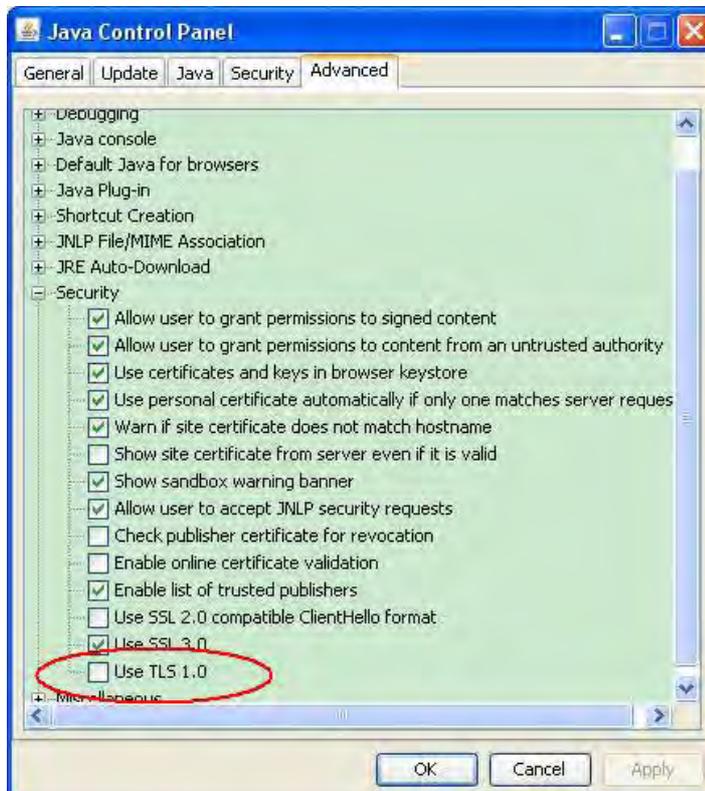


9. After that, you can access into Windows 7 via a browser. Note the message below the window. In which, TLS means Transport Layer Security.



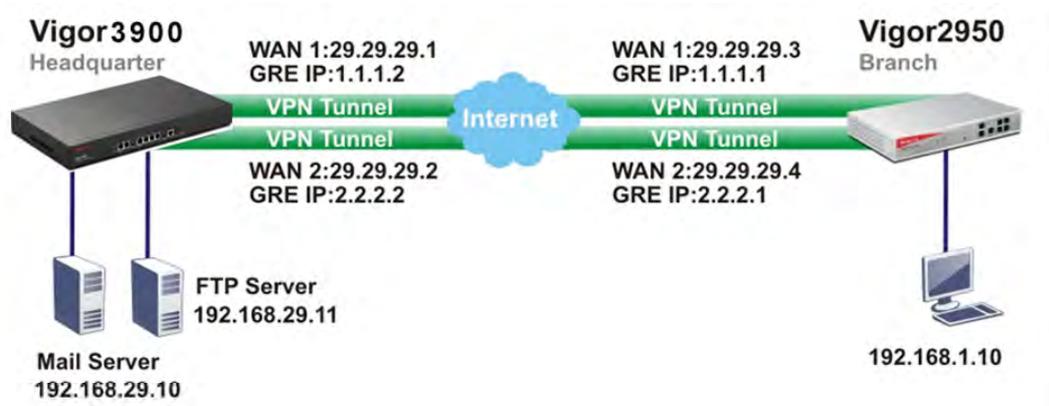
Troubleshooting

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.



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

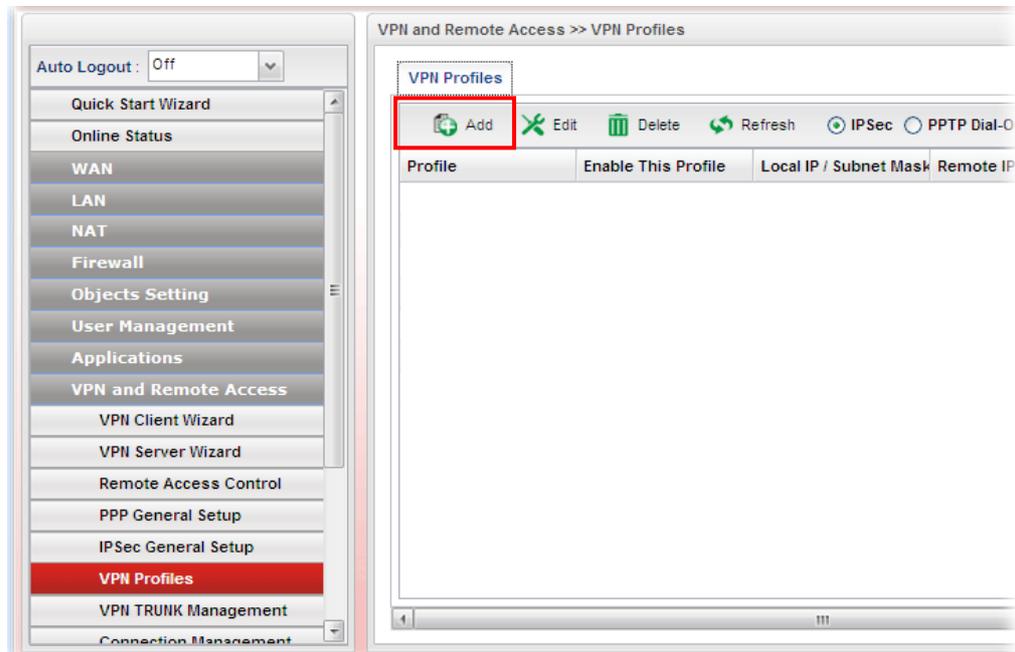
The staff in branch office can access into mail server/FTP server installed in the headquarters via VPN Load Balance tunnels. Refer to the following figure.



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**.

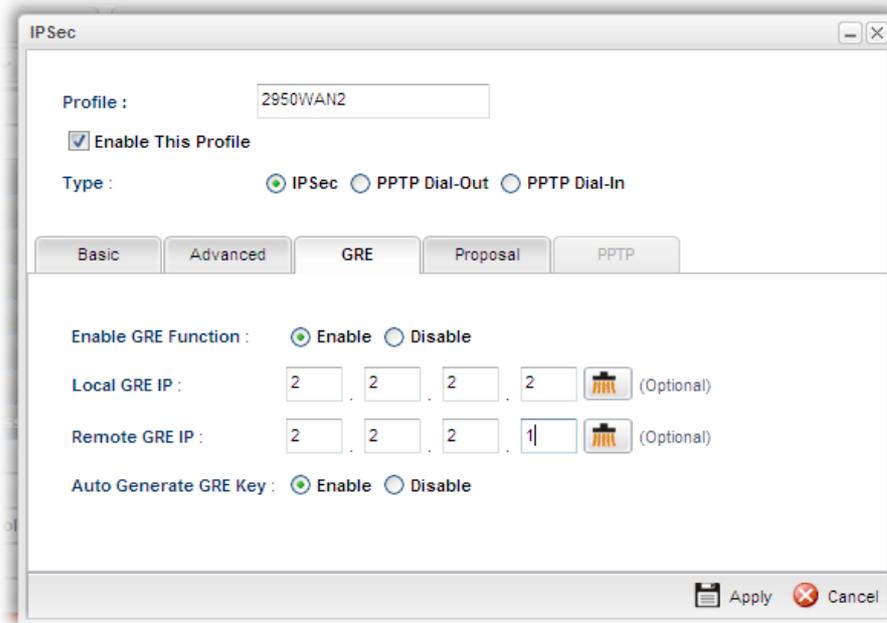
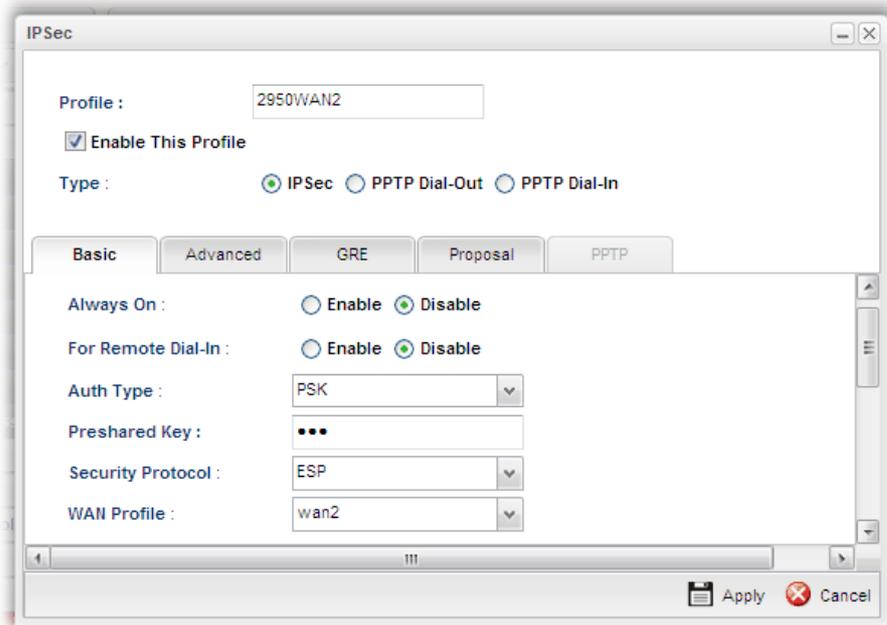


2. Create a profile for WAN 1 (named 2950WAN1). Type the settings as shown below:

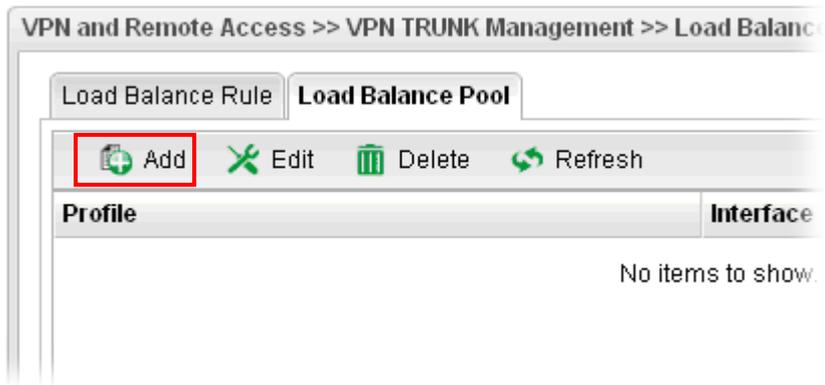
The screenshot shows the 'IPSec' configuration window with the 'Basic' tab selected. The 'Profile' field is set to '2950WAN1'. The 'Enable This Profile' checkbox is checked. The 'Type' is set to 'IPSec'. The 'Always On' and 'For Remote Dial-In' options are both set to 'Disable'. The 'Auth Type' is 'PSK', the 'Preshared Key' is masked with three dots, the 'Security Protocol' is 'ESP', and the 'WAN Profile' is 'wan1'. The 'Apply' and 'Cancel' buttons are at the bottom right.

The screenshot shows the 'IPSec' configuration window with the 'GRE' tab selected. The 'Profile' field is '2950WAN1', 'Enable This Profile' is checked, and 'Type' is 'IPSec'. The 'Enable GRE Function' option is set to 'Enable'. The 'Local GRE IP' is set to '1.1.1.2' and the 'Remote GRE IP' is set to '1.1.1.1', both with '(Optional)' icons. The 'Auto Generate GRE Key' option is set to 'Enable'. The 'Apply' and 'Cancel' buttons are at the bottom right.

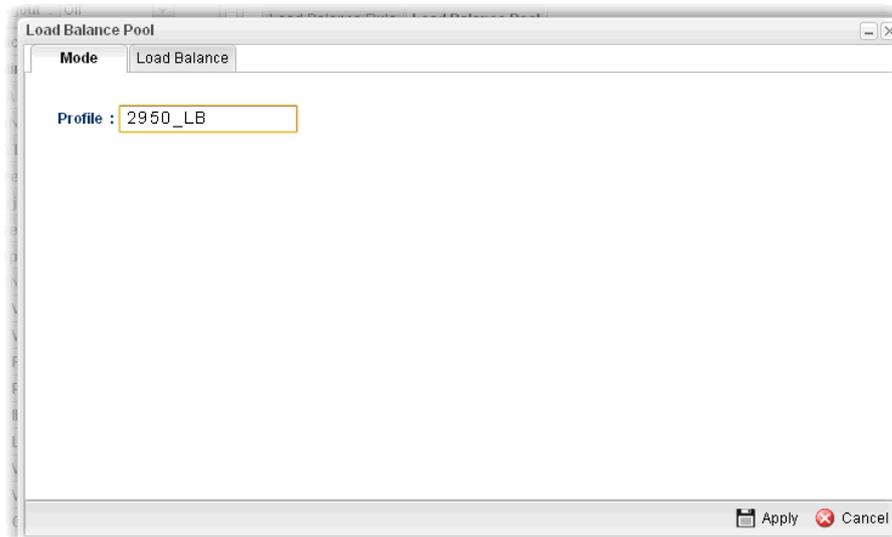
3. Click **Apply** to save the settings and exit the dialog.
4. Create a profile for WAN 2 (named 2950WAN2).



- Click **Apply** to save the settings and exit the dialog.
- Open **VPN and Remote Access >> VPN Trunk Management** and click the **Load Balance Pool** tab. Click **Add** to add a Load Balance Pool profile.



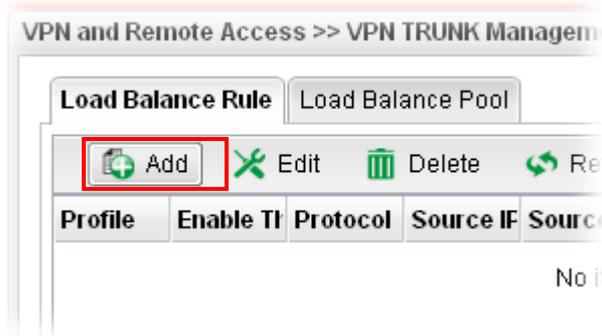
- The following window will pop up. Give a name for the profile.



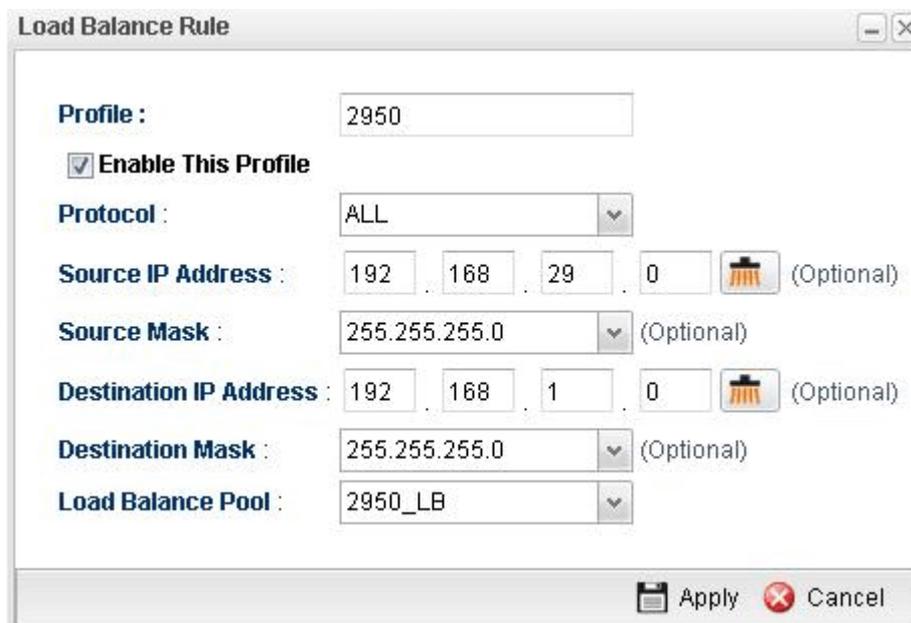
- Click the **Load Balance** tab. Select the IPSec GRE profiles (e.g., 2950WAN1) set for Vigor2950 then click **Apply**.



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



- 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.



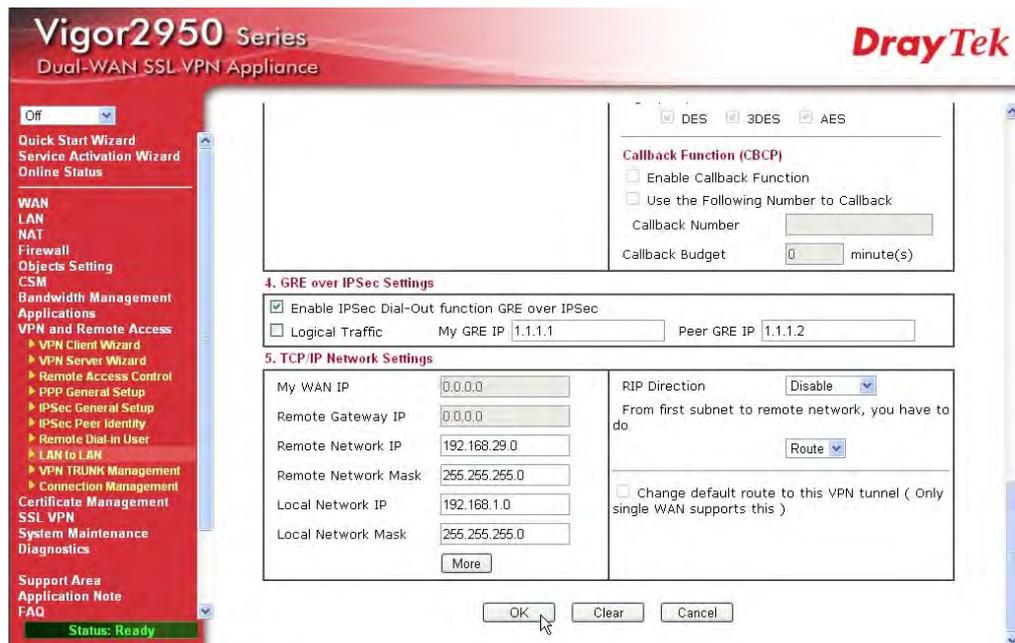
Configuring Vigor2950

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**.

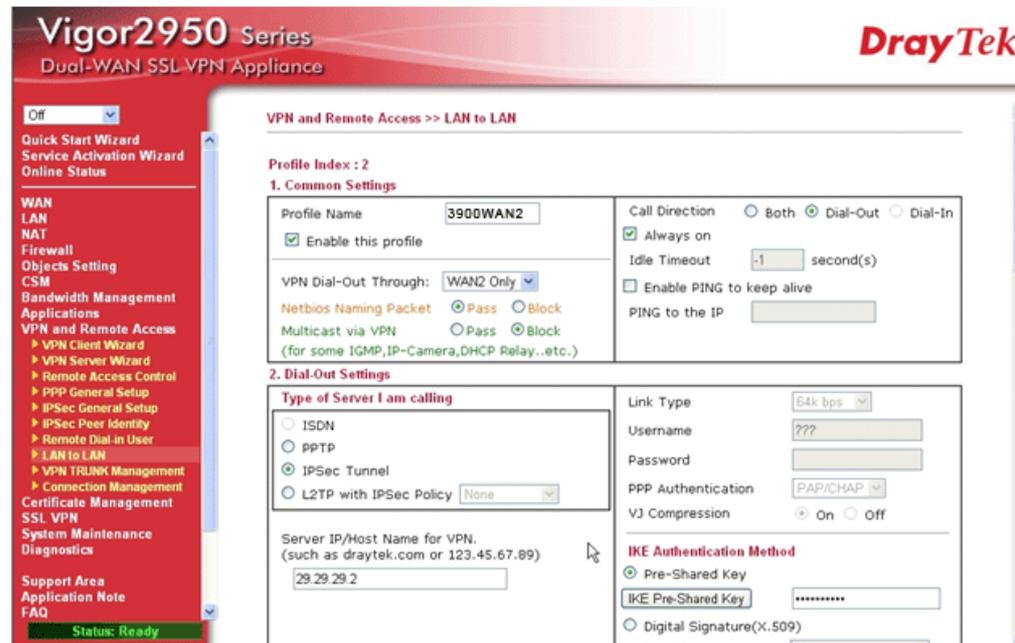
The screenshot displays the Web User Interface of a Vigor2950 Series Dual-WAN SSL VPN Appliance. The interface is titled 'Vigor2950 Series Dual-WAN SSL VPN Appliance' and features the DrayTek logo. A left-hand navigation menu includes options like 'Quick Start Wizard', 'Service Activation Wizard', 'Online Status', 'WAN', 'LAN', 'NAT', 'Firewall', 'Objects Setting', 'CSM', 'Bandwidth Management', 'Applications', 'VPN and Remote Access', 'VPN Client Wizard', 'VPN Server Wizard', 'Remote Access Control', 'PPP General Setup', 'IPSec General Setup', 'IPSec Peer Identity', 'Remote Dial-in User', 'LAN to LAN', 'VPN TRUNK Management', 'Connection Management', 'Certificate Management', 'SSL VPN', 'System Maintenance', and 'Diagnostics'. The 'Status' is shown as 'Ready'.

The main configuration area is titled 'VPN and Remote Access >> LAN to LAN'. It shows 'Profile Index : 1' and '1. Common Settings'. The 'Profile Name' is '2960WAN1'. The 'Call Direction' is set to 'Dial-Out'. The 'Always on' checkbox is checked. The 'Idle Timeout' is set to '-1' second(s). The 'VPN Dial-Out Through' is set to 'WAN1 Only'. The 'Netbios Naming Packet' is set to 'Pass'. The 'Multicast via VPN' is set to 'Block'. The '2. Dial-Out Settings' section shows 'Type of Server I am calling' as 'IPSec Tunnel'. The 'Link Type' is '64k bps'. The 'Username' is '???' and the 'Password' is empty. The 'PPP Authentication' is 'PAP/CHAP'. The 'VJ Compression' is 'On'. The 'IKE Authentication Method' is 'Pre-Shared Key', with the 'IKE Pre-Shared Key' field containing a masked value. The 'Server IP/Host Name for VPN' is '29.29.29.1'.

- 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**.

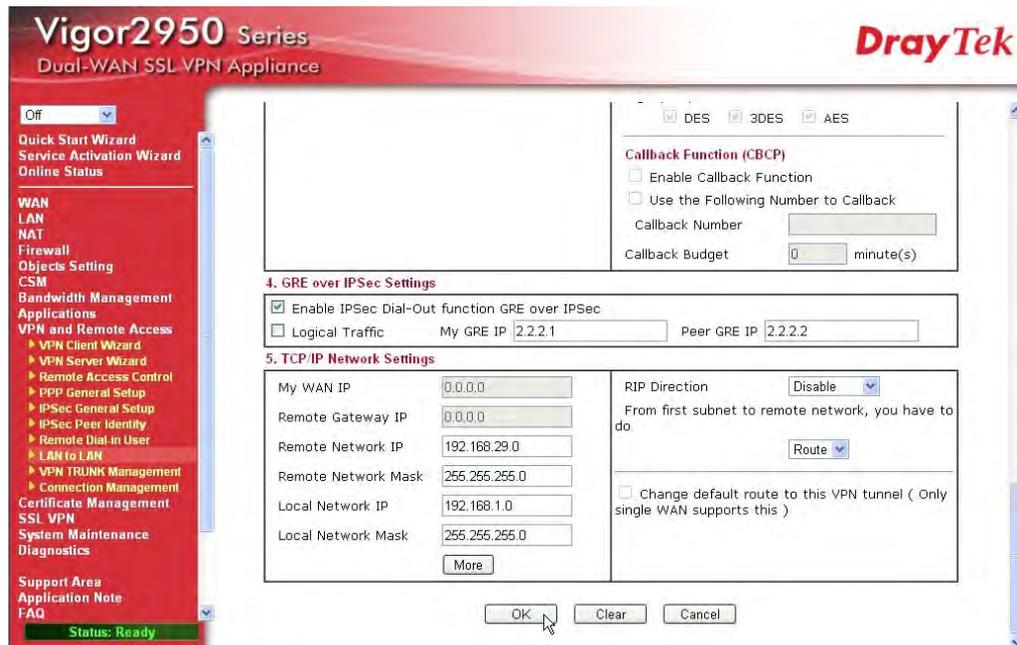


- Please type the network IP address and subnet of Vigor3900 in the field of Remote Network IP and Remote Network Mask. Type the network IP address and subnet of Vigor2950 in the field of Local Network IP and Local Network Mask.
2. Continue to set the second VPN connection (profile name is 3900WAN2). 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**.

General Setup

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	3900
Member1	1 3900WAN1 IPsec 29.29.29.1 (192.168.29.0)
Member2	2 3900WAN2 IPsec 29.29.29.2 (192.168.29.0)
Active Mode	<input type="radio"/> Backup <input checked="" type="radio"/> Load Balance

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.

VPN	Type	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect
2950WAN1	IPsec/DES_N	29.29.29.3	1.1.1.1/32	00:47:13	0	0	
2950WAN2	IPsec/DES_N	29.29.29.4	2.2.2.1/32	00:47:12	0	0	

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

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds :

General Mode: <input type="text" value=""/> <input type="button" value="Dial"/>
Backup Mode: <input type="text" value=""/> <input type="button" value="Dial"/>
Load Balance Mode: <input type="text" value="(3900) 29.29.29.1"/> <input type="button" value="Dial"/>

VPN Connection Status

Current Page: 1 Page No.

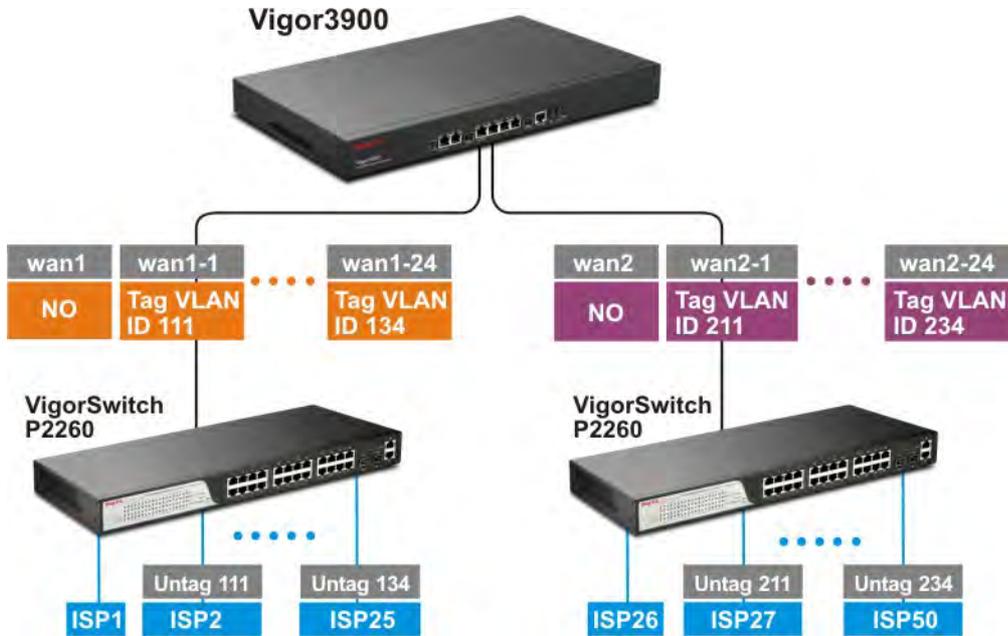
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (3900WAN1)	IPSec Tunnel DES-No Auth	29.29.29.1 via WAN1	192.168.29.0/24	0	0	0	0	0:0:0	<input type="button" value="Drop"/>
2 (3900WAN2)	IPSec Tunnel DES-No Auth	29.29.29.2 via WAN2	192.168.29.0/24	0	0	0	0	0:0:16	<input type="button" value="Drop"/>

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

3.6 How to Setup 50 WANs on Vigor3900

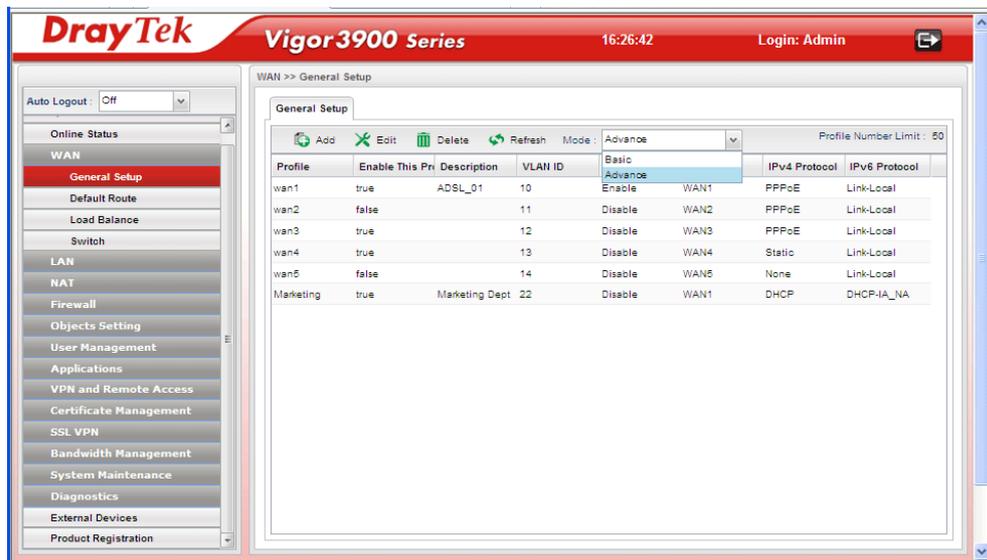
Vigor3900 has 5 physical WANs; however, it can be extended to 50 WANs at most by using VLAN Tagging technology.

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

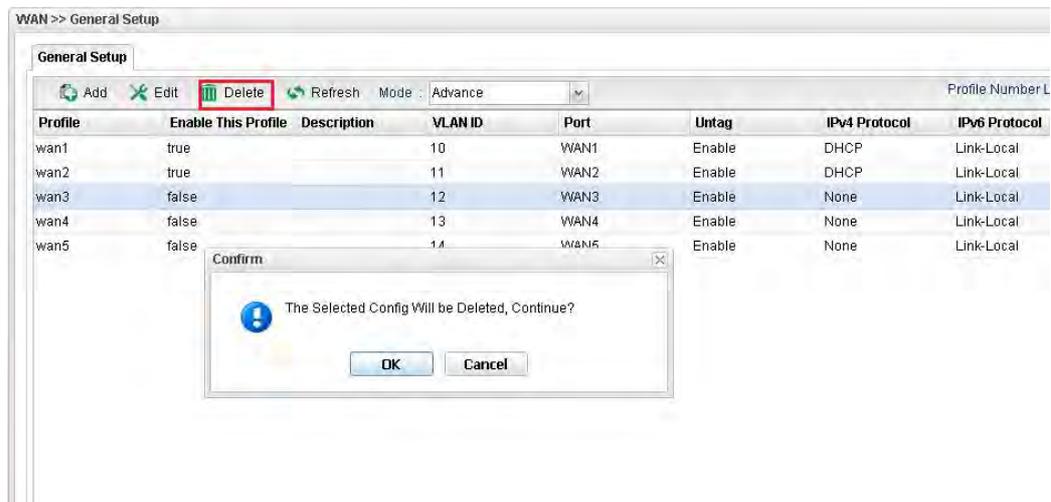
1. Change mode from **Basic** to **Advance** via **WAN>>General Setup** page.



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.

General Setup

Global PPTP Static DHCP PPPoE StaticV6 DHCPV6

Profile : wan1_1

Enable This Profile

Description : (Optional)

VLAN ID : 111

VLAN Tag : Disable

Port : WAN1

Default MAC Address : Enable Disable

MAC Address : 00 : 50 : 7f : e7 : cb : 21

Mode : NAT

IPv4 Protocol : None

IPv6 Protocol : Link-Local

Apply Cancel

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.

DrayTek

Auto Logout 3 min

VigorSwitch P2260

System

Port

PoE

Loop Detection

SNMP

DHCP Boot

IGMP Snooping

VLAN

VLAN Mode

Tag-based Group

PVID

Port-based Group

Management Vlan

MAC Table

GVRP

STP

Trunk

802.1X

Alarm

Configuration

Security

Bandwidth

QoS

Diagnostics

TFTP Server

Log

Firmware Upgrade

Reboot

Logout

Tag-based Group

No	VLAN NAME	VID
1	default	1

Add Edit Delete

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

Tag-based VLAN

VLAN name	111							
VID	111							
Member	1. <input checked="" type="checkbox"/>	2. <input type="checkbox"/>	3. <input type="checkbox"/>	4. <input type="checkbox"/>	5. <input type="checkbox"/>	6. <input type="checkbox"/>	7. <input type="checkbox"/>	8. <input type="checkbox"/>
	9. <input type="checkbox"/>	10. <input type="checkbox"/>	11. <input type="checkbox"/>	12. <input type="checkbox"/>	13. <input type="checkbox"/>	14. <input type="checkbox"/>	15. <input type="checkbox"/>	16. <input type="checkbox"/>
	17. <input type="checkbox"/>	18. <input type="checkbox"/>	19. <input type="checkbox"/>	20. <input type="checkbox"/>	21. <input type="checkbox"/>	22. <input type="checkbox"/>	23. <input type="checkbox"/>	24. <input type="checkbox"/>
	25. <input type="checkbox"/>	26. <input checked="" type="checkbox"/>						
Untag	1. <input checked="" type="checkbox"/>	2. <input type="checkbox"/>	3. <input type="checkbox"/>	4. <input type="checkbox"/>	5. <input type="checkbox"/>	6. <input type="checkbox"/>	7. <input type="checkbox"/>	8. <input type="checkbox"/>
	9. <input type="checkbox"/>	10. <input type="checkbox"/>	11. <input type="checkbox"/>	12. <input type="checkbox"/>	13. <input type="checkbox"/>	14. <input type="checkbox"/>	15. <input type="checkbox"/>	16. <input type="checkbox"/>
	17. <input type="checkbox"/>	18. <input type="checkbox"/>	19. <input type="checkbox"/>	20. <input type="checkbox"/>	21. <input type="checkbox"/>	22. <input type="checkbox"/>	23. <input type="checkbox"/>	24. <input type="checkbox"/>
	25. <input type="checkbox"/>	26. <input type="checkbox"/>						

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.
- 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**

- 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

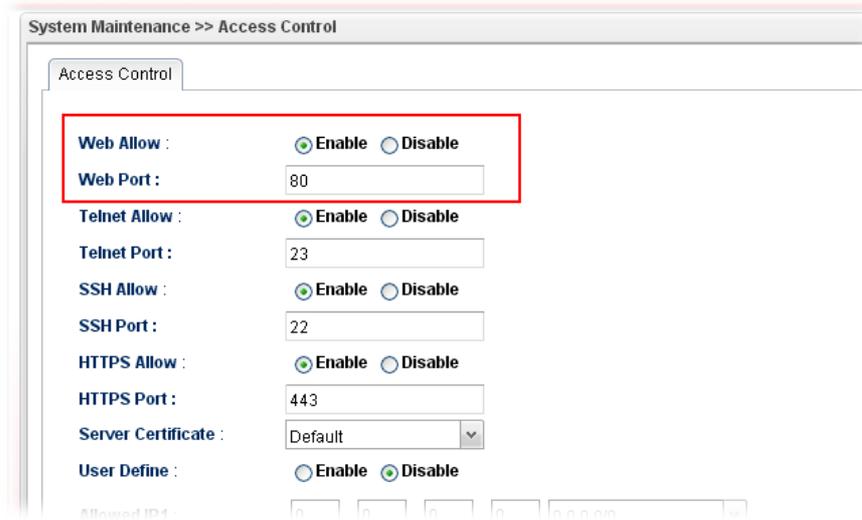
- PVID means VigorSwitch2260 will check and add VLAN tags while receiving packets from Ports.
 - ISP modem 1 which connects to Port 1 doesn't support VLAN Tag.
 - While the switch receives packets from Port 1, it will add VLAN Tag 111 to the packets Then Vigor3900 wan1_1 will receive the packets.
- After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

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

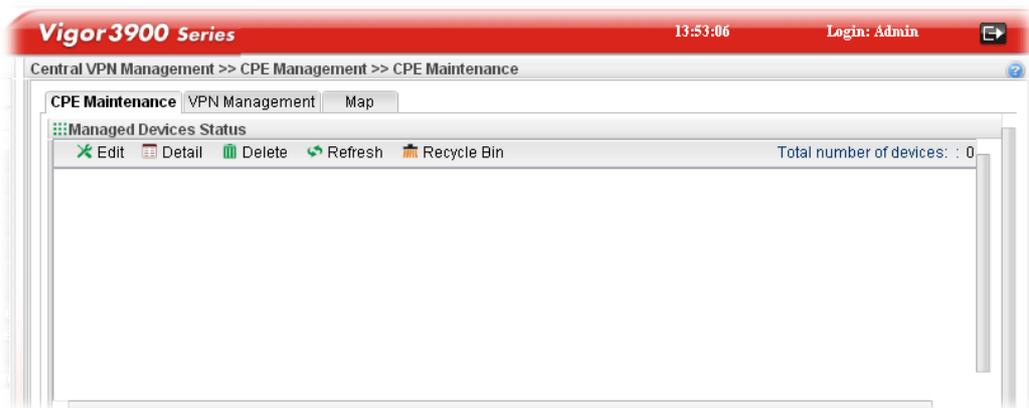
To manage CPEs through Vigor3900, you have to set URL on CPE first and set username and password for Vigor3900. For this section, we use Vigor2830 series as the example. The firmware upgrade for the CPE can be done through Vigor2830 series.

3.7.1 Configure Settings on Vigor3900

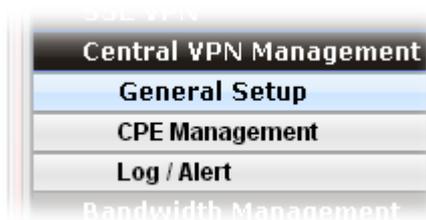
1. Access into the web user interface of Vigor3900.
2. Open **System Maintenance**>>**Access Control**. Check **Enable** for **Web Allow** and type the value for **Web Port**. Then click **Apply** to save the settings.



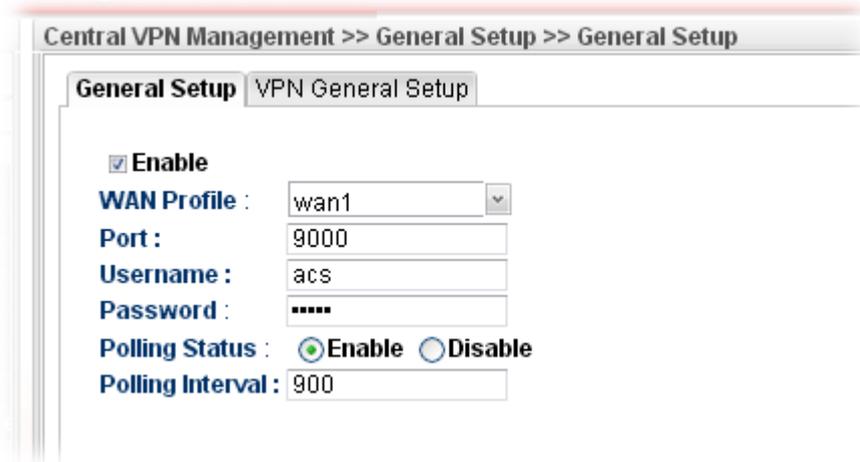
3. Open **Central VPN Management**>>**CPE Management**. On the page of **CPE Maintenance**, there is no CPE managed by Vigor3900.



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



- 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.



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

3.7.2 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.

- Connect one CPE (e.g., Vigor2830 series) and get ready to access into the web user interface of the CPE.
- Open a web browser (for example, **IE**, **Mozilla Firefox** or **Netscape**) on your computer and type **http://192.168.1.1**.
- 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.
- Open **System Maintenance >> TR-069**.



- 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.

ACS and CPE Settings

ACS Server On Internet

ACS Server

URL

Username

Password

CPE Client

Enable Disable

URL

Port

Username

Password

Periodic Inform Settings

Disable

Enable

Interval Time second(s)

3.7.3 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.

IPv4 Management Setup IPv6 Management Setup

Router Name

Management Access Control

Allow management from the Internet

FTP Server

HTTP Server

HTTPS Server

Telnet Server

SSH Server

Disable PING from the Internet

Access List

List	IP	Subnet Mask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

OK

3.7.4 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**.

WAN >> Internet Access

WAN 1

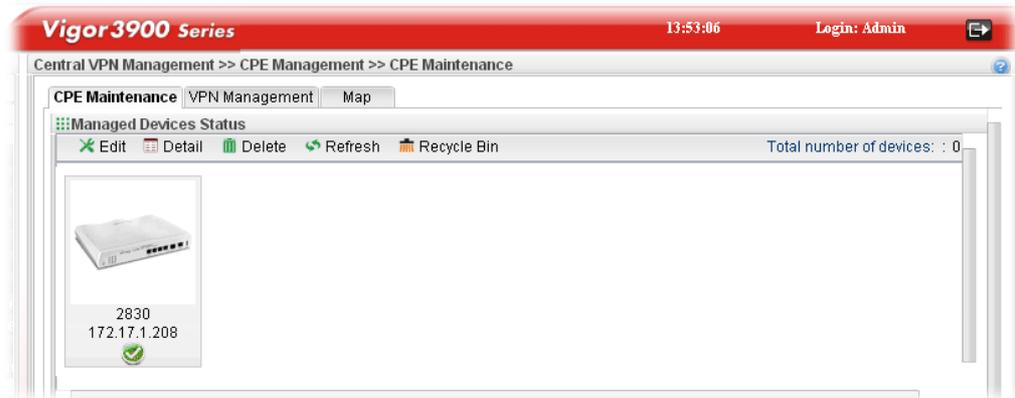
PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
DSL Modem Settings		
Multi-PVC channel	Channel 2	
Encapsulation	1483 Bridged IP LLC	
VPI	0	
VCI	88	
Modulation	Multimode	
WAN Connection Detection		
Mode	ARP Detect	
Ping IP		
TTL:		
RIP Protocol		
<input type="checkbox"/> Enable RIP		
Bridge Mode		
<input type="checkbox"/> Enable Bridge Mode		
WAN IP Network Settings WAN IP Alias		
<input type="radio"/> Obtain an IP address automatically		
Router Name	Vigor	
Domain Name		
* : Required for some ISPs		
<input checked="" type="radio"/> Specify an IP address		
IP Address	172.16.3.229	
Subnet Mask	255.255.0.0	
Gateway IP Address	172.16.3.4	
<input checked="" type="radio"/> Default MAC Address		
<input type="radio"/> Specify a MAC Address		
MAC Address:	00 . 50 . 7F : 00 . 00 . 01	
DNS Server IP Address		
Primary IP Address		
Secondary IP Address		

OK Cancel

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**.

3.7.5 Check CPE Maintenance Page

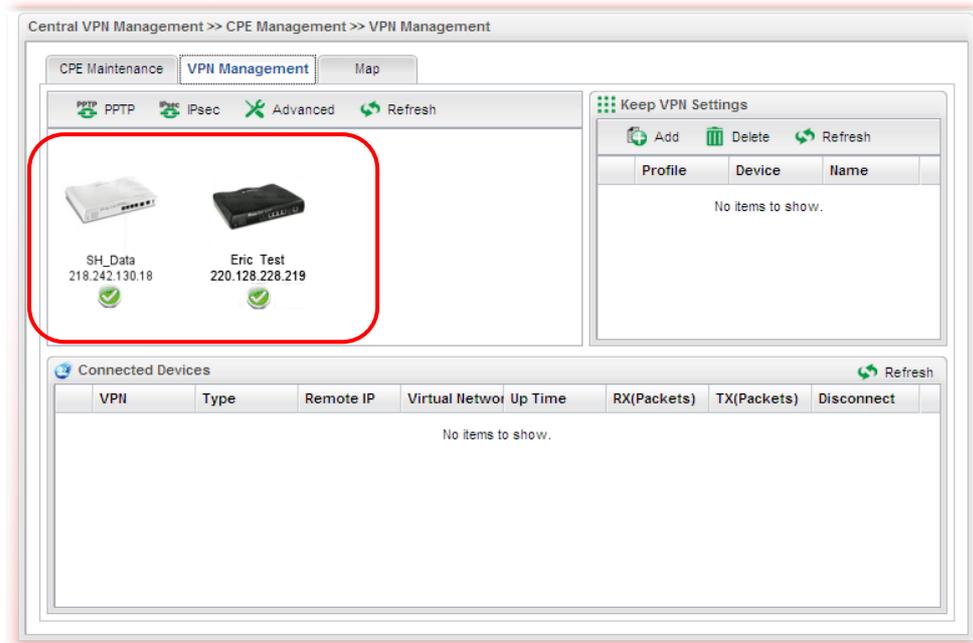
1. Return to the web user interface of Vigor3900.
2. Open **Central VPN Management>>CPE Management**.
3. Now there is one CPE managed (Vigor2830) by Vigor3900 on the page of **CPE Maintenance**.



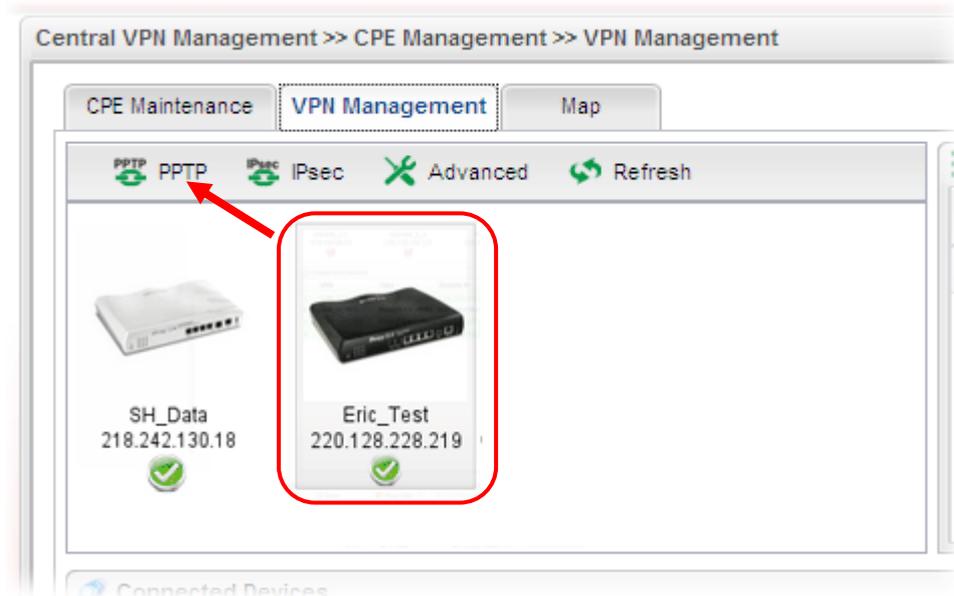
3.8 CVM Application - How to build the VPN between remote devices and Vigor3900?

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

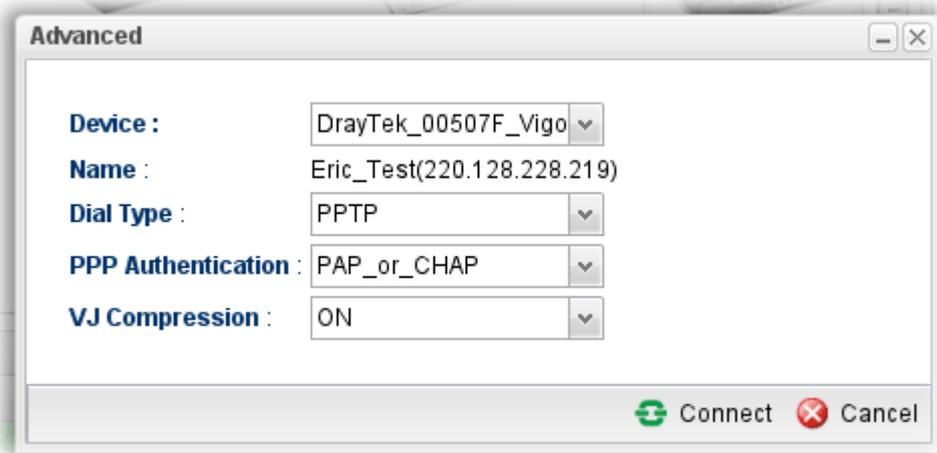
1. Access into the web user interface of Vigor3900 series.
2. Open **Central VPN Management>>CPE Management**. The icons displayed on the screen means the remote devices are ready for building VPN with Vigor3900.



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



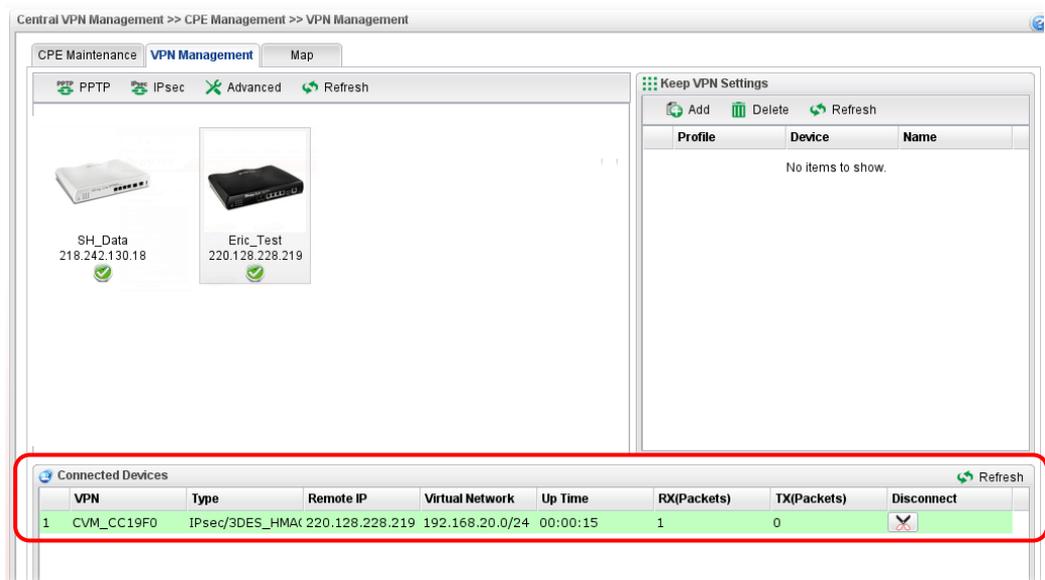
Or click **Advanced** to open the following page for specified the CPE you want. Click **Connect** after finished the settings.



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.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: All Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	CVM_CC19F0	<input checked="" type="checkbox"/>	online	17.	???	<input type="checkbox"/>	---



Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="cvm_CC19F0"/>	Call Direction <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="0"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	PING to the IP <input type="text"/>

3. Dial-In Settings

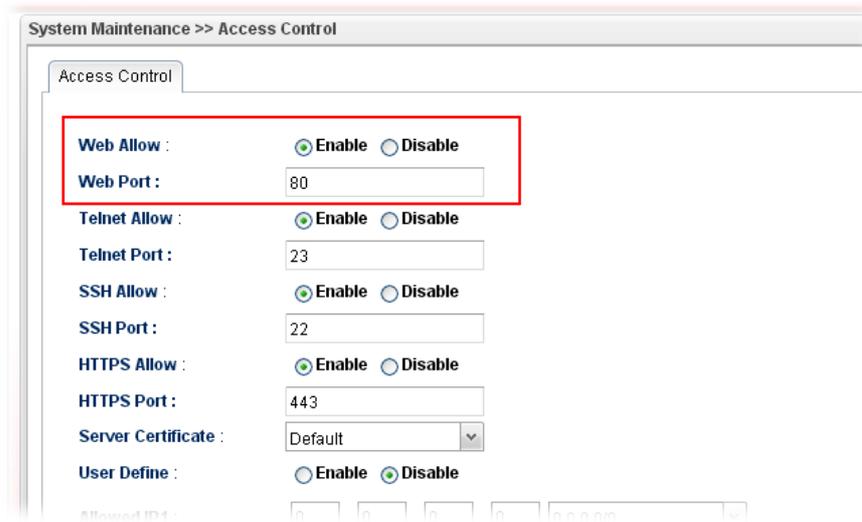
Allowed Dial-In Type	Username <input type="text" value="7D9D00"/>
<input checked="" type="checkbox"/> PPTP	Password(Max 11 char) <input type="text" value="●●●●●●●"/>
<input type="checkbox"/> IPsec Tunnel	VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/>	IKE Authentication Method

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

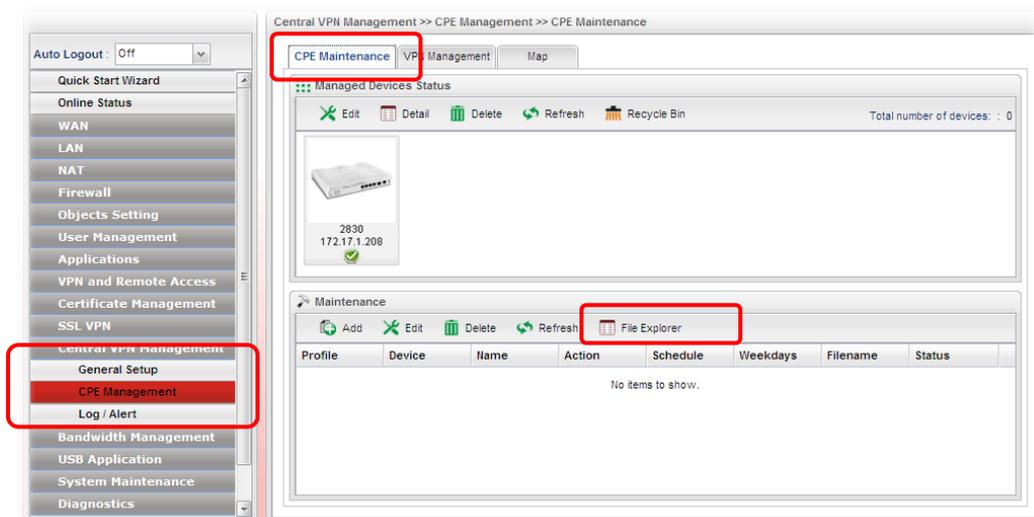
3.9 CVM Application - How to upgrade CPE firmware through Vigor3900?

3.9.1 Import firmware file from your PC to Vigor3900

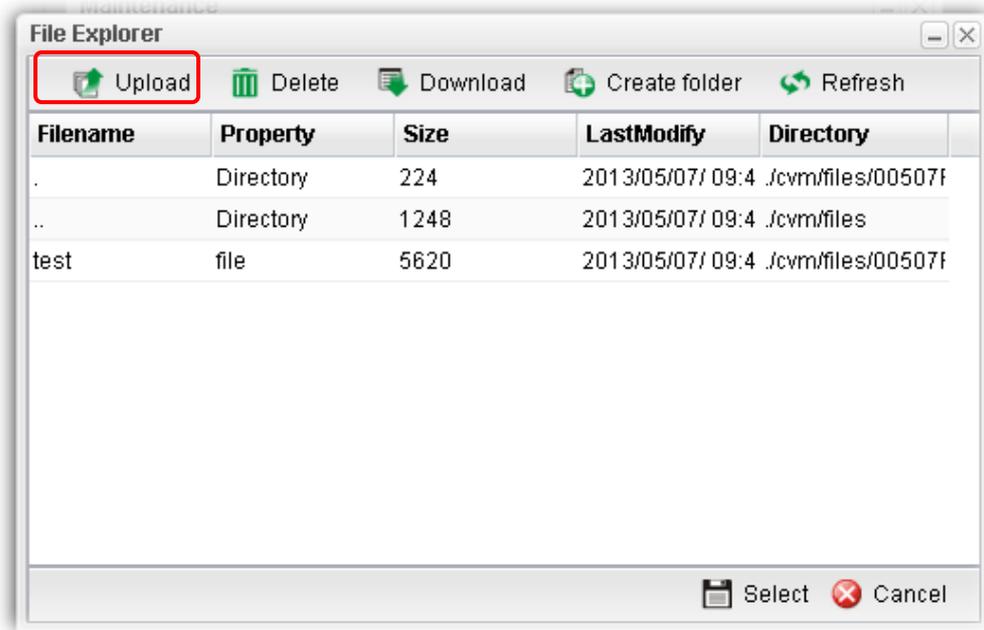
1. Suppose the newest firmware file is located on your PC. You can upload it from your PC to Vigor3900.
2. Log into the web user interface of Vigor3900.
3. Open **System Maintenance**>>**Access Control**. Check **Enable** for **Web Allow** and type the value for **Web Port**. Then click **Apply** to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



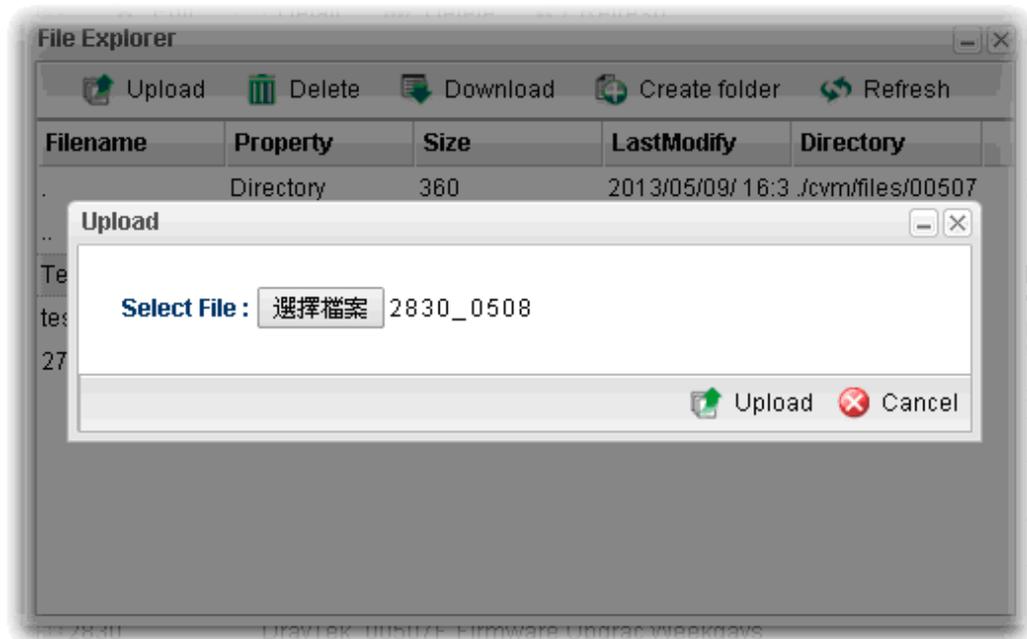
4. Open **Central VPN Management**>>**CPE Management**. Click **CPE Maintenance**. In the **Maintenance** area, click **File Explorer**.



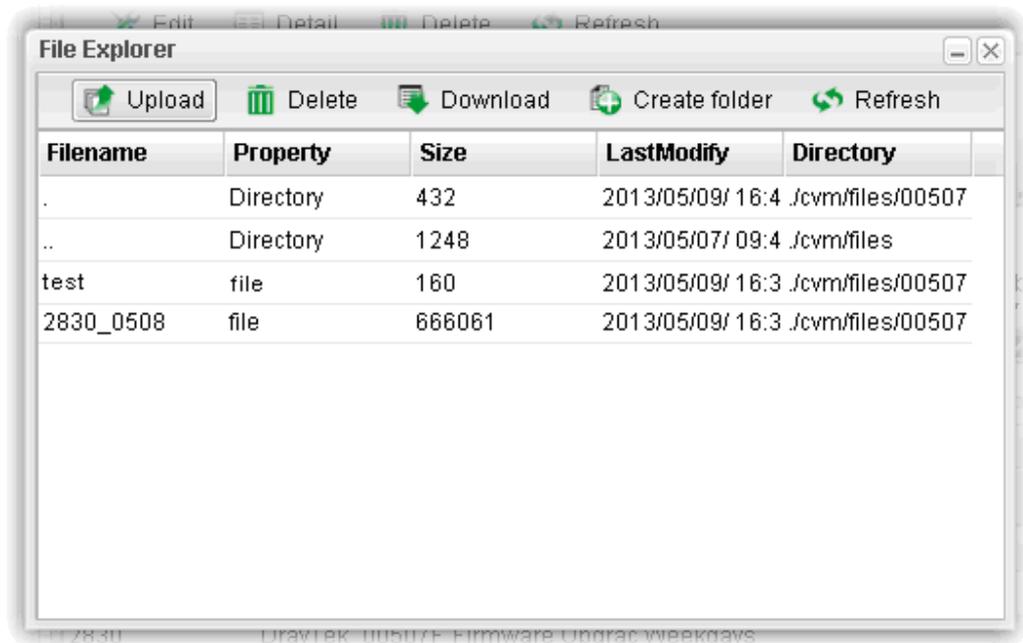
- In the File Explorer dialog, click **Upload**.



- 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**.



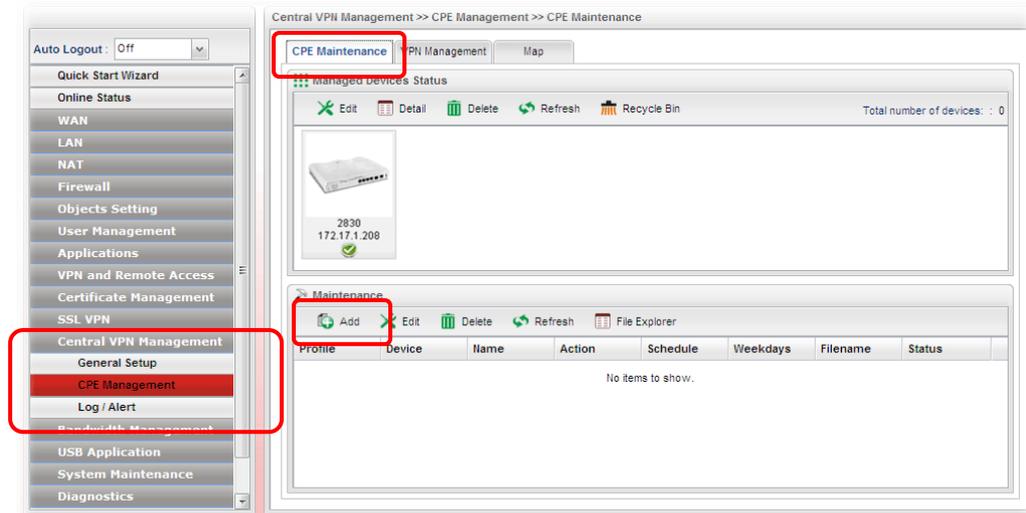
7. When the file is uploaded successfully, later you will find the one in the File Explorer dialog.



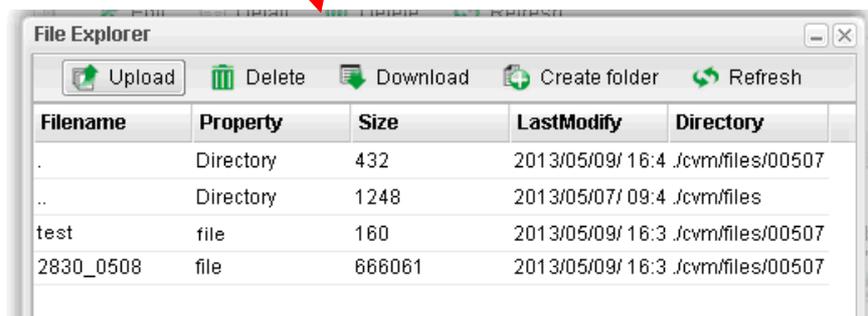
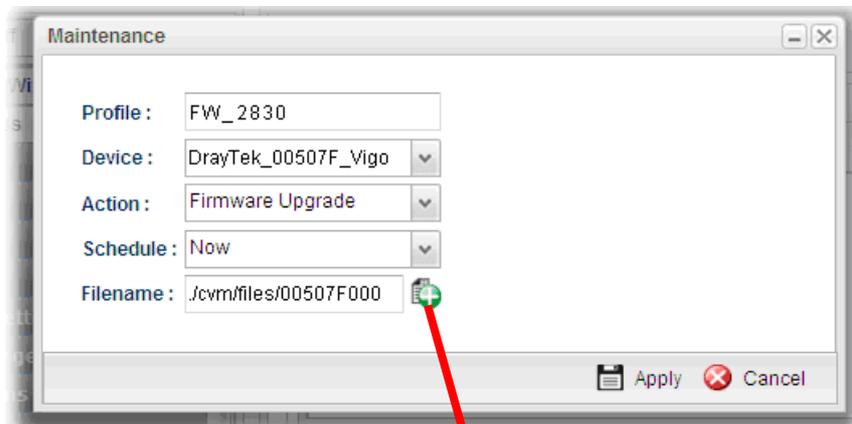
3.9.2 Set a new firmware upgrade profile

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.

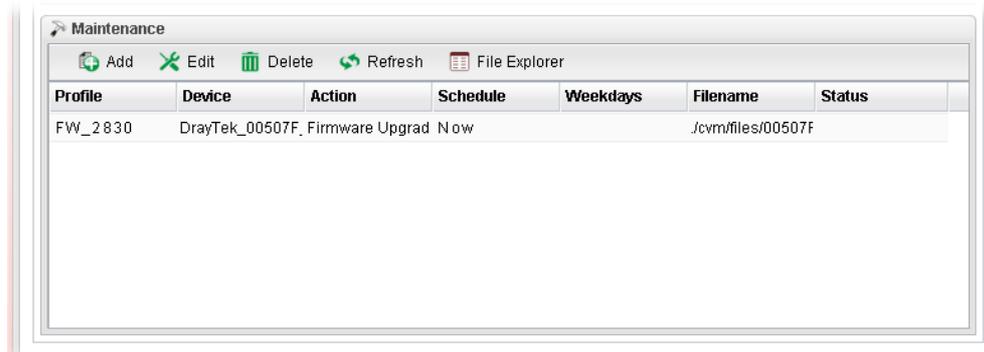
1. Open **Central VPN Management>>CPE Management**. Click **CPE Maintenance**. In the **Maintenance** area, click **Add**.



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.

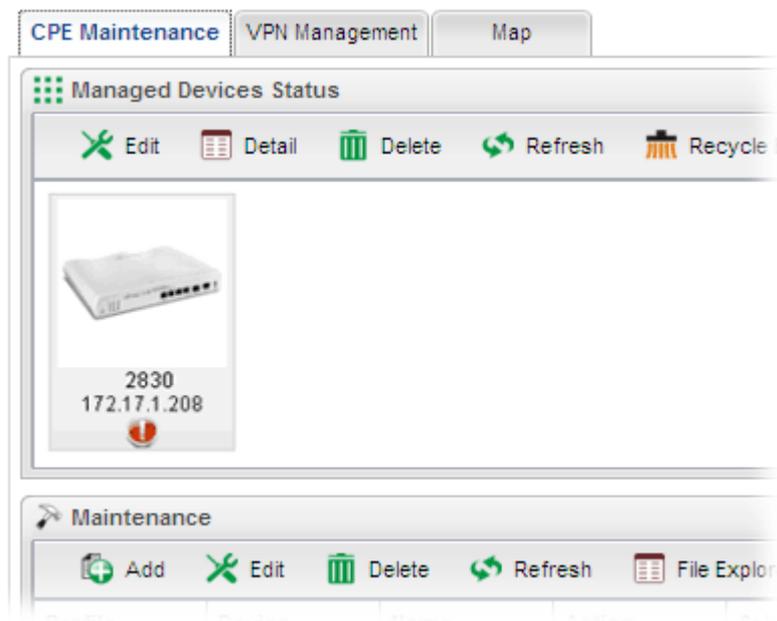


- When you finished the above settings, click **Apply** to save them. The new maintenance profile has been created and displayed on the Maintenance area.



- 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.

fw upgrade on going

Firmware upgrade on going, please wait for a moment.
Upgrade last for 19 seconds.

- 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.

ID	Time	Device Name	Type	Description
1	2013-05-17 14:58:20 UTC	DrayTek_00507F_Vigor_(Firmware Upgrade	[Processing][1] Request CPE to download firm
2	2013-05-17 14:58:21 UTC	DrayTek_00507F_Vigor_(Firmware Upgrade	[Processing][1] CPE start to download firmwar
3	2013-05-17 15:01:42 UTC	DrayTek_00507F_Vigor_(Firmware Upgrade	[Finished] Profile: V2830_Test, CPE firmware

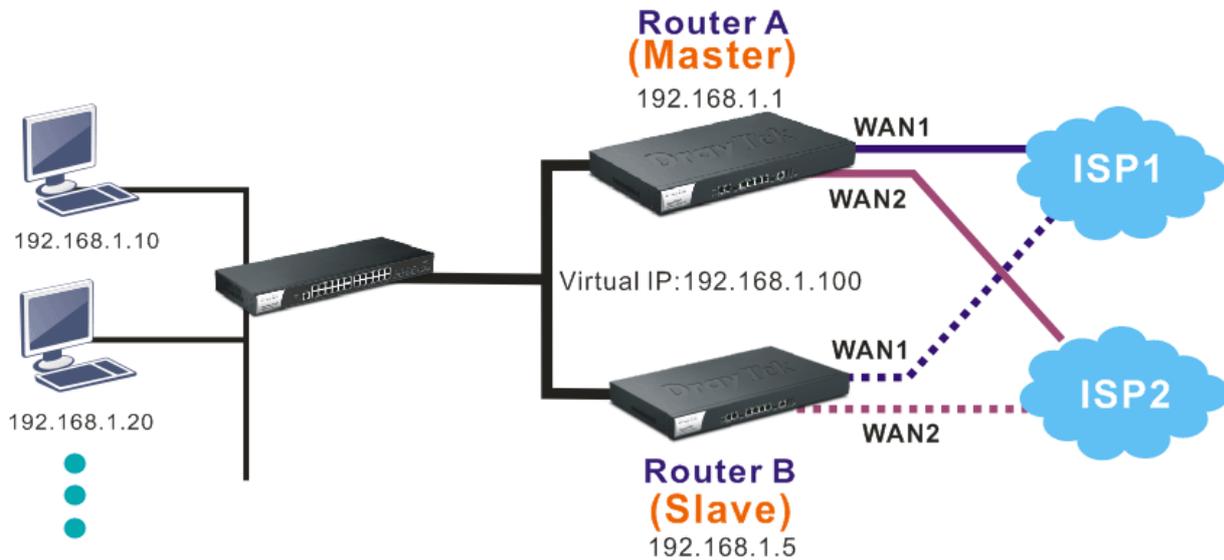
3.9.3 Check the Device Information

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

Model Name :	Vigor2830V
Device Name :	DrayTek_00507F_Vigor2830V_001DAAA82238
Name :	
Manufacturer :	DrayTek
OUI :	00507F
Product Class :	Vigor2830V
Mac Address :	001DAAA82238
Location :	
Lating :	
IP :	172.17.1.208
Port :	8069
URI :	/cwm/CRN.html
Description :	DrayTek Vigor Router
Hardware Version :	101
Software Version :	3.3.6.1db
Modem Firmware Version :	211011_A Annex_A

3.10 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.



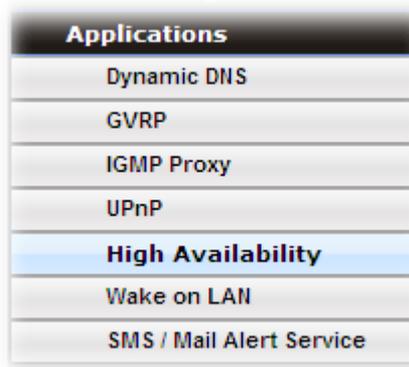
When the HA feature is enabled, the network administrator can set another Vigor3900(s) as the backup device(s) to deliver full routing services during the shutdown of the main Vigor3900. The network administrator can use a Virtual IP (e.g. 192.168.1.100) for both master device and backup device. During 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.

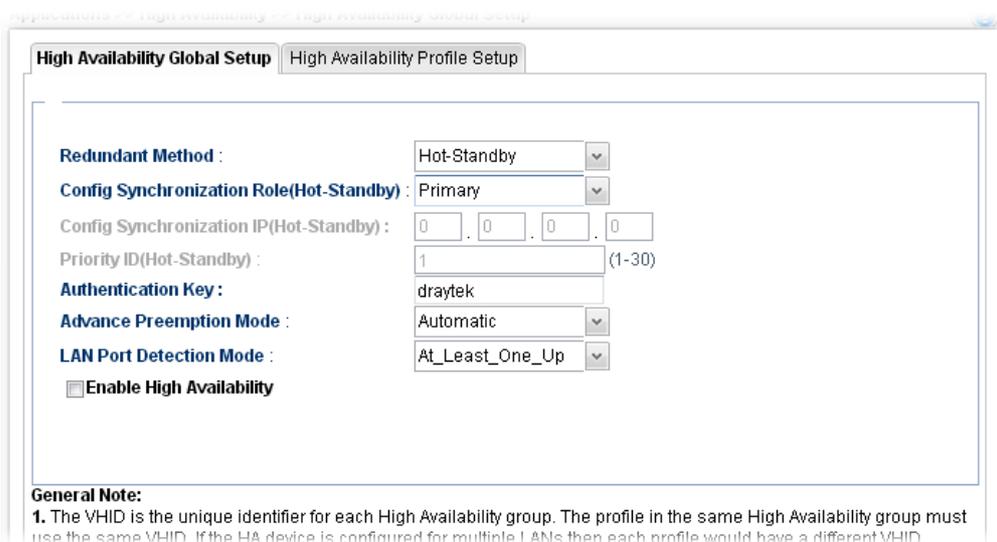
Note: For advanced applications, please refer to FAQ/Application Notes on www.draytek.com.

For router A

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



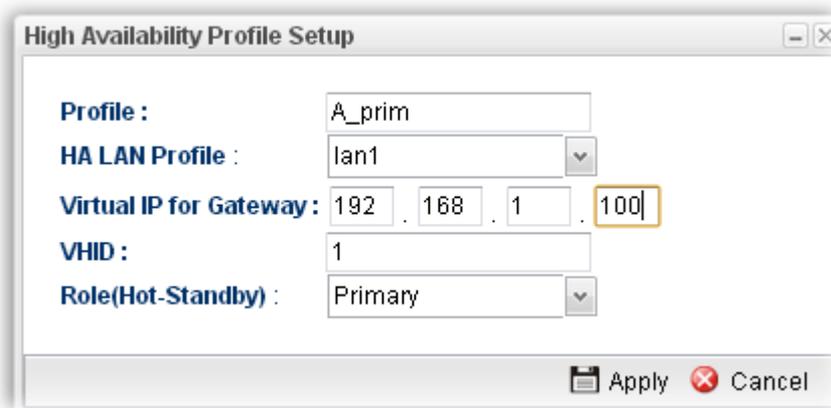
3. In the tab of **High Availability Global Setup**, choose **Hot-Standby** as Redundant Method; choose **Primary** as Config Synchronization Rule; type **draytek** as Authentication Key; choose **Automatic** as Advance Preemption Mode. Click **Apply** to save the settings.



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.



The image shows a 'High Availability Profile Setup' dialog box with the following fields:

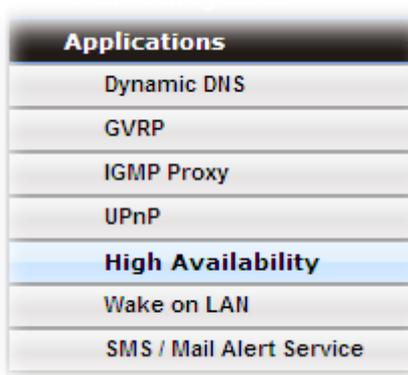
- Profile: A_prim
- HA LAN Profile: lan1
- Virtual IP for Gateway: 192 . 168 . 1 . 100
- VHID: 1
- Role(Hot-Standby): Primary

Buttons: Apply, Cancel

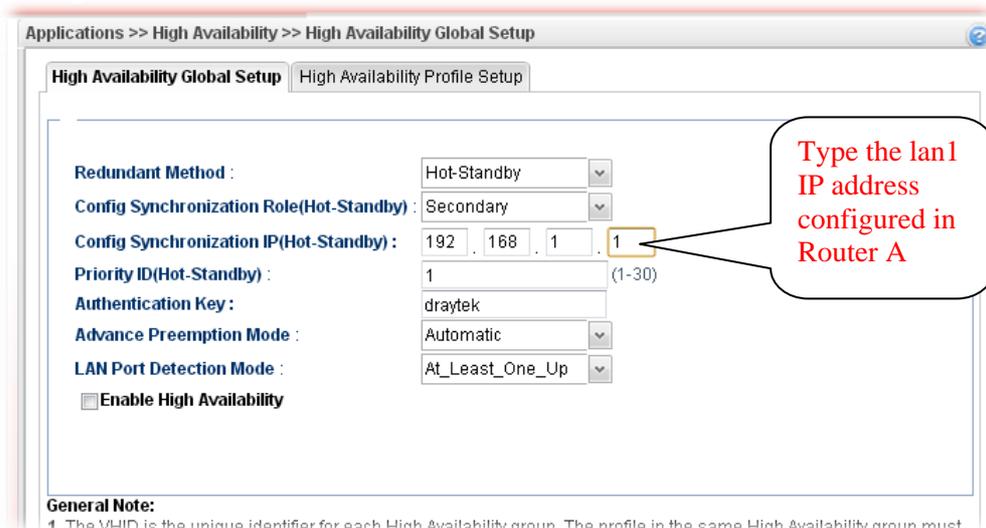
6. Now, the configuration for router A has been finished.

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.



The image shows the 'High Availability Global Setup' configuration page with the following settings:

- Redundant Method: Hot-Standby
- Config Synchronization Rule(Hot-Standby): Secondary
- Config Synchronization IP(Hot-Standby): 192 . 168 . 1 . 1
- Priority ID(Hot-Standby): 1 (1-30)
- Authentication Key: draytek
- Advance Preemption Mode: Automatic
- LAN Port Detection Mode: At_Least_One_Up
- Enable High Availability

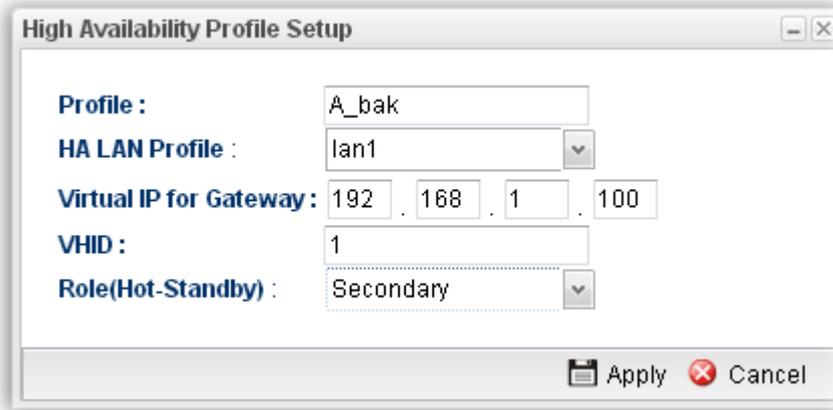
A callout box points to the 'Config Synchronization IP' field with the text: 'Type the lan1 IP address configured in Router A'.

General Note:
1. The VHID is the unique identifier for each High Availability group. The profile in the same High Availability group must

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



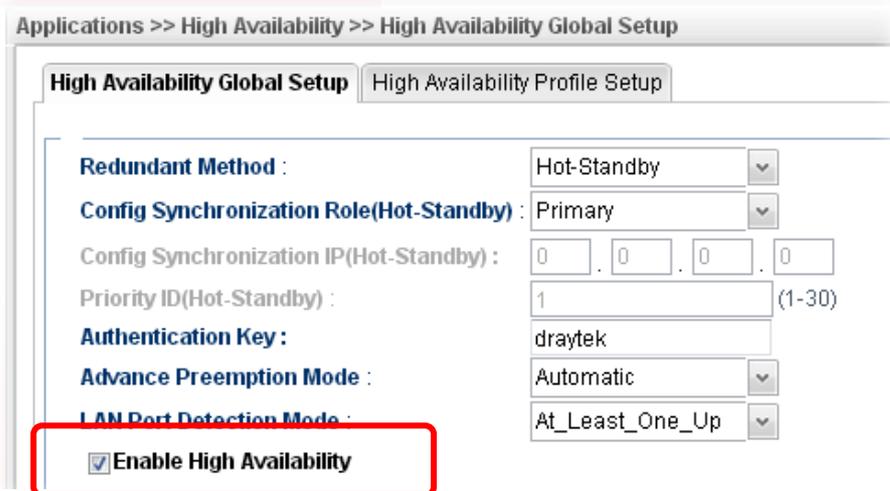
- Create an HA profile. Refer to the following figures.



- 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.

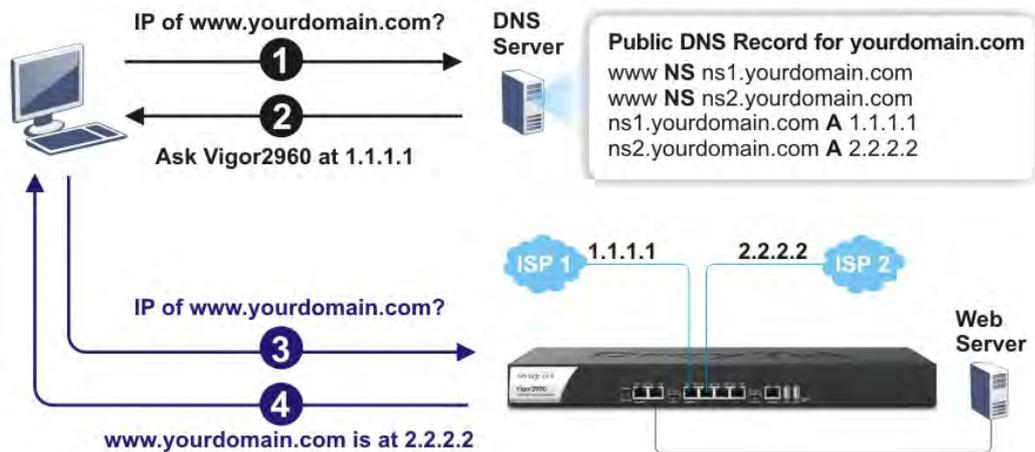


Under such construction, when Router A (defined as Master device) is powered off, Router B (defined as Slave device) will be up and take over all the jobs that Router A performs. Later, when Router A is powered on again, all the jobs will return to Router A.

3.11 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.

Inbound Load Balance



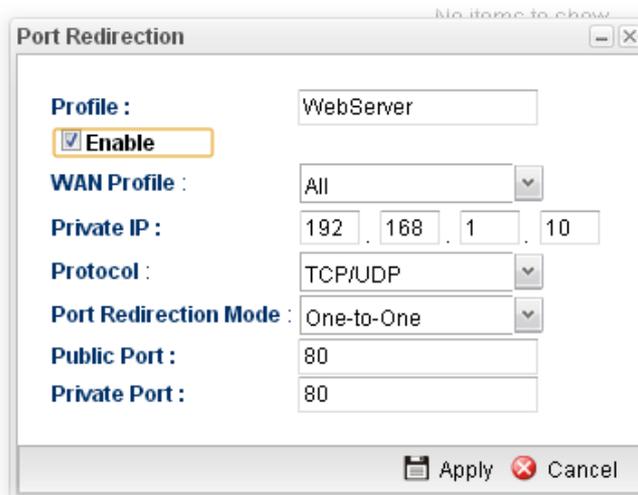
WAN1 IP Address: 1.1.1.1

WAN2 IP Address: 2.2.2.2

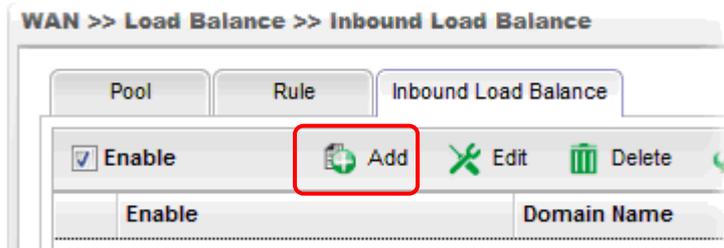
Inbound Load Balance allows Vigor3900 acting as a DNS Server to separate the traffic for each WAN interface according to the DNS query time. Follow the steps listed below to Configure DNS Inbound Load Balance.

Enabling Web service on the Router

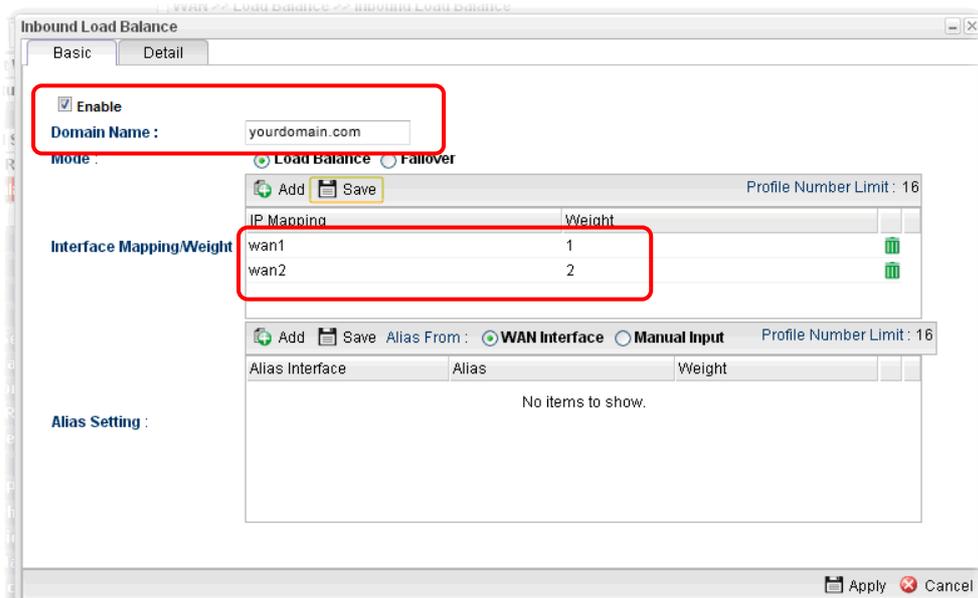
1. Open NAT >> **Port Redirection** to set up Port Redirection rules for the Web server. Click **Apply** to save the settings.



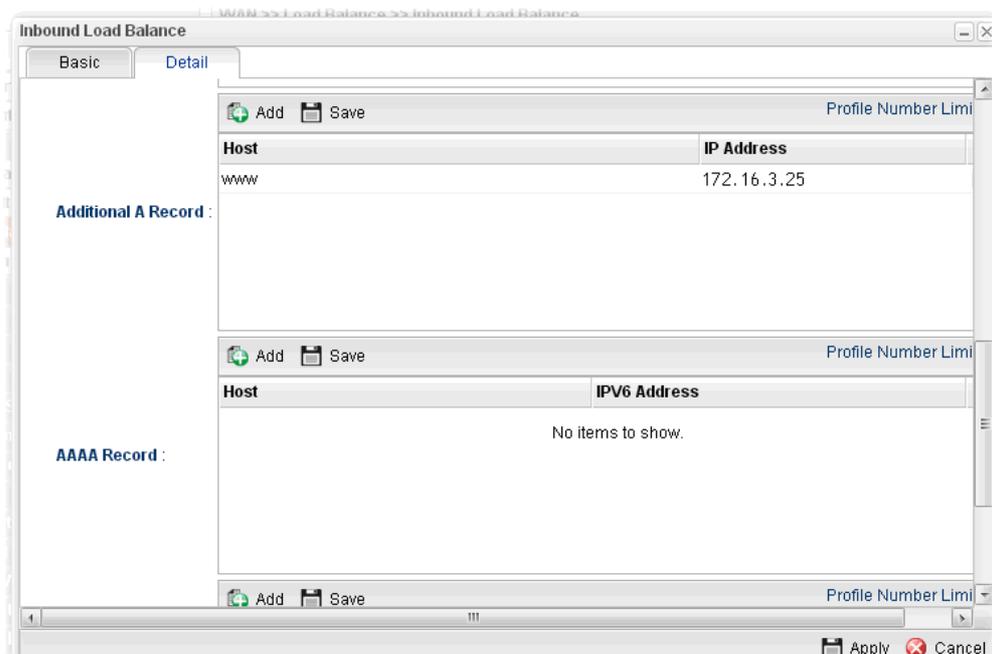
2. Open WAN >> **Load Balance** and click the tab of **Inbound Load Balance** to enable the service. Click **Add**.



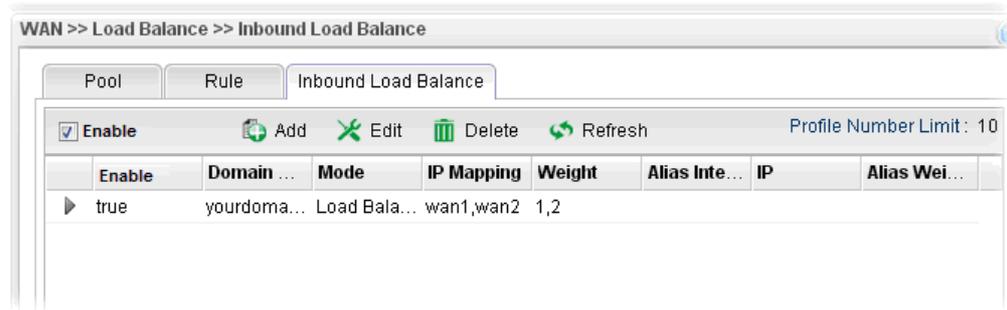
3. Add a profile named “yourdomain.com”. Define WAN1 weights 1 and WAN2 weights 2. It means the total DNS query time will be three, one will pass through WAN1; two will pass through WAN2.



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.

This page is left blank.

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

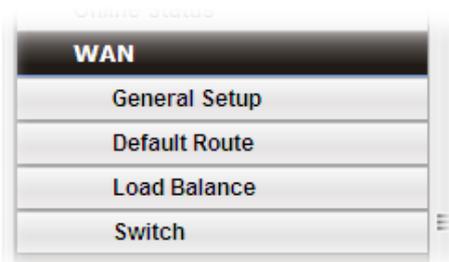
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

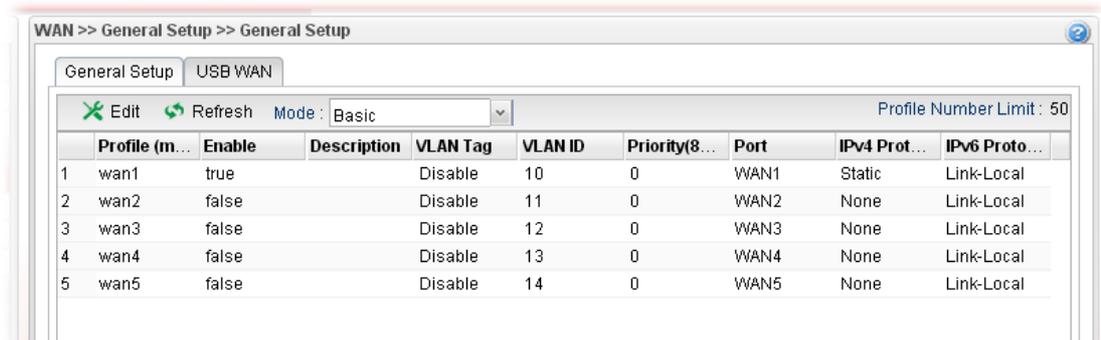
This router supports multi-WAN function. It allows users to access Internet and combine the bandwidth of the WAN profiles to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such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

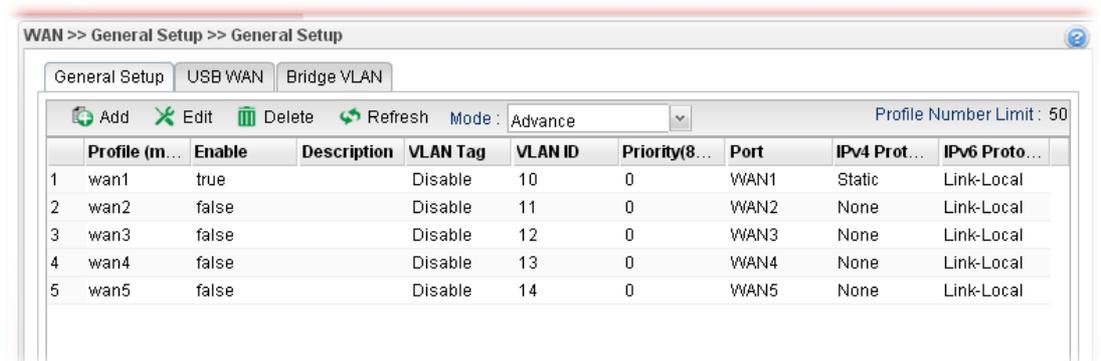
When you switch the Mode setting from Advance to Basic or from Basic to Advance, the system will ask you to re-login web configuration interface to activate some parameters.

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

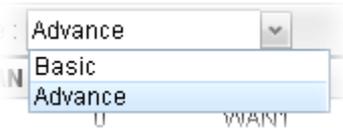
Web Page in Basic Mode



Web Page in Advance Mode



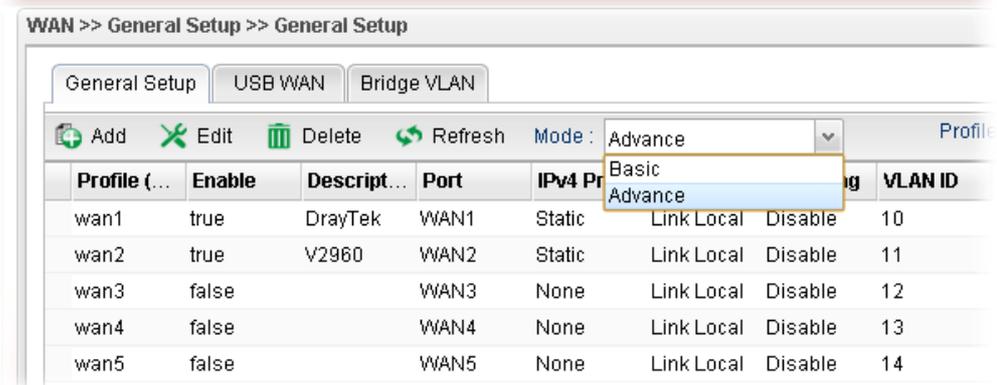
Each item will be explained as follows:

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.

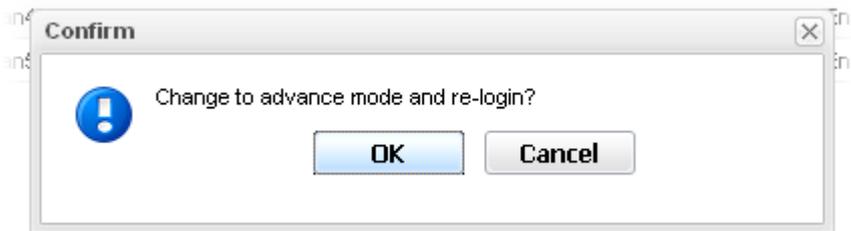
4.1.1.1 Ethernet WAN Profiles

How to add a new WAN profile:

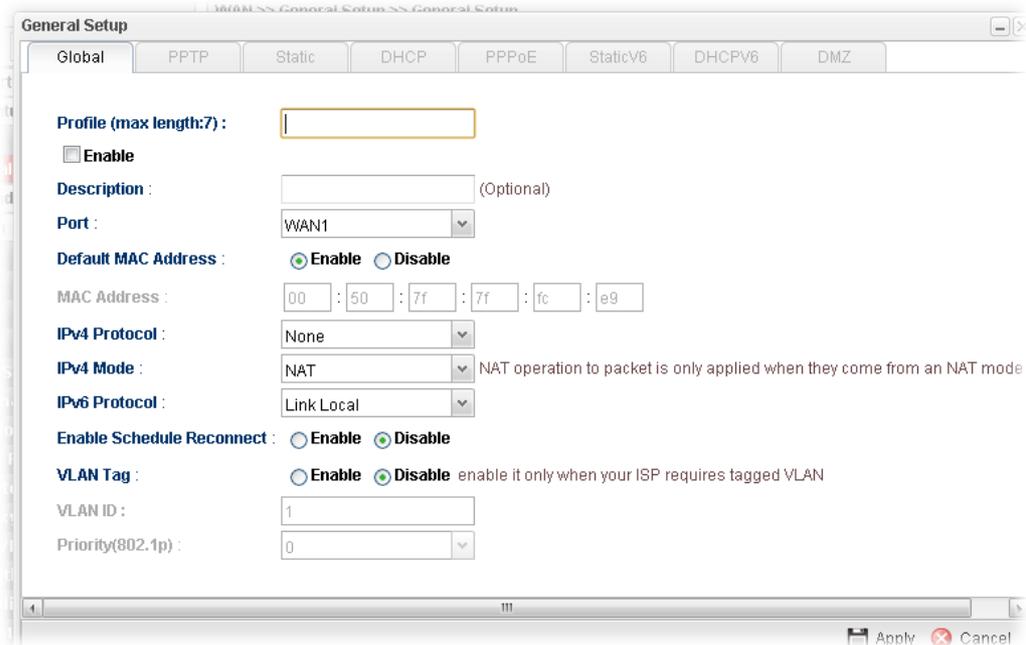
1. If the router is under **Basic** mode, you have to switch into **Advance** mode. If the router is under **Advance** mode, go to Step 4 directly.



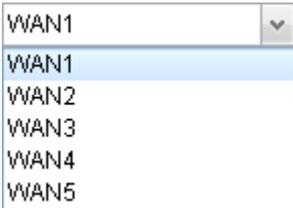
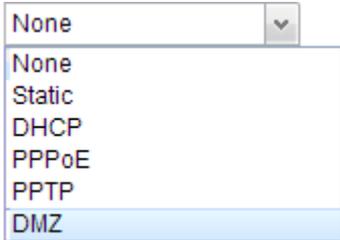
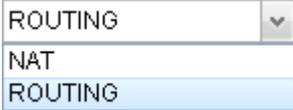
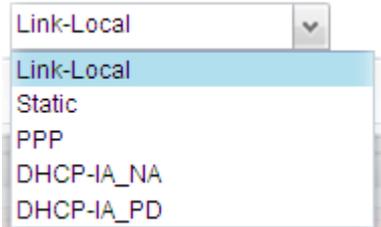
2. A confirmation dialog will appear. Click **OK** to apply the related settings for **Advance** mode.

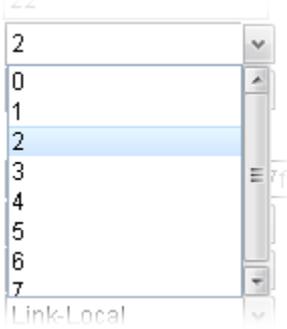


3. Re-login the system.
4. Open **WAN>>General Setup**. Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.



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.
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	Enable – Click it to enable the function of reconnecting the

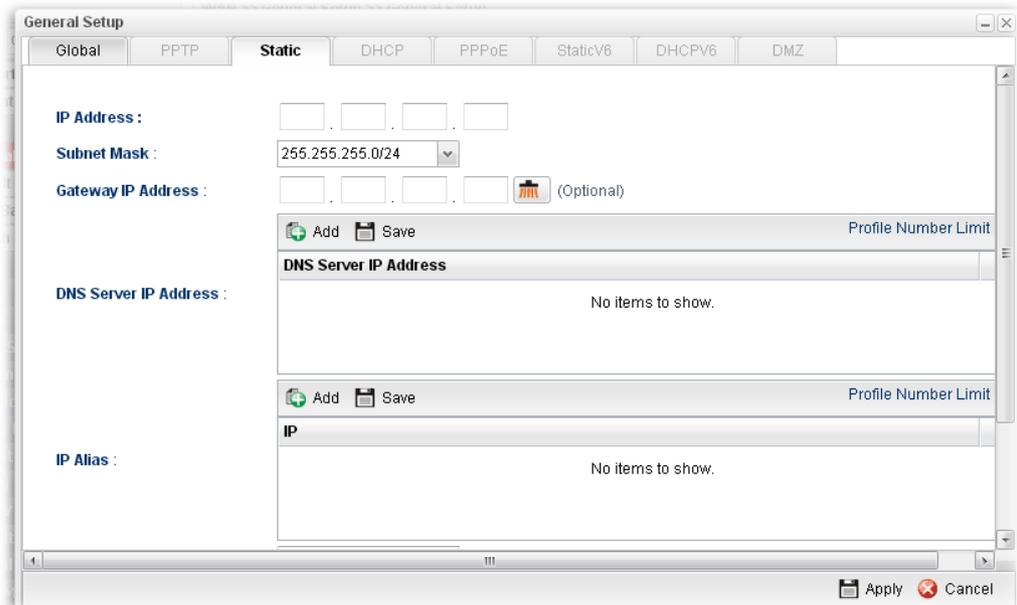
Reconnect	network automatically within the time schedule. Disable – Click it to disable the schedule reconnect function.
Schedule Time Object	Choose the time object profile to be applied by such WAN.
VLAN Tag	Enable – Click it to enable the function of VLAN Tag. Data transmitted through the router will 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.

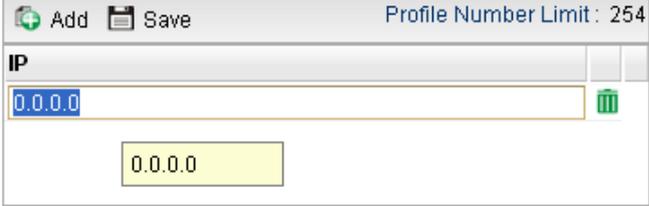
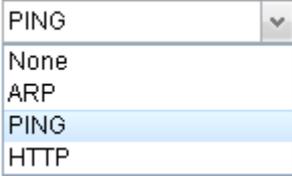
Different IPv4 and IPv6 protocol types specified will bring up different configuration web page.

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



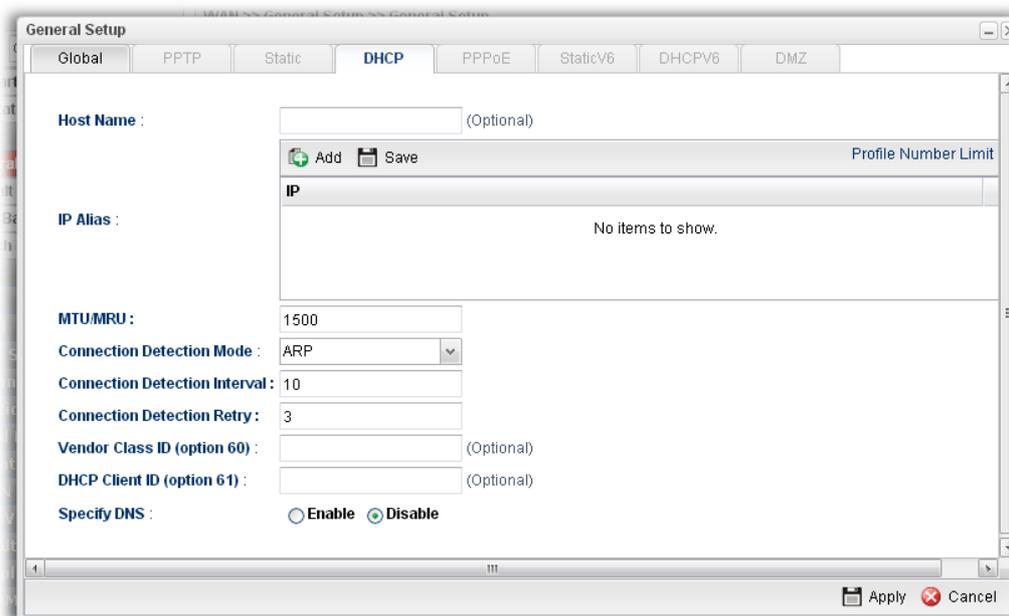
Available parameters are listed as follows:

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 field. The following dialog will appear. <div style="text-align: center;"> </div> <p>Add – click this button to have a field for adding a new IP address.</p> <p>Save – click this button to save the setting.</p> <p> – click the icon to remove the selected entry.</p>
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). <p>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.</p>

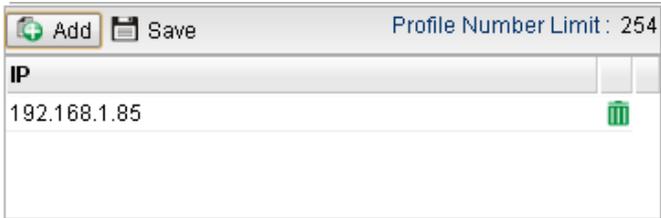
	 <p>Save – Click this button to save the setting.</p>  <p> – click the icon to remove the selected entry.</p>
MTU/MRU	Type the value of MTU/MRU. The default value is 1500.
Connection Detection Mode	<p>Select a detecting mode for this WAN interface. There are three ways ARP, PING and HTTP supported in Vigor router for you to choose to send the request out.</p> 
Connection Detection Host	<p>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.</p>  <p>Save – click this button to save the setting.</p> <p> – click the icon to remove the selected entry.</p>
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.

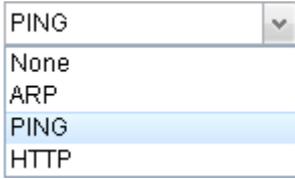
Cancel	Click it to exit the dialog without saving the configuration.
---------------	---

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



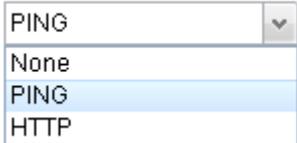
Available parameters are listed as follows:

Item	Description
Host Name (Optional)	Type a name as the host name for identification.
IP Alias	<p>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).</p> <p>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.</p>  <p>Save – click this button to save the setting.</p> <p> – click the icon to remove the selected entry.</p>
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

	<p>router for you to choose to send the request out.</p> 
Connection Detection Host	<p>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.</p>  <p>Save – click this button to save the setting.</p>  – 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)	It used to specify a DHCP client identifier in a host declaration, so that DHCP can find the host record by matching against the client identifier.
Specify DNS	<p>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.</p> <p>Disable – Click it to disable the function of DNS specified.</p>
DNS	<p>Add – click this button to have a field for adding a new IP address.</p> <p>Save – click this button to save the setting.</p>  – 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:*

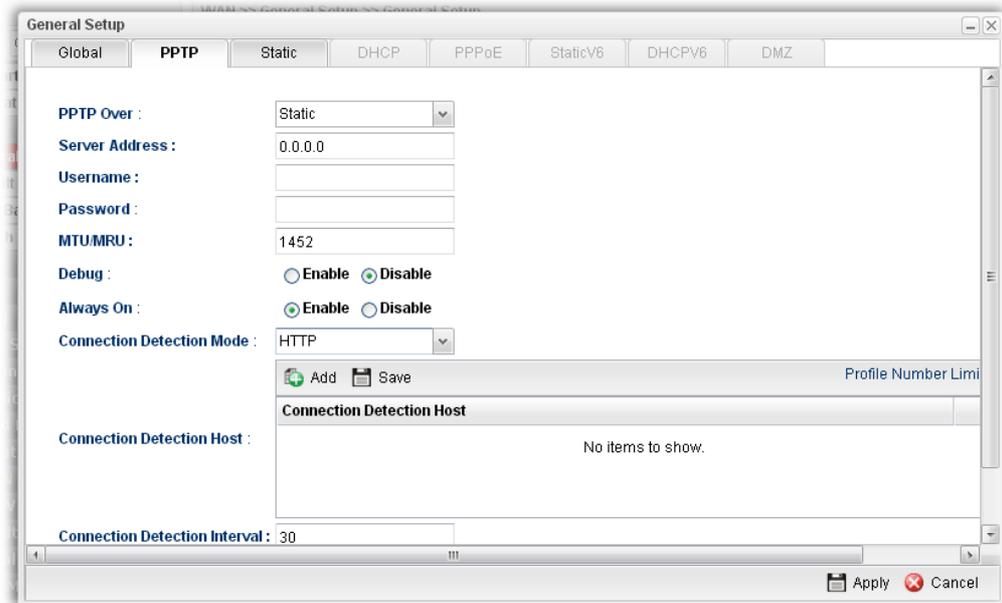
Available parameters are listed as follows:

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.

	<p>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.</p>  <p>Save – click this button to save the setting.</p>  – click the icon to remove the selected entry.
<p>Connection Detection Interval</p>	<p>Assign an interval period of time for each detecting.</p>
<p>Connection Detection Retry</p>	<p>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.</p>
<p>IP Alias</p>	<p>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).</p> <p>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.</p>  <p>Save – After finished the IP address configuration, click Save to save the setting onto the router.</p>  <p> – Click the icon to remove the selected entry.</p>
<p>Specify DNS</p>	<p>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.</p> <p>Disable – Click it to disable the function of DNS specified.</p>

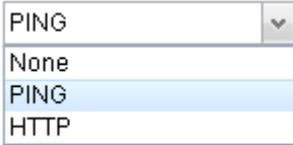
DNS	<p>Add – click this button to have a field for adding a new IP address.</p> <p>Save – click this button to save the setting.</p> <p> – click the icon to remove the selected entry.</p>
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the 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

	<p>router will keep network connection all the time.</p> <p>Disable – Click it to disable the function of Always On.</p>
Connection Detection Mode	<p>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.</p> 
Connection Detection Host	<p>If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection host address in this field. Use the default setting.</p> <p>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.</p>  <p>Save – click this button to save the setting.</p> <p> – click the icon to remove the selected entry.</p>
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.

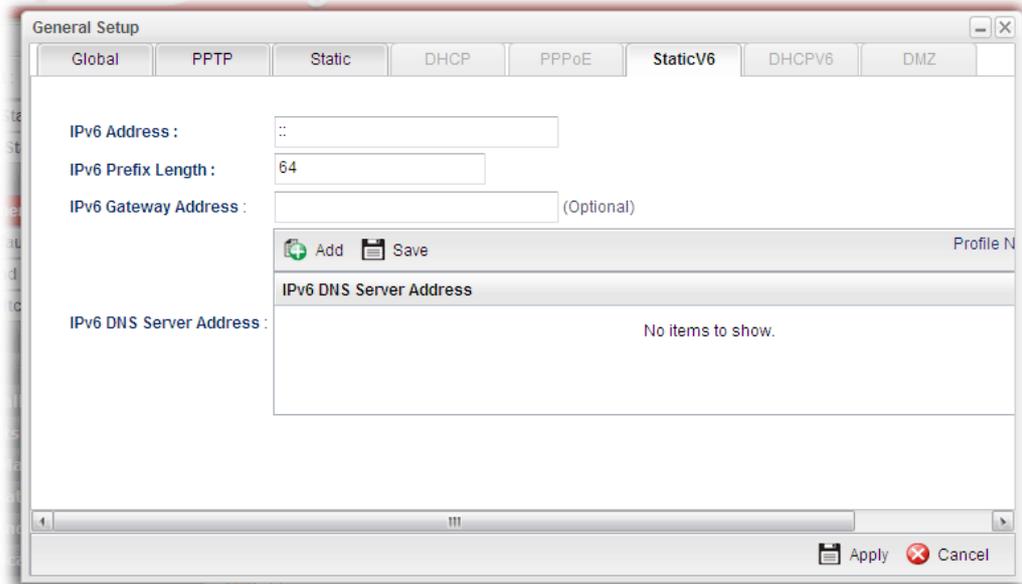
- ***If you choose Link-Local as IPv6 protocol type***

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.

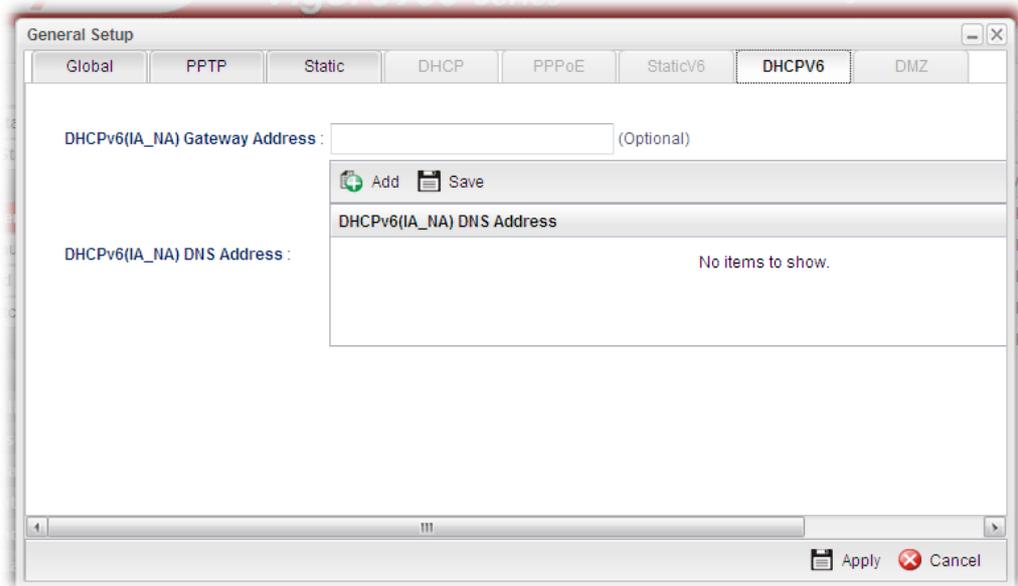
- *If you choose Static as IPv6 protocol type, click the StaticV6 tab to open the following page:*



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.  <p>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.</p>
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

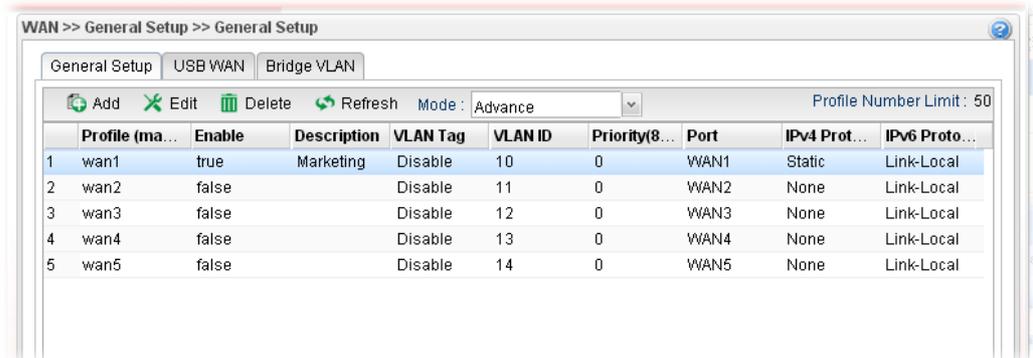
- If you choose *DHCP-IA_NA* as IPv6 protocol type, click the *DHCPV6* Tab to open the following page:



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.
5. 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.

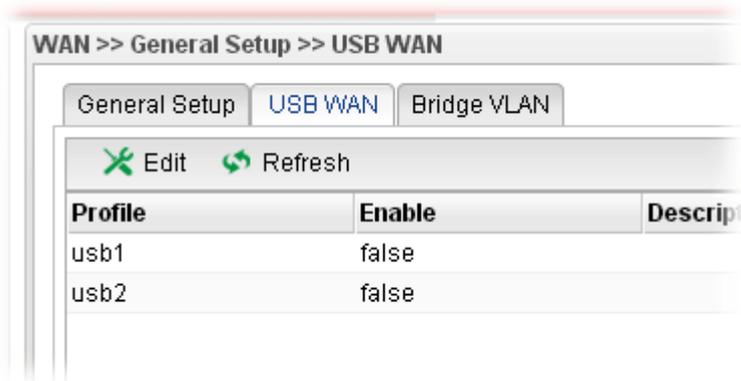


Each item will be explained as follows:

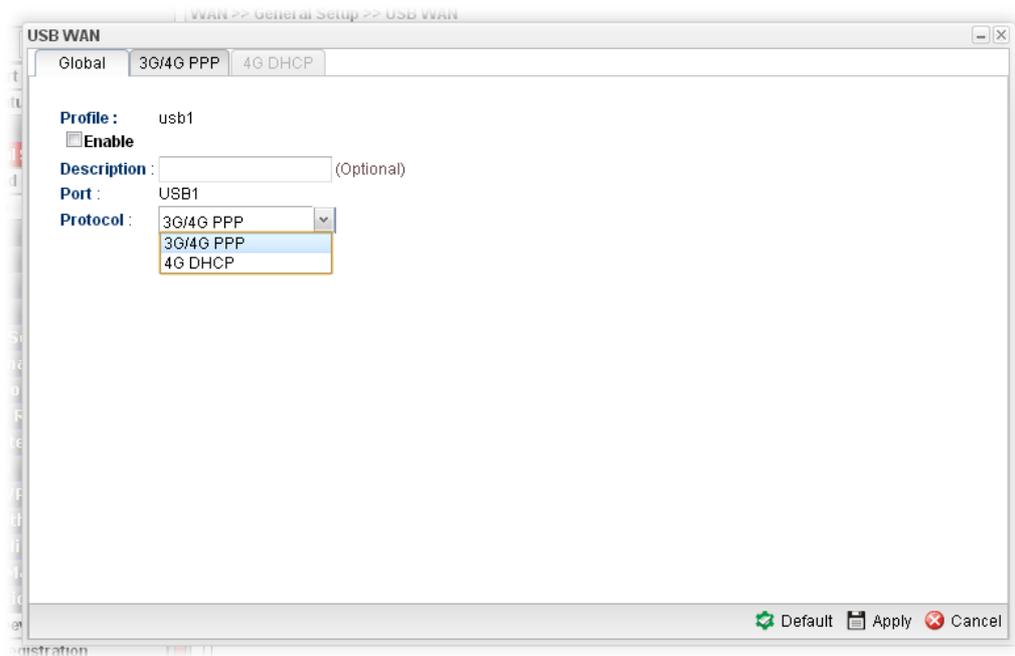
Item	Description
Edit	Modify the selected USB WAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the profile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



- 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. <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> 3G/4G PPP ▼ 3G/4G PPP 4G DHCP </div>
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.

- 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	<p>SIM PIN code -Type PIN code of the SIM card that will be used to access Internet.</p> <p>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.</p> <p>Modem Initial String 2-The initial string 1 is shared with APN. In some cases, user may need another initial AT</p>

	<p>command to restrict 3G band or do any special settings.</p> <p>APN -APN means Access Point Name which is provided and required by some ISPs. Type the name.</p> <p>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.</p> <p>PPP Username -Type the PPP username (optional).</p> <p>PPP Password -Type the PPP password (optional).</p>
4G DHCP	<p>SIM Pin code –Type PIN code of the SIM card that will be used to access Internet.</p> <p>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.</p>  <p>APN Name – APN means Access Point Name which is provided and required by some ISPs.</p>
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.

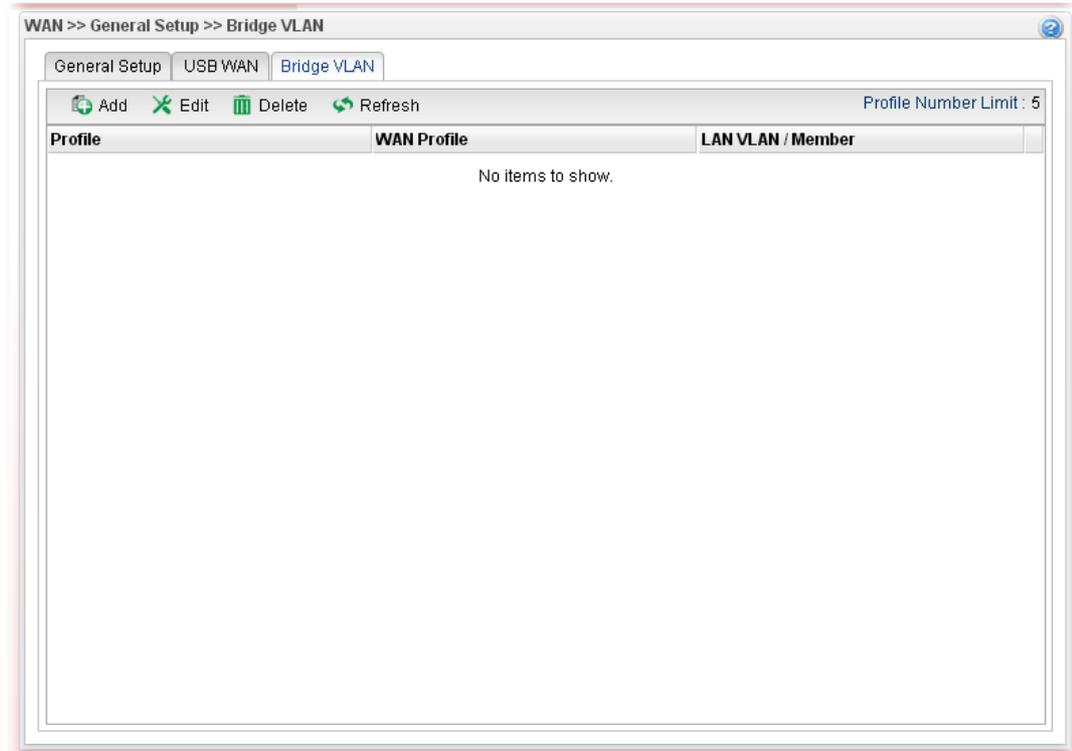
4. Enter all the settings and click **Apply**. The modified profile will be shown as below.



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:

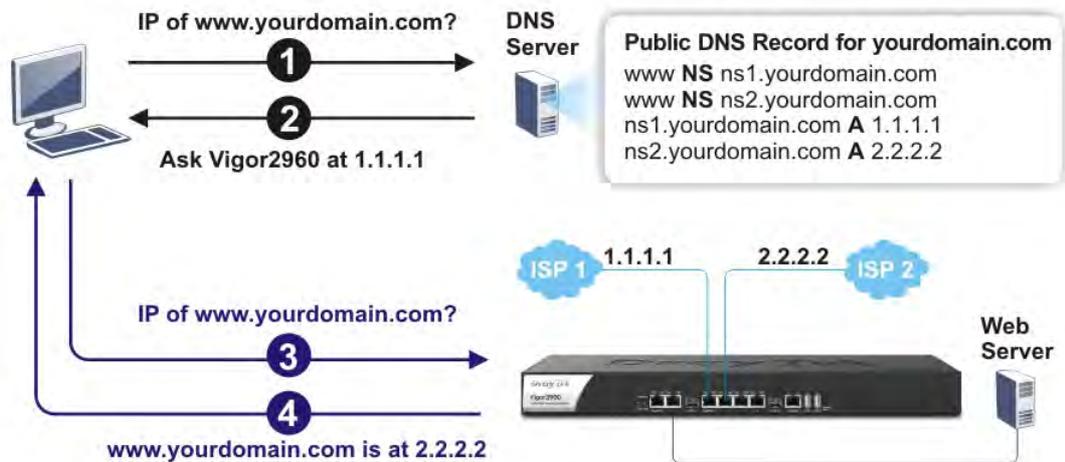
Item	Description
Profile	Type the name of the profile.
WAN Profile	Use the drop down list to choose the WAN interface.
LAN VLAN/Member	Choose a VLAN profile from the drop down list. You have to open LAN>>Switch page and click 802.1Q VLAN for creating VLAN ID number bound with LAN port (802.1Q VLAN profile) first. Otherwise, no profiles will be displayed here for you to specify.
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.

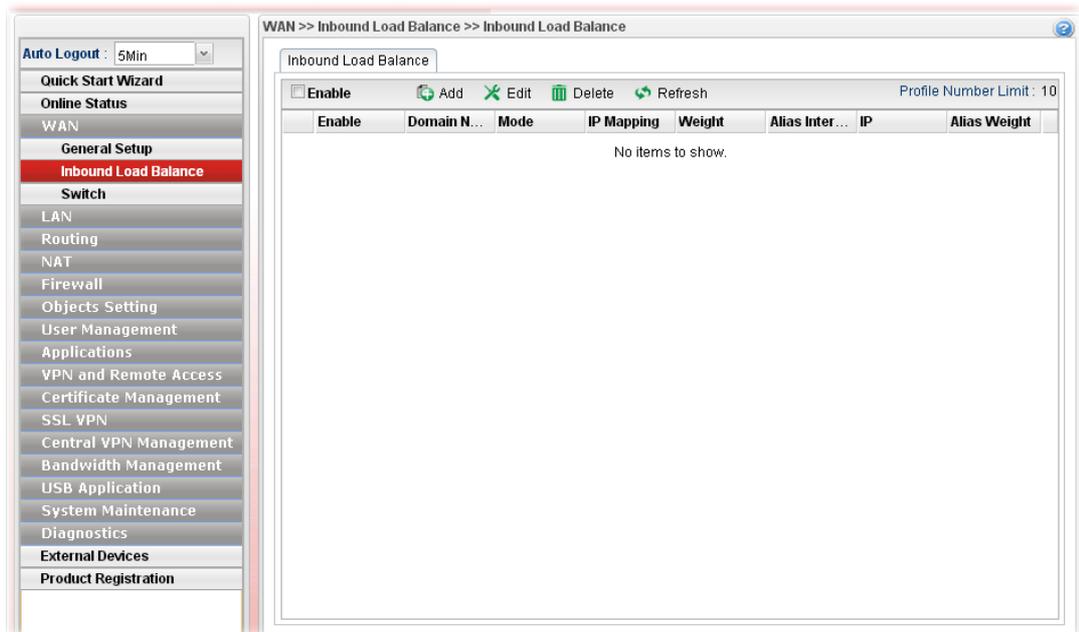
4.1.2 Inbound Load Balance

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.

Inbound Load Balance



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



Each item will be explained as follows:

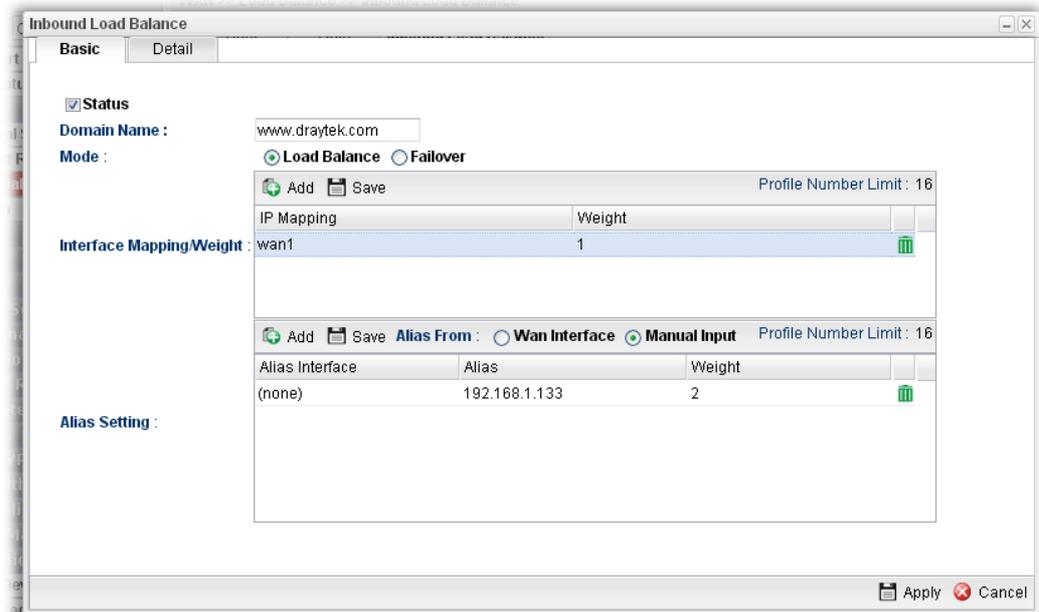
Item	Description
Enable	Check the box the enable inbound load balance function.
Add	Add a new WAN profile for inbound load balance.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify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

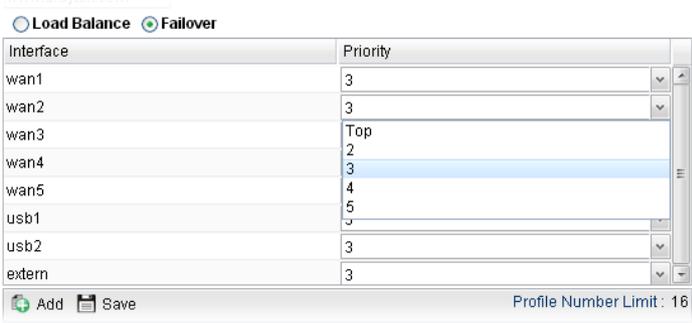
Such page allows you to create a new WAN profile for inbound load balance.

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

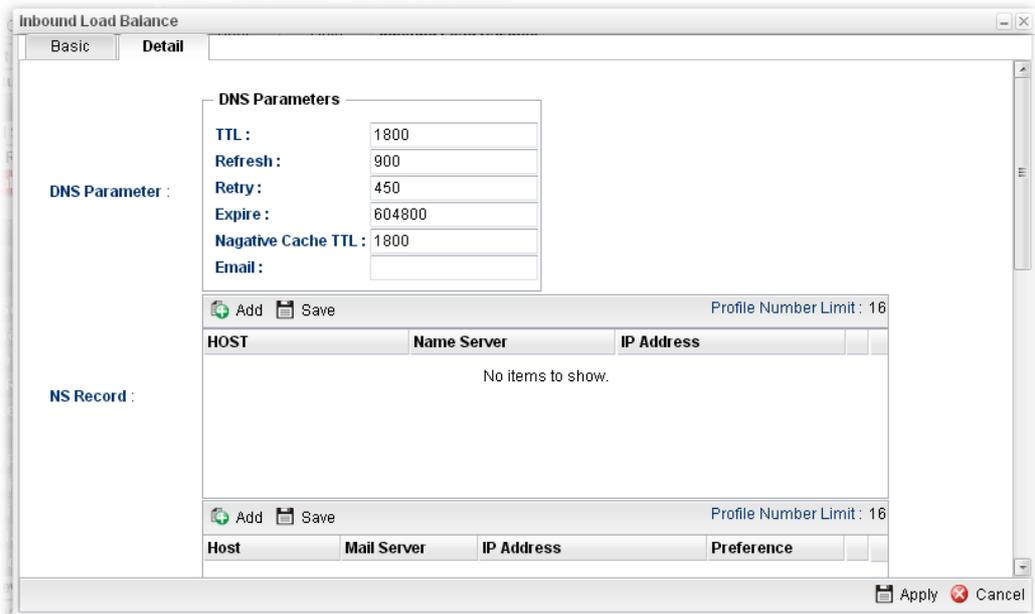


Available parameters are listed as follows:

Item	Description
Status	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	<p>It is available only when Failover is selected as the Mode.</p> <p>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).</p> 
Interface Mapping/Weight	<p>The domain name will inform the remote end with the IP address for DNS query asked by the remote end.</p> <p>The incoming query from the WAN interfaces specified in IP Mapping will be processed according to the weight value.</p> <p>Add – Click it to choose a WAN interface and weight.</p> <p>Save – Click it to save the settings.</p> <p>IP Mapping – Use the drop down list to choose a WAN interface profile which will be used by the domain.</p> <p>Weight – Use the drop down list to choose the one you want.</p>
Alias Setting	<p>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.</p> <p>Add – Click it to add a new IP address.</p> <p>Save – Click it to save the settings.</p> <p>Alias From WAN Interface – The alias IP setting can be specified from existed WAN IP alias.</p> <p>Alias From Manual Input – The alias IP setting can be specified manually. The Alias Interface is not necessary for such method.</p> <p>Alias Interface –Use the drop down list to choose a WAN interface profile for the alias IP setting.</p> <p>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).</p> <p>Weight –Use the drop down list to choose the one you want.</p>

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



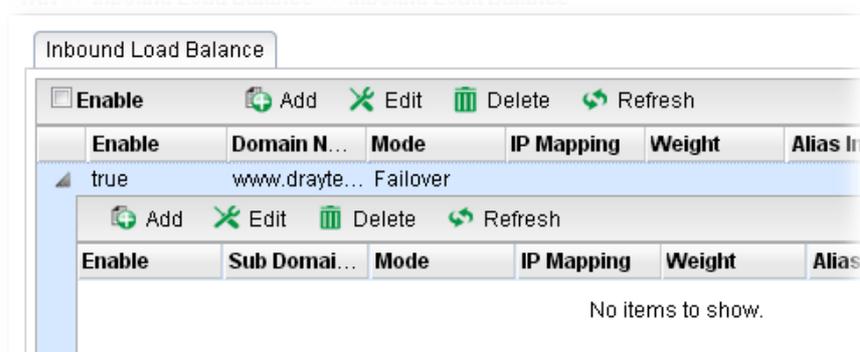
Available parameters are listed as follows:

Item	Description
DNS Parameter	<p>To configure Vigor router as a DNS server, type the related information for applying the function of DNS.</p> <p>TTL – It means Time to live of a DNS response. Available setting range is from 0 to 2147483647.</p> <p>Refresh – Set the time for the PC in LAN to refresh the data.</p> <p>Retry – Set the times of retry if the PC fails to contact with Vigor router before the refreshing expired.</p> <p>Expire – PC stops responding to the query from Vigor router when such time setting has expired.</p> <p>Negative Cache TTL – Set the negative caching time (name error).</p> <p>Email – Type the e-mail address of the administrator.</p>
NS Record	<p>This page is used to specify name server which will be used as DNS server.</p> <p>Add – Click it to add a new server with specified name and IP address.</p> <p>Save – Click it to save the settings.</p> <p>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.</p> <p>Name Server –Type the URL for the name server which will be used to receive the DNS query forwarded by HOST.</p> <p>IP Address – This is optional. If required, simply type the IP address of the NS record server.</p>
MX Record	<p>This is used to specify the mail server with IP address.</p> <p>Add –Click it to add a new server with specified name and IP</p>

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

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

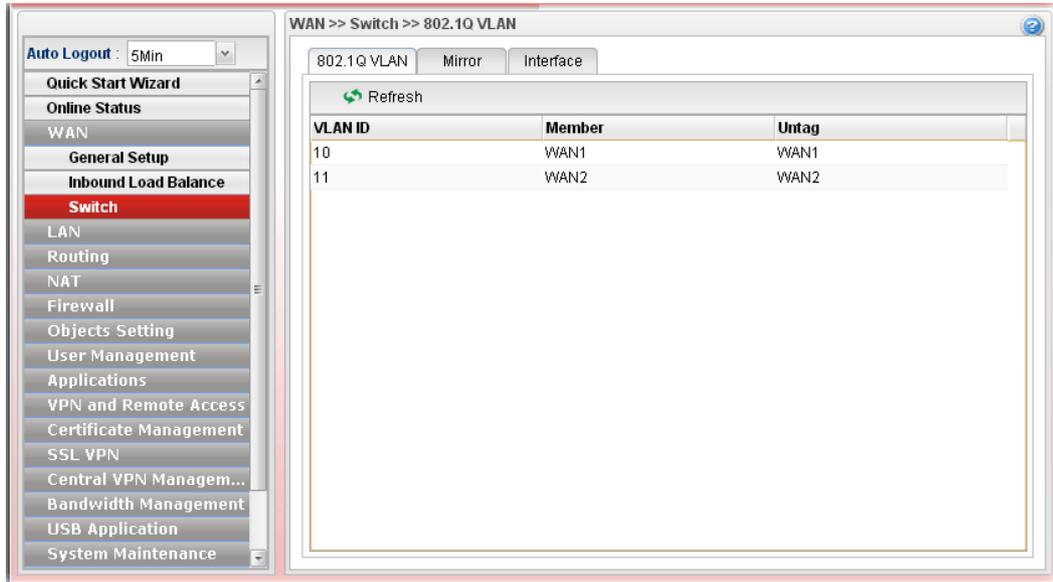
You can create sub-domain by clicking  on the left side of the selected inbound load balance profile. A **sub-domain** setting page will appear for you to add new profile.



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

4.1.3 Switch

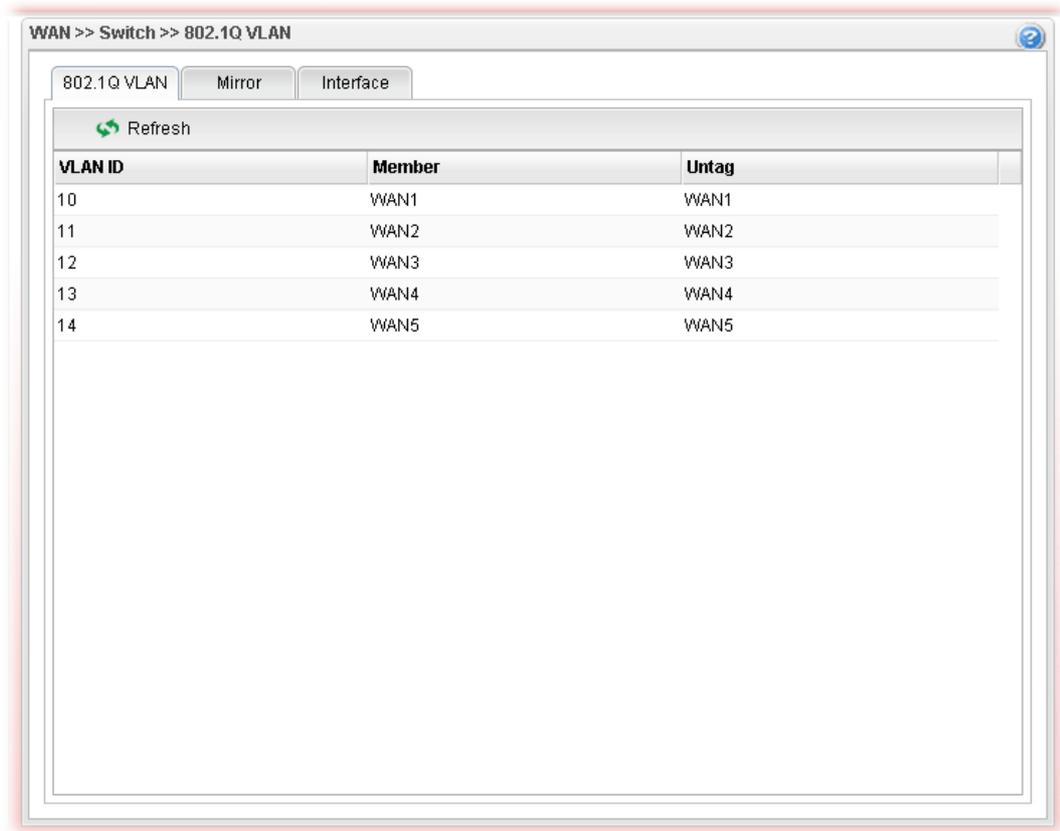
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable WAN interface, and configure 802.1Q VLAN ID for different WAN interfaces, and so on.



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.

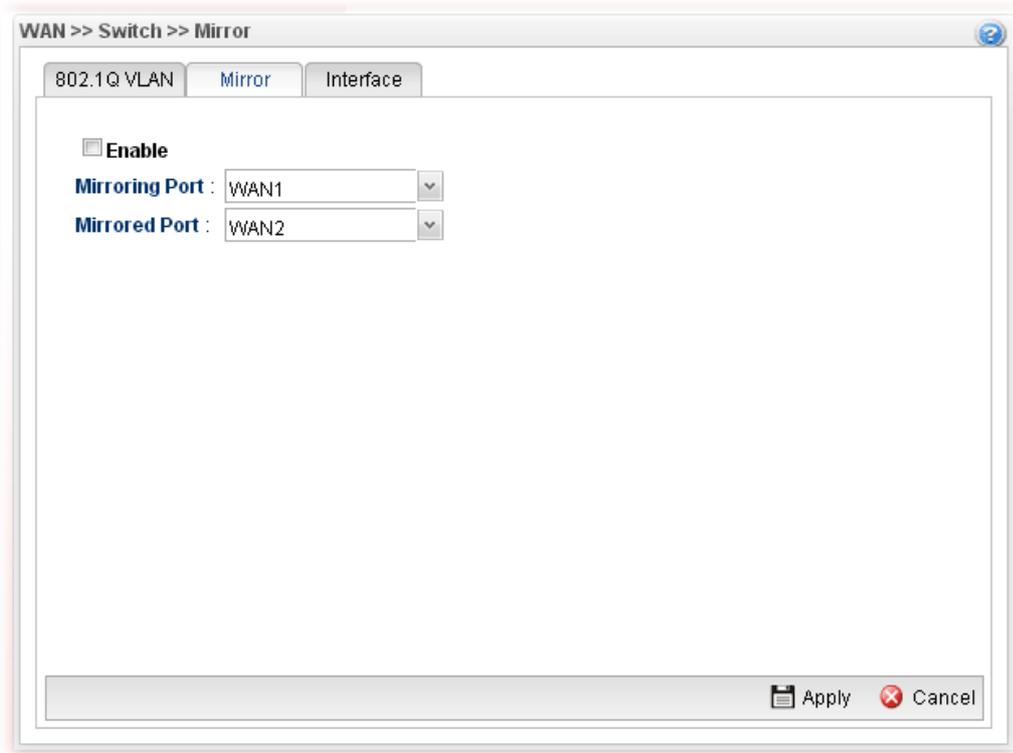


Each item will be explained as follows:

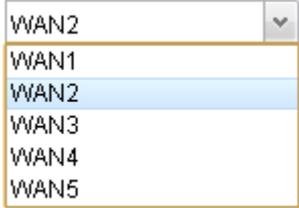
Item	Description
Refresh	Click it to reload this page.
VLAN ID	Display the VLAN ID number.
Member	Display number of the WAN interface for the packets tagged with such VLAN ID number to pass through.
Untag	Display number of the WAN interface for the VLAN ID will be untagged for packets passing through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

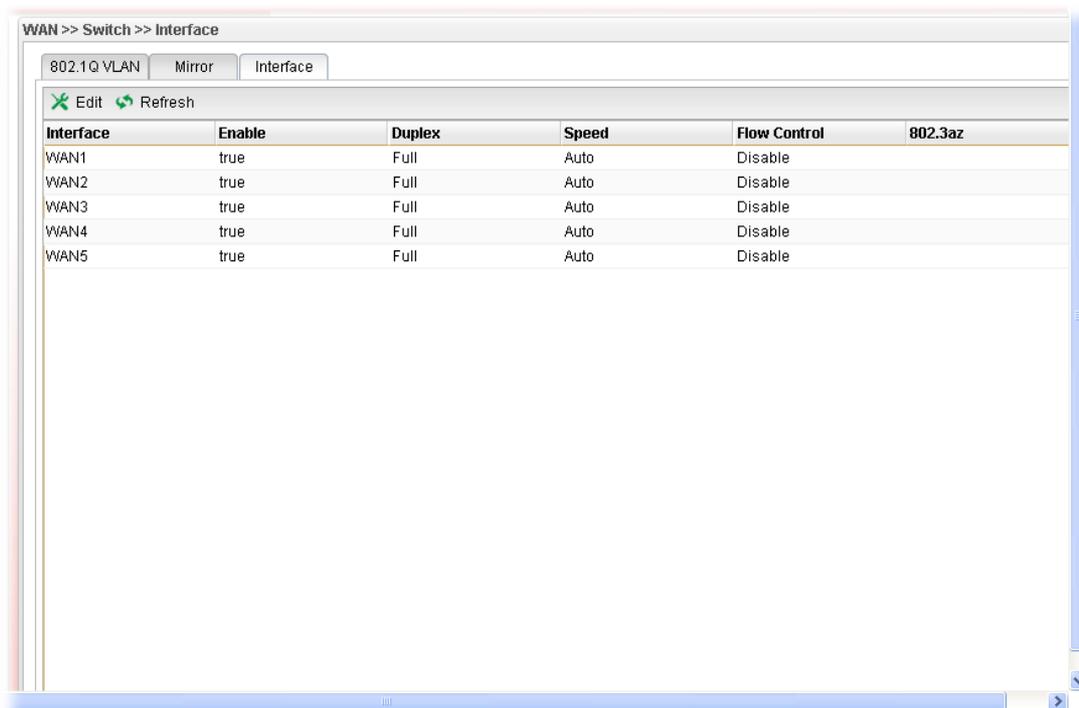


Available parameters are listed as follows:

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:

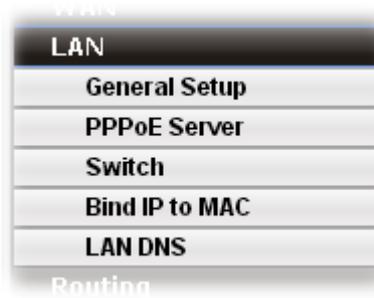
Item	Description
Edit	<p>Choose the interface listed below and click the Edit button to modify the settings. A pop up window will appear for you to change the settings.</p> <p>Interface – Display the name of WAN interface.</p> <p>Enable – Check it to enable such interface.</p> <p>Speed – Use the drop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

	<p>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.</p> <p>Apply – Click it to save and exit the dialog.</p> <p>Cancel – Click it to exit the dialog without saving anything.</p>
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.

Profile (m...	Enable	Description	VLAN ID	IPv4 Proto...	IP Address	Subnet M...	DHCP Ser...	IPv6 Proto
1 lan1	true		10	static	192.168.1.1	255.255.25...	Enable	Link Local

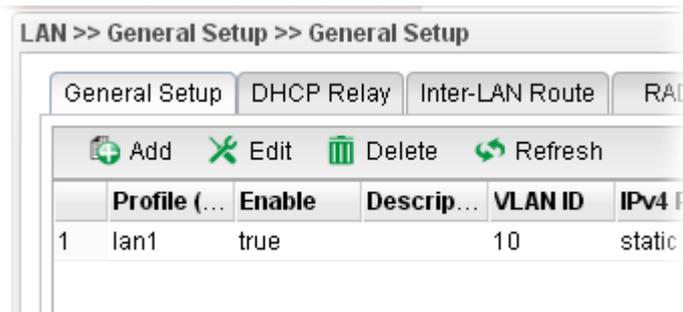
Each item will be explained as follows:

Item	Description
Add	Add a new LAN profile.

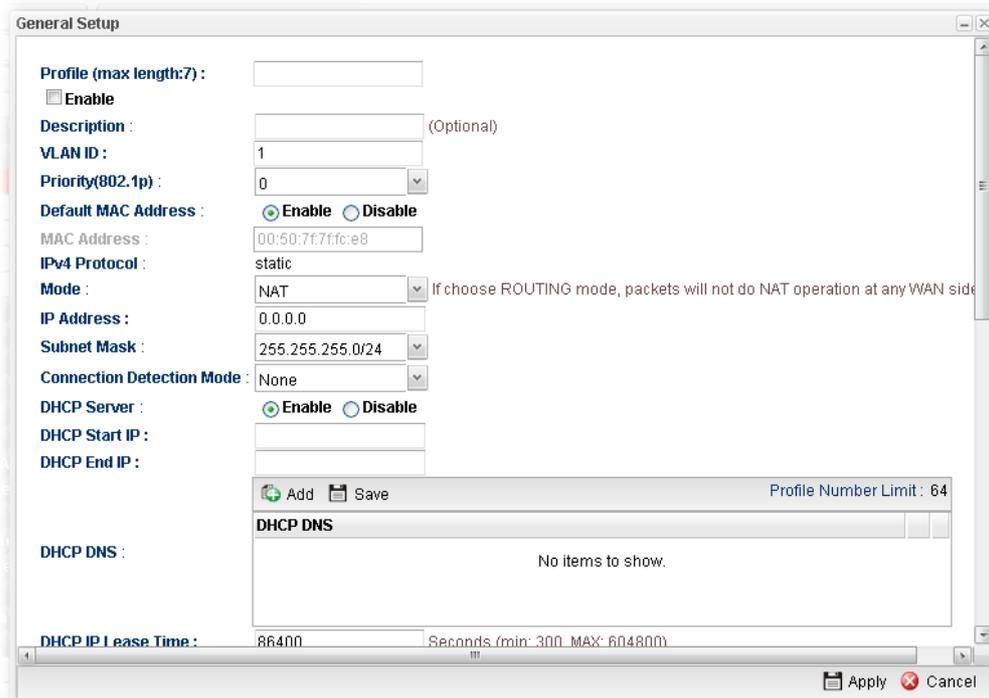
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected LAN profile. To delete a rule, simply select the one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

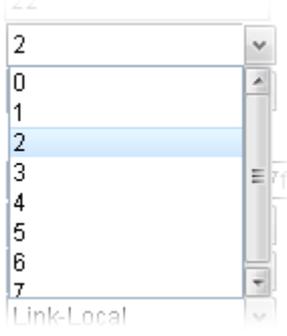
1. Open LAN>>General Setup and click the **General Setup** tab.

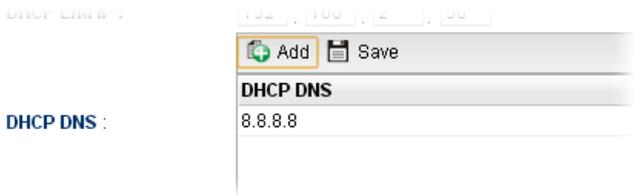


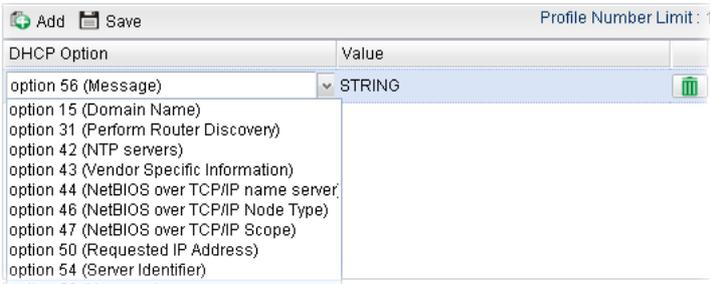
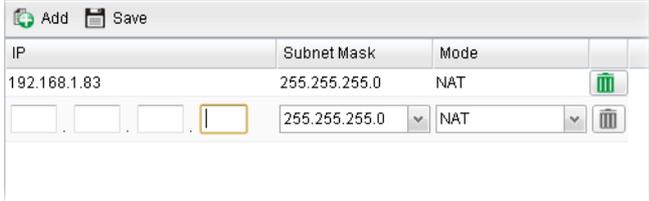
- Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.



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	<p>In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user.</p> <p>However, if you want to use other gateway, please assign the IP address in this field.</p>
DHCP Next Server	Type the IP address of the secondary DHCP server.
DHCP Options	<p>DHCP packets can be processed by adding option number and data information when such function is enabled.</p> <p>Each DHCP option is composed by an option number with data. For example,</p> <p style="padding-left: 40px;">Option number:100 Data: abcd</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p>  <p>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.</p>
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	<p>Different subnets can be created under one LAN profile. Specify other subnets which might be needed in the future.</p>  <p>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.</p>

	<p>Subnet Mask – Use the drop down list to choose the one you want.</p> <p>Mode – Specify NAT or Routing as the mode.</p> <p>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.</p> <p>Start IP – Type an IP address as a starting point.</p> <p>End IP – Type an IP address as an ending point.</p>
DNS Redirection	<p>Enable – It can redirect DNS queries from such LAN profile to router's DNS Server. It must work with LAN DNS function.</p>
IPv6 Protocol	<p>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.</p> <p>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.</p> <p>Static –This type allows you to setup static IPv6 address for LAN.</p> <p>DHCP-SLA- DHCPv6 client mode would use IA_NA option of DHCPv6 protocol to obtain IPv6 address from server.</p>
IPv6 Address	<p>If Static is chosen as IPv6 Protocol, please type the IPv6 address in this field.</p>
IPv6 Prefix Length	<p>Display the IPv6 prefix length.</p>
DHCPv6 SLA WAN Interface	<p>If DHCP-SLA is chosen as IPv6 Protocol, please choose one of the WAN profiles in this field.</p>
DHCPv6 SLA ID	<p>The ID number set here is used by an individual organization to create its own local addressing hierarchy and to identify subnets.</p>
Apply	<p>Click it to save and exit the dialog.</p>
Cancel	<p>Click it to exit the dialog without saving anything.</p>

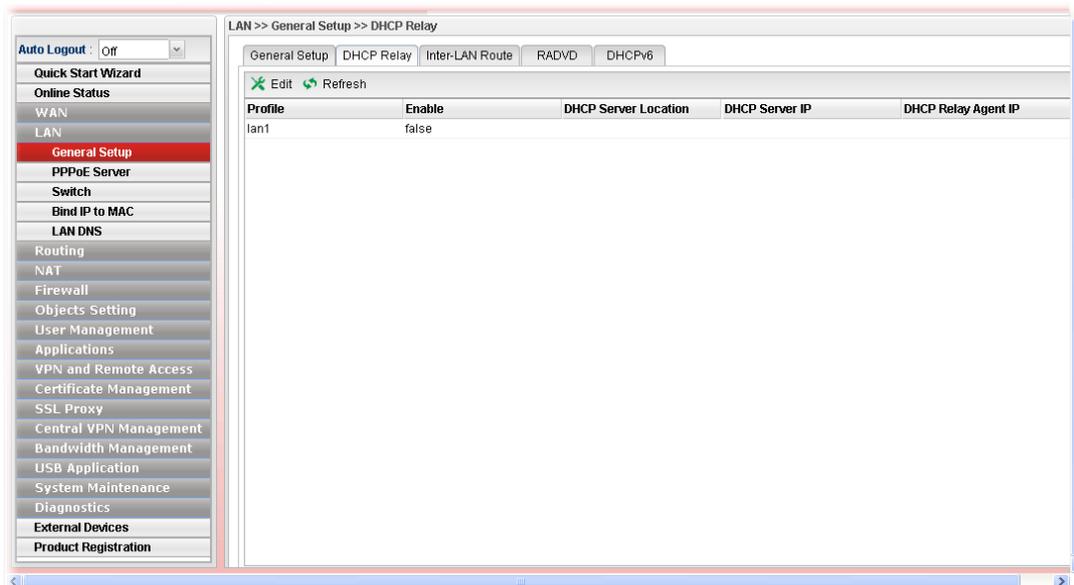
- When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.

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.

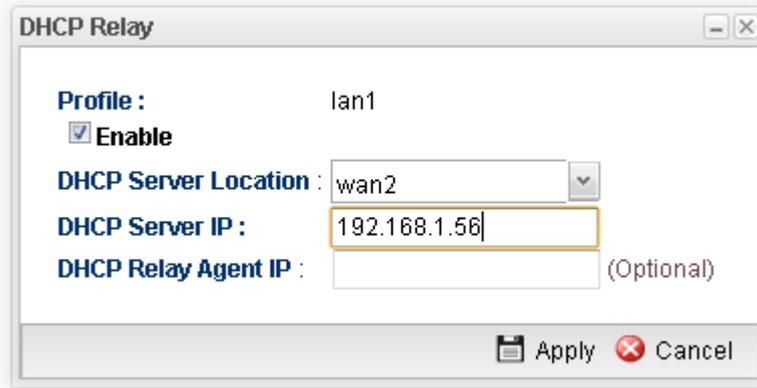


Each item will be explained as follows:

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.



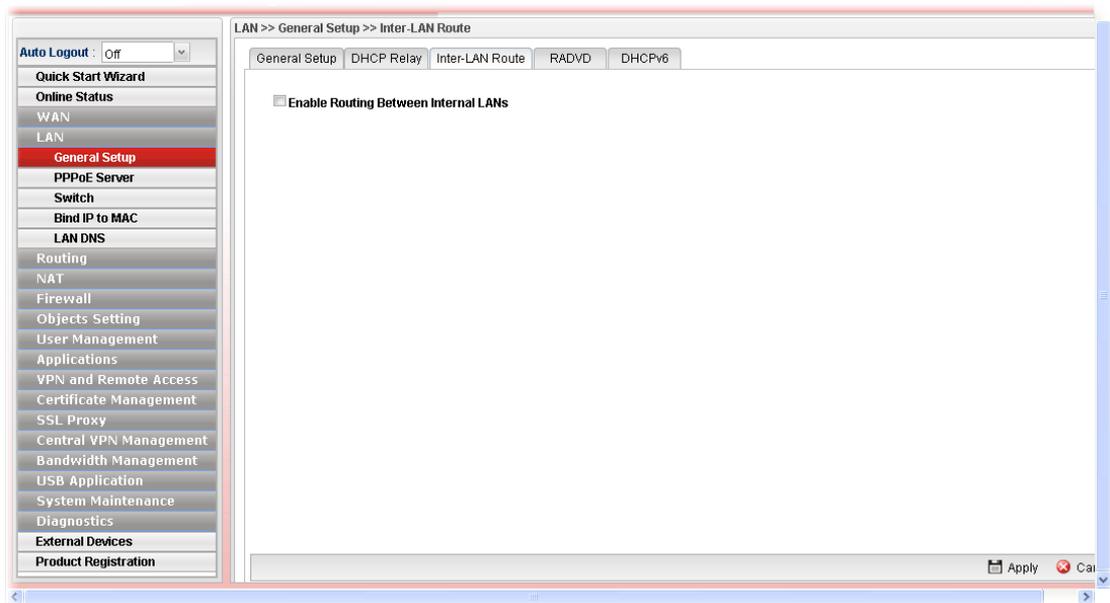
Available parameters are listed as follows:

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.

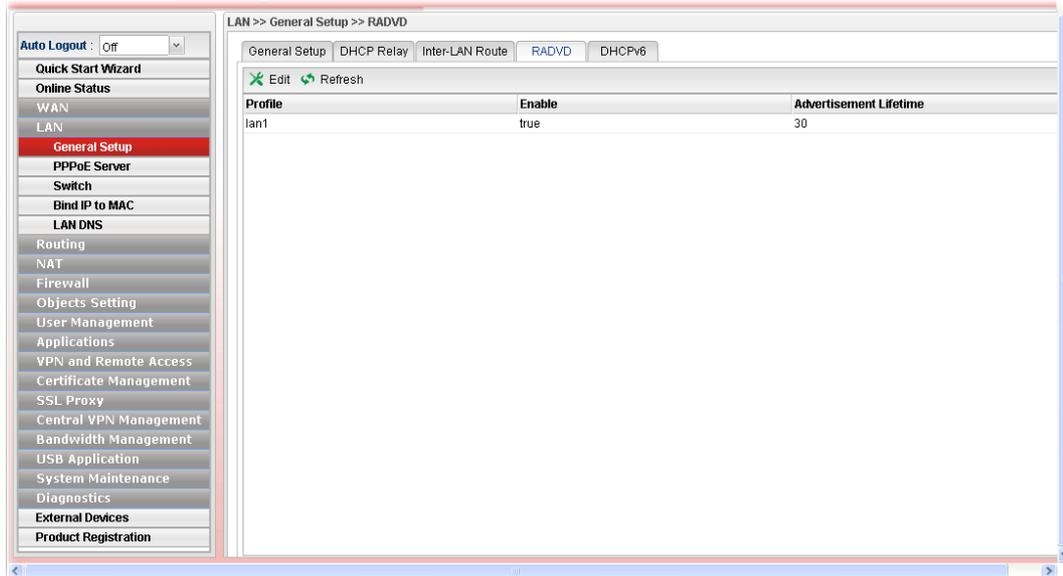
4.2.1.3 Inter-LAN Route

To make the users in different LAN communicating with each other, please check the box to enable Inter-LAN route function.



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.

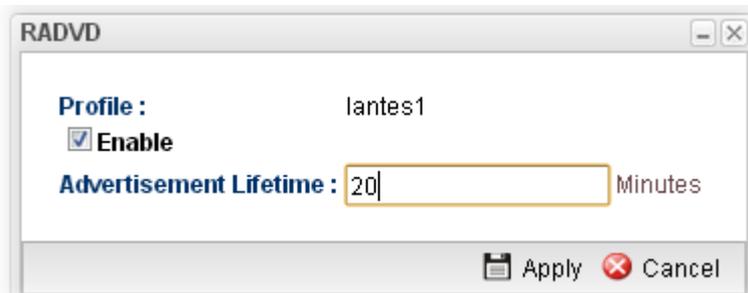


Each item will be explained as follows:

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.



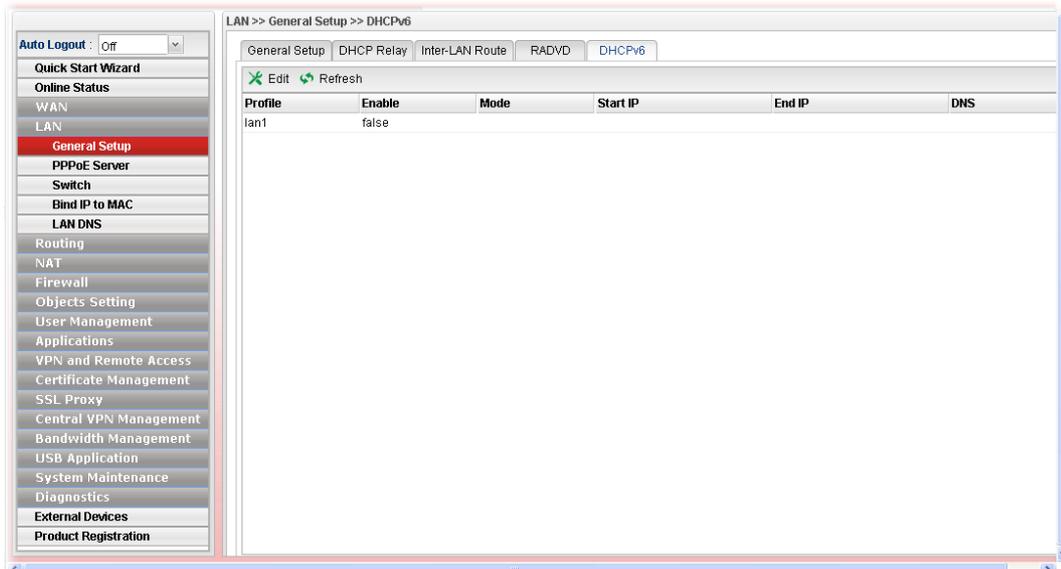
Available parameters are listed as follows:

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.

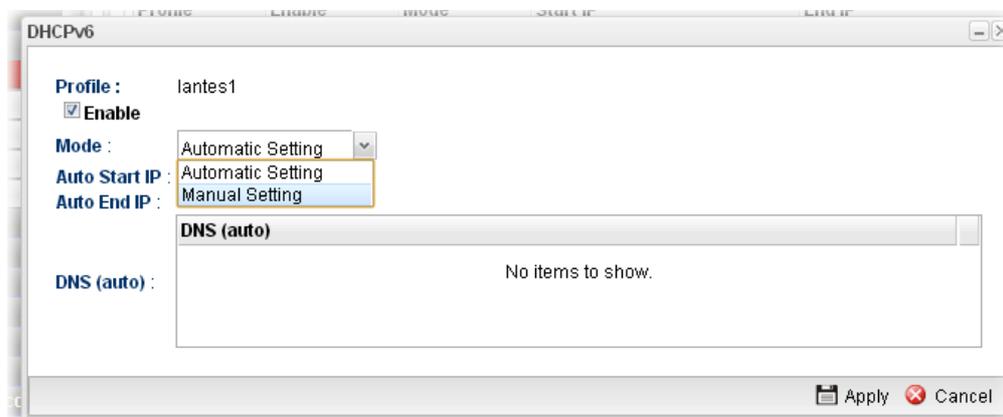


Each item will be explained as follows:

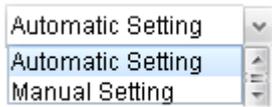
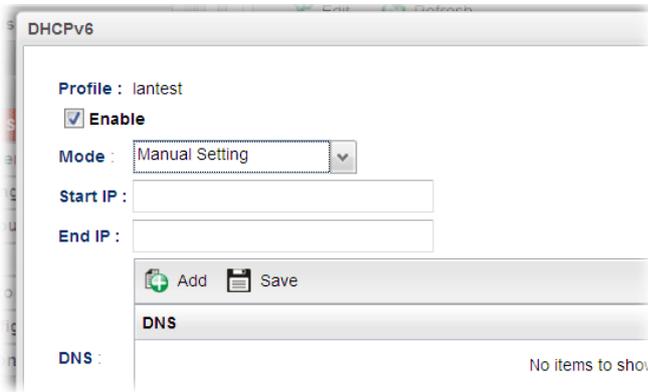
Item	Description
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the name of the 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.

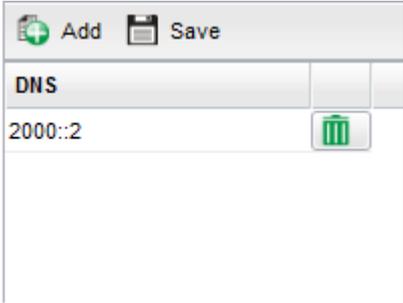
How to edit a LAN profile for DHCPv6

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	<p>Choose Automatic Setting or Manual Setting.</p>  <p>Automatic Setting – It is not necessary to configure Start IP, End IP and DNS setting. The system will assign suitable address automatically.</p> <p>Manual Setting – You should type the Start IP address and End IP address manually.</p> 
Start IP	<p>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:</p> <p>2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.</p>

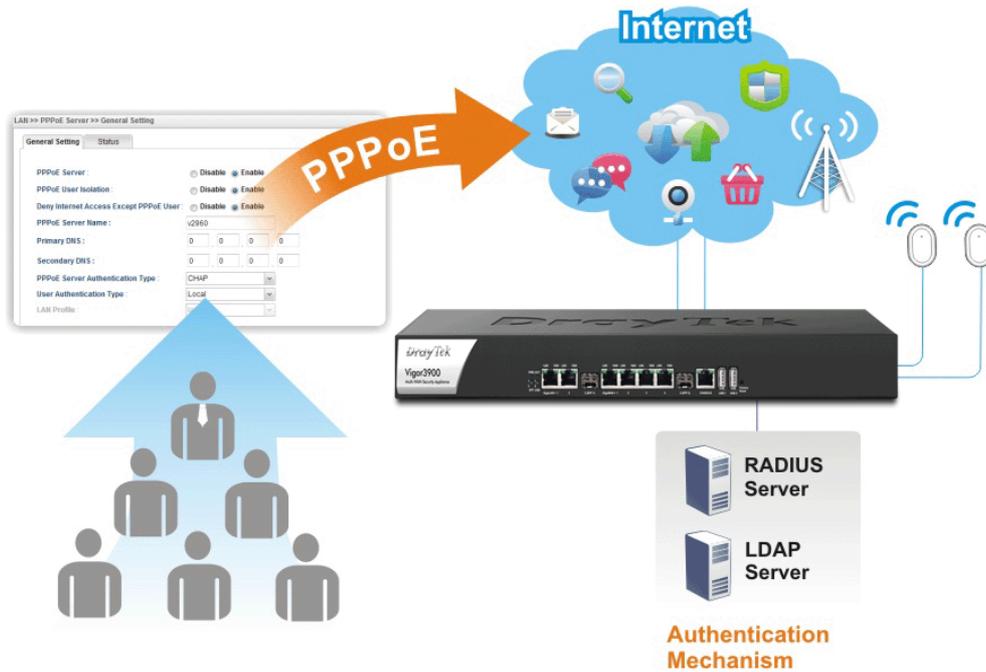
End IP	Set the ending IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.
DNS	<p>It is available when Manual Setting is selected as Mode. Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.</p>  <p>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.</p>
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.

4.2.2 PPPoE Server

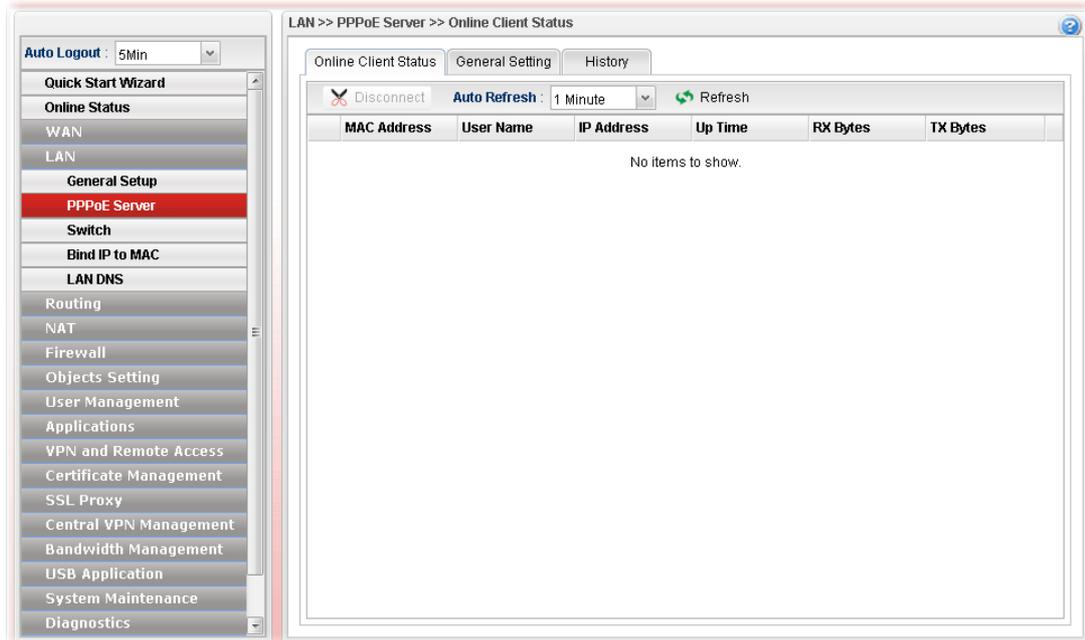
This feature makes the router working like an ISP, providing PPPoE connections to LAN PCs. The only difference is that local PCs don't need an ADSL modem.

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

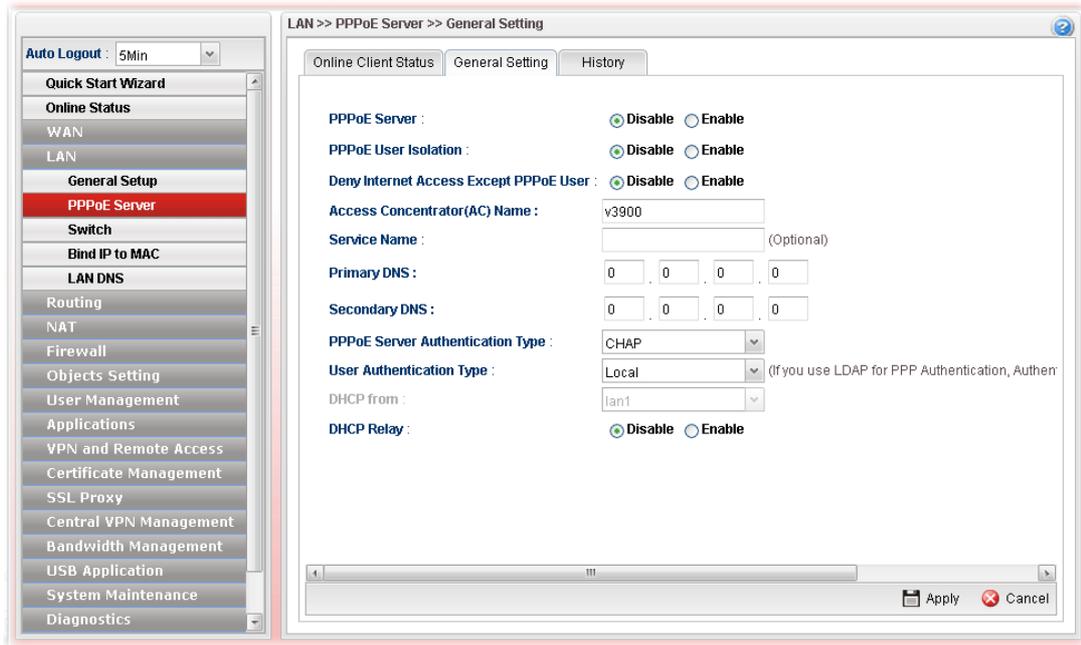
This page displays general information for PPPoE server; allows you to disconnect the network connection to PPPoE server.



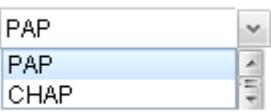
Each item will be explained as follows:

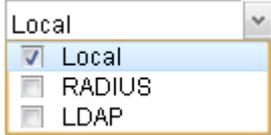
Item	Description
Refresh	Renew current web page.
Disconnect	Click it to disconnect the profile connection.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
MAC Address	Display the MAC address of 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



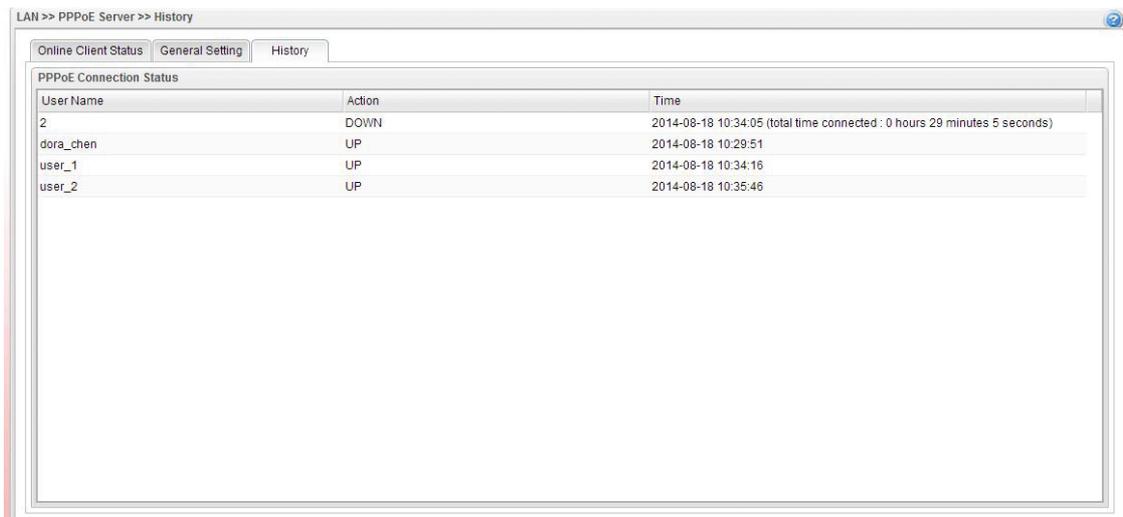
Available parameters are listed as follows:

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 Type	<p>Users in LAN can access into Internet through Vigor router with RADIUS, LDAP or local authentication. Specify the type for the users.</p> 
LDAP Profile	<p>It is available when LDAP is selected as User Authentication Type.</p> <p>If you choose LDAP as the authentication type, use the drop down list to specify the LDAP profile.</p>
DHCP From	<p>It is available when RADIUS is selected as User Authentication Type.</p>
DHCP Relay	<p>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.</p> <p>DHCP Server Location – Choose one of the interfaces for DHCP server.</p> <p>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.</p>
Apply	<p>Click it to save and exit the dialog.</p>
Cancel	<p>Click it to discard current page modification.</p>

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.



User Name	Action	Time
2	DOWN	2014-08-18 10:34:05 (total time connected : 0 hours 29 minutes 5 seconds)
dora_chen	UP	2014-08-18 10:29:51
user_1	UP	2014-08-18 10:34:16
user_2	UP	2014-08-18 10:35:46

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

4.2.3 Switch

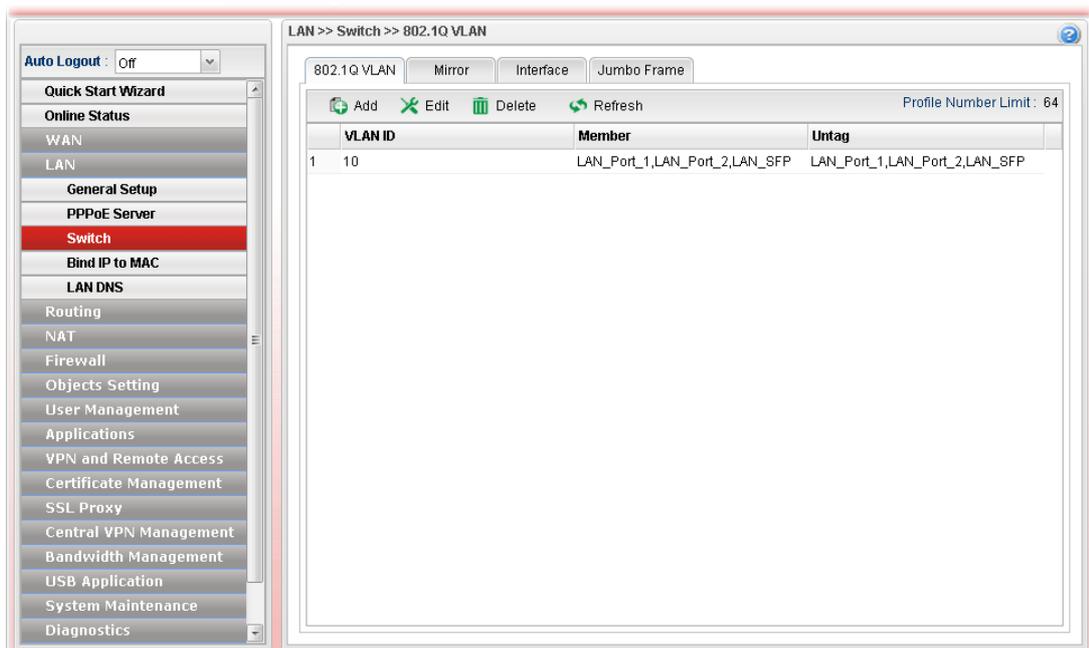
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable LAN interface, and configure 802.1Q VLAN ID for different LAN interfaces, and so on.

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.

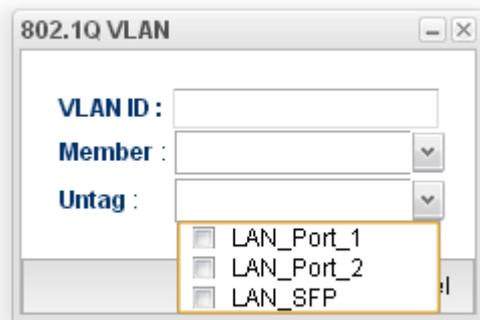


Each item will be explained as follows:

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.

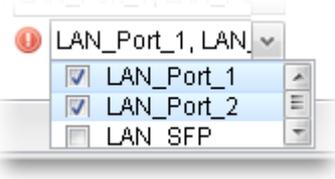
How to add a new 802.1Q VLAN profile

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

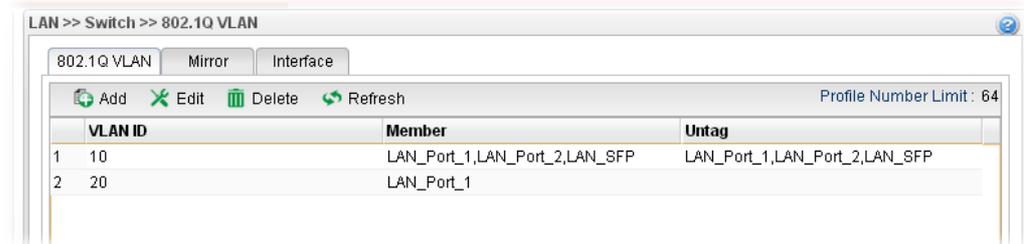


Available parameters are listed as follows:

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.

	<p>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, then return this page and make the selection again.</p> 
Untag	<p>Determine if the packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or not.</p> <p>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, then return this page and make the selection again.</p>
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

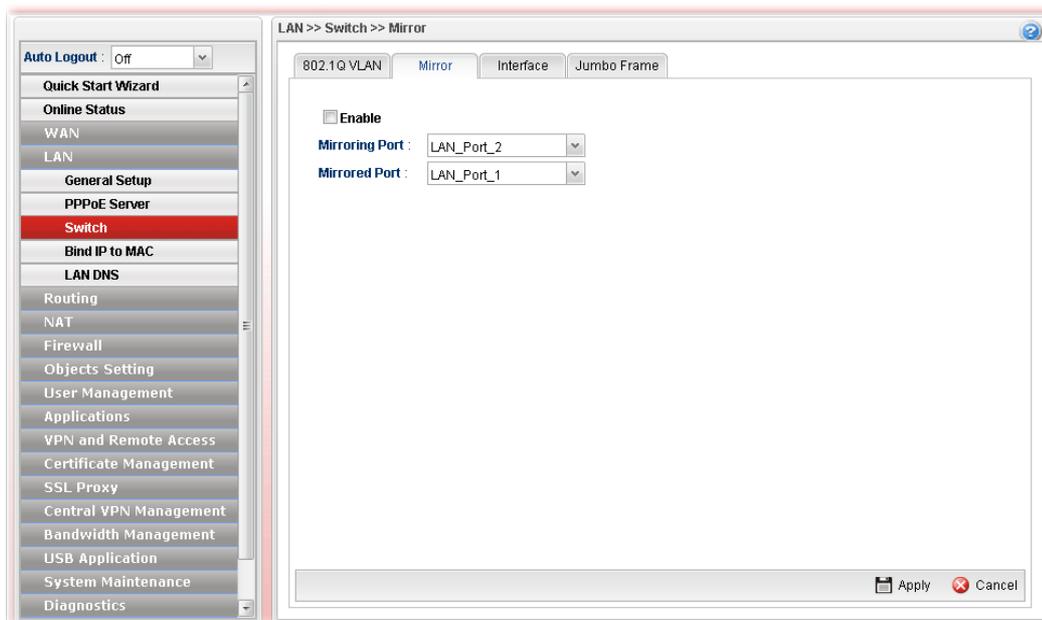
4. Enter all the settings and click **Apply**. The new profile will be added on the screen.



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.

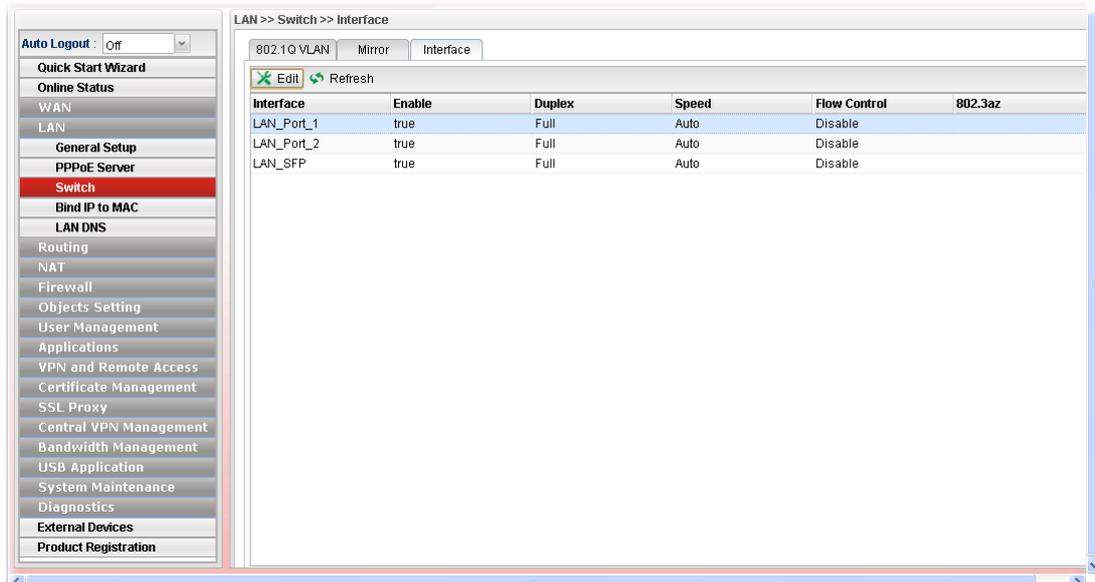


Available parameters are listed as follows:

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. <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> LAN_Port_1 LAN_Port_1 LAN_Port_2 LAN_SFP </div>
Mirrored Port	Select which port is necessary to be mirrored. <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> LAN_Port_1 LAN_Port_1 LAN_Port_2 LAN_SFP </div>
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.

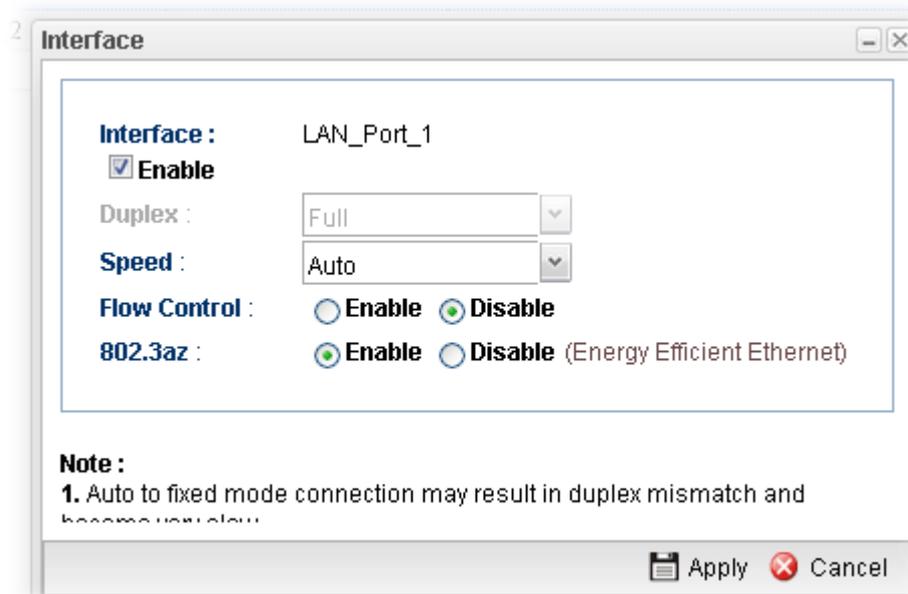


Each item will be explained as follows:

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.



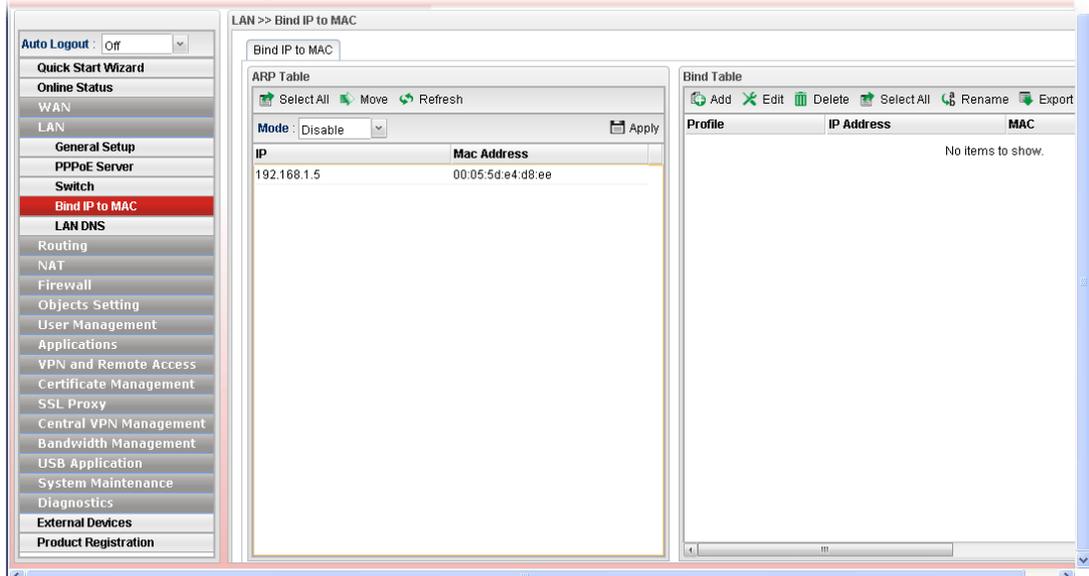
Available parameters are listed as follows:

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 Vigor2960 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 strengthened 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	<p>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.</p> <p>Mode -</p> <ul style="list-style-type: none"> ● 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. <p>Select All - Allow you to choose all the items listed in ARP Table.</p> <p>Move - Move the selected item to IP Bind List.</p> <p>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.</p> <p>IP Address - Display the IP address of one device.</p> <p>MAC Address - Display the MAC address of the device.</p>
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.

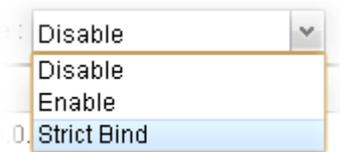
IP Address - Display the IP address specified for the profile.

MAC - Display the MAC address specified for the profile.

Comment – Display the brief description for such profile.

How to configure Bind IP to MAC

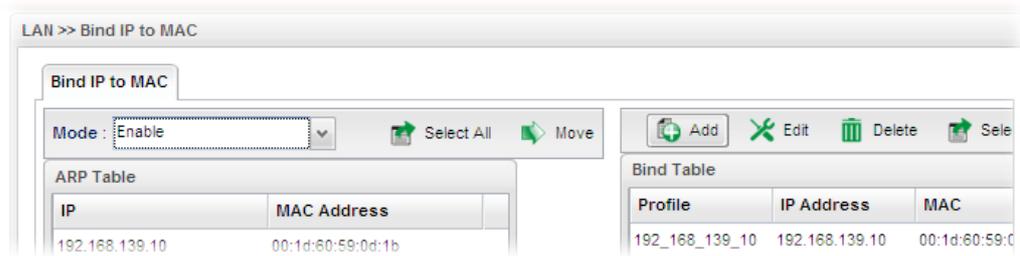
1. Open LAN>>Bind IP to MAC.
2. Use the drop down menu to specify a suitable mode.



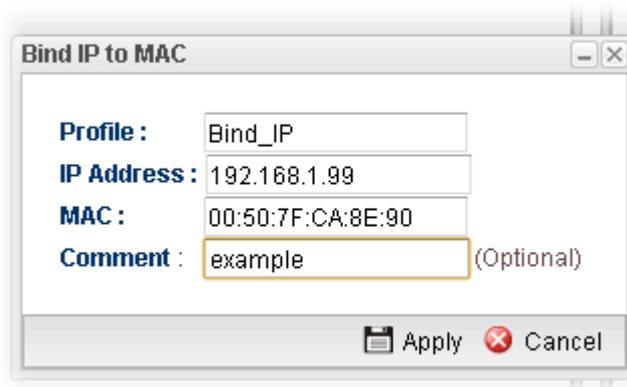
There are three modes offered for you to choose.

- **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**.



4. The following dialog appears.



Available parameters are listed as follows:

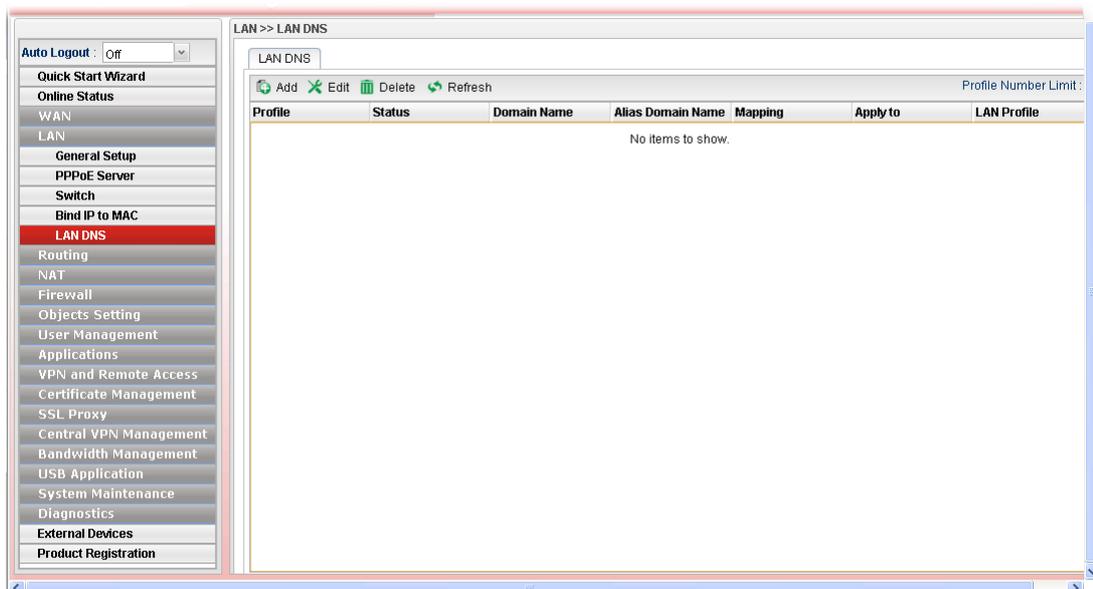
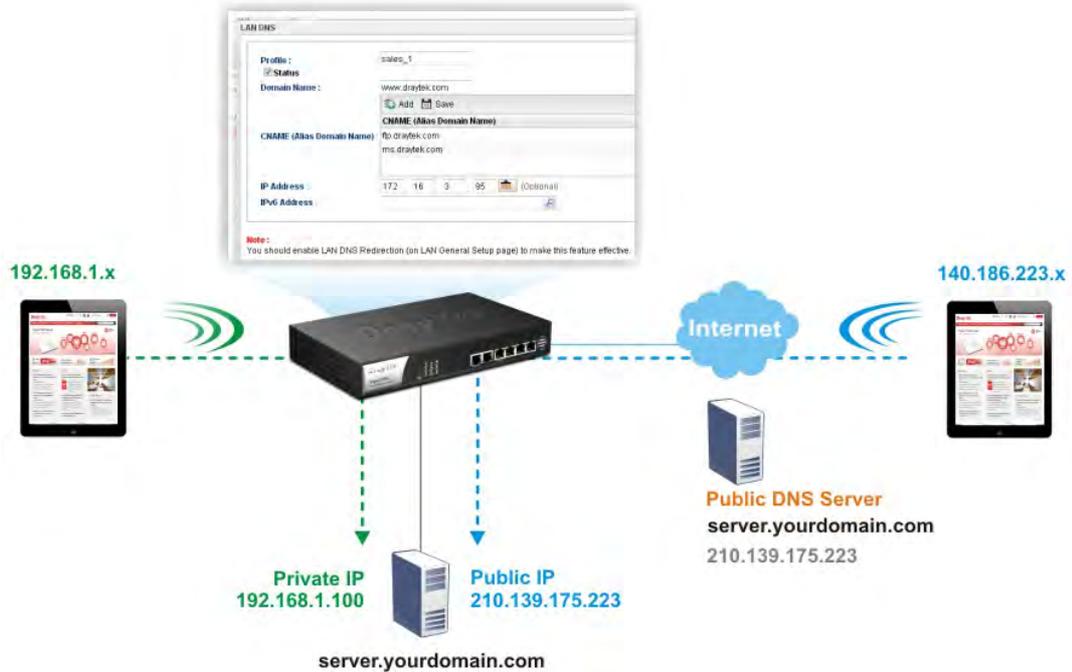
Item	Description
Profile	Type the name of the profile.
IP Address	Type the IP address that will be used for the specified MAC address.
MAC	Type the MAC address that is used to bind with the assigned IP address.
Comment	Type a brief description for such profile.
Apply	Click it to save and exit the dialog.
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.



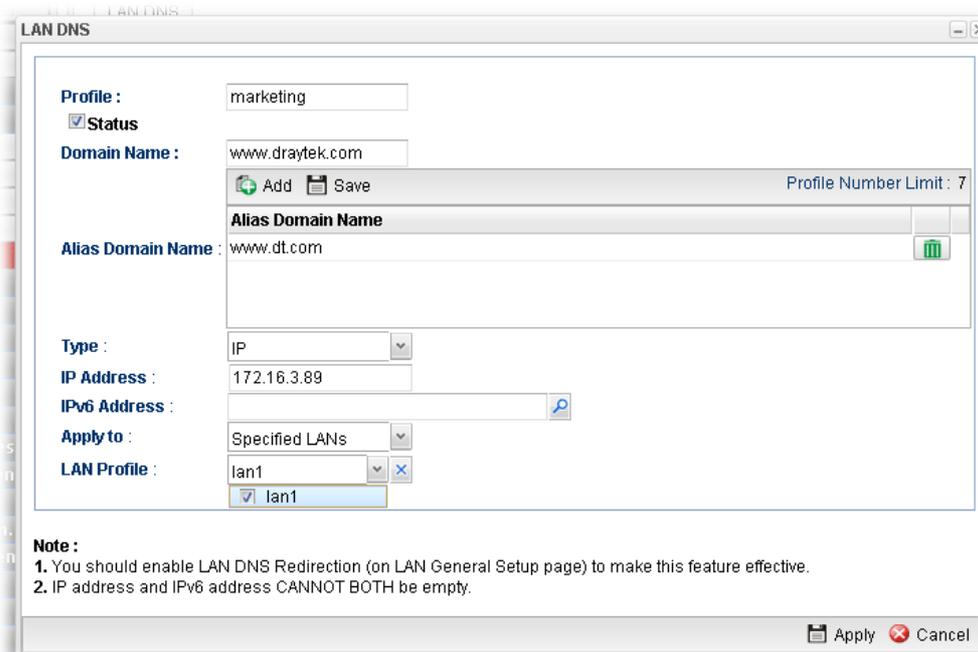
Each item will be explained as follows:

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.



LAN DNS

Profile : marketing

Status

Domain Name : www.draytek.com

Add Save Profile Number Limit : 7

Alias Domain Name : www.dt.com

Type : IP

IP Address : 172.16.3.89

IPv6 Address :

Apply to : Specified LANs

LAN Profile : lan1

Note :

1. You should enable LAN DNS Redirection (on LAN General Setup page) to make this feature effective.
2. IP address and IPv6 address CANNOT BOTH be empty.

Apply Cancel

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.

Status	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.
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.
Applied to	LAN DNS can be applied to specified LAN interfaces or all of the LAN interfaces. LAN Profile – When you choose Specified LANs , 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.

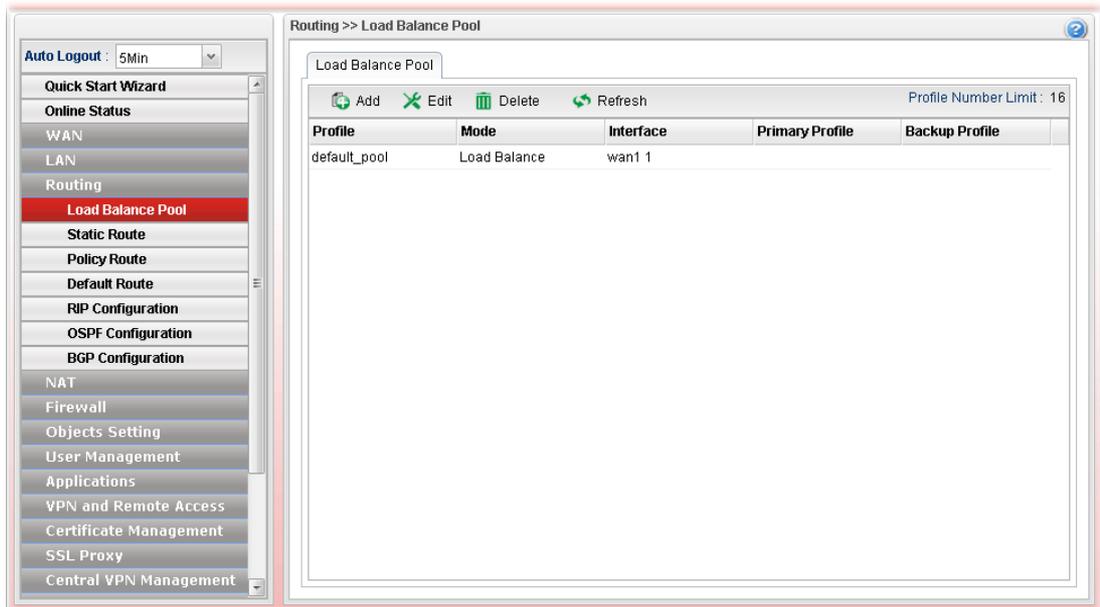


4.3.1 Load Balance Pool

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:

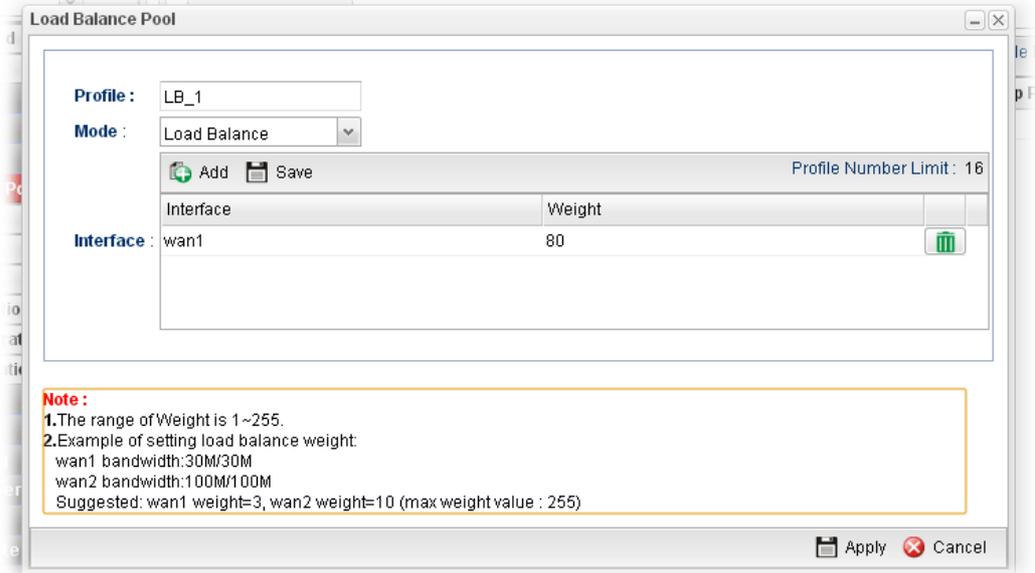
Item	Description
Add	Add a new pool profile.
Edit	Modify the selected pool profile.

	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

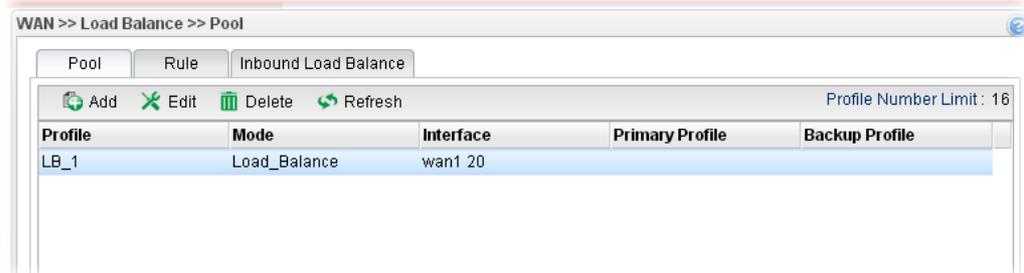
1. Open **Routing>>Load Balance Pool**.
2. Simply click the **Add** button to open the following dialog. Type a name (e.g., LB_1) for such profile.



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 Failover

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 **Failover** as the **Mode** selection.

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Mode	Choose Failover 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.

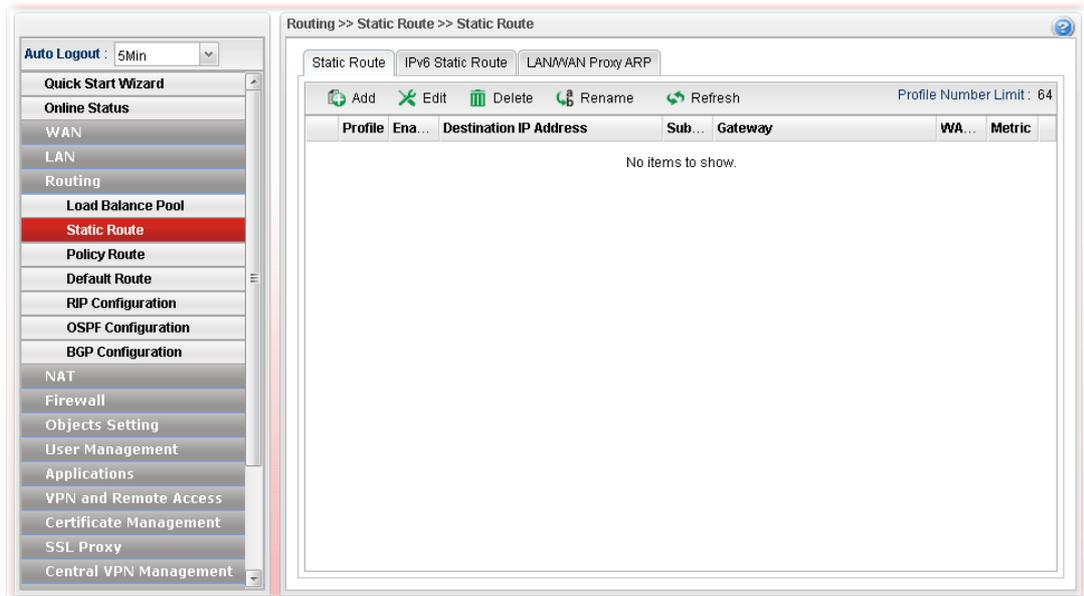
3. Click **Apply**. A new profile will be added on the page.

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.

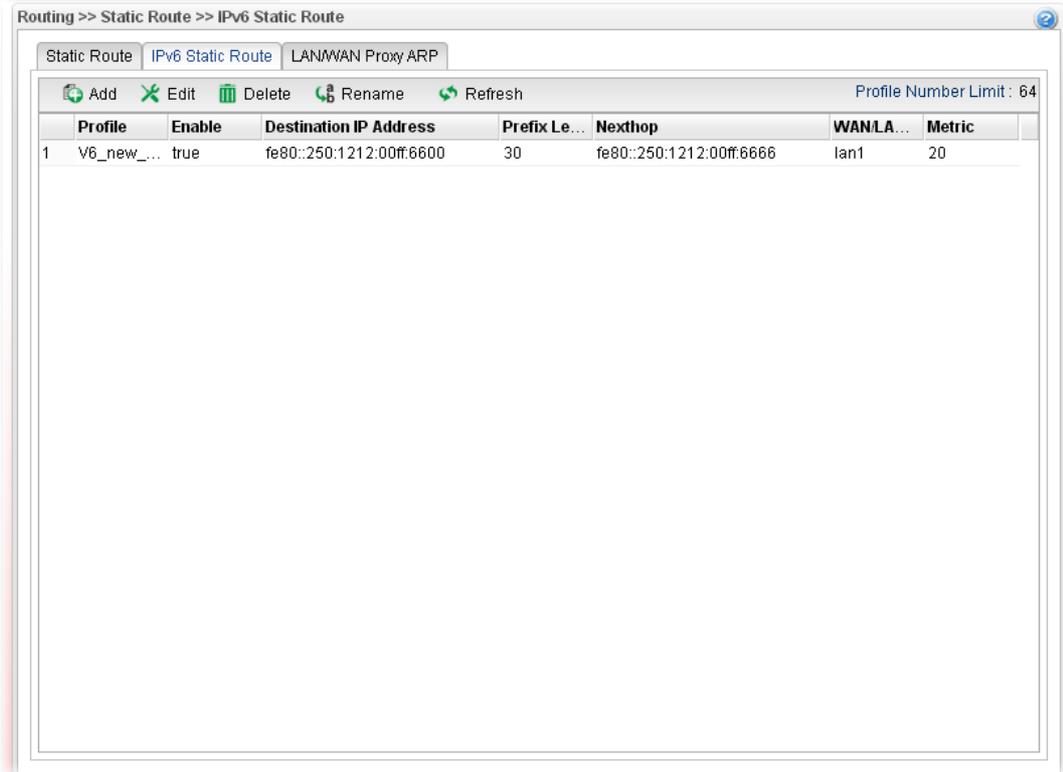
Available parameters are listed as follows:

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:

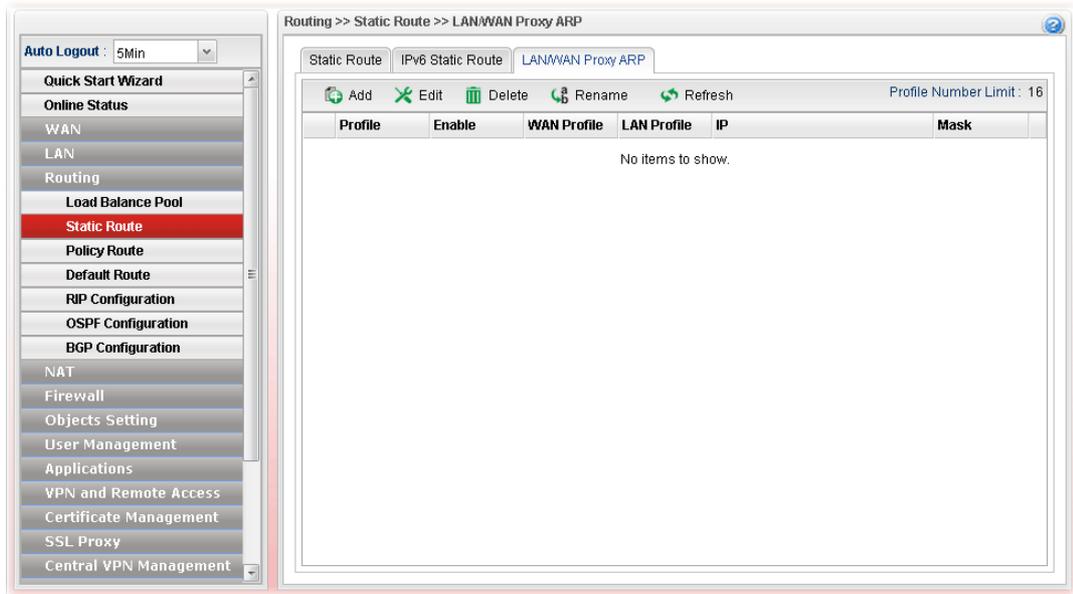
Item	Description
Profile Name	Type the name of the static route profile.
Enable	Check this box to enable such profile.
Destination IP Address	Type the IP address for such static route profile.
Prefix Length	Type the prefix length for such profile.
Nexthop	Type the nexthop address for such static route 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.

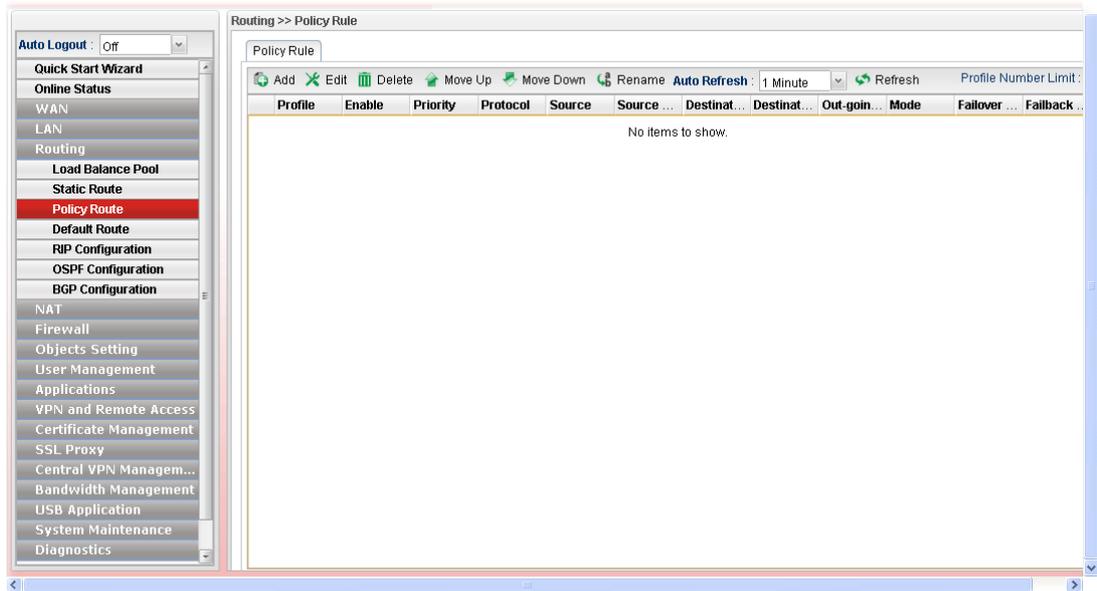
- **Address Mapping.**

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.
Protocol	Display the protocol of such rule.
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.

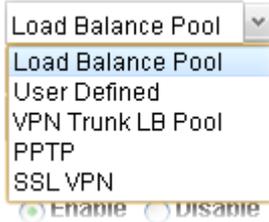
How to add a new policy rule

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.
Source	Source Type - Choose the address type (Any, Subnet or Object) for such rule.

	<div data-bbox="683 197 976 340"> </div> <p>Each type will bring different settings for configuration.</p> <hr/> <p>When Subnet is selected as Source Type</p> <ul style="list-style-type: none"> ● 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. <hr/> <p>When Object is selected as Source Type</p> <ul style="list-style-type: none"> ● 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.
<p>Destination</p>	<p>Destination Type - Choose the address type (Any, Subnet, Object or Country) for such rule.</p> <div data-bbox="683 900 951 1070"> </div> <p>Each type will bring different settings for configuration.</p> <hr/> <p>When Subnet is selected as Destination Type</p> <ul style="list-style-type: none"> ● 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. <hr/> <p>When Object is selected as Destination Type</p> <ul style="list-style-type: none"> ● 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. <hr/> <p>When Country is selected as Destination Type</p> <ul style="list-style-type: none"> ● Country Object - Use the drop down list to choose the country object(s) for such rule profile.
<p>Route Rule</p>	<p>Out-going Rule - It determines the way (interface) that the incoming traffic will be forwarded to.</p>



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 an 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.

	<ul style="list-style-type: none"> ● 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.
	<hr/> <p>When PPTP selected as Out-going Rule</p> <hr/>
	<ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ◆ 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: <p>Out-going Rule : User Defined Out-going interface : wan1 Failover : Enable when target [8.8.8.8] ping [Fail] for [5] seconds</p> 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.
	<hr/> <p>When SSL VPN selected as Out-going Rule</p> <hr/>
	<ul style="list-style-type: none"> ● SSL Profile – VPN SSL profiles can be selected by such policy route. ● Mode – Specify which mode (NAT or Routing)

	<p>will be used for such route rule.</p> <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ◆ 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: <p>Out-going Rule : User Defined Out-going interface : wan1 Failover : Enable when target [8.8.8.8] ping [Fail] for [5] seconds</p> 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).

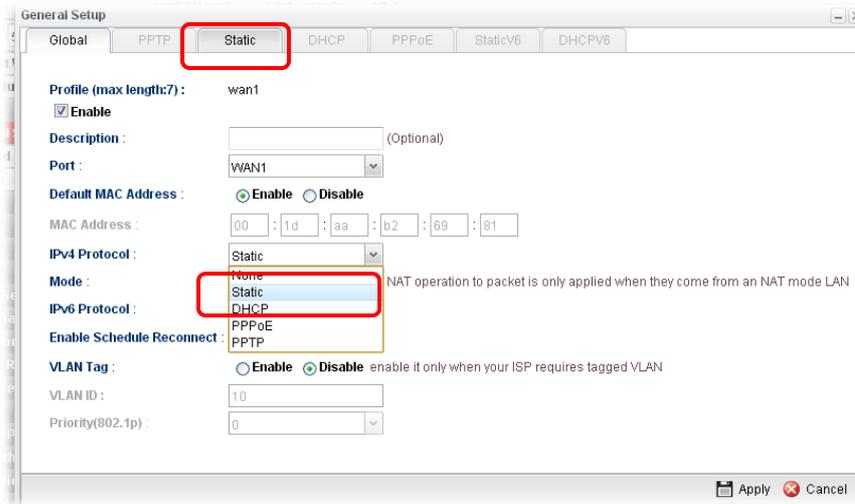
With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2)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

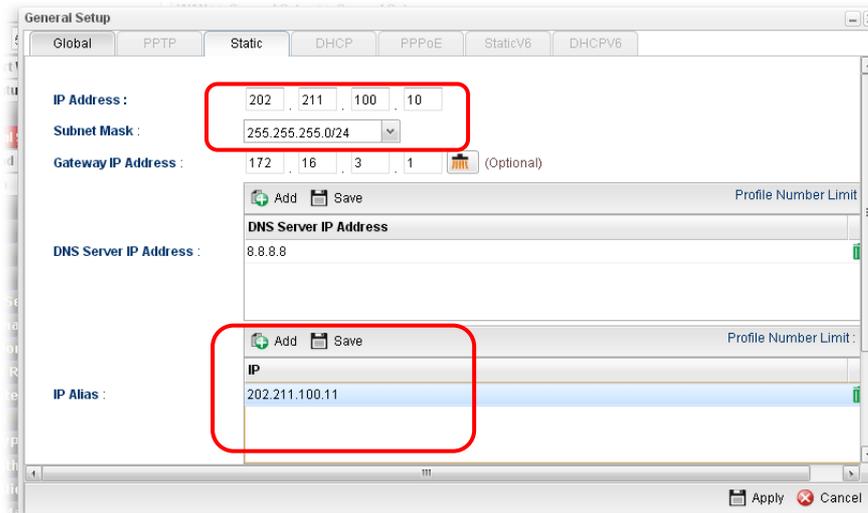
We will take an example to introduce how to make use of this feature.

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**.

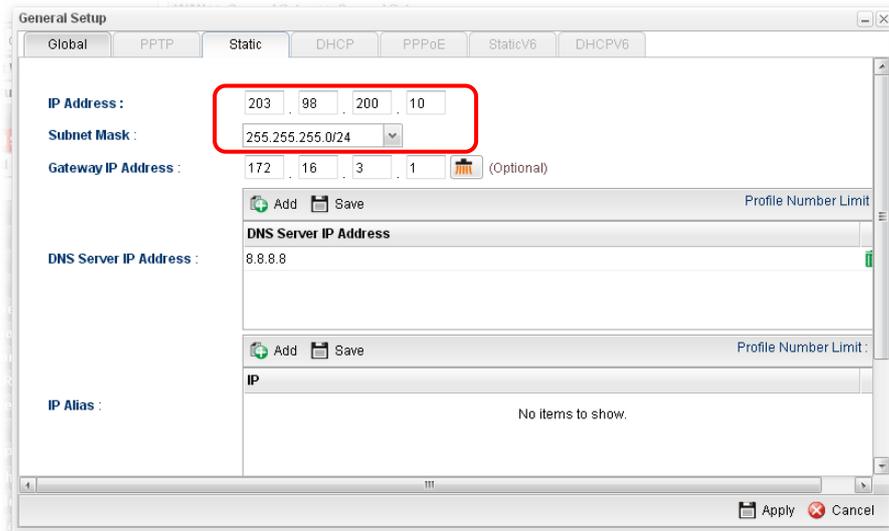


3. From the following page, set main WAN IP address as *202.211.100.10*.

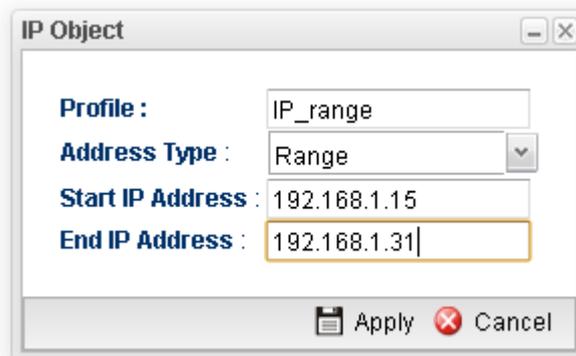


Click **Add** on IP Alias to configure the other IP address which is *202.211.100.11*.

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**>>**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.

- 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.

Policy Rule

Profile : Rule_WAN1

Enable

Priority : Normal

Protocol : ALL

Source

Source Type : Object

IP Object : IP_range

IP Group :

Destination

Destination Type : Any

Route Rule

Out-going Rule : Load Balance Pool

Load Balance Rule : wan1

Mode : NAT

Use IP Alias : Enable Disable

Failover to Next Rule : Enable Disable

when interface down

when target ping Fail for 3 seconds

Failback (Quick Recover) : Enable Disable

Apply Cancel

And,

Policy Rule

Profile : Rule_WAN2

Enable

Priority : Normal

Protocol : ALL

Source

Source Type : Subnet

IP Address : 192.168.1.100

Subnet Mask : 255.255.255.0/24

Destination

Destination Type : Any

Route Rule

Out-going Rule : Load Balance Pool

Load Balance Rule : wan1

Mode : NAT

Use IP Alias : Enable Disable

IP Alias : 202.211.100.11

Failover to Next Rule : Enable Disable

when interface down

when target ping Fail for 3 seconds

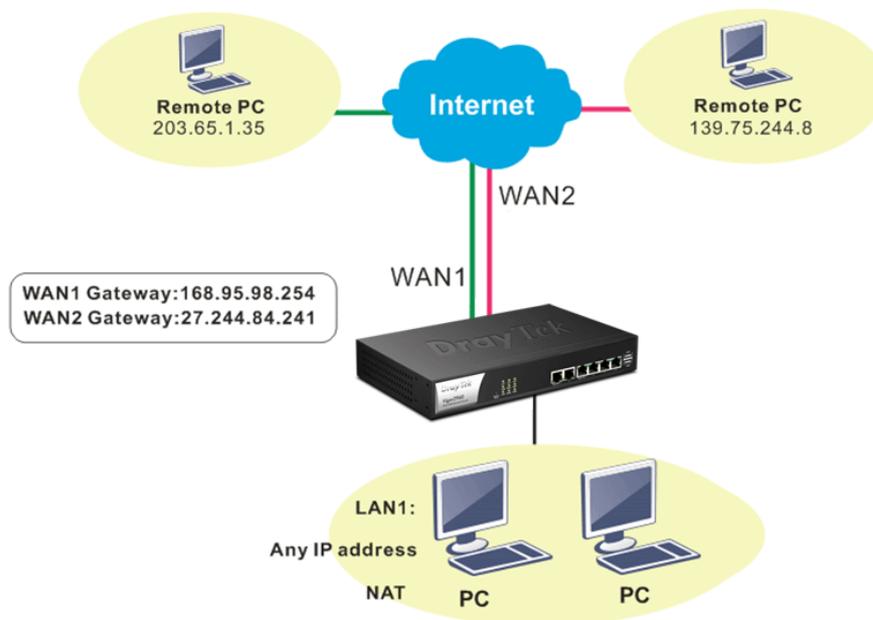
Apply Cancel

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

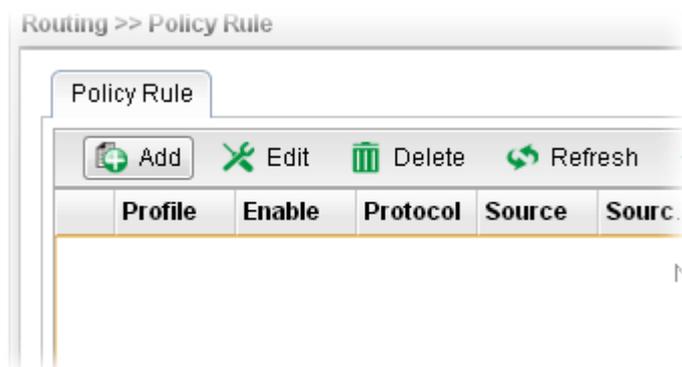
Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

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.



- 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**.

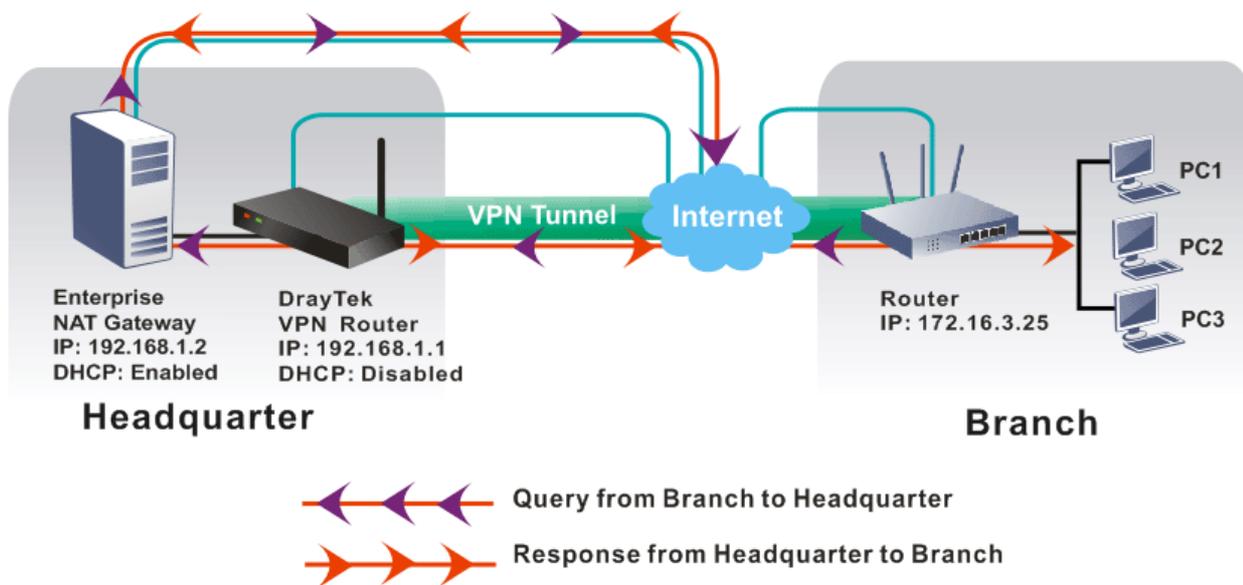
- After finished the above settings, click **Apply** to save the configuration.

	Profile	Enable	Protocol	Source	So...	Destination	De...	Out-go...	Mode
1	Rule_WAN1	true	ALL	[IP] IP_range	-	Any	-	wan1	NAT
2	Rule_WAN2	true	ALL	192.168.1.100/24	-	Any	-	wan1	NAT w
3	Special_1	true	ALL	Any	-	203.65.1.35/24	-	wan1	NAT

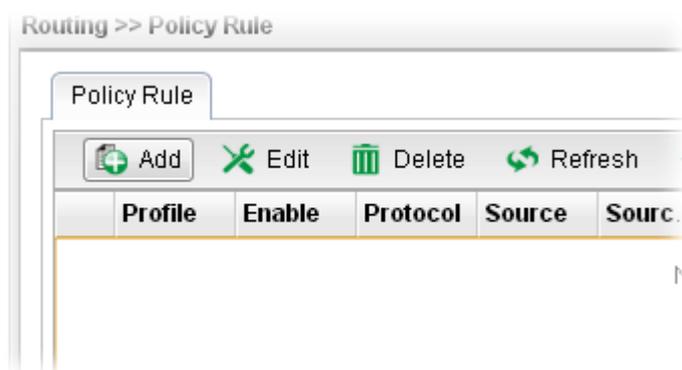
Now, any packets from LAN1 sent to the remote PC (IP address: 203.65.1.35) will be forcefully to pass through WAN1.

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.



- 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 **Ian1** as the **Out-going Interface**; type 192.168.1.2 as the **Out-going (Gateway)**; and click **Disable** for **Failover to Next Rule**.

Policy Rule configuration window showing the following settings:

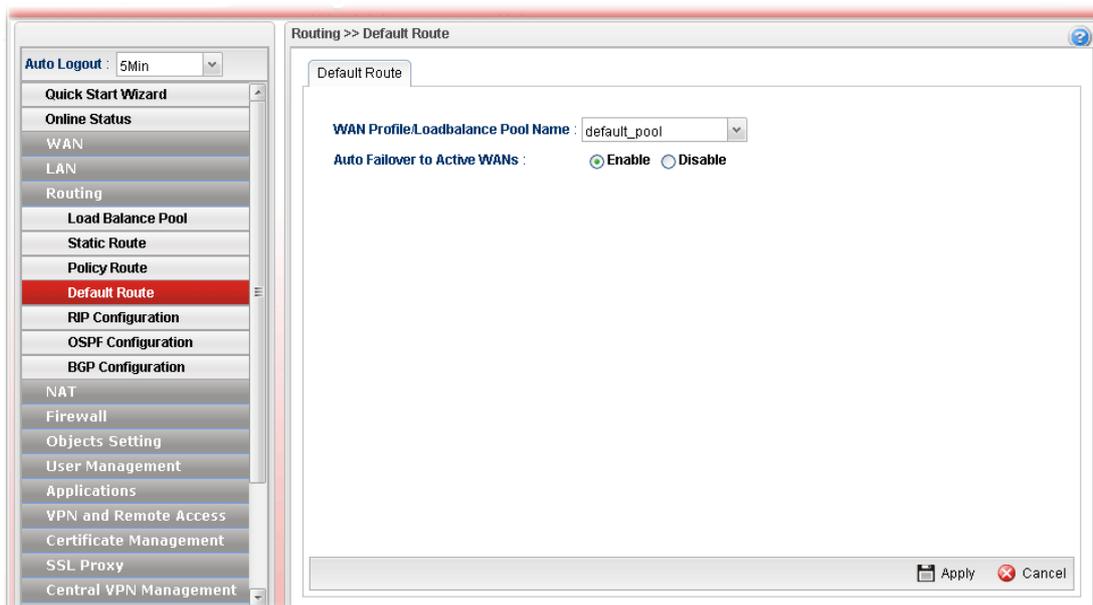
- Profile: Secure_route
- Enable
- Priority: Normal
- Protocol: ALL
- Source Type: Subnet
- IP Address: 172.16.3.25
- Subnet Mask: 255.255.255.0/24
- Destination Type: Any
- Out-going Rule: User Defined
- Out-going Interface: lan1
- Out-going (Gateway): 192.168.1.2 (Optional)
- Mode: Routing
- Failover to Next Rule:
 - when interface down
 - when target ping Fail for 3 seconds

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

Profile	Enable	Proto...	Source	Source...	Destin...	De...	Out-going Rule	Mode	Failove...
1 Secure...	true	ALL	192.168.1.0/24	-	Any	-	Ian1 GW:192.168.1.2	ROUTING	Disable

4.3.4 Default Route

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



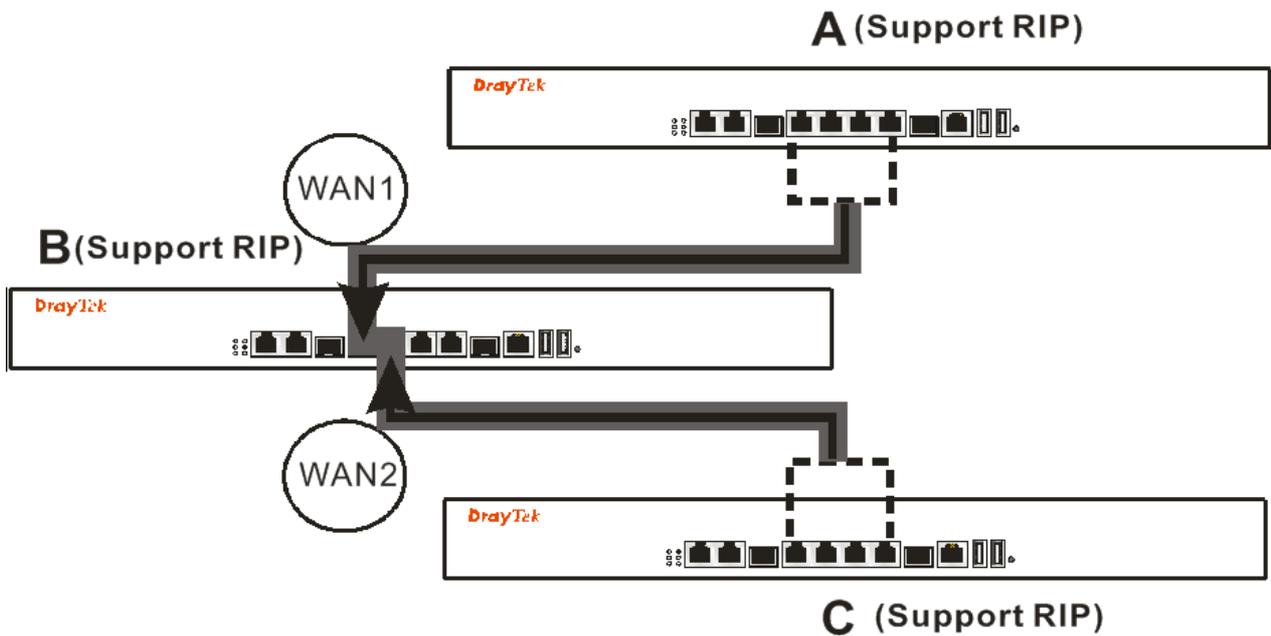
Available parameters are listed as follows:

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.
Apply	Click it to save the configuration.
Cancel	Discard current page modification.

4.3.5 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.

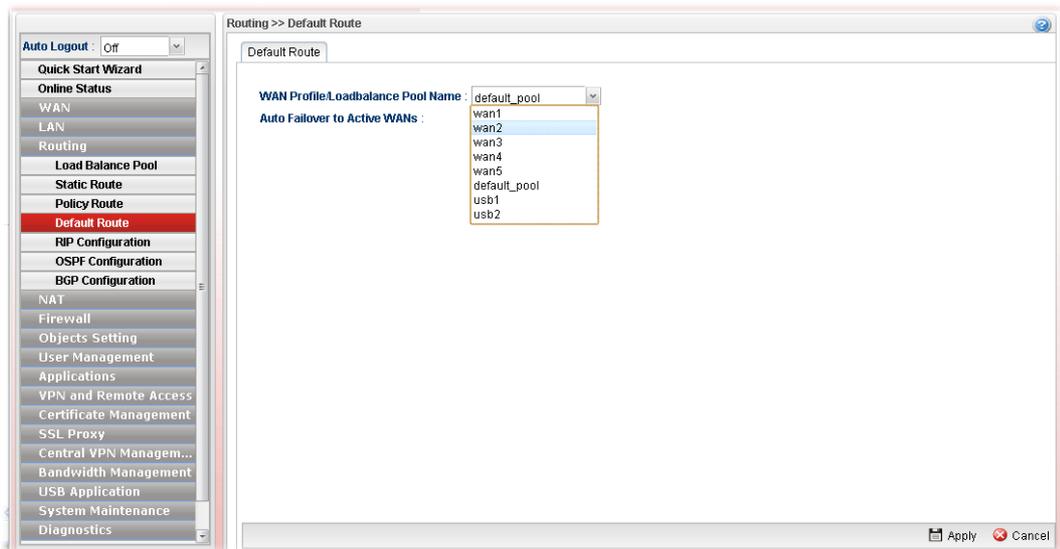
RIP can update the routing table automatically and find a route to send packet. See the following figure as an example:



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.

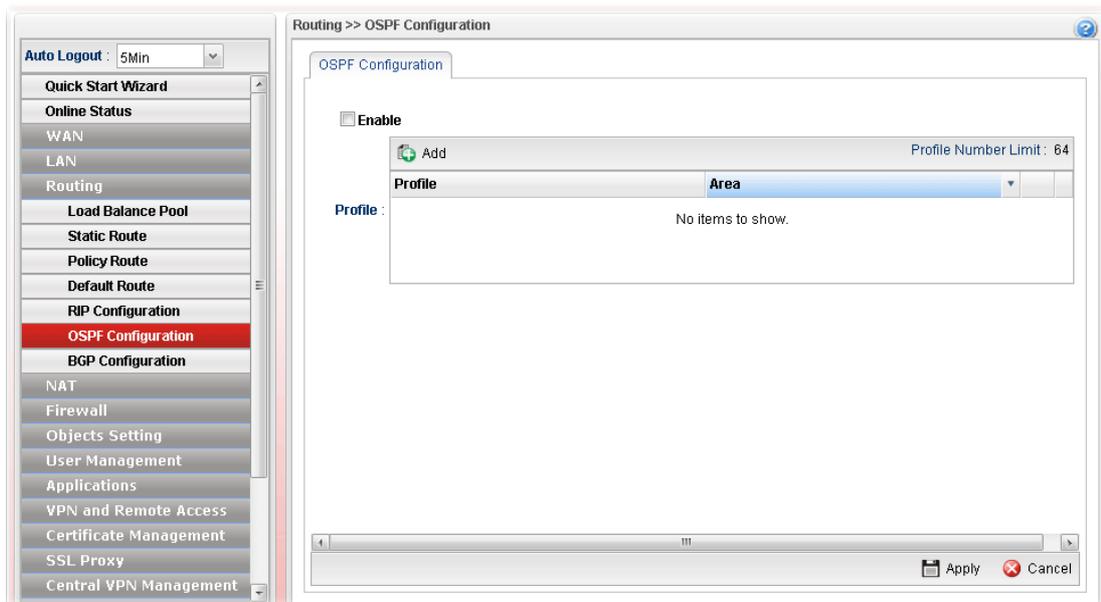
After finished the settings, click **Apply** to save them.

4.3.6 OSPF Configuration

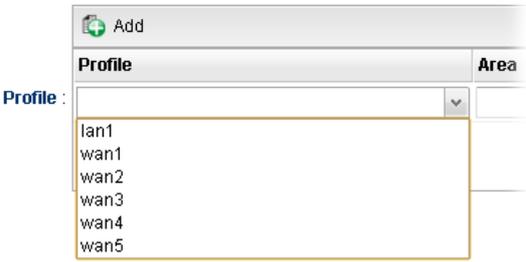
OSPF (Open Shortest Path First) uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor 2960 supports up to OSPF version 2(only for IPv4).

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.
Profile	<p>Add- Click it to create a new profile.</p> <p><input type="checkbox"/> Enable</p>  <p>Profile - Choose a LAN/WAN profile from the drop down list to apply for such configuration.</p> <p>Area – An AS will be divided into several areas. Each area must be assigned with a dedicated number.</p> <p>Note: For the detailed information of OSPF application, refer to section “3.2 How to Configure OSPF?”.</p>
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. Click the space of **Profile**. A pop-up dialog will appear. Click **Add**.

Enable

Add Profile Number Limit : 64

Profile	Area	
lan1		
lan1es1		
wan1		
wan2		
wan3		
wan4		
wan5		

- 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

Add Profile Number Limit : 64

Profile	Area	
lan1es1	30	

If you are not satisfied the settings, simply click to remove the entry, and then re-type the settings.

- Click **Apply** to save the settings and exit the dialog. A new profile is created and displayed on the screen.

Enable

Add Profile Number Limit : 64

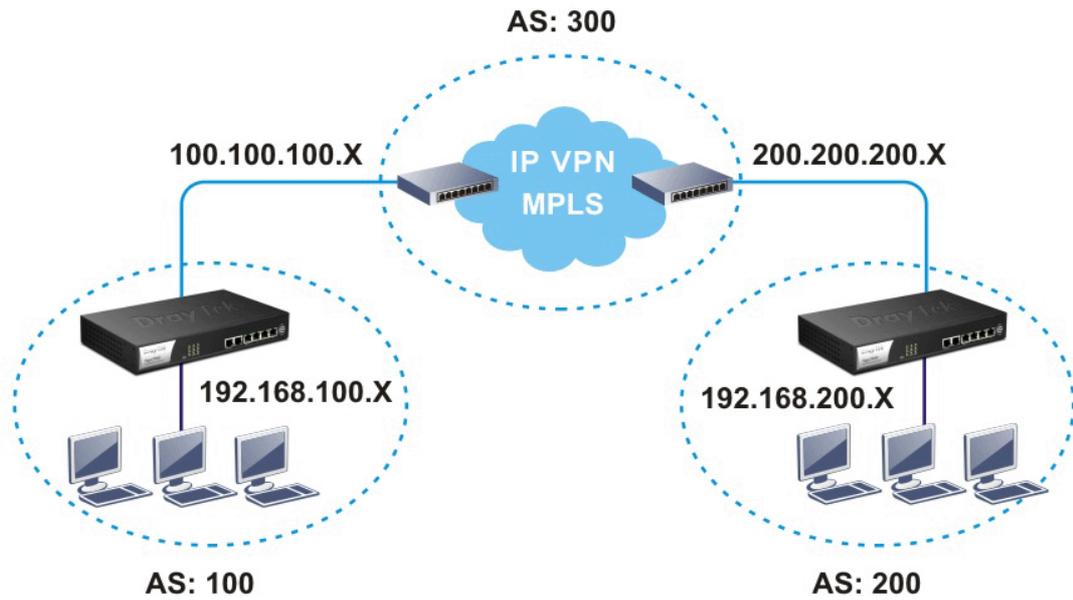
Profile	Area	
lan1es1	30	

4.3.7 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.

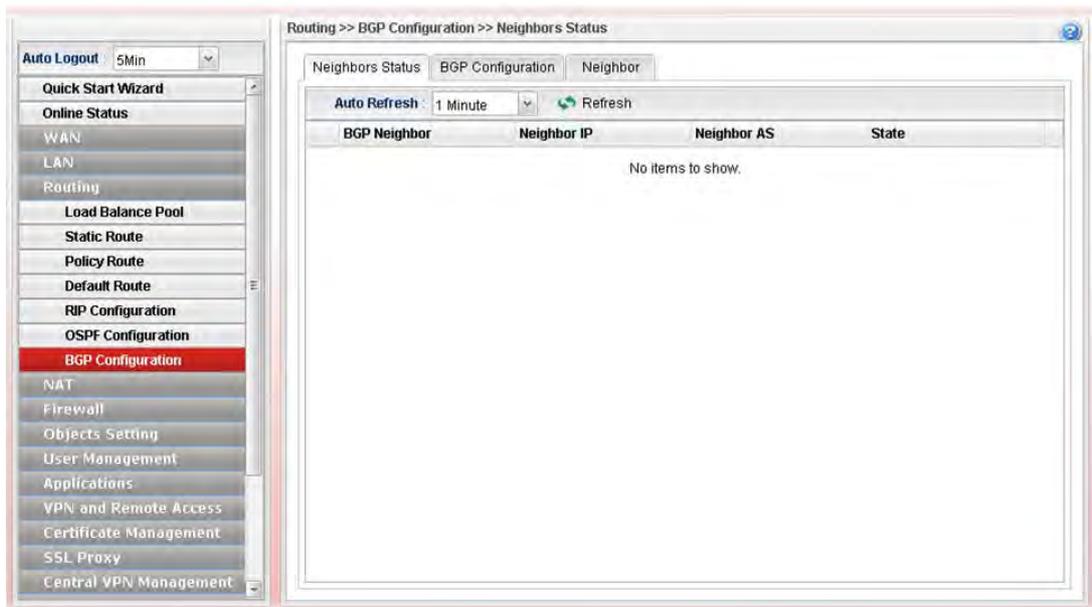
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the “neighbor” of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

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.

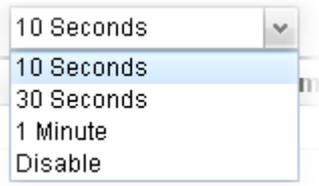


4.3.7.1 Neighbors Status

Such page displays current neighbors status in BGP routing environment.

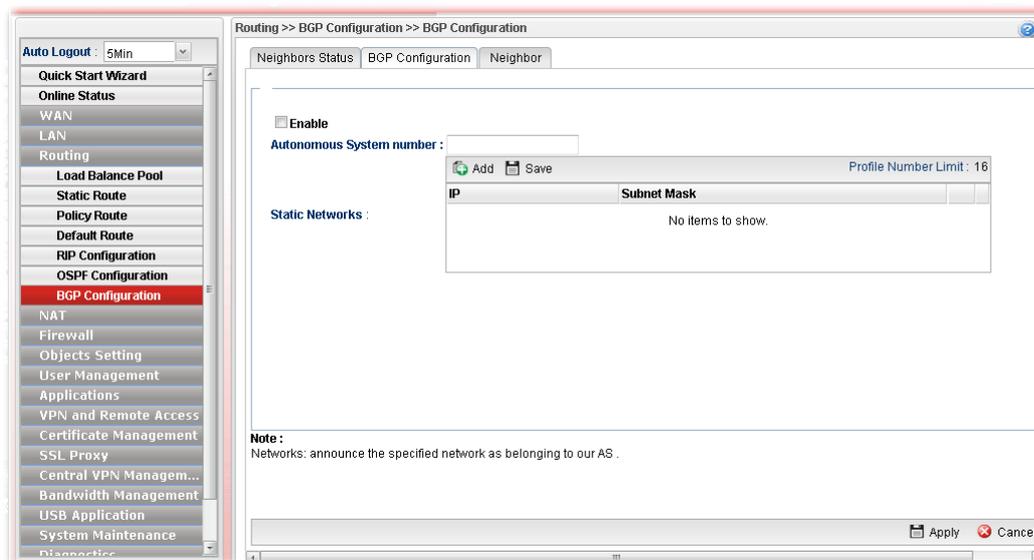


Available parameters are listed as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	<p>Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.</p> 
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.

4.3.7.2 BGP Configuration

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



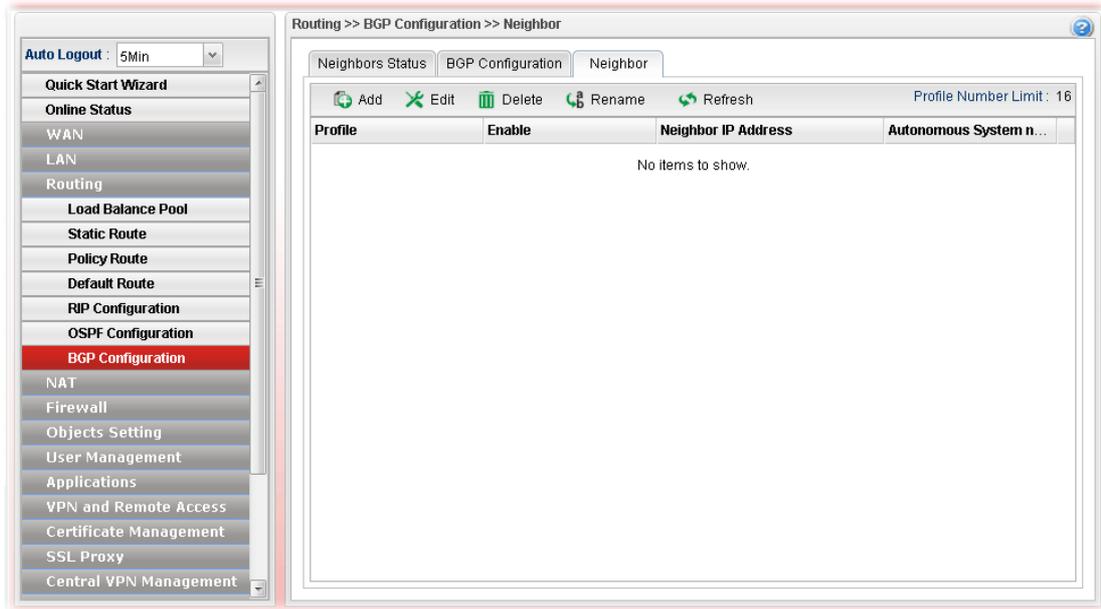
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable BGP function.
Autonomous System number	Type the autonomous system number for the host in BGP application.
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.

4.3.7.3 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.



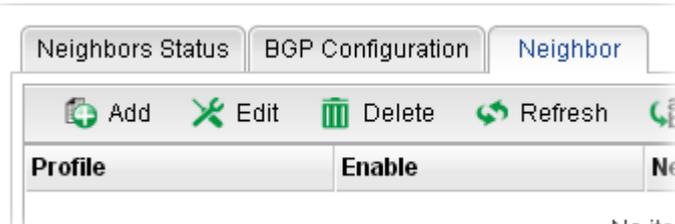
Available parameters are listed as follows:

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. <div data-bbox="686 1518 1220 1809" data-label="Image"> </div> <p>Before using such function, there is one profile existed at least.</p>
Refresh	Renew current web page.
Profile	Display the name of the profile.

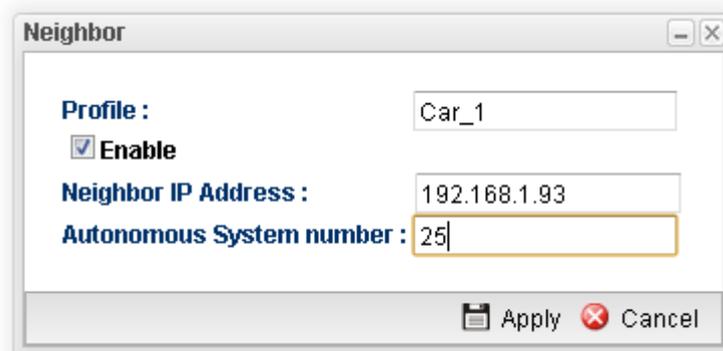
Enable	Display the status of the profile. False means disabled; True means enabled.
Neighbor IP Address	Display the IP address of the neighbor.
Autonomous System Number	Display the autonomous system number of the neighbor in BGP application.

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.



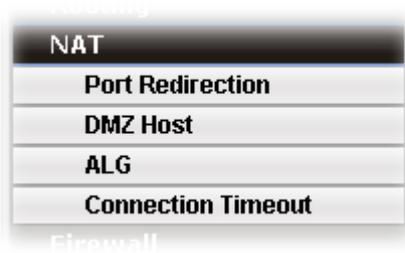
Available parameters are listed as follows:

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.
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.

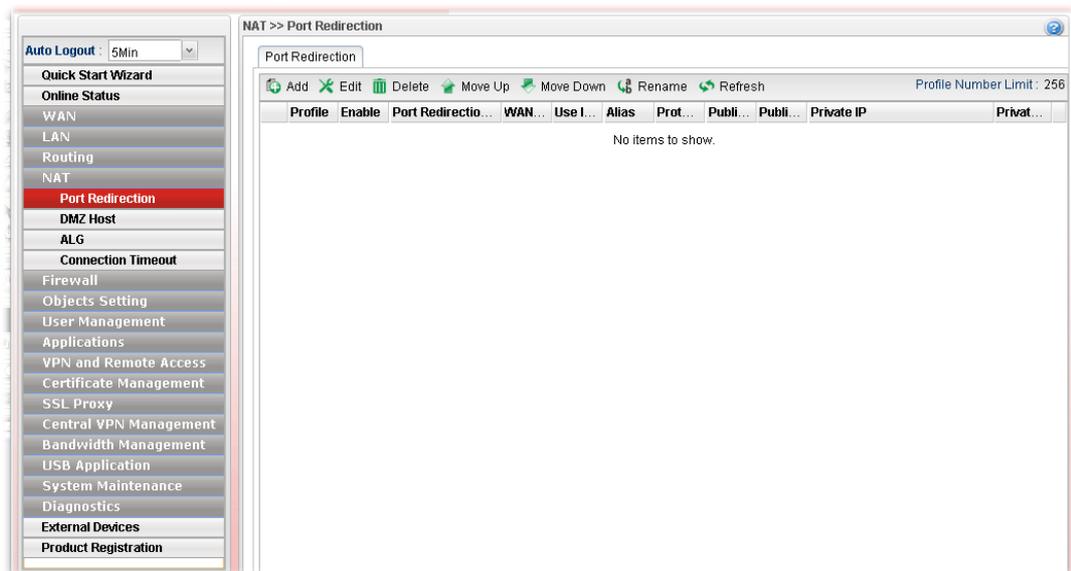
4.4 NAT

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	<p>Modify the selected profile.</p> <p>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.</p>
Delete	<p>Remove the selected profile.</p> <p>To delete a profile, simply select the one you want to delete and click the Delete button.</p>
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	<p>Allow to modify the selected profile name.</p> 
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 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.
Private IP	Display the private IP used for this entry.
Protocol	Display the protocol used for the entry.
Port Redirection Mode	Display the direction for the port to be redirected.
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:

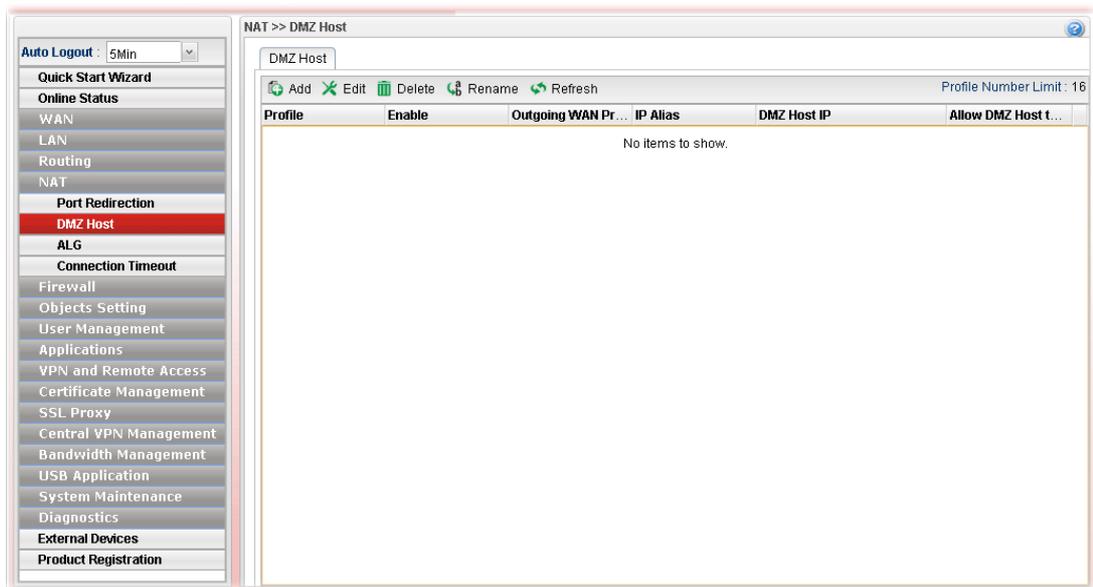
Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Port Redirection Mode	Specify the direction for the port to be redirected. <div style="border: 1px solid black; padding: 2px;"> One to One Range to One Range to Range(p... Range to Range(IP) </div>
WAN Profile	Specify the WAN profile for such profile. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> usb1 All wan1 wan2 wan3 wan4 wan5 usb1 usb2 </div>
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. <div style="border: 1px solid black; padding: 2px; margin-top: 10px;"> No Single Alias All </div> <p>Single Alias – You have to type one IP address used for IP Alias.</p> <p>All – All the IP address can be treated as IP Alias.</p>

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. 
Public Port Start/ Public Port End	It is available when Range to One (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.
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 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.



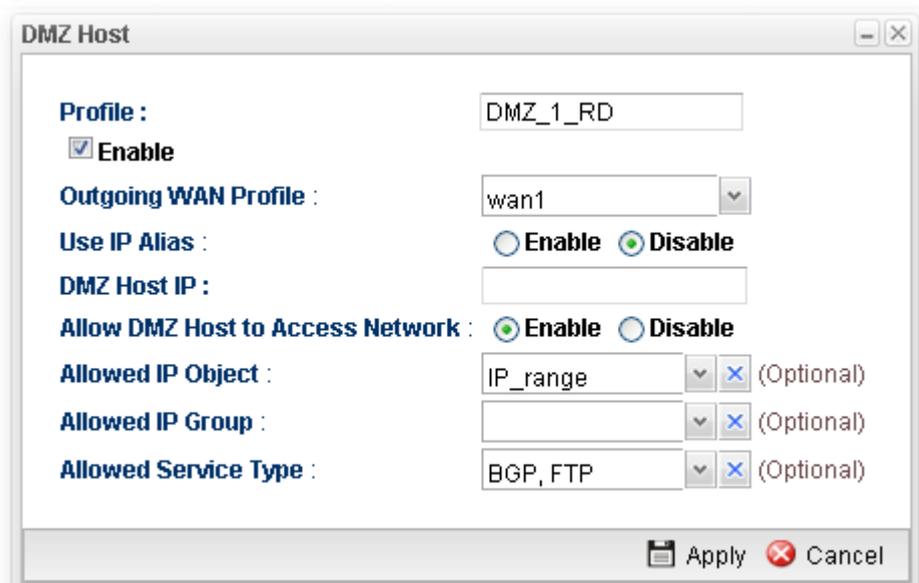
Each item will be explained as follows:

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.
Outgoing 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.

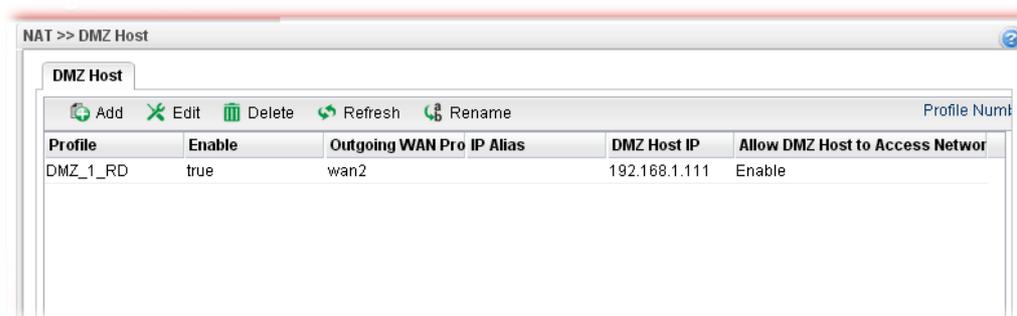


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable the DMZ Host profile.

Outgoing 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 DMS 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.

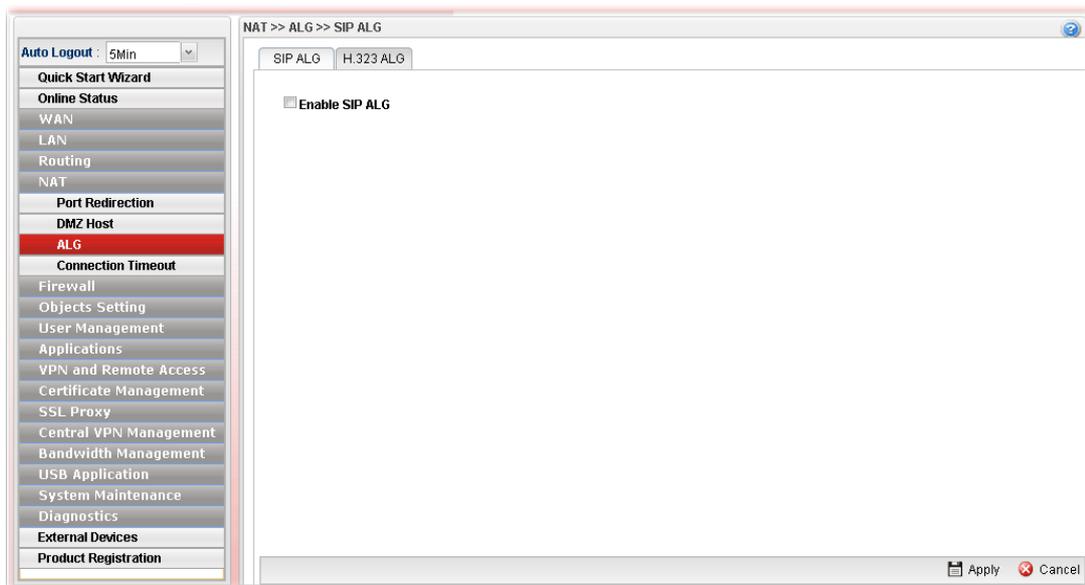
4. Enter all the settings and click **Apply**.
5. A new profile has been added onto **DMZ Host** table.



4.4.3 ALG

4.4.3.1 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.



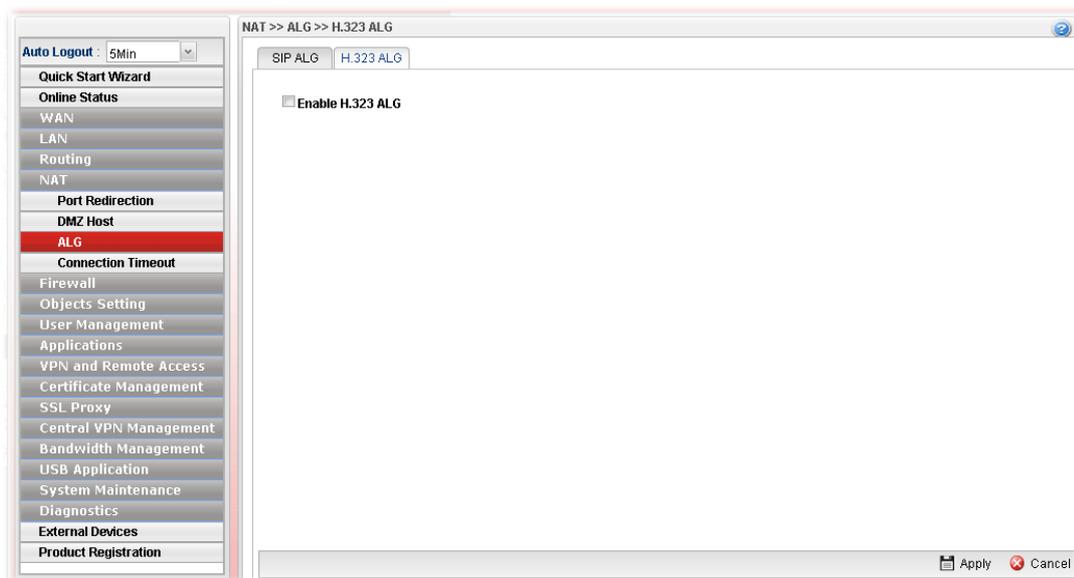
Available parameters are listed as follows:

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.

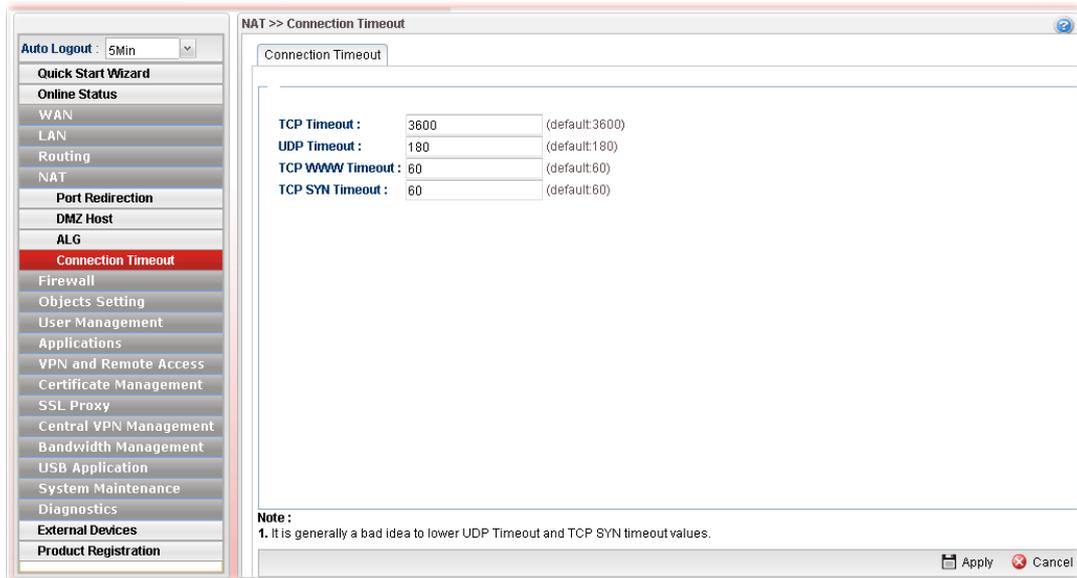
4.4.3.2 H.323 ALG

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.



4.4.4 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:

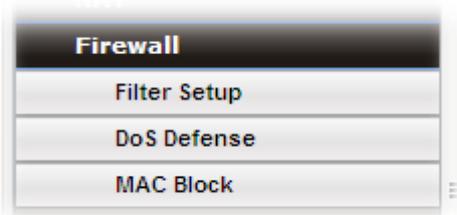
Item	Description
TCP Timeout	Set a time limit for sessions established by TCP (except Port 80 and Port 443).
UDP Timeout	Set a time limit for sessions established by UDP.
TCP WWW Timeout	Set a time limit for sessions established by TCP Port 80 and Port 443.
TCP SYN Timeout	Set a time limit for sessions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

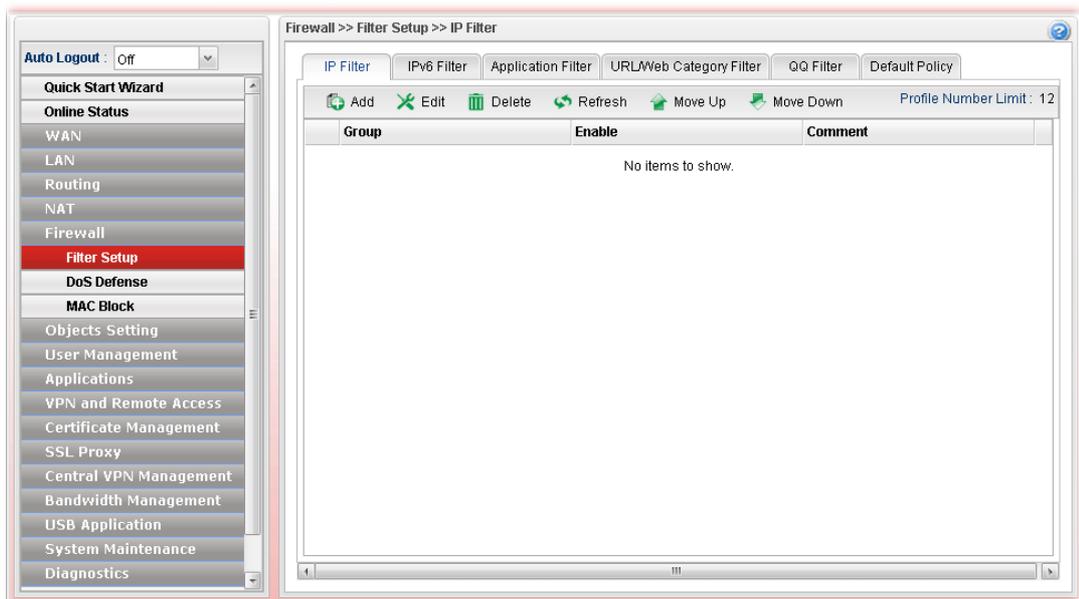


4.5.1 Filter Setup

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:

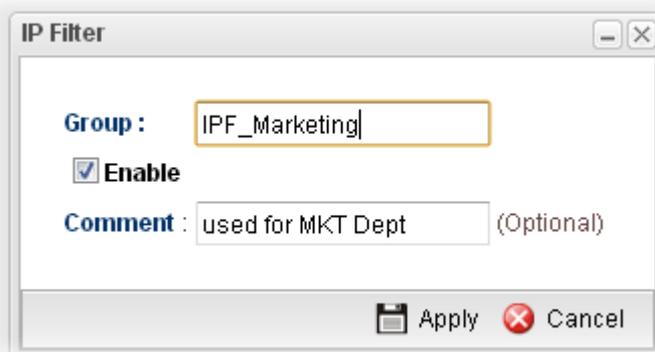
Item	Description
------	-------------

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:

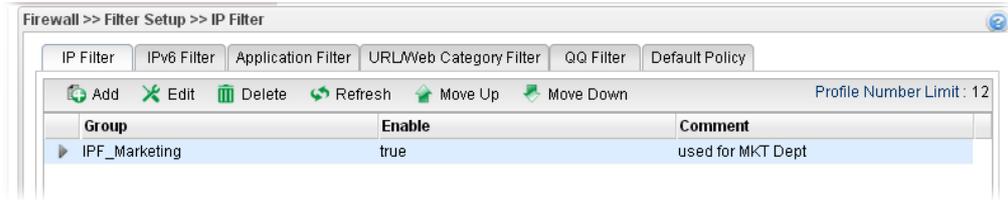
1. Open **Firewall>>Filter Setup** and click the **IP Filter** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.



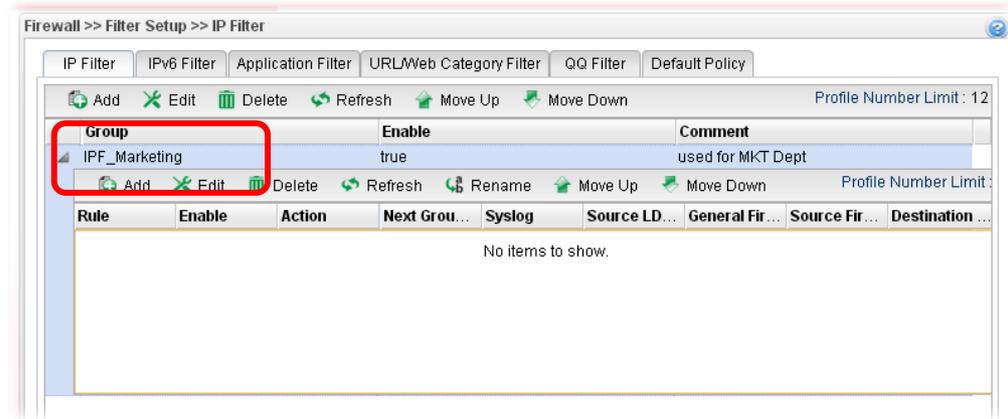
Available parameters are listed as follows:

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.

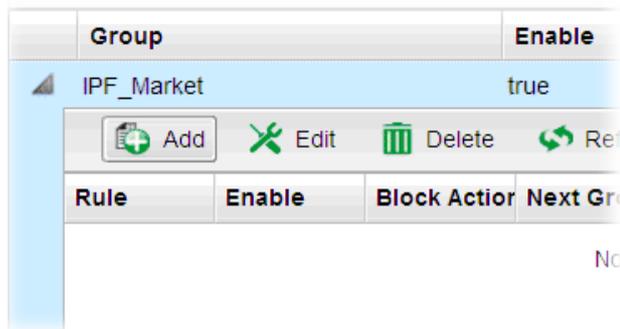
4. Enter all the settings and click **Apply**.
5. A new filter group has been added.



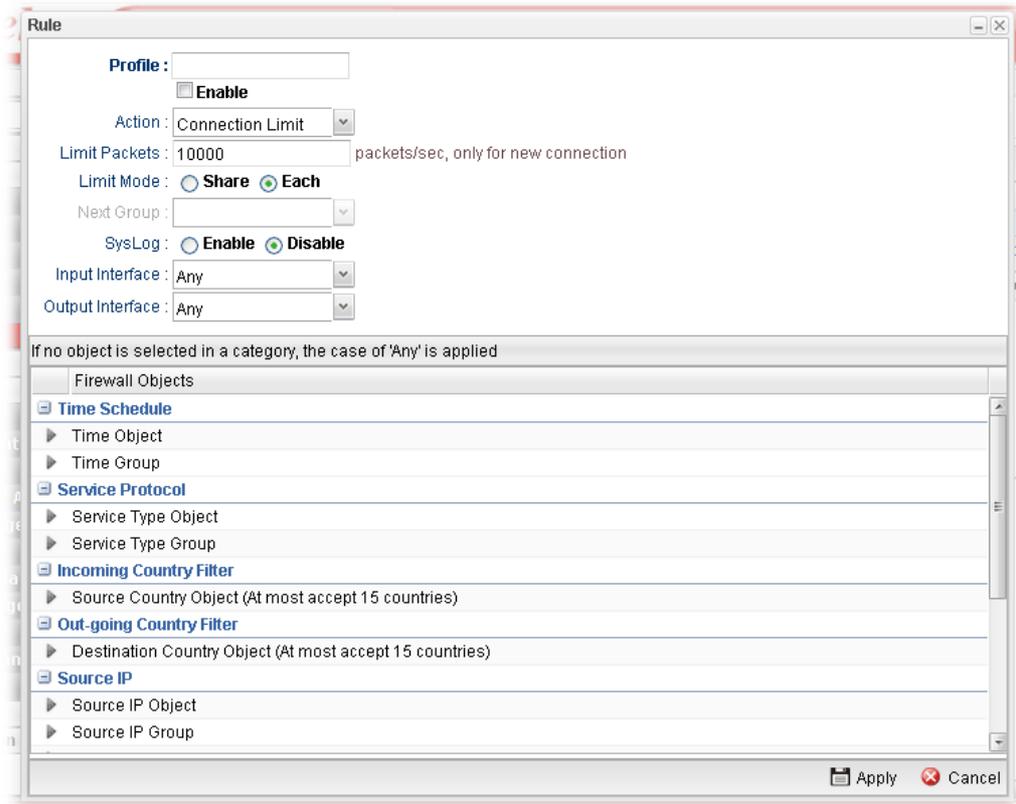
6. You can create filter rule by clicking ▶ on the left side of the selected IP filter group profile. A setting page will appear for you to add new IP filter rule profile.



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

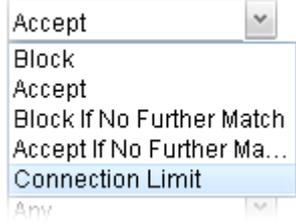
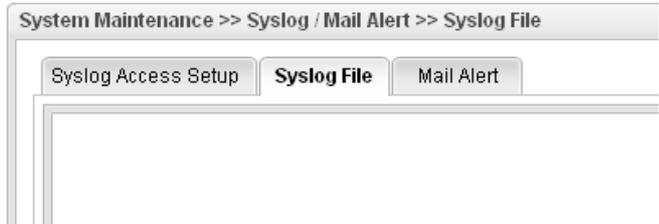


8. The following page for configuration will appear.



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	<p>The action to be taken when packets match the rule.</p> <p>Block - Packets matching the rule will be dropped immediately</p> <p>Accept- Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Accept If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p> <p>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.</p>

	
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 Mode	<p>When you choose Connection Limit as Action, you have to choose Share or Each in addition to the number of packets limits.</p> <p>Share – It means the total IP addresses in a segment will be limited with certain packets number per second.</p> <p>Each –It means each IP will be limited with certain packets number per second.</p>
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	<p>Click Enable to make the history of firewall actions appearing on the System Maintenance >> Syslog/Mail Alert >> Syslog File.</p> 
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	<p>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.</p> <p>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.</p>
Service Protocol	<p>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.</p> <p>Service Type Group –Click the triangle icon ▶ to display</p>

	<p>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.</p>
Incoming Country Filter	<p>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.</p>
Outgoing Country Filter	<p>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.</p>
Source IP	<p>Source IP 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.</p> <p>Source IP Group - Click the triangle icon  to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new IP group profile.</p> <p>Source User Profile - Click the triangle icon  to display the profile selection box. Choose one or more user profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new user object profile.</p> <p>Source User Group - Click the triangle icon  to display the profile selection box. Choose one or more user group profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new user group profile.</p> <p>Source LDAP Group - Click the triangle icon  to display the profile selection box. Choose one or more user LDAP profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new LDAP group profile.</p>
Destination IP	<p>Destination IP 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.</p> <p>Destination IP Group - Click the triangle icon  to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile</p>

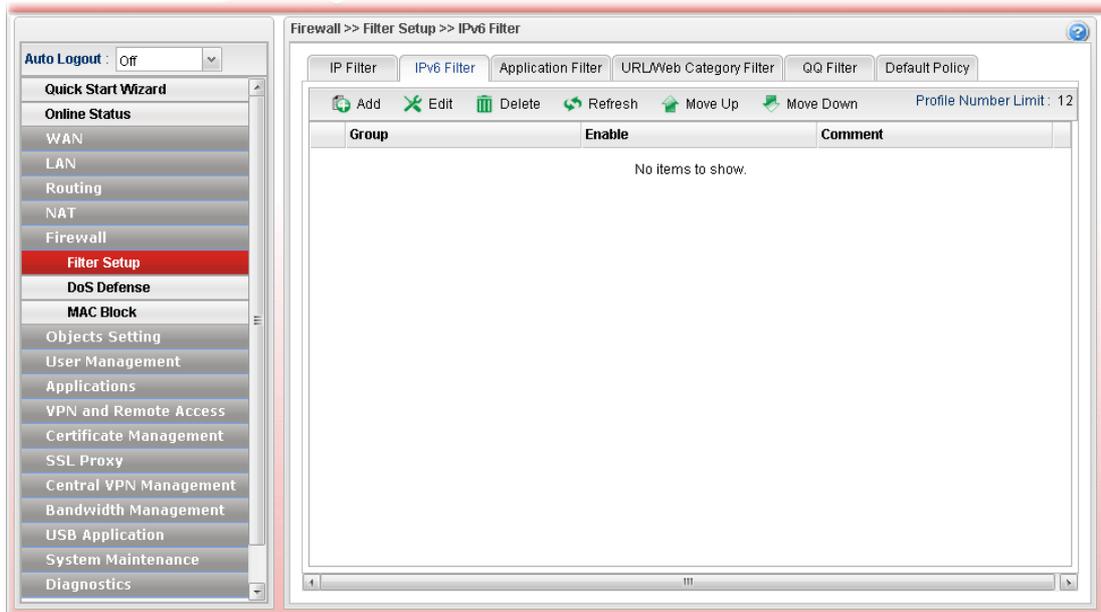
	<p>will be treated as destination target. You can click  to create another new IP group profile.</p> <p>Destination DNS Object- Click the triangle icon  to display the profile selection box. Choose one or more DNS object profiles from the drop down list. The selected profile will be treated as destination target. You can click  to create another new DNS object profile.</p> <p>Destination User Profile –Click the triangle icon  to display the profile selection box. Choose one or more user profiles from the drop down list. The selected profile will be treated as destination target. You can click  to create another new user object profile.</p> <p>Destination User Group –Click the triangle icon  to display the profile selection box. Choose one or more user group profiles from the drop down list. The selected profile will be treated as destination target. You can click  to create another new user group profile.</p> <p>Destination LDAP Group –Click the triangle icon  to display the profile selection box. Choose one or more LDAP group profiles from the drop down list. The selected profile will be treated as destination target. You can click  to create another new LDAP group profile.</p>
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:

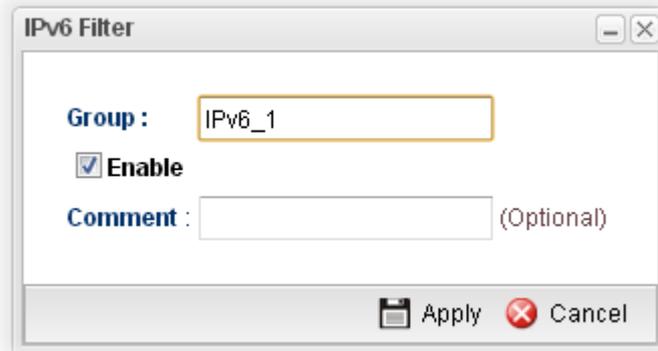
Item	Description
Add	Add a new group profile for IPv6 filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected 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.

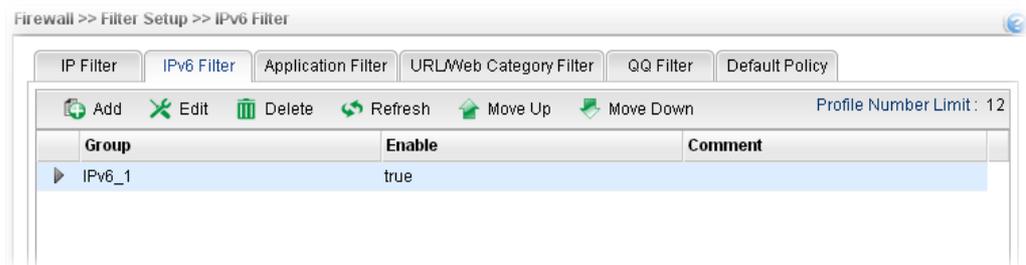
- Simply click the **Add** button.
- The following dialog will appear.



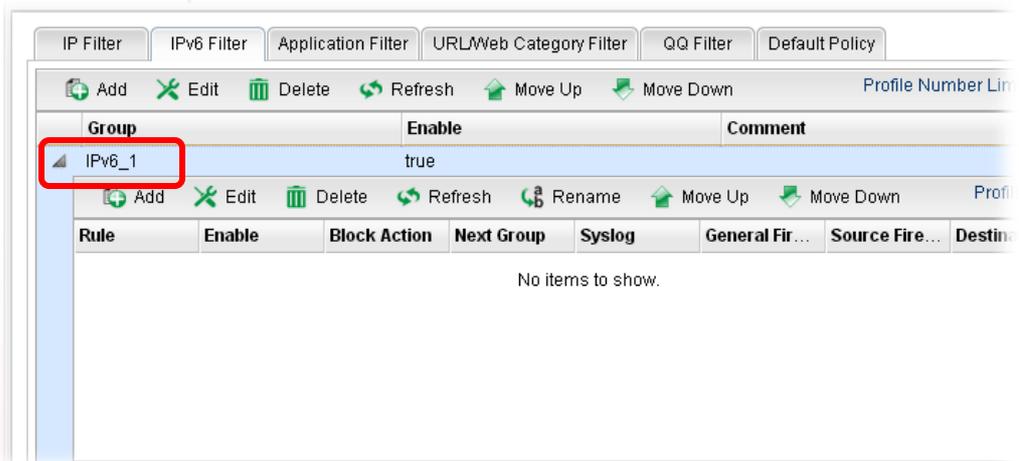
Available parameters are listed as follows:

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.

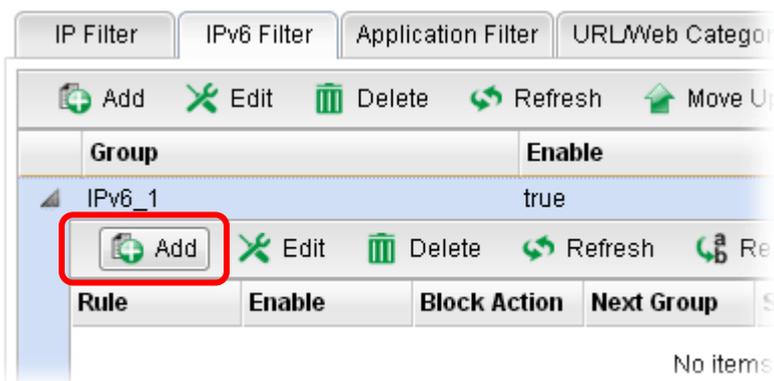
- Enter all of the settings and click **Apply**.
- A new filter group has been added.



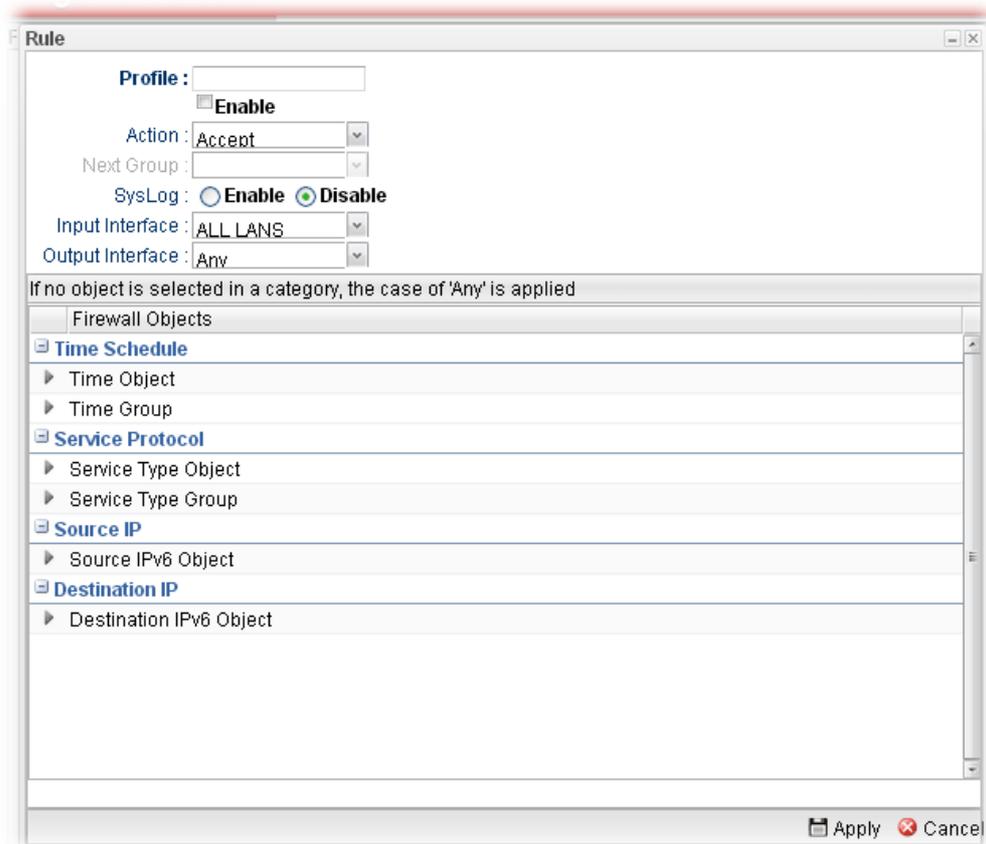
- You can create filter rule by clicking  on the left side of the selected IP filter group profile. A setting page will appear for you to add new IP filter rule profile.



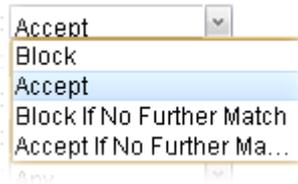
7. Move your mouse to click **Add**.

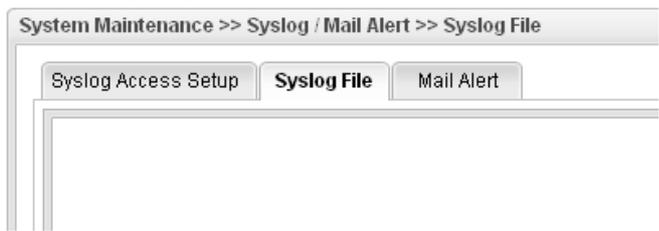


8. The following page for configuration will appear.

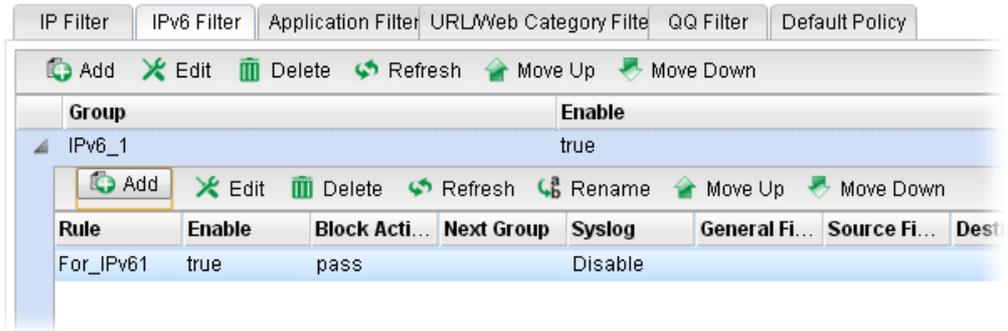


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Action	<p>The action to be taken when packets match the rule.</p> <p>Block - Packets matching the rule will be dropped immediately</p> <p>Accept- Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Accept If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p> 
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

	<p>appearing on the System Maintenance >> Syslog/Mail Alert >> Syslog File.</p> 
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	<p>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.</p> <p>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.</p>
Service Protocol	<p>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.</p> <p>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.</p>
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.

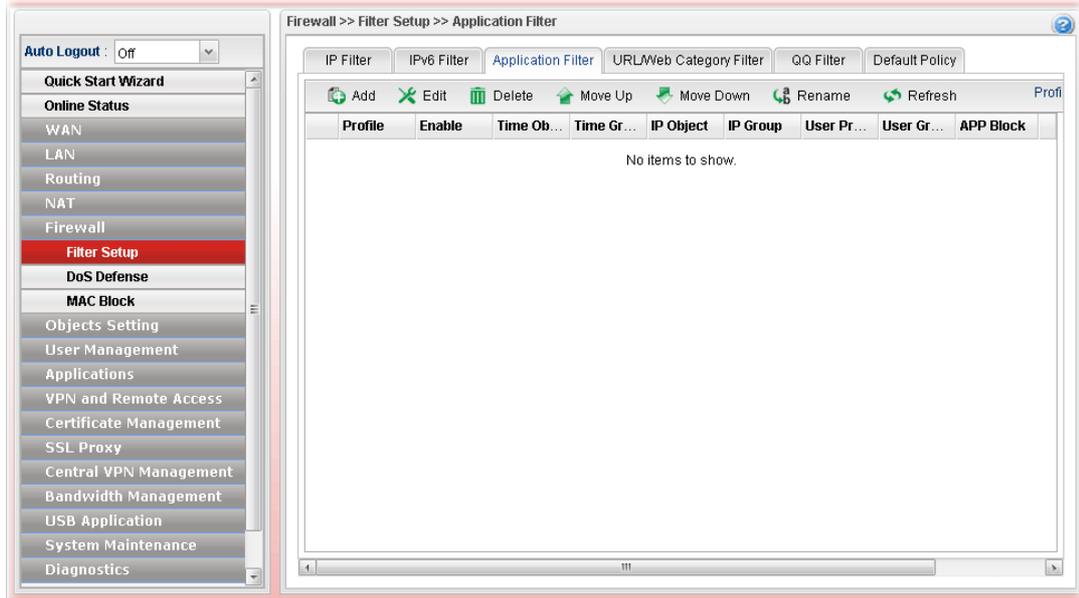
9. Enter all of the settings and click **Apply**.
10. A new IPv6 filter rule has been added under the IPv6 Filter Group (named For_IPv61 in this case).



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.



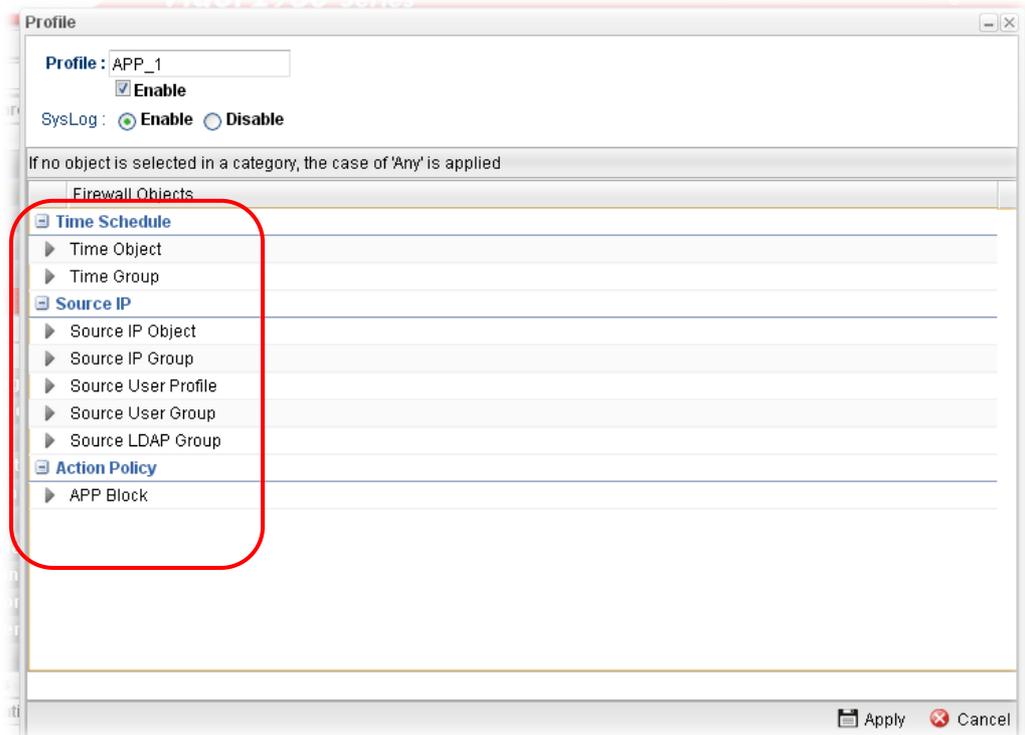
Each item will be explained as follows:

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.
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	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
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.

Item	Description
IP Object	Display the IP object profile selected for such application profile.
IP Group	Display the IP group profile selected for such application profile.
User Profile	Display the user object profile selected for such application profile.
User Group	Display the user group profile selected for such application profile.
APP Block	Display the APP object profile selected for such application profile.

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).



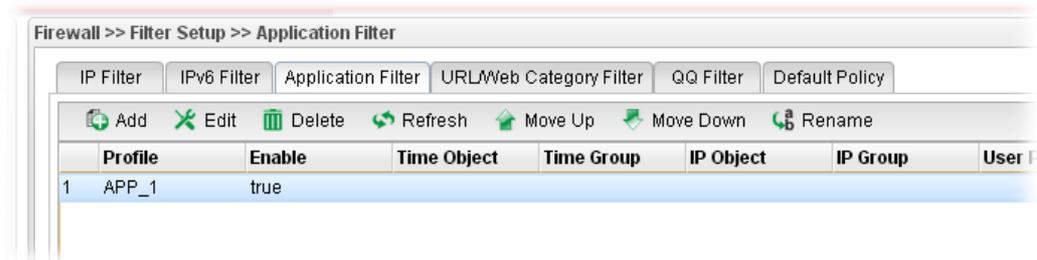
Available parameters are listed as follows:

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	<p>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.</p> <p>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.</p>
Source IP	<p>Source IP 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 IP will be filtered by the router when such application filter profile is applied. You can click  to create another new IP object profile.</p> <p>Source IP Group - Click the triangle icon  to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be filtered by the router when such application filter profile is applied. You can click  to create another new IP group profile, or you can click the edit icon  to modify the existed group profile.</p> <p>Source User Profile - Click the triangle icon  to display the profile selection box. Choose one or more user profiles from the drop down list. The user specified in the selected profile will be filtered by the router when such application filter profile is applied. You can click  to create another new user profile, or you can click the edit icon  to modify the existed user profile.</p> <p>Source User Group - Click the triangle icon  to display the profile selection box. Choose one or more user group profiles from the drop down list. The users within the selected profile will be filtered by the router when such application filter profile is applied. You can click  to create another new user group profile, or you can click the edit icon  to modify the existed group profile.</p> <p>Source LDAP Group - Click the triangle icon  to display the profile selection box. Choose one or more user LDAP profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another</p>

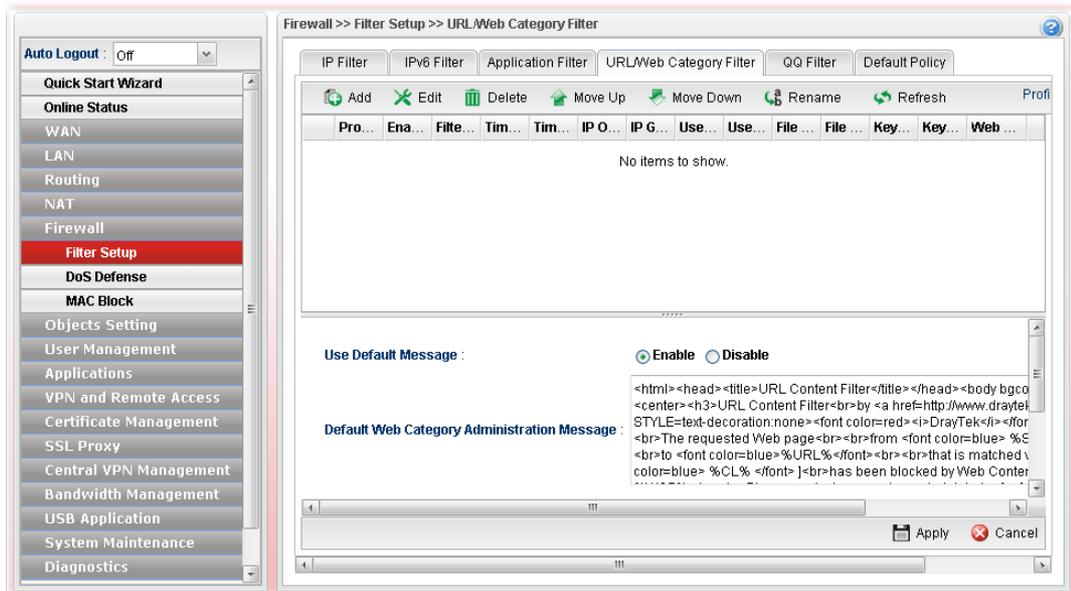
	new LDAP group profile.
Action Policy	APP Block - Click the triangle icon  to display the profile selection box. Choose one or more APP object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click  to create another new APP object profile, or 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:

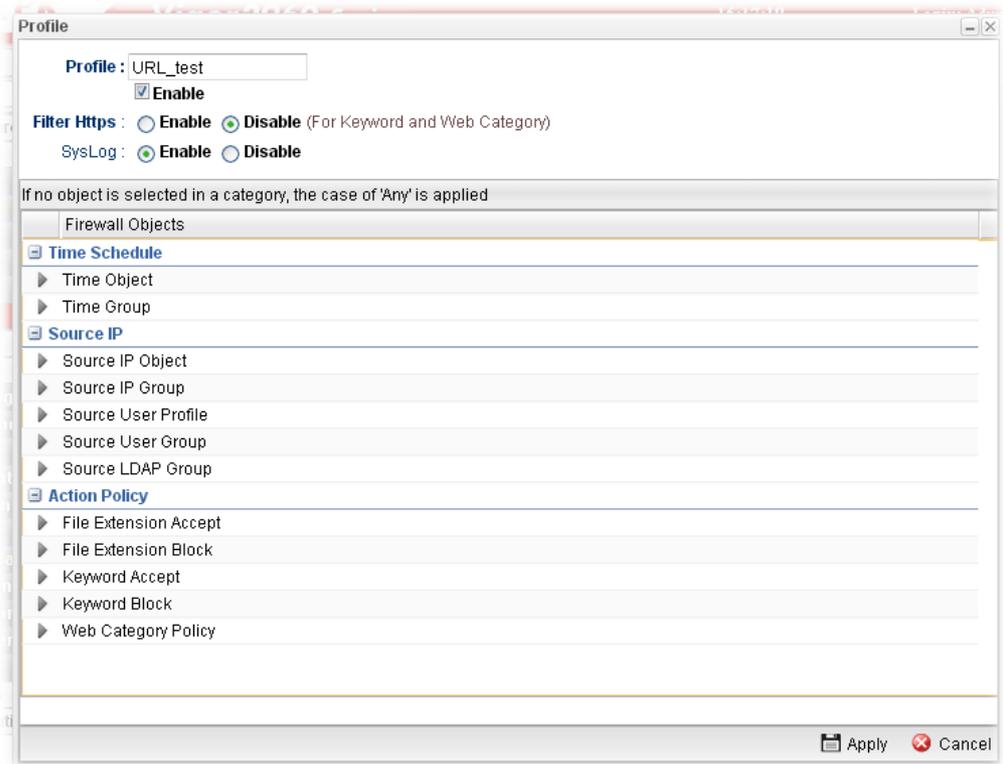
Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected 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.
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.
IP Object	Display the IP object profile selected for each rule.
IP Group	Display the IP group profile selected for each rule.
User Profile	Display the user object profile selected for each rule.
User Group	Display the user group profile selected for each rule.
File Extension Pass	Display the file extension object profile selected for each rule which is allowed to pass through the router.
File Extension Block	Display the file extension object profile selected for each rule which is not allowed to pass through the router.
Keyword Pass	Display the keyword object profile selected for each rule which is allowed to pass through the router.
Keyword Block	Display the keyword object profile selected for each rule which is not allowed to pass through the router.
Web Category Block	Display the web category object profile selected for each rule which is not allowed to pass through the router.
China Web Category	Display the China web category object profile selected for each rule which is not allowed to pass through the router.
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.

Item	Description
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

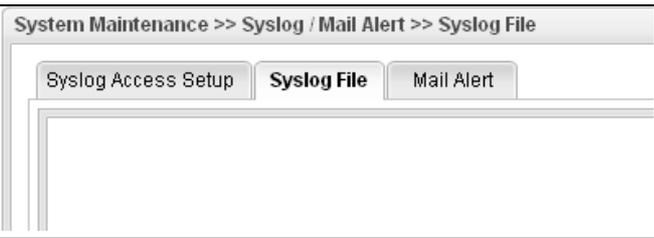
How to create a URL Filter profile

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.



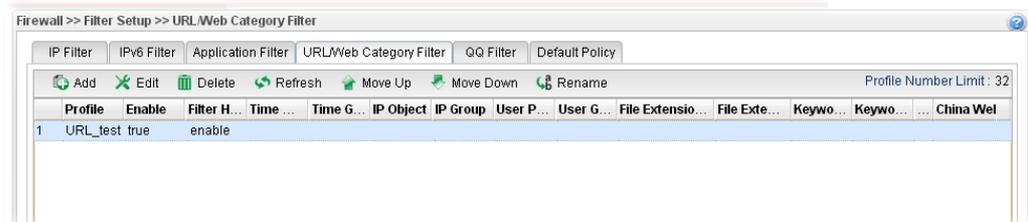
Available parameters are listed as follows:

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 .

Item	Description
	
Time Schedule	<p>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.</p> <p>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.</p>
Source IP	<p>Source IP 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 IP will be filtered by the router when such URL filter profile is applied. You can click  to create another new IP object profile.</p> <p>Source IP Group - Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be filtered by the router when such URL filter profile is applied. You can click  to create another new IP group profile, or you can click the edit icon  to modify the existed group profile.</p> <p>Source User Profile - Click the triangle icon ▶ to display the profile selection box. Choose one or more user profiles from the drop down list. The user specified in the selected profile will be filtered by the router when such URL filter profile is applied. You can click  to create another new user profile, or you can click the edit icon  to modify the existed user profile.</p> <p>Source User Group - Click the triangle icon ▶ to display the profile selection box. Choose one or more user group profiles from the drop down list. The users within the selected profile will be filtered by the router when such URL filter profile is applied. You can click  to create another new user group profile, or you can click the edit icon  to modify the existed group profile.</p> <p>Source LDAP Group - Click the triangle icon ▶ to display the profile selection box. Choose one or more user LDAP profiles from the drop down list. The selected profile will be</p>

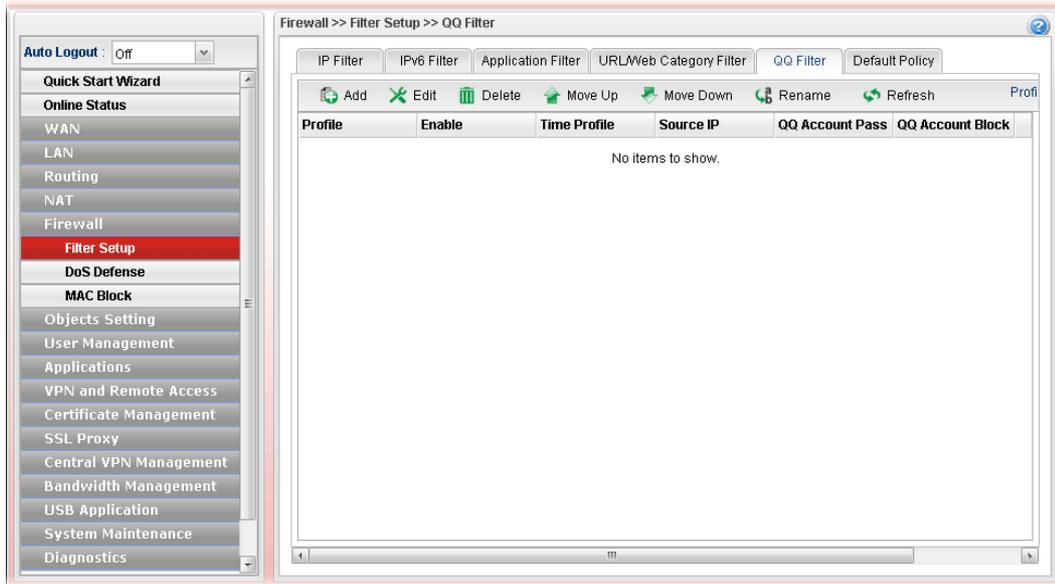
Item	Description
	treated as source target. You can click  to create another new LDAP group profile.
Action Policy	<p>File Extension Accept / File Extension Block - Click the triangle icon  to display the profile selection box. Choose one or more File Extension object profiles from the drop down list 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.</p> <p>Keyword Accept / Keyword Block - Click the triangle icon  to display the profile selection box. Choose 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.</p> <p>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.</p> <p>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.</p>
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.



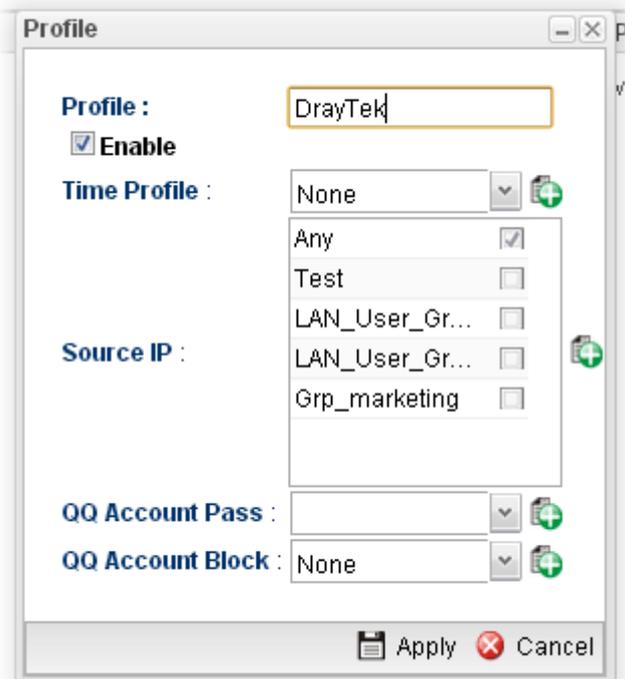
Each item will be explained as follows:

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.

Item	Description
QQ Account Block	Display the account name which will be blocked if the 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.

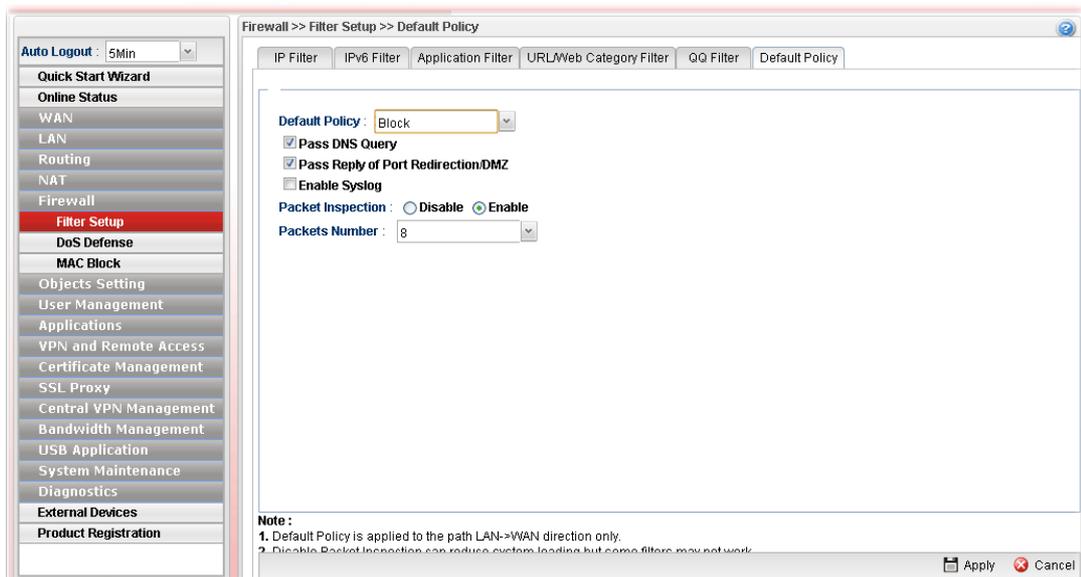
Item	Description
	You can click  to create another new QQ account.
QQ Account Block	Use the drop down list to specify a QQ account profile for such profile. The select account will be blocked by Vigor router. You can click  to create another new QQ account.
Apply	Click it to save and exit the dialog.
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	<p>Pass – All of the incoming packets can pass through Vigor router without any filtering.</p> <p>Block – All of the incoming packets will be blocked except the following rules.</p> <ul style="list-style-type: none"> ● Pass DNS Query – Check the box to make the DNS

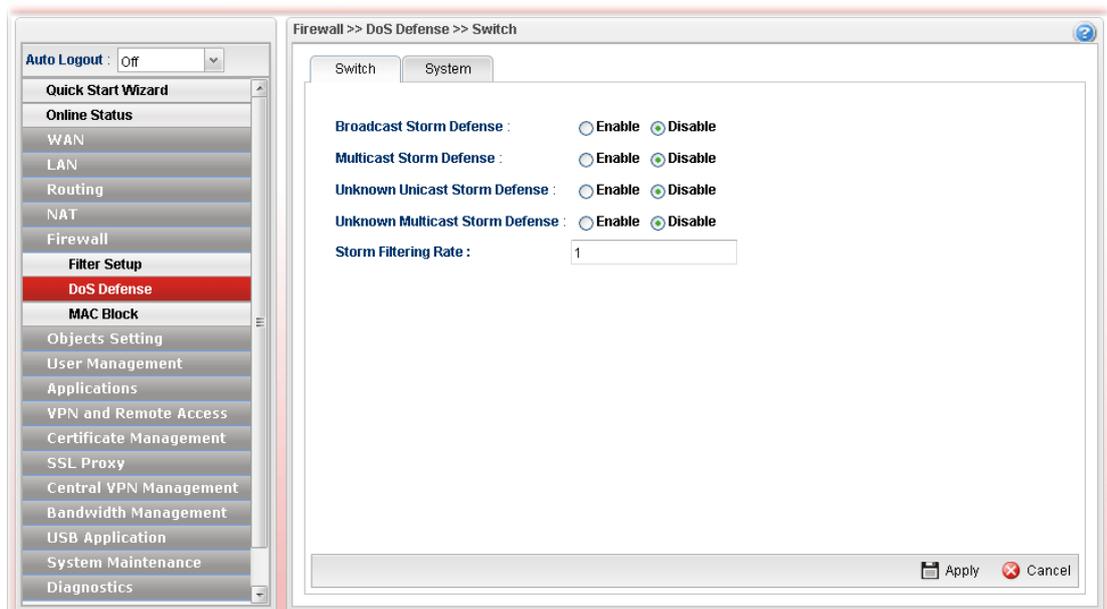
Item	Description
	<p>query passing through Vigor router's firewall.</p> <ul style="list-style-type: none"> ● Pass Reply of Port Redirection /DMZ – Check the box to make the outgoing packets processed by Port Redirection/DMZ passing through Vigor router's firewall. ● Enable Syslog – Check the box to make related information for the blocked packets being recorded in Syslog. <p>The above three policies also can be configured in Firewall>>Filter Setup>>IP Filter/Application Filter.</p>
Packet Inspection	<p>Disable – No inspection will be performed.</p> <p>Enable – Packet inspection will be performed.</p>
Packets Number	<p>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.</p>
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

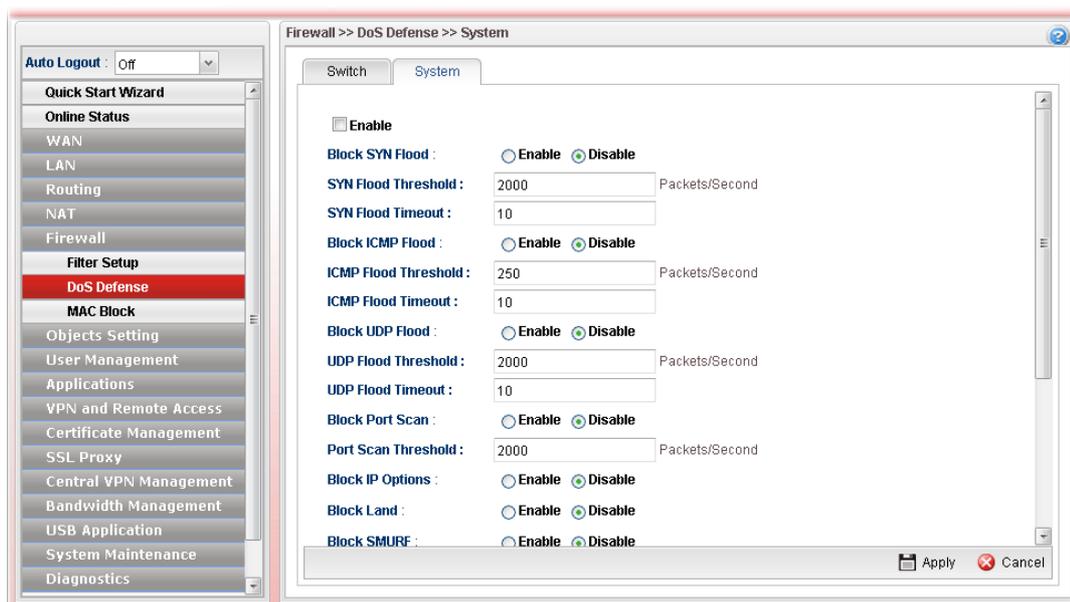


Available parameters are listed as follows:

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.
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.
Block SYN Flood	Click Enable to activate the SYN flood defense function. If the amount of TCP SYN packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN packets within

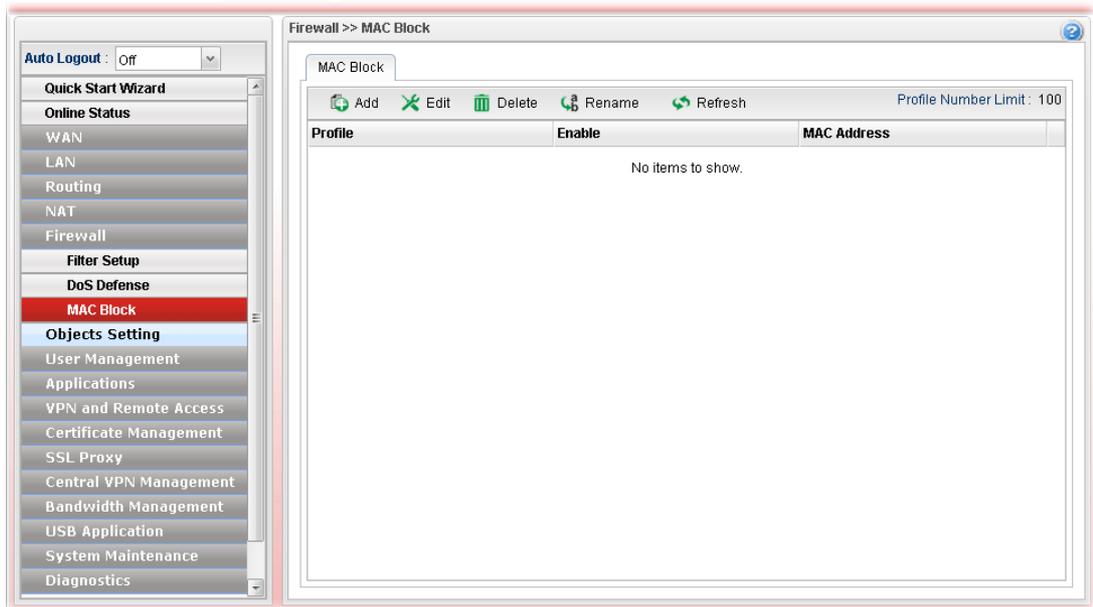
Item	Description
	the user-defined timeout period.
SYN Flood Threshold	The default setting for threshold is 2000 packets per second.
SYN Flood Timeout	The default setting for timeout is 10 seconds.
Block ICMP Flood	Click Enable to activate the ICMP flood defense function. If the amount of ICMP echo requests 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.
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

Item	Description
	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.



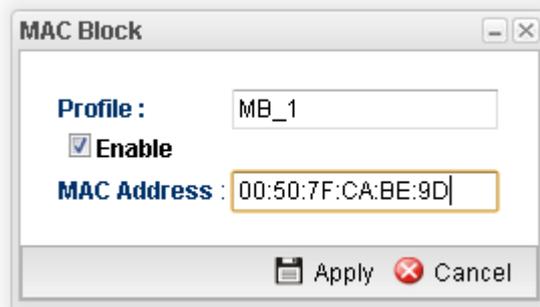
Each item will be explained as follows:

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

Item	Description
	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.
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 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.

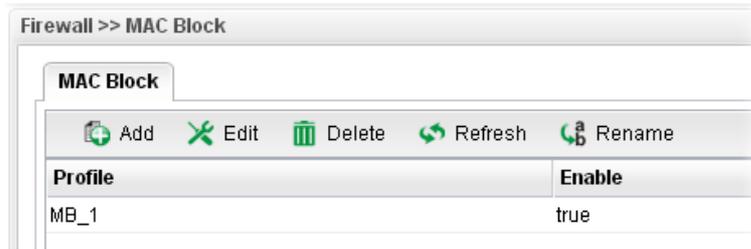


Available parameters are listed as follows:

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.



4.6 Objects Setting

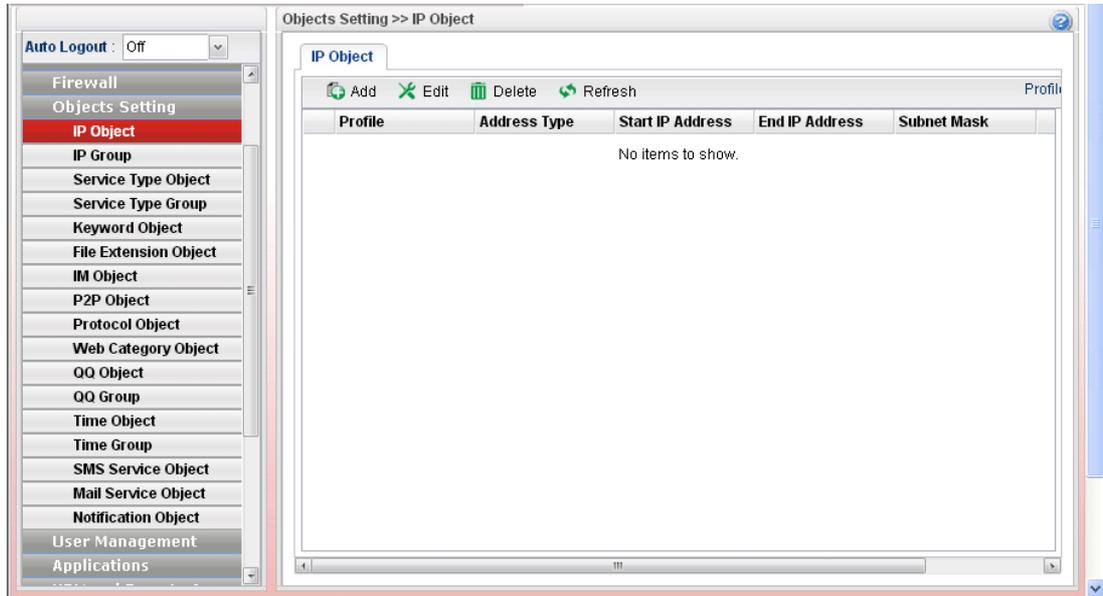
Vigor3900 allows users to set different filter profiles based on IP, service type, keyword, file extension, instant message application, P2P application, protocol application, web category, QQ application, time setting, SMS service, mail service and notification. These objects setting profiles can be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

Objects Setting
IP Object
IP Group
IPv6 Object
Country Object
Service Type Object
Service Type Group
Keyword / DNS Object
File Extension Object
APP Object
Web Category Object
QQ Object
QQ Group
Time Object
Time Group
SMS Service Object
Mail Service Object
Notification Object

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**.



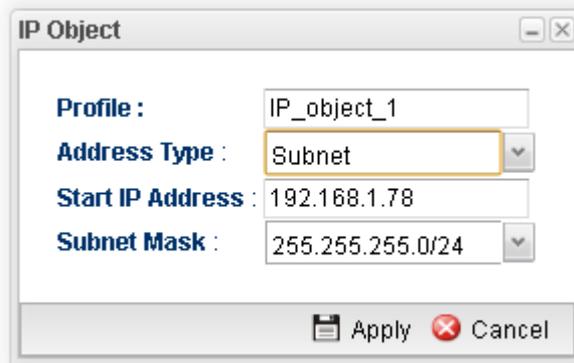
Each item will be explained as follows:

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 .

Item	Description
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.



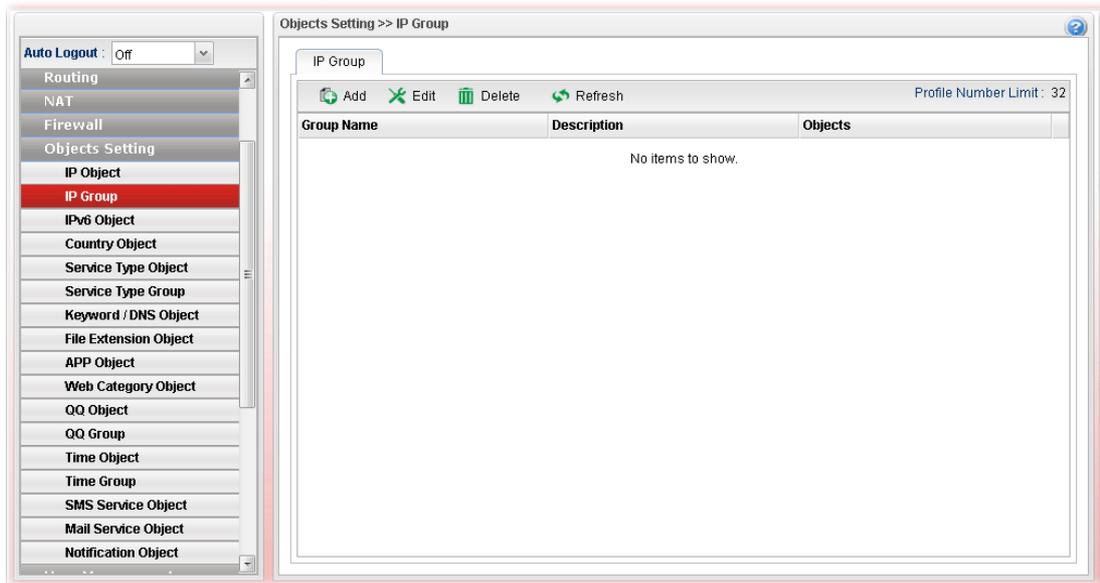
Available parameters are listed as follows:

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.

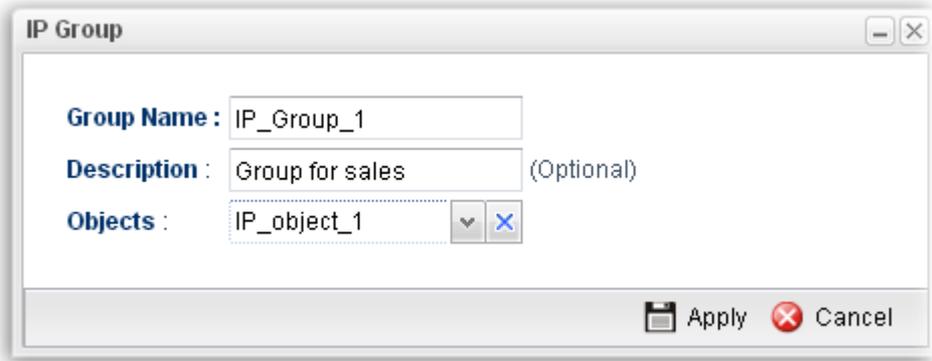


Each item will be explained as follows:

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.



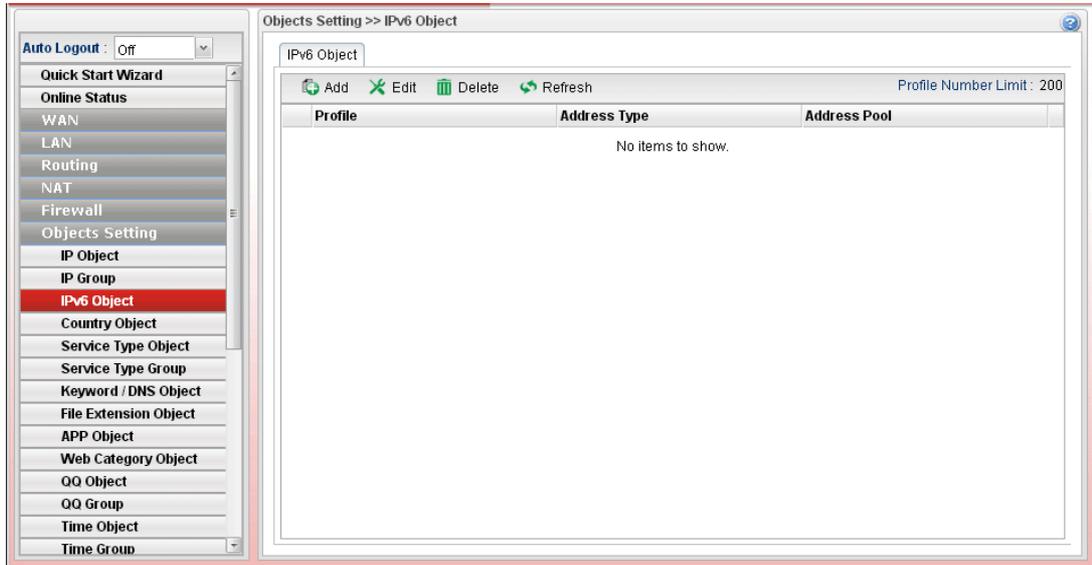
Available parameters are listed as follows:

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.



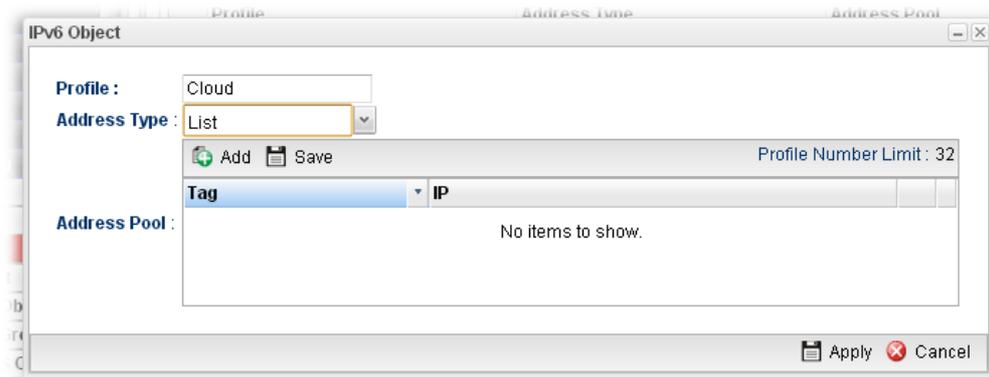
Each item will be explained as follows:

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.

- The following dialog will appear.



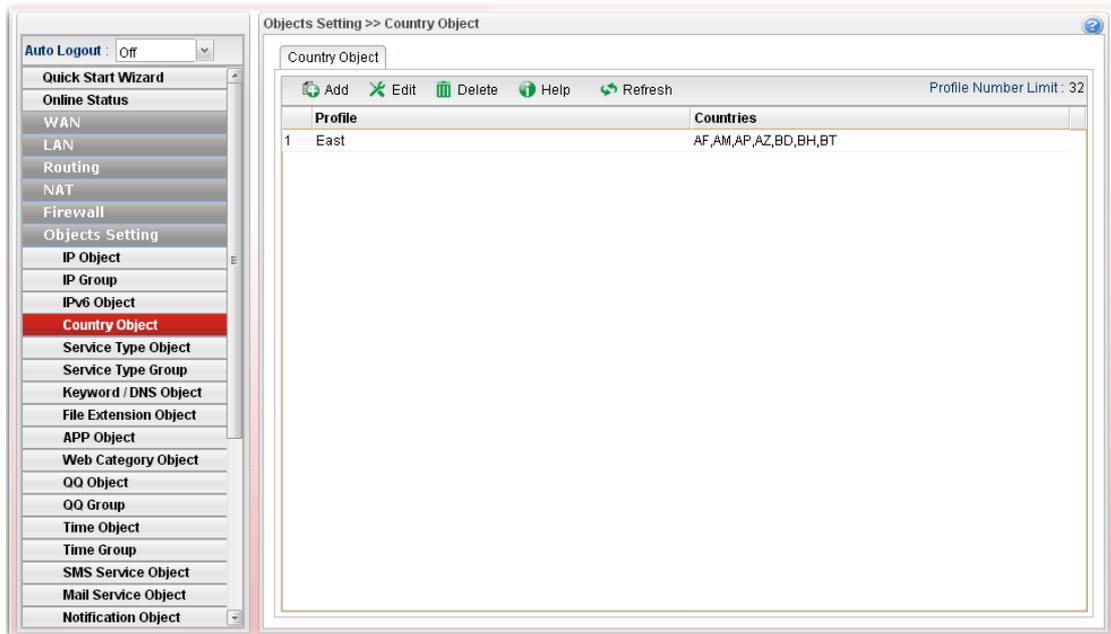
Available parameters are listed as follows:

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. Subnet – Allow to specify subnet mask.
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.

- Enter all of the settings and click **Apply**.
A new IPv6 Object profile has been created.

4.6.4 Country Object

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

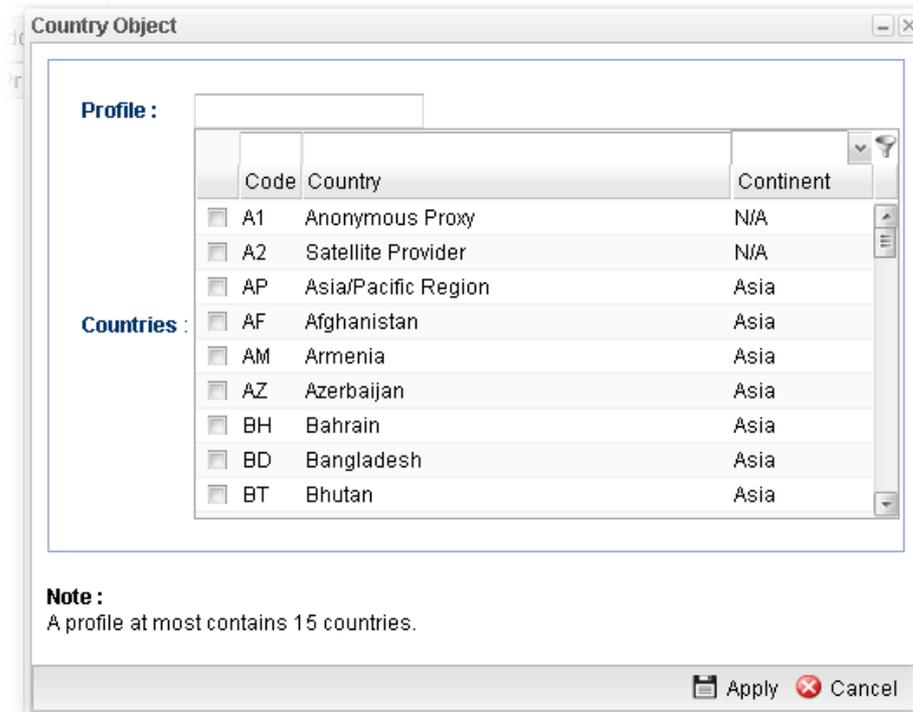


Each item will be explained as follows:

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.
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:

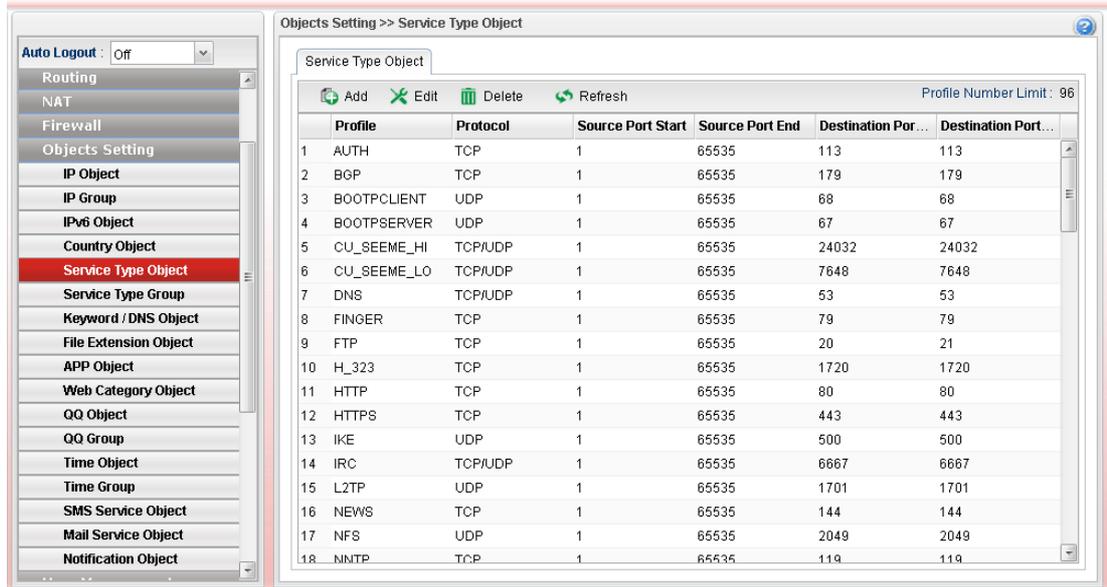
Item	Description
Profile	Type a name for such profile.
Countries	Check the box(es) for the country/countries to be blocked by Firewall.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

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

4.6.5 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.

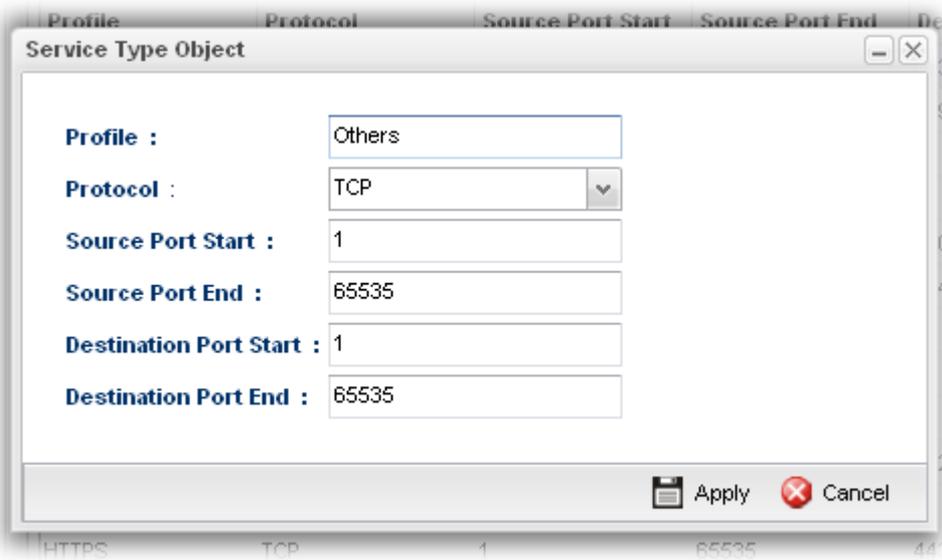


Each item will be explained as follows:

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:

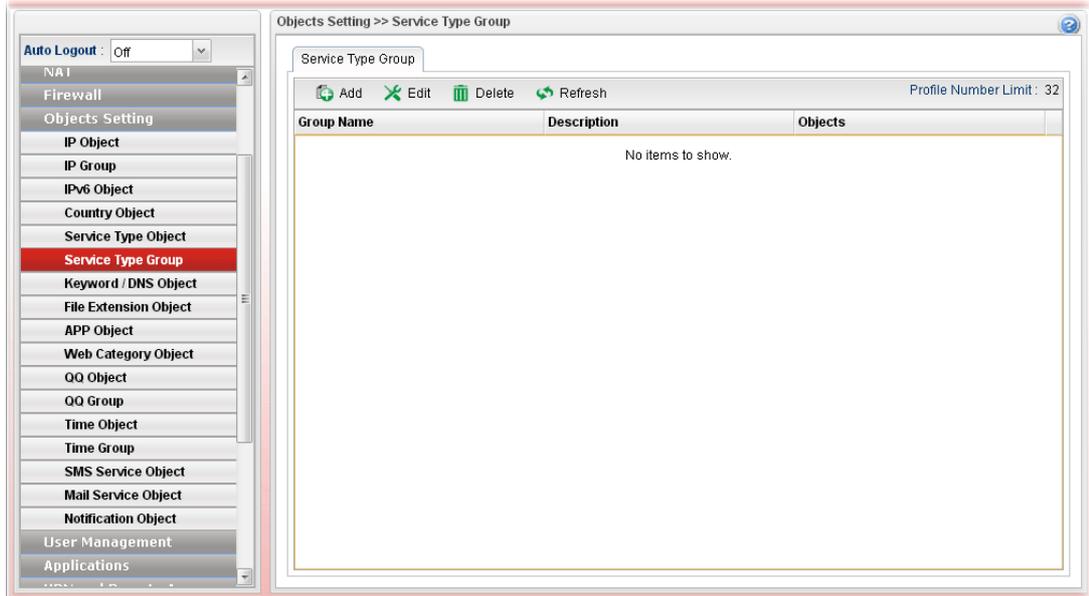
Item	Description
Profile	Type a name for such profile. The number of the characters allowed to be typed here is 10.
Protocol	Specify one of the protocols for such profile.
Source Port Start	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the starting 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.

4.6.6 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.

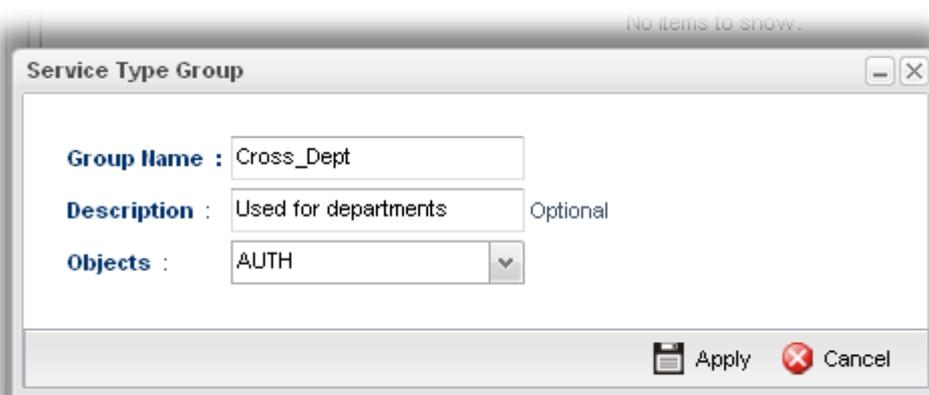


Each item will be explained as follows:

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:

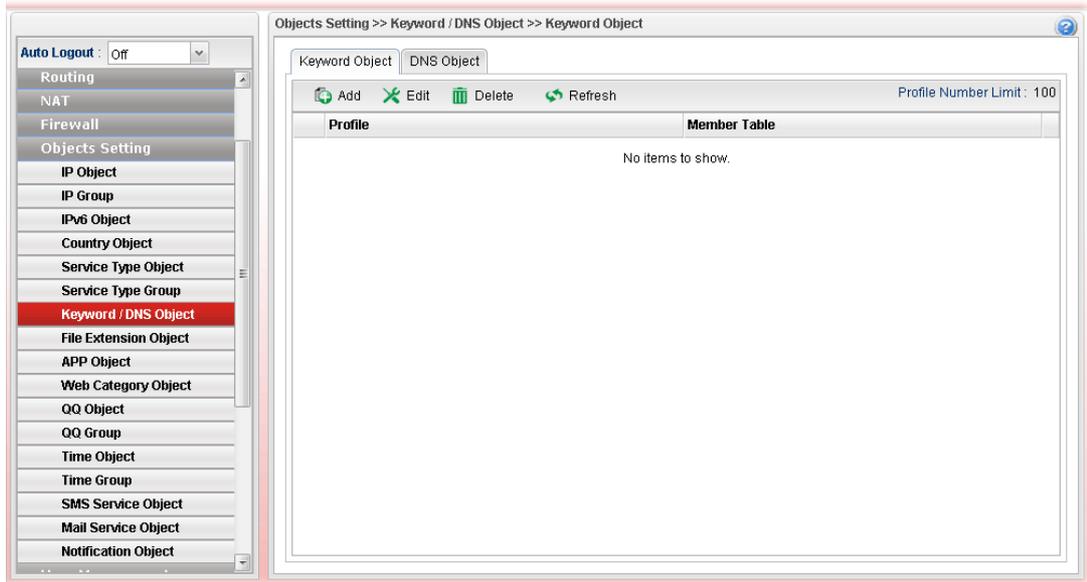
Item	Description
Group Name	Type the name of the service type object group. The number of the characters allowed to be typed here is 10.
Description	Type some words to describe such group.
Objects	Use the drop down list to check the service type object profiles under such group. All the available service 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.

4.6.7 Keyword /DNS Object

4.6.7.1 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.

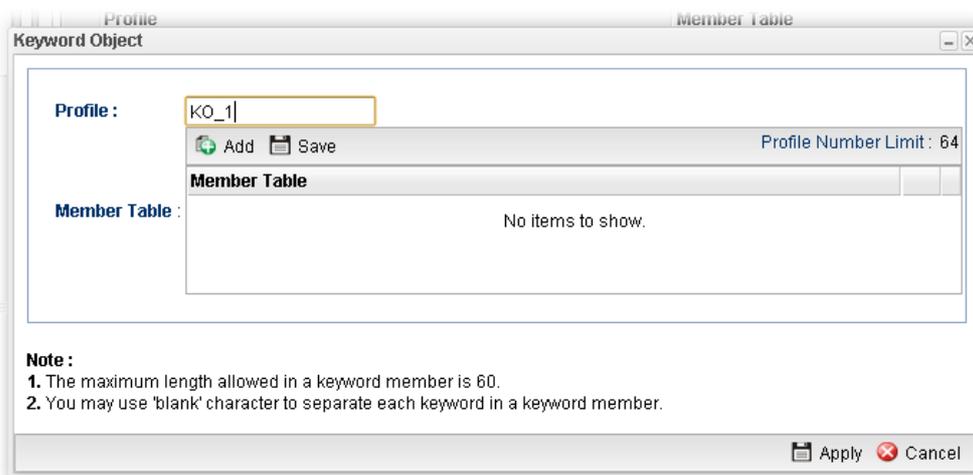


Each item will be explained as follows:

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	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.



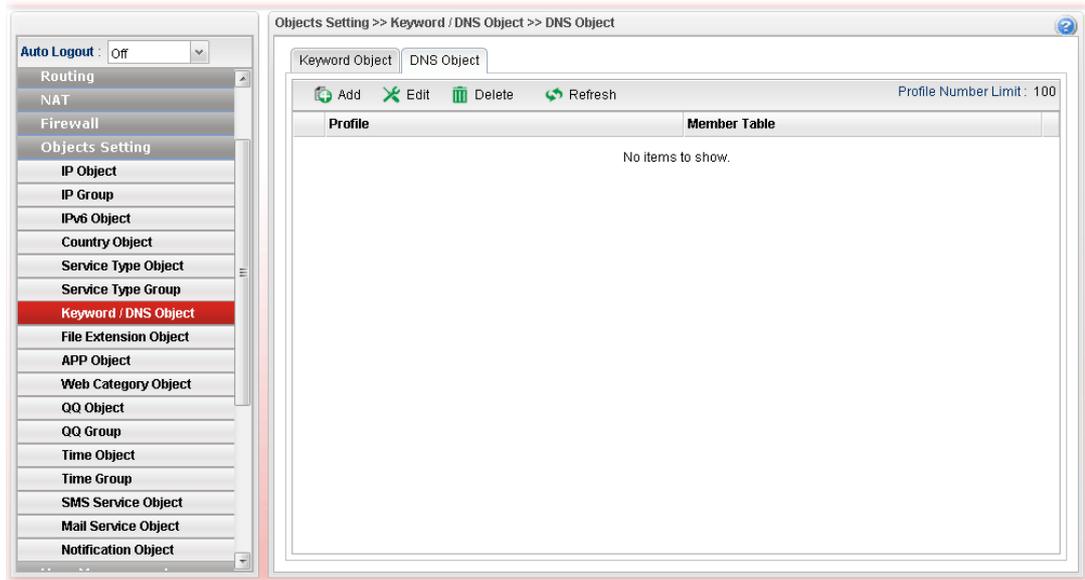
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the Keyword Object.
Member	Type the content for such profile. For example, type <i>gambling</i> 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.

4.6.7.2 DNS Object

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

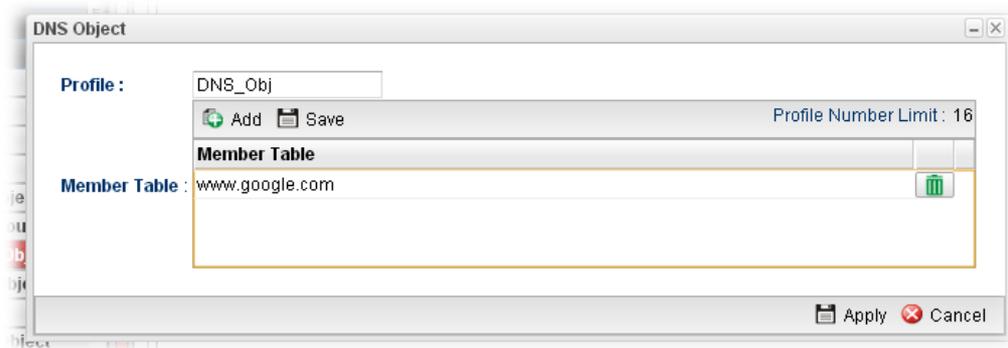


Each item will be explained as follows:

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.



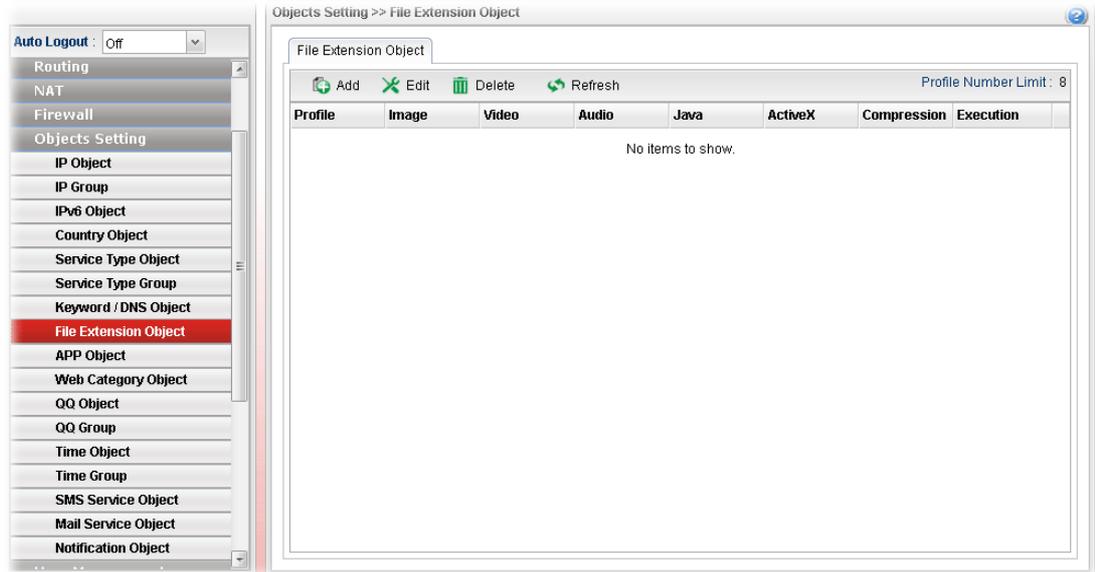
Available parameters are listed as follows:

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.

4.6.8 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.

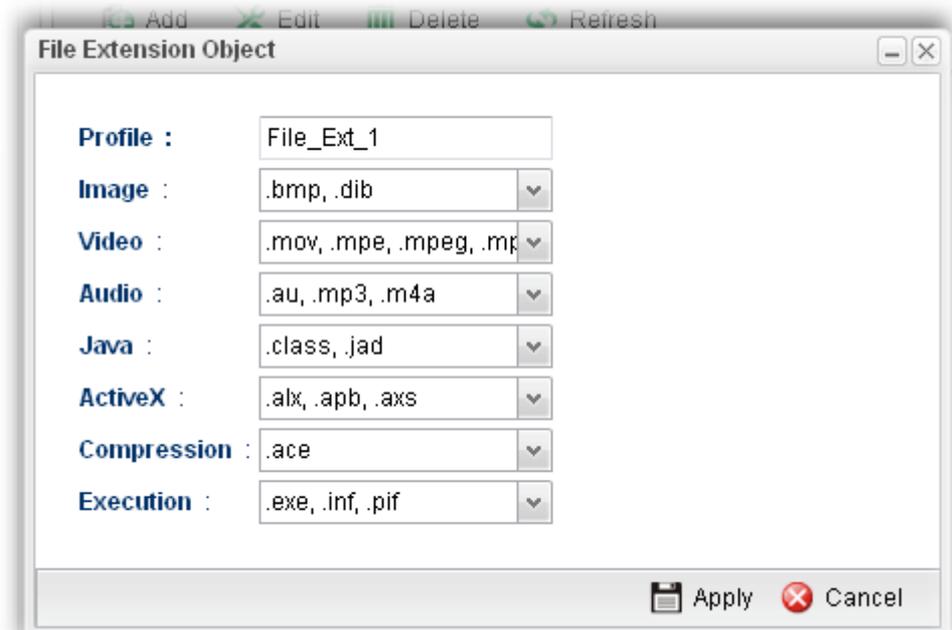


Each item will be explained as follows:

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.

Item	Description
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.

4.6.9 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:

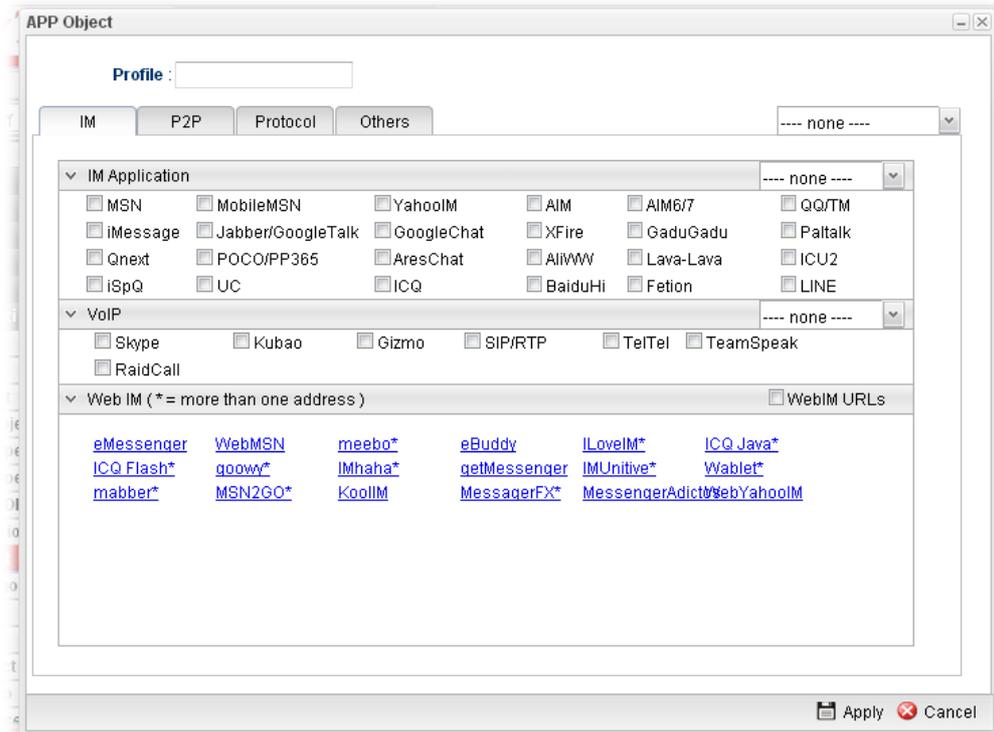
Item	Description
APP Signature Upgrade	Click it to open System Maintenance>>APP Signature Upgrade configuration page.
APP Support List	APP Support List will display all of the applications with versions supported by Vigor router. They are separated with types of IM, P2P, Protocol and Others. Each tab 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.

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 .
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.

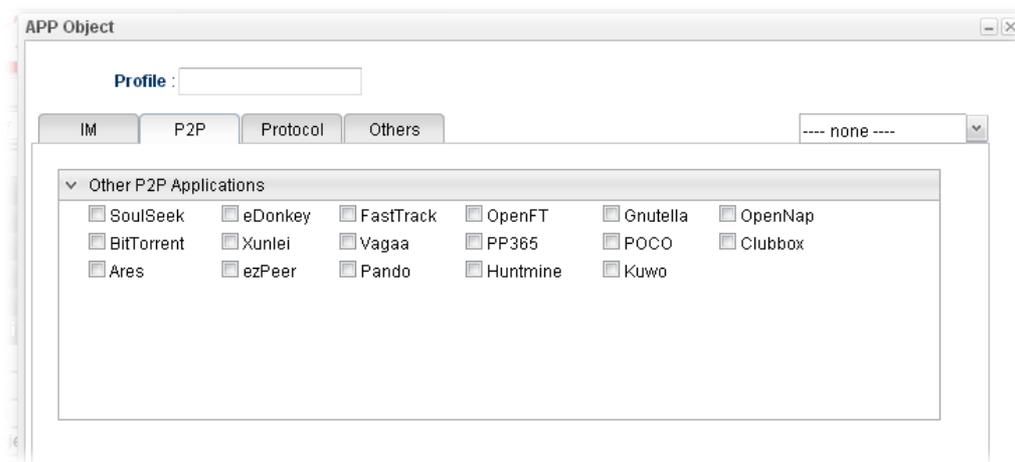


Available parameters are listed as follows:

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 can check the box to include all of them.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

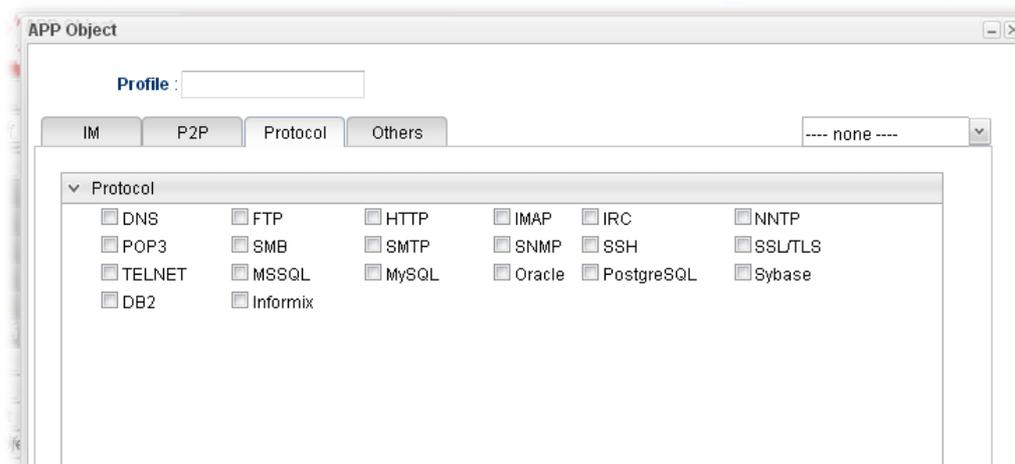
Click **P2P** to get the following page. Vigor3900 can block P2P application for users, especially for the ones who always upload or download improper files to Internet.

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.



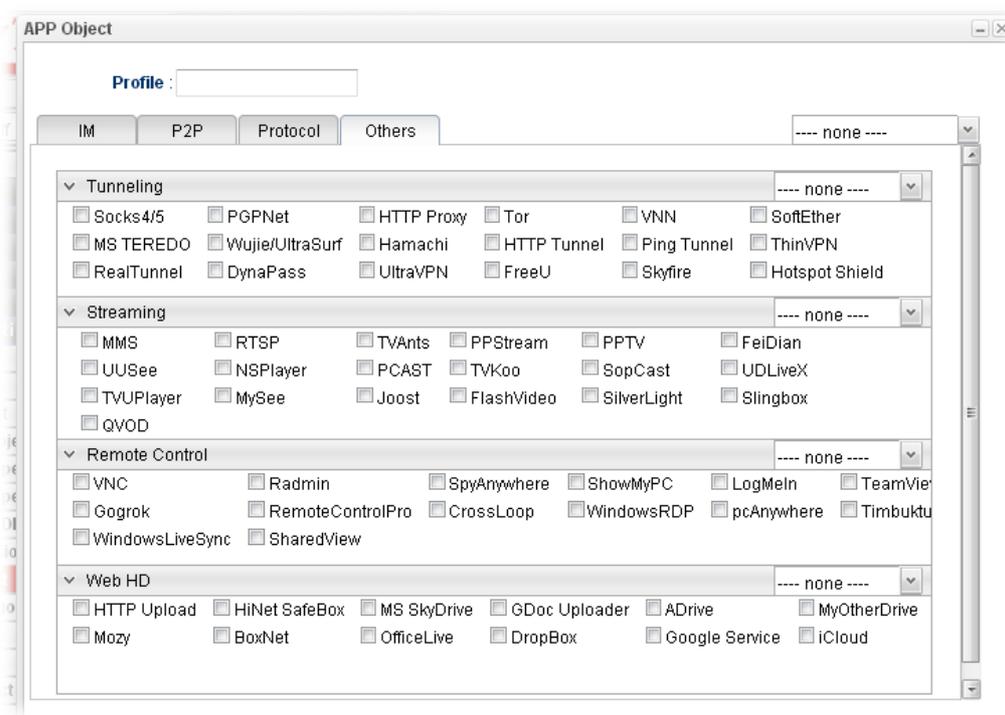
Item	Description
Other P2P Applications	Several P2P applications offered for you to choose. Check the one(s) you want to add for such profile.

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.

4.6.10 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.

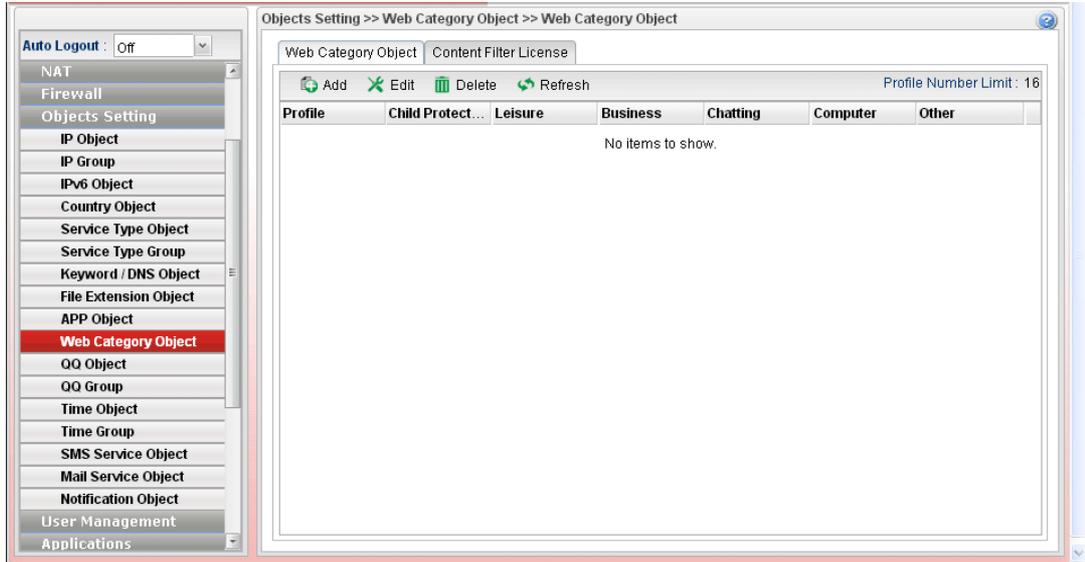
WCF adopts the mechanism developed and offered by certain service provider. No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate URL** to satisfy your request. Note that service provider matching with Vigor router currently offers a period of 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.

4.6.10.1 Web Category Object



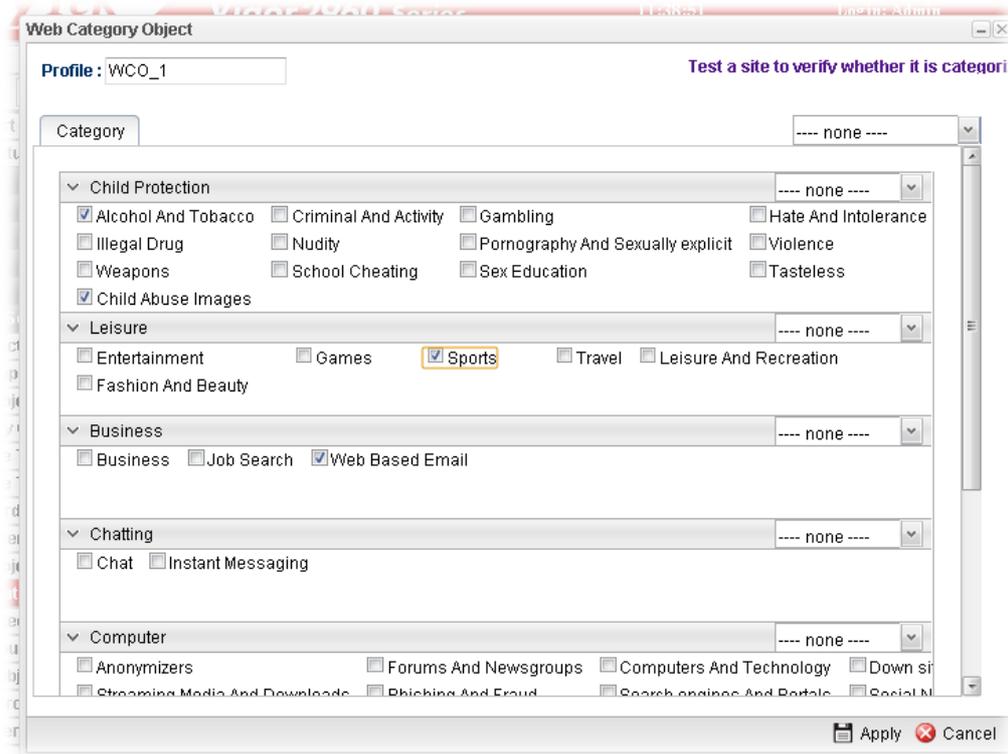
Each item will be explained as follows:

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

Item	Description
	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:

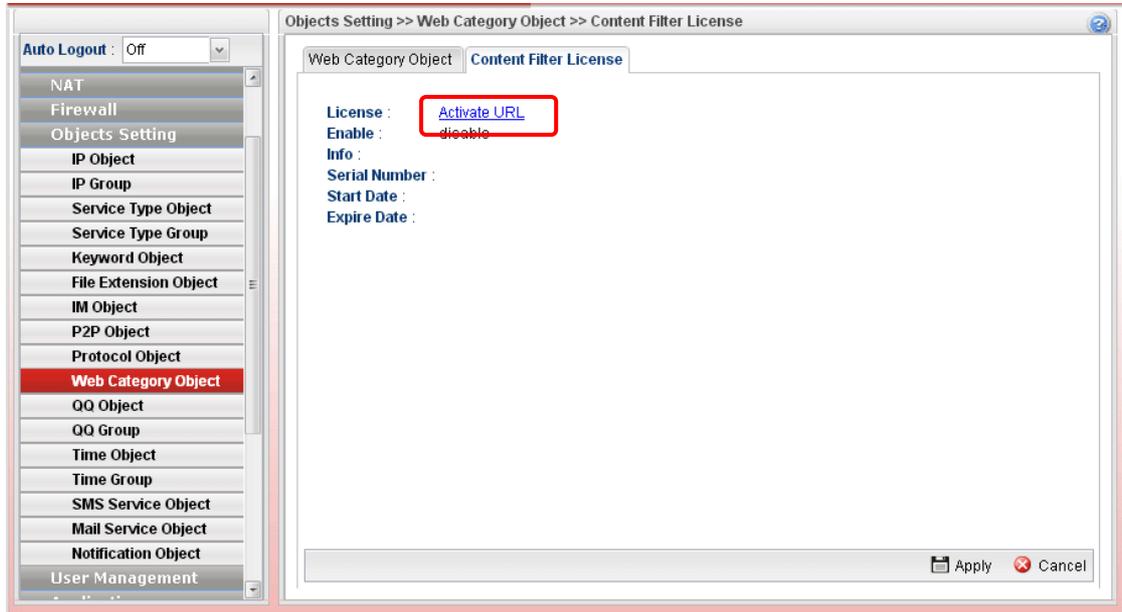
Item	Description
Profile	Type the name of the web category object profile. The number of the characters allowed to be typed here is 10.
Child Protection	The web pages which are not suitable for children will be classified into different categories. Simply check the one(s) that you don't want the children to visit. <div style="border: 1px solid gray; padding: 5px; width: fit-content;"> <p>Child Protection : Alcohol-And-Tobacco, C</p> <p>Leisure : <input checked="" type="checkbox"/> Alcohol-And-Tobacco <input checked="" type="checkbox"/> Criminal-And-Activity <input checked="" type="checkbox"/> Gambling <input type="checkbox"/> Hate-And-Intolerance <input type="checkbox"/> Illegal-Drug</p> </div>
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.

4.6.10.2 Content Filter License

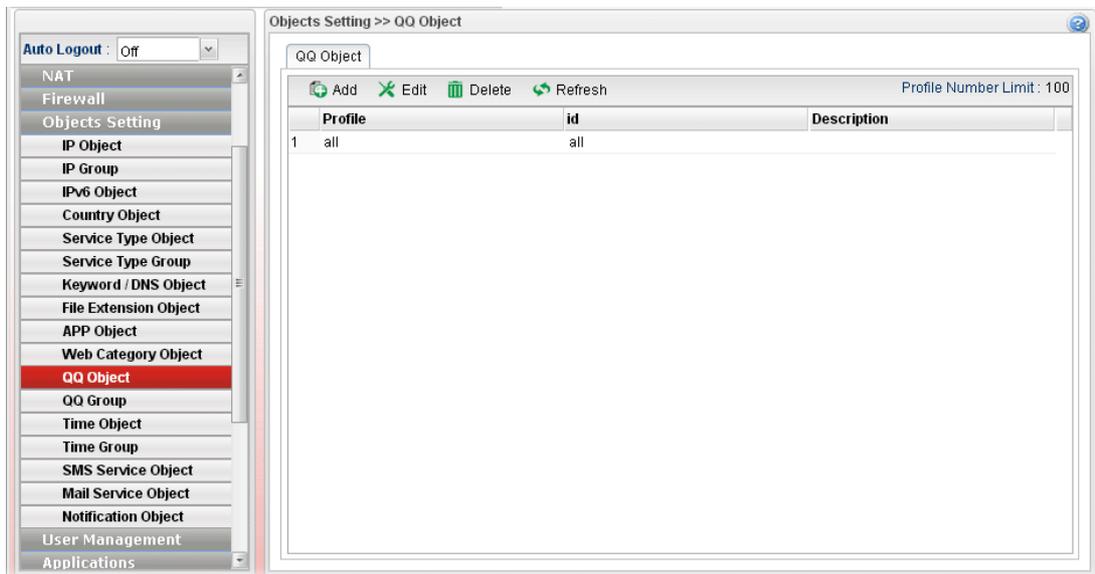
Move your mouse to the link of **Activate URL** and click it. The system will guide you to access into MyVigor website.



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 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.



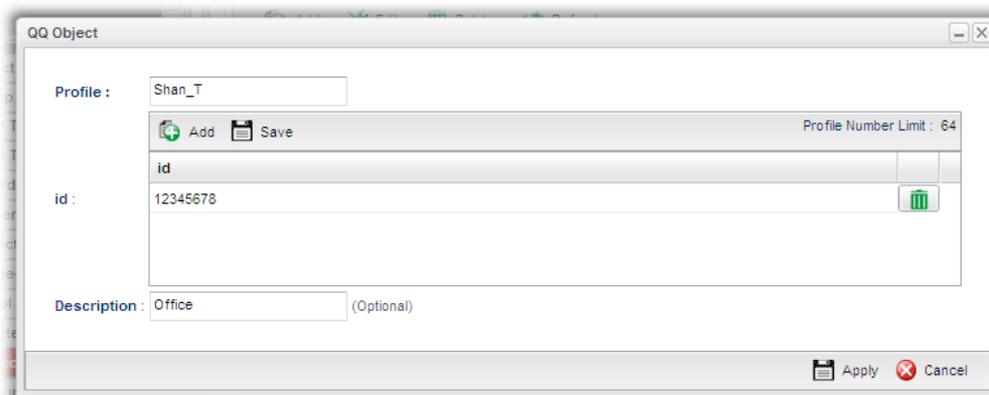
Each item will be explained as follows:

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

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.
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.



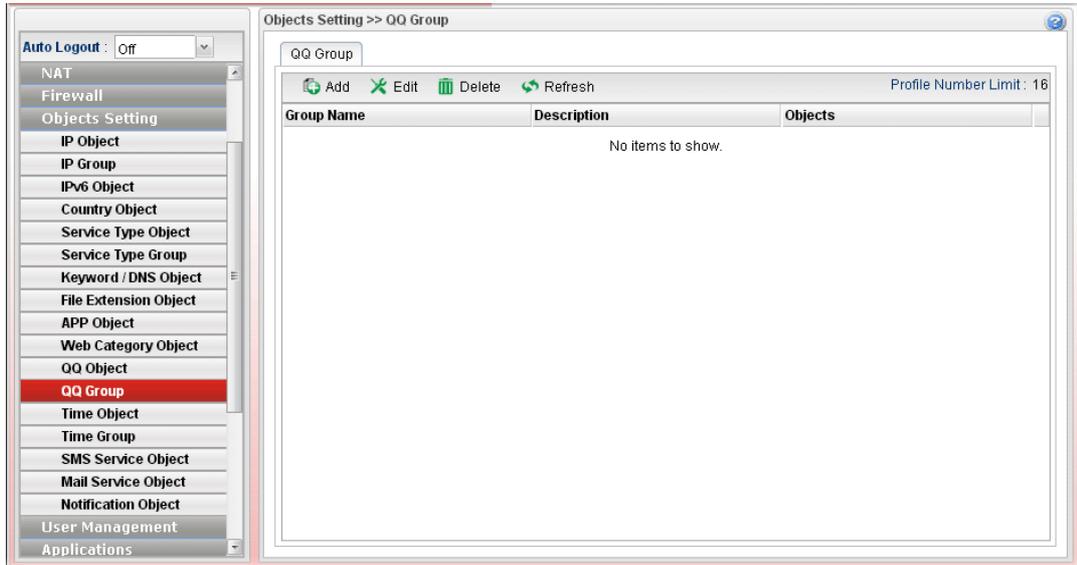
Available parameters are listed as follows:

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 to 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.

4.6.12 QQ Group

This page allows you to group several QQ object profiles.

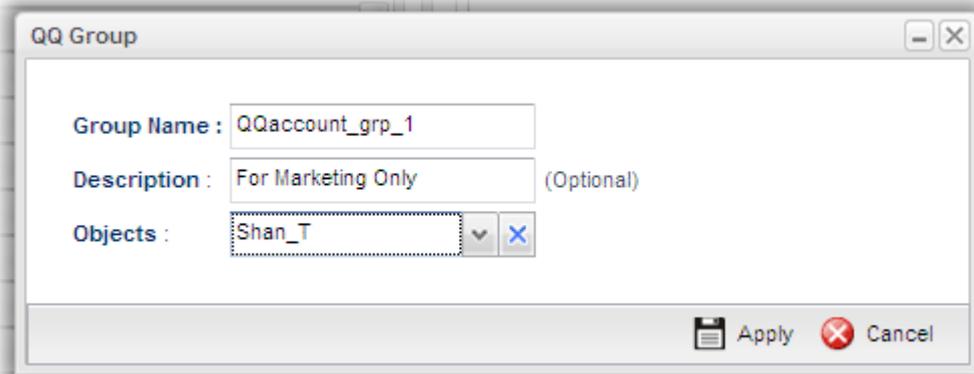


Each item will be explained as follows:

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.



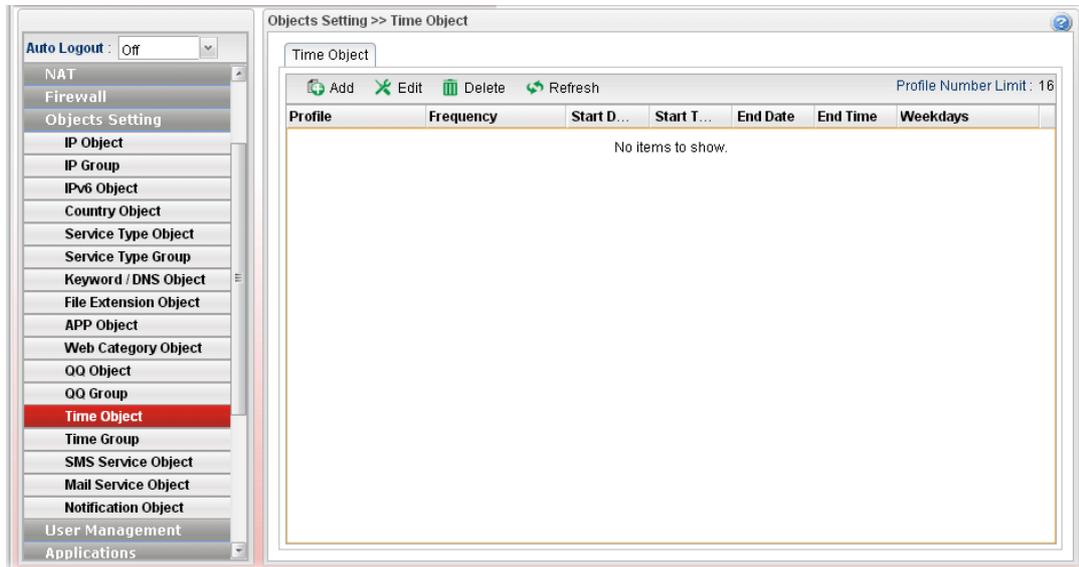
Available parameters are listed as follows:

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.

4.6.13 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.



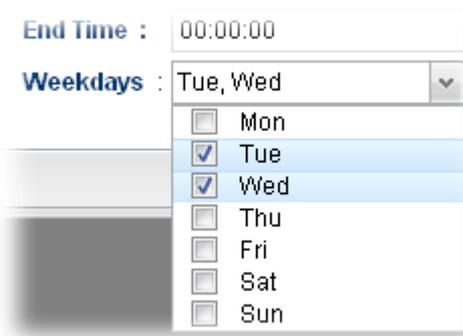
Each item will be explained as follows:

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:

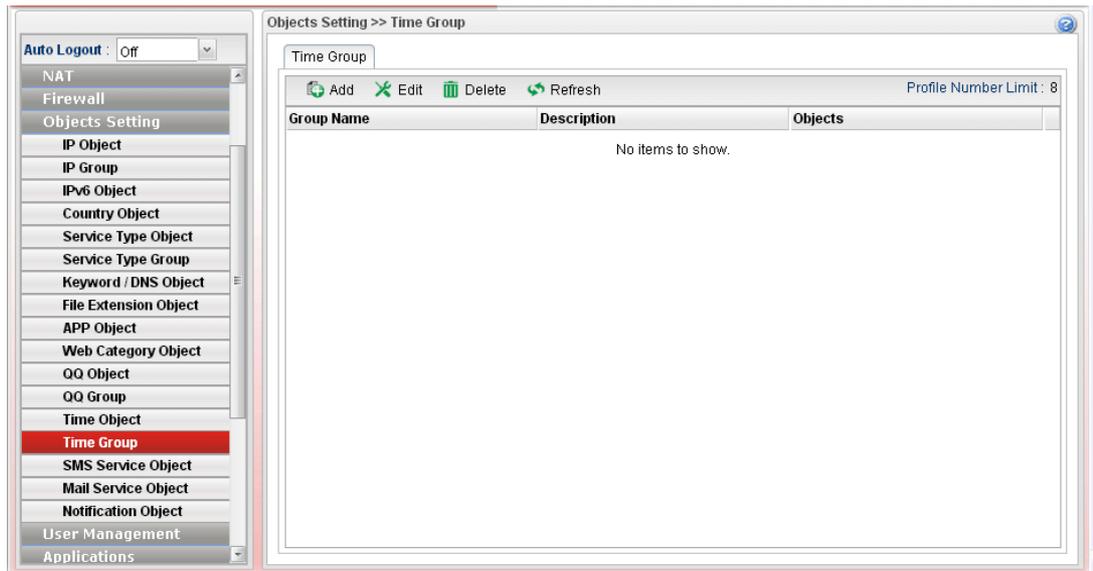
Item	Description
Profile	Type the name of the time object profile. The number of the characters allowed to be typed here is 10.
Frequency	Specify how often (Weekdays or Once) the schedule will be applied.
Start Date	Specify the starting date of the time object profile.
Start Time	Specify the starting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

4.6.14 Time Group

This page allows you to group several time object profiles.

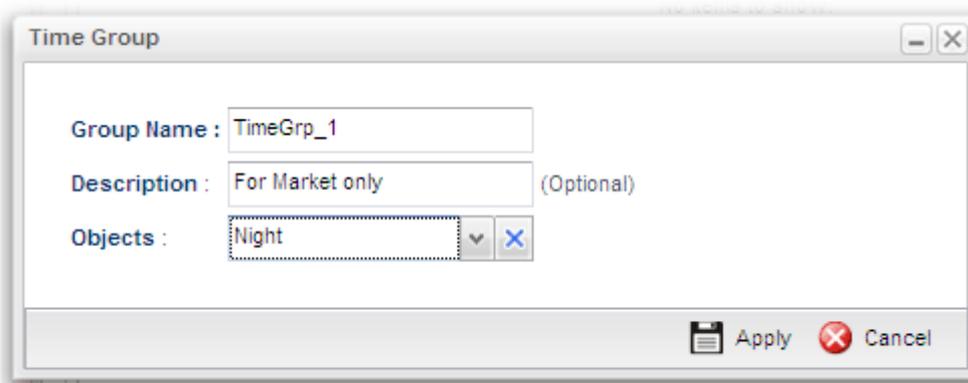


Each item will be explained as follows:

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.

4.6.15 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 (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.
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:

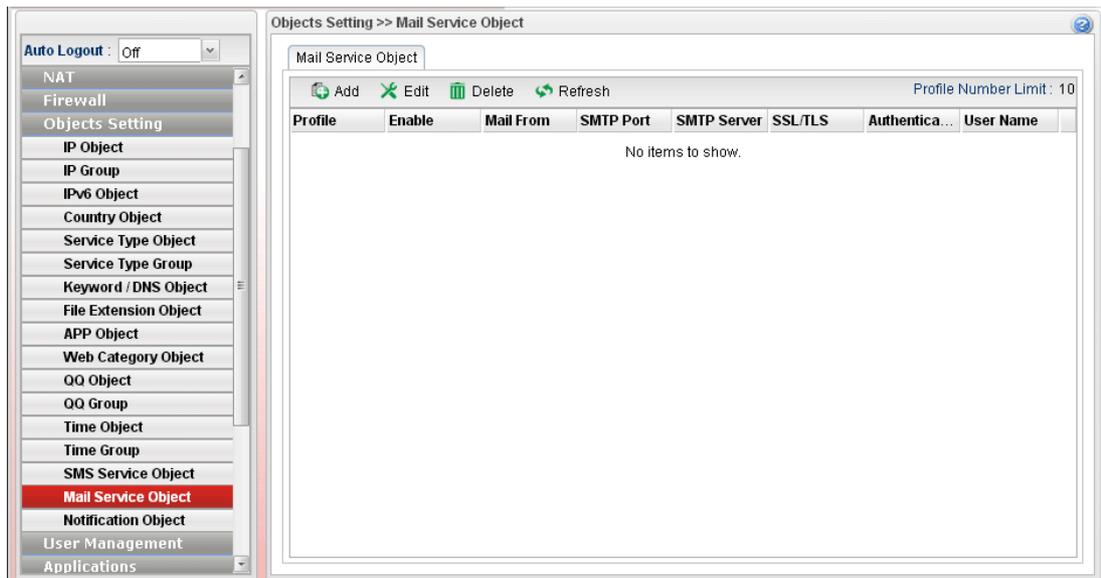
Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.
Enable	Check this box to enable such profile.
SMS Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the 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.

4.6.16 Mail Service Object

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



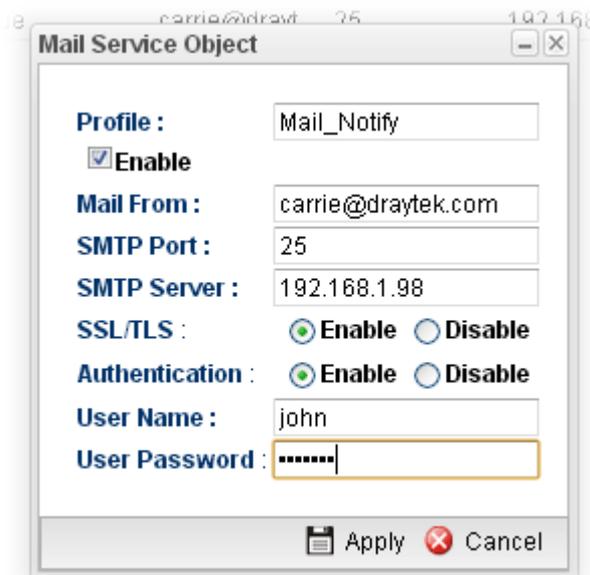
Each item will be explained as follows:

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.

Item	Description
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 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:

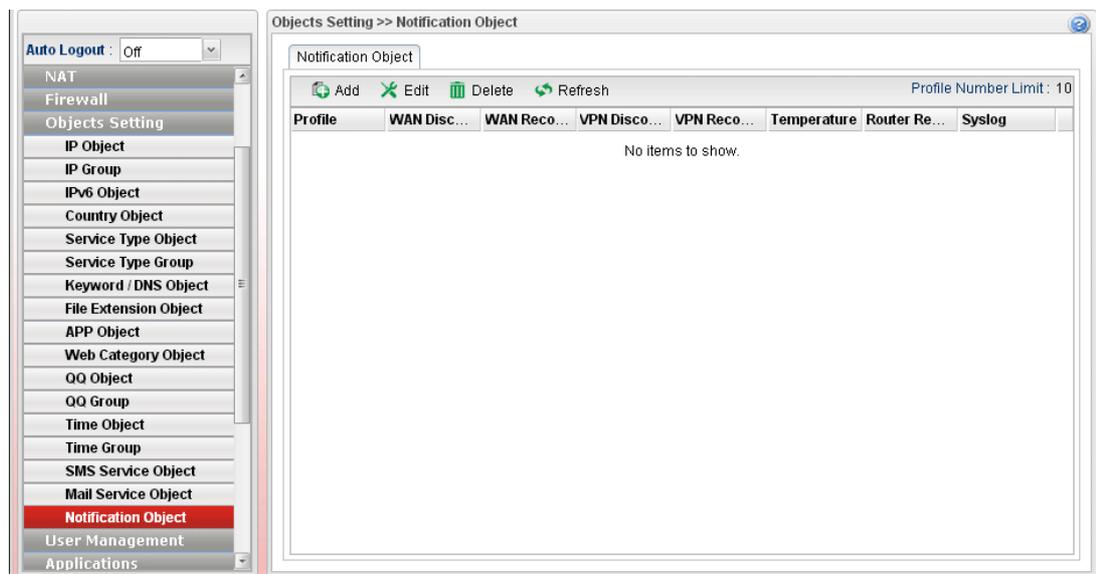
Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.
Enable	Check this box to enable such profile.
Mail From	Type the e-mail address of the sender.
SMTP Port	Type the port number for SMTP server.
SMTP Server	Type the IP address of the mail server.
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.

4.6.17 Notification Object

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



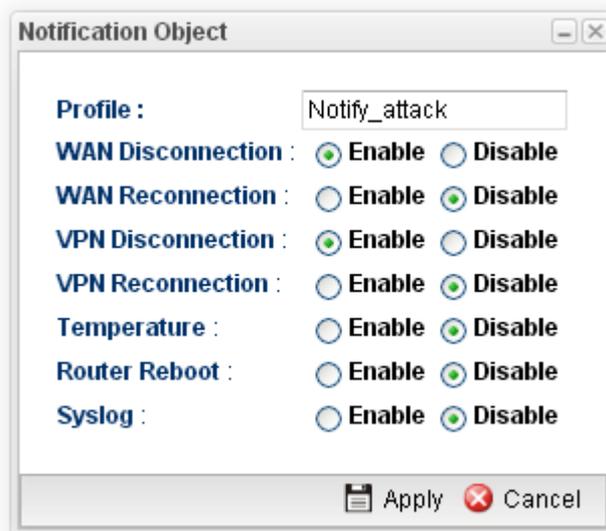
Each item will be explained as follows:

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.

Item	Description
Profile Number Limit	Display the total number (8) 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:

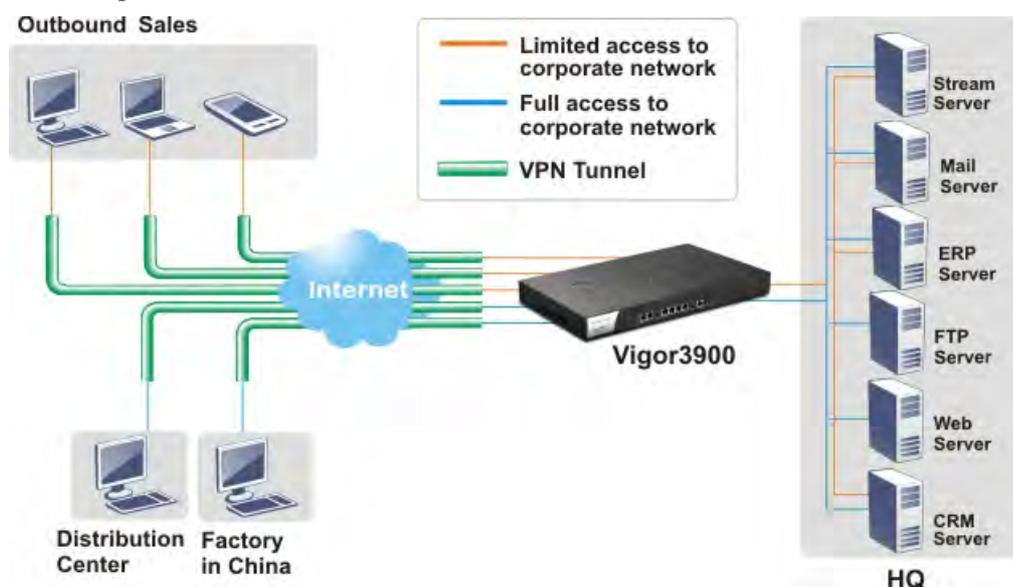
Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters. There are several situations to be monitored by such profile.
WAN Disconnection	Enable – When disconnection happened to WAN interface, the router system will send the alert message 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.
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.

4.7 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

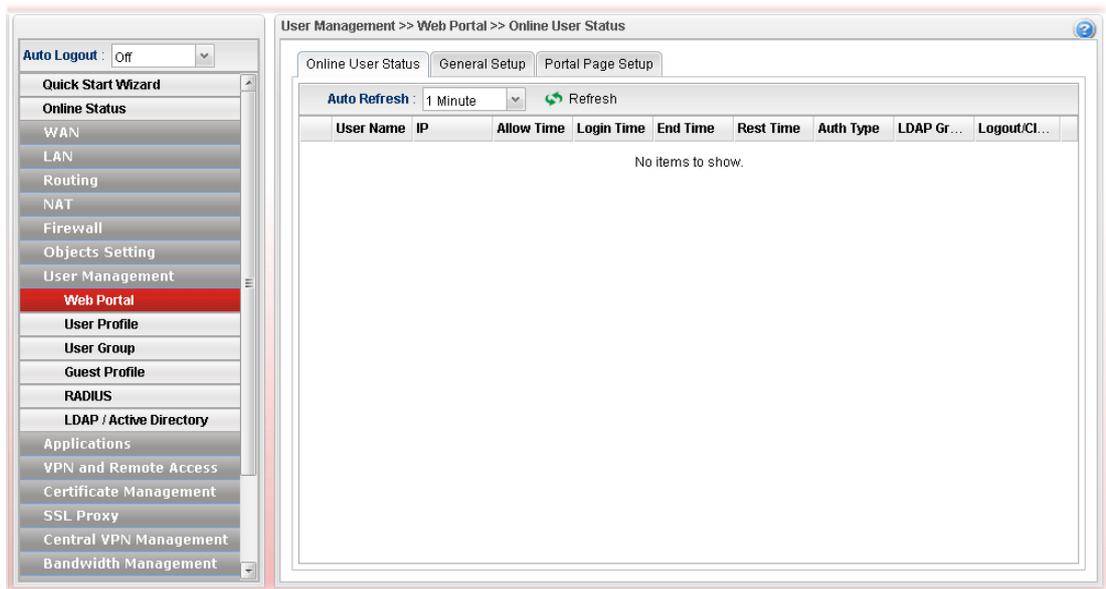
Web Portal is a gateway which organizes the network access of LAN hosts. The identity of LAN host can be recognized by web portal mechanism and then be managed for functions like firewall or load balance.

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.

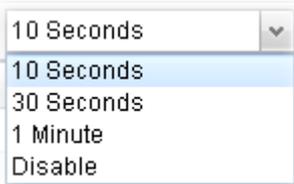
4.7.1.1 Online User Status

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.



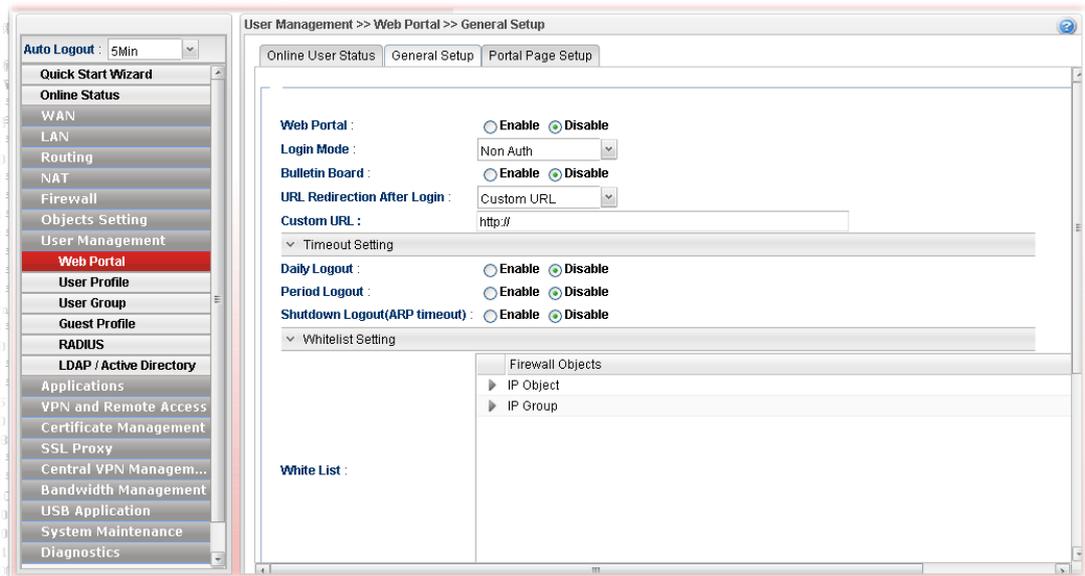
Available parameters will be explained as follows:

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

Item	Description
	log-in user.
Start 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.
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.
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.

Item	Description
Web Portal	Click Enable to enable such function.
	 <p>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.</p>
Bulletin Board	<p>Disable – The function of Bulletin Board is disabled.</p> <p>Enable – The function of Bulletin Board is enabled. The message on the Bulletin Board will be displayed on the screen when the user logs into the web user interface of Vigor router.</p> <p>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.</p> 
URL Redirection After Login	 <p>User Requested – After passed the authentication made by Vigor router, the user will be redirected to original requested web page.</p> <p>Bulletin – If it is selected, users will be forced to see the information displayed on bulletin after passing through web portal.</p> <p>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</p>

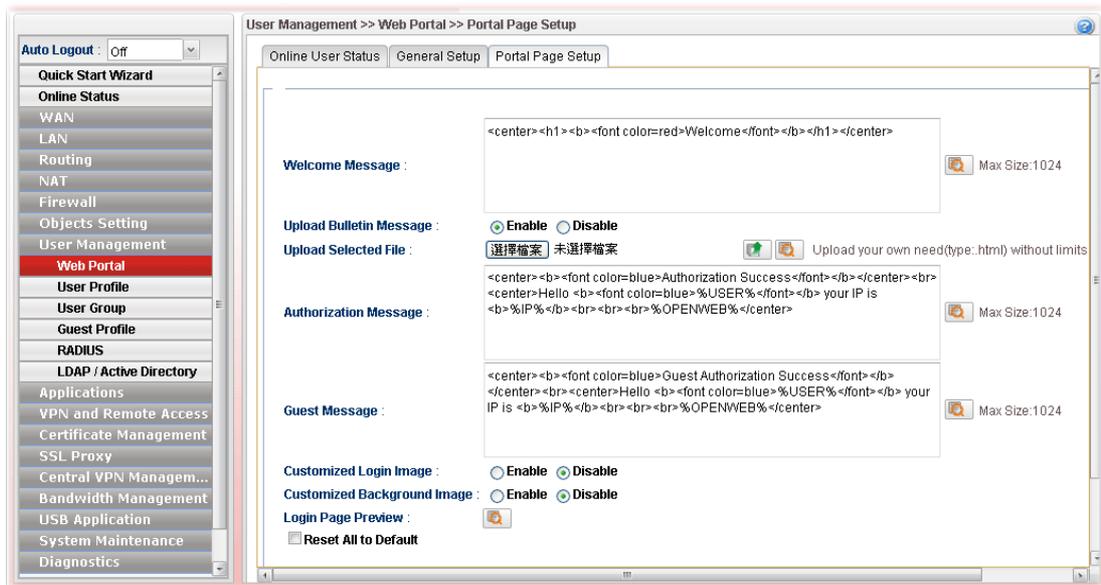
Item	Description
Web Portal	Click Enable to enable such function.
	web page that the hotel wants the user(s) to visit. <ul style="list-style-type: none"> ● Custom URL – Type the URL of specified web page for redirection if Custom URL is selected as URL Redirection After Login.
Daily Logout	Enable - Force the online user logging out the web user interface of Vigor router everyday. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● Period Time to Logout - It is available when Period Logout is enabled.
Shutdown Logout(ARP timeout)	Enable - Force the online user logging out the web user interface of Vigor router when the router shuts down.
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 Vigor2960.
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 .

Item	Description
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.

4.7.2 User Profile

This function allows to configure all accounts (user profiles) in Vigor3900, including PPTP/L2TP/SSL/PPPoE, System user, and so on.

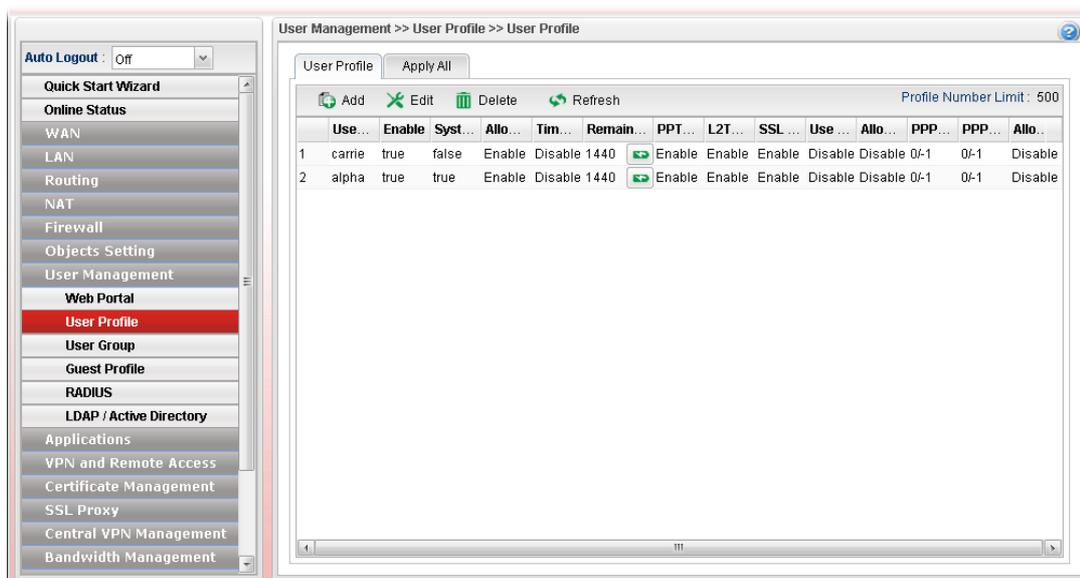
4.7.2.1 User Profile

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.

Item	Description
	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 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.

How to create a new User Profile

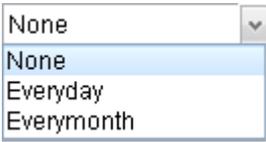
1. Open **User Management>>User Profile**.
2. Simply click the **Add** button.

3. The following dialog will appear.

Available parameters are listed as follows:

Item	Description
Username	Type a name for such user profile (e.g., <i>LAN_User_Group_1</i> , <i>WLAN_User_Group_A</i> , <i>WLAN_User_Group_B</i> , 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., <i>lug123</i> , <i>wug123</i> , <i>wug456</i> , 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	<p>Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router.</p> <p>False – Choose it to disable the function of System User. Such user profile does not have the right to operate the router's function.</p> <p>True – Choose it to enable the function of System User.</p> <p>Privilege Level – If true is selected for System User, you have to specify the privilege level (User/Operator/Admin) for such profile.</p>  <p>Admin has the greatest authority for router operation; User has the smallest authority for router operation.</p>
PPTP/L2TP/SSL/PPPoE 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	
Allow Web Portal Login	<p>Enable – Click it to enable web portal login with such profile.</p> <p>Disable – Click it to disable the option.</p>
Time Quota	<p>Enable – Click it to enable time quota function.</p> <ul style="list-style-type: none"> ● Set Time Quota (min) – Type the time value. ● Remaining Time – Display the remaining time for the user profile. <p>Disable – Click it to disable the function.</p> <p>Note: The range of Time Quota is 1~14400 minutes.</p>
Max Simultaneous Login	<p>It means the maximum online number of clients logging with this profile.</p> <p>The range is from 1 to 255. -1 means not limit; 0 means No access.</p>
PPTP/L2TP/SSL 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.

Use mOTP	<p>Click Enable to make the authentication with mOTP function.</p> <ul style="list-style-type: none"> ● 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).
SSL Proxy	<p>It is available when System User is set with false. The web proxy over SSL will be applied for VPN.</p> <p>To clear the selected one, click  to remove current object selections.</p>
SSL Application (VNC)	<p>It is available when System User is set with false. Choose one of the SSL Application profiles (VNC) for applying into this profile.</p> <p>To clear the selected one, click  to remove current object selections.</p>
SSL Application (RDP)	<p>It is available when System User is set with false. Choose one of the SSL Application profiles (RDP) for applying into this profile.</p> <p>To clear the selected one, click  to remove current object selections.</p>
PPPoE Server	
Allow PPPoE Server Login	<p>Click Enable to activate related PPPoE configuration.</p>
Quota Reset Frequency	<p>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).</p> <p>Everyday – The quota for PPPoE will be reset every day. Everymonth – The quota for PPPoE will be reset every month.</p> 
Time Quota (min)	<p>Type a time quota for PPPoE connection. Note: The range of Time Quota is 1~14400 minutes.</p>
Current Time Used (min)	<p>Display the cumulative amount of time that the user used. Reset - Click it to reset the setting to default value (0).</p>
Traffic Quota(MB)	<p>It is used to set the maximum traffic (MB) for such user profile.</p>
Current Traffic Quota (MB)	<p>Display the cumulative amount of data traffic that the user used. Reset - Click it to reset the setting to default value (0).</p>

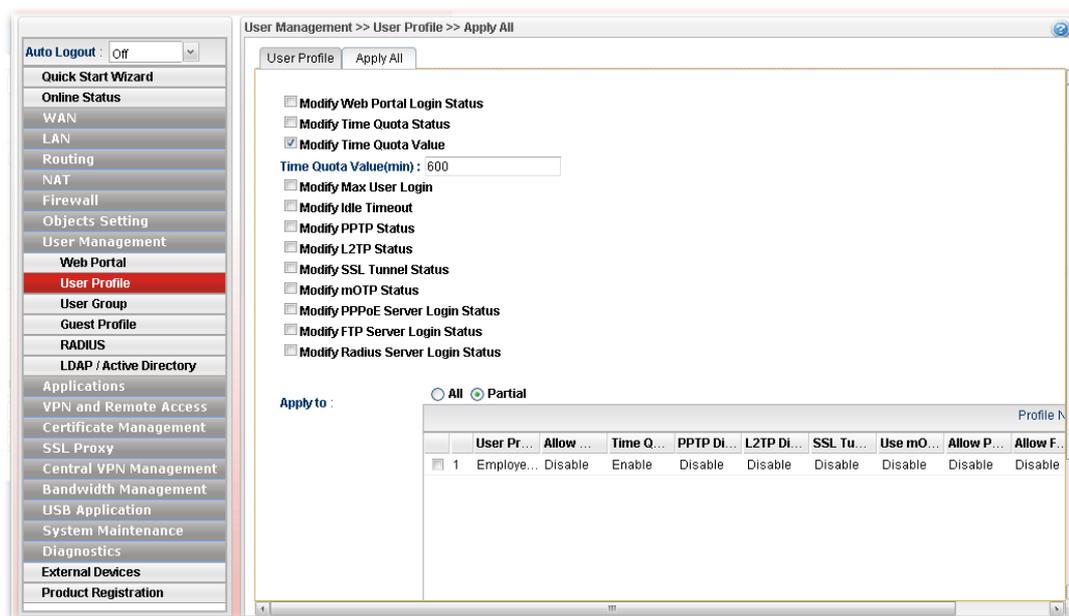
MAC Binding	Specify a MAC address which is limited and used for such PPPoE account. Enable – Click it to enable the function. MAC Address – If MAC Binding is enabled, simply type the MAC address of the router in this field.
FTP User Setting	
Allow FTP Server Login	Click Enable to allow the remote user accessing into Internet via FTP server.
Radius User Setting	
Allow 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 PPPoE/FTP/Radius Server Login	Check the box to configure detailed setting. Enable – Click it to enable the PPPoE/FTP/Radius 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.

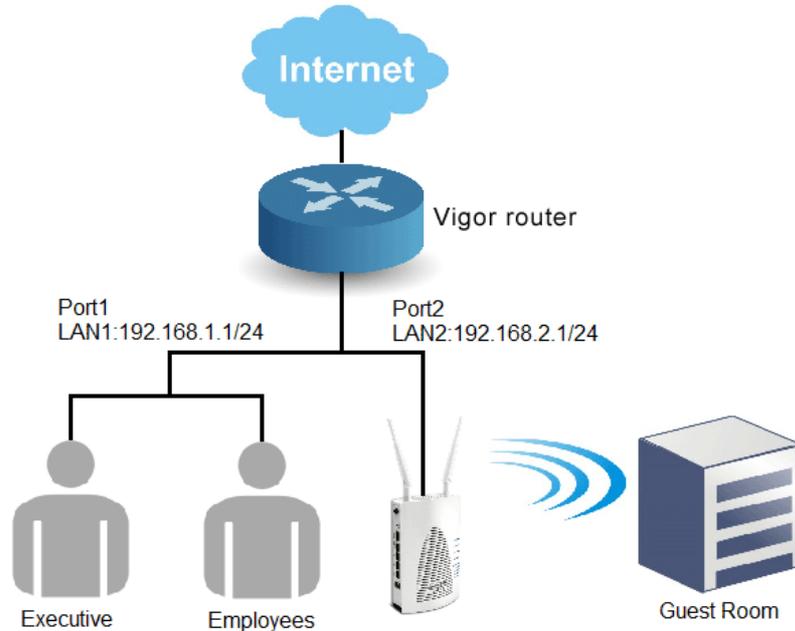
After finished the above settings, click **Apply** to save the configuration.

Example: How to Generate Mass LAN Clients with User Management on Vigor2960/Vigor3900

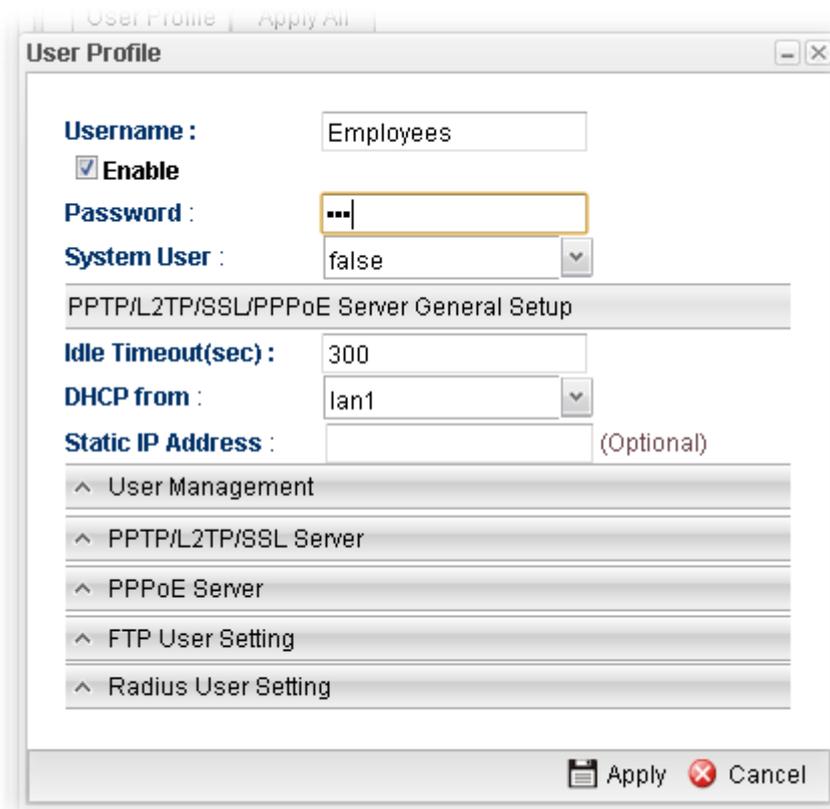
The following table shows the function differences between User Profile and Guest Profile (created by using Mass Guest Generator):

	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

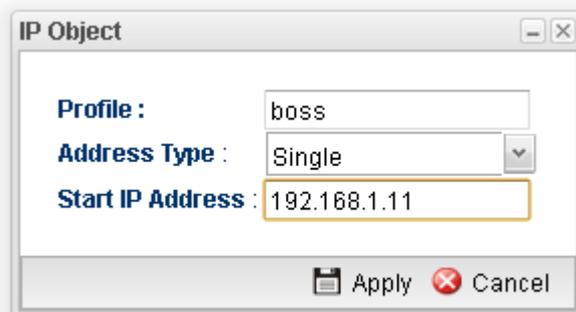
Usage Restriction /Expired Time	Time Quota (1~14400 minutes)	Time Quota (1~14400 minutes) Validity Period (days)
Authentication	YES	YES
Max Simultaneous user	YES	NO
Bind IP	YES	NO



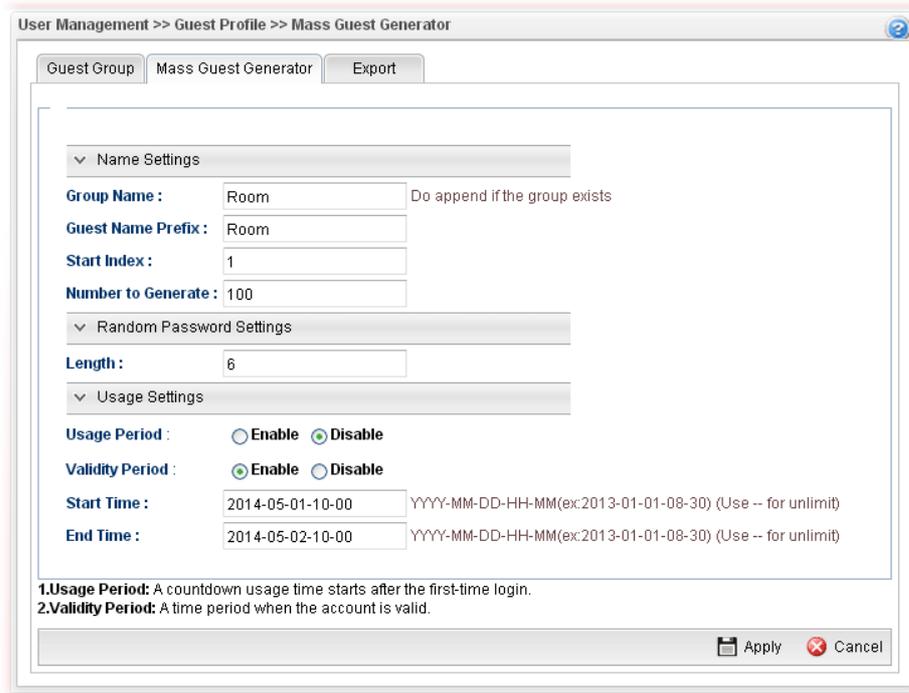
1. Open **User Management >> User Profile**, and click **Add**.
2. Set up user profile as shown below. Type **Username**; check **Enable** and type **Password**. Then, type **Max User Login**. Click **Apply** to save the settings.



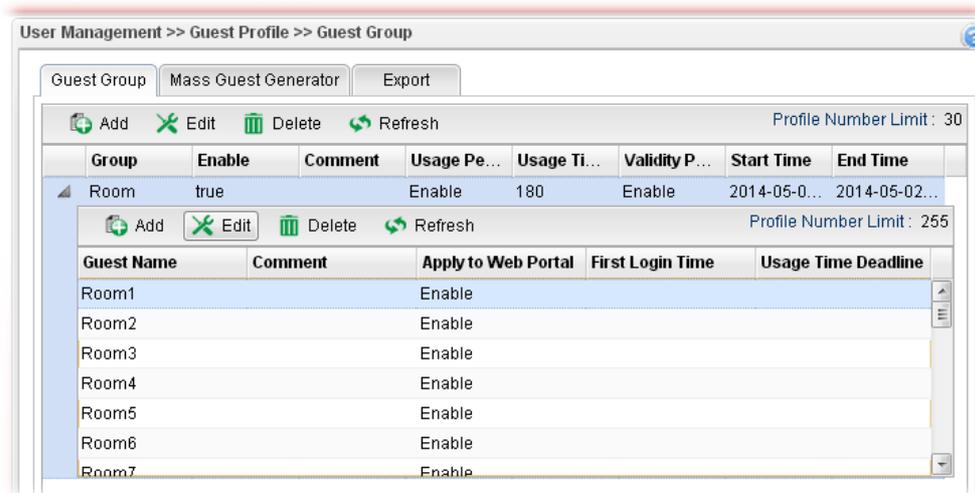
3. Open **Objects Setting >> IP Object**, and click **Add**.
4. Set up **IP Object** for Executive. Type the name of the **Profile** (e.g., boss in this case); choose Single as the **Address Type**; and type 192.168.1.11 as **Start IP Address**. Click **Apply** to save the settings.



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.



- 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.

Username

Guest Name : Room1

Comment : (Optional)

Password : Audyzi

Apply to Web Portal : Enable Disable

Clean Deadline

Apply Cancel

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.

User Management >> Guest Profile >> Export

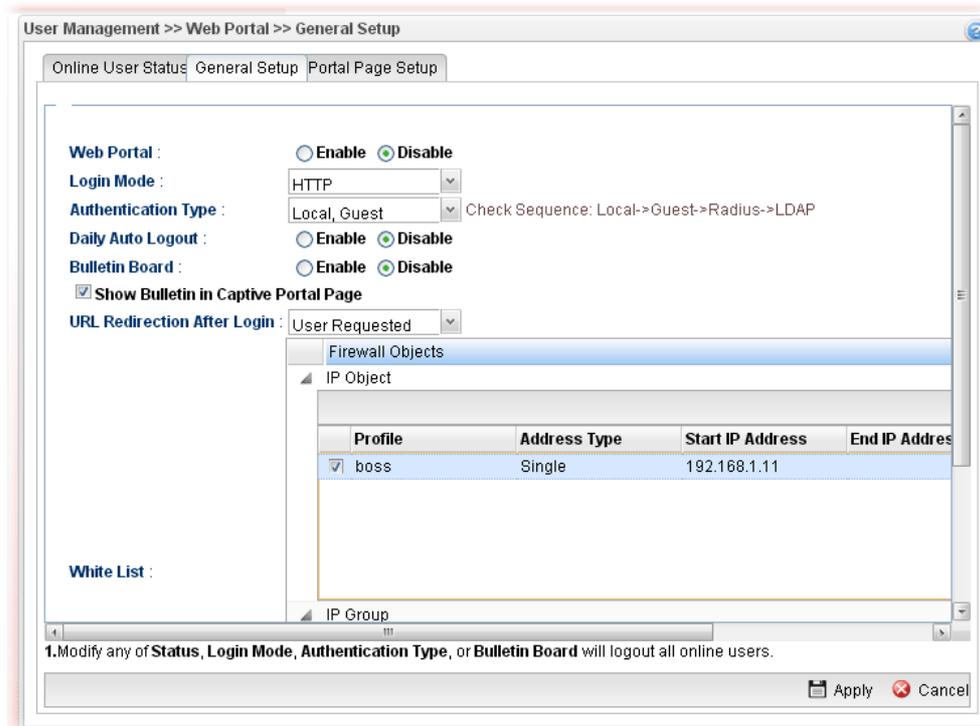
Guest Group Mass Guest Generator Export

Guest Group : Room

Export File Name : V3900_2014-08-26 .CSV

	A1	Name
	A	B
1	Name	Password
2	Room1	Audyzi
3	Room2	H7LFGw
4	Room3	3ASAWq
5	Room4	7JptaZ
6	Room5	mcFdeb
7	Room6	iJv18V
8	Room7	uJSagu
9	Room8	w9UjDK
10	Room9	zElNXq
11	Room10	IftiiB
12	Room11	jrBJGe
13	Room12	v1Nh6U
14	Room13	...

- 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.



- After finishing configuration, Vigor3900 will redirect users to the authentication page when they try accessing to the Internet.

For Employees to access into Internet:

Welcome

Username

Password

Login

Powered by DrayTek Corp. Copyright © 2014. All rights reserved.



For Room guest to access into Internet:

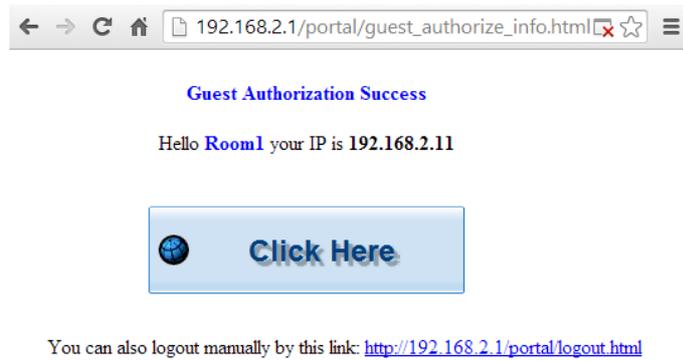
Welcome

Username

Password

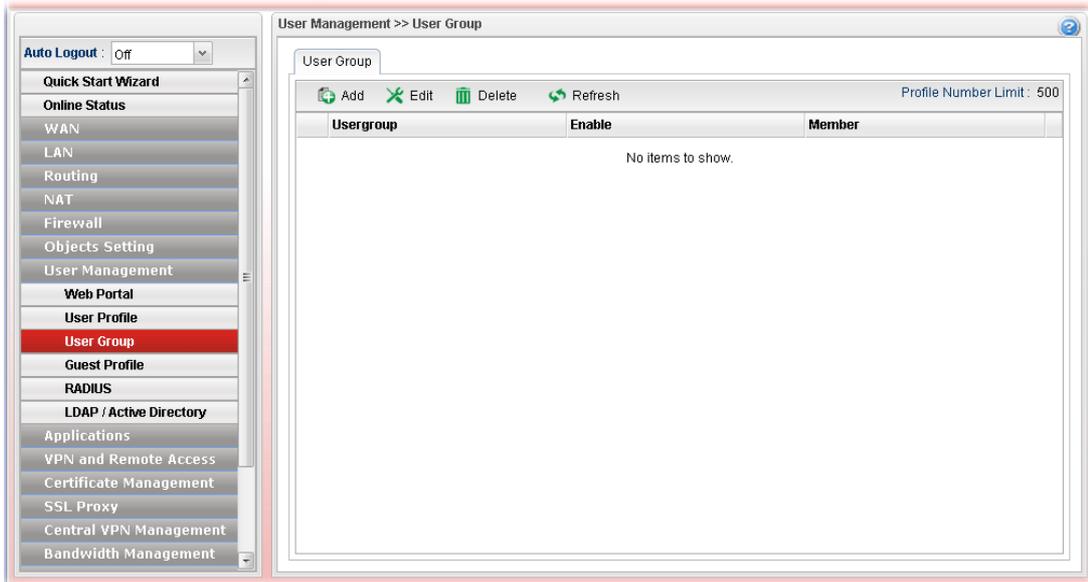
Login

Powered by DrayTek Corp. Copyright © 2014. All rights reserved.



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.

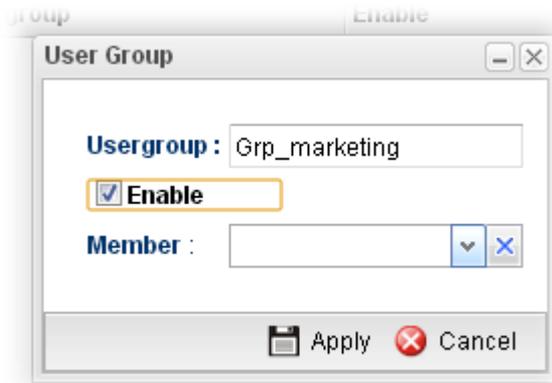


Each item will be explained as follows:

Item	Description
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:

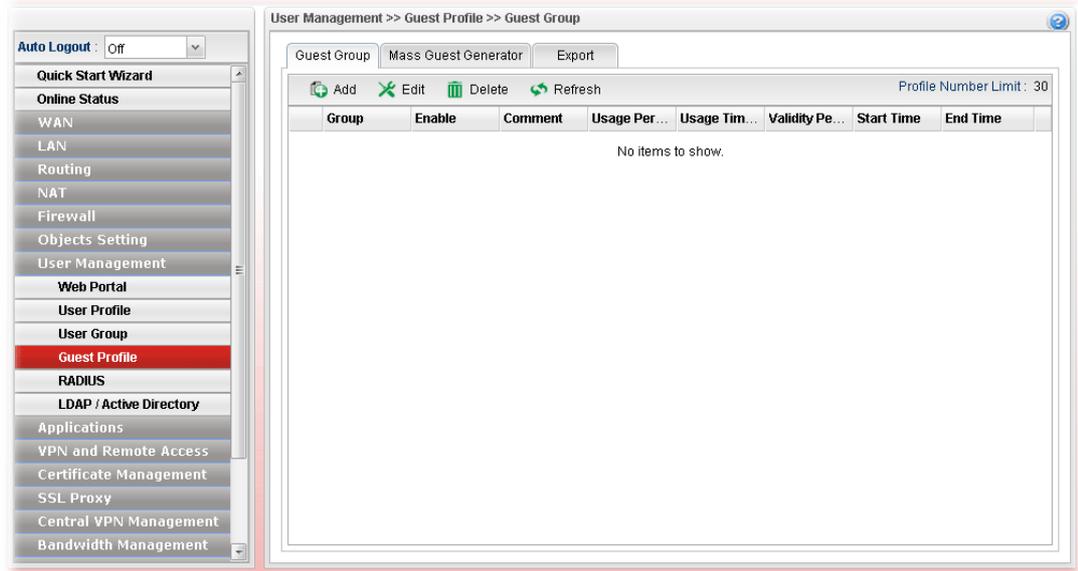
Item	Description
Usergroup	Type the name of such profile.
Enable	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group. To clear the selected one, click  to remove current object selections.
Apply	Click it to save the configuration.
Cancel	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



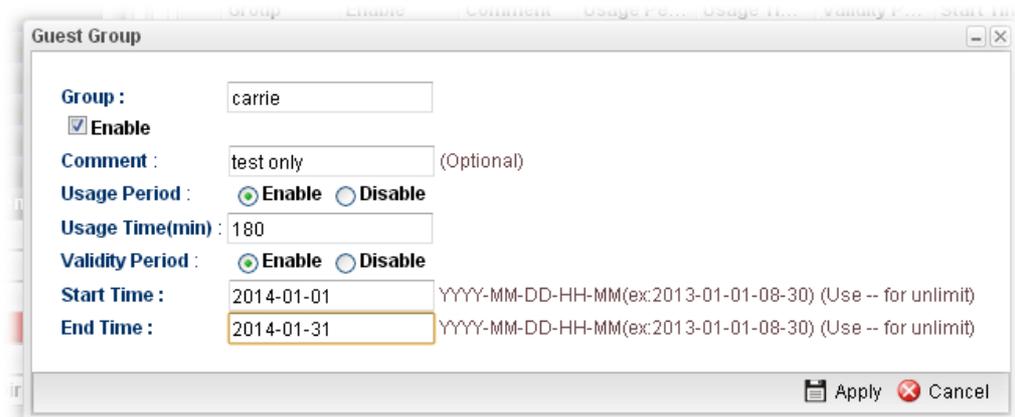
Available parameters are listed as follows:

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.
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.
Validity Period	Display the valid period for the guest accessing into Internet.

Item	Description
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:

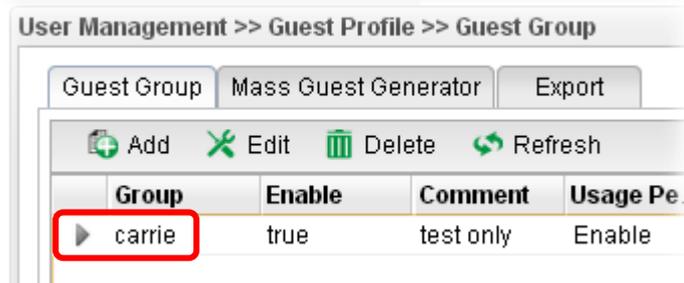
Item	Description
Group	Type the name of such profile.
Enable	Check this box to enable such profile.
Comment	Give a brief description for the profile.
Usage Period	It determines the usage time for the guest accessing into Internet each time. Click Enable to enable such option. Usage Time(min) - Determines 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.
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**.

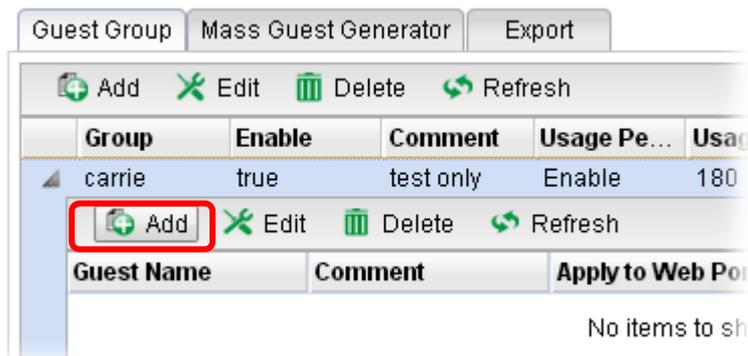
5. A new guest group profile has been created.



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	Enable – Click it to make such profile being applied to web

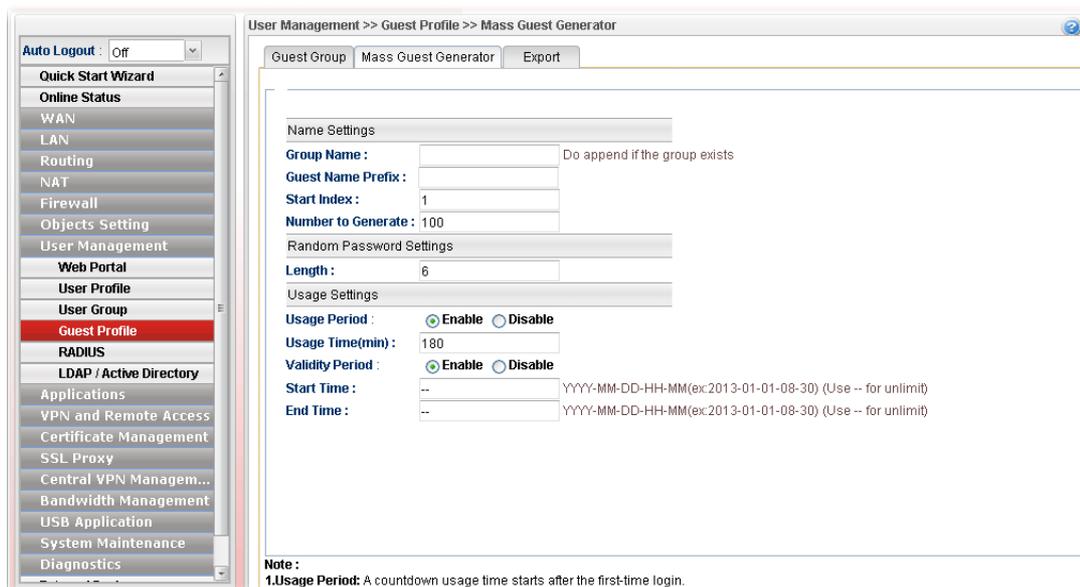
Portal	portal. Disable – Click it to disable the option.
Clean Deadline	The guest profile can be unlocked to be used by other users.

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).

The screenshot shows a web interface for configuring guest profiles. At the top, there are tabs for 'Guest Group', 'Mass Guest Generator', and 'Export'. Below the tabs is a toolbar with 'Add', 'Edit', 'Delete', and 'Refresh' icons, and a 'Profile Number Limit : 30' indicator. The main content area contains a table with the following columns: Group, Enable, Comment, Usage Pe..., Usage Ti..., Validity P..., Start Time, and End Time. A row is highlighted for the 'carrie' group, with values: true, test only, Enable, 180, Enable, 2014-01-01, 2014-01-31. Below this table is another toolbar with 'Add', 'Edit', 'Delete', and 'Refresh' icons, and a 'Profile Number Limit : 255' indicator. At the bottom, there is another table with columns: Guest Name, Comment, Apply to Web Portal, First Login Time, and Usage Time Deadl... A row is highlighted for the 'Mark' guest, with values: Practice, Enable.

4.7.4.2 Mass Guest Generator

This option is useful to create a lot of guest profiles with the most expeditious manner.



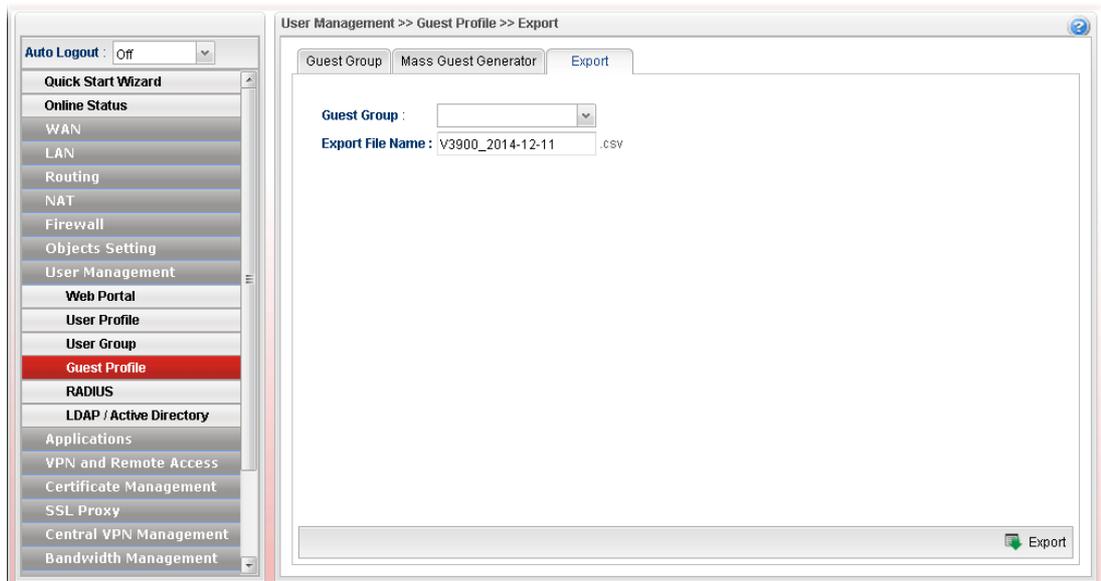
Available parameters are listed as follows:

Item	Description
Name Settings	<p>Group Name – Type the name of the guest group.</p> <p>Guest Name Prefix – The guest names created with such manner requires a prefix as the basis of name input.</p> <div style="border: 1px solid black; padding: 2px;"> <p>Note: Guest Name Prefix disallows these 6 characters "<code>^?\$.%&</code>".</p> </div> <p>Start Index – Type a number which will be treated as the starting number for generating mass guest profiles.</p> <div style="border: 1px solid black; padding: 2px;"> <p>Note: The range of Start index is 1~10000.</p> </div> <p>Number to Generate – Type the total number of guests to be generated at one time.</p> <p>The guest name will be named by combining “Guest Name Prefix” + “Start Index”, for example:</p> <p>Guest Name Prefix => teashop_ Start Index => 100 Number to Generate => 50</p> <p>Then, the guests names generated will be:</p> <p>teashop_100 (starting) teashop_101 teashop_102 ... teashop_150 (ending)</p>
Random Password Settings	<p>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.</p>

Item	Description
Usage Settings	<p>Usage Period –It determines the usage time for the guest accessing into Internet each time. Click Enable to enable such option.</p> <ul style="list-style-type: none"> ● Usage Time(min)-The default setting is 180 minutes. <p>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.</p> <ul style="list-style-type: none"> ● Start Time/End Time – Specify the valid period by typing the time with the format of HH-MM-SS.
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.

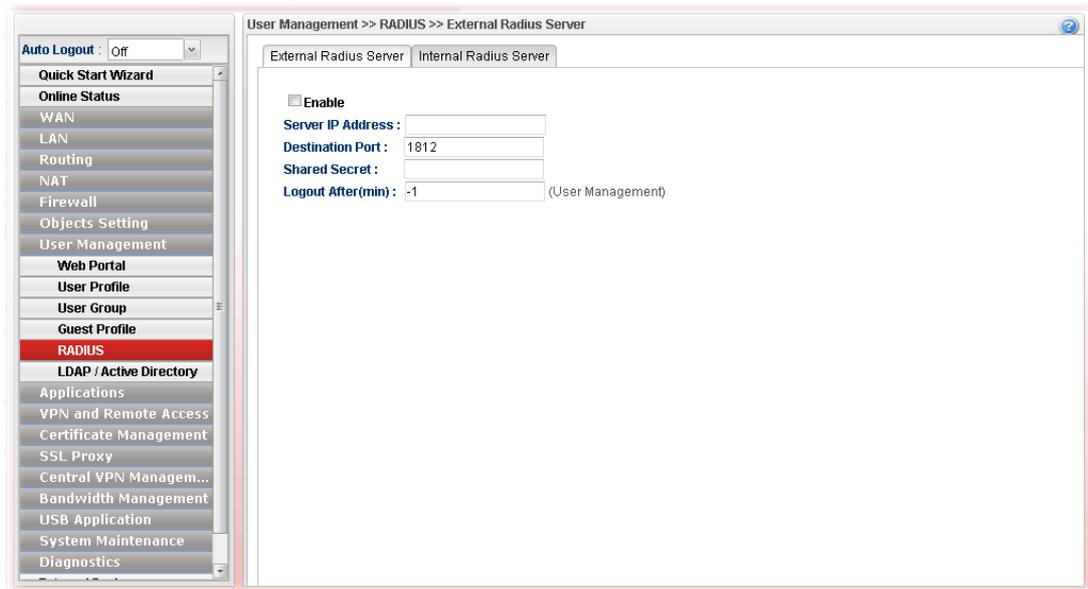
4.7.5 RADIUS

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.



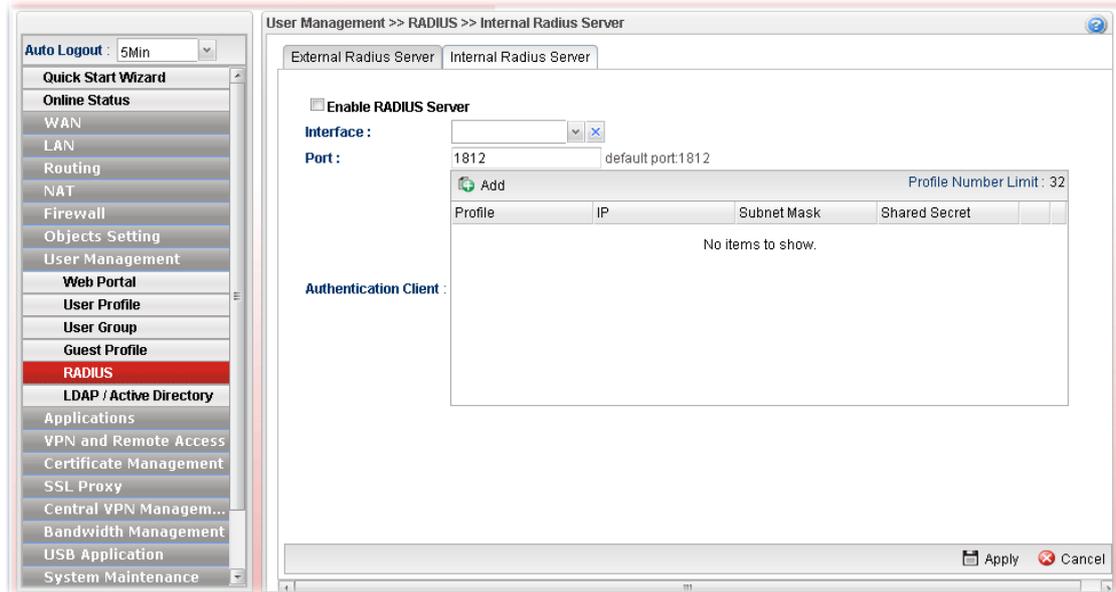
Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
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 Internal 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.

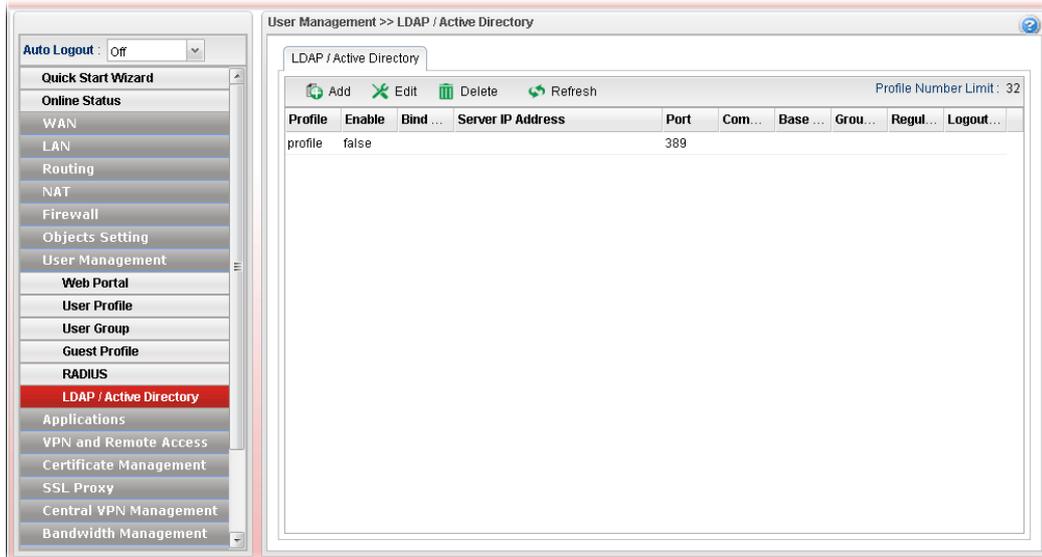
After finished the above settings, click **Apply** to save the configuration.

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.

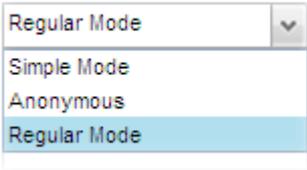
Item	Description
Port	Display the port number set for such profile.
Common Name Identifier	Display the name for identification.
Base DN	Display the configured Base DN if Bind Type is set with Simple Mode.
Group DN	Display the configured Group DN if Bind Type is set with Simple Mode.
Regular DN	Display the configured regular DN if Bind Type is set with Regular Mode.
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:

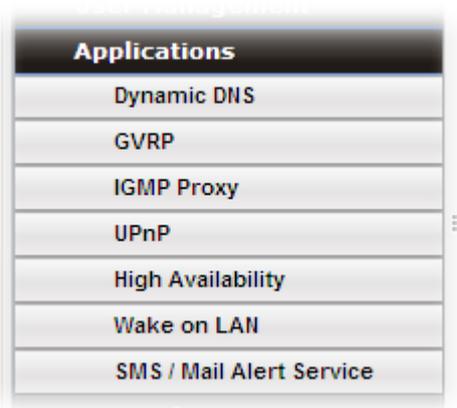
Item	Description
Profile	Type a name for such profile.
Enable This Profile	Check this box to enable such profile.

Bind Type	<p>There are three types of bind type supported.</p>  <p>Simple Mode – Just simply do the bind authentication without any search action.</p> <p>Anonymous – Perform a search action first with Anonymous account then do the bind authentication.</p> <p>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.</p> <p>For the regular mode, you’ll need to type in the Regular DN and Regular Password.</p>
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.



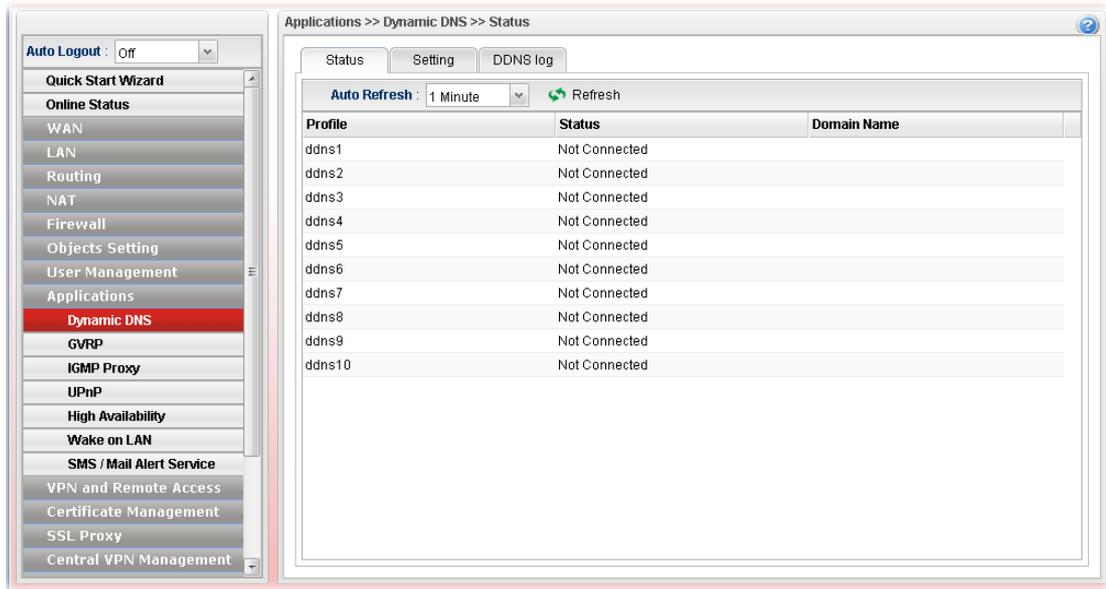
4.8.1 Dynamic DNS

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.

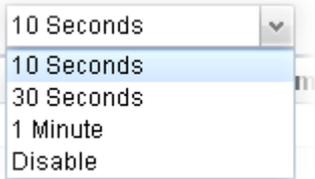
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to ten accounts from eight different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers 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.

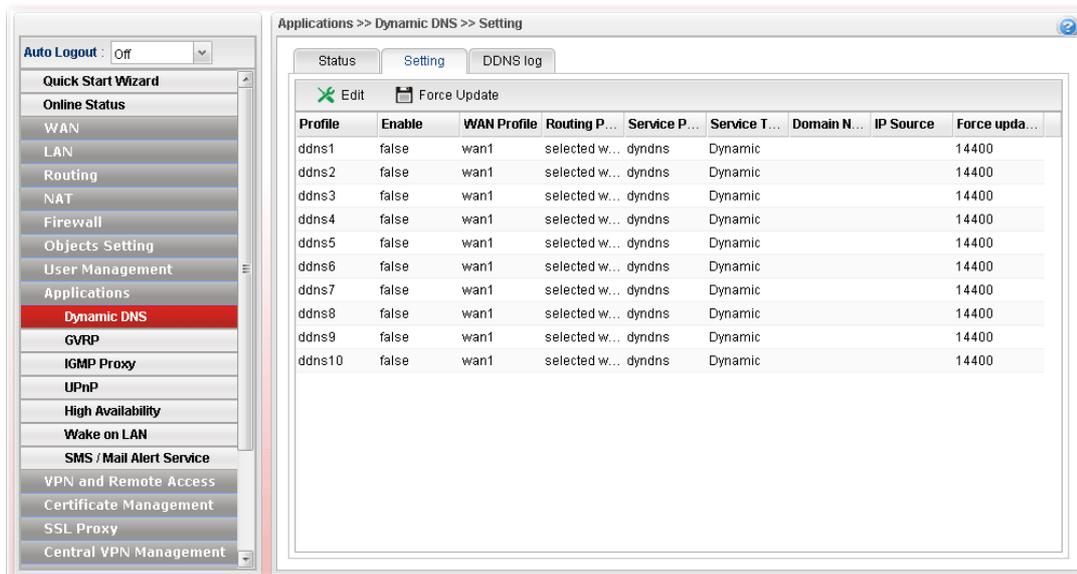


Each item will be explained as follows:

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:

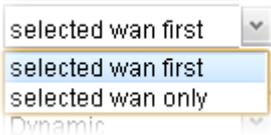
Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Force Update	Force the router updates its information to DDNS server 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.

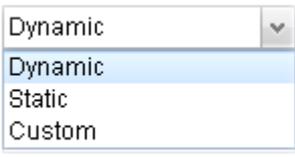
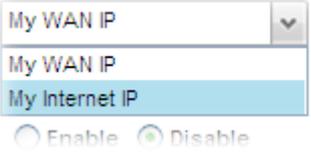
How to edit a DDNS Profile

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.

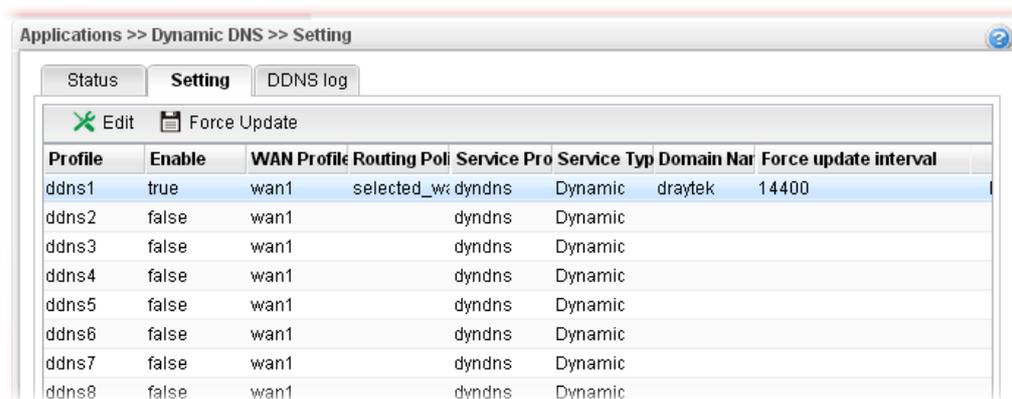
1. Open **Applications>>Dynamic DNS** and click the **Setting** tab.
2. Choose one of the DDNS profiles and click the **Edit** button.

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	<p>Choose a routing policy applied to the DDNS profile.</p>  <p>selected wan first – The DDNS profile will be applied to the traffic via WAN interface first, then applied to other interface.</p> <p>selected wan only – The DDNS profile will be applied to the traffic via WAN interface only. No other interface will be used.</p>
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.



Applications >> Dynamic DNS >> Setting

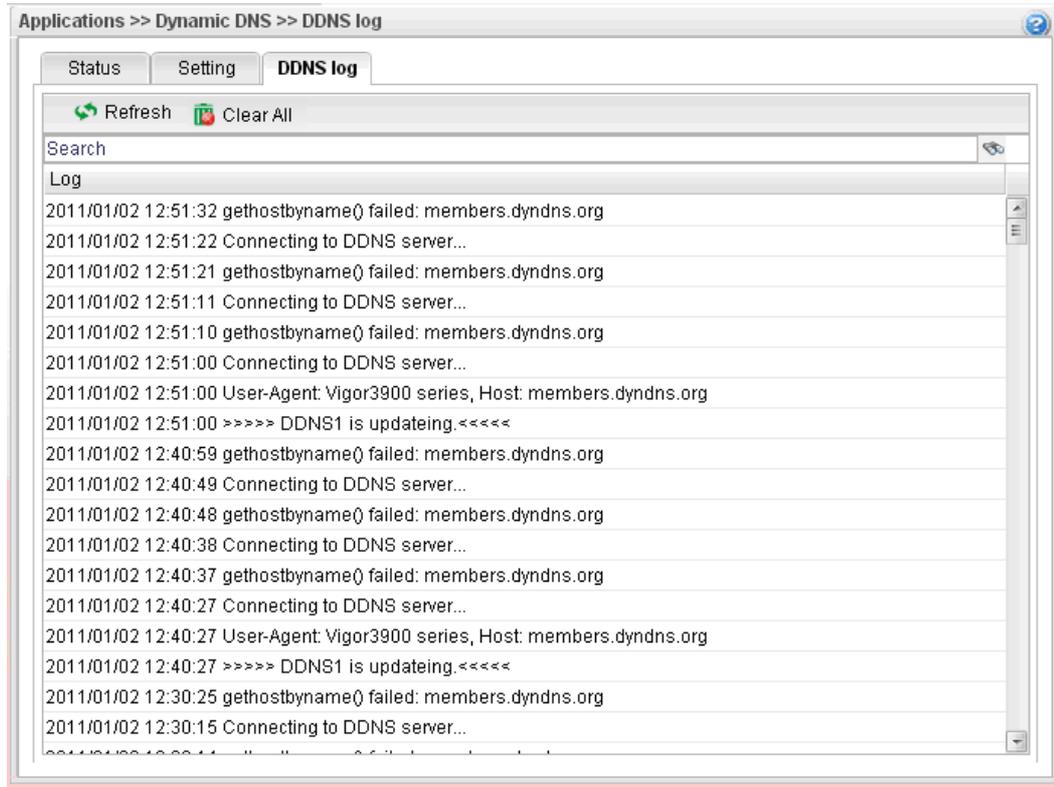
Status **Setting** DDNS log

Edit Force Update

Profile	Enable	WAN Profile	Routing Pol	Service Pro	Service Typ	Domain Nar	Force update interval
ddns1	true	wan1	selected_wx	dyndns	Dynamic	draytek	14400
ddns2	false	wan1		dyndns	Dynamic		
ddns3	false	wan1		dyndns	Dynamic		
ddns4	false	wan1		dyndns	Dynamic		
ddns5	false	wan1		dyndns	Dynamic		
ddns6	false	wan1		dyndns	Dynamic		
ddns7	false	wan1		dyndns	Dynamic		
ddns8	false	wan1		dyndns	Dynamic		

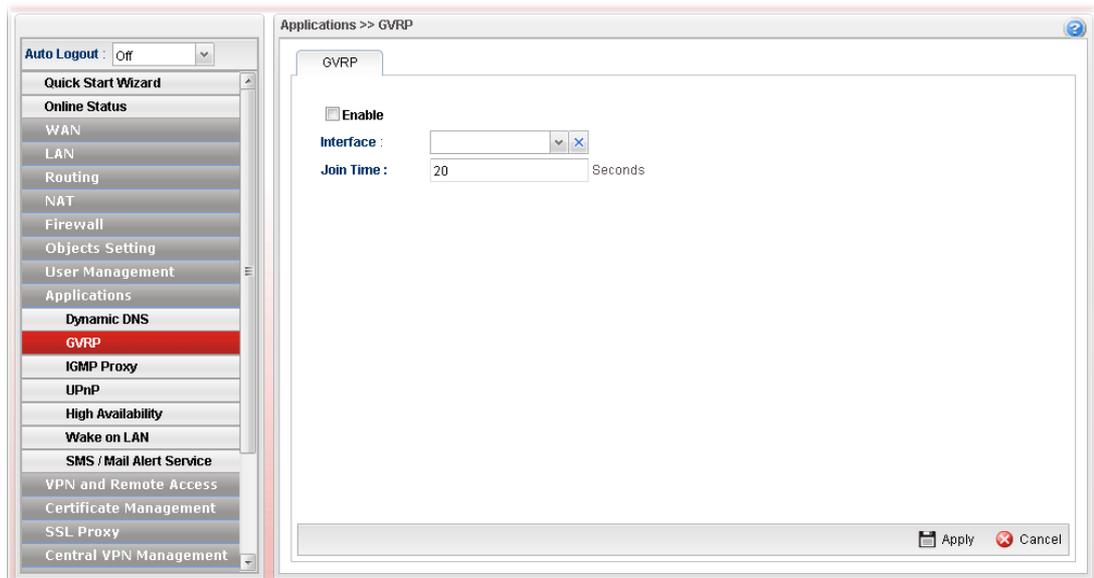
4.8.1.3 DDNS Log

This page displays the information related to all DDNS.



4.8.2 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.



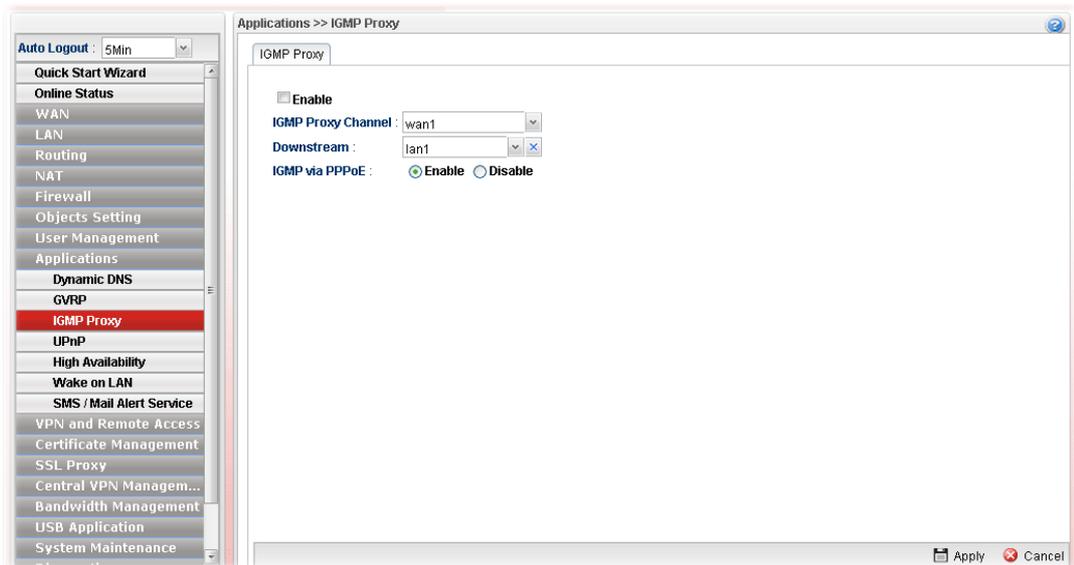
Available parameters are listed as follows:

Item	Description
------	-------------

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.

4.8.3 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.



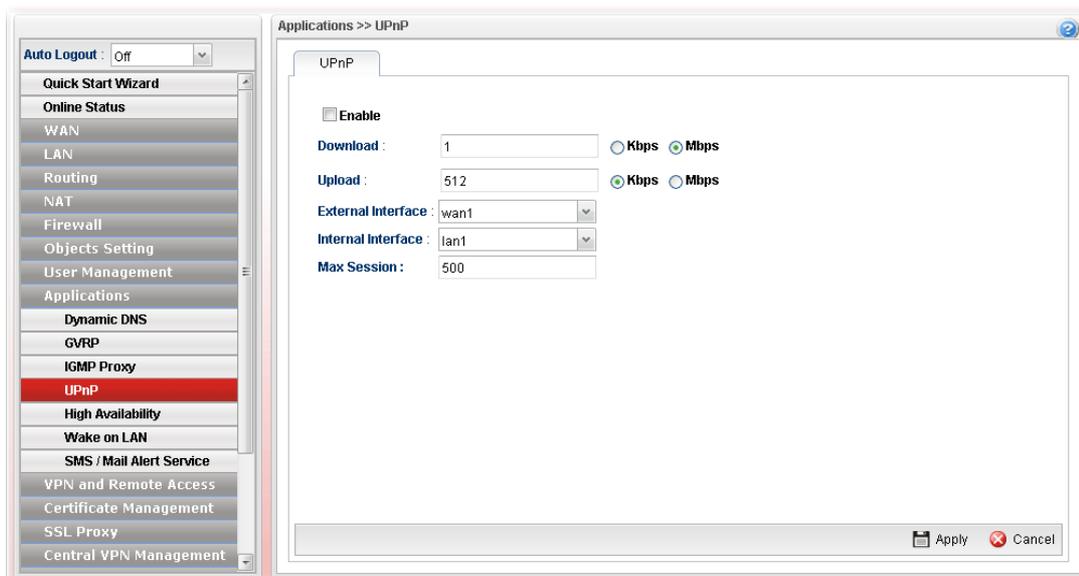
Available parameters are listed as follows:

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).

Item	Description
IGMP via PPPoE	<p>Enable – In LAN, the PC which uses PPPoE connection to communicate with Vigor router can accept the packets transmitted from IGMP proxy.</p> <p>Disable –In LAN, the PC which uses PPPoE connection to communicate with Vigor router can NOT accept the packets transmitted from IGMP proxy.</p> <ul style="list-style-type: none"> ● 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.

4.8.4 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.

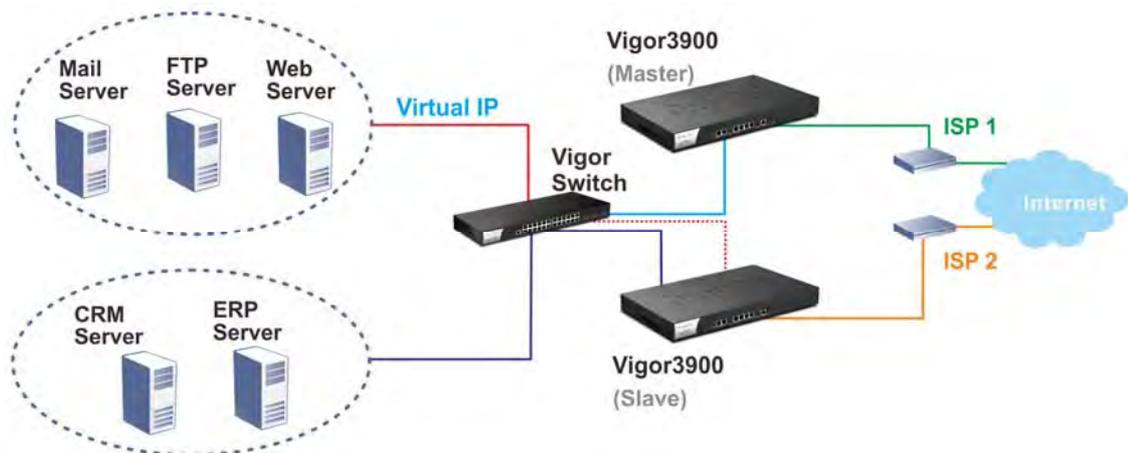
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.8.5 High Availability

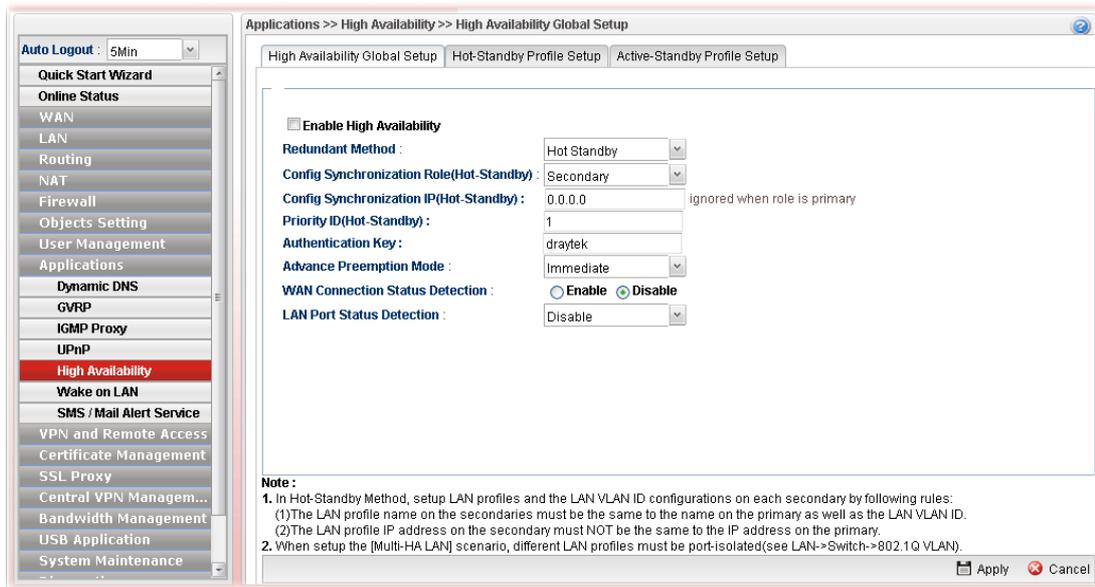
The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, provide nearly full-time availability, typically have redundant hardware 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.

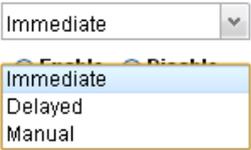
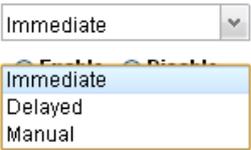


4.8.5.1 High Availability Global Setup



Available parameters are listed as follows:

Item	Description
Enable High Availability	Check this box to enable HA function.
Redundant Method	<p>Choose Hot-Standby or Active-Standby as the method for HA.</p> <p>Hot-Standby</p> <p>Hot-Standby Active-Standby</p> <p>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.</p> <p>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.</p>
Settings under Hot-Standby	<p>Config Synchronization Role(Hot-Standby) – Specify the role for such Vigor router.</p> <p>Primary</p> <p>Primary Secondary</p> <p>Primary – It means such Vigor router is treated as the primary device (master device).</p> <p>Authentication Key – Type a string as the authentication key.</p>

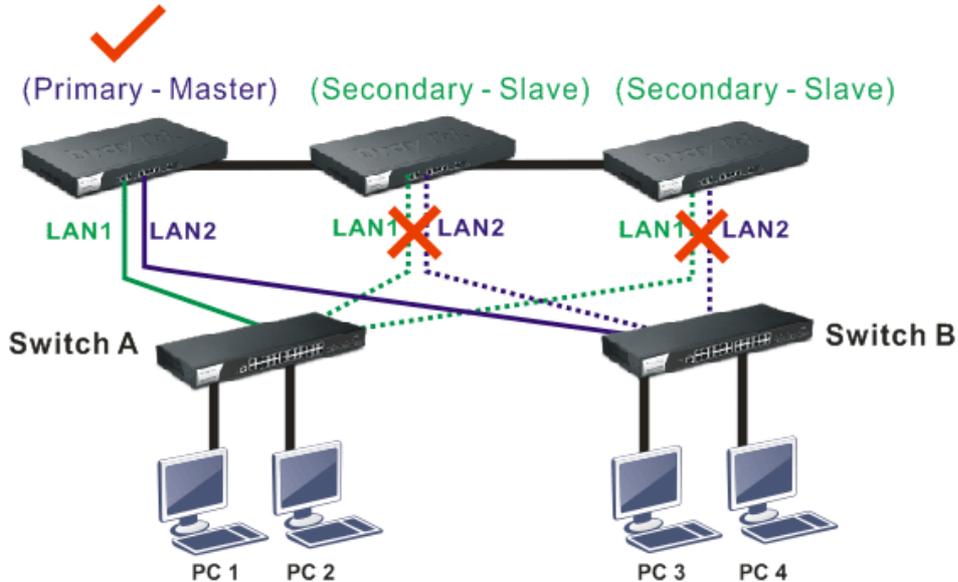
Item	Description
	<p>It is used for encrypting the HA session communication to prevent malicious attack.</p> <p>Advance Preemption Mode – Specify a mode for changing the Config Synchronization Role.</p> <p>Advance Preemption Mode : </p> <ul style="list-style-type: none"> ● Automatic – The router will 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. <p>If the router is set as Primary (Master) router, and you change the Manual Preemption Status from Active to Inactive. Once the router (Primary) 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:</p> <ol style="list-style-type: none"> 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 (primary) router existing, then Manual Preemption Status will be reset to Active to locate the master router.
	<p>Secondary – It means such Vigor router is treated as the secondary device (slave device). The secondary router will copy the configuration from the primary router to make itself as primary.</p>
	<p>Authentication Key – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack.</p> <p>Advance Preemption Mode – Specify a mode for changing the Config Synchronization Role.</p> <p>Advance Preemption Mode : </p> <ul style="list-style-type: none"> ● Automatic – The router will be restored to primary

Item	Description
	<p>(master) router once the service is restored.</p> <ul style="list-style-type: none"> ● 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. <p>If the router is set as Primary (Master) router, and you change the Manual Preemption Status from Active to Inactive. Once the router (Primary) 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:</p> <ol style="list-style-type: none"> 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 (primary) router existing, then Manual Preemption Status will be reset to Active to locate the master router. <hr/> <p>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:</p> <div data-bbox="655 1341 922 1440" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>Disable At Least One Up All Must Be Up</p> </div> <ul style="list-style-type: none"> ● 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. <hr/> <p>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.</p>
Settings under Active-Standby	<p>Authentication Key – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack.</p> <p>WAN Connection Status Detection – Click Enable to make the router detecting WAN connection status. It is similar to</p>

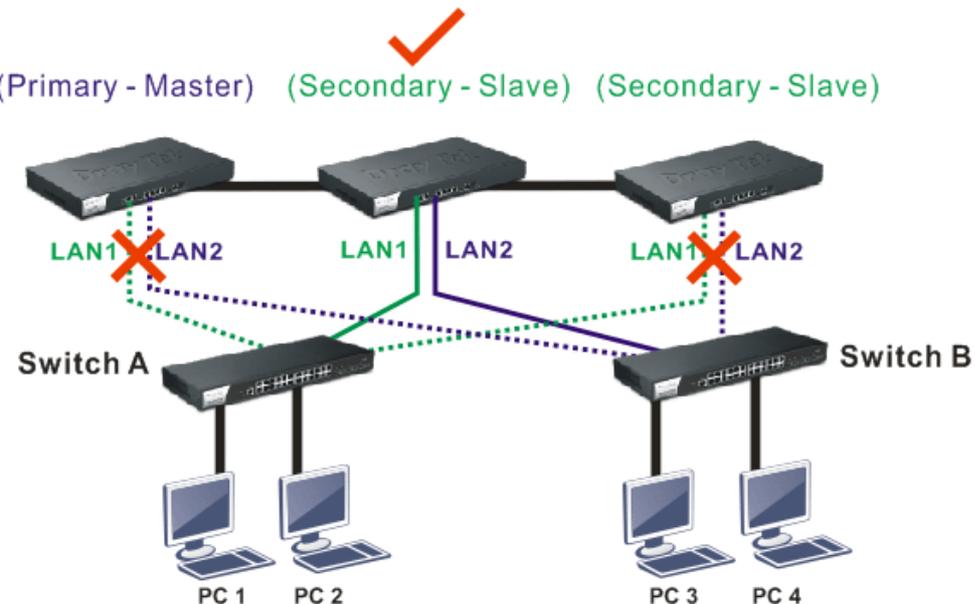
Item	Description
	"LAN Port Detection Mode" but will detect connection status of all enabled WAN profiles. If connection status of all enabled WAN profiles are down , the master router hands off its position.

4.8.5.2 Hot-Standby Mechanism

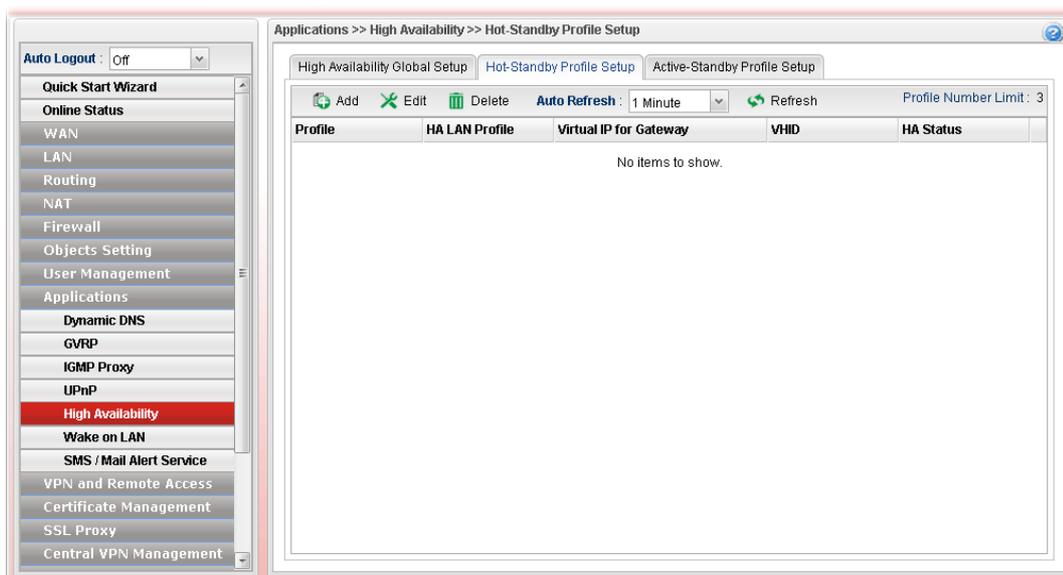
The hot-standby mechanism is that each secondary access point will be a backup device for the primary access point (router). When the primary device fails, one of the rest ones will be elected as the new master device.



When the Master device fails, one of the slave devices will be chosen as the Master device to offer the network service for the connected PCs.



The following page is used to create Hot-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.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.

How to create a new HA Hot-Standby Profile

1. Open **Applications>>High Availability** and click the **Hot-Standby Profile Setup** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.

The screenshot shows a window titled "Hot-Standby Profile Setup". It contains the following fields and values:

- Profile :** HA_1
- HA LAN Profile :** lan1
- Virtual IP for Gateway :** 192.168.1.55
- VHID :** 1

At the bottom of the window, there are two buttons: "Apply" and "Cancel".

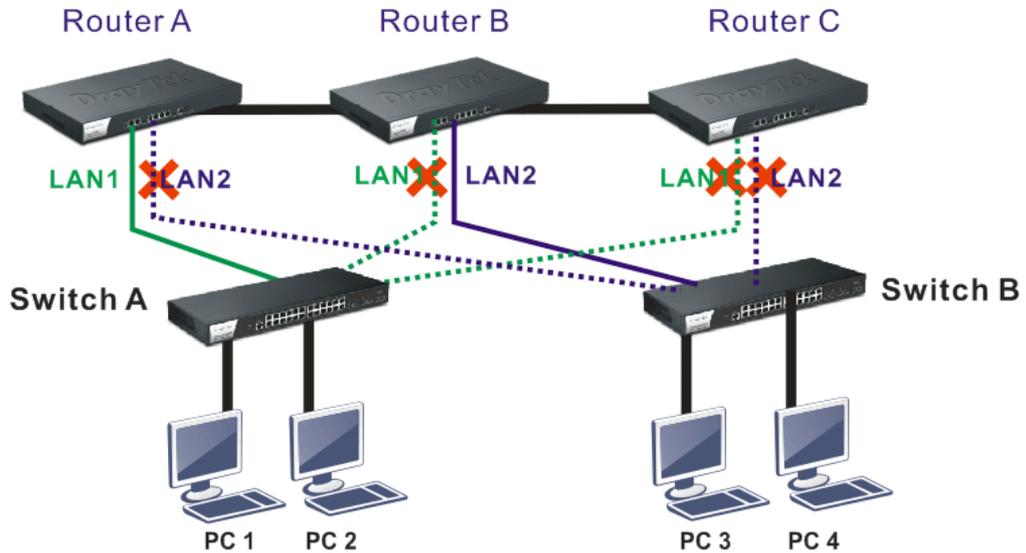
Available parameters are listed as follows:

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.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

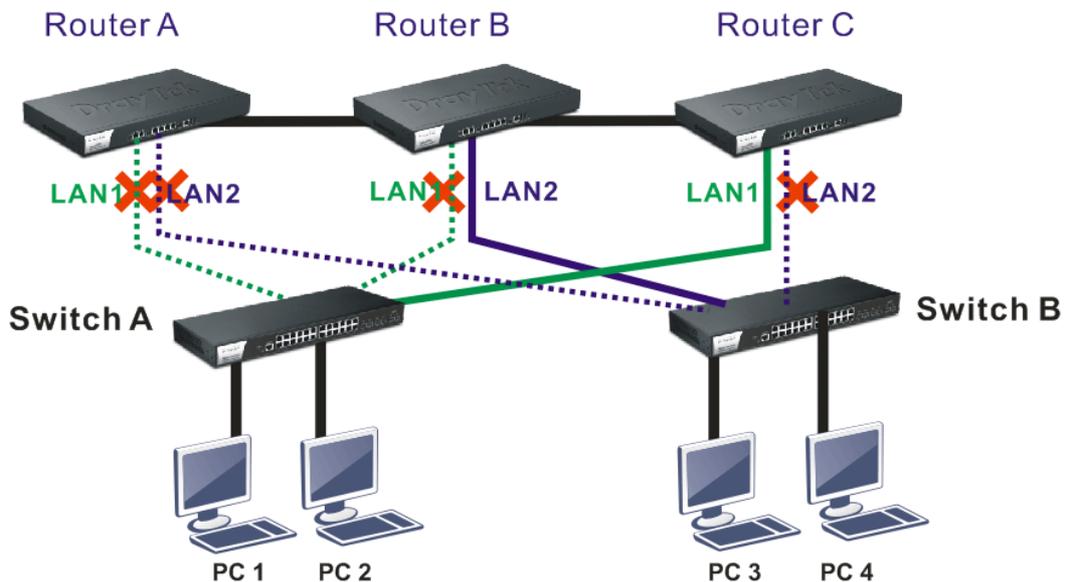
4. Enter all of the settings and click **Apply**.

4.8.5.3 Active-Standby Mechanism

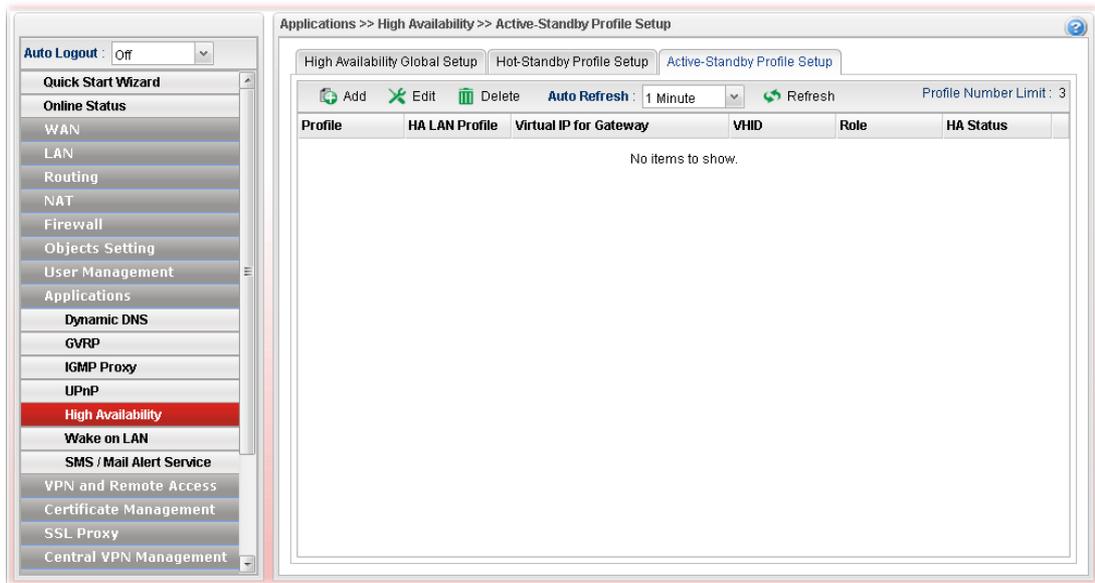
The active-standby Mechanism is that each access point in LAN will participate in different high availability sessions. All the WAN interfaces can be active which provide more flexible utilization of network service.



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.



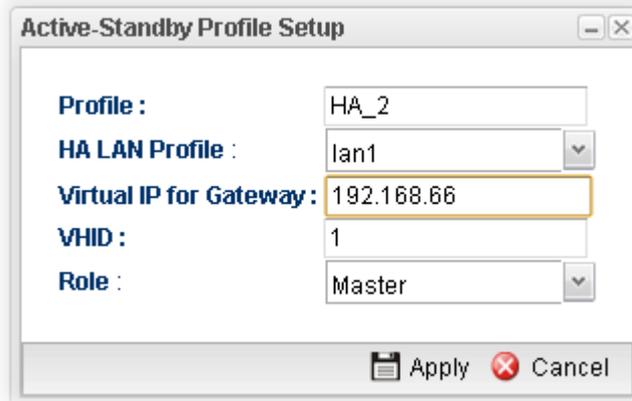
Available parameters are listed as follows:

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.

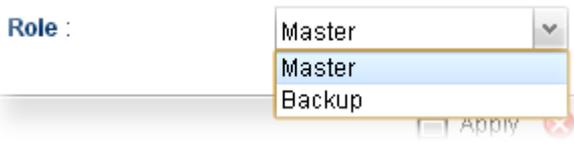
How to create a new Active-Standby Profile

1. Open **Applications>>High Availability** and click the **Active-Standby Profile Setup** tab.

- Simply click the **Add** button.
- 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	<p>LAN profiles configured for HA application can run independently and will not interfere with each other.</p> <p>Therefore, LAN1 (Backup) of router A can be the backup of LAN1 (Master) of router B; LAN2 (Backup) of router B can be the backup of LAN2 of router A(Master).</p> <p>Each HA LAN profile (configured under the same router) must be specified a role as Master or Backup.</p> 
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

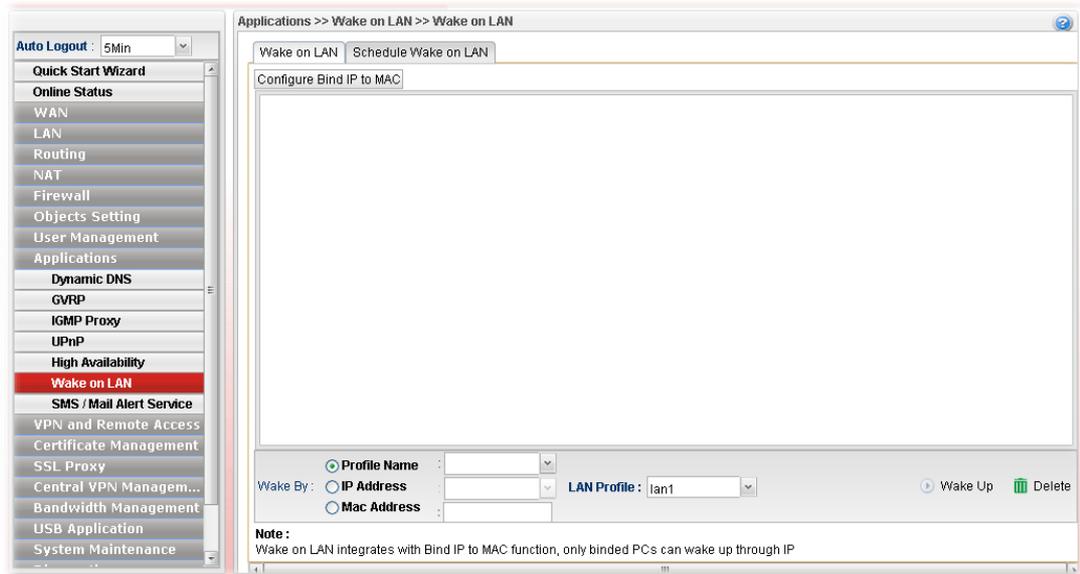
- Enter all of the settings and click **Apply**.

4.8.6 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.

4.8.6.1 Wake on LAN

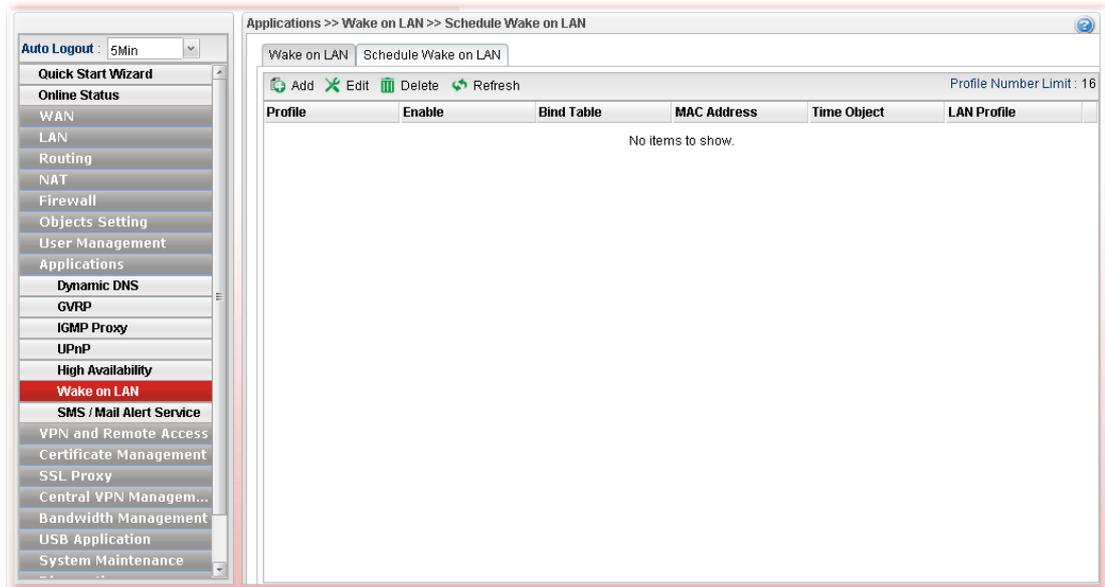


Available parameters are listed as follows:

Item	Description
Configure Bind IP to MAC	Click it to open the setting page of Bind IP to MAC.
Wake by	<p>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.</p> <p>Profile Name – Choose a profile (created by LAN>>Bind IP to MAC) from the drop down list.</p> <p>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.</p> <p>MAC Address - Type any one of the MAC address of the bind PCs.</p> <p>LAN Profile – Use the drop down list to choose one of the LAN profiles.</p>
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.

4.8.6.1 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**.

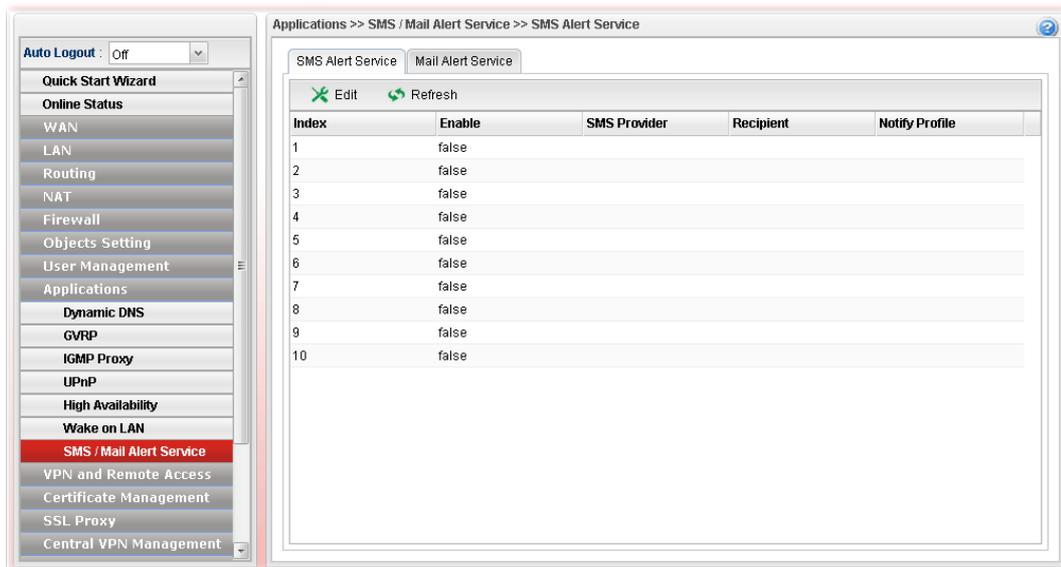
4.8.7 SMS / Mail Alert Service

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.

4.8.7.1 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:

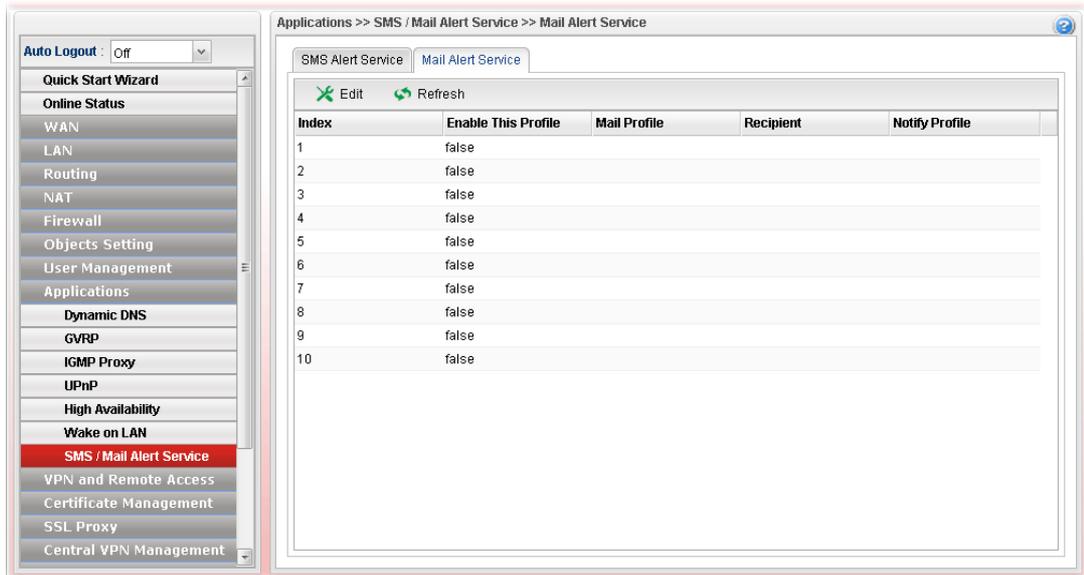
Item	Description
Enable	Check this box to enable such profile.
SMS Provider	Choose the SMS provider object profile from the drop down list. Such profiles can be created from Object Setting>>SMS Service Object .
Recipient	Type the cell phone number to receive the SMS.
Notify Profile	Choose a profile (specify 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.

Index	Enable	SMS Provider	Recipient	Notify Profile
1	true	Line_down	123456789	Notify_attack
2	false			
3	false			
4	false			

4.8.7.2 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.

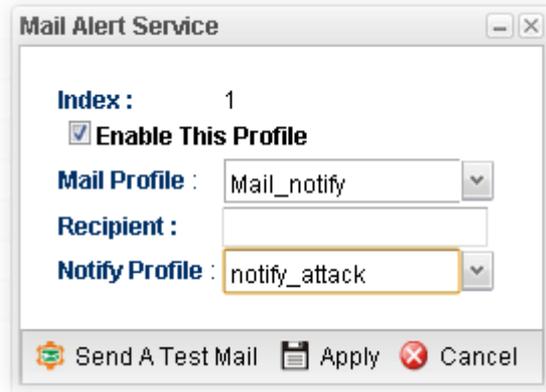


Each item will be explained as follows:

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

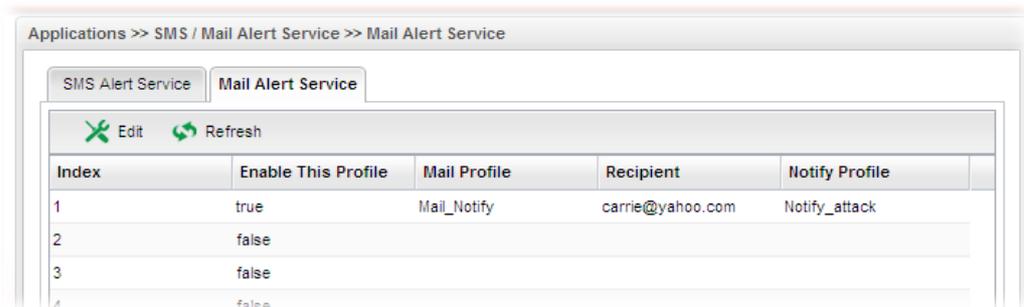
1. Open **Applications>> SMS/Mail Alert Service** and click the **Mail Alert Service** tab.
2. Choose one of the index numbers and click the **Edit** button.
3. The following dialog will appear.



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

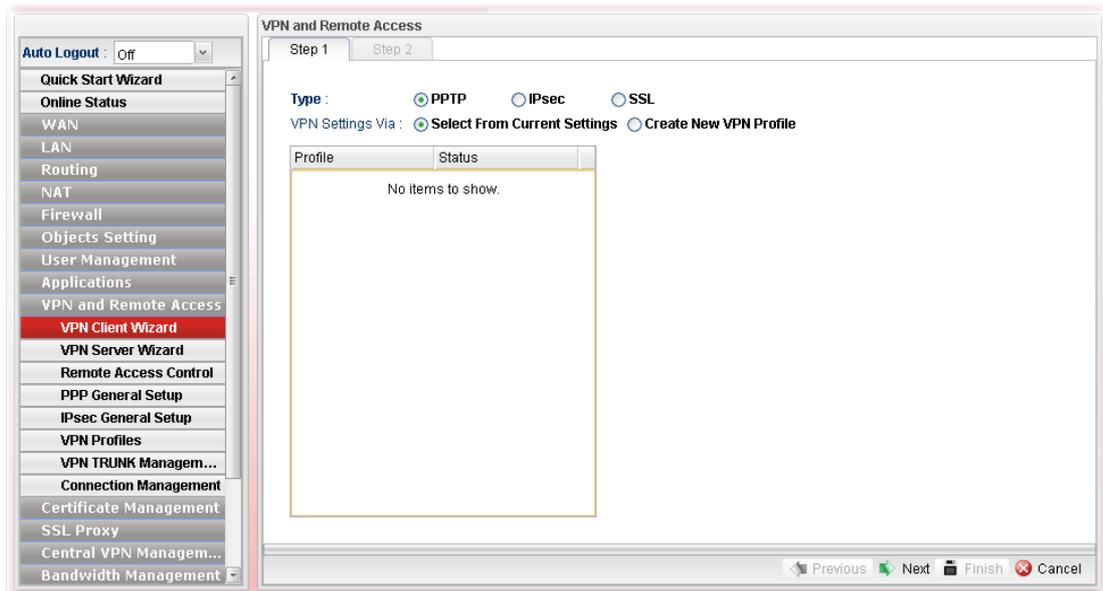
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



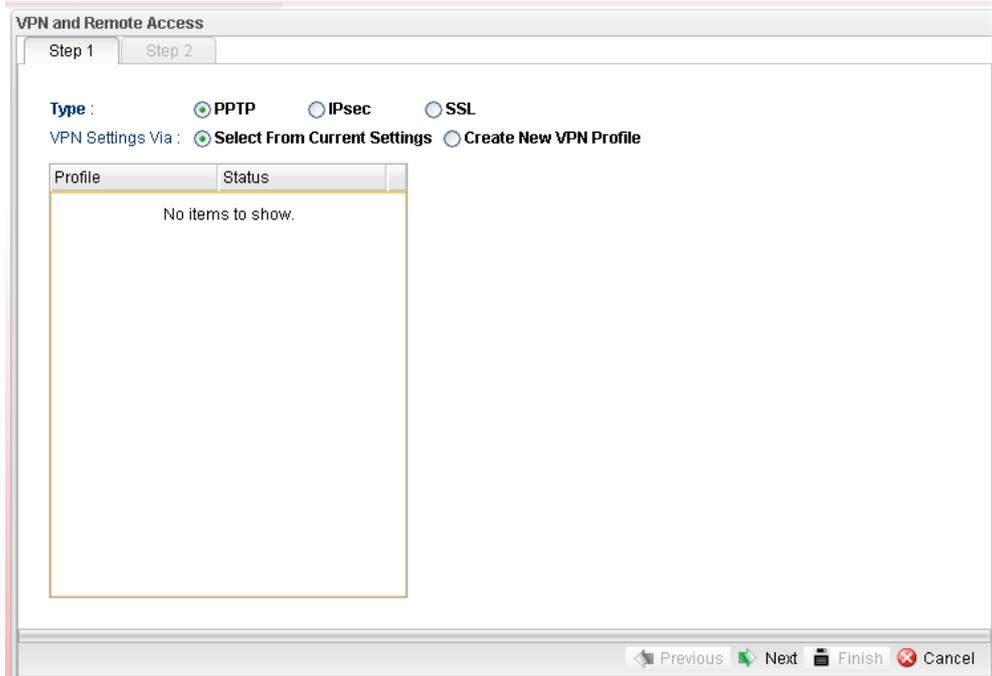
4.9.1 VPN Client Wizard

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.

- Specify the type. Click **Create New VPN Profile** and type the name of the profile. Then, click **Next**.

VPN and Remote Access

Step 1 Step 2

Type : PPTP IPsec SSL

VPN Settings Via : Select From Current Settings Create New VPN Profile

Profile Name :

Previous Next Finish Cancel

- If you choose **PPTP** as the Type, you will get the following screen:

VPN and Remote Access

Step 1 Step 2

Profile : VPN_CLI_1

Enable

Always On : Enable Disable

Dial-Out Through : Default WAN IP WAN Alias IP

Failover to :

Idle Timeout (sec) : (Optional)

Server IP/Host Name :

PPTP User Name :

PPTP Password :

Local IP / Subnet Mask :

Add Save Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

Remote IP / Subnet Mask :

Route / NAT Mode :

Netbios Naming Packet : Enable Disable

Previous Next Finish Cancel

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	<p>Enable – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.
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.
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.

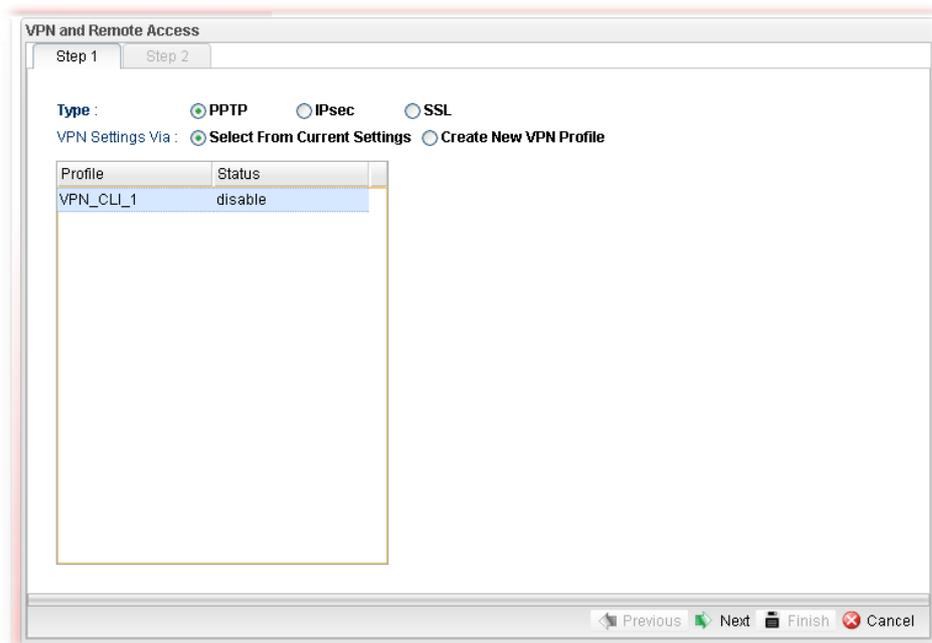
If you choose **SSL** as the Type, you will get the following screen:

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.

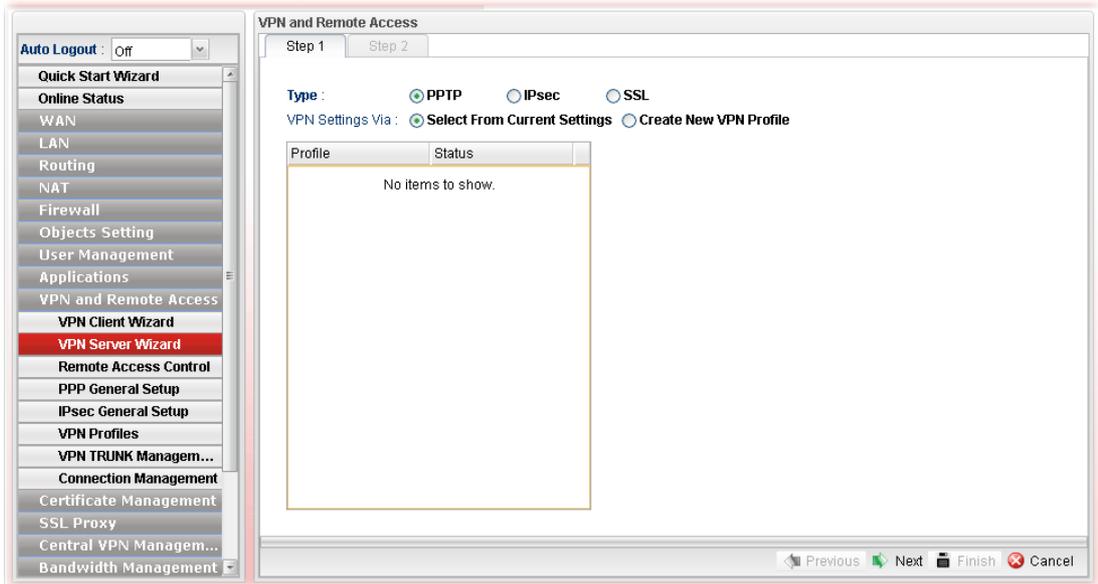
SSL Password	Type a password for authentication in SSL VPN connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP/Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Route/NAT Mode	Specify the purpose for such profile. 
Netbios Naming Packet	<p>Enable – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.



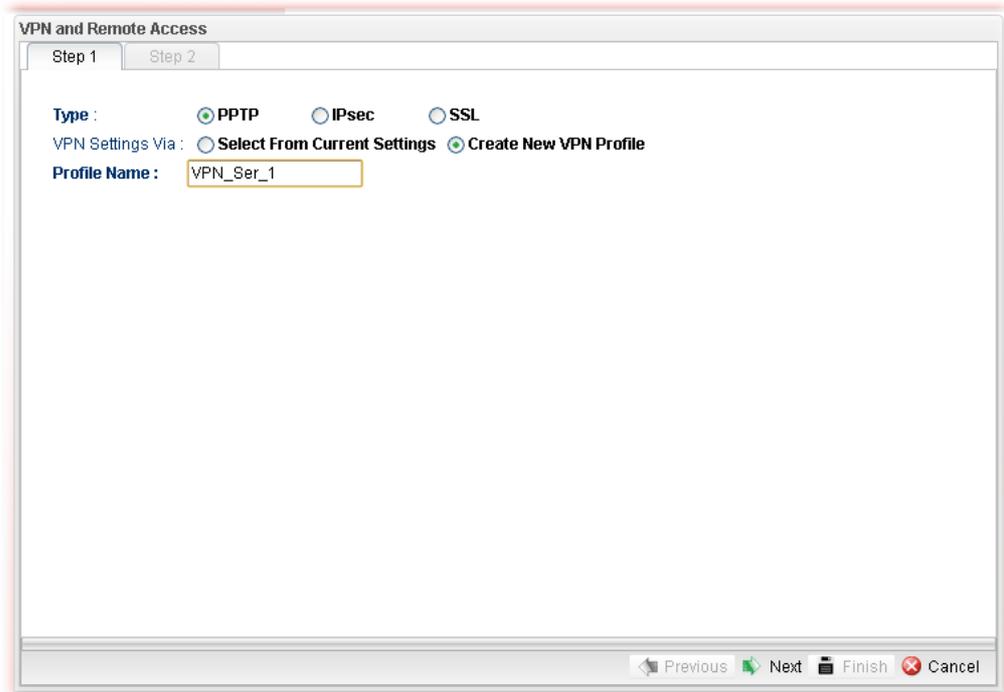
4.9.2 VPN Server Wizard

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	<p>Select From Current Settings - Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need.</p> <p>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.</p>
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	<p>Enable – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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:

The screenshot shows the 'VPN and Remote Access' configuration window, Step 2. The profile name is 'VPN_Ser_1'. The 'Enable' checkbox is checked. The WAN Profile is set to 'wan1'. The Local IP/Subnet Mask is 192.168.1.0/255.255.255.0/24. The Local Next Hop is 0.0.0.0. The Remote Host is 172.16.1.88. The Remote IP/Subnet Mask is 192.168.2.45/255.255.255.255/32. The 'More Remote Subnet' table is empty. The Aggressive Mode is set to 'Main Mode'. The Auth Type is 'PSK'. The Security Protocol is 'ESP'. The DPD Delay is 30. The window has 'Previous', 'Next', 'Finish', and 'Cancel' buttons at the bottom.

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.
Aggressive Mode	<p>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.</p> <p>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.</p> <p>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.</p>
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.

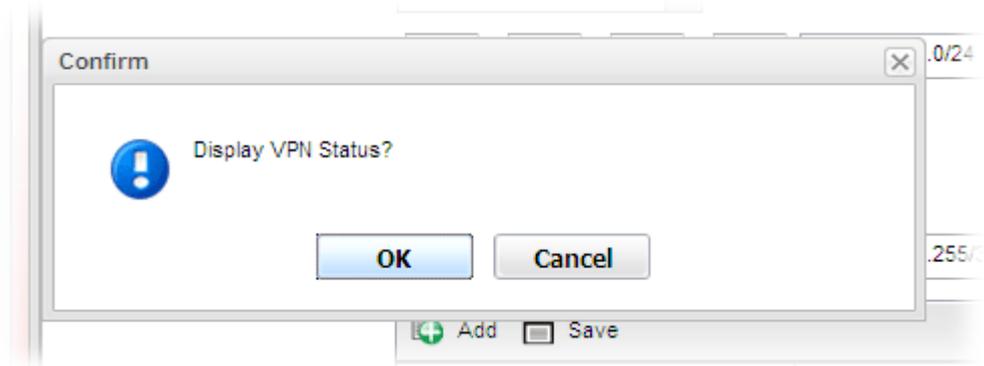
If you choose **SSL** as the **Type** in Step 1, you will get the following page:

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. <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Enable – Click it to exchange routing information

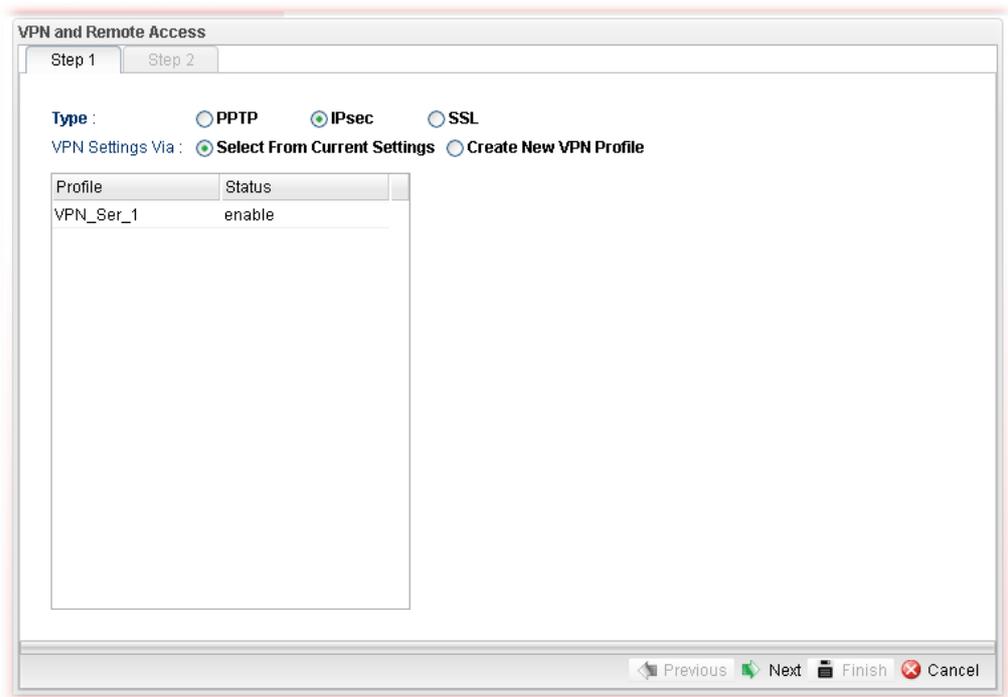
packets via VPN connection.

- **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.

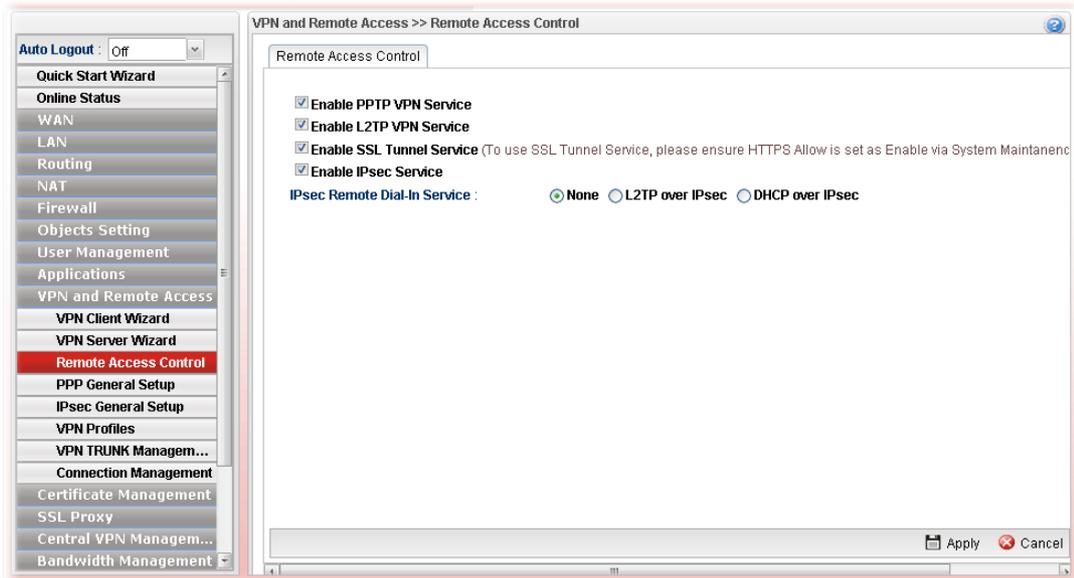


5. Click **OK**. Then, return to **VPN and Remote Access >> VPN Server Wizard**. The new added VPN server profile will be displayed on the screen.



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, IPsec etc.) of Vigor Router to allow VPN tunnel pass through.



Available parameters are listed as follows:

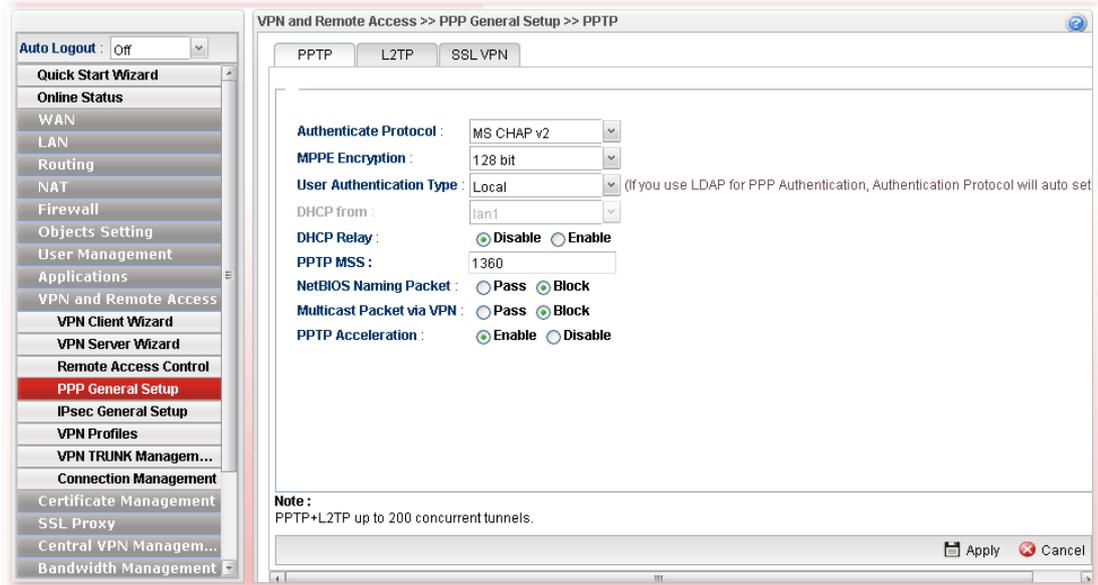
Item	Description
Enable PPTP/L2TP VPN Service / Enable SSL Tunnel /IPsec Service	Check the box(es) to enable the service.
IPSec Remote Dial-In Service	Choose one of the services by clicking on the radio button.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured 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.

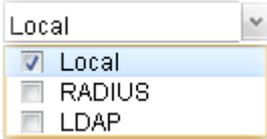
4.9.4.1 PPTP

This page display current status for VPN tunnel built with PPTP protocol.



Available parameters are listed as follows:

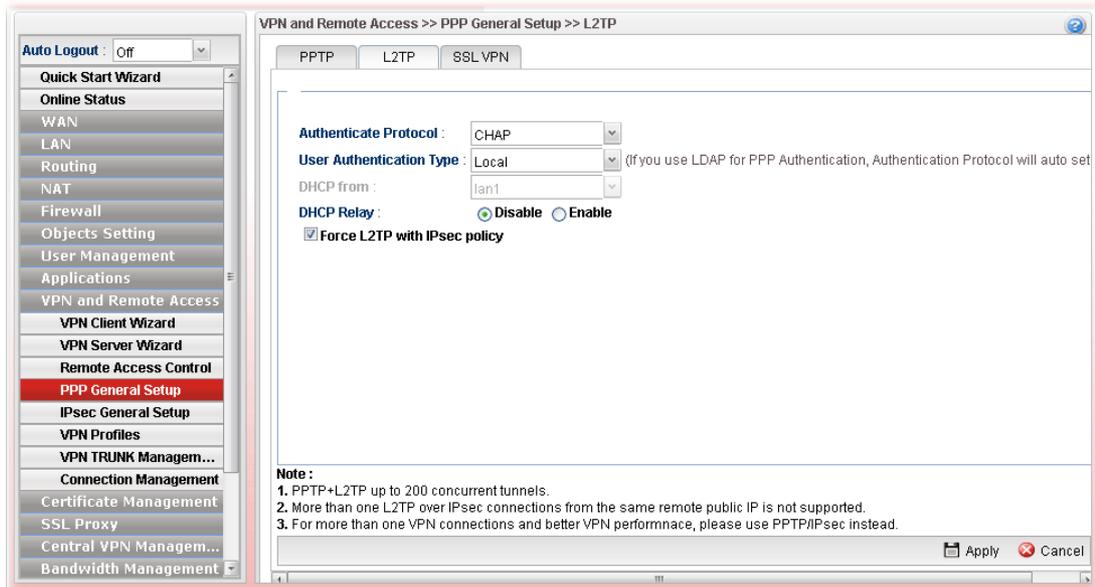
Item	Description
Authenticate Protocol	<p>The router will authenticate the dial-in user with the protocol selected here.</p>  <p>PAP - It means the router will attempt to authenticate dial-in users with the PAP protocol.</p> <p>CHAP - It means the router will attempt to authenticate dial-in users with the CHAP protocol.</p>
MPPE Encryption	<p>Specify one of the encryptions for such server. It is available only when MS-CHAP or MS-CHAP_v2 is selected.</p> 
User Authentication Type	<p>Set user authentication to Local server, RADIUS server or LDAP server.</p>

	
LDAP profiles	<p>Choose a LDAP profile for PPTP Server if LDAP is selected as user authentication type.</p> <p>To clear the selected one, click  to remove current object selections.</p>
DHCP from	Choose a LAN profile for PPTP Server if RADIUS is selected as user authentication type.
DHCP Relay	<p>Enable - Let the router assign IP address to every host in the LAN.</p> <p>Disable - Let you manually assign IP address to every host in the LAN.</p>
PPTP MSS	Type the maximum segment size (MSS) for PPTP VPN tunnel.
DHCP Server Location	<p>It is available when DHCP Relay is enabled.</p> <p>Choose the WAN/LAN interface for the DHCP server.</p>
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.
NetBIOS Naming Packet	<p>Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast Packet via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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.

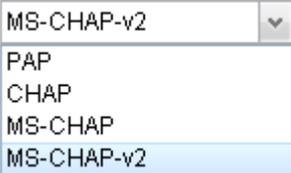
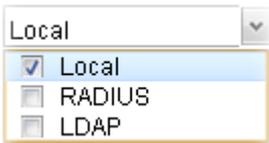
Enter all the settings and click **Apply**.

4.9.4.2 L2TP

This page display current status for VPN tunnel built with L2TP protocol.



Available parameters are listed as follows:

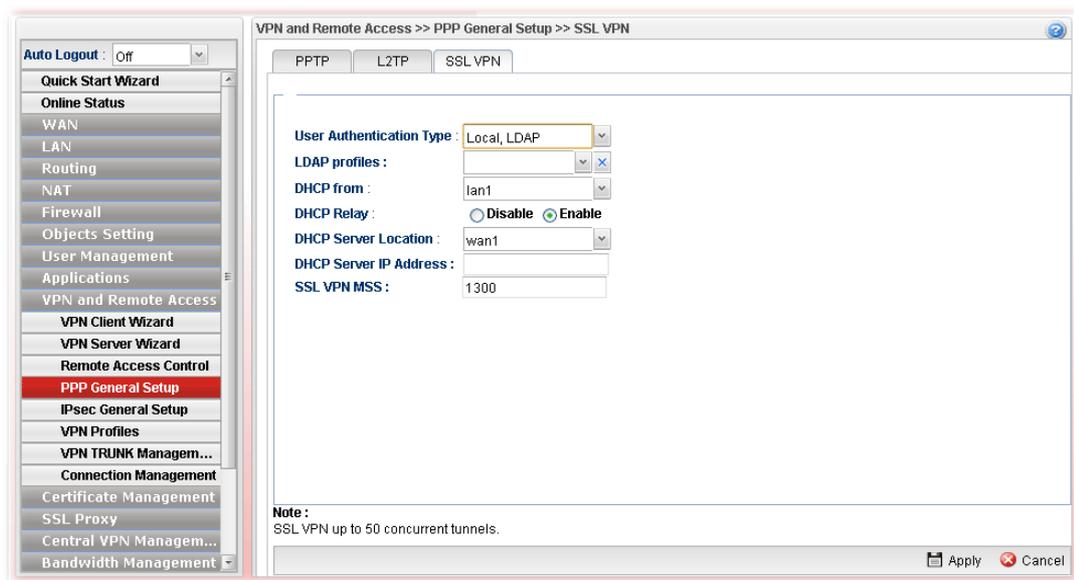
Item	Description
Authenticate Protocol	<p>The router will authenticate the dial-in user with the protocol selected here.</p>  <p>PAP - It means the router will attempt to authenticate dial-in users with the PAP protocol.</p> <p>CHAP - It means the router will attempt to authenticate dial-in users with the CHAP protocol.</p>
User Authentication Type	<p>Set user authentication to Local server or RADIUS server.</p> 
LDAP profiles	<p>Choose a LDAP profile for PPTP Server if LDAP is selected as user authentication type.</p> <p>To clear the selected one, click  to remove current object selections.</p>
DHCP from	<p>Choose a LAN profile for L2TP Server if RADIUS is selected as user authentication type.</p>
DHCP Relay	<p>Enable - Let the router assign IP address to every host in the LAN.</p>

	Disable - Let you manually 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.
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:

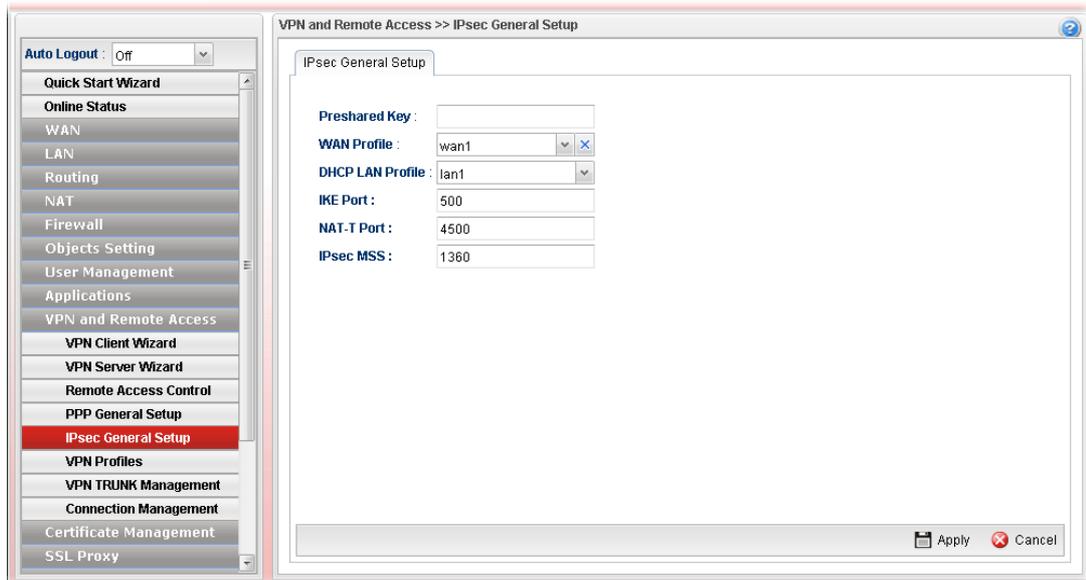
Item	Description
User Authentication Type	Set user authentication to Local server or RADIUS server.
LDAP profiles	Choose a LDAP profile for PPTP Server if LDAP is selected as user authentication type. To clear the selected one, click  to remove current object selections.
DHCP from	Choose a LAN profile 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. Disable - Let you manually 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.
SSL VPN MSS	Type the maximum segment size (MSS) for SSL VPN tunnel.
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 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 Confirm Pre-Shared Key - Retype the characters to confirm the pre-shared key.
WAN Profile	Choose a WAN interface profile to be used. To clear the selected one, click  to remove current profile selections.

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.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

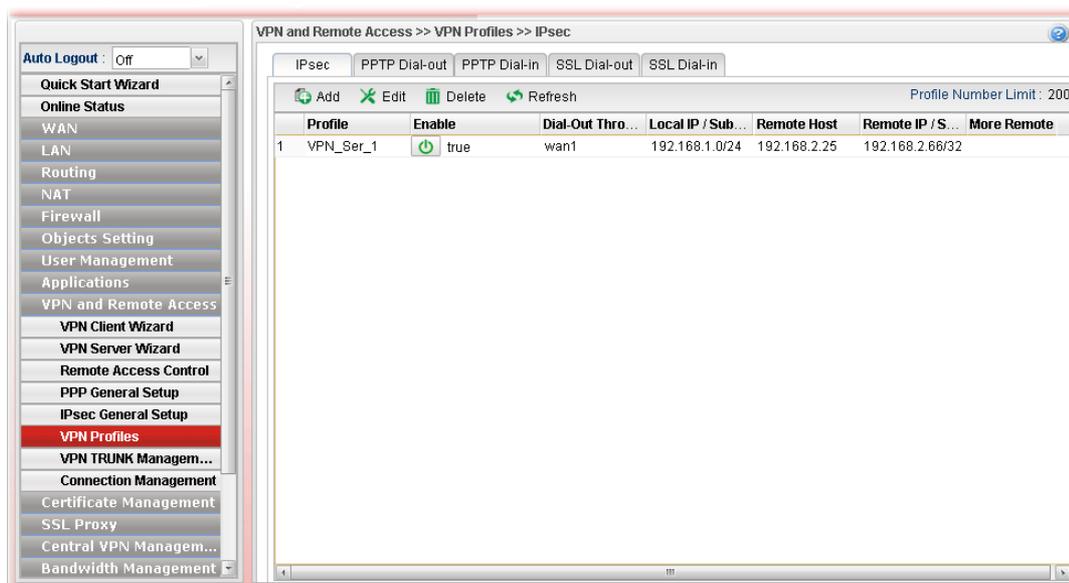
Enter all the settings and click **Apply**.

4.9.6 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.

4.9.6.1 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.

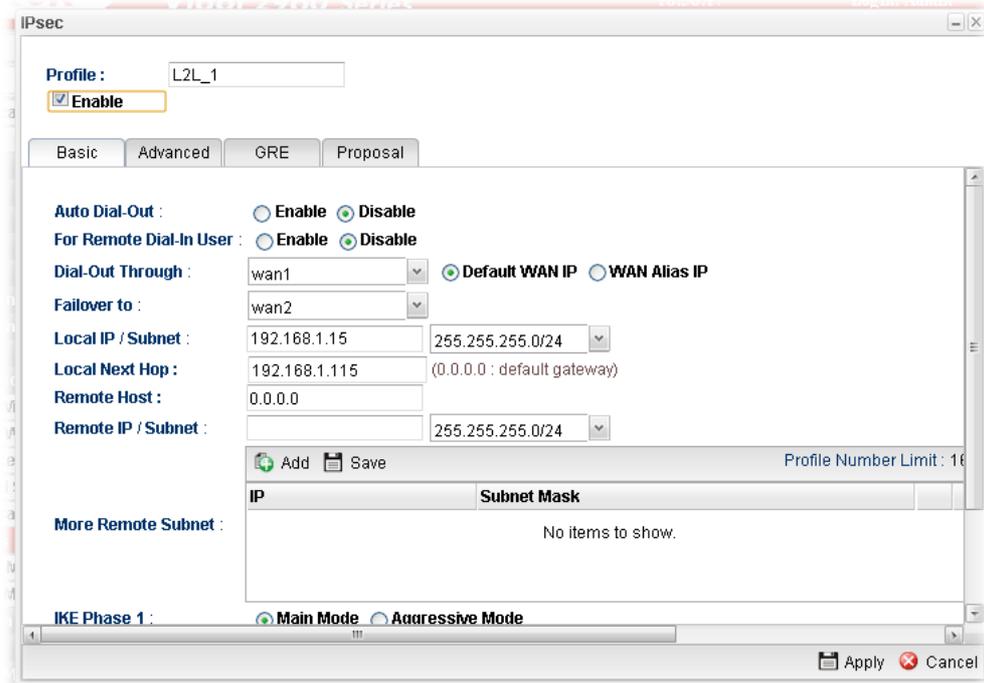
Refresh	Renew current web page.
IPSec	Display the LAN to LAN profile with IPSec policy.
PPTP Dial-out	Display the LAN to LAN profile with PPTP Dial-out policy.
PPTP Dial-in	Display the LAN to LAN profile with PPTP Dial-in policy.
Profile Number Limit	Display the total number (500) of the object profiles 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 >> LAN to LAN**.
2. Simply click the **Add** button.

3. The following dialog will appear. Click the **Basic** tab to configure the settings.

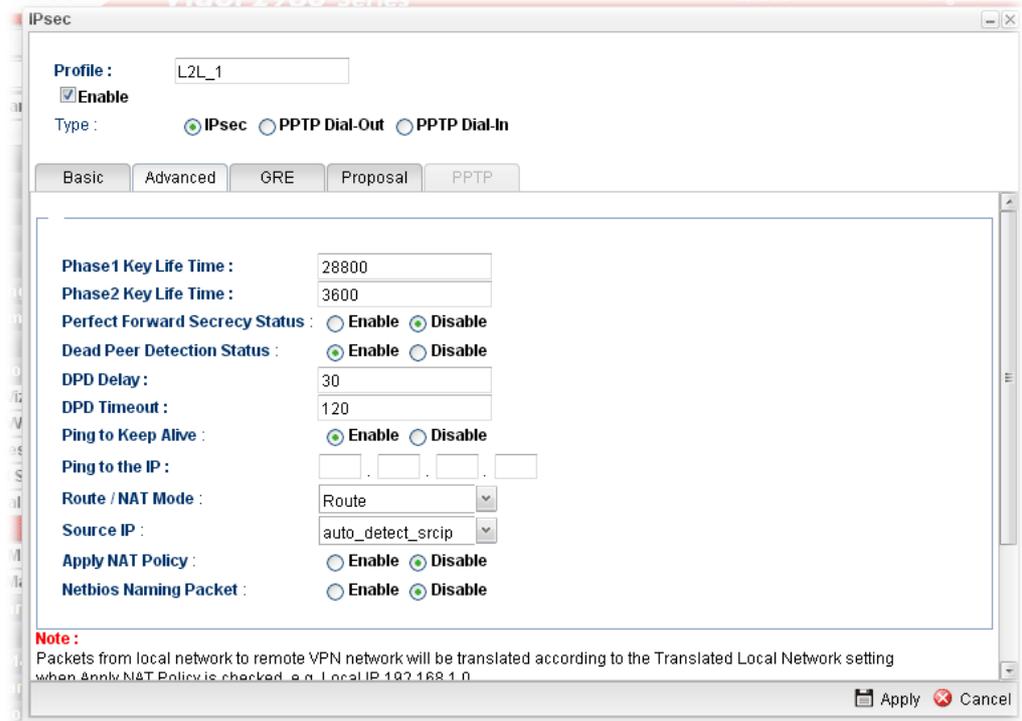


Available parameters are listed as follows:

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	<p>Always On – Click Enable to make router always keeping connection.</p> <p>For Remote Dial-In User- Click Enable to allow the connection via IPSec remote dial-in host.</p> <p>Dial-Out Through- Choose a wan profile to be used by such profile.</p> <p>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.</p> <p>Local IP/Subnet - Type the IP address and subnet mask of local host.</p> <p>Local Next Hop - Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).</p> <p>Remote Host - Type the WAN IP address for the remote host.</p> <p>Remote IP / Subnet Mask - Type the LAN IP address and LAN subnet mask for the remote host.</p> <p>More Remote Subnet – Add more remote subnet in this field if required.</p>

	<p>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.</p> <p>Auth Type - The authentication to be used by Pre-Shared Key or RSA Signature. Choose PSK or RSA for such profile.</p> <p>Local Certificate - Choose a local certificate from the drop down list if RSA is selected as Auth Type.</p> <p>Local Peer ID –Type the ID for Vigor3900 which can be configured by the remote end. It is available for Aggressive Mode enabled only.</p> <p>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.</p> <p>Preshared Key – Specify a key for IKE authentication if PSK is selected as Auth Type.</p> <p>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.</p>
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

4. After filling the required information for **Basic**, click the **Advanced** tab to open the following page.



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	<p>Enable – Click it to enable such function.</p> <p>Ping to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.</p>
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	<p>Enable – This option allows for performing one-to-one NAT for all traffic flowing across the VPN.</p> <p>Translated Local Network – Specify the IP address with subnet mask of the network that all traffic will be translated into.</p>
Netbios Naming Packet	<p>Enable – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.

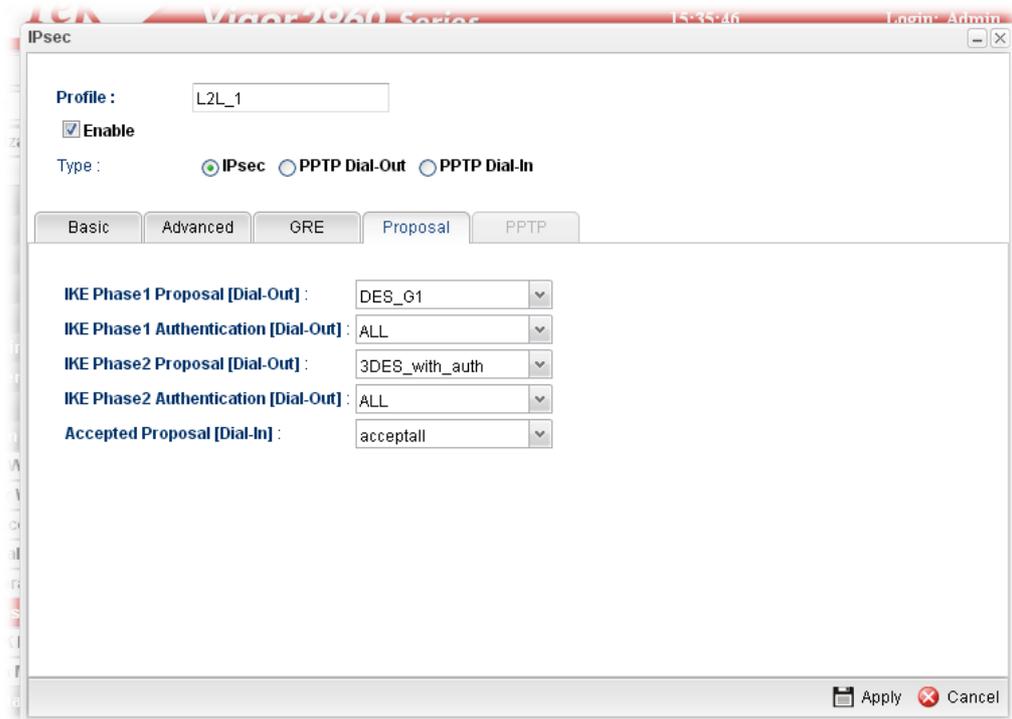
- After filling the required information for **Advanced**, click the **GRE** tab to open the following page.

The screenshot shows the IPsec configuration window with the GRE tab selected. The profile is 'L2L_1' and is enabled. The GRE function is also enabled. The local GRE IP is 192.168.1.66 and the remote GRE IP is 192.168.1.84. The auto-generate GRE key option is disabled. There are optional fields for GRE In Key and GRE Out Key. A note at the bottom indicates that it is necessary to create a Load Balance Pool/Rule in VPN Trunk Management for GRE tunnels to work.

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.

6. After filling the required information for **GRE**, click the **Proposal** tab to open the following page.



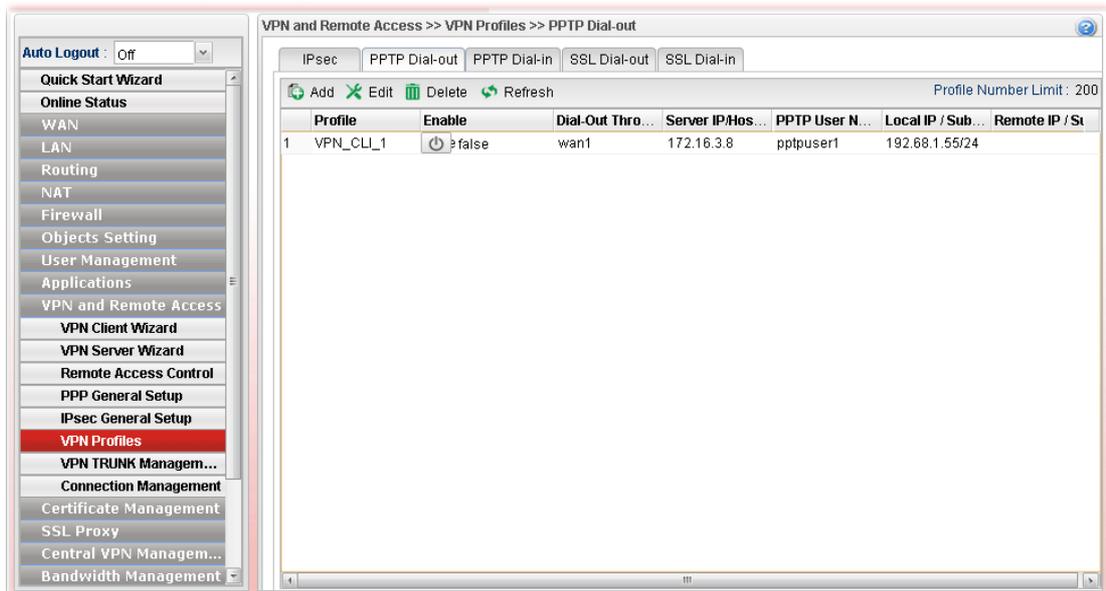
Available parameters are listed as follows:

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.

7. Enter all the settings and click **Apply**.
8. A new IPsec LAN-to-LAN profile has been created.

4.9.6.2 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:

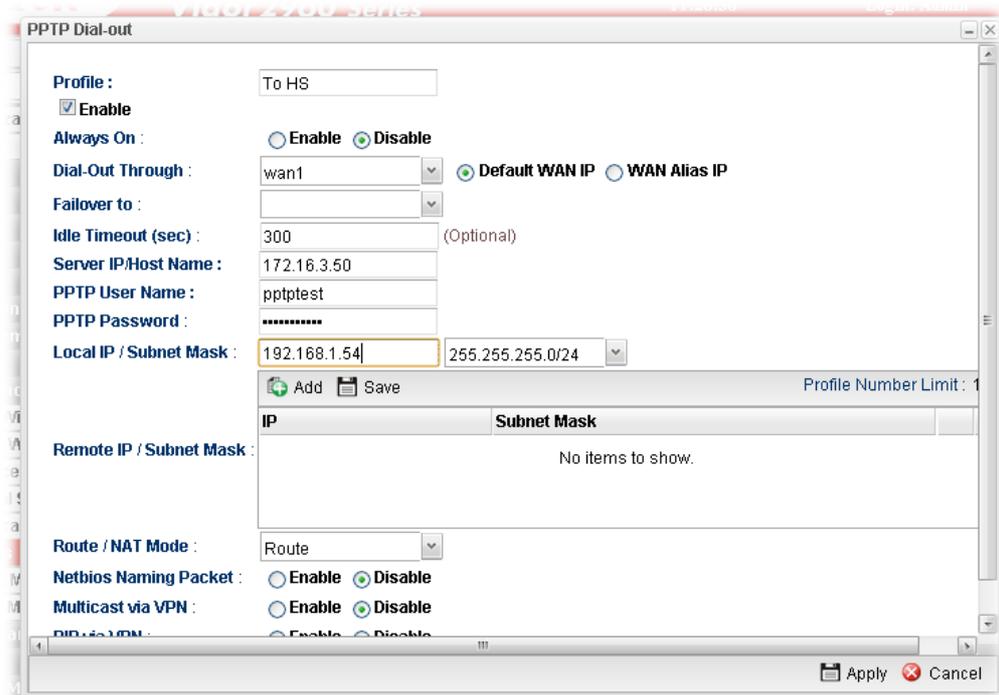
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete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



Available parameters are listed as follows:

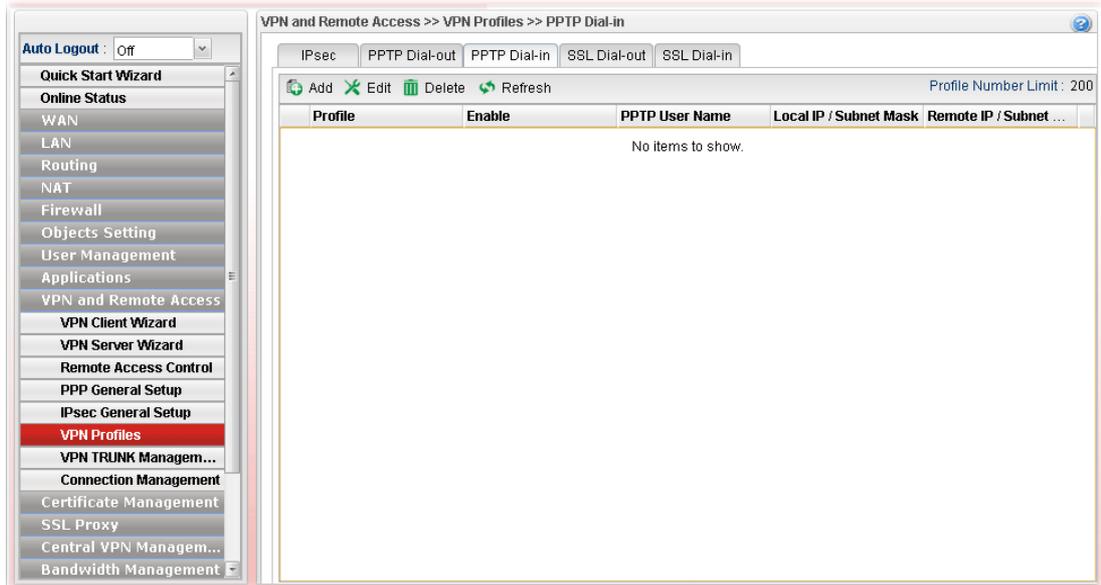
Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Always On	Click Enable to make the profile being always on.
Dial-Out Through	Choose a wan interface to be used by such profile. Then, use the default WAN IP or specify a WAN Alias IP for VPN tunnel.
Failover 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	Type the IP address or the host name of PPTP/SSL server.

Name	
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	<p>Enable – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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.

4.9.6.3 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. <ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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 VPN Trunk Management

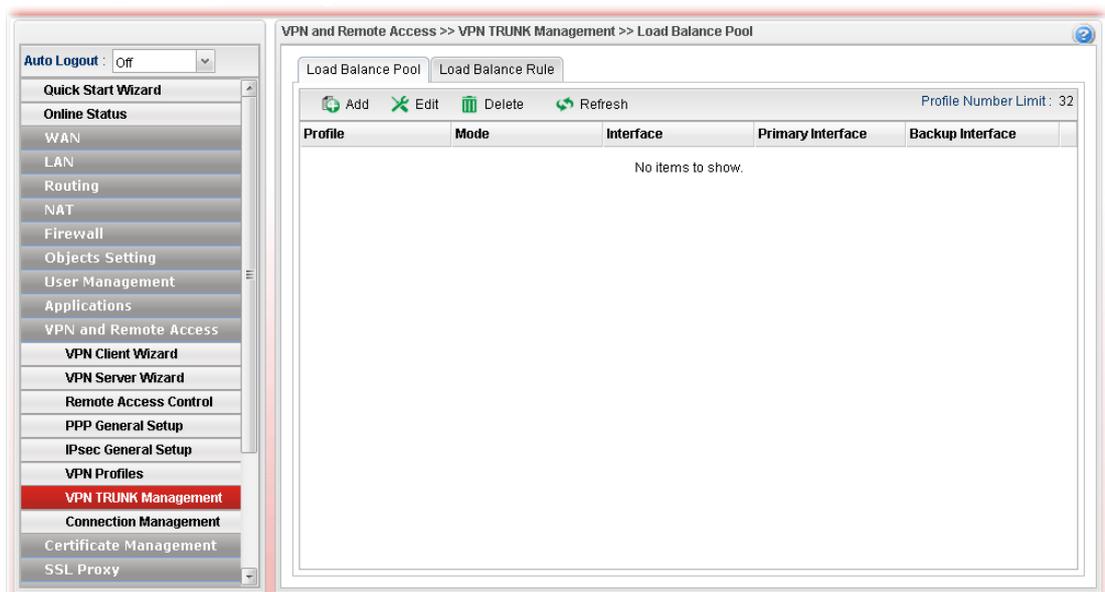
VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism 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.

4.9.7.1 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.

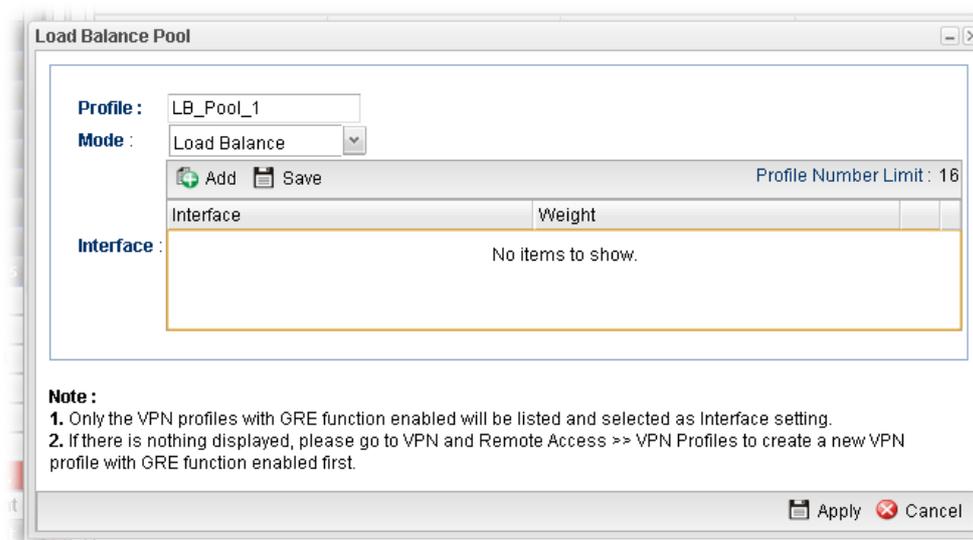


Each item will be explained as follows:

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 <ul style="list-style-type: none"> ● 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 <ul style="list-style-type: none"> ● Primary Interface / Backup Interface - Use the drop down list to specify the VPN profiles for Primary Interface and Backup Interface respectively.

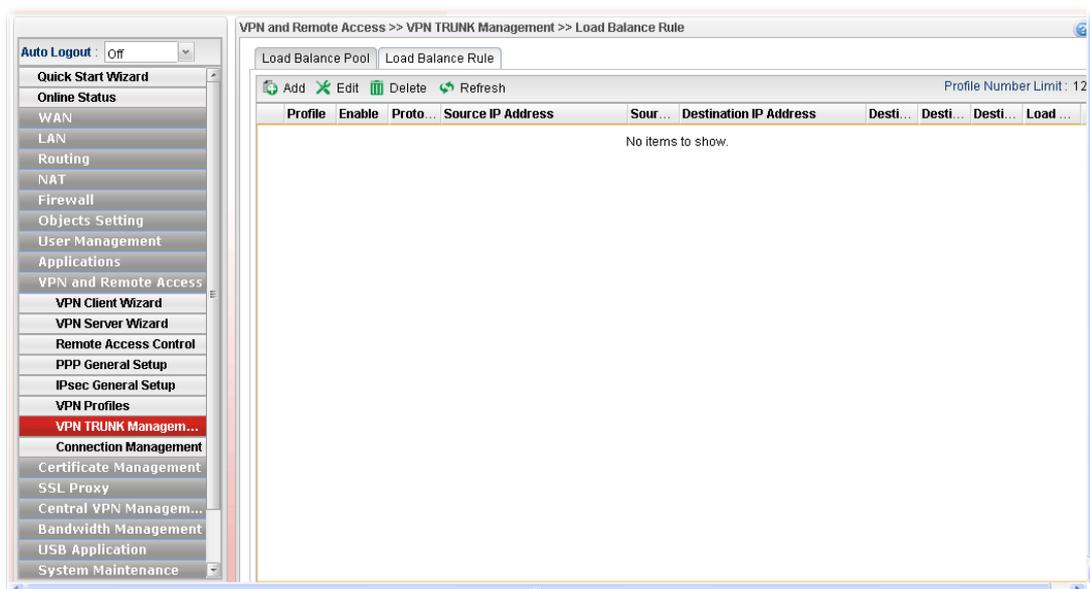
Important!!! If there is no selection for Interface option, please go to **VPN and Remote Access>>VPN Profiles** to create a new IPsec LAN to LAN profile with **enabled GRE** setting. Then, return to this page to specify the Interface option.

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.

4.9.7.2 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.

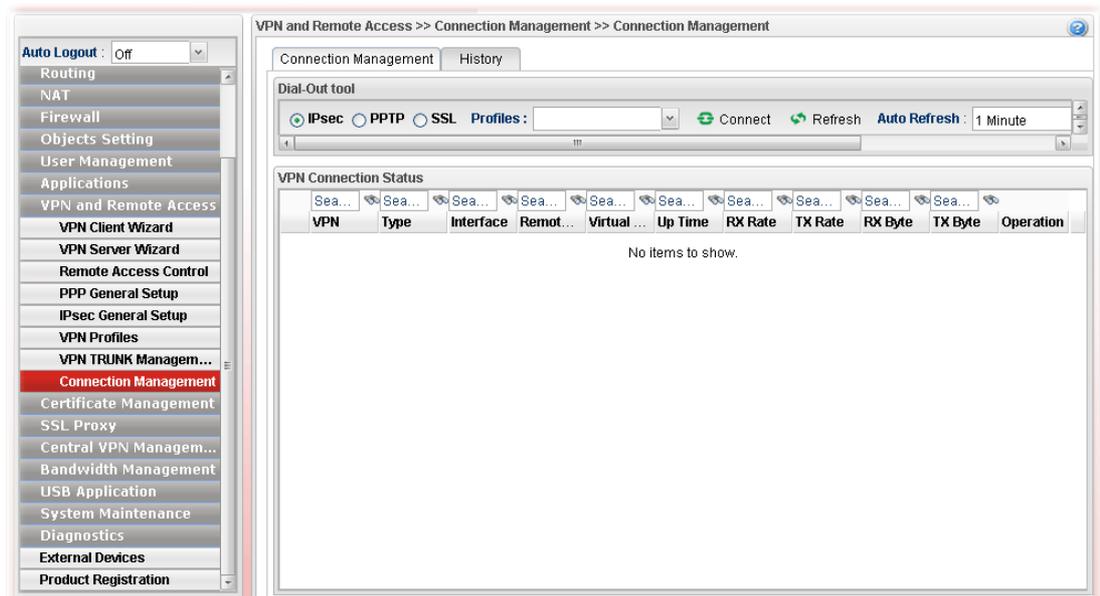
Load Balance Pool	Use the drop down list to choose one profile configured in load balance pool. Then, such rule will be applied by the pool.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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

4.9.8 Connection Management

4.9.8.1 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Disconnect** button.



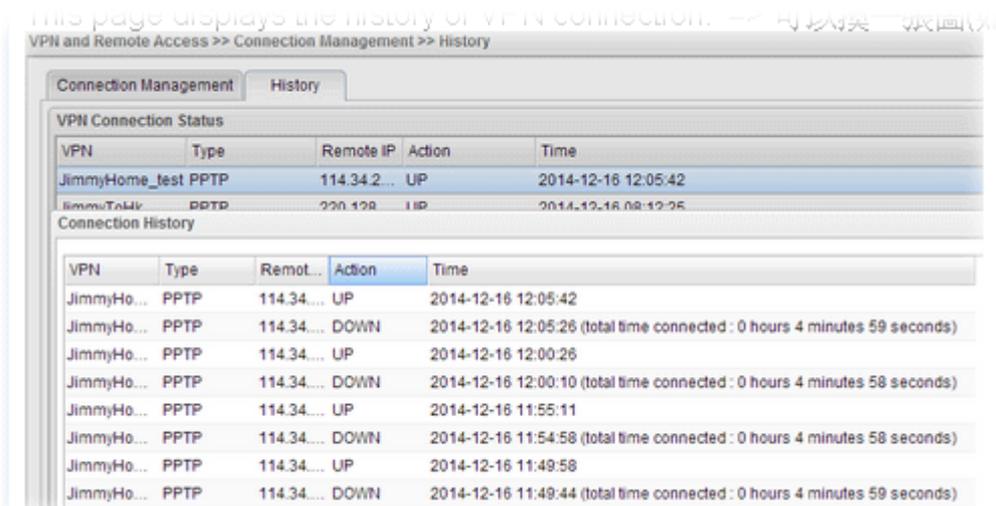
Each item will be explained as follows:

Item	Description
IPsec/PPTP/SSL	Click it to perform IPsec VPN/PPTP/SSL connection.
PPTP	Click it to perform PPTP VPN connection.
Profile	This field 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.

4.9.8.2 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.

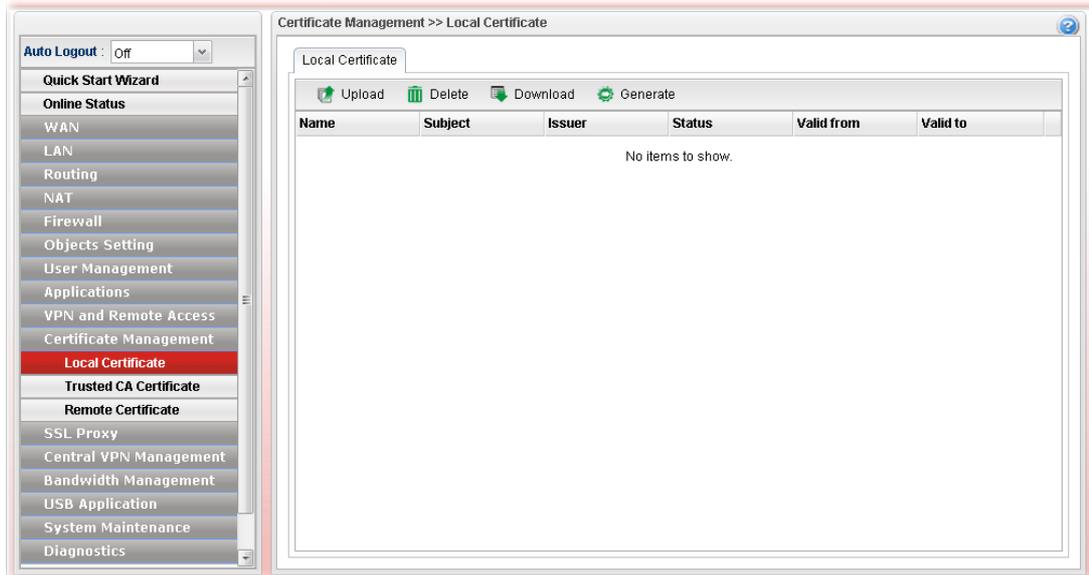


Local certificate is created by the end user and must be signed by a trusted CA center. Vigor3900 can serve as a trusted CA and is called with “Root CA”. Therefore, any user can ask for certificate signed by Vigor3900.

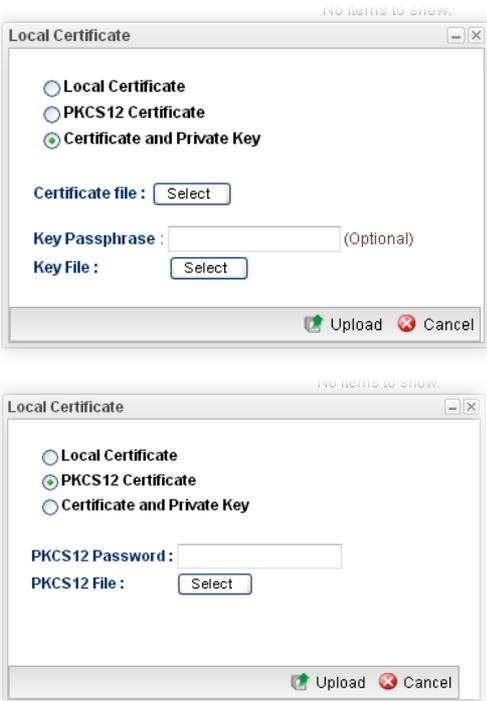
When Vigor3900 serves as a Root CA, it can sign the certificates coming from the users. First, building a Root CA for Vigor3900 by clicking **Trusted CA Certificate**. Later, certificate coming from other users can be uploaded to Root CA (Vigor3900) and be signed by Vigor3900.

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
<p>Upload</p>	<p>Click this button to open the following dialog to upload selected certificate onto the router.</p>  <p>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.</p>

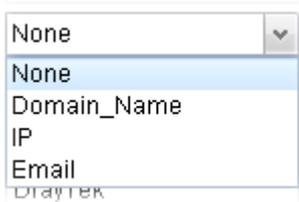
Delete	Remove the selected item of Trusted CA listed below.
Download	Allow you to download an existing CA certificate to the router.
Generate	Open another web page for generating the local certificate.
Name	Display the name of trusted CA built.
Subject	Display the subject of the trusted CA built.
Issuer	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.

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	<p>The ID type for such certificate. There are four types:</p> <p>Domain Name: Certificated by domain name.</p> <p>IP: Certificated by IP address.</p> <p>Email: Certificated by email address.</p> <p>None: Do not enter an ID value.</p> 
ID Value	<p>The ID value is determined by the ID Type selected for such certificate.</p> <p>For example, if you choose Domain Name as the ID Type, please type the domain name in this field.</p>
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	<p>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.</p> <p>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.</p>
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.

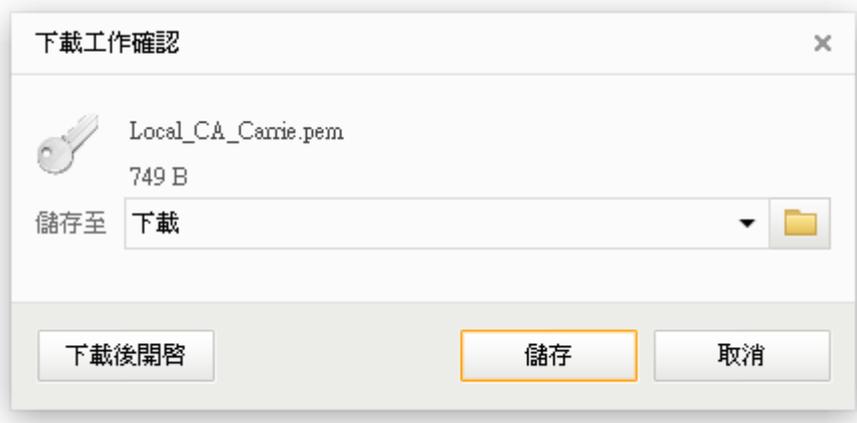
4. Enter all the settings and click **Apply**.
5. A new generated Local Certificate has been created.

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.

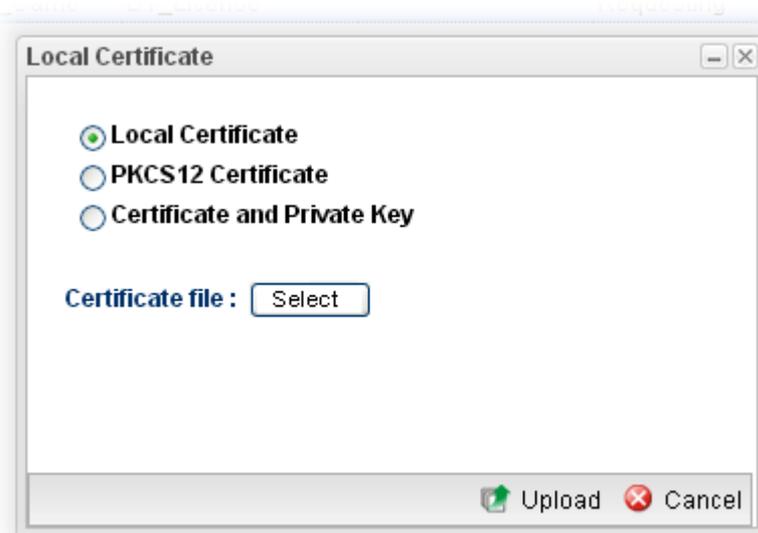
1. Open **Certificate Management>> Local Certificate**.
2. Specify a certificate and click the **Download** button.



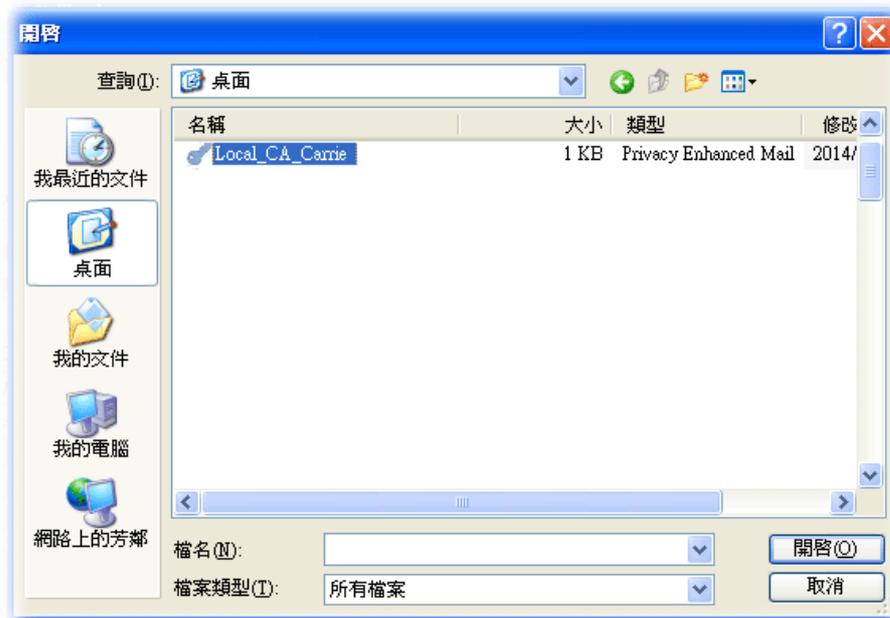
3. Click **Save**. The file will be stored under the folder you specified above.

How to upload a local certificate

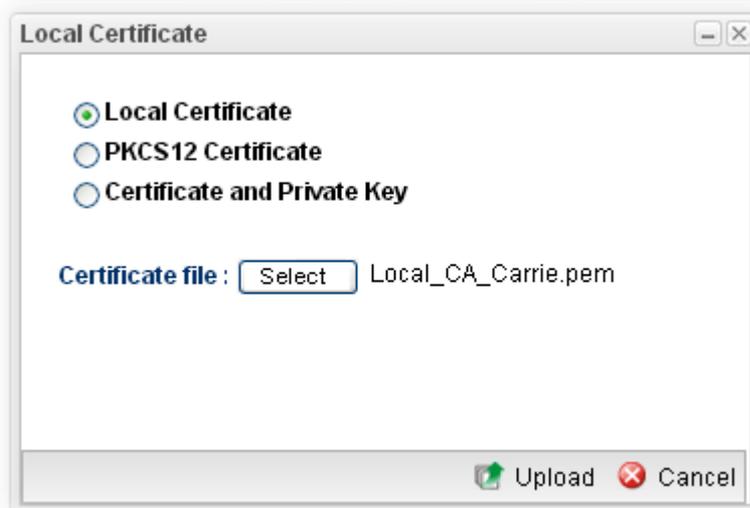
1. Open **Certificate Management>> Local Certificate**.
2. Click **Upload** to open the following dialog.



3. Choose **Local Certificate** and click the **Select** button to open the following 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.

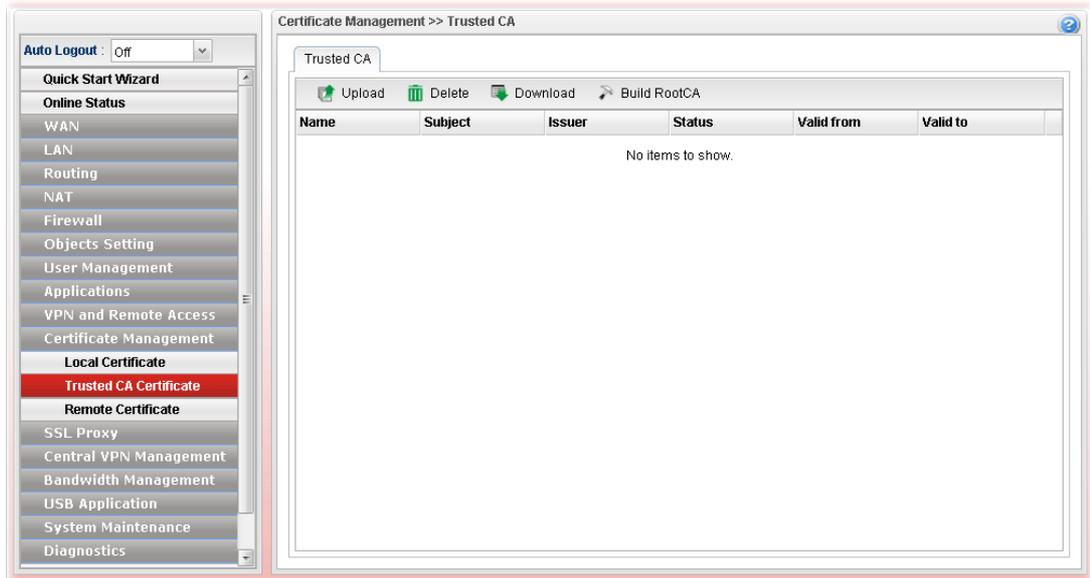


5. Click **Upload**. The system will start to upload the selected file.

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
<p>Upload</p>	<p>Click this button to open the following dialog to upload selected certificate onto the router.</p> <div style="display: flex; flex-direction: column; align-items: center;"> <div data-bbox="699 1189 1182 1509"> <p>This dialog box is titled 'Trusted CA' and contains three radio button options: 'Local Certificate', 'PKCS12 Certificate' (which is selected), and 'Certificate and Private Key'. Below the options are two input fields: 'PKCS12 Password:' and 'PKCS12 File:' with a 'Select' button next to it. At the bottom are 'Upload' and 'Cancel' buttons.</p> </div> <div data-bbox="699 1547 1182 1868"> <p>This dialog box is also titled 'Trusted CA' and contains three radio button options: 'Local Certificate', 'PKCS12 Certificate', and 'Certificate and Private Key' (which is selected). Below the options are three input fields: 'Certificate file:' with a 'Select' button, 'Key Passphrase:' (Optional), and 'Key File:' with a 'Select' button. At the bottom are 'Upload' and 'Cancel' buttons.</p> </div> </div> <p>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</p>

	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

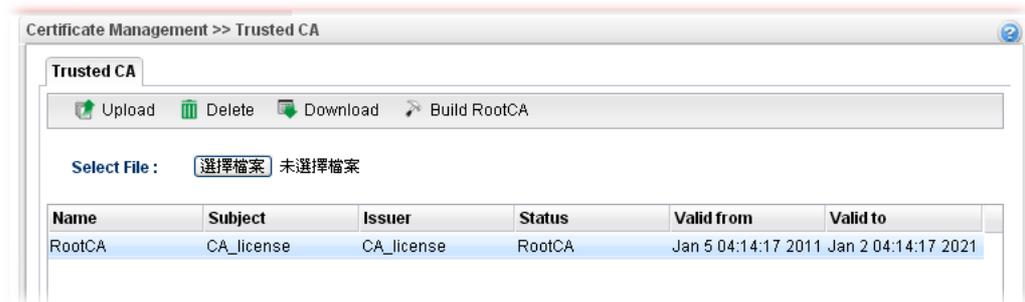
1. Open **Certificate Management>>Trusted CA Certificate**.
2. Simply click the **Build RootCA** button.
3. The following dialog will appear.

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.

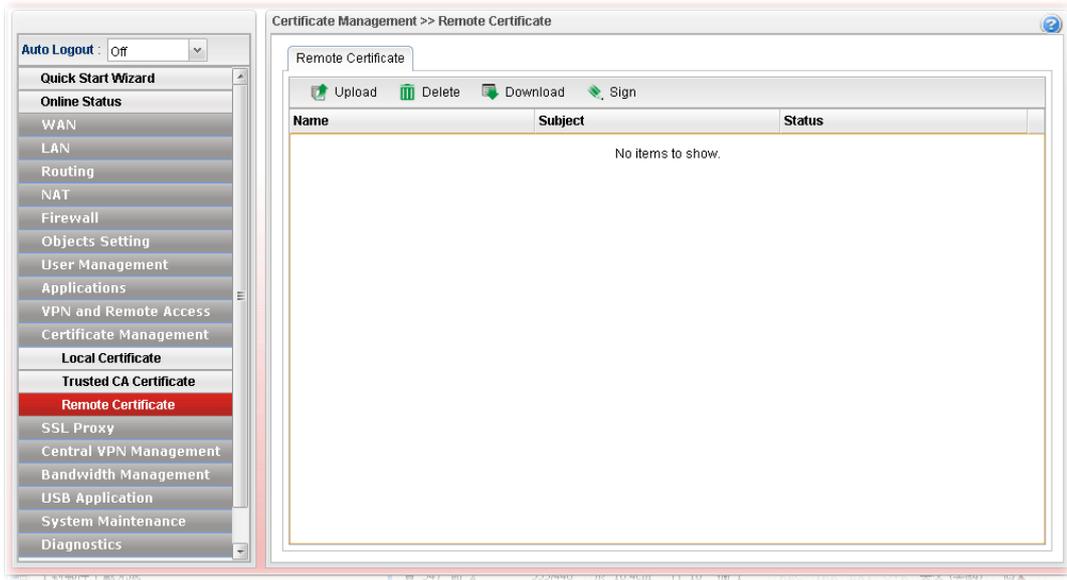
Organization	Type the name of the organization.
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state / province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
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.
Name	Display the name of remote certificate built.
Subject	Display the subject of remote certificate built.
Status	Display the status of remote certificate built.

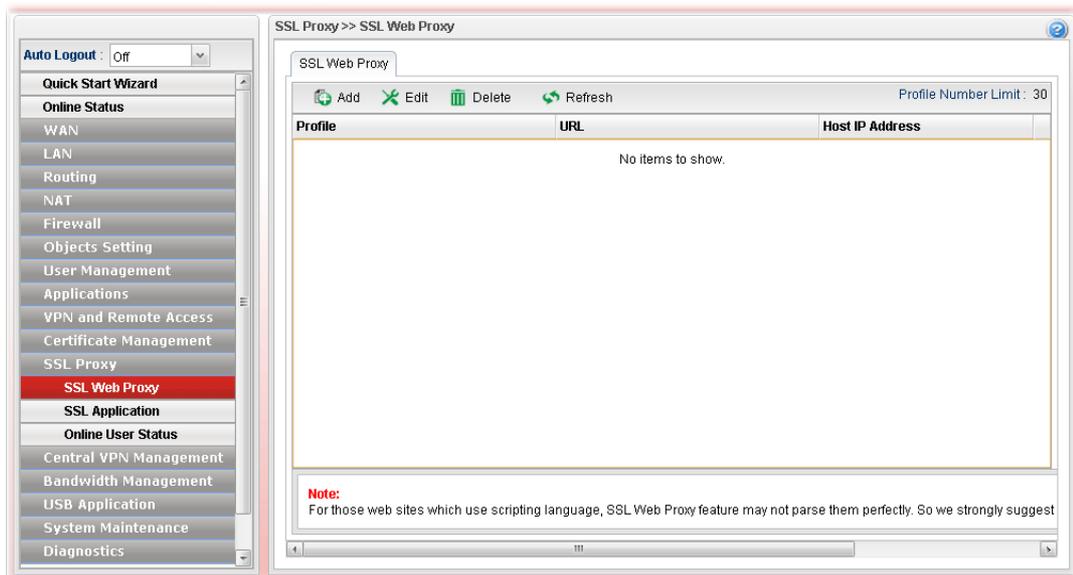
4.11 SSL Proxy

The profiles configured under such menu will be applied by **User Management>>User Profiles** for performing SSL VPN.



4.11.1 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.



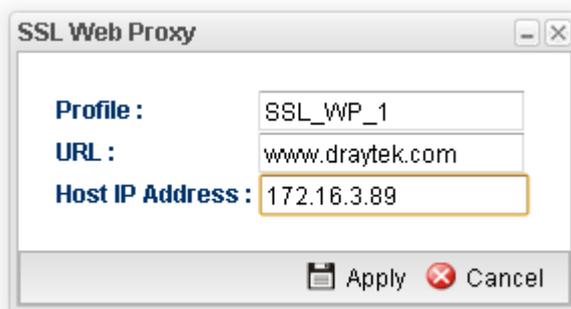
Each item will be explained as follows:

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 field. 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.

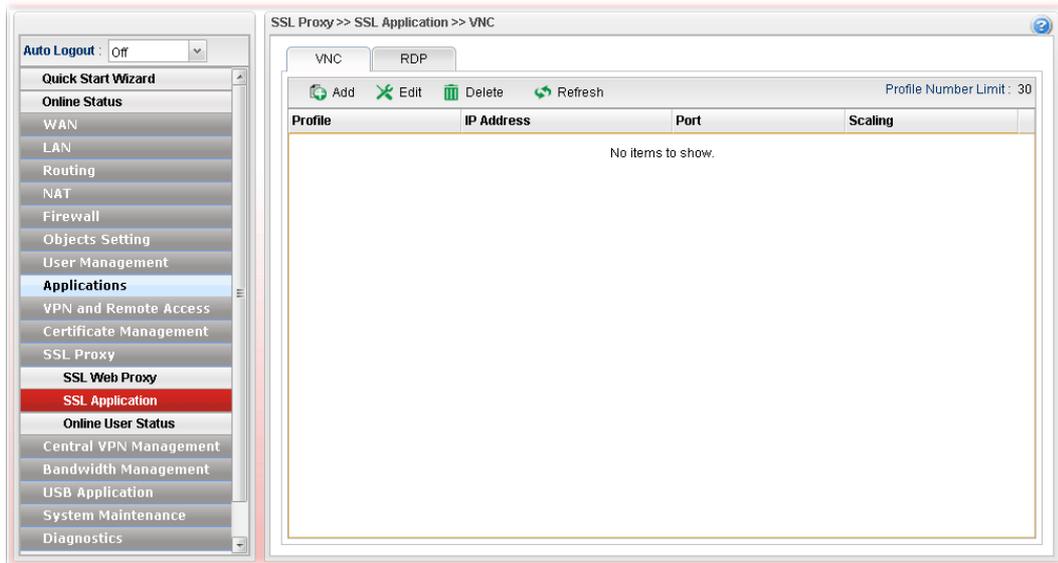
4. Enter all the settings and click **Apply**.
5. A new SSL Web Proxy profile has been created.

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.



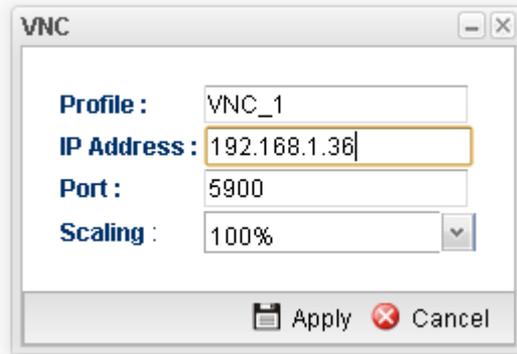
Each item will be explained as follows:

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.

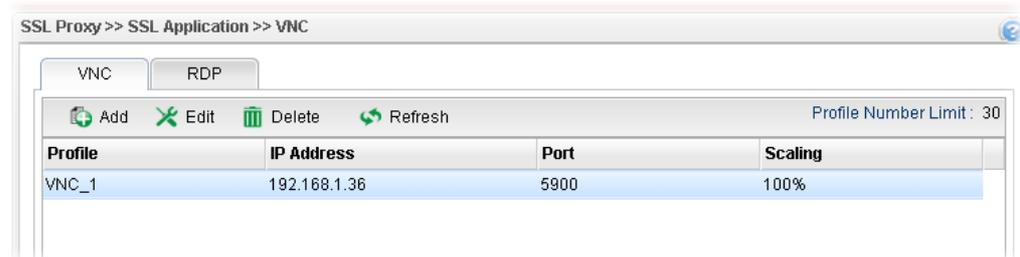
2. Simply click the **Add** button.
3. The following dialog will appear.



Available parameters are listed as follows:

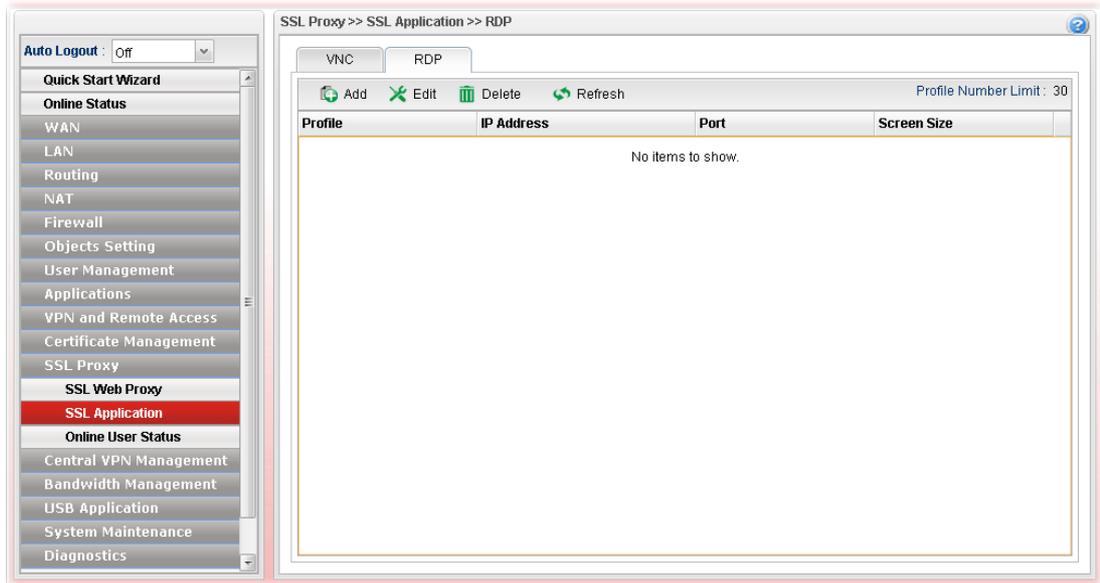
Item	Description
Profile	Type the name of the profile that you create.
IP Address	Type the IP address for this protocol.
Port	Specify the port used for this protocol. The default setting is 5900.
Scaling	Chose the percentage (100%, 80%, 60) for such application.
Apply	Click it to save the configuration.
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.

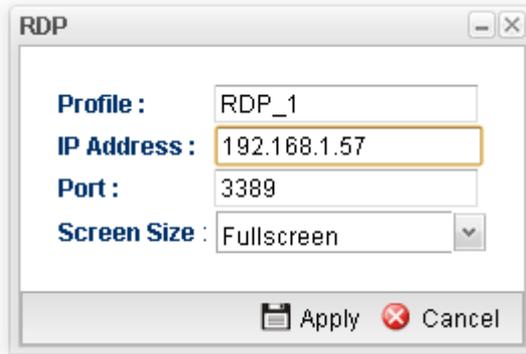


Each item will be explained as follows:

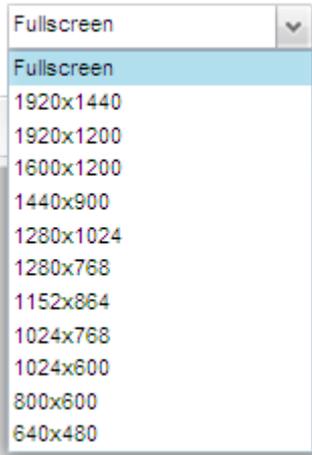
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete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



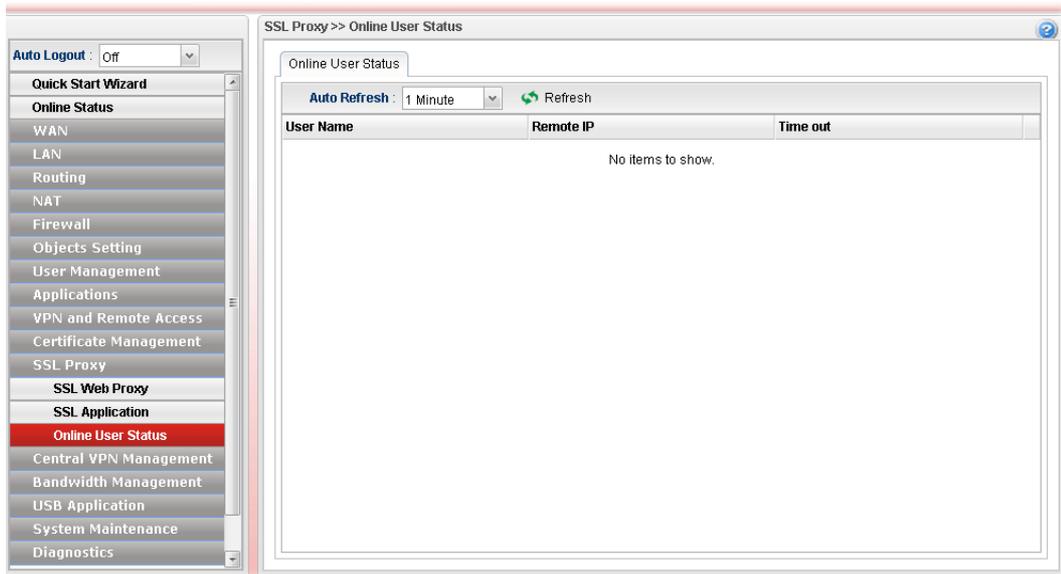
Available parameters are listed as follows:

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.



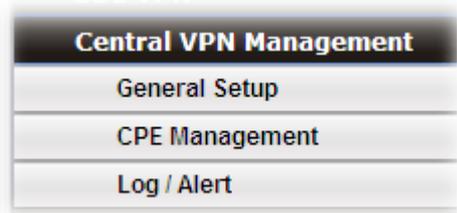
Each item will be explained as follows:

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 Central VPN Management

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:

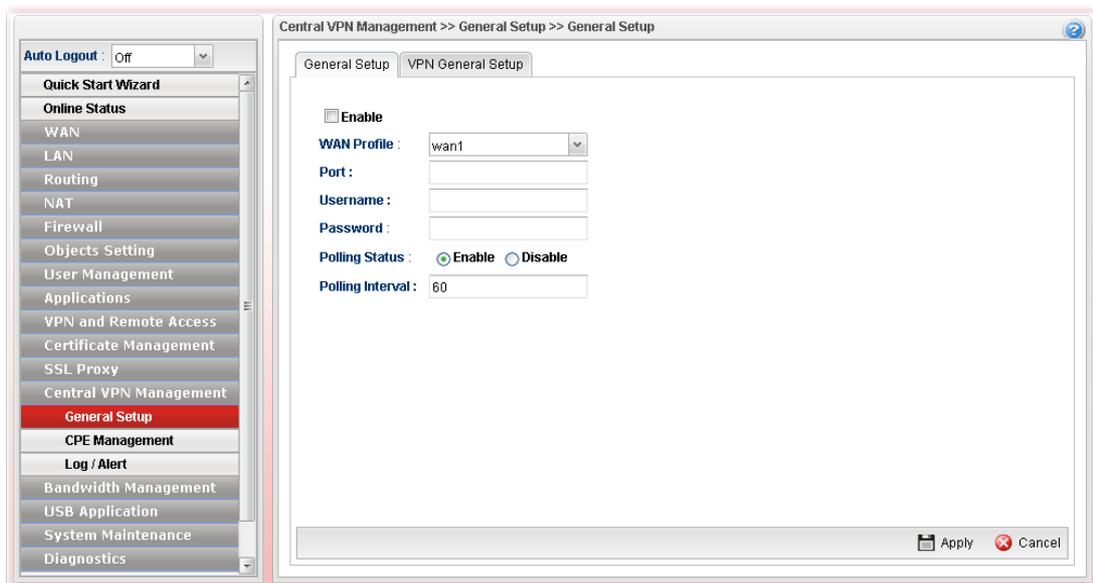


- Note:**
1. Such menu can manage the CPE connected through WAN only.
 2. Up to 16 devices can be managed.

4.12.1 General Setup

4.12.1.1 General Setup

This page is used to configure settings which will be used by the clients to register to such Vigor router.



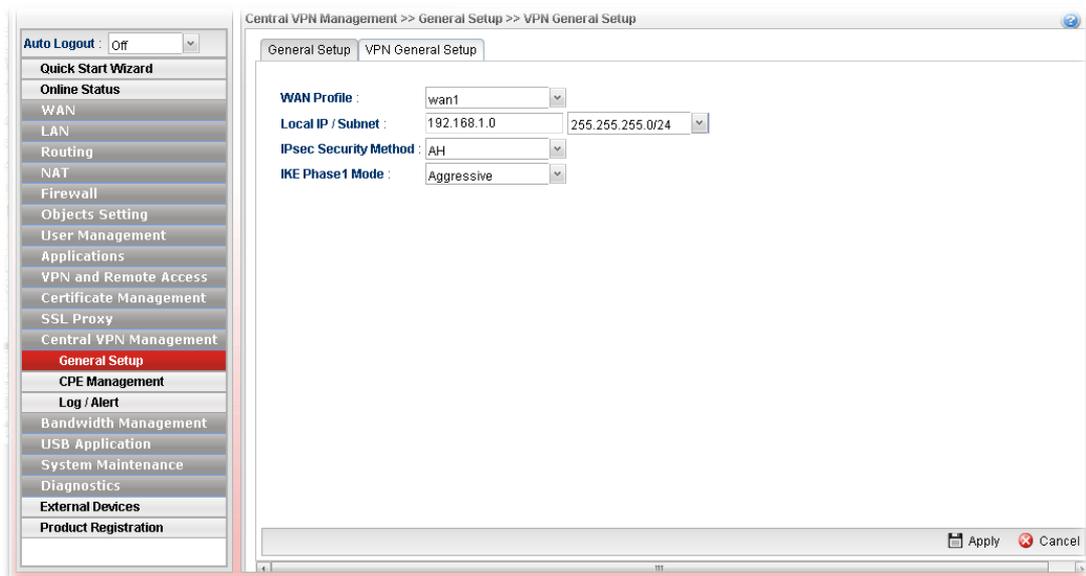
Available parameters are listed as follows:

Item	Description
Enable	Check it to enable the settings.
WAN Profile	Specify an interface for VPN management.
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.

4.12.1.2 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	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. <div data-bbox="683 1664 979 1937" data-label="Image"> </div>
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.

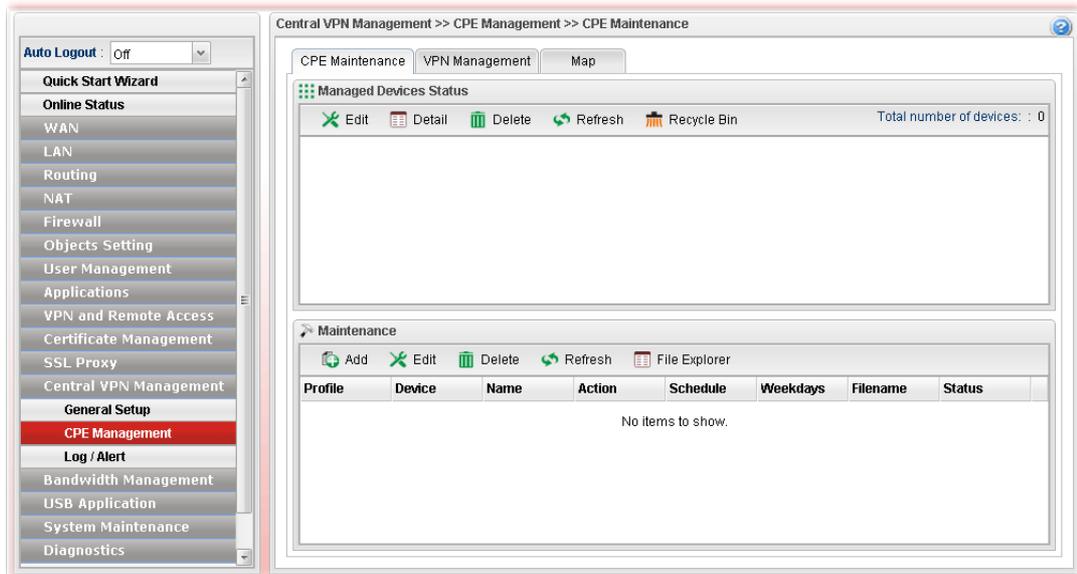
4.12.2 CPE Management

All the CPEs managed by Vigor3900 can be seen with icons from this page.

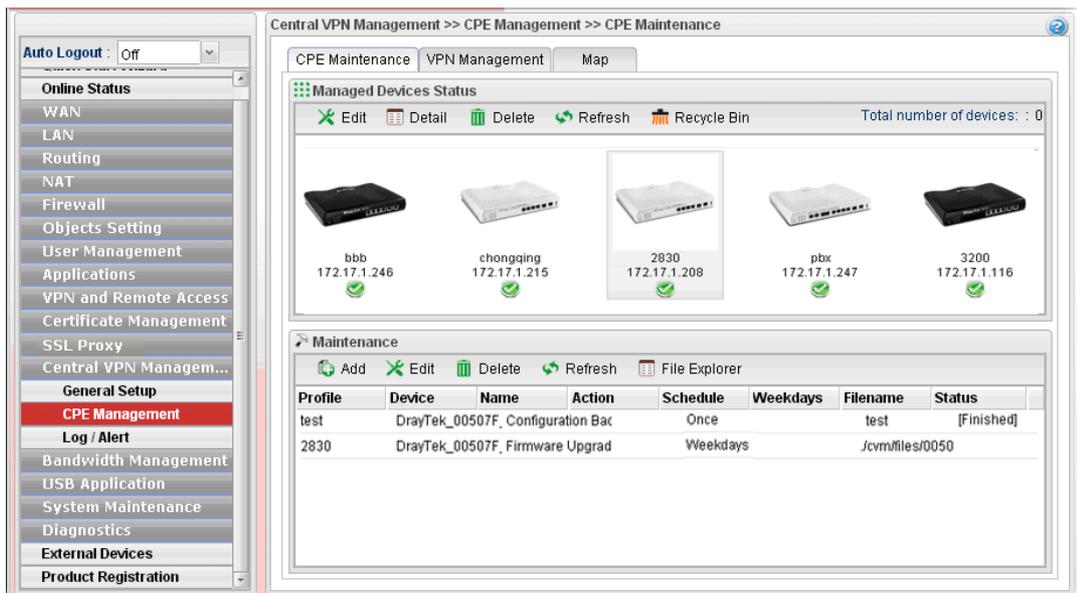
4.12.2.1 CPE Maintenance

This page allows you to manage the CPEs connected to Vigor3900.

- Page without CPE connected



- Page with CPE connected



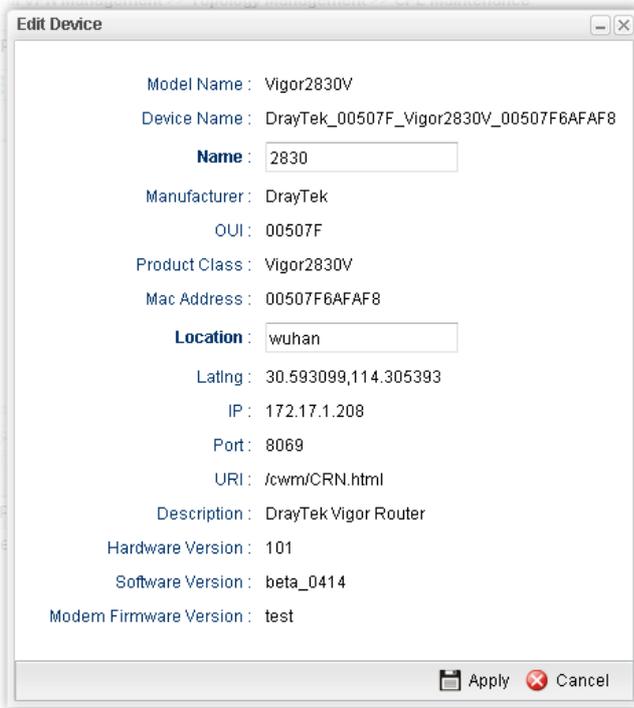
Available parameters are listed as follows:

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.



The screenshot shows a dialog box titled "Edit Device" with the following fields and values:

- Model Name : Vigor2830V
- Device Name : DrayTek_00507F_Vigor2830V_00507F6AFAF8
- Name : 2830
- Manufacturer : DrayTek
- OUI : 00507F
- Product Class : Vigor2830V
- Mac Address : 00507F6AFAF8
- Location : wuhan
- Latlng : 30.593099,114.305393
- IP : 172.17.1.208
- Port : 8069
- URI : /cwm/CRN.html
- Description : DrayTek Vigor Router
- Hardware Version : 101
- Software Version : beta_0414
- Modern Firmware Version : test

At the bottom right, there are "Apply" and "Cancel" buttons.

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.

Filename	Property	Size	LastModify	Directory
.	Directory	1248	2013/05/07/ 09:4	.jcvn/files
..	Directory	224	2013/01/10/ 11:3	.jcvn
00507F000000	Directory	224	2013/05/07/ 09:4	.jcvn/files
00507FC20A9C	Directory	880	2011/01/01/ 08:0	.jcvn/files
00507FC291A0	Directory	424	2013/05/07/ 11:4	.jcvn/files
00507FC291C0	Directory	400	2013/04/11/ 10:1	.jcvn/files
00507FC9FB9C	Directory	224	2013/01/16/ 18:1	.jcvn/files
00507FBFAD00	Directory	712	2013/03/22/ 15:0	.jcvn/files
00507F223344	Directory	304	2013/03/11/ 17:5	.jcvn/files
001DAA8B800	Directory	224	2013/01/16/ 18:1	.jcvn/files

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.

	<p>Filename – Display the filename of the firmware.</p> <p>Status – Display current status of the profile has been finished or not.</p>
--	---

Refer to sections “3.7 How to manage the CPE (router) through Vigor3900?” and “3.9 How to upgrade CPE firmware through Vigor3900?” for more detailed information.

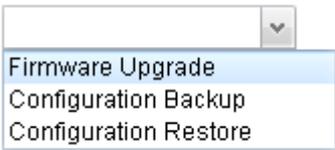
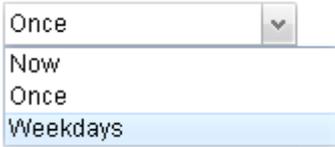
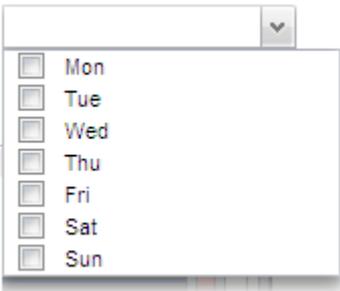
How to add a new Maintenance Profile

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	<p>The drop down list will display all the devices detected by Vigor3900. Choose the one which will be applied with such new created profile.</p> <p>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</p>

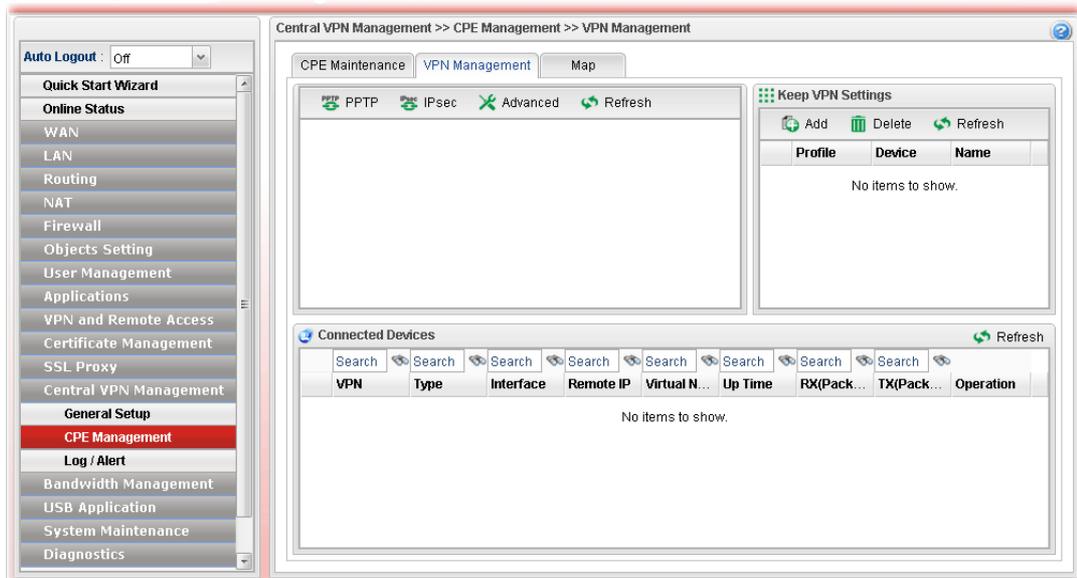
	specify another name for the device additionally.
Name	Display the name (can be modified by the administrator) of the device.
Action	<p>There are three actions for you to choose for such profile.</p>  <p>Firmware Upgrade – It means such profile will be used for firmware upgrade.</p> <p>Configuration Backup – It means such profile will be used for configuration backup of the selected CPE.</p> <p>Configuration Restore – It means such profile will be used for restoring the configuration of the selected CPE.</p>
Schedule	<p>The new created profile can be applied to the selected CPE based on the schedule configured here.</p>  <p>Now – The action will be performed for the selected CPE immediately.</p> <p>Once – The action will be performed for the selected CPE at the specified time, and will be done for once.</p> <p>Weekdays – The action will be performed for the selected CPE at the time and date specified below every week.</p>
Start Date / End Date	<p>It is available only when Once is selected as Schedule. Specify the starting date /ending date with the format YYYY-MM-DD.</p>
Start Time / End Time	<p>It is available only when Once is selected as Schedule. Specify the starting time /ending time with the format YYYY-MM-DD.</p>
Weekdays	<p>It is available only when Weekdays is selected as Schedule. Simply check the day you want.</p> 
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.

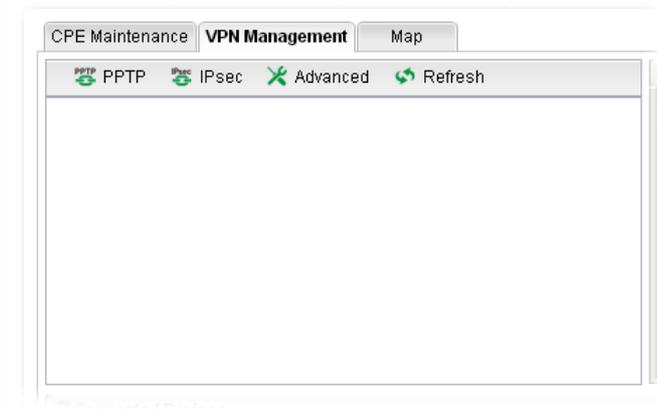
4.12.2.2 VPN Management

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:

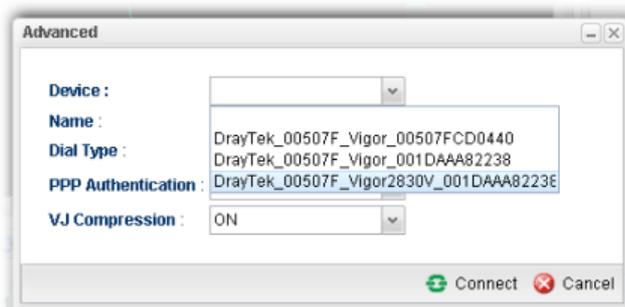
Item	Description
Display Screen	<p>Once the device is managed (controlled) by Vigor3900, it will be displayed on such screen automatically. If not, refer to sections “3.7 How to manage the CPE (router) through Vigor3900?” for more detailed information.</p> <p>If the VPN isn’t established successfully, a red line will appear instead.</p>



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.

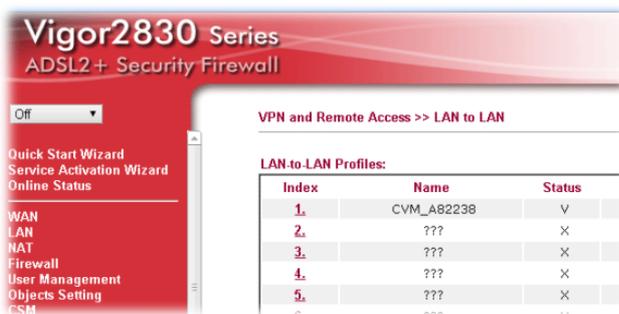
Advanced

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.

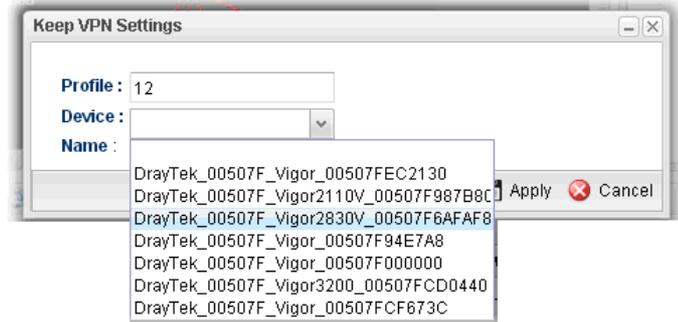
Note: If the VPN connection has been established successfully, a new **LAN to LAN profile** will be created for the CPE automatically. See the following example.



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.

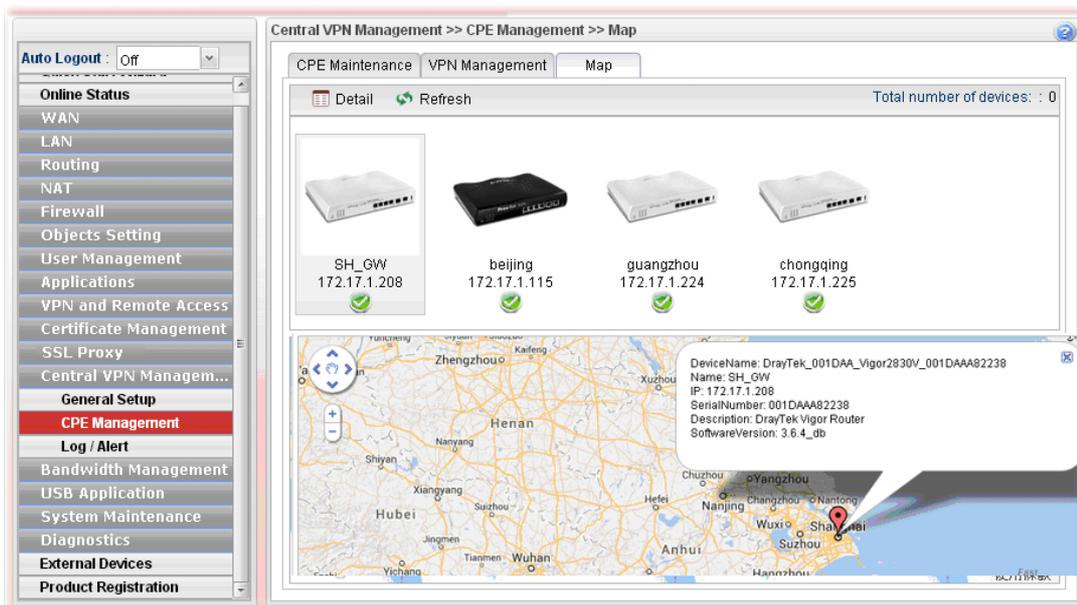
Up Time – Display the connection time of such VPN.

RX(Packets) /TX(Packets) – Display the number of the packets exchanged in such VPN.

Disconnect – Click it to disconnect the VPN.

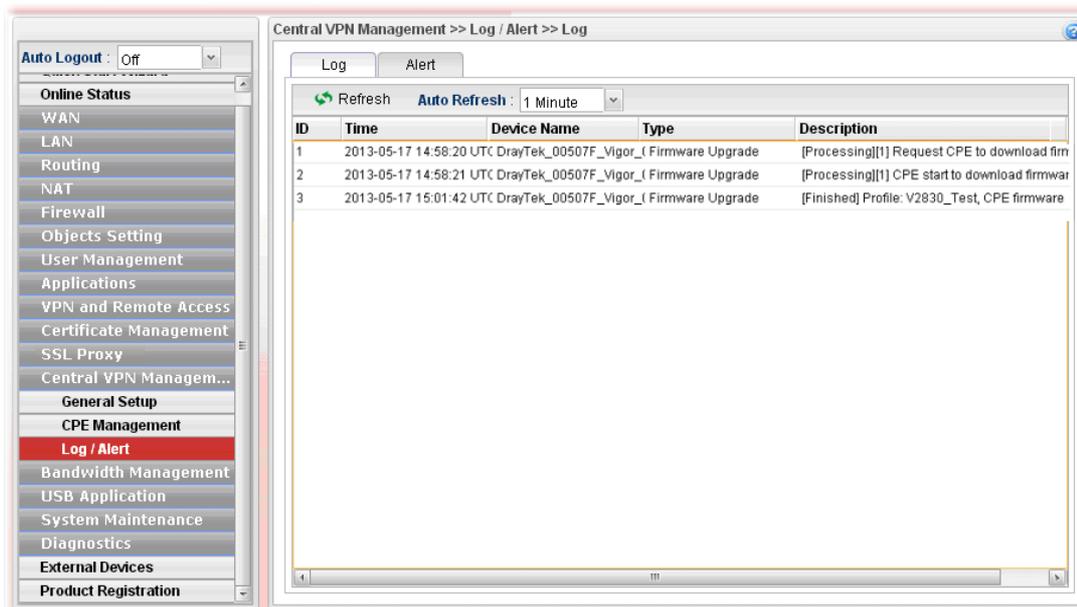
4.12.2.3 Map

To display the **location** of the selected CPE with a bird's eye view, open **Central VPN Management>>CPE Management** and click the tab of **Map**.



4.12.3 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.

Central VPN Management >> Log / Alert >> Alert

Log Alert

Refresh Auto Refresh: 1 Minute

ID	Time	Device Name	Type	Description
1	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!
2	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!
3	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!
4	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor2'	CPE Connection	CPE is offline!
5	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor2!	CPE Connection	CPE is offline!
6	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor2!	CPE Connection	CPE is offline!
7	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!
8	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!
9	2011-01-01 08:00:48 UTC	DrayTek_00507F_Vigor_I	CPE Connection	CPE is offline!

4.13 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.

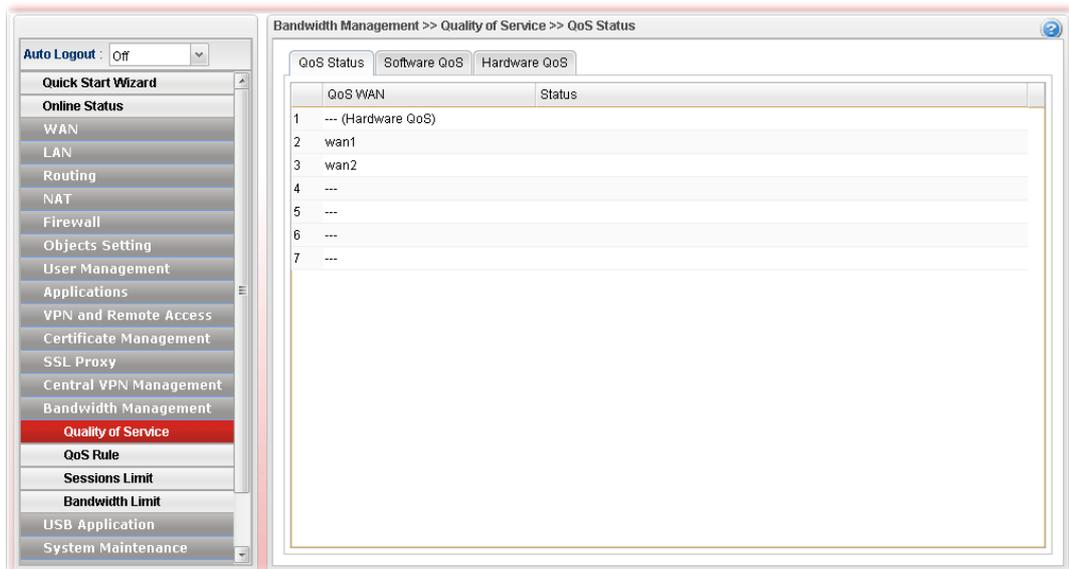
Differentiated quality of service is therefore one of the most important issues over the Internet infrastructure. In Vigor router, DSCP (Differentiated Service Code Point) support is also taken into consideration in the design of the QoS-guaranteed control module.

4.13.1 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.

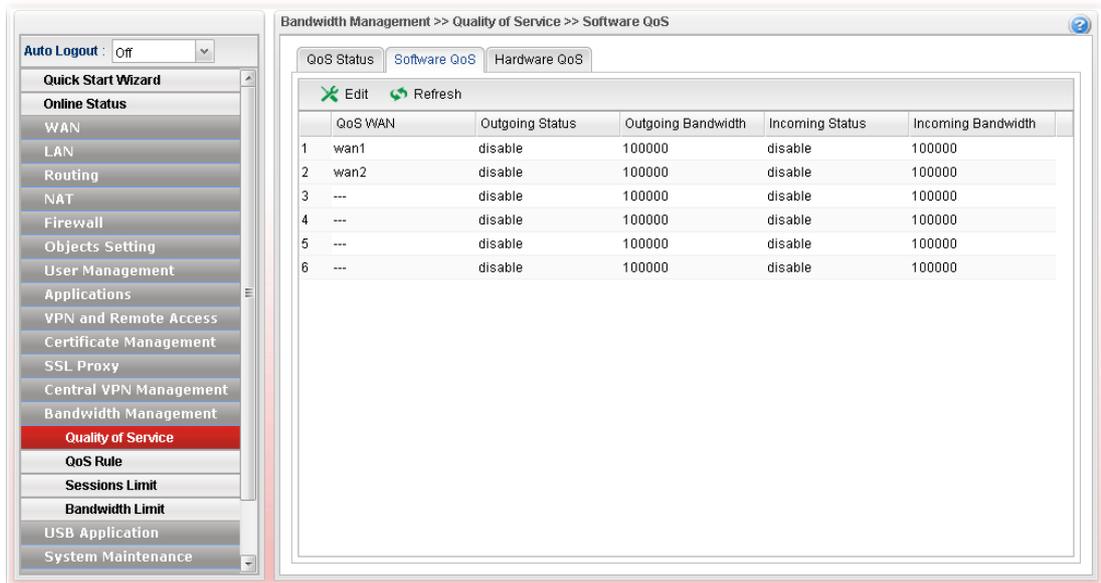
4.13.1.1 QoS Status

This page displays current QoS Status.



4.13.1.2 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.



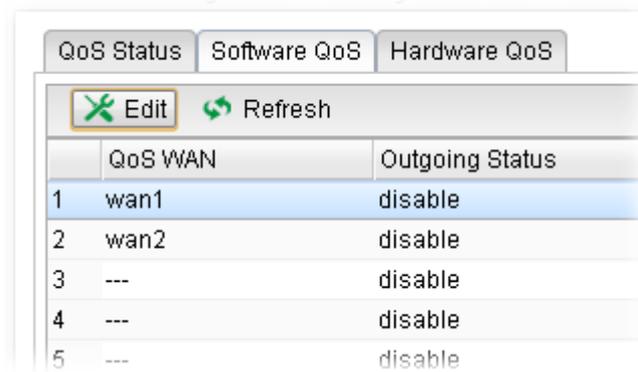
Available parameters are listed as follows:

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.
QoS 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.

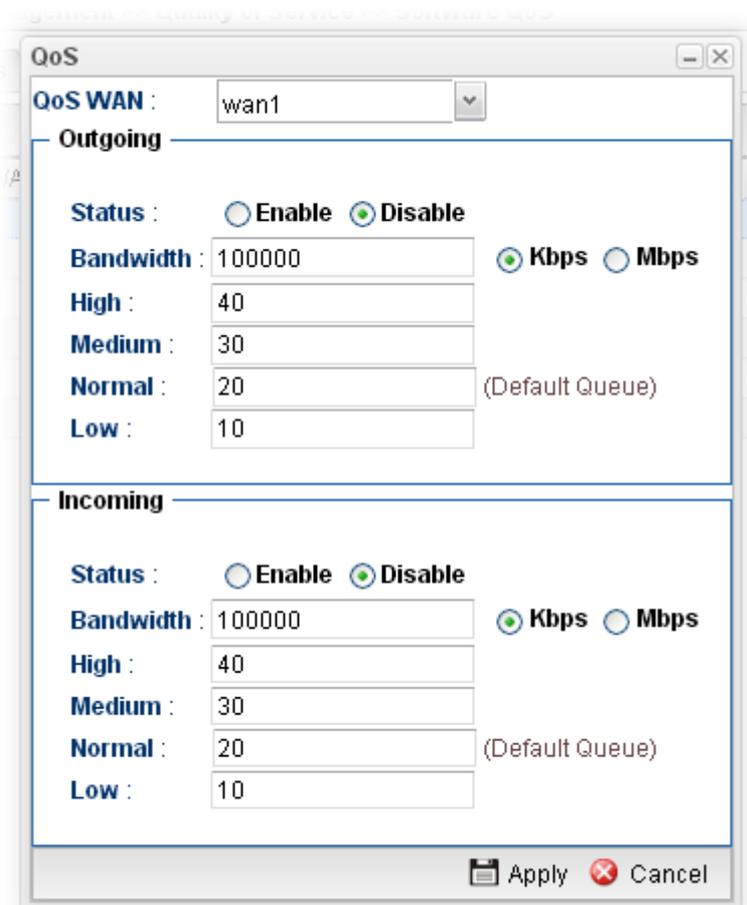
How to edit a QoS Profile

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**.



- The QoS settings page appears.



Available parameters are listed as follows:

Item	Description
QoS 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.

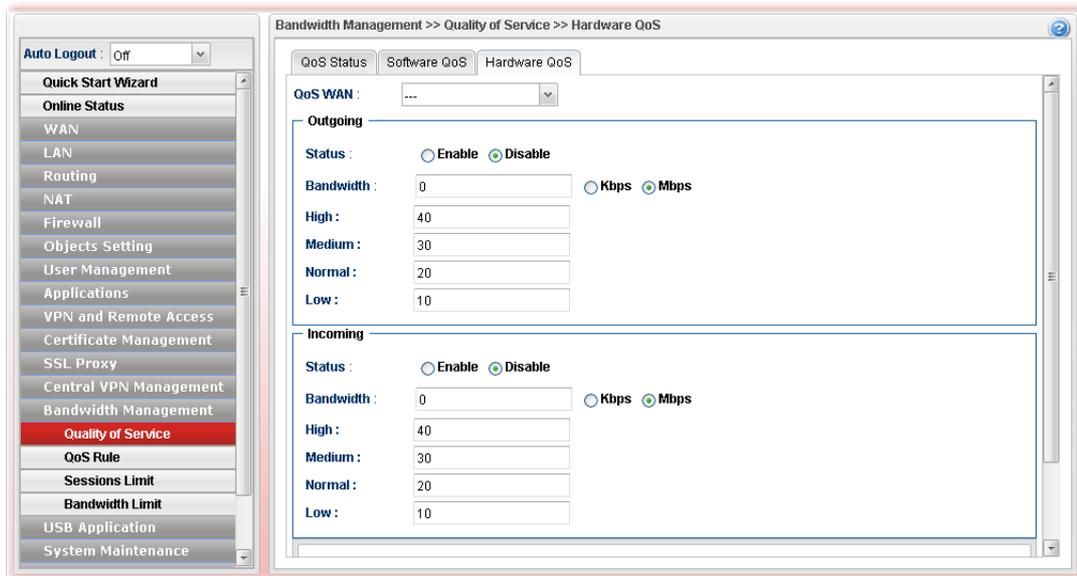
High/Medium/ Normal/Low	There are several available outgoing queues. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.13.1.3 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
QoS 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

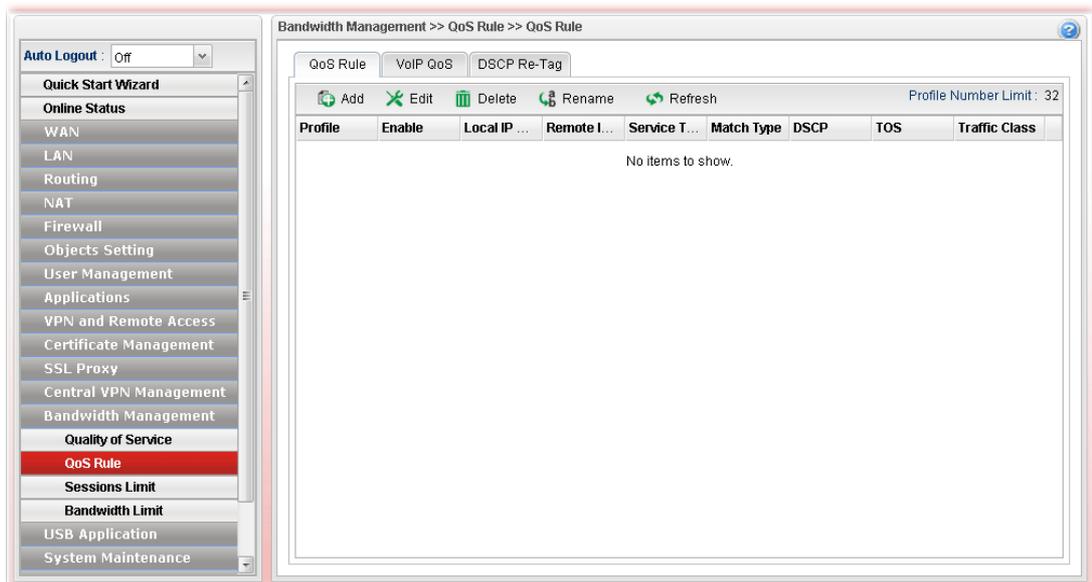
Normal/Low	data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.13.2 QoS Rule

There are 32 filter rules that can be configured in such page for incoming and outgoing data.

4.13.2.1 QoS Rule



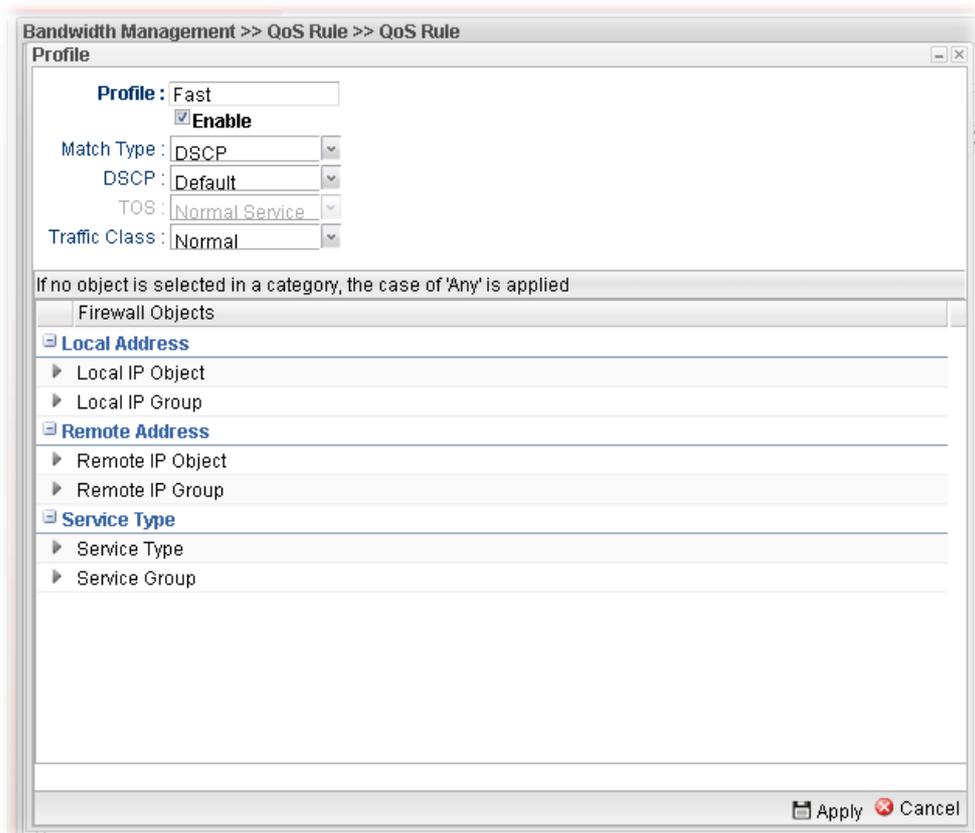
Available parameters are listed as follows:

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.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile for the filter.
Profile Number Limit	Display the total number (32) of the profiles to be created.

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.

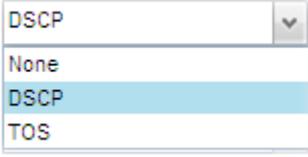
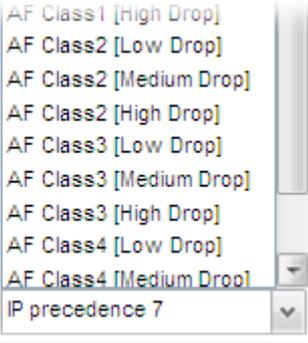
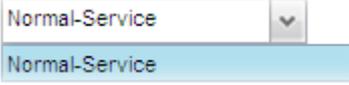
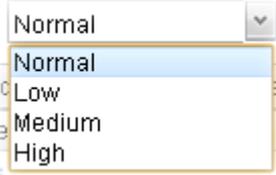
How to add a QoS rule profile

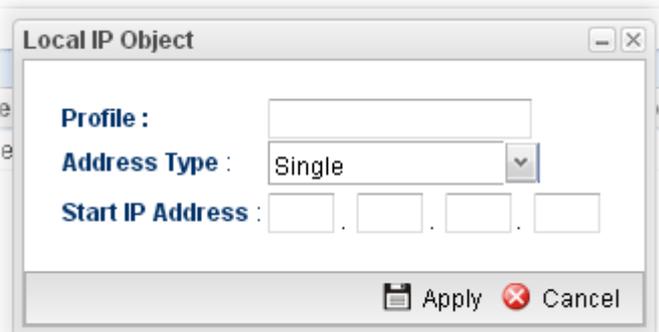
1. Open **Bandwidth Management>> QoS Rule**.
2. Simply click the **Add** button.
3. The following dialog will appear.



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	<p>It is available when DSCP is selected as the Match type.</p> 
TOS	<p>It is available when TOS is selected as the Match type.</p> 
Traffic Class	<p>Choose the traffic class to category the packets matching with the condition configured as above. High is the highest; Normal is the lowest.</p> 
Local Address	<p>Click  on the left side of the Source IP Object/Source IP Group profile. Check the object profile(s) as the source target.</p>  <p>Local IP Object – Use the drop down list to choose one of the IP objects for such rule profile.</p> <p>Local IP Group – Use the drop down list to choose one of the IP group for such rule profile.</p> <p>If you want to create a new IP object, simply click  to open the following dialog.</p>



- **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**.

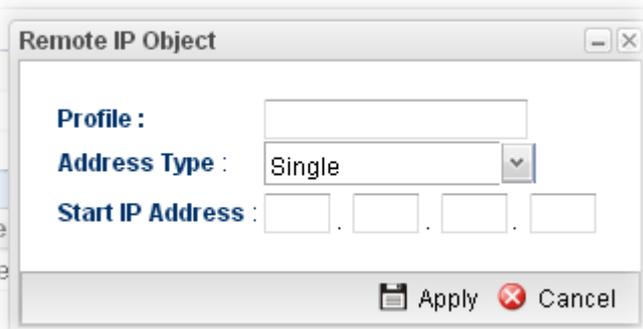
Remote Address

Click on the left side of the **Remote IP Object/ Remote IP Group** profile. Check the object profile(s) as the destination target.

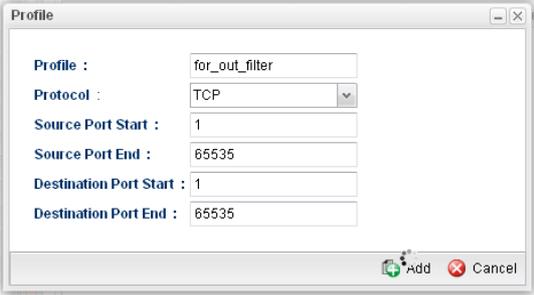
Remote IP Object – Use the drop down list to choose one of the destination IP objects for such rule profile.

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.



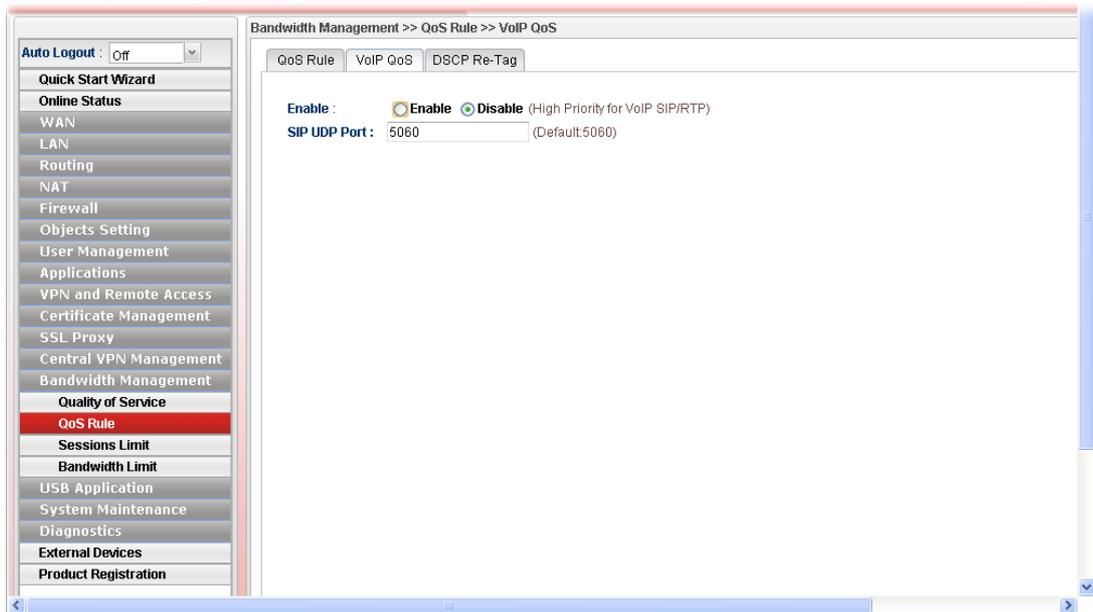
- **Profile** – Type a new name for such IP object.
- **Address Type** – Choose the address type (Single or Range) for such rule. Each type will bring different settings for configuration.
- **Start IP Address** - Type the IP address of the starting point for such profile.
- **End IP Address** - Type the IP address of the ending point for such profile if you choose **Range** as **Address**

	<p>Type.</p> <ul style="list-style-type: none"> ● Subnet Mask – Choose the subnet mask from the drop down list if you choose Subnet as Address Type.
<p>Service Type</p>	<p>Service Type - Choose one of the service types from the drop down list.</p>  <p>If you want to create a new service type, simply click  to open the following dialog.</p>  <ul style="list-style-type: none"> ● 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.
<p>Apply</p>	<p>Click it to save the configuration and exit the page.</p>
<p>Cancel</p>	<p>Click it to exit the page without saving the configuration.</p>

4. Enter all the settings and click **Apply**.
5. A QoS rule profiler has been created.

4.13.2.2 VoIP QoS

When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority during the process of data transmission.

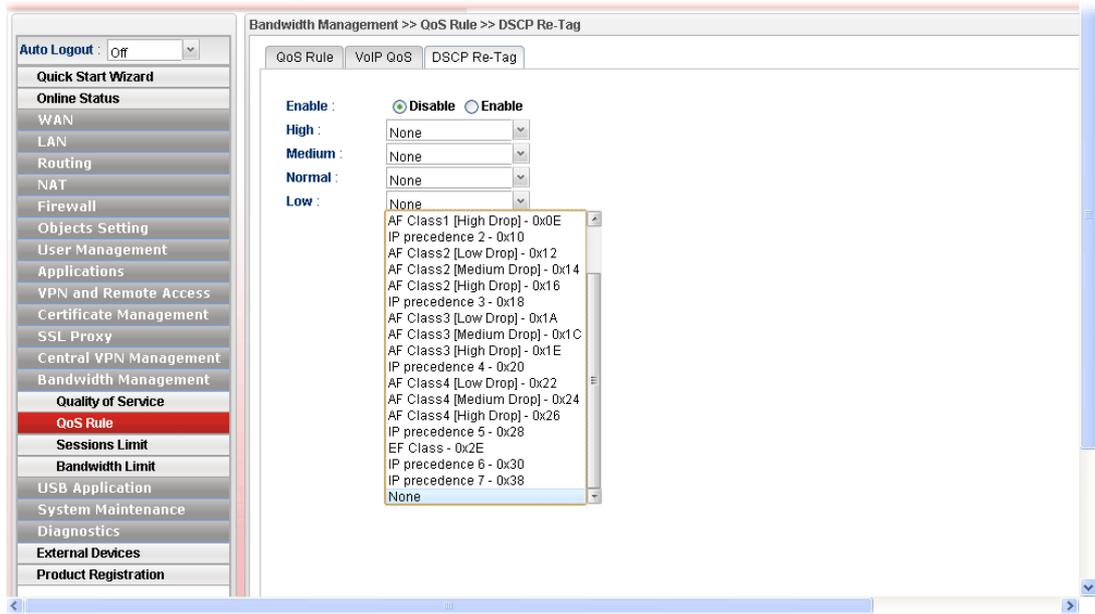


Each item will be explained as follows:

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.

4.13.2.3 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.



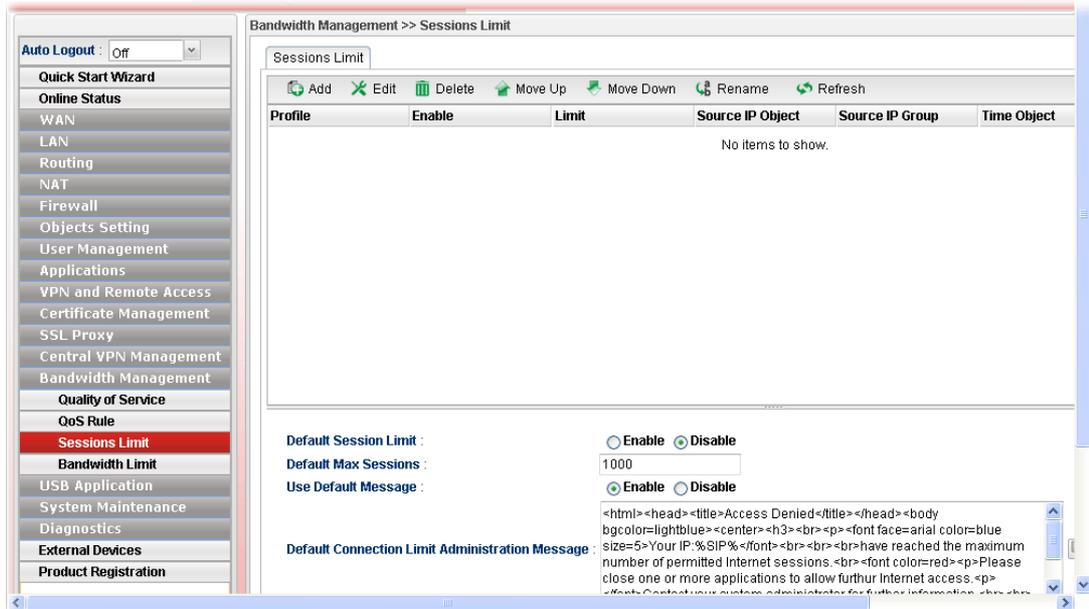
Each item will be explained as follows:

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.

4.13.3 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.



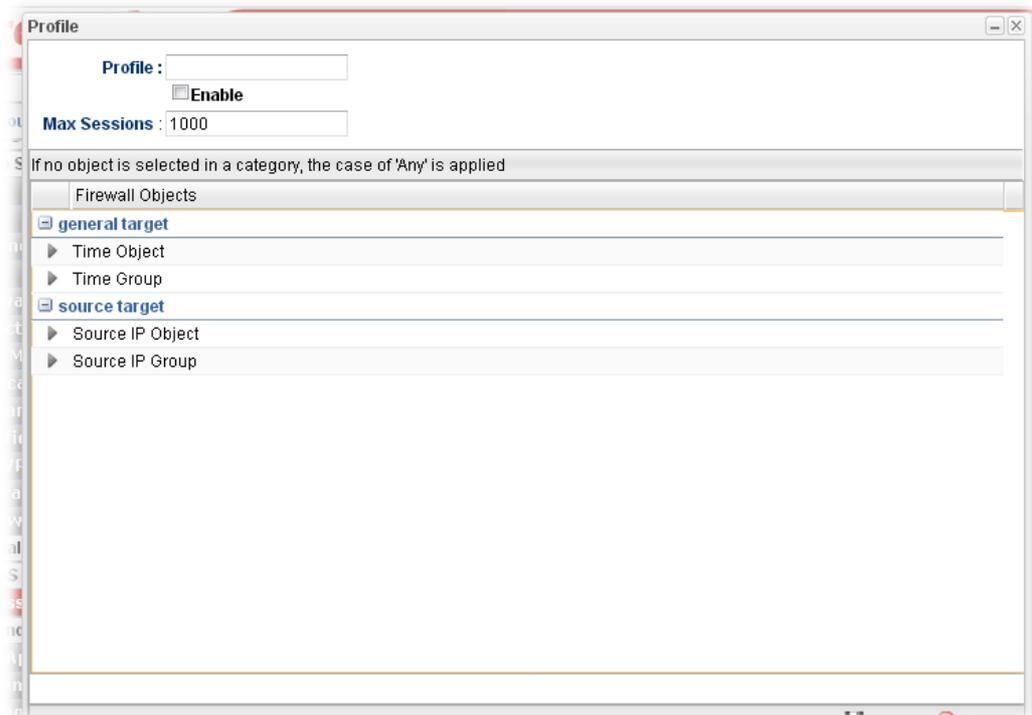
Each item will be explained as follows:

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

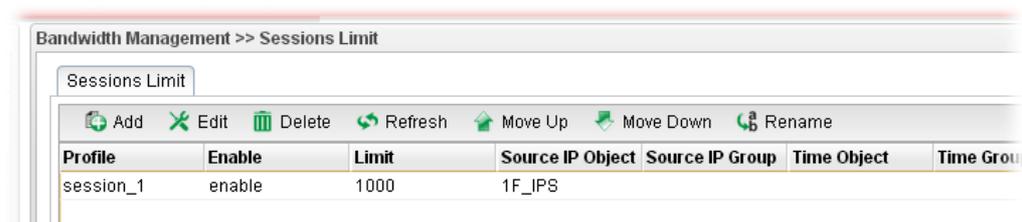
1. Open **Bandwidth Management>> Sessions Limit**.
2. Simply click the **Add** button.
3. The following dialog will appear.



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	<p>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.</p>  <p>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.</p>
source target	<p>Source IP 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.</p> <p>Source IP Group - Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new IP group profile.</p>
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.

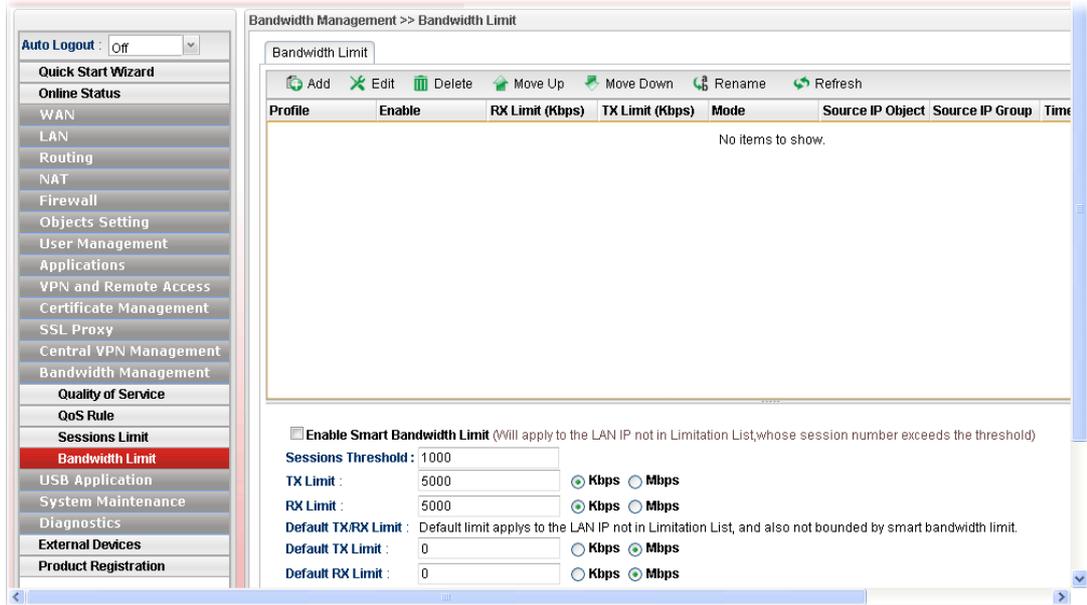


Profile	Enable	Limit	Source IP Object	Source IP Group	Time Object	Time Group
session_1	enable	1000	1F_IPS			

4.13.4 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.



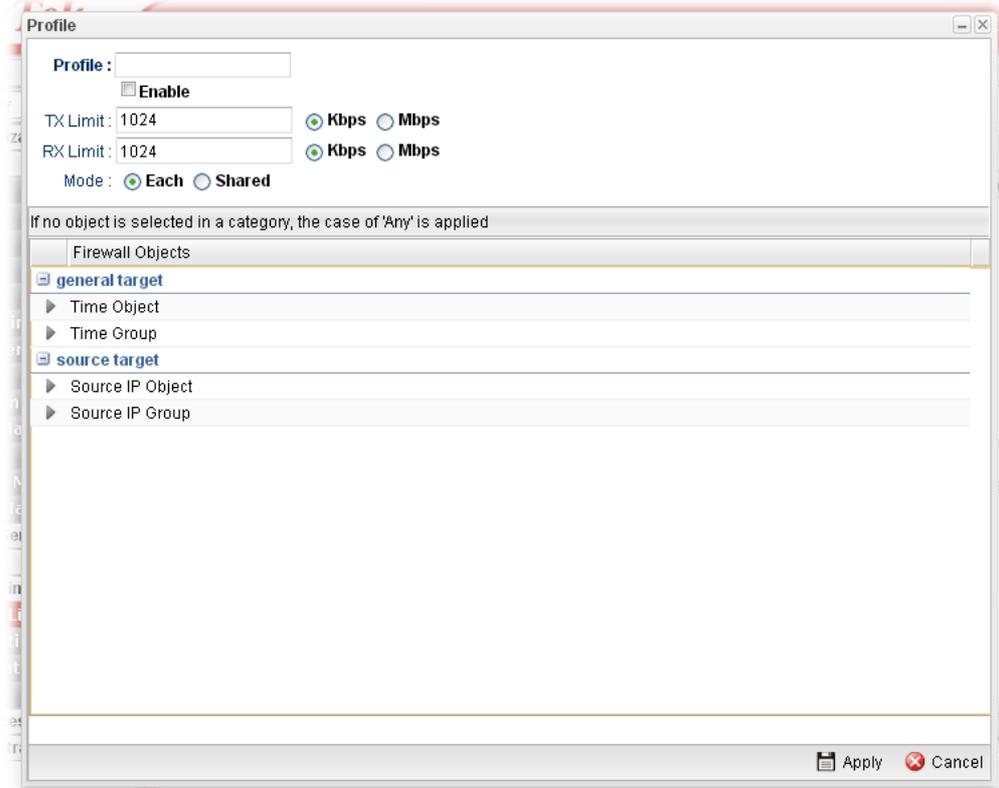
Each item will be explained as follows:

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.
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.
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.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

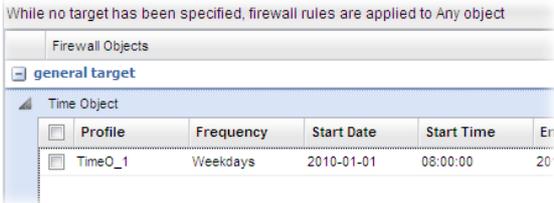
How to add a bandwidth limit profile

1. Open **Bandwidth Management>>Bandwidth Limit**.
2. Simply click the **Add** button.
3. The following dialog will appear.

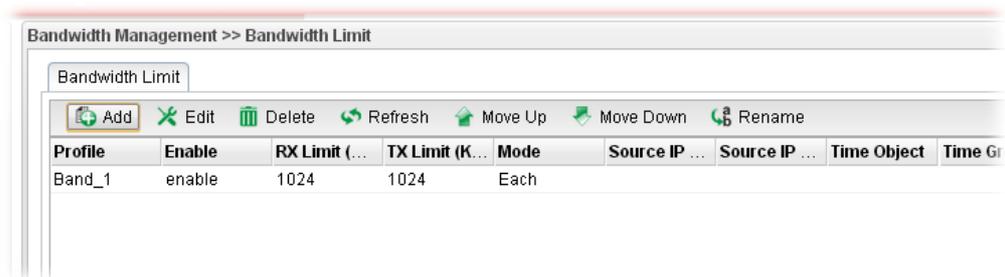


Available parameters are listed as follows:

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	<p>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.</p>  <p>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.</p>
source target	<p>Source IP 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.</p> <p>Source IP Group - Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be treated as source target. You can click  to create another new IP group profile.</p>
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

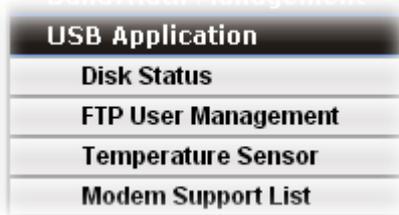
4. Enter all the settings and click **Apply**.
5. A bandwidth limit profile has been created.



4.14 USB Application

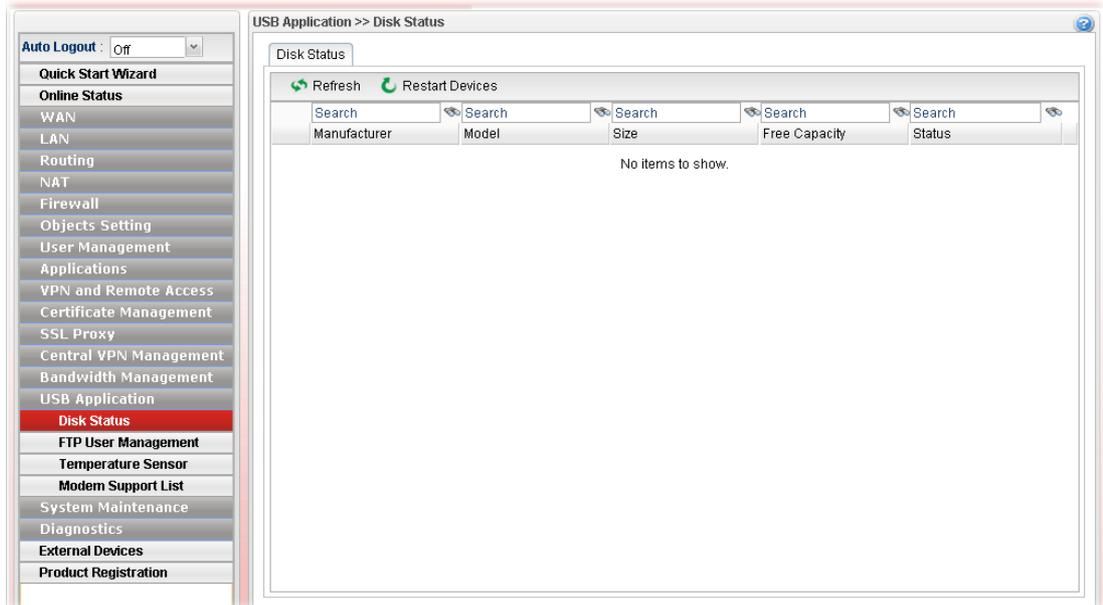
By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **User Management>>User Profile** on 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.



4.14.1 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.

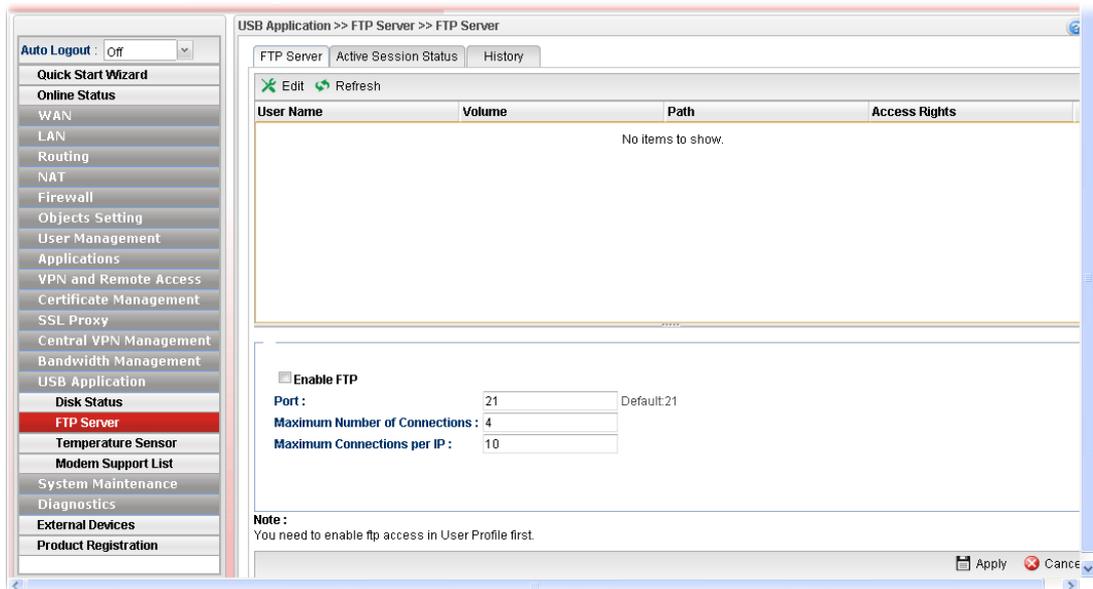
Size	Display the total disk capacity of the USB device.
Free Capacity	Display the remaining disk space of the USB device.
Status	Display the status of the USB device.
 (Remove Icon)	At present, FAT, EXT2, EXT3 USB format can be supported by Vigor router. If such USB is inserted into the USB slot, the 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.

4.14.2 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”.

4.14.3 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.

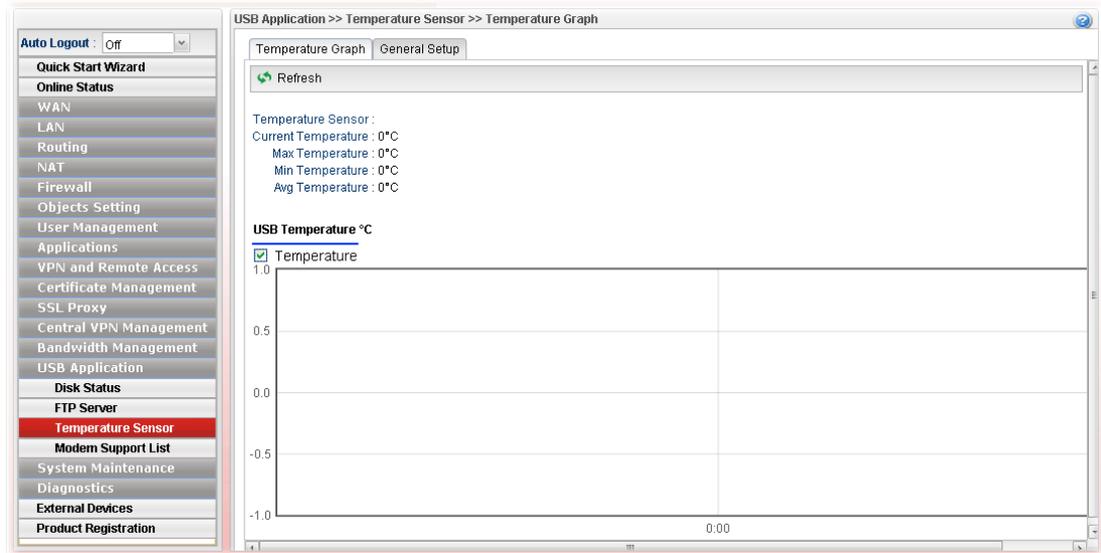


During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

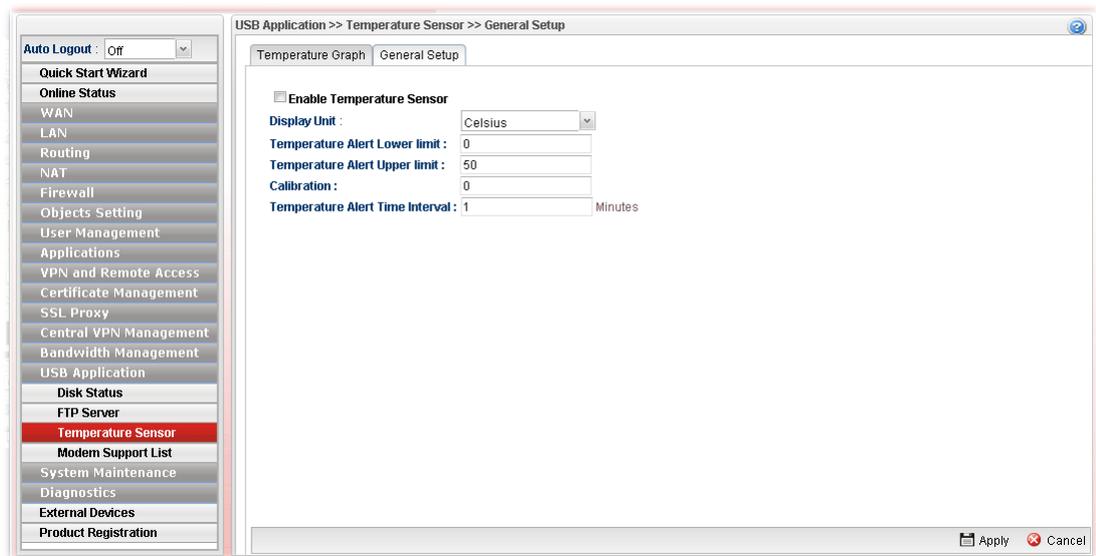
The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

4.14.3.1 Temperature Graph

Below shows an example of temperature graph:



4.14.3.2 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	The default setting is one minute. That means, the

Interval	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**.

4.14.4 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.

The screenshot shows the 'Modem Support List' page in the Vigor router's web interface. The left sidebar contains a navigation menu with 'Modem Support List' highlighted. The main content area displays a table of supported USB modems under the 'LTE' tab. The table has four columns: Brand, Module, PPP, and DHCP. Below the table, there is a 'Note' section explaining the compatibility test results.

Brand	Module	PPP	DHCP
Huawei	Huawei E3272	Y	Y
Huawei	Huawei E3276	-	Y
Huawei	Huawei E392	Y	Y
Huawei	Huawei E398	Y	Y
LG	VL800	M	M
Novatel Wireless	Novatel 551L	M	M
Novatel Wireless	UML290VV	M	M
Samsung	Samsung GT-B3730	M	M
Vodafone	Vodafone K4201	-	Y
ZTE	ZTE MF820D	Y	Y
ZTE	ZTE MF821D	-	Y
ZTE	ZTE MF880D	M	M
Alcatel	One Touch L100V	Y	-
4G Systems	XS-Stick W100	Y	-

Note:
The following compatibility tests listed above Vigor router models with USB modems / mobiles. If it is confirmed as the latest and st
Y: Tested and is supported.
M: Has not been tested but might be supported.
C: Supported with specific circumstances.
-: Not supported.

4.15 System Maintenance

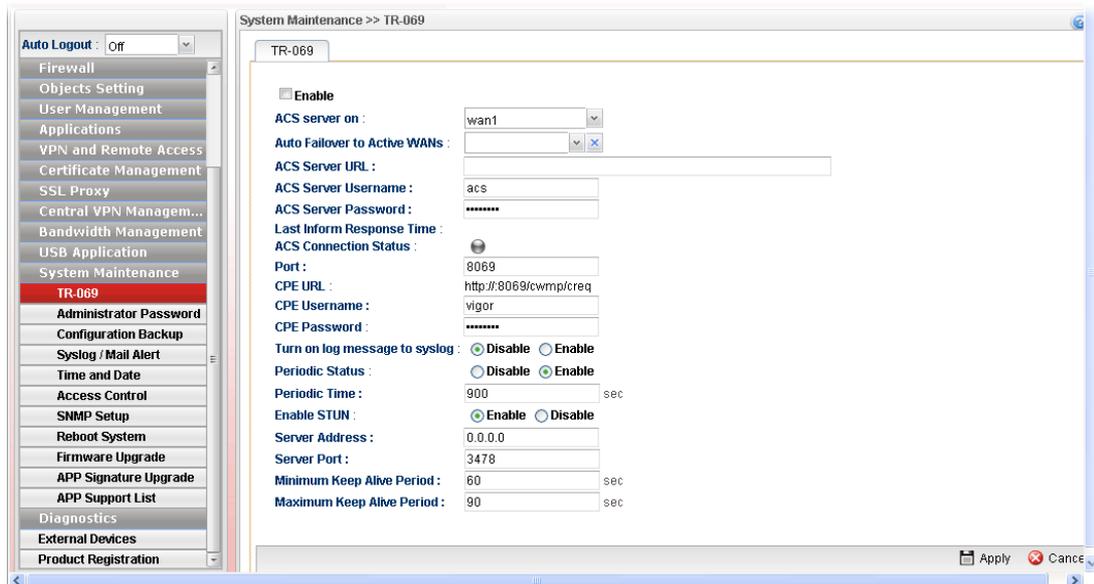
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Access Control, SNMP Setup, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.15.1 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	Specify the WAN interface to take over the job of network

WANs	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.
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**.

4.15.2 Administrator Password

This page allows you to set new password for accessing into the web user interface of the router.

The screenshot shows a web browser window with the title "System Maintenance >> Administrator Password". On the left is a navigation menu with "Administrator Password" selected. The main content area has three input fields labeled "Original Password:", "New Password:", and "Confirm Password:". Below these fields is a red "Note" stating: "Passwords can be up to 100 characters in length, and only the following characters are allowed: a-z A-Z 0-9 : ; , - ~ * ' < > * + = | ~ ^ / @ \$ %". An "Apply" button is located at the bottom right of the form area.

Each item will be explained as follows:

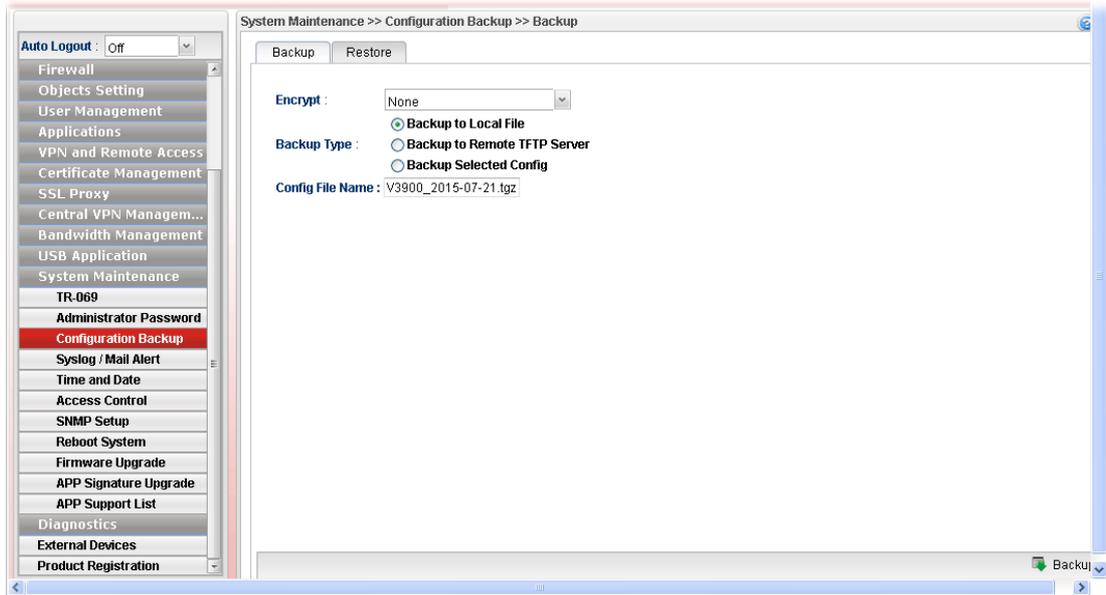
Item	Description
Original Password	Type the old password.
New Password	Type the new password.
Confirm Password	Re-type the new password for confirmation.
Apply	Click this button to save the configuration and exit the web page.

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

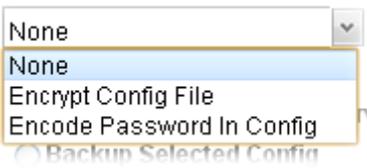
4.15.3 Configuration Backup

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.

4.15.3.1 Backup

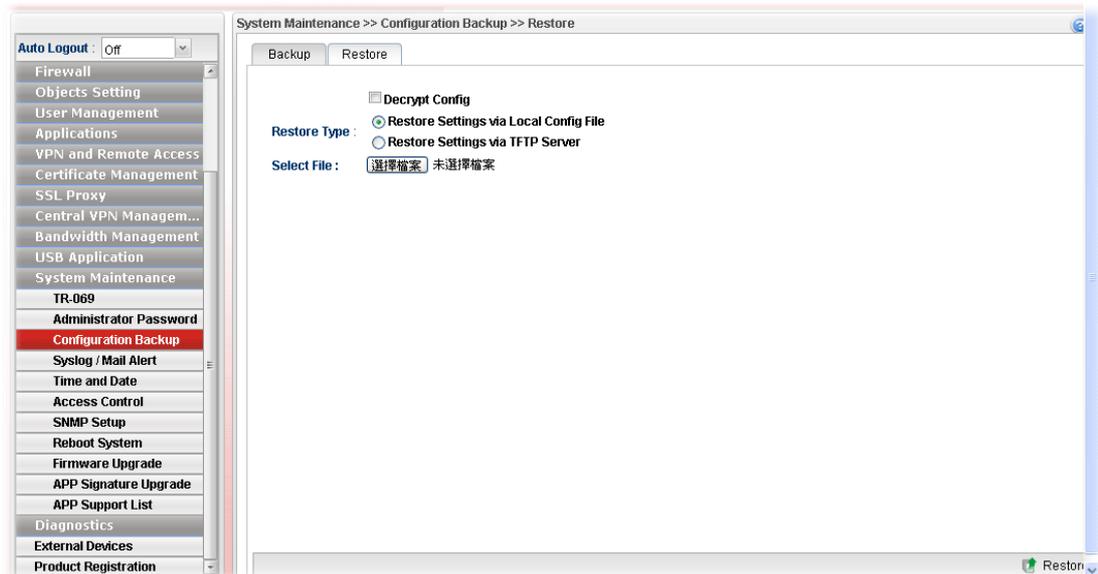


Each item will be explained as follows:

Item	Description
Encrypt	<p>None – No encryption will be used.</p> <p>Encrypt Config File – Choose it to encrypt the whole configuration file.</p> <ul style="list-style-type: none"> ● Password – Type a password for encrypting the file. ● Confirm Password – Retype the password for confirmation.  <p>Encode Password in Config – Choose it to encrypt the password information in configuration file.</p>
Backup Type	<p>Choose one of the types to determine where the file will be stored.</p> <p>Backup to Local File – The configuration file will be stored in local host.</p> <p>Backup to Remote TFTP Server – The configuration file will be stored in the remote TFTP server specified.</p> <p>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.</p>

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.

4.15.3.2 Restore



Each item will be explained as follows:

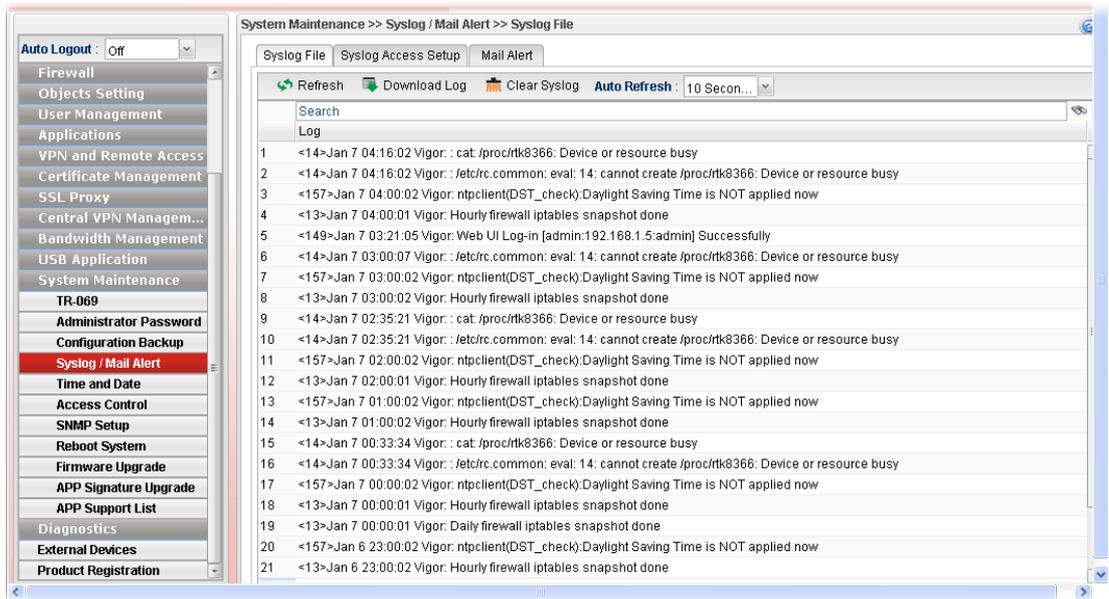
Item	Description
Decrypt Config	<p>Check this box to decrypt an encrypted configuration file. You can specify a password for decrypting the file for restoring it for use next time.</p> <p>Password – Type a password for encrypting the file.</p> <p>Confirm Password – Retype the password for confirmation.</p>
Restore Type	<p>Choose one of the types to determine where the file will be downloaded from.</p> <p>Restore Settings via Local Config File – Click it to restore the configuration settings through a configuration file stored locally.</p> <p>Restore Settings via TFTP Server – Click it to restore the configuration settings through TFTP server.</p>
Select File	Use the Select button to locate the file for uploading to the router.
Restore	<p>Click it to upload the selected file to the router. After finishing the restoration, the system will ask you to reboot the router.</p> 

4.15.4 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.

4.15.4.1 SysLog File

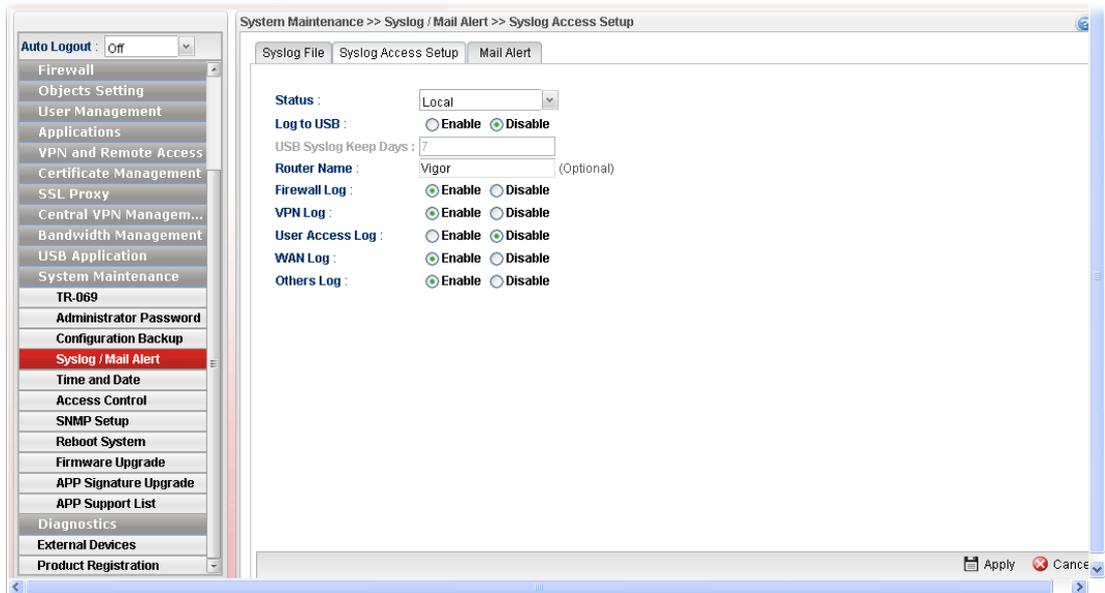
This page displays all the operation logs for the router.



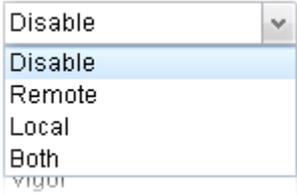
Available parameters are listed as follows:

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.

4.15.4.2 Syslog Access Setup



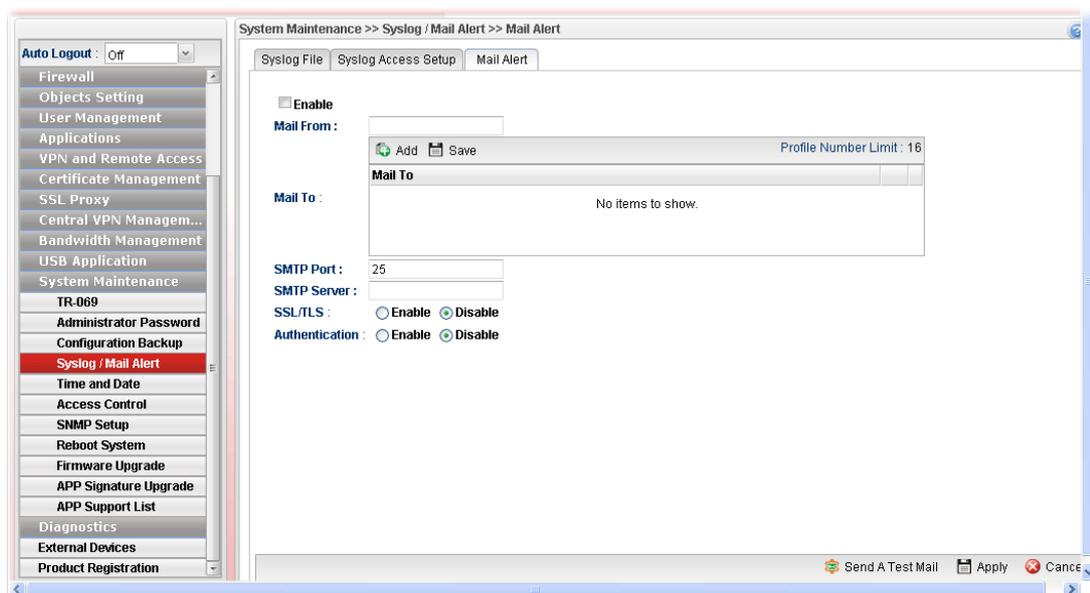
Available parameters are listed as follows:

Item	Description
Status	<p>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.</p> 
Log to USB	<p>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.</p>
Server IP	<p>Type the IP address of the Syslog server. It is available when Remote or Both is selected as Status.</p>
Server Port	<p>Type the port number for the Syslog server. It is available when Remote or Both is selected as Status.</p>
Router Name	<p>Type the name of the router. The default name is Vigor.</p>
Firewall Log	<p>Click Enable to make the firewall log recorded in the Syslog.</p>
VPN Log	<p>Click Enable to make the VPN log recorded in the Syslog.</p>
User Access Log	<p>Click Enable to make the user access log recorded in the Syslog.</p>
WAN Log	<p>Click Enable to make the WAN log recorded in the Syslog.</p>

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**.

4.15.4.3 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 Port	Type the port number for SMTP server.
SMTP Server	Type the IP address for SMTP server.
SSL/TLS	Click Enable to activate SSL/TLS 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.
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

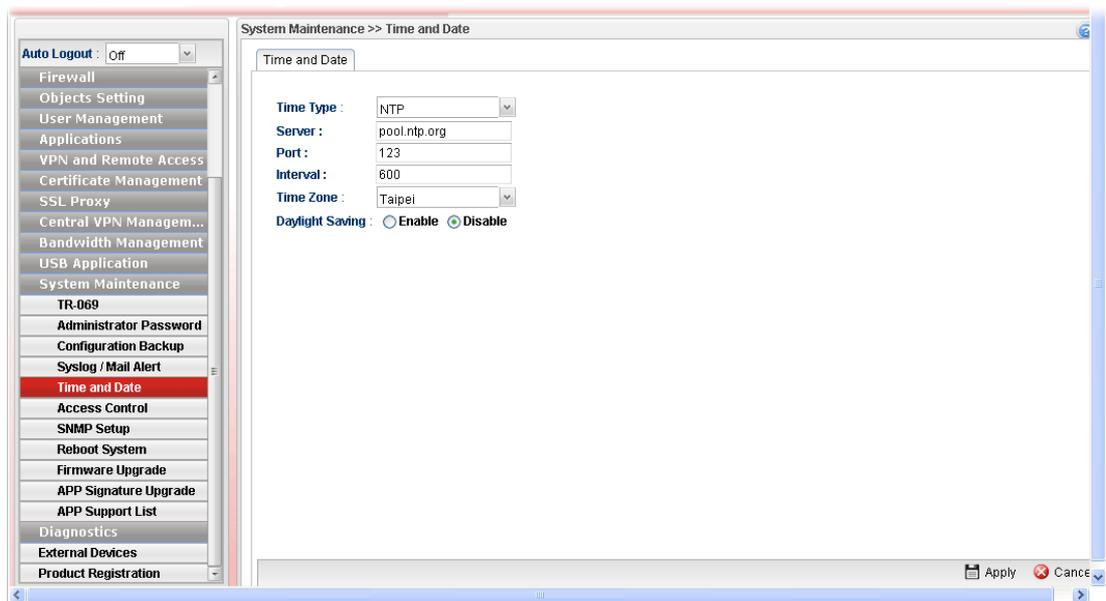
	page.
Cancel	Click it to discard the settings configured in this page.

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

4.15.5 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:

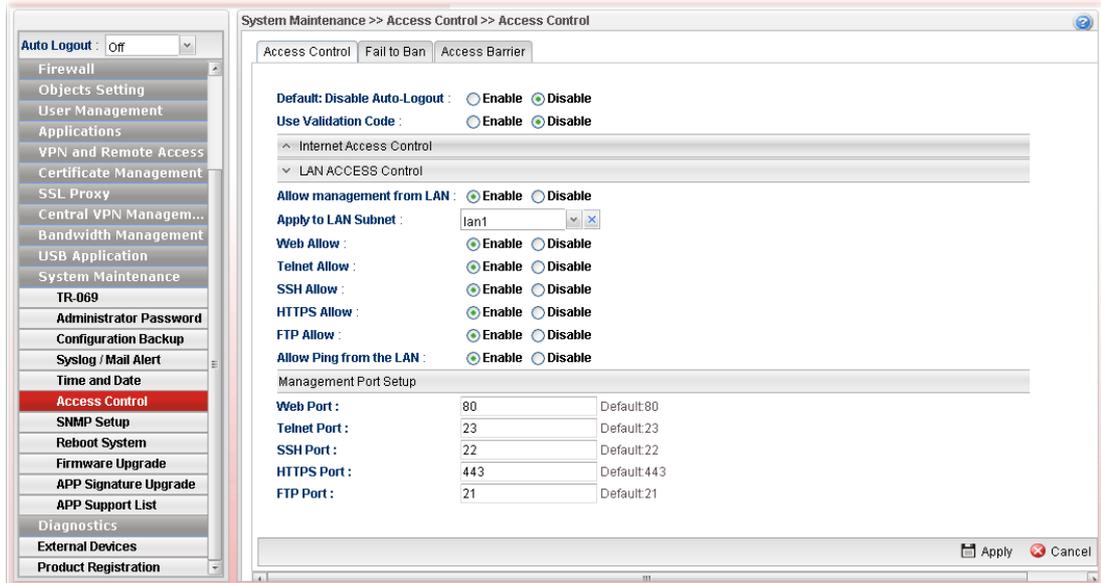
Item	Description
Time Type	NTP – Select to inquire time information from Time Server on the Internet using assigned protocol. Browser - Select this option to use the browser time from the remote administrator PC host as router's system time.
Server	Type the domain name of the server.
Port	Type the port 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**.

4.15.6 Access Control

4.15.6.1 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	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. Disable – No validation will be done when a user tries to log into the web user interface of Vigor router.
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.
Internet Access Control	
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

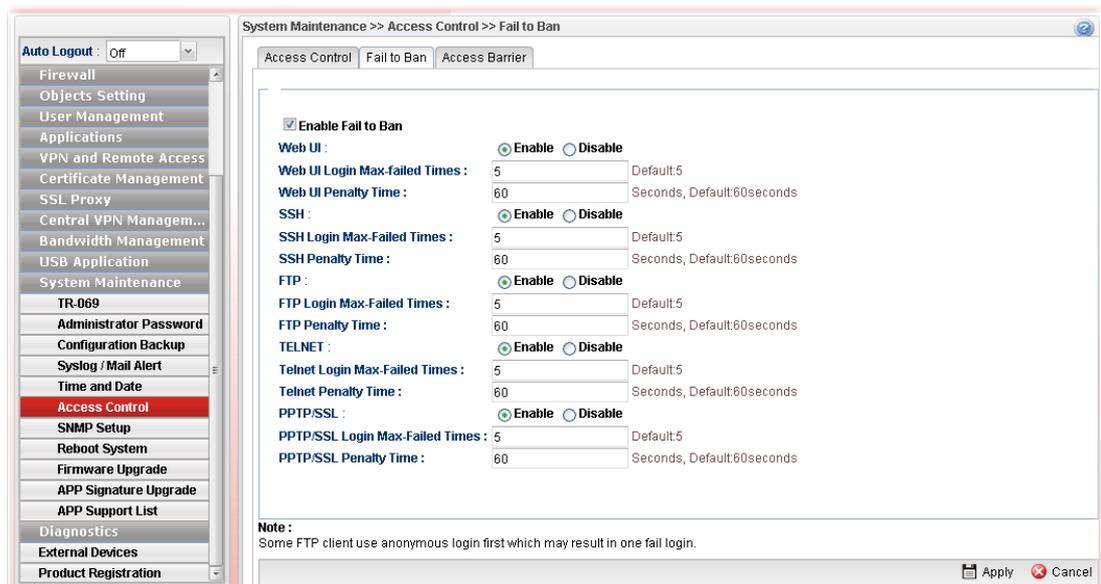
	HTTPS server and management the web page of the router.
FTP Allow	Click Enable to allow system administrator to login from the FTP server and management the web page of the router.
Server Certificate	Use the default setting.
Access List	Click Enable to allow system administrator to login from the user 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.
Allow Ping form LAN	Click Enable to allow system administrator to ping the router from LAN interface.
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.
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**.

4.15.6.2 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.



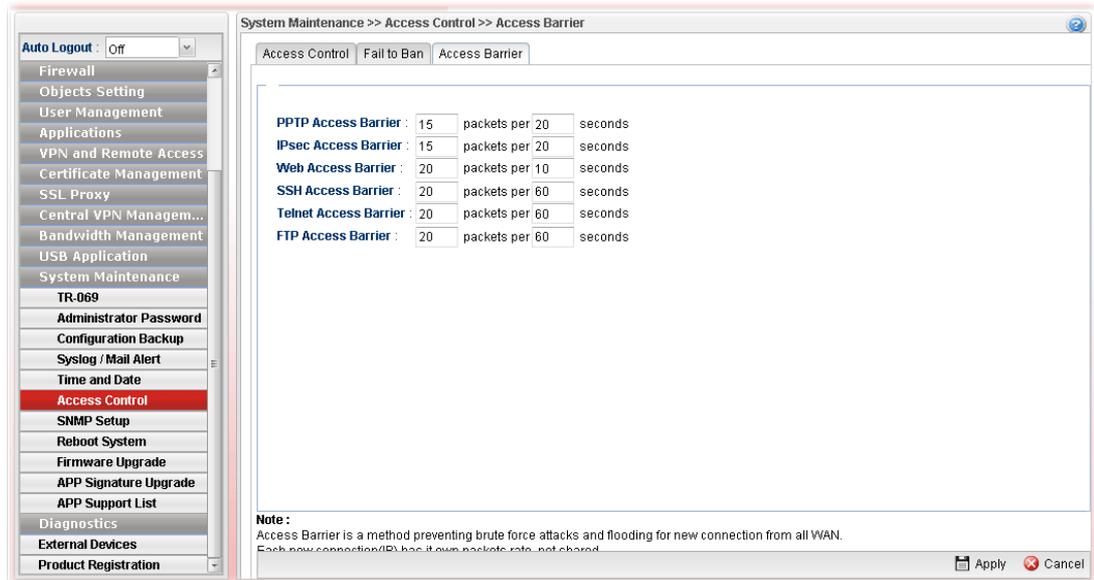
Available parameters are listed as follows:

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	<p>Enable – Enable the function of Fail to Ban via different protocols (Web UI/SSH/FTP/TELNET/PPTP/SSL).</p> <ul style="list-style-type: none"> ● 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.
Apply	Click this button to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.15.6.3 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.



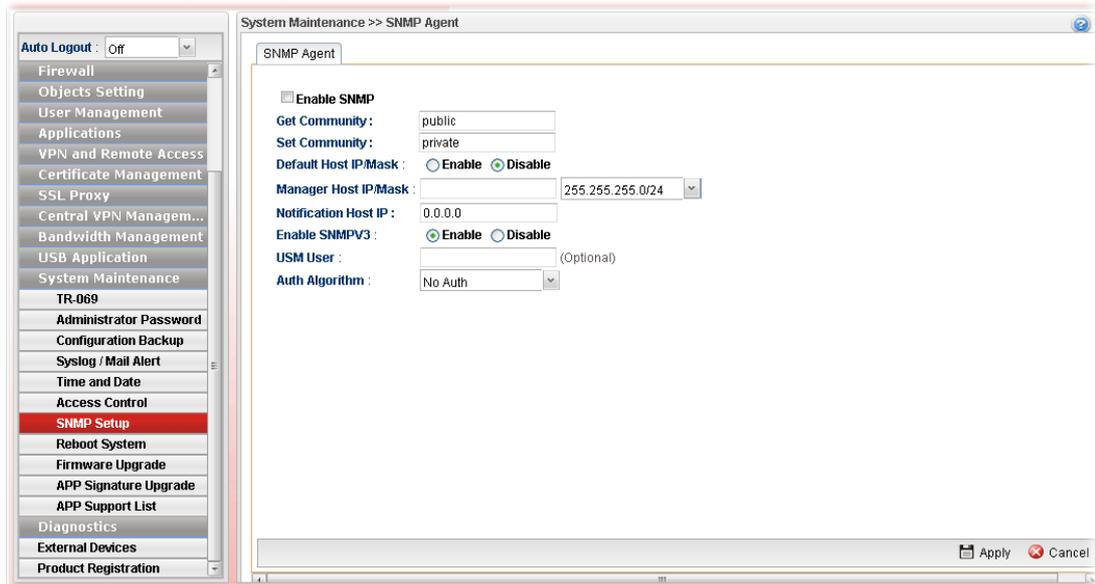
Available parameters are listed as follows:

Item	Description
PPTP/IPsec/Web/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.

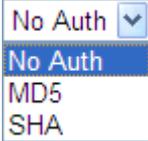
4.15.7 SNMP Setup

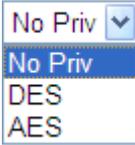
This page allows you to manage the settings for SNMP setup.

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 Snpv3	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	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	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**.

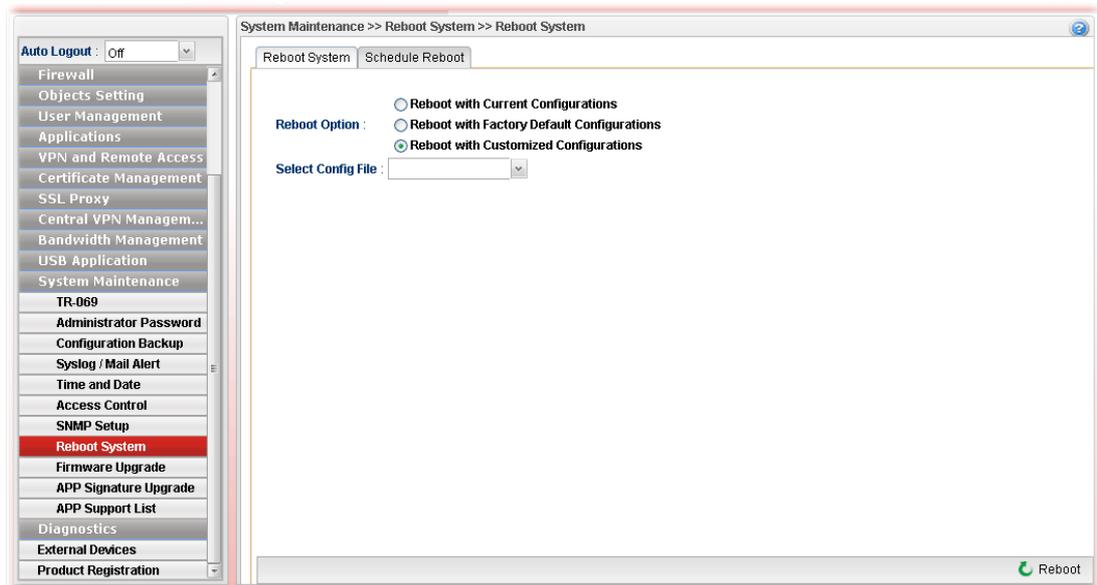
4.15.8 Reboot System

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.

4.15.8.1 Reboot System

Open **System Maintenance**>> **Reboot System**.



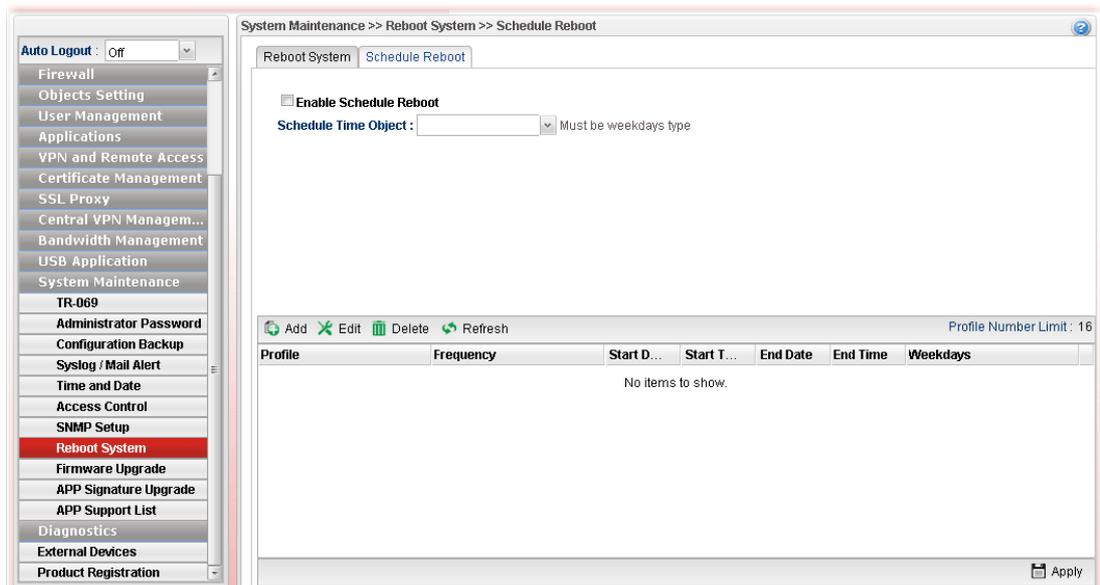
Available parameters are listed as follows:

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 .

<p>Reboot with Customized Configurations</p>	<p>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.</p> <p> <input type="radio"/> Reboot with Current Configurations <input type="radio"/> Reboot with Factory Default Configurations <input checked="" type="radio"/> Reboot with Customized Configurations </p> <p> Reboot Option : </p> <p> Select Config File : lan_wan_profile, wan_... </p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> lan_wan_profile <input type="checkbox"/> load_balance <input checked="" type="checkbox"/> wan_vlan <input checked="" type="checkbox"/> lan_vlan <input type="checkbox"/> switch_mirror <input type="checkbox"/> static_route <input type="checkbox"/> ipbind_mac <input type="checkbox"/> port_redirect <p>After choosing the configuration files, click Reboot.</p>
<p>Reboot</p>	<p>Click this button to execute the rebooting job.</p>

4.15.8.2 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.



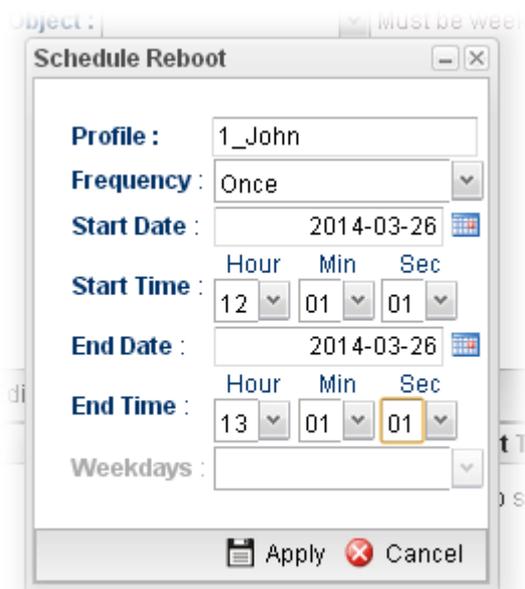
Available parameters are listed as follows:

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.

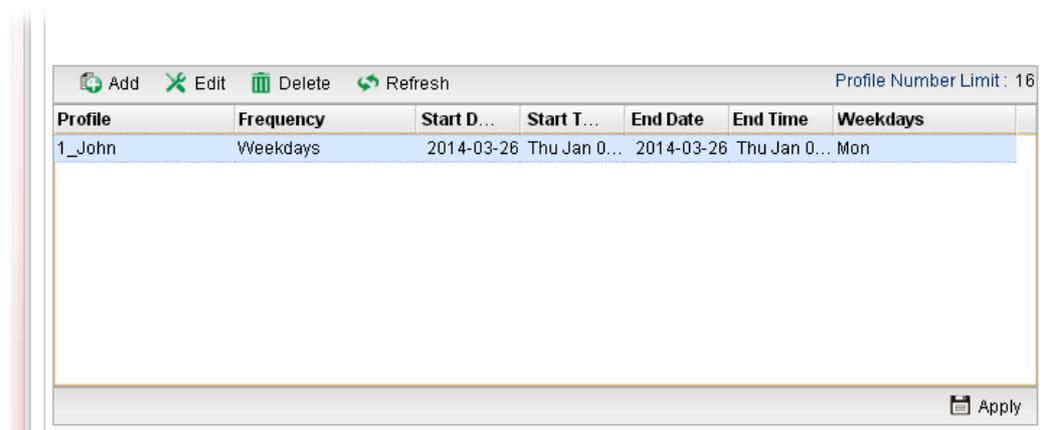


Available parameters are listed as follows:

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.



4.15.9 Firmware Upgrade

The following web page will guide you to upgrade firmware by using such page.

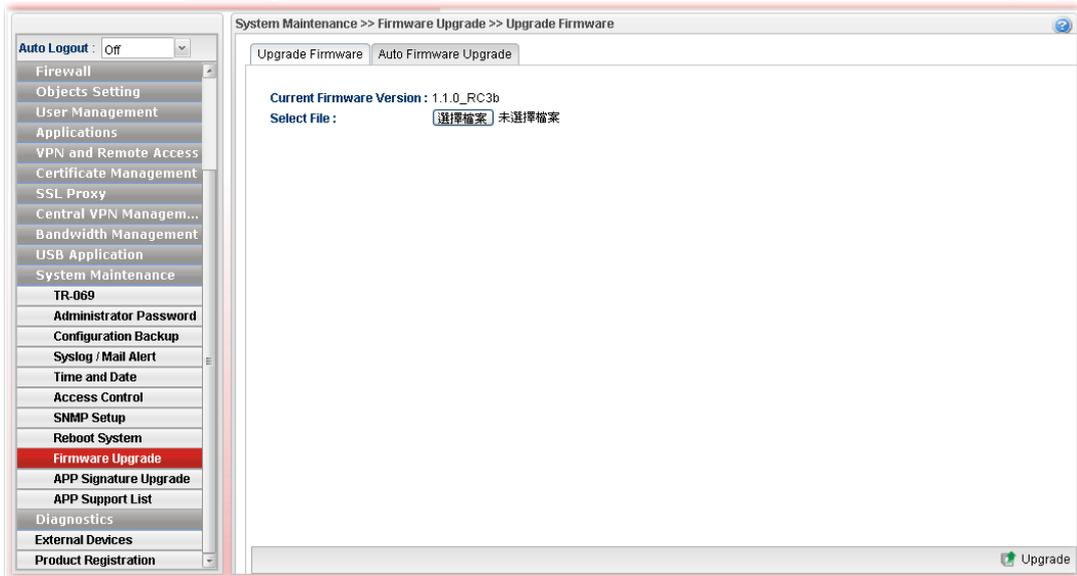
Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and the FTP site is [ftp.DrayTek.com](ftp://DrayTek.com).

Click **System Maintenance**>> **Firmware Upgrade**.

4.15.9.1 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.

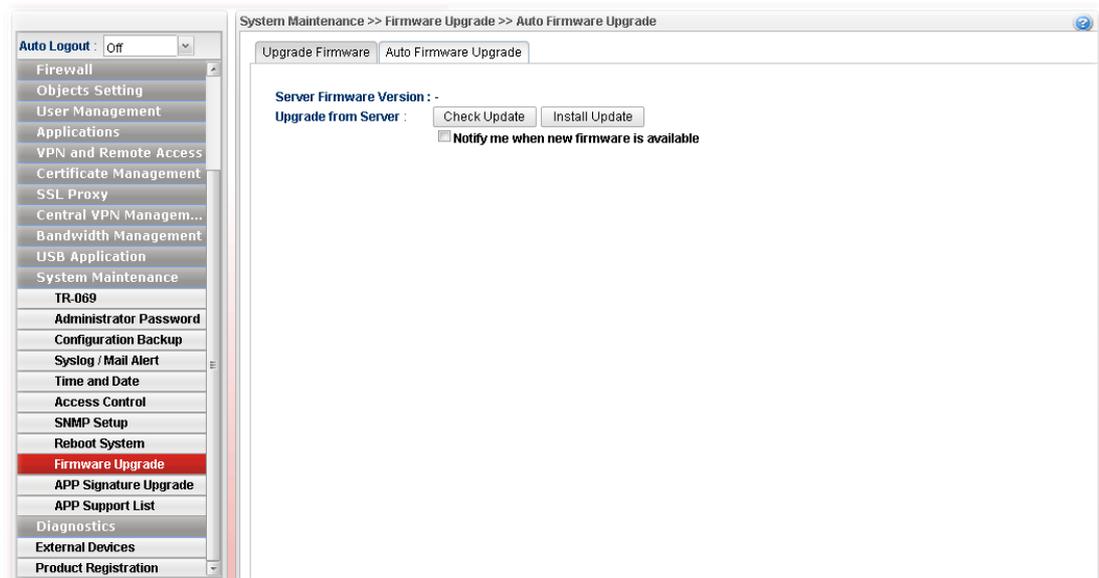


Available parameters are listed as follows:

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.

4.15.9.1 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
Server Firmware	Display the firmware version shown on website

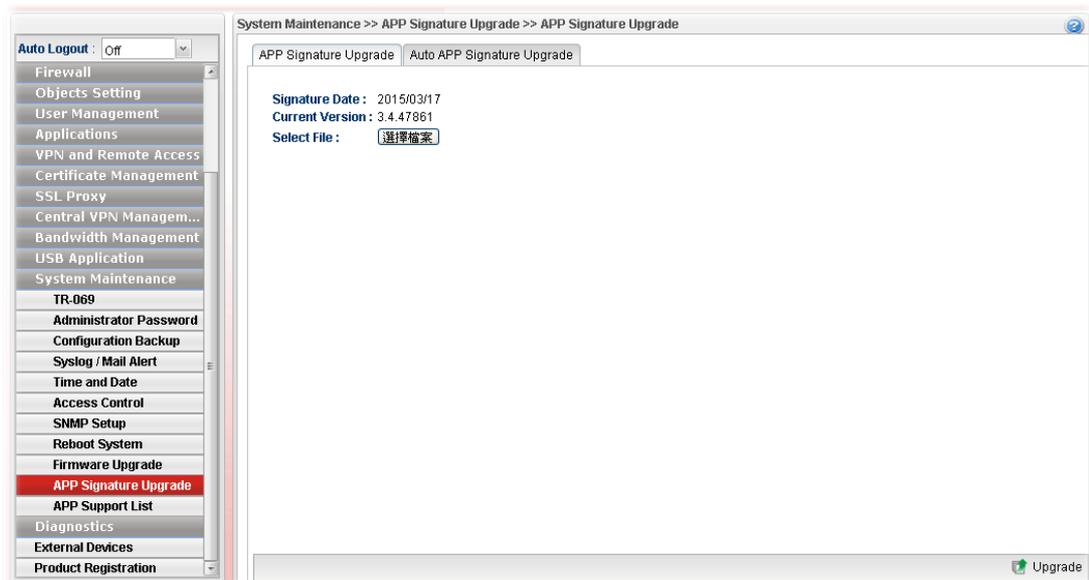
Version	(http://www.draytek.com.tw/ftp).
Upgrade from Server	<p>Check Update –Vigor router will inquire to website (http://www.draytek.com.tw/ftp) if there is any newest firmware available for use. If yes, Vigor router will download the newest firmware from the website to the host (Vigor router) automatically.</p> <p>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.</p> <p>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.</p>

4.15.10 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.

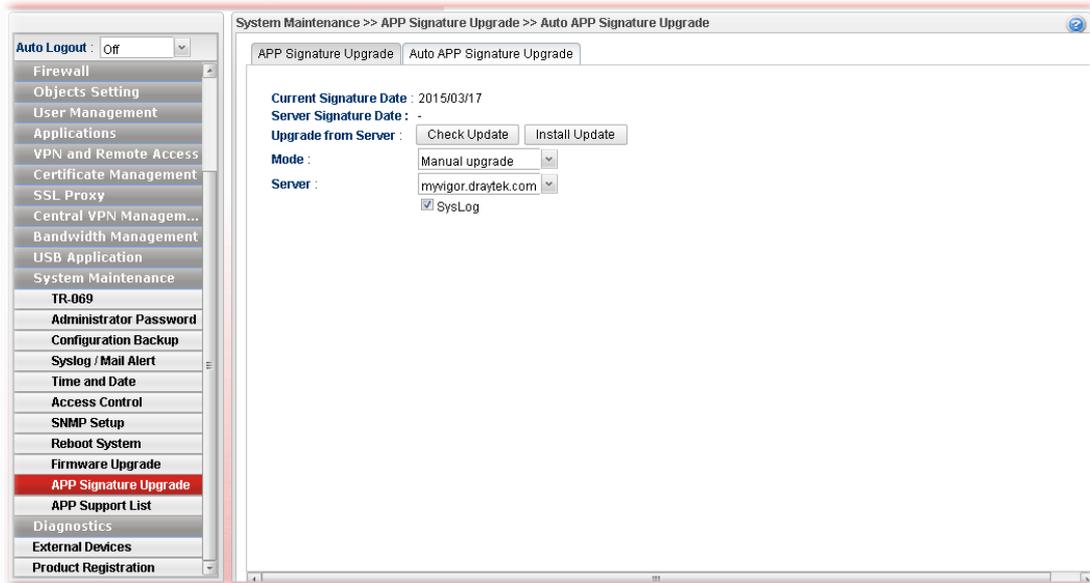
4.15.10.1 APP Signature Upgrade

Before upgrading APP signature to Vigor3900, open this page and specify a signature file by clicking **Select**. Later, click **Upgrade** to execute signature upgrade.



4.15.10.2 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	<p>Get the newest signature from MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com).</p> <p>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.</p> <p>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.</p>
Mode	<p>Choose the condition to execute APP signature upgrade or send a notification.</p> <p>Manual upgrade</p> <p>Manual upgrade Notify me when new signature is available Auto upgrade when new signature is availa...</p> <p>Manual upgrade – If it is selected, check and installation for signature will be executed only when Check Update/Install Update is pressed.</p> <p>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</p>

	<p>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.</p> <p>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.</p>
Server	<p>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.</p>
Syslog	<p>Check the box to record related information on Syslog.</p>

4.15.11 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.

System Maintenance >> APP Support List >> IM

[APP Signature Upgrade](#)

IM	P2P	Protocol	Others
Type	Name	Version	Note
IM	AIM	5.9	
IM	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.
IM	AIMWV	2008	
IM	Ares	2.0.9	
IM	BaiduHi	37378	
IM	Fetion	2010	
IM	GaduGadu Prot...		
IM	Google Chat		
IM	iMessage		
IM	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or fo...
IM	ICU2	8.0.6	
IM	iSpQ	8.0.60	
IM	Jabber Protocol/...		
IM	Lava-Lava	2007	
IM	MobileMSN		
IM	MSN	2011	
IM	Paltalk	9	
IM	POCO	2007	To block P2P, please check the P2P Object item.
IM	Gnext	3.0.1	
IM	QQ/TM	2012/2009 b...	
IM	UC	2009	
IM	YFire	25432	

4.16 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** and **Traffic Graph** for the user to review such information.

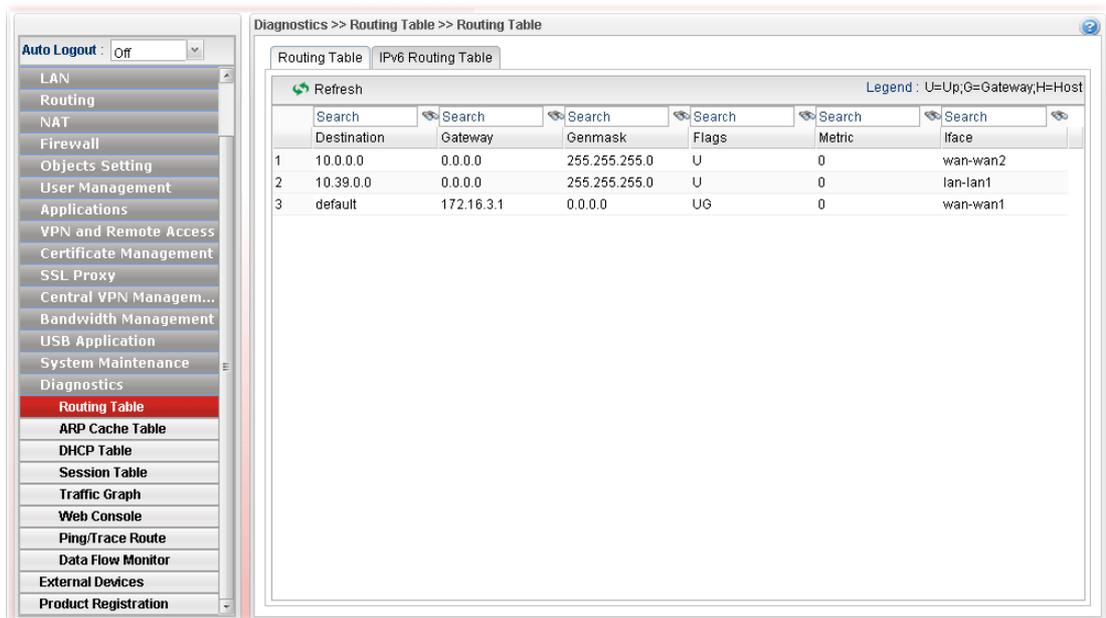


4.16.1 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

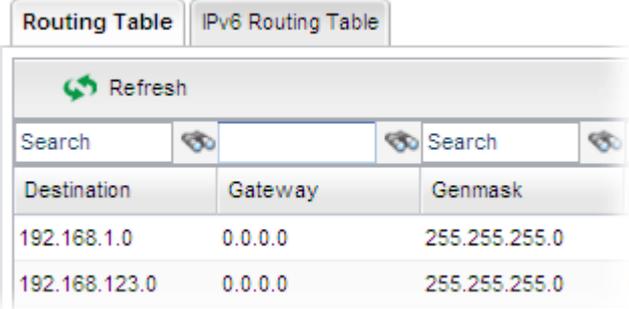
4.16.1.2 Routing Table

Display the information for each route.



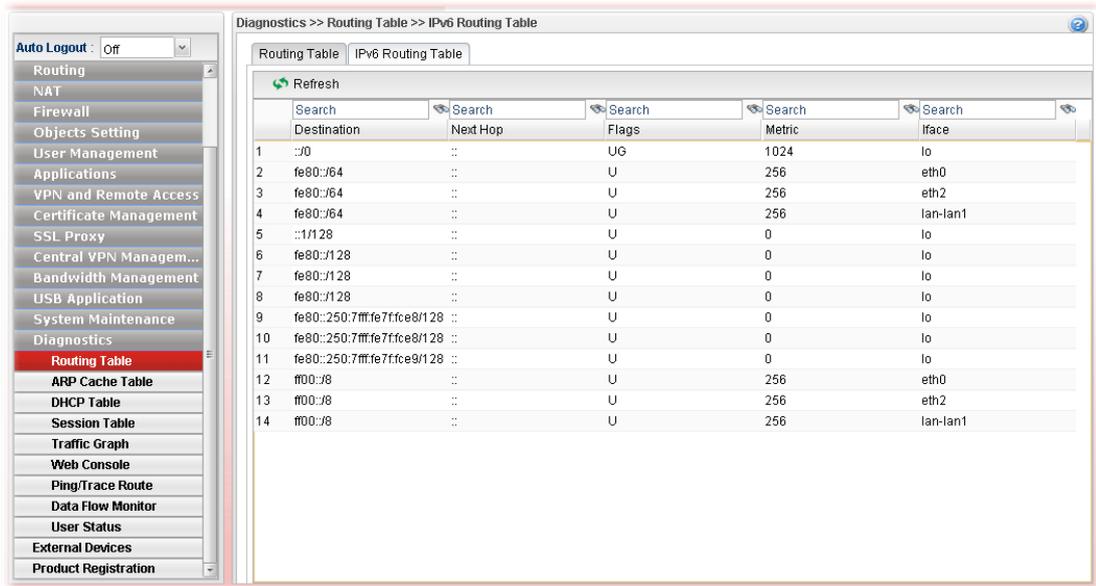
Each item will be explained as follows:

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.

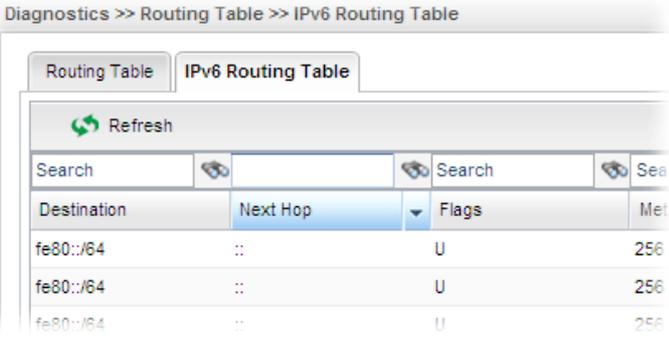
	
Destination	Display the destination IP address for various routings.
Gateway	Display the default gateway.
Genmask	Display the subnet mask for various routings.
Flags	<p>Display the flag of the routing entry. Possible flags include:</p> <ul style="list-style-type: none"> U (route is up) H (target is a 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 <i>addrconf</i>) 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).

4.16.1.2 IPv6 Routing Table

Display the information for each route with IPv6 protocol.



Each item will be explained as follows:

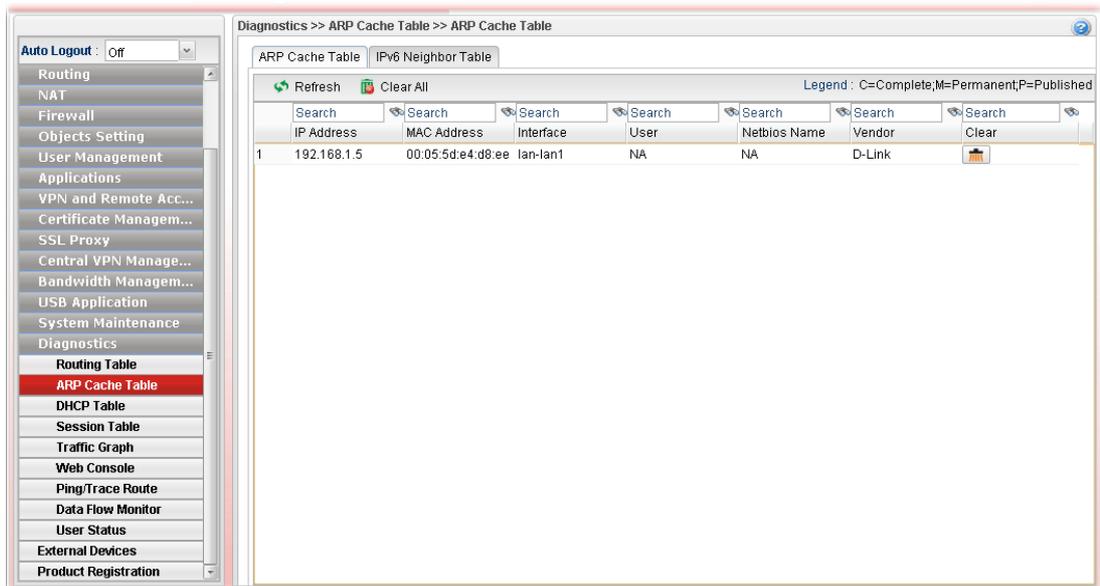
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
Destination	Display the destination IP address for various routings.
Next Hop	Display 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 <i>addrconf</i>) 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).

4.16.2 ARP Cache Table

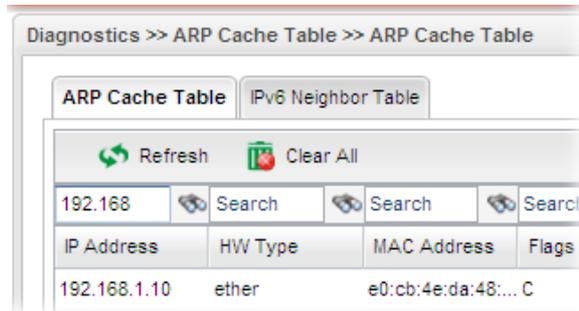
Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

4.16.2.1 ARP Cache Table



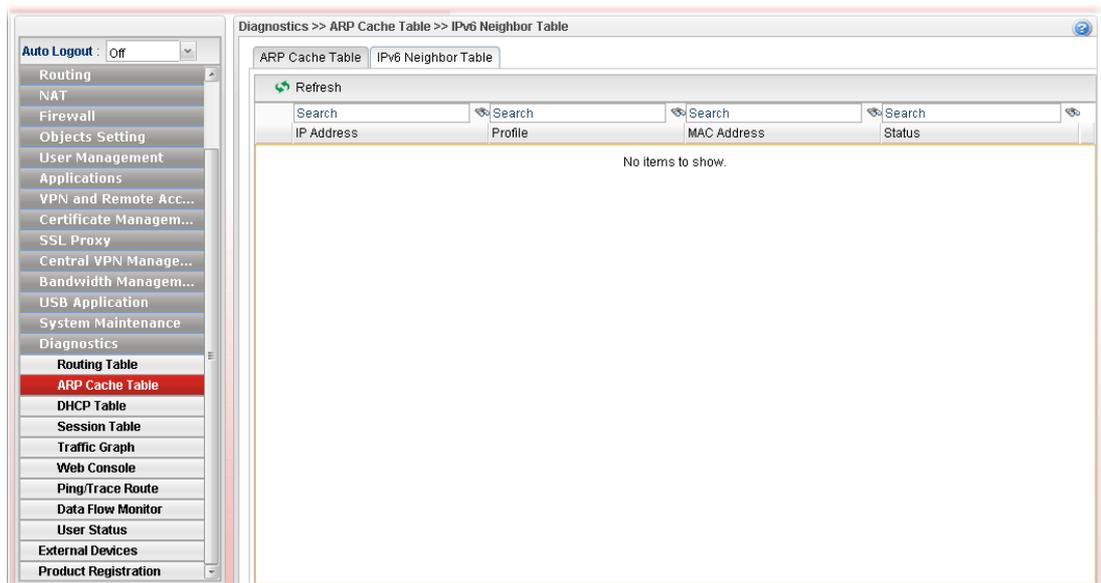
Each item will be explained as follows:

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.



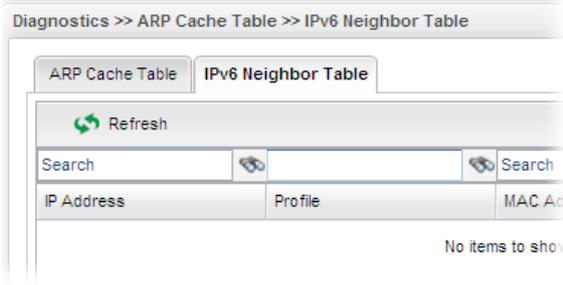
Item	Description
HW type	Display the hardware type of the address from RFC 826.
MAC Address	Display the MAC address for different ARP cache.
Flags	C means complete entry. M means permanent entries. P means published entries.
Profile	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).
User	Display the identity of the user.
Clear	Delete the selected profile.

4.16.2.2 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.



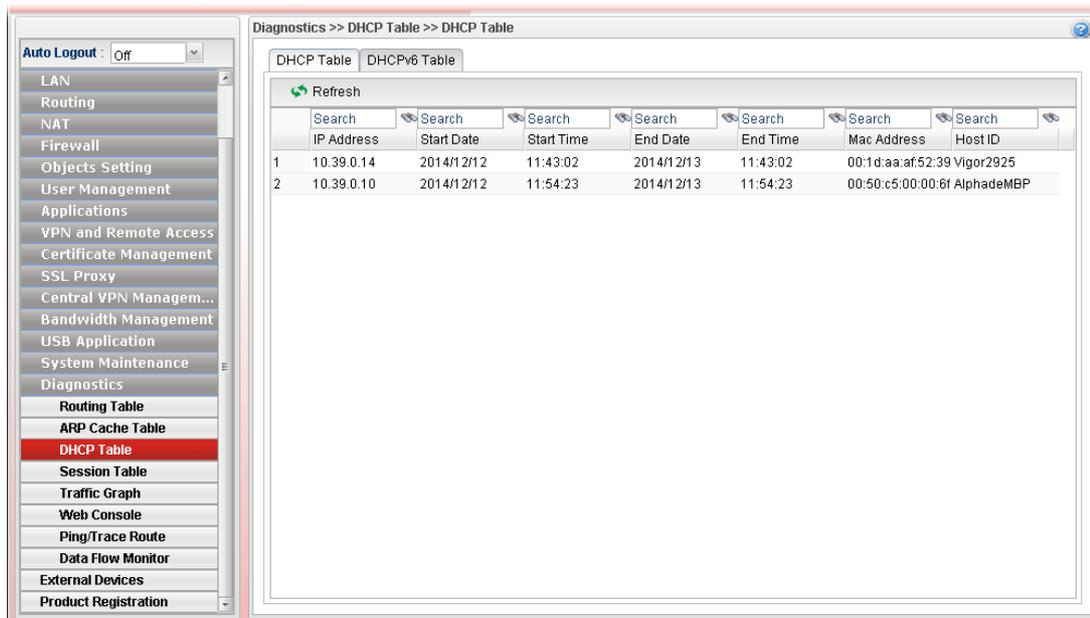
Item	Description
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.
Status	<p>Display the status for such neighbor.</p> <p>INCOMPLETE - Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.</p> <p>REACHABLE - The neighbor is reachable recently (within tens of seconds ago).</p> <p>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.</p> <p>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.</p> <p>PROBE - The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.</p>

4.16.3 DHCP Table

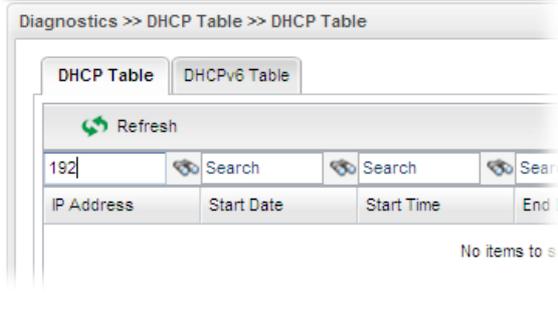
The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

4.16.3.1 DHCP Table

Click **Diagnostics** and click **DHCP Table** to open the web page.

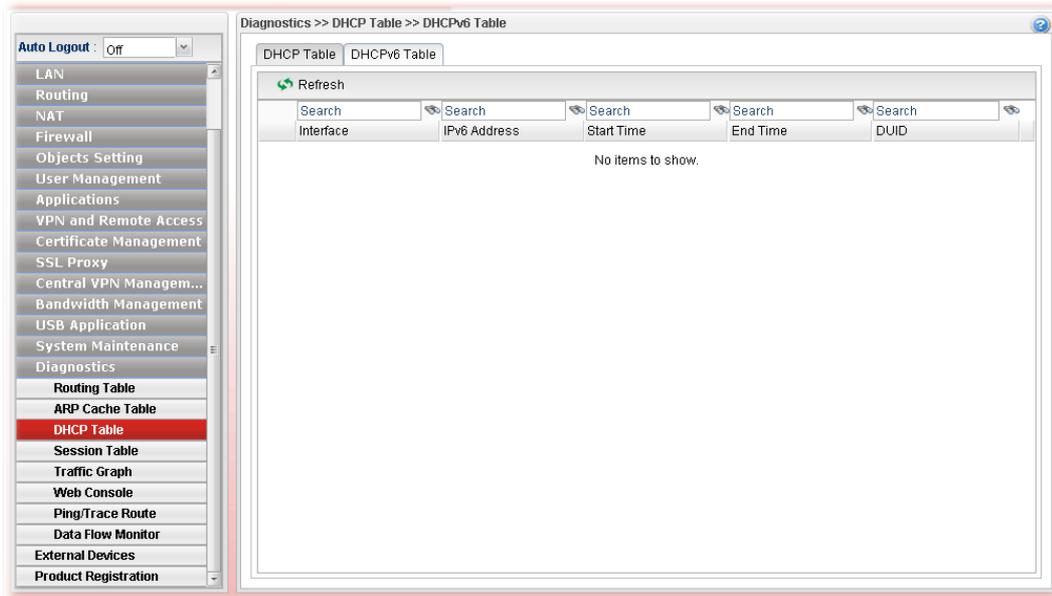


Each item will be explained as follows:

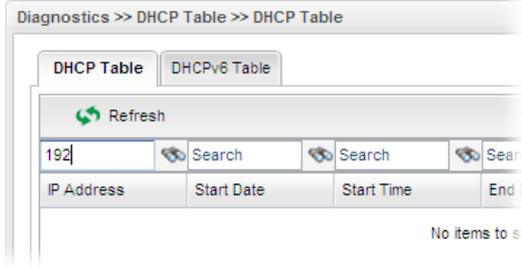
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword. 
IP Address	Display the IP address of the static DHCP server.
Start Date	Display the 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.
Mac Address	Display the MAC address of the static DHCP server.

4.16.3.2 DHCPv6 Table

Click **DHCPv6 Table** to open the web page.

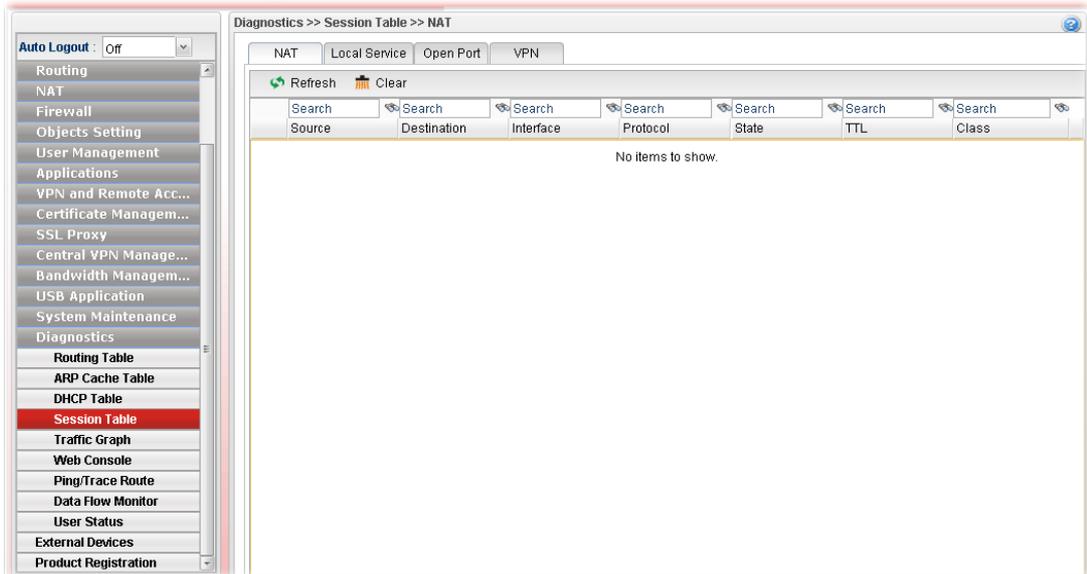


Each item will be explained as follows:

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 Table detailed information for DUID.

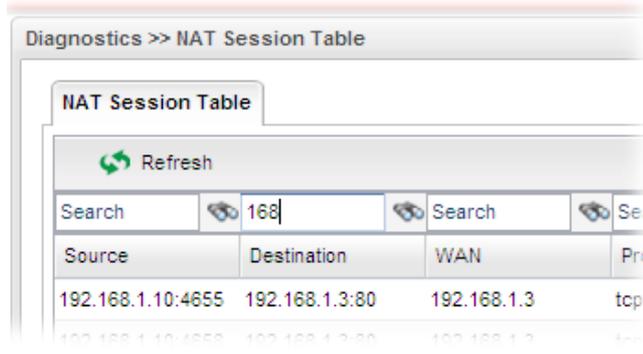
4.16.4 Session Table

This table can display about 30000 sessions with 20 pages.



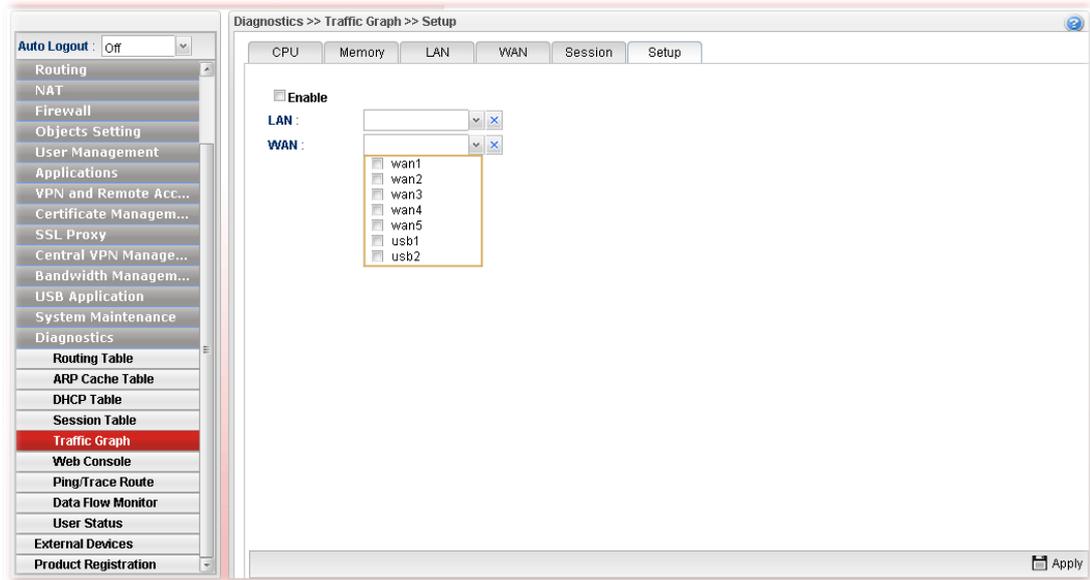
Each item will be explained as follows:

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.
WAN	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.



4.16.5 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.

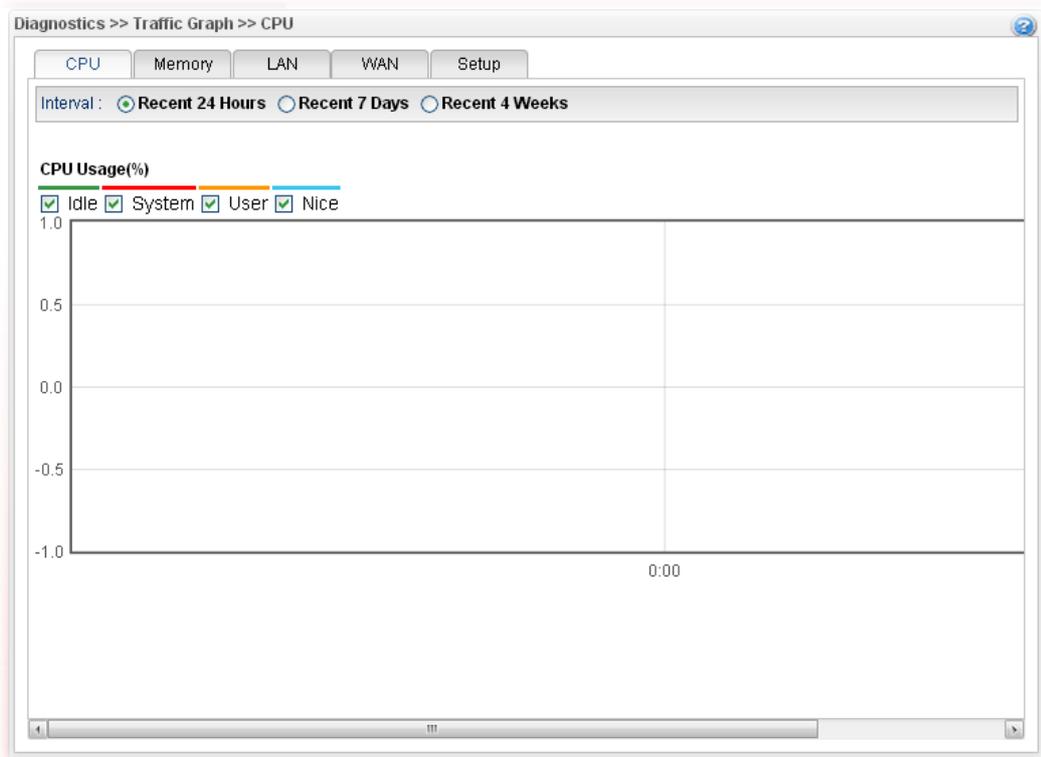


Each item will be explained as follows:

Item	Description
Setup	<p>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.</p> <p>Enable – Check this box to enable such profile.</p> <p>LAN – Use the drop down menu to choose a LAN profile.</p> <p>WAN – Use the drop down menu to choose a WAN profile.</p> <p>Apply - Click it to save the configuration configured under the Setup tab.</p>
CPU	<p>Click the CPU tab.</p> <p>There are three selections provided for you to specify.</p> <p>Recent 24 Hours – Display the information of CPU operation about recent 24 hours.</p> <p>Recent 7 Days – Display the information of CPU operation about recent 7 days.</p> <p>Recent 4 Weeks – Display the information of CPU operation about recent 4 weeks.</p>
Memory	<p>Click the Memory tab.</p> <p>There are three selections provided for you to specify.</p> <p>Recent 24 Hours – Display the information of memory operation about recent 24 hours.</p> <p>Recent 7 Days – Display the information of memory operation about recent 7 days.</p> <p>Recent 4 Weeks – Display the information of memory operation about recent 4 weeks.</p>

Item	Description
LAN	<p>Click the LAN tab.</p> <p>Network Interface – Display the information of LAN operation.</p> <p>There are three selections provided for you to specify.</p> <p>Recent 24 Hours – Display the information of LAN operation about recent 24 hours.</p> <p>Recent 7 Days – Display the information of LAN operation about recent 7 days.</p> <p>Recent 4 Weeks – Display the information of LAN operation about recent 4 weeks.</p>
WAN	<p>Click the WAN tab.</p> <p>Network Interface – Display the information of WAN operation.</p> <p>There are three selections provided for you to specify.</p> <p>Recent 24 Hours – Display the information of WAN operation about recent 24 hours.</p> <p>Recent 7 Days – Display the information of WAN operation about recent 7 days.</p> <p>Recent 4 Weeks – Display the information of WAN operation about recent 4 weeks.</p>

Below show a graphic for CPU:



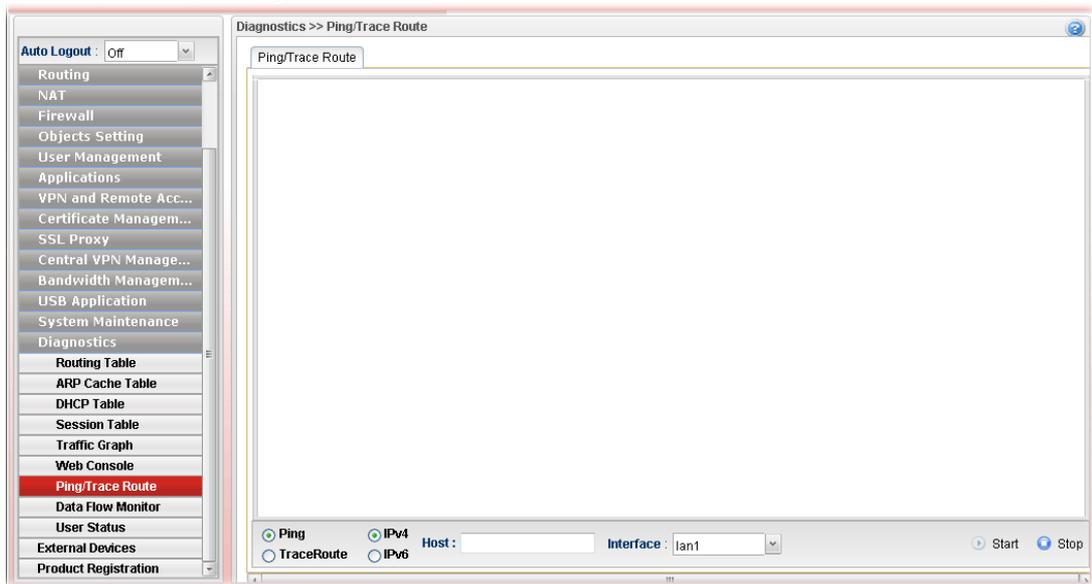
4.16.6 Web Console

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.



4.16.7 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.

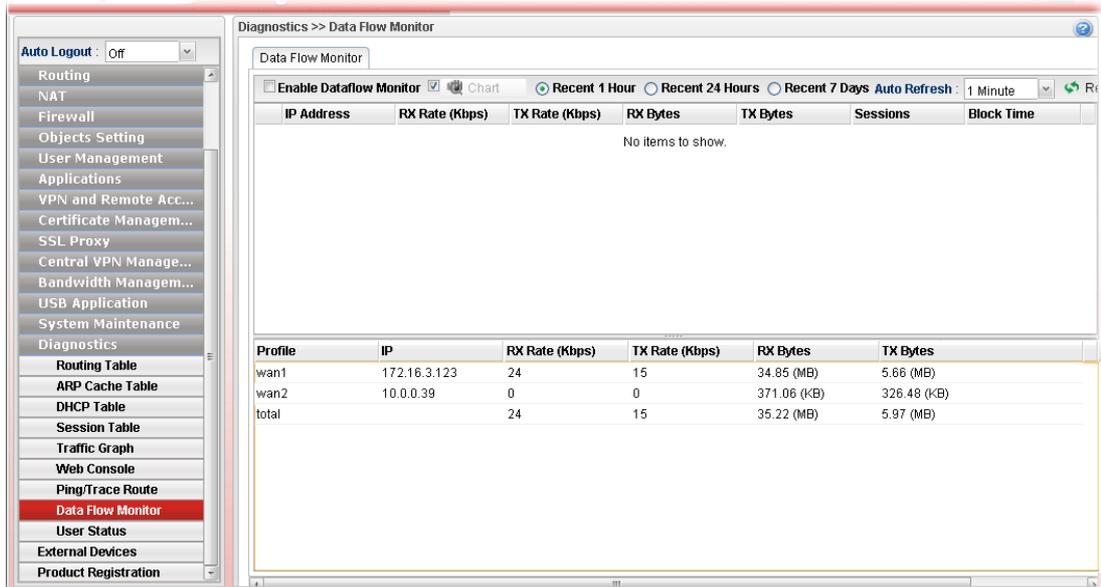


Each item will be explained as follows:

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.

4.16.8 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.



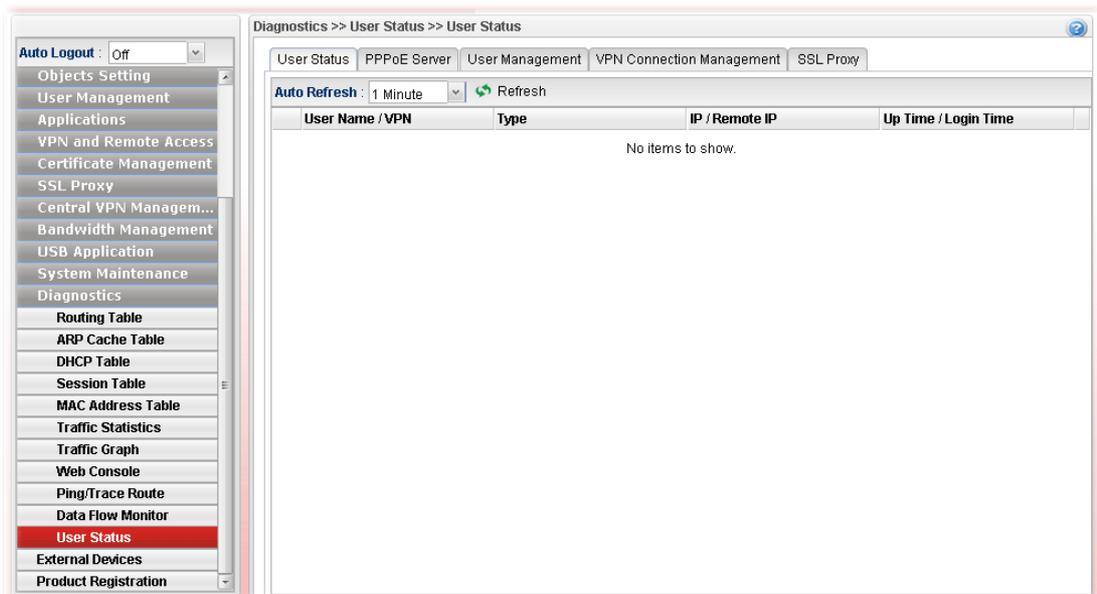
Each item will be explained as follows:

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. <div data-bbox="686 1288 1348 1556" data-label="Figure"> </div>
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.

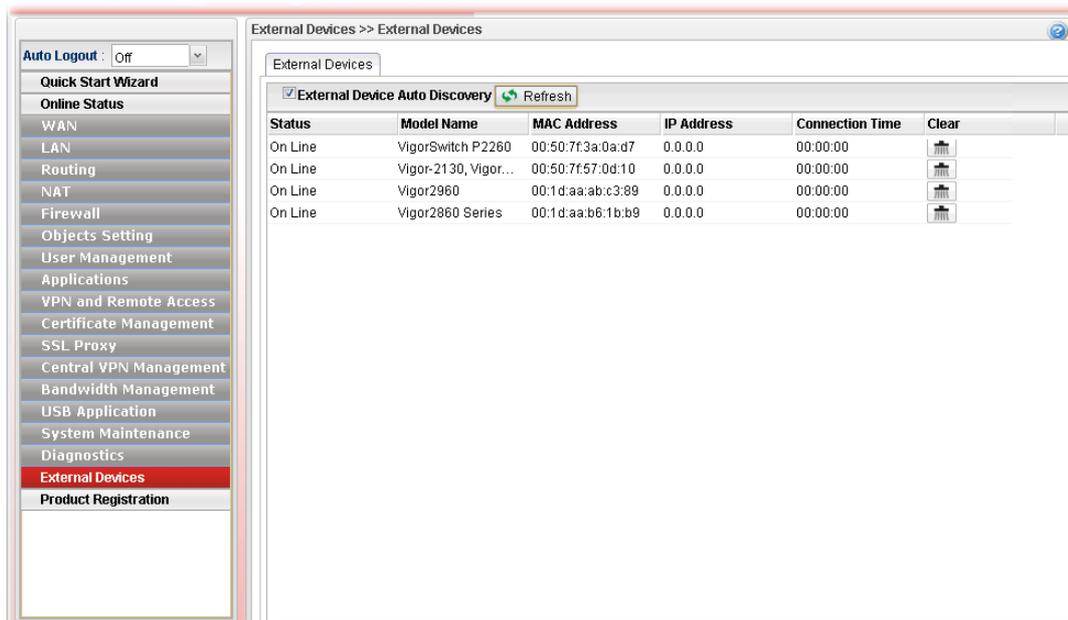
4.16.9 User Status

This page displays related information of user status, PPPoE Server, User Management, VPN Connection Management and SSL Proxy for reference.



4.17 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.
Status	Display
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.

4.18 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.

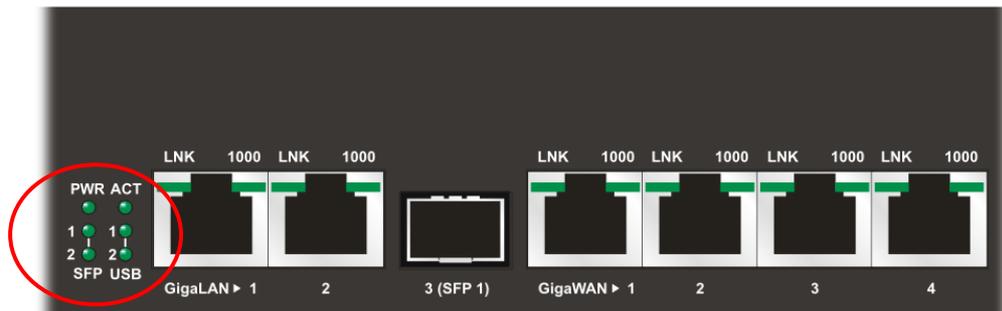
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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 still failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

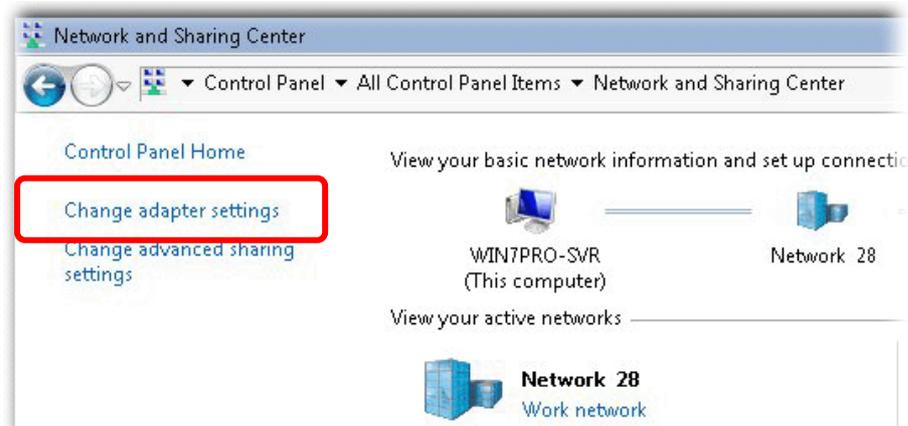


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

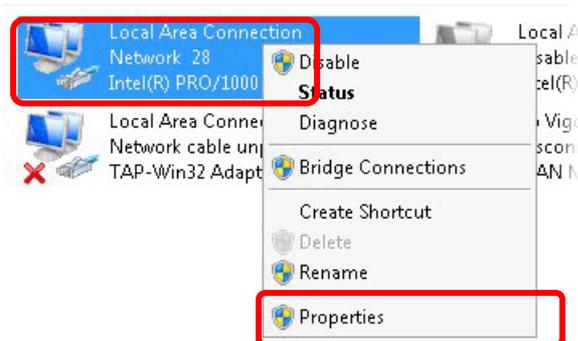
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



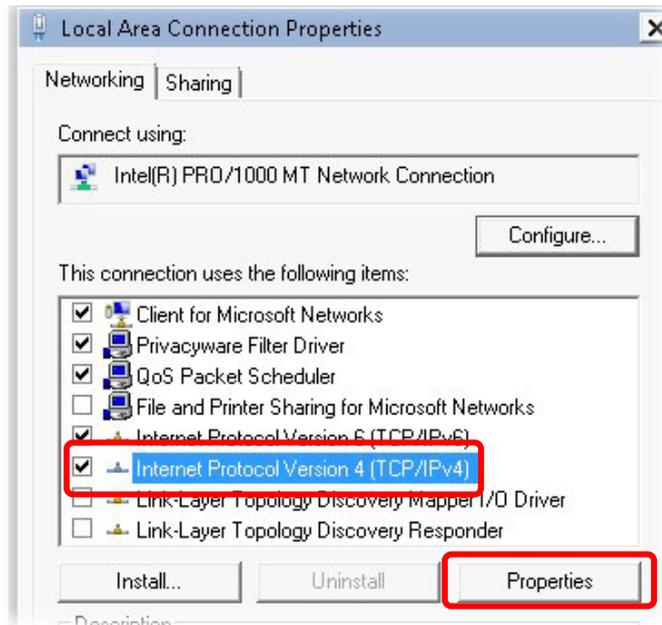
2. In the following window, click **Change adapter settings**.



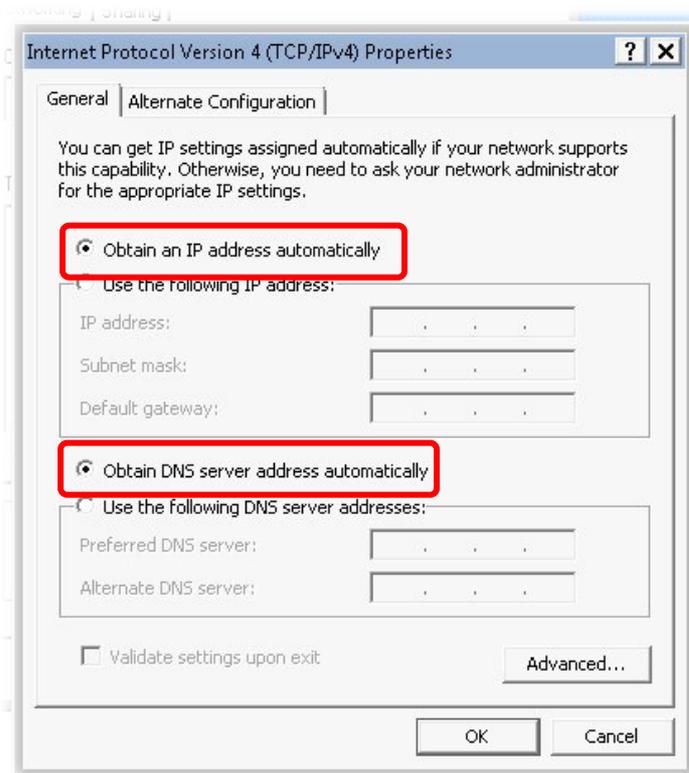
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

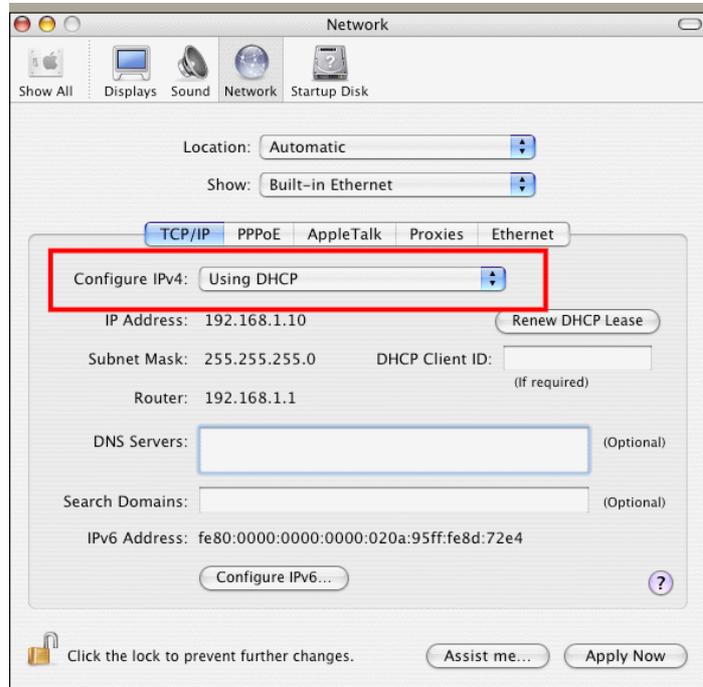


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



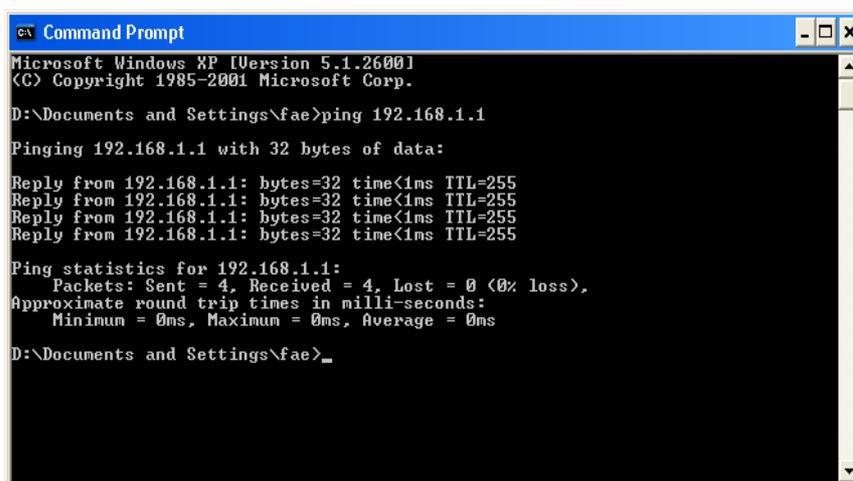
5.3 Pinging the Router from Your Computer

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.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

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.

```

Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

```

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.

The screenshot displays the DrayTek Vigor3900 web management interface. At the top, there is a 'Refresh' button and a 'DrayTek Vigor3900 Multi-WAN Security Appliance' header. Below the header is a hardware status bar showing various ports (SFP, USB, Gigabit LAN, Gigabit WAN, Console, USB) with their respective link and power status indicators.

The main content area is divided into two columns:

- Device Information:**
 - Model: Vigor3900
 - Hardware: 1.0
 - Firmware: 1.0.9_RC5
 - Build Date: 2014-12-01 03:44:55
 - Revision: 4542
- System Information:**
 - CPU Usage: 1%
 - Memory Usage: Memory Usage:34% Memory Cached:9%
 - Coprocessor: CPU Usage:0% Memory Usage:0%
 - System Up Time: 0 days 1:34:0
 - Current System Time: Fri Dec 12 13:15:34 2014

Below the system information, there are tabs for 'IPv4' and 'IPv6'. The 'IPv4' tab is active, showing a table of network profiles:

Profile	Conn...	Desc...	Up Time	Mac	Proto...	IP	Gate...	DNS	RX R...	TX Ra...	RX By...	TX By...	Operation
lan1	up		0 days...	00:50:...	Static(...	10.39...			0	0	165.8...	492.7...	
wan1	up	DrayTek	0 days...	00:50:...	Static(...	172.1...	172.1...	8.8.8.8	17	0	10.81...	3.01 (...	
wan2	up	V2960	0 days...	00:50:...	Static(...	10.0.0...	10.0.0...	8.8.8.8	0	0	114.1...	101.2...	

At the bottom of the interface, there is a 'VPN Connection Status' section.

If there is something wrong with the configuration, please go to **WAN** page and choose **General Setup** again to modify the WAN connection.

WAN >> General Setup >> General Setup

General Setup | USB WAN | Bridge VLAN

Add Edit Delete Refresh Mode: Advance Profile Number Limit: 50

Profile (m...	Enable	Description	Port	IPv4 Prot...	IPv6 Prot...	VLAN Tag	VLAN ID	Priority(80...
1 wan1	true	DrayTek	WAN1	Static	Link Local	Disable	10	0
2 wan2	true	V2960	WAN2	Static	Link Local	Disable	11	0
3 wan3	false		WAN3	None	Link Local	Disable	12	0
4 wan4	false		WAN4	None	Link Local	Disable	13	0
5 wan5	false		WAN5	None	Link Local	Disable	14	0

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.

System Maintenance >> Reboot System >> Reboot System

Reboot System | Schedule Reboot

Reboot Option :

- Reboot with Current Configurations
- Reboot with Factory Default Configurations
- Reboot with Customized Configurations

Reboot

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.