DrayTek

Vigor300B

Multi-WAN Load Balancer

Your reliable networking solutions partner

User's Guide

V2.1

Vigor300B
Multi-WAN Load Balancer
User's Guide

Version: 2.1

Firmware Version: V1.2.0

(For future update, please visit DrayTek website)

Date: March 31, 2016

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu County, Taiwan 303
Product: Vigor300B

DrayTek Corp. declares that Vigor300B 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.

GPL Notice

This DrayTek product uses software partially or completely licensed under the terms of the GNU GENERAL PUBLIC LICENSE. The author of the software does not provide any warranty. A Limited Warranty is offered on DrayTek products. This Limited Warranty does not cover any software applications or programs.

To download source codes please visit:

http://gplsource.draytek.com

GNU GENERAL PUBLIC LICENSE:

https://gnu.org/licenses/gpl-2.0

Version 2, June 1991

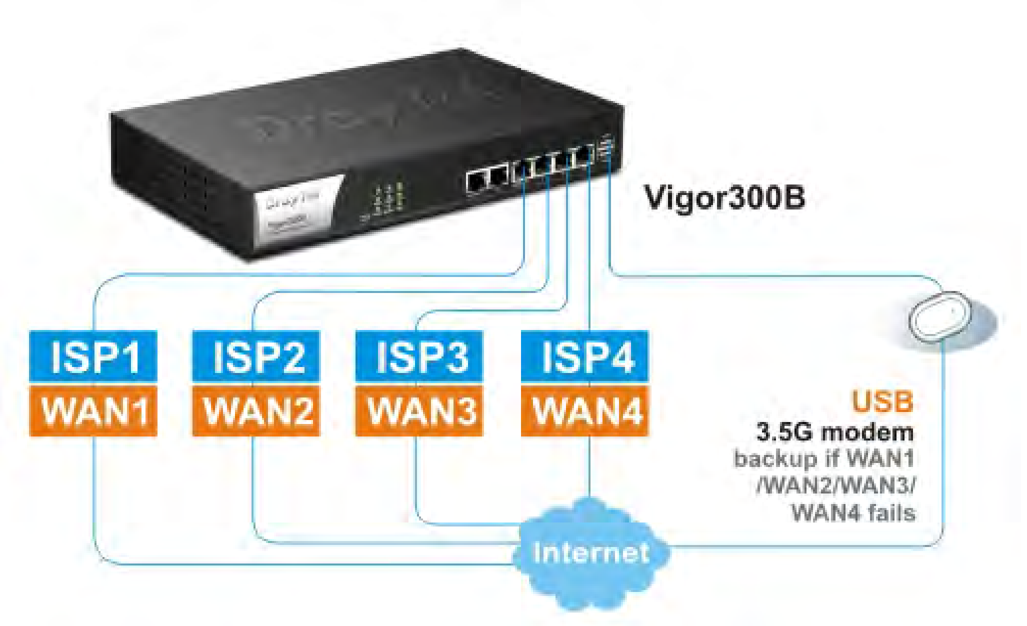
For any question, please feel free to contact DrayTek technical support at support@draytek.com for further information.

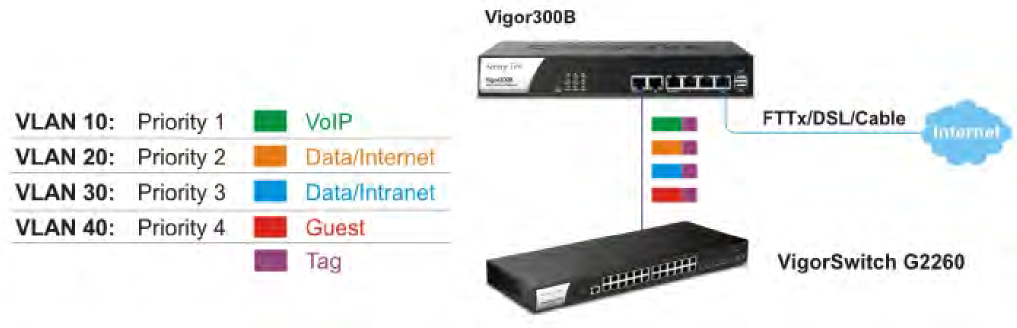
Table of Contents

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.

Vigor300B, a firewall broadband router with multi-WAN interface, can connect to xDSL/cable/VDSL2/Ethernet FTTx. The multi-WAN and LAN switch facilitate unified communication applications in business CO/remote site to handle large data from subscribed fatter pipe. The state-of-art routing feature, and multi-WAN provide integrated benefits for professional users and small offices.

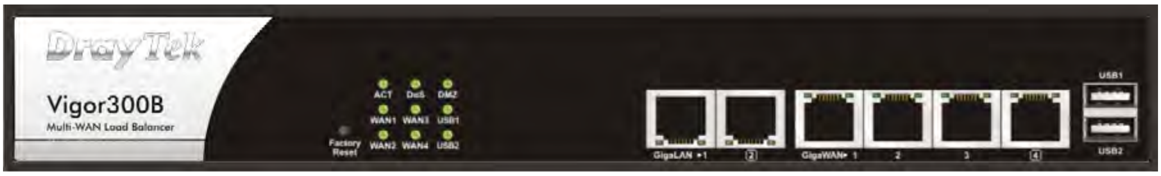



Vigor300B
VLAN 10: Priority 1 🟩 VoIP
VLAN 20: Priority 2 🟧 Data/Internet
VLAN 30: Priority 3 🟦 Data/Intranet
VLAN 40: Priority 4 🟥 Guest
🟪 Tag
FTTx/DSL/Cable
Internet
VigorSwitch G2260

1.1 LED Indicators and Connectors

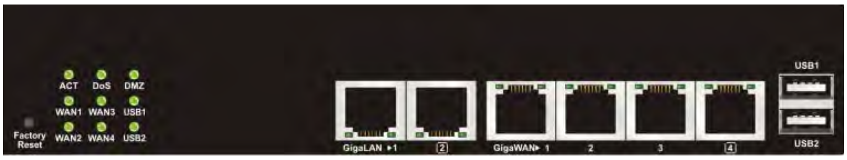
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

Description for LED



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while detecting an attack.
DMZ		On	DMZ Host is specified in certain site.
		Off	DMZ Host is inactive.
WAN1 ~ WAN4		On	The WAN1 or WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
USB1 ~ USB2		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
LED on Connector			
LAN 1/2 (Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
WAN 1/2/3/4 (Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.

Connectors



Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
LAN1/2 (Giga)	Connecters for local networked devices.
WAN1/2/3/4 (Giga)	Connecters for remote networked devices.
USB1/2	Connecter for Mobile HDD, 3G Modem or printer.
	Connecter for a power cord. ON/OFF - Power switch.

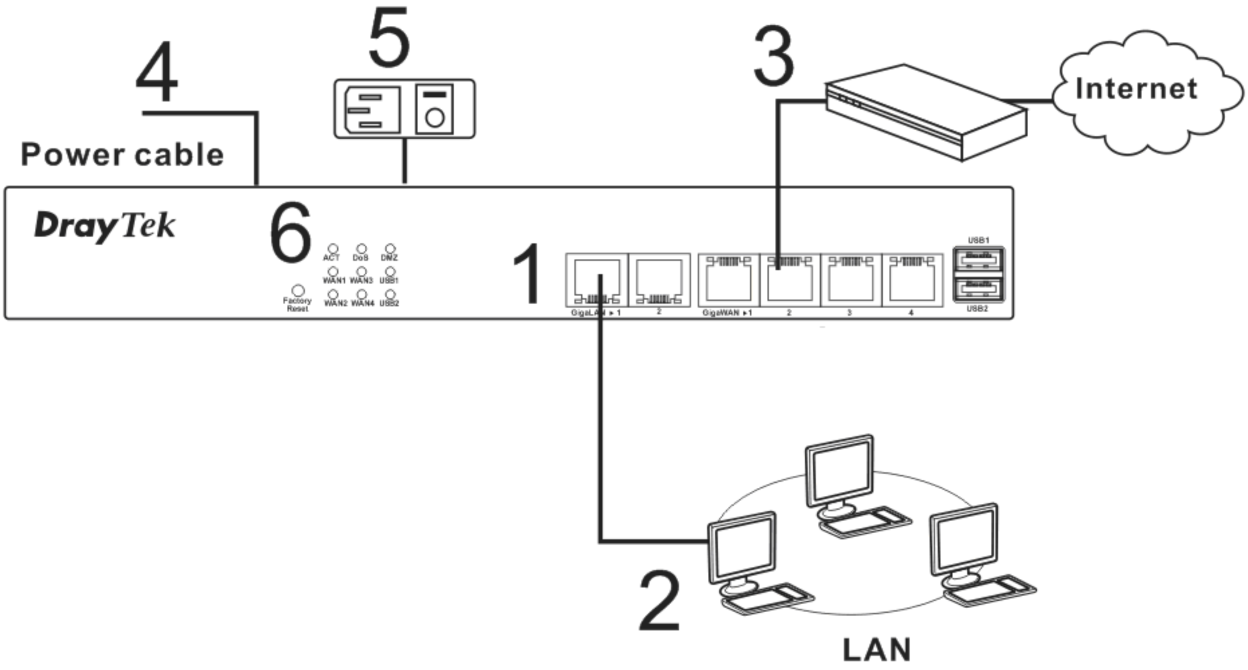
1.2 Hardware Installation

1.2.1 Network Connection

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

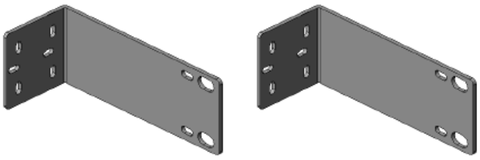
1. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of Vigor300B.
2. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The **LAN** LED for that port on the front panel will light up.
3. Connect a server/modem/router (depends on your requirement) to any WAN port of Vigor300B with Ethernet cable (RJ-45). The **WAN1 (to WAN4)** LED will light up.
4. Connect the power cord to Vigor300B'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

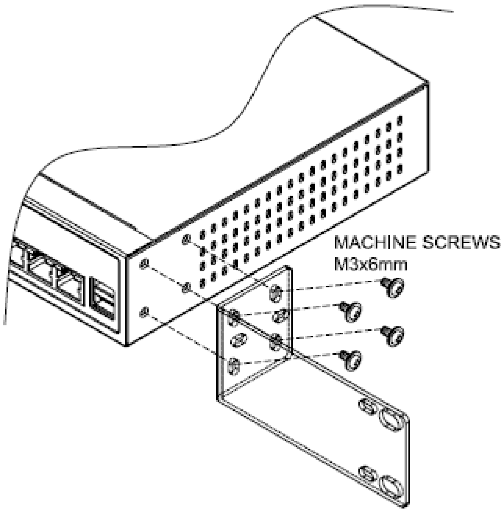
The Vigor300B Series can be mounted on the wall by using standard brackets shown below.



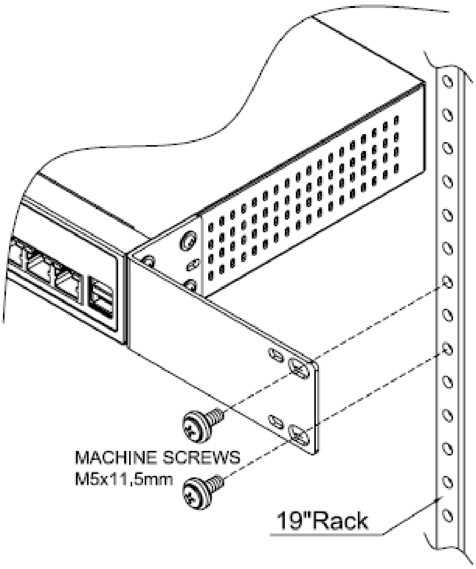
Before mounting the router on the wall or the rack, you have to make sure that power is OFF. Remember to remove the power cable and all network interface cables, and consider the cable limitations and the wall structure when choosing a wall for mounting.

Do the following steps to mount the router on rack:

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

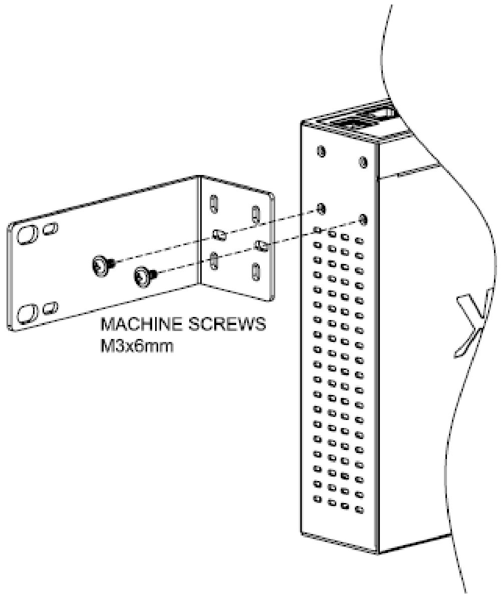


2. Make the holes on the brackets align to the holes on the rack. Use machine screws to fasten the brackets on the rack. Each side requires two screws.



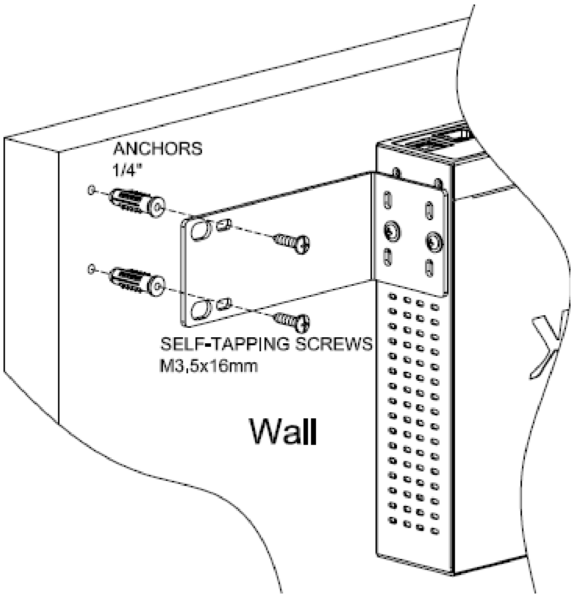
Do the following steps to mount the router on wall:

1. Attach the brackets on each side of the chassis by using the machine screws. Each side requires two screws.



2. Locate the wall studs for attaching the router. Drill wall-mount screw holes and put the studs on the holes first.

3. Make the reserved holes on the brackets align to the studs on the wall. Use machine screws to fasten the brackets on the wall. Each side requires two screws.



Note: Make the front and the rear of the chassis being perpendicular to the floor. The front panel should be installed upward that you can read the LEDs.

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.

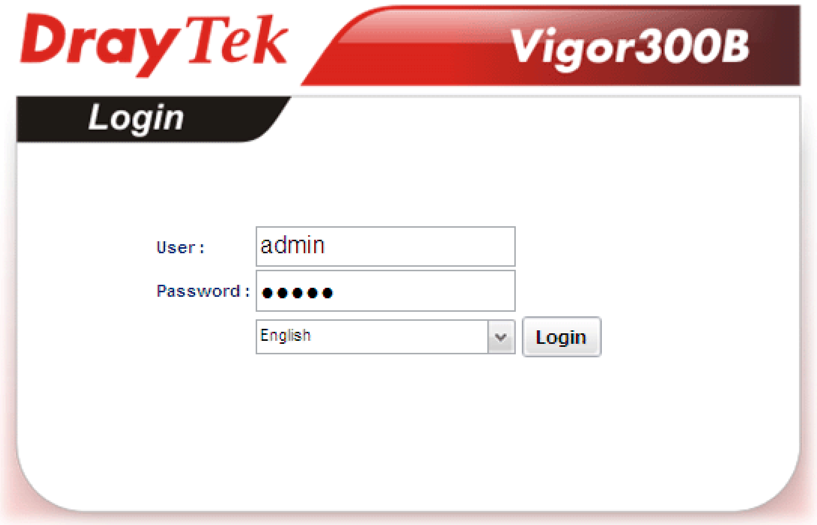
2.1 Changing Password

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.

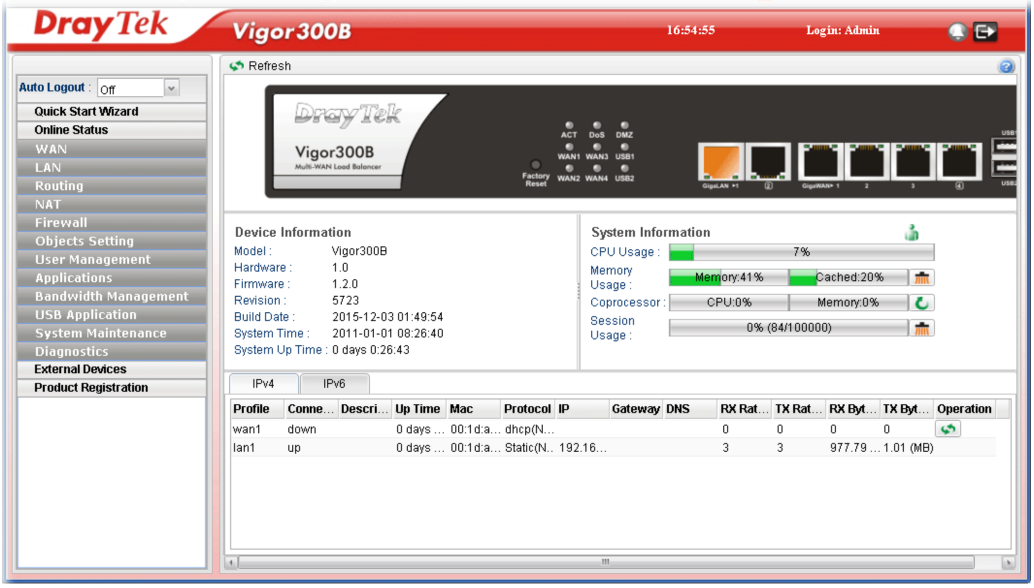
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type default values on the window for the first time accessing. The default value for user name is **admin** and the password is **admin**. Next, click **Login**.



User : admin

Password : ●●●●●

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



Device Information

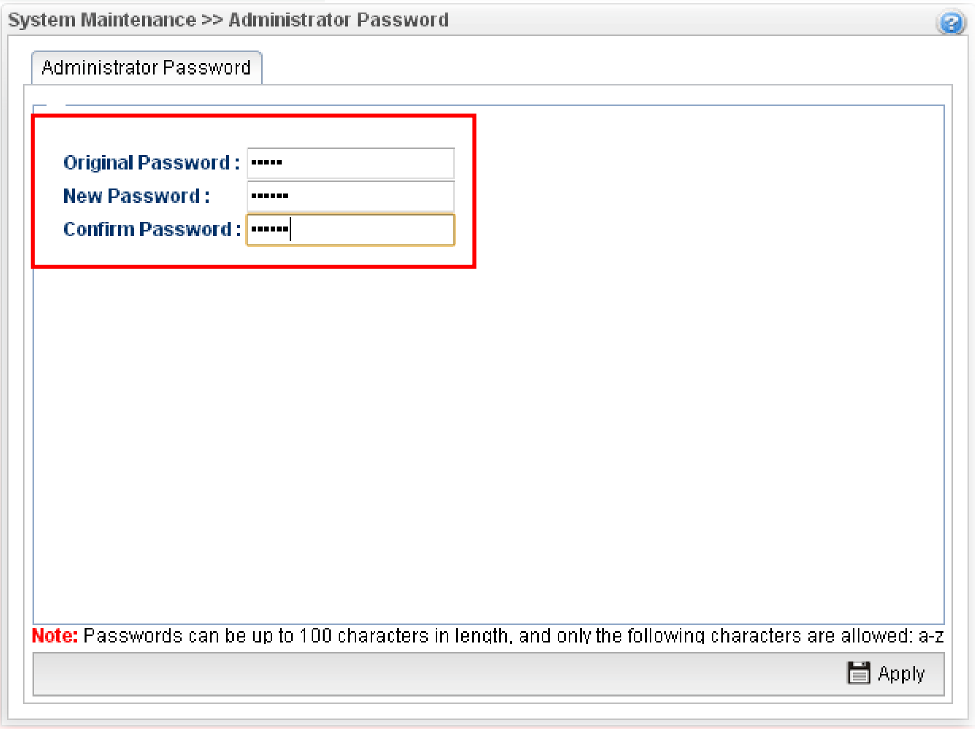
Model : Vigor300B
Hardware : 1.0
Firmware : 1.2.0
Revision : 5723
Build Date : 2015-12-03 01:49:54
System Time : 2011-01-01 08:26:40
System Up Time : 0 days 0:26:43

System Information

CPU Usage : 7%
Memory Usage : Memory:41% Cached:20%
Coprocessor : CPU:0% Memory:0%
Session Usage : 0% (84/100000)

Profile	Conne...	Descri...	Up Time	Mac	Protocol	IP	Gateway	DNS	RX Rat...	TX Rat...	RX Byt...	TX Byt...	Operation
wan1	down		0 days ...	00:1d:a...	dhcp(N...				0	0	0	0	
lan1	up		0 days ...	00:1d:a...	Static(N..	192.16...			3	3	977.79 ...	1.01 (MB)	

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



System Maintenance >> Administrator Password

Original Password : ·····

New Password : ······

Confirm Password : ······

Note: Passwords can be up to 100 characters in length, and only the following characters are allowed: a-z

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

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

2.2 Quick Start Wizard

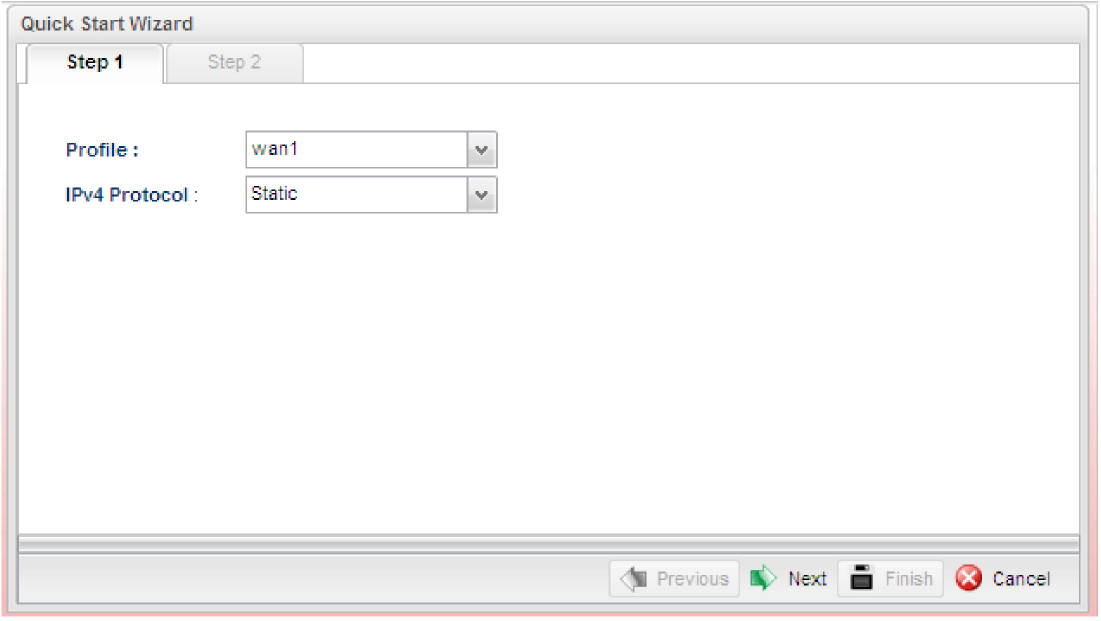
Quick Start Wizard is a wizard which is designed for configuring your router accessing Internet with simply steps. In the **Quick Start Wizard** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes.

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

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

2.2.1 Step 1 - Specifying the WAN Profile

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



Quick Start Wizard

Step 1 | Step 2

Profile : wan1

IPv4 Protocol : Static

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. **Static -** If **Static** is selected, you can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings. **DHCP -** It allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for Vigor300B automatically. It is not necessary for you to assign any setting. (Host Name and Domain Name are required for some ISPs). **PPPoE -** PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards:

Item	Description
	PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection. PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode. If your ISP provides you the **PPPoE** (Point-to-Point Protocol over Ethernet) connection, please select **PPPoE** for this router to get the following page. Enter the **username** and **password** provided by your ISP on the web page.

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

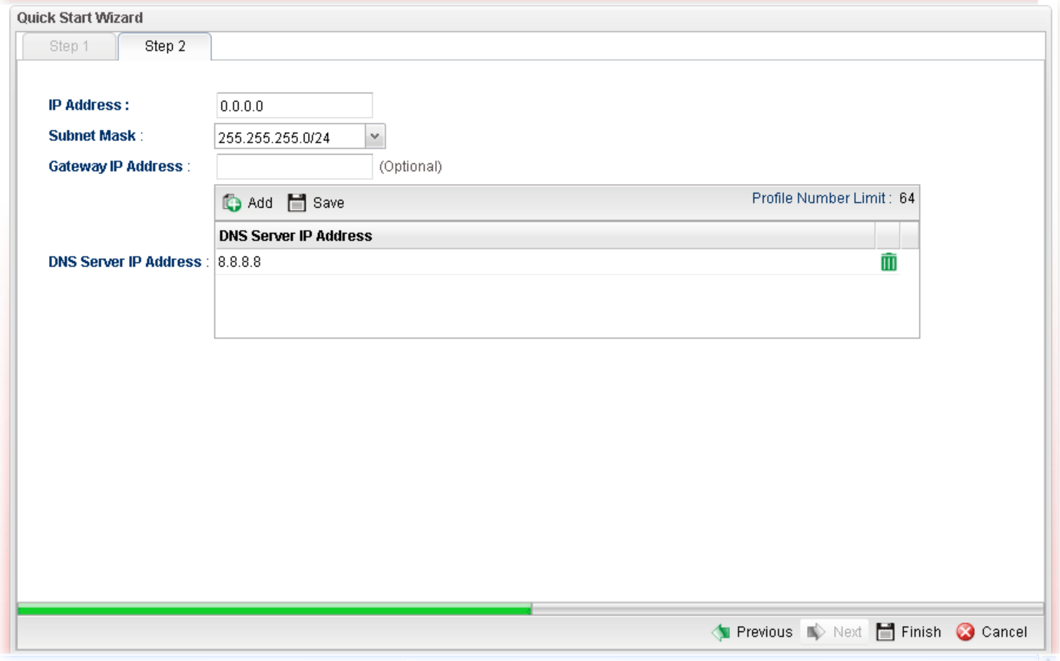
When you finish the above settings, please click **Next** to go to next page.

2.2.2 Step 2 - Configuring the Selected Protocol

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

If Static is selected

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



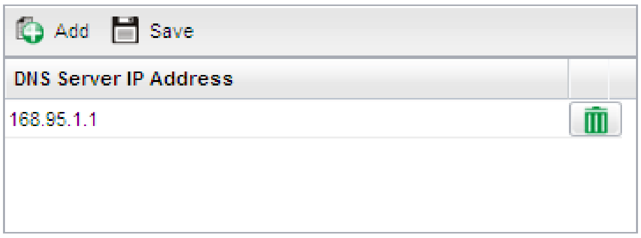
IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0/24

Gateway IP Address : (Optional)

DNS Server IP Address : 8.8.8.8

Available parameters are listed as follows:

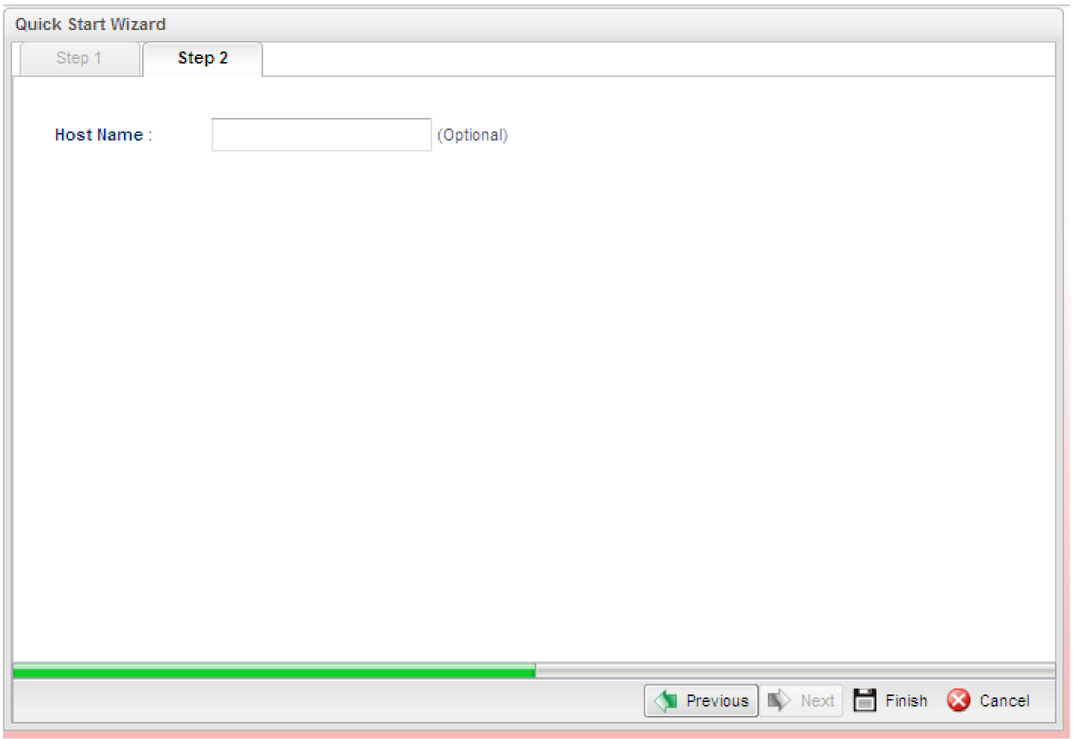
Item	Description
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile.
DNS Server IP Address	**Add** – Click this button to display the IP address field for adding a 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.  168.95.1.1 🗑 – 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 Vigor300B automatically. It is not necessary for you to assign any setting. (Host Name is required for some ISPs).



Host Name : (Optional)

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.

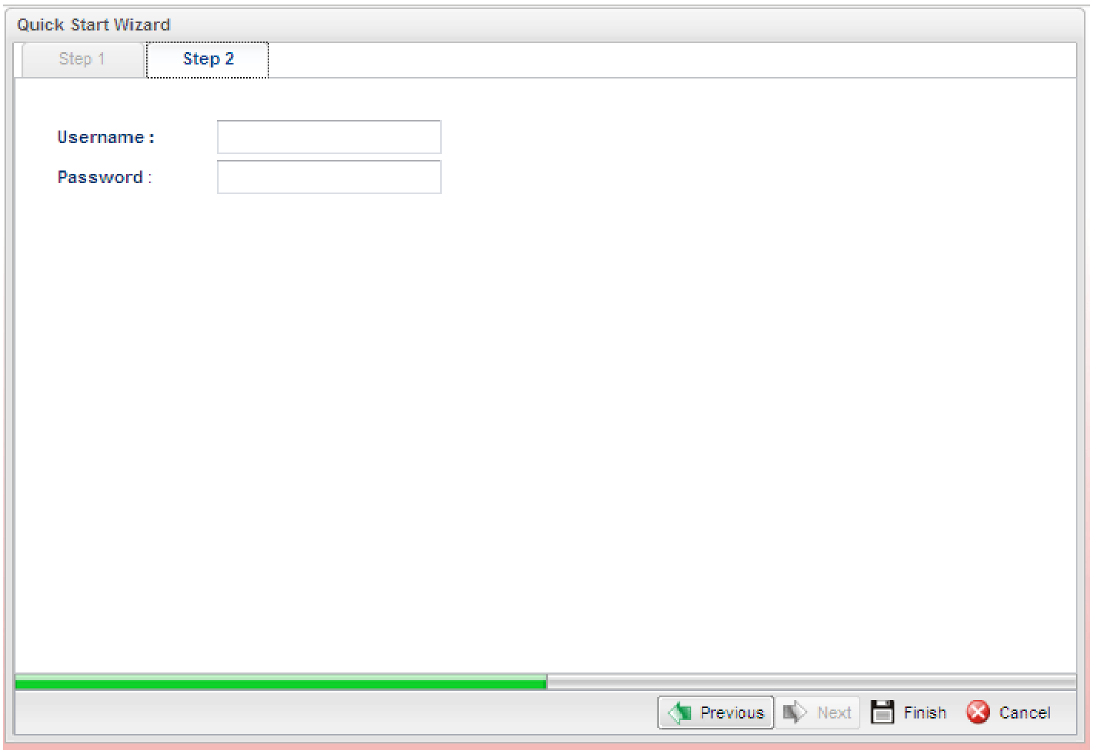
When you finished the above settings, please click **Finish**.

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.



Quick Start Wizard

Step 1 | Step 2

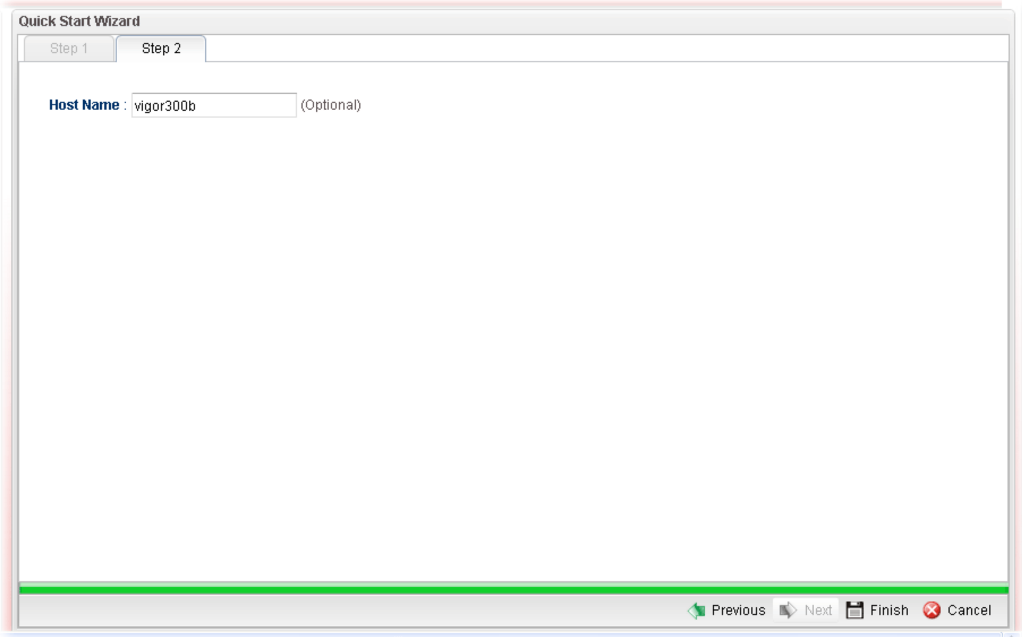
Username :

Password :

Available parameters are listed as follows:

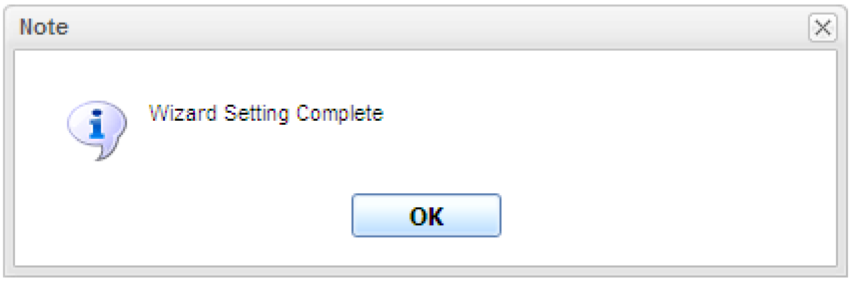
Item	Description
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

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



Host Name : vigor300b (Optional)

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

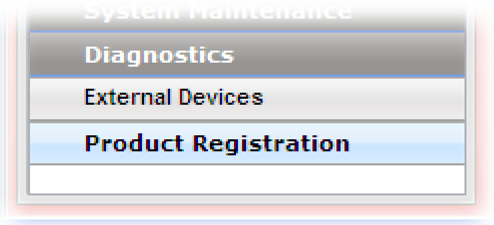


Wizard Setting Complete

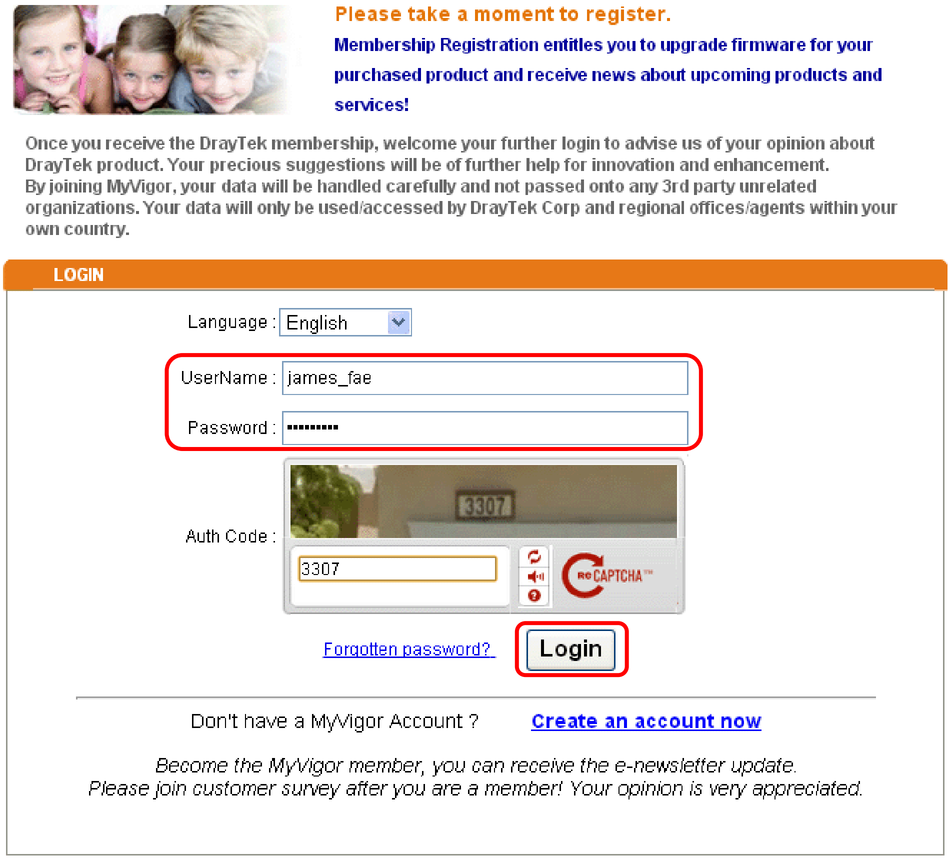
2.3 Register Vigor Router

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 Vigor300B 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.

LOGIN

Language : English

UserName : james_fae

Password : ••••••••••

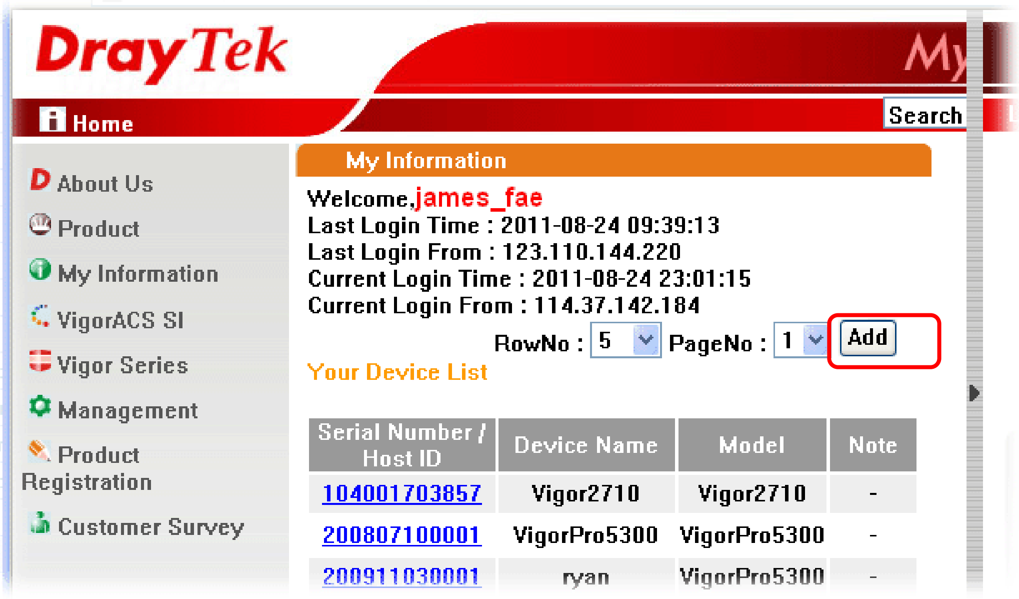
Auth Code : 3307

Don't have a MyVigor Account ? Create an account now

Become the MyVigor member, you can receive the e-newsletter update.
Please join customer survey after you are a member! Your opinion is very appreciated.

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

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



My Information

Welcome,james_fae
Last Login Time : 2011-08-24 09:39:13
Last Login From : 123.110.144.220
Current Login Time : 2011-08-24 23:01:15
Current Login From : 114.37.142.184

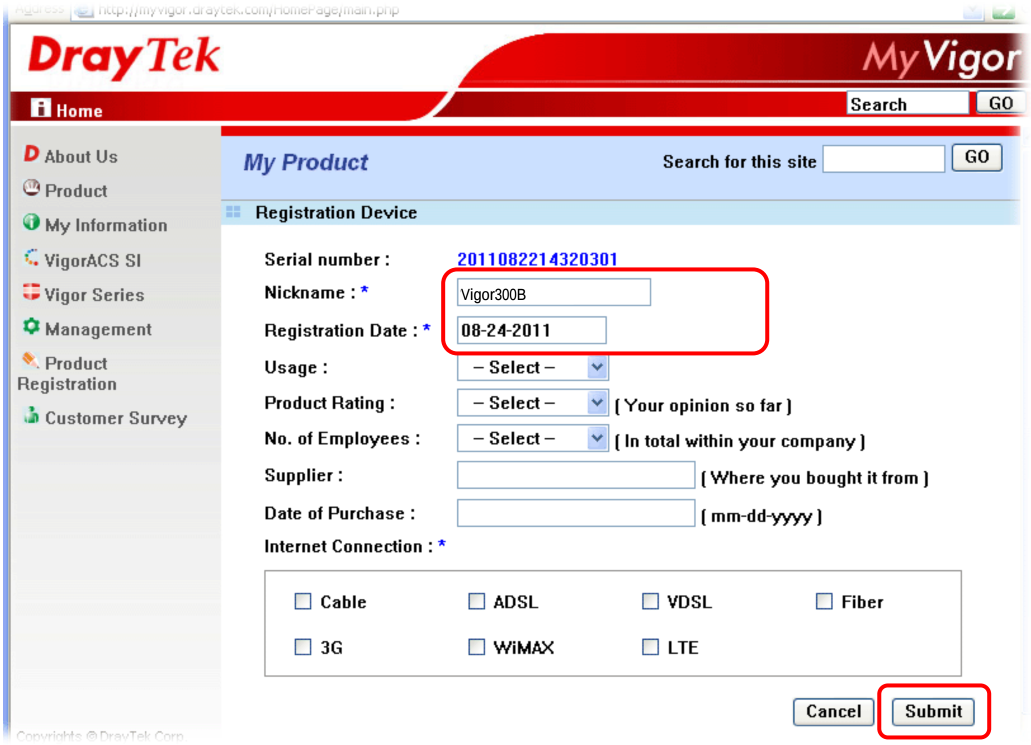
RowNo : 5 PageNo : 1

Your Device List

Serial Number / Host ID	Device Name	Model	Note
104001703857	Vigor2710	Vigor2710	-
200807100001	VigorPro5300	VigorPro5300	-
200911030001	ryan	VigorPro5300	-

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

4 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**.



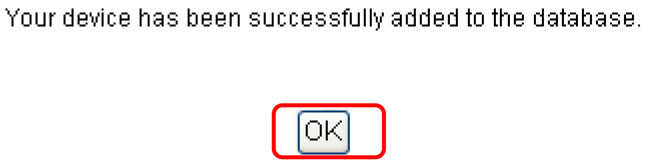
My Product

Registration Device

Serial number : 2011082214320301
Nickname : * Vigor300B
Registration Date : * 08-24-2011
Usage : – Select –
Product Rating : – Select – (Your opinion so far)
No. of Employees : – Select – (In total within your company)
Supplier : (Where you bought it from)
Date of Purchase : (mm-dd-yyyy)
Internet Connection : *

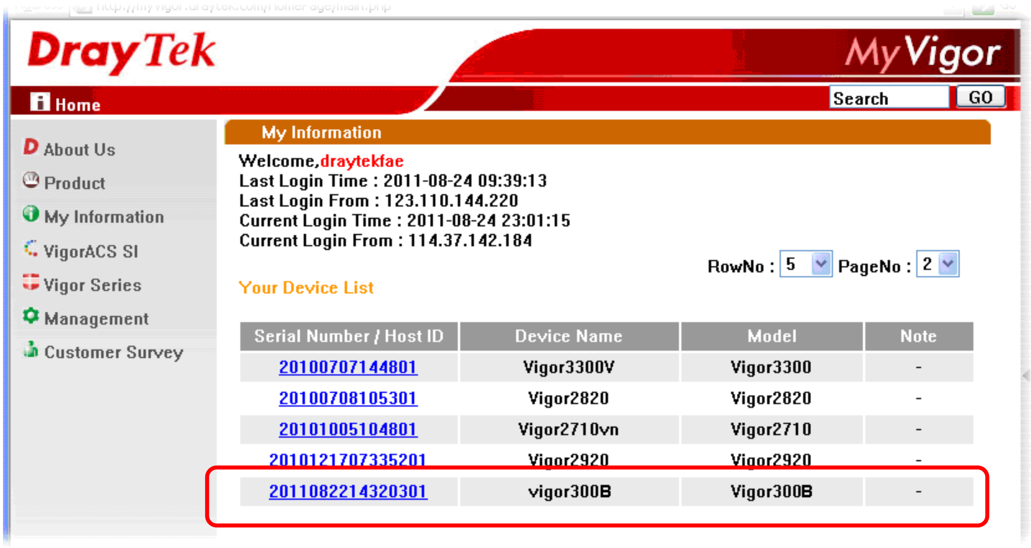
☐ Cable ☐ ADSL ☐ VDSL ☐ Fiber
☐ 3G ☐ WiMAX ☐ LTE

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 Vigor300B is listed under **Your Device List**.



My Information

Welcome,draytekfae
Last Login Time : 2011-08-24 09:39:13
Last Login From : 123.110.144.220
Current Login Time : 2011-08-24 23:01:15
Current Login From : 114.37.142.184

RowNo : 5 PageNo : 2

Your Device List

Serial Number / Host ID	Device Name	Model	Note
20100707144801	Vigor3300V	Vigor3300	-
20100708105301	Vigor2820	Vigor2820	-
20101005104801	Vigor2710vn	Vigor2710	-
2010121707335201	Vigor2920	Vigor2920	-
2011082214320301	vigor300B	Vigor300B	-

This page is left blank.

Chapter 3: Application and Tutorial

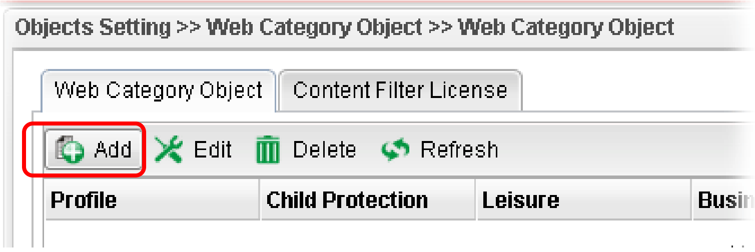
3.1 How to Use Web Content Filter (WCF)?

There are many kinds of benefits of Web Content Filtering, such as productivity enhancement, bandwidth regulation, HR policy compliance, and preventing web threats. Plus, with the pre-categorized items, IT staff can save plenty of time from creating firewall rules for unwanted contents.

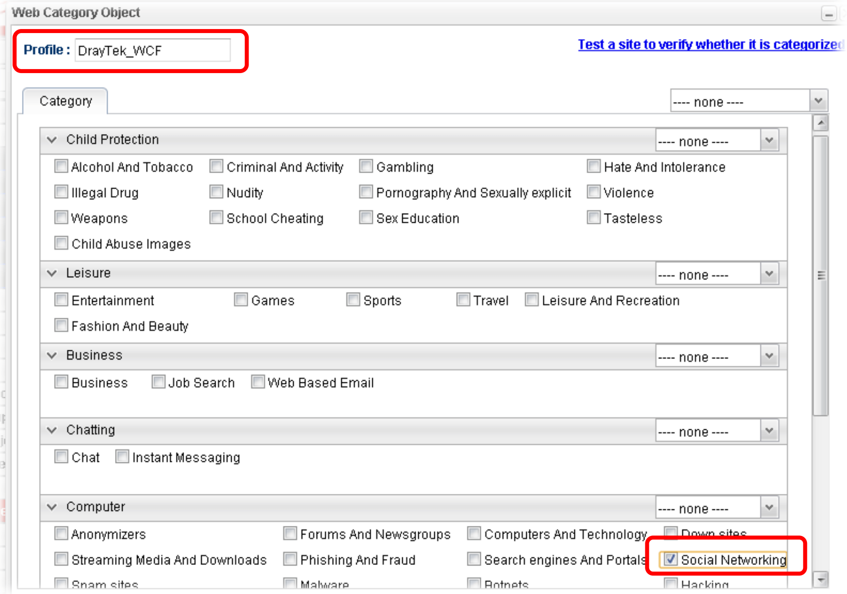
> **Note:** The Web Content Filter (WCF) is license-required with the annual renewal fee. You can get the 30-day free trial directly via Vigor300B after completing the registration at MyVigor portal.

In the following example, we assume that Administrator prohibits users surfing Facebook.

1. Please go to **Object Setting** >> **Web Category Object** >> **Web Category Object**. After activating the Web Content Filter service via "**Content Filter License**", click "**Add**" in the "**Web Category Object**" to start.



2. Create the profile name (e.g. DrayTek_WCF), and choose any section(s) which you want to do filtering, including Child Protection, Leisure, Business, Chatting, Computer and Other. Here we choose Social Networking since facebook is categorized in social networking. Press the **Apply** button.



Profile : DrayTek_WCF

Child Protection ---- none ----

□ Alcohol And Tobacco □ Criminal And Activity □ Gambling □ Hate And Intolerance
□ Illegal Drug □ Nudity □ Pornography And Sexually explicit □ Violence
□ Weapons □ School Cheating □ Sex Education □ Tasteless
□ Child Abuse Images

Leisure ---- none ----

□ Entertainment □ Games □ Sports □ Travel □ Leisure And Recreation
□ Fashion And Beauty

Business ---- none ----

□ Business □ Job Search □ Web Based Email

Chatting ---- none ----

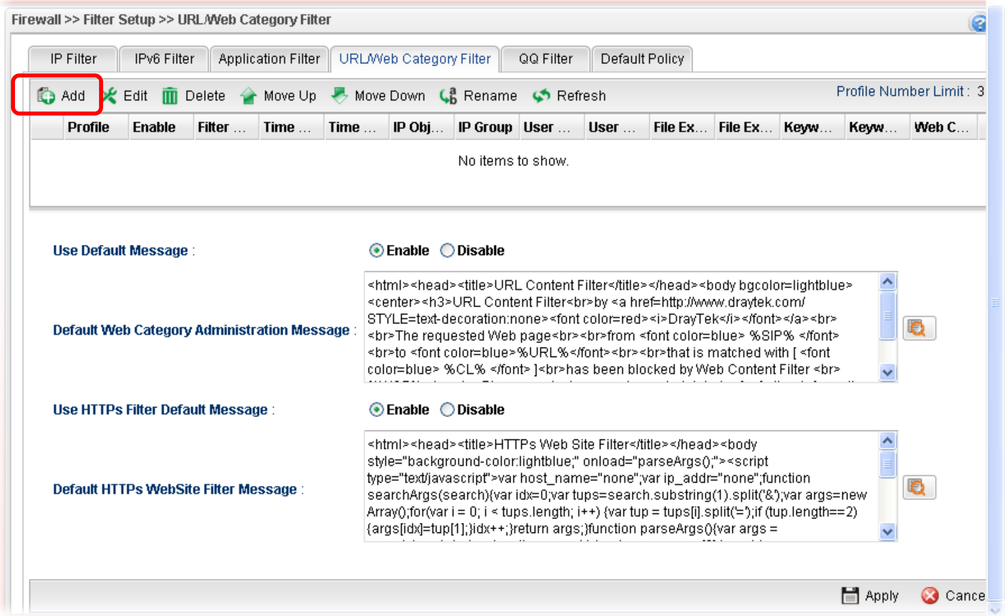
□ Chat □ Instant Messaging

Computer ---- none ----

□ Anonymizers □ Forums And Newsgroups □ Computers And Technology □ Down sites
□ Streaming Media And Downloads □ Phishing And Fraud □ Search engines And Portals ☑ Social Networking
□ Spam sites □ Malware □ Botnets □ Hacking

Note: We can check out which category the URL belongs to by visiting the following website. http://www.cyren.com/url-category-check.html.

3. Go to **Firewall** >> **Filter Setup**, select “**URL/Web Category Filter**”, and click “**Add**”.



Firewall >> Filter Setup >> URL/Web Category Filter

Profile Number Limit : 3

Profile	Enable	Filter ...	Time ...	Time ...	IP Obj...	IP Group	User ...	User ...	File Ex...	File Ex...	Keyw...	Keyw...	Web C...

No items to show.

Use Default Message : ● Enable ○ Disable

Default Web Category Administration Message :

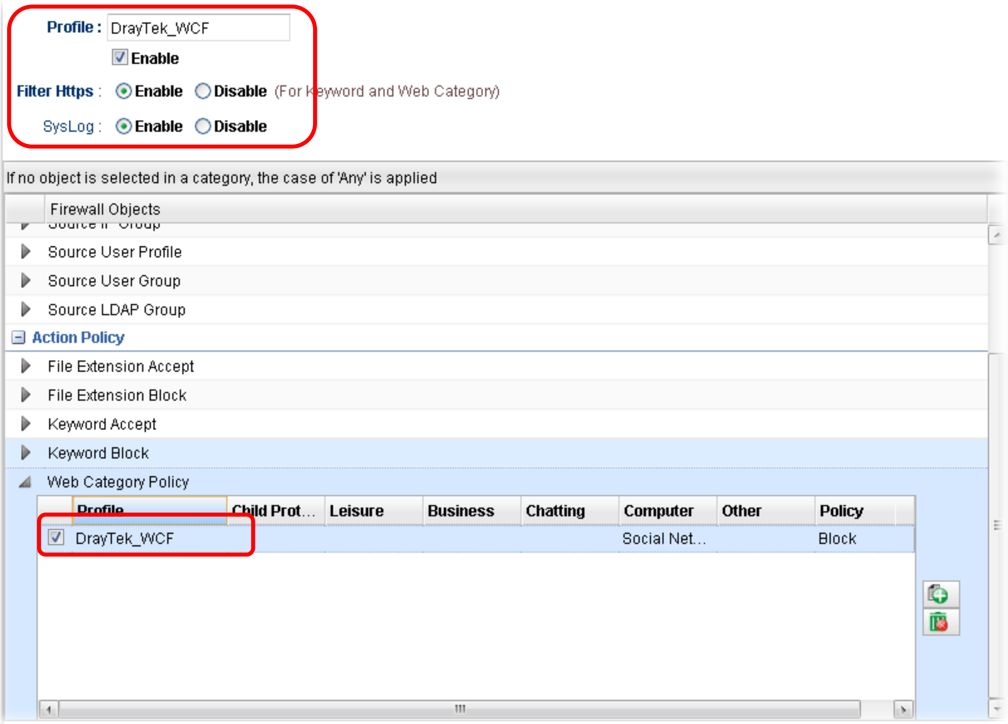
```
<html><head><title>URL Content Filter</title></head><body bgcolor=lightblue>
<center><h3>URL Content Filter<br>by <a href=http://www.draytek.com/
STYLE=text-decoration:none><font color=red><i>DrayTek</i></font></a><br>
<br>The requested Web page<br><br>from <font color=blue> %SIP% </font>
<br>to <font color=blue>%URL%</font><br><br>that is matched with [ <font
color=blue> %CL% </font> ]<br>has been blocked by Web Content Filter <br>
```

Use HTTPs Filter Default Message : ● Enable ○ Disable

Default HTTPs WebSite Filter Message :

```
<html><head><title>HTTPs Web Site Filter</title></head><body
style="background-color:lightblue;" onload="parseArgs();"><script
type="text/javascript">var host_name="none";var ip_addr="none";function
searchArgs(search){var idx=0;var tups=search.substring(1).split('&');var args=new
Array();for(var i = 0; i < tups.length; i++) {var tup = tups[i].split('=');if (tup.length==2)
{args[idx]=tup[1];}idx++;}return args;}function parseArgs(){var args =
```

4. Type Profile name, tick **Enable** and enable **Filter HTTPS**. Tick DrayTek_WCF in **Web Category Policy** under the **Action Policy**. Click **Apply**.



Profile : DrayTek_WCF

☑ Enable

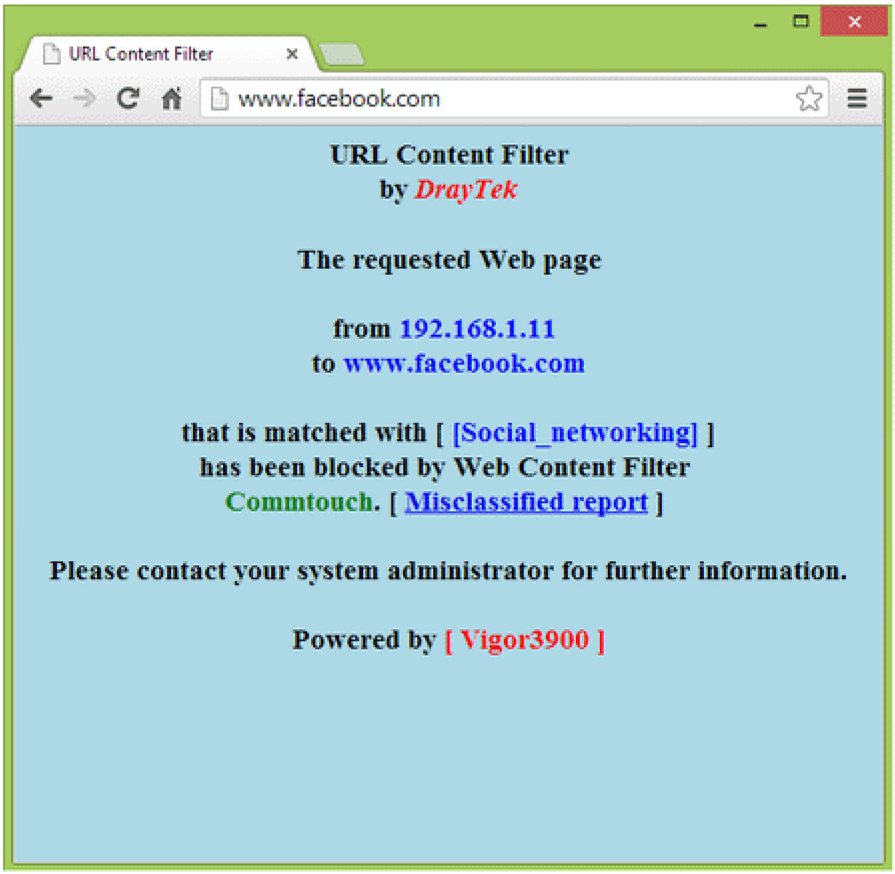
Filter Https : ● Enable ○ Disable (For Keyword and Web Category)

SysLog : ● Enable ○ Disable

If no object is selected in a category, the case of 'Any' is applied

Profile	Child Prot...	Leisure	Business	Chatting	Computer	Other	Policy
☑ DrayTek_WCF					Social Net...		Block

5. The message window will be shown when we try to access facebook.



URL Content Filter
by DrayTek

The requested Web page

from 192.168.1.11
to www.facebook.com

that is matched with [[Social_networking]]
has been blocked by Web Content Filter
Commtouch. [Misclassified report]

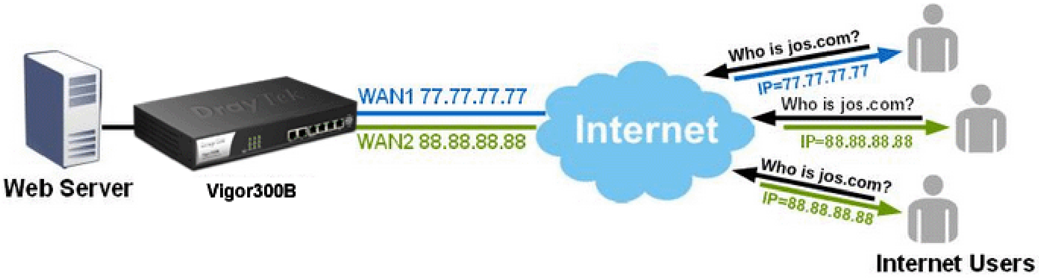
Please contact your system administrator for further information.

Powered by [Vigor3900]

Every time the connection matches the category we selected to block, the user will see the block message above.

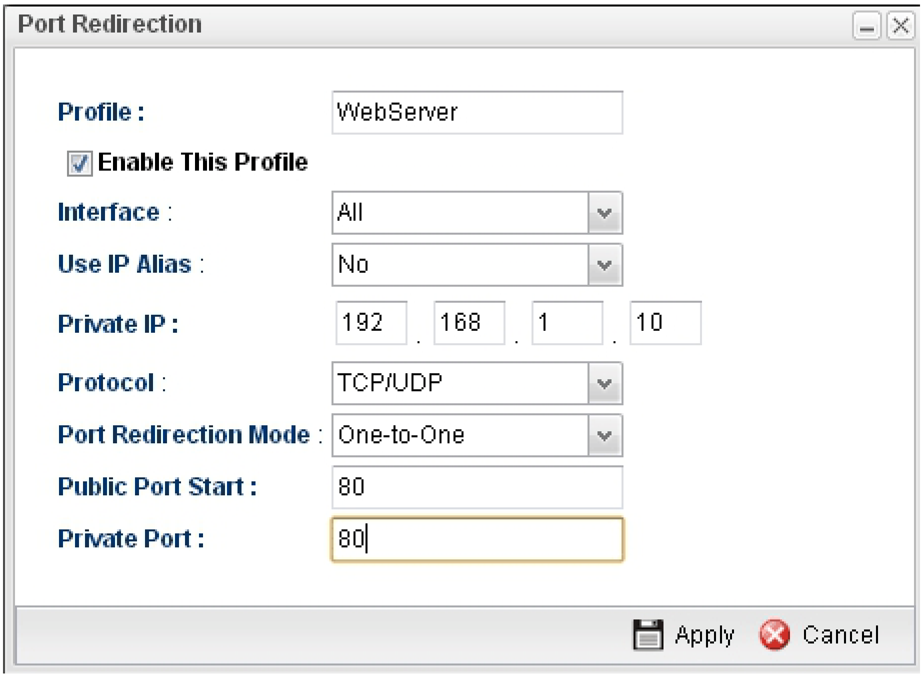
3.2 How to Configure WAN Inbound Load Balance?

The document introduces Inbound Load Balance, which is a feature allows Vigor 2960/300B/3900, when acting as a DNS Server, to distribute the traffic across multiple WAN interfaces. There will be five parts of setting: enabling Web/FTP services on the router, setting weight for the Web server, setting weight for the FTP server, and setting CNAME for the FILE server, and setting NS Record (optional).



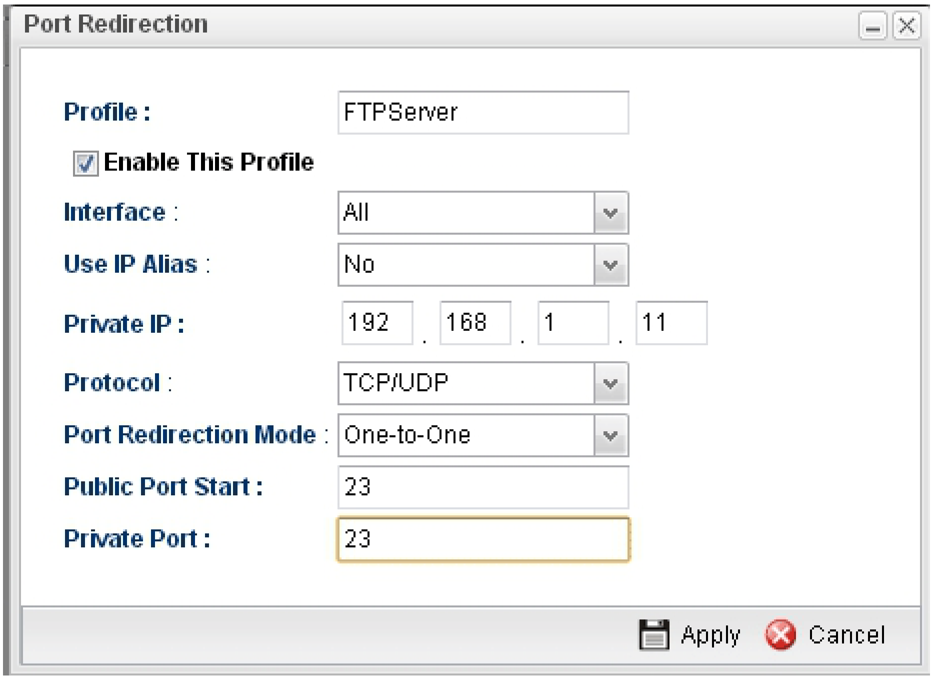
A. Enabling Web/FTP services on the router

1. Please go to **NAT >> Port Redirection** to set up Port Redirection rule for the Web/FTP Servers.



Port Redirection

Profile :	WebServer
☑ Enable This Profile	
Interface :	All
Use IP Alias :	No
Private IP :	192 . 168 . 1 . 10
Protocol :	TCP/UDP
Port Redirection Mode :	One-to-One
Public Port Start :	80
Private Port :	80



Port Redirection

Profile : FTPServer

☑ Enable This Profile

Interface : All

Use IP Alias : No

Private IP : 192 . 168 . 1 . 11

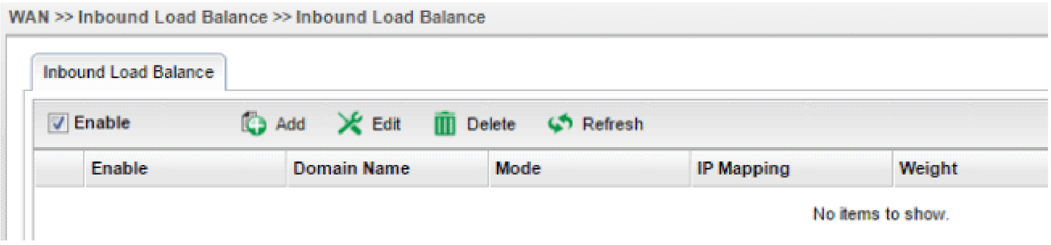
Protocol : TCP/UDP

Port Redirection Mode : One-to-One

Public Port Start : 23

Private Port : 23

2. Go to **WAN >> Load Balance** to enable the services.



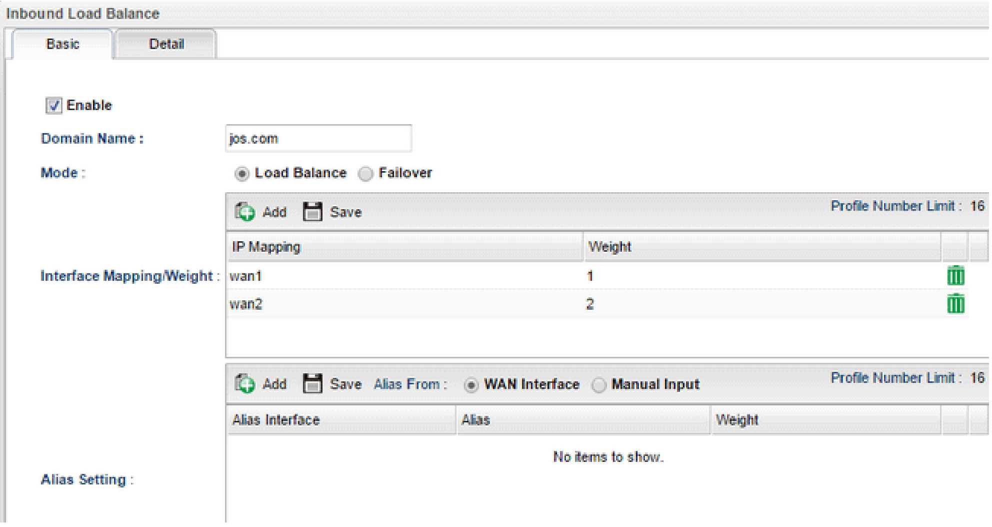
WAN >> Inbound Load Balance >> Inbound Load Balance

	Enable	Domain Name	Mode	IP Mapping	Weight

No items to show.

B. Setting weight for the Web server

1. Add a profile for domain name “jos.com” and “www.jos.tw”, then assign a weight of 1 to WAN 1 and 2 for WAN2. This meas that when receiving three DNS queries, DNS server will return WAN1's IP for the first time, and WAN'2 IP for the next two times.



Inbound Load Balance

☑ Enable

Domain Name : jos.com

Mode : ● Load Balance ○ Failover

Interface Mapping/Weight :

Profile Number Limit : 16

IP Mapping	Weight
wan1	1
wan2	2

Alias Setting :

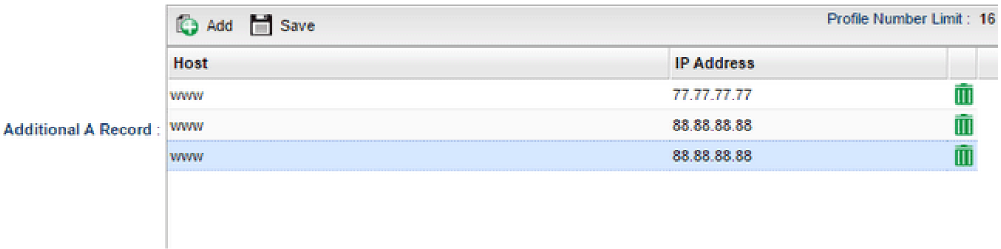
Add Save Alias From : ● WAN Interface ○ Manual Input

Profile Number Limit : 16

Alias Interface	Alias	Weight

No items to show.

2. Click **Detail** tab to add Additional A Record for Host Name “www.jos.com” to corresponds with “jos.com” with same weight 1:2.



Additional A Record :

Add | Save | Profile Number Limit : 16

Host	IP Address	
www	77.77.77.77	🗑
www	88.88.88.88	🗑
www	88.88.88.88	🗑

After the settings have done, we do “**nslookup**” to query the domain name for 3 times, and the results are reflecting the Interface Weights.

The test of query for “jos.com”

```
First DNS query
>jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: jos.com
Address: 77.77.77.77
Second DNS query
>jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: jos.com
Address: 88.88.88.88
Third DNS query
>jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: jos.com
Address: 88.88.88.88
```

The test of query for “www.jos.com”

```
First DNS query
>www.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: jos.com
Address: 77.77.77.77
Aliases: www.jos.com
Second DNS query
>www.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: jos.com
```

Address: 88.88.88.88

Aliases: www.jos.com

Third DNS query

>www.jos.com

Server: [77.77.77.77]

Address: 77.77.77.77

Name: jos.com

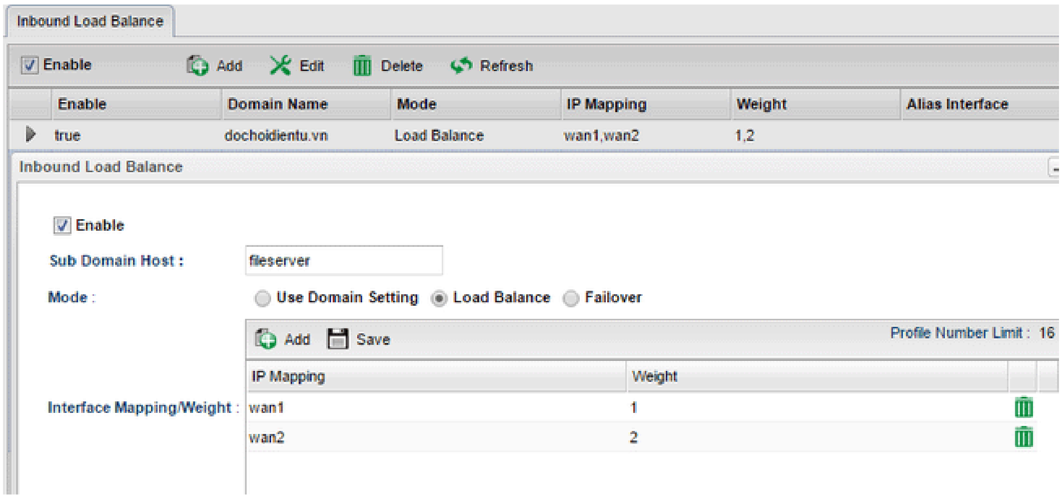
Address: 88.88.88.88

Aliases: www.jos.com

C. Setting weight for the File server (Sub-domain)

1. Add a profile for Sub-domain “fileserver.jos.com" with Load Balance Mode, and assign a weight of 1 to WAN 1 and 2 for WAN2.

> *Note*: “Use Domain Setting” Mode means the weight will be the same as the weight of Domain Name “jos.com”.



Inbound Load Balance

☑ Enable

Enable	Domain Name	Mode	IP Mapping	Weight	Alias Interface
true	dochoidientu.vn	Load Balance	wan1,wan2	1,2	

Inbound Load Balance

☑ Enable

Sub Domain Host : fileserver

Mode : ○ Use Domain Setting ● Load Balance ○ Failover

Profile Number Limit : 16

Interface Mapping/Weight :

IP Mapping	Weight
wan1	1
wan2	2

After the settings has done we do “**nslookup**” and query the sub-domain name for 3 times, and the results are reflecting the Interface Weight.

First DNS query

>fileserver.jos.com

Server: [77.77.77.77]

Address: 77.77.77.77

Name: fileserver.jos.com

Address: 77.77.77.77

Second DNS query

>fileserver.jos.com

Server: [77.77.77.77]

Address: 77.77.77.77

Name: fileserver.jos.com

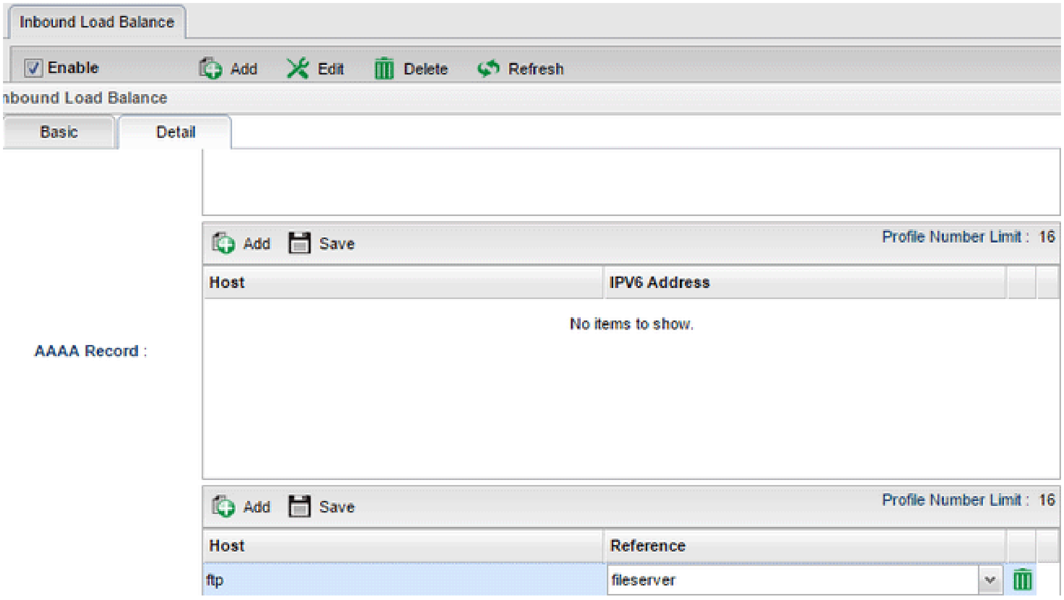
Address: 77.77.77.77

Third DNS query

```
>fileserver.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: fileserver.jos.com
Address: 88.88.88.88
```

D. Setting CNAME for the File server (Sub-domain)

1. After creating profile for Sub-domain “fileserver.jos.com", we may add CNAME Record for Sub-domain “fileserver.jos.com" via **Inbound Load Balance** >> **Detail page**.
2. Click **Add** then input host "ftp" and select "fileserver" as Reference.



Host	IPV6 Address
No items to show.	

Host	Reference
ftp	fileserver

After the settings we do **nslookup** and query “ftp.jos.com” for 3 times, and we could see the results are reflecting the Interface Weight.

First DNS query

```
>ftp.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: fileserver.jos.com
Address: 77.77.77.77
Aliases: ftp.jos.com
```

Second DNS query

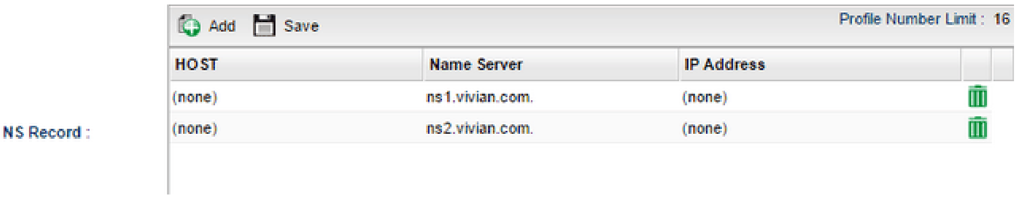
```
>ftp.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: fileserver.jos.com
Address: 77.77.77.77
Aliases: ftp.jos.com
```

Third DNS query

```
>ftp.jos.com
Server: [77.77.77.77]
Address: 77.77.77.77
Name: fileserver.jos.com
Address: 88.88.88.88
Aliases: ftp.jos.com
```

E. Setting up NS Records (Optional)

1. NS Record is not necessary since the NS records should be already available in the upper DNS servers.
2. When NS server is with different domain name, such as “vivian.com”, please add the NS Record with name server field and end it with “.” (a dot)

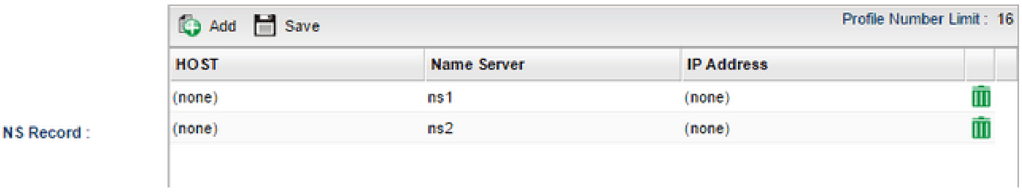


Profile Number Limit : 16

NS Record :

HOST	Name Server	IP Address	
(none)	ns1.vivian.com.	(none)	🗑
(none)	ns2.vivian.com.	(none)	🗑

3. When NS server is with same domain name, such as “jos.com”, please add the NS Record with name server field ns1 and ns2.



Profile Number Limit : 16

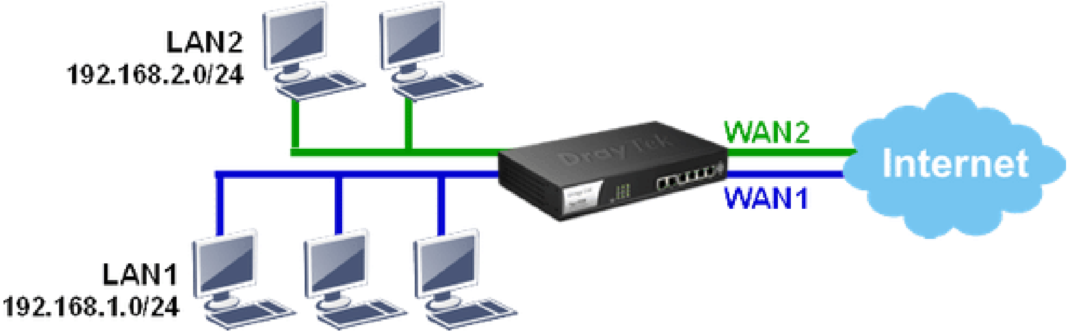
NS Record :

HOST	Name Server	IP Address	
(none)	ns1	(none)	🗑
(none)	ns2	(none)	🗑

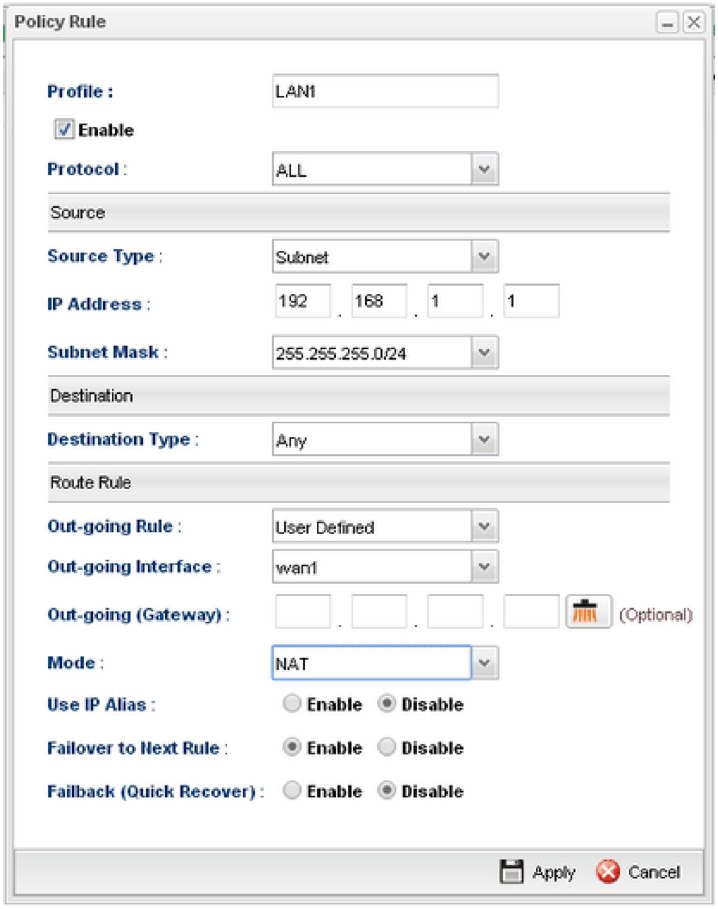
3.3 How to Configure WAN Load Balancing with Policy Route on Vigor300B?

This document demonstrates how to do WAN load balancing with Policy Route feature in Routing. In the firmware before version 1.0.9, this is a feature in WAN menu called Load Balance Rule. After upgrading firmware to version 1.0.9, the Rules set in WAN >> Load Balance will be transferred to Policy Rule automatically.

In this example, we have WAN1 and WAN2 connected on Vigor3900, and we would like to balance the traffic across them. Suppose we would like the traffic from LAN1 (192.168.1.0/24) to go to the Internet via WAN1 and traffic from LAN2 (192.168.2.0/24) to go to the Internet via WAN2. To achieve this, we need one Policy Rule for each LAN subnet.



1. Create a Route Policy for traffic from LAN1 to go to the Internet via WAN1. Go to **Routing** >> **Policy Route**, click **Add** to add a new policy rule.



Profile : LAN1

☑ Enable

Protocol : ALL

Source

Source Type : Subnet

IP Address : 192 . 168 . 1 . 1

Subnet Mask : 255.255.255.0/24

Destination

Destination Type : Any

Route Rule

Out-going Rule : User Defined

Out-going Interface : wan1

Out-going (Gateway) : . . . (Optional)

Mode : NAT

Use IP Alias : ○ Enable ● Disable

Failover to Next Rule : ● Enable ○ Disable

Failback (Quick Recover) : ○ Enable ● Disable

a. Enter rule name.

b. **Enable** this rule.

c. Select **Source Type** as Subnet, and enter the **IP address** and **Subnet Mask** of LAN1.

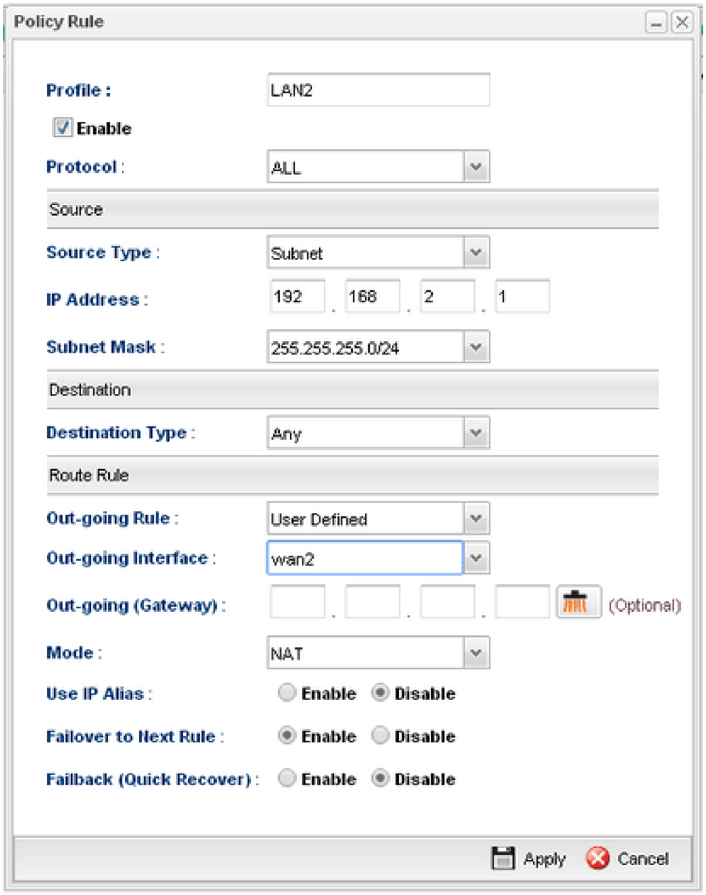
d. Select **Out-Going Rule** as User Defined, and **Interface** as WAN1.

e. Enable **Failover to Next Rule** so that when WAN1 fails, it will follow the next rule.

f. Click **Apply** to save the configuration.

With the above configuration, traffic from LAN1 will be sent to WAN1. When WAN1 is not available, because Failover to Next Rule in enabled, the router will check if there is another Policy Rule matched. If there is not, the Default Route will be applied.

2. Similarly, add a Policy Rule for traffic from LAN2 to go to the Internet via WAN2.



Policy Rule

Profile : LAN2

☑ Enable

Protocol : ALL

Source

Source Type : Subnet

IP Address : 192 . 168 . 2 . 1

Subnet Mask : 255.255.255.0/24

Destination

Destination Type : Any

Route Rule

Out-going Rule : User Defined

Out-going Interface : wan2

Out-going (Gateway) : . . . (Optional)

Mode : NAT

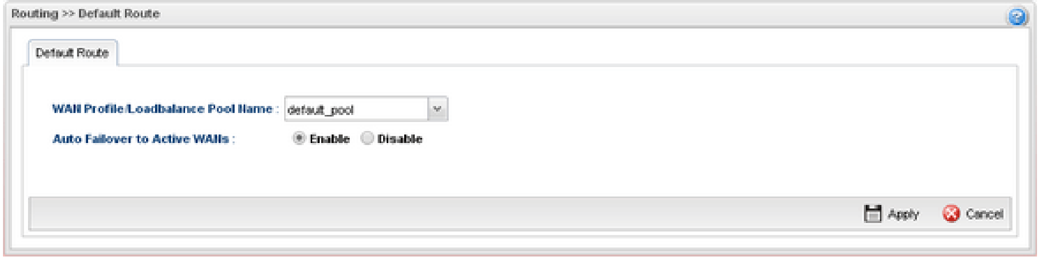
Use IP Alias : ○ Enable ● Disable

Failover to Next Rule : ● Enable ○ Disable

Failback (Quick Recover) : ○ Enable ● Disable

3. Configure the Default Route at **Routing >>Default Route**.

Default Route is the rule to be applied if there are no Policy Rule matched. You may set Default Route to a specific WAN interface or to “default pool”. Enable “Auto Failover to Active WANs” will swap the sessions to other active WANs when the original WAN connection is lost.



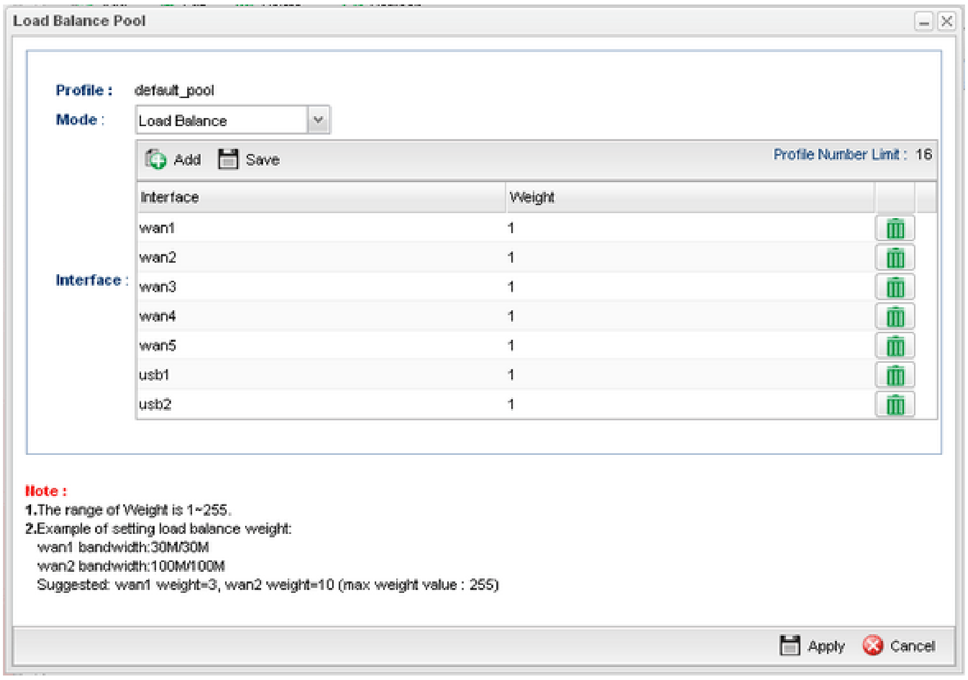
Routing >> Default Route

Default Route

WAN Profile/Loadbalance Pool Name : default_pool

Auto Failover to Active WANs : ● Enable ○ Disable

Default Pool can be configured at **Routing>>Load Balance Pool**.



Load Balance Pool

Profile : default_pool

Mode : Load Balance

Profile Number Limit : 16

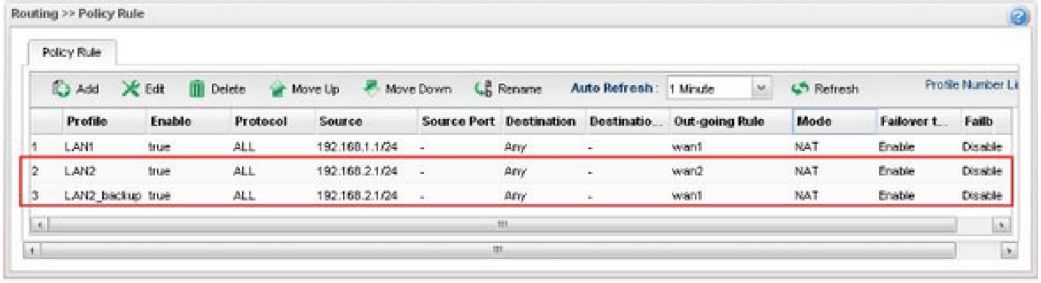
Interface :

Interface	Weight
wan1	1
wan2	1
wan3	1
wan4	1
wan5	1
usb1	1
usb2	1

Note :
1.The range of Weight is 1~255.
2.Example of setting load balance weight:
wan1 bandwidth:30M/30M
wan2 bandwidth:100M/100M
Suggested: wan1 weight=3, wan2 weight=10 (max weight value : 255)

By default, every WAN interface has the same weight. So that when Default Route is applied, every available WAN interface will be used equally.

4. If you want to use a specific WAN interface to be the failover interface, please create another Policy Rule. For example, you can create a second rule for LAN2 to go to the Internet via WAN1.



Routing >> Policy Rule

Policy Rule

Auto Refresh : 1 Minute

Profile Number Li

	Profile	Enable	Protocol	Source	Source Port	Destination	Destinatio...	Out-going Rule	Mode	Failover t...	Failb
1	LAN1	true	ALL	192.168.1.1/24	-	Any	-	wan1	NAT	Enable	Disable
2	LAN2	true	ALL	192.168.2.1/24	-	Any	-	wan2	NAT	Enable	Disable
3	LAN2_backup	true	ALL	192.168.2.1/24	-	Any	-	wan1	NAT	Enable	Disable

Now there are two policy rules with the same Source but different Out-going Rule. The one with smaller index number will be implemented first, so if WAN2 is available, traffic from LAN2 will always go via WAN2. Only when WAN2 is down, because “Failover to Next Rule” is enabled, the next rule matched will be applied; thus, traffic will be sent to WAN1.

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

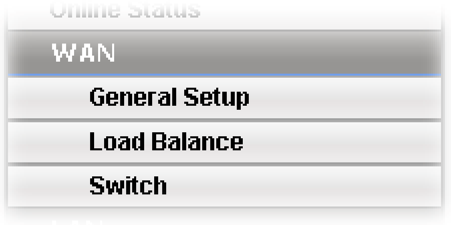
What are Public IP Address and Private IP Address

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.

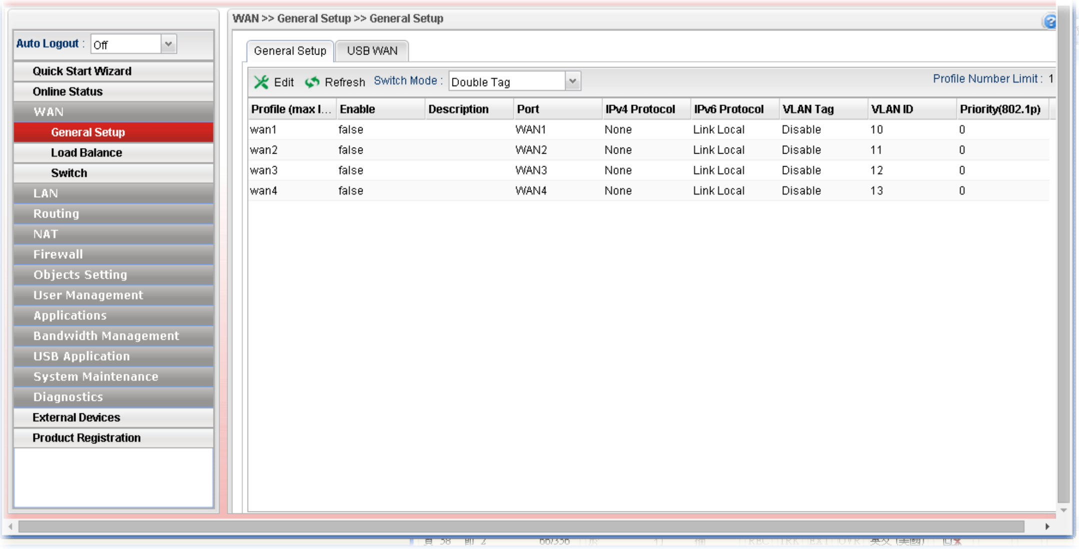
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information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



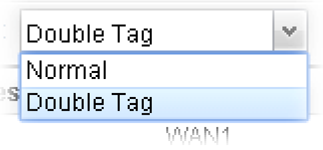
WAN >> General Setup >> General Setup

Switch Mode : Double Tag

Profile Number Limit : 1

Profile (max l...	Enable	Description	Port	IPv4 Protocol	IPv6 Protocol	VLAN Tag	VLAN ID	Priority(802.1p)
wan1	false		WAN1	None	Link Local	Disable	10	0
wan2	false		WAN2	None	Link Local	Disable	11	0
wan3	false		WAN3	None	Link Local	Disable	12	0
wan4	false		WAN4	None	Link Local	Disable	13	0

Each item will be explained as follows:

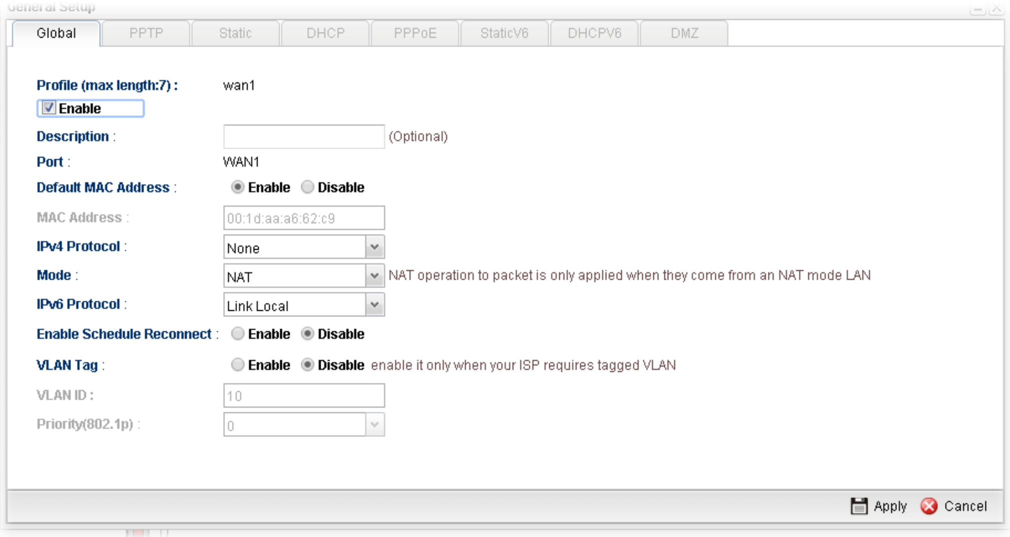
Item	Description
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Switch Mode	Specify the mode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

1. Open **WAN>>General Setup**. Choose wan1/wan2/wan3/wan4 profile and click the **Edit** button to open the following dialog. Only the tab of the protocol specified in **IPv4 Protocol** field will be available for you to modify. If you want to change and specify another connection mode for such WAN profile, remember to choose the mode from the drop down list of **IPv4 Protocol**.



General Setup

Profile (max length:7) : wan1

☑ Enable

Description : (Optional)

Port : WAN1

Default MAC Address : ● Enable ○ Disable

MAC Address : 00:1d:aa:a6:62:c9

IPv4 Protocol : None

Mode : NAT NAT operation to packet is only applied when they come from an NAT mode LAN

IPv6 Protocol : Link Local

Enable Schedule Reconnect : ○ Enable ● Disable

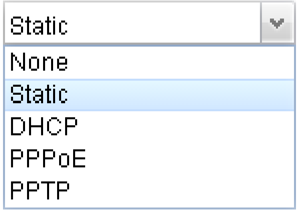
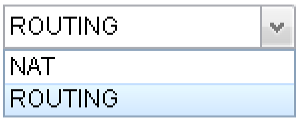
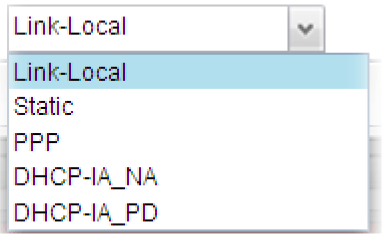
VLAN Tag : ○ Enable ● Disable enable it only when your ISP requires tagged VLAN

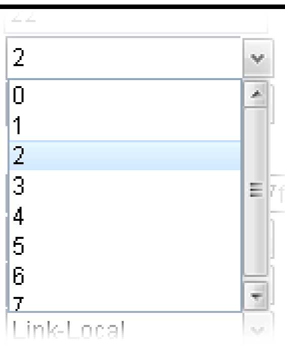
VLAN ID : 10

Priority(802.1p) : 0

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	Display 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.  Link-Local Link-Local Static PPP DHCP-IA_NA DHCP-IA_PD
Enable Schedule Reconnect	**Enable** – Click it to enable the function of reconnecting the network automatically within the time schedule. **Disable** – Click it to disable the schedule reconnect function.
Schedule Time Object	Choose the time object profile to be applied by such WAN.
VLAN Tag	**Enable** – Click it to enable the function of VLAN Tag. Data transmitted through the router will be tagged with specified number for identification. **Disable** – Click it to disable the function of VLAN Tag. Data transmitted through the router will not be tagged with any number.
VLAN ID	Type the VLAN ID number for such profile.
Priority(802.1p)	Type the packet priority number for such VLAN. The range is from 0 to 7.

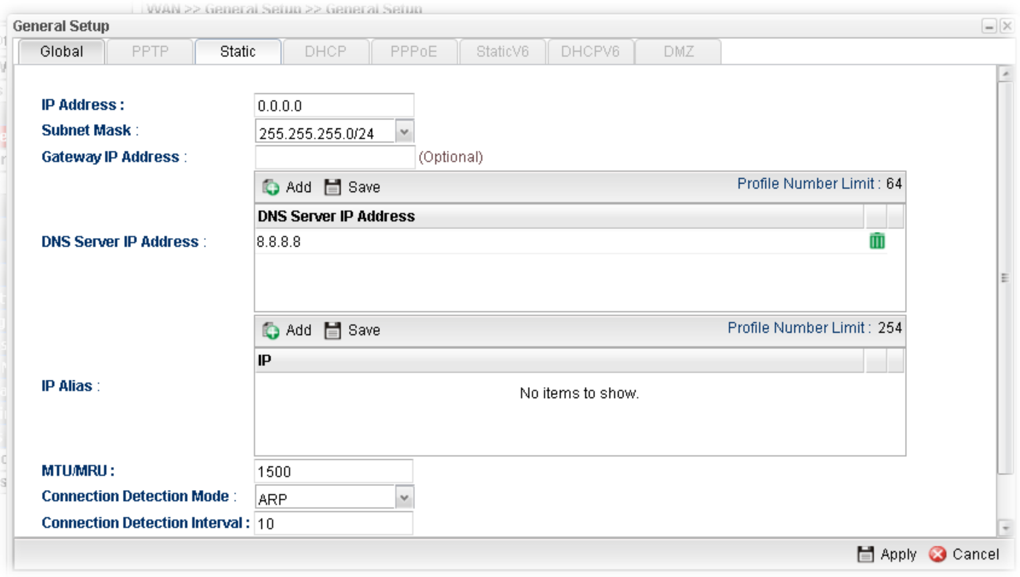
	
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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

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

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

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



General Setup

IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0/24

Gateway IP Address : (Optional)

Profile Number Limit : 64

DNS Server IP Address :

DNS Server IP Address
8.8.8.8

Profile Number Limit : 254

IP Alias :

IP
No items to show.

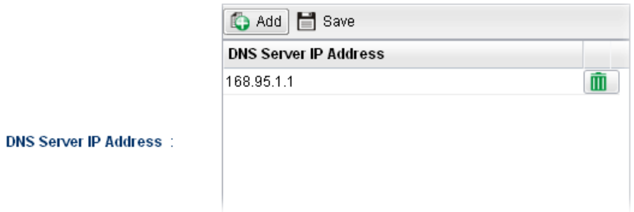
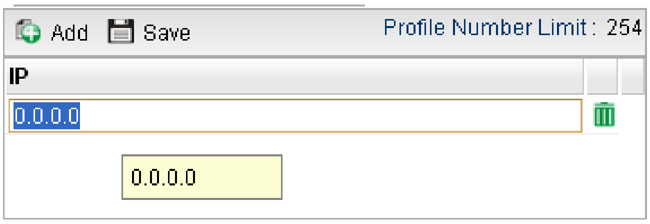
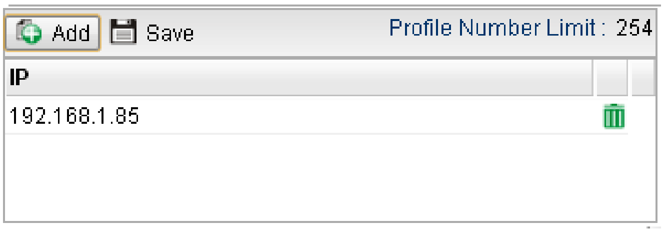
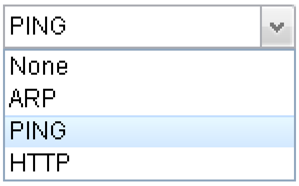
MTU/MRU : 1500

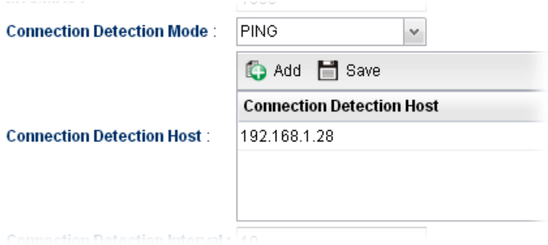
Connection Detection Mode : ARP

Connection Detection Interval : 10

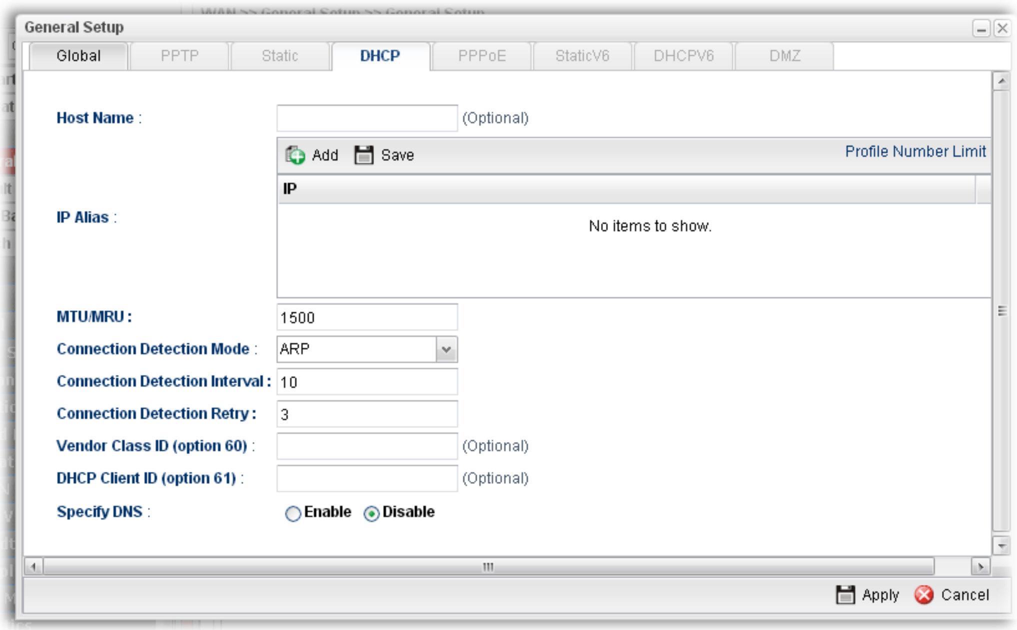
Available parameters are listed as follows:

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	Type a public IP address as the primary DNS (Domain Name Server). To add a new IP address, simply place the mouse

Address	cursor on this filed. The following dialog will appear.  Add Save DNS Server IP Address DNS Server IP Address : 168.95.1.1 **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny boxes one by one.  0.0.0.0 0.0.0.0 **Save** – Click this button to save the setting.  192.168.1.85 🗑 – click the icon to remove the selected entry.
MTU/MRU	Type the value of MTU/MRU. The default value is 1500.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are three ways **ARP**, **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**. **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.  Connection Detection Mode : PING Connection Detection Host : 192.168.1.28 **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



Host Name : (Optional)

IP Alias : No items to show.

MTU/MRU : 1500

Connection Detection Mode : ARP

Connection Detection Interval : 10

Connection Detection Retry : 3

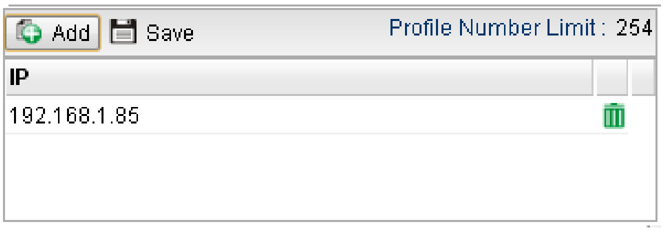
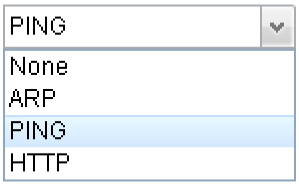
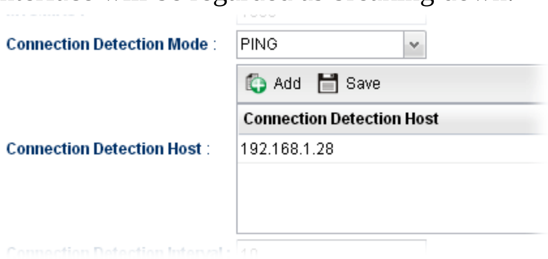
Vendor Class ID (option 60) : (Optional)

DHCP Client ID (option 61) : (Optional)

Specify DNS : ○ Enable ● Disable

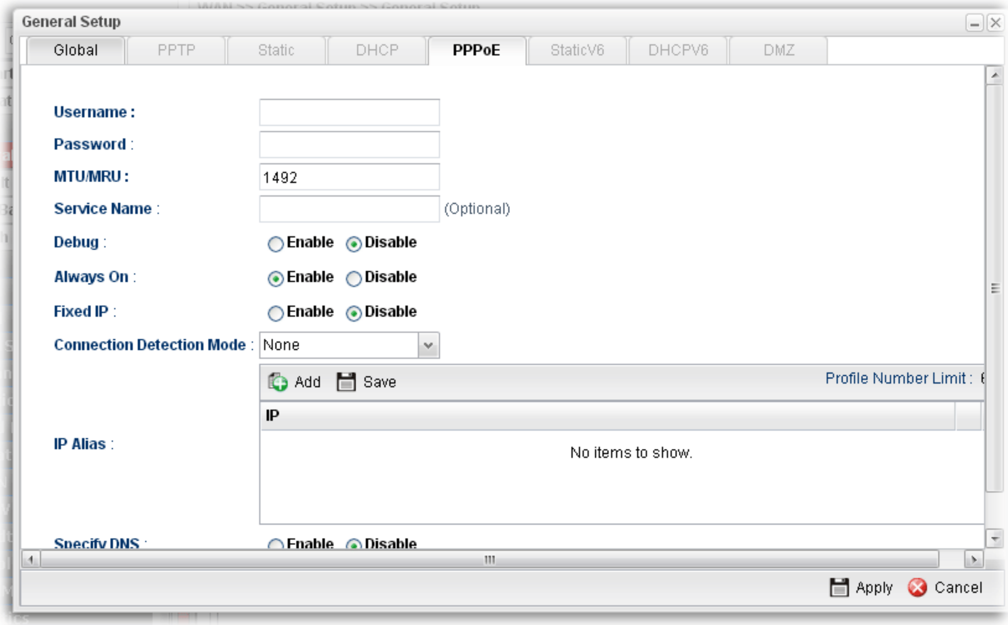
Available parameters are listed as follows:

Item	Description
Host Name (Optional)	Type a name as the host name for identification.
IP Alias	Type other IP addresses to be bound to this interface. This

	setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – To add a new IP address, click **Add.** Type the IP address and use the drop down list to specify the subnet mask. Next, click **Save**. The new one will be added and displayed on the field under the box.  192.168.1.85 **Save –** click this button to save the setting. 🗑 – click the icon to remove the selected entry.
MTU/MRU	It means Max Transmit Unit for packet. The default setting is 1500.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are three ways **ARP**, **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**. **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.  Connection Detection Mode : PING Connection Detection Host : 192.168.1.28 **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN

	interface will be regarded as breaking down.
Vendor Class ID (option 60)	It is used to identify the vendor type and the configuration of a DHCP client.
DHCP Client ID (option 61)	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	**Enable** – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. **Disable** – Click it to disable the function of DNS specified.
DNS	**Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



Username :

Password :

MTU/MRU : 1492

Service Name : (Optional)

Debug : ○ Enable ● Disable

Always On : ● Enable ○ Disable

Fixed IP : ○ Enable ● Disable

Connection Detection Mode : None

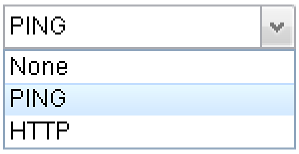
IP Alias : Add Save Profile Number Limit : 6

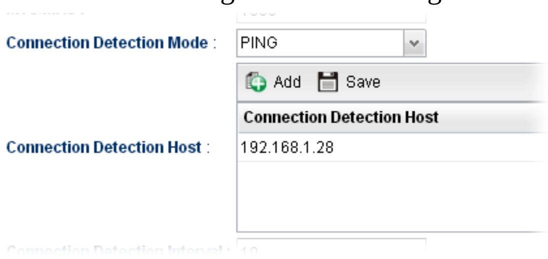
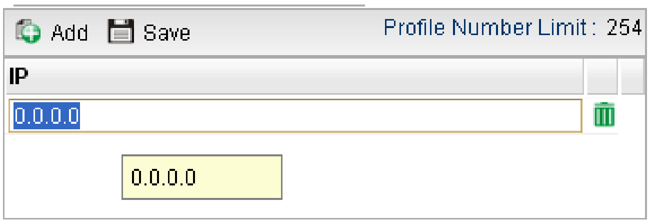
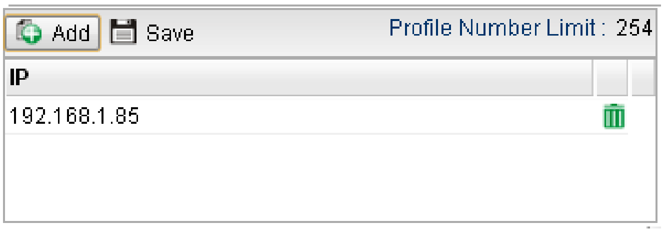
IP

No items to show.

Specify DNS : ○ Enable ● Disable

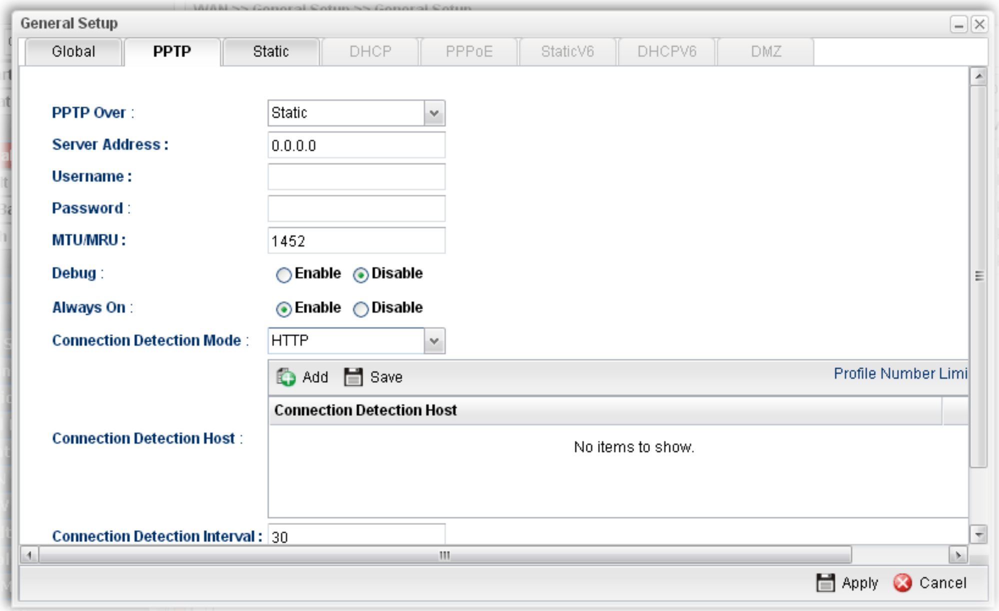
Available parameters are listed as follows:

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.  PING None PING HTTP
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field. Use the default setting.

	Add – Click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down.  Connection Detection Mode : PING Connection Detection Host Connection Detection Host : 192.168.1.28 **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. **Add** – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny boxes one by one.  Profile Number Limit : 254 IP 0.0.0.0 0.0.0.0 **Save** – After finished the IP address configuration, click **Save** to save the setting onto the router.  Profile Number Limit : 254 IP 192.168.1.85 🗑 – Click the icon to remove the selected entry.
Specify DNS	**Enable** – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. **Disable** – Click it to disable the function of DNS specified.

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

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



General Setup

Global | PPTP | Static | DHCP | PPPoE | StaticV6 | DHCPV6 | DMZ

PPTP Over : Static

Server Address : 0.0.0.0

Username :

Password :

MTU/MRU : 1452

Debug : ○ Enable ● Disable

Always On : ● Enable ○ Disable

Connection Detection Mode : HTTP

Connection Detection Host : Add | Save | Profile Number Limi

Connection Detection Host

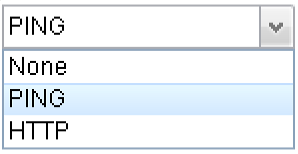
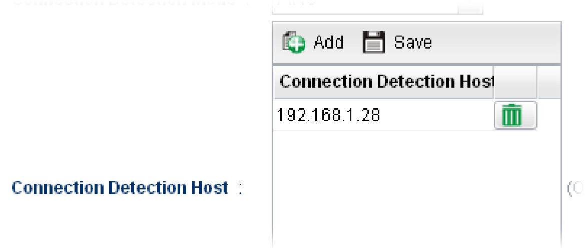
No items to show.

Connection Detection Interval : 30

Apply | Cancel

Available parameters are listed as follows:

Item	Description
PPTP Over	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. **Please contact your ISP before you want to use this function.** Choose a proper protocol, **Static** or **DHCP**. After finished the settings in such page, you need to open the Static or DHCP tab for configuring the settings there.
Server Address	Type the IP address of PPTP server offered by your ISP.
Username	Type the user name offered by your ISP.
Password	Type the password offered by your ISP.
MTU/MRU	Type the value of MTU/MRU. The default value is 1452.
Debug	Click **Enable** to display the PPTP debug message in syslog. The default setting is **Disable**.
Always On	**Enable** – Click it to enable the function of Always On. The

	router will keep network connection all the time. **Disable** – Click it to disable the function of Always On.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field. Use the default setting. **Add** – Click this button to have a field for adding a new IP address. Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down.  Add Save Connection Detection Host Connection Detection Host : 192.168.1.28 **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Apply	After finished the PPTP configuration, please click **Static** or **DHCP** (according to the PPTP Over Protocol setting) to modify the Static/DHCP configuration for such profile. Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

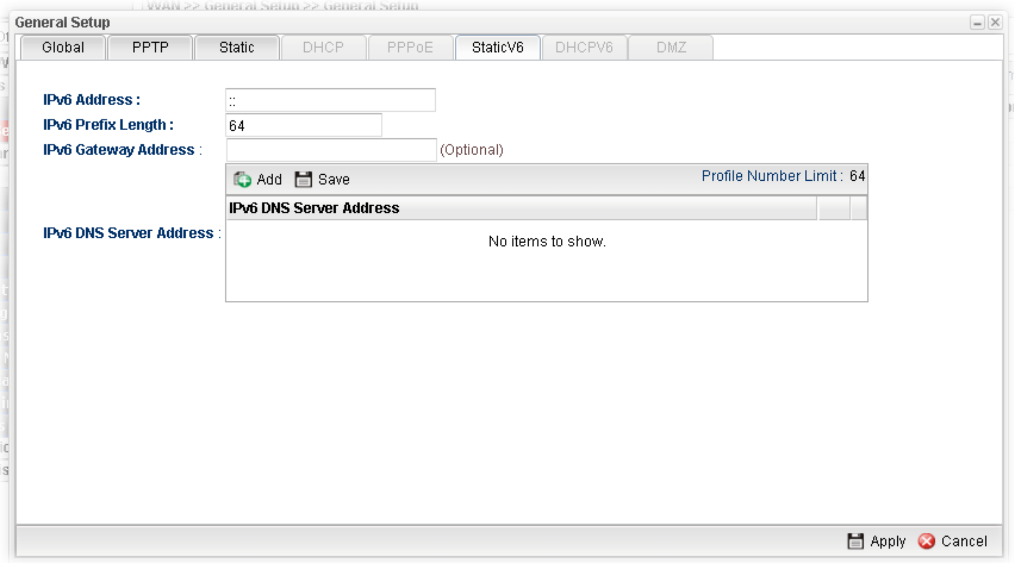
- ***If you choose Link-Local as IPv6 protocol type***

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

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

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

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



IPv6 Address : ::

IPv6 Prefix Length : 64

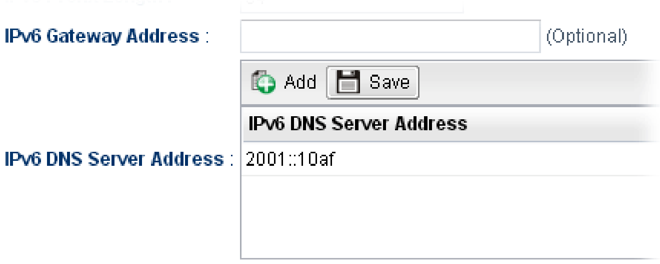
IPv6 Gateway Address : (Optional)

Profile Number Limit : 64

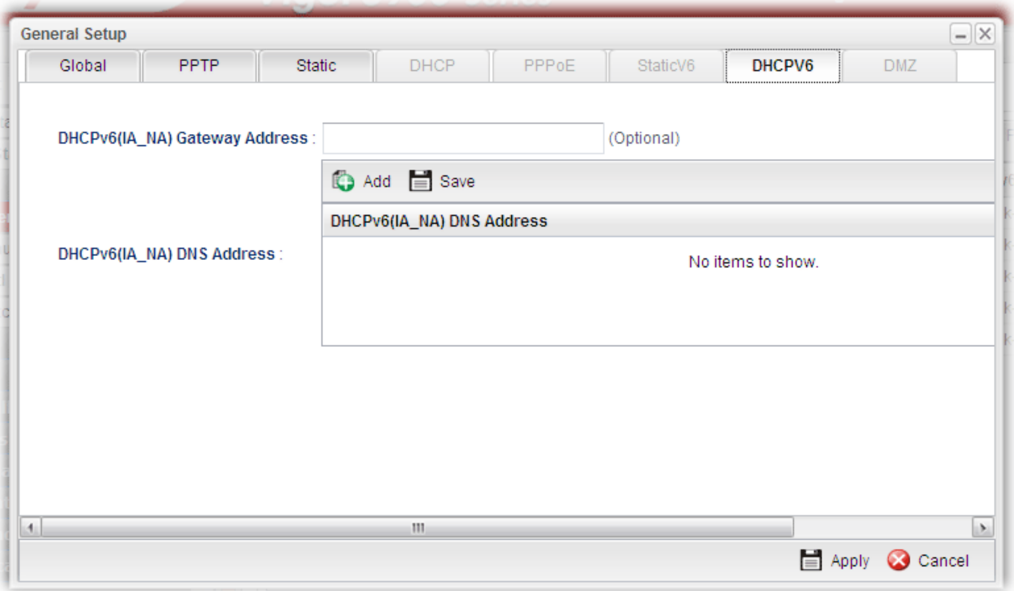
IPv6 DNS Server Address :

IPv6 DNS Server Address
No items to show.

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.  IPv6 Gateway Address : (Optional) IPv6 DNS Server Address : 2001::10af **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



General Setup

Global | PPTP | Static | DHCP | PPPoE | StaticV6 | DHCPV6 | DMZ

DHCPv6(IA_NA) Gateway Address : (Optional)

DHCPv6(IA_NA) DNS Address :

Add Save

DHCPv6(IA_NA) DNS Address

No items to show.

Apply Cancel

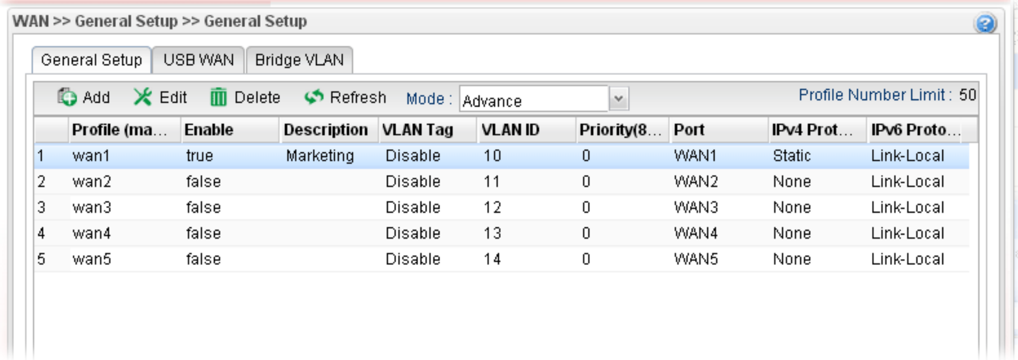
Available parameters are listed as follows:

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.

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



WAN >> General Setup >> General Setup

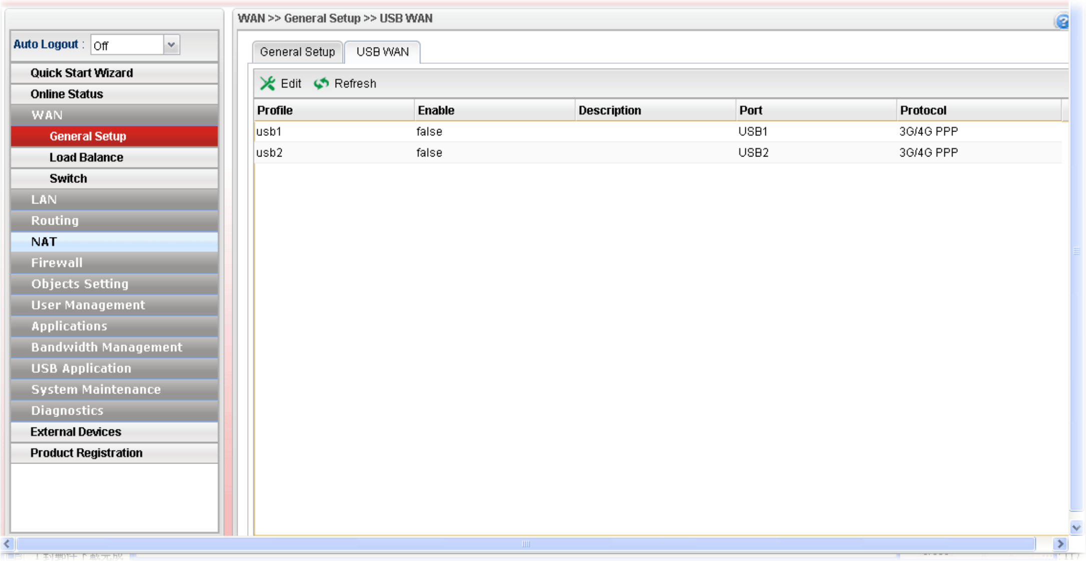
General Setup | USB WAN | Bridge VLAN

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

	Profile (ma...	Enable	Description	VLAN Tag	VLAN ID	Priority(8...	Port	IPv4 Prot...	IPv6 Proto...
1	wan1	true	Marketing	Disable	10	0	WAN1	Static	Link-Local
2	wan2	false		Disable	11	0	WAN2	None	Link-Local
3	wan3	false		Disable	12	0	WAN3	None	Link-Local
4	wan4	false		Disable	13	0	WAN4	None	Link-Local
5	wan5	false		Disable	14	0	WAN5	None	Link-Local

4.1.1.2 USB WAN Profiles

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



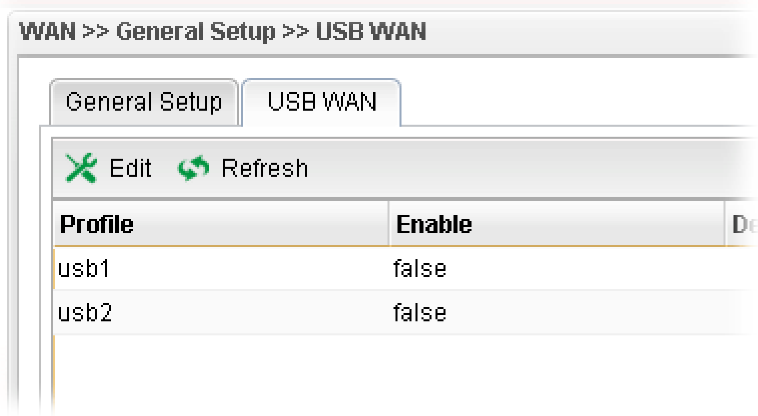
Profile	Enable	Description	Port	Protocol
usb1	false		USB1	3G/4G PPP
usb2	false		USB2	3G/4G PPP

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 USB WAN profile

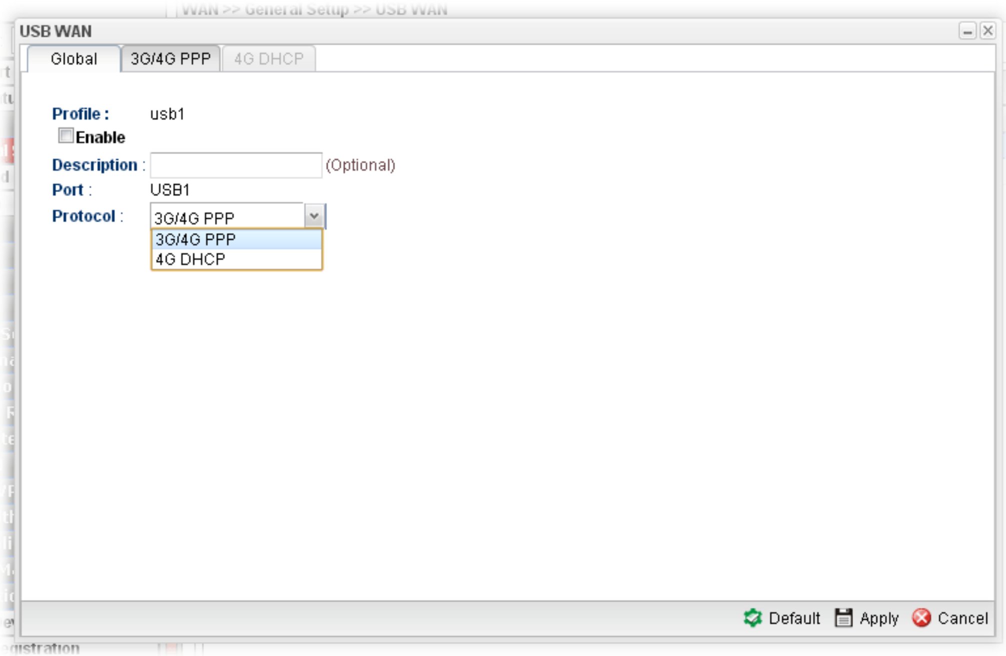
1. Choose one of the USB WAN profiles and click **Edit**.



WAN >> General Setup >> USB WAN

Profile	Enable
usb1	false
usb2	false

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



USB WAN

Profile : usb1

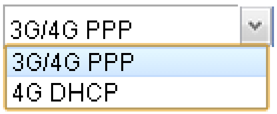
□ Enable

Description : (Optional)

Port : USB1

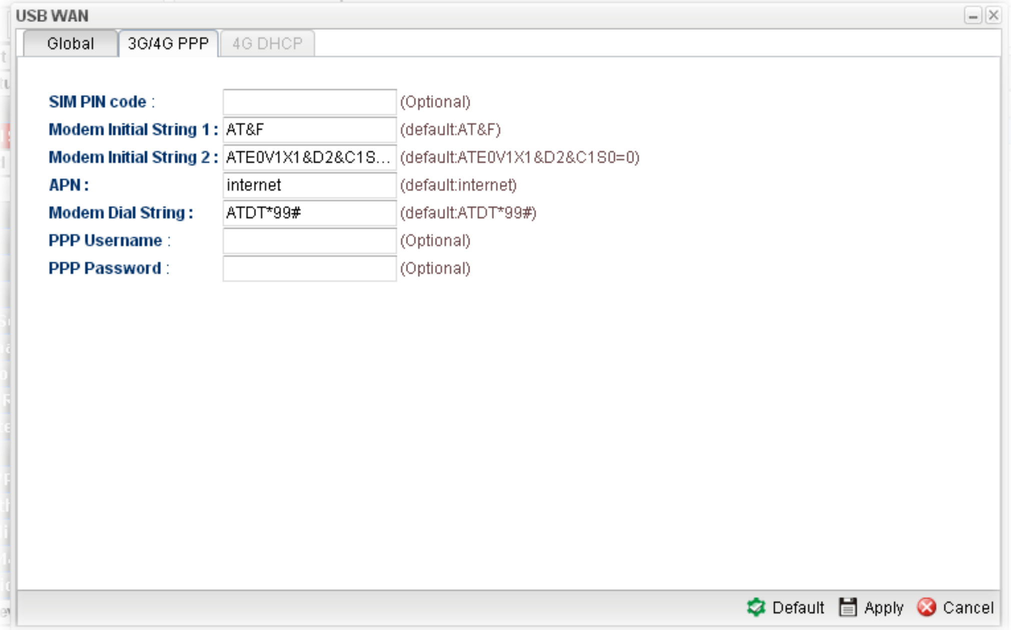
Protocol : 3G/4G PPP

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. 

Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

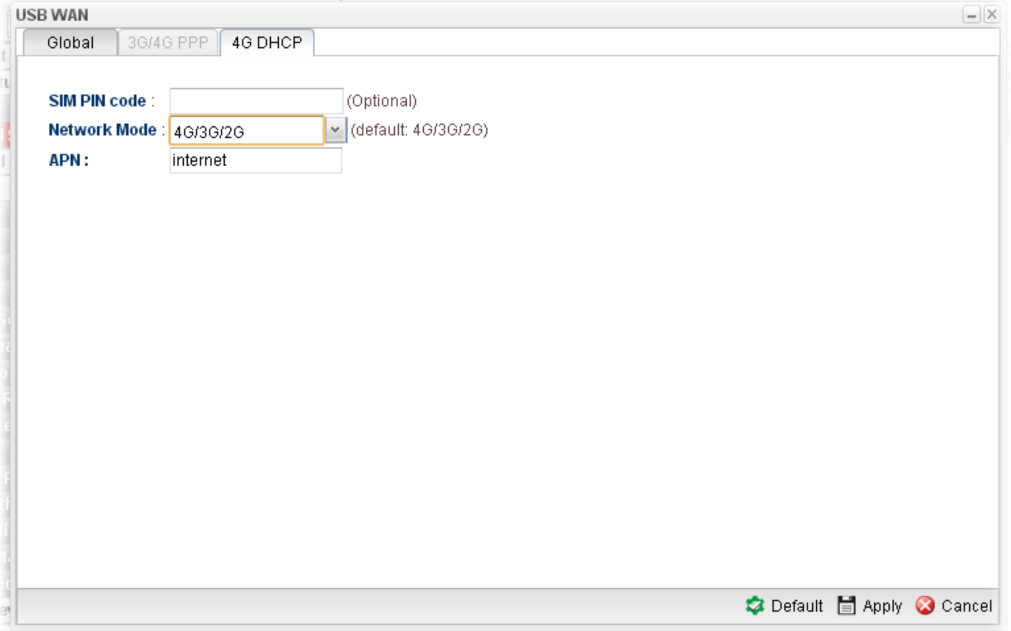
3. After finished the settings above, click the 3G/4G PPP or 4G DHCP tab (based on the Protocol specified) to display the following page:



USB WAN

SIM PIN code : (Optional)
Modem Initial String 1 : AT&F (default:AT&F)
Modem Initial String 2 : ATE0V1X1&D2&C1S... (default:ATE0V1X1&D2&C1S0=0)
APN : internet (default:internet)
Modem Dial String : ATDT*99# (default:ATDT*99#)
PPP Username : (Optional)
PPP Password : (Optional)

Or,

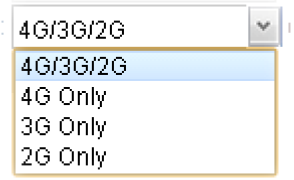


USB WAN

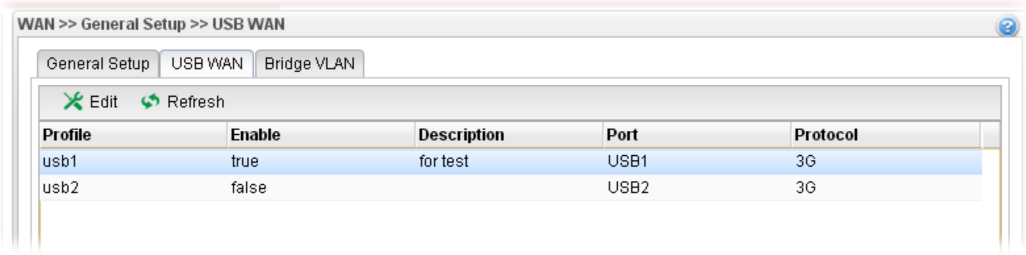
SIM PIN code : (Optional)
Network Mode : 4G/3G/2G (default: 4G/3G/2G)
APN : internet

Available parameters are listed as follows:

Item	Description

3G/4G PPP	**SIM PIN code -**Type PIN code of the SIM card that will be used to access Internet. **Modem Initial String 1**-Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. **Modem Initial String 2**-The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. **APN -**APN means Access Point Name which is provided and required by some ISPs. Type the name. **Modem Dial String** -Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. **PPP Username -**Type the PPP username (optional). **PPP Password -**Type the PPP password (optional).
4G DHCP	**SIM Pin code** –Type PIN code of the SIM card that will be used to access Internet. **Network Mode** – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.  **APN Name** – APN means Access Point Name which is provided and required by some ISPs.
Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

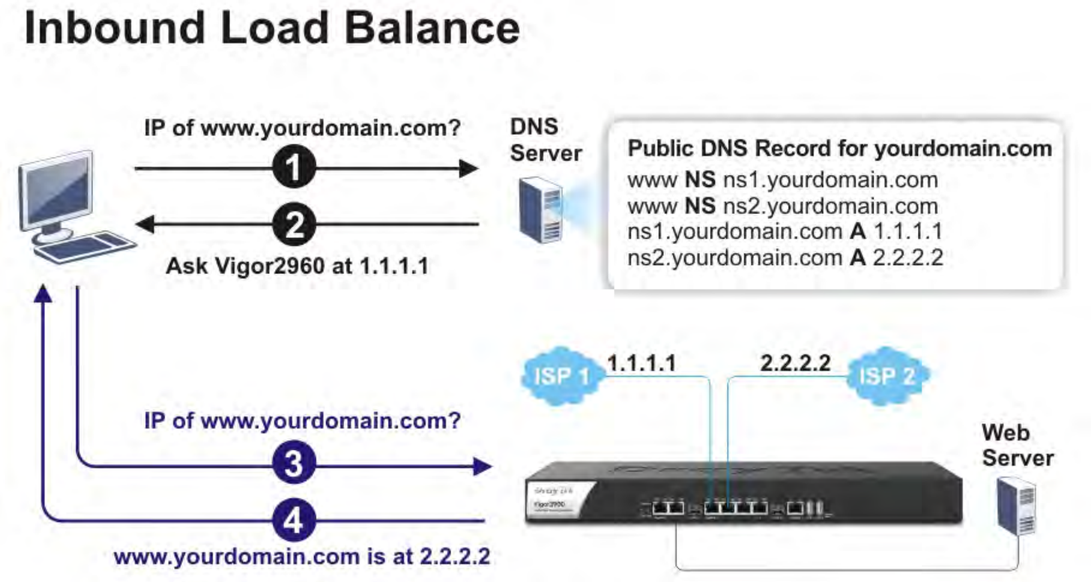
4. Enter all the settings and click **Apply**. The modified profile will be shown as below.



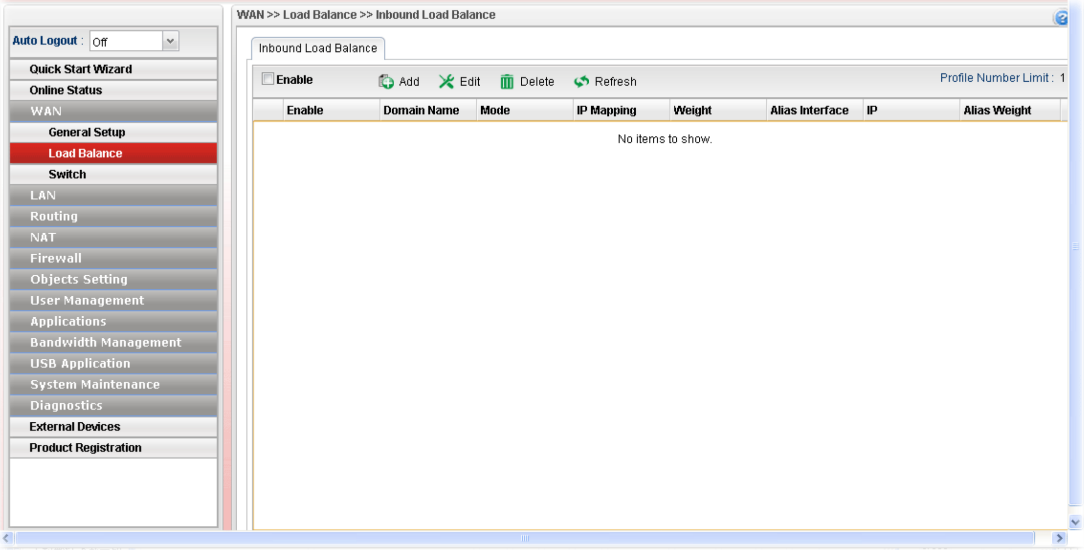
Profile	Enable	Description	Port	Protocol
usb1	true	for test	USB1	3G
usb2	false		USB2	3G

4.1.2 Inbound Load Balance

Vigor300B 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
IP of www.yourdomain.com?
1
2
Ask Vigor2960 at 1.1.1.1
DNS Server
Public DNS Record for yourdomain.com
www NS ns1.yourdomain.com
www NS ns2.yourdomain.com
ns1.yourdomain.com A 1.1.1.1
ns2.yourdomain.com A 2.2.2.2
ISP 1
1.1.1.1
2.2.2.2
ISP 2
IP of www.yourdomain.com?
3
4
www.yourdomain.com is at 2.2.2.2
Web Server

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



□ Enable

Profile Number Limit : 1

Enable	Domain Name	Mode	IP Mapping	Weight	Alias Interface	IP	Alias Weight

No items to show.

Each item will be explained as follows:

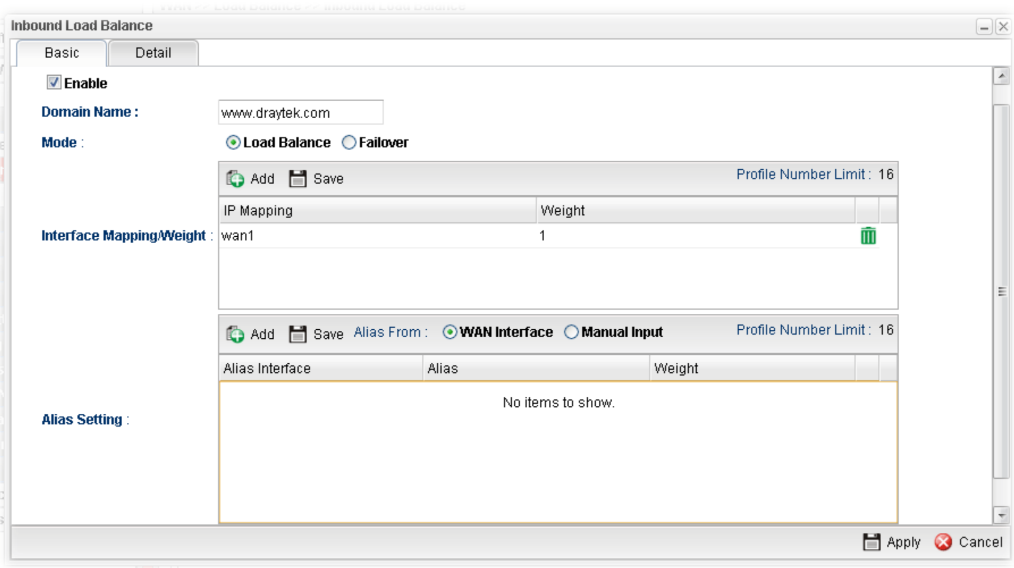
Item	Description
Enable	Check the box the enable inbound load balance function.
Add	Add a new WAN profile for inbound load balance.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify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



Inbound Load Balance

Basic | Detail

☑ Enable

Domain Name : www.draytek.com

Mode : ● Load Balance ○ Failover

Interface Mapping/Weight :

Add Save Profile Number Limit : 16

IP Mapping	Weight
wan1	1

Alias Setting :

Add Save Alias From : ● WAN Interface ○ Manual Input Profile Number Limit : 16

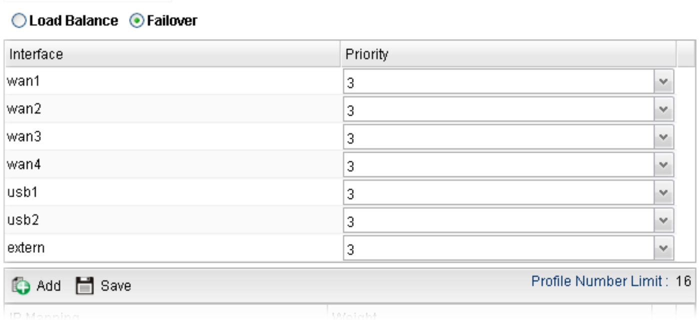
Alias Interface	Alias	Weight

No items to show.

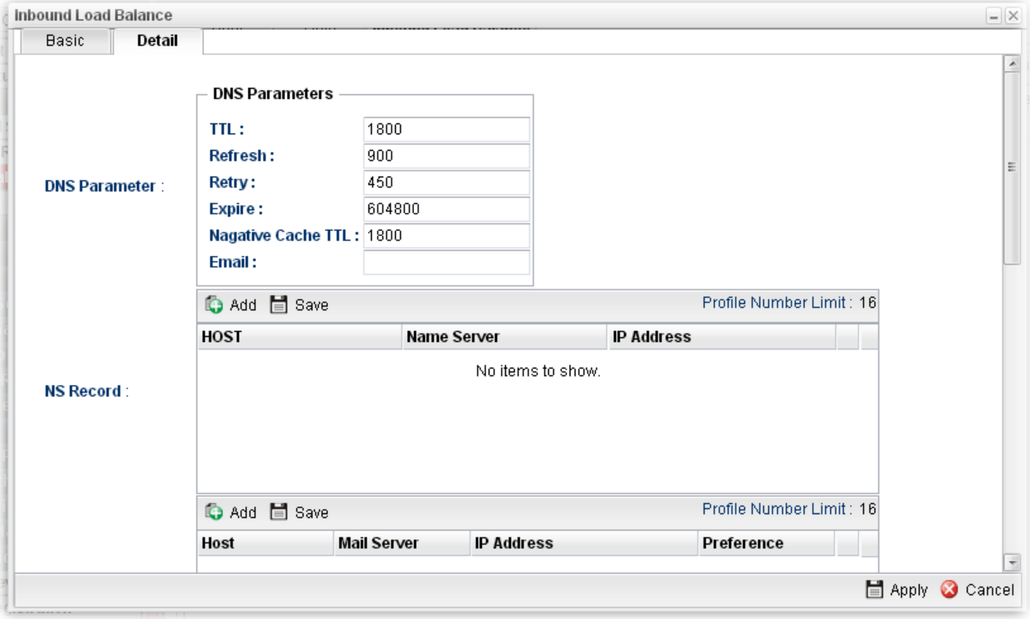
Apply Cancel

Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
Domain Name	Type an available domain name to serve the inbound load balance.

<table>
<tr><td><b>Mode</b></td><td>Specify the type (Load Balance or Failover) of the WAN profile for inbound load balance</td></tr>
<tr><td><b>Priority Setting</b></td><td>It is available only when <b>Failover</b> is selected as the Mode.
There are five levels (Top, 2, 3, 4 and 5) which can be specified for WAN profiles (including default WAN profiles and user-defined WAN profiles).

○ Load Balance ● Failover
<table>
<tr><th>Interface</th><th>Priority</th></tr>
<tr><td>wan1</td><td>3</td></tr>
<tr><td>wan2</td><td>3</td></tr>
<tr><td>wan3</td><td>3</td></tr>
<tr><td>wan4</td><td>3</td></tr>
<tr><td>usb1</td><td>3</td></tr>
<tr><td>usb2</td><td>3</td></tr>
<tr><td>extern</td><td>3</td></tr>
</table>
</td></tr>
<tr><td><b>Interface Mapping/Weight</b></td><td>The domain name will inform the remote end with the IP address for DNS query asked by the remote end.
The incoming query from the WAN interfaces specified in IP Mapping will be processed according to the weight value.
<b>Add</b> – Click it to choose a WAN interface and weight.
<b>Save</b> – Click it to save the settings.
<b>IP Mapping</b> – Use the drop down list to choose a WAN interface profile which will be used by the domain.
<b>Weight</b> – Use the drop down list to choose the one you want.</td></tr>
<tr><td><b>Alias Setting</b></td><td>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.
<b>Add</b> – Click it to add a new IP address.
<b>Save</b> – Click it to save the settings.
<b>Alias From WAN Interface</b> – The alias IP setting can be specified from existed WAN IP alias.
<b>Alias From Manual Input</b> – The alias IP setting can be specified manually. The Alias Interface is not necessary for such method.
<b>Alias Interface</b> –Use the drop down list to choose a WAN interface profile for the alias IP setting.
<b>Alias</b> – Use the drop down list to choose an alias IP setting (for <b>Alias From WAN Interface</b>) or type an IP address manually (for <b>Alias From Manual Input</b>).
<b>Weight</b> –Use the drop down list to choose the one you want.</td></tr>
</table>

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



DNS Parameter :

DNS Parameters

TTL :	1800
Refresh :	900
Retry :	450
Expire :	604800
Nagative Cache TTL :	1800
Email :	

NS Record :

Profile Number Limit : 16

HOST	Name Server	IP Address

No items to show.

Profile Number Limit : 16

Host	Mail Server	IP Address	Preference

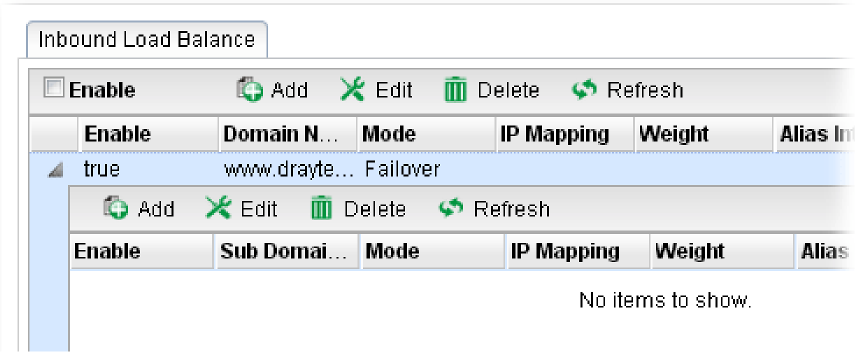
Available parameters are listed as follows:

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

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

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

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



Enable	Domain N...	Mode	IP Mapping	Weight	Alias In
true	www.drayte...	Failover			

Enable	Sub Domai...	Mode	IP Mapping	Weight	Alias

No items to show.

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

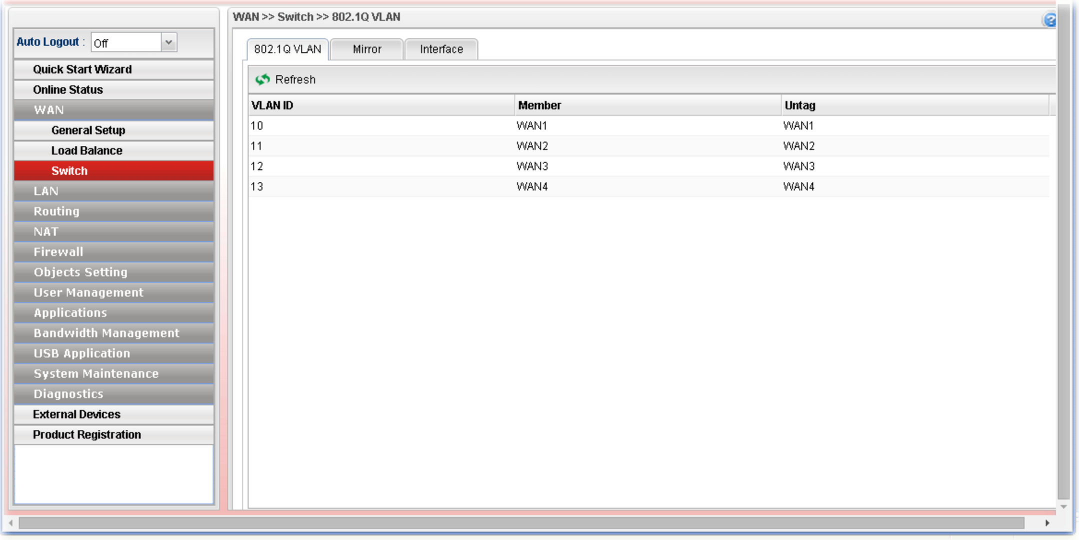
4.1.3 Switch

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.



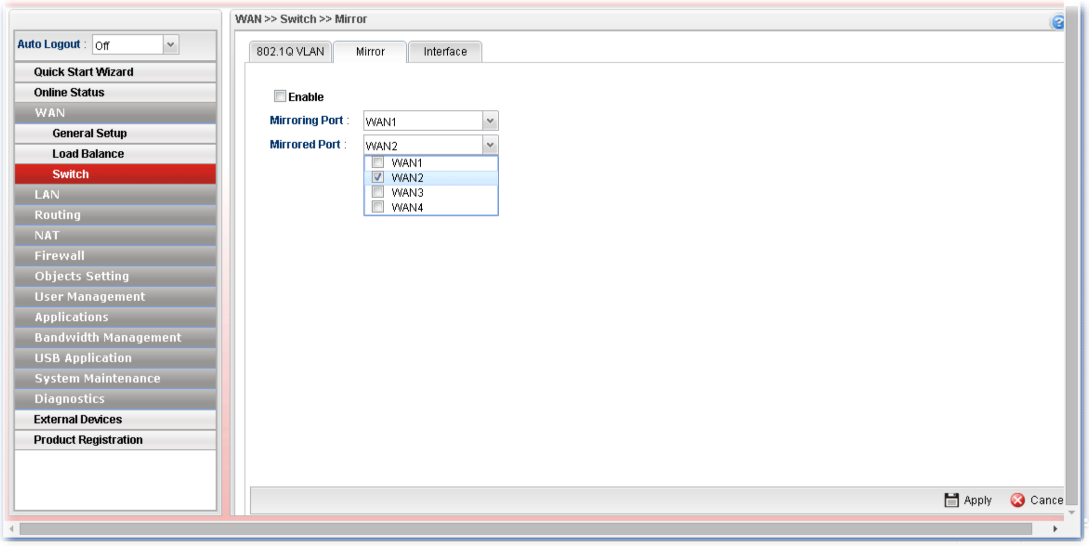
VLAN ID	Member	Untag
10	WAN1	WAN1
11	WAN2	WAN2
12	WAN3	WAN3
13	WAN4	WAN4

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.



□ Enable

Mirroring Port : WAN1

Mirrored Port : WAN2

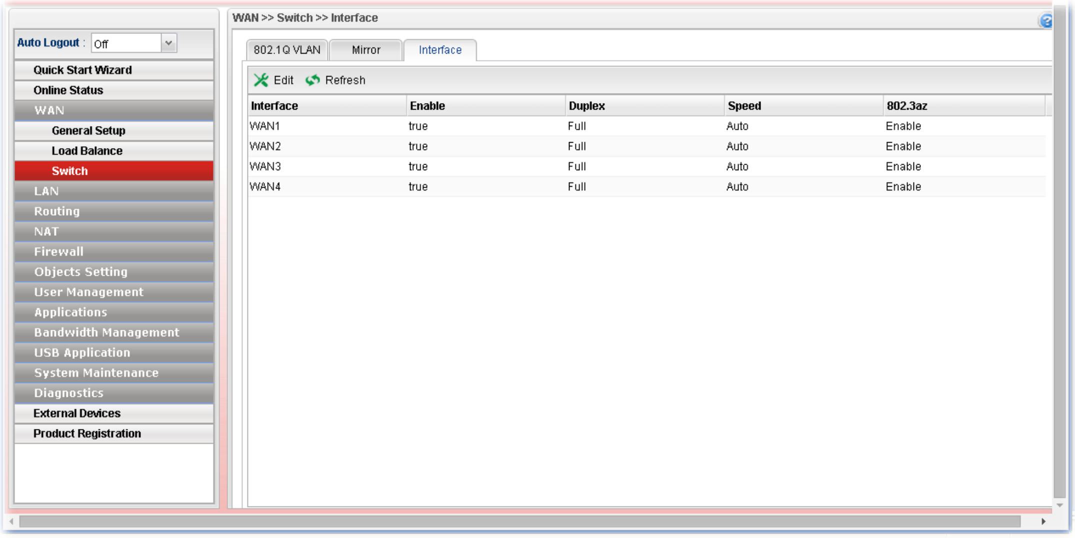
□ WAN1
☑ WAN2
□ WAN3
□ WAN4

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.

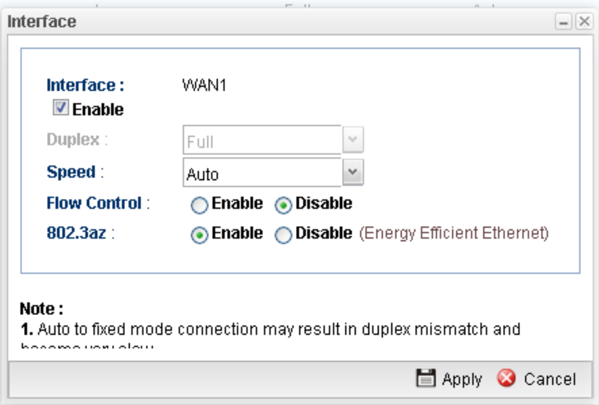
4.1.3.3 Interface Configuration

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



Interface	Enable	Duplex	Speed	802.3az
WAN1	true	Full	Auto	Enable
WAN2	true	Full	Auto	Enable
WAN3	true	Full	Auto	Enable
WAN4	true	Full	Auto	Enable

Each item will be explained as follows:

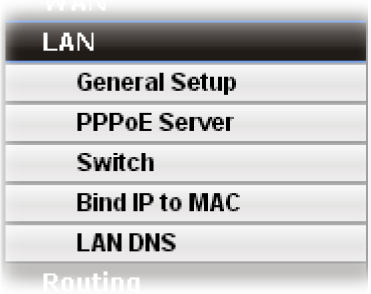
Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.  Interface Interface : WAN1 ☑ Enable Duplex : Full Speed : Auto Flow Control : ○ Enable ● Disable 802.3az : ● Enable ○ Disable (Energy Efficient Ethernet) Note : 1. Auto to fixed mode connection may result in duplex mismatch and become very slow. Apply Cancel **Interface** – Display the name of WAN interface. **Enable** – Check it to enable such interface. **Speed** – Use the drop down list to specify the transmission rate (**Auto, 10M, 100M** or **1000M**) for such interface. **Flow Control** – The default setting is **Disable**. If **Enabled** is clicked, Vigor router will drop the packet if too much to handle. **802.3az –** It is a function of energy-efficient Ethernet. It can detect the network traffic automatically to adjust the power output and let Vigor300B save the energy during the period of low traffic. Click **Enable** to activate the

	power/energy saving function if required. **Apply** – Click it to save and exit the dialog. **Cancel** – Click it to exit the dialog without saving anything.
Refresh	Renew current web page.
Interface	Display the name of the WAN port on the router.
Enable	Display the status of the profile. False means disabled; True means enabled.
Duplex	Display the duplex used (full or half) by such profile.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.
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.



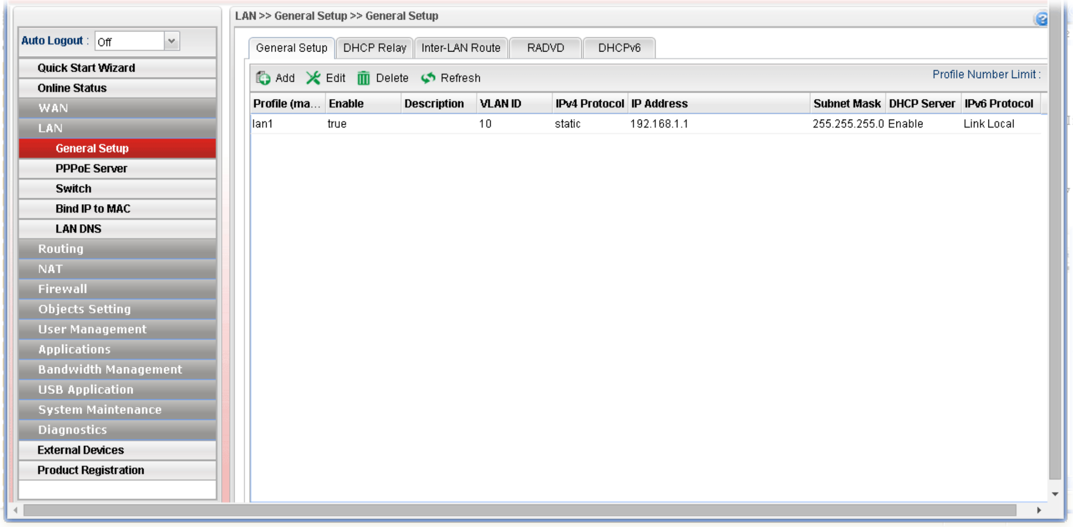
4.2.1 General Setup

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 (ma...	Enable	Description	VLAN ID	IPv4 Protocol	IP Address	Subnet Mask	DHCP Server	IPv6 Protocol
lan1	true		10	static	192.168.1.1	255.255.255.0	Enable	Link Local

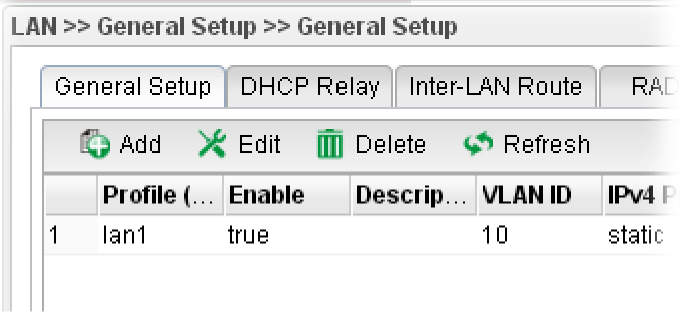
Each item will be explained as follows:

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.

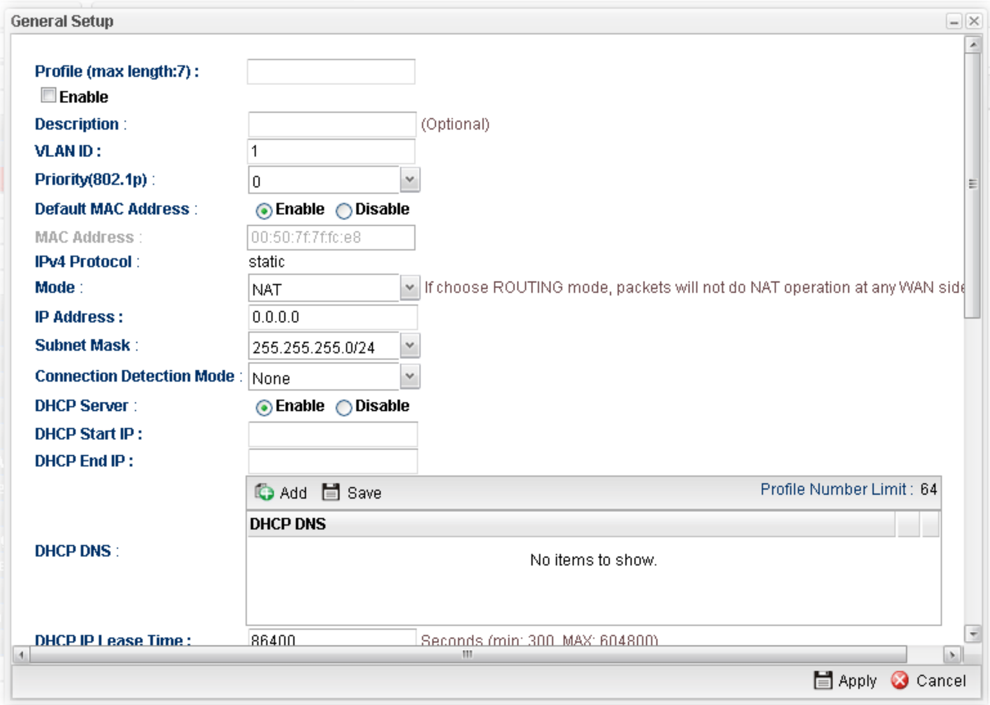
How to add a new LAN profile

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



	Profile (...	Enable	Descrip...	VLAN ID	IPv4 P
1	lan1	true		10	static

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



General Setup

Profile (max length:7) :

□ Enable

Description : (Optional)

VLAN ID : 1

Priority(802.1p) : 0

Default MAC Address : ● Enable ○ Disable

MAC Address : 00:50:7f:7f:fc:e8

IPv4 Protocol : static

Mode : NAT If choose ROUTING mode, packets will not do NAT operation at any WAN side

IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0/24

Connection Detection Mode : None

DHCP Server : ● Enable ○ Disable

DHCP Start IP :

DHCP End IP :

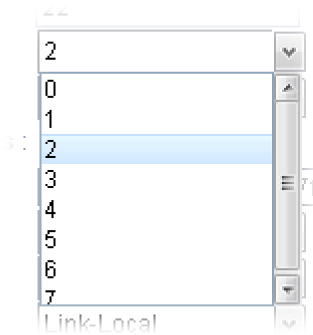
DHCP DNS :

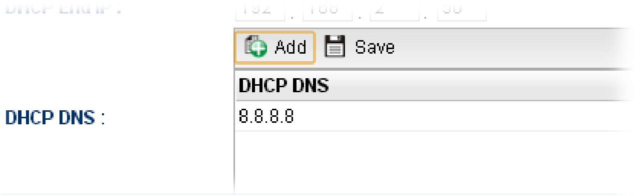
DHCP DNS
No items to show.

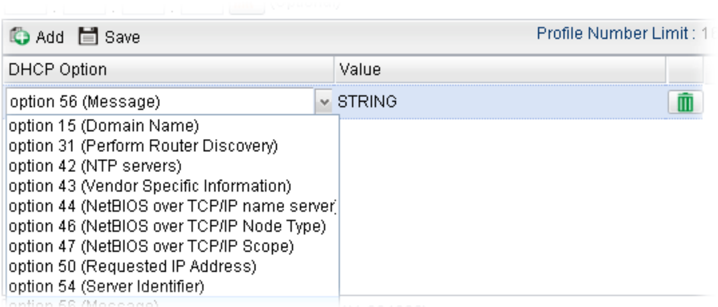
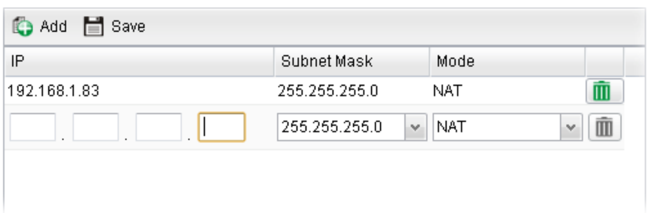
Profile Number Limit : 64

DHCP IP Lease Time : 86400 Seconds (min: 300, MAX: 604800)

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.  2 0 1 2 3 4 5 6 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 Vigor300B as the DNS server.  DHCP DNS : DHCP DNS 8.8.8.8 **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting.

DHCP IP Lease Time	Set a lease time for the DHCP server. The time unit is minute.
DHCP Routers	In general, this box will be blank. It means Vigor300B will be regarded as the gateway for the user. However, if you want to use other gateway, please assign the IP address in this field.
DHCP Next Server	Type the IP address of the secondary DHCP server.
DHCP Options	DHCP packets can be processed by adding option number and data information when such function is enabled. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.  Add Save Profile Number Limit : 1 DHCP Option Value option 56 (Message) STRING option 15 (Domain Name) option 31 (Perform Router Discovery) option 42 (NTP servers) option 43 (Vendor Specific Information) option 44 (NetBIOS over TCP/IP name server option 46 (NetBIOS over TCP/IP Node Type) option 47 (NetBIOS over TCP/IP Scope) option 50 (Requested IP Address) option 54 (Server Identifier) option 56 (Message) **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.
More Subnet	Different subnets can be created under one LAN profile. Specify other subnets which might be needed in the future.  IP / Subnet Mask / Mode 192.168.1.83 / 255.255.255.0 / NAT . . . / 255.255.255.0 / NAT **Add** – Click it to add a new subnet mask with IP address and specified mode. **Save** – Click it to save the settings. **IP** – Type the IP address if you click Add for adding a new entry. **Subnet Mask** – Use the drop down list to choose the one you want. **Mode** – Specify NAT or Routing as the mode. **DHCP** – Click **Enable** to activate the DHCP function on such

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

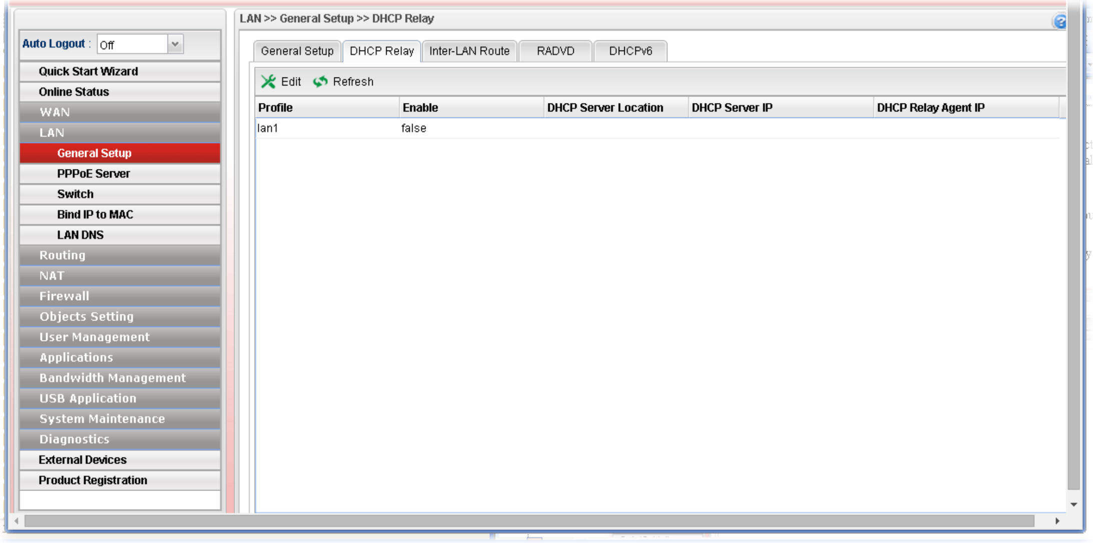
3. When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.

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.



LAN >> General Setup >> DHCP Relay

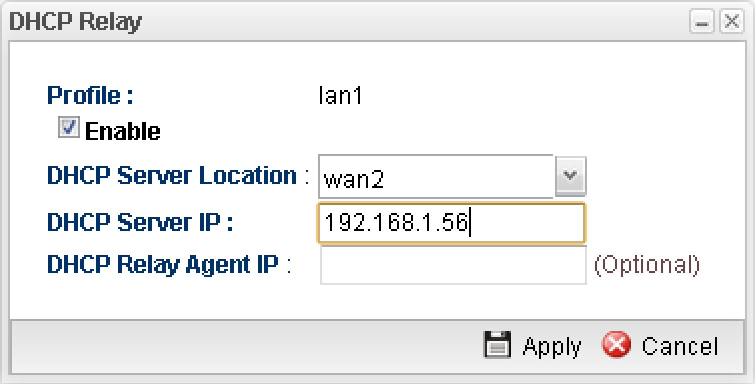
Profile	Enable	DHCP Server Location	DHCP Server IP	DHCP Relay Agent IP
lan1	false			

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.


DHCP Relay

Profile : lan1

☑ Enable

DHCP Server Location : wan2

DHCP Server IP : 192.168.1.56

DHCP Relay Agent IP : (Optional)

Available parameters are listed as follows:

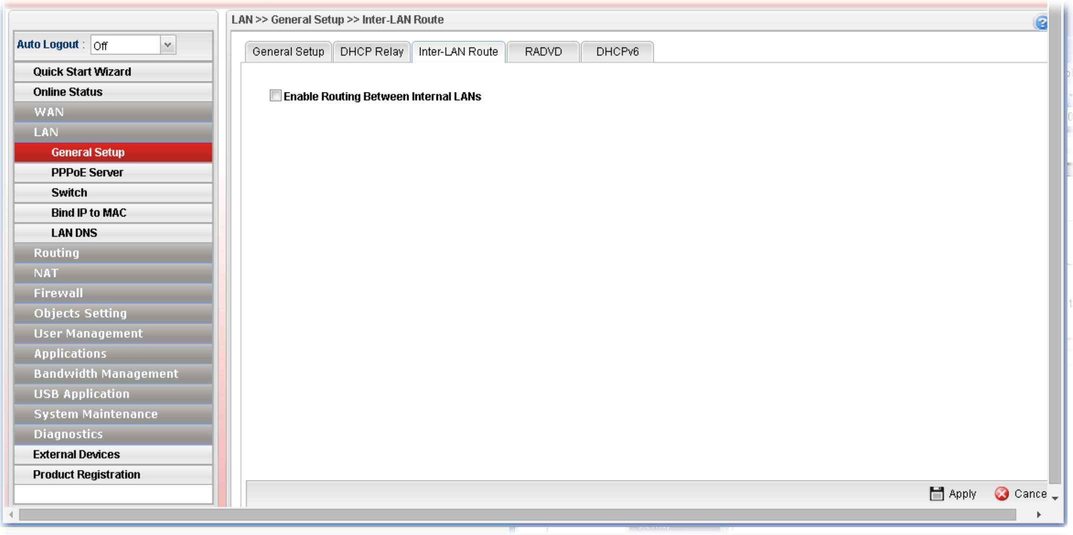
Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
DHCP Server Location	Choose the interface for the DHCP server.
DHCP Server IP	Type the IP address of DHCP Server.
DHCP Relay Agent IP	Type the IP address of DHCP Relay Agent.
Apply	Click it to 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

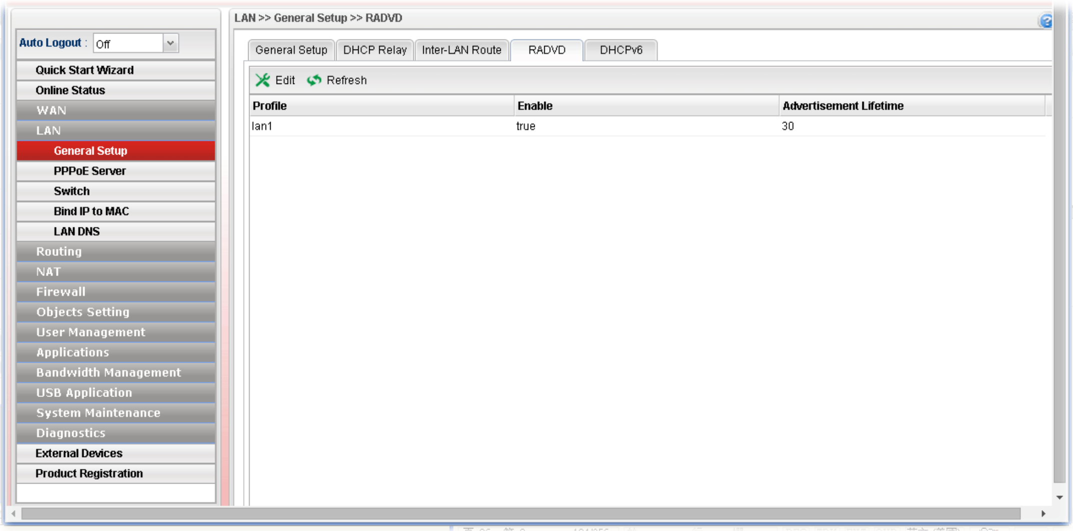
To make the users in different LAN communicating with each other, please check the box to enable Inter-LAN route function.



□ Enable Routing Between Internal LANs

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.



LAN >> General Setup >> RADVD

Profile	Enable	Advertisement Lifetime
lan1	true	30

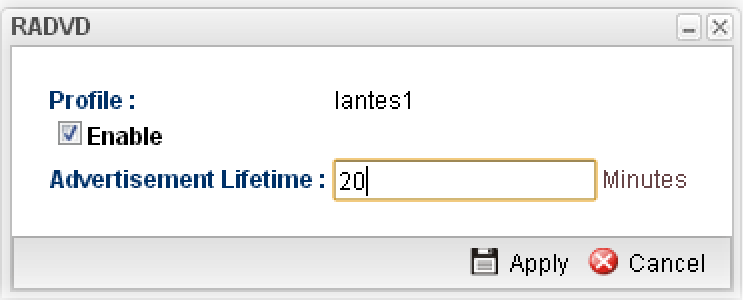
Each item will be explained as follows:

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.



RADVD

Profile : lantes1

☑ Enable

Advertisement Lifetime : 20 Minutes

Available parameters are listed as follows:

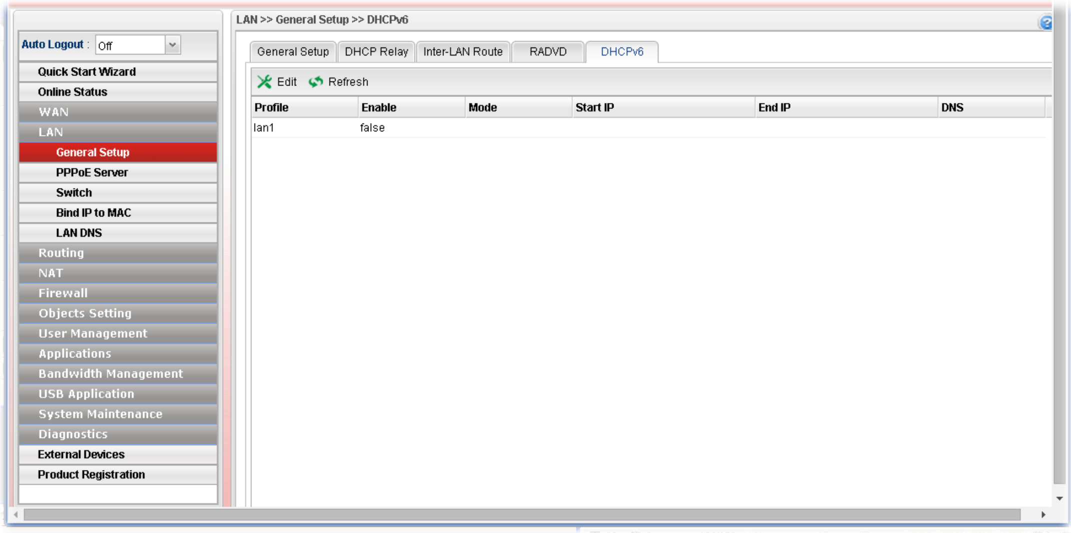
Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
Advertisement Lifetime	Type a value for advertisement lifetime. The lifetime associated with the default router in units of minutes, ranging from 10 ~ 150. It is used to control the lifetime of 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.



LAN >> General Setup >> DHCPv6

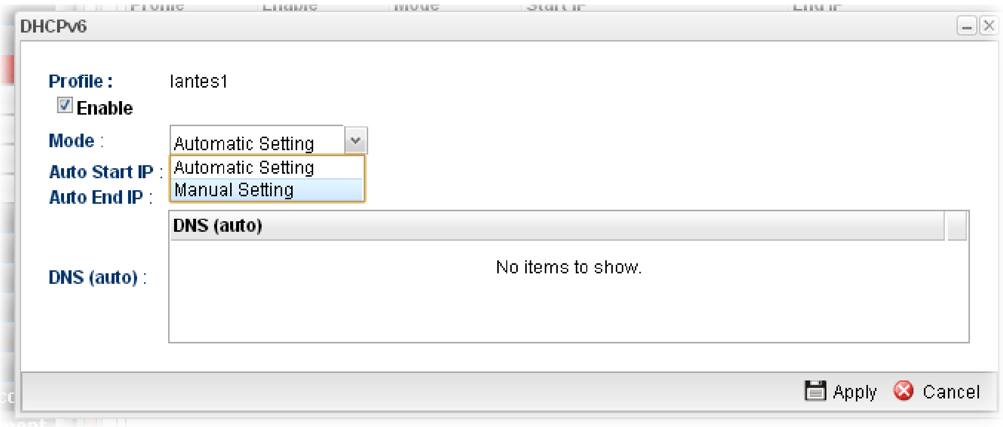
Profile	Enable	Mode	Start IP	End IP	DNS
lan1	false				

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.



Profile : lantes1

☑ Enable

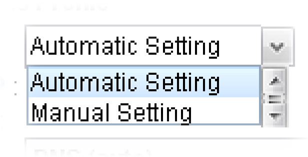
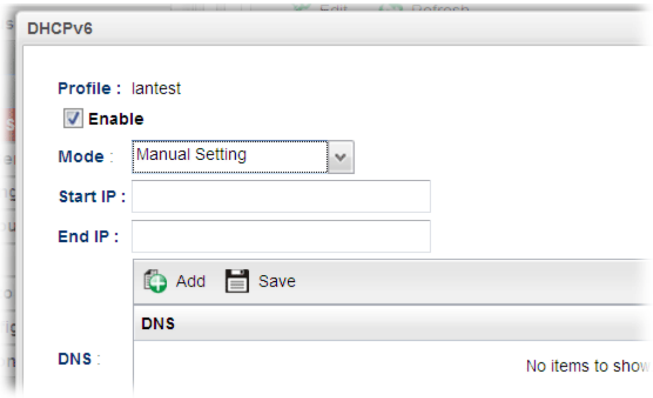
Mode : Automatic Setting

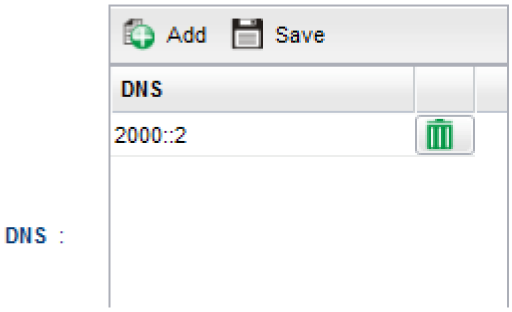
Auto Start IP :

Auto End IP :

DNS (auto) : No items to show.

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
Mode	Choose **Automatic Setting** or **Manual Setting**.  **Automatic Setting** – It is not necessary to configure Start IP, End IP and DNS setting. The system will assign suitable address automatically. **Manual Setting** – You should type the Start IP address and End IP address manually.  Profile : lantest ☑ Enable Mode : Manual Setting Start IP : End IP : DNS : No items to show
Start IP	Set the starting IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.

End IP	Set the ending IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.
DNS	It is available when **Manual Setting** is selected as **Mode**. Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor300B as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

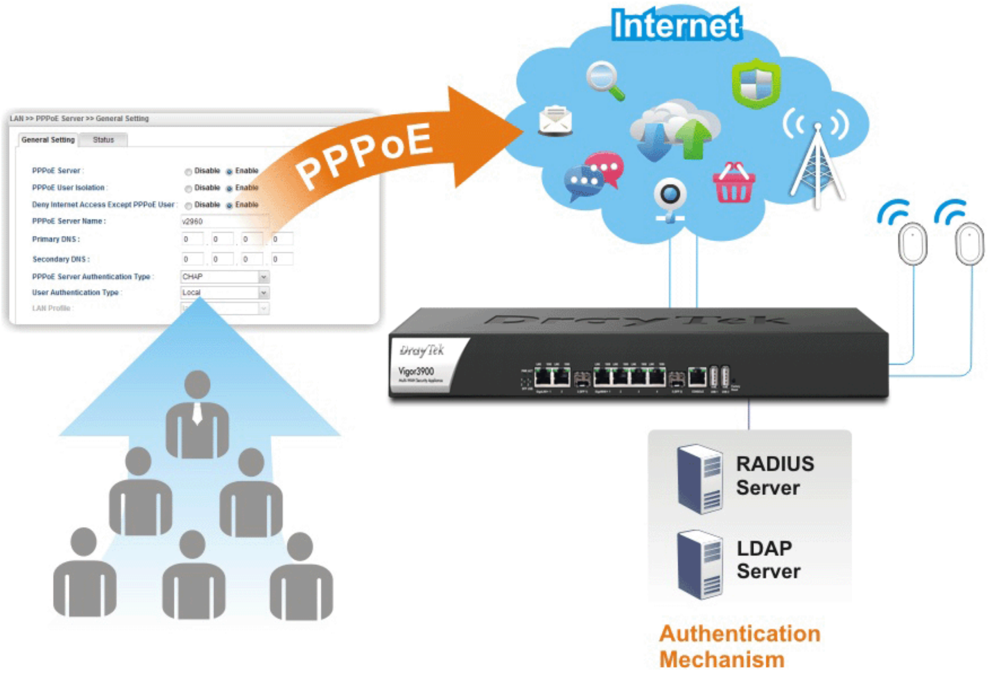
3. When you finish the above settings, please click **Apply** to save the configuration and exit the dialog.

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.



LAN >> PPPoE Server >> General Setting

General Setting | Status

PPPoE Server : ○ Disable ● Enable

PPPoE User Isolation : ○ Disable ● Enable

Deny Internet Access Except PPPoE User : ○ Disable ● Enable

PPPoE Server Name : v2960

Primary DNS : 0 . 0 . 0 . 0

Secondary DNS : 0 . 0 . 0 . 0

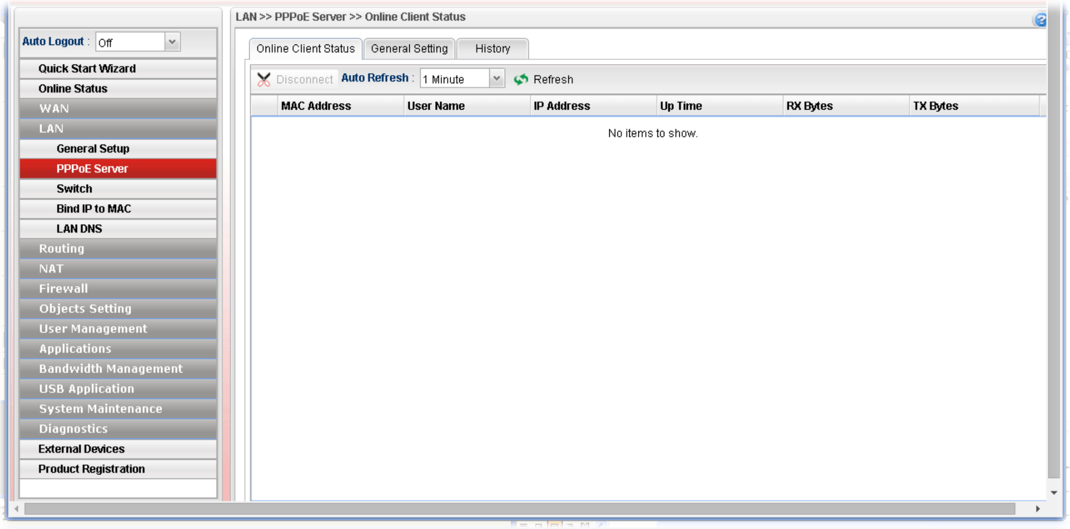
PPPoE Server Authentication Type : CHAP

User Authentication Type : Local

LAN Profile :

4.2.2.1 Online Client Status

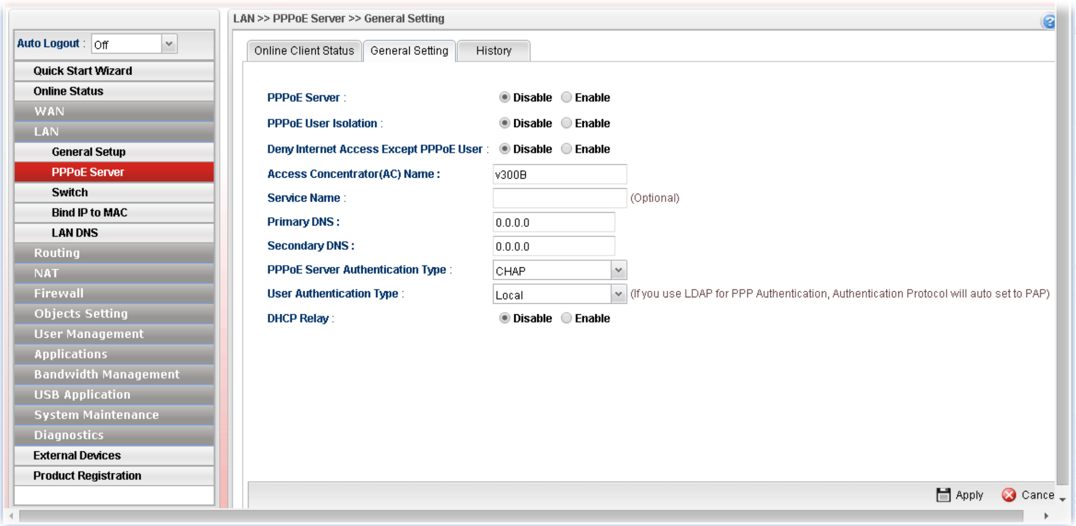
This page displays general information for PPPoE server; allows you to disconnect the network connection to PPPoE server.



Each item will be explained as follows:

Item	**Description**
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.
Refresh	Renew current web page.
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



PPPoE Server : ● Disable ○ Enable

PPPoE User Isolation : ● Disable ○ Enable

Deny Internet Access Except PPPoE User : ● Disable ○ Enable

Access Concentrator(AC) Name : v300B

Service Name : (Optional)

Primary DNS : 0.0.0.0

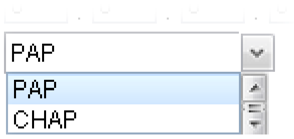
Secondary DNS : 0.0.0.0

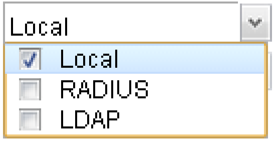
PPPoE Server Authentication Type : CHAP

User Authentication Type : Local (If you use LDAP for PPP Authentication, Authentication Protocol will auto set to PAP)

DHCP Relay : ● Disable ○ Enable

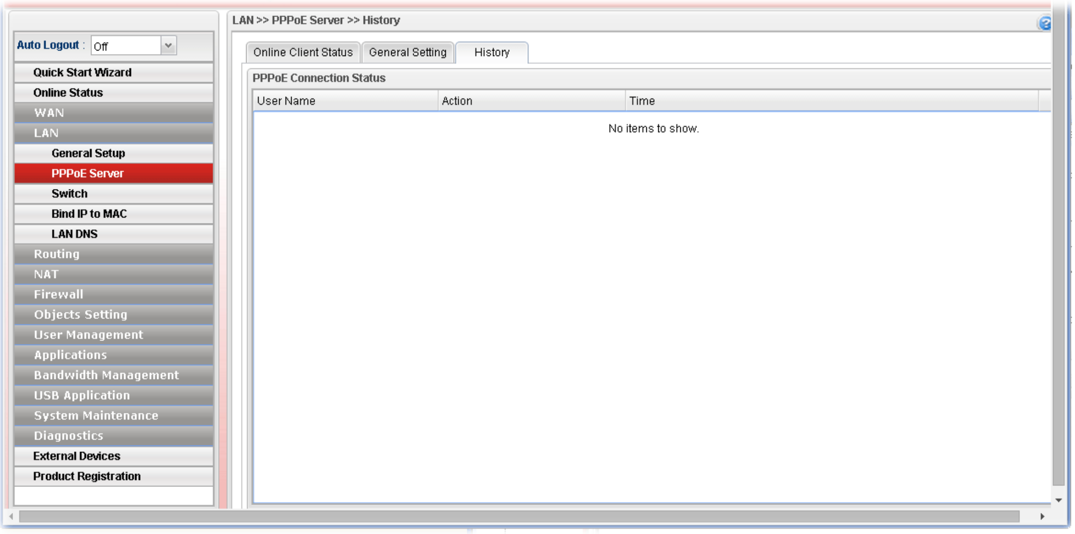
Available parameters are listed as follows:

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	Users in LAN can access into Internet through Vigor router with RADIUS, LDAP or local authentication. Specify the type for the users.

	 Local ☑ Local □ RADIUS □ LDAP
LDAP profiles	It is available when **LDAP** is selected as User Authentication Type. If you choose LDAP as the authentication type, use the drop down list to specify the LDAP profile.
DHCP From	It is available when **RADIUS** is selected as User Authentication Type.
DHCP Relay	**Enable -** If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **DHCP Server Location** – Choose one of the interfaces for DHCP server. **DHCP Server IP Address -** Set the IP address of the DHCP server you are going to use so DHCP Relay can help to forward the DHCP request to the DHCP server.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard current page modification.

4.2.2.3 History

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



LAN >> PPPoE Server >> History

PPPoE Connection Status

User Name	Action	Time

No items to show.

Each item will be explained as follows:

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

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

4.2.3 Switch

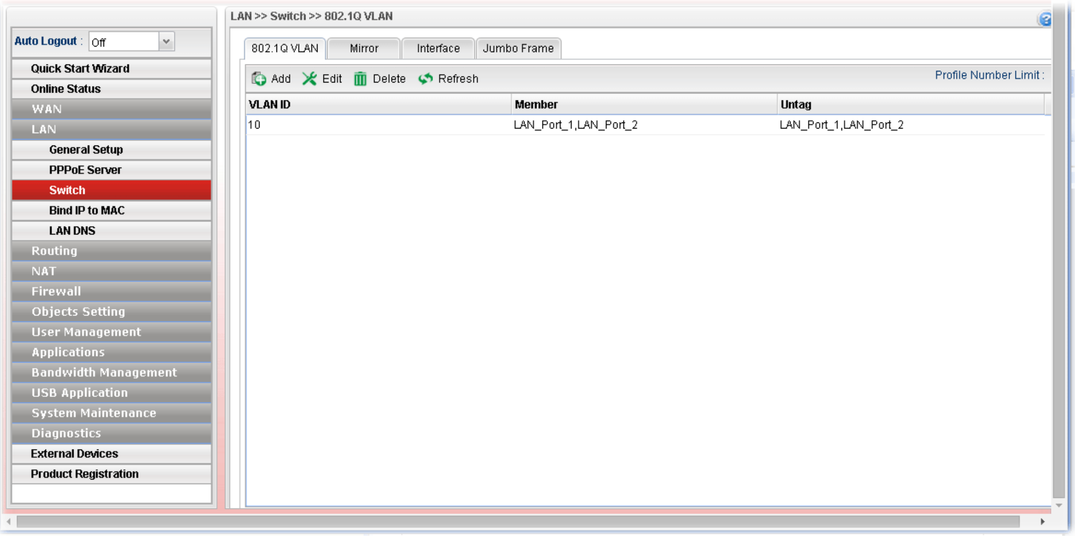
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable LAN interface, and configure 802.1Q VLAN ID for different LAN interfaces, and so on.

4.2.3.1 802.1Q VLAN

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

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

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



VLAN ID	Member	Untag
10	LAN_Port_1,LAN_Port_2	LAN_Port_1,LAN_Port_2

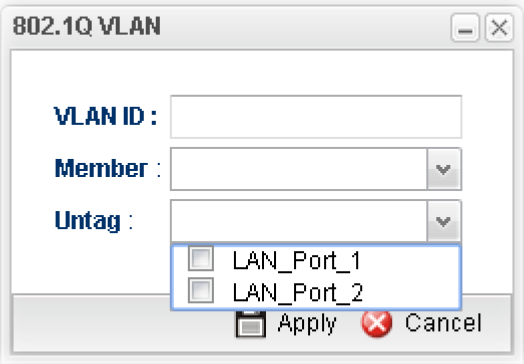
Each item will be explained as follows:

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.



802.1Q VLAN

VLAN ID :

Member :

Untag :

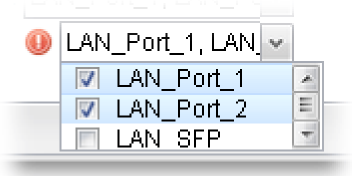
☐ LAN_Port_1

☐ LAN_Port_2

Apply Cancel

Available parameters are listed as follows:

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

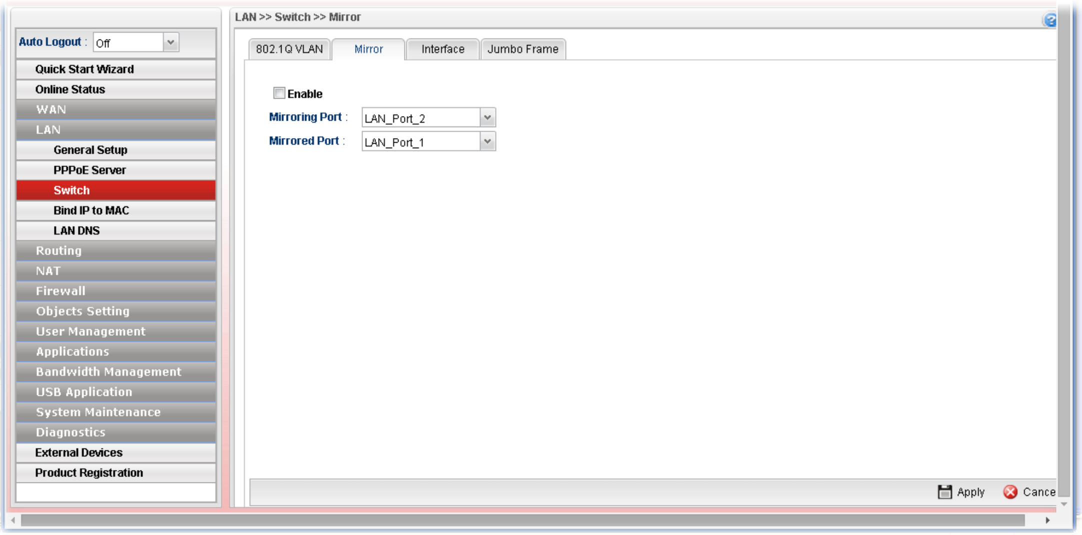
	profile, please exit this dialog to release that selection from its original VLAN profile, than return this page and make the selection again.  LAN_Port_1, LAN_ ☑ LAN_Port_1 ☑ LAN_Port_2 □ LAN_SFP
Untag	Determine if the packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or not. If the icon ❗ appears in front of the drop down list, it means one of the selections has been chosen by other profile. You cannot choose it. If you want to specify that one for such profile, please exit this dialog to release that selection from its original VLAN profile, than return this page and make the selection again.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.2.3.2 Mirror

Vigor300B 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.

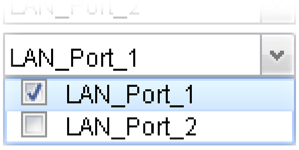
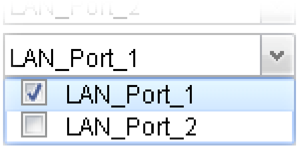


□ Enable

Mirroring Port : LAN_Port_2

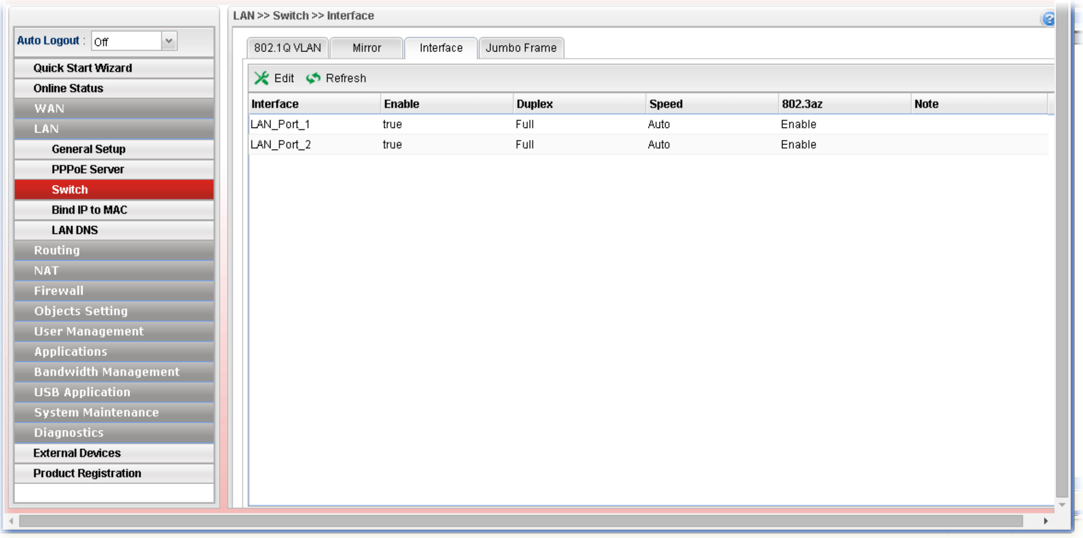
Mirrored Port : LAN_Port_1

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.  LAN_Port_1 ☑ LAN_Port_1 □ LAN_Port_2
Mirrored Port	Select which port is necessary to be mirrored.  LAN_Port_1 ☑ LAN_Port_1 □ LAN_Port_2
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.



Auto Logout : Off

LAN >> Switch >> Interface

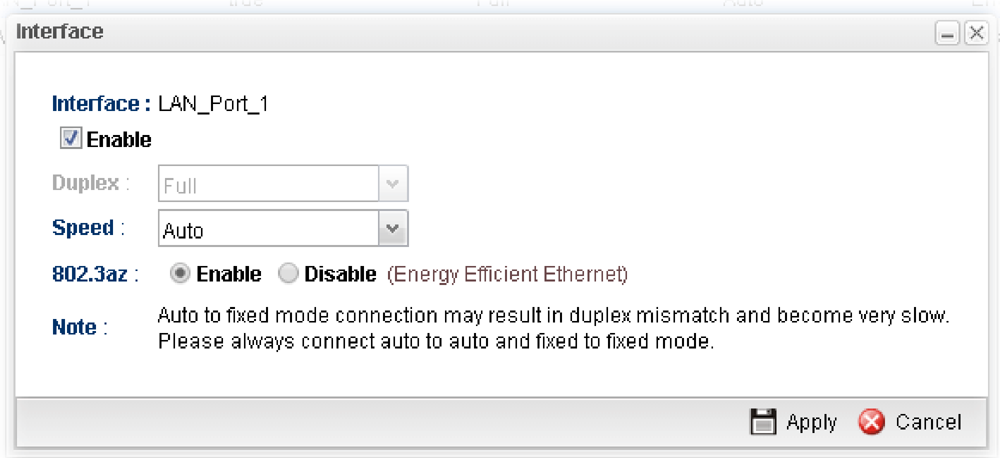
Interface	Enable	Duplex	Speed	802.3az	Note
LAN_Port_1	true	Full	Auto	Enable	
LAN_Port_2	true	Full	Auto	Enable	

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.
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.



Interface : LAN_Port_1

☑ Enable

Duplex : Full

Speed : Auto

802.3az : ● Enable ○ Disable (Energy Efficient Ethernet)

Note : Auto to fixed mode connection may result in duplex mismatch and become very slow. Please always connect auto to auto and fixed to fixed mode.

Available parameters are listed as follows:

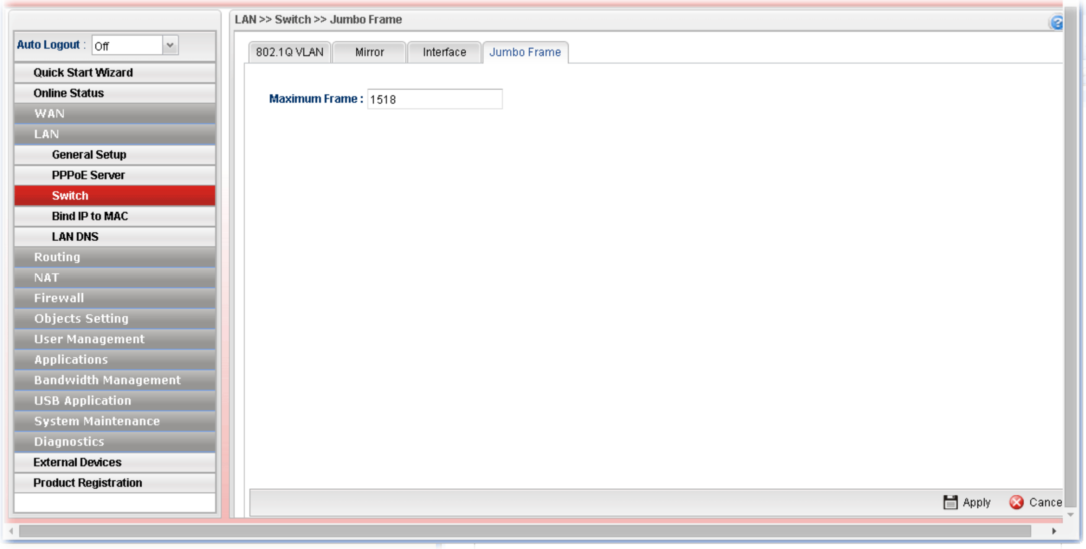
Item	Description
Interface	Display the name of LAN interface profile.
Enable	Check the box to enable the Mirror function for the switch.
Speed	Use the drop down list to specify the transmission rate for such profile.
802.3az	It is a function of energy-efficient Ethernet. It can detect the network traffic automatically to adjust the power output and let Vigor300B 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.

4.2.3.4 Jumbo Frame

The purpose of Jumbo Frame is to increase the transmission rate for the packets coming from LAN via enlarging data size.

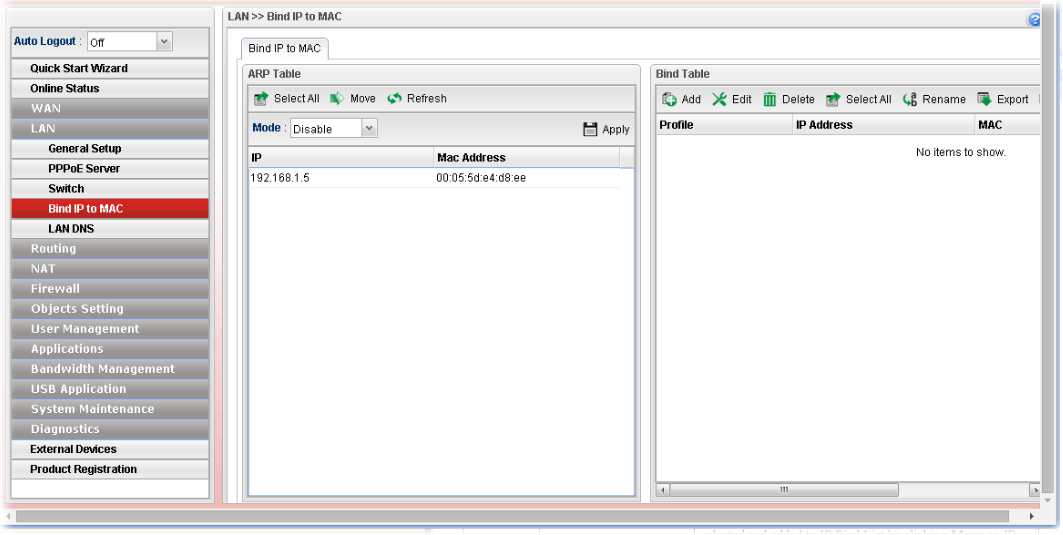
MTU (Max Transmit Unit) determines the largest size of a packet. When a packet with large size is transmitted through Vigor router, the router will cut it into several segments to facilitate the transmission. It always takes a lot of time. To reduce the sending number of times, wasted bandwidth and transmission time, use Jumbo Frame to enlarge the size of the data and speed up the transmission rate for packets coming from LAN.



Maximum Frame : 1518

4.2.4 Bind IP to MAC

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



Mode : Disable

IP	Mac Address
192.168.1.5	00:05:5d:e4:d8:ee

Profile	IP Address	MAC

No items to show.

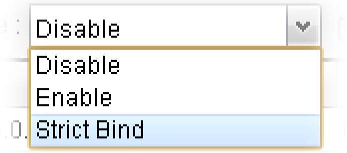
Each item will be explained as follows:

Item	Description
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Move** on IP Bind List. **Mode -** ● **Enable -** Choose it to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet. ● **Disable -** Choose it to disable this function. All the settings on this page will be invalid. ● **Strict Bind** – Choose it to lock the connection of the IP/MAC which is not listed in IP Bind List. **Select All -** Allow you to choose all the items listed in ARP Table. **Move -**Move the selected item to IP Bind List. **Refresh -** It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information. **IP Address -** Display the IP address of one device. **MAC Address -** Display the MAC address of the device.
Bind Table	It displays a list for the IP bind to MAC information. **Add -**It allows you to add one pair of IP/MAC address and

	display on the table of **IP Bind List**. **Edit** -It allows you to edit and modify the selected IP address and MAC address that you create before. **Delete** -You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**. **Select All** -Choose all of the selections at one time. **Rename** -Allow to modify the selected profile name. **Export –** The list for the IP bind to MAC information can be stored as a text file. Such file can be imported by other Vigor router. Thus, it is not necessary for that router to create Bind IP to MAC one by one. **Import –** Click it to import an IP bind to MAC information (e.g., 123.txt) obtained from other Vigor router and to be applied by Vigor300B. **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

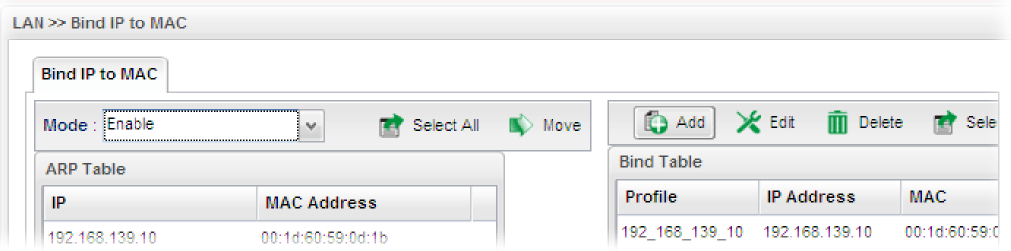
1. Open **LAN>>Bind IP to MAC**.
2. Use the drop down menu to specify a suitable mode.



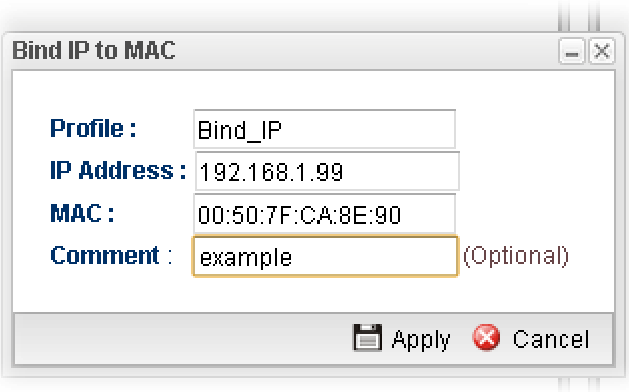
There are three modes offered for you to choose.

- **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.



Profile : Bind_IP

IP Address : 192.168.1.99

MAC : 00:50:7F:CA:8E:90

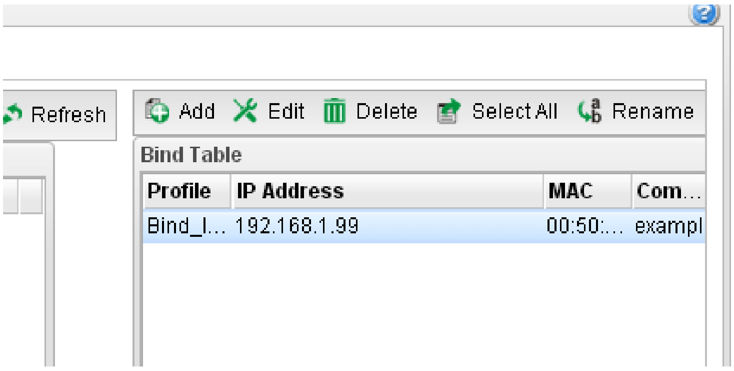
Comment : example (Optional)

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**.

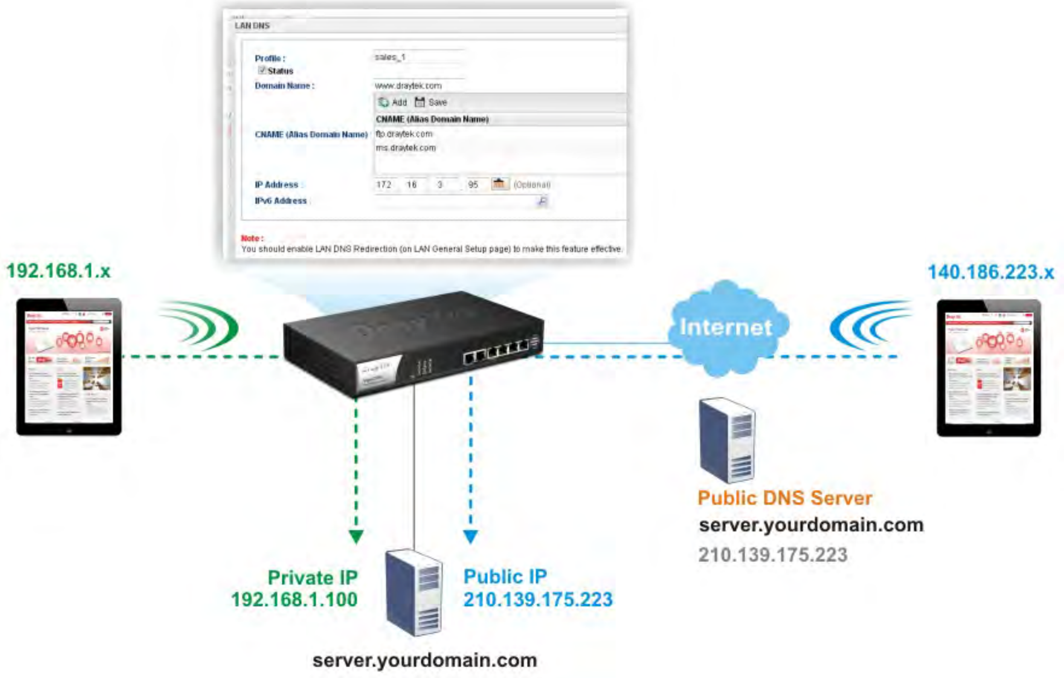
6. A new profile has been added onto **Bind Table**.



Profile	IP Address	MAC	Com...
Bind_I...	192.168.1.99	00:50:...	exampl

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.



LAN DNS

Profile : sales_1

☑ Status

Domain Name : www.draytek.com

Add Save

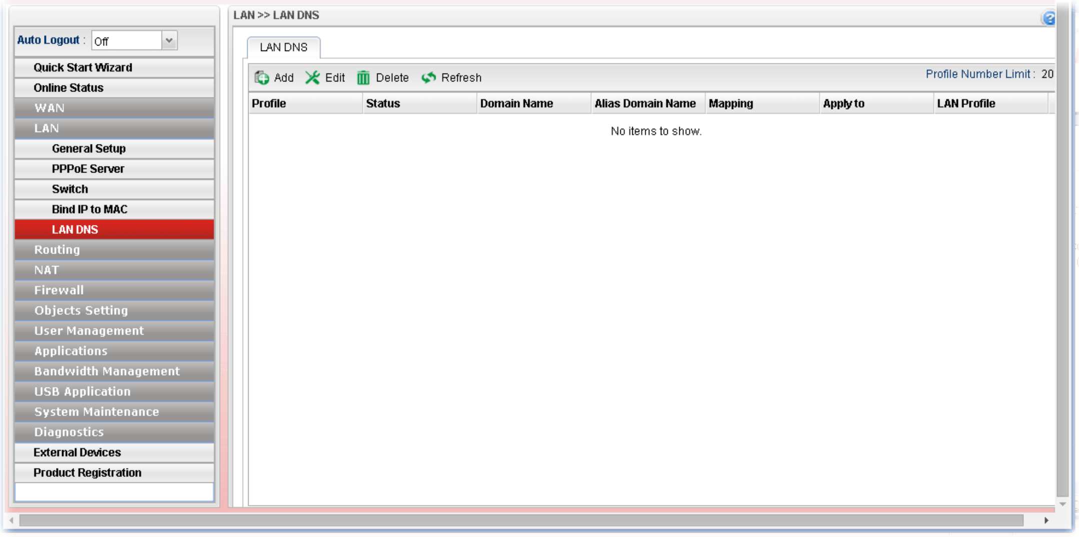
CNAME (Alias Domain Name) :

CNAME (Alias Domain Name)
ftp.draytek.com
ms.draytek.com

IP Address : 172 . 16 . 3 . 95 (Optional)

IPv6 Address :

Note :
You should enable LAN DNS Redirection (on LAN General Setup page) to make this feature effective.



LAN >> LAN DNS

LAN DNS

Add Edit Delete Refresh Profile Number Limit : 20

Profile	Status	Domain Name	Alias Domain Name	Mapping	Apply to	LAN Profile

No items to show.

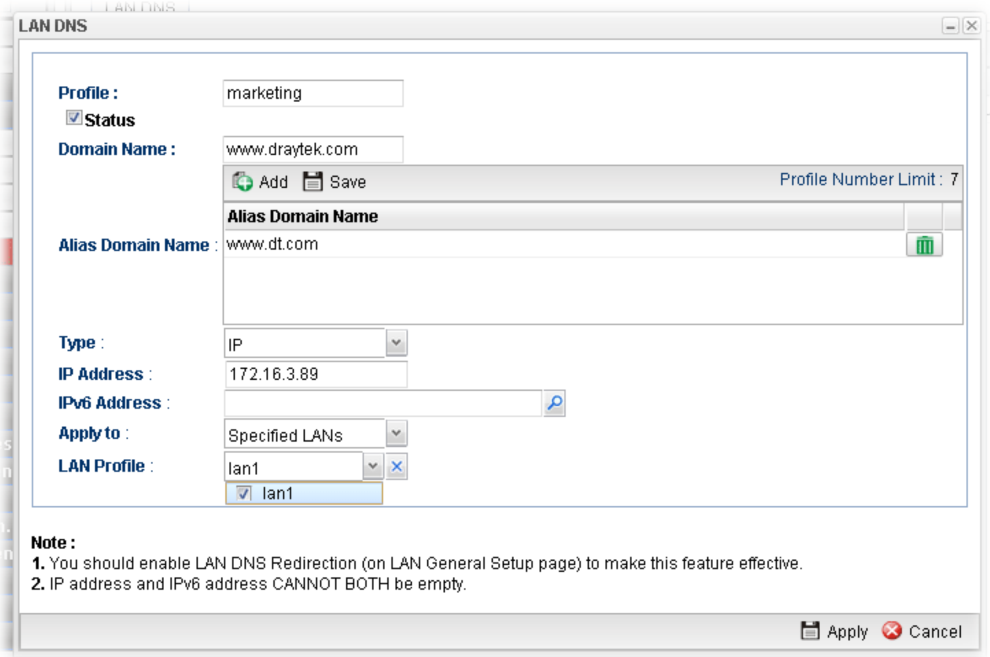
Each item will be explained as follows:

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

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

☑ 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.

Available parameters are listed as follows:

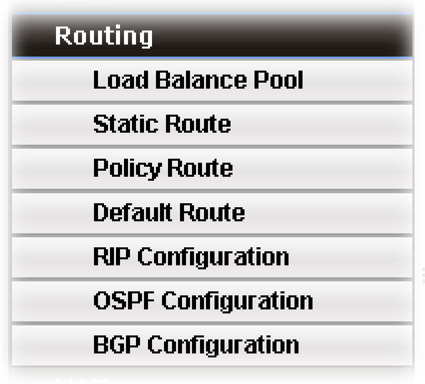
Item	Description
Profile	Type a name for such profile.
Status	Check the box to enable such profile.

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 LAN**s, it is necessary to specify at least one LAN profile in this field.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.3 Routing

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

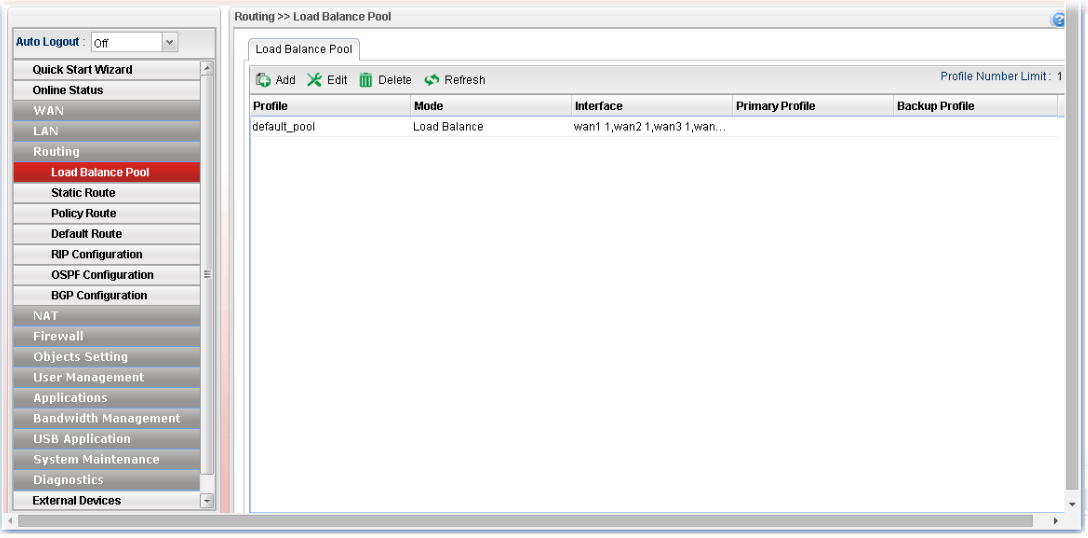


4.3.1 Load Balance Pool

Vigor300B 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.



Routing >> Load Balance Pool

Profile Number Limit : 1

Profile	Mode	Interface	Primary Profile	Backup Profile
default_pool	Load Balance	wan1 1,wan2 1,wan3 1,wan...		

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

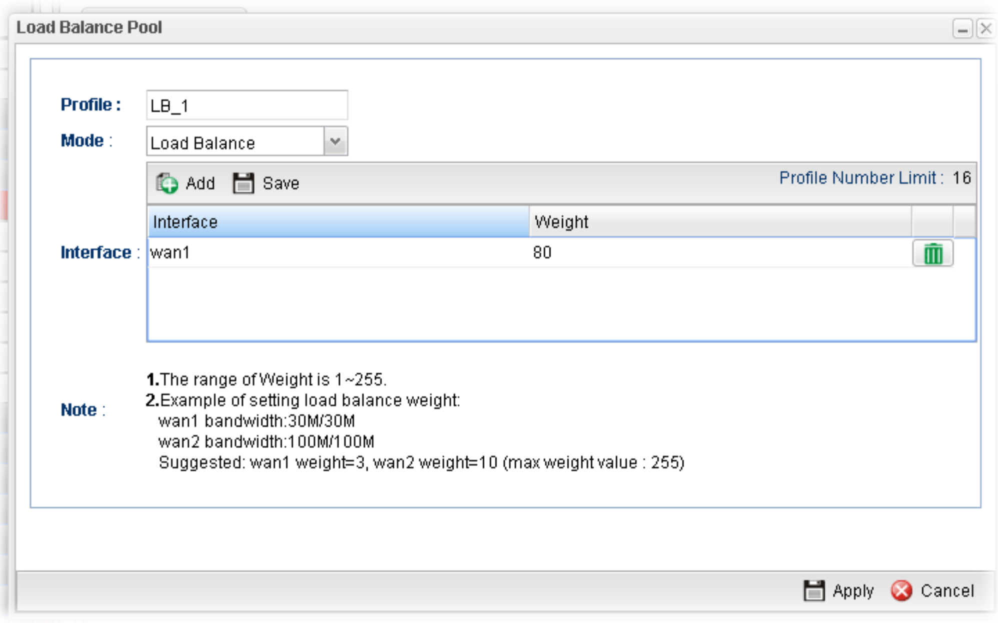
	you to modify the corresponding settings for the selected rule.
Delete	Remove the selected rule profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the load balance profile.
Mode	Display the mode (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 Backup page for such profile.
Backup Profile	Display the backup profile configured in Backup page for such profile.

There are two modes, **Load Balance** and **Backup**, 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 **Backup**, the tab of **Backup** 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.



Profile : LB_1

Mode : Load Balance

Profile Number Limit : 16

Interface :

Interface	Weight
wan1	80

Note : 1.The range of Weight is 1~255.
2.Example of setting load balance weight:
wan1 bandwidth:30M/30M
wan2 bandwidth:100M/100M
Suggested: wan1 weight=3, wan2 weight=10 (max weight value : 255)

Available parameters are listed as follows:

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

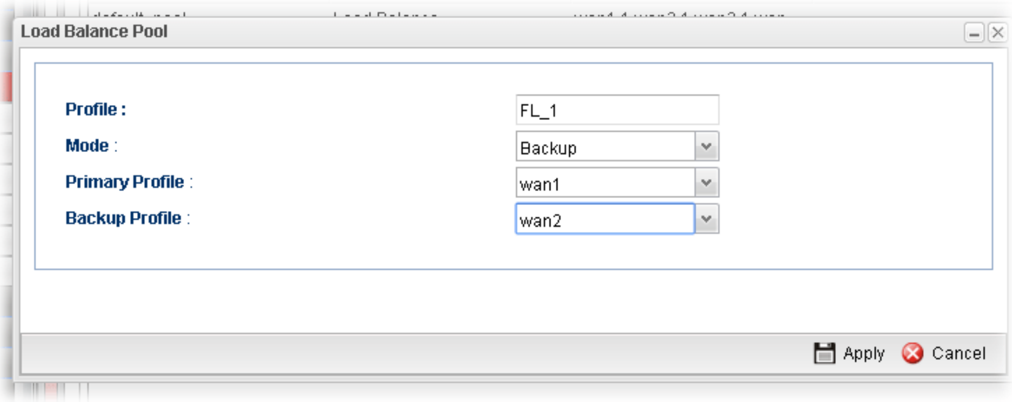
3. Click **Apply**. A new profile will be added on the page.

How to add a Pool profile for Backup

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

1. Open **Routing >>Load Balance Pool**.

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



Load Balance Pool

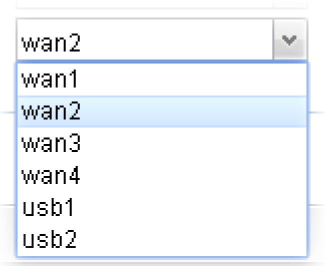
Profile : FL_1

Mode : Backup

Primary Profile : wan1

Backup Profile : wan2

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Mode	Choose **Backup** as the **Mode** selection.
Primary Profile	In default, the system will apply Primary Profile. If Primary Profile cannot be used any more, the Backup Profile will be used instead. Use the drop down list to choose the one you need.
Backup Profile	Use the drop down list to choose the one you need.  wan2 wan1 wan2 wan3 wan4 usb1 usb2

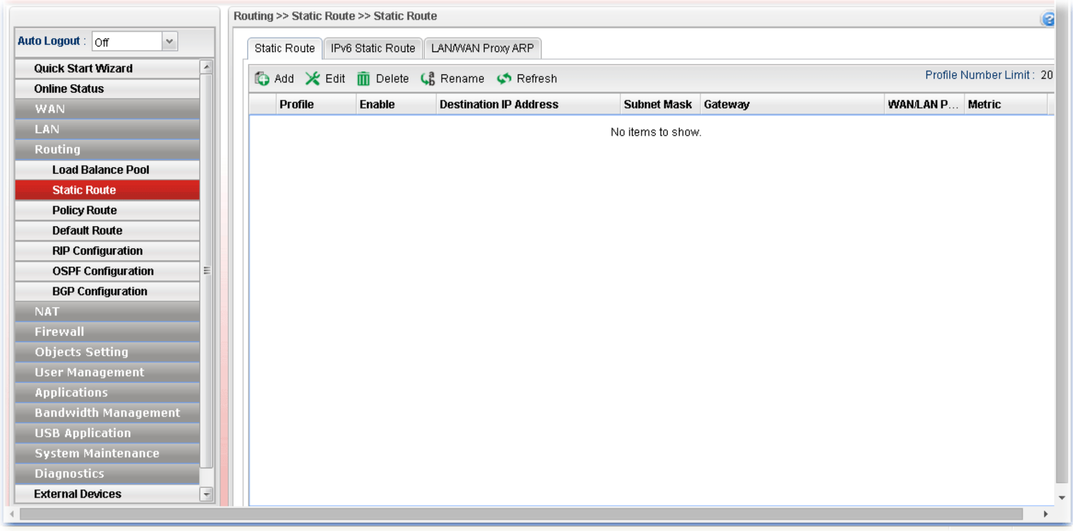
3. Click **Apply**. A new profile will be added on the page.

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.


Routing >> Static Route >> Static Route

Auto Logout : Off

Profile Number Limit : 20

Profile	Enable	Destination IP Address	Subnet Mask	Gateway	WAN/LAN P...	Metric

No items to show.

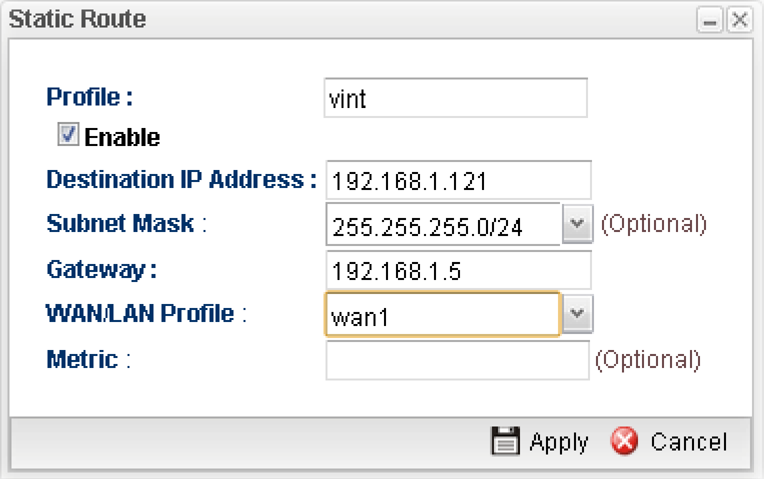
Each item will be explained as follows:

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.



Static Route

Profile : vint

☑ Enable

Destination IP Address : 192.168.1.121

Subnet Mask : 255.255.255.0/24 (Optional)

Gateway : 192.168.1.5

WAN/LAN Profile : wan1

Metric : (Optional)

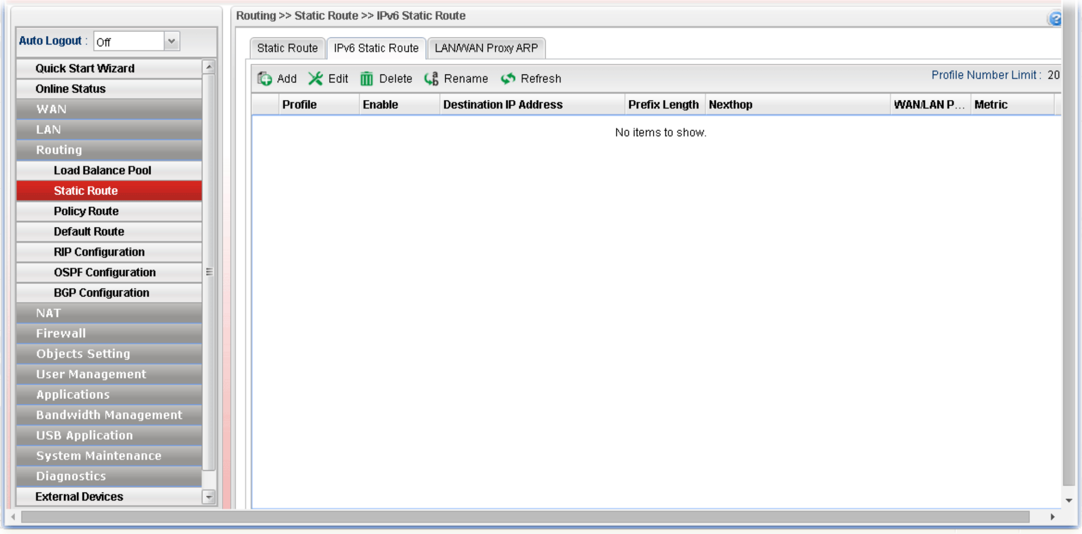
Available parameters are listed as follows:

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.



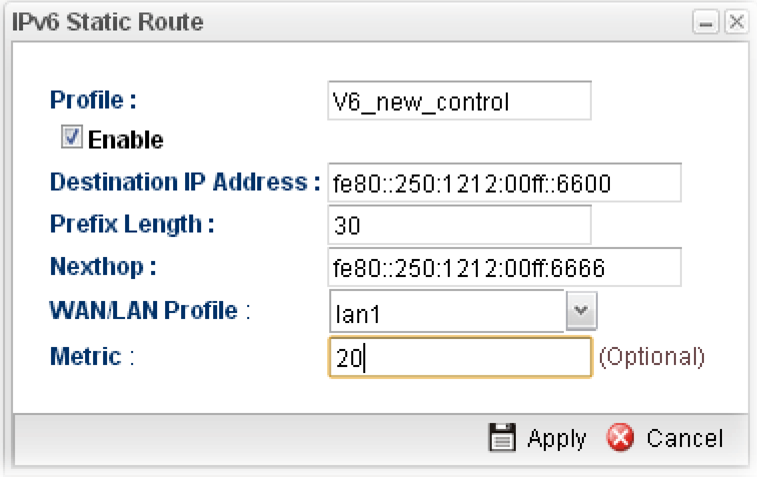
No items to show.

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.
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.



IPv6 Static Route

Profile : V6_new_control

☑ Enable

Destination IP Address : fe80::250:1212:00ff::6600

Prefix Length : 30

Nexthop : fe80::250:1212:00ff:6666

WAN/LAN Profile : lan1

Metric : 20 (Optional)

Available parameters are listed as follows:

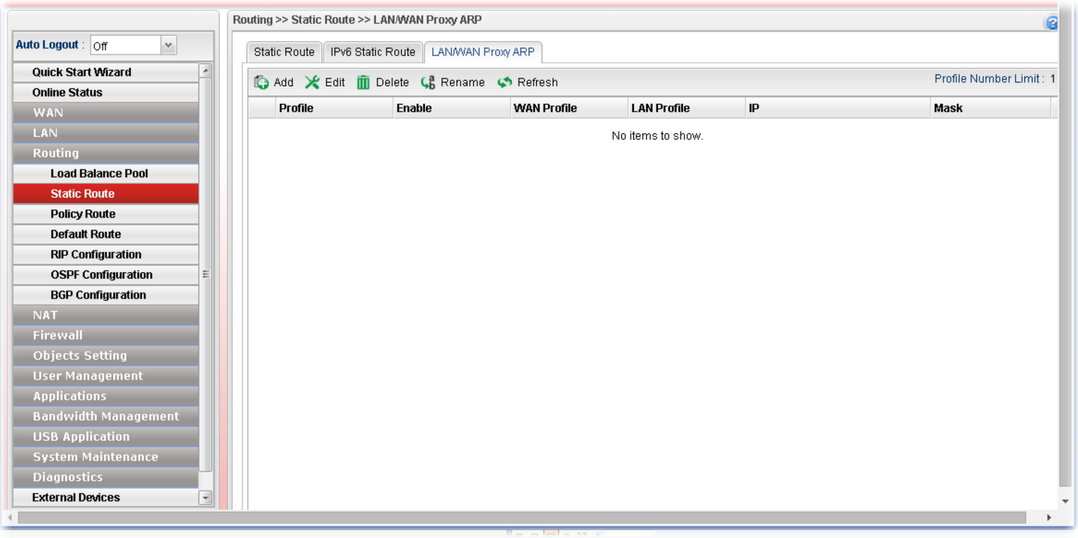
Item	Description
Profile Name	Type the name of the static route profile.
Enable	Check this box to enable such profile.
Destination IP Address	Type the IP address for such static route profile.
Prefix Length	Type the prefix length for such profile.
Nexthop	Type the nexthop address for such static route 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, Vigor300B 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.



No items to show.

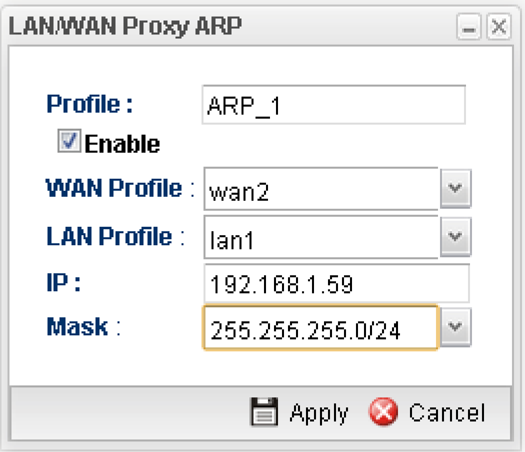
Each item will be explained as follows:

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.



Profile : ARP_1

☑ Enable

WAN Profile : wan2

LAN Profile : lan1

IP : 192.168.1.59

Mask : 255.255.255.0/24

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.

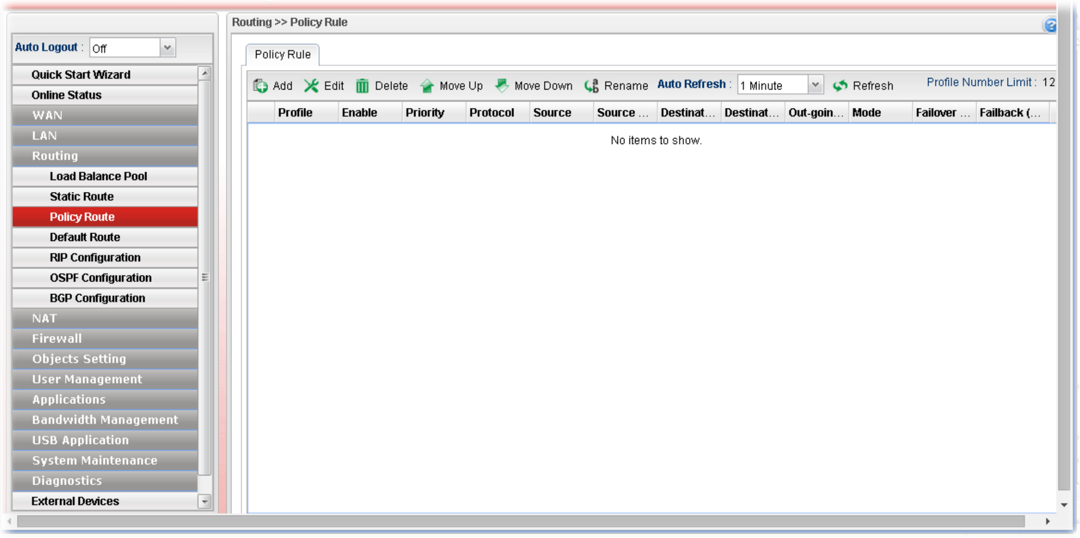
- **Address Mapping.**

  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.



Auto Logout : Off

Auto Refresh : 1 Minute

Profile Number Limit : 12

Profile	Enable	Priority	Protocol	Source	Source ...	Destinat...	Destinat...	Out-goin...	Mode	Failover ...	Failback (...

No items to show.

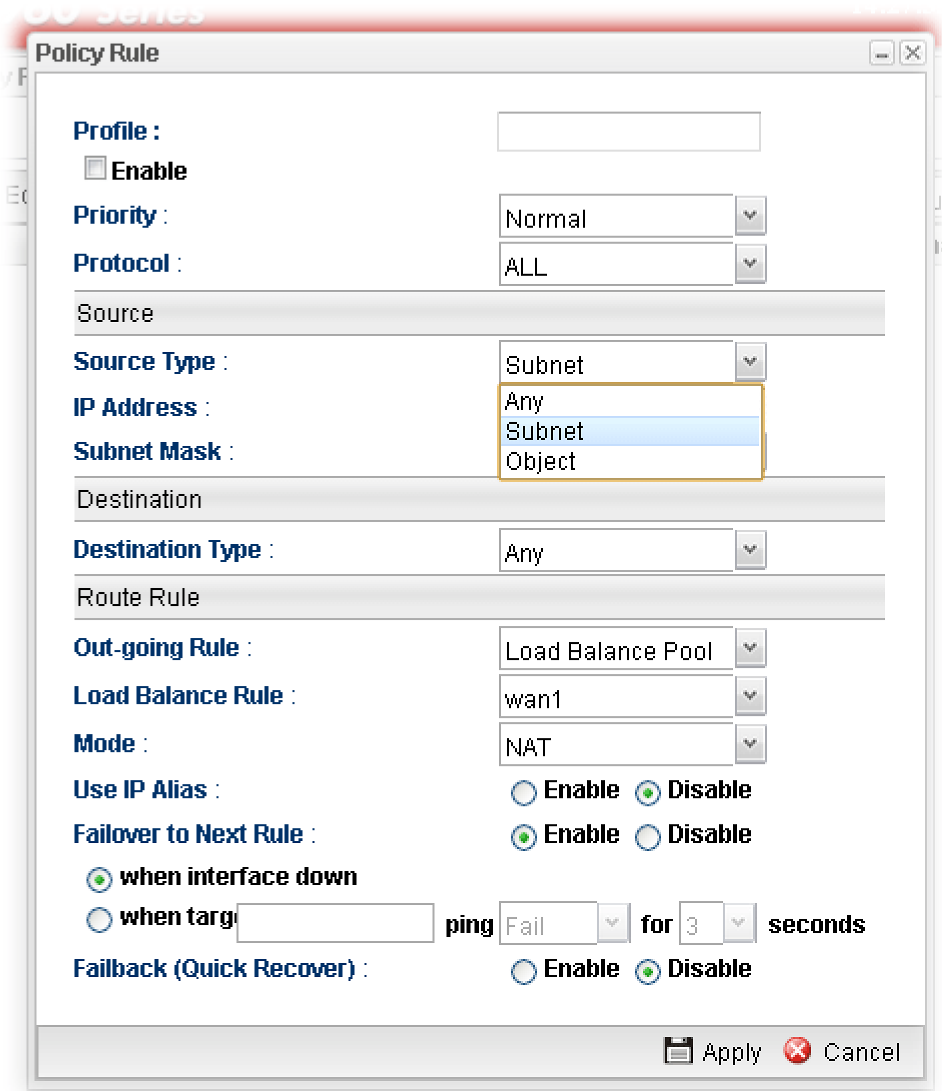
Each item will be explained as follows:

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

	rule.
Delete	Remove the selected rule profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Move Up / Move Down	Move the selected profile up or down.
Rename	Allow to modify the selected profile name.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Refresh	Renew current web page.
Profile	Display the name of the rule.
Enable	Display the status of the profile. False means disabled; True means enabled.
Priority	Display the priority (top, high and normal) of such rule.
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.



Policy Rule

Profile :
□ Enable
Priority : Normal
Protocol : ALL

Source

Source Type : Subnet
Any
Subnet
Object
IP Address :
Subnet Mask :

Destination

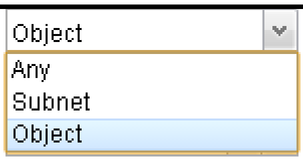
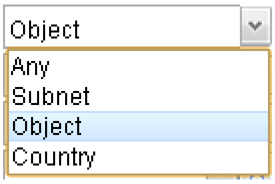
Destination Type : Any

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 targ ping Fail for 3 seconds
Failback (Quick Recover) : ○ Enable ● Disable

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.

	 Each type will bring different settings for configuration.
	When Subnet is selected as Source Type
	● **IP Address** - Type an IP address here as the source IP address for such rule. ● **Subnet Mask** - Use the drop down list on the right to choose a suitable mask for the source.
	When Object is selected as Source Type
	● **IP Object –** Use the drop down list to choose the source IP object(s) for such rule profile. ● **IP Group –**Use the drop down list to choose the source IP group(s) for such rule profile.
Destination	**Destination Type** - Choose the address type (Any, Subnet, Object or Country) for such rule.  Each type will bring different settings for configuration.
	When Subnet is selected as Destination Type
	● **IP Address** - Type an IP address here as the destination IP address for such rule. ● **Subnet Mask** - Use the drop down list on the right to choose a suitable mask for the destination.
	When Object is selected as Destination Type
	● **IP Object –** Use the drop down list to choose the destination IP object(s) for such rule profile. ● **IP Group –**Use the drop down list to choose the destination IP group(s) for such rule profile. ● **DNS Object -** Use the drop down list to choose DNS object(s) for such rule profile.
	When Country is selected as Destination Type
	● **Country Object -** Use the drop down list to choose the country object(s) for such rule profile.
Route Rule	**Out-going Rule** - It determines the way (interface) that the incoming traffic will be forwarded to. **Load Balance Pool –**The incoming traffic will be forwarded to specified WAN interface or load balance pool. **User Defined –**The incoming traffic will be forwarded to the specified WAN or LAN interface with a user defined gateway.

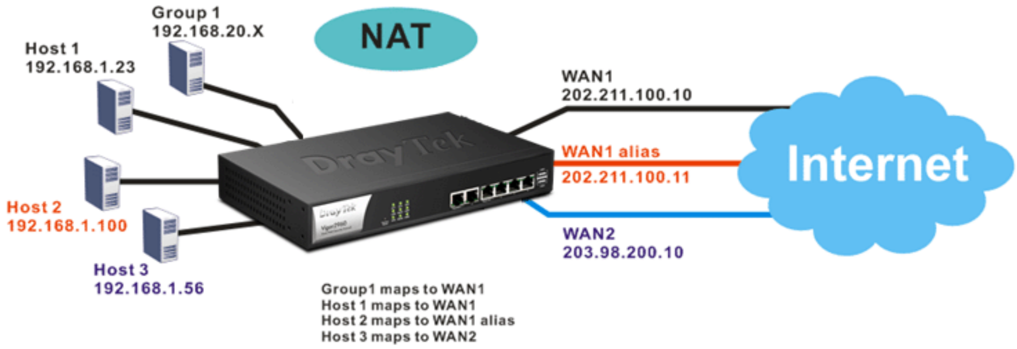
	PPTP – The incoming traffic will be forwarded to specified PPTP profile.
	When Load Balance Pool is selected as Out-going Rule
	● **Load Balance Rule -** Choose one of the profiles to be used by such rule. In which, wan1 to wan2 profiles are configured in default. In addition, profiles configured in **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.
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).

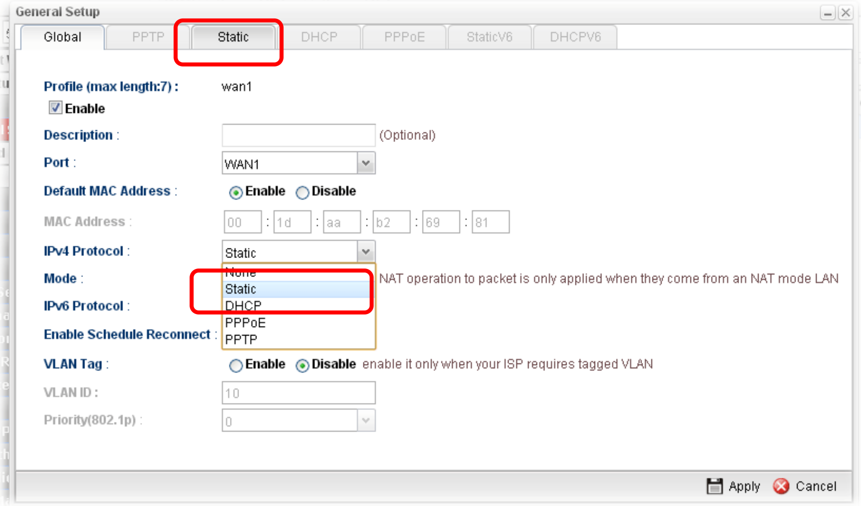
With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2) 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 Vigor300B.

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



General Setup

Profile (max length:7) : wan1

☑ Enable

Description : (Optional)

Port : WAN1

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 1d : aa : b2 : 69 : 81

IPv4 Protocol : Static

Mode : NAT operation to packet is only applied when they come from an NAT mode LAN

IPv6 Protocol :

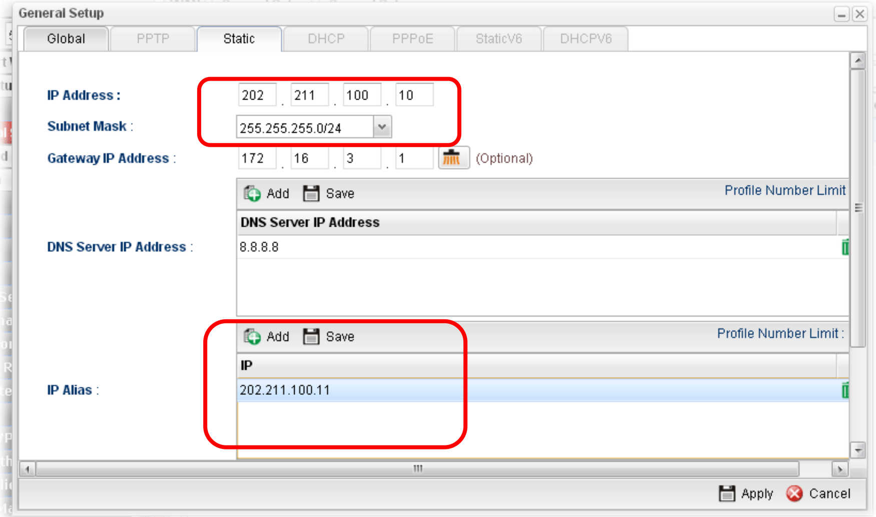
Enable Schedule Reconnect :

VLAN Tag : ○ Enable ● Disable enable it only when your ISP requires tagged VLAN

VLAN ID : 10

Priority(802.1p) : 0

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



General Setup

IP Address : 202 . 211 . 100 . 10

Subnet Mask : 255.255.255.0/24

Gateway IP Address : 172 . 16 . 3 . 1 (Optional)

DNS Server IP Address :

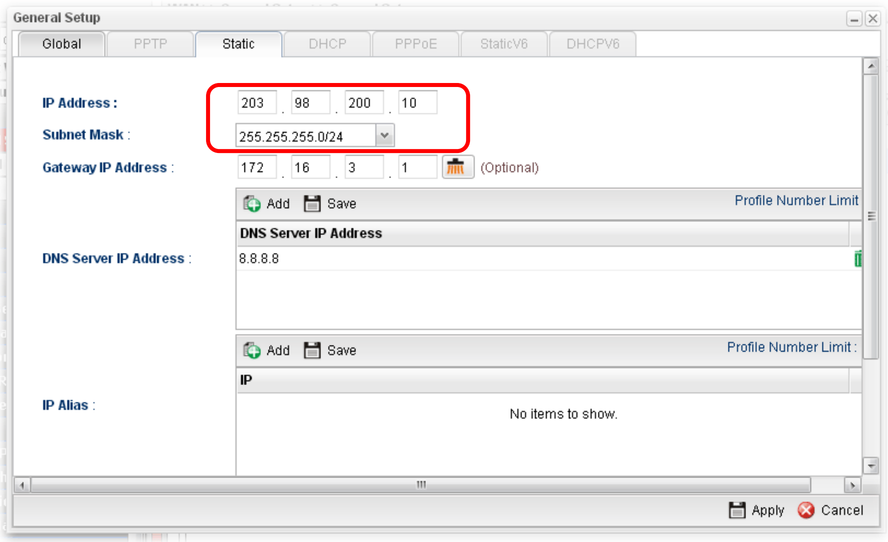
DNS Server IP Address
8.8.8.8

IP Alias :

IP
202.211.100.11

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*”.



IP Address : 203 . 98 . 200 . 10

Subnet Mask : 255.255.255.0/24

Gateway IP Address : 172 . 16 . 3 . 1 (Optional)

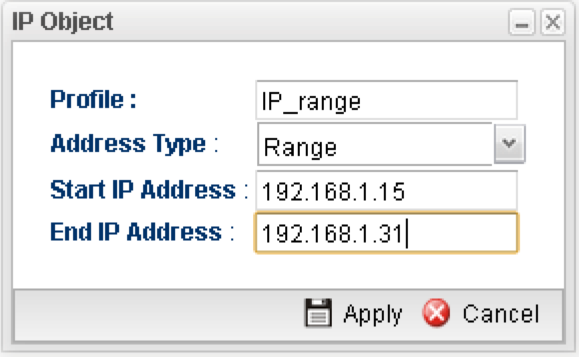
DNS Server IP Address :

DNS Server IP Address
8.8.8.8

IP Alias :

IP
No items to show.

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.



Profile : IP_range

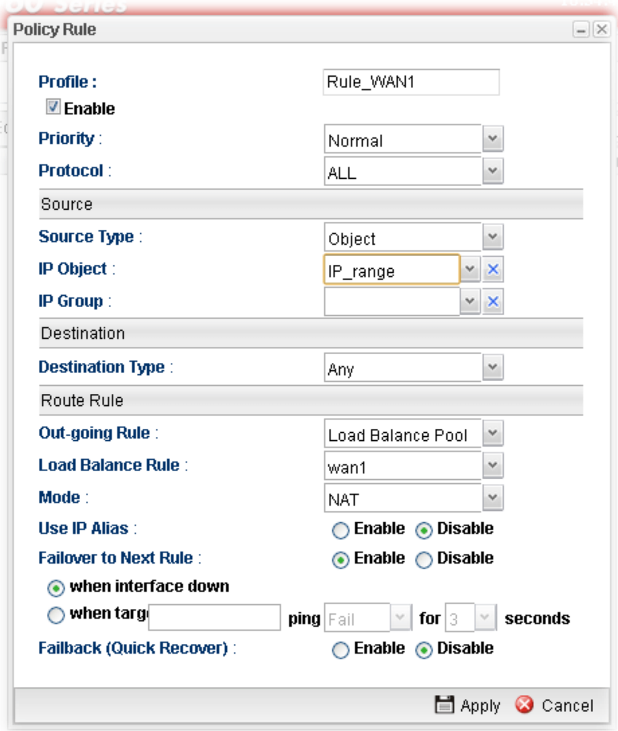
Address Type : Range

Start IP Address : 192.168.1.15

End IP Address : 192.168.1.31

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

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



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

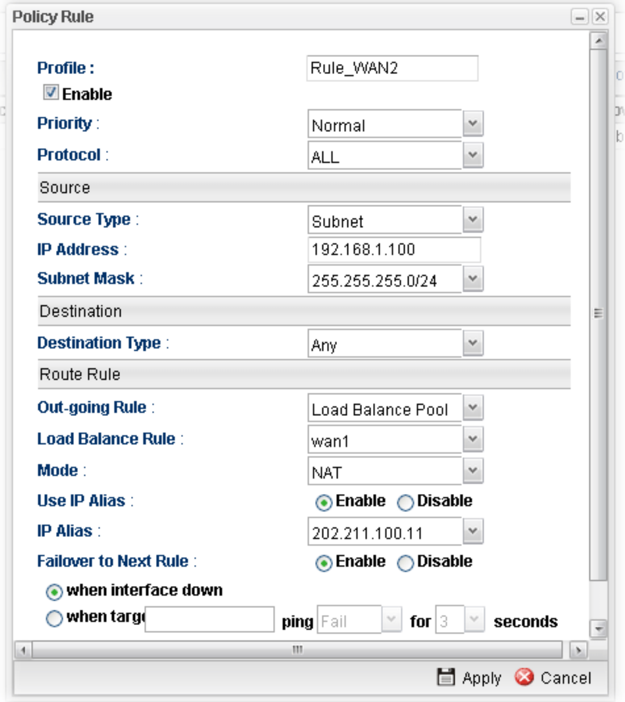
● when interface down

○ when targ 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 targ ping Fail for 3 seconds

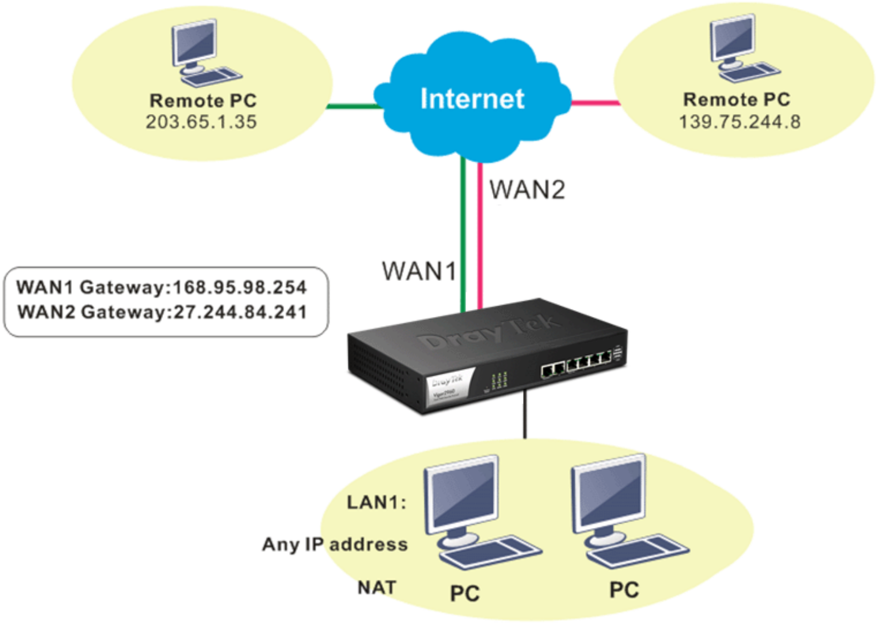
Apply Cancel

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

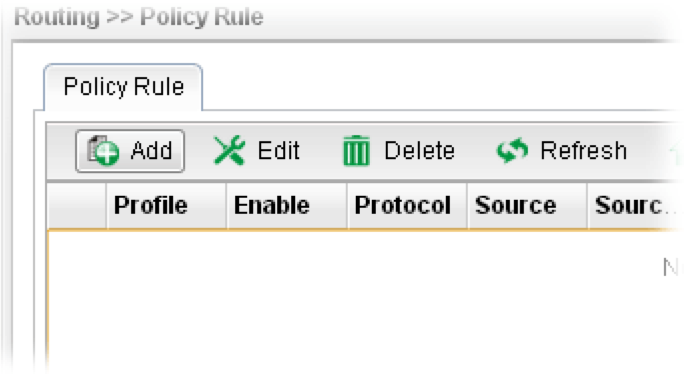
Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

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

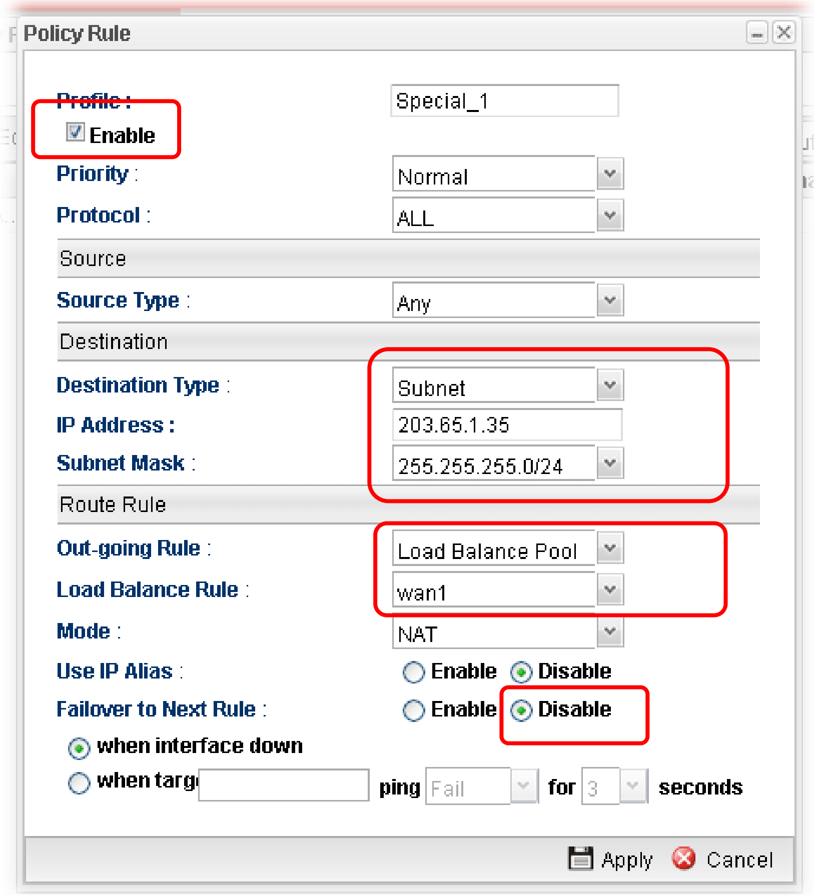
The following figure shows a simple application of load balance. WAN1 and WAN2 can be used to access into Internet. The PC in LAN1 can send the data to the remote PC through the specified WAN1.



1. Access into web user interface of Vigor300B.
2. Open **Routing>> Policy Route** and click **Add** to create a new profile.



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



Policy Rule

Profile : Special_1

☑ Enable

Priority : Normal

Protocol : ALL

Source

Source Type : Any

Destination

Destination Type : Subnet

IP Address : 203.65.1.35

Subnet Mask : 255.255.255.0/24

Route Rule

Out-going Rule : Load Balance Pool

Load Balance Rule : wan1

Mode : NAT

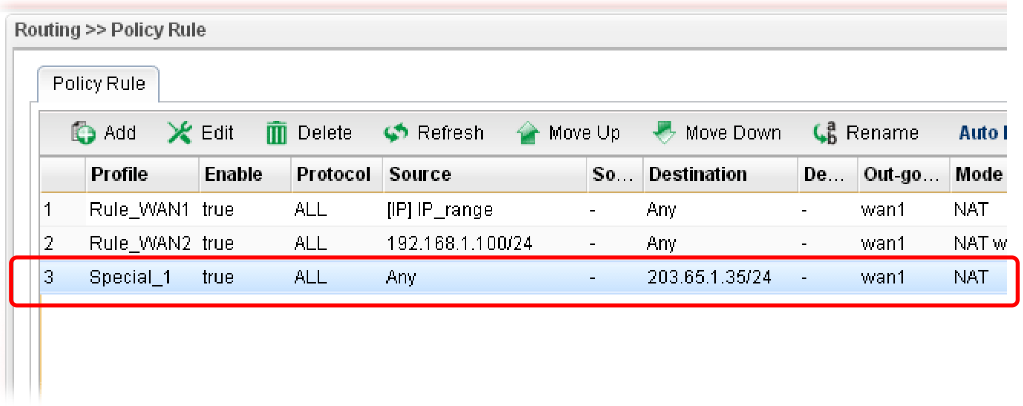
Use IP Alias : ○ Enable ● Disable

Failover to Next Rule : ○ Enable ● Disable

● when interface down

○ when targ ping Fail for 3 seconds

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



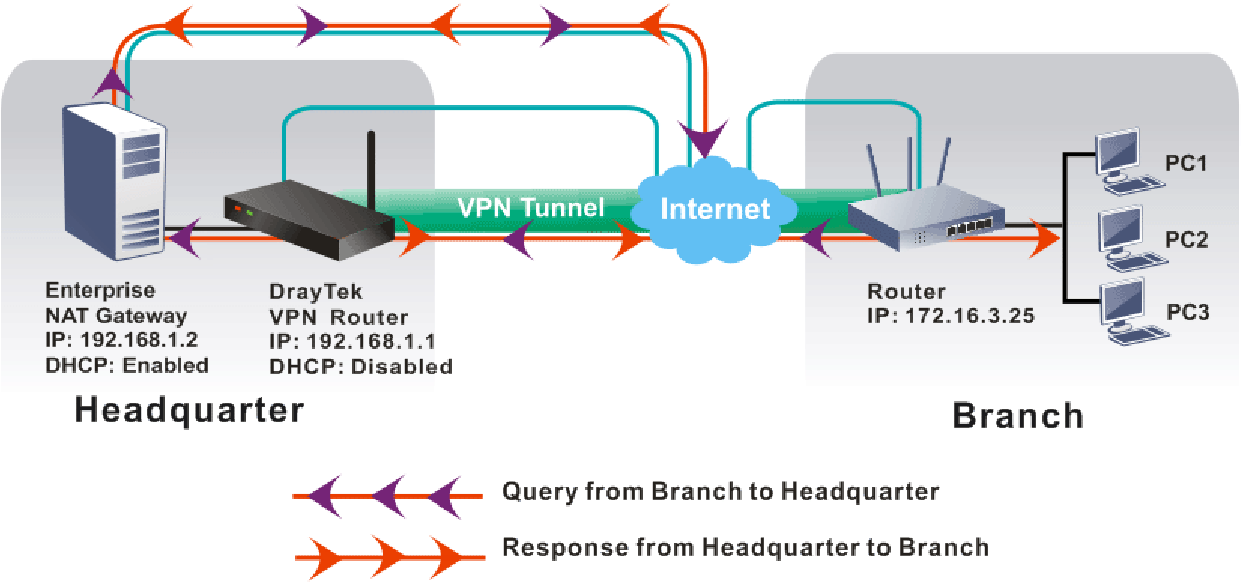
Routing >> Policy Rule

	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

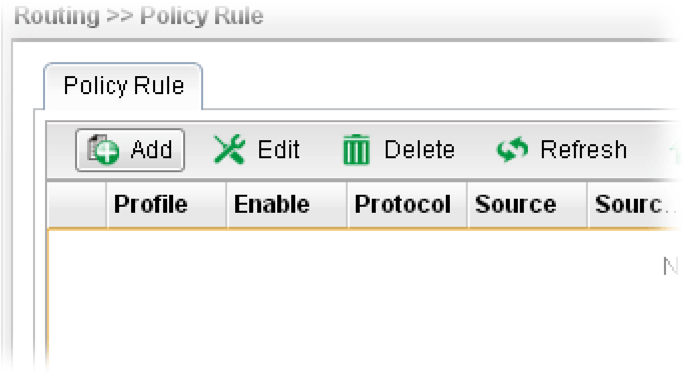
Now, any packets from LAN1 sent to the remote PC (IP address: 203.65.1.35) will be forcefully to pass through WAN1.

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

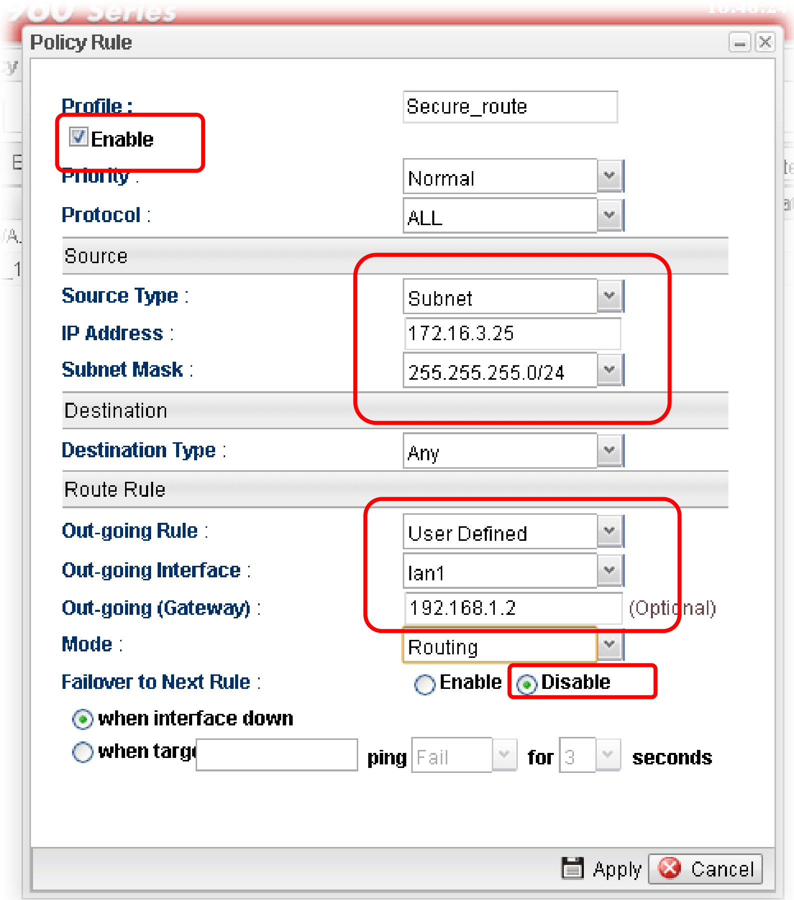
A LAN to LAN VPN tunnel is built between DrayTek VPN router (e.g., Vigor300B) and the remote router. Enterprise firewall router (in Headquarter) can control the all of the traffic coming from the remote PC (in Branch) which wants to access into Internet.



1. Access into web user interface of Vigor300B.
2. Open **Routing>> Policy Route** and click **Add** to create a new profile.



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



Policy Rule

Profile : Secure_route

☑ Enable

Priority : Normal

Protocol : ALL

Source

Source Type : Subnet

IP Address : 172.16.3.25

Subnet Mask : 255.255.255.0/24

Destination

Destination Type : Any

Route Rule

Out-going Rule : User Defined

Out-going Interface : lan1

Out-going (Gateway) : 192.168.1.2 (Optional)

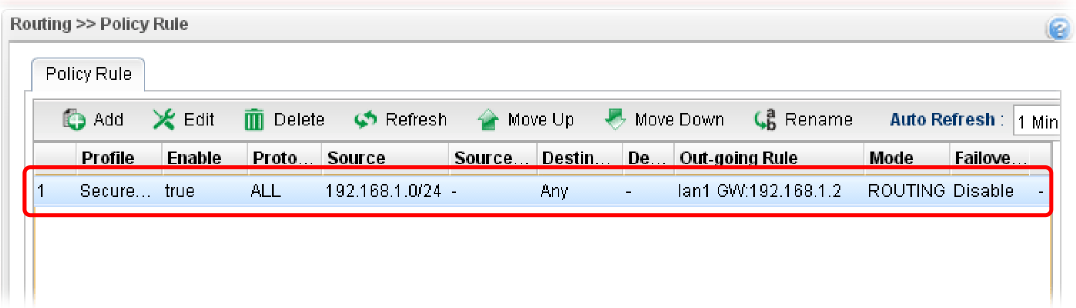
Mode : Routing

Failover to Next Rule : ○ Enable ● Disable

● when interface down

○ when targ[ ] ping Fail for 3 seconds

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



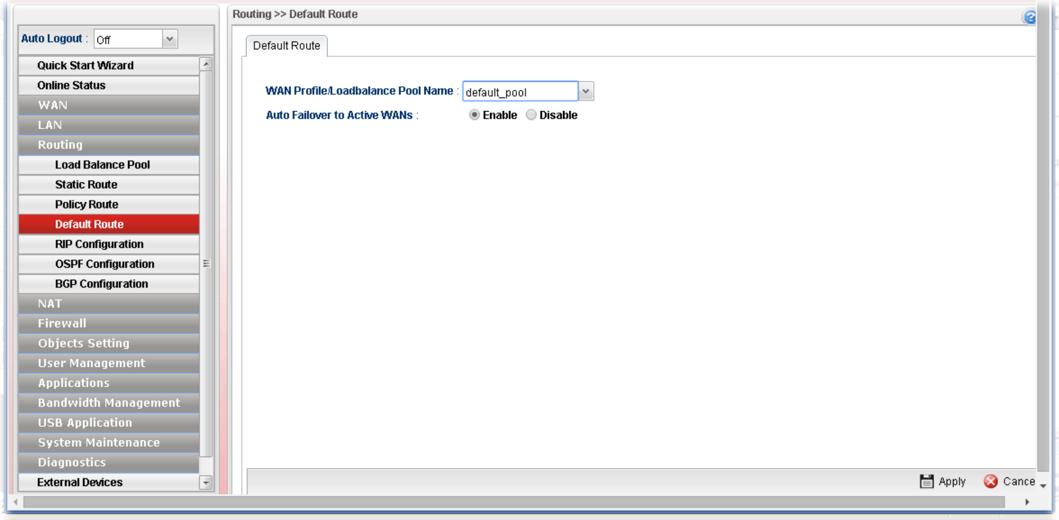
Routing >> Policy Rule

Policy Rule

	Profile	Enable	Proto...	Source	Source...	Destin...	De...	Out-going Rule	Mode	Failove...	
1	Secure...	true	ALL	192.168.1.0/24	-	Any	-	lan1 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.



WAN Profile/Loadbalance Pool Name : default_pool

Auto Failover to Active WANs : ● Enable ○ Disable

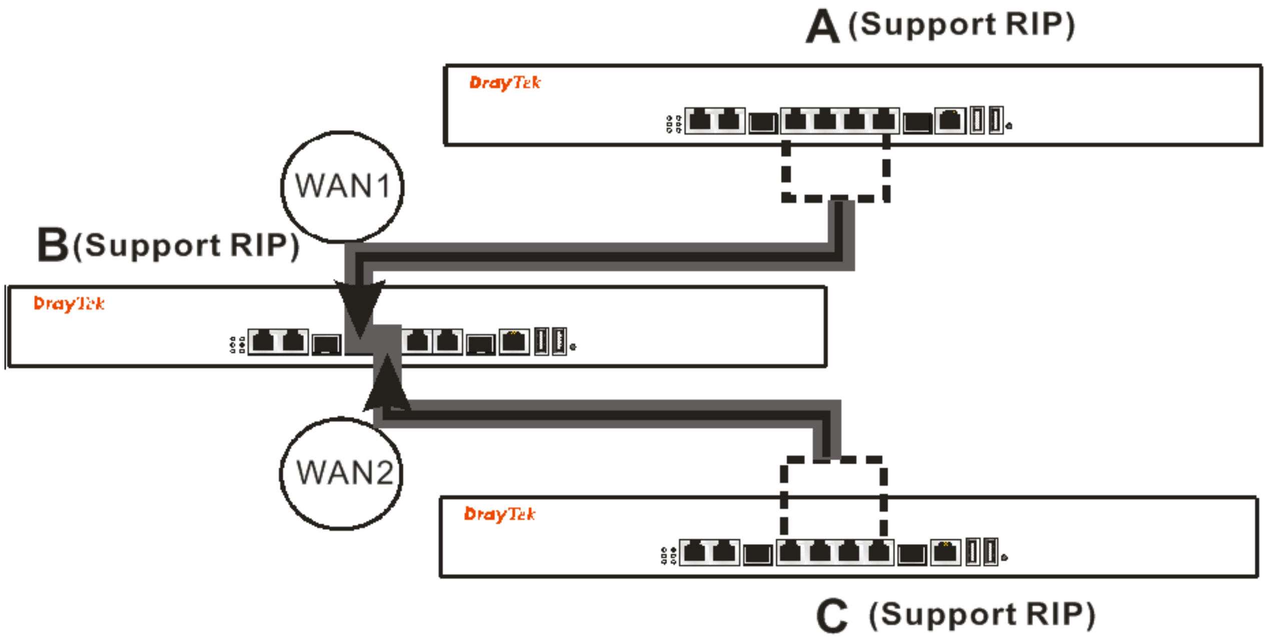
Available parameters are listed as follows:

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.

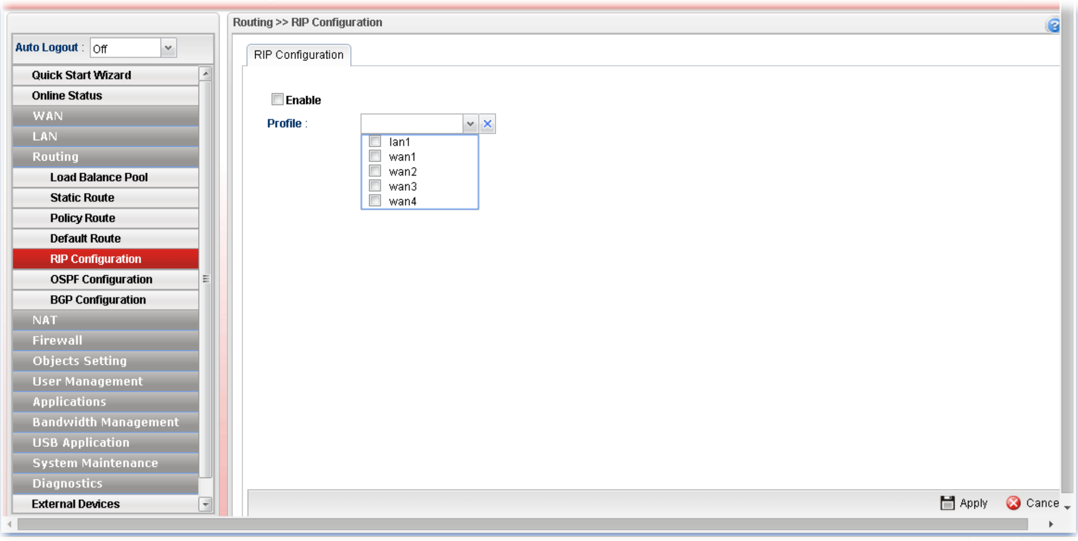
RIP can update the routing table automatically and find a route to send packet. See the following figure as an example:



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.



Routing >> RIP Configuration

RIP Configuration

□ Enable

Profile :

□ lan1
□ wan1
□ wan2
□ wan3
□ wan4

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.

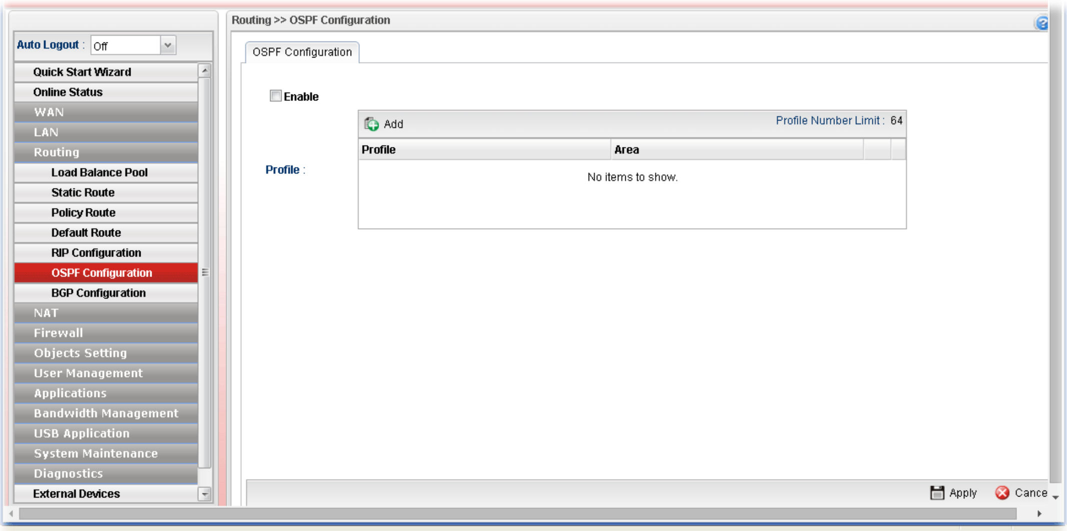
After finished the settings, click **Apply** to save them.

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.



Routing >> OSPF Configuration

Auto Logout : Off

□ Enable

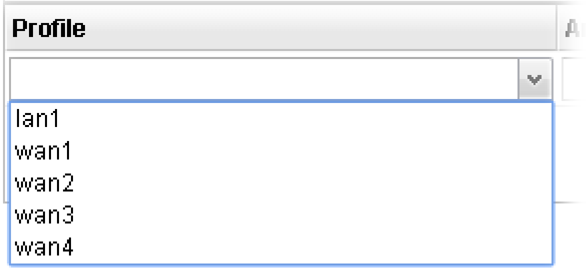
Profile Number Limit : 64

Profile	Area

No items to show.

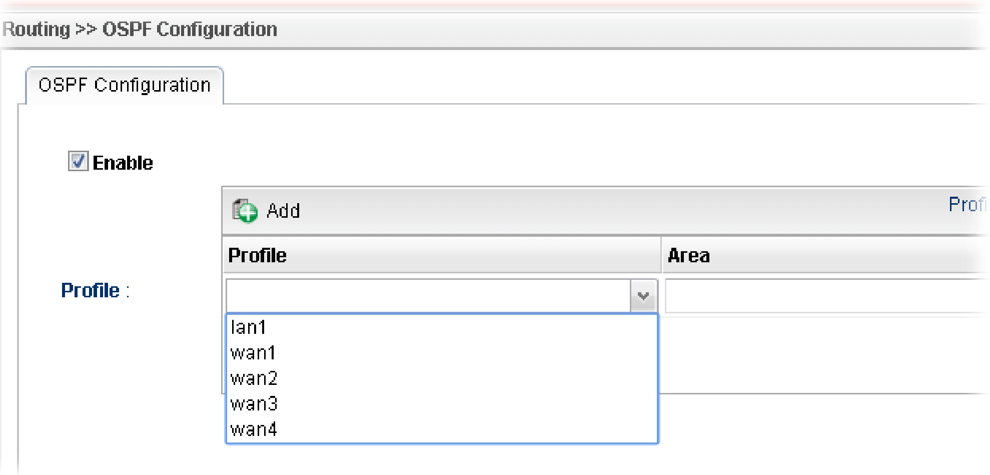
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable the Mirror function for the switch.
Profile	**Add-** Click it to create a new profile.

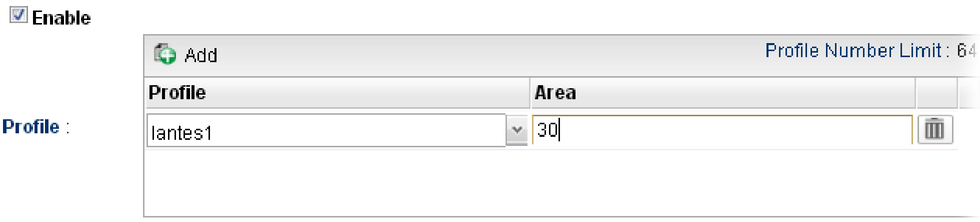
	 **Profile -** Choose a LAN/WAN profile from the drop down list to apply for such configuration. **Area** – An AS will be divided into several areas. Each area must be assigned with a dedicated number. **Note**: For the detailed information of OSPF application, refer to section *"3.2 How to Configure OSPF?"*.
Apply	Click it to save the settings.
Cancel	Click it to discard the settings configured in this page.

How to add a new profile

1. Open **Routing>>OSPF Configuration**.
2. Check **Enable**.
3. Click the space of **Profile**. A pop-up dialog will appear. Click **Add**.

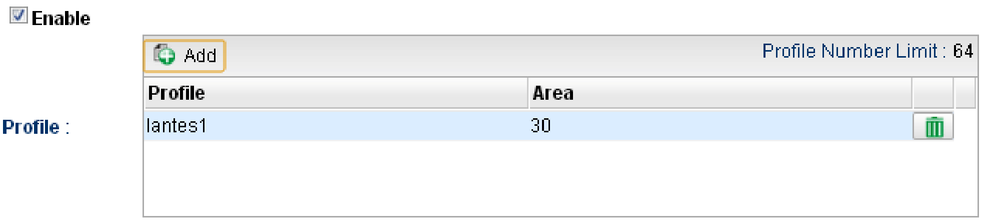


4. Use the drop down list of LAN/WAN Profile to choose the one you need. And specify the value of Area (either 0.0.0.0 ~ 255.255.255.255 or 0 ~ 4294967295) for that profile.



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

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



☑ Enable

Profile :

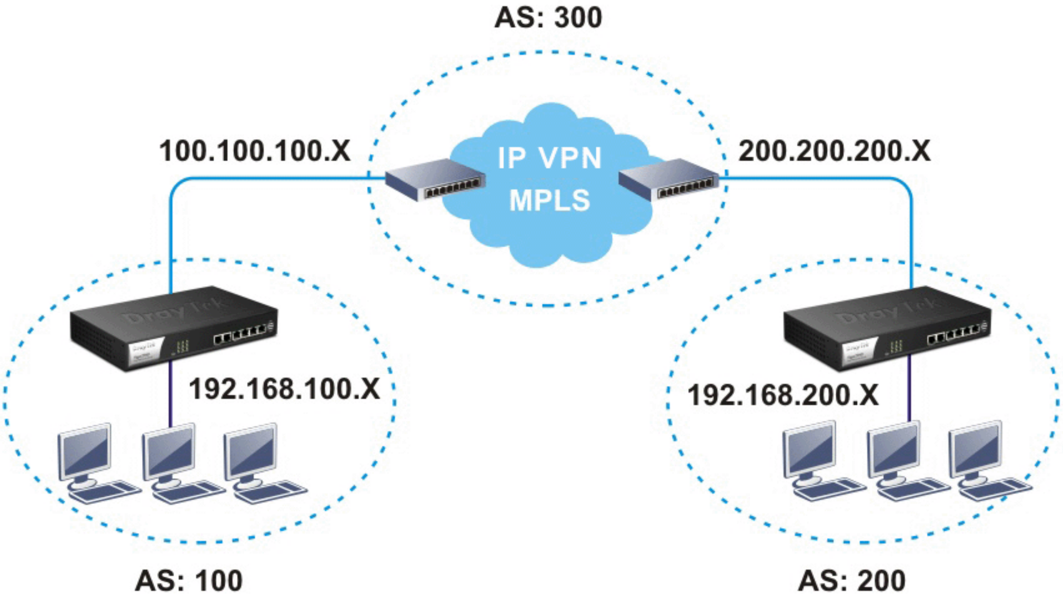
Profile	Area	
lantes1	30	🗑

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.

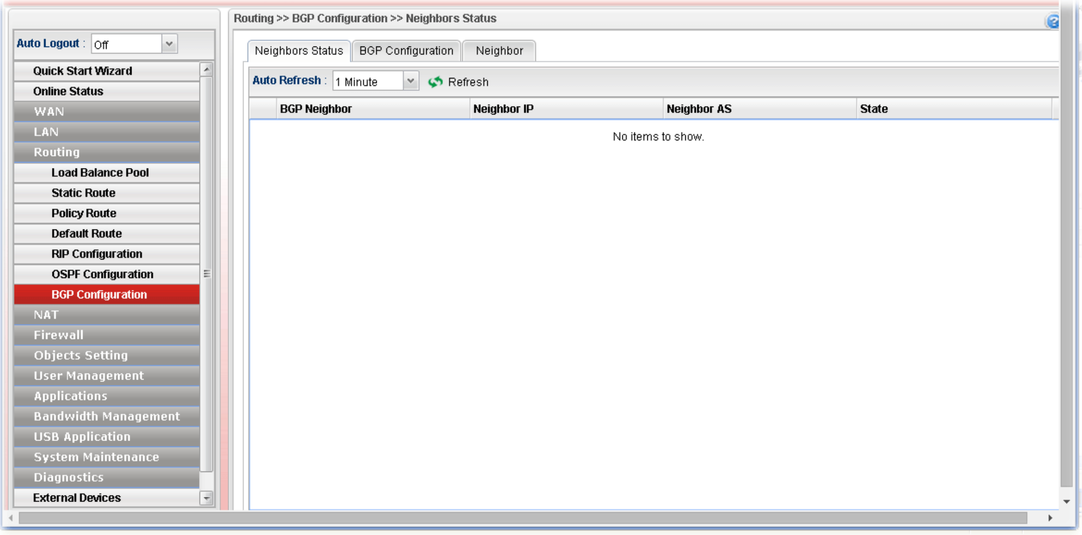
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the “neighbor” of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

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.



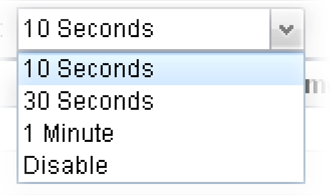
Routing >> BGP Configuration >> Neighbors Status

Auto Refresh : 1 Minute

BGP Neighbor	Neighbor IP	Neighbor AS	State

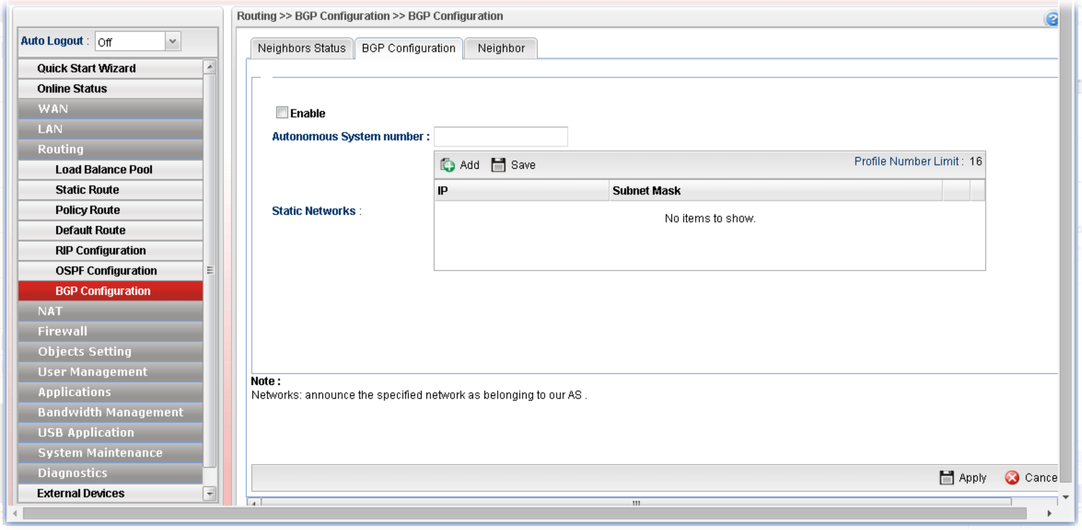
No items to show.

Available parameters are listed as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked.  10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
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.



Routing >> BGP Configuration >> BGP Configuration

□ Enable

Autonomous System number :

Static Networks :

Profile Number Limit : 16

IP	Subnet Mask
No items to show.	

Note :
Networks: announce the specified network as belonging to our AS .

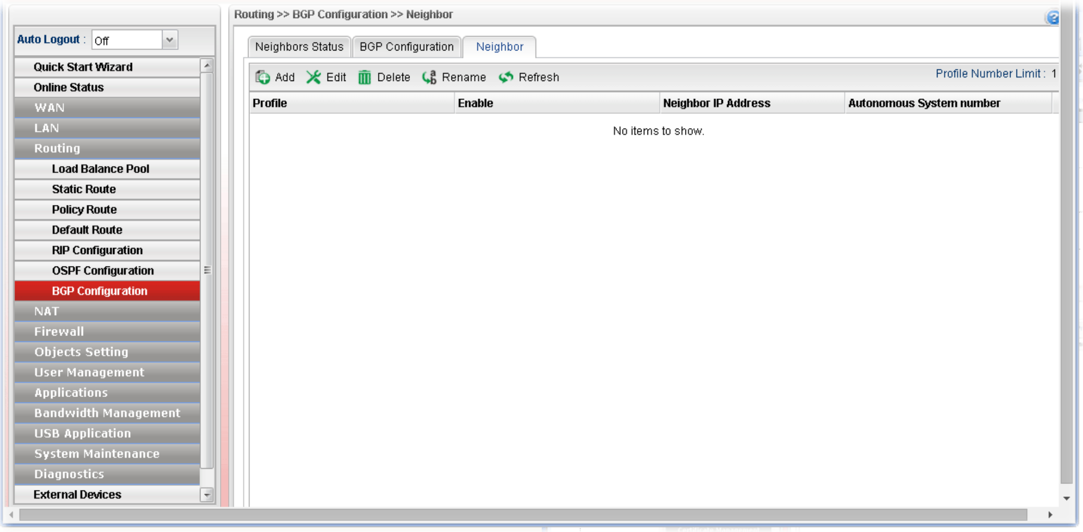
Available parameters are listed as follows:

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

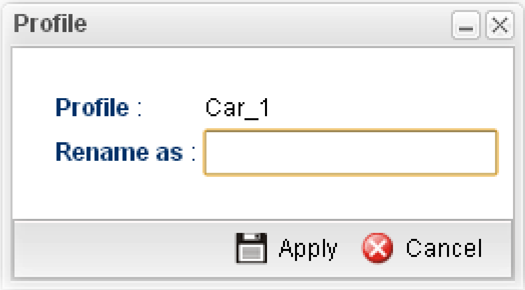
This page is used to configure the IP address and AS number for the neighbor which will exchange BGP routing information with your Vigor router.



Profile	Enable	Neighbor IP Address	Autonomous System number

No items to show.

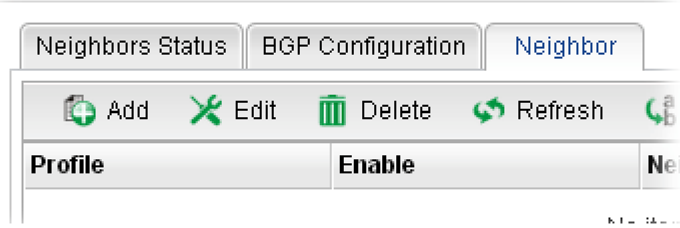
Available parameters are listed as follows:

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.  Profile : Car_1 Rename as : Before using such function, there is one profile existed at least.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.

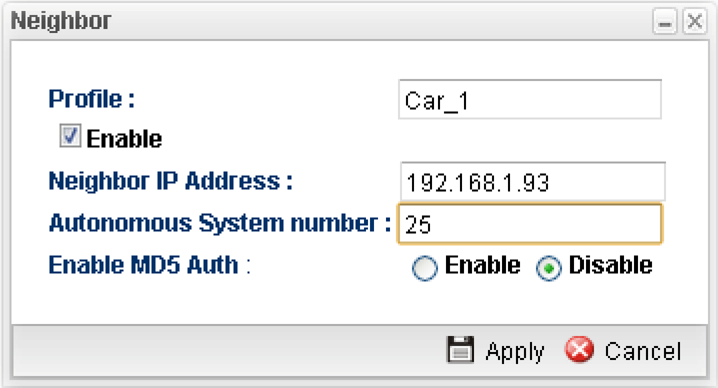
Neighbor IP Address	Display the IP address of the neighbor**.**
Autonomous System Number	Display the autonomous system number of the neighbor in BGP application.

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.



Profile : Car_1

☑ Enable

Neighbor IP Address : 192.168.1.93

Autonomous System number : 25

Enable MD5 Auth : ○ Enable ● Disable

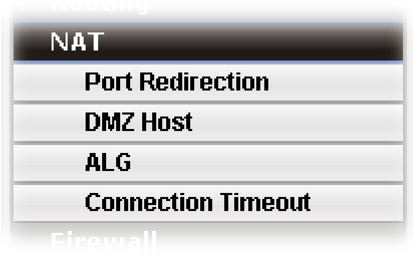
Available parameters are listed as follows:

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

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

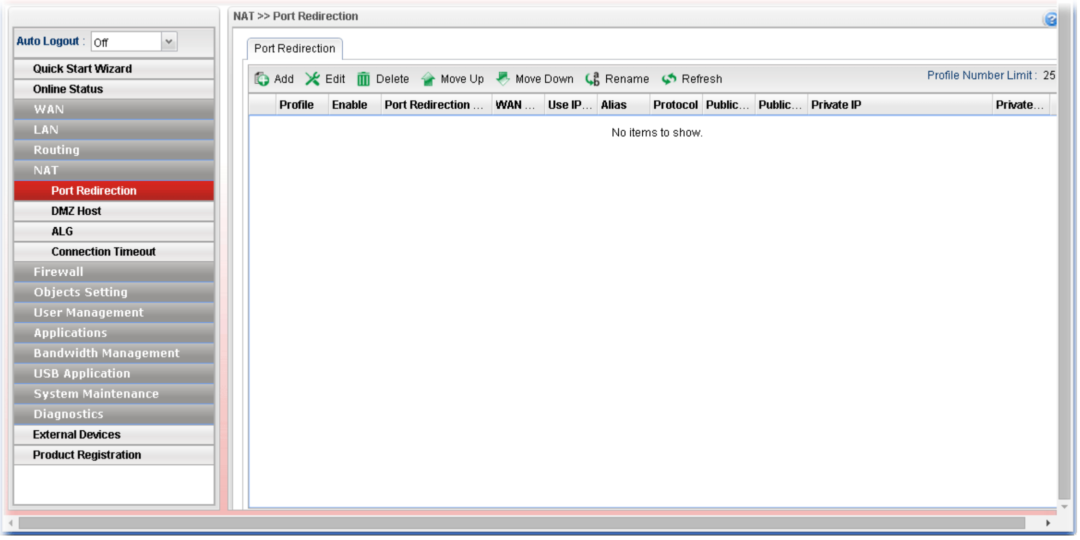
4.4 NAT

NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services. It allows the internal IP addresses of many computers on a LAN to be translated to one public address to save costs and resources of multiple public IP addresses. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. The Vigor300B Series is NAT-enabled by default and gets one globally routable IP addresses from the ISP by Static, PPPoE, or DHCP mechanism. The Vigor300B Series assigns private network IP addresses according to RFC-1918 protocol and translates the private network addresses to a globally routable IP address so that local hosts can communicate with the router and access the Internet.



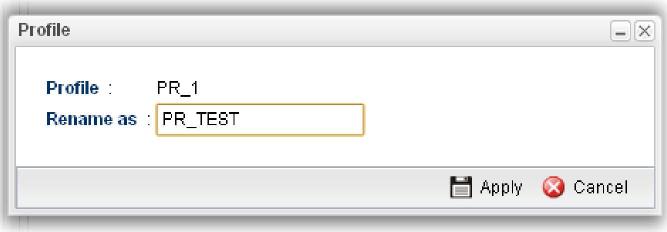
4.4.1 Port Redirection

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



Each item will be explained as follows:

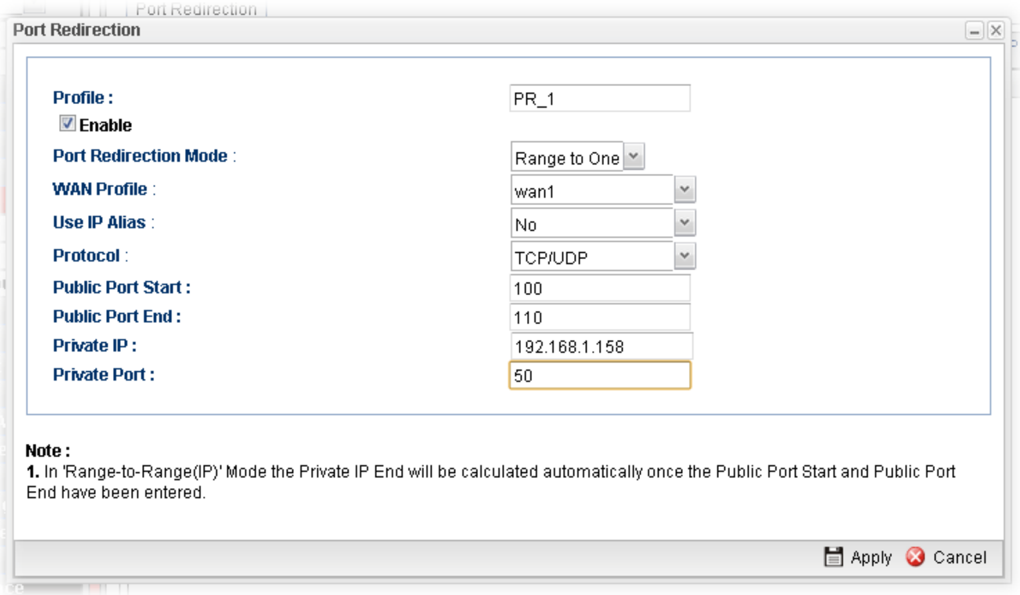
Item	Description
Add	Add a new port redirect profile.

Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.  Profile Profile : PR_1 Rename as : PR_TEST Apply Cancel
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Port Redirection Mode	Display the direction for the port to be redirected.
WAN Profile	Display the WAN interface of this profile.
Use IP Alias	Display the type (no, Single_Alias, All) the IP Alias used.
Alias	Display the selected WAN IP address.
Protocol	Display the protocol used for the entry.
Public Port Start	Display the starting number of the public port.
Public Port End	Display the ending number of the public port.
Private IP	Display the private IP used for this entry.
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.



Port Redirection

Profile : PR_1

☑ Enable

Port Redirection Mode : Range to One

WAN Profile : wan1

Use IP Alias : No

Protocol : TCP/UDP

Public Port Start : 100

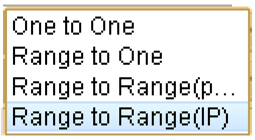
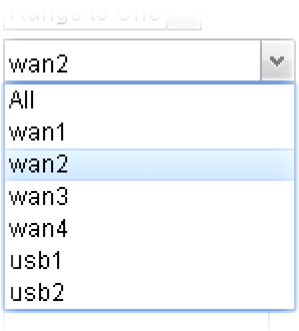
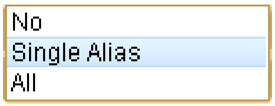
Public Port End : 110

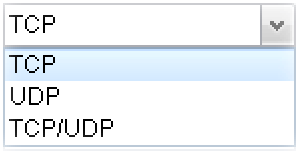
Private IP : 192.168.1.158

Private Port : 50

Note :
1. In 'Range-to-Range(IP)' Mode the Private IP End will be calculated automatically once the Public Port Start and Public Port End have been entered.

Available parameters are listed as follows:

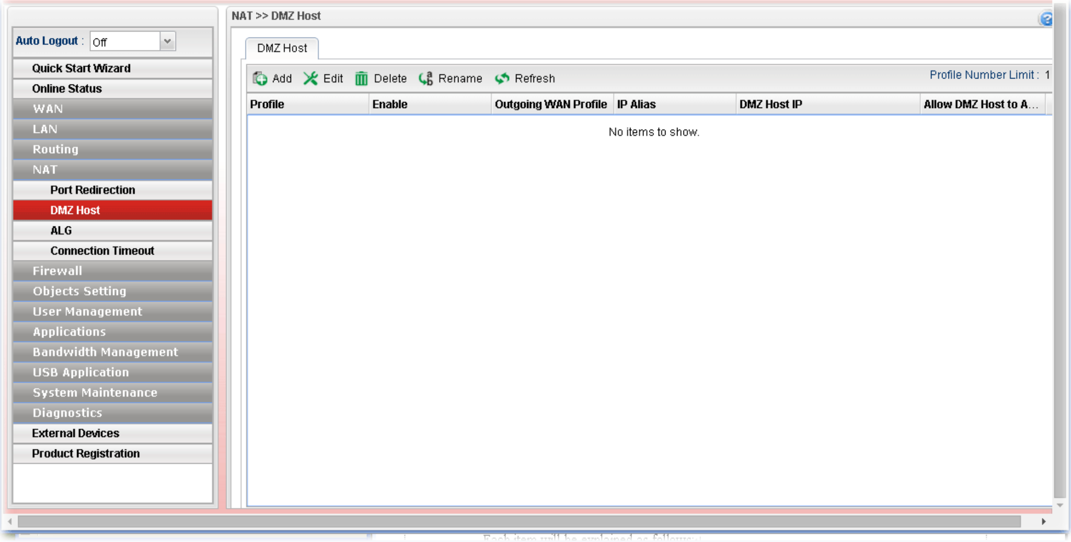
Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Port Redirection Mode	Specify the direction for the port to be redirected.  One to One Range to One Range to Range(p... Range to Range(IP)
WAN Profile	Specify the WAN profile for such profile.  wan2 All wan1 wan2 wan3 wan4 usb1 usb2
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.  No Single Alias All **Single Alias** – You have to type one IP address used for IP Alias. **All** – All the IP address can be treated as IP Alias.

Alias	WAN IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
Protocol	Choose the protocol used for the entry. 
Public Port Start/ Public Port End	It is available when **Range to One** or **Range to Range (port) or Range to Range (IP)** is selected as Port Redirection Mode. Type the starting/ending number of the public port. For Range-to-One, set both Start and End values with the same value.
Private IP 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 IP	Specify the private IP address of the internal host providing the service. Simply type the private IP used for this entry.
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.

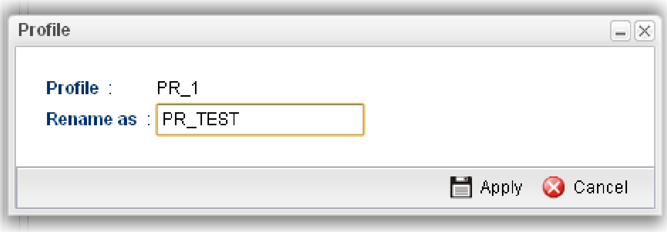


Profile	Enable	Outgoing WAN Profile	IP Alias	DMZ Host IP	Allow DMZ Host to A...

No items to show.

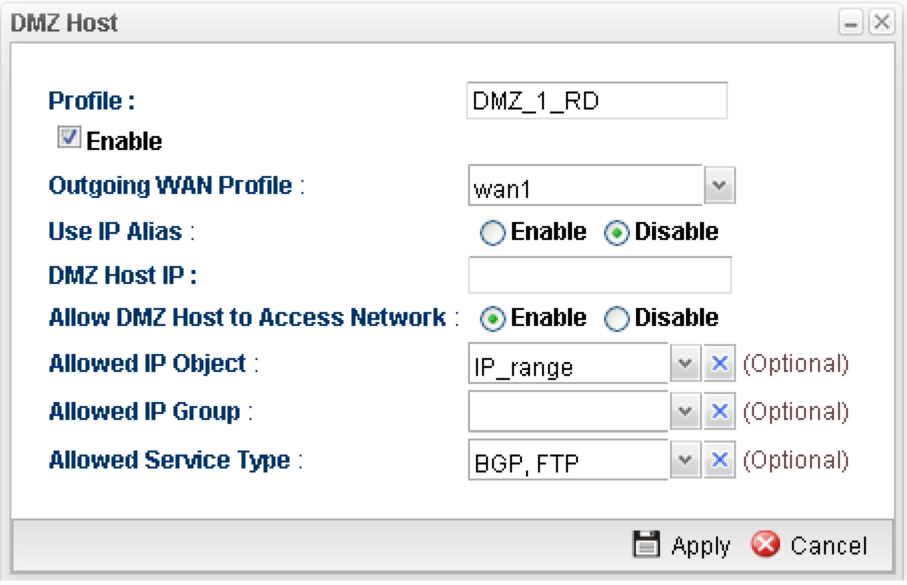
Each item will be explained as follows:

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.  Profile Profile : PR_1 Rename as : PR_TEST
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.



DMZ Host

Profile : DMZ_1_RD

☑ Enable

Outgoing WAN Profile : wan1

Use IP Alias : ○ Enable ● Disable

DMZ Host IP :

Allow DMZ Host to Access Network : ● Enable ○ Disable

Allowed IP Object : IP_range (Optional)

Allowed IP Group : (Optional)

Allowed Service Type : BGP, FTP (Optional)

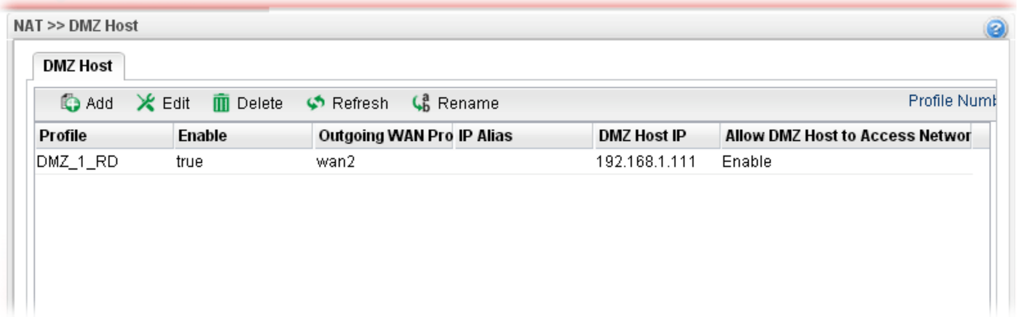
Available parameters are listed as follows:

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.

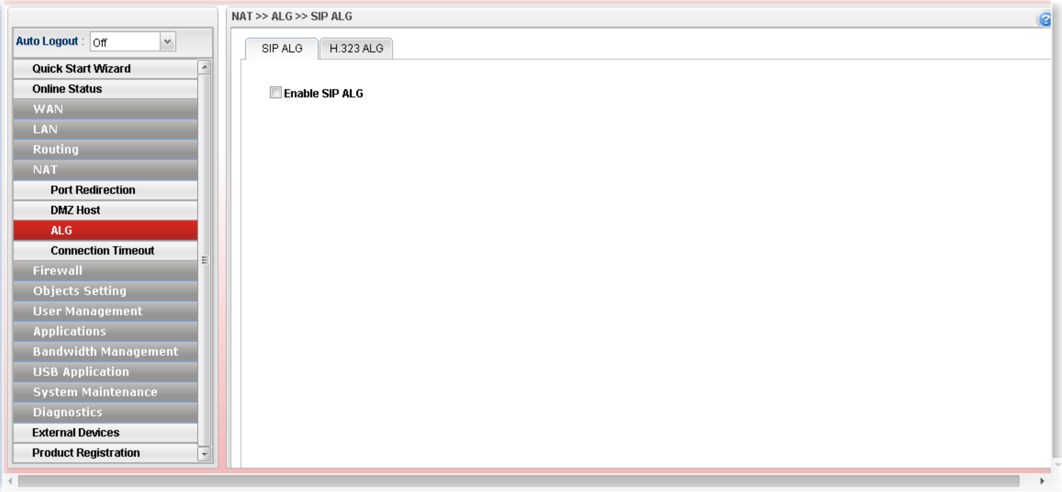


Profile	Enable	Outgoing WAN Pro	IP Alias	DMZ Host IP	Allow DMZ Host to Access Networ
DMZ_1_RD	true	wan2		192.168.1.111	Enable

4.4.3 ALG

4.4.3.1 SIP ALG

SIP ALG means **Session Initiation Protocol, Application Layer Gateway**. This page allows you to choose LAN and WAN profiles for Vigor router to make SIP message and RTP packets of voice being transmitting and receiving correctly via NAT.



□ Enable SIP ALG

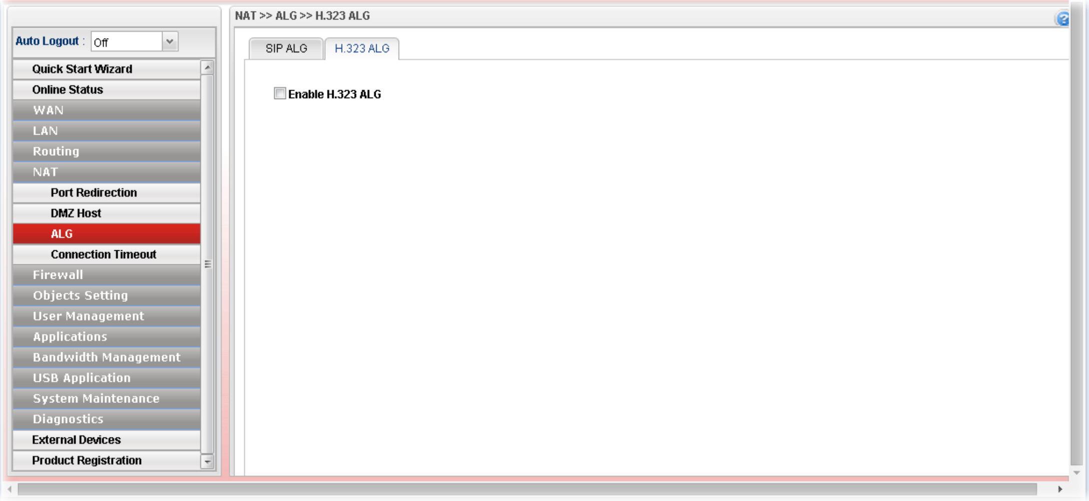
Available parameters are listed as follows:

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

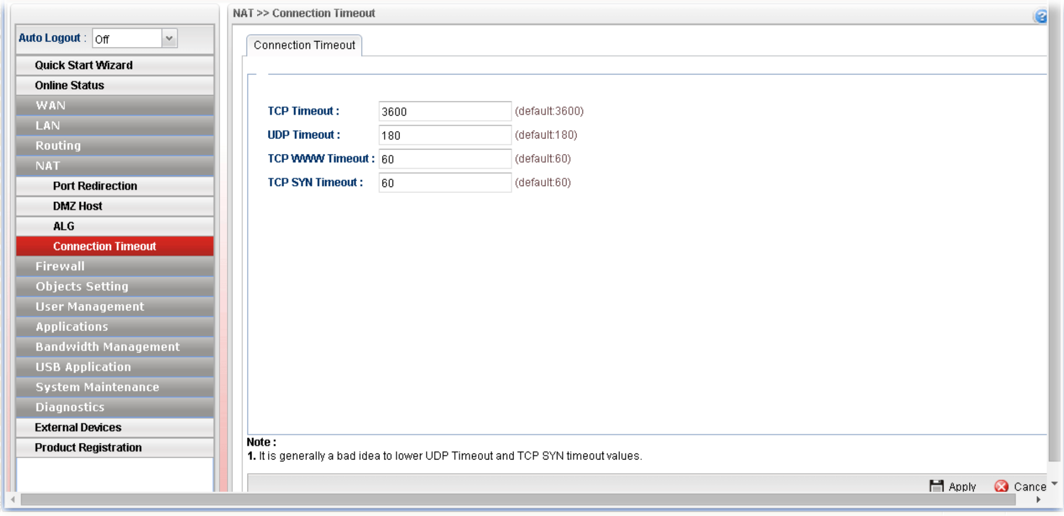
The H.323 ALG allows incoming and outgoing VoIP calls passing through NAT. If required, check the box and click **Apply** to save the settings.



□ Enable H.323 ALG

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.



TCP Timeout : 3600 (default:3600)

UDP Timeout : 180 (default:180)

TCP WWW Timeout : 60 (default:60)

TCP SYN Timeout : 60 (default:60)

Note :
1. It is generally a bad idea to lower UDP Timeout and TCP SYN timeout values.

Available parameters are listed as follows:

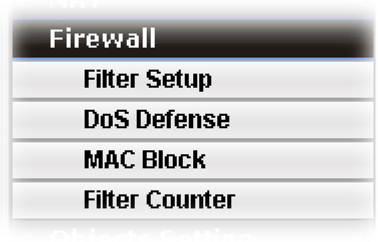
Item	Description
TCP Timeout	Set a time limit for sessions established by TCP (except Port 80 and Port 443).
UDP Timeout	Set a time limit for sessions established by UDP.
TCP WWW Timeout	Set a time limit for sessions established by TCP Port 80 and Port 443.
TCP SYN Timeout	Set a time limit for sessions 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 Vigor300B Series mainly consists of packet filtering, Denial of Service (DoS) and URL (Universal Resource Locator) content filtering facilities. These firewall filters help to protect your local network against attack from outsiders. A firewall also provides a way of restricting users on the local network from accessing inappropriate Internet content and can filter out specific packets, which may trigger unexpected outgoing connection such as a Trojan.

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

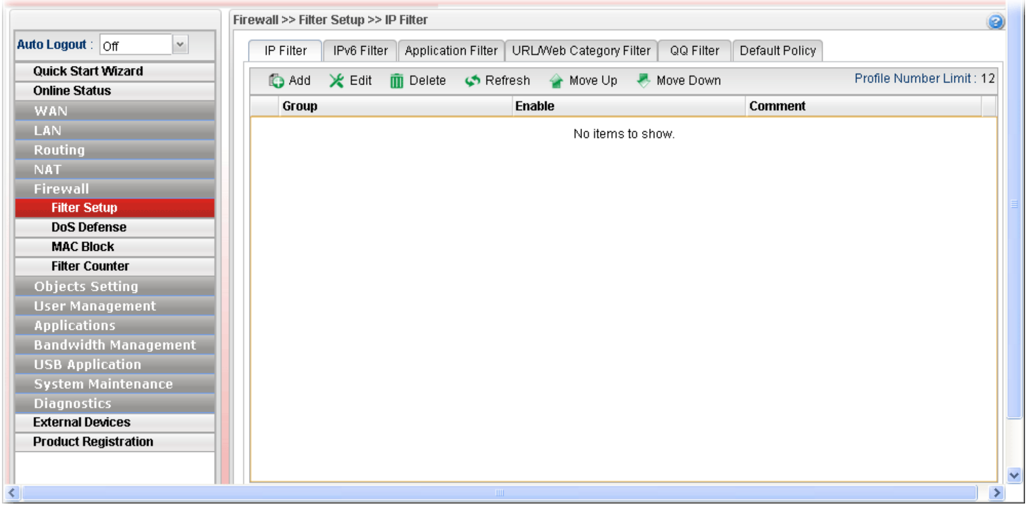


4.5.1 Filter Setup

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

4.5.1.1 IP Filter

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



Each item will be explained as follows:

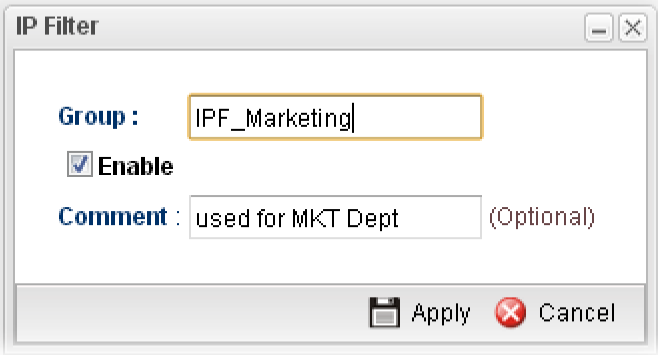
Item	Description
Add	Add a new group profile for IP filter.
Edit	Modify the selected profile.

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

How to create an IP Filter group

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

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



IP Filter

Group : IPF_Marketing

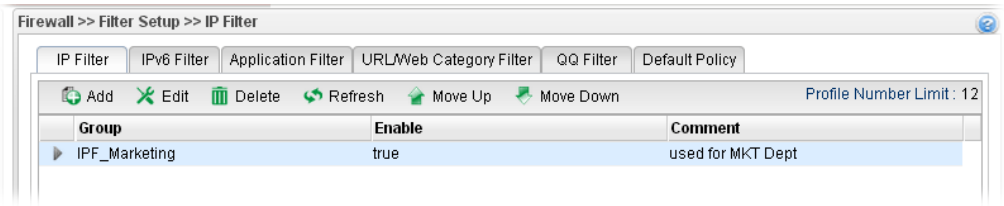
☑ Enable

Comment : used for MKT Dept (Optional)

Available parameters are listed as follows:

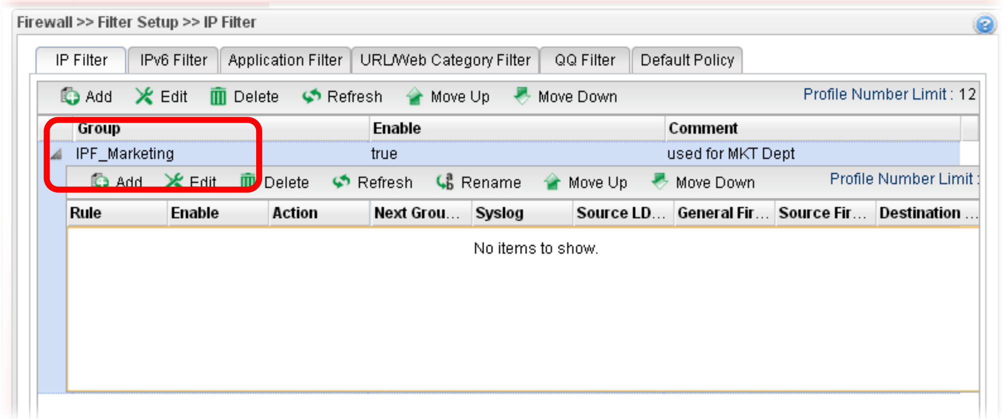
Item	Description
Group	Type the name of the IP filter group.
Enable	Check the box to enable this profile.
Comment	Give a brief description for the profile.

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



Group	Enable	Comment
IPF_Marketing	true	used for MKT Dept

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.

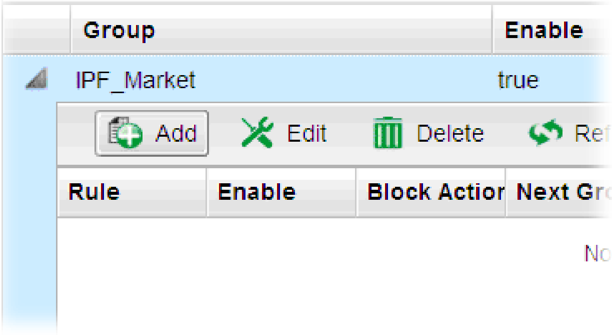


Group	Enable	Comment
IPF_Marketing	true	used for MKT Dept

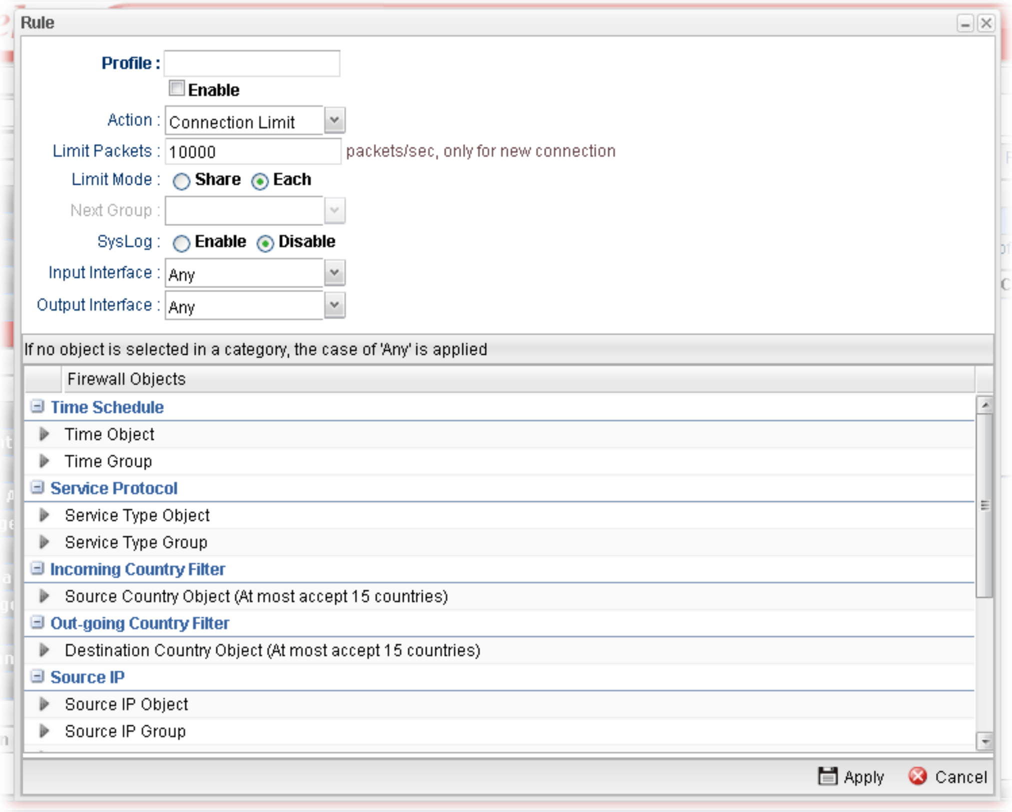
Rule	Enable	Action	Next Grou...	Syslog	Source LD...	General Fir...	Source Fir...	Destination ...

No items to show.

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



8. The following page for configuration will appear.



Rule

Profile :

□ Enable

Action : Connection Limit

Limit Packets : 10000 packets/sec, only for new connection

Limit Mode : ○ Share ● Each

Next Group :

SysLog : ○ Enable ● Disable

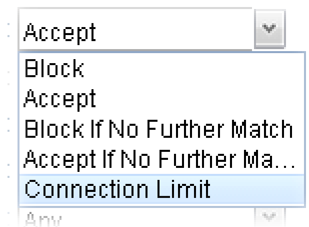
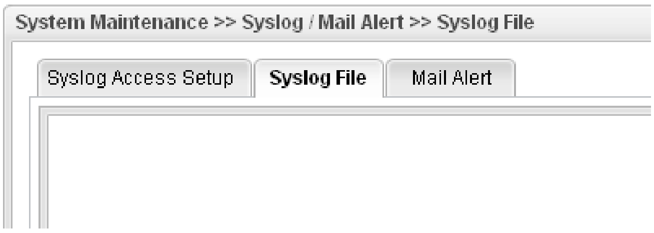
Input Interface : Any

Output Interface : Any

If no object is selected in a category, the case of 'Any' is applied

Available parameters are listed as follows:

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

	 Accept Block Accept Block If No Further Match Accept If No Further Ma... Connection Limit Any
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	When you choose **Connection Limit** as **Action,** you have to choose Share or Each in addition to the number of packets limits. **Share** – It means the total IP addresses in a segment will be limited with certain packets number per second. **Each** –It means each IP will be limited with certain packets number per second.
Next Group	When you choose **Block If No Further Match** or **Accept If No Further Match** as **Action**, you have to specify next IP filter group for further matching.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance >> Syslog/Mail Alert >> Syslog File**.  System Maintenance >> Syslog / Mail Alert >> Syslog File Syslog Access Setup Syslog File Mail Alert
Input Interface	Choose one of the LAN or WAN profiles as data receiving interface.
Output Interface	Choose one of the LAN or WAN profiles as data transmitting interface.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
Service Protocol	**Service Type Object** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type object profiles from the drop down list. The selected profile will be treated as service type. You can click ⊕ to create another new service type object profile. **Service Type Group** –Click the triangle icon ▶ to display

	the profile selection box. Choose one or more service type group profiles from the drop down list. The selected profile will be treated as service type. You can click ⊕ to create another new service type group profile.
Incoming Country Filter	**Source Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an incoming country filter. You can click ⊕ to create another new filter profile.
Outgoing Country Filter	**Destination Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an outgoing country filter. You can click ⊕ to create another new filter profile.
Source IP	**Source IP Object -** 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. **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. **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. **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. **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.
Destination IP	**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. **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

	will be treated as destination target. You can click ⊕ to create another new IP group profile. **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. **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. **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. **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.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

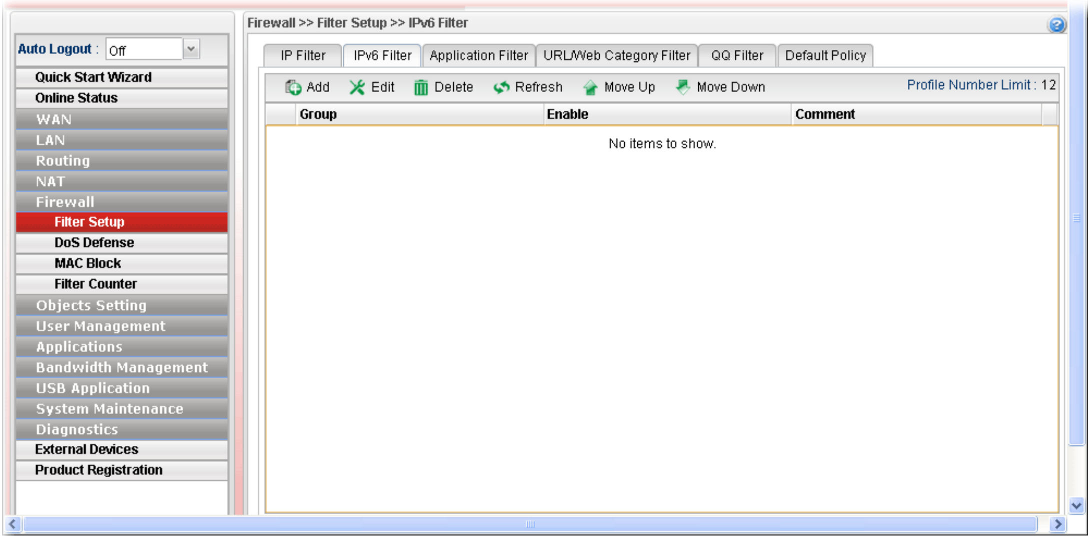
9. Enter all the settings and click **Apply**.

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

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

4.5.1.2 IPv6 Filter

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



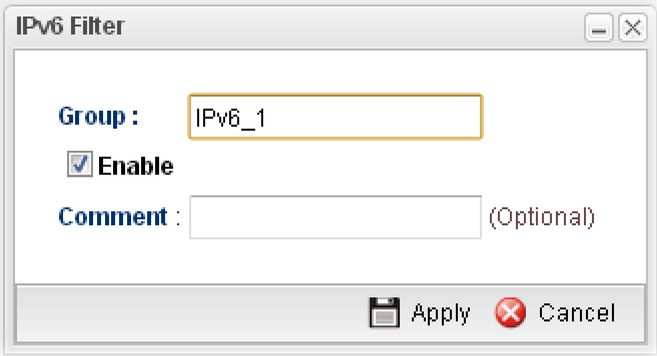
Each item will be explained as follows:

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

How to create an IPv6 Filter group

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

1. Open **Firewall>>Filter Setup** and click the **IPv6 Filter** tab.
2. Simply click the **Add** button.
3. The following dialog will appear.



Group : IPv6_1

☑ Enable

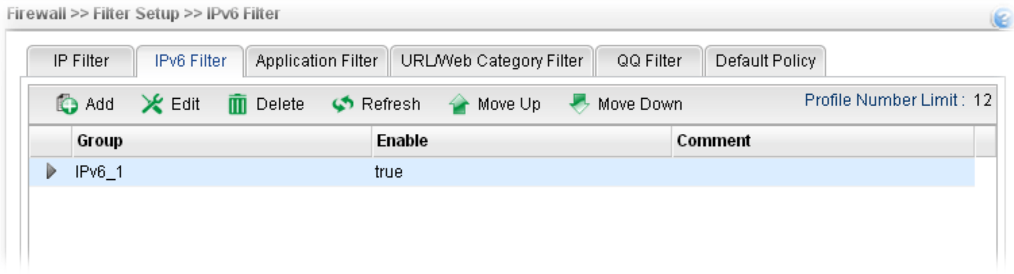
Comment : (Optional)

Available parameters are listed as follows:

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

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

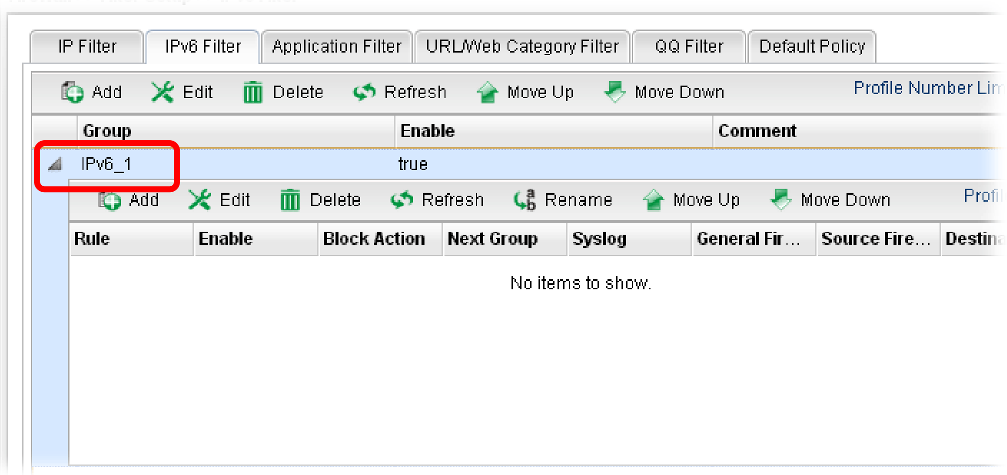
5. A new filter group has been added.



Profile Number Limit : 12

Group	Enable	Comment
IPv6_1	true	

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.

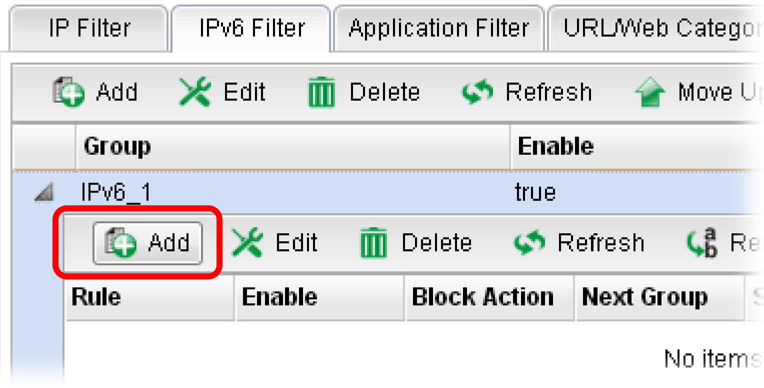


Group	Enable	Comment
IPv6_1	true	

Rule	Enable	Block Action	Next Group	Syslog	General Fir...	Source Fire...	Destin

No items to show.

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

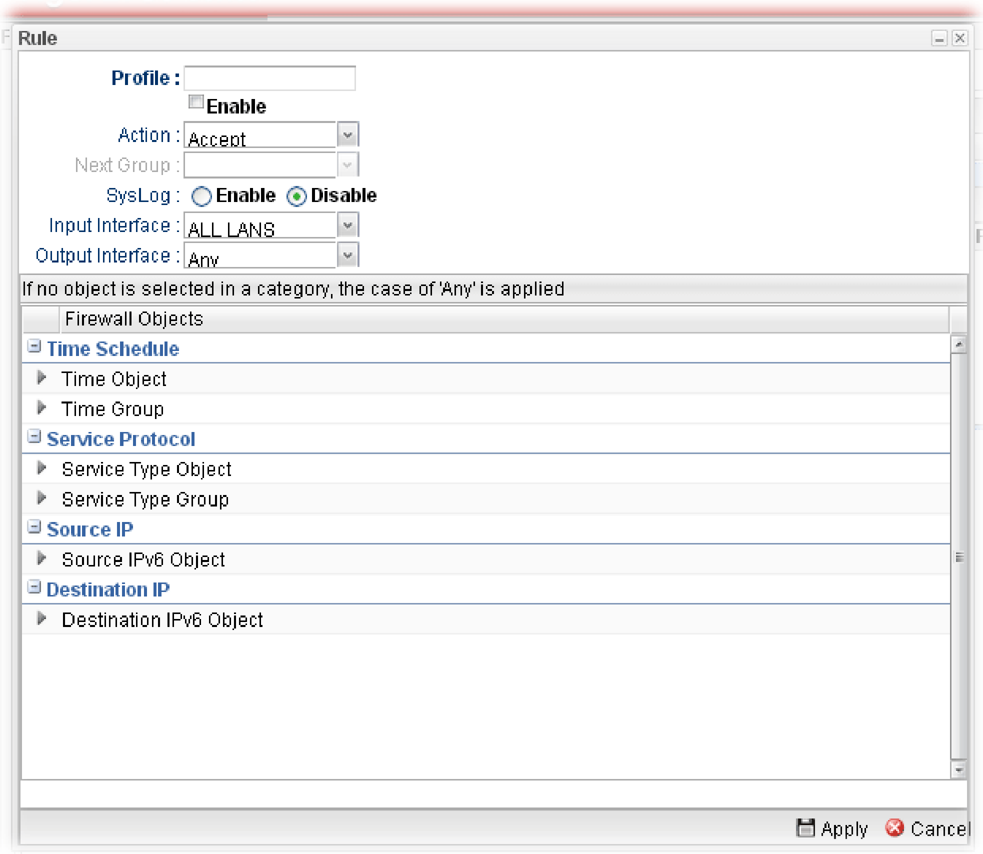


Group	Enable
IPv6_1	true

Rule	Enable	Block Action	Next Group

No items

8. The following page for configuration will appear.



Profile :

□ Enable

Action : Accept

Next Group :

SysLog : ○ Enable ● Disable

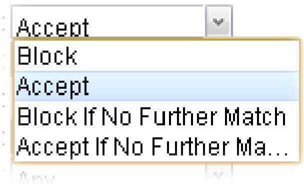
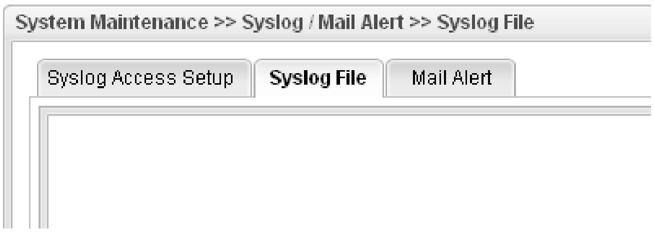
Input Interface : ALL LANS

Output Interface : Any

If no object is selected in a category, the case of 'Any' is applied

Available parameters are listed as follows:

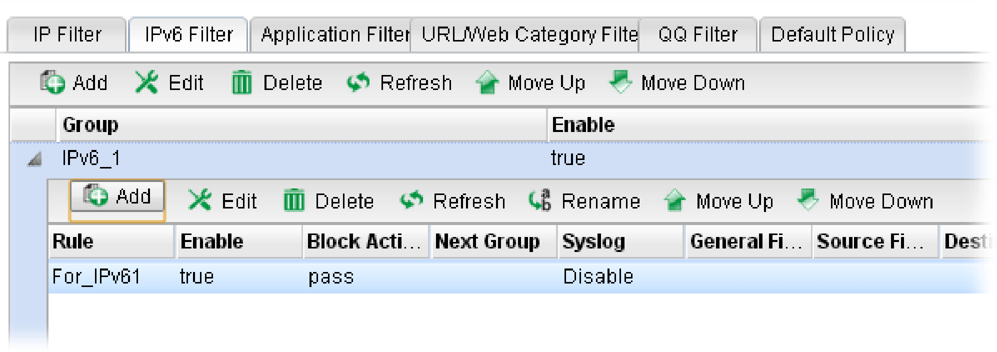
Item	Description
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Action	The action to be taken when packets match the rule. **Block -** Packets matching the rule will be dropped immediately **Accept-** Packets matching the rule will be passed immediately. **Block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

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

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

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

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



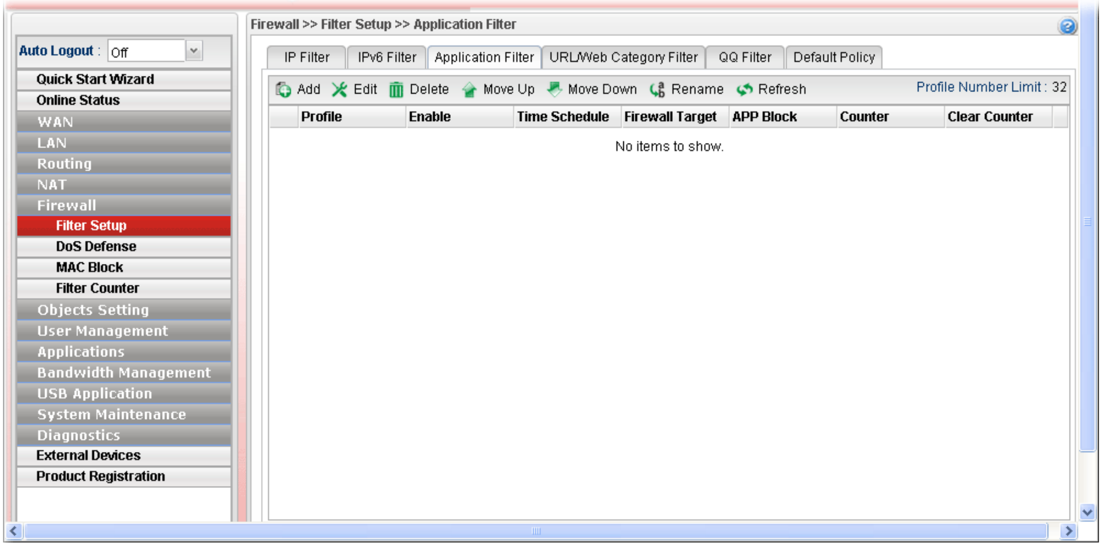
Group	Enable
IPv6_1	true

Rule	Enable	Block Acti...	Next Group	Syslog	General Fi...	Source Fi...	Dest
For_IPv61	true	pass		Disable			

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.



Profile	Enable	Time Schedule	Firewall Target	APP Block	Counter	Clear Counter

No items to show.

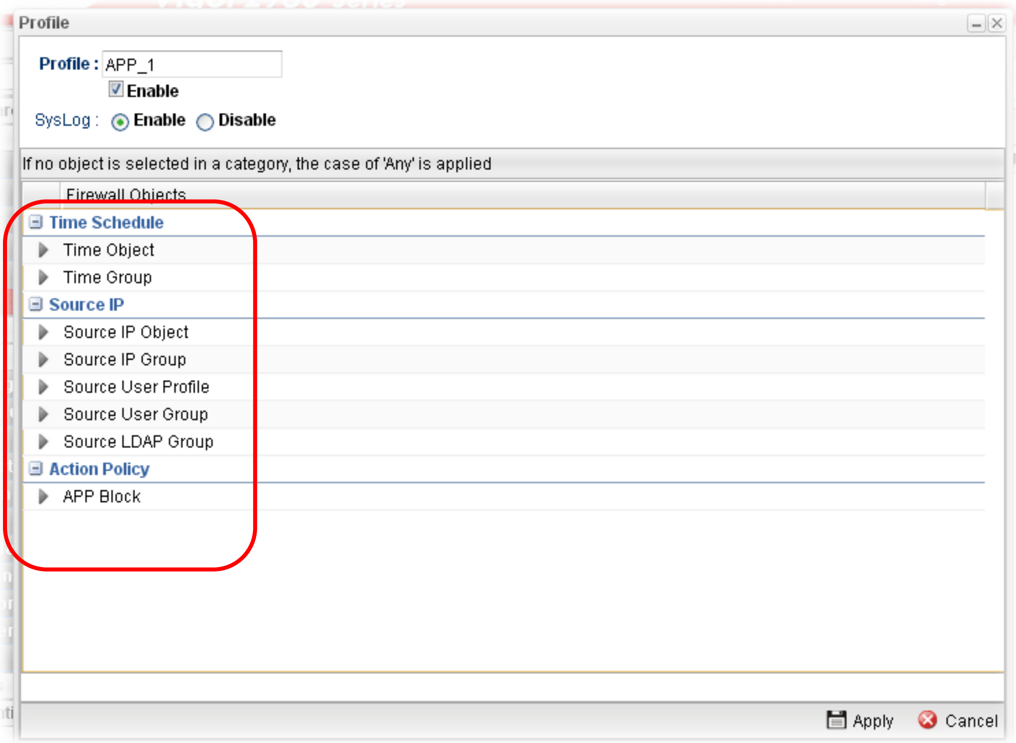
Each item will be explained as follows:

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.
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).

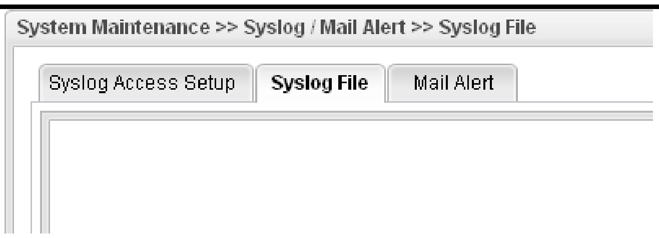


Profile : APP_1
☑ Enable
SysLog : ● Enable ○ Disable

If no object is selected in a category, the case of 'Any' is applied

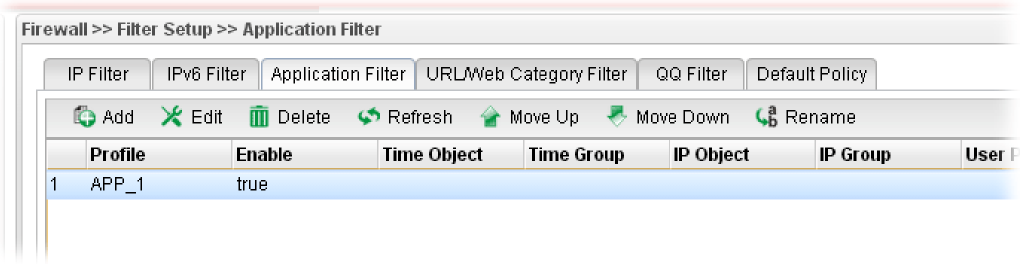
Available parameters are listed as follows:

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**.

	 System Maintenance >> Syslog / Mail Alert >> Syslog File
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click ⊕ to create another new time object profile, or you can click the edit icon ✎ to modify the existed object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile, or you can click the edit icon ✎ to modify the existed group profile.
Source IP	**Source IP Object -** Click the triangle icon ▶ to display the profile selection box. **C**hoose 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. **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. **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. **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. **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.
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.

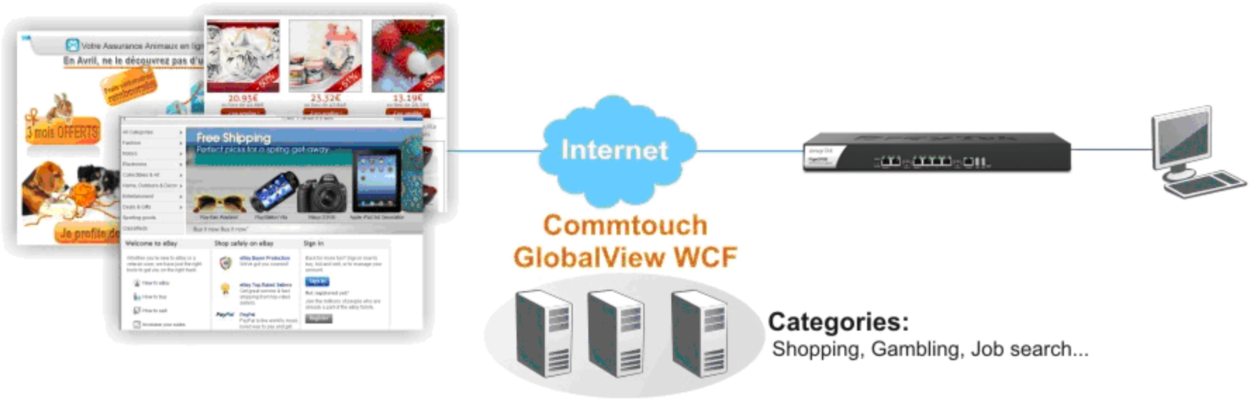
4. Enter all the settings and click **Apply**.
5. A new Application filter profile has been added.

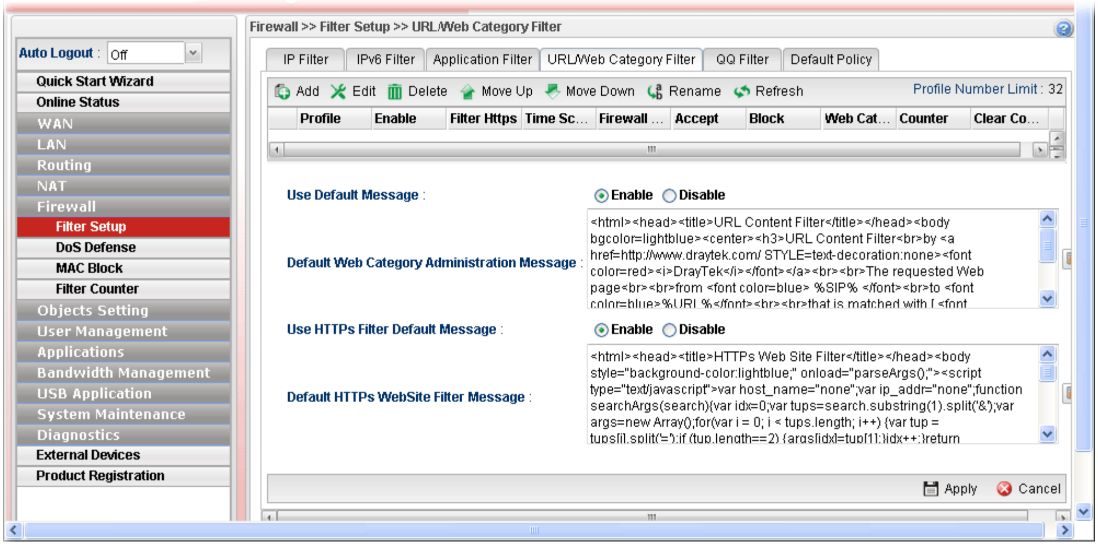


	Profile	Enable	Time Object	Time Group	IP Object	IP Group	User P
1	APP_1	true					

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.





Profile Number Limit : 32

Profile	Enable	Filter Https	Time Sc…	Firewall …	Accept	Block	Web Cat…	Counter	Clear Co…

Use Default Message : ● Enable ○ Disable

Default Web Category Administration Message :

```
<html><head><title>URL Content Filter</title></head><body
bgcolor=lightblue><center><h3>URL Content Filter<br>by <a
href=http://www.draytek.com/ STYLE=text-decoration:none><font
color=red><i>DrayTek</i></font></a><br><br>The requested Web
page<br><br>from <font color=blue> %SIP% </font><br>to <font
color=blue>%URL %</font><br><br>that is matched with [ <font
```

Use HTTPs Filter Default Message : ● Enable ○ Disable

Default HTTPs WebSite Filter Message :

```
<html><head><title>HTTPs Web Site Filter</title></head><body
style="background-color:lightblue;" onload="parseArgs();"><script
type="text/javascript">var host_name="none";var ip_addr="none";function
searchArgs(search){var idx=0;var tups=search.substring(1).split('&');var
args=new Array();for(var i = 0; i < tups.length; i++) {var tup =
tups[i].split('=');if (tup.length==2) {args[idx]=tup[1];}idx++;}return
```

Each item will be explained as follows:

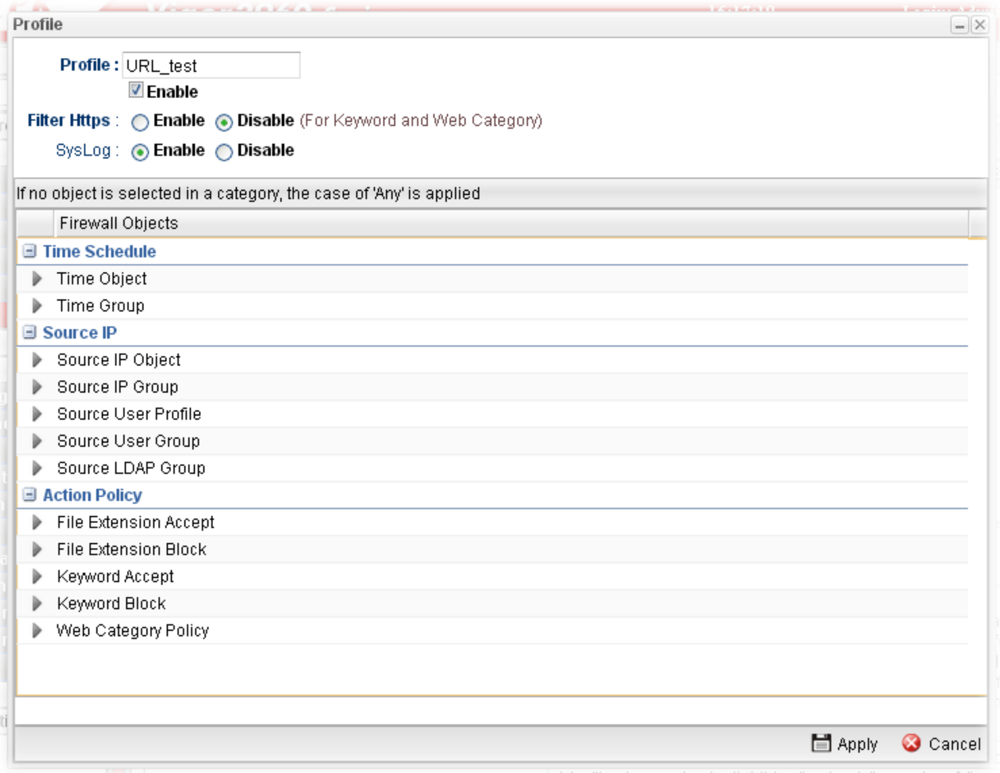
Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected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

Item	Description
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.
Apply	Click it to save and exit the dialog.

Item	Description
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.



Profile

Profile : URL_test

☑ Enable

Filter Https : ○ Enable ● Disable (For Keyword and Web Category)

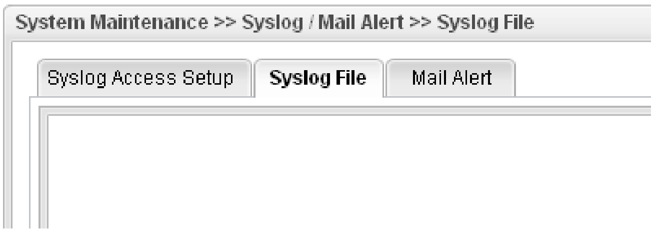
SysLog : ● Enable ○ Disable

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

- Time Schedule
  - Time Object
  - Time Group
- Source IP
  - Source IP Object
  - Source IP Group
  - Source User Profile
  - Source User Group
  - Source LDAP Group
- Action Policy
  - File Extension Accept
  - File Extension Block
  - Keyword Accept
  - Keyword Block
  - Web Category Policy

Available parameters are listed as follows:

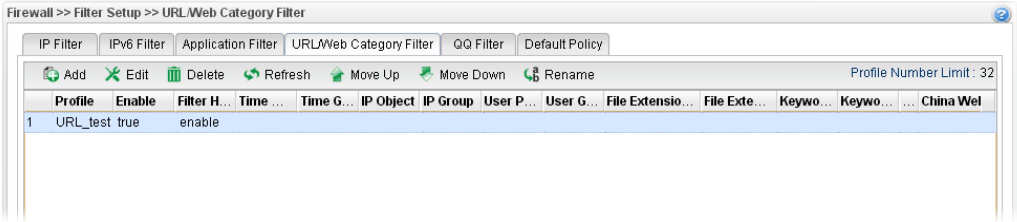
Item	Description
Profile	Type the name of the URL filter profile.
Enable	Check the box to enable this profile.
Filter https	**Enable** – Click it to enable the HTTPS filtering job. **Disable** – When only keyword and web category are selected for such rule, choose Disable.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance** >> **Syslog/Mail Alert** >> **Syslog File**.  System Maintenance >> Syslog / Mail Alert >> Syslog File

Item	Description
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click ➕ to create another new time object profile, or you can click the edit icon ✎ to modify the existed object profile. **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ➕ to create another new time group profile, or you can click the edit icon ✎ to modify the existed group profile.
Source IP	**Source IP Object** - 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. **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. **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. **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. **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.
Action Policy	**File Extension Accept / File Extension Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more File Extension object profiles from the drop down list which will be allowed / not be allowed to pass

Item	Description
	through the router. You can click to create another new File Extension object profile, or you can click the edit icon to modify the existed object profile. **Keyword Accept / Keyword Block -** Click the triangle icon ▶ to display the profile selection box. Choose e one or more keyword object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click to create another new keyword object profile, or you can click the edit icon to modify the existed object profile. **Web Category Policy -** Click the triangle icon ▶ to display the profile selection box. Choose one or more web category object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new web category object profile, or you can click the edit icon to modify the existed object profile. **China Web Category Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more web category object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new web category object profile, or you can click the edit icon to modify the existed object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

5. A new URL filter profile has been added.



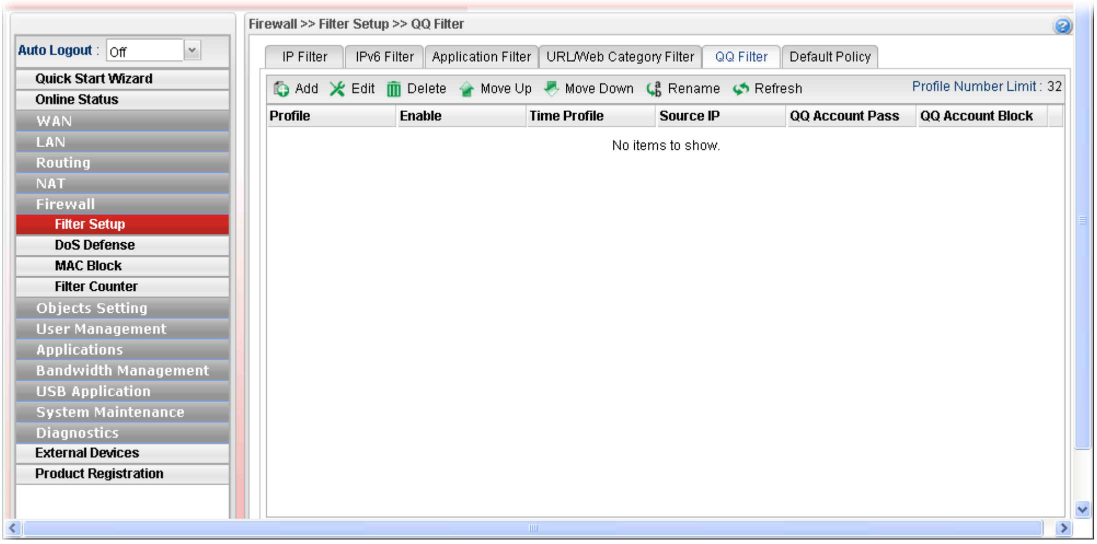
Firewall >> Filter Setup >> URL/Web Category Filter

Profile Number Limit : 32

	Profile	Enable	Filter H...	Time ...	Time G...	IP Object	IP Group	User P...	User G...	File Extensio...	File Exte...	Keywo...	Keywo...	...	China Wel
1	URL_test	true	enable												

4.5.1.5 QQ Filter

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



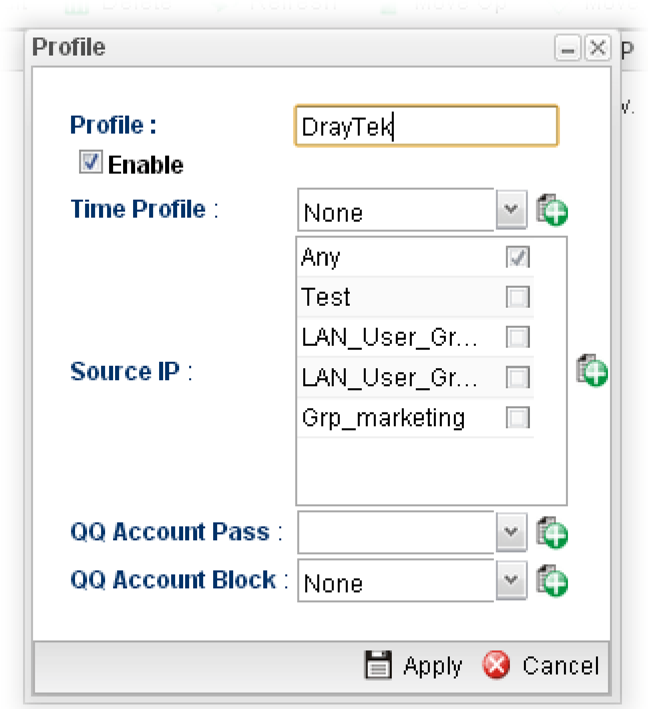
Each item will be explained as follows:

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



Profile

Profile : DrayTek

☑ Enable

Time Profile : None

Source IP :

Any	☑
Test	□
LAN_User_Gr...	□
LAN_User_Gr...	□
Grp_marketing	□

QQ Account Pass :

QQ Account Block : None

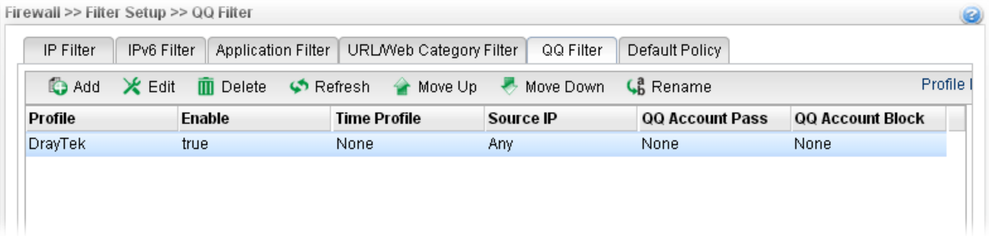
Available parameters are listed as follows:

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

Item	Description
	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.

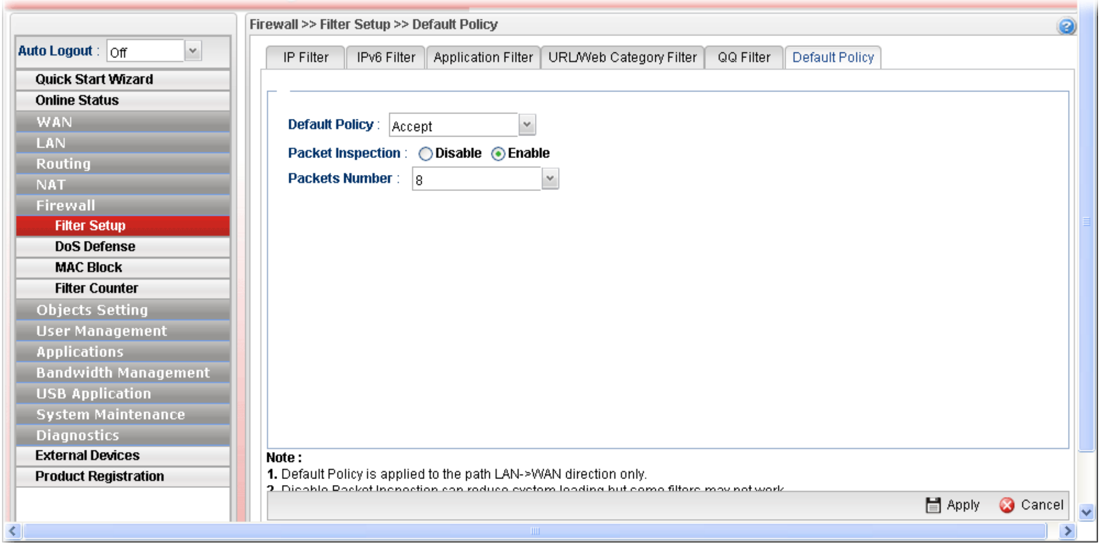


Firewall >> Filter Setup >> QQ Filter

Profile	Enable	Time Profile	Source IP	QQ Account Pass	QQ Account Block
DrayTek	true	None	Any	None	None

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.



Firewall >> Filter Setup >> Default Policy

Default Policy : Accept

Packet Inspection : ○ Disable ● Enable

Packets Number : 8

Note :

1. Default Policy is applied to the path LAN->WAN direction only.

2. Disable Packet Inspection can reduce system loading but some filters may not work.

Available parameters are listed as follows:

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

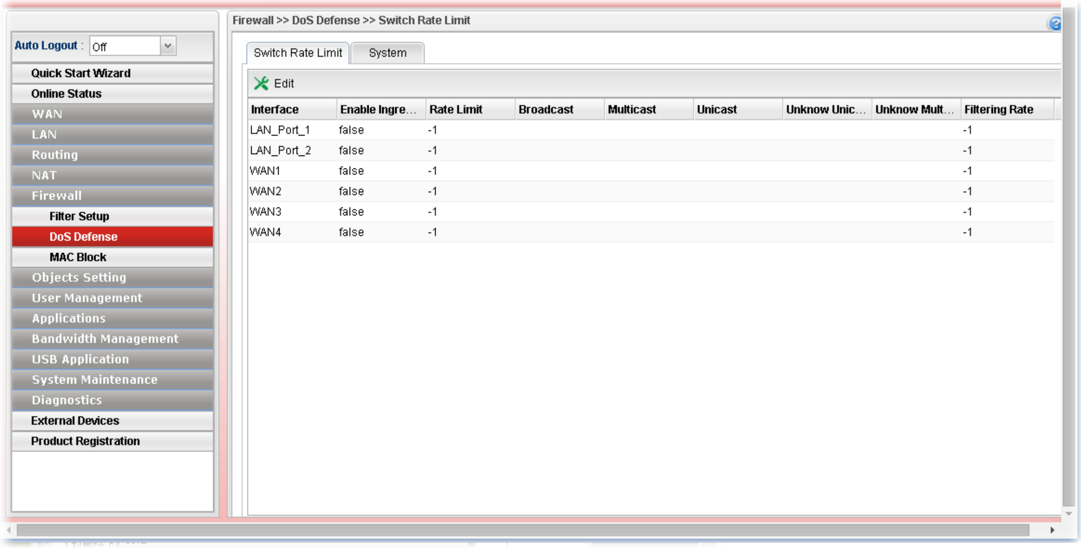
After finished the above settings, click **Apply** to save the configuration.

4.5.2 DoS Defense

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

4.5.2.1 Switch Rate Limit

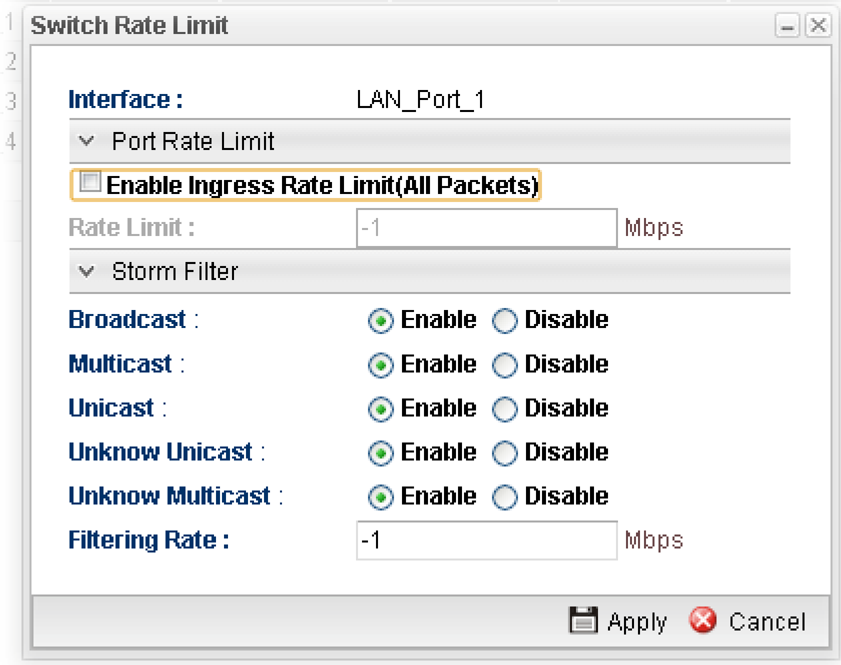
Default interface profiles will be shown on the page.



Firewall >> DoS Defense >> Switch Rate Limit

Interface	Enable Ingre...	Rate Limit	Broadcast	Multicast	Unicast	Unknow Unic...	Unknow Mult...	Filtering Rate
LAN_Port_1	false	-1						-1
LAN_Port_2	false	-1						-1
WAN1	false	-1						-1
WAN2	false	-1						-1
WAN3	false	-1						-1
WAN4	false	-1						-1

Choose one of the profiles and click **Edit**. You can modify the rate limit manually for each interface profile.



Switch Rate Limit

Interface : LAN_Port_1

Port Rate Limit

□ Enable Ingress Rate Limit(All Packets)

Rate Limit : -1 Mbps

Storm Filter

Broadcast : ● Enable ○ Disable

Multicast : ● Enable ○ Disable

Unicast : ● Enable ○ Disable

Unknow Unicast : ● Enable ○ Disable

Unknow Multicast : ● Enable ○ Disable

Filtering Rate : -1 Mbps

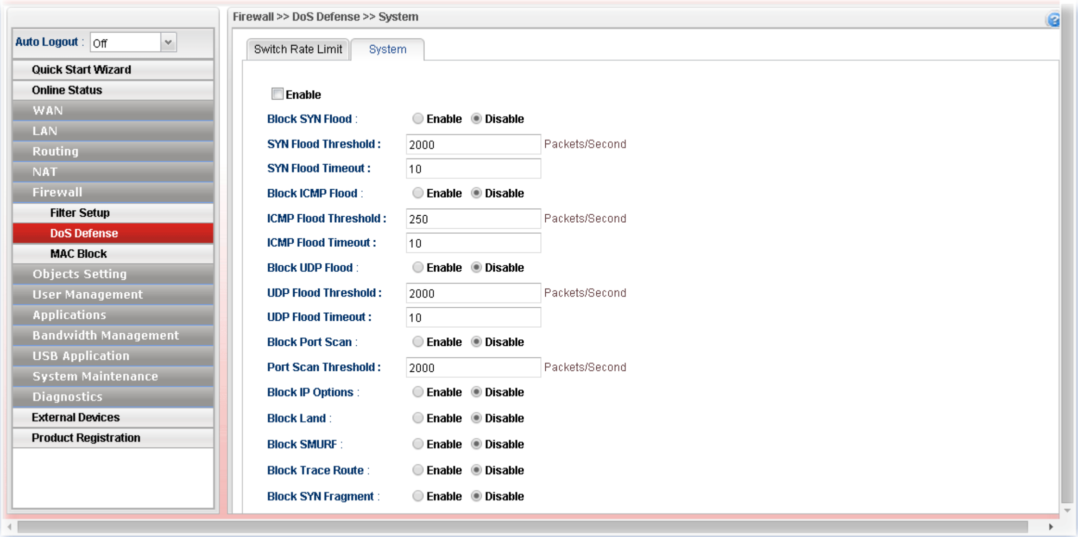
Available parameters are listed as follows:

Item	Description
Interface	Display the interface selected.
Port Rate Limit	**Enable Ingress Rate Limit (All Packets)** – Check the box to make all packets will be limited by the rate limit. **Rate Limit** – The default setting is “-1”. It means no limit.
Storm Filter	**Broadcast -** Click **Enable** to block the packets attacks coming from broadcast storm. **Multicast -** Click **Enable** to block the packets attacks coming from multicast storm. **Unicast -** Click **Enable** to block the packets attacks coming from unicast storm. **Unknown Unicast –**Click **Enable** to block the packets attacks coming from unknown unicast storm. **Unknown Multicast -** Click **Enable** to block the packets attacks coming from unknown multicast storm. **Filtering Rate –** Type a number (1~4096, unit is 64Kpbs) required for filtering.
Apply	Click it to save the configuration.

After finished the above settings, click **Apply** 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.



Firewall >> DoS Defense >> System

□ Enable

Block SYN Flood : ○ Enable ● Disable

SYN Flood Threshold : 2000 Packets/Second

SYN Flood Timeout : 10

Block ICMP Flood : ○ Enable ● Disable

ICMP Flood Threshold : 250 Packets/Second

ICMP Flood Timeout : 10

Block UDP Flood : ○ Enable ● Disable

UDP Flood Threshold : 2000 Packets/Second

UDP Flood Timeout : 10

Block Port Scan : ○ Enable ● Disable

Port Scan Threshold : 2000 Packets/Second

Block IP Options : ○ Enable ● Disable

Block Land : ○ Enable ● Disable

Block SMURF : ○ Enable ● Disable

Block Trace Route : ○ Enable ● Disable

Block SYN Fragment : ○ Enable ● Disable

Available parameters are listed as follows:

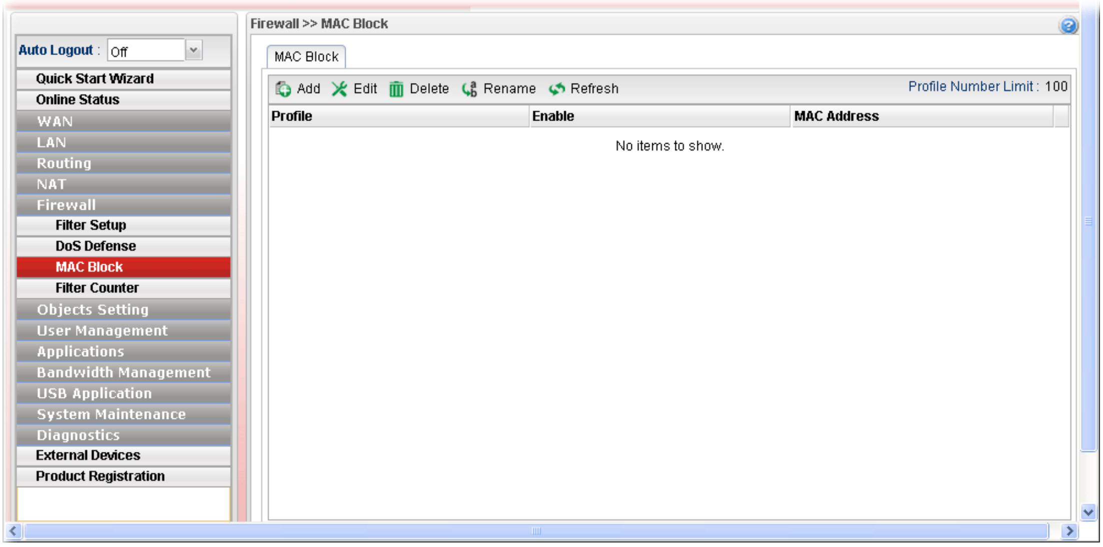
Item	Description
Enable	Check the box to enable this profile.
Block SYN Flood	Click **Enable** to activate the SYN flood defense function. If the amount of TCP SYN packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN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

Item	Description
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 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.

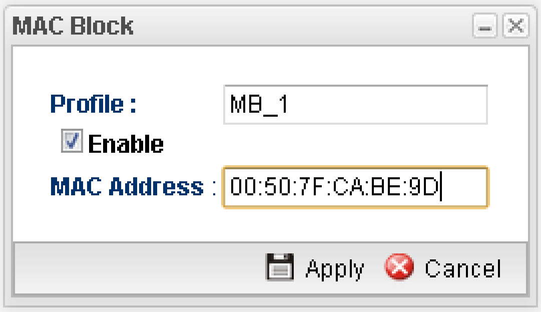


Each item will be explained as follows:

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

How to create a new MAC Block profile

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



Profile : MB_1

☑ Enable

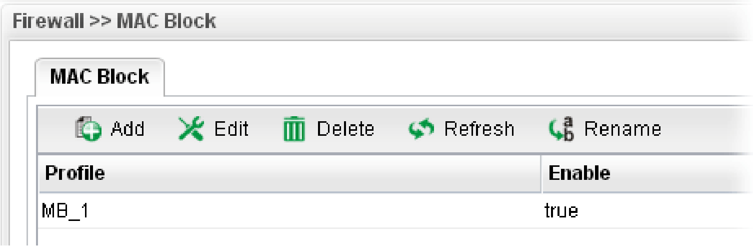
MAC Address : 00:50:7F:CA:BE:9D

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.

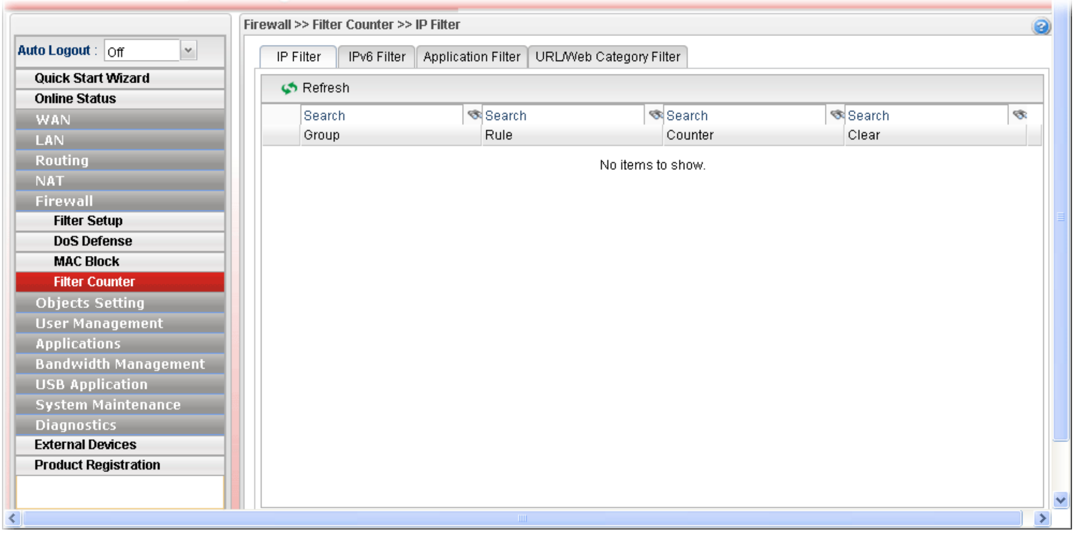


Profile	Enable
MB_1	true

4.5.4 Filter Counter

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

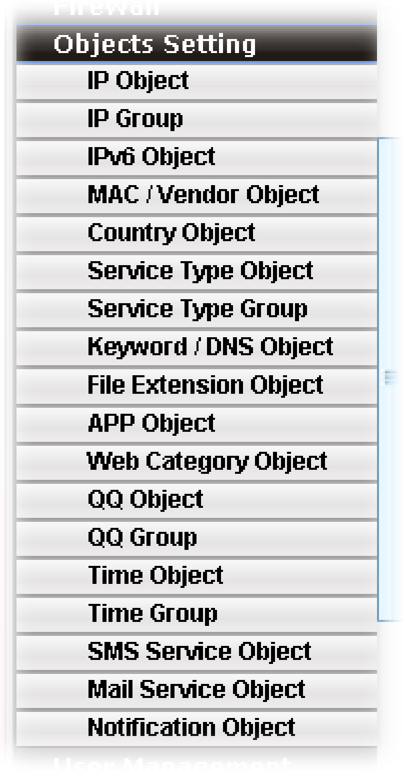
Simply click the tab of IP Filter, IPv6 Filter, Application Filter or URL/Web Category Filter to get the status for each filter.



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

4.6 Objects Setting

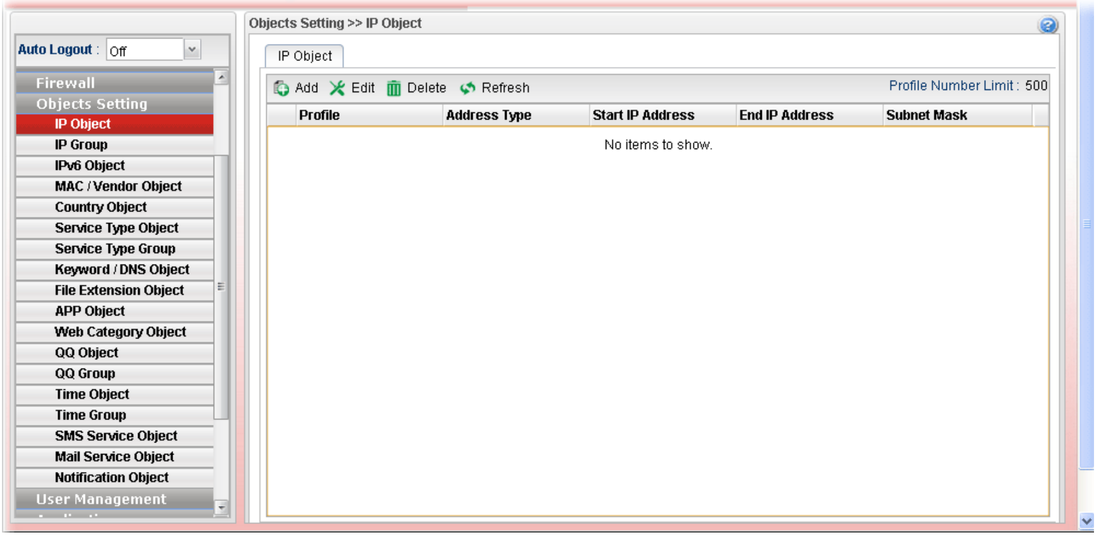
Vigor300B allows users to set different filter profiles based on IP, service type, keyword, file extension, instant message application, P2P application, protocol application, web category, QQ application, time setting, SMS service, mail service and notification. These objects setting profiles can be applied in **Firewall**.



4.6.1 IP Object

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

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

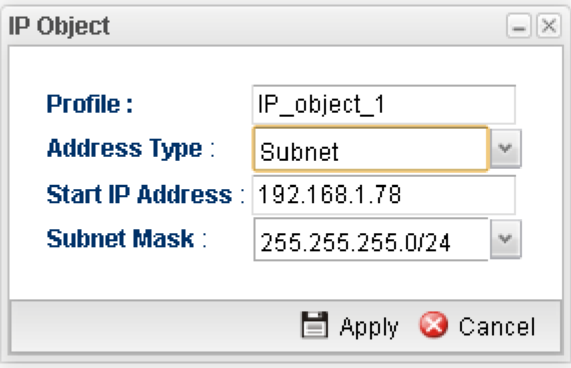


Each item will be explained as follows:

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

How to create a new IP object profile

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



IP Object

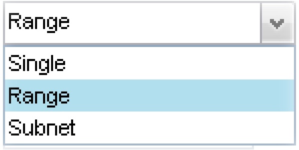
Profile : IP_object_1

Address Type : Subnet

Start IP Address : 192.168.1.78

Subnet Mask : 255.255.255.0/24

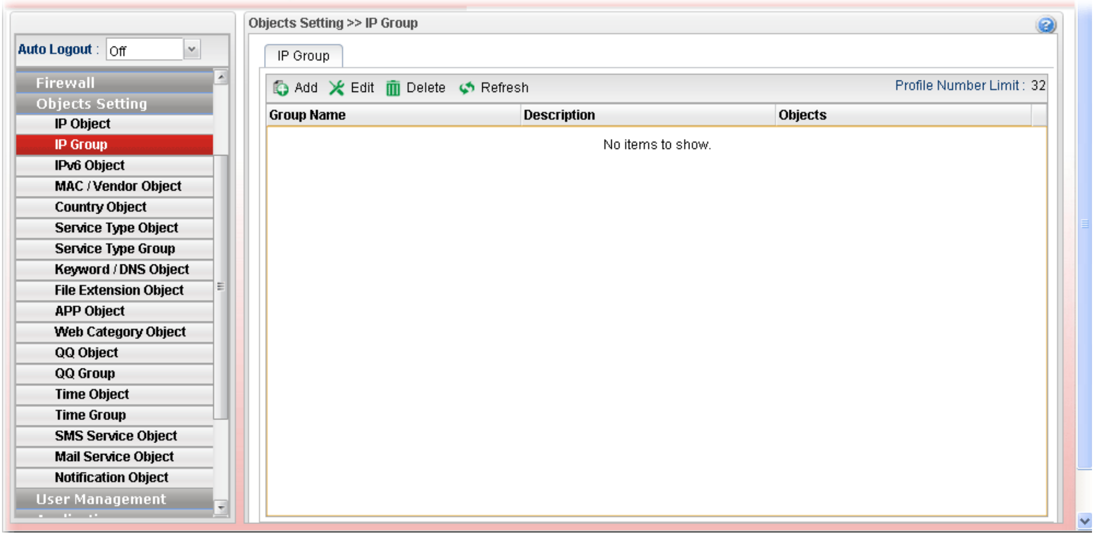
Available parameters are listed as follows:

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.

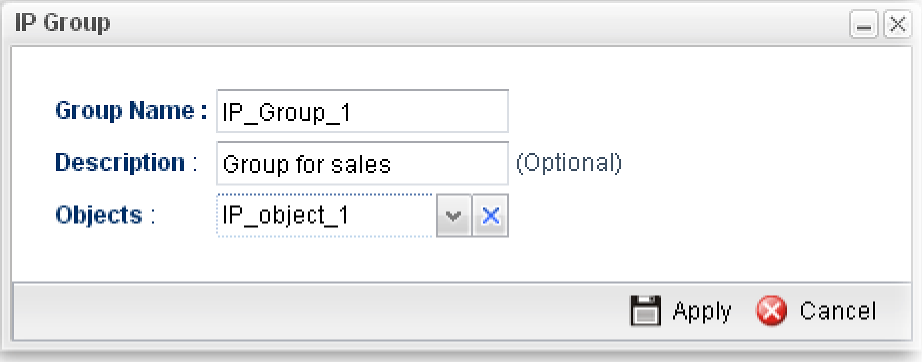


Each item will be explained as follows:

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.



Group Name : IP_Group_1

Description : Group for sales (Optional)

Objects : IP_object_1

Available parameters are listed as follows:

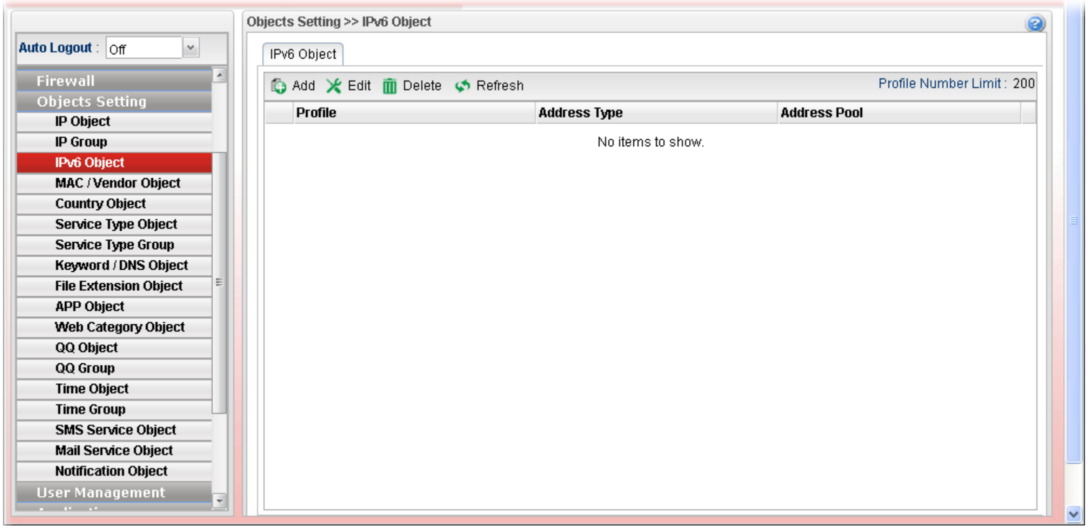
Item	Description
Group Name	Type the name of the object group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the IP object profiles under such group. All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

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

5. A new IP Group profile has been created.

4.6.3 IPv6 Object

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



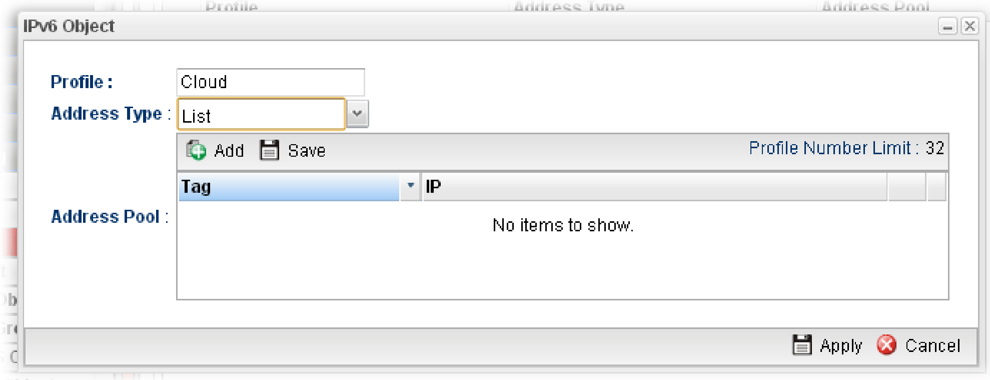
Each item will be explained as follows:

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

How to create a new IPv6 Object profile

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

3. The following dialog will appear.



Profile : Cloud

Address Type : List

Profile Number Limit : 32

Address Pool :

Tag	IP

No items to show.

Available parameters are listed as follows:

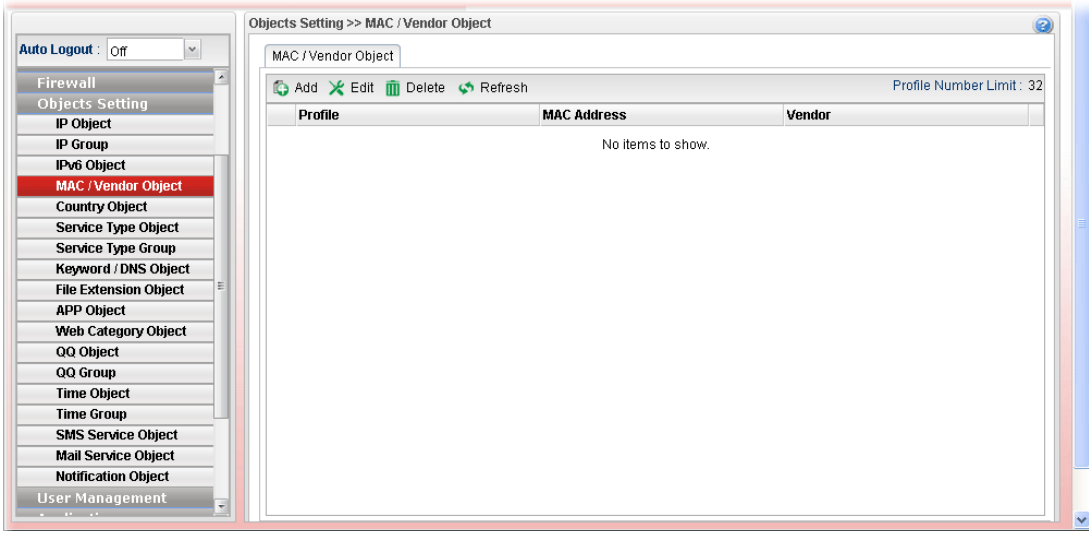
Item	Description
Profile	Type the name of the object.
Address Type	There are three types: **List** – Allow to specify IP address. **Range** – Allow to specify a range of IP addresses. **Subnet** – Allow to specify subnet mask.
Address Pool	This field allows you to type IP address, specify Tag number 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.

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

A new IPv6 Object profile has been created.

4.6.4 MAC/Vendor Object

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



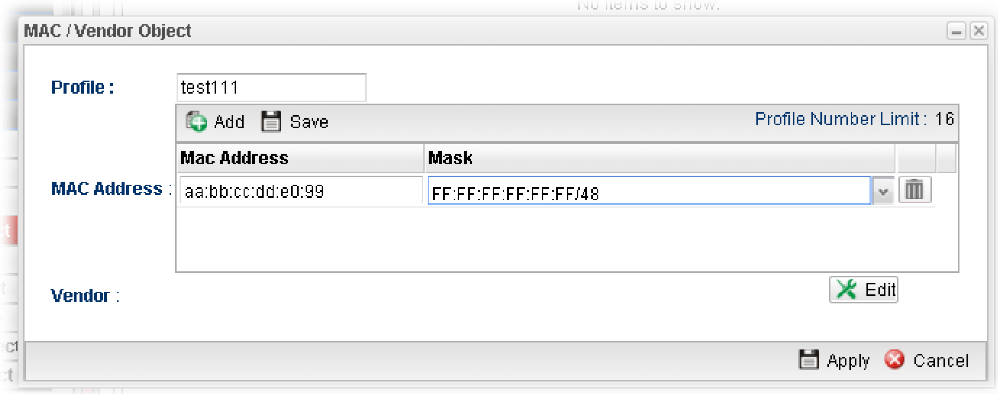
No items to show.

Each item will be explained as follows:

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

How to create a new MAC / Vendor profile

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



MAC / Vendor Object

Profile : test111

Profile Number Limit : 16

Mac Address	Mask
aa:bb:cc:dd:e0:99	FF:FF:FF:FF:FF:FF/48

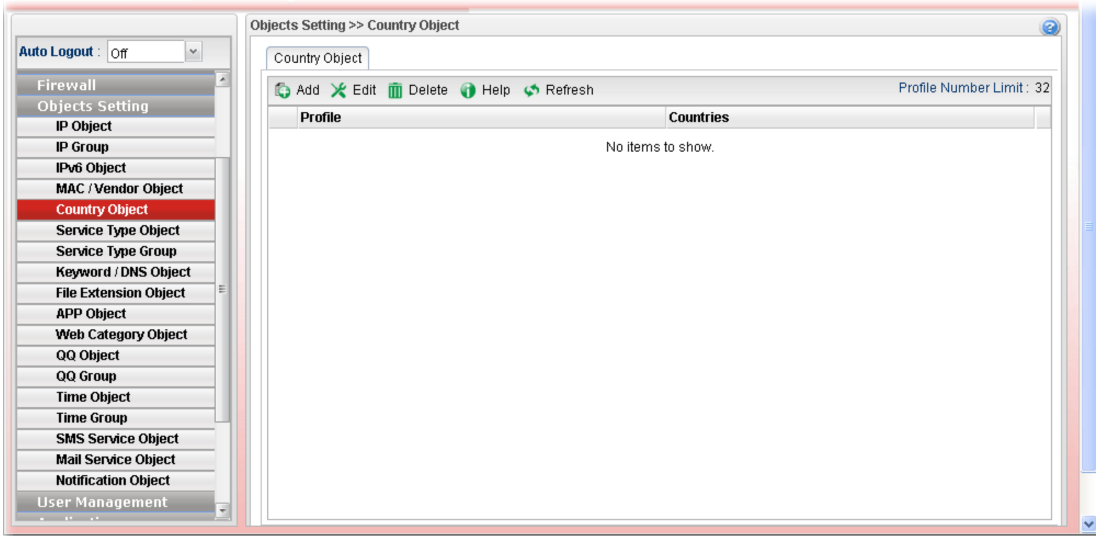
Available parameters are listed as follows:

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

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

4.6.5 Country Object

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

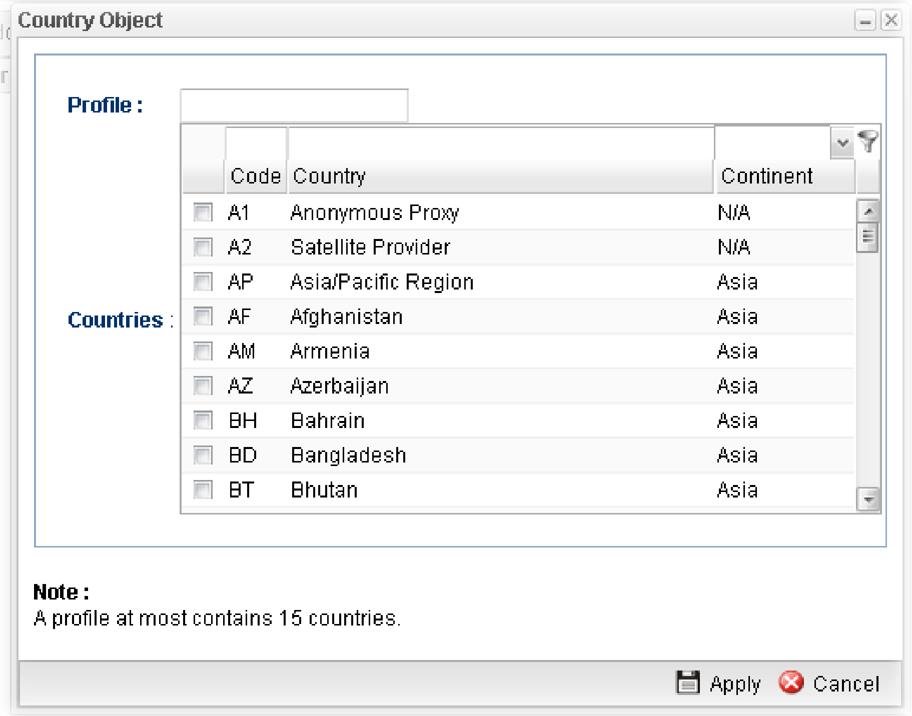


Each item will be explained as follows:

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

6. Open **Objects Setting>>Country Object.**
7. Simply click the **Add** button.
8. The following dialog will appear.



Country Object

Profile :

Countries :

	Code	Country	Continent
□	A1	Anonymous Proxy	N/A
□	A2	Satellite Provider	N/A
□	AP	Asia/Pacific Region	Asia
□	AF	Afghanistan	Asia
□	AM	Armenia	Asia
□	AZ	Azerbaijan	Asia
□	BH	Bahrain	Asia
□	BD	Bangladesh	Asia
□	BT	Bhutan	Asia

Note :
A profile at most contains 15 countries.

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.

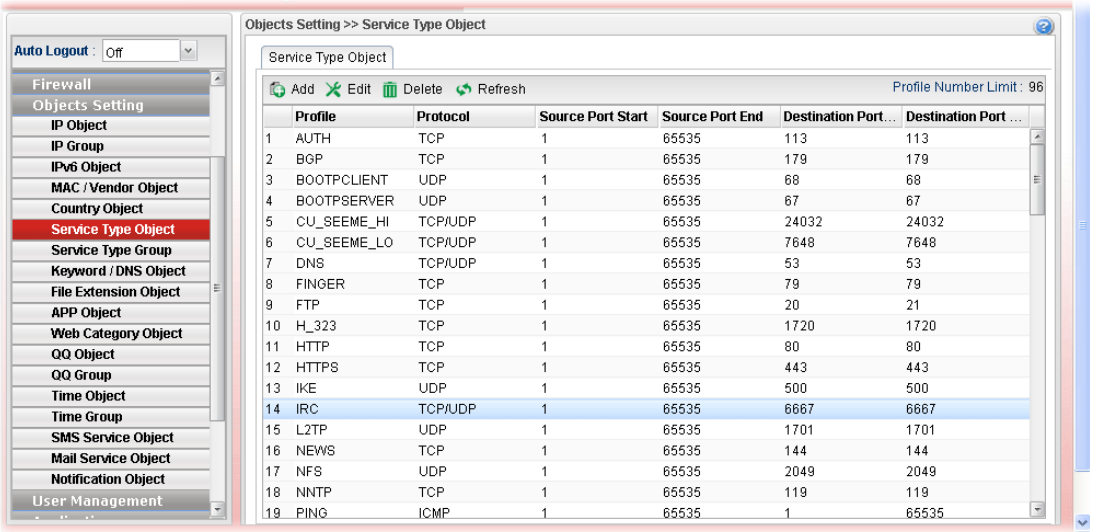
9. Enter all of the settings and click **Apply**.

10. A new Country Object profile has been created.

4.6.6 Service Type Object

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

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



Auto Logout : Off

Objects Setting >> Service Type Object

Service Type Object

Profile Number Limit : 96

	Profile	Protocol	Source Port Start	Source Port End	Destination Port...	Destination Port ...
1	AUTH	TCP	1	65535	113	113
2	BGP	TCP	1	65535	179	179
3	BOOTPCLIENT	UDP	1	65535	68	68
4	BOOTPSERVER	UDP	1	65535	67	67
5	CU_SEEME_HI	TCP/UDP	1	65535	24032	24032
6	CU_SEEME_LO	TCP/UDP	1	65535	7648	7648
7	DNS	TCP/UDP	1	65535	53	53
8	FINGER	TCP	1	65535	79	79
9	FTP	TCP	1	65535	20	21
10	H_323	TCP	1	65535	1720	1720
11	HTTP	TCP	1	65535	80	80
12	HTTPS	TCP	1	65535	443	443
13	IKE	UDP	1	65535	500	500
14	IRC	TCP/UDP	1	65535	6667	6667
15	L2TP	UDP	1	65535	1701	1701
16	NEWS	TCP	1	65535	144	144
17	NFS	UDP	1	65535	2049	2049
18	NNTP	TCP	1	65535	119	119
19	PING	ICMP	1	65535	1	65535

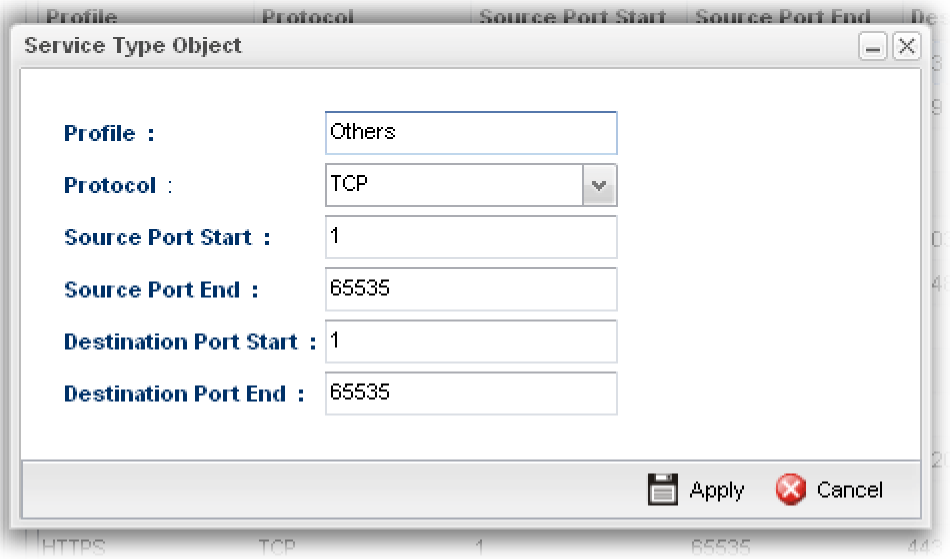
Each item will be explained as follows:

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.



Service Type Object

Profile : Others

Protocol : TCP

Source Port Start : 1

Source Port End : 65535

Destination Port Start : 1

Destination Port End : 65535

Available parameters are listed as follows:

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

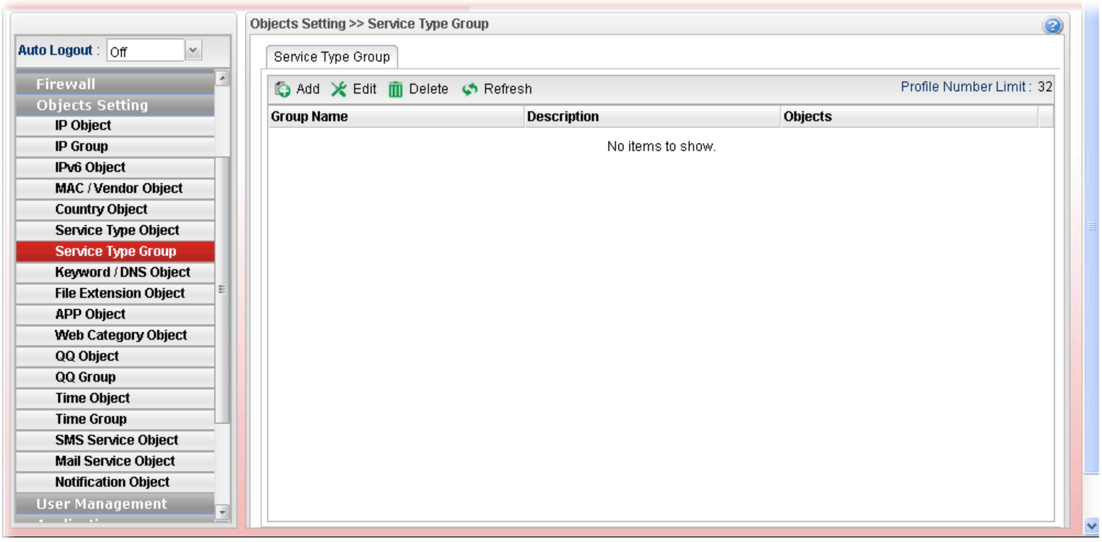
4. Enter all the settings and click **Apply**.

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

4.6.7 Service Type Group

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

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

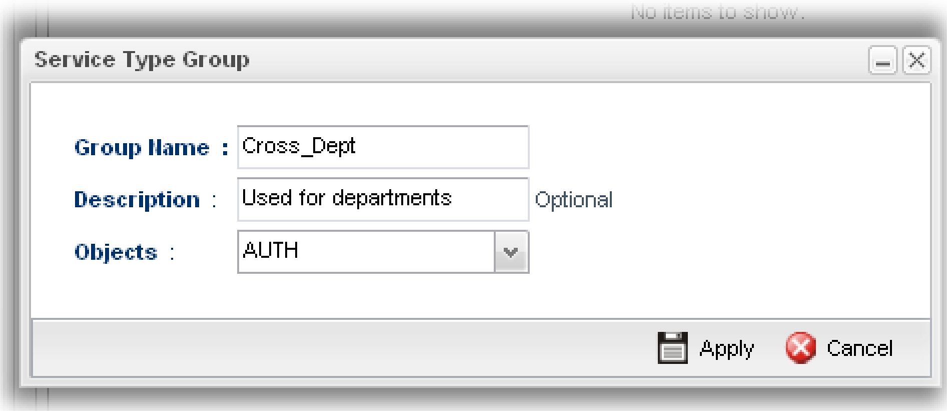


Each item will be explained as follows:

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

How to create a new service type group profile

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



Group Name : Cross_Dept

Description : Used for departments

Objects : AUTH

Available parameters are listed as follows:

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

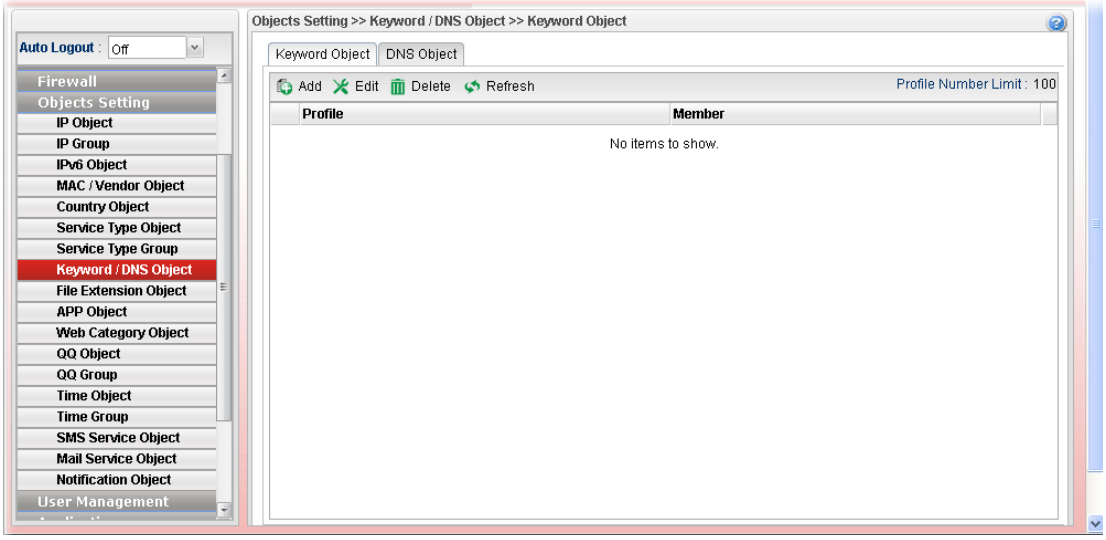
4. Enter all the settings and click **Apply**.

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

4.6.8 Keyword /DNS Object

4.6.8.1 Keyword Object

Keyword can be set as a filter rule to be applied in Firewall. Vigor300B allows users to set keyword profile with several keywords. Even, it allows users to group several keyword profiles within a keyword group.



Objects Setting >> Keyword / DNS Object >> Keyword Object

Auto Logout : Off

Profile Number Limit : 100

Profile	Member

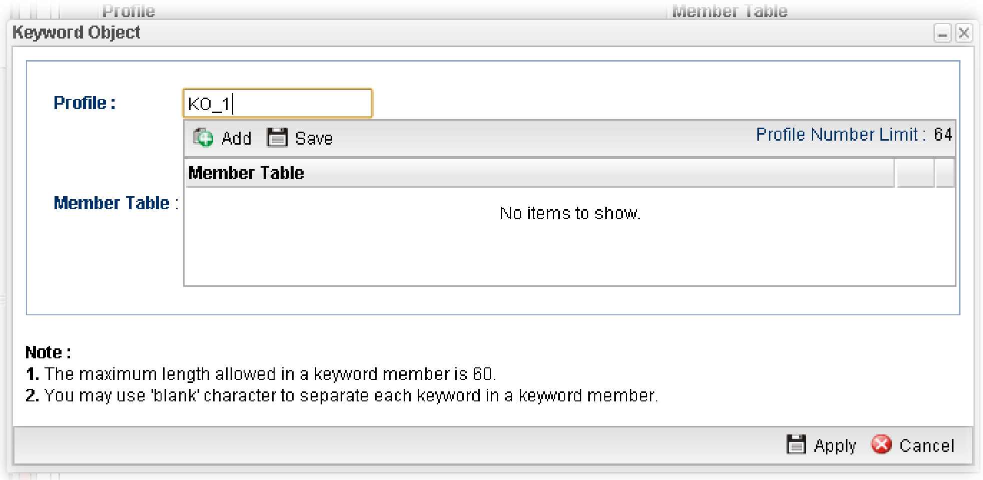
No items to show.

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.



Keyword Object

Profile : KO_1

Member Table :

Note :
1. The maximum length allowed in a keyword member is 60.
2. You may use 'blank' character to separate each keyword in a keyword member.

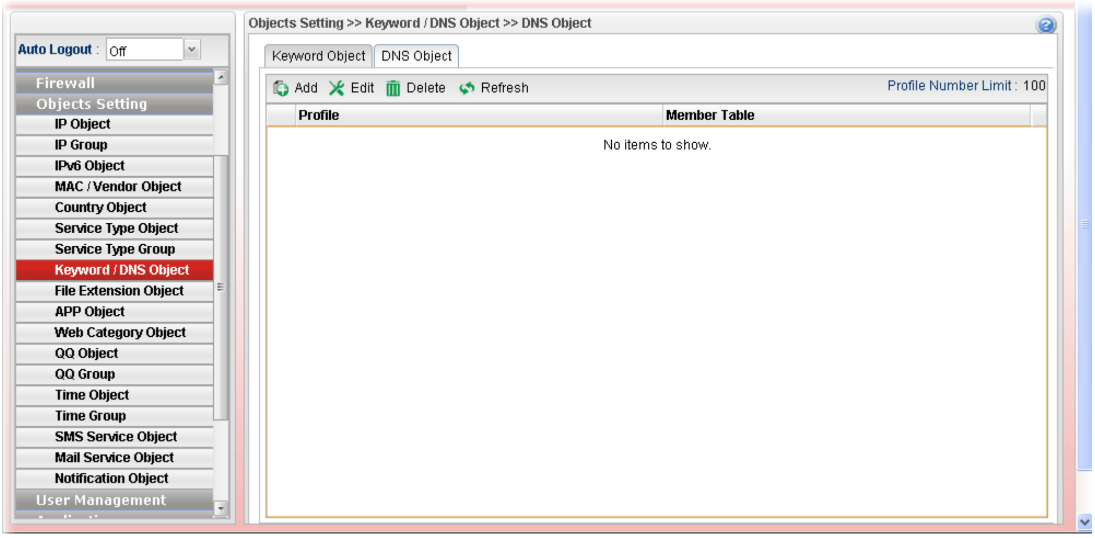
Available parameters are listed as follows:

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

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

4.6.8.2 DNS Object

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

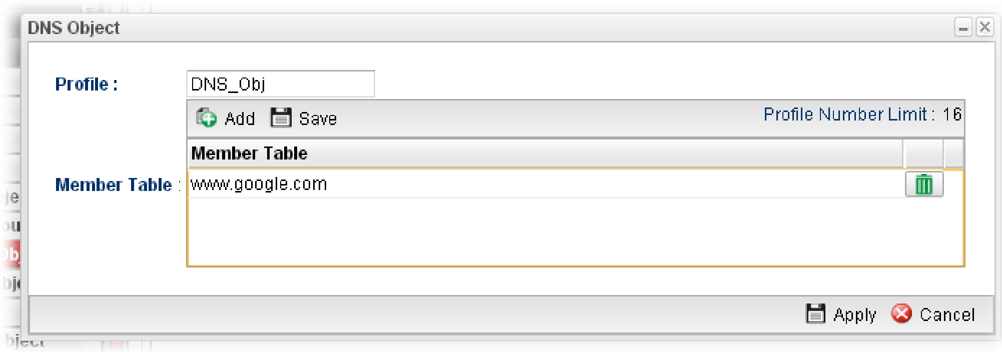


Each item will be explained as follows:

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

How to create a new DNS Object profile

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



Profile : DNS_Obj

Profile Number Limit : 16

Member Table : www.google.com

Available parameters are listed as follows:

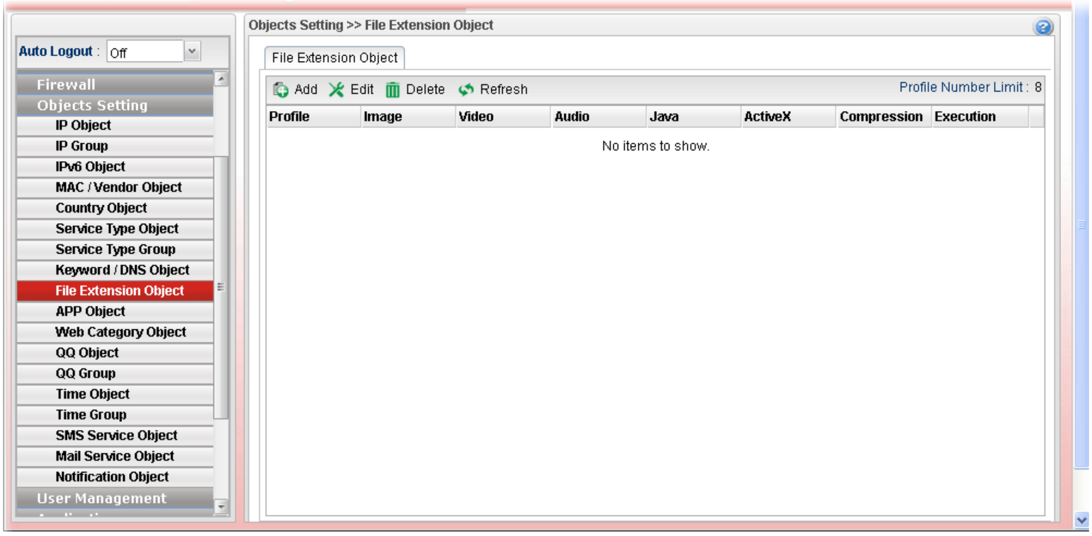
Item	Description
Profile	Type the name of the DNS object profile.
Member Table	Type the domain name of the DNS that you want to filter. **Add** – Type the word in the box of Member and click this button to add the new word as DNS object. **Save** – Click it to save the setting. 🗑 – click the icon to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

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

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

4.6.9 File Extension Object

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



Objects Setting >> File Extension Object

File Extension Object

Add Edit Delete Refresh Profile Number Limit : 8

Profile	Image	Video	Audio	Java	ActiveX	Compression	Execution

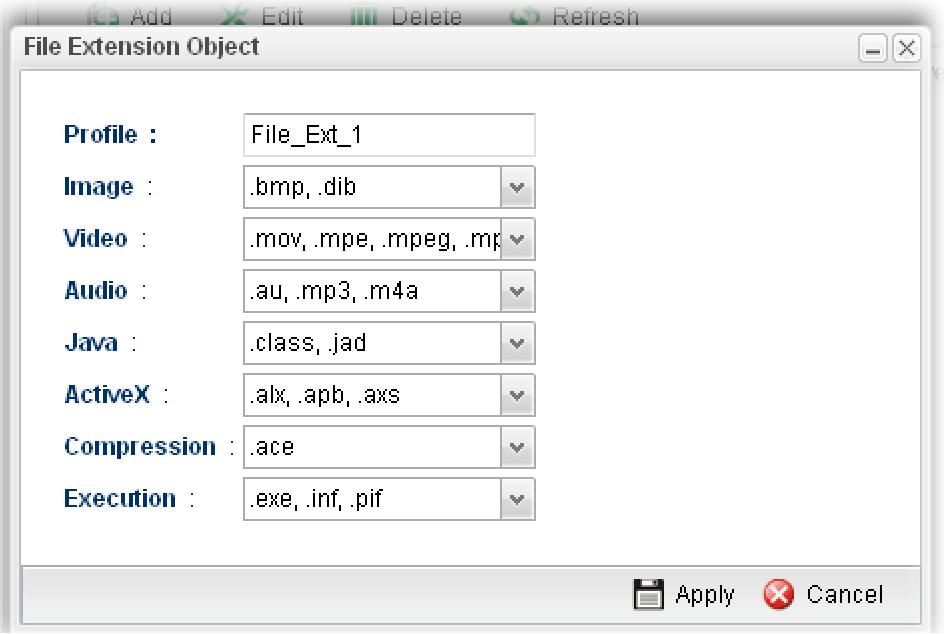
No items to show.

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.



Profile : File_Ext_1

Image : .bmp, .dib

Video : .mov, .mpe, .mpeg, .mp

Audio : .au, .mp3, .m4a

Java : .class, .jad

ActiveX : .alx, .apb, .axs

Compression : .ace

Execution : .exe, .inf, .pif

Available parameters are listed as follows:

Item	**Description**
Profile	Type the name of the File Extension Object group..
Image	Several file extensions for Image offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Video	Several file extensions for Video offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Audio	Several file extensions for Audio offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Java	Several file extensions for Java offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
ActiveX	Several file extensions for ActiveX offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Compression	Several file extensions for compression offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Execution	Several file extensions for execution offered for you to choose. Use the drop down list to check the box (es) to select

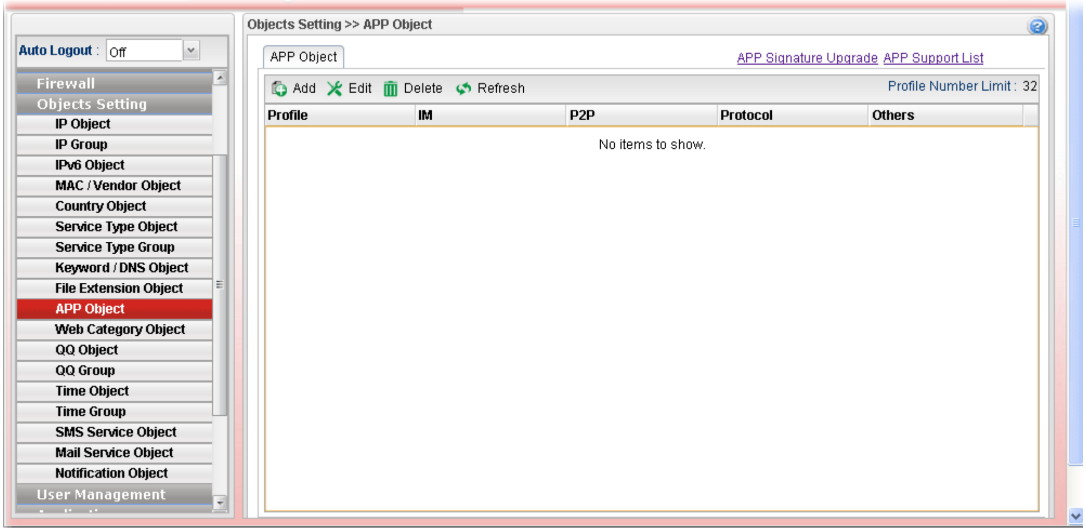
	the file extension you need.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

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

4.6.10 APP Object

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



Each item will be explained as follows:

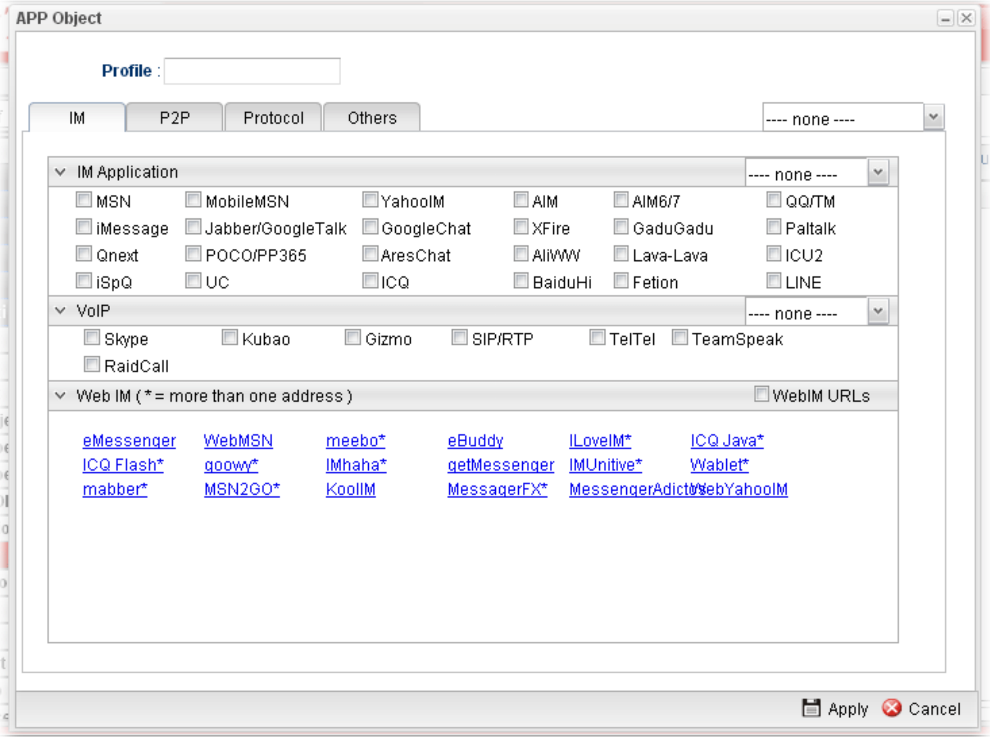
Item	Description
APP Signature Upgrade	Click it to open **System Maintenance>>APP Signature Upgrade** configuration page.
APP Support List	APP Support List will display all of the applications with versions supported by Vigor router. They are separated with types of IM, P2P, Protocol and Others. Each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

Profile Number Limit	Display the total number (32) of the object profiles to be created.
Profile	Display the name of the IM object profile.
IM	Display the IM application specified in such profile.
P2P	Display the P2P specified in such profile.
Protocol	Display the protocol specified in such profile.
Others	Display other types specified in such profile.

How to create a new APP Object Profile

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

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



APP Object

Profile :

IM Application ---- none ----

☐ MSN ☐ MobileMSN ☐ YahooIM ☐ AIM ☐ AIM6/7 ☐ QQ/TM
☐ iMessage ☐ Jabber/GoogleTalk ☐ GoogleChat ☐ XFire ☐ GaduGadu ☐ Paltalk
☐ Qnext ☐ POCO/PP365 ☐ AresChat ☐ AliWW ☐ Lava-Lava ☐ ICU2
☐ iSpQ ☐ UC ☐ ICQ ☐ BaiduHi ☐ Fetion ☐ LINE

VoIP ---- none ----

☐ Skype ☐ Kubao ☐ Gizmo ☐ SIP/RTP ☐ TelTel ☐ TeamSpeak
☐ RaidCall

Web IM (* = more than one address) ☐ WebIM URLs

eMessenger WebMSN meebo* eBuddy ILoveIM* ICQ Java*
ICQ Flash* goowy* IMhaha* getMessenger IMUnitive* Wablet*
mabber* MSN2GO* KoolIM MessagerFX* MessengerAdictWebYahooIM

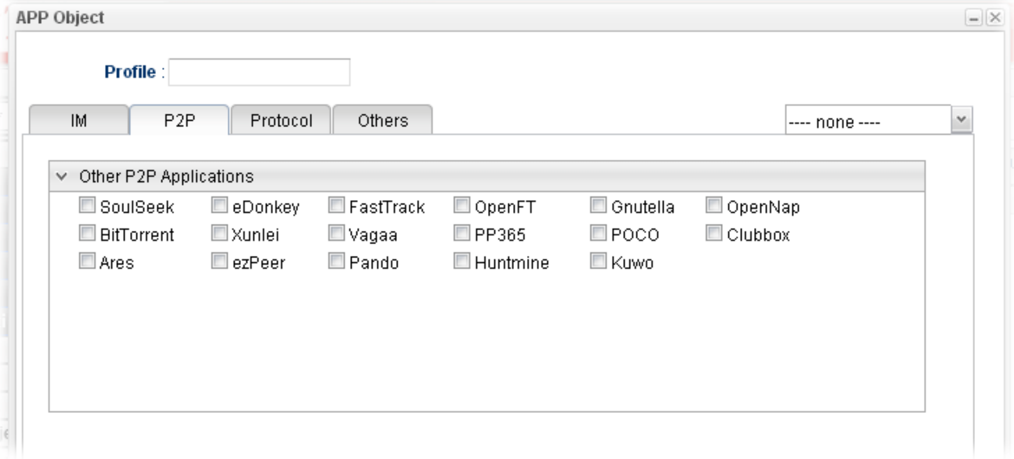
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IM object group. The number of the characters allowed to be typed here is 10.

IM Application	Several IM applications offered for you to choose. Check the one(s) you want to add for such profile.
WebIM	It lists a package of IM application based on web page. You may check the box to include all of them.
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. Vigor300B 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.



APP Object

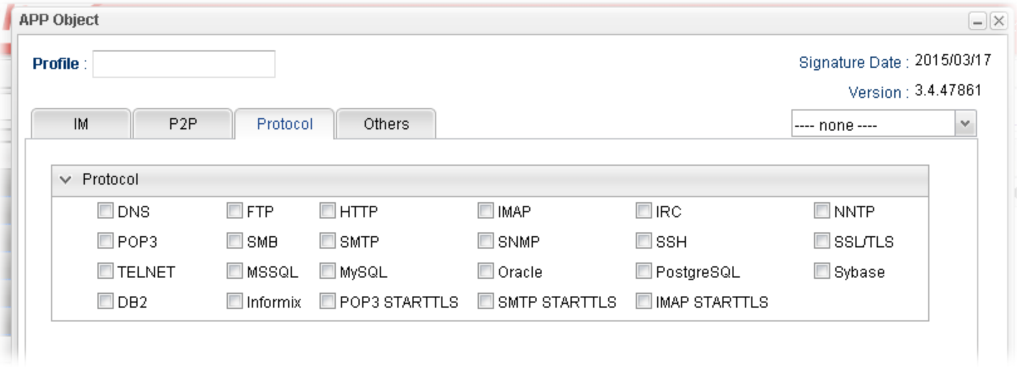
Profile :

Other P2P Applications

□ SoulSeek □ eDonkey □ FastTrack □ OpenFT □ Gnutella □ OpenNap
□ BitTorrent □ Xunlei □ Vagaa □ PP365 □ POCO □ Clubbox
□ Ares □ ezPeer □ Pando □ Huntmine □ Kuwo

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 Vigor300B. Common services will be listed in this function and can be selected to be blocked by the router.



APP Object

Profile :

Signature Date : 2015/03/17

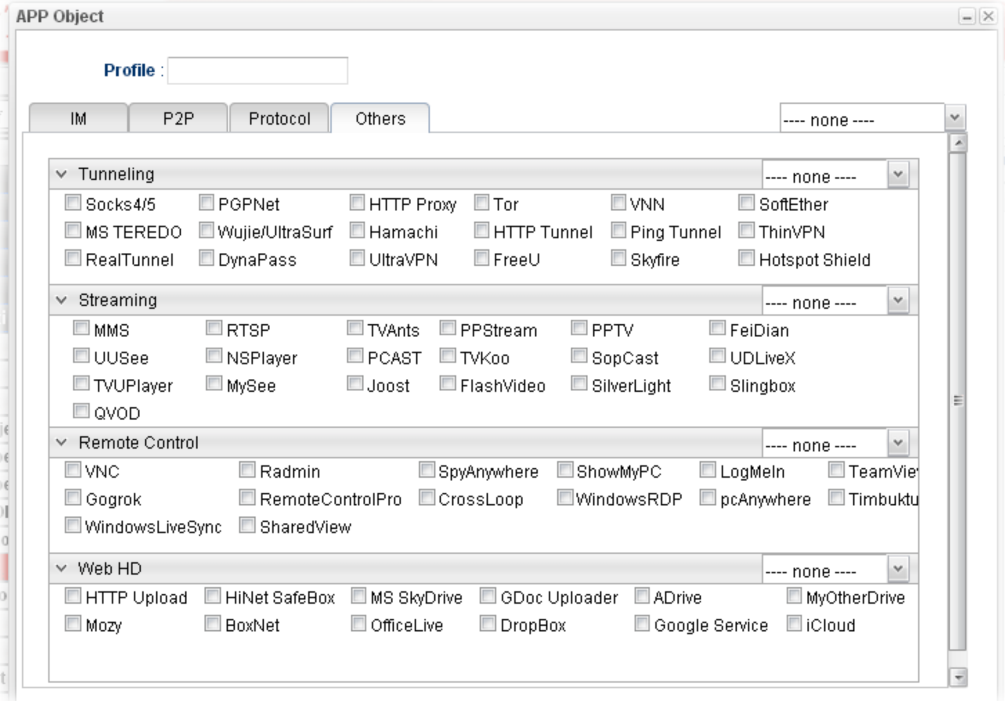
Version : 3.4.47861

Protocol

□ DNS □ FTP □ HTTP □ IMAP □ IRC □ NNTP
□ POP3 □ SMB □ SMTP □ SNMP □ SSH □ SSL/TLS
□ TELNET □ MSSQL □ MySQL □ Oracle □ PostgreSQL □ Sybase
□ DB2 □ Informix □ POP3 STARTTLS □ SMTP STARTTLS □ IMAP STARTTLS

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.



APP Object

Profile :

IM | P2P | Protocol | Others ---- none ----

Tunneling ---- none ----

□ Socks4/5 □ PGPNet □ HTTP Proxy □ Tor □ VNN □ SoftEther
□ MS TEREDO □ Wujie/UltraSurf □ Hamachi □ HTTP Tunnel □ Ping Tunnel □ ThinVPN
□ RealTunnel □ DynaPass □ UltraVPN □ FreeU □ Skyfire □ Hotspot Shield

Streaming ---- none ----

□ MMS □ RTSP □ TVAnts □ PPStream □ PPTV □ FeiDian
□ UUSee □ NSPlayer □ PCAST □ TVKoo □ SopCast □ UDLiveX
□ TVUPlayer □ MySee □ Joost □ FlashVideo □ SilverLight □ Slingbox
□ QVOD

Remote Control ---- none ----

□ VNC □ Radmin □ SpyAnywhere □ ShowMyPC □ LogMeIn □ TeamVie
□ Gogrok □ RemoteControlPro □ CrossLoop □ WindowsRDP □ pcAnywhere □ Timbuktu
□ WindowsLiveSync □ SharedView

Web HD ---- none ----

□ HTTP Upload □ HiNet SafeBox □ MS SkyDrive □ GDoc Uploader □ ADrive □ MyOtherDrive
□ Mozy □ BoxNet □ OfficeLive □ DropBox □ Google Service □ iCloud

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

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

4.6.11 Web Category Object

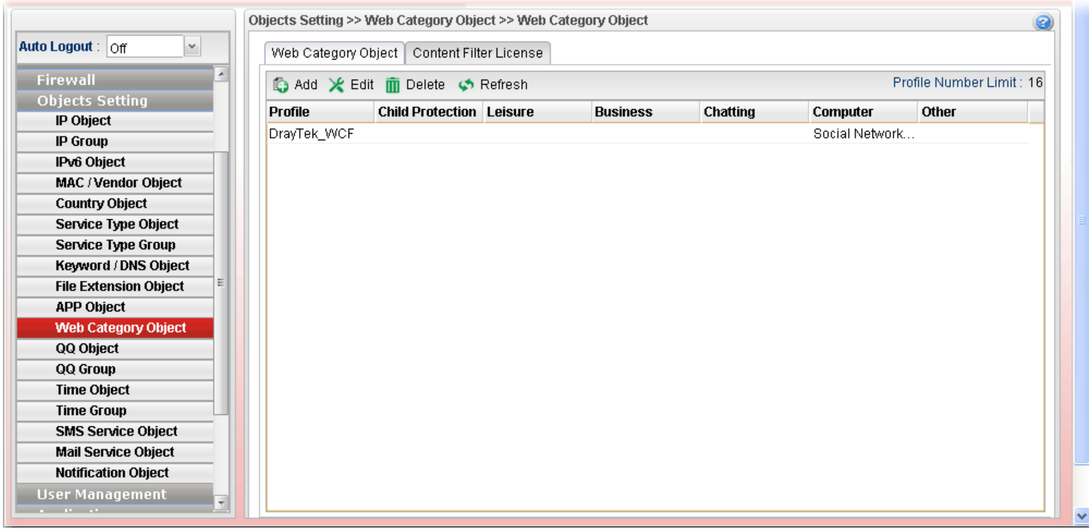
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With web category filtering service of the Vigor router, you can protect your business from common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

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

> **Note 1:** Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **Commtouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
> **Note 2**: Commtouch is merged by Cyren and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

Note 3: fragFINN service will be terminated from 2015.

4.6.11.1 Web Category Object



Profile	Child Protection	Leisure	Business	Chatting	Computer	Other
DrayTek_WCF					Social Network...	

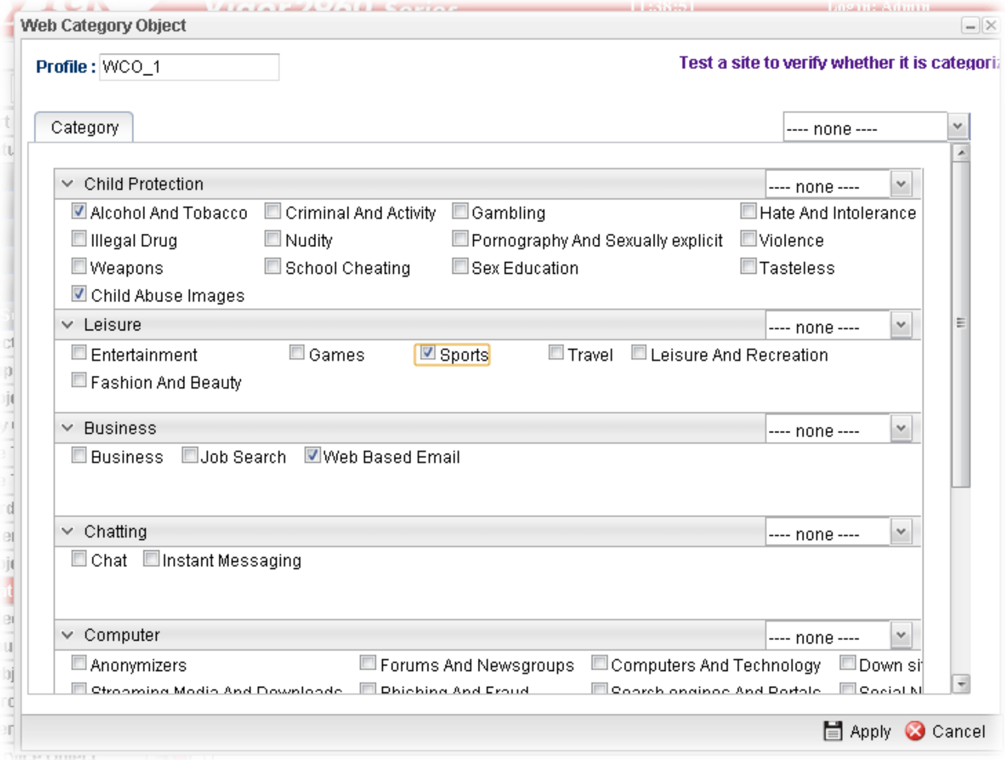
Each item will be explained as follows:

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 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.



Web Category Object

Profile : WCO_1

Test a site to verify whether it is categori

Category ---- none ----

Child Protection ---- none ----

☑ Alcohol And Tobacco ☐ Criminal And Activity ☐ Gambling ☐ Hate And Intolerance
☐ Illegal Drug ☐ Nudity ☐ Pornography And Sexually explicit ☐ Violence
☐ Weapons ☐ School Cheating ☐ Sex Education ☐ Tasteless
☑ Child Abuse Images

Leisure ---- none ----

☐ Entertainment ☐ Games ☑ Sports ☐ Travel ☐ Leisure And Recreation
☐ Fashion And Beauty

Business ---- none ----

☐ Business ☐ Job Search ☑ Web Based Email

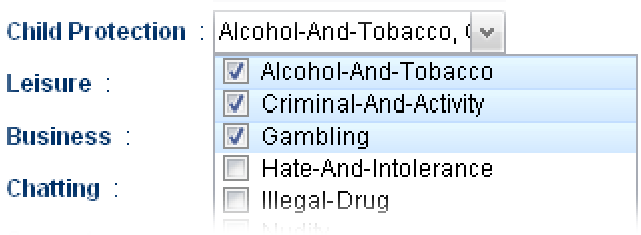
Chatting ---- none ----

☐ Chat ☐ Instant Messaging

Computer ---- none ----

☐ Anonymizers ☐ Forums And Newsgroups ☐ Computers And Technology ☐ Down si
☐ Streaming Media And Downloads ☐ Phishing And Fraud ☐ Search engines And Portals ☐ Social N

Available parameters are listed as follows:

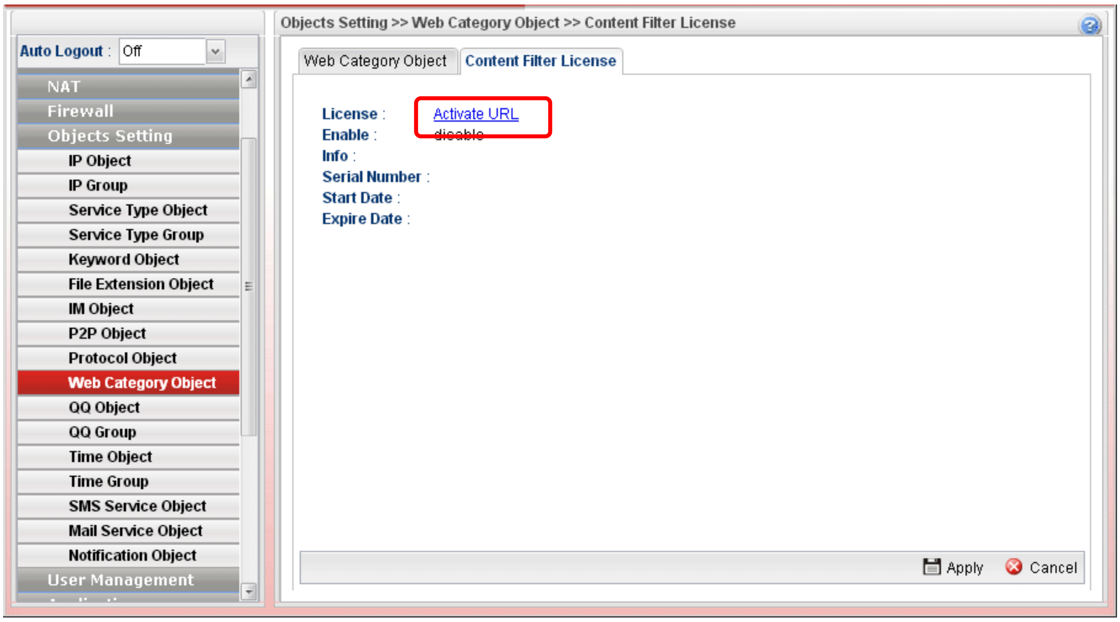
Item	Description
Profile	Type the name of the web category object profile. The number of the characters allowed to be typed here is 10.
Child Protection	The web pages which are not suitable for children will be classified into different categories. Simply check the one(s) that you don’t want the children to visit.  Child Protection : Alcohol-And-Tobacco, (Leisure : Business : Chatting : ☑ Alcohol-And-Tobacco ☑ Criminal-And-Activity ☑ Gambling ☐ Hate-And-Intolerance ☐ Illegal-Drug
Leisure	Simply check the one(s) that you don’t want the user to visit.
Business	Simply check the one(s) that you don’t want the user to visit.

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

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

4.6.11.2 Content Filter License

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

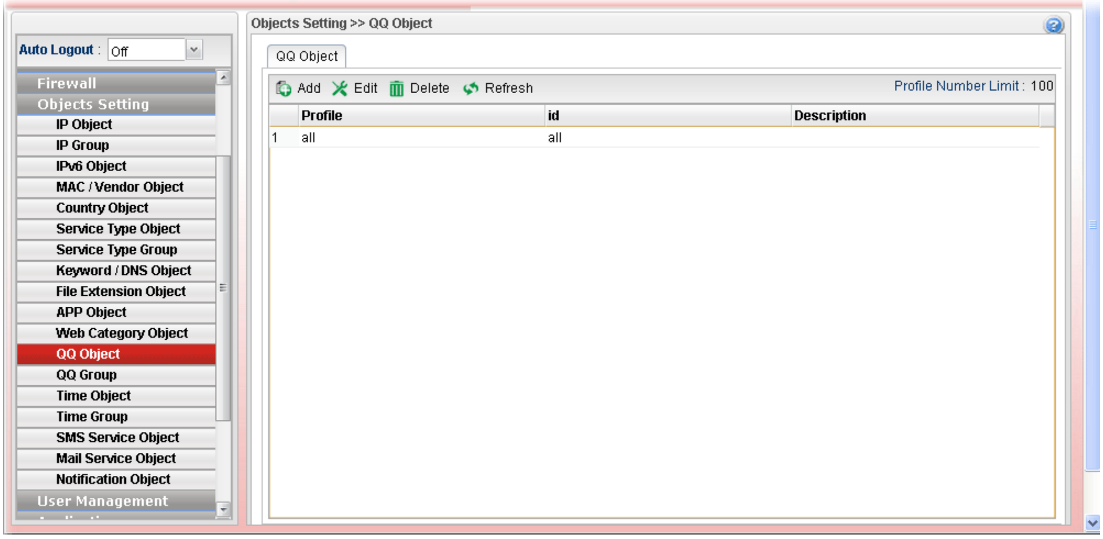


License : Activate URL
Enable : disable
Info :
Serial Number :
Start Date :
Expire Date :

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

4.6.12 QQ Object

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



Objects Setting >> QQ Object

Profile Number Limit : 100

	Profile	id	Description
1	all	all	

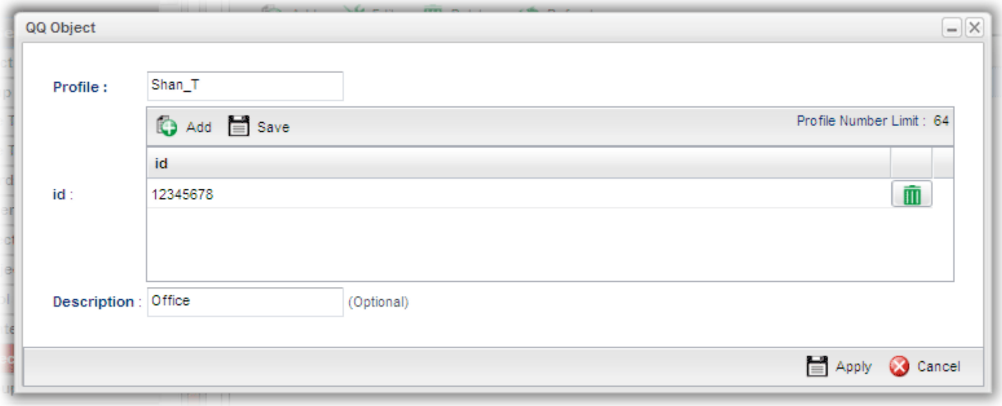
Each item will be explained as follows:

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

How to create a new QQ object profile

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

3. The following dialog will appear.



Profile : Shan_T

id : 12345678

Description : Office

Available parameters are listed as follows:

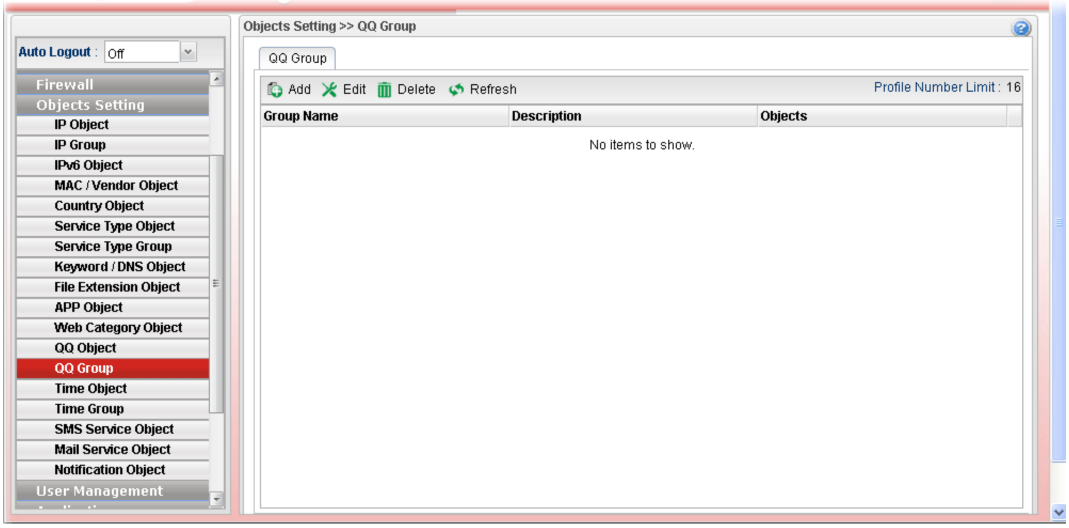
Item	Description
Profile	Type the name of the QQ object profile. The number of the characters allowed to be typed here is 10.
id	Create the account name for such QQ object profile. **Add** – Click this button to add a new account. **Save** – Click this button o save the new account. 🗑 - Click this button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

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

5. A new QQ Object profile has been created.

4.6.13 QQ Group

This page allows you to group several QQ object profiles.

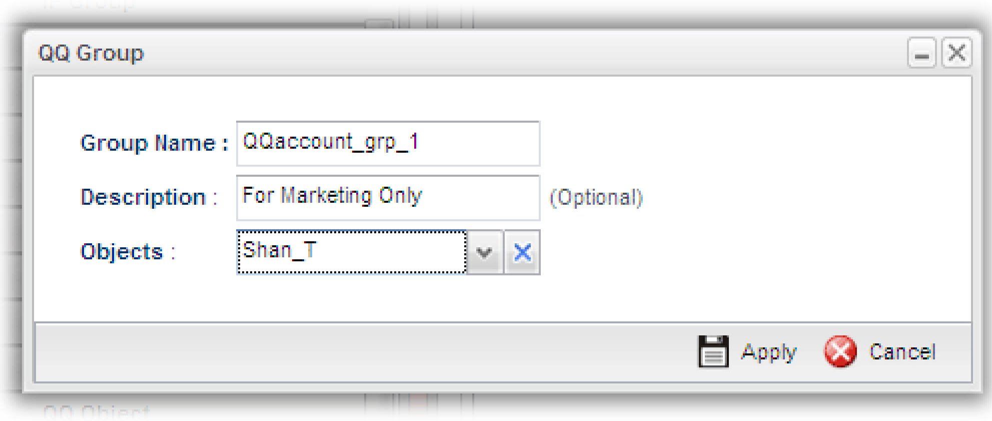


Each item will be explained as follows:

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

How to create a new QQ group profile

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



Group Name : QQaccount_grp_1

Description : For Marketing Only (Optional)

Objects : Shan_T

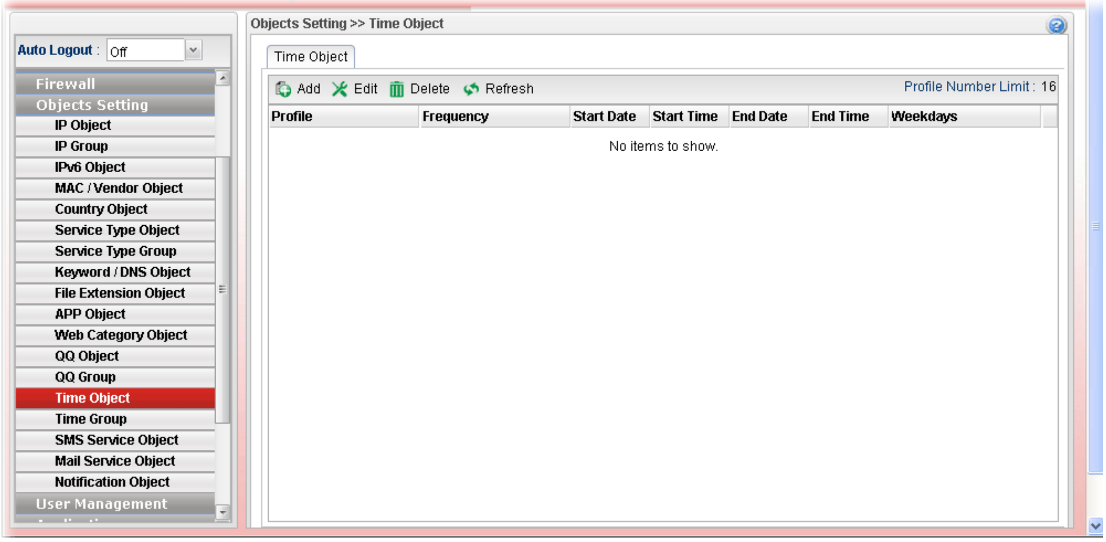
Available parameters are listed as follows:

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

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

4.6.14 Time Object

You restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions, e.g., Firewall.



Profile	Frequency	Start Date	Start Time	End Date	End Time	Weekdays

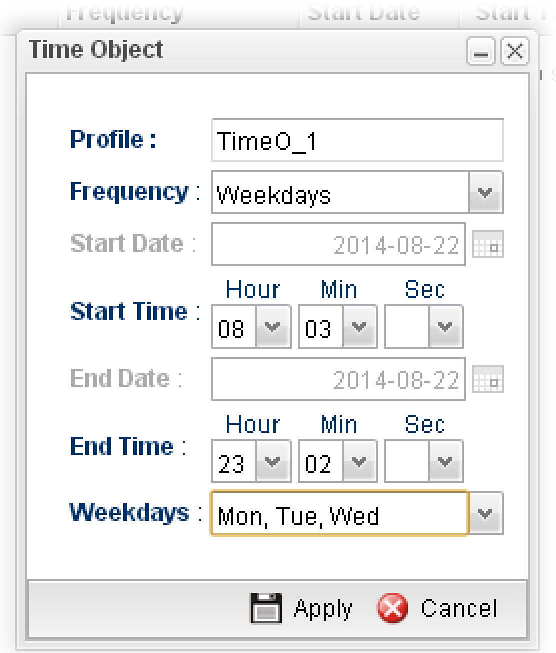
No items to show.

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.



Time Object

Profile : TimeO_1

Frequency : Weekdays

Start Date : 2014-08-22

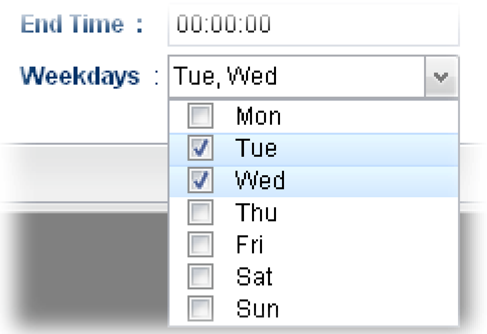
Start Time : Hour 08 Min 03 Sec

End Date : 2014-08-22

End Time : Hour 23 Min 02 Sec

Weekdays : Mon, Tue, Wed

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.  End Time : 00:00:00 Weekdays : Tue, Wed ☐ Mon ☑ Tue ☑ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

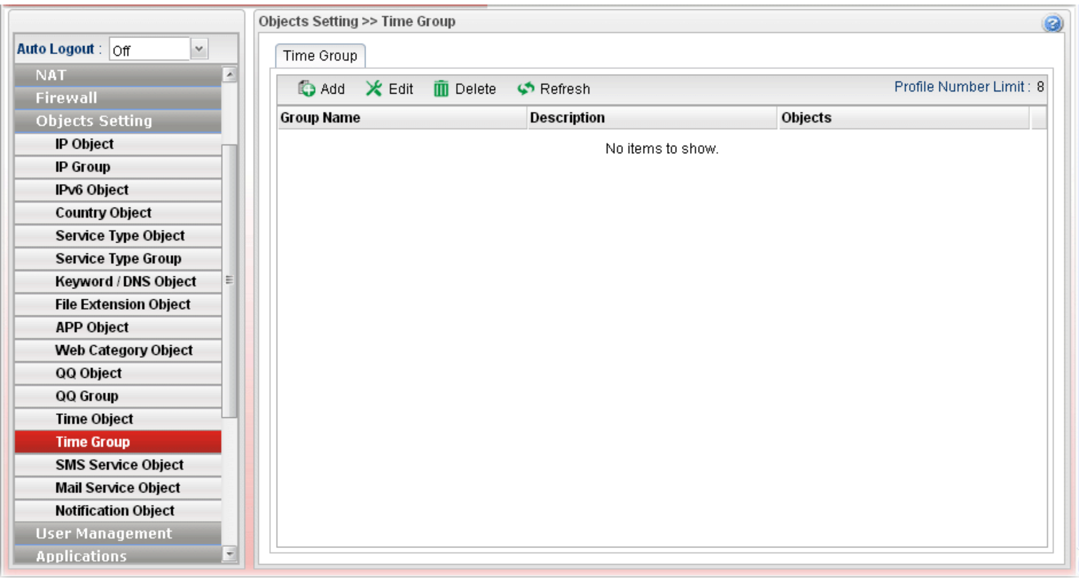
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A new Time Object profile has been created.

4.6.15 Time Group

This page allows you to group several time object profiles.



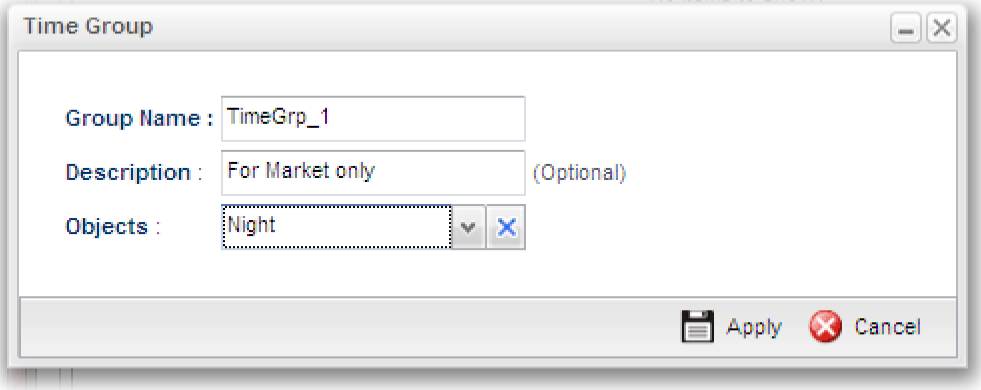
Group Name	Description	Objects
No items to show.		

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.



Group Name : TimeGrp_1

Description : For Market only (Optional)

Objects : Night

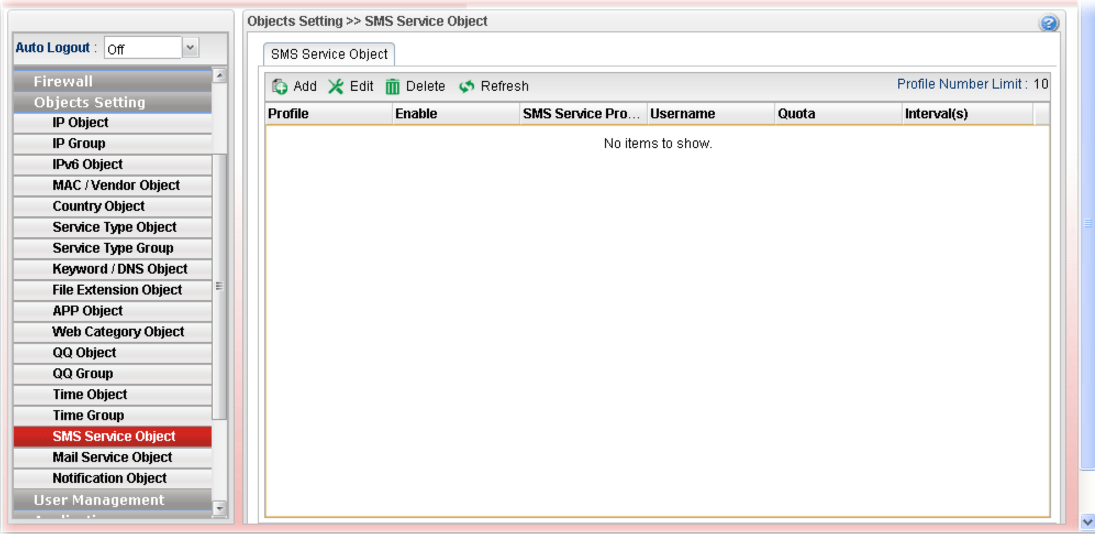
Available parameters are listed as follows:

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

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

4.6.16 SMS Service Object

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

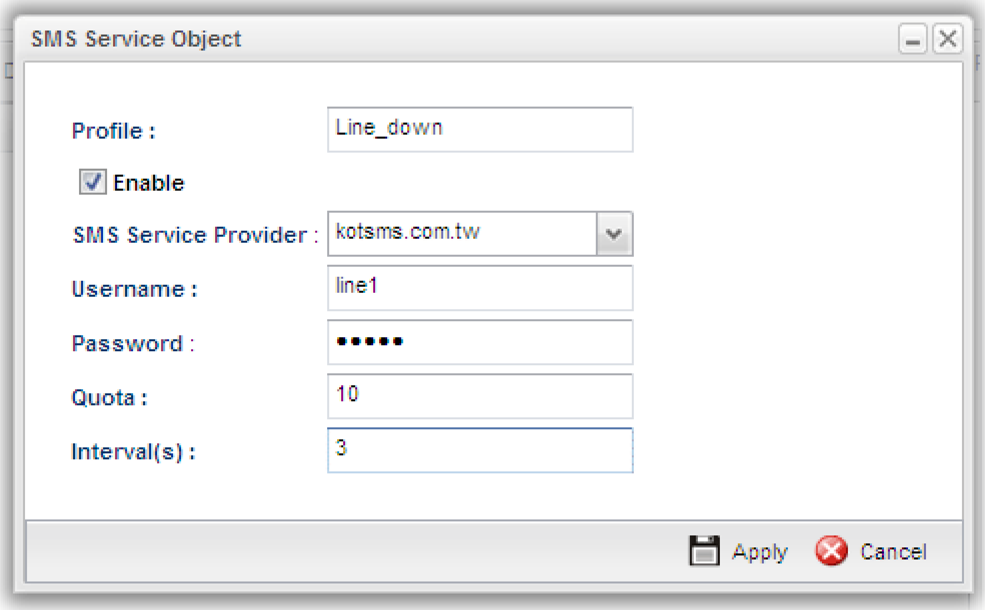


Each item will be explained as follows:

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



Profile : Line_down

☑ Enable

SMS Service Provider : kotsms.com.tw

Username : line1

Password : •••••

Quota : 10

Interval(s) : 3

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.
Enable	Check this box to enable such profile.
SMS Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Interval(s)	To avoid quota being exhausted soon, type time interval for sending the SMS.
Apply	Click it to save the configuration.

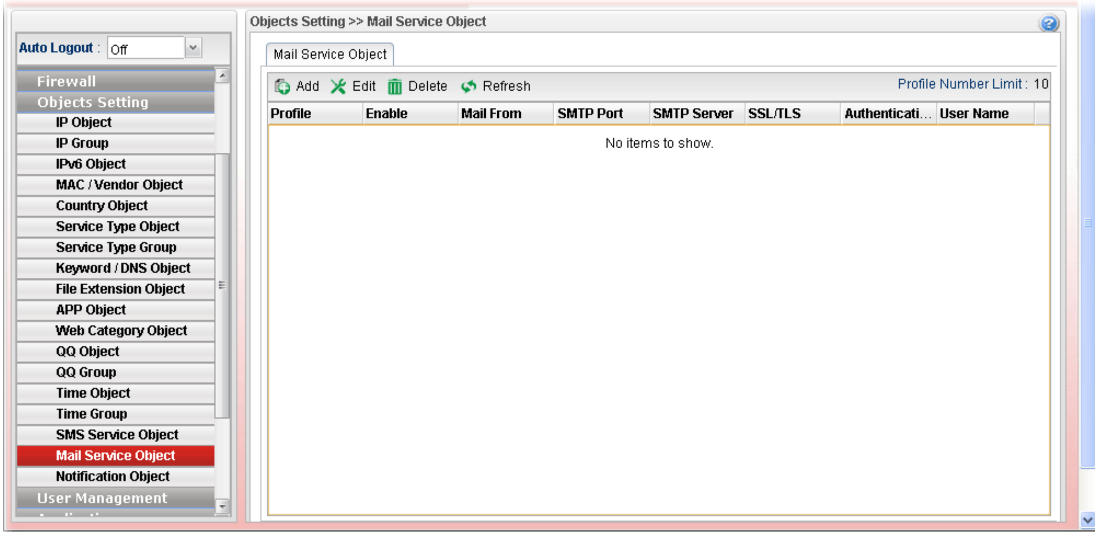
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A new SMS object profile has been created.

4.6.17 Mail Service Object

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



Profile	Enable	Mail From	SMTP Port	SMTP Server	SSL/TLS	Authenticati...	User Name

No items to show.

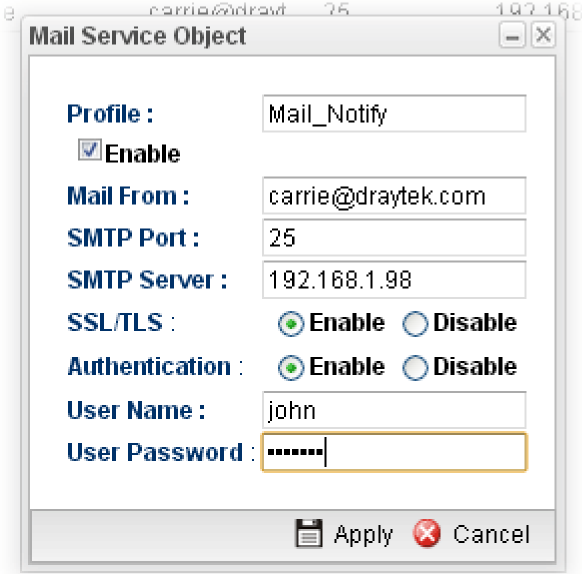
Each item will be explained as follows:

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

Item	Description
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.



Mail Service Object

Profile :	Mail_Notify
☑ Enable	
Mail From :	carrie@draytek.com
SMTP Port :	25
SMTP Server :	192.168.1.98
SSL/TLS :	● Enable ○ Disable
Authentication :	● Enable ○ Disable
User Name :	john
User Password :	•••••••

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.

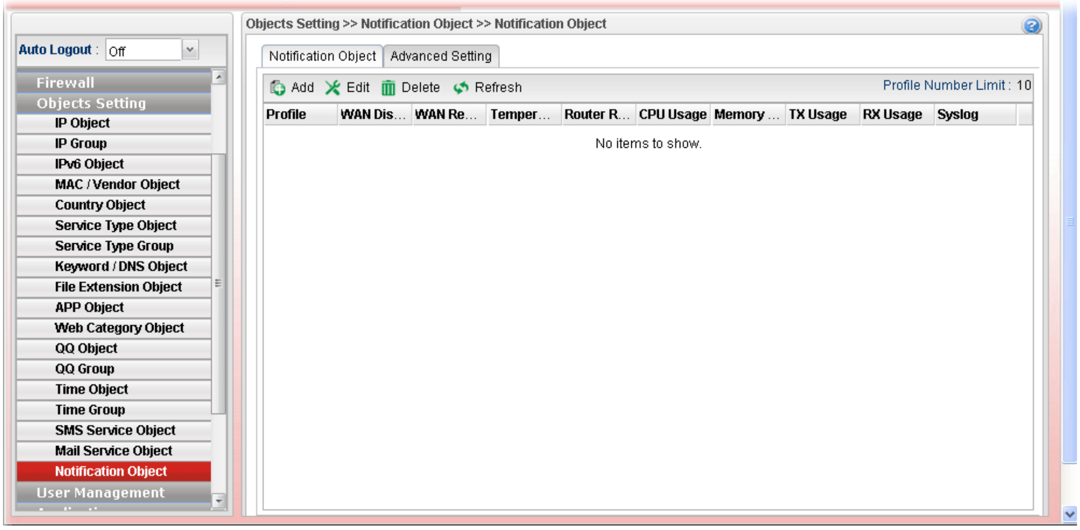
	User Password – Type a password for authentication. The maximum length of the password you can set is 31 characters.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

4.6.18 Notification Object

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

4.6.18.1 Notification Object



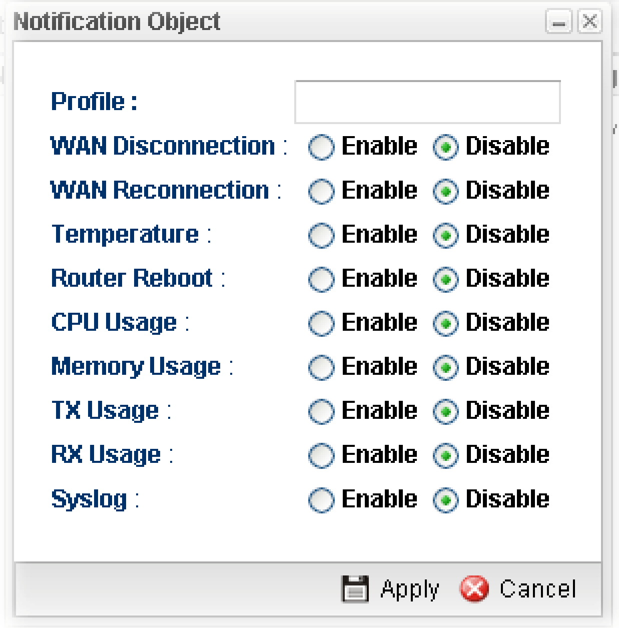
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
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.
WAN Disconnection	Display if such function is enabled or disabled.

Item	Description
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.



Notification Object

Profile :

WAN Disconnection : ○ Enable ● Disable

WAN Reconnection : ○ Enable ● Disable

Temperature : ○ Enable ● Disable

Router Reboot : ○ Enable ● Disable

CPU Usage : ○ Enable ● Disable

Memory Usage : ○ Enable ● Disable

TX Usage : ○ Enable ● Disable

RX Usage : ○ Enable ● Disable

Syslog : ○ Enable ● Disable

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.
Temperature	**Enable -** When the temperature is out of range, the router system will send the alert message to the recipient.

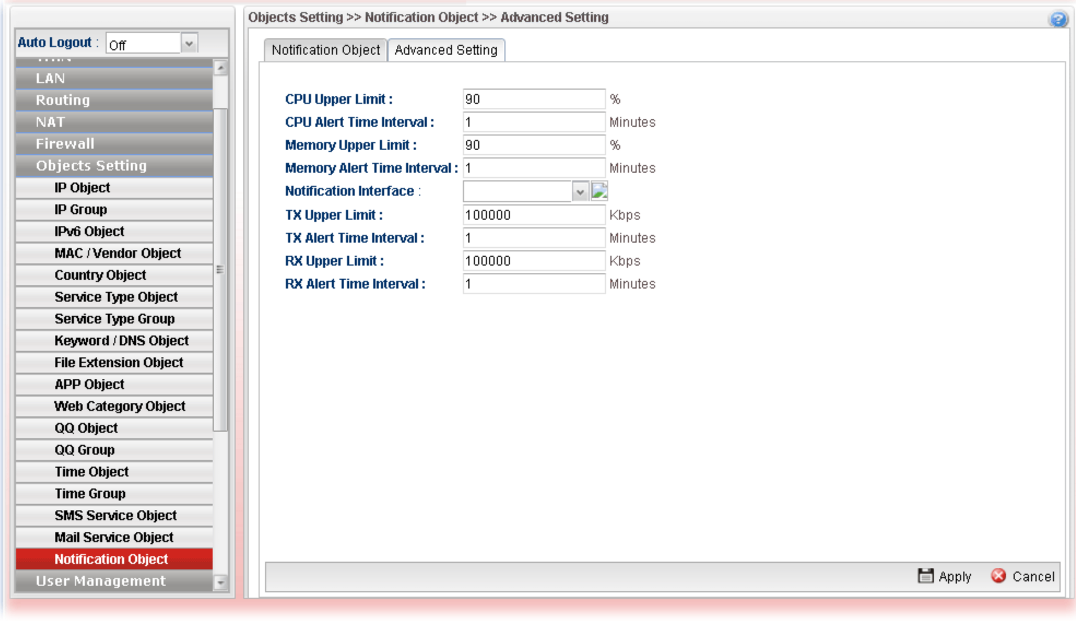
Router Reboot	**Enable -** When the router reboots, the router system will send the alert message to the recipient.
CPU Usage	**Enable** – When the CPU usage reaches a certain value, the router system will send the alert message to the recipient.
Memory Usage	**Enable** – When the memory usage reaches a certain value, the router system will send the alert message to the recipient.
TX Usage/RX Usage	**Enable** – When TX/RX usage reaches a certain value, the router system will send the alert message to the recipient.
Syslog	**Enable** – Such notification will be recorded in Syslog.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A new notification object profile has been created.

4.6.18.2 Advanced Setting

Such page is used to set the limit value for CPU, Memory, TX / RX. When CPU, Memory, TX / RX usage reaches the threshold, the router system will send the alert message to the recipient.



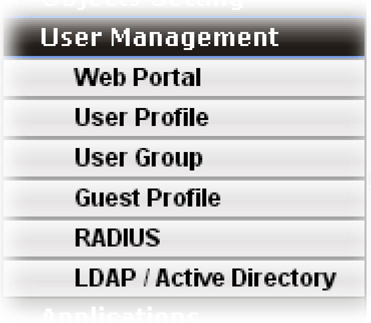
Objects Setting >> Notification Object >> Advanced Setting

CPU Upper Limit :	90	%
CPU Alert Time Interval :	1	Minutes
Memory Upper Limit :	90	%
Memory Alert Time Interval :	1	Minutes
Notification Interface :		
TX Upper Limit :	100000	Kbps
TX Alert Time Interval :	1	Minutes
RX Upper Limit :	100000	Kbps
RX Alert Time Interval :	1	Minutes

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

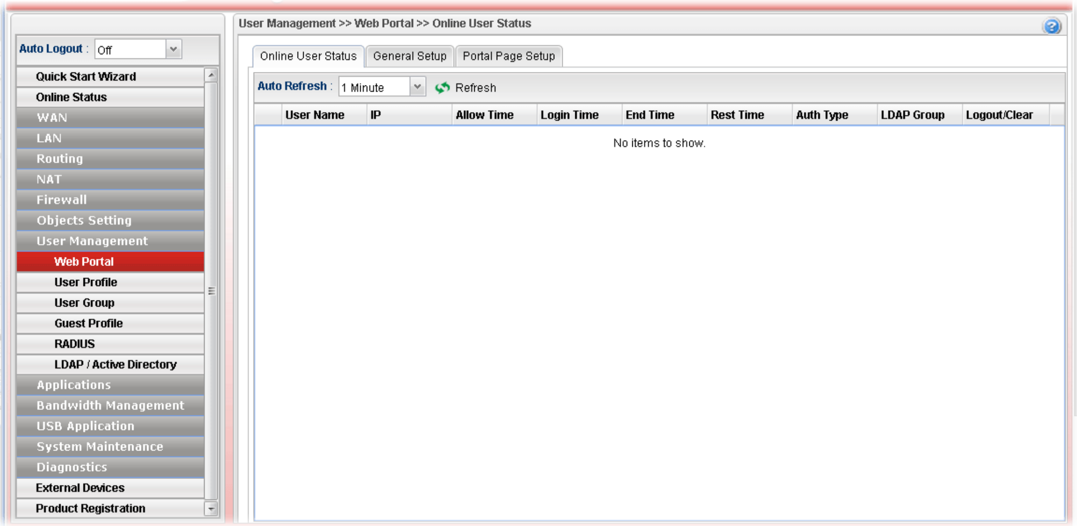
Web Portal is a gateway which organizes the network access of LAN hosts. The identity of LAN host can be recognized by web portal mechanism and then be managed for functions like firewall or load balance.

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.



User Management >> Web Portal >> Online User Status

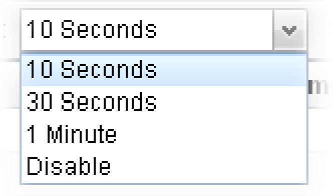
Auto Logout : Off

Auto Refresh : 1 Minute

User Name	IP	Allow Time	Login Time	End Time	Rest Time	Auth Type	LDAP Group	Logout/Clear

No items to show.

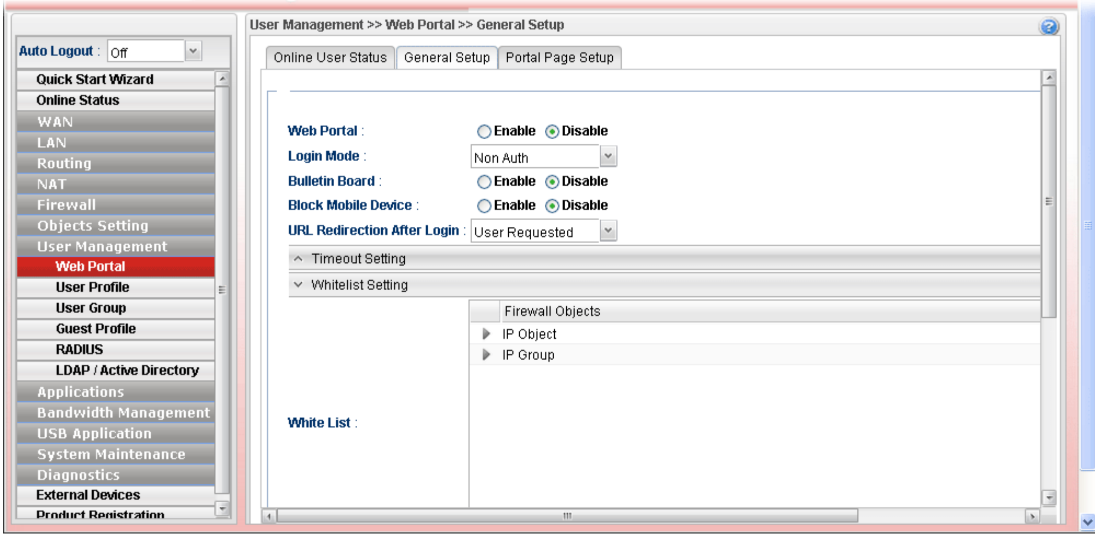
Available parameters will be explained as follows:

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.  10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
User Name	Display the name information for the user who logs into the WUI of Vigor300B.
IP	Display the IP address of the user who logs into the WUI of Vigor300B.
Allow Time	Display the total network connection time allowed for the log-in user.

Item	Description
Login Time	Display the starting time of the network connection.
End Time	Display the ending time of the network connection.
Rest Time	Display the rest time of the network connection.
Auth Type	Display the authentication type (local, RADIUS, LDAP, Login Disable, Guest) used by such user.
LDAP Group	Display the LDAP group used by such user.
Logout/Clear	It is a button which is used to disconnect the connection manually.

4.7.1.2 General Setup

This page configures the main settings of web portal function**.**



User Management >> Web Portal >> General Setup

Auto Logout : Off

Web Portal : ○ Enable ● Disable

Login Mode : Non Auth

Bulletin Board : ○ Enable ● Disable

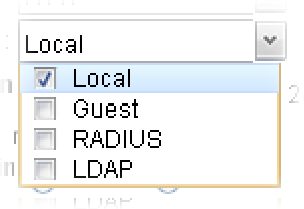
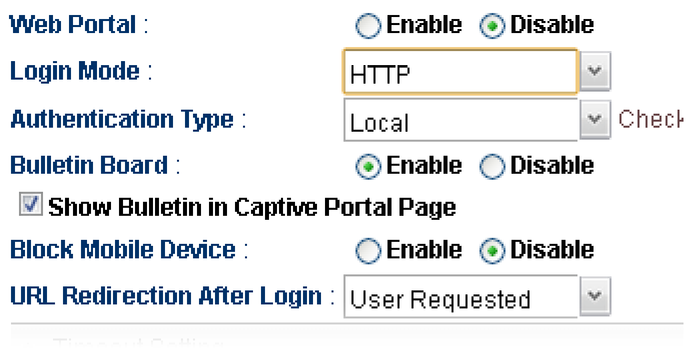
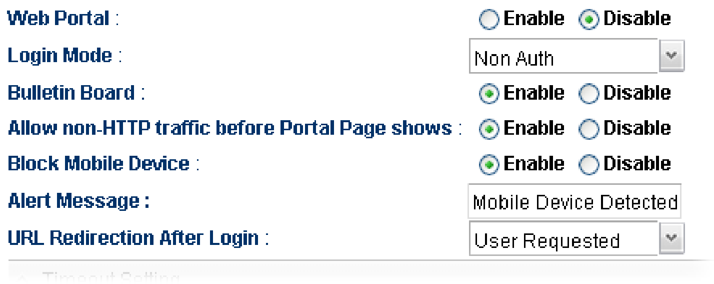
Block Mobile Device : ○ Enable ● Disable

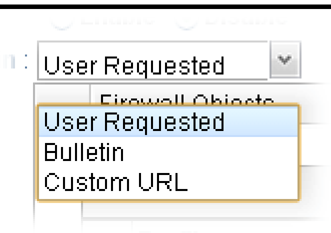
URL Redirection After Login : User Requested

White List :

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.

	 Local ☑ Local □ Guest □ RADIUS □ LDAP **LDAP Profiles -** It is available when **LDAP** is selected as **Authentication Type**. You have to specify one profile (defined in User Management>>LDAP/Active Directory) from the drop down list for LDAP authentication.
Bulletin Board	**Disable –** The function of Bulletin Board is disabled. **Enable –** The function of Bulleting Board is enabled. The message on the Bulleting Board will be displayed on the screen when the user logs into the web user interface of Vigor router. **Show Bulletin in Captive Portal Page –** It is available when **Bulletin Board** is enabled and **HTTP/HTTPS** is selected as **Login Mode**. It is used to determine showing bulletin in web portal login page or not.  Web Portal : ○ Enable ● Disable Login Mode : HTTP Authentication Type : Local Check Bulletin Board : ● Enable ○ Disable ☑ Show Bulletin in Captive Portal Page Block Mobile Device : ○ Enable ● Disable URL Redirection After Login : User Requested **Allow non-HTTP traffic before Portal Page shows –** It is available when **Bulletin Board** is enabled and **Non Auth** is selected as **Login Mode**. When it is enabled, non-HTTP traffic is allowed before the portal page appears.  Web Portal : ○ Enable ● Disable Login Mode : Non Auth Bulletin Board : ● Enable ○ Disable Allow non-HTTP traffic before Portal Page shows : ● Enable ○ Disable Block Mobile Device : ● Enable ○ Disable Alert Message : Mobile Device Detected URL Redirection After Login : User Requested
Block Mobile Device	**Enable –** Vigor router will detect and block if there is any mobile device trying to access into Internet via Vigor router. **Alert Message** – If a mobile device is detected, a warning message (typed in this field) will be displayed on the screen of mobile device. The default content is "Mobile Device Detected".

URL Redirection After Login	 User Requested User Requested Bulletin Custom URL **User Requested –** After passed the authentication made by Vigor router, the user will be redirected to original requested web page. **Bulletin** – If it is selected, users will be forced to see the information displayed on bulletin after passing through web portal. **Custom URL -** Any user who wants to access into Internet through this router will be forcefully redirected to the URL specified here first no matter what URL he types. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit. ● **Custom URL** – Type the URL of specified web page for redirection if **Custom URL** is selected as **URL Redirection After Login**.
Timeout Setting	
Daily Logout	**Enable -** Force the online user logging out the web user interface of Vigor router everyday. ● **Daily Time to Logout -** It is available when **Daily Logout** is enabled. Type that time setting (HH:MM) for the router to force online user leaving Vigor router. ● **Fully Recharge Time Quota After…. -** It is available when **Daily Logout** is enabled. The time quota of all local users will be recharged whenever Daily Logout is executed.
Period Logout	**Enable -** Force the online user logging out the web user interface of Vigor router after passing a period of time. ● **Period Time to Logout -** It is available when **Period Logout** is enabled.
Idle Logout	**Enable -** Force the online user logging out the web user interface of Vigor router when the router is idle. Enable such feature if time quota is used. ● **Idle Time(min)** – Set a time period. When the time is up, Vigor router will terminate the network connection for the online user.
Whitelist Setting	
White List	Select the source IP objects/groups that are ignored by web portal function.
White List IPv6	Select the source IP objects/groups that are ignored by web portal function.
Apply	Click it to save the configuration.

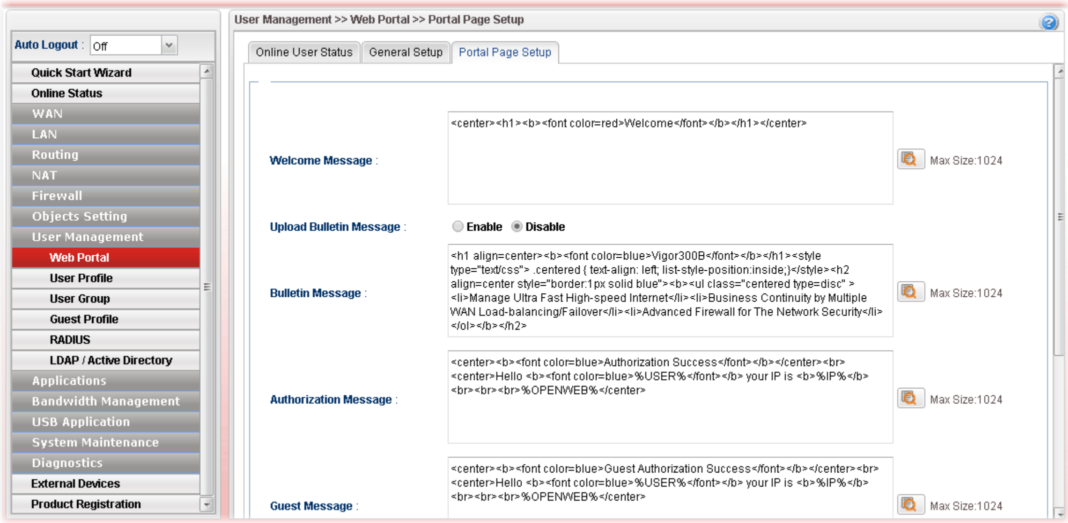
Cancel	Click it to exit the dialog without saving the configuration.

> **Note**: To turn off the web portal function, disable Login Mode and Bulletin Board at the same time.

4.7.1.3 Portal Page Setup

This page allows you to configure specified messages (HTML-supported) in web portal pages, and shows them to users accessing into Internet via web portal.

No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal



User Management >> Web Portal >> Portal Page Setup

Welcome Message :

```
<center><h1><b><font color=red>Welcome</font></b></h1></center>
```

Max Size:1024

Upload Bulletin Message : ○ Enable ● Disable

Bulletin Message :

```
<h1 align=center><b><font color=blue>Vigor300B</font></b></h1><style
type="text/css"> .centered { text-align: left; list-style-position:inside;}</style><h2
align=center style="border:1px solid blue"><b><ul class="centered type=disc" >
<li>Manage Ultra Fast High-speed Internet</li><li>Business Continuity by Multiple
WAN Load-balancing/Failover</li><li>Advanced Firewall for The Network Security</li>
</ol></b></h2>
```

Max Size:1024

Authorization Message :

```
<center><b><font color=blue>Authorization Success</font></b></center><br>
<center>Hello <b><font color=blue>%USER%</font></b> your IP is <b>%IP%</b>
<br><br><br>%OPENWEB%</center>
```

Max Size:1024

Guest Message :

```
<center><b><font color=blue>Guest Authorization Success</font></b></center><br>
<center>Hello <b><font color=blue>%USER%</font></b> your IP is <b>%IP%</b>
<br><br><br>%OPENWEB%</center>
```

Max Size:1024

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 Vigor300B.
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.

Item	Description
	Upload Login Image – Choose a file to upload to Vigor300B. 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 Vigor300B.
Login Page Preview	Click it to have a preview of login page (including welcome message, and bulletin message).
Reset All to Default	Reset the above message fields to default settings. Check the box and then press **Apply**.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

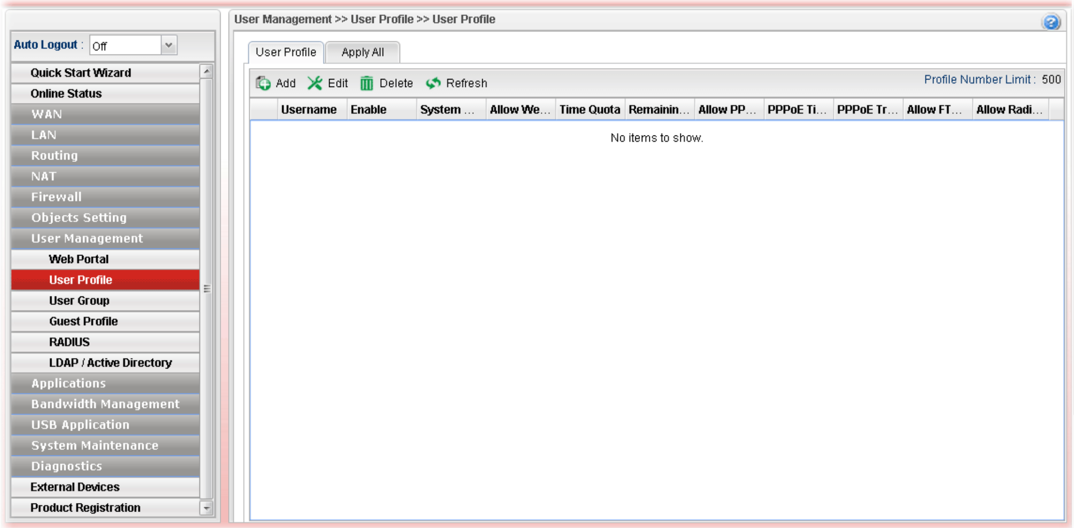
After finished the above settings, click **Apply** to save the configuration.

4.7.2 User Profile

This function allows to configure all accounts (user profiles) in Vigor300B, 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, PPTP/L2TP/PPPoE server, system administration, etc., for different users.



User Management >> User Profile >> User Profile

Auto Logout : Off

Profile Number Limit : 500

Username	Enable	System ...	Allow We...	Time Quota	Remainin...	Allow PP...	PPPoE Ti...	PPPoE Tr...	Allow FT...	Allow Radi...

No items to show.

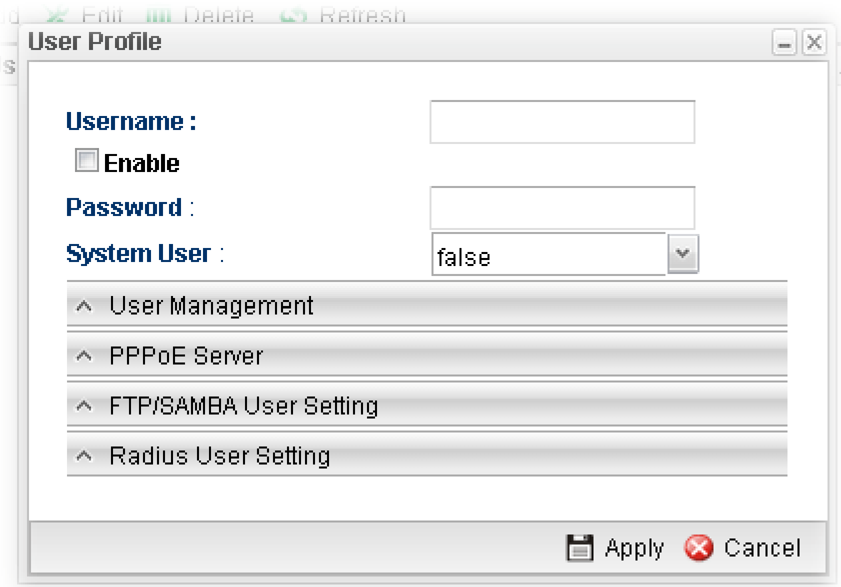
Each item will be explained as follows:

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.

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


User Profile

Username :

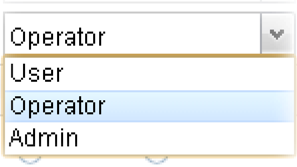
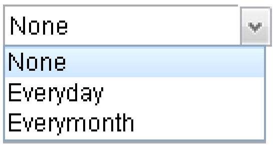
□ Enable

Password :

System User : false

Available parameters are listed as follows:

Item	Description
Username	Type a name for such user profile (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the Username specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Enable	Check this box to enable such profile.
Password	Type a password for such profile (e.g., *lug123*, *wug123,wug456*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.
System User	Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router. **False –** Choose it to disable the function of System User. Such user profile does not have the right to operate the router's function. **True –** Choose it to enable the function of System User. **Privilege Level –** If **true** is selected for **System User**, you have to specify the privilege level (User/Operator/Admin) for such profile.

	 **Admin** has the greatest authority for router operation; **User** has the smallest authority for router operation.
User Management	
Allow Web Portal Login	**Enable** – Click it to enable web portal login with such profile. **Disable** – Click it to disable the option.
Time Quota	**Enable** – Click it to enable time quota function. ● **Set Time Quota (min)** – Type the time value. ● **Remaining Time** – Display the remaining time for the user profile. **Disable** – Click it to disable the function. **Note**: The range of Time Quota is 1~14400 minutes.
Max Simultaneous Login	It means the maximum online number of clients logging with this profile. The range is from 1 to 255. -1 means not limit; 0 means No access.
PPPoE Server	
Allow PPPoE Server Login	Click **Enable** to activate related PPPoE configuration.
Quota Reset Frequency	It is used to configure the cycle time for PPPoE quota. Note that each time when the quota is reset, the value of Current Time Used/Current Traffic Quota will be reset to initial situation (0). **Everyday** – The quota for PPPoE will be reset every day. **Everymonth** – The quota for PPPoE will be reset every month. 
Time Quota (min)	Type a time quota for PPPoE connection. **Note**: The range of Time Quota is 1~14400 minutes.
Current Time Used (min)	Display the cumulative amount of time that the user used. **Reset -** Click it to reset the setting to default value (0).
Traffic Quota(MB)	It is used to set the maximum traffic (MB) for such user profile.
Current Traffic Quota (MB)	Display the cumulative amount of data traffic that the user used. **Reset -** Click it to reset the setting to default value (0).

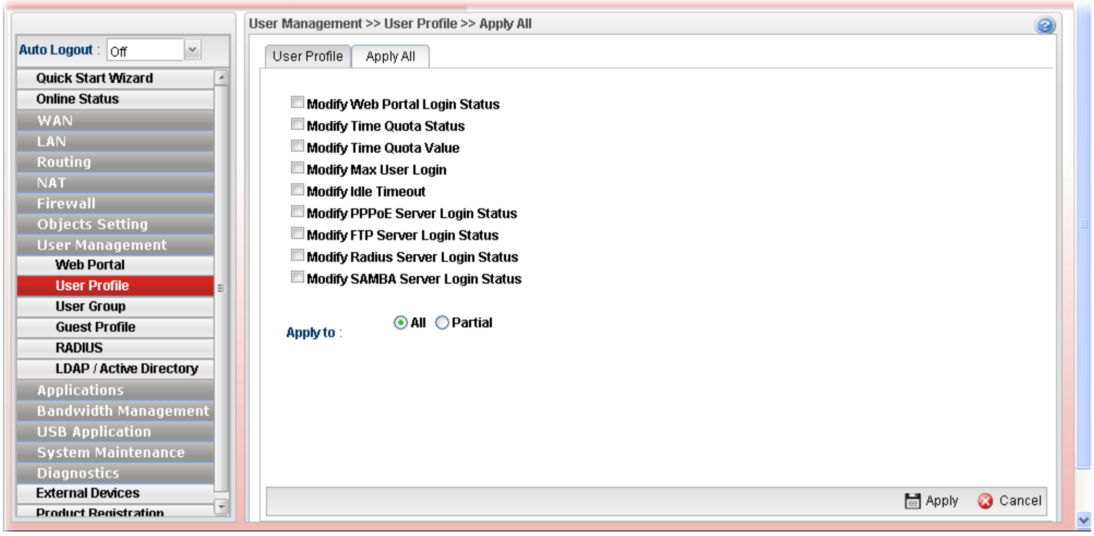
MAC Binding	Specify a MAC address which is limited and used for such PPPoE account. **Enable –** Click it to enable the function. **MAC Address** – If MAC Binding is enabled, simply type the MAC address of the router in this field.
Idle Timeout (sec)	If the user is idle over the limitation of the timer, 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.
FTP/SAMBA User Setting	
Allow FTP/SAMBA Server Login	Click **Enable** to allow the remote user accessing into Internet via FTP/SAMBA 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.



User Management >> User Profile >> Apply All

□ Modify Web Portal Login Status
□ Modify Time Quota Status
□ Modify Time Quota Value
□ Modify Max User Login
□ Modify Idle Timeout
□ Modify PPPoE Server Login Status
□ Modify FTP Server Login Status
□ Modify Radius Server Login Status
□ Modify SAMBA Server Login Status

Apply to : ● All ○ Partial

Available parameters are listed as follows:

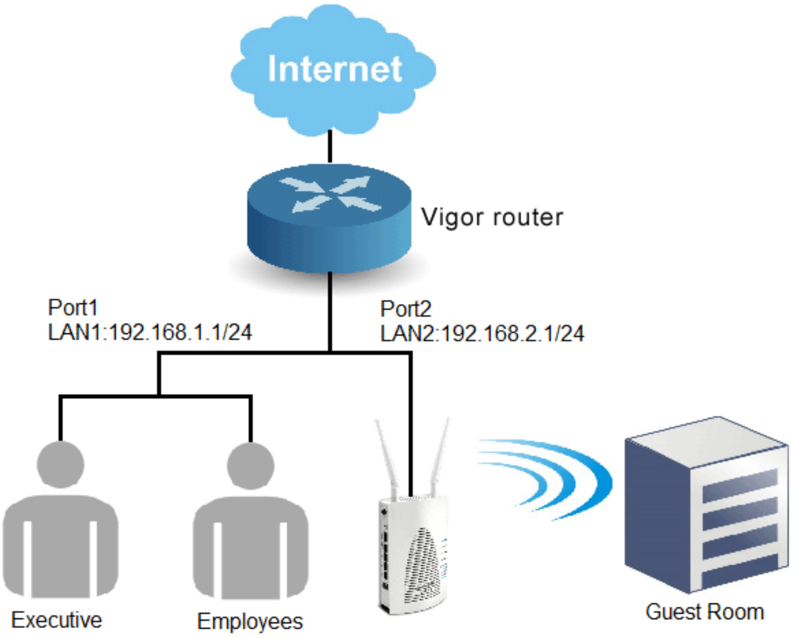
Item	Description
Modify Web Portal Login Status	Check the box to configure detailed setting. **Enable –** Click it to enable the web portal login function for remote client.
Modify Time Quota Status	Check the box to configure detailed setting. **Enable –** Click it to enable the time quota function for 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 PPPoE/FTP/Radius /SAMBA Server Login	Check the box to configure detailed setting. **Enable –** Click it to enable the PPPoE/FTP/Radius/SAMBA 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.

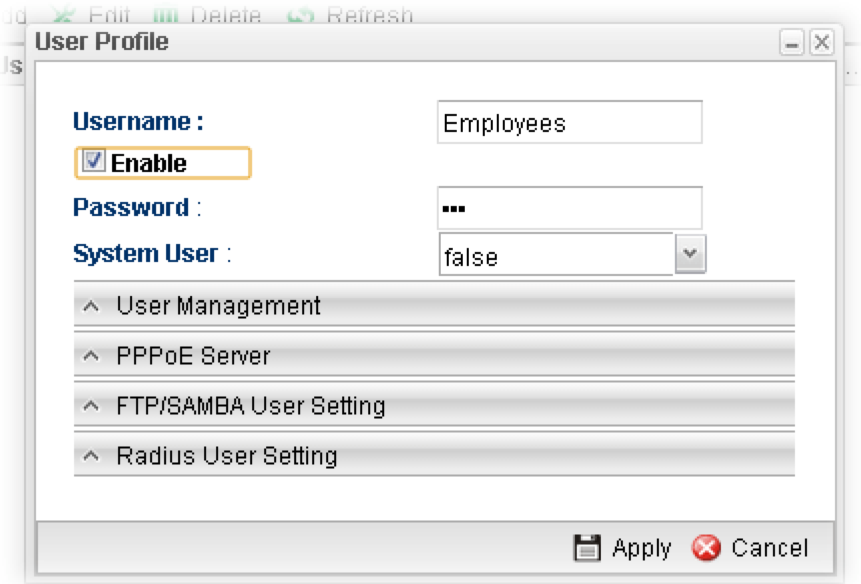
Example: How to Generate Mass LAN Clients with User Management on Vigor300B

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.



User Profile

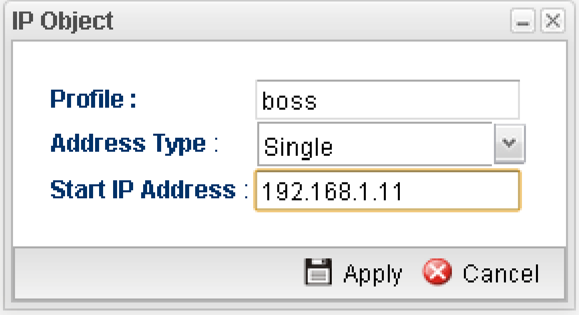
Username : Employees

☑ Enable

Password : •••

System User : false

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.



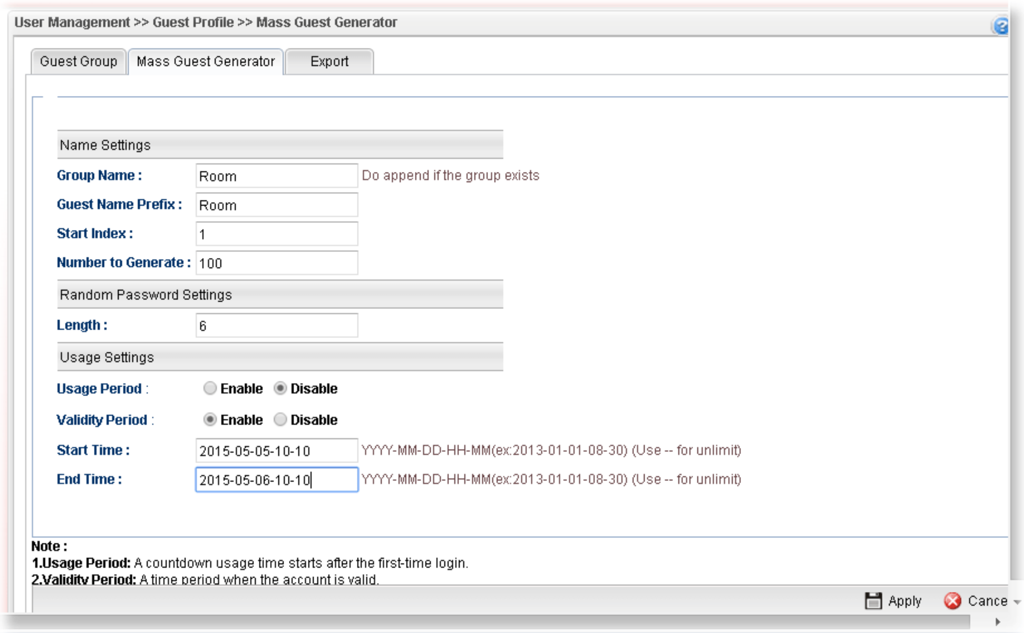
IP Object

Profile : boss

Address Type : Single

Start IP Address : 192.168.1.11

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.



User Management >> Guest Profile >> Mass Guest Generator

Name Settings

Group Name : Room   Do append if the group exists

Guest Name Prefix : Room

Start Index : 1

Number to Generate : 100

Random Password Settings

Length : 6

Usage Settings

Usage Period : ○ Enable ● Disable

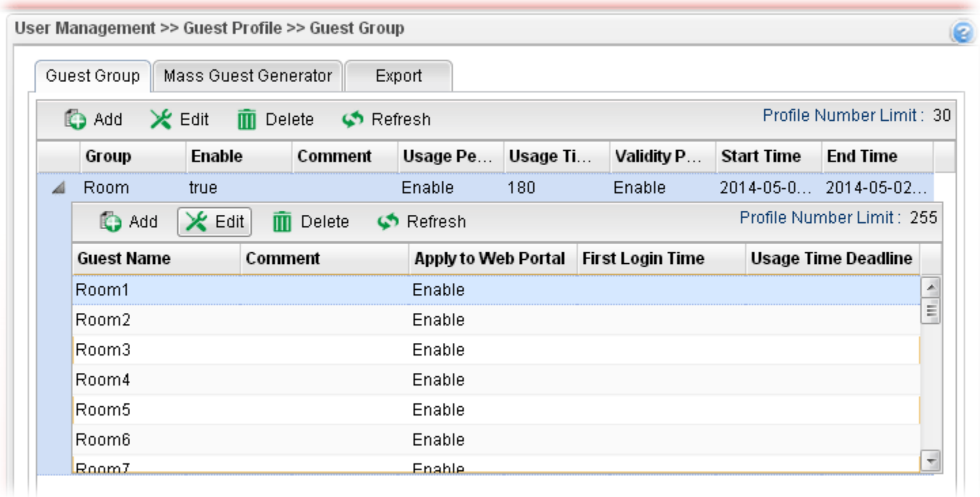
Validity Period : ● Enable ○ Disable

Start Time : 2015-05-05-10-10   YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

End Time : 2015-05-06-10-10   YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

Note :
1.Usage Period: A countdown usage time starts after the first-time login.
2.Validity Period: A time period when the account is valid.

6. Open **User Management** >> **Guest Profile** and click **Guest Group** to check the **mass user account group**.



User Management >> Guest Profile >> Guest Group

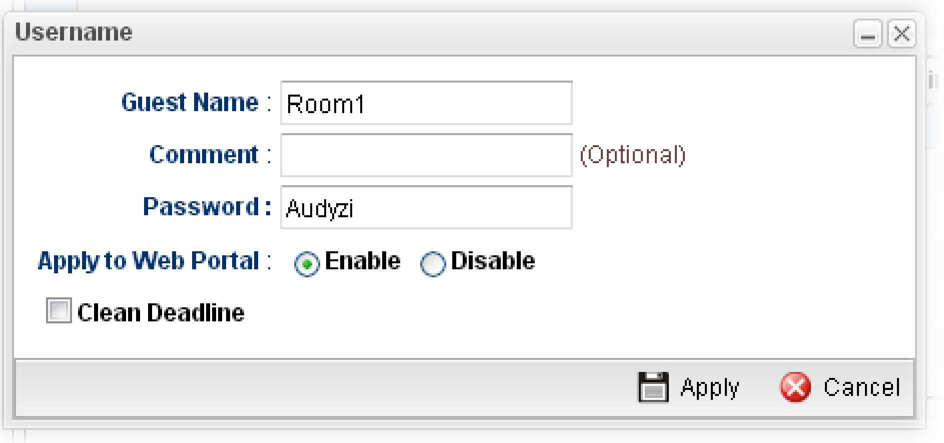
Profile Number Limit : 30

Group	Enable	Comment	Usage Pe...	Usage Ti...	Validity P...	Start Time	End Time
Room	true		Enable	180	Enable	2014-05-0...	2014-05-02...

Profile Number Limit : 255

Guest Name	Comment	Apply to Web Portal	First Login Time	Usage Time Deadline
Room1		Enable		
Room2		Enable		
Room3		Enable		
Room4		Enable		
Room5		Enable		
Room6		Enable		
Room7		Enable		

By clicking each account (e.g., choose **Room1** 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

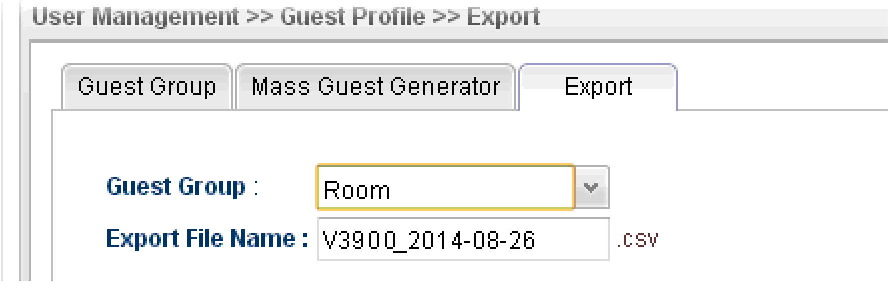
Comment : (Optional)

Password : Audyzi

Apply to Web Portal : ● Enable ○ Disable

□ Clean Deadline

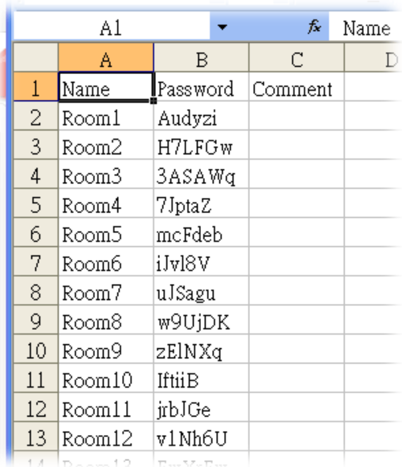
Note that Administrator is able to **Export** the information for the whole group to a *.csv* file, which is useful to **redistribute** the account and password combinations to guests.



User Management >> Guest Profile >> Export

Guest Group : Room

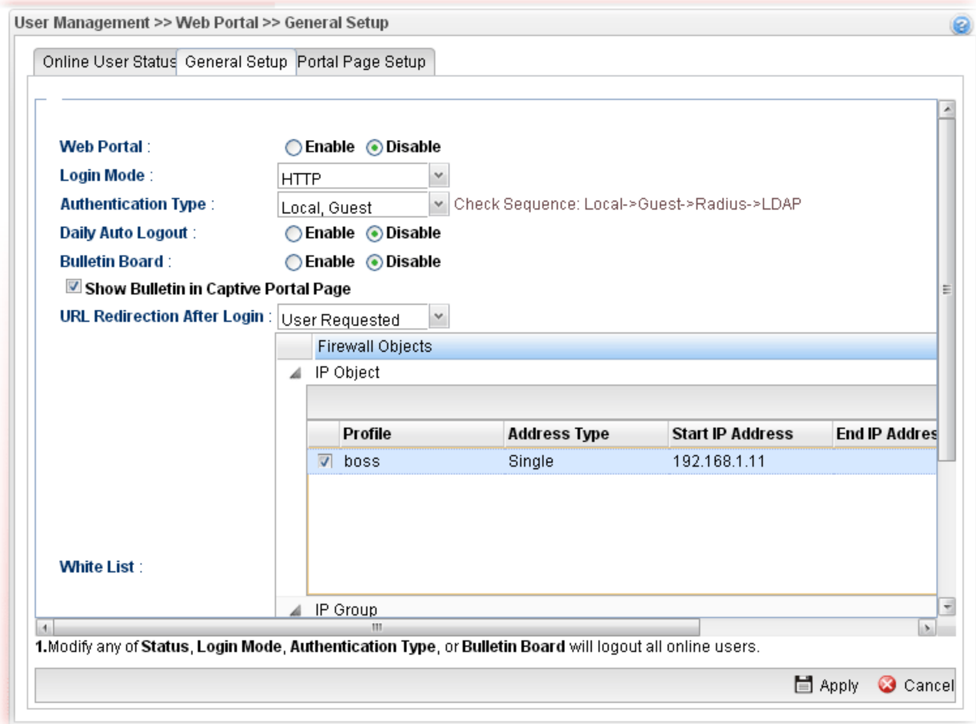
Export File Name : V3900_2014-08-26 .csv



A1 Name

	A	B	C	D
1	Name	Password	Comment	
2	Room1	Audyzi		
3	Room2	H7LFGw		
4	Room3	3ASAWq		
5	Room4	7JptaZ		
6	Room5	mcFdeb		
7	Room6	iJvl8V		
8	Room7	uJSagu		
9	Room8	w9UjDK		
10	Room9	zElNXq		
11	Room10	IftiiB		
12	Room11	jrbJGe		
13	Room12	v1Nh6U		
14	Room13	[illegible]		

7. Open **User Management** >> **Web Portal** and click the **General Setup** tab to open the following page. Check **Local** and **Guest** as **Authentication Type**. Check IP object named of **Boss** to put it into the white list, and this will allow this IP address to access to the Internet without authentication.



User Management >> Web Portal >> General Setup

Web Portal : ○ Enable ● Disable

Login Mode : HTTP

Authentication Type : Local, Guest Check Sequence: Local->Guest->Radius->LDAP

Daily Auto Logout : ○ Enable ● Disable

Bulletin Board : ○ Enable ● Disable

☑ Show Bulletin in Captive Portal Page

URL Redirection After Login : User Requested

White List :

Firewall Objects

IP Object

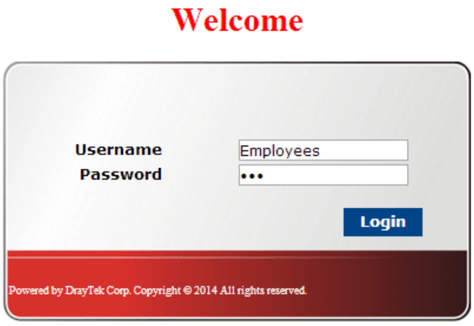
	Profile	Address Type	Start IP Address	End IP Addres
☑	boss	Single	192.168.1.11	

IP Group

1.Modify any of **Status**, **Login Mode**, **Authentication Type**, or **Bulletin Board** will logout all online users.

8. After finishing configuration, Vigor300B will redirect users to the authentication page when they try accessing to the Internet.

For Employees to access into Internet:



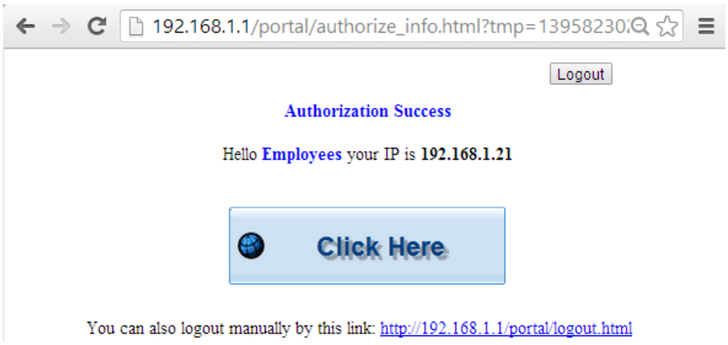
Welcome

Username Employees

Password •••

Login

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



192.168.1.1/portal/authorize_info.html?tmp=13958230

Logout

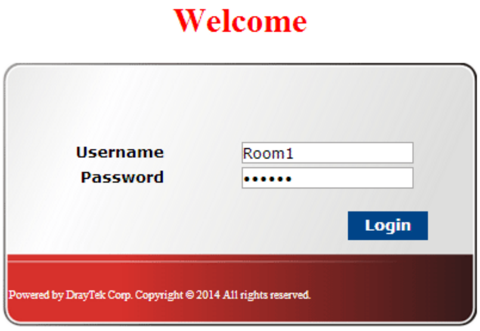
Authorization Success

Hello **Employees** your IP is **192.168.1.21**

Click Here

You can also logout manually by this link: http://192.168.1.1/portal/logout.html

For Room guest to access into Internet:



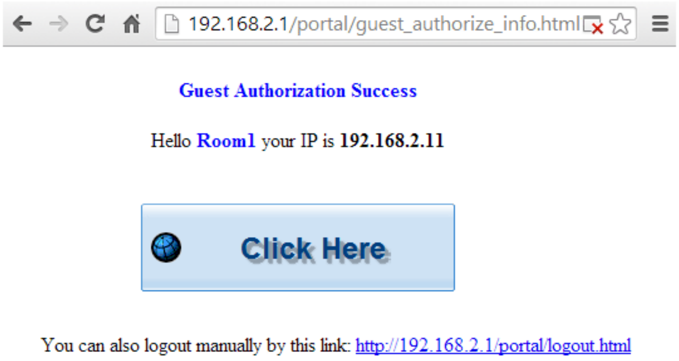
Welcome

Username Room1

Password ••••••

Login

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



192.168.2.1/portal/guest_authorize_info.html

Guest Authorization Success

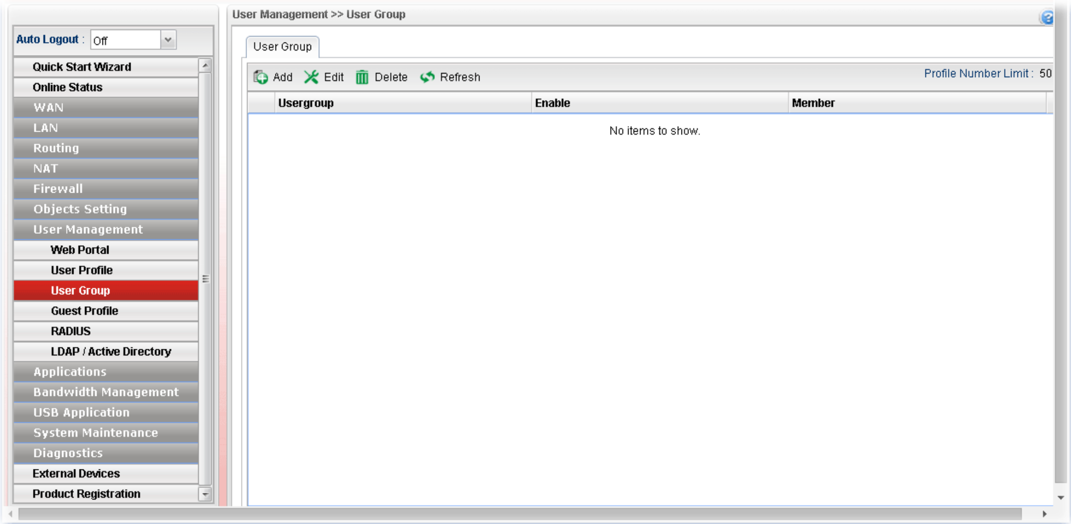
Hello **Room1** your IP is **192.168.2.11**

Click Here

You can also logout manually by this link: http://192.168.2.1/portal/logout.html

4.7.3 User Group

The **User Group** can consist of several us er profiles, which help the administrator to manage a large number of users conveniently.

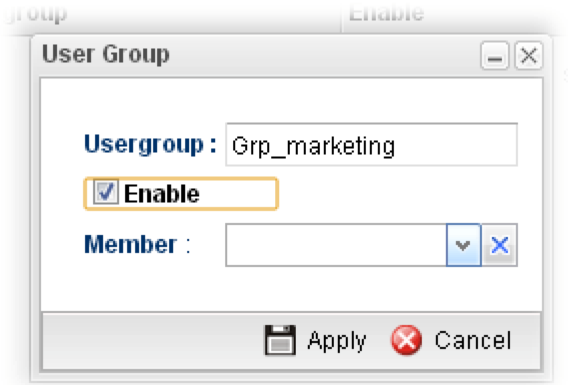


Each item will be explained as follows:

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.



User Group

Usergroup : Grp_marketing

☑ Enable

Member :

Available parameters are listed as follows:

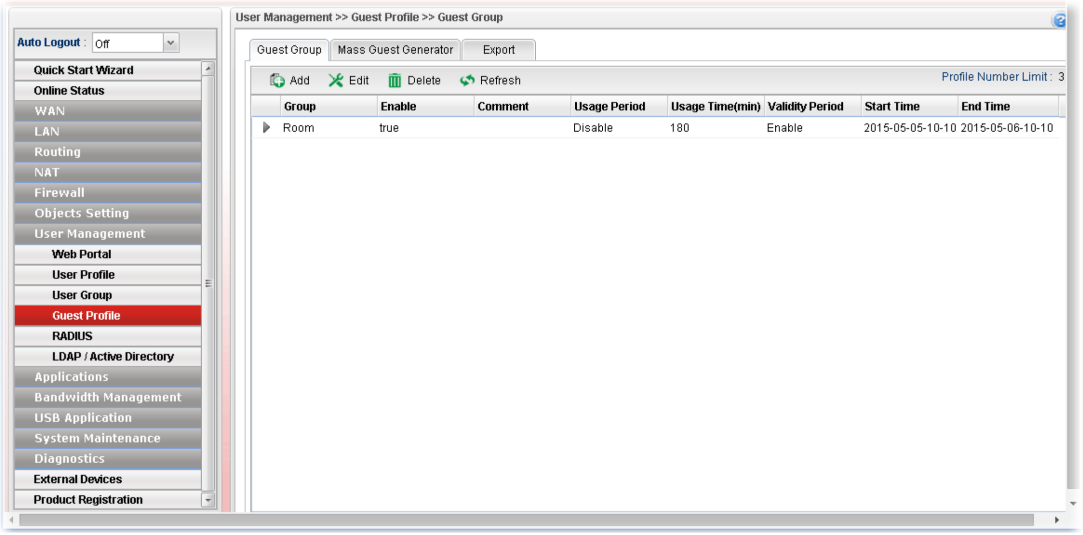
Item	Description
Usergroup	Type the name of such profile.
Enable	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group. To clear the selected one, click ☒ to remove current object selections.
Apply	Click it to save the configuration.
Cancel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



User Management >> Guest Profile >> Guest Group

Auto Logout : Off

Profile Number Limit : 3

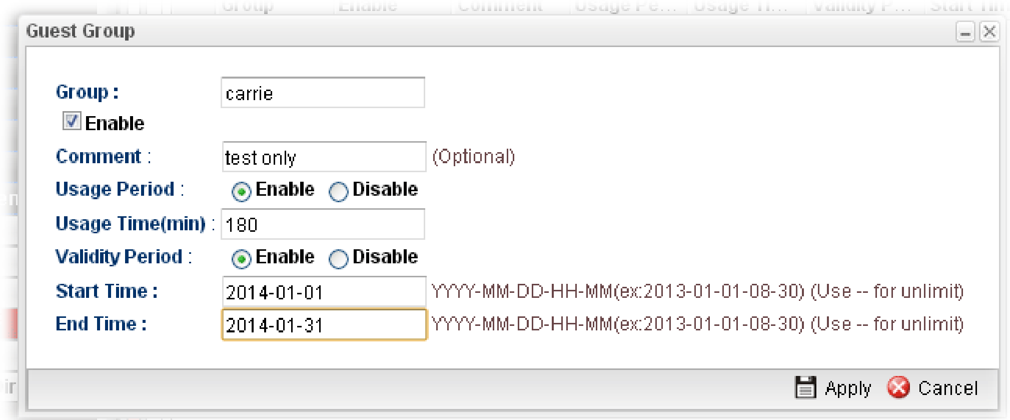
	Group	Enable	Comment	Usage Period	Usage Time(min)	Validity Period	Start Time	End Time
▶	Room	true		Disable	180	Enable	2015-05-05-10-10	2015-05-06-10-10

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.
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.



Guest Group

Group : carrie

☑ Enable

Comment : test only (Optional)

Usage Period : ● Enable ○ Disable

Usage Time(min) : 180

Validity Period : ● Enable ○ Disable

Start Time : 2014-01-01 YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

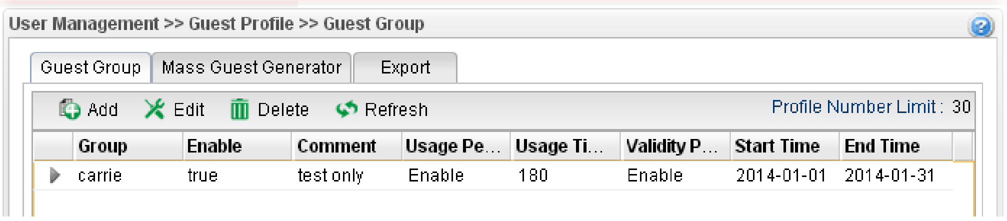
End Time : 2014-01-31 YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

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.



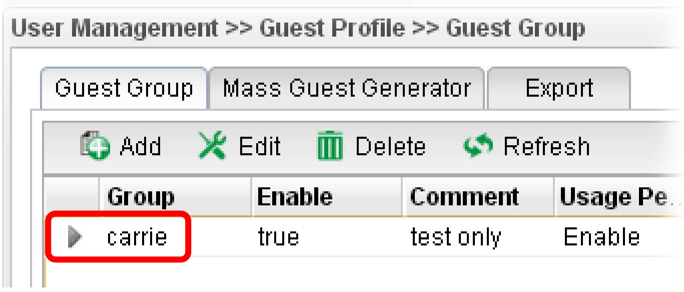
User Management >> Guest Profile >> Guest Group

Guest Group | Mass Guest Generator | Export

Add Edit Delete Refresh Profile Number Limit : 30

	Group	Enable	Comment	Usage Pe...	Usage Ti...	Validity P...	Start Time	End Time
▶	carrie	true	test only	Enable	180	Enable	2014-01-01	2014-01-31

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.



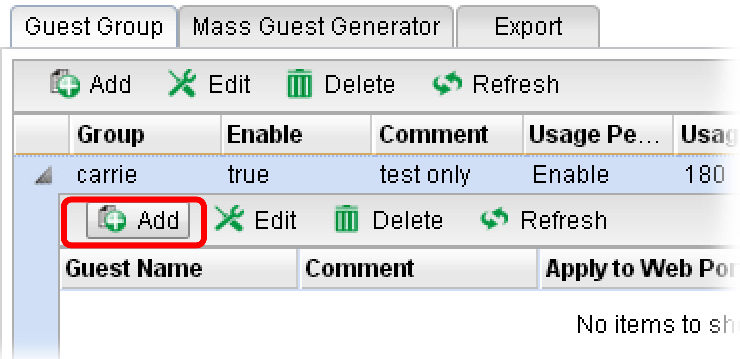
User Management >> Guest Profile >> Guest Group

Guest Group | Mass Guest Generator | Export

Add Edit Delete Refresh

	Group	Enable	Comment	Usage Pe
▶	carrie	true	test only	Enable

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



Guest Group | Mass Guest Generator | Export

Add Edit Delete Refresh

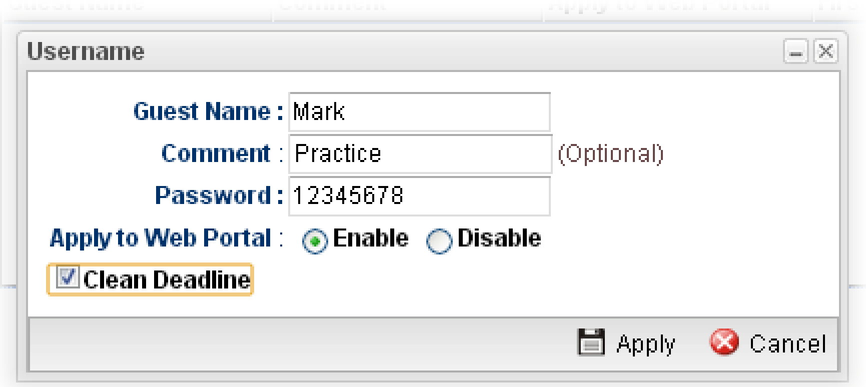
	Group	Enable	Comment	Usage Pe...	Usag
◢	carrie	true	test only	Enable	180

Add Edit Delete Refresh

Guest Name	Comment	Apply to Web Por

No items to sh

8. The following page for configuration will appear.



Username

Guest Name : Mark

Comment : Practice (Optional)

Password : 12345678

Apply to Web Portal : ● Enable ○ Disable

☑ Clean Deadline

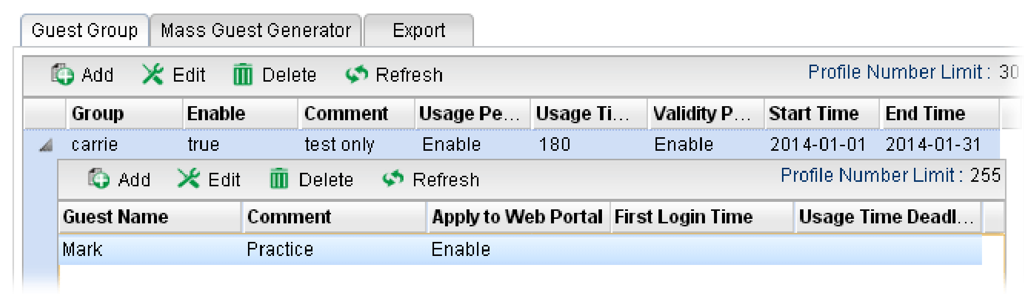
Available parameters are listed as follows:

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).

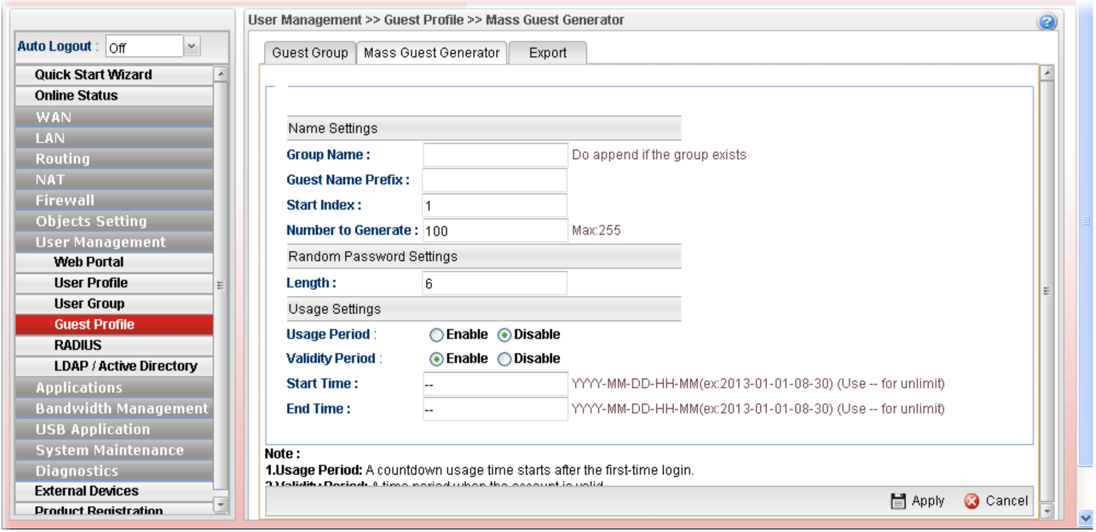


Group	Enable	Comment	Usage Pe...	Usage Ti...	Validity P...	Start Time	End Time
carrie	true	test only	Enable	180	Enable	2014-01-01	2014-01-31

Guest Name	Comment	Apply to Web Portal	First Login Time	Usage Time Deadl...
Mark	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.



User Management >> Guest Profile >> Mass Guest Generator

Name Settings

Group Name : Do append if the group exists

Guest Name Prefix :

Start Index : 1

Number to Generate : 100 Max:255

Random Password Settings

Length : 6

Usage Settings

Usage Period : ○ Enable ● Disable

Validity Period : ● Enable ○ Disable

Start Time : -- YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

End Time : -- YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

Note :
1.Usage Period: A countdown usage time starts after the first-time login.
2.Validity Period: A time period when the account is valid

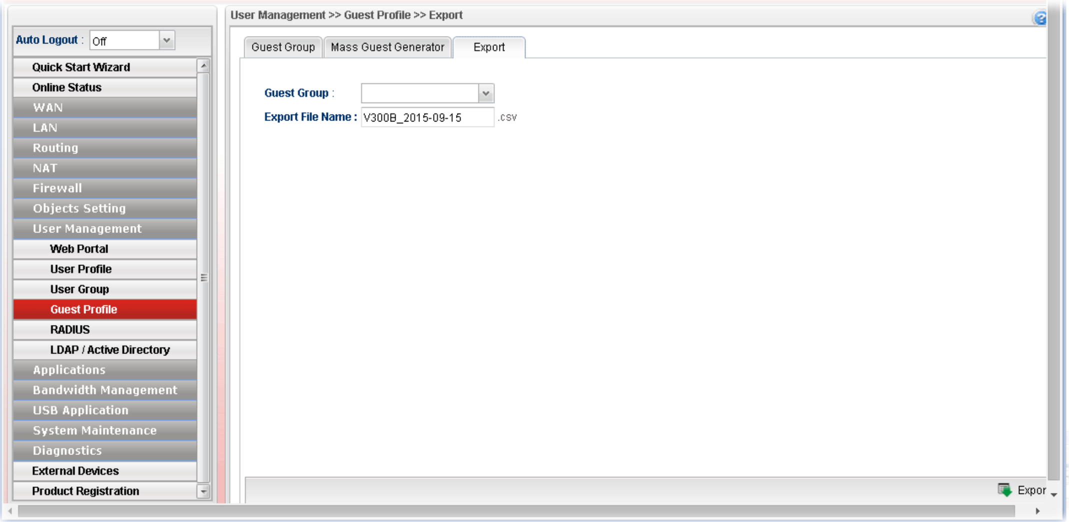
Available parameters are listed as follows:

Item	Description
Name Settings	**Group Name** – Type the name of the guest group. **Guest Name Prefix** – The guest names created with such manner requires a prefix as the basis of name input. **Note:** Guest Name Prefix disallows these 6 characters "^?$%.&". **Start Index** – Type a number which will be treated as the starting number for generating mass guest profiles. **Note:** The range of Start index is 1~10000. **Number to Generate** – Type the total number of guests to be generated at one time. The guest name will be named by combining “Guest Name Prefix” + “Start Index”, for example: Guest Name Prefix => teashop_ Start Index => 100 Number to Generate => 50 Then, the guests names generated will be: teashop_100 (starting) teashop_101 teashop_102 ... teashop_150 (ending)
Random Password Settings	**Length** – Type a number to determine the length of the random passwords which will be assigned to the mass guest profiles by the system. The range of Password Length is 6~12.

Item	Description
Usage Settings	**Usage Period** –It determines the usage time for the guest accessing into Internet each time. Click **Enable** to enable such option. ● **Usage Time(min)-**The default setting is 180 minutes. **Validity Period** –It determines the valid period for the guest accessing into Internet. That is, the guest cannot access into the Internet anytime outside the valid period. Click **Enable** to enable such option. ● **Start Time/End Time** – Specify the valid period by typing the time with the format of HH-MM-SS.
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.



User Management >> Guest Profile >> Export

Guest Group :

Export File Name : V300B_2015-09-15 .csv

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.

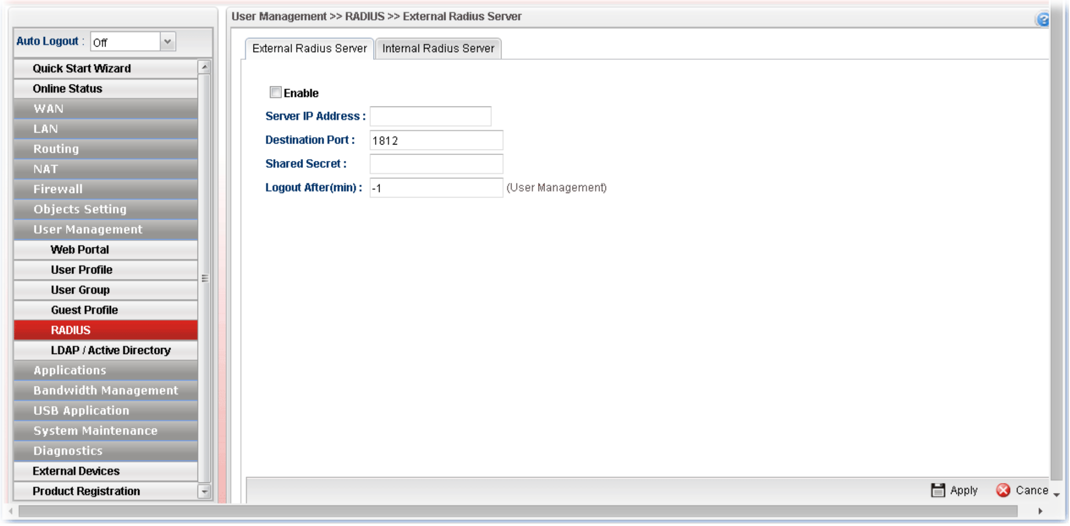
4.7.5 RADIUS

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.



User Management >> RADIUS >> External Radius Server

Auto Logout : Off

External Radius Server | Internal Radius Server

□ Enable

Server IP Address :

Destination Port : 1812

Shared Secret :

Logout After(min) : -1 (User Management)

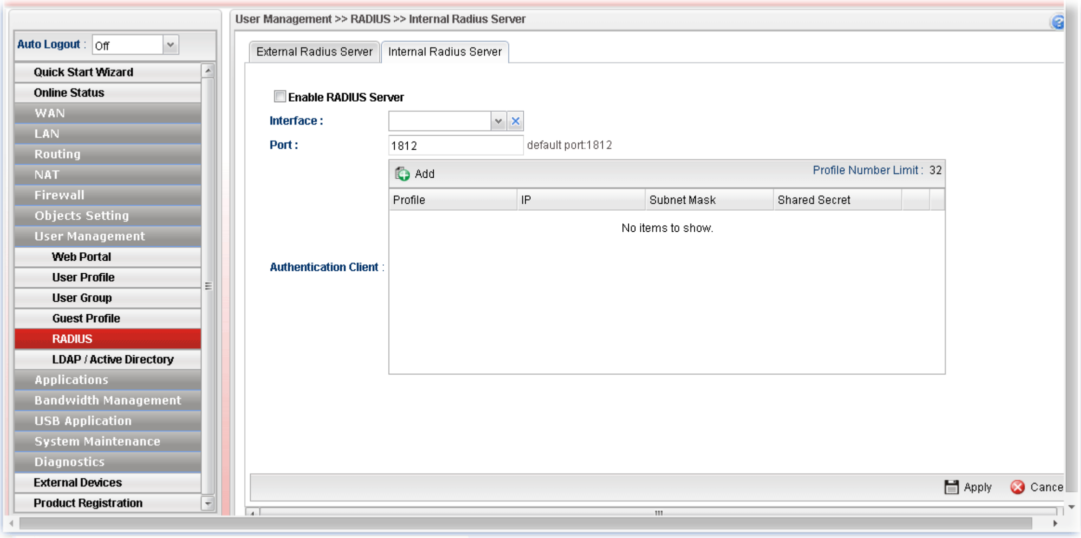
Available parameters are listed as follows:

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.



User Management >> RADIUS >> Internal Radius Server

□ Enable RADIUS Server

Interface :

Port : 1812 default port:1812

Profile Number Limit : 32

Profile	IP	Subnet Mask	Shared Secret
No items to show.			

Authentication Client :

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.

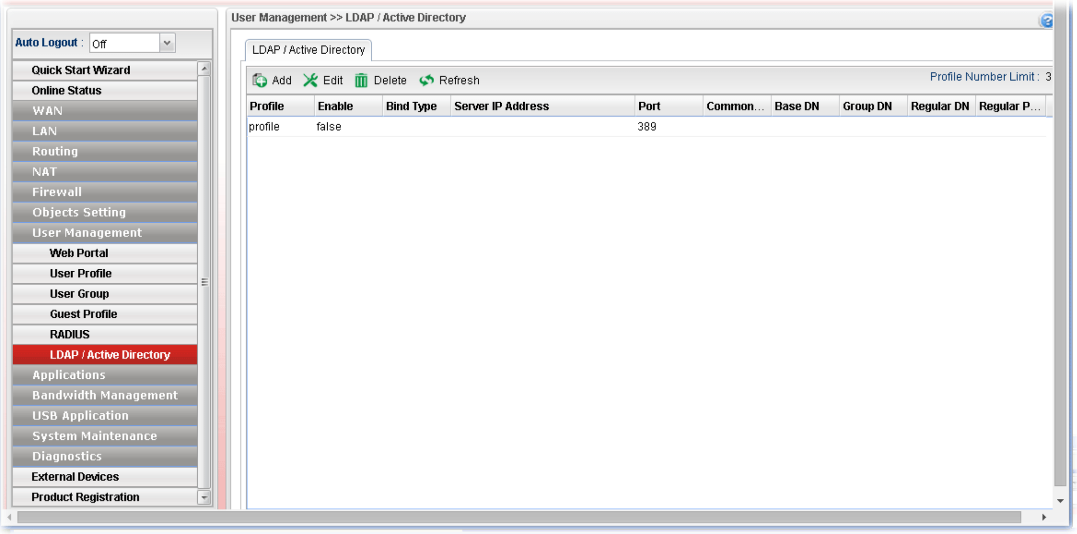
After finished the above settings, click **Apply** to save the configuration.

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.



Profile	Enable	Bind Type	Server IP Address	Port	Common...	Base DN	Group DN	Regular DN	Regular P...
profile	false			389					

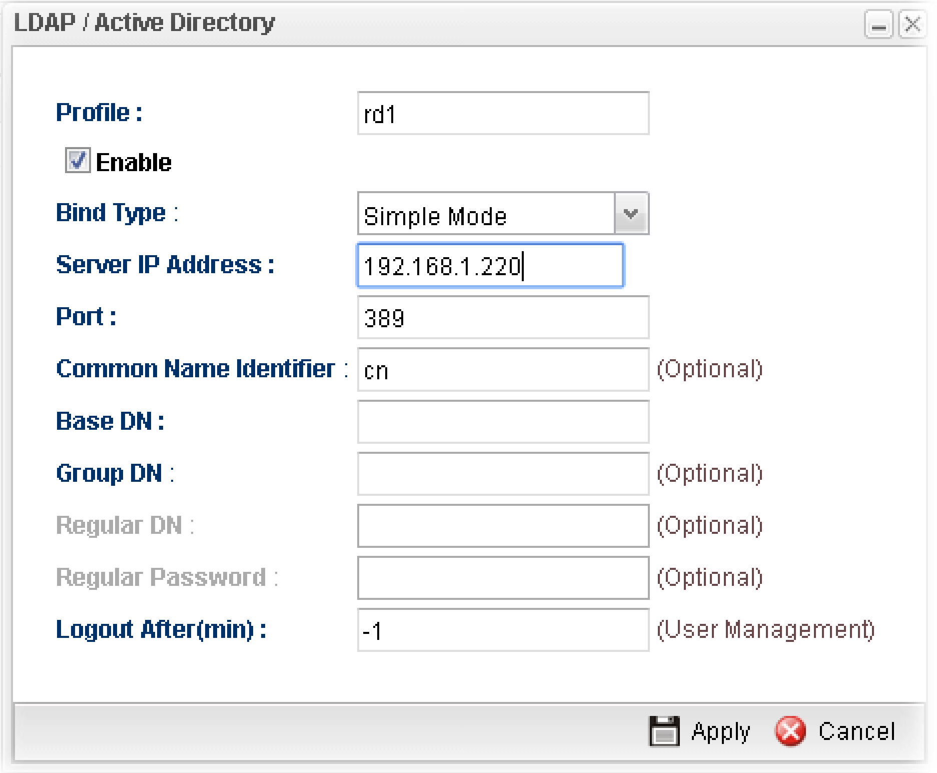
Available parameters are listed as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Bind Type	Display the type setting selected for such profile.
Server IP Address	Display the IP address of the LDAP server.
Port	Display the port number set for such profile.

Item	Description
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

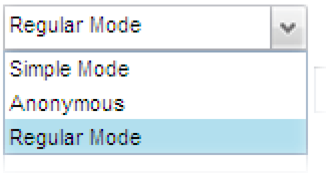
1. Open **User Management>>LDAP/Active Directory.**
2. Simply click the **Add** button.
3. The following dialog will appear.



Profile :	rd1	
☑ Enable		
Bind Type :	Simple Mode	
Server IP Address :	192.168.1.220	
Port :	389	
Common Name Identifier :	cn	(Optional)
Base DN :		
Group DN :		(Optional)
Regular DN :		(Optional)
Regular Password :		(Optional)
Logout After(min) :	-1	(User Management)

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.

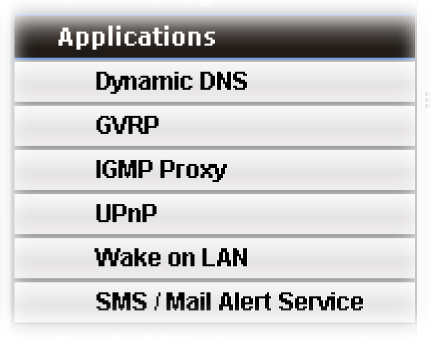
Bind Type	There are three types of bind type supported.  Regular Mode Simple Mode Anonymous Regular Mode **Simple Mode** – Just simply do the bind authentication without any search action. **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication. **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
Server IP Address	Enter the IP address of LDAP server.
Port	Type a port number as the destination port for LDAP server.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn"
Base DN	It means "**Base Distinguished Name**". Type the distinguished name used to look up entries on the LDAP server.
Group DN	It means "**Group Distinguished Name**". Type the distinguished name used to look up entries on the LDAP server.
Regular DN	Type this setting if **Regular Mode** is selected as **Bind Type.**
Regular Password	Specify a password if **Regular Mode** is selected as **Bind Type.**
Logout After(min)	It means the maximum usage duration for RADIUS authentication.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A new LADP/Active Directory Profile has been created.

4.8 Application

Below shows the menu items for Applications.



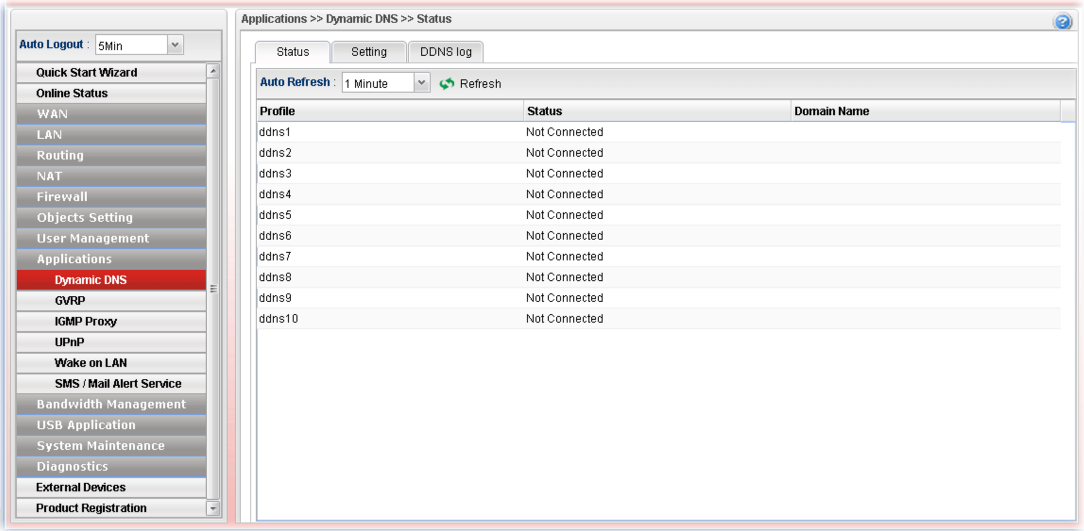
4.8.1 Dynamic DNS

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

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

4.8.1.1 Status

This page displays the status for all the available DDNS profiles.

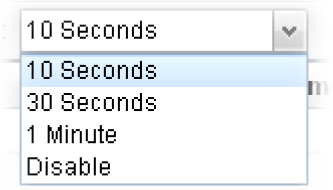


Applications >> Dynamic DNS >> Status

Auto Refresh : 1 Minute

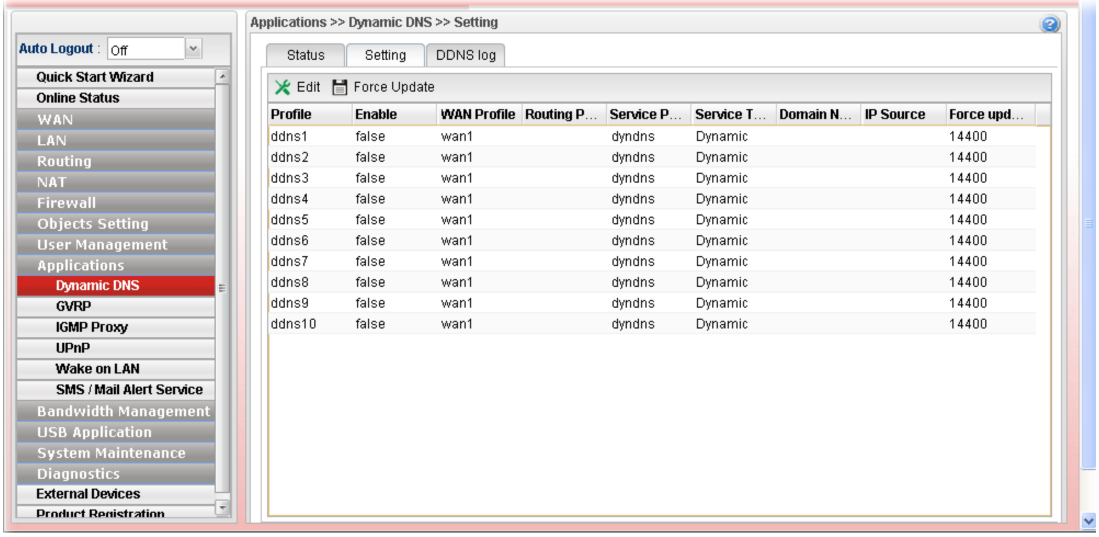
Profile	Status	Domain Name
ddns1	Not Connected	
ddns2	Not Connected	
ddns3	Not Connected	
ddns4	Not Connected	
ddns5	Not Connected	
ddns6	Not Connected	
ddns7	Not Connected	
ddns8	Not Connected	
ddns9	Not Connected	
ddns10	Not Connected	

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.  10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
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.



Profile	Enable	WAN Profile	Routing P...	Service P...	Service T...	Domain N...	IP Source	Force upd...
ddns1	false	wan1		dyndns	Dynamic			14400
ddns2	false	wan1		dyndns	Dynamic			14400
ddns3	false	wan1		dyndns	Dynamic			14400
ddns4	false	wan1		dyndns	Dynamic			14400
ddns5	false	wan1		dyndns	Dynamic			14400
ddns6	false	wan1		dyndns	Dynamic			14400
ddns7	false	wan1		dyndns	Dynamic			14400
ddns8	false	wan1		dyndns	Dynamic			14400
ddns9	false	wan1		dyndns	Dynamic			14400
ddns10	false	wan1		dyndns	Dynamic			14400

Each item will be explained as follows:

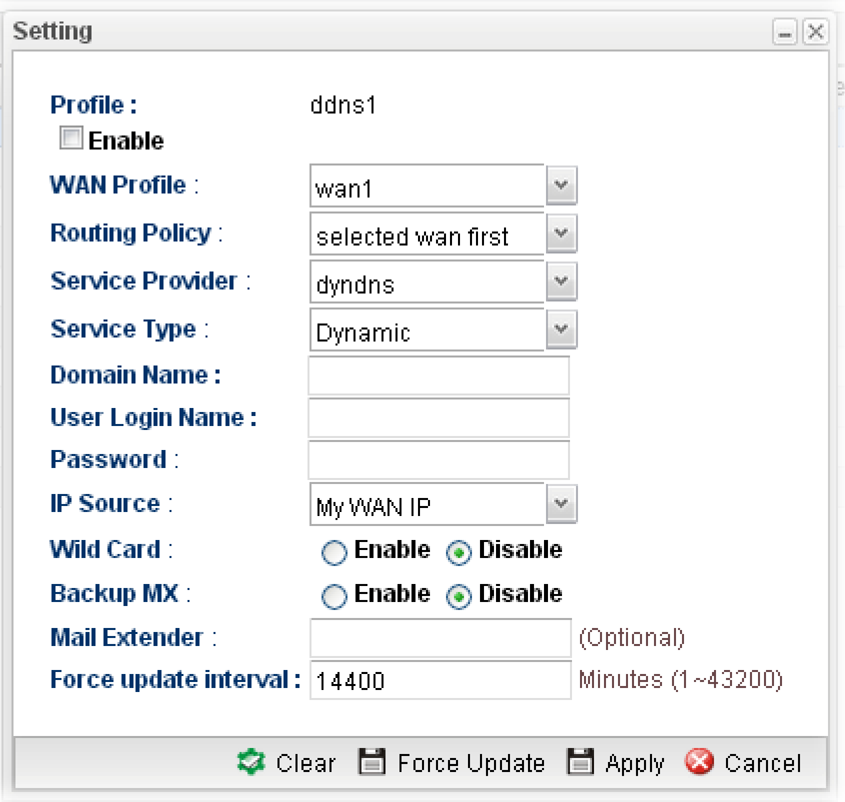
Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Force Update	Force the router updates its information to DDNS server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



Setting

Profile : ddns1

□ Enable

WAN Profile : wan1

Routing Policy : selected wan first

Service Provider : dyndns

Service Type : Dynamic

Domain Name :

User Login Name :

Password :

IP Source : My WAN IP

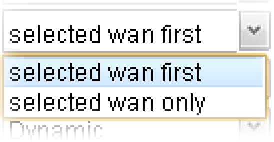
Wild Card : ○ Enable ● Disable

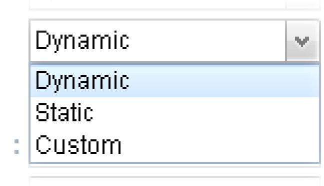
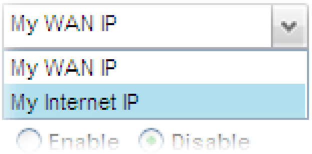
Backup MX : ○ Enable ● Disable

Mail Extender : (Optional)

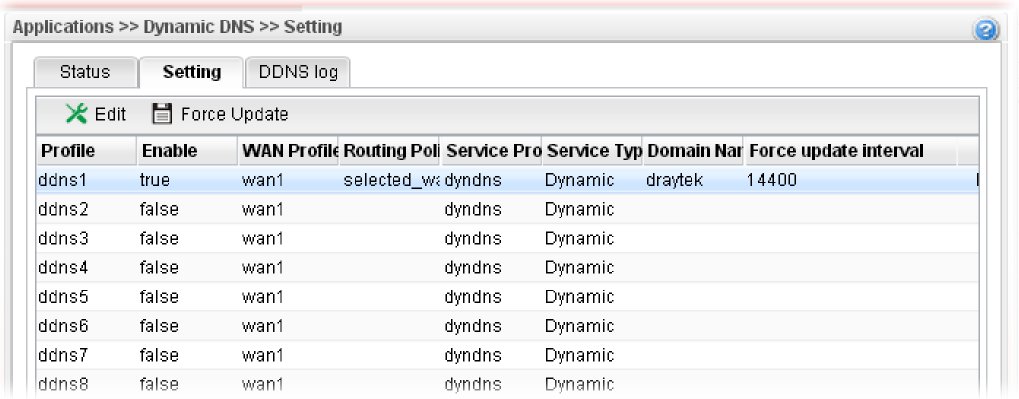
Force update interval : 14400 Minutes (1~43200)

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose a WAN interface that such profile will apply to.
Routing Policy	Choose a routing policy applied to the DDNS profile.  selected wan first selected wan first selected wan only **selected wan first** – The DDNS profile will be applied to the traffic via WAN interface first, then applied to other interface. **selected wan only** – The DDNS profile will be applied to the traffic via WAN interface only. No other interface will be used.
Service Provider	Select the service provider for the DDNS account.

Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. 
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
User Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
IP Source	Choose My WAN IP or My Internet IP as the source for the DDNS profile.  My WAN IP My WAN IP My Internet IP ○ Enable ● Disable
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.

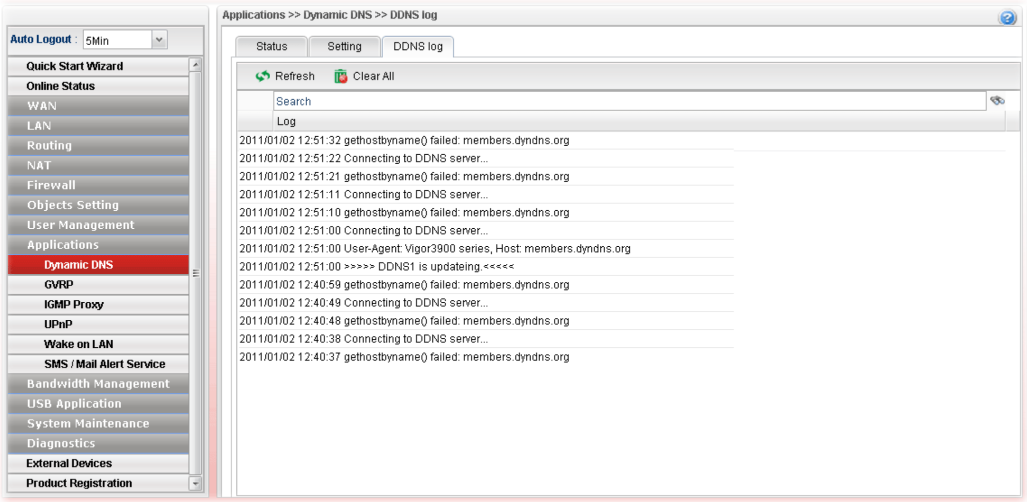


Applications >> Dynamic DNS >> Setting

Profile	Enable	WAN Profile	Routing Poli	Service Pro	Service Typ	Domain Nar	Force update interval
ddns1	true	wan1	selected_w:	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

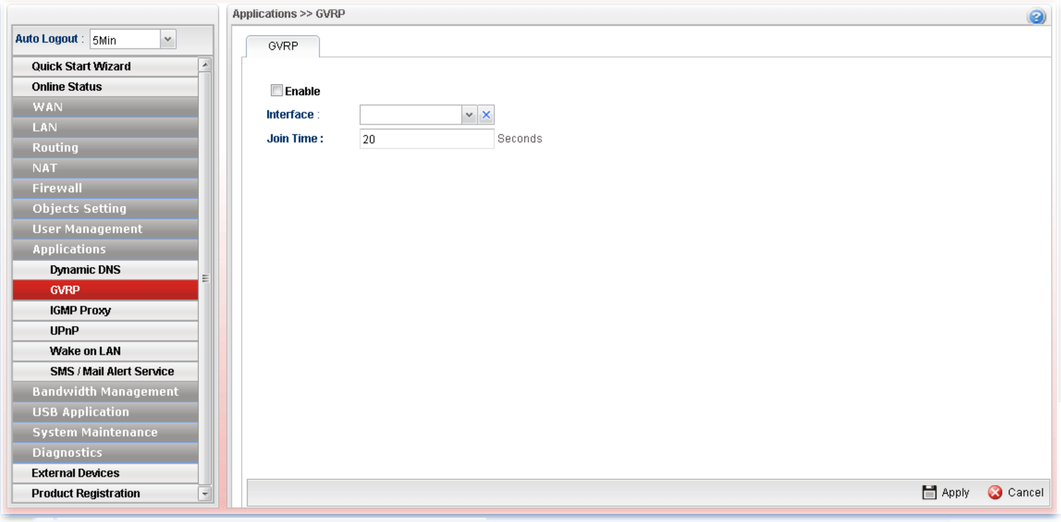
This page displays the information related to all DDNS.



```
2011/01/02 12:51:32 gethostbyname() failed: members.dyndns.org
2011/01/02 12:51:22 Connecting to DDNS server...
2011/01/02 12:51:21 gethostbyname() failed: members.dyndns.org
2011/01/02 12:51:11 Connecting to DDNS server...
2011/01/02 12:51:10 gethostbyname() failed: members.dyndns.org
2011/01/02 12:51:00 Connecting to DDNS server...
2011/01/02 12:51:00 User-Agent: Vigor3900 series, Host: members.dyndns.org
2011/01/02 12:51:00 >>>>> DDNS1 is updateing.<<<<<
2011/01/02 12:40:59 gethostbyname() failed: members.dyndns.org
2011/01/02 12:40:49 Connecting to DDNS server...
2011/01/02 12:40:48 gethostbyname() failed: members.dyndns.org
2011/01/02 12:40:38 Connecting to DDNS server...
2011/01/02 12:40:37 gethostbyname() failed: members.dyndns.org
```

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.



□ Enable

Interface :

Join Time : 20 Seconds

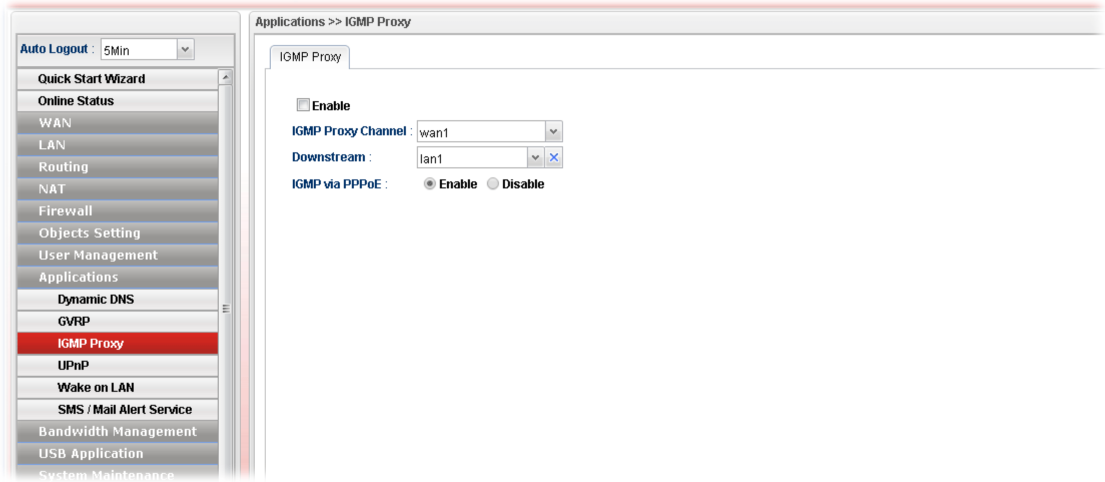
Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable GVRP function.
Interface	Choose LAN and/or WAN profiles. To clear the selected one, click ☒ to remove current object selections.
Join Time	Define the time for the system to send GVRP packet to other device. The unit is second.
Apply	Click it to save the configuration.

Item	Description
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.



Applications >> IGMP Proxy

IGMP Proxy

□ Enable

IGMP Proxy Channel : wan1

Downstream : lan1

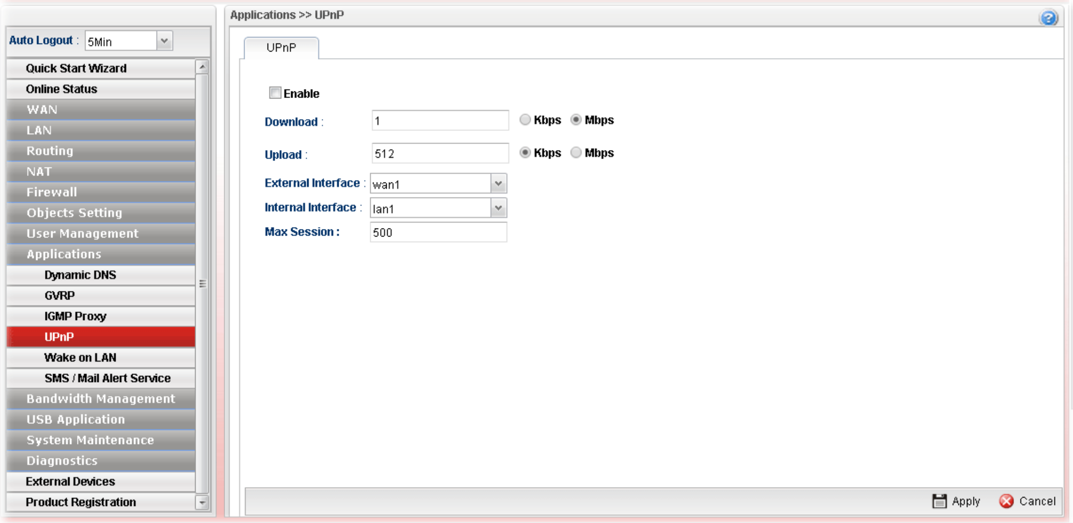
IGMP via PPPoE : ● Enable ○ Disable

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).
IGMP via PPPoE	**Enable** – In LAN, the PC which uses PPPoE connection to communicate with Vigor router can accept the packets transmitted from IGMP proxy. **Disable** –In LAN, the PC which uses PPPoE connection to communicate with Vigor router can NOT accept the packets transmitted from IGMP proxy. ● **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.



□ Enable

Download : 1 ○ Kbps ● Mbps

Upload : 512 ● Kbps ○ Mbps

External Interface : wan1

Internal Interface : lan1

Max Session : 500

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.

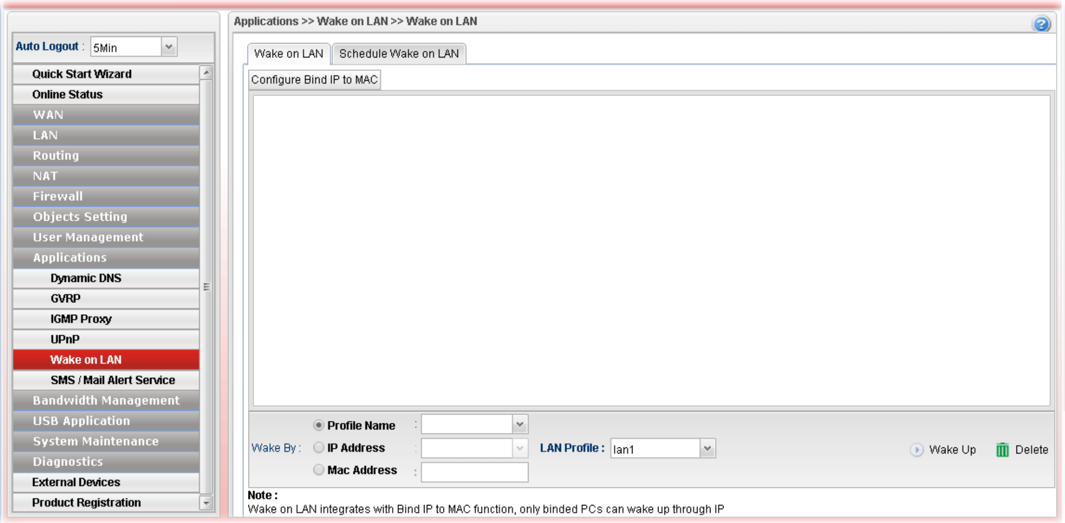
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.8.5 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.

4.8.5.1 Wake on LAN



Wake By : ● Profile Name : ○ IP Address : ○ Mac Address :

LAN Profile : lan1

Note :
Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP

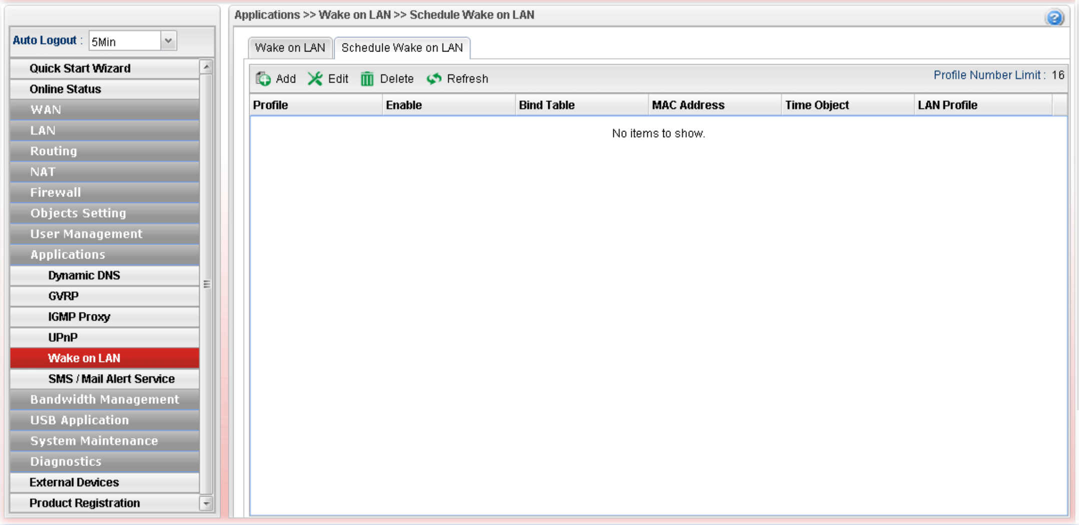
Available parameters are listed as follows:

Item	Description
Configure Bind IP to MAC	Click it to open the setting page of Bind IP to MAC.
Wake by	Three types provide for you to wake up the bound IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address. **Profile Name** – Choose a profile (created by **LAN>>Bind**

Item	Description
	IP to MAC) from the drop down list. **IP Address -** The IP addresses that have been configured in **Firewall>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up. **MAC Address -** Type any one of the MAC address of the bind PCs. **LAN Profile** – Use the drop down list to choose one of the LAN profiles.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.
Delete	Click this button to remove all the settings.

4.8.5.2 Schedule Wake on LAN

This page is used to set profiles which will perform WOL based on the conditions specified by Bind Table profile, MAC address, LAN profile and time profile.



Applications >> Wake on LAN >> Schedule Wake on LAN

Auto Logout : 5Min

Profile Number Limit : 16

Profile	Enable	Bind Table	MAC Address	Time Object	LAN Profile

No items to show.

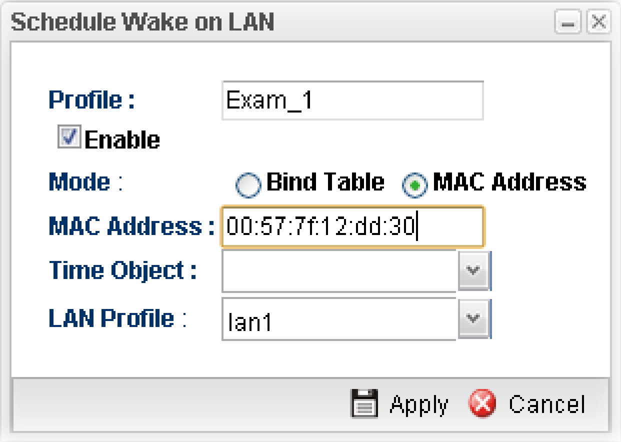
Available parameters are listed as follows:

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.


Schedule Wake on LAN

Profile : Exam_1

☑ Enable

Mode : ○ Bind Table ● MAC Address

MAC Address : 00:57:7f:12:dd:30

Time Object :

LAN Profile : lan1

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**.

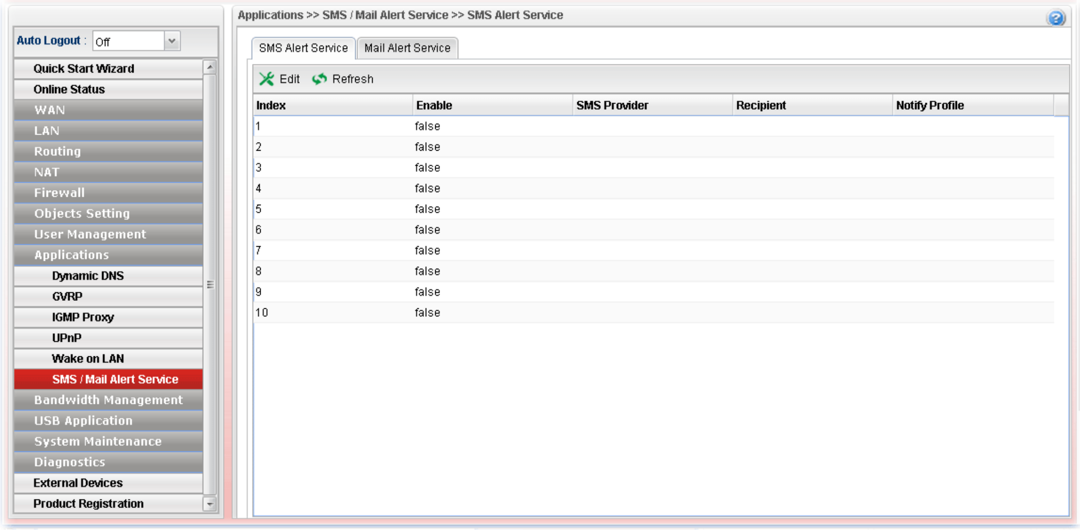
4.8.6 SMS / Mail Alert Service

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.

4.8.6.1 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.



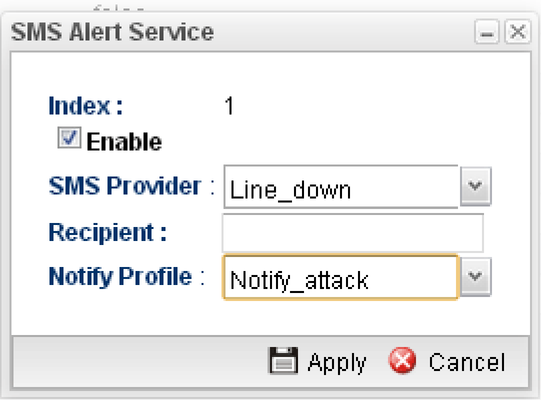
Index	Enable	SMS Provider	Recipient	Notify Profile
1	false			
2	false			
3	false			
4	false			
5	false			
6	false			
7	false			
8	false			
9	false			
10	false			

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.



Index : 1

☑ Enable

SMS Provider : Line_down

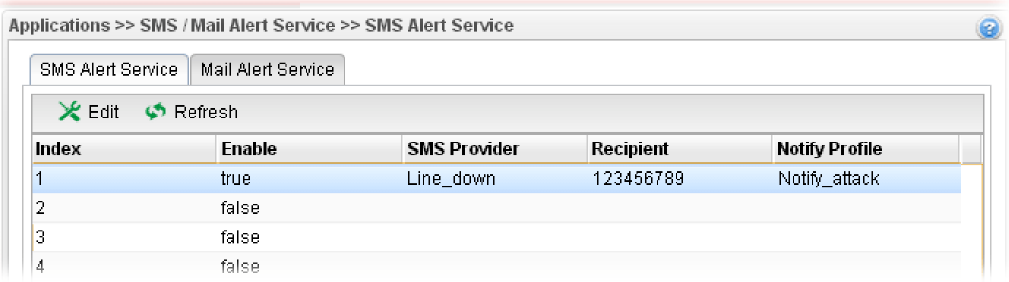
Recipient :

Notify Profile : Notify_attack

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.

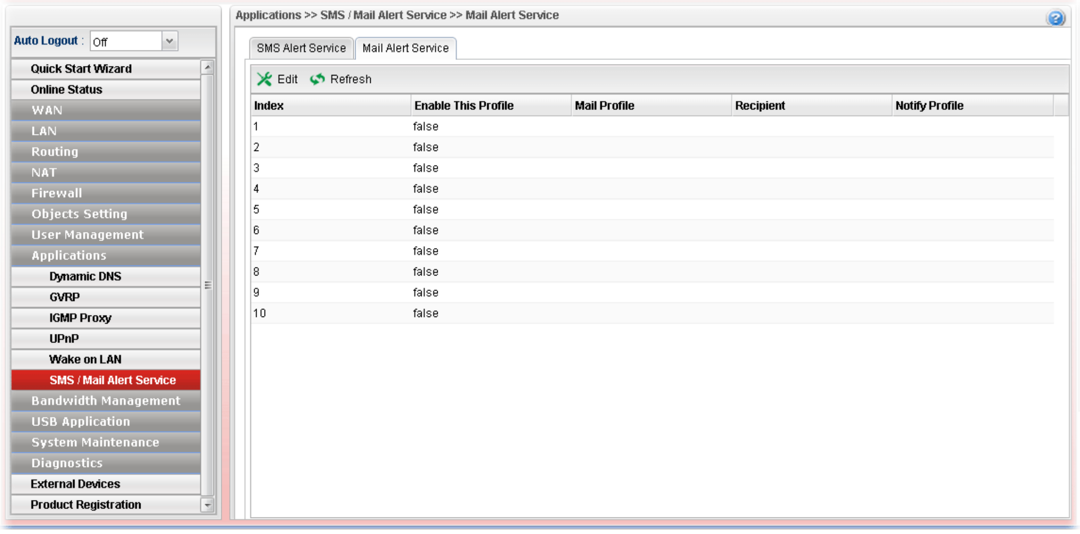
4. Enter all the settings and click **Apply**.
5. The SMS alert service profile has been modified.


Applications >> SMS / Mail Alert Service >> SMS Alert Service
SMS Alert Service
Mail Alert Service
Edit
Refresh

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

4.8.6.2 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.



Applications >> SMS / Mail Alert Service >> Mail Alert Service

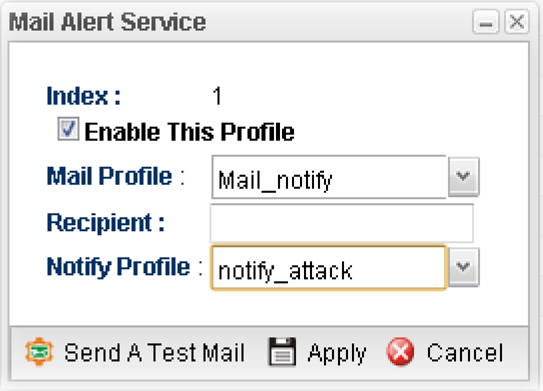
Index	Enable This Profile	Mail Profile	Recipient	Notify Profile
1	false			
2	false			
3	false			
4	false			
5	false			
6	false			
7	false			
8	false			
9	false			
10	false			

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.



Mail Alert Service

Index : 1

☑ Enable This Profile

Mail Profile : Mail_notify

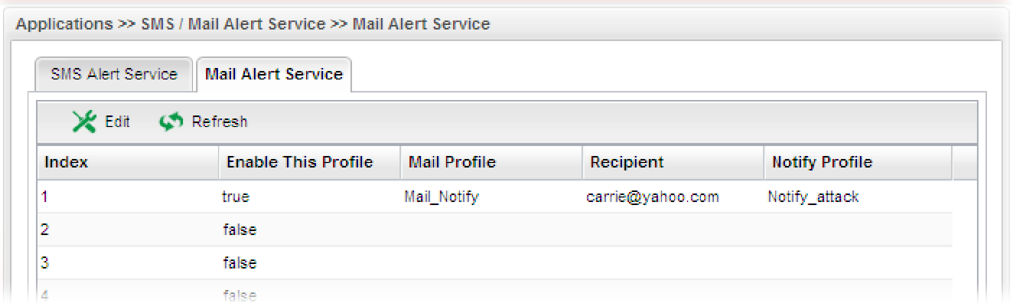
Recipient :

Notify Profile : notify_attack

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.

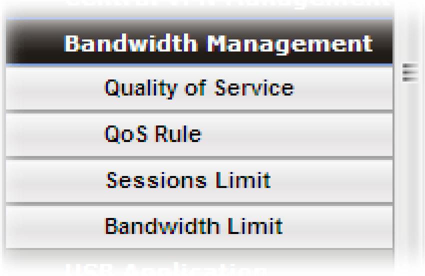


Applications >> SMS / Mail Alert Service >> Mail Alert Service

Index	Enable This Profile	Mail Profile	Recipient	Notify Profile
1	true	Mail_Notify	carrie@yahoo.com	Notify_attack
2	false			
3	false			
4	false			

4.9 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.

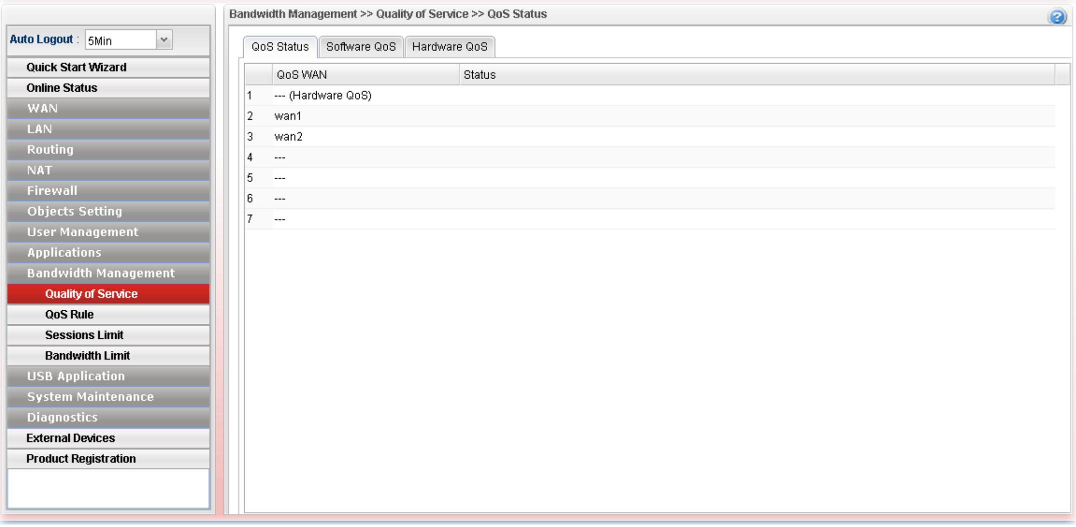
Differentiated quality of service is therefore one of the most important issues over the Internet infrastructure. In Vigor router, DSCP (Differentiated Service Code Point) support is also taken into consideration in the design of the QoS-guaranteed control module.

4.9.1 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.

4.9.1.1 QoS Status

This page displays current QoS Status.

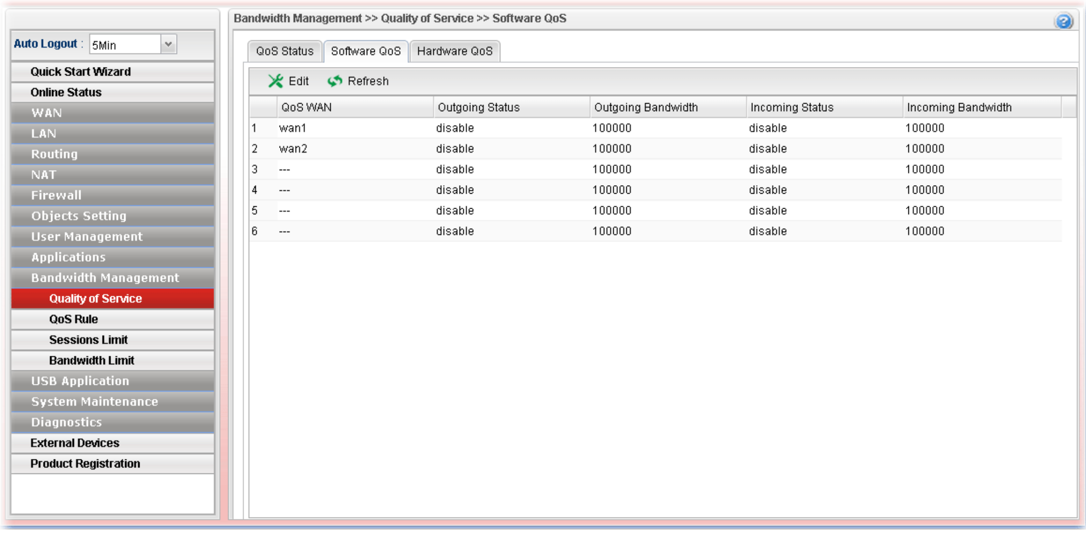


Bandwidth Management >> Quality of Service >> QoS Status

	QoS WAN	Status
1	--- (Hardware QoS)	
2	wan1	
3	wan2	
4	---	
5	---	
6	---	
7	---	

4.9.1.2 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.



Bandwidth Management >> Quality of Service >> Software QoS

	QoS WAN	Outgoing Status	Outgoing Bandwidth	Incoming Status	Incoming Bandwidth
1	wan1	disable	100000	disable	100000
2	wan2	disable	100000	disable	100000
3	---	disable	100000	disable	100000
4	---	disable	100000	disable	100000
5	---	disable	100000	disable	100000
6	---	disable	100000	disable	100000

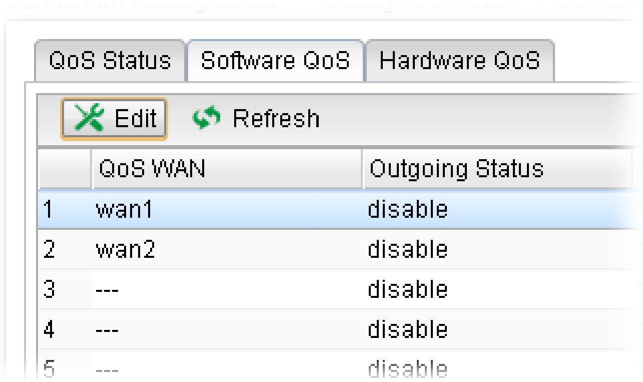
Available parameters are listed as follows:

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

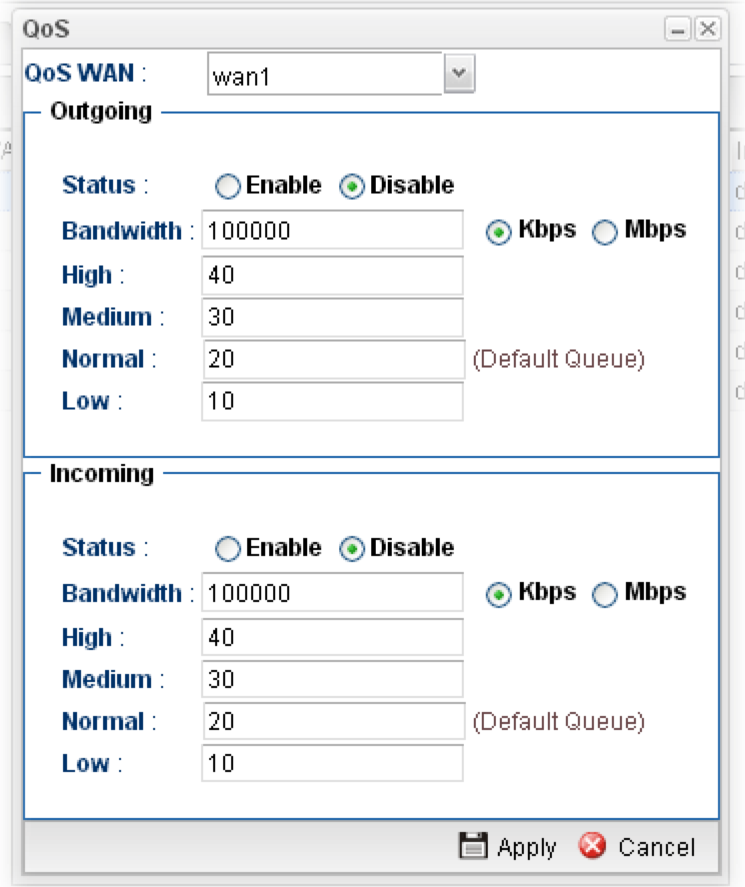
Follow the steps below to create a new maintenance profile.

1. Click one of the QoS WAN profiles to select the one you want to edit.
2. Click **Edit**.



	QoS WAN	Outgoing Status
1	wan1	disable
2	wan2	disable
3	---	disable
4	---	disable
5	---	disable

3. The QoS settings page appears.



QoS WAN : wan1

Outgoing

Status : ○ Enable ● Disable

Bandwidth : 100000 ● Kbps ○ Mbps

High : 40

Medium : 30

Normal : 20 (Default Queue)

Low : 10

Incoming

Status : ○ Enable ● Disable

Bandwidth : 100000 ● Kbps ○ Mbps

High : 40

Medium : 30

Normal : 20 (Default Queue)

Low : 10

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.

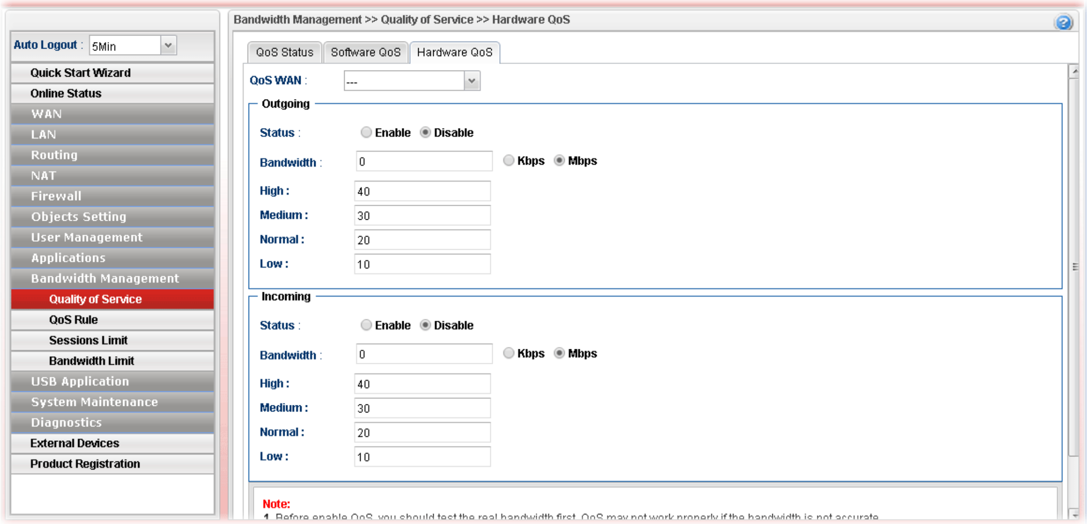
High/Medium/ Normal/Low	There are several available outgoing queues. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save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

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

4.9.1.3 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.



Bandwidth Management >> Quality of Service >> Hardware QoS

QoS WAN : ---

Outgoing

Status : ○ Enable ● Disable

Bandwidth : 0 ○ Kbps ● Mbps

High : 40

Medium : 30

Normal : 20

Low : 10

Incoming

Status : ○ Enable ● Disable

Bandwidth : 0 ○ Kbps ● Mbps

High : 40

Medium : 30

Normal : 20

Low : 10

Note:

1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.

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 data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all

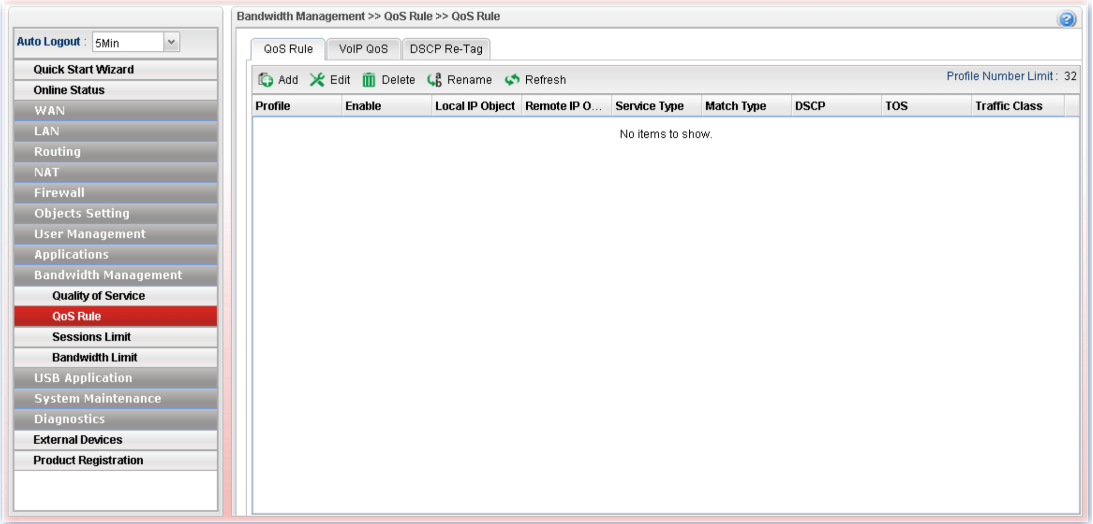
	queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.9.2 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



Bandwidth Management >> QoS Rule >> QoS Rule

Profile Number Limit : 32

Profile	Enable	Local IP Object	Remote IP O...	Service Type	Match Type	DSCP	TOS	Traffic Class

No items to show.

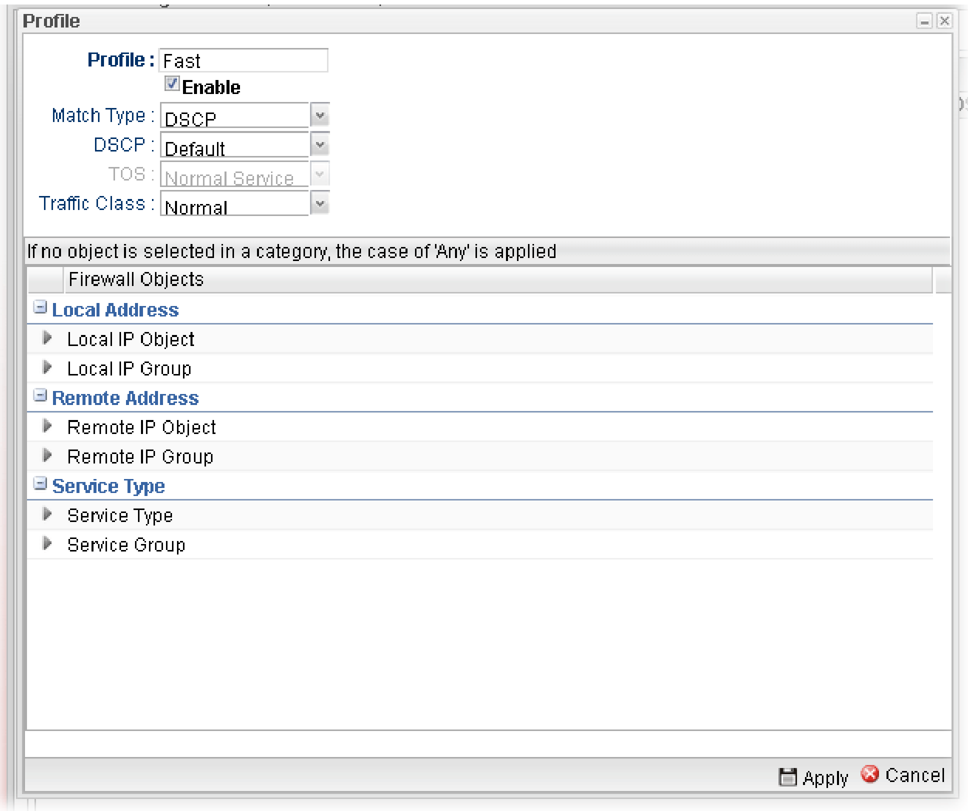
Available parameters are listed as follows:

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 Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile for the filter.
Enable	Display the status of the profile. False means disabled; True means enabled.
Local IP Object	Display the source IP address for the filter.

Remote IP Object	Display the destination IP address for the filter.
Service Type	Display the service type (e.g., IKE, HTTP, AUTH and etc) for the filter.
Match Type	Display the match type (e.g., TOS or DSCP) for the filter.
DSCP	Display the setting of DSCP.
TOS	Display the setting of TOS.
Traffic Class	Display the queue number that such filter is categorized.

How to add a QoS rule profile

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



Profile : Fast

☑ Enable

Match Type : DSCP

DSCP : Default

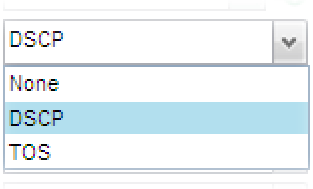
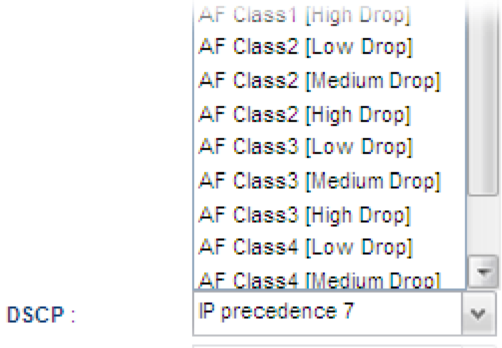
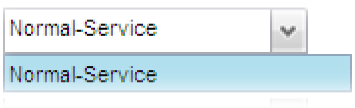
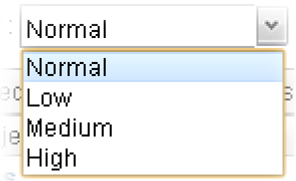
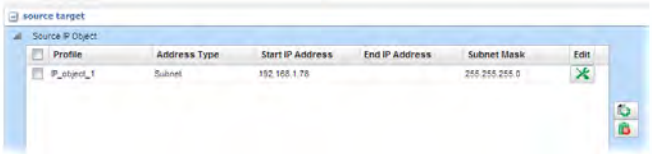
TOS : Normal Service

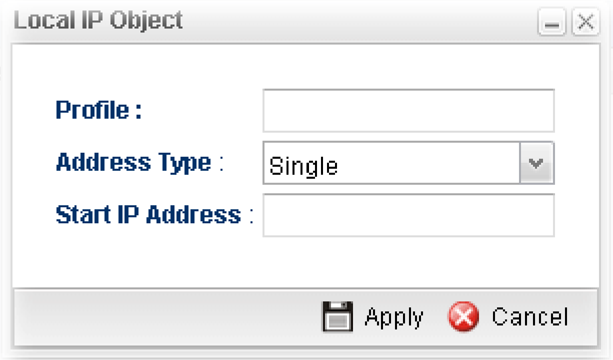
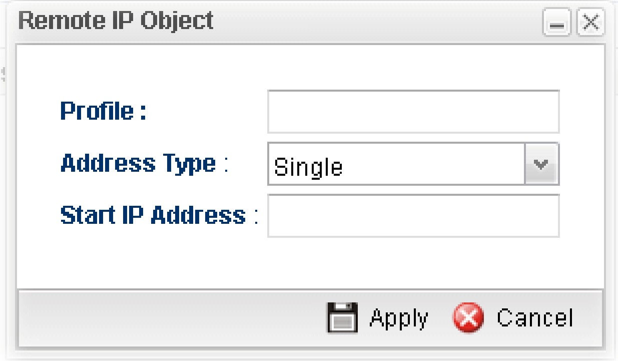
Traffic Class : Normal

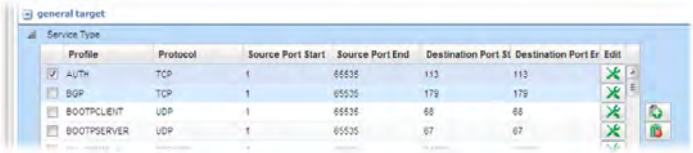
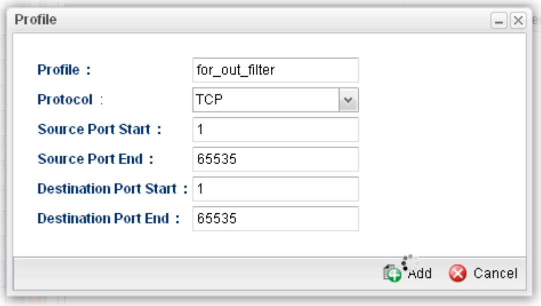
If no object is selected in a category, the case of 'Any' is applied

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the filter profile.
Enable	Check this box to enable such profile.
Match Type	Use the drop down list to specify a suitable match type.

	
DSCP	It is available when DSCP is selected as the Match type.  AF Class1 [High Drop] AF Class2 [Low Drop] AF Class2 [Medium Drop] AF Class2 [High Drop] AF Class3 [Low Drop] AF Class3 [Medium Drop] AF Class3 [High Drop] AF Class4 [Low Drop] AF Class4 [Medium Drop] DSCP : IP precedence 7
TOS	It is available when TOS is selected as the Match type. 
Traffic Class	Choose the traffic class to category the packets matching with the condition configured as above. High is the highest; Normal is the lowest. 
Local Address	Click ▶ on the left side of the **Source IP Object/Source IP Group** profile. Check the object profile(s) as the source target.  source target Source IP Object Profile Address Type Start IP Address End IP Address Subnet Mask Edit IP_object_1 Subnet 192.168.1.78 255.255.255.0 **Local IP Object –** Use the drop down list to choose one of the IP objects for such rule profile. **Local IP Group –** Use the drop down list to choose one of the IP group for such rule profile. If you want to create a new IP object, simply click ⊕ to open the following dialog.

	 Local IP Object Profile : Address Type : Single Start IP Address : Apply Cancel ● **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.  Remote IP Object Profile : Address Type : Single Start IP Address : Apply Cancel ● **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.

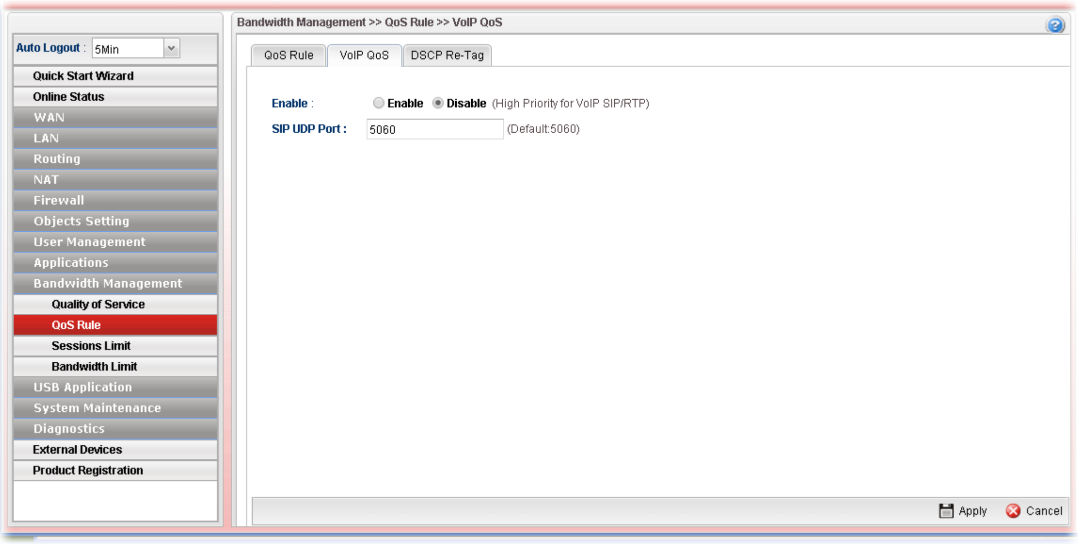
<table>
<tr><td></td><td>- <b>End IP Address -</b> Type the IP address of the ending point for such profile if you choose <b>Range</b> as <b>Address Type</b>.
- <b>Subnet Mask</b> – Choose the subnet mask from the drop down list if you choose <b>Subnet</b> as <b>Address Type</b>.</td></tr>
<tr><td><b>Service Type</b></td><td><b>Service Type -</b> Choose one of the service types from the drop down list.

general target
Service Type
<table><tr><th></th><th>Profile</th><th>Protocol</th><th>Source Port Start</th><th>Source Port End</th><th>Destination Port St</th><th>Destination Port Er</th><th>Edit</th></tr><tr><td>☑</td><td>AUTH</td><td>TCP</td><td>1</td><td>65535</td><td>113</td><td>113</td><td></td></tr><tr><td>□</td><td>BGP</td><td>TCP</td><td>1</td><td>65535</td><td>179</td><td>179</td><td></td></tr><tr><td>□</td><td>BOOTPCLIENT</td><td>UDP</td><td>1</td><td>65535</td><td>68</td><td>68</td><td></td></tr><tr><td>□</td><td>BOOTPSERVER</td><td>UDP</td><td>1</td><td>65535</td><td>67</td><td>67</td><td></td></tr></table>
If you want to create a new service type, simply click to open the following dialog.

Profile
Profile : for_out_filter
Protocol : TCP
Source Port Start : 1
Source Port End : 65535
Destination Port Start : 1
Destination Port End : 65535

- <b>Profile</b> – type a new name for such service type.
- <b>Protocol</b> –There are two options: <b>TCP</b>, <b>UDP</b> and <b>TCP/UDP</b>. Select the protocol that you want to use.
- <b>Source Port Start /End -</b> Type the start /end number for the port range of the source port for such filter.
- <b>Destination Port Start / End -</b> Type the start /end number for the port range of the destination port for such filter.</td></tr>
<tr><td><b>Apply</b></td><td>Click it to save the configuration and exit the page.</td></tr>
<tr><td><b>Cancel</b></td><td>Click it to exit the page without saving the configuration.</td></tr>
</table>

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

4.9.2.2 VoIP QoS

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



Bandwidth Management >> QoS Rule >> VoIP QoS

Enable : ○ Enable ● Disable (High Priority for VoIP SIP/RTP)

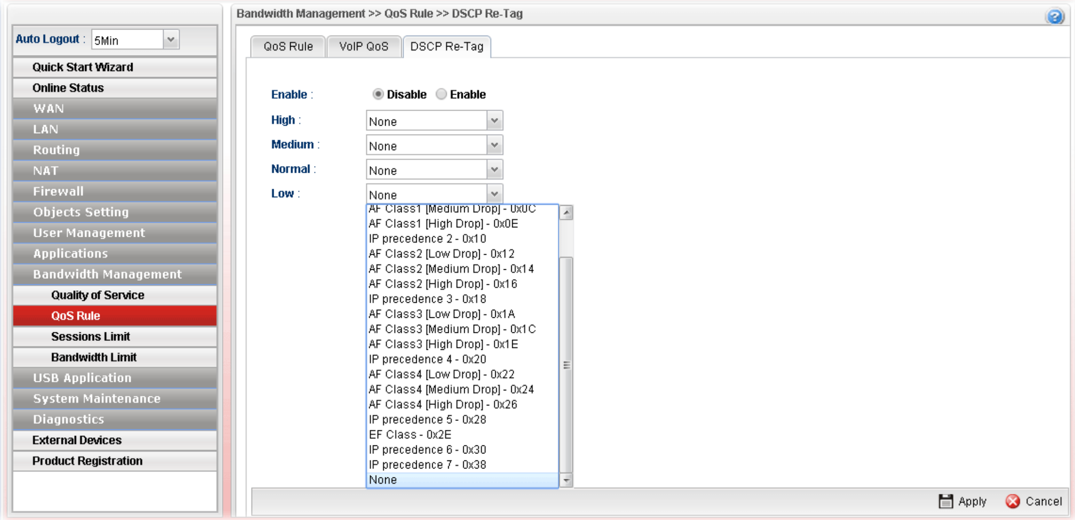
SIP UDP Port : 5060 (Default:5060)

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.

4.9.2.3 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.



Bandwidth Management >> QoS Rule >> DSCP Re-Tag

Enable : ● Disable ○ Enable

High : None

Medium : None

Normal : None

Low : None

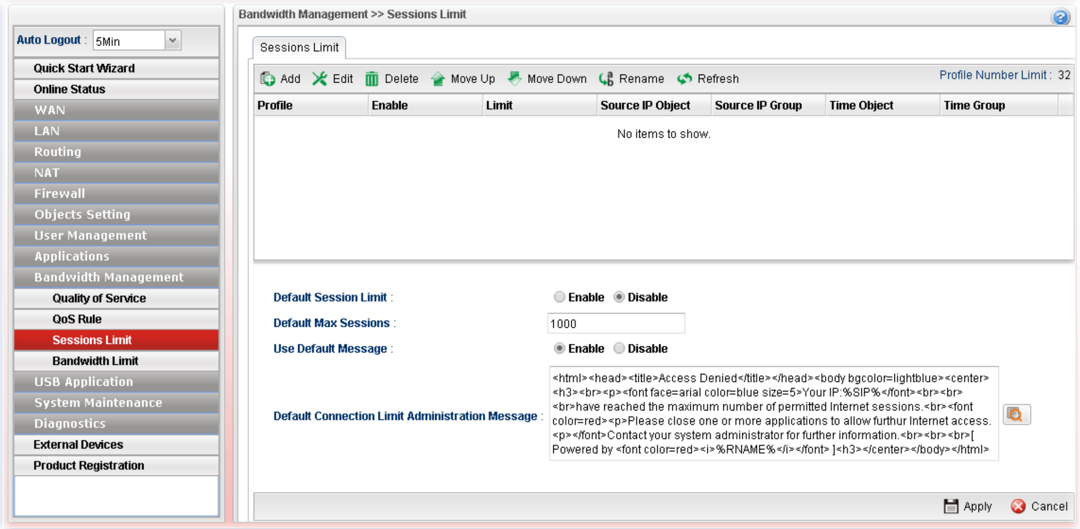
Each item will be explained as follows:

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.

4.9.3 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.



Profile Number Limit : 32

Profile	Enable	Limit	Source IP Object	Source IP Group	Time Object	Time Group

No items to show.

Default Session Limit : ○ Enable ● Disable

Default Max Sessions : 1000

Use Default Message : ● Enable ○ Disable

Default Connection Limit Administration Message :

```
<html><head><title>Access Denied</title></head><body bgcolor=lightblue><center>
<h3><br><p><font face=arial color=blue size=5>Your IP:%SIP%</font><br><br>
<br>have reached the maximum number of permitted Internet sessions.<br><font
color=red><p>Please close one or more applications to allow furthur Internet access.
<p></font>Contact your system administrator for further information.<br><br><br>[
Powered by <font color=red><i>%RNAME%</i></font> ]<h3></center></body></html>
```

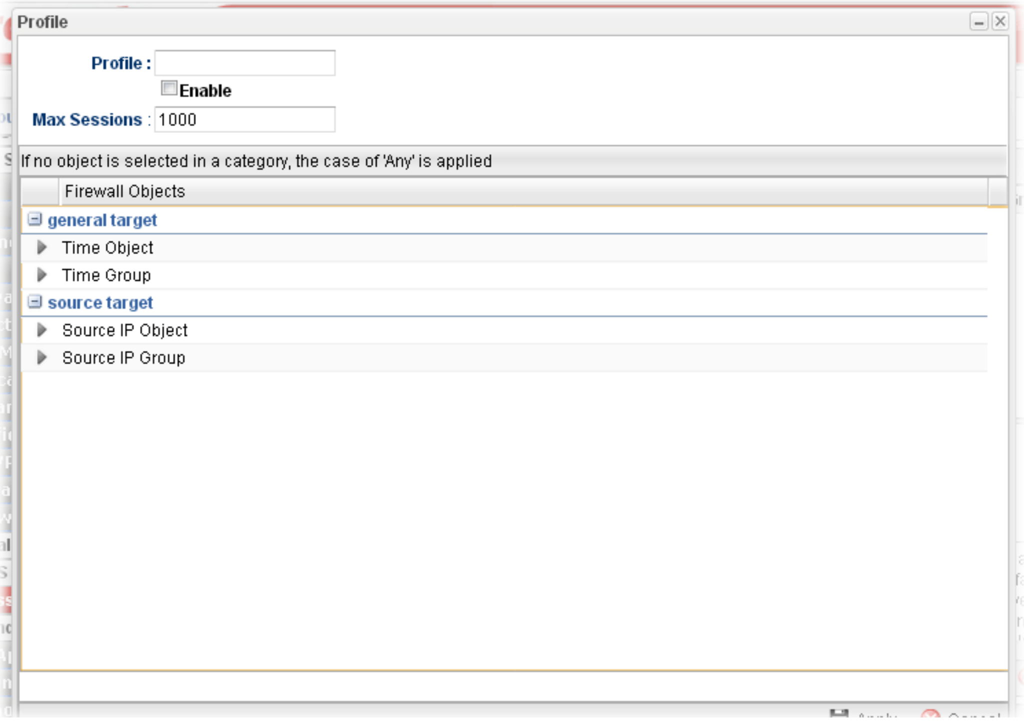
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Limit	Display the maximum session number allowed for the profile.
Source IP Object	Display the source IP object profile name.

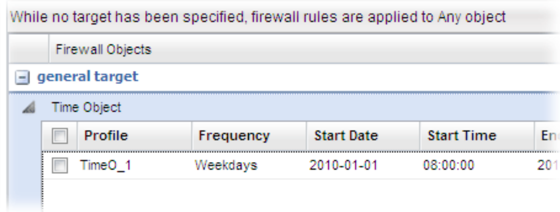
Source IP Group	Display the source IP group profile name.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application profile.
Default Session Limit	Display the default session number used for each computer in LAN.
Default Max Sessions	Display the default maximum session number used for each computer in LAN.
Use Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page.. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Connection Limit Administration Message	Such field is available when you disable the function of **Use Default Message**. The message will display on the user's browser when he/she tries to access the blocked web page.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to add a session limit profile

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

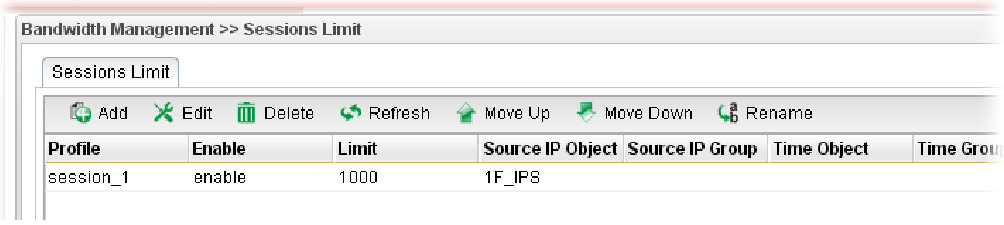


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
Max Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index. This field cannot be typed with “0”, otherwise the profile cannot be saved.
general target	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile.  While no target has been specified, firewall rules are applied to Any object Firewall Objects ⊟ general target Time Object □ Profile | Frequency | Start Date | Start Time | En □ TimeO_1 | Weekdays | 2010-01-01 | 08:00:00 | 201 **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
source target	**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. **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.
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.



Bandwidth Management >> Sessions Limit

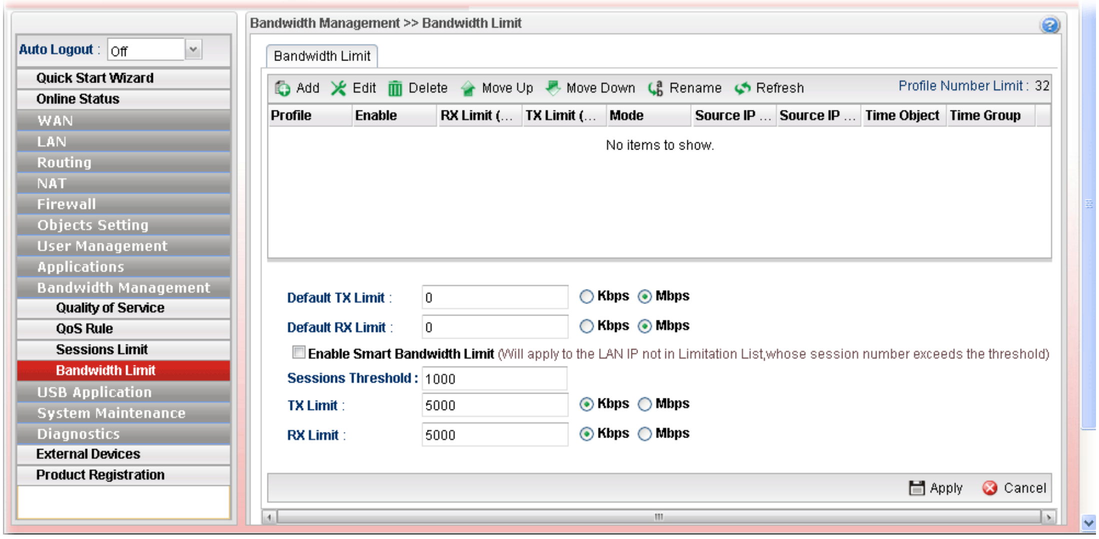
Sessions Limit

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

4.9.4 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.



Profile Number Limit : 32

Profile	Enable	RX Limit (...	TX Limit (...	Mode	Source IP ...	Source IP ...	Time Object	Time Group

No items to show.

Default TX Limit : 0 ○ Kbps ● Mbps

Default RX Limit : 0 ○ Kbps ● Mbps

□ Enable Smart Bandwidth Limit (Will apply to the LAN IP not in Limitation List,whose session number exceeds the threshold)

Sessions Threshold : 1000

TX Limit : 5000 ● Kbps ○ Mbps

RX Limit : 5000 ● Kbps ○ Mbps

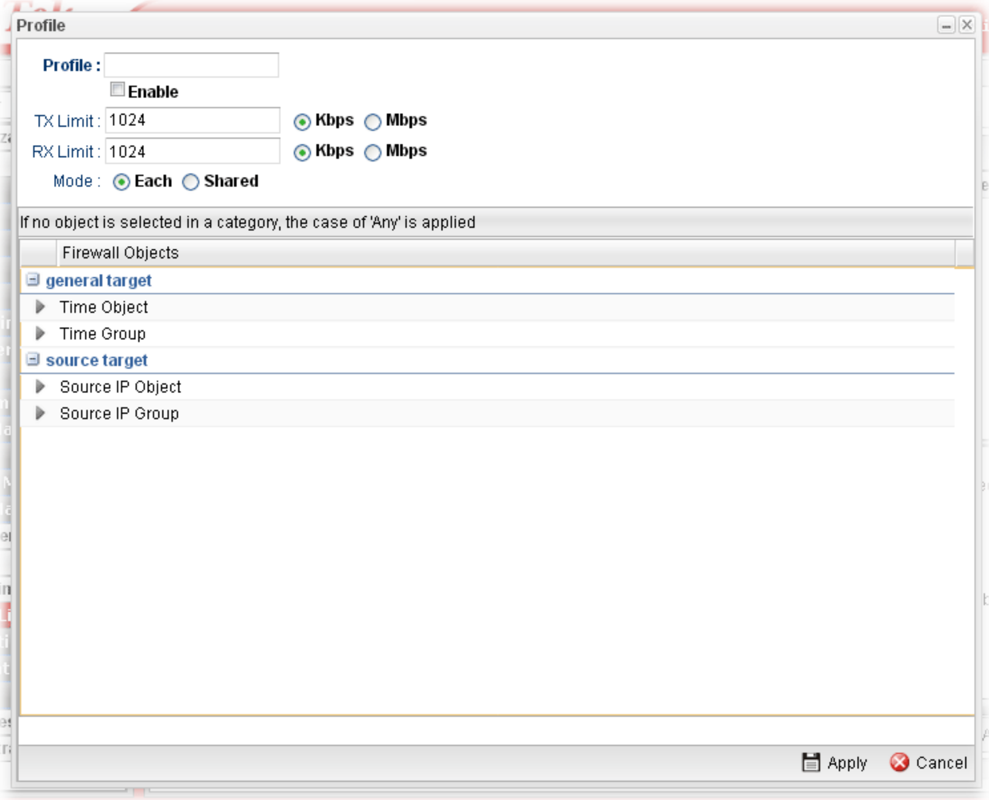
Each item will be explained as follows:

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.
Default TX/RX Limit	The default limit will apply to LAN IP(s) not in the above configuration profiles **Default TX Limit** – Define the limitation for the speed of the upstream. **Default RX Limit** –Define the limitation for the speed of the downstream.
Enable Smart Bandwidth Limit	Check this radio button to configure the default limitation for bandwidth for any LAN IP not included in the Limitation List.
Session Threshold	When session number exceeds the set threshold, Smart Bandwidth limit will work.
TX Limit	Define the speed of the upstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission.
RX Limit	Define the speed of the downstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to add a bandwidth limit profile

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



Profile

Profile :

□ Enable

TX Limit : 1024 ● Kbps ○ Mbps

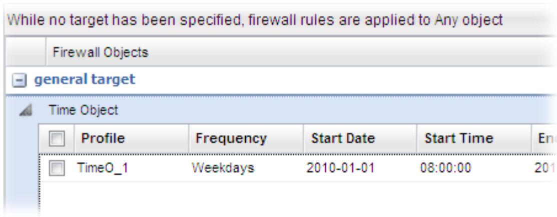
RX Limit : 1024 ● Kbps ○ Mbps

Mode : ● Each ○ Shared

If no object is selected in a category, the case of 'Any' is applied

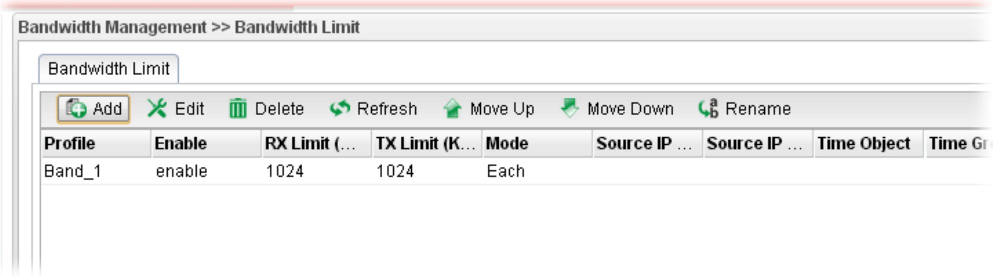
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
TX Limit(Kbps)	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
RX Limit(Kbps)	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
Mode	Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.

general target	**Time Object** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile.  While no target has been specified, firewall rules are applied to Any object Firewall Objects general target Time Object Profile | Frequency | Start Date | Start Time | En TimeO_1 | Weekdays | 2010-01-01 | 08:00:00 | 201 **Time Group** - Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
source target	**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. **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.
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.



Bandwidth Management >> Bandwidth Limit

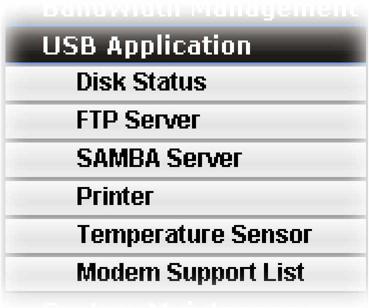
Bandwidth Limit

Profile	Enable	RX Limit (...	TX Limit (K...	Mode	Source IP ...	Source IP ...	Time Object	Time Gr
Band_1	enable	1024	1024	Each				

4.10 USB Application

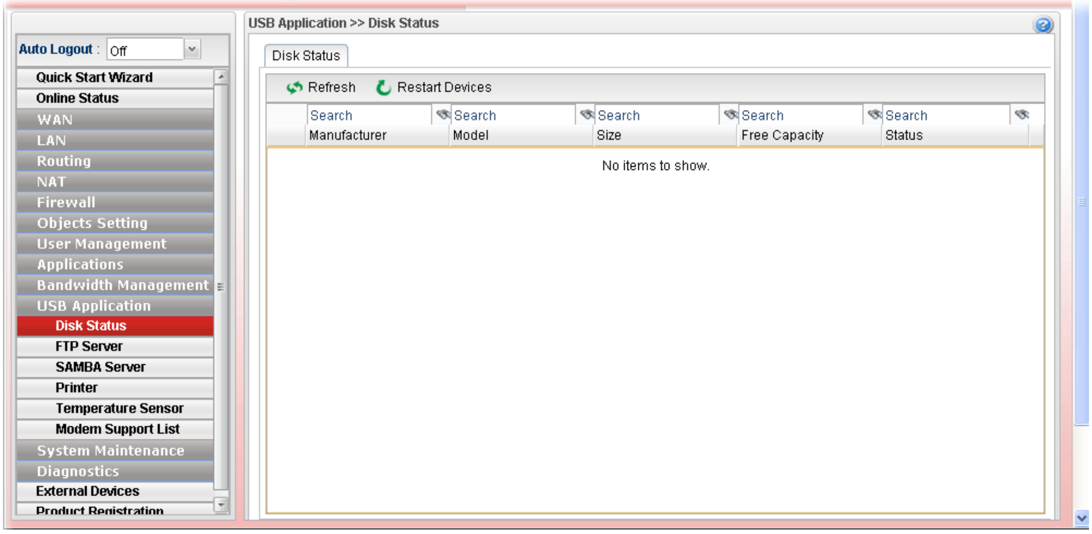
By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **User Management>>User Profile** on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



4.10.1 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.



No items to show.

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.

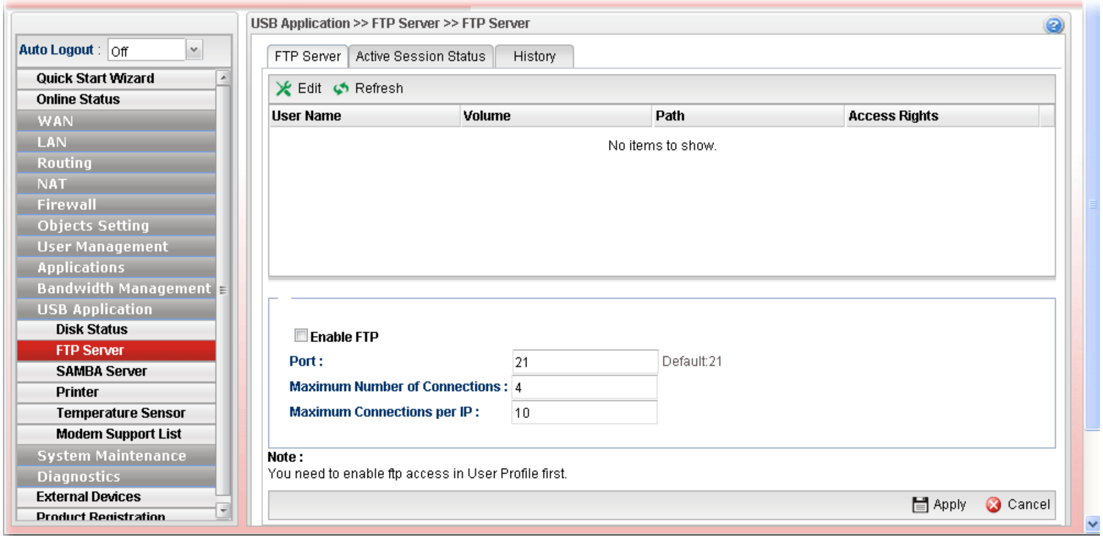
Size	Display the total disk capacity of the USB device.
Free Capacity	Display the remaining disk space of the USB device.
Status	Display the status of the USB device.
(Remove Icon)	At present, FAT, EXT2, EXT3 USB format can be supported by Vigor router. If such USB is inserted into the USB slot, the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

4.10.2 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.



User Name	Volume	Path	Access Rights

No items to show.

□ Enable FTP

Port : 21 Default:21

Maximum Number of Connections : 4

Maximum Connections per IP : 10

Note :
You need to enable ftp access in User Profile first.

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.

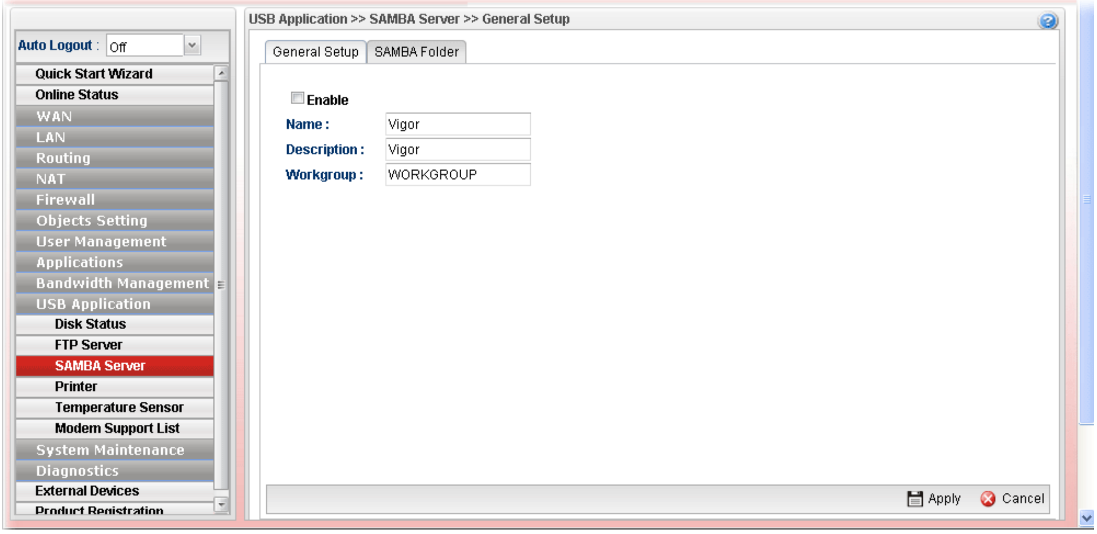
Access Rights	It displays the access right for the connected USB disk.
Enable FTP	Check the box to enable FTP server.
Port	Type required port number for FTP server. Or, use the default value.
Maximum Number of Connections	It means the maximum session limit for the FTP server. The default setting is “4” 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”.
Apply	Click it to save the configuration.
Cancel	Click it to clear current configuration.

4.10.3 SAMBA Server

SAMBA server offers the file sharing service for users through a specified file folder. Any user who wants to access into the USB storage disk must type the same name and use the same workgroup. Before adding or modifying settings in this page, please insert a USB storage disk first.

4.10.3.1 General Setup

This page allows you to configure settings for SAMBA server.



□ Enable

Name : Vigor

Description : Vigor

Workgroup : WORKGROUP

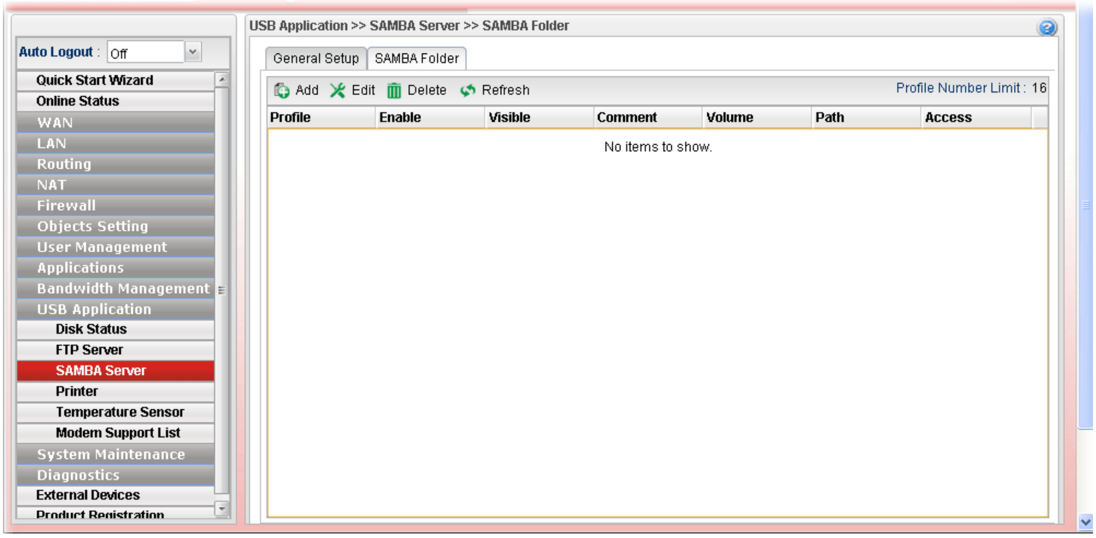
Available settings are explained as follows:

Item	Description
Enable	Check the box to enable SAMBA server.
Name	Type the NetBios name of the SAMBA Server.
Description	Type any text to describe SMABA server.
Workgroup	Type the name of the workgroup for the SAMBA server

	to be located by Windows system. Default name will be offered for Windows XP user.

4.10.3.2 SAMBA Folder

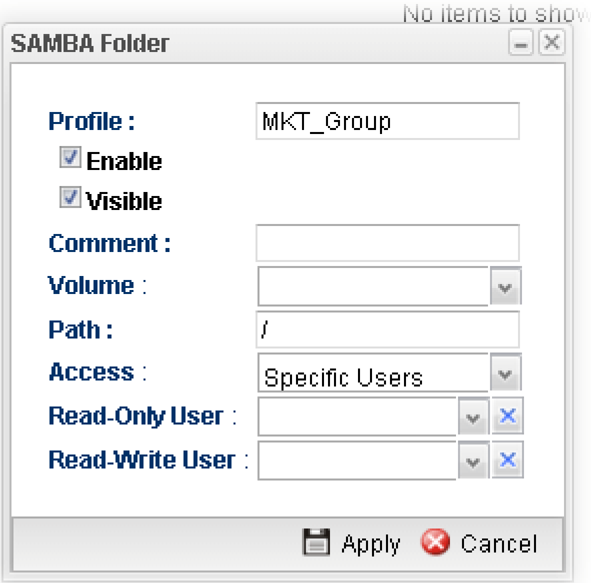
Due to the file sharing feature of SAMBA server, this page allows you to create any profile which can be shared by clients on the network.



No items to show.

How to add/edit a SMABA folder profile

1. Open **USB Application>>SMABA Server** and click **SAMBA Folder** tab.
2. Click the **Add** button. For an existed profile, simply choose that profile and click the **Edit** button.
3. The following dialog will appear.



Profile : MKT_Group

☑ Enable

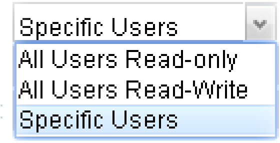
☑ Visible

Path : /

Access : Specific Users

Available parameters are listed as follows:

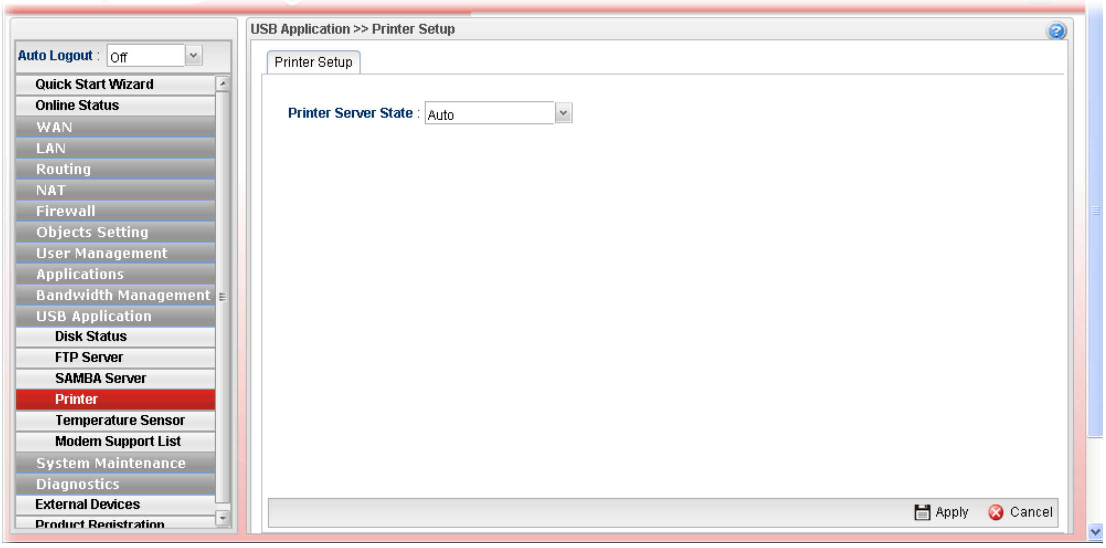
Item	Description
Profile	Type the name of the profile to be shared.

Enable	Check this box to enable such profile.
Visible	Check this box to make such profile be seen by users. If not, the user must know and type the path of the folder name to access into that folder.
Comment	Type any text to describe such profile if required.
Volume	Use the drop down list to specify the proper volume for the connected USB disk.
Path	It indicates the directory name for the connected USB disk. The default setting is "/".
Access	There are three options for you to specify.  Specific Users All Users Read-only All Users Read-Write Specific Users **All Users Read-only** – Such option allows all of the users sharing the SAMBA service to read the file stored under the sharing folder. **All Users Read-Write** – Such option allows all of the users sharing the SAMBA service to read and write the file stored under the sharing folder. If **Specific Users** is selected, you have to additionally specify Read-Only User and Read-Write User. ● **Read-Only User** – User profiles (with **Allow SAMBA Server Login** Enabled) created under **User Management>>User Profile** will be displayed here. Choose the one to have the right to read the file on SAMBA folder. ● **Read-Write User -** User profiles (with **Allow SAMBA Server Login** Enabled) created under **User Management>>User Profile** will be displayed here. Choose the one to have the right to read and write the file on SAMBA folder.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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

4.10.4 Printer

This page is used to enable the printer server state when a printer device is connected via USB port.



Printer Server State : Auto

Available settings are explained as follows:

Item	Description
Printer Server State	**Auto-** It's the default setting. Vigor router will detect if the connected device is printer or not. If yes, the printer server will be enabled automatically to activate the printer. **Enable** – The printer server will be enabled. **Disable** – The printer server will be disabled.
Apply	Click it to save the configuration.
Cancel	Click it to return to factory default setting.

4.10.5 Temperature Sensor

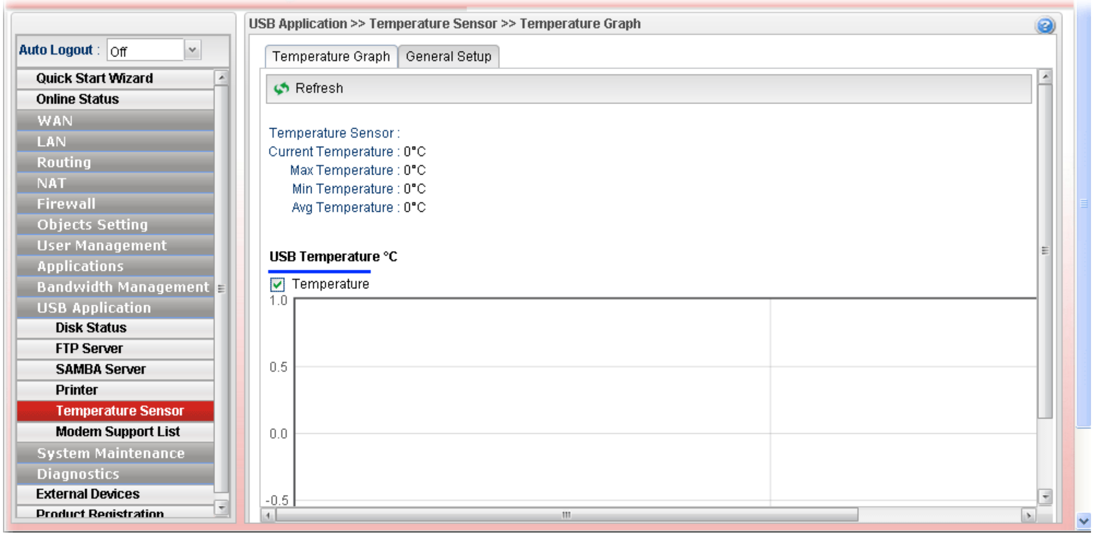
A USB Thermometer is now available that complements your installed DrayTek router installations that will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

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

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

4.10.5.1 Temperature Graph

Below shows an example of temperature graph:



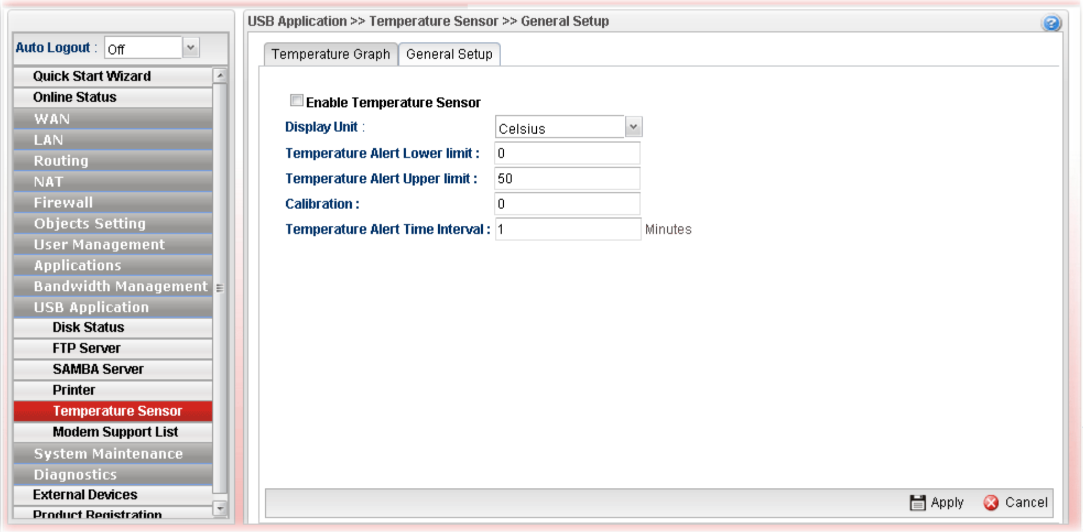
USB Application >> Temperature Sensor >> Temperature Graph

Temperature Sensor :
Current Temperature : 0°C
Max Temperature : 0°C
Min Temperature : 0°C
Avg Temperature : 0°C

USB Temperature °C

☑ Temperature

4.10.5.2 General Setup



USB Application >> Temperature Sensor >> General Setup

□ Enable Temperature Sensor

Display Unit : Celsius

Temperature Alert Lower limit : 0

Temperature Alert Upper limit : 50

Calibration : 0

Temperature Alert Time Interval : 1 Minutes

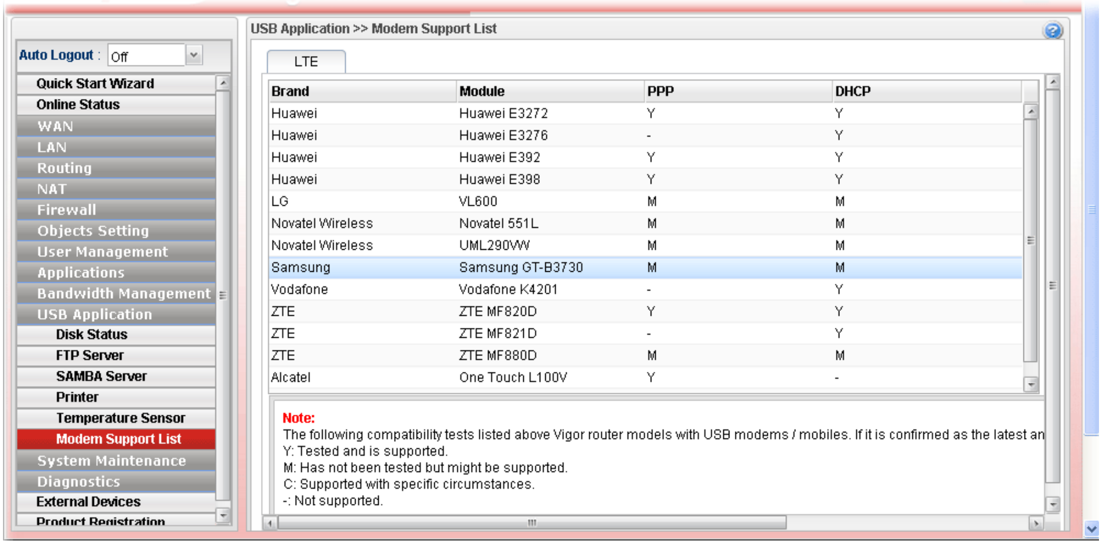
Available settings are explained as follows:

Item	Description
Enable Temperature Sensor	Check this box to enable such function.
Display Unit	Choose **Celsius** or **Fahrenheit** as the display unit.
Temperature Alert Lower limit / Temperature Alert Upper limit	Type the upper limit and lower limit for the system to send out temperature alert.
Calibration	Type a value used for correcting the temperature error.
Temperature Alert Time Interval	The default setting is one minute. That means, the temperature alert will be sent per minute.
Apply	Click it to save the configuration.
Cancel	Click it to clear current configuration.

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

4.10.6 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.



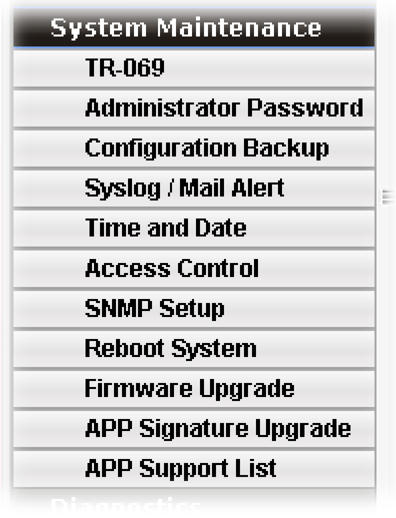
Brand	Module	PPP	DHCP
Huawei	Huawei E3272	Y	Y
Huawei	Huawei E3276	-	Y
Huawei	Huawei E392	Y	Y
Huawei	Huawei E398	Y	Y
LG	VL600	M	M
Novatel Wireless	Novatel 551L	M	M
Novatel Wireless	UML290VW	M	M
Samsung	Samsung GT-B3730	M	M
Vodafone	Vodafone K4201	-	Y
ZTE	ZTE MF820D	Y	Y
ZTE	ZTE MF821D	-	Y
ZTE	ZTE MF880D	M	M
Alcatel	One Touch L100V	Y	-

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

4.11 System Maintenance

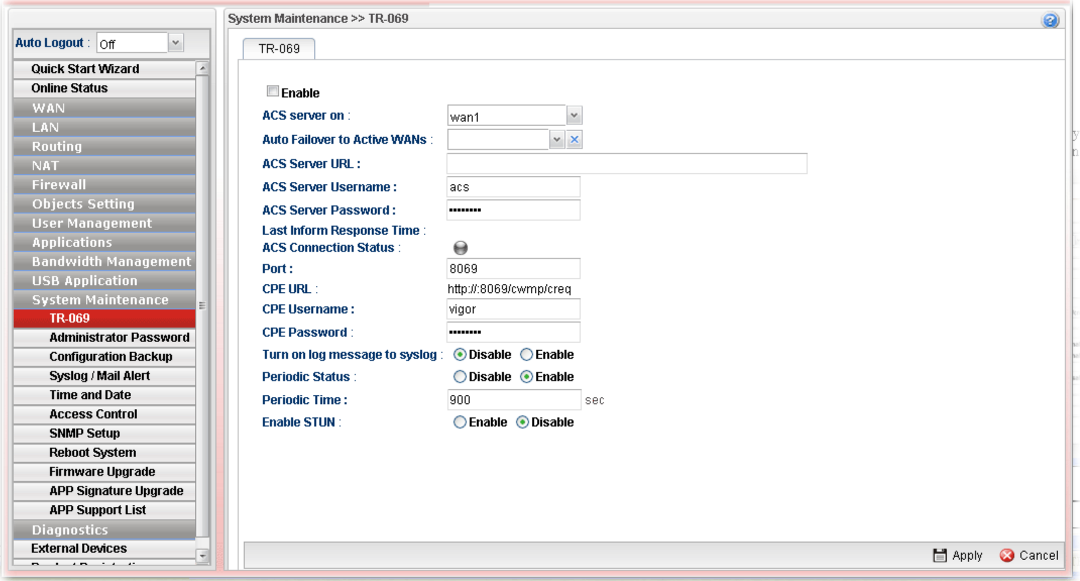
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Access Control, SNMP Setup, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.11.1 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.



System Maintenance >> TR-069

TR-069

□ Enable

ACS server on : wan1

Auto Failover to Active WANs :

ACS Server URL :

ACS Server Username : acs

ACS Server Password : ••••••••

Last Inform Response Time :

ACS Connection Status :

Port : 8069

CPE URL : http://:8069/cwmp/creq

CPE Username : vigor

CPE Password : ••••••••

Turn on log message to syslog : ● Disable ○ Enable

Periodic Status : ○ Disable ● Enable

Periodic Time : 900 sec

Enable STUN : ○ Enable ● Disable

Each item will be explained as follows:

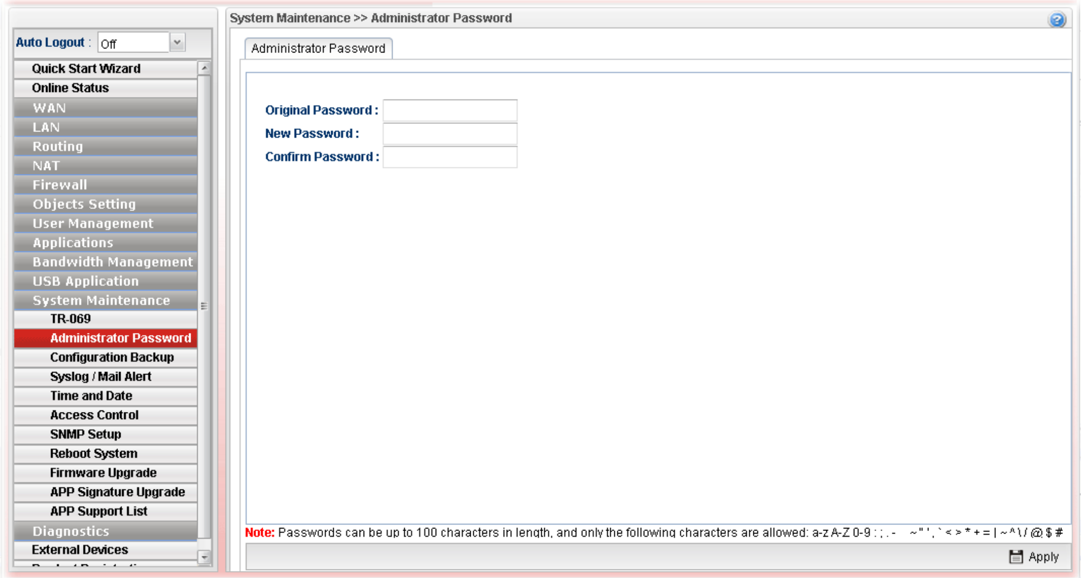
Item	Description
Enable	Check this box to enable such profile.
ACS server on	Choose one of the WAN/LAN profiles which will be recognized by VigorACS.
Auto Failover to Active	Specify the WAN interface to take over the job of network

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 Vigor300B 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 Vigor300B.
CPE Password	Type the password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor300B.
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**.

4.11.2 Administrator Password

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



Note: Passwords can be up to 100 characters in length, and only the following characters are allowed: a-z A-Z 0-9 : ; . - ~ " ' , ` < > * + = | ~ ^ \ / @ $ #

Each item will be explained as follows:

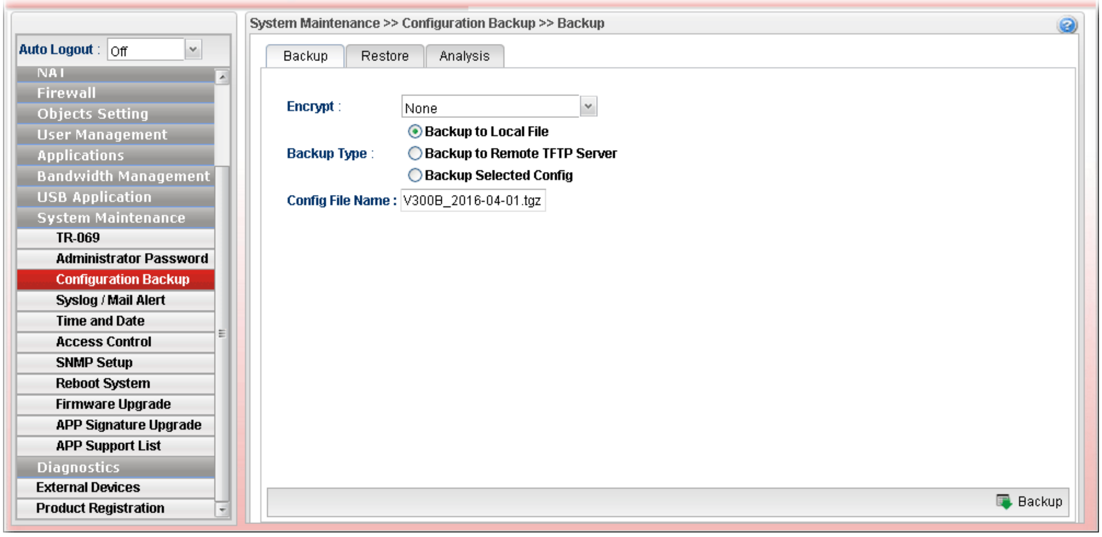
Item	Description
Original Password	Type the old password.
New Password	Type the new password.
Confirm Password	Re-type the new password for confirmation.
Apply	Click this button to save the configuration and exit the web page.

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

4.11.3 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.

4.11.3.1 Backup



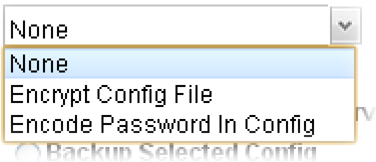
System Maintenance >> Configuration Backup >> Backup

Encrypt : None

Backup Type : ◉ Backup to Local File ○ Backup to Remote TFTP Server ○ Backup Selected Config

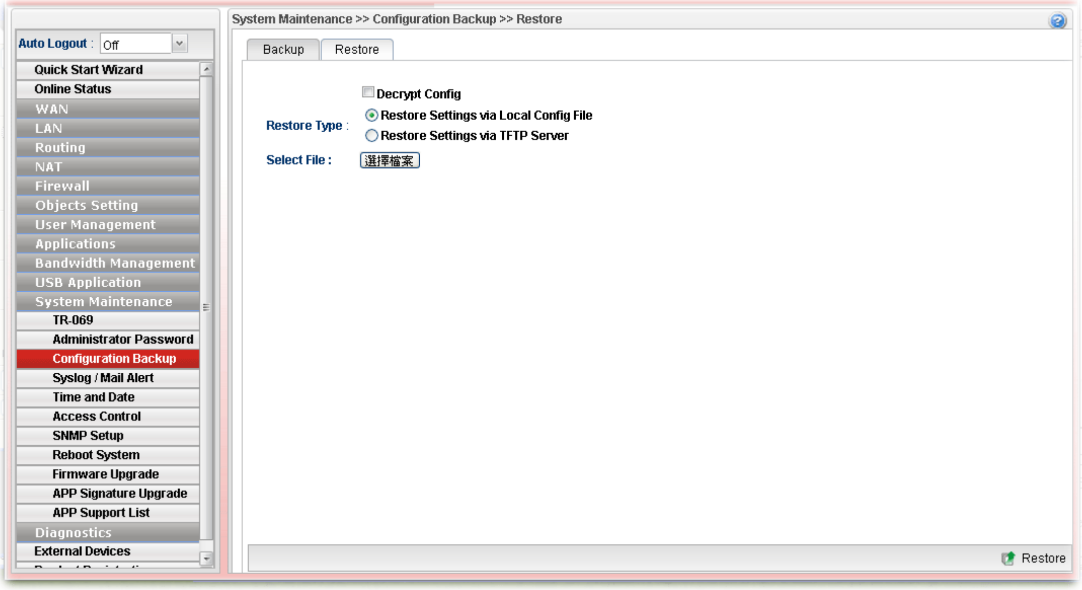
Config File Name : V300B_2016-04-01.tgz

Each item will be explained as follows:

Item	Description
Encrypt	**None** – No encryption will be used. **Encrypt Config File** – Choose it to encrypt the whole configuration file. ● **Password** – Type a password for encrypting the file. ● **Confirm Password –** Retype the password for confirmation.  None None Encrypt Config File Encode Password In Config Backup Selected Config **Encode Password in Config** – Choose it to encrypt the password information in configuration file.
Backup Type	Choose one of the types to determine where the file will be stored. **Backup to Local File** – The configuration file will be stored in local host. **Backup to Remote TFTP Server** – The configuration file will be stored in the remote TFTP server specified. **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.
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.

4.11.3.2 Restore


System Maintenance >> Configuration Backup >> Restore

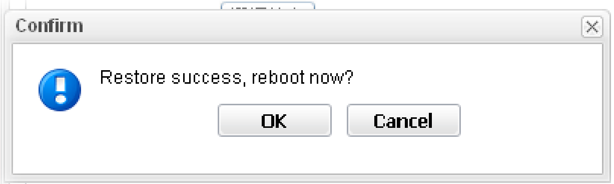
Auto Logout : Off

□ Decrypt Config

Restore Type : ● Restore Settings via Local Config File ○ Restore Settings via TFTP Server

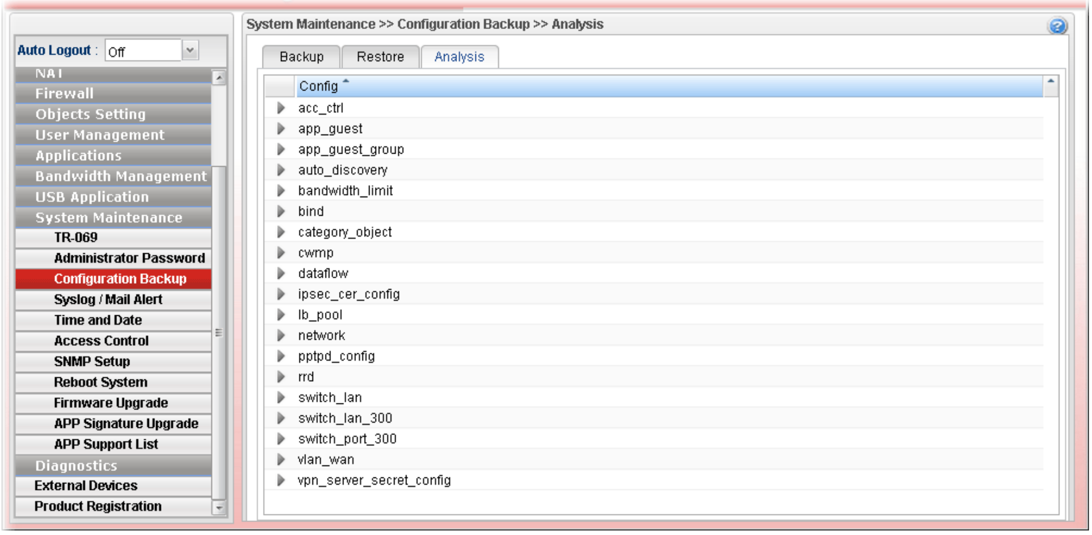
Select File : 選擇檔案

Each item will be explained as follows:

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

4.11.3.3 Analysis

Such analysis page will show user defined settings result. In comparing the default settings with information displayed in this page, it will be convenient for administrator, user or RD member for debug possible error.



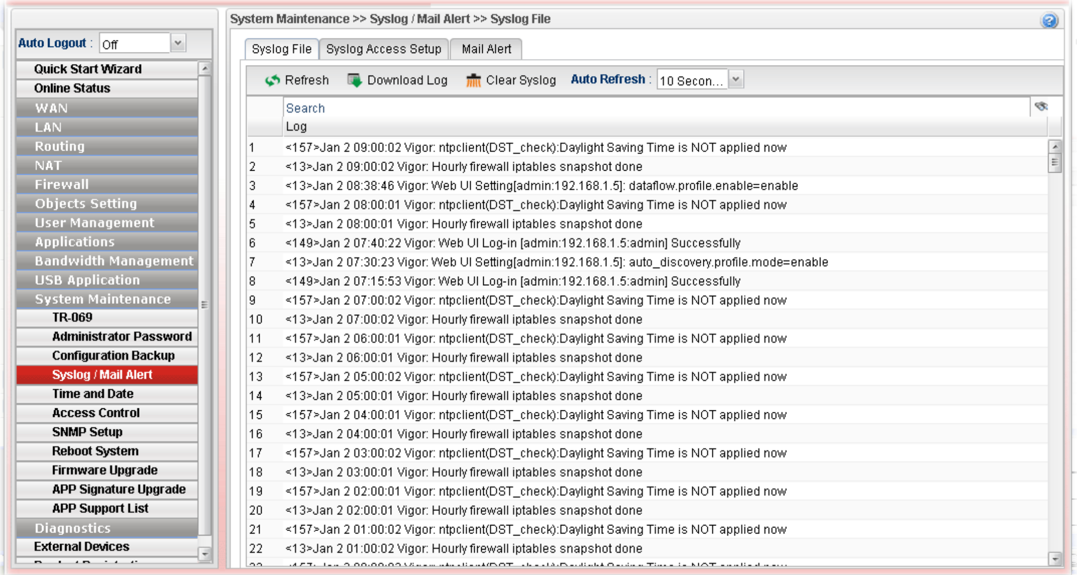
```
acc_ctrl
app_guest
app_guest_group
auto_discovery
bandwidth_limit
bind
category_object
cwmp
dataflow
ipsec_cer_config
lb_pool
network
pptpd_config
rrd
switch_lan
switch_lan_300
switch_port_300
vlan_wan
vpn_server_secret_config
```

4.11.4 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.

4.11.4.1 SysLog File

This page displays all the operation logs for the router.



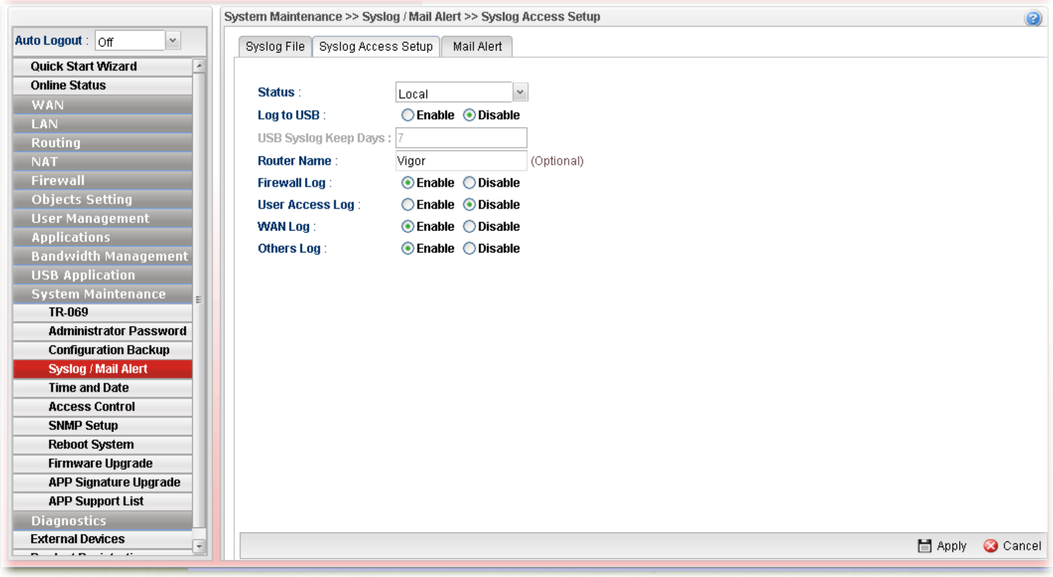
```
1   <157>Jan 2 09:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
2   <13>Jan 2 09:00:02 Vigor: Hourly firewall iptables snapshot done
3   <13>Jan 2 08:38:46 Vigor: Web UI Setting[admin:192.168.1.5]: dataflow.profile.enable=enable
4   <157>Jan 2 08:00:01 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
5   <13>Jan 2 08:00:01 Vigor: Hourly firewall iptables snapshot done
6   <149>Jan 2 07:40:22 Vigor: Web UI Log-in [admin:192.168.1.5:admin] Successfully
7   <13>Jan 2 07:30:23 Vigor: Web UI Setting[admin:192.168.1.5]: auto_discovery.profile.mode=enable
8   <149>Jan 2 07:15:53 Vigor: Web UI Log-in [admin:192.168.1.5:admin] Successfully
9   <157>Jan 2 07:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
10  <13>Jan 2 07:00:02 Vigor: Hourly firewall iptables snapshot done
11  <157>Jan 2 06:00:01 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
12  <13>Jan 2 06:00:01 Vigor: Hourly firewall iptables snapshot done
13  <157>Jan 2 05:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
14  <13>Jan 2 05:00:01 Vigor: Hourly firewall iptables snapshot done
15  <157>Jan 2 04:00:01 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
16  <13>Jan 2 04:00:01 Vigor: Hourly firewall iptables snapshot done
17  <157>Jan 2 03:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
18  <13>Jan 2 03:00:01 Vigor: Hourly firewall iptables snapshot done
19  <157>Jan 2 02:00:01 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
20  <13>Jan 2 02:00:01 Vigor: Hourly firewall iptables snapshot done
21  <157>Jan 2 01:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
22  <13>Jan 2 01:00:02 Vigor: Hourly firewall iptables snapshot done
```

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.

4.11.4.2 Syslog Access Setup



System Maintenance >> Syslog / Mail Alert >> Syslog Access Setup

Status : Local

Log to USB : ○ Enable ● Disable

USB Syslog Keep Days : 7

Router Name : Vigor (Optional)

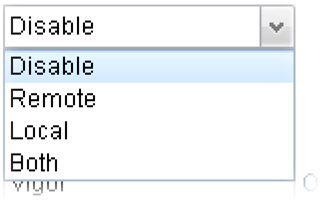
Firewall Log : ● Enable ○ Disable

User Access Log : ○ Enable ● Disable

WAN Log : ● Enable ○ Disable

Others Log : ● Enable ○ Disable

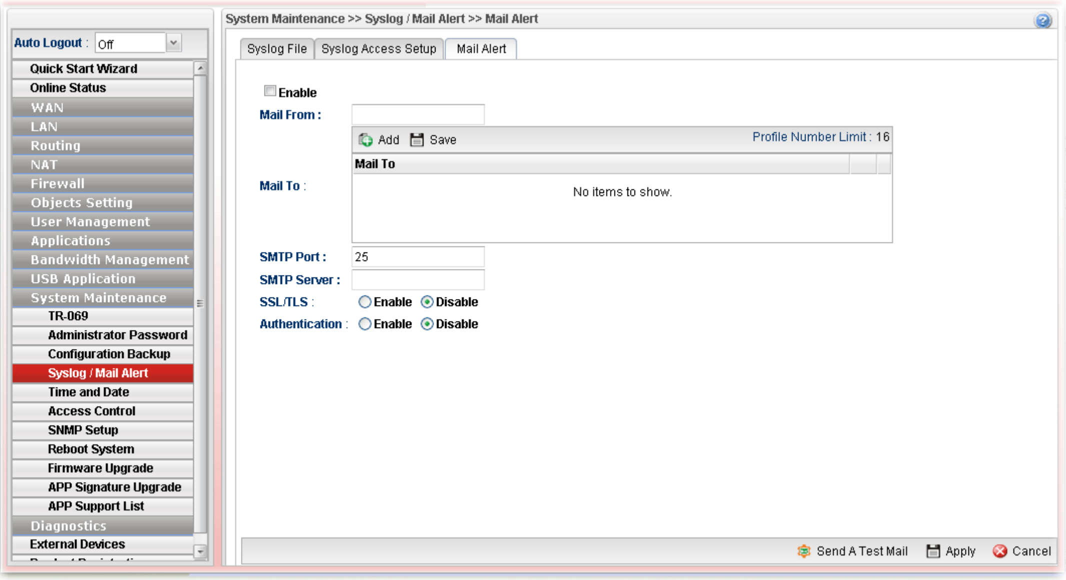
Available parameters are listed as follows:

Item	Description
Status	Choose one of the selections to determine current status for Syslog access. If you choose **Local** as Status, you don't need to type any server IP and port. Just give a name for the router. 
Log to USB	**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.
Server IP	Type the IP address of the Syslog server. It is available when **Remote** or **Both** is selected as **Status**.
Server Port	Type the port number for the Syslog server. It is available when **Remote** or **Both** is selected as **Status**.
Router Name	Type the name of the router. The default name is ***Vigor.***
Firewall Log	Click **Enable** to make the firewall log recorded in the

	Syslog.
User Access Log	Click **Enable** to make the user access log recorded in the Syslog.
WAN Log	Click **Enable** to make the WAN log recorded in the Syslog.
Others Log	Click **Enable** to make other logs recorded in the Syslog.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

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

4.11.4.3 Mail Alert



System Maintenance >> Syslog / Mail Alert >> Mail Alert

□ Enable

Mail From :

Mail To :

Profile Number Limit : 16

Mail To
No items to show.

SMTP Port : 25

SMTP Server :

SSL/TLS : ○ Enable ● Disable

Authentication : ○ Enable ● Disable

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.

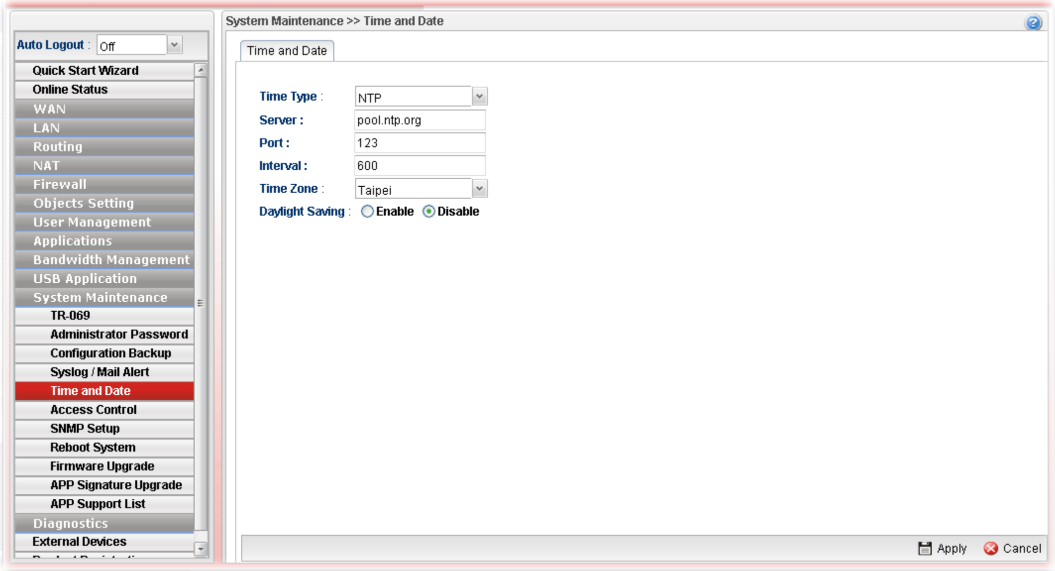
User Password	Type the password for authentication.
Send A Test Mail	Click it to send a test mail to the specified address.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

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

4.11.5 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.



System Maintenance >> Time and Date

Time and Date

Time Type : NTP

Server : pool.ntp.org

Port : 123

Interval : 600

Time Zone : Taipei

Daylight Saving : ○ Enable ● Disable

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.

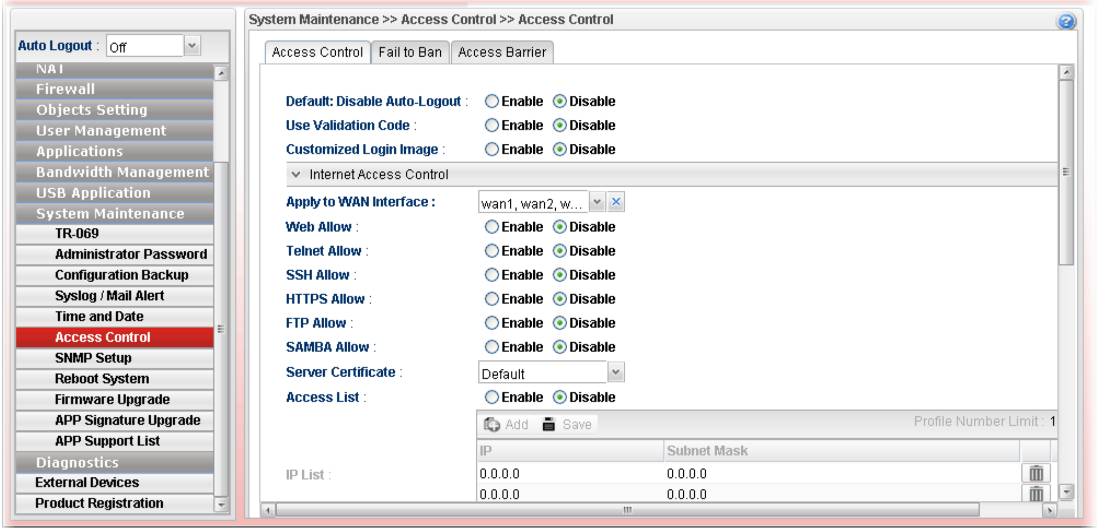
Cancel	Click it to discard the settings configured in this page.

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

4.11.6 Access Control

4.11.6.1 Access Control

This page allows you to open or close the Web User Interface of Vigor300B by using Telnet, SSH, HTTP, HTTPS… and etc…



Default: Disable Auto-Logout : ○ Enable ● Disable

Use Validation Code : ○ Enable ● Disable

Customized Login Image : ○ Enable ● Disable

Internet Access Control

Apply to WAN Interface : wan1, wan2, w...

Web Allow : ○ Enable ● Disable

Telnet Allow : ○ Enable ● Disable

SSH Allow : ○ Enable ● Disable

HTTPS Allow : ○ Enable ● Disable

FTP Allow : ○ Enable ● Disable

SAMBA Allow : ○ Enable ● Disable

Server Certificate : Default

Access List : ○ Enable ● Disable

Profile Number Limit : 1

IP List :

IP	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

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.
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.
Internet Access Control	
Apply to WAN Interface	Choose the WAN interface(s) to apply such feature.

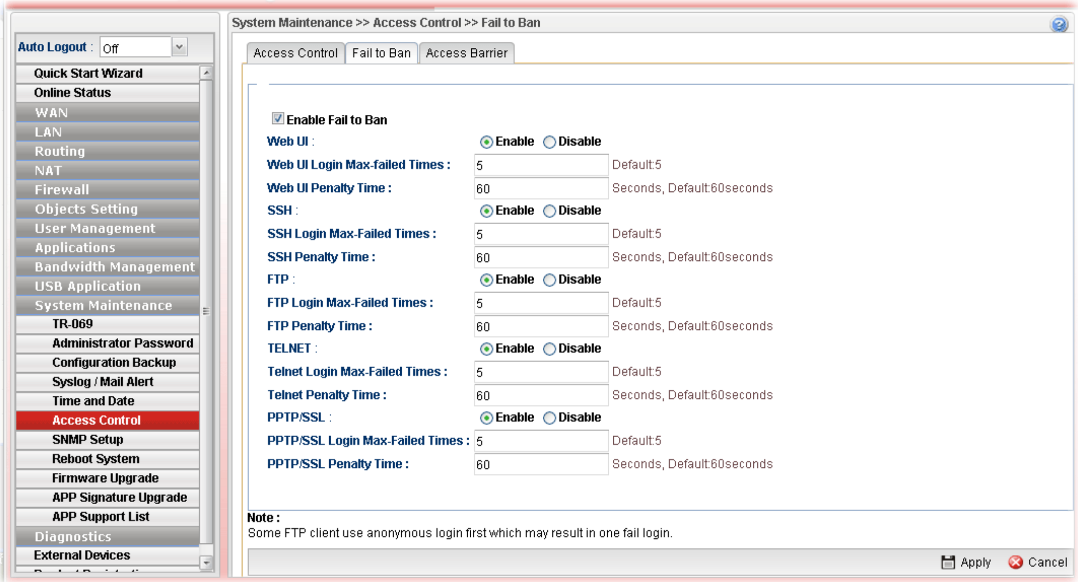
Web Allow	Click **Enable** to allow system administrator to login from the Internet and management the web page of the router.
Telnet Allow	Click **Enable** to allow system administrator to login from the telnet and management the web page of the router.
SSH Allow	Click **Enable** to allow system administrator to login from the SSH server and management the web page of the router.
HTTPS Allow	Click **Enable** to allow system administrator to login from the HTTPS server and management the web page of the router.
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.
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 Vigor300B.
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**.

4.11.6.2 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.



System Maintenance >> Access Control >> Fail to Ban

☑ Enable Fail to Ban

Web UI :	● Enable ○ Disable	
Web UI Login Max-failed Times :	5	Default:5
Web UI Penalty Time :	60	Seconds, Default:60seconds
SSH :	● Enable ○ Disable	
SSH Login Max-Failed Times :	5	Default:5
SSH Penalty Time :	60	Seconds, Default:60seconds
FTP :	● Enable ○ Disable	
FTP Login Max-Failed Times :	5	Default:5
FTP Penalty Time :	60	Seconds, Default:60seconds
TELNET :	● Enable ○ Disable	
Telnet Login Max-Failed Times :	5	Default:5
Telnet Penalty Time :	60	Seconds, Default:60seconds
PPTP/SSL :	● Enable ○ Disable	
PPTP/SSL Login Max-Failed Times :	5	Default:5
PPTP/SSL Penalty Time :	60	Seconds, Default:60seconds

Note :
Some FTP client use anonymous login first which may result in one fail login.

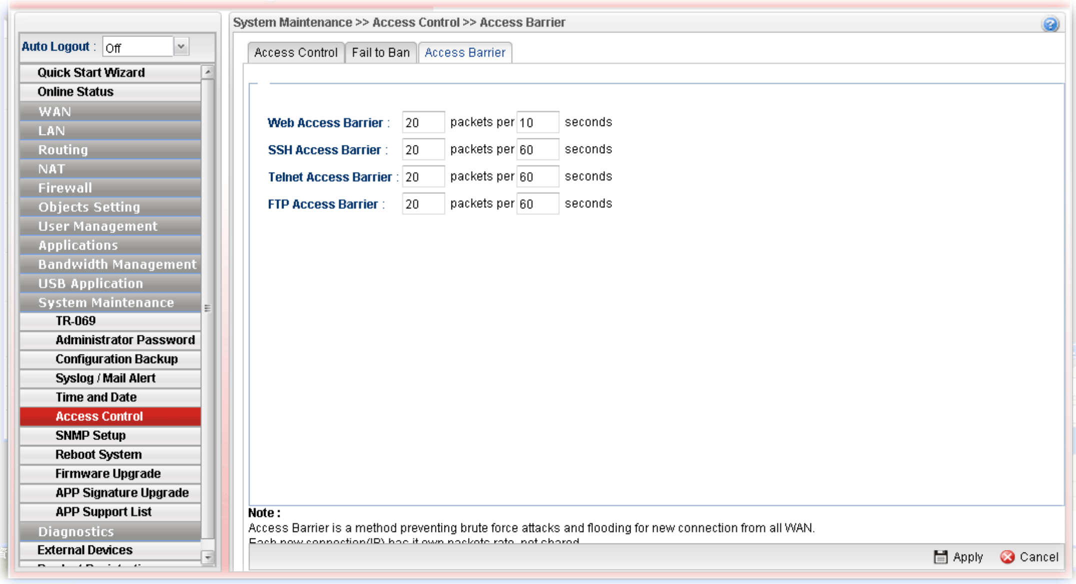
Available parameters are listed as follows:

Item	Description
Enable Fail to Ban	Enable the function to protect Vigor system while being attacked by malicious accounts and passwords.
Web UI/SSH/FTP/ TELNET/PPTP/SSL	**Enable –** Enable the function of Fail to Ban via different protocols (Web UI/SSH/FTP/TELNET/PPTP/SSL)**.** ● **Login Max-failed Times –** The number typed here means the maximum logging times allowed for a group of user account and password trying to login Vigor router.

	● **Penalty Time –** This field is used to configure the blocking time. The default setting is 60 seconds. It means, when a user tries to login Vigor router with a user account for many times (defined in Login Max-failed Times) but fails, he/she will be prohibited to login for a period of time. When the penalty time limit is up, he/she is allowed to login into Vigor router again. **Disable** - Disable the function of Fail to Ban for Web UI/SSH/FTP/TELNET/PPTP/SSL.
Apply	Click this button to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.11.6.3 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.



System Maintenance >> Access Control >> Access Barrier

Web Access Barrier : 20 packets per 10 seconds

SSH Access Barrier : 20 packets per 60 seconds

Telnet Access Barrier : 20 packets per 60 seconds

FTP Access Barrier : 20 packets per 60 seconds

Note :
Access Barrier is a method preventing brute force attacks and flooding for new connection from all WAN.
Each new connection(IP) has it own packets rate, not shared.

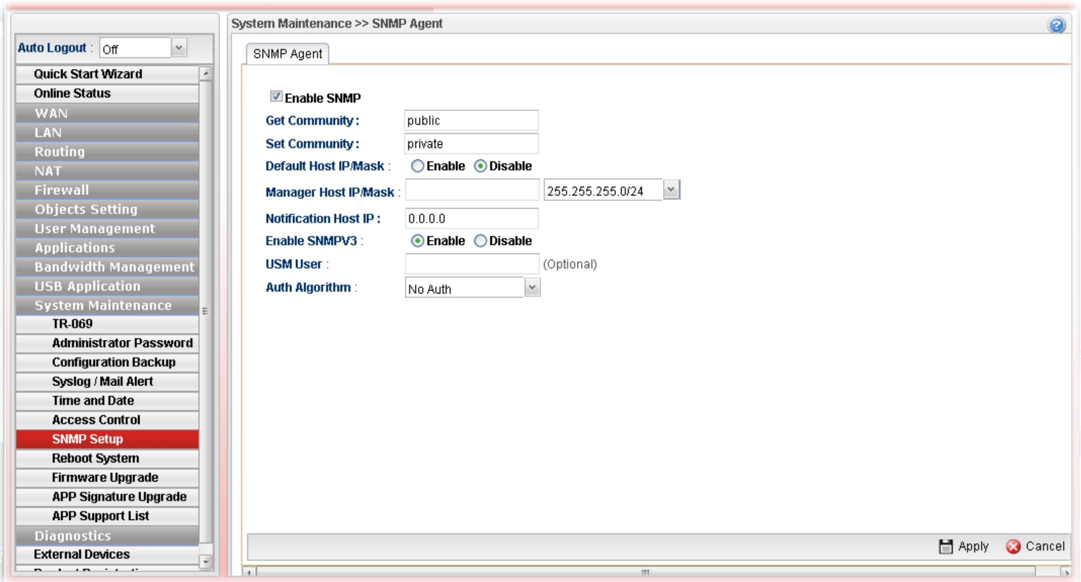
Available parameters are listed as follows:

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.

4.11.7 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.

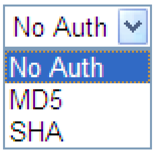


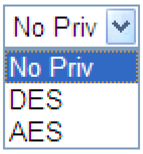
System Maintenance >> SNMP Agent

SNMP Agent

☑ Enable SNMP
Get Community : public
Set Community : private
Default Host IP/Mask : ○ Enable ● Disable
Manager Host IP/Mask : 255.255.255.0/24
Notification Host IP : 0.0.0.0
Enable SNMPV3 : ● Enable ○ Disable
USM User : (Optional)
Auth Algorithm : No Auth

Available parameters are listed as follows:

Item	Description
Enable SNMP	Check the box to enable the function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**
Set Community	Set community by typing a proper name. The default setting is **private.**
Default Host IP/Mask	Click **Enable** to use the default IP and mask of the host as the SNMP agent. If you click **Disable,** you need to type the IP address and choose the mask manually in related fields.
Notification Host IP	Type the IP address of the host for notification.
Enable SnmpV3	Click **Enable** to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm (Min. Length:8)	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password	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**.

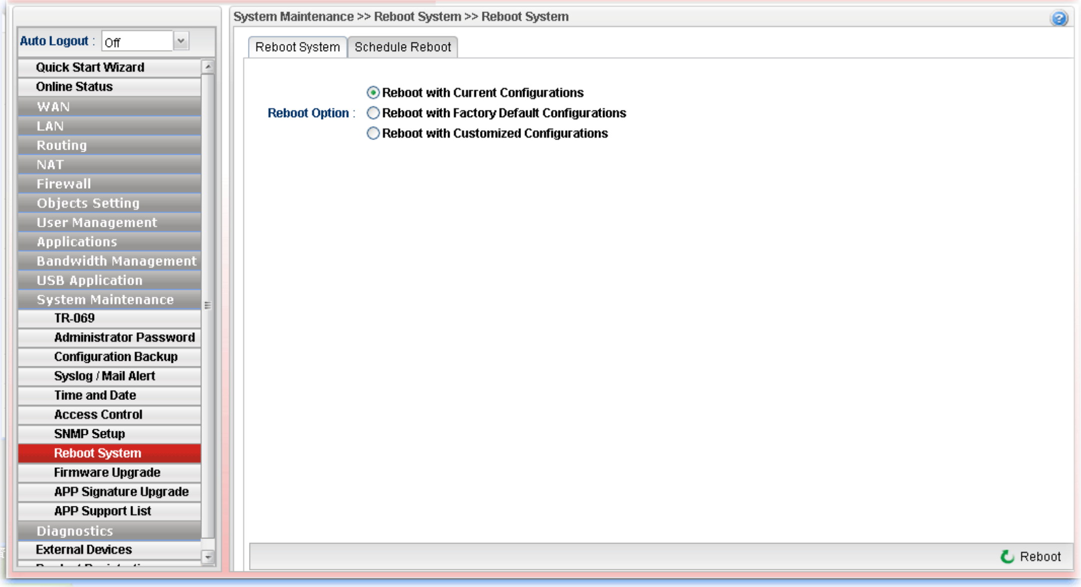
4.11.8 Reboot System

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.

4.11.8.1 Reboot System

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

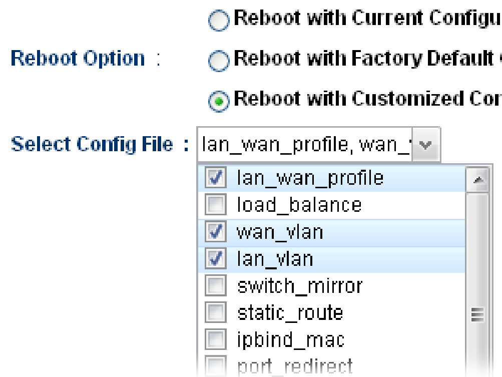


System Maintenance >> Reboot System >> Reboot System

Reboot Option : ● Reboot with Current Configurations
○ Reboot with Factory Default Configurations
○ Reboot with Customized Configurations

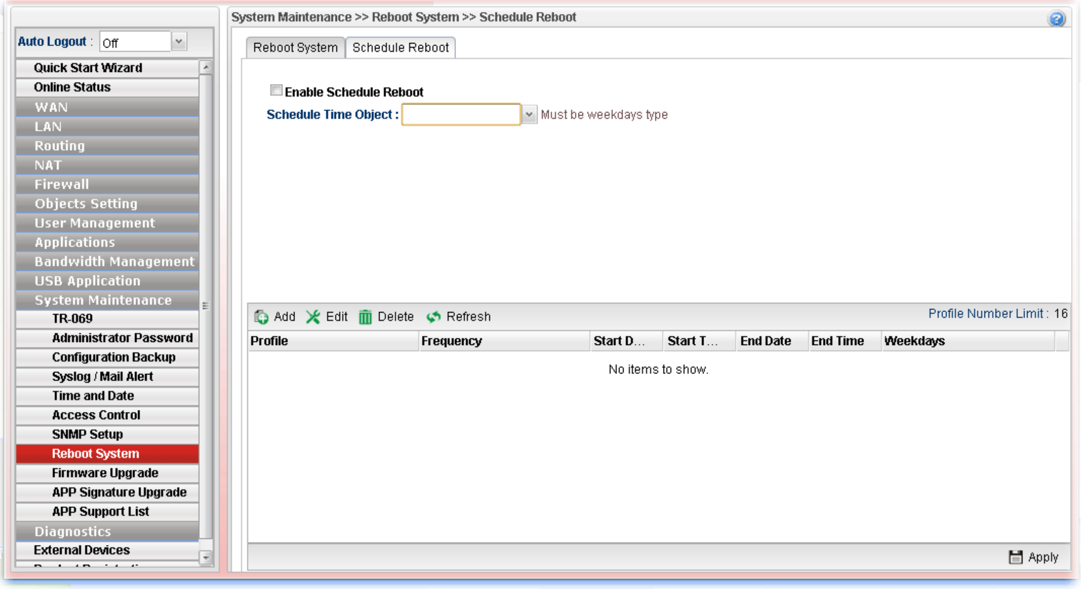
Available parameters are listed as follows:

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**.

Reboot with Customized Configurations	Click it to reboot the router using the current configuration (only the configuration settings listed and selected below). If you choose this option, **Select Config File** will be available for you to select.  Reboot Option : ○ Reboot with Current Configurations ○ Reboot with Factory Default Configurations ● Reboot with Customized Configurations Select Config File : lan_wan_profile, wan_ ☑ lan_wan_profile □ load_balance ☑ wan_vlan ☑ lan_vlan □ switch_mirror □ static_route □ ipbind_mac □ port_redirect After choosing the configuration files, click **Reboot**.
Reboot	Click this button to execute the rebooting job.

4.11.8.2 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.



System Maintenance >> Reboot System >> Schedule Reboot

□ Enable Schedule Reboot

Schedule Time Object : Must be weekdays type

Profile Number Limit : 16

Profile	Frequency	Start D...	Start T...	End Date	End Time	Weekdays

No items to show.

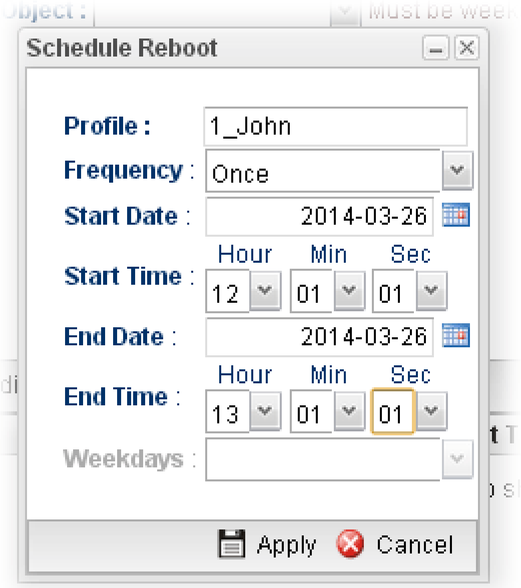
Available parameters are listed as follows:

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.



Schedule Reboot

Profile : 1_John

Frequency : Once

Start Date : 2014-03-26

Start Time : Hour 12 Min 01 Sec 01

End Date : 2014-03-26

End Time : Hour 13 Min 01 Sec 01

Weekdays :

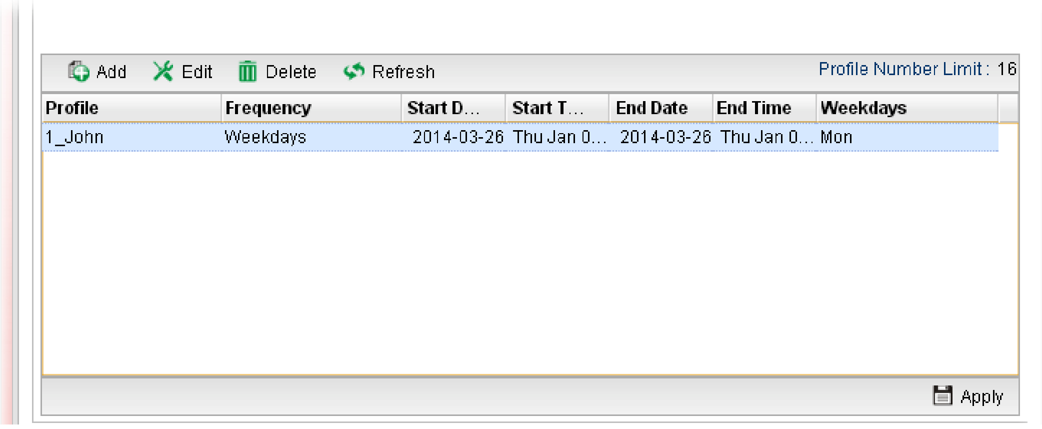
Available parameters are listed as follows:

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.



Profile	Frequency	Start D...	Start T...	End Date	End Time	Weekdays
1_John	Weekdays	2014-03-26	Thu Jan 0...	2014-03-26	Thu Jan 0...	Mon

4.11.9 Firmware Upgrade

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

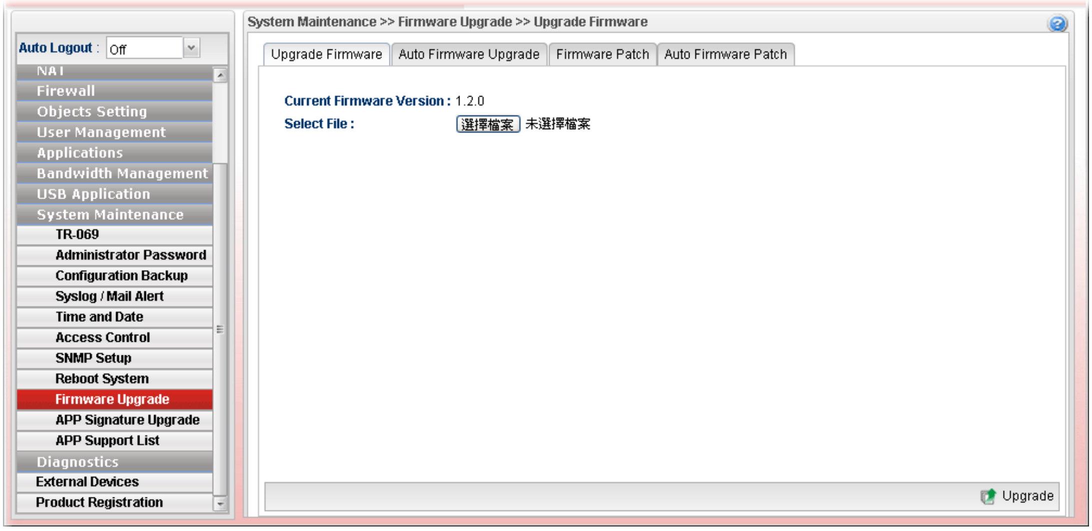
Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and the FTP site is ftp.DrayTek.com.

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

4.11.9.1 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.



Current Firmware Version : 1.2.0

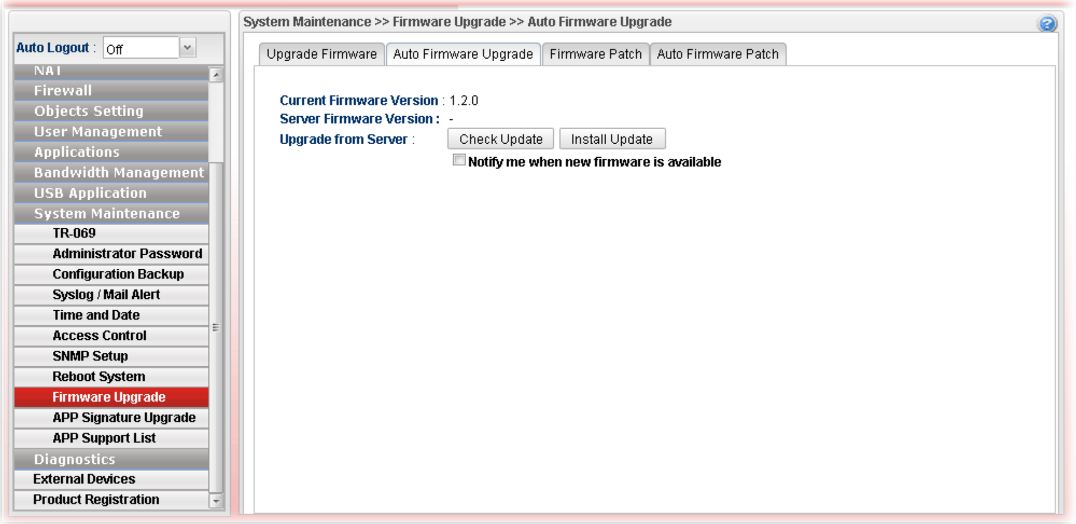
Select File : 未選擇檔案

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.

4.11.9.2 Auto Firmware Upgrade

By clicking **Check Update/Install Update**, Vigor router can download/upgrade firmware directly from website (http://www.draytek.com.tw/ftp) automatically.



Current Firmware Version : 1.2.0

Server Firmware Version : -

Upgrade from Server :

□ Notify me when new firmware is available

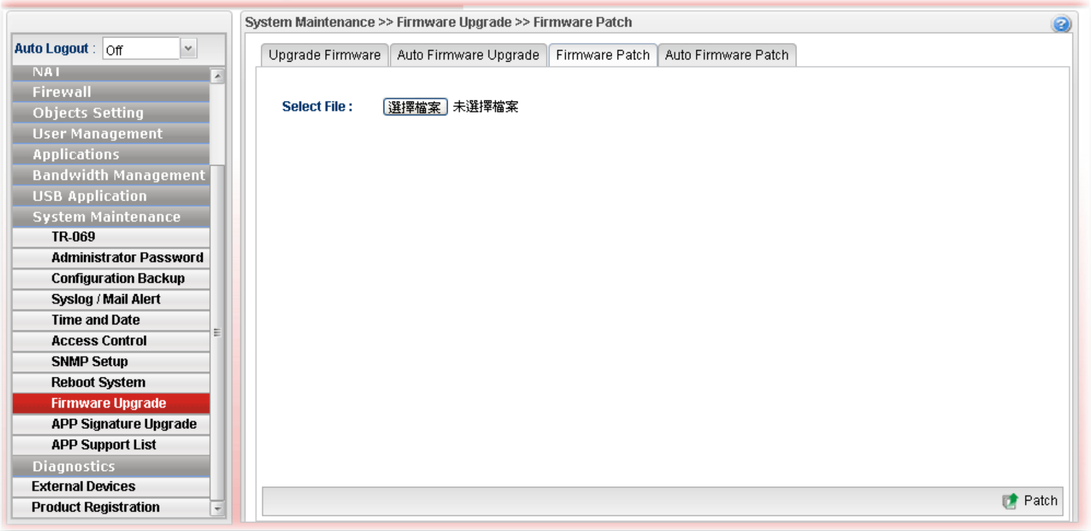
Available parameters are listed as follows:

Item	Description
Server Firmware Version	Display the firmware version shown on website (http://www.draytek.com.tw/ftp).
Server Firmware Version	Display the firmware version shown on website (http://www.draytek.com.tw/ftp).

Upgrade from Server	**Check Update** –Vigor router will inquire to website (http://www.draytek.com.tw/ftp) if there is any newest firmware available for use. If yes, Vigor router will download the newest firmware from the website to the host (Vigor router) automatically. **Install Update** –If the firmware version stored on the website (http://www.draytek.com.tw/ftp) is newer than the version used by the host (Vigor router), then Vigor router will download and install the newest firmware version automatically. **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.

4.11.9.3 Firmware Patch

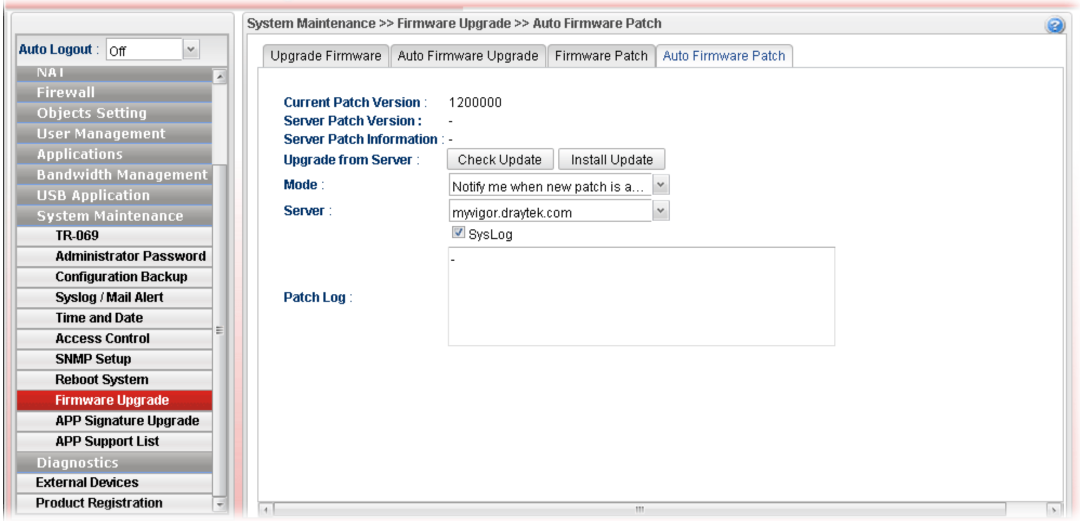
Vigor router administrator/user can manually select file (.pat) to fix/modify the mistakes, bugs or error occurred on current firmware. Usually, such firmware with instant modifications can be obtained from DrayTek MyVigor Patch Server.



4.11.9.4 Auto Firmware Patch

A firmware contains hundreds of files, and a firmware patch could be a single file or several files of a firmware. Since firmware 1.2.0, Vigor300B supports Firmware Patch feature which allows upgrading a specific firmware patch only, but not the whole firmware. The benefit is Vigor300B doesn't need to reboot the system after updating the firmware patch.

Auto Firmware Patch is similar to Auto Firmware Upgrade. While configuring Mode as “Notify me when a new patch is available”, Vigor300B will check if there is a new patch available on DrayTek server daily. When a new patch is available, Vigor300B will pop-up notification window when Administrator logs in.



System Maintenance >> Firmware Upgrade >> Auto Firmware Patch

Current Patch Version : 1200000
Server Patch Version : -
Server Patch Information : -
Upgrade from Server :
Mode : Notify me when new patch is a...
Server : myvigor.draytek.com
☑ SysLog
Patch Log : -

Available parameters are listed as follows:

Item	Description
Current Patch Version	Display the installed patch version on local system
Server Patch Version	Display the latest patch version on DrayTek MyVigor server.
Server Patch Information	Display detailed patch information.
Upgrade from Server	**Check Update** – Click the button to let the system check and get server patch version. **Install Update** – Click it to install the server patch version onto Vigor router.
Mode	There are three modes available for you to choose. **Manual upgrad**e – If it is selected, check and installation for patch will be executed only when **Check Update/Install Update** is pressed. **Notify me when new patch is available -** If it is specified, after detecting the newest patch from MyVigor server, Vigor router’s system will automatically download the patch information and store on the host. Later, when the user logs into the router’s web user interface, the system will give a hint to notify the user in the logging window. **Auto upgrade when new patch is available -** If the patch information stored on MyVigor server is newer than information stored in the host (Vigor router), then Vigor

	router will download and upgrade the newest information automatically.
Server	Use the drop down list to specify a suitable server.
Syslog	Check the box to store the patch log into Syslog.
Patch Log	This area will show log related to firmware patch automatically if firmware patch is executed.

When the router is doing daily firmware patch check, Syslog will have the logs below:

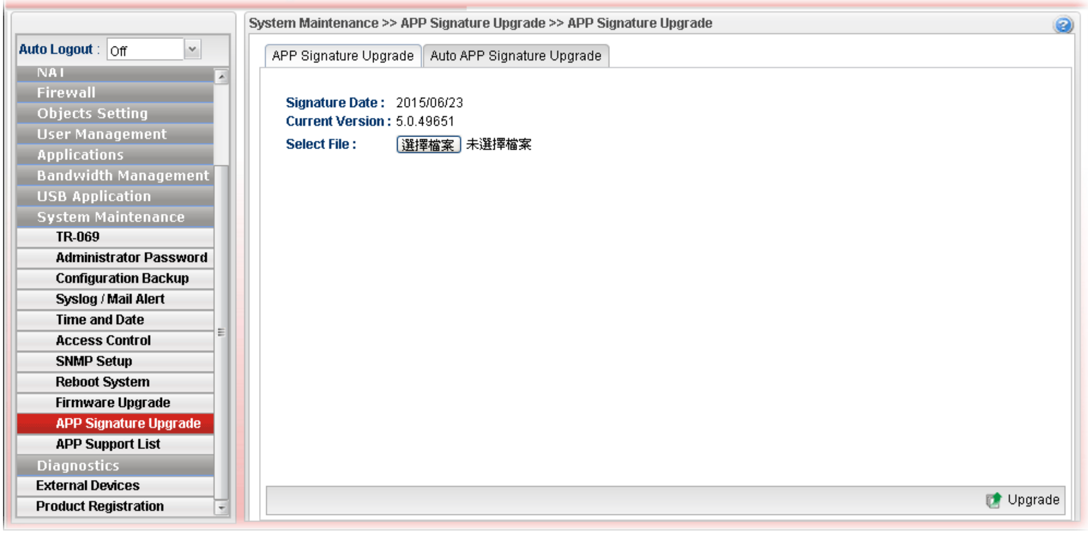
```
<13>Dec 18 13:59:18 Vigor: [patupgrade_auto][1] Check latest patch version from server ...

<13>Dec 18 13:59:18 Vigor: [patupgrade_auto][0] Try get version from
http://myvigor.draytek.com/sig/APPE/dlm/c1k/latver.txt

<13>Dec 18 13:59:19 Vigor: [patupgrade_auto][0] Get version: 1200000 (latest=1200000)

<13>Dec 18 13:59:19 Vigor: [patupgrade_auto][1] Success: Your firmware is up-to-date and
need not to patch.
```

4.11.10 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.

4.11.10.1 APP Signature Upgrade

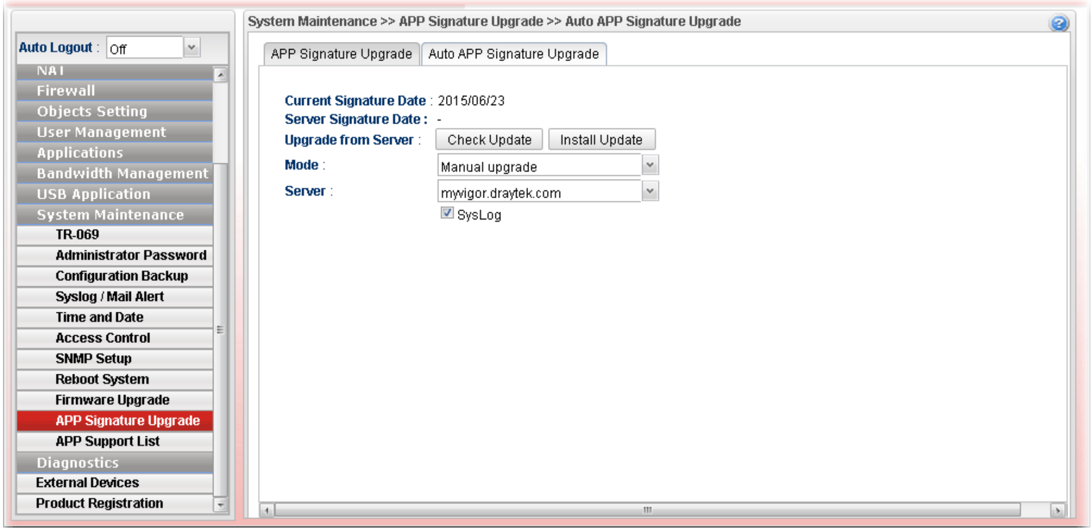
Before upgrading APP signature to Vigor300B, open this page and specify a signature file by clicking **Select**. Later, click **Upgrade** to execute signature upgrade.



Signature Date : 2015/06/23
Current Version : 5.0.49651
Select File : 選擇檔案 未選擇檔案

4.11.10.2 Auto APP Signature Upgrade

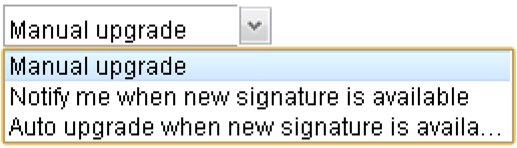
This page allows Vigor router to execute signature upgrade automatically.



System Maintenance >> APP Signature Upgrade >> Auto APP Signature Upgrade

Current Signature Date : 2015/06/23
Server Signature Date : -
Upgrade from Server : Check Update | Install Update
Mode : Manual upgrade
Server : myvigor.draytek.com
☑ SysLog

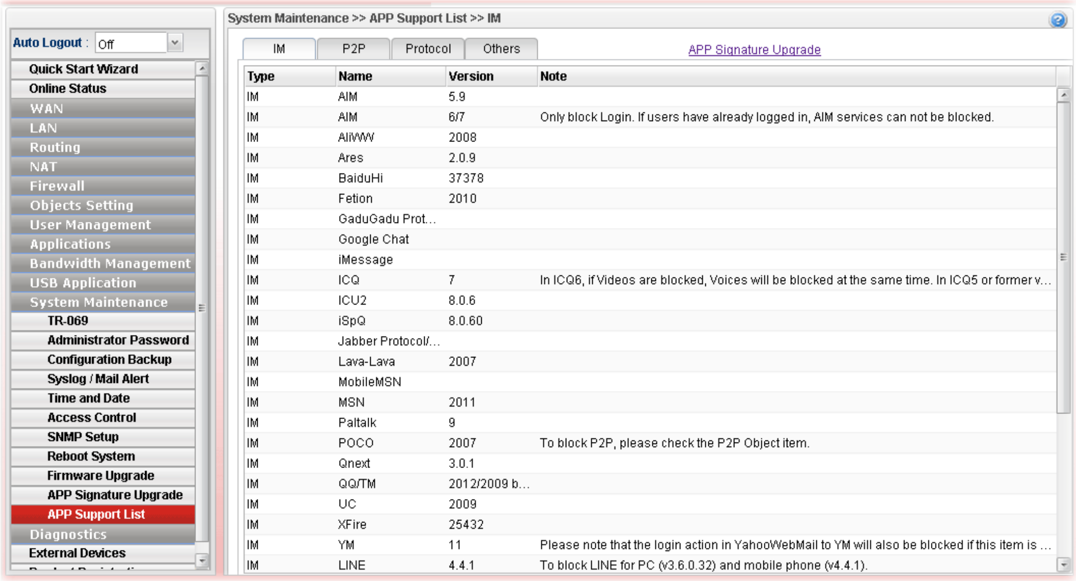
Available parameters are listed as follows:

Item	Description
Current Signature Date	Display the date of current signature installed on Vigor300B.
Server Signature Date	Display the newest signature version recorded on server (myvigor.draytek.com or myvigoreu.draytek.com).
Upgrade from Server	Get the newest signature from MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com). **Check Update** –Vigor router will inquire to MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com) if there is any newest signature available for use. If yes, Vigor router will download the newest signature from the website to the host (Vigor router) automatically. **Install Update** –If the signature information stored on MyVigor server (myvigor.draytek.com or myvigoreu.draytek.com) is newer than the version used by the host (Vigor router), then the system will install the newest signature version information automatically.
Mode	Choose the condition to execute APP signature upgrade or send a notification.  Manual upgrade Manual upgrade Notify me when new signature is available Auto upgrade when new signature is availa... **Manual upgrade** – If it is selected, check and installation for signature will be executed only when **Check Update/Install Update** is pressed. **Notify me when new signature is available -** If it is specified, after detecting the newest signature from MyVigor server, Vigor router's system will automatically download the signature information and store on the host. Later, when

	the user logs into the router’s web user interface, the system will give a hint to notify the user in the logging window. **Auto upgrade when new signature is available -** If the signature information stored on MyVigor server is newer than information stored in the host (Vigor router), then Vigor router will download and upgrade the newest information automatically.
Server	Choose a proper server for signature upgrade from the drop down list. At present, only two servers (myvigor.draytek.com or myvigoreu.draytek.com) are supported.
Syslog	Check the box to record related information on Syslog.

4.11.11 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.

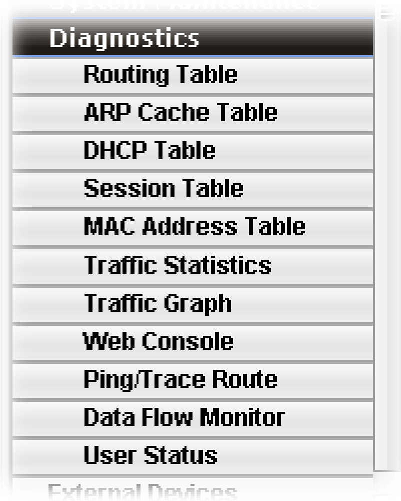


System Maintenance >> APP Support List >> IM

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	AliWW	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 former v...
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	Qnext	3.0.1	
IM	QQ/TM	2012/2009 b...	
IM	UC	2009	
IM	XFire	25432	
IM	YM	11	Please note that the login action in YahooWebMail to YM will also be blocked if this item is ...
IM	LINE	4.4.1	To block LINE for PC (v3.6.0.32) and mobile phone (v4.4.1).

4.12 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 Vigor300B supports five functions, **Routing Table**, **ARP Cache Table**, **DHCP Assignment Table**, **Sessions Table** and **Traffic Graph** for the user to review such information.

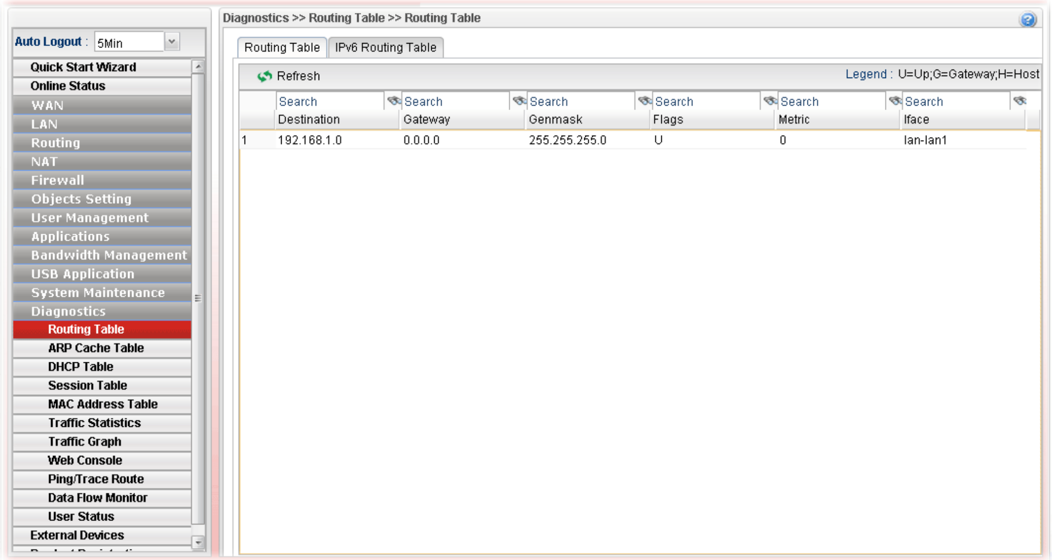


4.12.1 Routing Table

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

4.12.1.2 Routing Table

Display the information for each route.



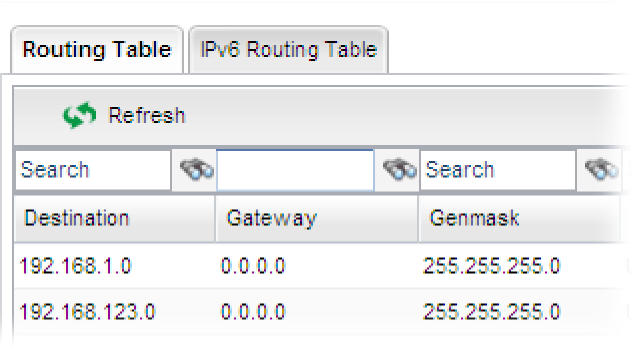
Diagnostics >> Routing Table >> Routing Table

Legend : U=Up;G=Gateway;H=Host

	Destination	Gateway	Genmask	Flags	Metric	Iface
1	192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1

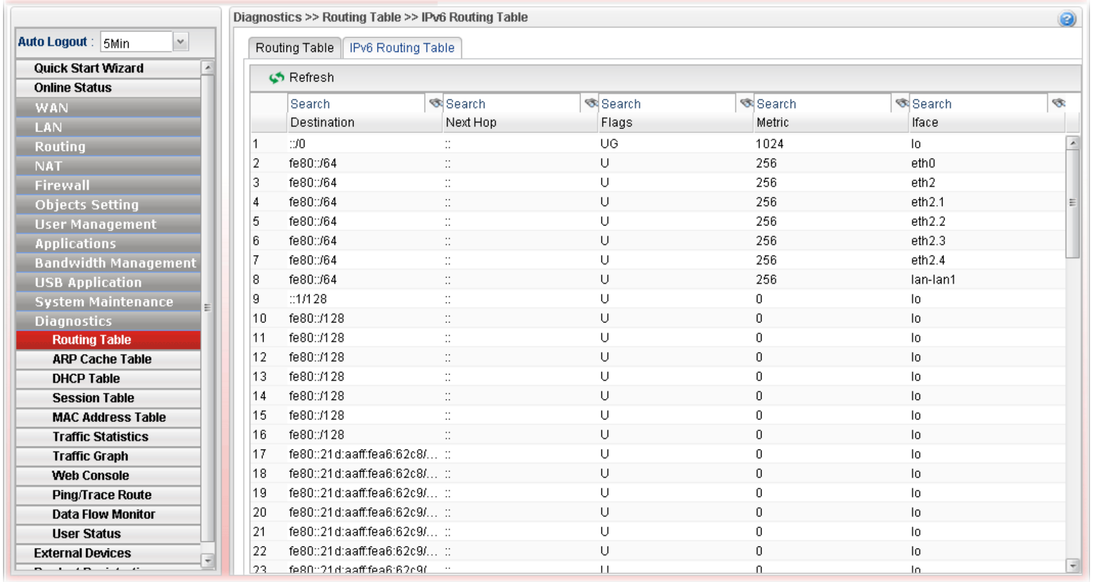
Each item will be explained as follows:

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.  Routing Table IPv6 Routing Table Refresh Search Search Destination Gateway Genmask 192.168.1.0 0.0.0.0 255.255.255.0 192.168.123.0 0.0.0.0 255.255.255.0
Destination	Display the destination IP address for various routings.
Gateway	Display the default gateway.
Genmask	Display the subnet mask for various routings.
Flags	Display the flag of the routing entry. Possible flags include: U (route is up) H (target is a host) G (use gateway) R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by *addrconf*) C (cache entry) ! (reject route)
Metric	Display the distance to the target (usually counted in hops). It may be needed by routing daemons.
Iface	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).

4.12.1.2 IPv6 Routing Table

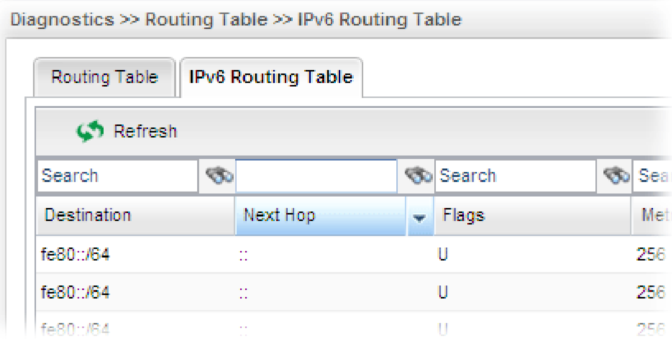
Display the information for each route with IPv6 protocol.



Diagnostics >> Routing Table >> IPv6 Routing Table

	Destination	Next Hop	Flags	Metric	Iface
1	::/0	::	UG	1024	lo
2	fe80::/64	::	U	256	eth0
3	fe80::/64	::	U	256	eth2
4	fe80::/64	::	U	256	eth2.1
5	fe80::/64	::	U	256	eth2.2
6	fe80::/64	::	U	256	eth2.3
7	fe80::/64	::	U	256	eth2.4
8	fe80::/64	::	U	256	lan-lan1
9	::1/128	::	U	0	lo
10	fe80::/128	::	U	0	lo
11	fe80::/128	::	U	0	lo
12	fe80::/128	::	U	0	lo
13	fe80::/128	::	U	0	lo
14	fe80::/128	::	U	0	lo
15	fe80::/128	::	U	0	lo
16	fe80::/128	::	U	0	lo
17	fe80::21d:aaff:fea6:62c8/...	::	U	0	lo
18	fe80::21d:aaff:fea6:62c8/...	::	U	0	lo
19	fe80::21d:aaff:fea6:62c9/...	::	U	0	lo
20	fe80::21d:aaff:fea6:62c9/...	::	U	0	lo
21	fe80::21d:aaff:fea6:62c9/...	::	U	0	lo
22	fe80::21d:aaff:fea6:62c9/...	::	U	0	lo
23	fe80::21d:aaff:fea6:62c9/	::	U	0	lo

Each item will be explained as follows:

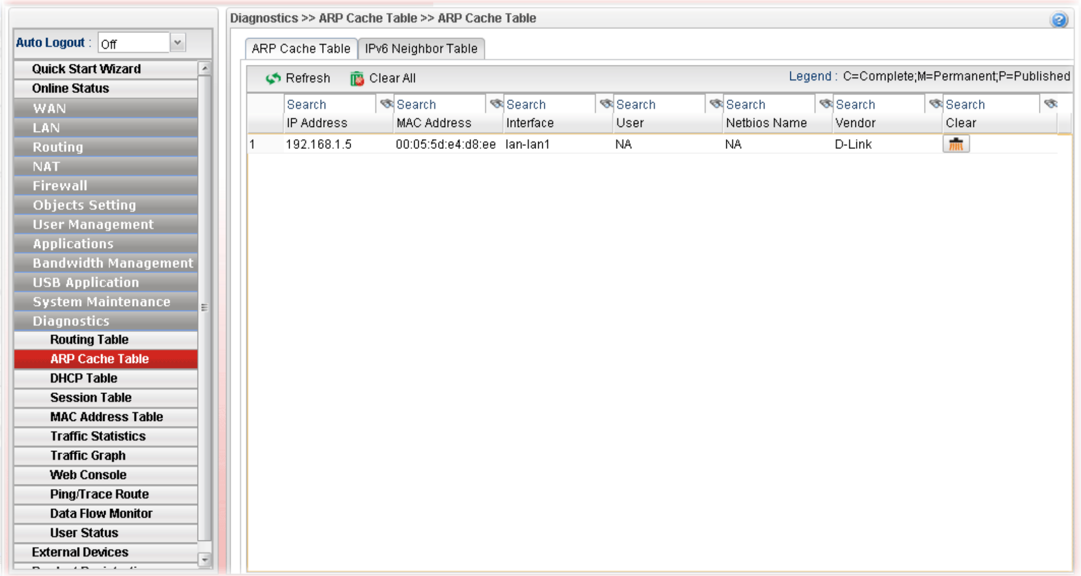
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> Routing Table >> IPv6 Routing Table Routing Table · IPv6 Routing Table · Refresh Destination · Next Hop · Flags · Met fe80::/64 · :: · U · 256 fe80::/64 · :: · U · 256
Destination	Display the destination IP address for various routings.
Next Hop	Display the next hop address for such route。
Flags	Display the flag of the routing entry. Possible flags include: U (route is up) H (target is a host) G (use gateway) R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by *addrconf*) C (cache entry) ! (reject route)

Metric	Display the distance to the target (usually counted in hops). It may be needed by routing daemons.
Iface	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).

4.12.2 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



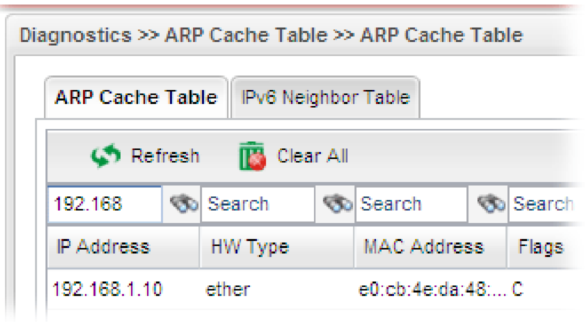
Diagnostics >> ARP Cache Table >> ARP Cache Table

ARP Cache Table | IPv6 Neighbor Table

Legend : C=Complete;M=Permanent;P=Published

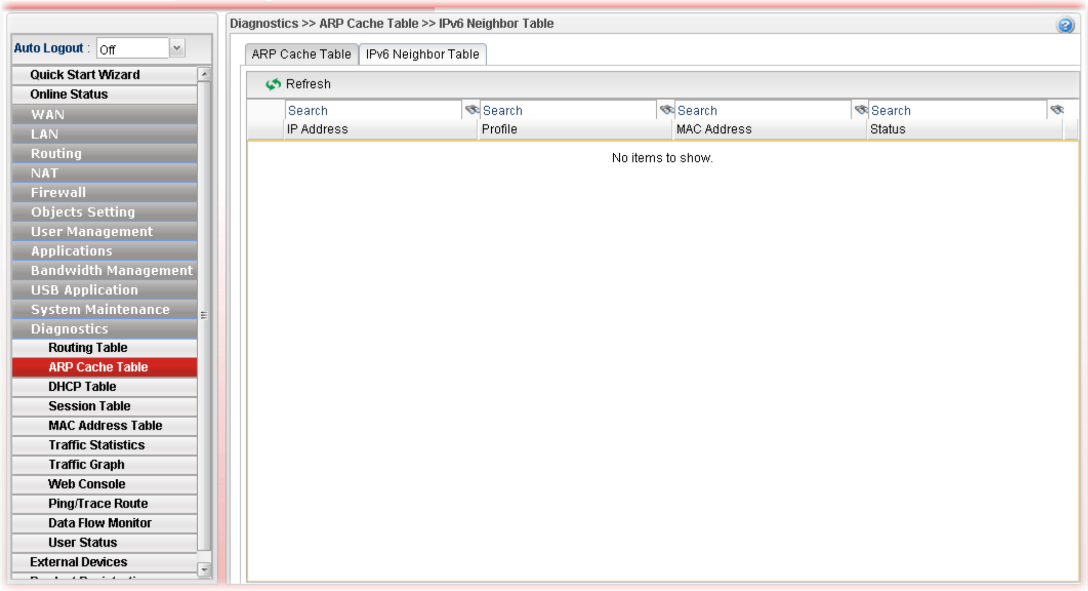
	IP Address	MAC Address	Interface	User	Netbios Name	Vendor	Clear
1	192.168.1.5	00:05:5d:e4:d8:ee	lan-lan1	NA	NA	D-Link	

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.  Diagnostics >> ARP Cache Table >> ARP Cache Table ARP Cache Table | IPv6 Neighbor Table Refresh Clear All 192.168 | Search | Search | Search IP Address | HW Type | MAC Address | Flags 192.168.1.10 | ether | e0:cb:4e:da:48:... | C
IP Address	Display the IP address for different ARP cache.

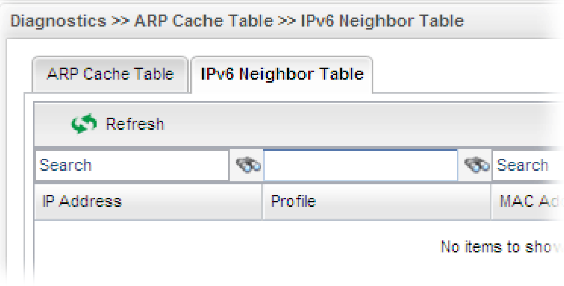
Item	Description
MAC Address	Display the MAC address for different ARP cache.
Interface	Display the LAN profiles used.
User	Display the name of the user.
Netbios Name	Display the Netbios name used by such device.
Vendor	Display the identity the vendor type.
Clear	Delete the selected profile.

4.12.2.2 IPv6 Neighbor Table



No items to show.

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.  Diagnostics >> ARP Cache Table >> IPv6 Neighbor Table ARP Cache Table · IPv6 Neighbor Table · Refresh · Search · IP Address · Profile · MAC Ad No items to sho
IP Address	Display the IPv6 address of the neighbor.
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.

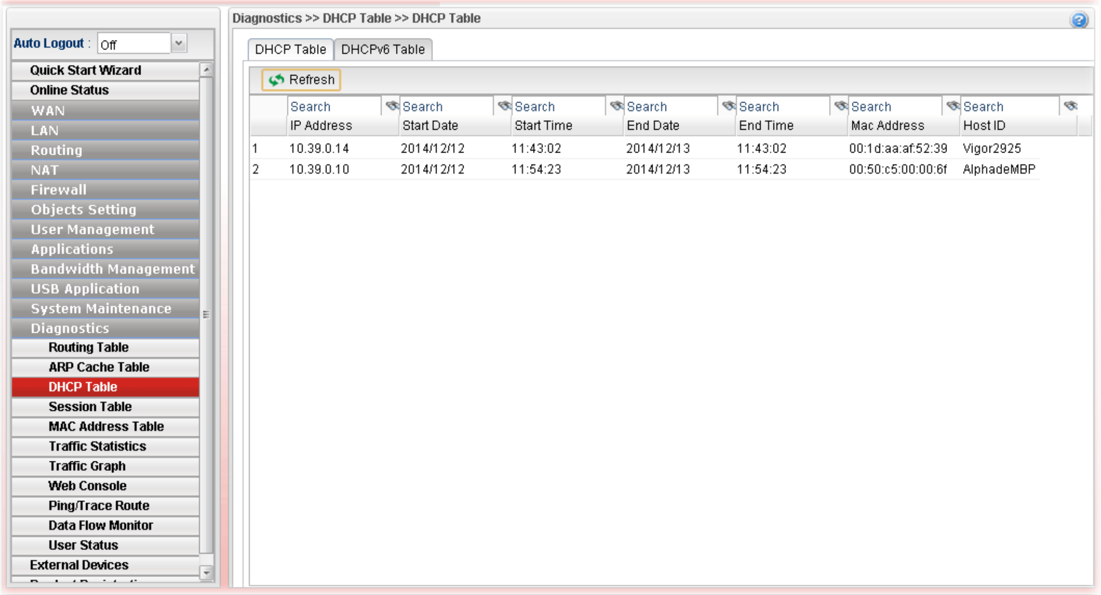
Item	Description
Status	Display the status for such neighbor. **INCOMPLETE -** Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. **REACHABLE -** The neighbor is reachable recently (within tens of seconds ago). **STALE-**The neighbor is no longer to be reachable. Yet, until traffic is sent to the neighbor, no attempt should be made to verify its reachability. **DELAY -** The neighbor is no longer to be reachable, and the traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, delay sending probes for a short while in order to give upper layer protocols a chance to provide reachability confirmation. **PROBE -** The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

4.12.3 DHCP Table

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

4.12.3.1 DHCP Table

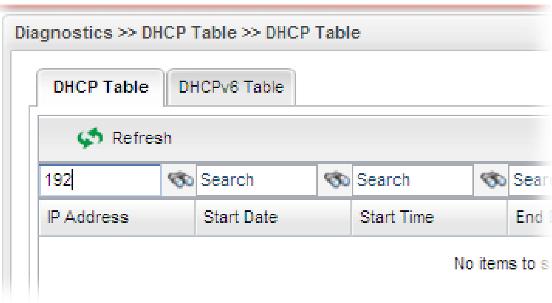
Click **Diagnostics** and click **DHCP Table** to open the web page.



Diagnostics >> DHCP Table >> DHCP Table

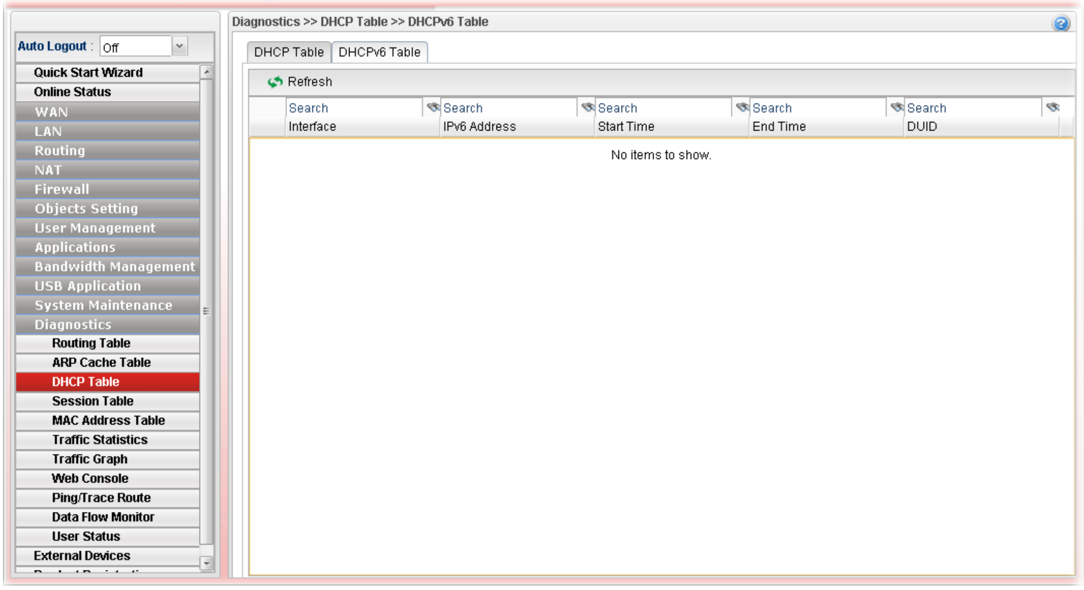
	IP Address	Start Date	Start Time	End Date	End Time	Mac Address	Host ID
1	10.39.0.14	2014/12/12	11:43:02	2014/12/13	11:43:02	00:1d:aa:af:52:39	Vigor2925
2	10.39.0.10	2014/12/12	11:54:23	2014/12/13	11:54:23	00:50:c5:00:00:6f	AlphadeMBP

Each item will be explained as follows:

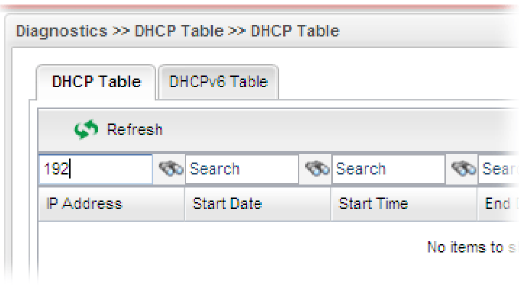
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> DHCP Table >> DHCP Table DHCP Table DHCPv6 Table Refresh 192 Search Search Sear IP Address Start Date Start Time End No items to s
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.

4.12.3.2 DHCPv6 Table

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

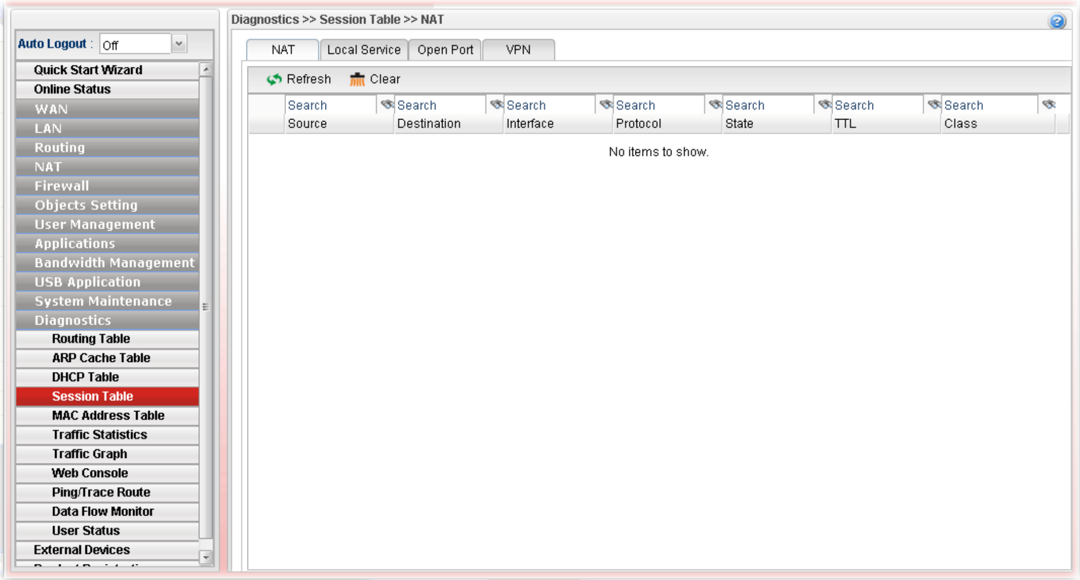


Each item will be explained as follows:

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 detailed information for DUID.

4.12.4 Session Table

This table can display about 30000 sessions with 20 pages.

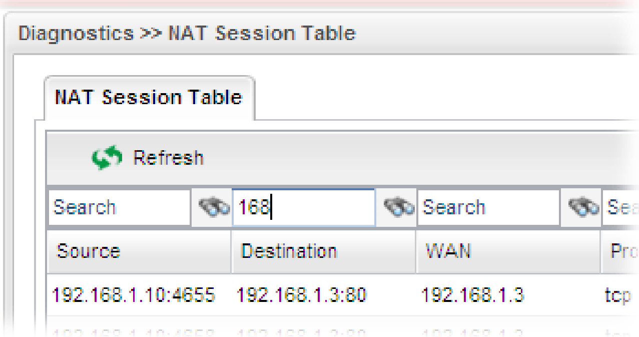


Diagnostics >> Session Table >> NAT

Source	Destination	Interface	Protocol	State	TTL	Class

No items to show.

Each item will be explained as follows:

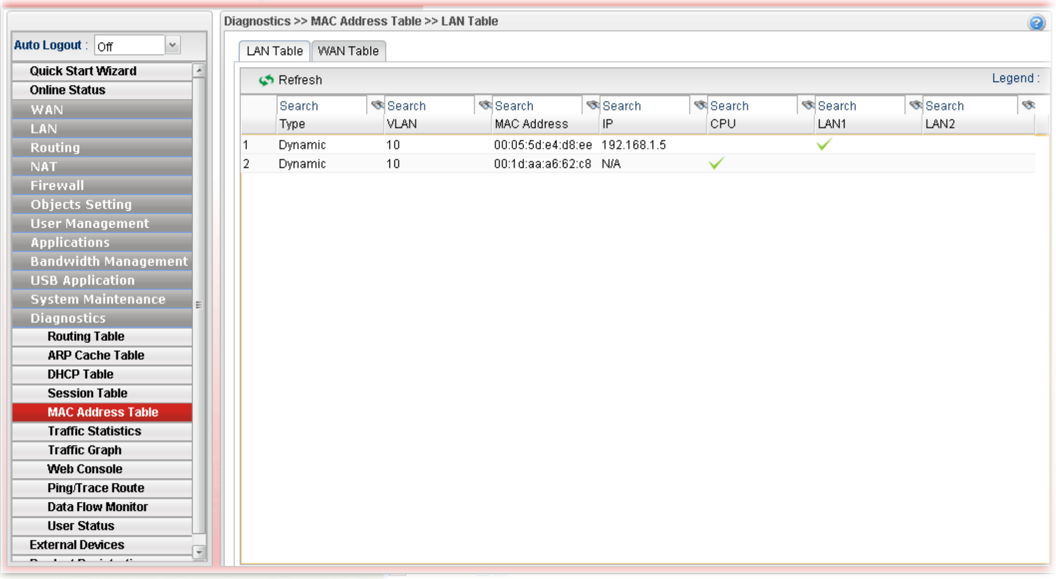
Item	Description
Refresh	Renew the web page.
Clear	Clear all of the information in this page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> NAT Session Table NAT Session Table Refresh Search · 168 · Search · Sea Source · Destination · WAN · Pro 192.168.1.10:4655 · 192.168.1.3:80 · 192.168.1.3 · tcp
Source	Display the source IP address and port of local PC.
Destination	Display the destination IP address and port of remote host.
Interface	Display the WAN IP address of the router.
Protocol	Display the protocol of such NAT session used.
State	Display the actual state of the TCP connection.
TTL	Display how long the conntrack entry has to live.

4.12.5 MAC Address Table

The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match.

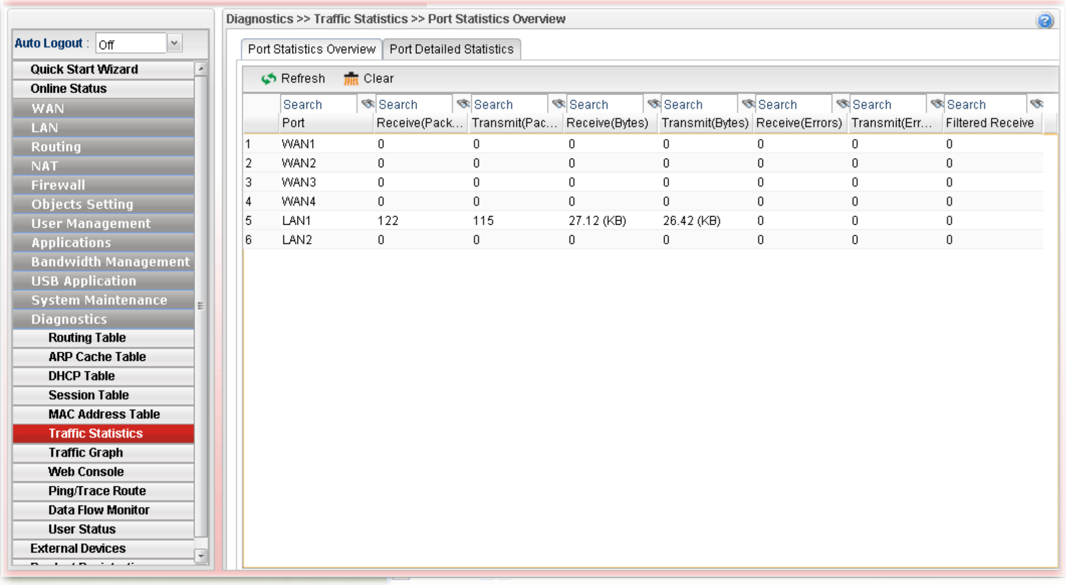


Diagnostics >> MAC Address Table >> LAN Table

	Type	VLAN	MAC Address	IP	CPU	LAN1	LAN2
1	Dynamic	10	00:05:5d:e4:d8:ee	192.168.1.5		✓	
2	Dynamic	10	00:1d:aa:a6:62:c8	N/A	✓		

4.12.6 Traffic Statistics

Port Statistics Overview offers an overview of general traffic statistics for all connecting ports.



Diagnostics >> Traffic Statistics >> Port Statistics Overview

	Port	Receive(Pack…	Transmit(Pac…	Receive(Bytes)	Transmit(Bytes)	Receive(Errors)	Transmit(Err…	Filtered Receive
1	WAN1	0	0	0	0	0	0	0
2	WAN2	0	0	0	0	0	0	0
3	WAN3	0	0	0	0	0	0	0
4	WAN4	0	0	0	0	0	0	0
5	LAN1	122	115	27.12 (KB)	26.42 (KB)	0	0	0
6	LAN2	0	0	0	0	0	0	0

Each item will be explained as follows:

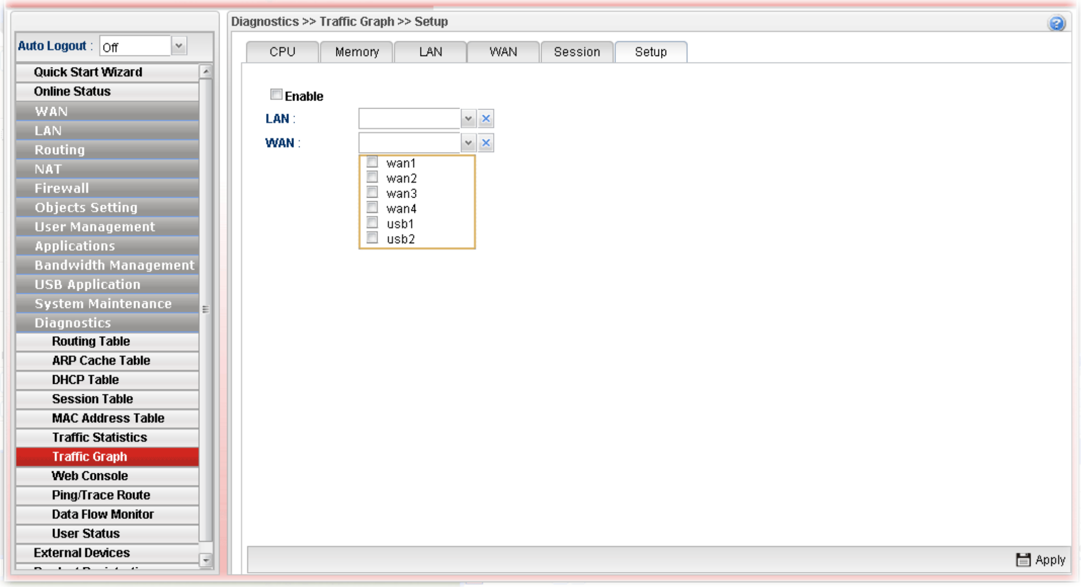
Item	Description

Refresh	Click it to reload the page.
Clear	Click it to clear the counters for all ports.
Port	Display the interface that data transmission passing through.
Receive/Transmit (Packets)	Display the packet sizes for data transmission in receiving and sending.
Receive/Transmit (Bytes)	Display the number of received and transmitted bytes per port.
Receive/Transmit (Error)	Display the number of the error occurred in data receiving and data sending.
Filtered Receive	Display the number of received frames filtered by the forwarding process.

Port Detailed Statistics displays detailed statistics for WAN/LAN interface.

4.12.7 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.



Diagnostics >> Traffic Graph >> Setup

☐ Enable

LAN :

WAN :

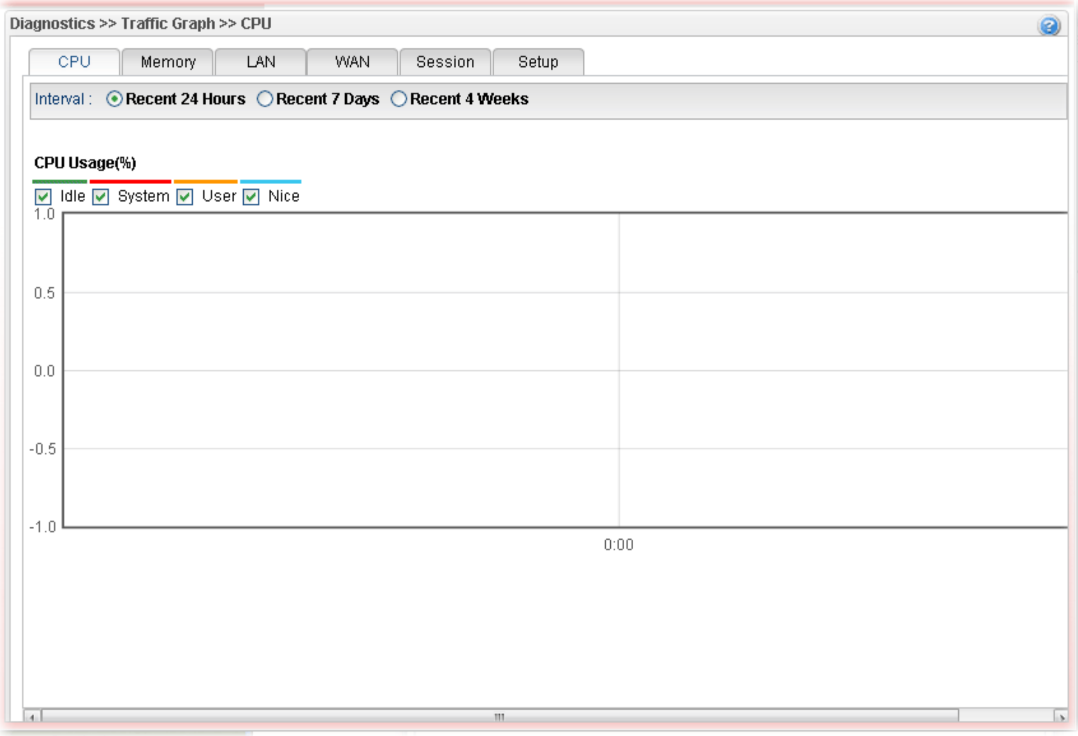
☐ wan1
☐ wan2
☐ wan3
☐ wan4
☐ usb1
☐ usb2

Each item will be explained as follows:

Item	Description
Setup	In this page, simply specify which LAN profile and WAN profile will be applied. The traffic graph will be drawn based on the profiles selected. **Enable** – Check this box to enable such profile. **LAN** – Use the drop down menu to choose a LAN profile. **WAN** –Use the drop down menu to choose a WAN profile. **Apply -** Click it to save the configuration configured under the Setup tab.
CPU	Click the CPU tab. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of CPU operation about recent 24 hours. **Recent 7 Days** – Display the information of CPU operation about recent 7 days. **Recent 4 Weeks** – Display the information of CPU operation about recent 4 weeks.
Memory	Click the Memory tab. There are three selections provided for you to specify. **Recent 24 Hours** – Display the information of memory operation about recent 24 hours. **Recent 7 Days** – Display the information of memory operation about recent 7 days. **Recent 4 Weeks** – Display the information of memory

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

Below show a graphic for CPU:



Diagnostics >> Traffic Graph >> CPU

Interval : ● Recent 24 Hours ○ Recent 7 Days ○ Recent 4 Weeks

CPU Usage(%)

☑ Idle ☑ System ☑ User ☑ Nice

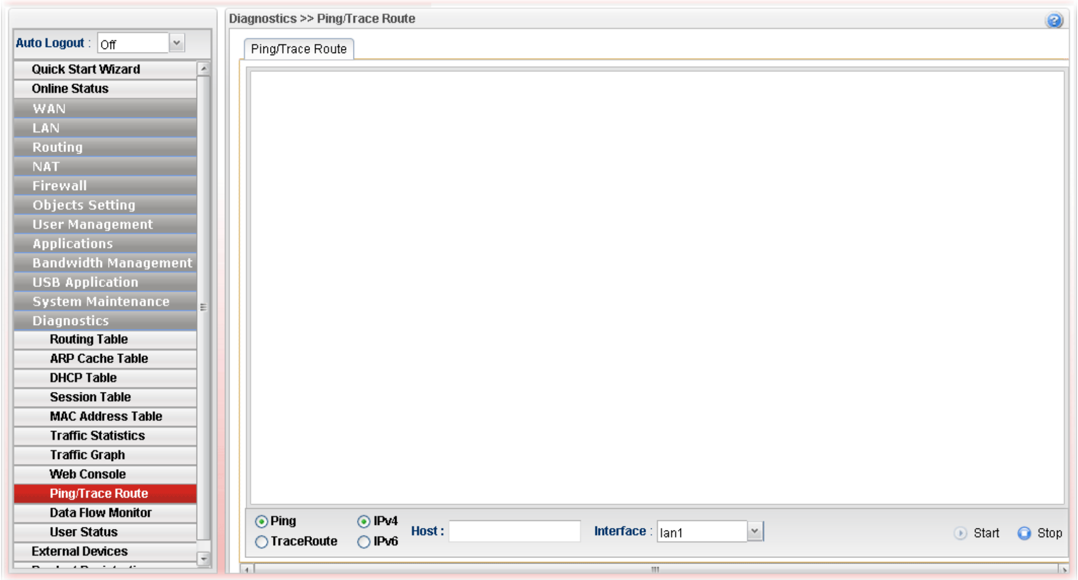
4.12.8 Web Console

Click **Diagnostics** and click **Web Console** to pen the web page for typing commands used in console connection. A remote user can operate Vigor300B from this web page without installing and opening other connection utility.

```
http://192.168.1.1/webshell/
login:
```

4.12.9 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.



Diagnostics >> Ping/Trace Route

Auto Logout : Off

● Ping ○ TraceRoute ● IPv4 ○ IPv6 Host : Interface : lan1

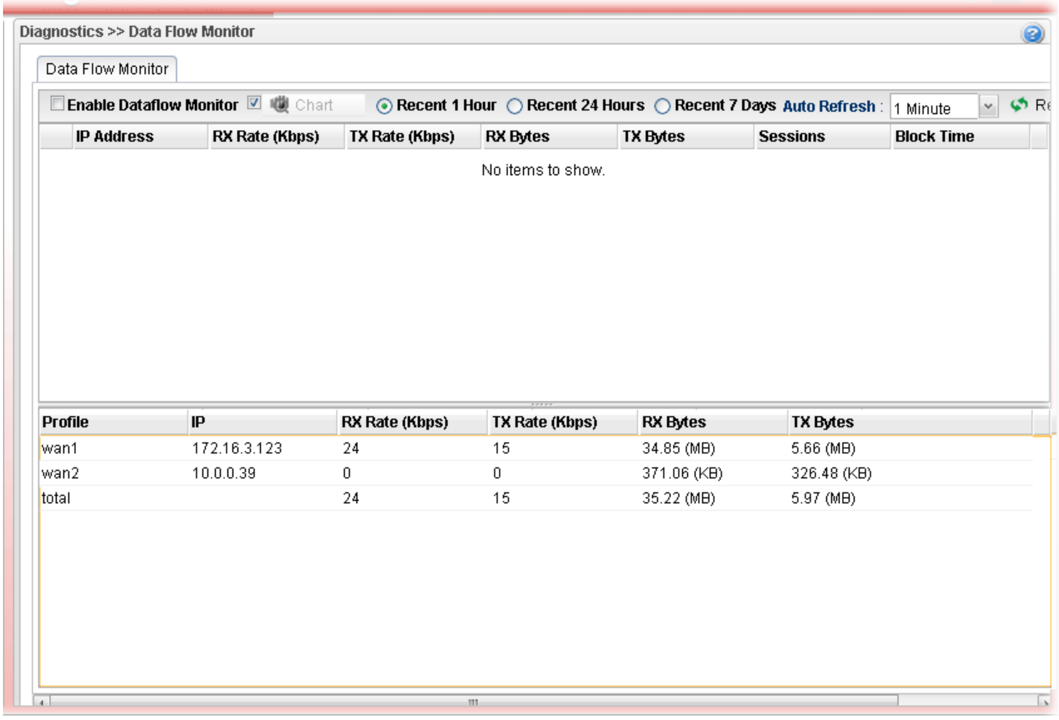
Each item will be explained as follows:

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.

4.12.10 Data Flow Monitor

This page displays the running procedure (such as IP address, session number, transmission rate, receiving rate, and duration of the time block) by list or by chart for the IP address monitored and refreshes the data in an interval of several seconds.

4.12.10.1 Data Flow Monitor



Diagnostics >> Data Flow Monitor

Data Flow Monitor

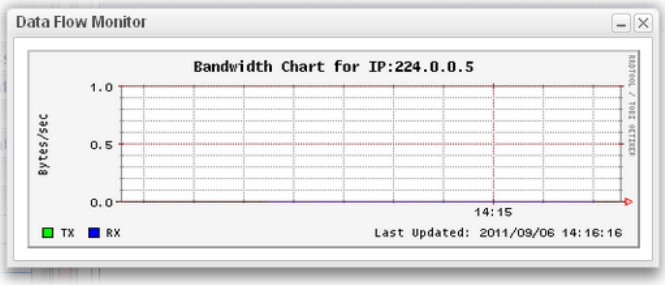
□ Enable Dataflow Monitor ☑ Chart ● Recent 1 Hour ○ Recent 24 Hours ○ Recent 7 Days Auto Refresh : 1 Minute Re

IP Address	RX Rate (Kbps)	TX Rate (Kbps)	RX Bytes	TX Bytes	Sessions	Block Time

No items to show.

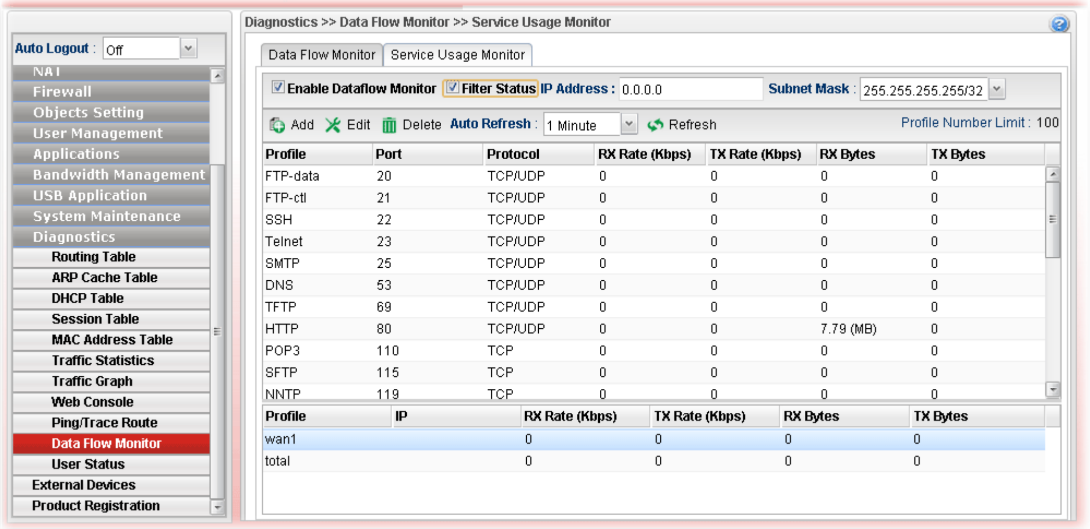
Profile	IP	RX Rate (Kbps)	TX Rate (Kbps)	RX Bytes	TX Bytes
wan1	172.16.3.123	24	15	34.85 (MB)	5.66 (MB)
wan2	10.0.0.39	0	0	371.06 (KB)	326.48 (KB)
total		24	15	35.22 (MB)	5.97 (MB)

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.  Data Flow Monitor Bandwidth Chart for IP:224.0.0.5 1.0 0.5 0.0 Bytes/sec 14:15 🟩 TX 🟦 RX Last Updated: 2011/09/06 14:16:16
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.
RX Rate (kbps)	Display the receiving speed of the monitored device.
TX Rate (kbps)	Display the transmission speed of the monitored device.
RX Bytes	Display the receiving file size of the monitored device.
TX Bytes	Display the transmitted file size 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(kbps)	Display the rate of data received.
TX Rate(kbps)	Display the rate of data transmitted.
RX Bytes	Display the file size of data received.
TX Bytes	Display the file size of data transmitted.

4.12.10.2 Service Usage Monitor



Diagnostics >> Data Flow Monitor >> Service Usage Monitor

☑ Enable Dataflow Monitor ☑ Filter Status IP Address : 0.0.0.0 Subnet Mask : 255.255.255.255/32

Auto Refresh : 1 Minute

Profile Number Limit : 100

Profile	Port	Protocol	RX Rate (Kbps)	TX Rate (Kbps)	RX Bytes	TX Bytes
FTP-data	20	TCP/UDP	0	0	0	0
FTP-ctl	21	TCP/UDP	0	0	0	0
SSH	22	TCP/UDP	0	0	0	0
Telnet	23	TCP/UDP	0	0	0	0
SMTP	25	TCP/UDP	0	0	0	0
DNS	53	TCP/UDP	0	0	0	0
TFTP	69	TCP/UDP	0	0	0	0
HTTP	80	TCP/UDP	0	0	7.79 (MB)	0
POP3	110	TCP	0	0	0	0
SFTP	115	TCP	0	0	0	0
NNTP	119	TCP	0	0	0	0

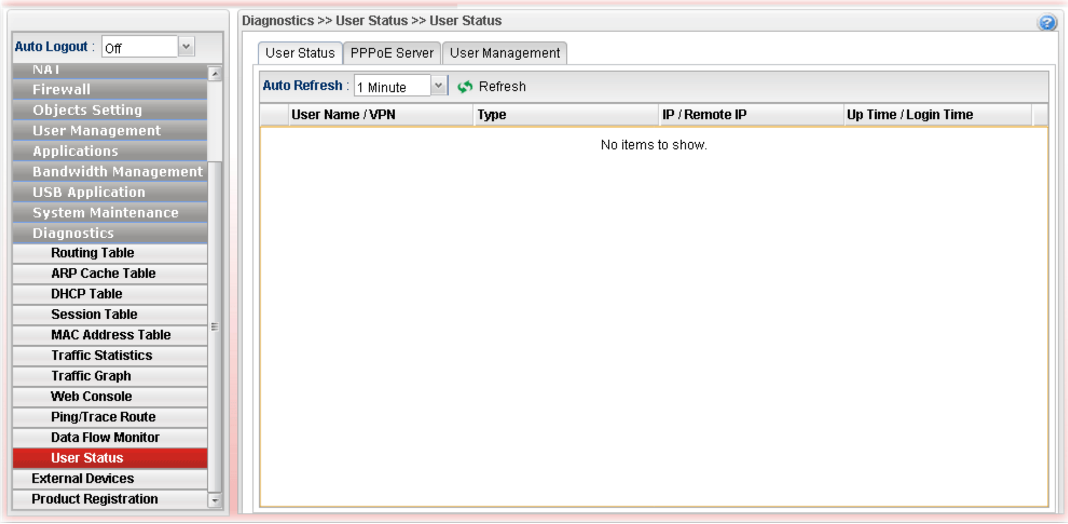
Profile	IP	RX Rate (Kbps)	TX Rate (Kbps)	RX Bytes	TX Bytes
wan1		0	0	0	0
total		0	0	0	0

Each item will be explained as follows:

Item	Description
Enable Dataflow Monitor	Check this box to enable such function.

4.12.11 User Status

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

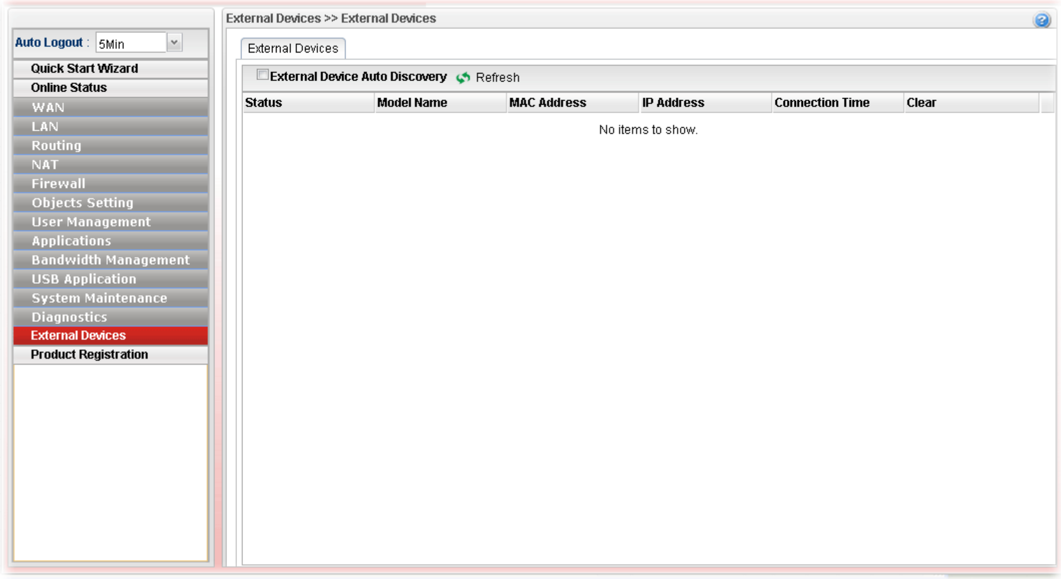


User Name / VPN	Type	IP / Remote IP	Up Time / Login Time

No items to show.

4.13 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.



External Devices >> External Devices

External Devices

□ External Device Auto Discovery   Refresh

Status	Model Name	MAC Address	IP Address	Connection Time	Clear

No items to show.

Each item will be explained as follows:

Item	Description
Enable External Devices	Check the box to detect the external device connected to Vigor300B.
Refresh	Click it to renew the web page.
Status	Display the status (on line or off line) of the external device.
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 Vigor300B.
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.

4.14 Product Registration

Please refer to section **2.3 Register Vigor Router** for more detailed information.

Chapter 5: Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

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

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check if the power line and WLAN/LAN cable connections is OK.
   If not, refer to "**1.3 Hardware Installation"** for reconnection.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.

3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

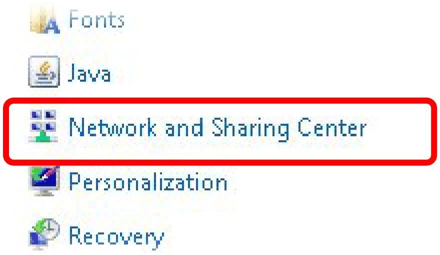
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

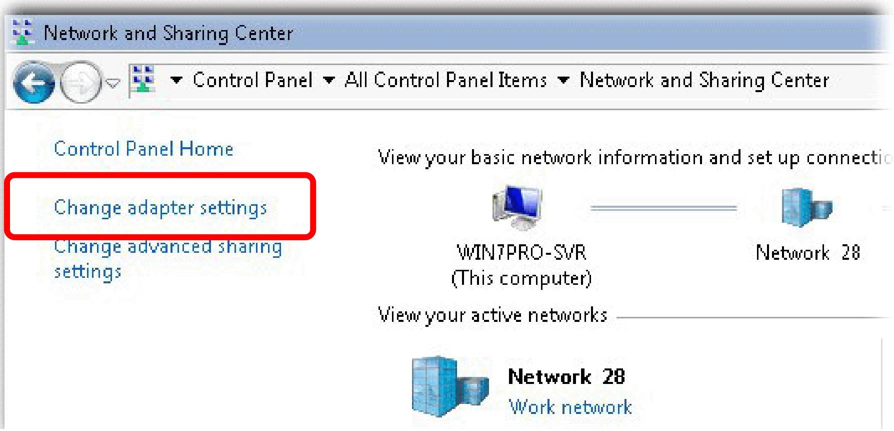
For Windows

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

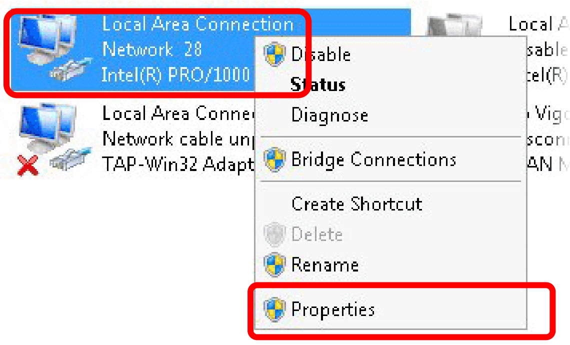
1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**



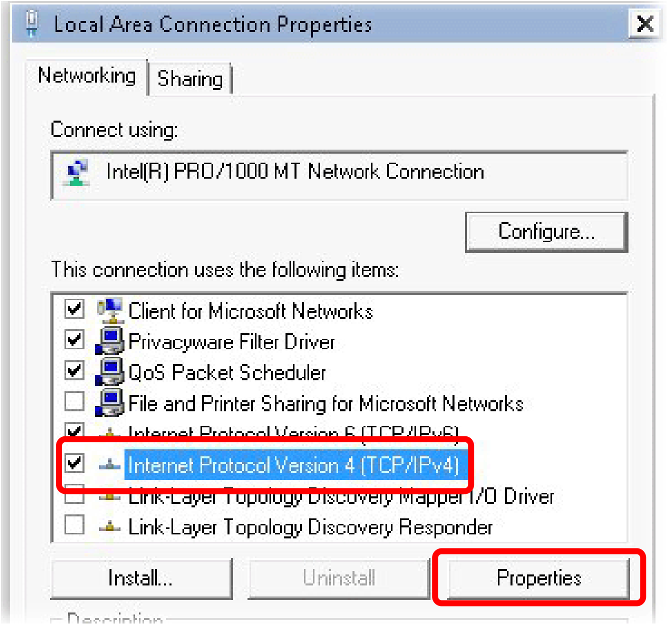
2. In the following window, click **Change adapter settings**.


Network and Sharing Center
Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connectio
WIN7PRO-SVR
(This computer)
Network 28
View your active networks
Network 28
Work network

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**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

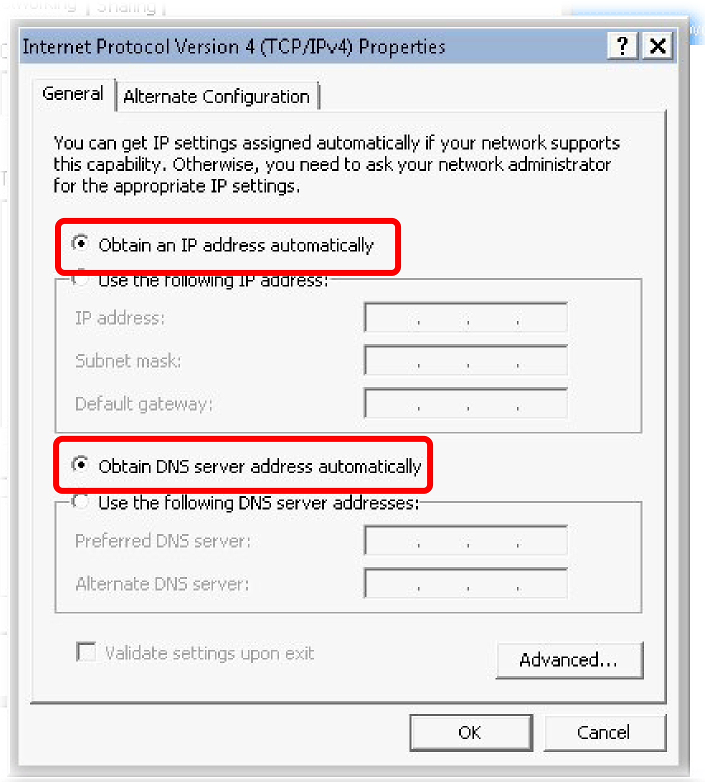
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Privacyware Filter Driver
- ☑ QoS Packet Scheduler
- □ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Link-Layer Topology Discovery Mapper I/O Driver
- □ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

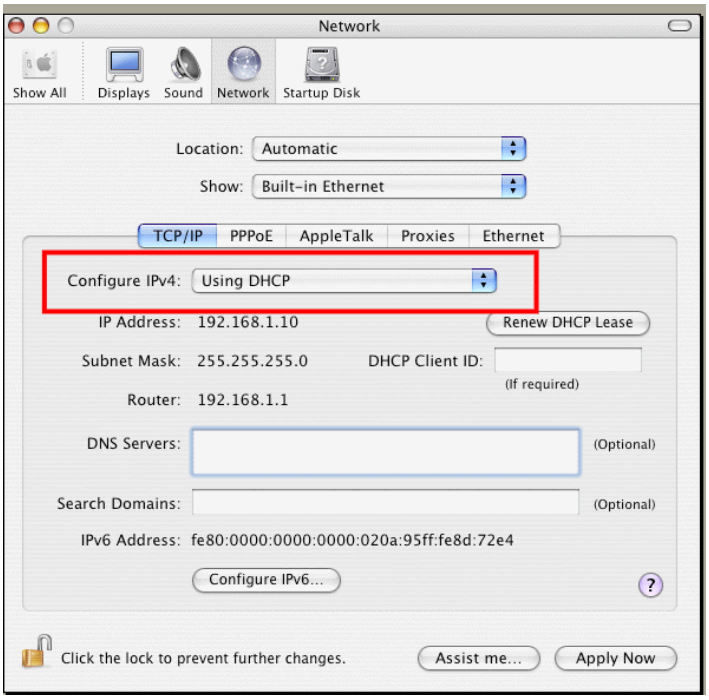
□ Validate settings upon exit

Advanced...

OK | Cancel

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.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

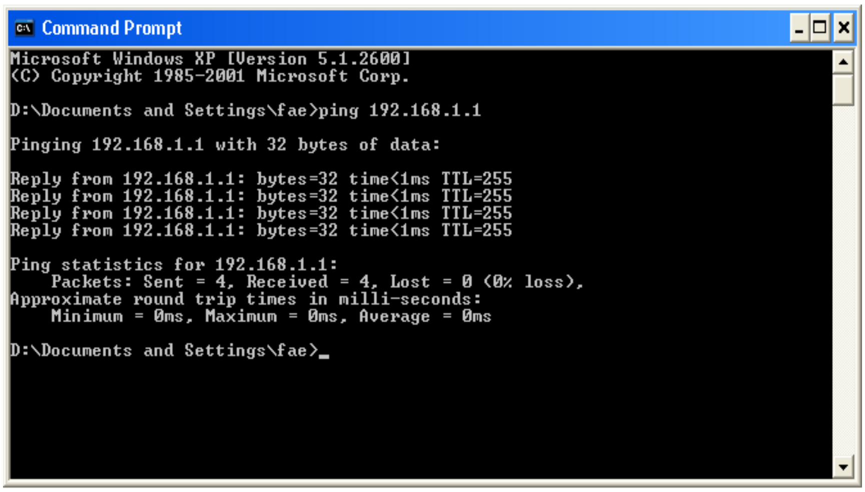
5.3 Pinging the Router from Your Computer

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.

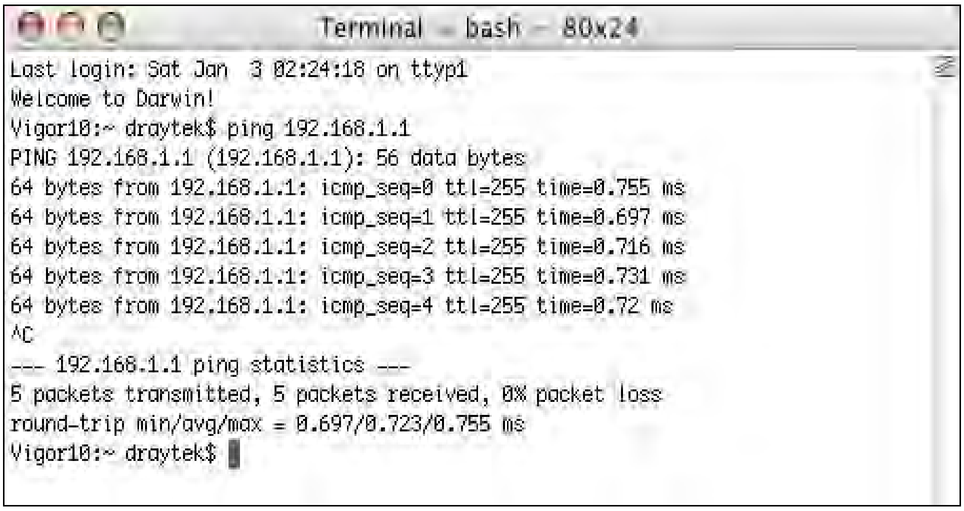


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

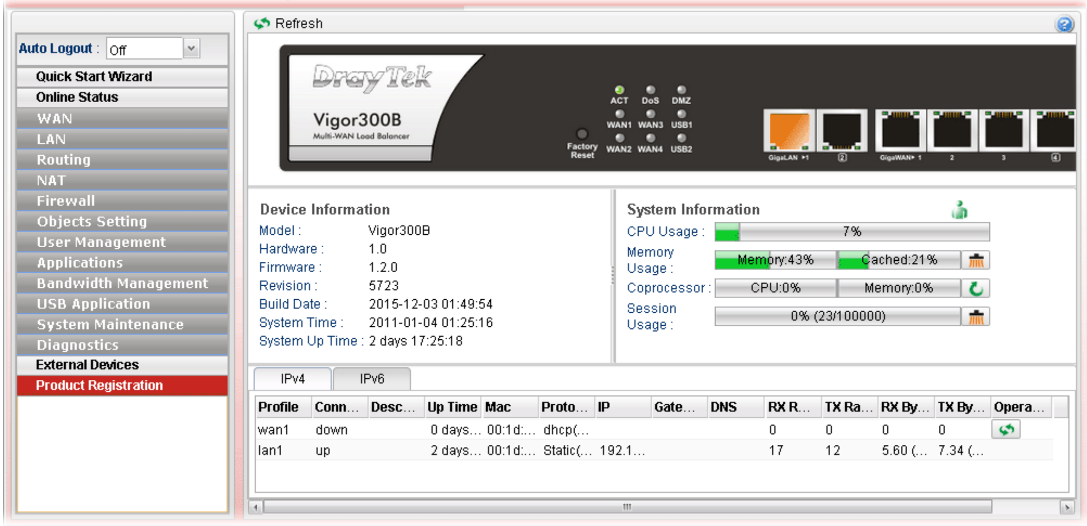
1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.



```
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$ 
```

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.



Device Information

Model : Vigor300B
Hardware : 1.0
Firmware : 1.2.0
Revision : 5723
Build Date : 2015-12-03 01:49:54
System Time : 2011-01-04 01:25:16
System Up Time : 2 days 17:25:18

System Information

CPU Usage : 7%
Memory Usage : Memory:43% Cached:21%
Coprocessor : CPU:0% Memory:0%
Session Usage : 0% (23/100000)

IPv4 | IPv6

Profile	Conn...	Desc...	Up Time	Mac	Proto...	IP	Gate...	DNS	RX R...	TX Ra...	RX By...	TX By...	Opera...
wan1	down		0 days...	00:1d:...	dhcp(...				0	0	0	0	
lan1	up		2 days...	00:1d:...	Static(...	192.1...			17	12	5.60 (...	7.34 (...	

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

5.5 Backing to Factory Default Setting If Necessary

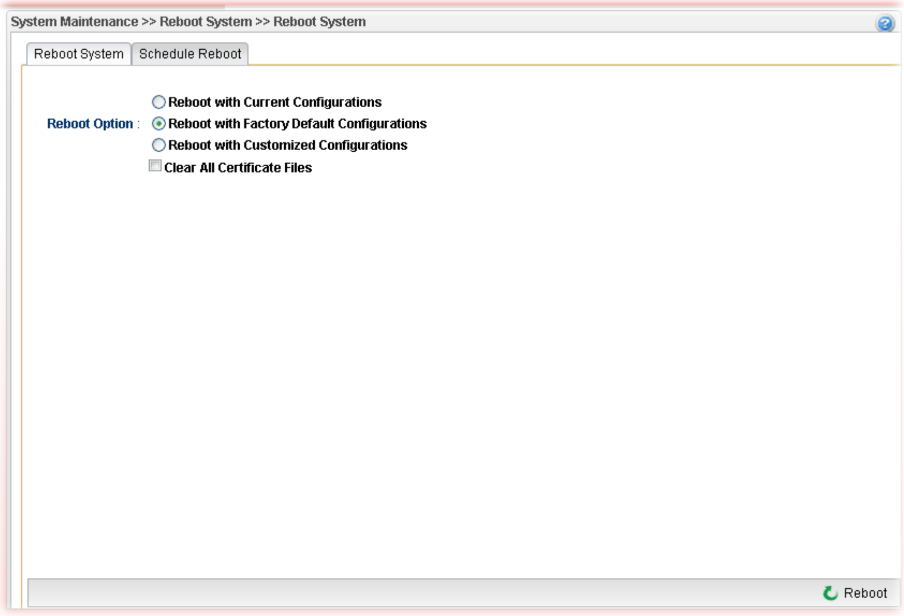
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of the factory default is null.

Software Reset

You can reset router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Reboot with Factory Default Configuration** and click **Reboot**. After few seconds, the router will return all the settings to the factory settings.

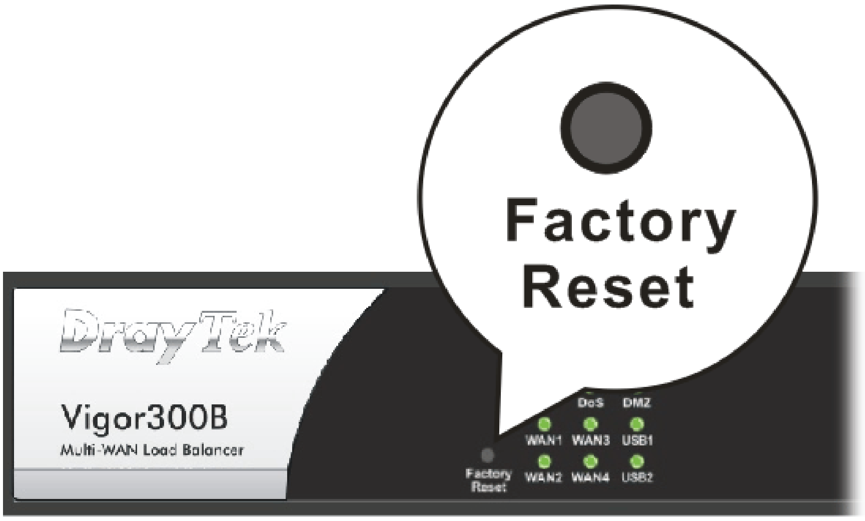


System Maintenance >> Reboot System >> Reboot System

Reboot Option : ○ Reboot with Current Configurations
● Reboot with Factory Default Configurations
○ Reboot with Customized Configurations
□ Clear All Certificate Files

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**.