DrayTek

Vigor3900

Multi-WAN Security Appliance

Providing Productivity and Security for
Small, Medium and Large Businesses

Your reliable networking solutions partner

User's Guide

V1.5

TAIWAN EXCELLENCE 2012

Vigor3900
Multi-WAN Security Appliance
User's Guide

Version: 1.5

Firmware Version: V1.0.5

(For future update, contact DrayTek)

Date: 30/08/2012

Copyright Information

Copyright Declarations

Copyright 2012 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista 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: Vigor3900

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

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

Please visit http://www.draytek.com/user/SupportDLRTTECE.php

Table of Contents

Chapter 1: Preface 1

1.1 Web Configuration Buttons Explanation 1

1.2 LED Indicators and Connectors 1

1.3 Hardware Installation 4

1.3.1 Network Connection 4
1.3.2 Rack-Mounted Installation 5

Chapter 2: Initialing Settings 7

2.1 Changing Password 7

2.2 Quick Start Wizard 9

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

2.3 Register Vigor Router 18

Chapter 3: Application and Tutorial 21

3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21

3.2 How to Configure OSPF? 27

3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33

3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36

3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41

3.6 How to Setup 50 WANs on Vigor3900 50

Chapter 4: Advanced Web Configuration 55

4.1 WAN Setup 55

4.1.1 General Setup 56
4.1.2 Default Route 70
4.1.3 Load Balance Policy 71
4.1.4 Switch 78

4.2 LAN 83

4.2.1 General Setup 83
4.2.2 IP Routing 97
4.2.3 Static Route 99
4.2.4 Switch 105
4.2.5 Bind IP to MAC 111
4.2.6 RIP Configuration 114
4.2.7 OSPF Configuration 115

4.3 NAT 118

4.3.1 Port Redirection 118
4.3.2 DMZ Host 122
4.3.3 Address Mapping 125
4.3.4 SIP ALG 128

4.4 Firewall 129
4.4.1 Filter Setup 129
4.4.2 DoS Defense 143
4.4.3 MAC Block 146
4.5 Objects Setting 148
4.5.1 IP Object 149
4.5.2 IP Group 152
4.5.3 Service Type Object 154
4.5.4 Service Type Group 157
4.5.5 Keyword Object 159
4.5.6 Keyword Group 161
4.5.7 File Extension Object 163
4.5.8 IM Object 166
4.5.9 P2P Object 169
4.5.10 Protocol Object 171
4.5.11 Web Category Object 173
4.5.12 Time Object 178
4.5.13 Time Group 181
4.6 User Management 183
4.6.1 General Setup 183
4.6.2 User Profile 186
4.6.3 User Group 190
4.6.4 RADIUS 192
4.6.5 LDAP/Active Directory 193
4.7 Application 194
4.7.1 Dynamic DNS 194
4.7.2 GVRP 198
4.7.3 UPnP 199
4.7.4 High Availability 201
4.7.5 Wake on LAN 204
4.8 VPN and Remote Access 205
4.8.1 VPN Client Wizard 205
4.8.2 VPN Server Wizard 211
4.8.3 Remote Access Control 216
4.8.4 PPP General Setup 216
4.8.5 IPSec General Setup 218
4.8.6 VPN Profiles 219
4.8.7 VPN Trunk Management 230
4.8.8 Connection Management 236
4.9 Certificate Management 237
4.9.1 Local Certificate 238
4.9.2 Trusted Certificate 241
4.9.3 Remote Certificate 244
4.10 SSL VPN 245
4.10.1 SSL Web Proxy 245
4.10.2 SSL Application 247
4.10.3 Online User Status 251
4.11 Bandwidth Management 252
4.11.1 Incoming Class 253
4.11.2 Incoming Filter 256
4.11.3 Outgoing Class 259
4.11.4 Outgoing Filter 264

4.11.5 Sessions Limit....267
4.11.6 Bandwidth Limit....269
4.12 System Maintenance....272
4.12.1 TR-069....272
4.12.2 Administrator Password....273
4.12.3 Configuration Backup....274
4.12.4 Syslog / Mail Alert....276
4.12.5 Time and Date....279
4.12.6 Access Control....280
4.12.7 SNMP Setup....281
4.12.8 Reboot System....282
4.12.9 Firmware Upgrade....283
4.13 Diagnostics....284
4.13.1 Routing Table....284
4.13.2 ARP Cache Table....286
4.13.3 DHCP Table....288
4.13.4 NAT Session Table....289
4.13.5 Traffic Graph....290
4.13.6 Web Console....292
4.13.7 Ping/Trace Route....292
4.13.8 Data Flow Monitor....293
4.14 External Devices....294
4.15 Product Registration....295

Chapter 5: Trouble Shooting....297

5.1 Checking If the Hardware Status Is OK or Not....297
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not....298
5.3 Pinging the Router from Your Computer....300
5.4 Checking If the ISP Settings are OK or Not....301
5.5 Backing to Factory Default Setting If Necessary....302
5.6 Contacting Your Dealer....303

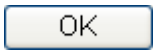
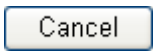
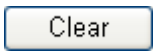
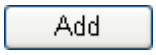
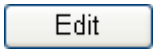
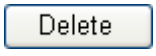
Chapter 1: Preface

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

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

1.1 Web Configuration Buttons Explanation

Several main buttons appeared on the web pages are defined as the following:

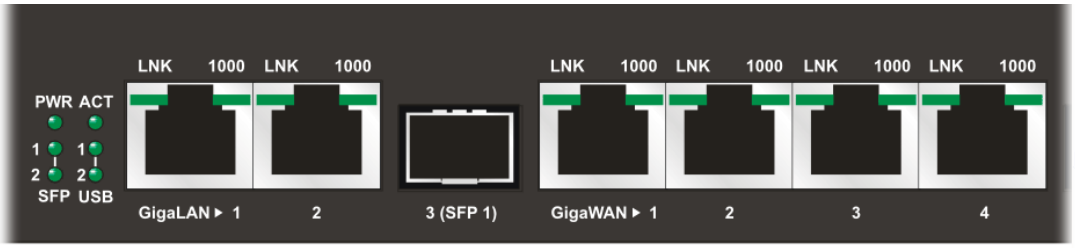
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the settings for the selected item.
	Delete the selected item with the corresponding settings.

Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.

1.2 LED Indicators and Connectors

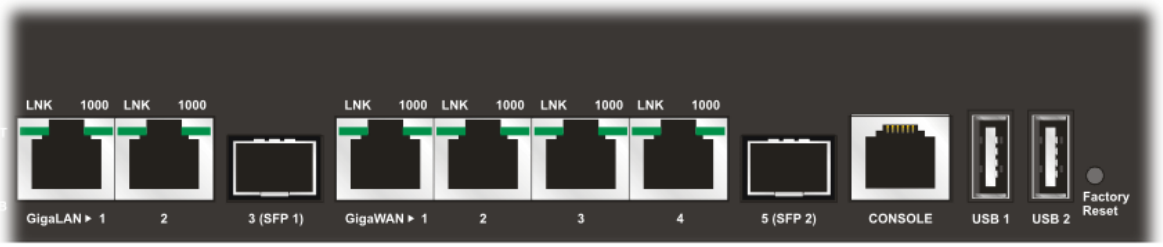
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

Description for LED



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

Connectors



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

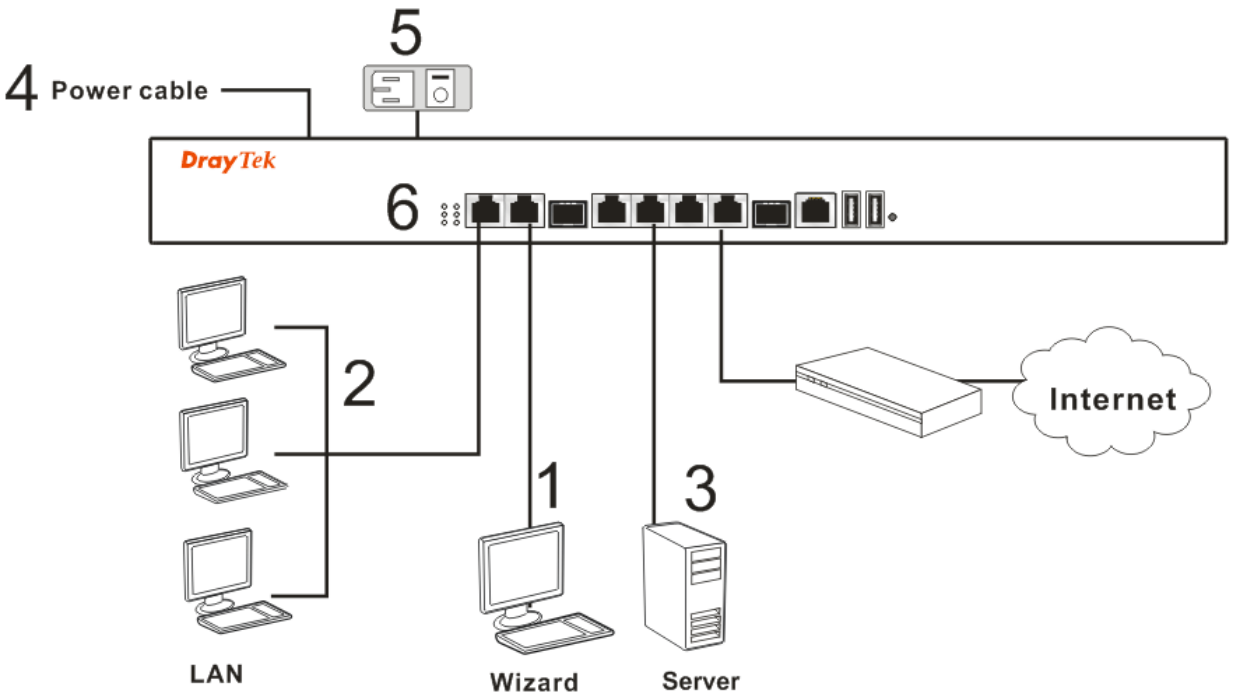
1.3 Hardware Installation

1.3.1 Network Connection

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

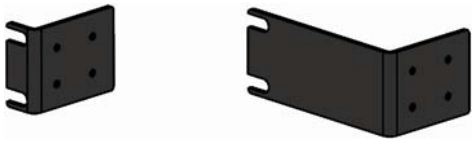
1. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of Vigor3900s.
2. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The **LAN** LED for that port on the front panel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

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

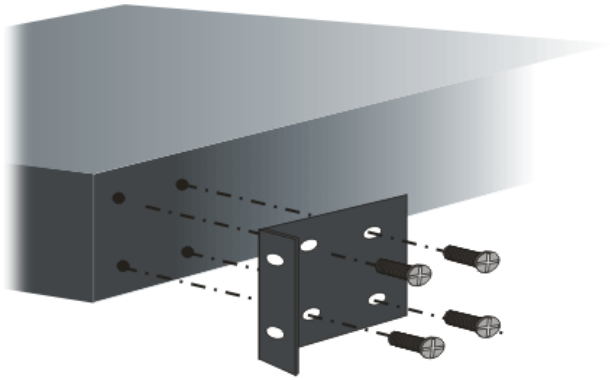


1.3.2 Rack-Mounted Installation

The Vigor3900 Series can be mounted on a rack by using standard brackets in a 19-inch rack or optional larger brackets on 23-inch rack (not included). The bracket for 19- and 23-inch racks are shown below.



Attach the brackets to the chassis of a 19- or a 23-inch rack. The second bracket attaches the other side of the chassis as above procedure.



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

Desktop Type Installation

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

This page is left blank.

Chapter 2: Initialing Settings

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

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

2.1 Changing Password

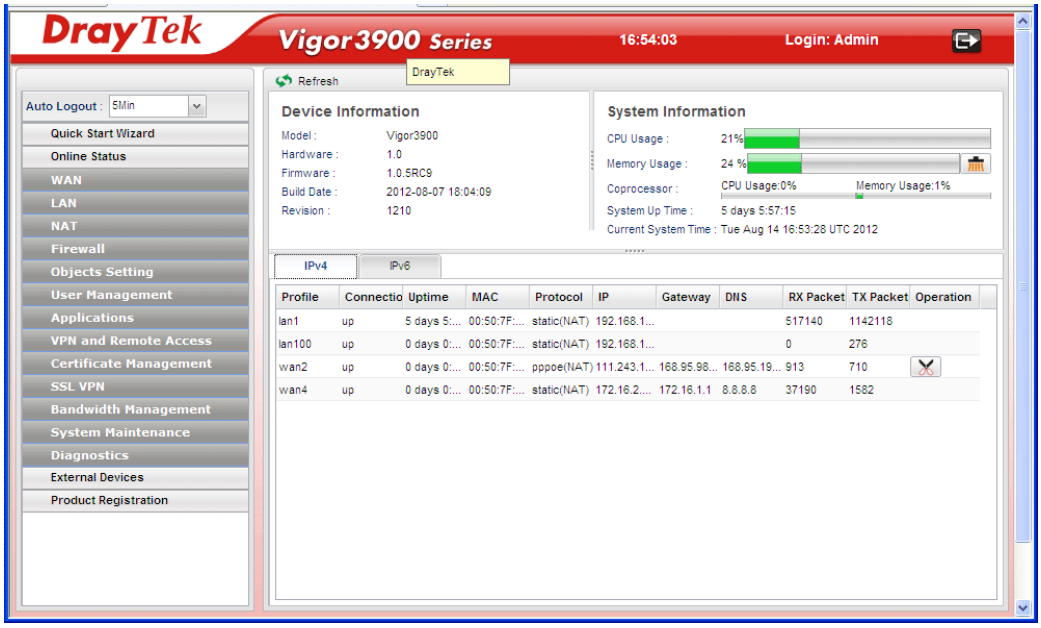
To change the password for this device, you have to access into the web browse with default password first.

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

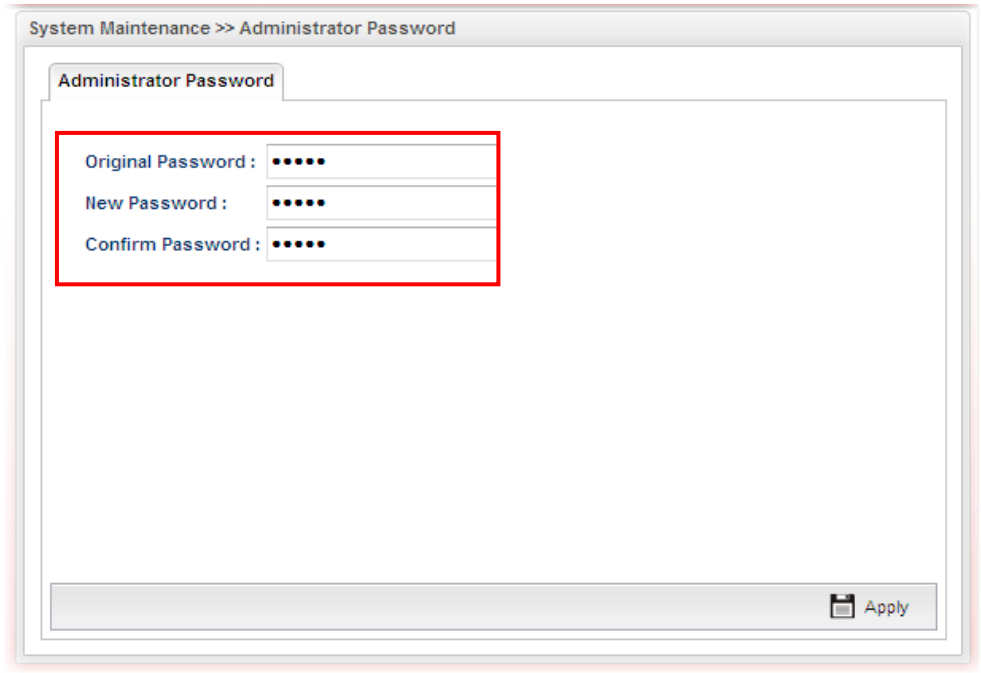
> **Notice:** You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of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

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

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



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



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

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

2.2 Quick Start Wizard

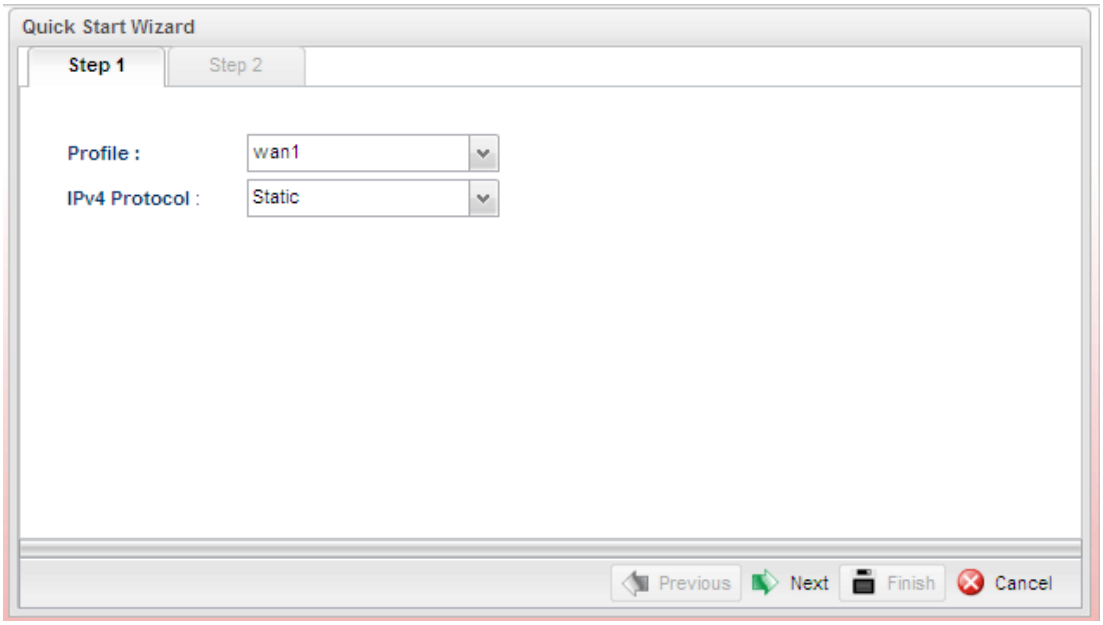
Quick Start Wizard is a wizard which is designed for configuring your router accessing Internet with simply steps. In the **Quick Start Wizard** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes.

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

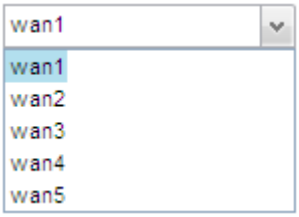
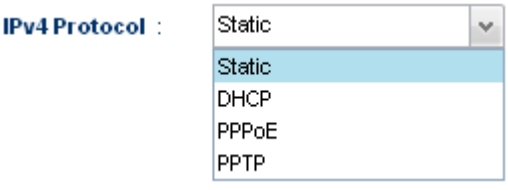
Click **Quick Start Wizard** from the home page. Quick Start Wizard will guide the user to establish LAN interface profile, WAN interface profile and select proper protocol for connection. The following will explain in more detail for the various broadband access configurations.

2.2.1 Step 1 - Specifying the WAN Profile

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



Available settings are explained as follows:

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

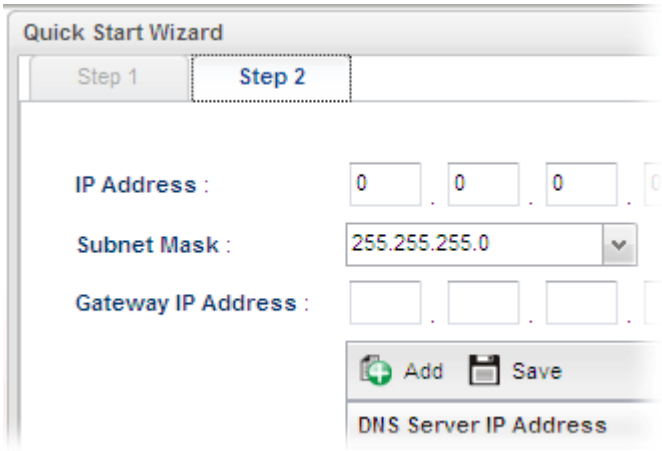
Item	Description
	Static - If **Static** is selected, you can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings. **DHCP** - It allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP**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

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

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

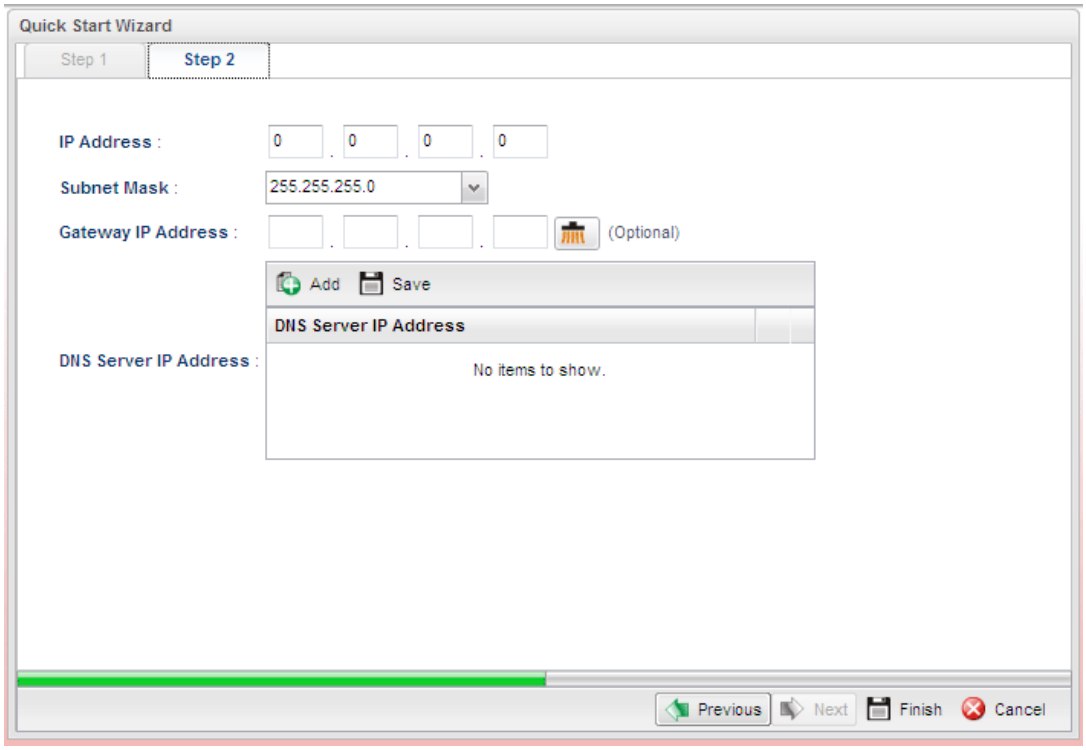
2.2.2 Step 2 - Configuring the Selected Protocol

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



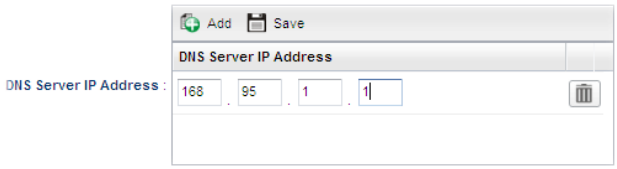
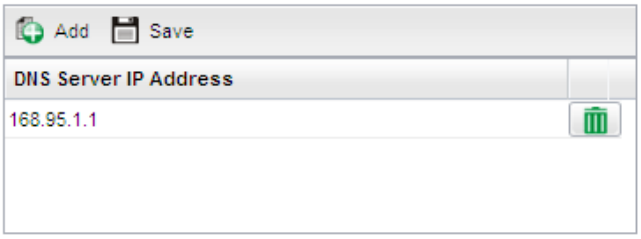
If Static is selected

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



Available parameters are listed as follows:

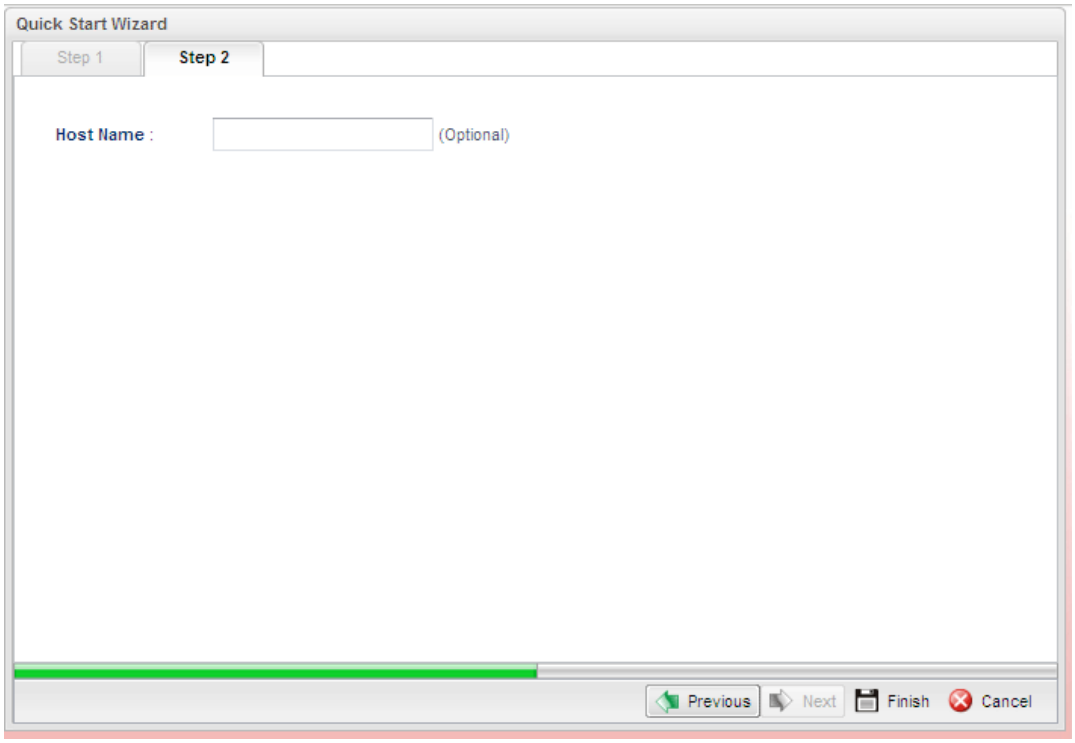
Item	Description
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile. - click it to remove the IP address if you are not satisfied with it.

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

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

If DHCP is selected

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for Vigor2960 automatically. It is not necessary for you to assign any setting. (Host Name is required for some ISPs).



Available parameters are listed as follows:

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

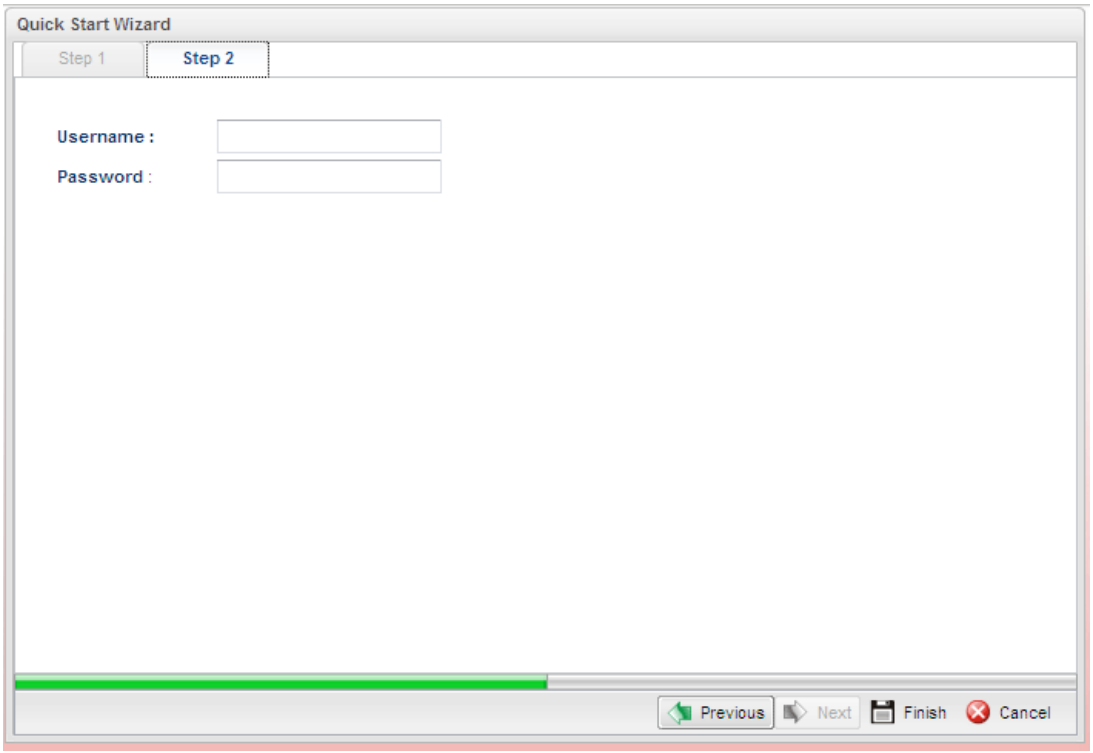
When you finished the above settings, please click **Finish**.

If PPPoE is selected

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

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

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



Available parameters are listed as follows:

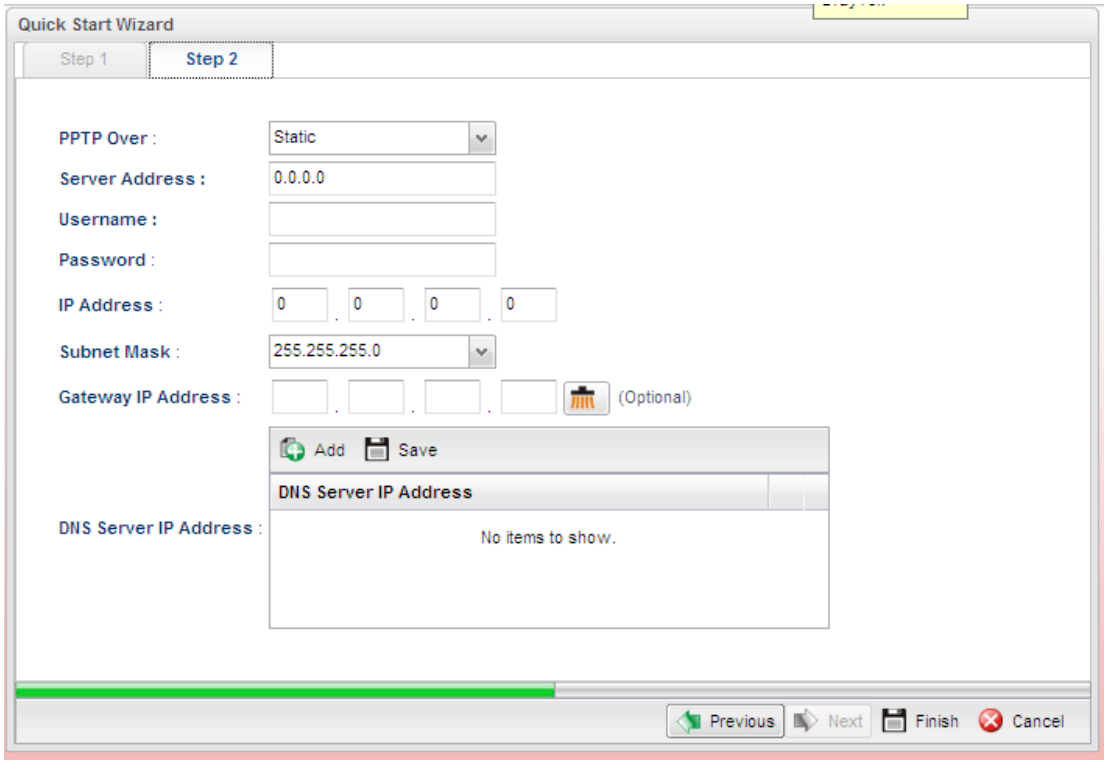
Item	Description
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

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

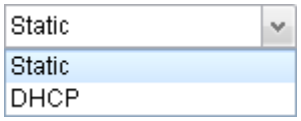
If PPTP is selected

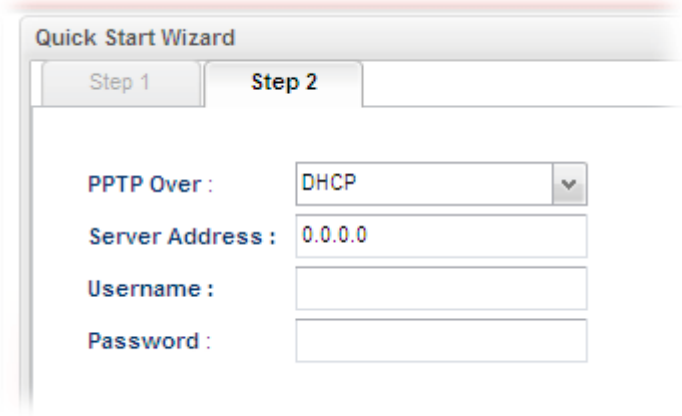
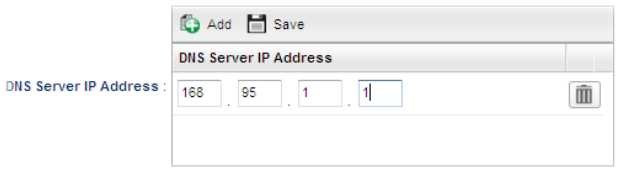
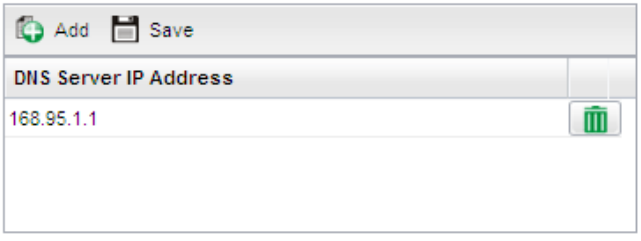
This mode lets user get the IP group information by a DSL modem with PPTP service from ISP. Your service provider will give you user name, password, and authentication mode for a PPTP setting. Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.

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

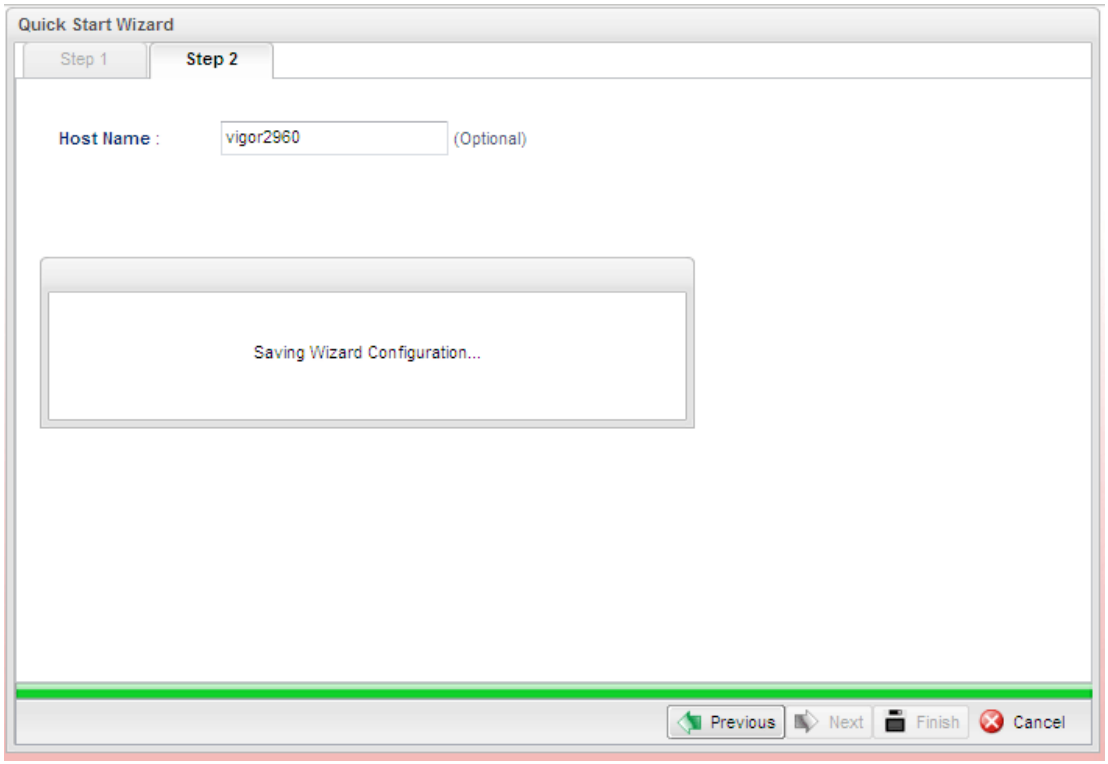


Available parameters are listed as follows:

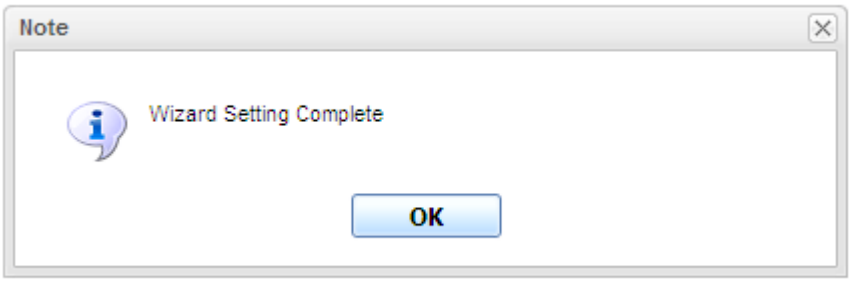
Item	Description
PPTP Over	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. **Please contact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

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

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



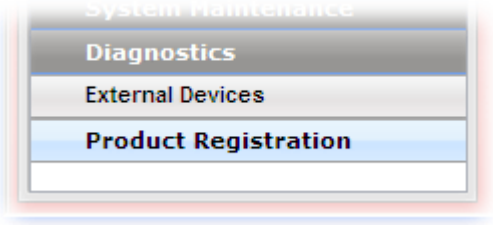
When the following screen appears, it means you have finished the Quick Start Wizard configuration.



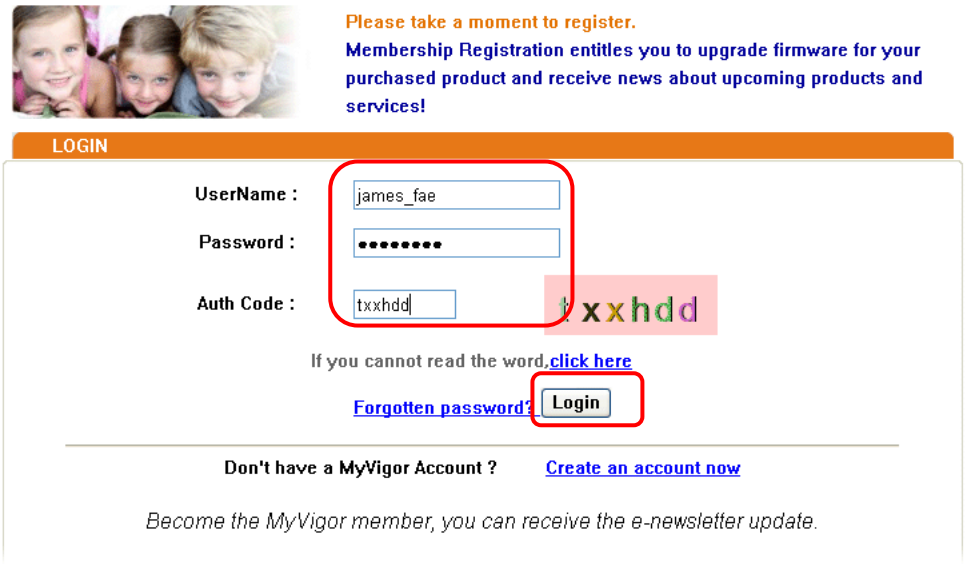
2.3 Register Vigor Router

Please follow the steps below to register the router.

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



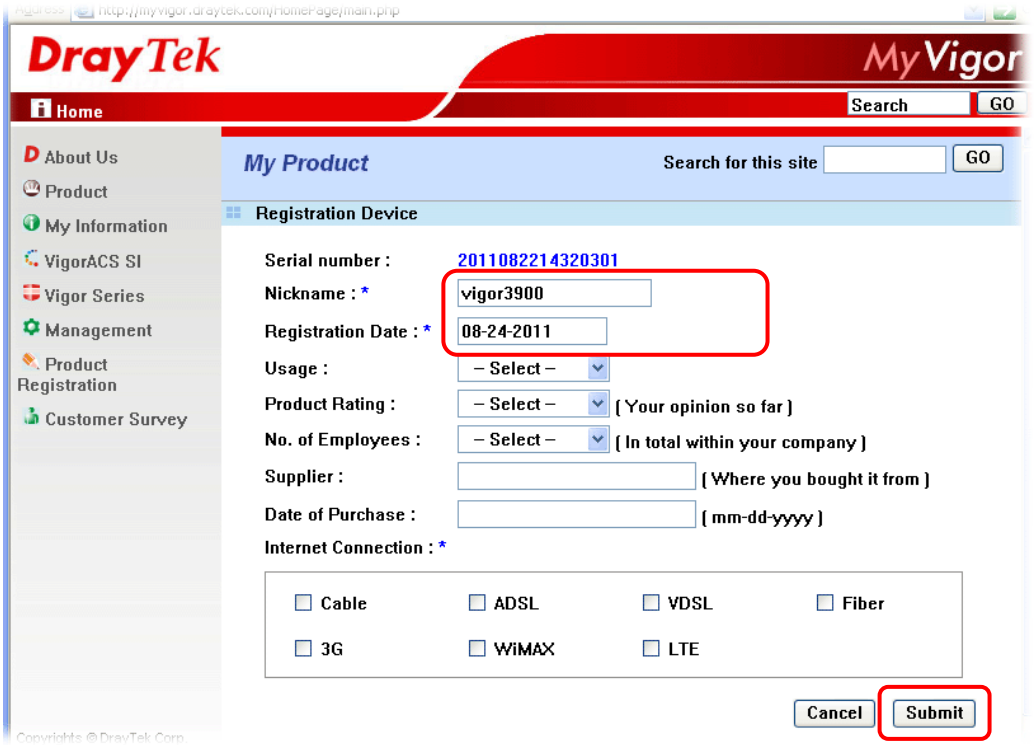
2 A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.



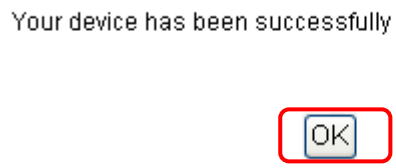
3 The following page will be displayed after you logging in MyVigor. From this page, please click **Add**.

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

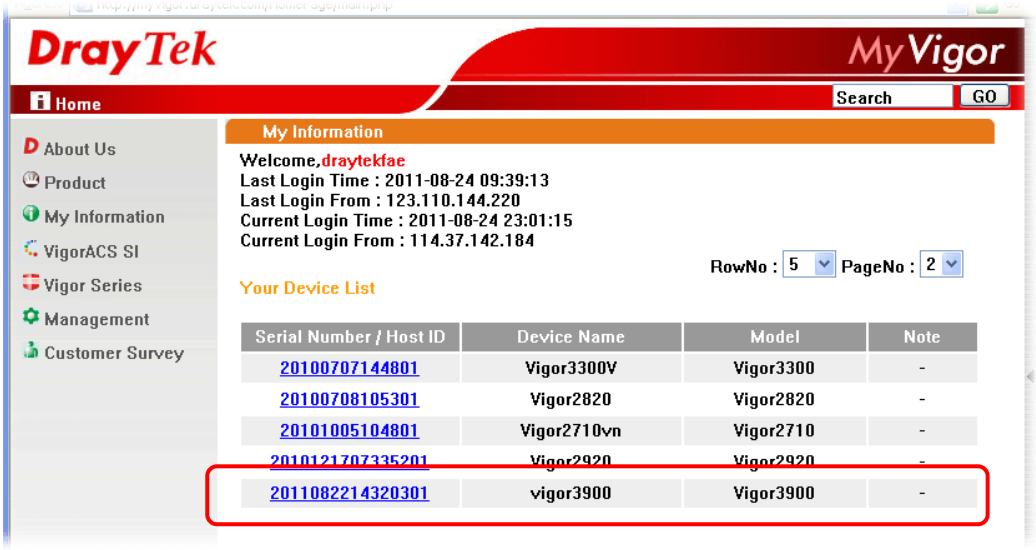
4 When the following page appears, please type in Nick Name (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.



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.



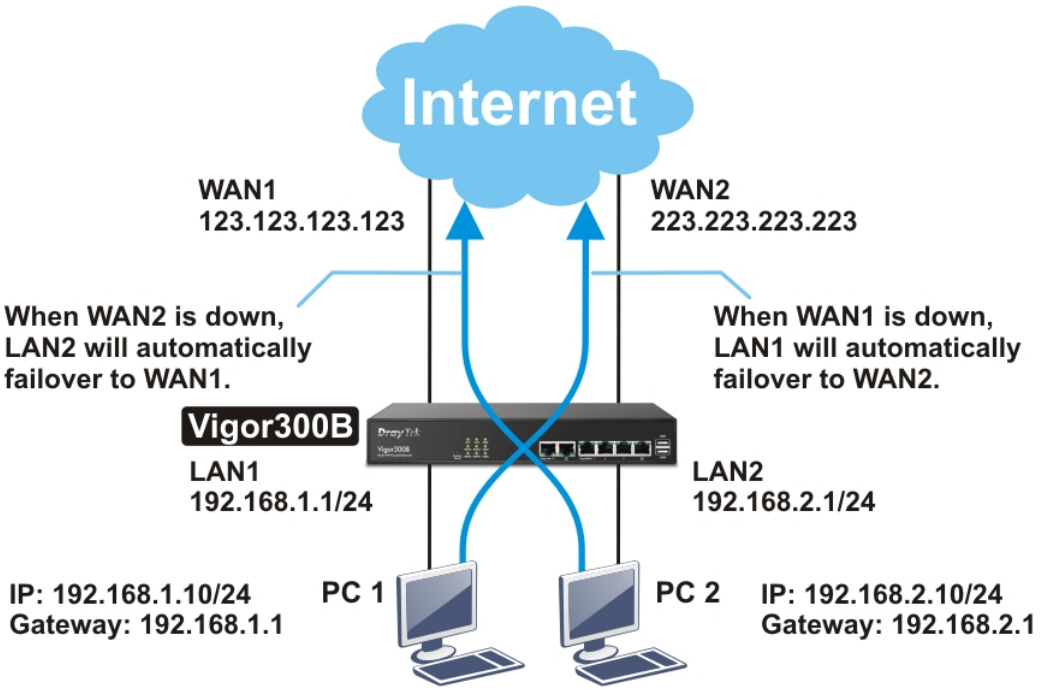
6 Take a look at the page of My Information, the new added Vigor3900 is listed under **Your Device List**.



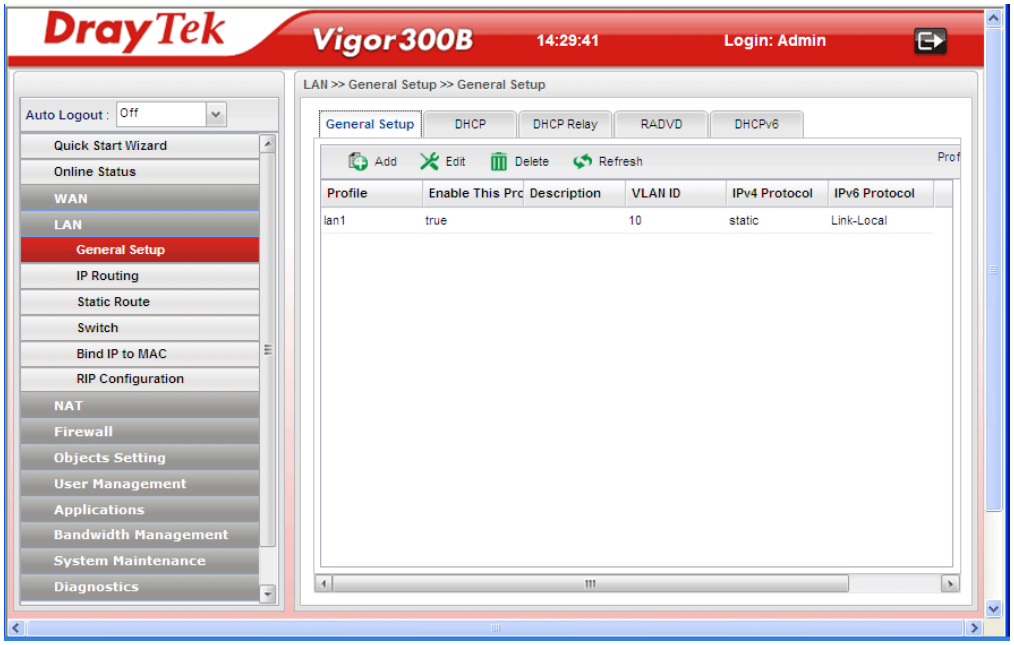
Chapter 3: Application and Tutorial

3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900?

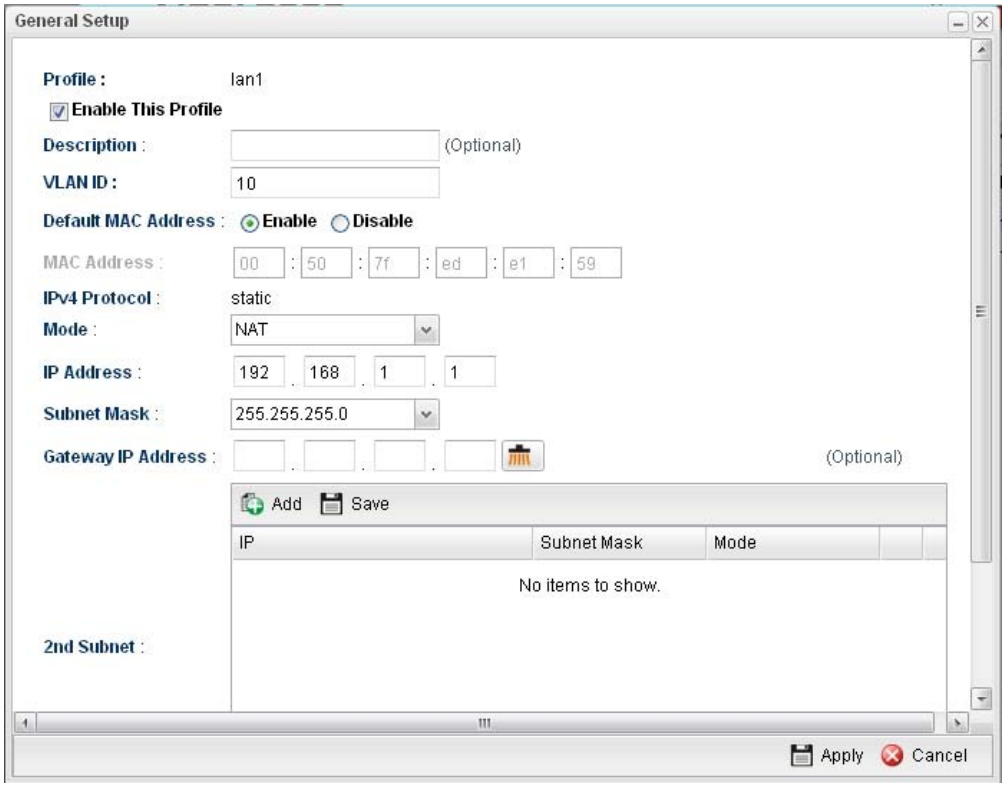
There are two different LANs configured in the following figure. One is for Sale (192.168.1.1/24) and the other is for FAE (192.168.2.1/24). Sale's LAN will be configured to go Internet always via WAN1. When WAN1 is down, Sale's LAN will automatically failover to WAN2. FAE's LAN will be configured to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



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

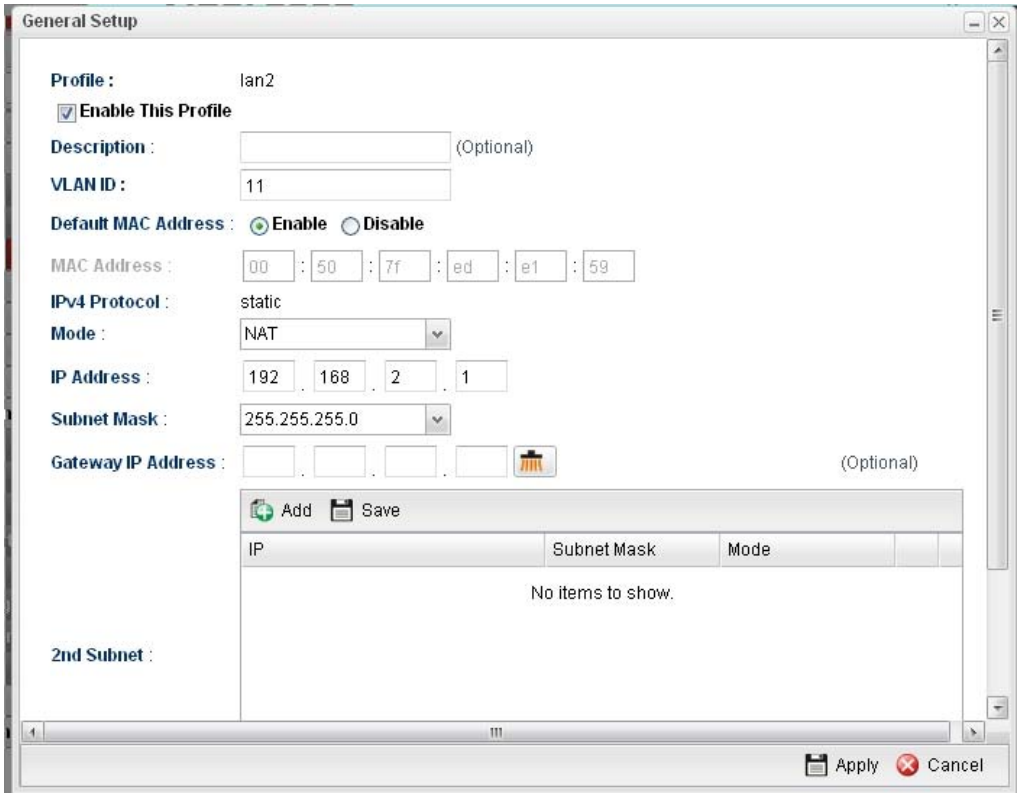


3. Click **Add** to open the following page.



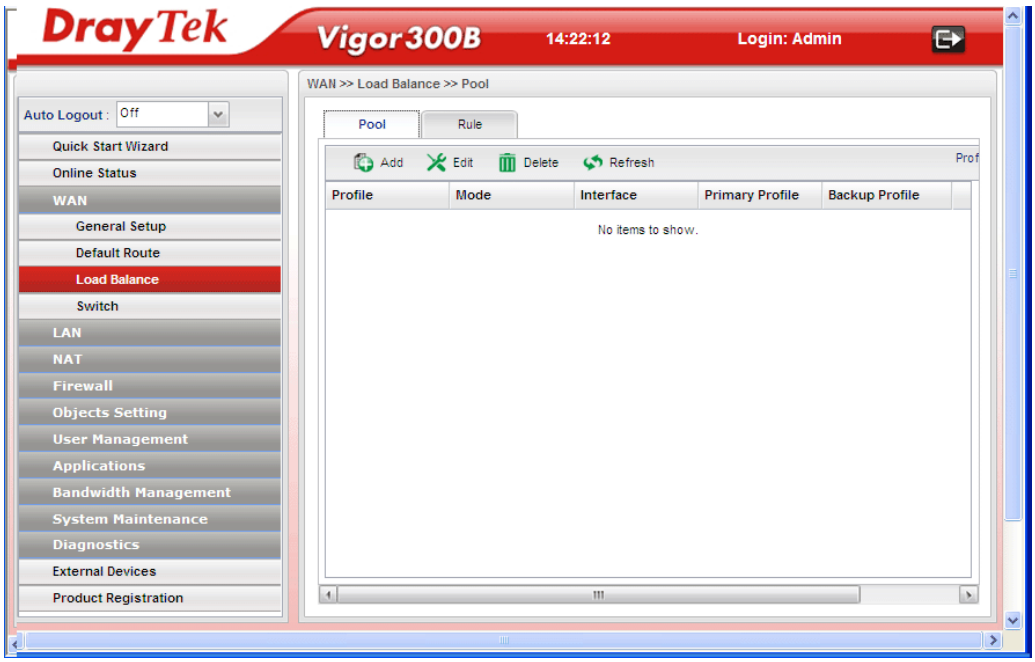
Type the information specified for LAN1 profile, then click **Apply** to save the settings and exit the screen.

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

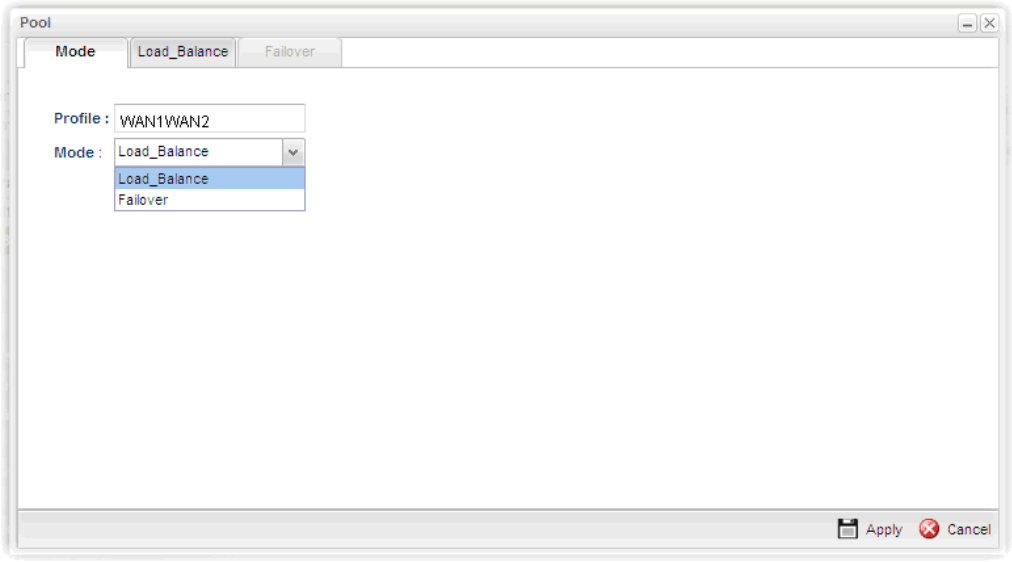


Type the information specified for LAN2 profile, then click **Apply** to save the settings and exit the screen.

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



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

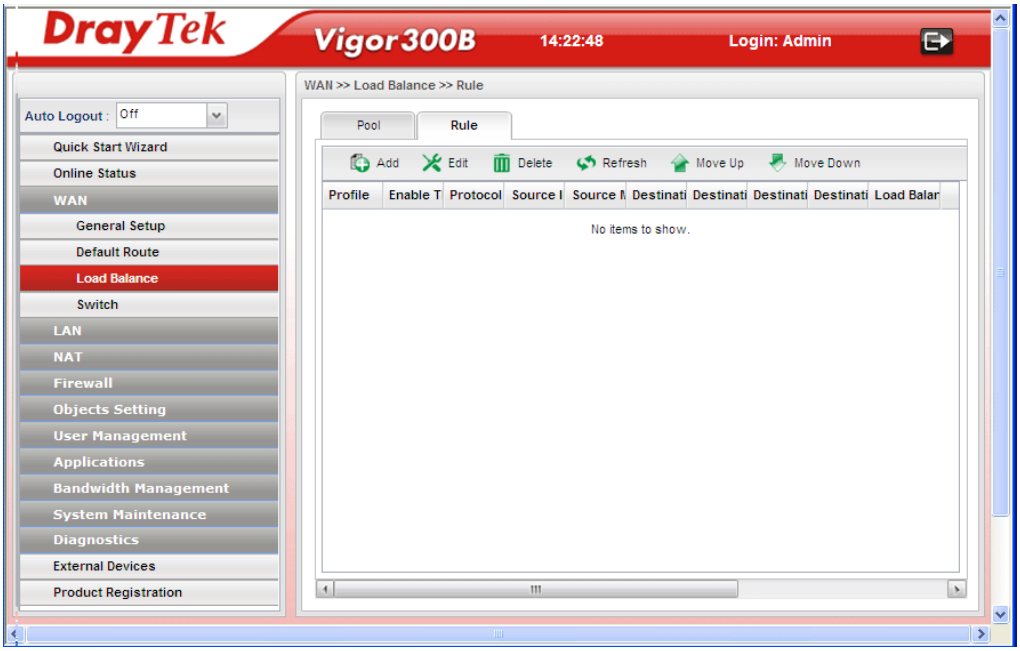


7. Click the **Load_Balance** tab to open the following page.

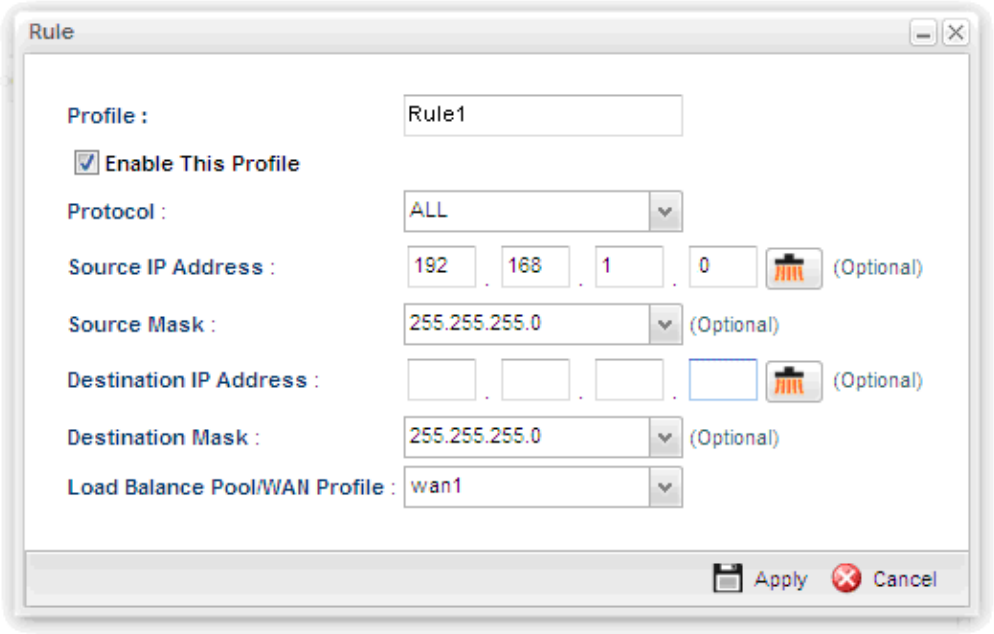
Setup the Weights (e.g, “1”) of WAN1 and WAN2 as you want. In this case ratio of WAN1 and WAN2 is 1:1. Also, you can type 2 and 1 for WAN1 and WAN2, then the ratio of line speed of WAN 1and line speed of WAN 2 will be 2:1.

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

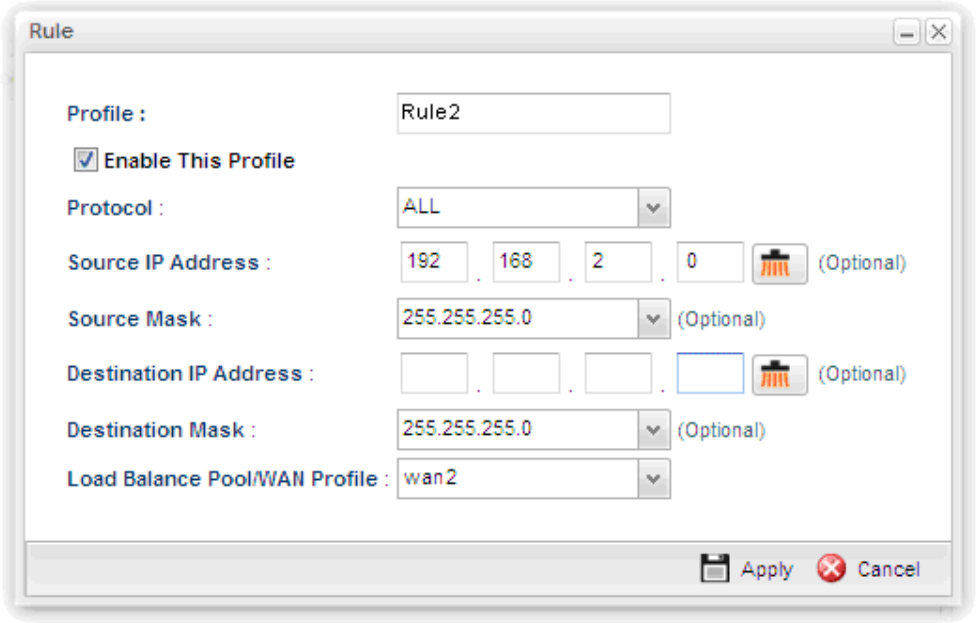
9. Open **WAN >> Load-Balance** and click the **Rule** tab.



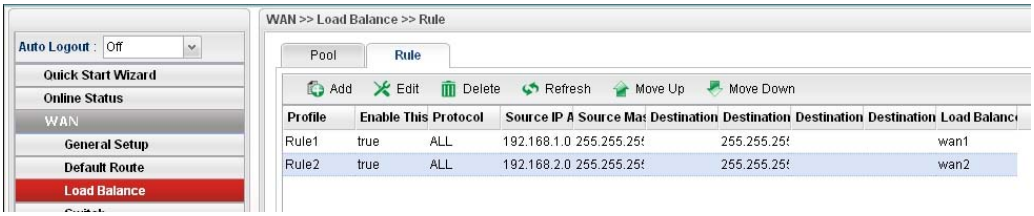
10. Click **Add** to create a profile for Rule1 accepting the data coming from 192.168.1.0/24 which always goes Internet via WAN1 when WAN1 is up. Type the information specified for such rule. (e.g., **Rule1** for Profile; **192.168.1.0** for **Source IP Address**; **wan1** for **Load Balance Pool/WAN Profile** and so on). Next, click **Apply** to save and exit.



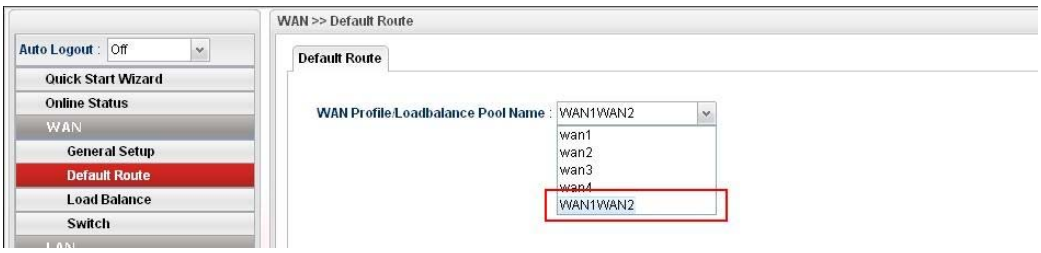
11. Click **Add** again to create a profile for Rule2 accepting 192.168.2.0/24 which always goes Internet via WAN2 when WAN2 is up.



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



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



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

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

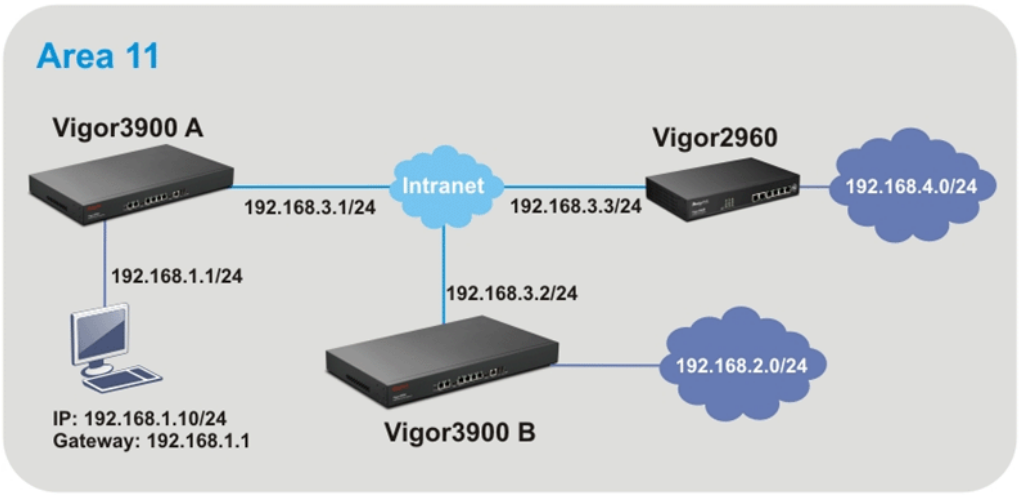
3.2 How to Configure OSPF?

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

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

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

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

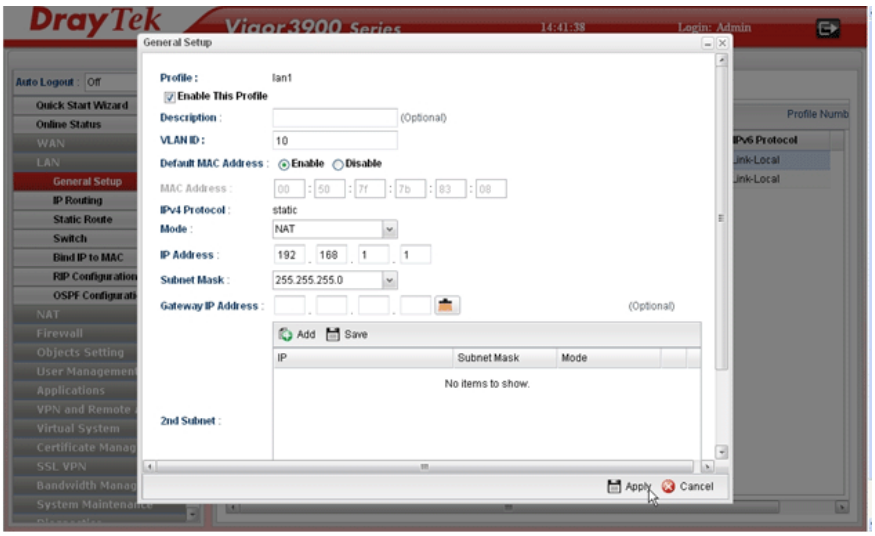


OSPF can place each router (e.g., Vigor3900A, Vigor3900B and Vigor2960 shown above) at the root of a tree and calculate the shortest path to each destination according to the cumulative cost to reach the destination.

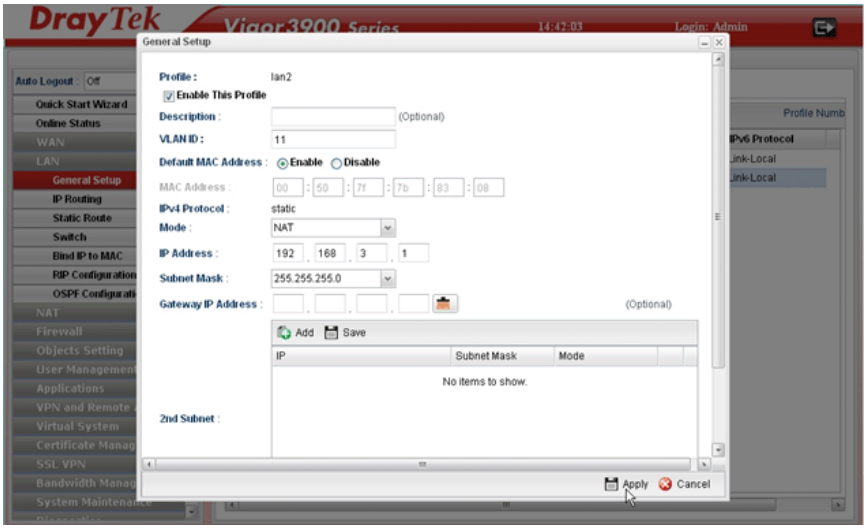
Each router has its own view of the topology and calculates its own SPF tree, even though all the routers build a shortest-path tree using the same link-state database.

Configuration for Vigor3900 A,

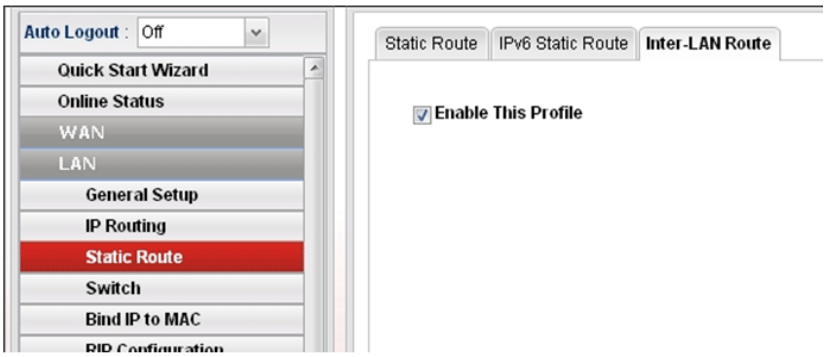
1. Open **LAN >> General Setup** to create a LAN (192.168.1.1/24) profile named lan1 with the settings shown below.



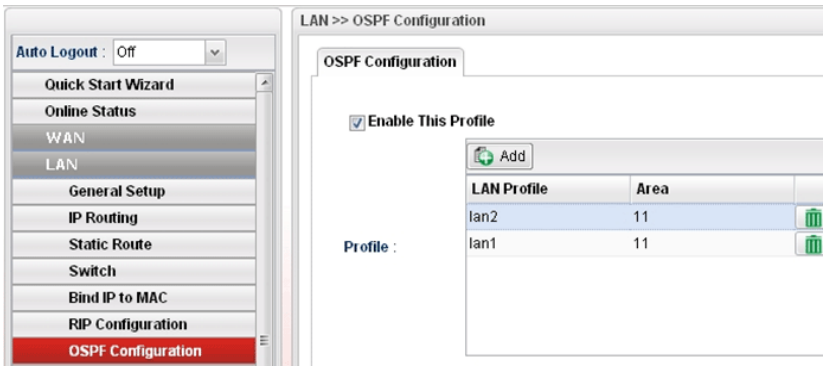
2. Next, continue to create a LAN (192.168.3.1/24) profile named lan2 with the settings shown below.



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

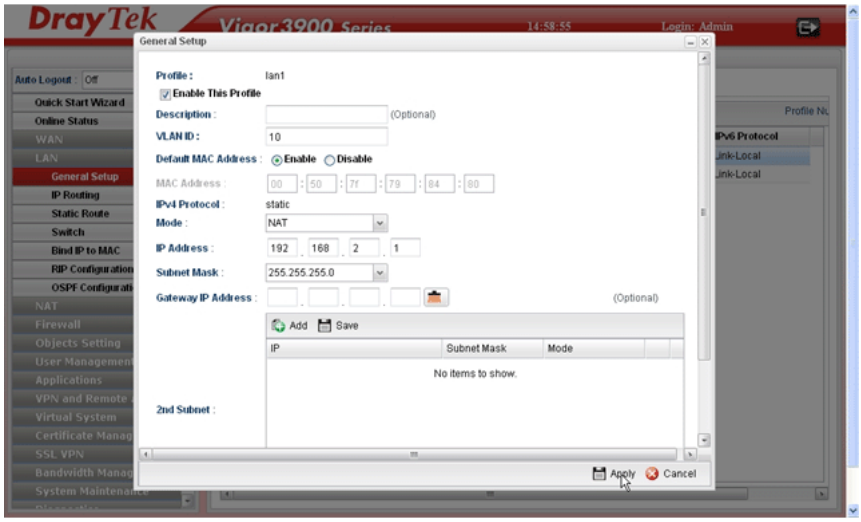


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

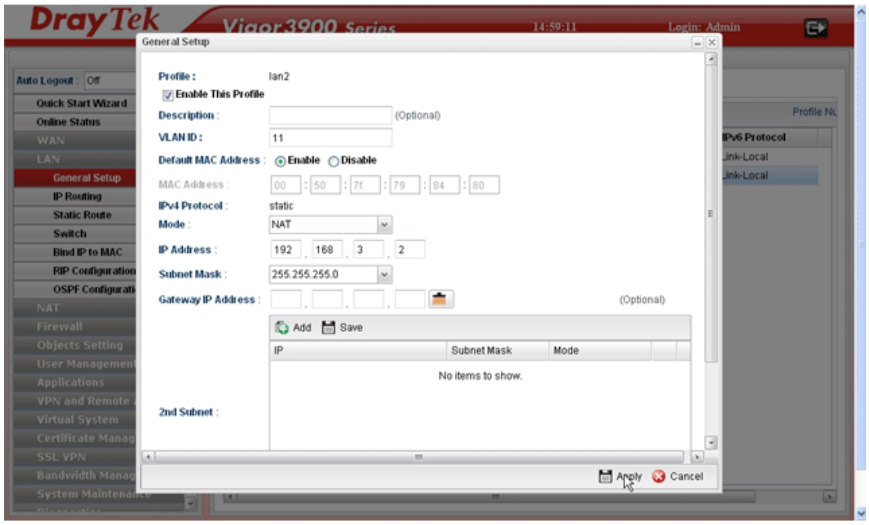


Configuration for Vigor3900 B,

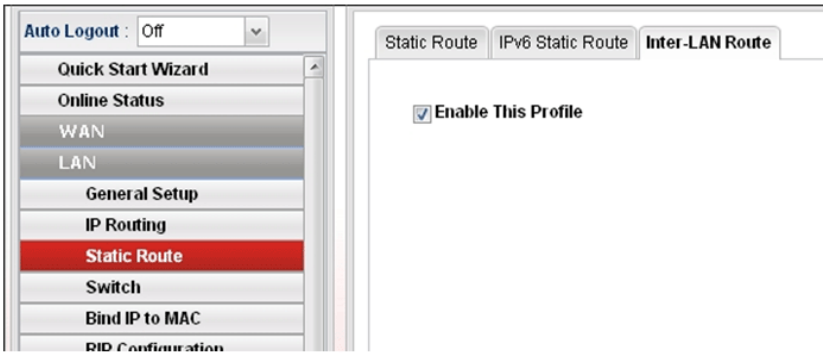
1. Open **LAN >> General Setup** to create a LAN (192.168.2.1/24) profile named lan1 with the settings shown below.



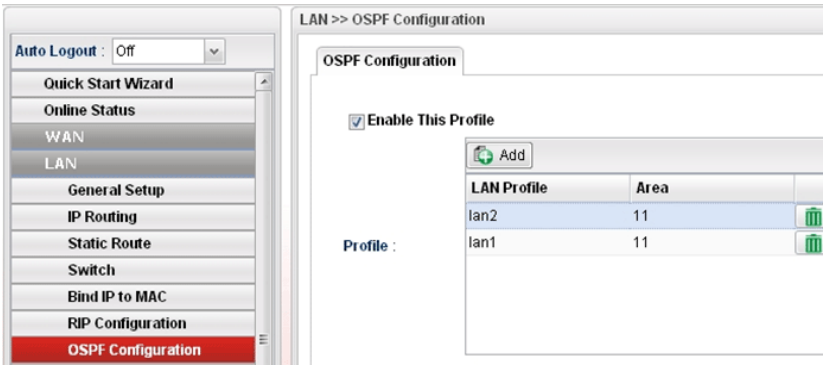
2. Next, continue to create a LAN (192.168.3.2/24) profile named lan2 with the settings shown below.



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

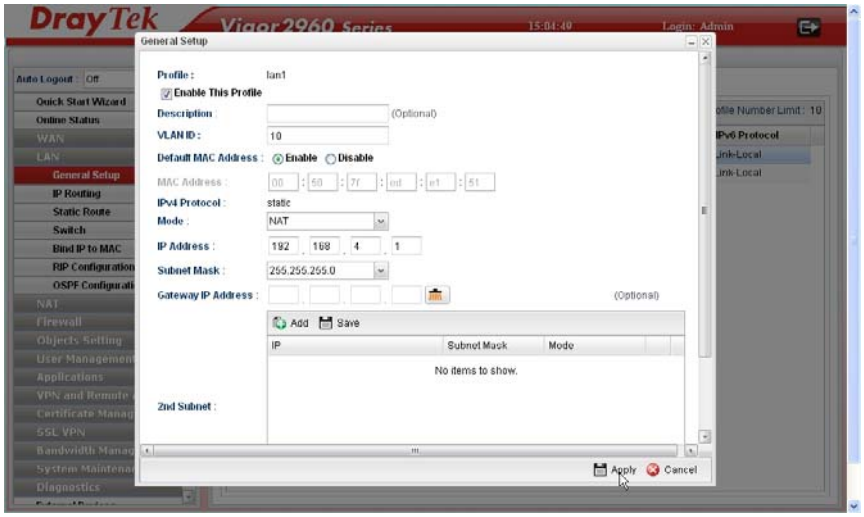


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)

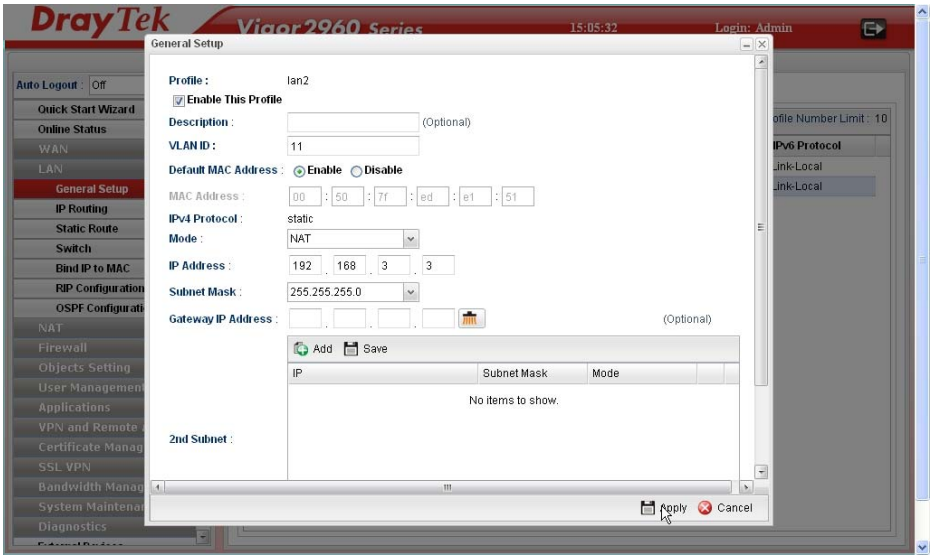


Configuration for Vigor2960,

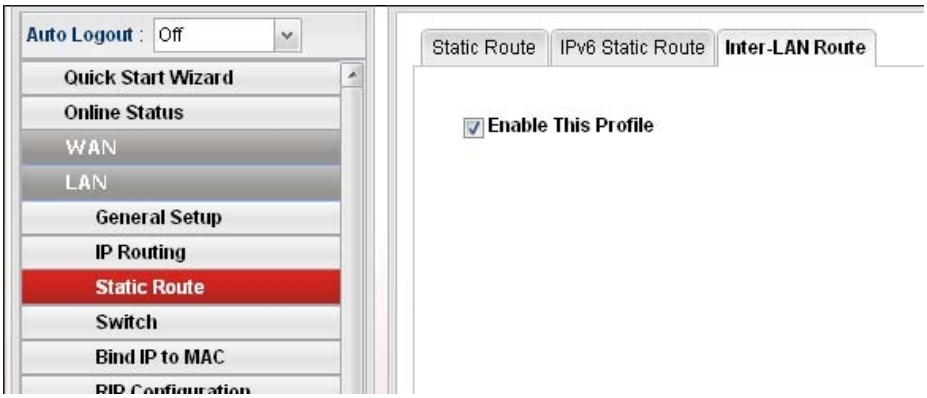
1. Open **LAN >> General Setup** to create a LAN (192.168.4.1/24) profile named lan1 with the settings shown below.



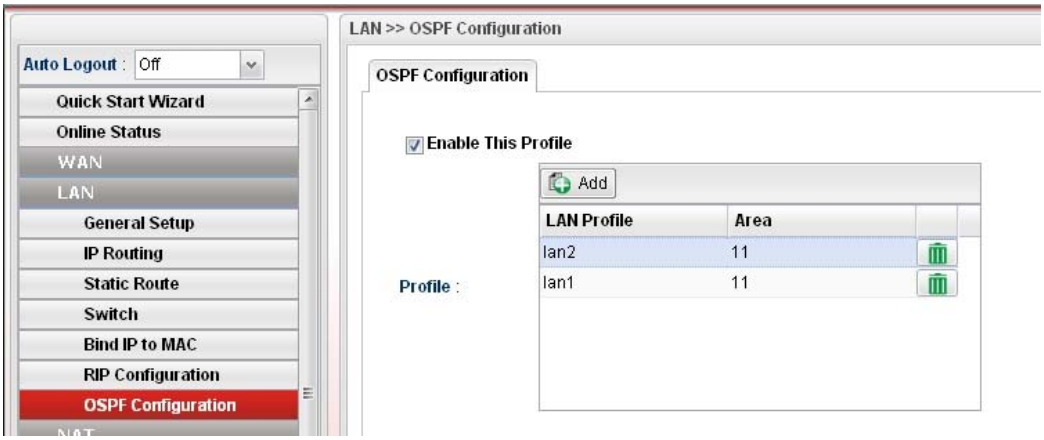
2. Next, continue to create a LAN (192.168.3.3/24) profile named lan2 with the settings shown below.



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

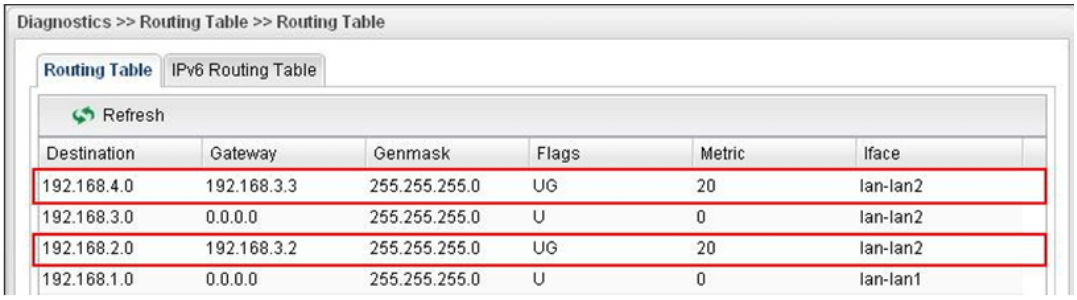


4. Open **LAN >> OSPF Configuration** to enable this profile. Click **Add** to make the LAN Profiles lan2 area setting as 11 and lan1 area as 11. (As shown in the topology diagram.)



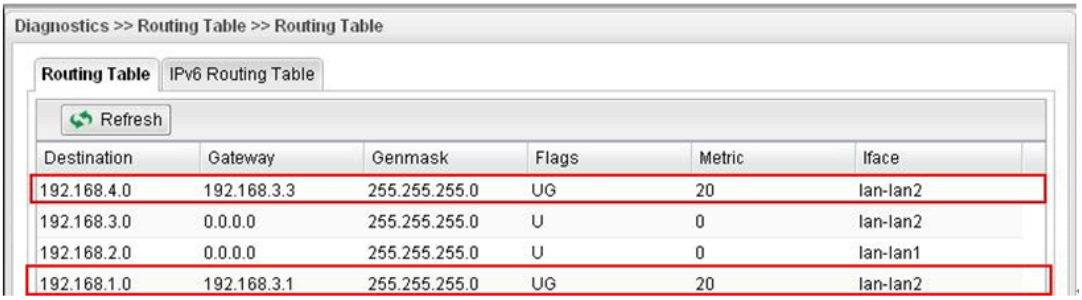
5. After setting, check the routing information (marked with red line) which is created by OSPF.

Routing information for Vigor3900 A



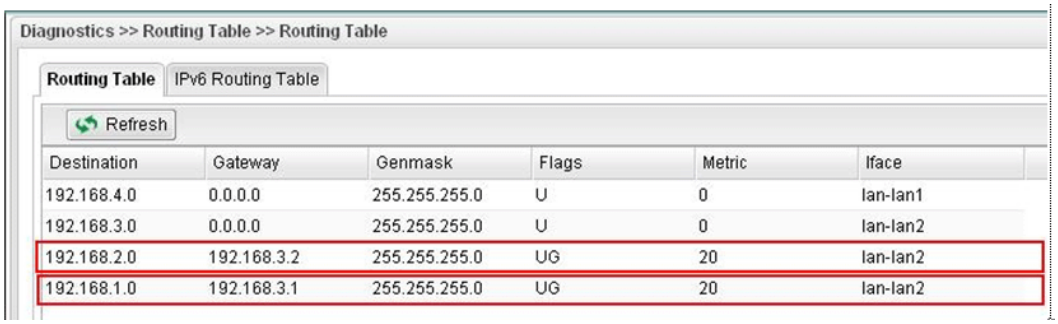
Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1

Routing information for Vigor3900 B



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

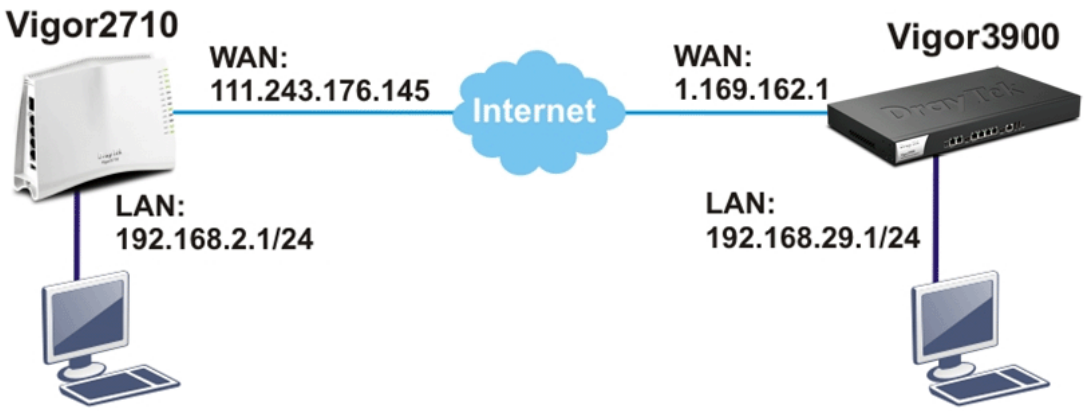
Routing information for Vigor2960



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

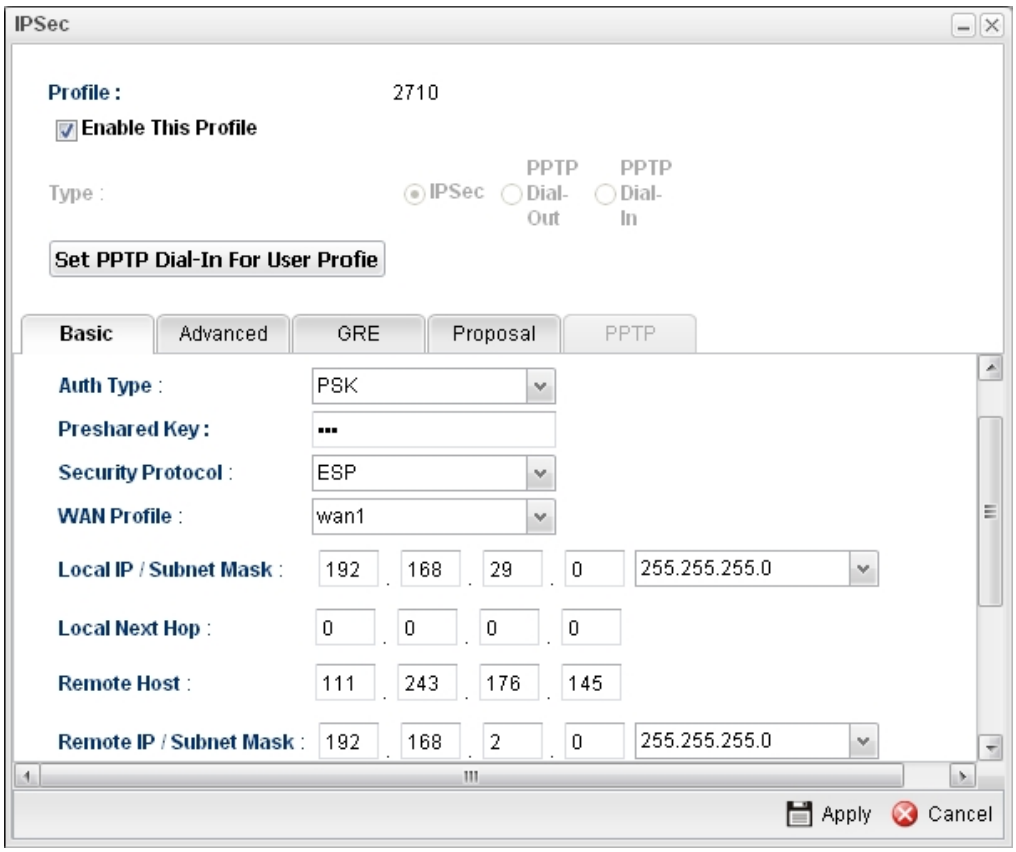
3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode)

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



Configuring Vigor3900

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

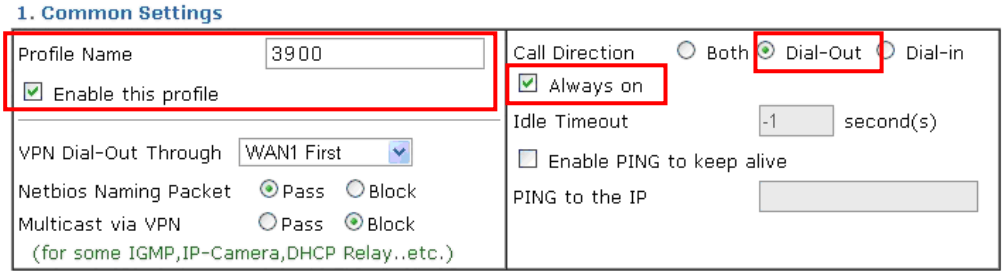


Type the Pre-shared key and choose a WAN Profile. Specify Local IP/Subnet Mask with 192.168.29.0/24. The Remote Host should be Vigor 2710's WAN IP address; and the Remote IP/Subnet Mask should be192.168.2.0/24.

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

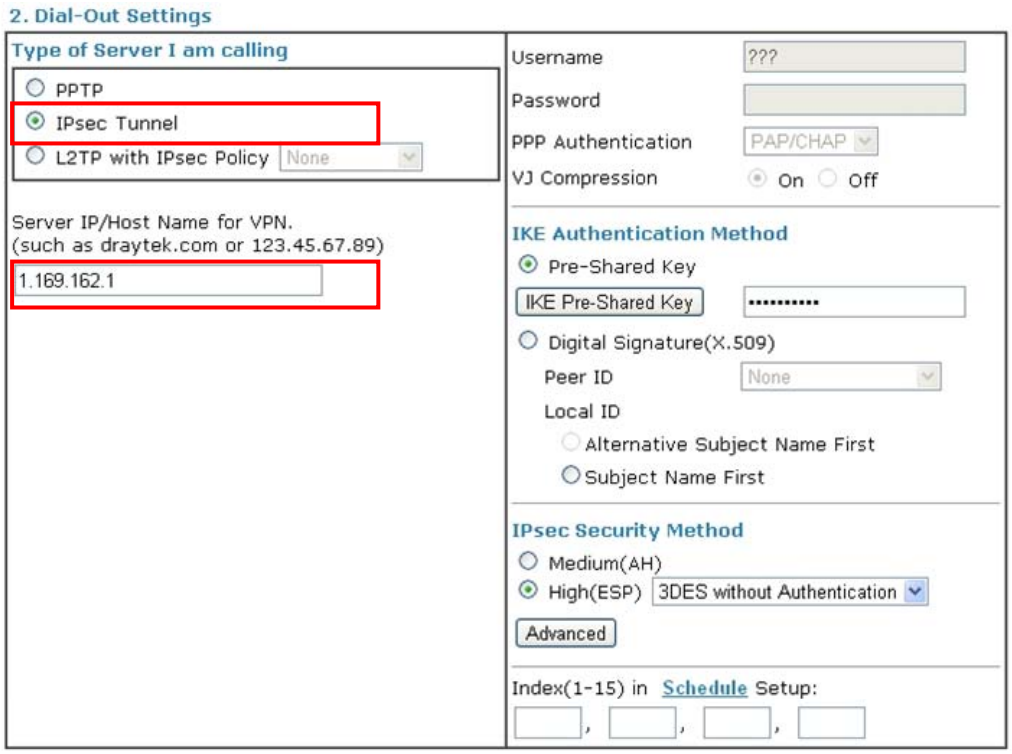
Configuring Vigor2710

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

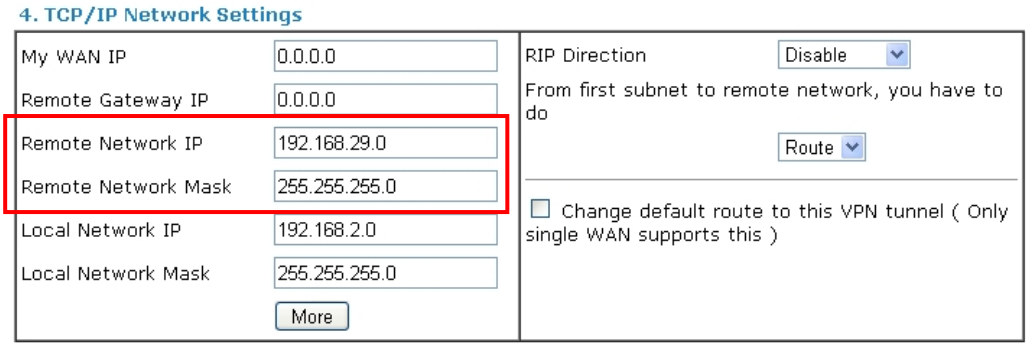


- First, please type the name of such VPN connection in the field of Profile Name (e.g., 3900).
- Check the box of **Enable this profile**.
- Choose **Dial-Out** as **Call Direction** and check the box of **Always on**.

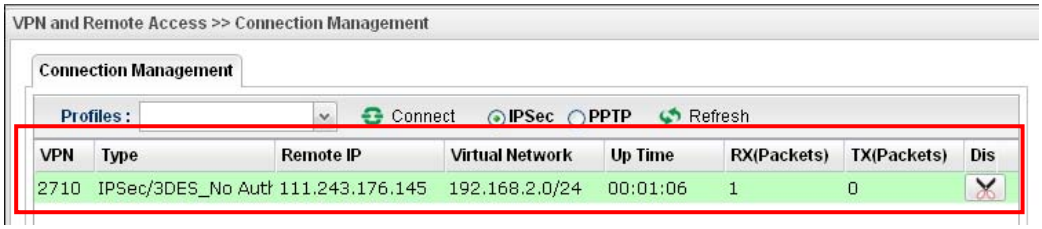
2. For **Dial-Out Settings**, please choose **IPSec Tunnel** and type WAN IP address of Vigor3900 in the field of **Server IP/Host Name for VPN** (e.g., 1.169.162.1). Type the same IKE Pre-Shared Key configured in Vigor3900.



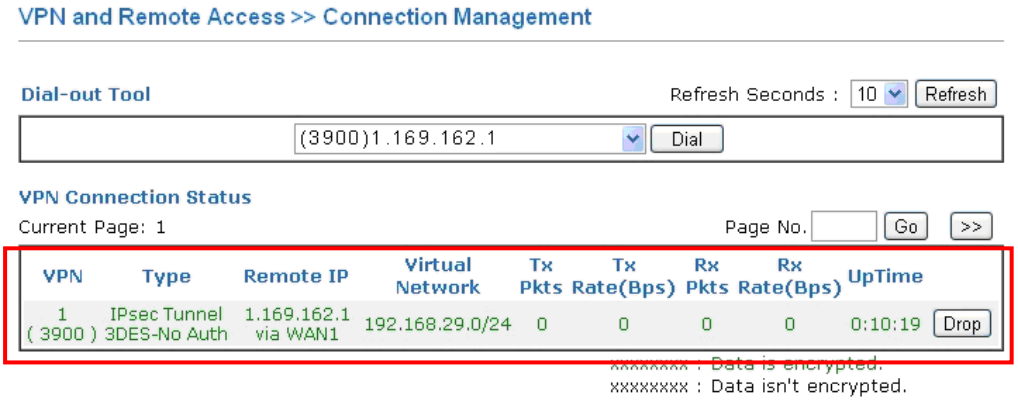
3. For the role of Vigor2710 is dialing-out, please skip Dial-In setting. Type the **Remote Network IP** and **Remote Network Mask** of Vigor3900 to complete configuration.



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

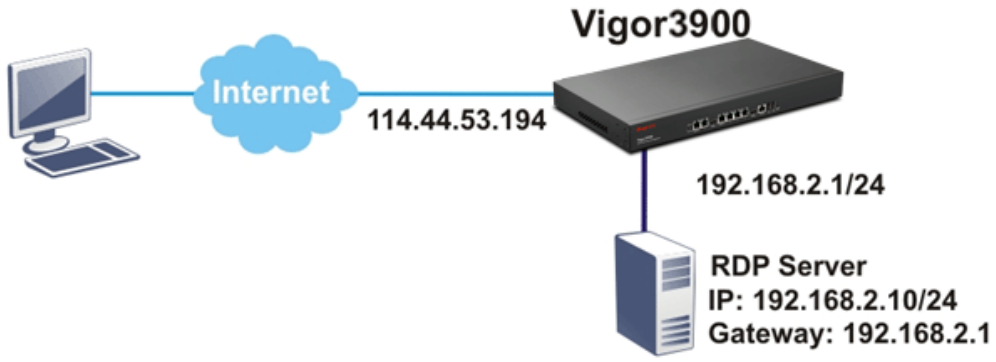


As to Vigor2710, please open **VPN and Remote Access>>Connection Management** to confirm the result.

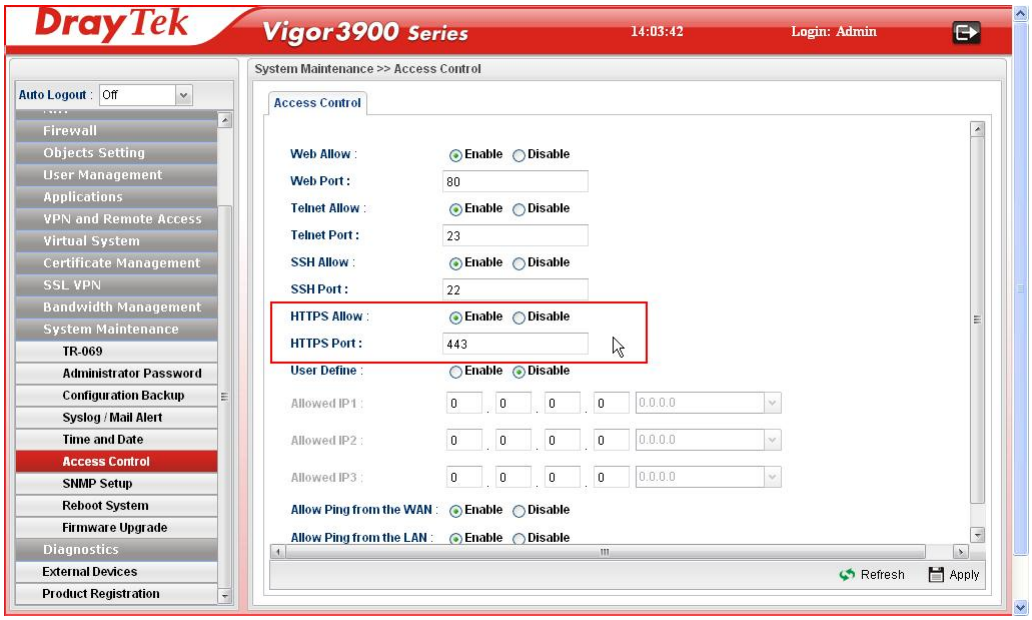


3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server?

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

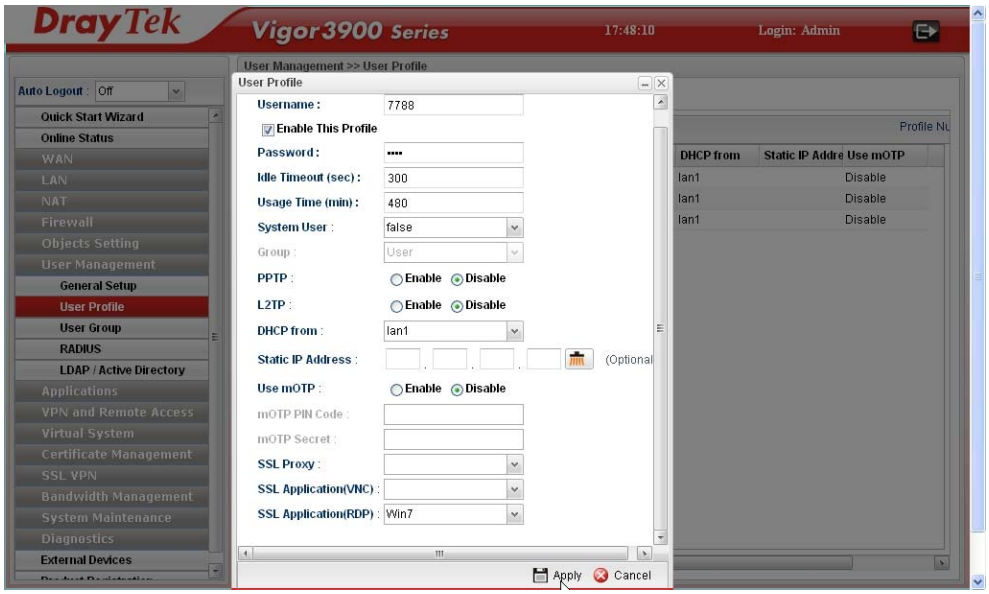


1. Open the web configurator of Vigor3900.
2. Enable the HTTPS service from **System Maintenance >> Access Control** by clicking **Enable** for **HTTPS Allow** and type **443** as the value of **HTTPS Port.**



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

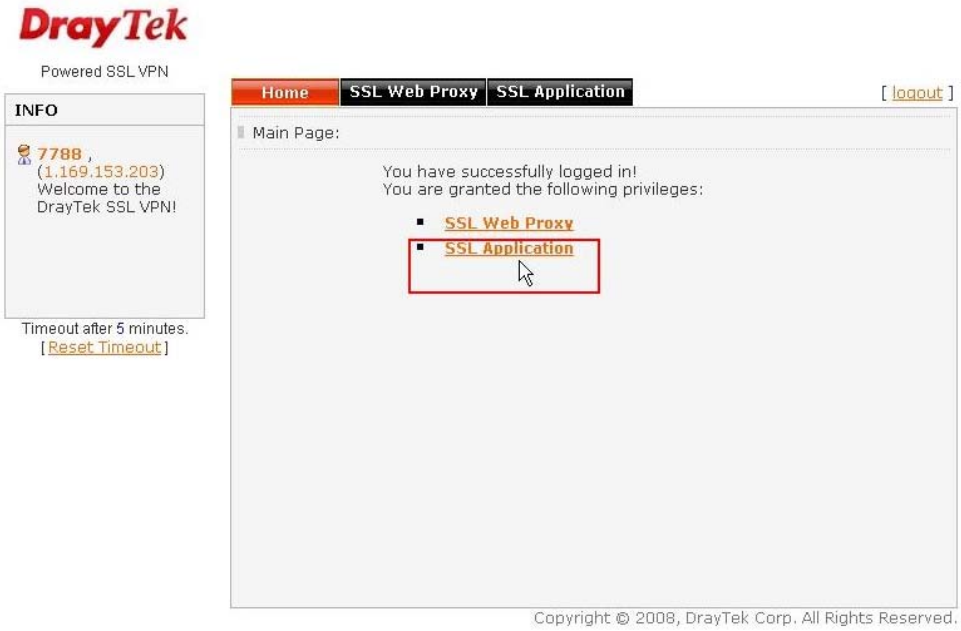
4. Open **User Management >> User Profile** to create a new profile named "7788". Set the **Password** as 7788 and choose the profile of **Win7** as **SSL Application (RDP)**. Click **Apply**.



5. Logout Vigor3900.

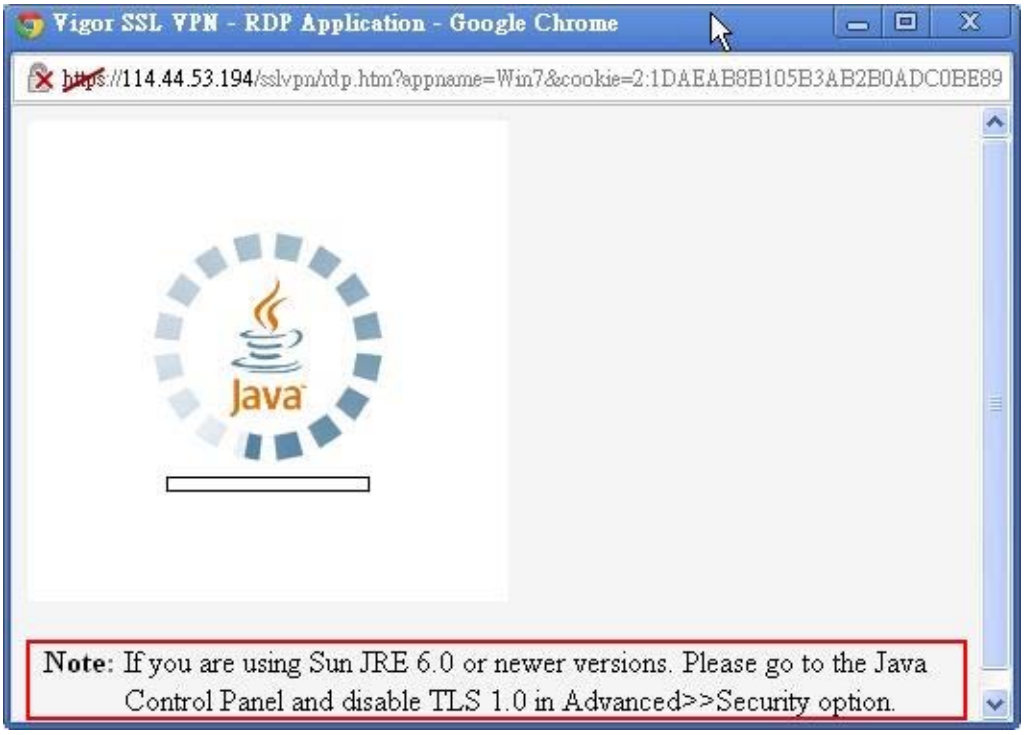
6. Login Vigor3900 HTTPS Server with 7788 for both Username and Password.

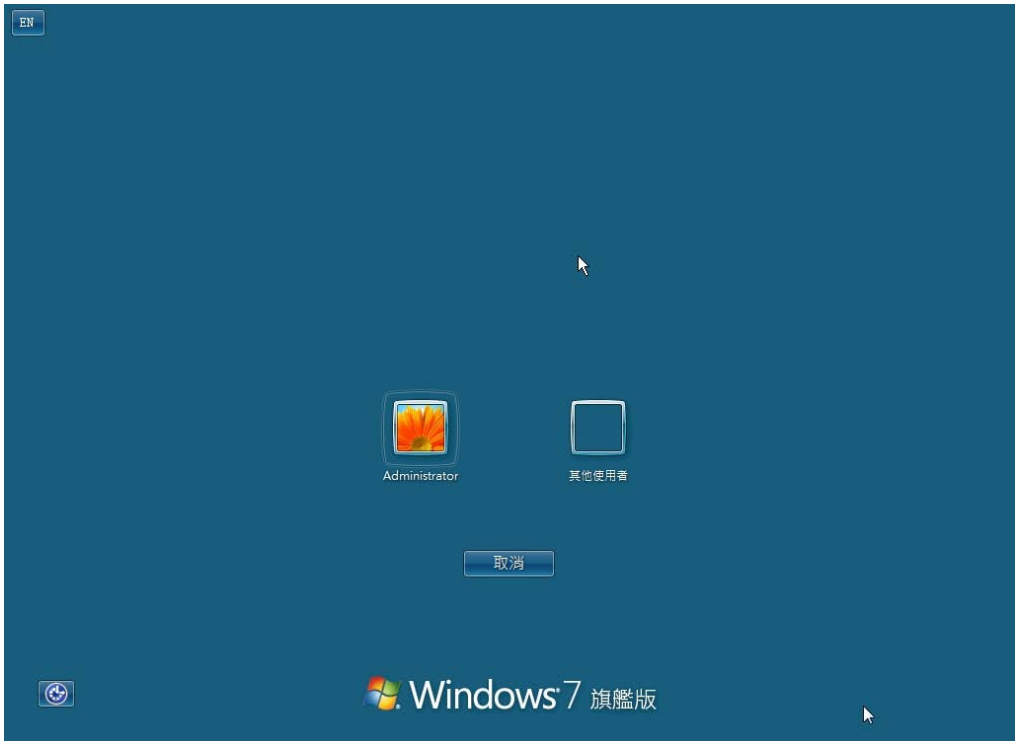
7. A screen like the following figure will appear. Simply click the **SSL Application** link.



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

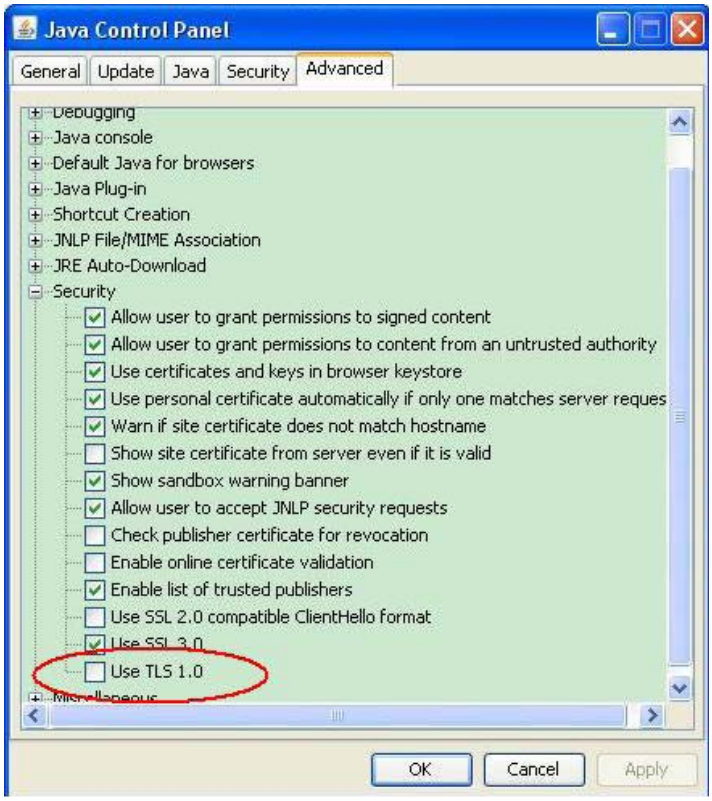
9. After that, you can access into Windows 7 via a browser. Note the message below the window. In which, TLS means Transport Layer Security.





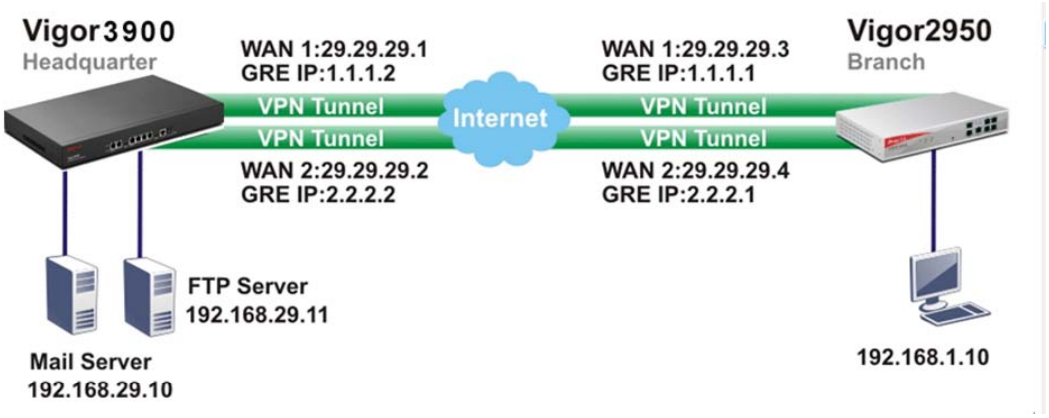
Troubleshooting

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



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

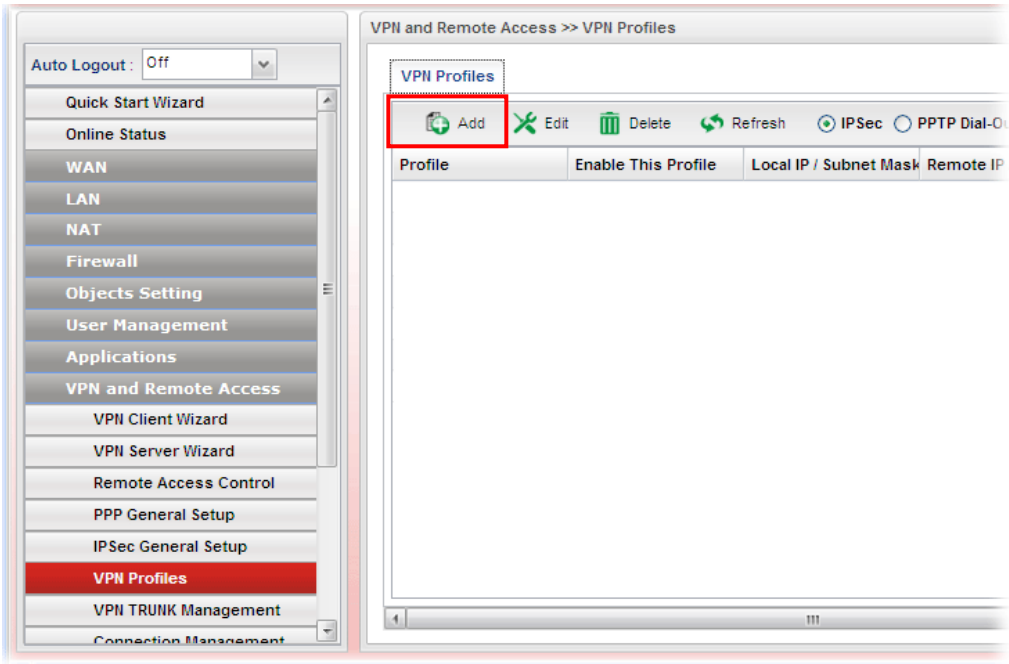
The staff in branch office can access into mail server/FTP server installed in the headquarters via VPN Load Balance tunnels. Refer to the following figure.



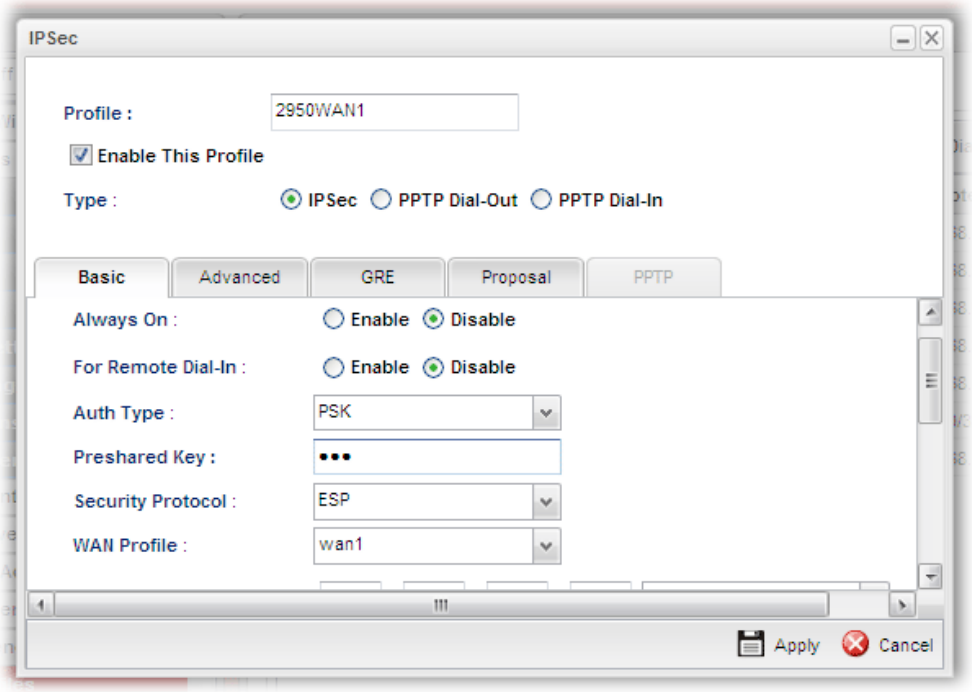
Vigor3900 allows users to build VPN load balance connection between Vigor3900 and other router. Take Vigor2950 for an example. There are two WANs on Vigor2950 and two WANs on Vigor3900. We will build VPN connection with load balance between Vigor3900 and two WANs of Vigor2950 respectively.

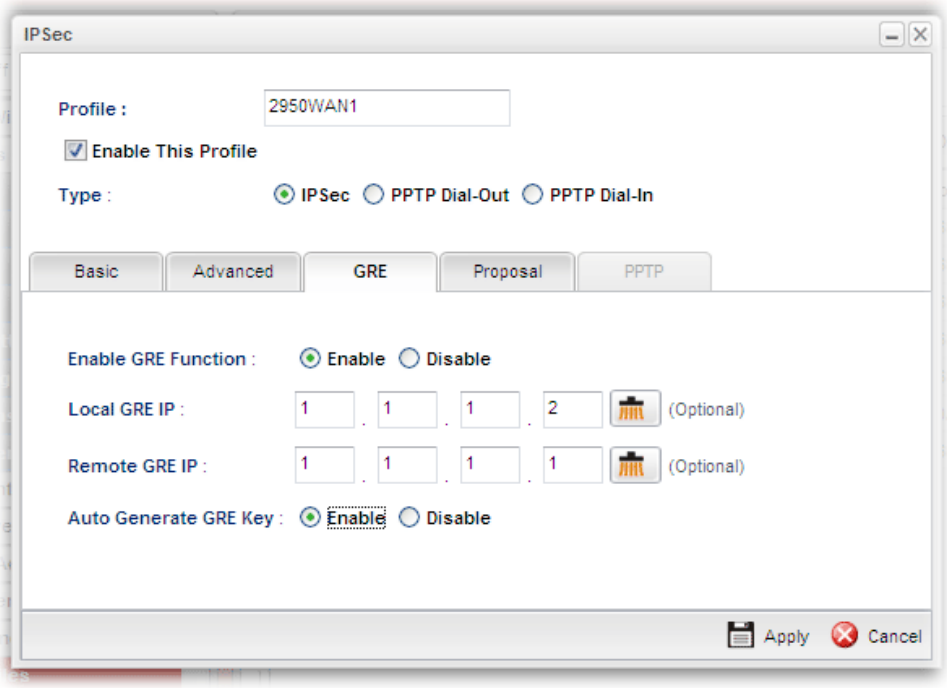
Configuring Vigor3900

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

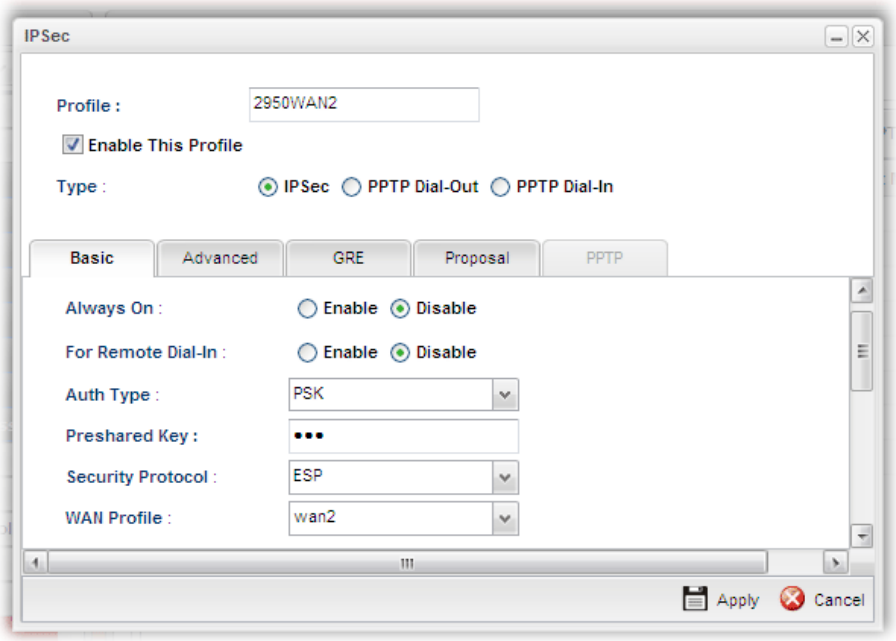


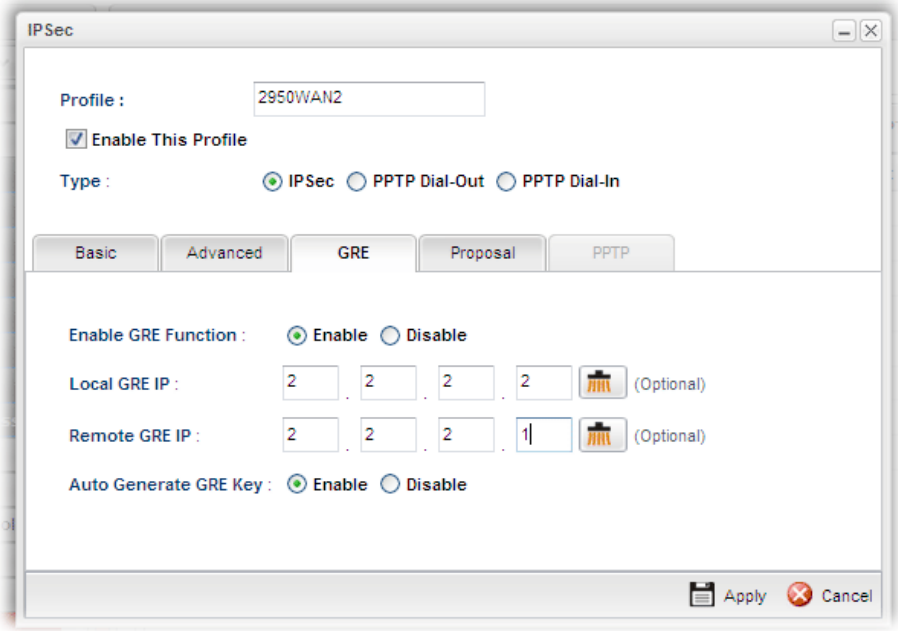
2. Create a profile for WAN 1 (named 2950WAN1). Type the settings as shown below:





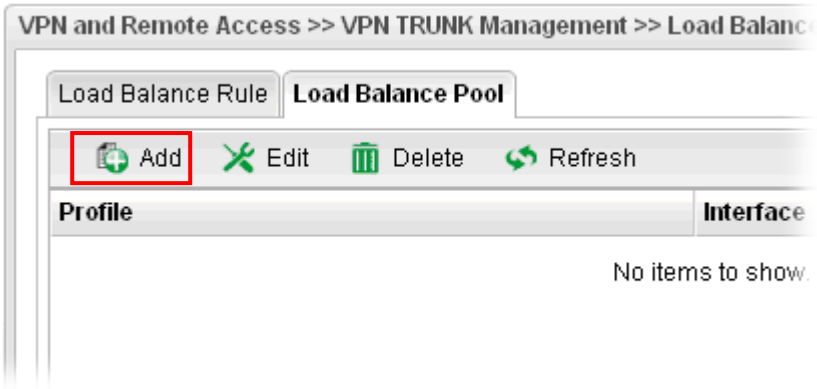
3. Click **Apply** to save the settings and exit the dialog.
4. Create a profile for WAN 2 (named 2950WAN2).



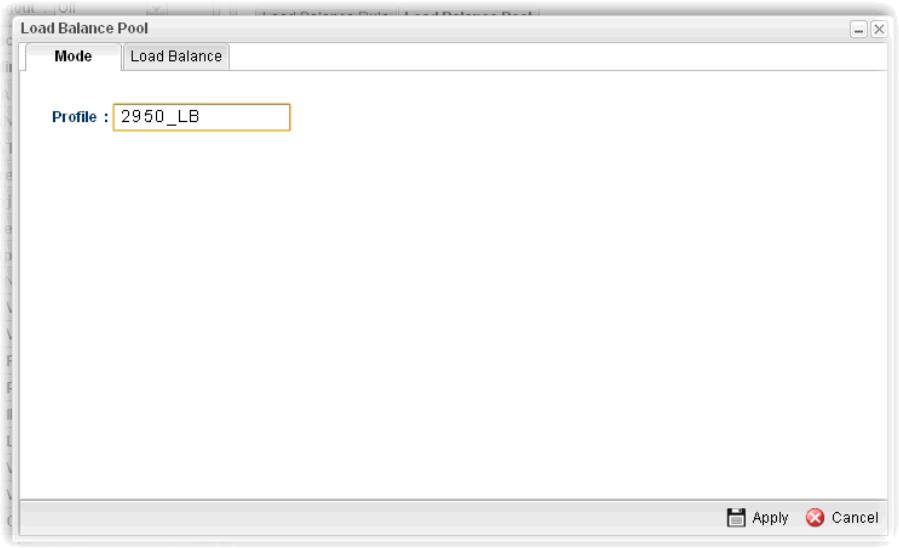


5. Click **Apply** to save the settings and exit the dialog.

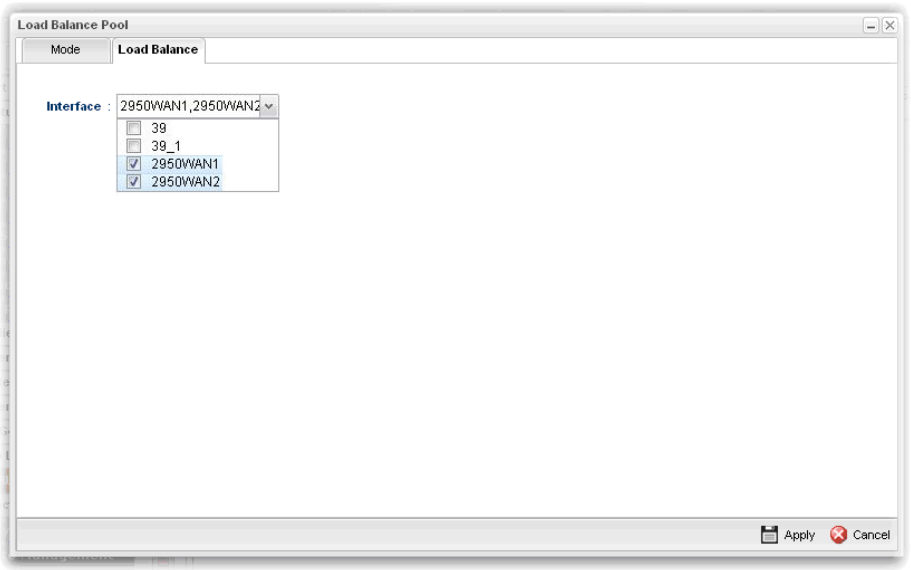
6. Open **VPN and Remove Access>>VPN Trunk Management** and click the **Load Balance Pool** tab. Click **Add** to add a Load Balance Pool profile.



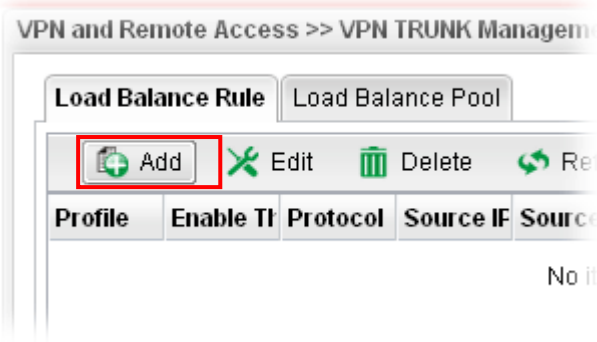
7. The following window will pop up. Give a name for the profile.



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

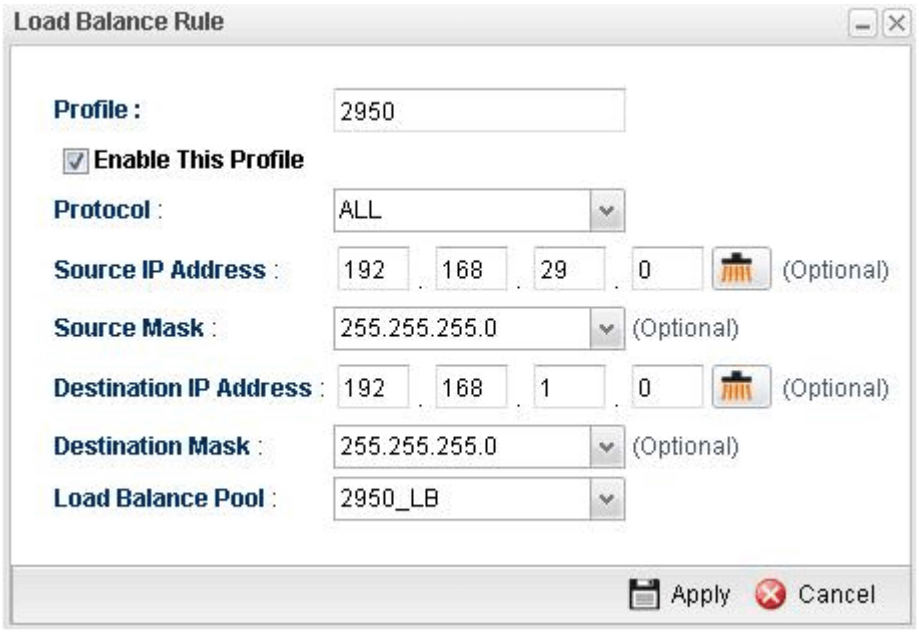


9. Click the **Load Balance Rule** tab and click **Add** to add a Load Balance rule profile.



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

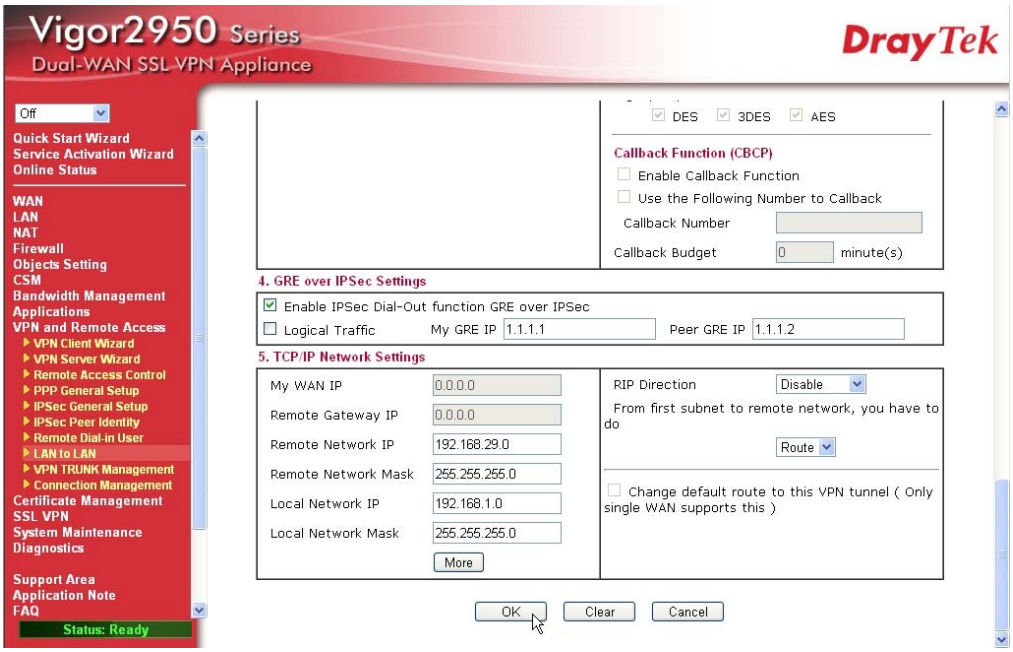
    Type the local network IP address and Mask of Vigor3900 as Source IP Address and Source Mask; type the network IP and Mask of Vigor2950 as Destination IP Address & Destination Mask. Select the Load Balance Pool profile (e.g., 2950_LB) set for Vigor2950.



Configuring Vigor2950

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

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

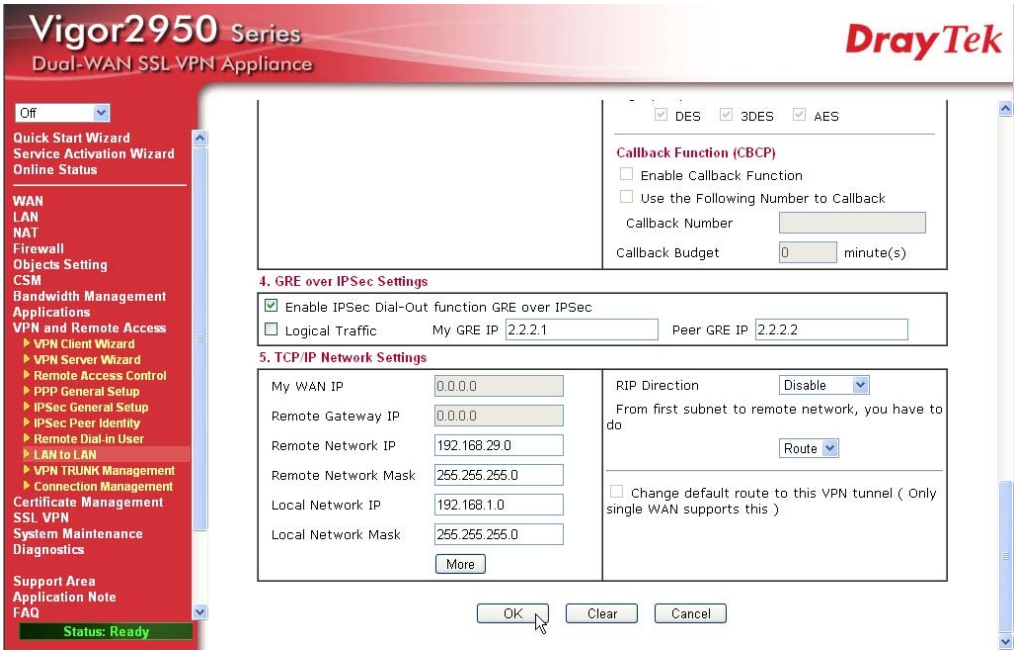


- Please type the network IP address and subnet of Vigor3900 in the field of Remote Network IP and Remote Network Mask. Type the network IP address and subnet of Vigor2950 in the field of Local Network IP and Local Network Mask.

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

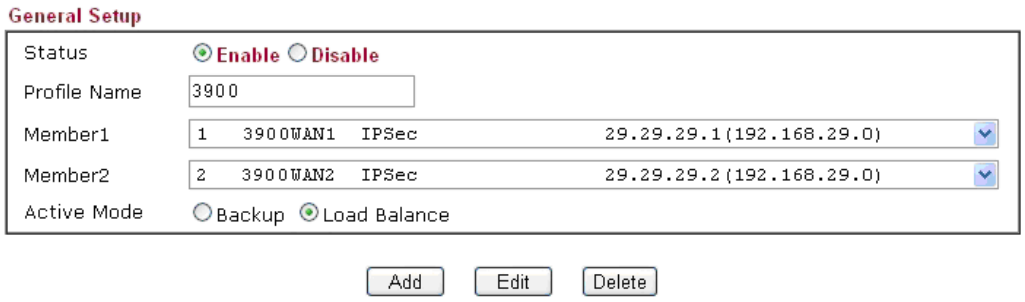
- Choose **IPSec Tunnel** and type the **Server IP** and Pre-shared Key as shown below.
- In the field of GRE over IPSec, please type the corresponding settings for Vigor3900. Refer to the following figure.In this example, please type the 2.2.2.1 in the field of **My GRE IP**; and type the GRE IP address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

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

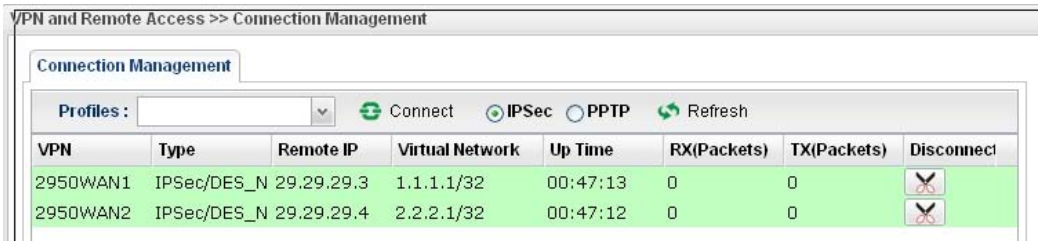


3. After finished the settings on both VPN connections, please access the web configurator of Vigor2950 and open **VPN and Remote Access > VPN Trunk Management** to make these two VPN connections into one **Load Balance** group.

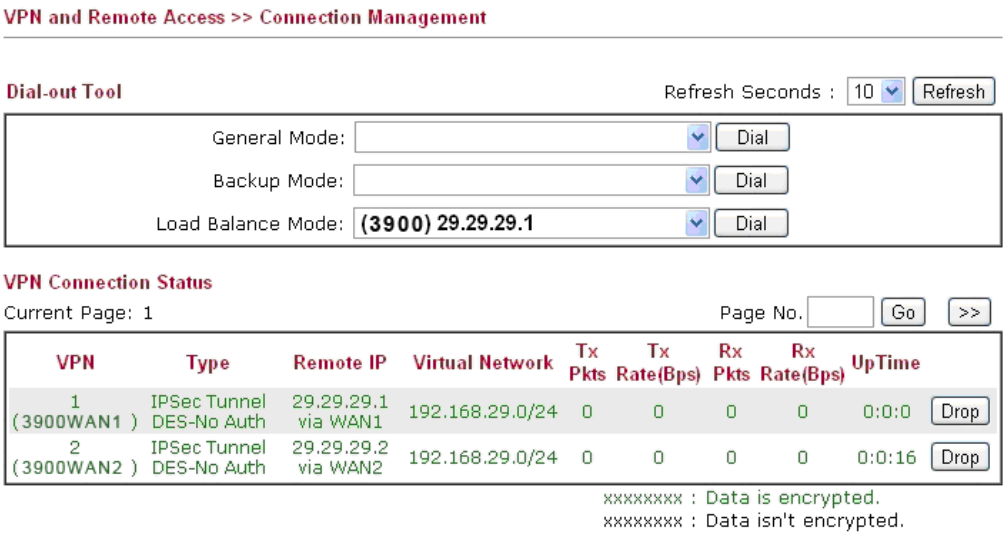
4. Type the name (e.g., 3900) of the **Load Balance** in the field of **Profile Name**. Specify the VPN profiles in Member 1 and Member 2 respectively. Then, choose **Load Balance** as the **Active Mode**.



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



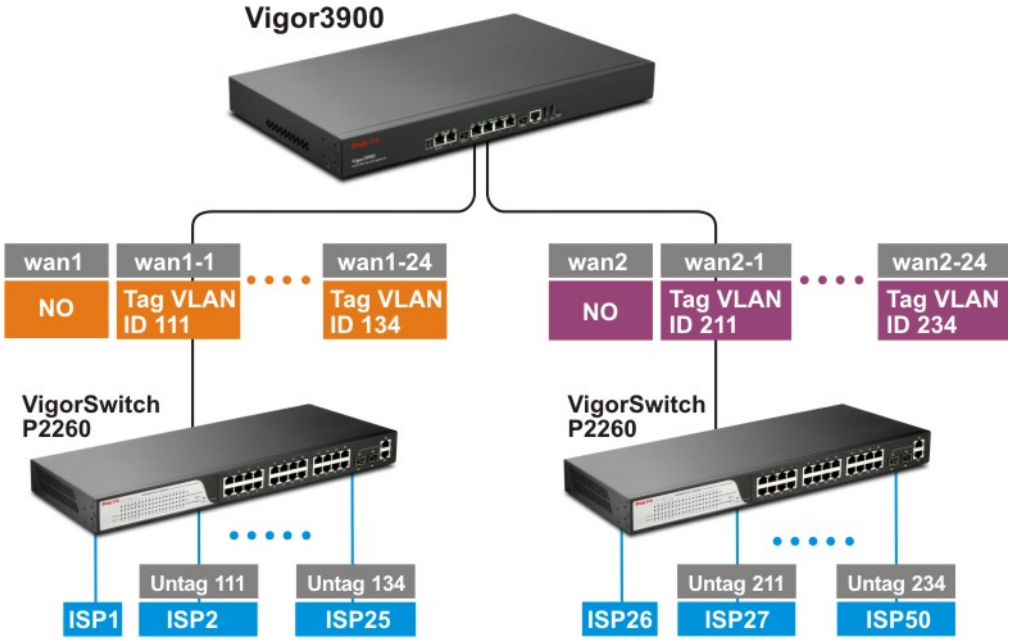
As to Vigor2950, please open **VPN and Remote Access>>Connection Management** to confirm the result.



3.6 How to Setup 50 WANs on Vigor3900

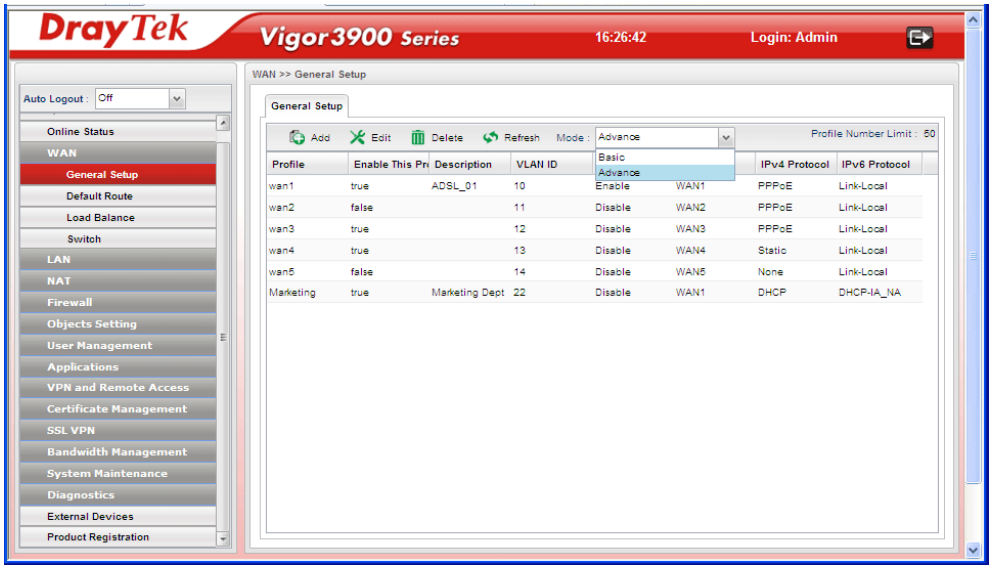
Vigor3900 has 5 physical WANs; however, it can be extended to 50 WANs at most by using VLAN Tagging technology.

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

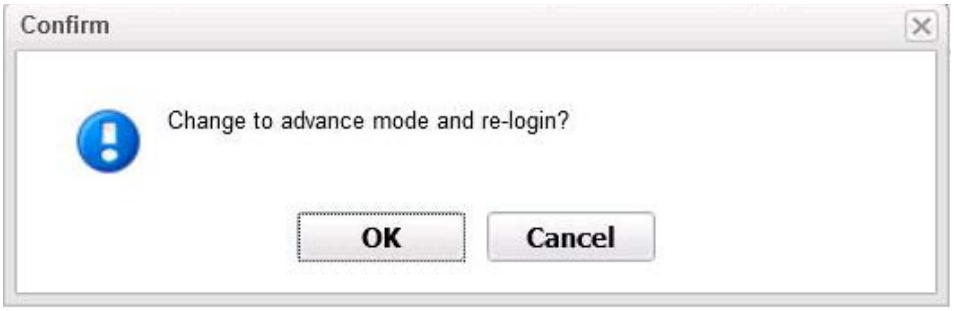


Configuring 50 WAN profiles on Vigor3900

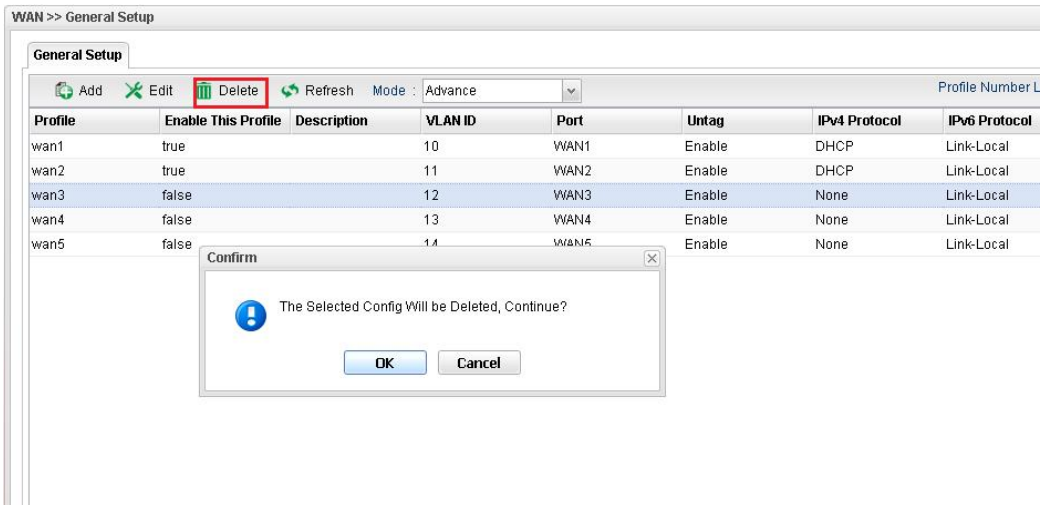
1. Change mode from **Basic** to **Advance** via **WAN>>General Setup** page.



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

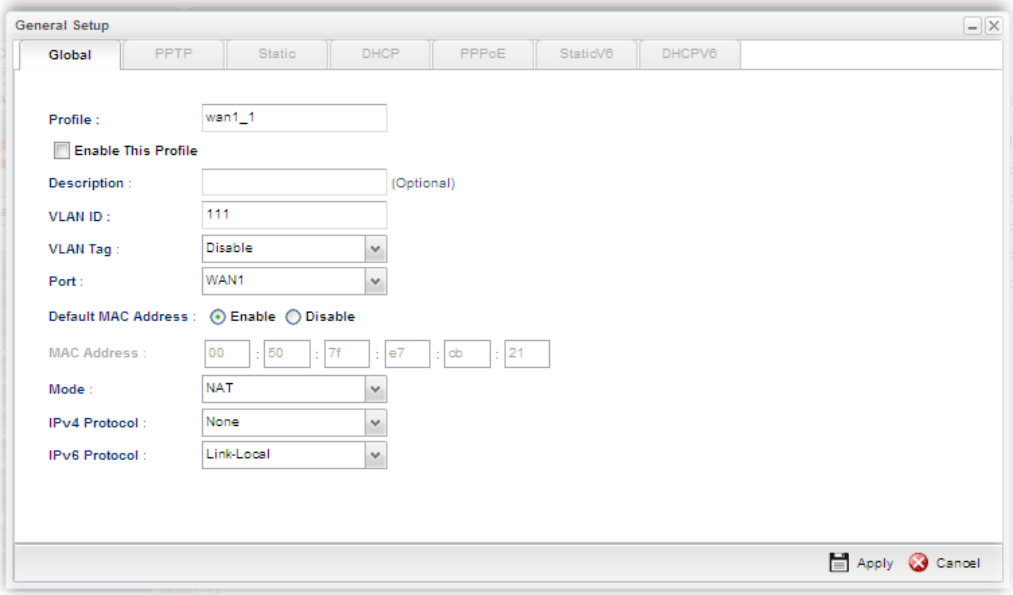


3. Delete default wan profiles for wan3, wan4 and wan5 by selecting the wan profile then click **Delete**.



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

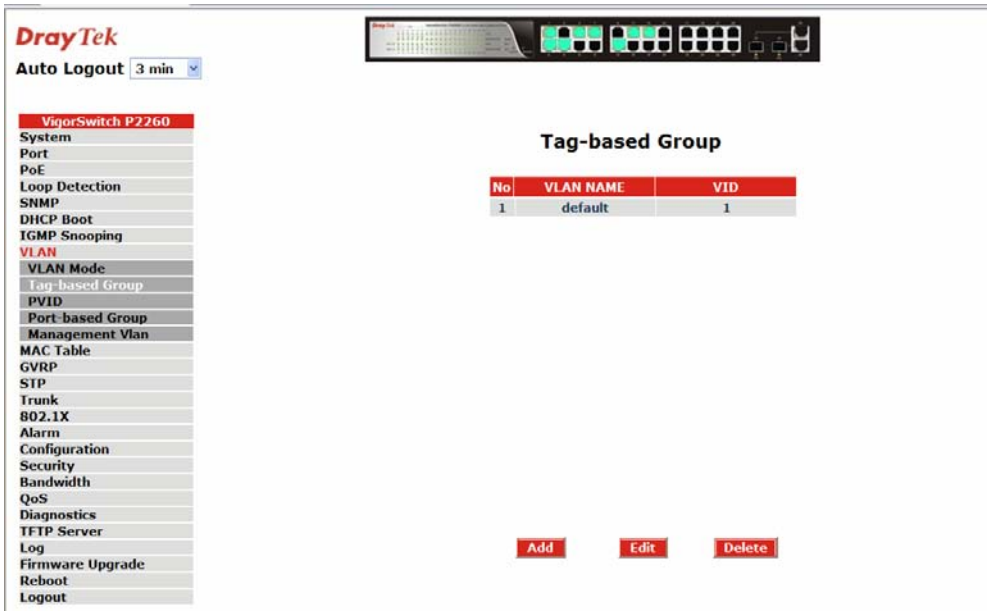
5. Create a new WAN profile named with **wan1_1,** and set VLAN ID named with **111** based on WAN Port 1(WAN1). Note that **Untag** must be set with **Disable**. It means wan1_1 can accept the packets tagged with VLAN ID 111. Next, click **Apply** to save the settings.



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

Configuration on VigorSwitch2260

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



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

Tag-based VLAN

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

Apply

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

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

Tag-based Group

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

Add Edit Delete

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

PVID

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

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

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

Chapter 4: Advanced Web Configuration

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

4.1 WAN Setup

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

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

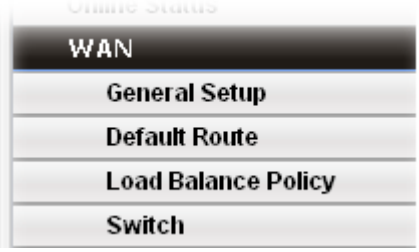
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

Get Your Public IP Address from ISP

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

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated

via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

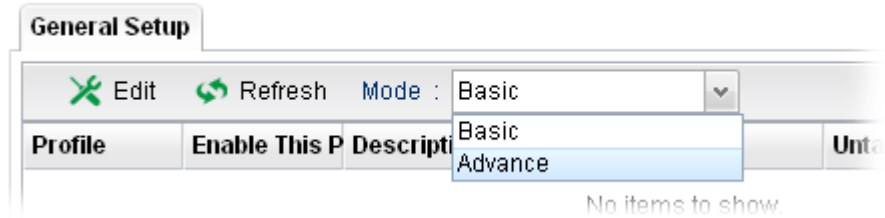


4.1.1 General Setup

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

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

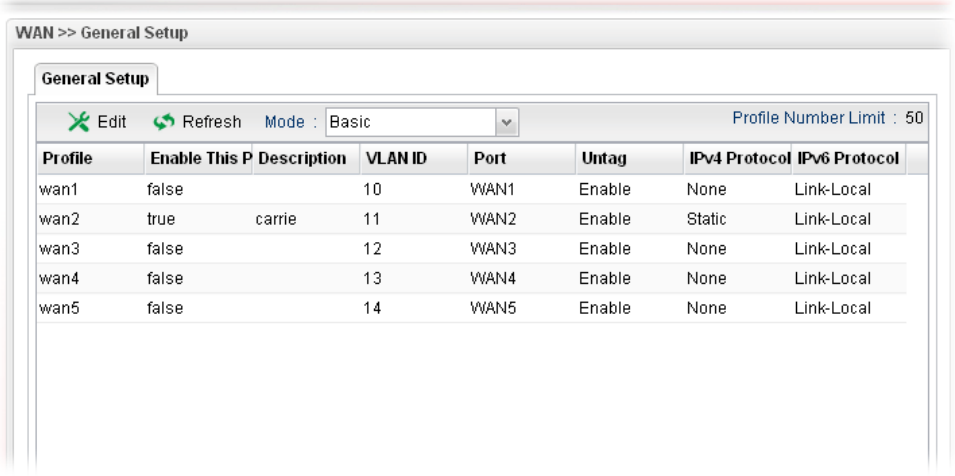
There are two modes for you to choose for setting a WAN profile. **Basic** mode allows you to view and edit the existing WAN profile. However, **Advance** mode allows you to define new WAN profile.



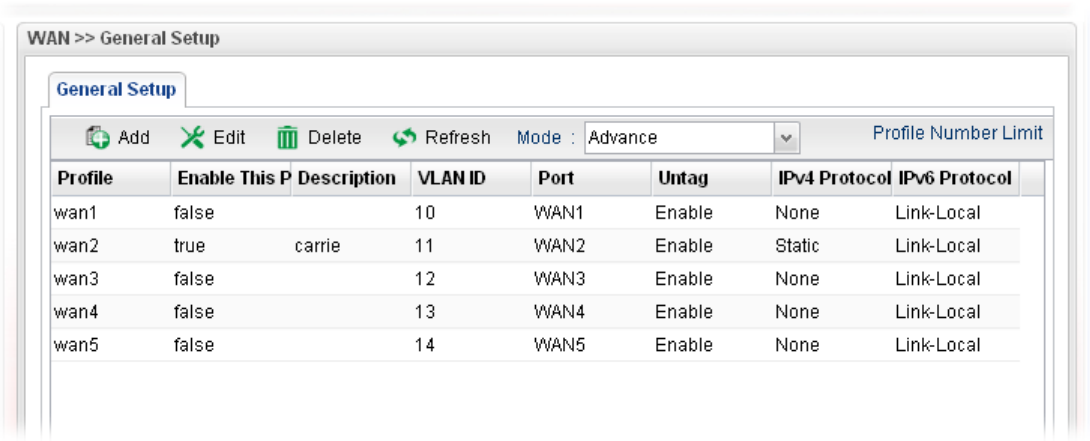
When you switch the Mode setting from Advance to Basic or from Basic to Advance, the system will ask you to re-login web configuration interface to activate some parameters.

Profile

Below shows settings in **Basic** mode:



If you switch into **Advance** mode, you will get the following page:

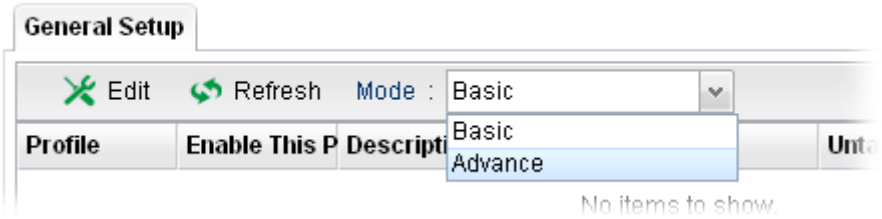


Each item will be explained as follows:

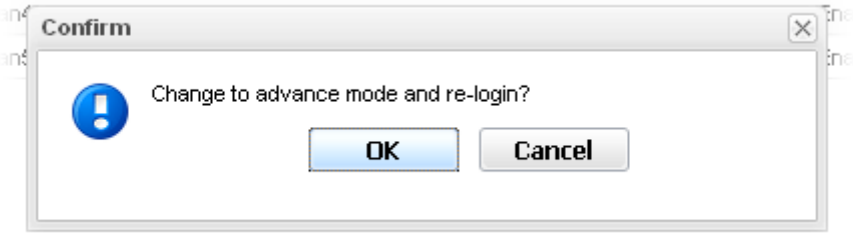
Item	Description
Add	Add a new WAN profile.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected WAN profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile	Display the profile name.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Description	Display a brief explanation for such profile.
VLAN ID	Display the VLAN ID of the profile.
Port	Display the physical WAN interface for such profile.
Untag	If the data transmitted with tag, **Enable** will be displayed in this field. Otherwise, **Disable** will be shown instead.
IPv4 Protocol Type	Display the IPv4 protocol selected by the profile.
IPv6 Protocol Type	Display the IPv6 protocol selected by the profile.

How to add a new WAN profile

1. First, you have to switch into **Advance** mode.

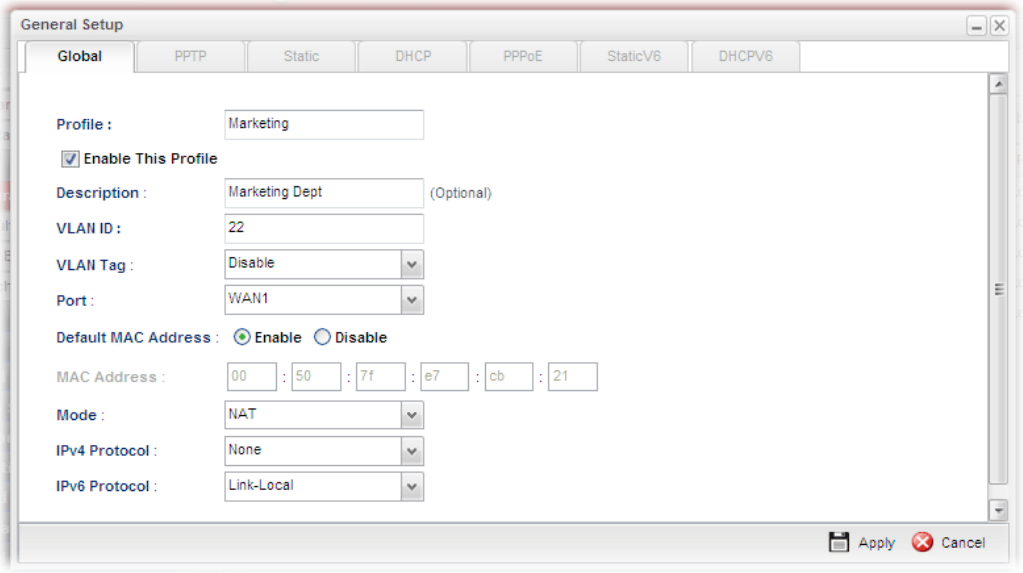


2. A confirmation dialog will appear. Click **OK** to apply the related settings for **Advance** mode.



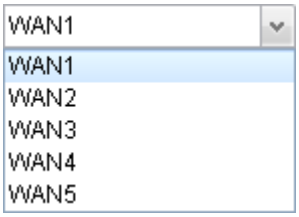
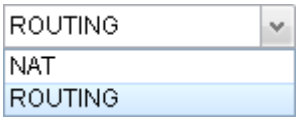
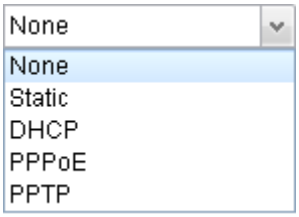
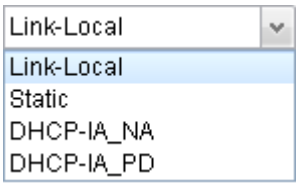
3. Re-login the system.

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



Available parameters are listed as follows:

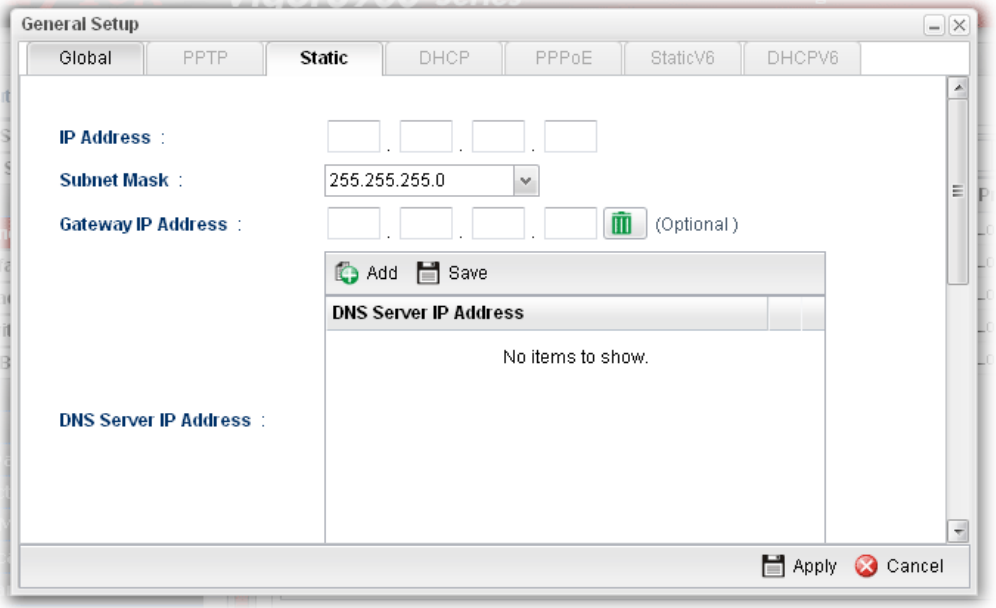
Item	Description
Profile	Type a name for such profile.
Enable This Profile	Check this box to enable such profile.
Description	Give the brief description for such profile.
VLAN ID	Type the VLAN ID number for such profile.

VLAN Tag	Choose **Enable** to tag the packets passing through the port specified below.
Port	Choose the physical WAN interface for such profile. 
Default MAC Address	**Enable** – Click it to enable the default MAC address for such profile. **Disable** – Click it to type the MAC address manually for such profile.
MAC Address	Specify the MAC address for such profile. In default, the system will determine it automatically.
Mode	Determine such profile will be used for. 
IPv4 Protocol Type	There are four connection modes for you to specify for IPv4 protocol type. Each mode will bring up different web page. 
IPv6 Protocol Type	There are four connection modes for you to specify for IPv6 protocol type. Each mode will bring up different web page. 

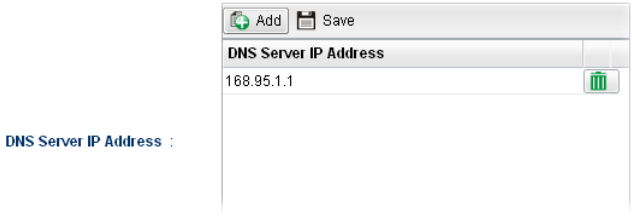
General Settings allows you to enable the profile, give a brief explanation for such profile, specify the VLAN ID, specify MAC address, choose IPv4 and IPv6 protocol, and specify the mode of the data transmission (**NAT** or **Routing**).

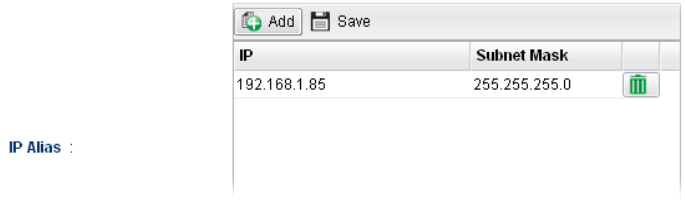
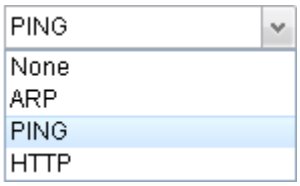
Different IPv4 and IPv6 protocol types specified will bring up different configuration web page.

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



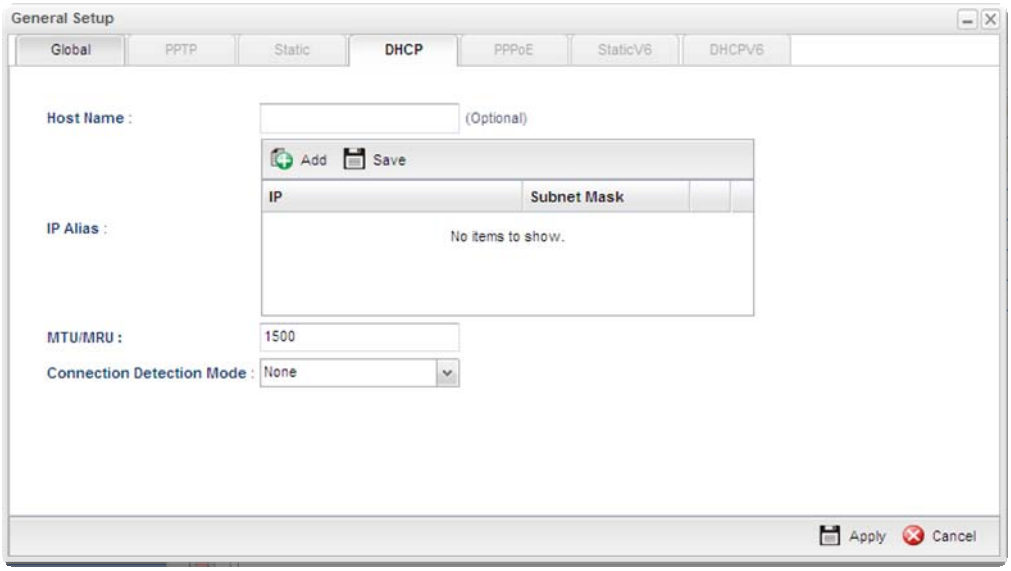
Available parameters are listed as follows:

Item	Description
IP Address	Type the IP address specified for such profile.
Subnet Mask	Use the drop down list to choose the subnet mask for such profile.
Gateway IP Address	Type the gateway address for such profile. – click the icon to clear the address setting.
DNS Server IP Address	Type a public IP address as the primary DNS (Domain Name Server). To add a new IP address, simply place the mouse cursor on this filed. The following dialog will appear.  **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the icon to remove the selected entry.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g.,

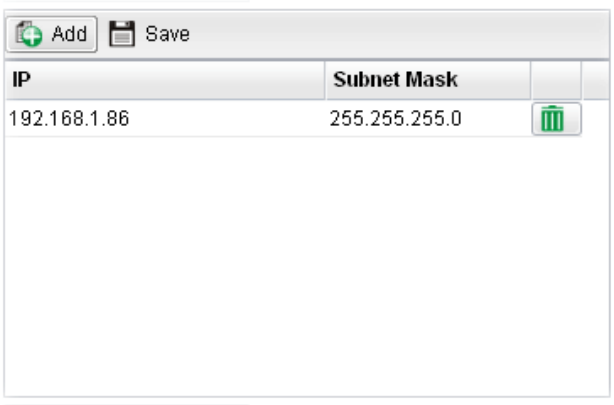
	NAT>>Port Redirection/DMZ Host). To add a new IP address, simply type the IP address on the box near to the **Add** button. Next, click **Add**. The new one will be added and displayed on the field under the box.  **Add** – click this button to have a field for adding a new IP address. **Save** – Click this button to save the setting. – click the icon to remove the selected entry.
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	Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**. **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.
Connection Detection Interval	Assign an interval period of time for each detecting.
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.

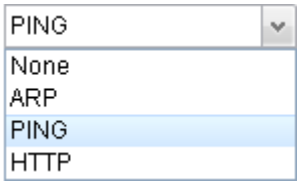
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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

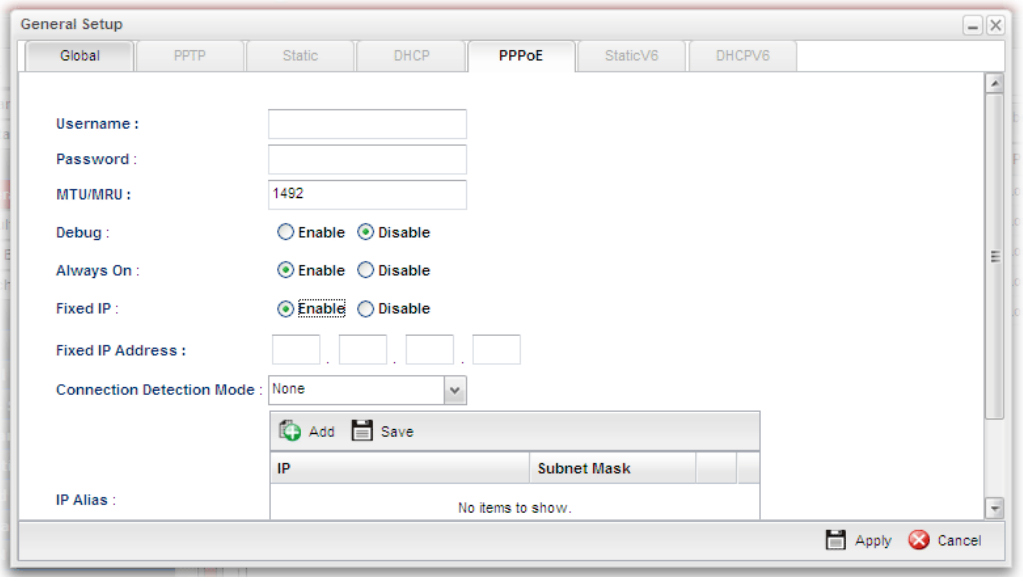


Available parameters are listed as follows:

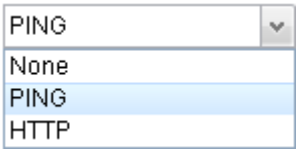
Item	Description
Host Name (Optional)	Type a name as the host name for identification.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**.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

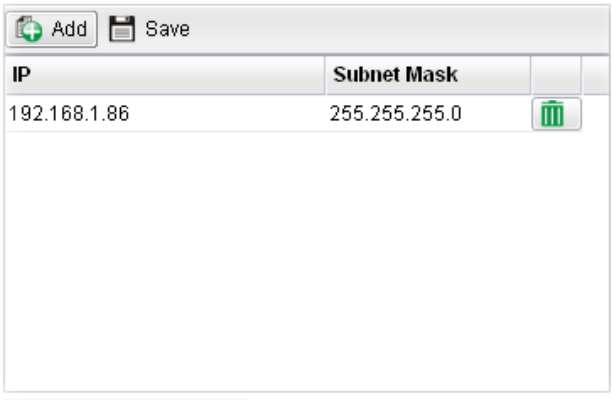
	address. **Save –** click this button to save the setting. – click the icon to remove the selected entry.
MTU/MRU	It means Max Transmit Unit for packet. The default setting is 1500.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are three ways **ARP**, **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Connection Detection Mode** is set with **PING** or **HTTP**. **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.
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 PPPoE as IPv4 protocol type, click the PPPoE Tab to open the following page:***

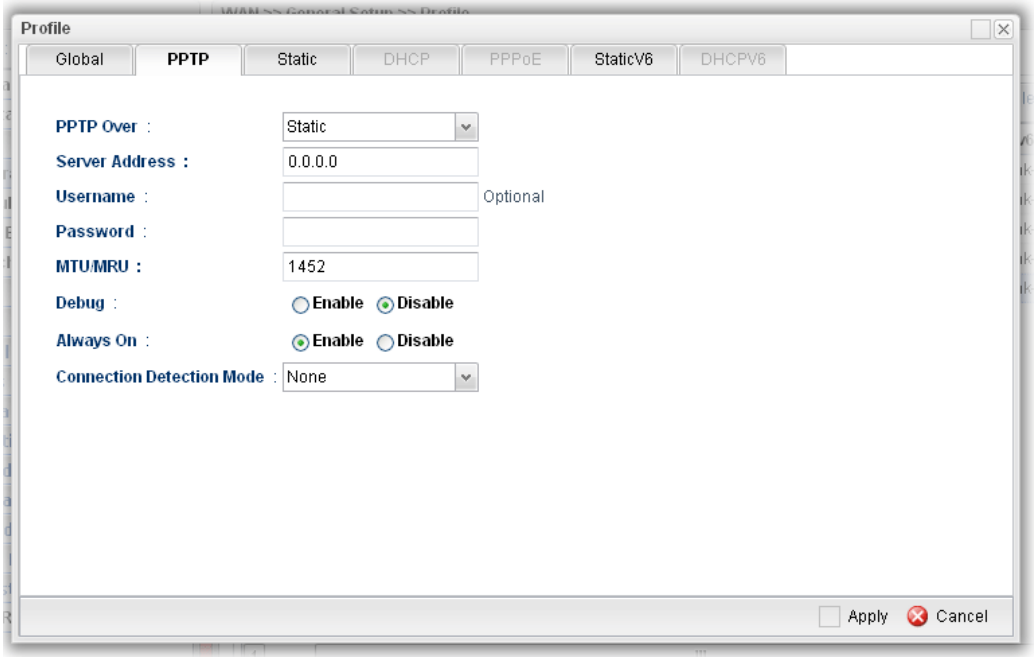


Available parameters are listed as follows:

Item	Description
Username	Type the user name offered by your ISP.
Password	Type the password offered by your ISP.
MTU/MRU	Type the value of MTU/MRU. The default value is 1492.
Debug	Click **Enable** to display the PPPoE debug message in Syslog. The default setting is **Disable**.
Always On	**Enable** – Click it to enable the function of Always On. The router will keep network connection all the time. **Disable** – Click it to disable the function of Always On.
Fixed IP	**Enable** – Click it to enable the function of fixed IP. **Disable** – Click it to disable the function of fixed IP.
Fixed IP Address	Type the IP address in the boxes.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways **PING** and **HTTP** supported in Vigor router for you to choose to send the request out. 
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field. Use the default setting.

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

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



Available parameters are listed as follows:

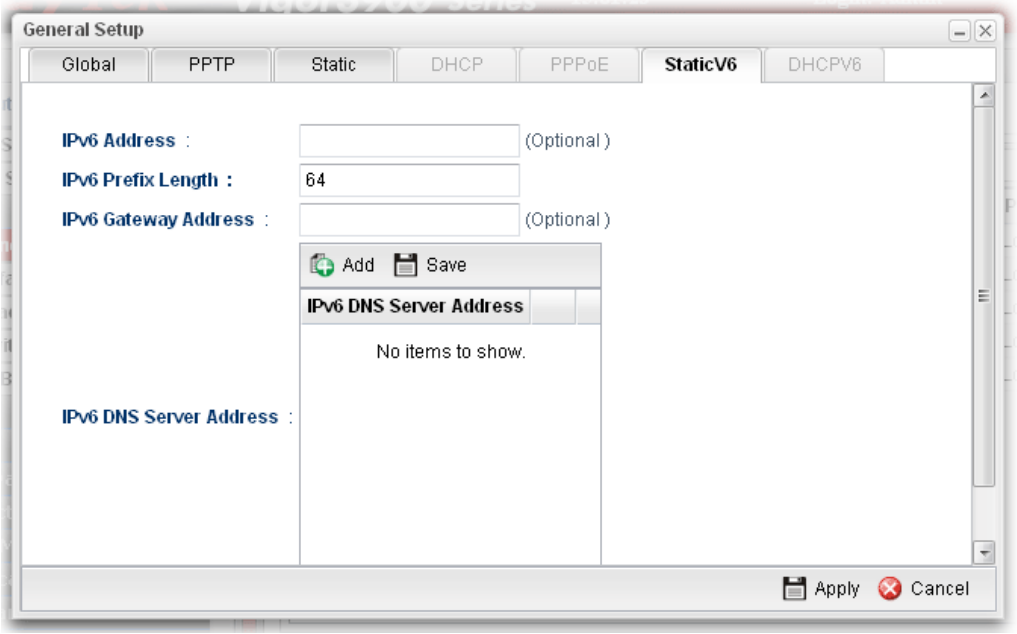
Item	Description
PPTP Over	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. **Please contact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

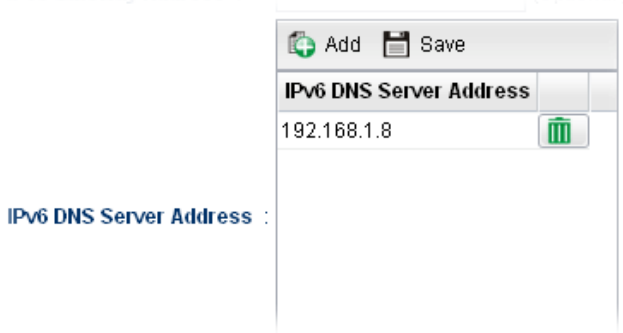
- ***If you choose Link-Local as IPv6 protocol type***

  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.

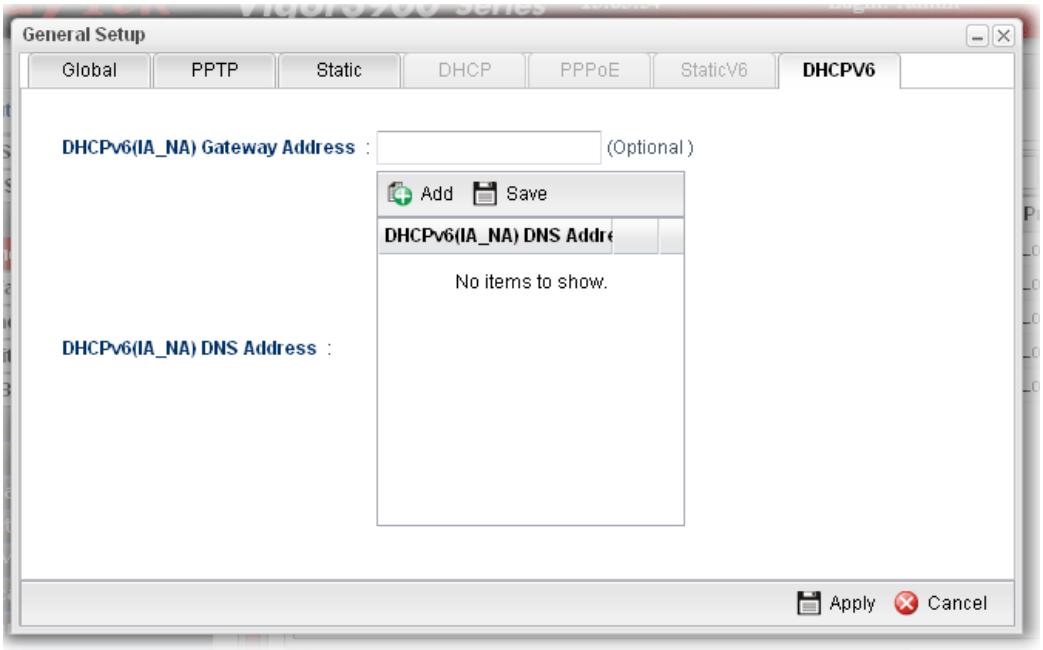
- ***If you choose Static as IPv6 protocol type, click the StaticV6 tab to open the following page:***



Available parameters are listed as follows:

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

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



Available parameters are listed as follows:

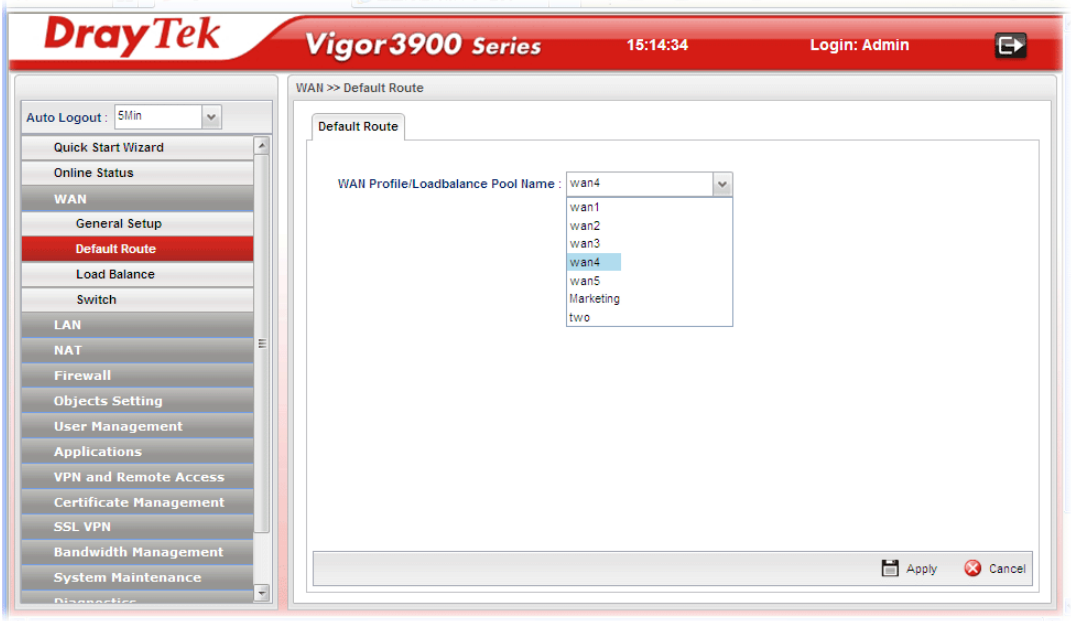
Item	Description
DHCP (IA_NA) Gateway Address	Type the gateway IP address for IPv6 DHCP IA_NA mode.
DHCP (IA_NA) DNS Address	Type your IPv6 primary DNS Server address. **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. – click the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

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

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

4.1.2 Default Route

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



Available parameters are listed as follows:

Item	Description
WAN Profile /Load Balance Pool Name	Display the WAN profiles for user to choose as a default route. In which, wan1 to wan5 are factory default settings.
Refresh	Renew the page configuration.
Apply	Click it to save the configuration.

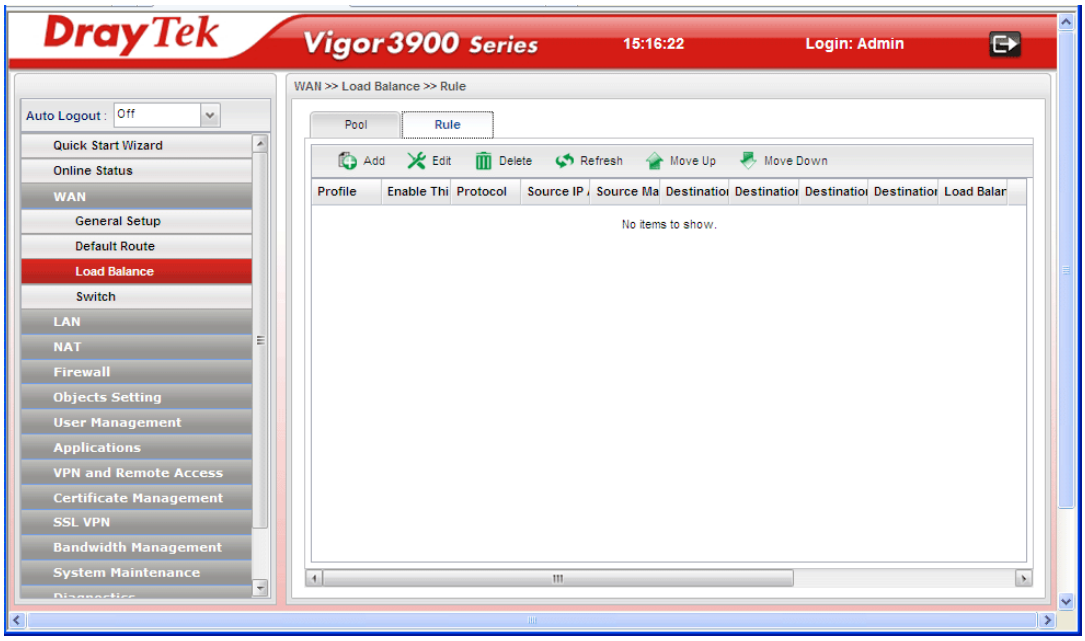
4.1.3 Load Balance Policy

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

In the **WAN** group, click the **Load Balance Policy** option.

Rule

This page will make the packets be transmitted with user defined profiles with IP address, protocol and WAN profile that is different with default route.



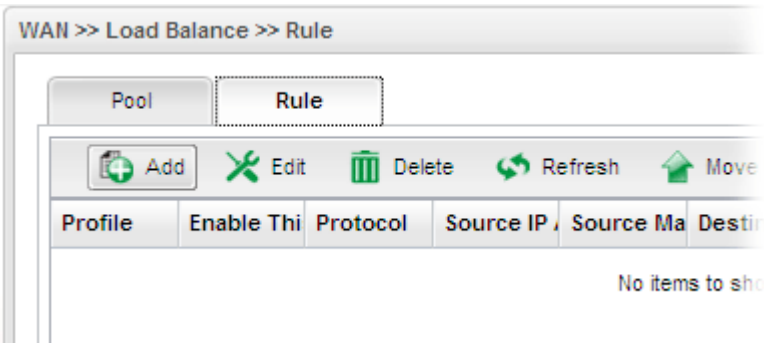
Each item will be explained as follows:

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.
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	Display the name of the rule.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.

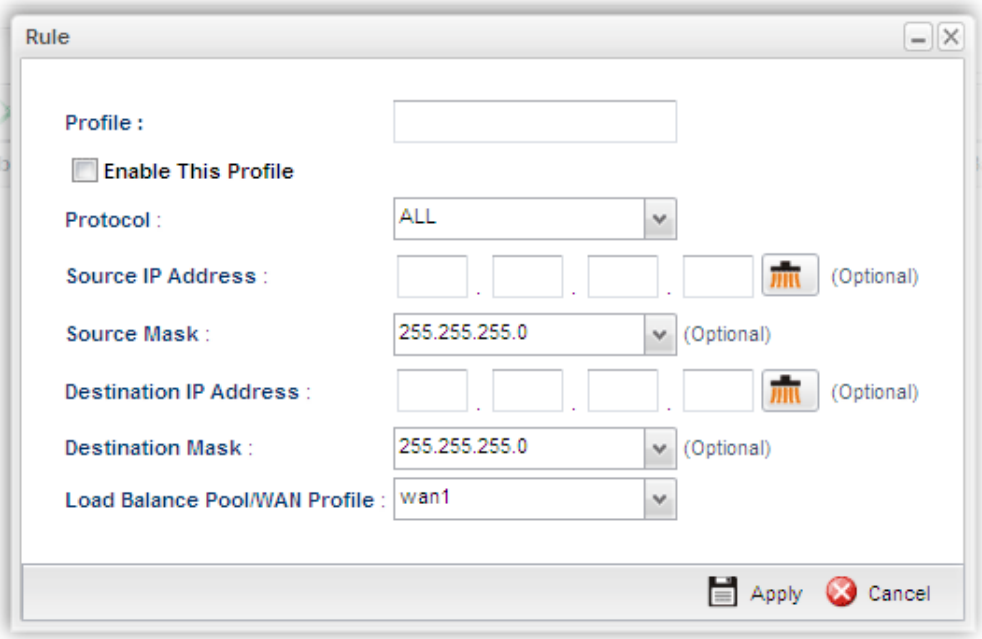
Protocol	Display the protocol of such rule.
Source IP Address	Display the WAN IP address here as the source IP address for such rule.
Source Mask	Display the mask for the source.
Destination IP Address	Display the WAN IP address here as the destination IP address for such rule.
Destination Mask	Display the mask for the destination.
Destination Port Start	Display the starting port value for the destination.
Destination Port End	Display the ending port value for the destination.
Load Balance Pool/WAN Profile	Display the WAN profile used by such rule.

How to add a new rule for Load Balance

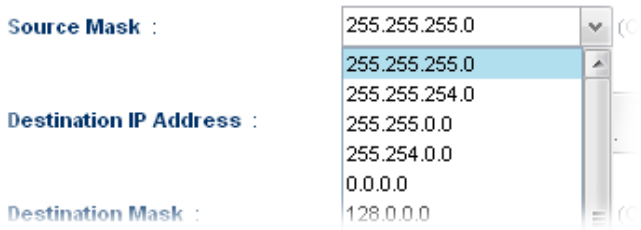
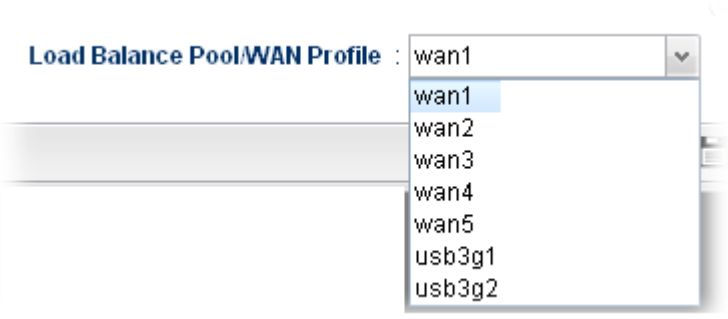
1. Open **WAN>>Load Balance** and click the tab of **Rule**.
2. Simply click the **Add** button.



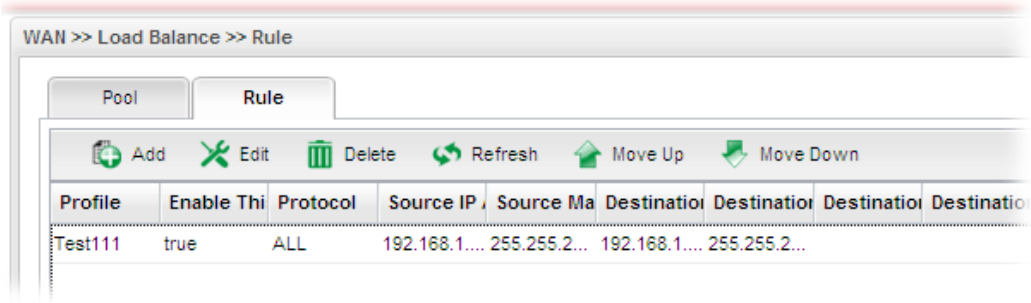
3. The following dialog will appear.



Available parameters are listed as follows:

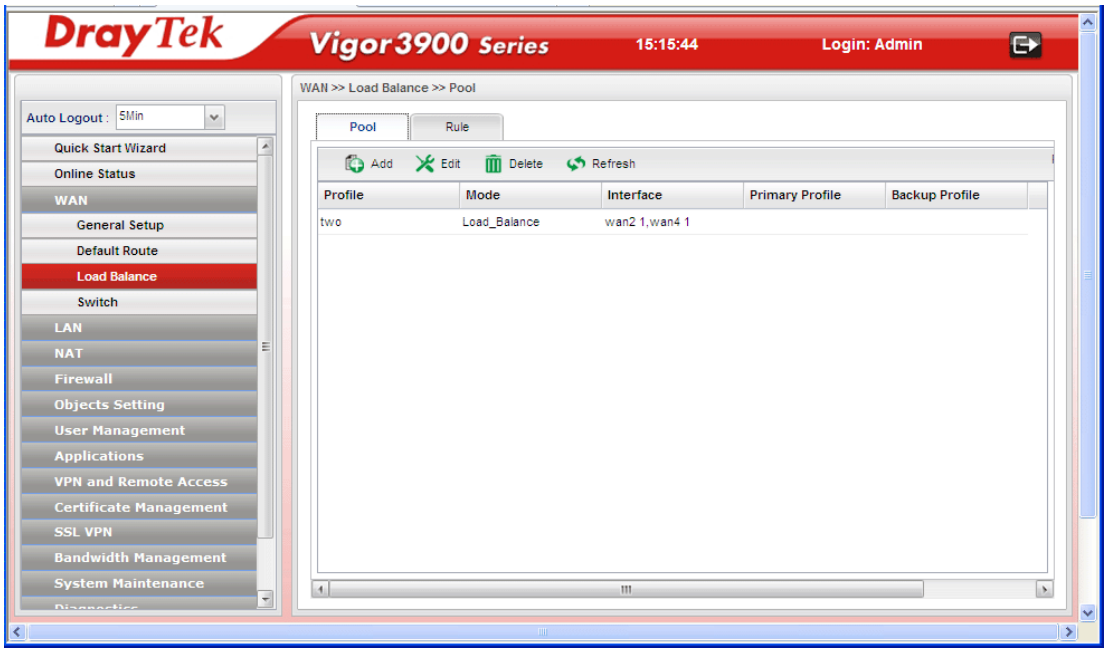
Item	Description
Profile	Type the name of the rule.
Enable This Profile	Check this box to enable such profile.
Protocol	Choose a protocol (ALL, TCP, UDP, ICMP, FTP, TFTP, HTTP, SMTP, POP3, TCP/UDP) for such rule applied to load balance. **All** is the default setting.
Source IP Address	Type a WAN IP address here as the source IP address for such rule. – click the icon to clear the IP setting.
Source Mask	Use the drop down list on the right to choose a suitable mask for the source. 
Destination IP Address	Type a WAN IP address here as the destination IP address for such rule. – click the icon to clear the IP setting.
Destination Mask	Use the drop down list on the right to choose a suitable mask for the destination.
Load Balance Pool /WAN Profile	Choose one of the profiles to be used by such rule. In which, wan1 to wan5 profiles are configured in default. In addition, profiles configured in **WAN>>Load Balance Policy>> Pool** page also will be displayed here. To have user-defined WAN profile, please refer to **WAN<<General Setup** for detailed information. 
Apply	Click it to save the configuration.
Cancel	Click it to return to the factory setting.

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



Pool

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 **WAN>>Default Route** page.



Each item will be explained as follows:

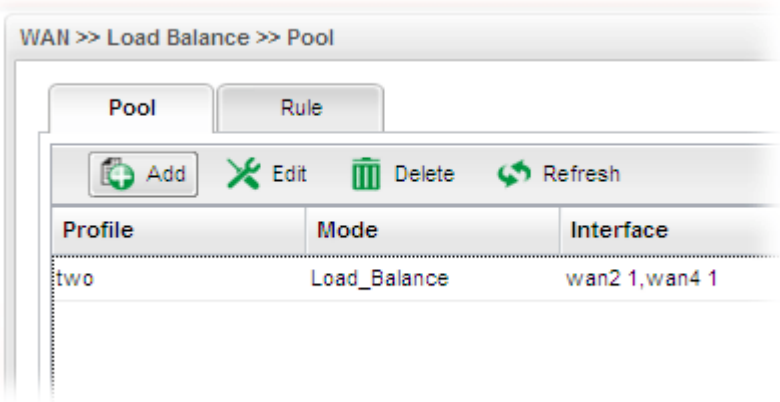
Item	Description
Add	Add a new pool profile.
Edit	Modify the selected pool profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected rule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

Mode	Display the mode (failover or load balance) used by the pool profile.
Interface	Display the name of the WAN profiles for Load Balance rule.
Primary Profile	Display the primary profile configured in Failover page for such profile.
Backup Profile	Display the backup profile configured in Failover page for such profile.

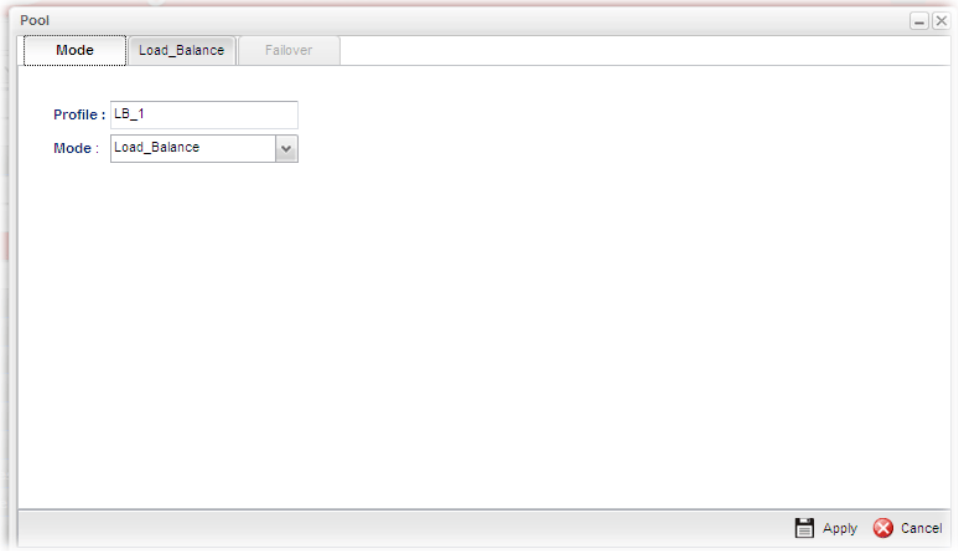
There are two modes, **Load_Balance** and **Failover**, for you to choose as the **Pool** configuration. If you choose **Load_Balance**, the tab of **Load_Balance** will be shown which allows you to configure for different WAN interfaces. If you choose **Failover**, the tab of **Failover** will be displayed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

How to add a Pool profile for Load Balance

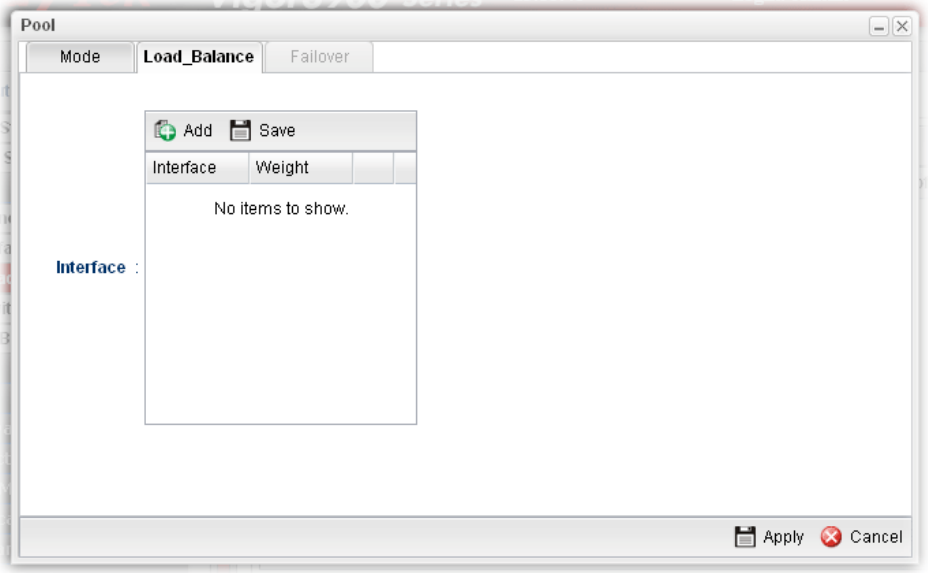
1. Open **WAN>>Load Balance Policy** and click the tab of **Pool**.



2. Simply click the **Add** button to open the following dialog. Type a name (e.g., LB_1) for such profile. Choose **Load_Balance** as the **Mode** selection.

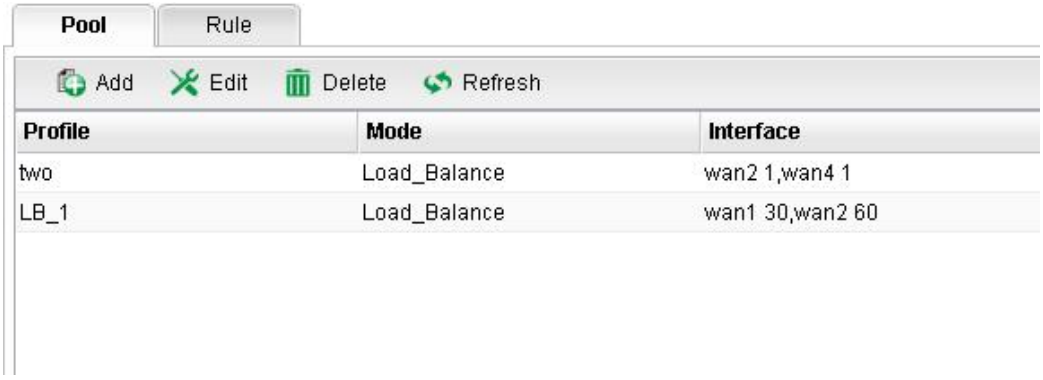


3. Click the **Load_Balance** Tab.



4. Click **Add**. A new line for adding new entry will appear.
5. 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**.

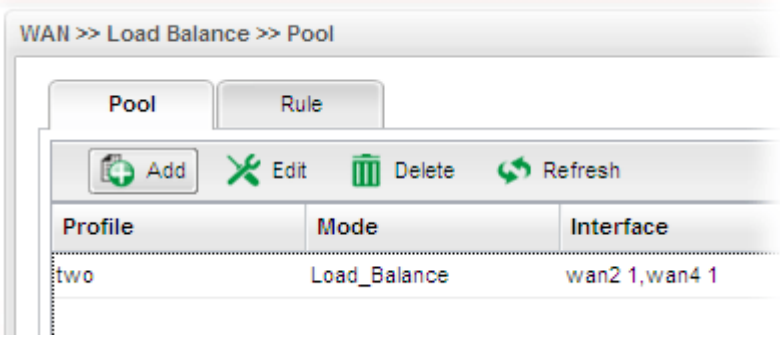
6. Click **Apply**. A new profile will be added on the page.



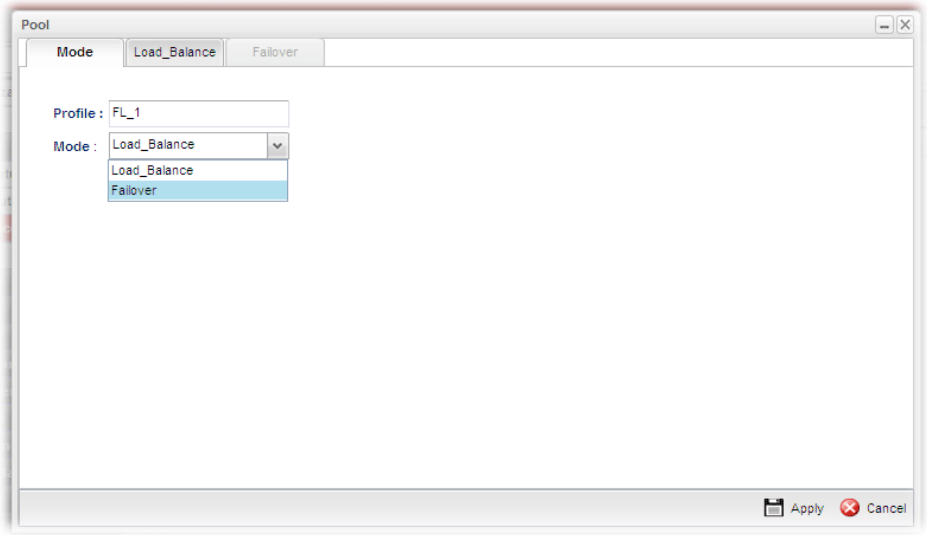
How to add a Pool profile for Failover

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

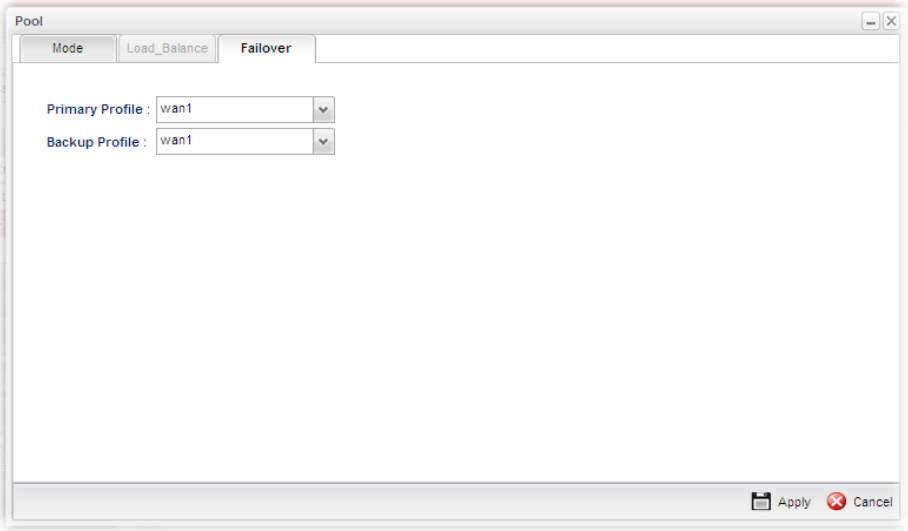
1. Open **WAN>>Load Balance Policy** and click the tab of **Pool**.



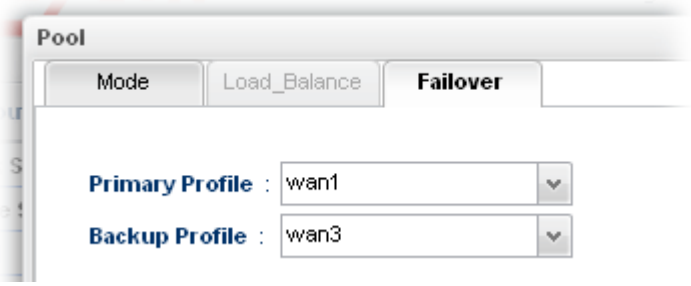
2. Simply click the **Add** button to open the following dialog. Type a name (e.g., FL_1) for such profile. Choose **Failover** as the **Mode** selection.



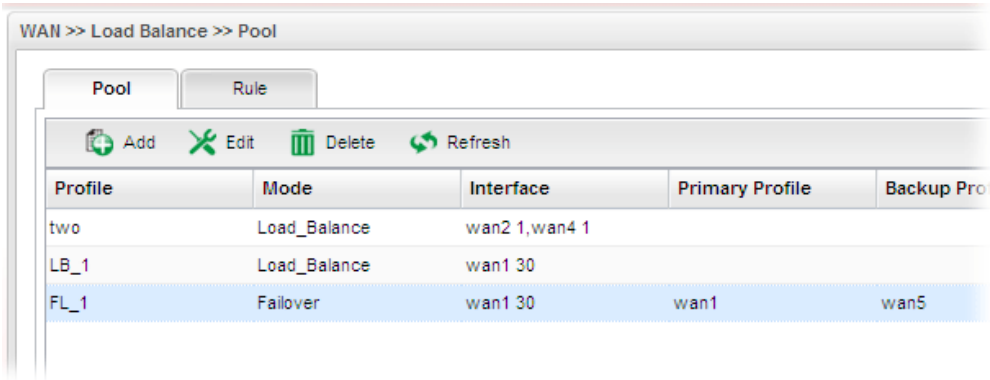
3. Click the **Failover** Tab. In default, the system will apply Primary Profile. If Primary Profile cannot be used any more, the Backup Profile will be used instead.



4. Use the drop down list to choose the one you need. "**wan1"** to **wan5**" are default settings.



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



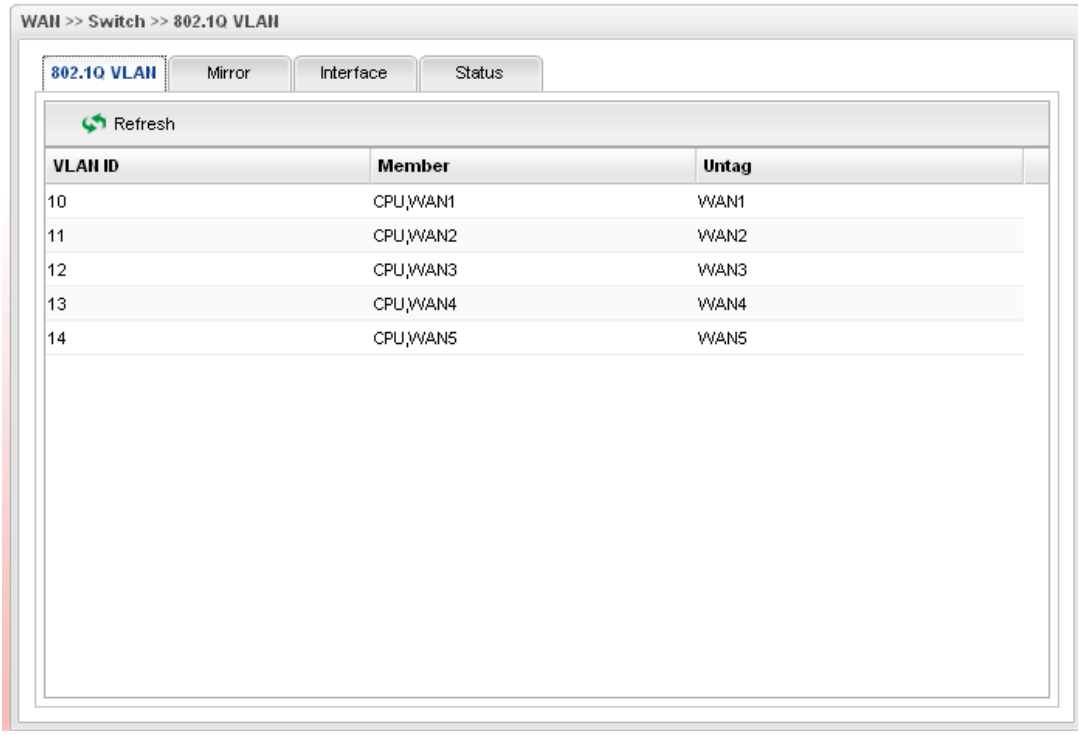
4.1.4 Switch

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.

802.1Q VLAN Configuration

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

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



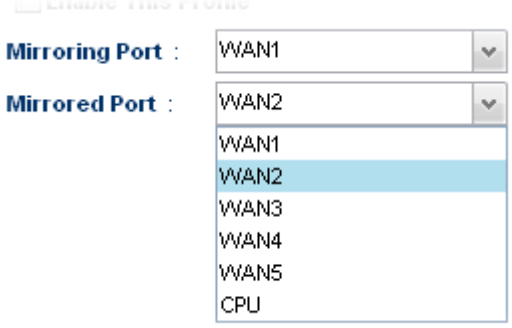
Each item will be explained as follows:

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

Mirror Configuration

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

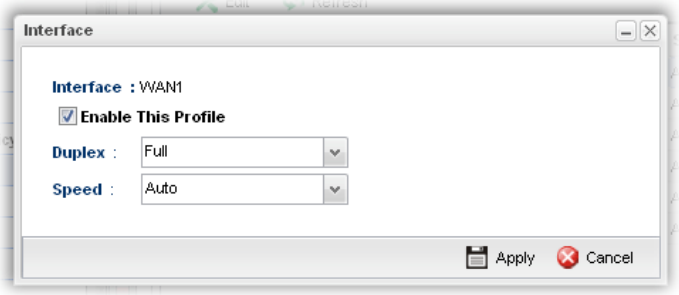
Available parameters are listed as follows:

Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Mirroring Port	Select a port for the administrator to use for viewing traffic sent from mirrored ports.
Mirrored Port	Select a port to make the packets passing through it monitored by the administrator. 
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

Interface Configuration

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

Each item will be explained as follows:

Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.  **Interface** – Display the name of WAN interface. **Enable This Profile** – Check it to enable such interface. **Duplex** – Use the drop down list to choose the duplex (**Full** or **Half**) for such profile. **Speed** – Use the drop down list to specify the transmission rate (**Auto, 10M, 100M** or **1000M**) for such interface. **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 This Profile	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.

Status of the Switch

This page provides information about speed, duplex, port connection (UP or Down) for the WAN ports.

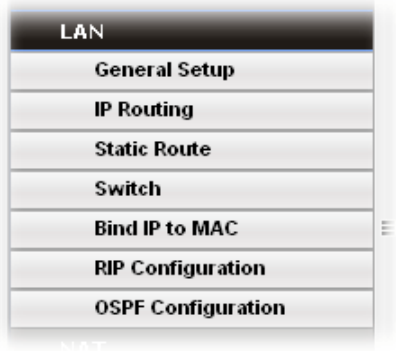
Available parameters are listed as follows:

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.
Interface	Display the physical port of the WAN interface.
Status	Display if the port connection for WAN interface is linked or not. **Up** means the network is connected; **Down** means the network is not connected.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such WAN interface.
Duplex	Display the duplex used (full or half) by such WAN interface.

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.

General Setup

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

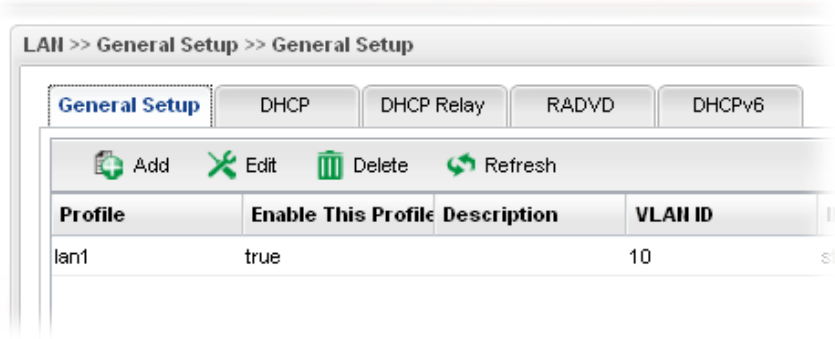
Each item will be explained as follows:

Item	Description
Add	Add a new LAN profile.

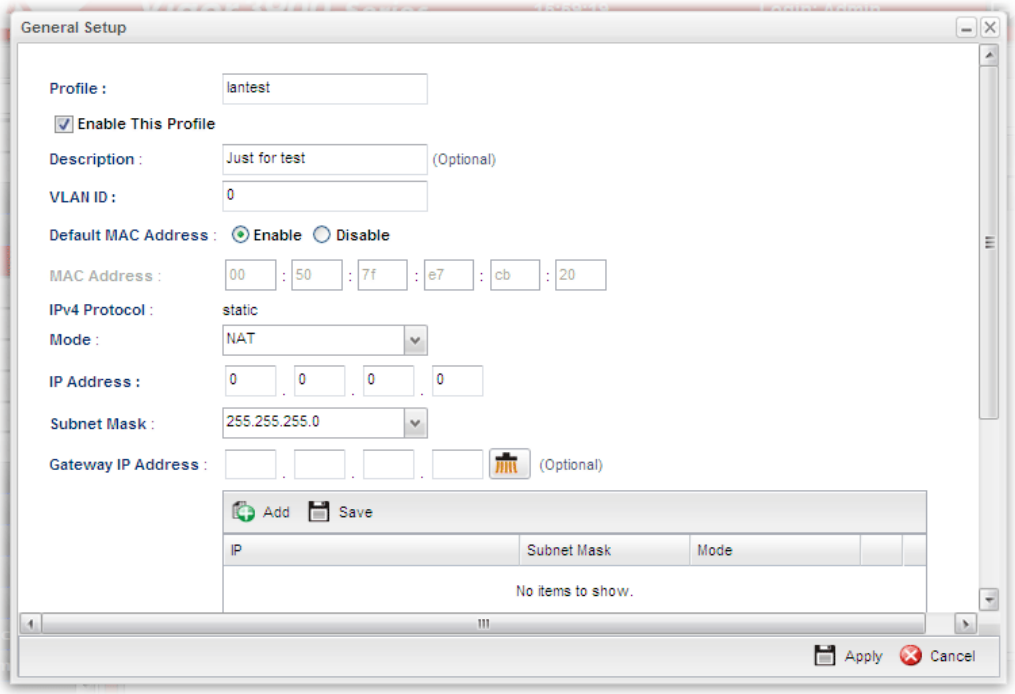
Edit	Modify the selected LAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected LAN profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page
Profile	Display the name of the LAN profile.
Enable This Profile	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 Type	Display the IPv4 protocol type for the LAN profile.
IPv6 Protocol Type	Display the IPv6 protocol type for the LAN profile.

How to add a new LAN profile

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

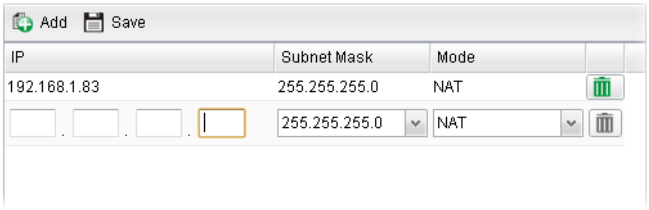


2. Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.

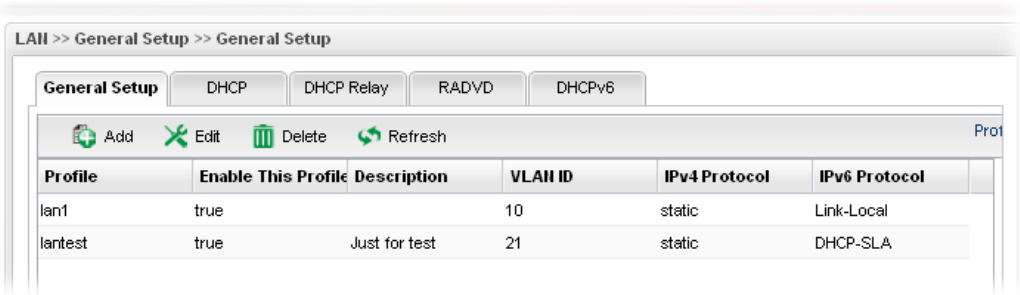


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the LAN profile.
Enable This Profile	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.
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 from the drop down list for such profile.
IPv4 Protocol	Display the type 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 of the router for the LAN profile.
Subnet Mask	Use the drop down list to choose a suitable mask for the LAN profile.
Gateway IP Address	Such IP address is ready for matching with the function of Virtual System. – click the icon to clear the IP setting.
2nd Subnet	Specify one 2nd subnet which might be needed in the future.

	 **Add** – Click it to add a new subnet mask with IP address and specified mode. **Save** – Click it to save the settings. **IP** – Type the IP address if you click Add for adding a new entry. **Subnet Mask** – Use the drop down list to choose the one you want. **Mode** – Specify NAT or Routing as the mode. – click the icon to remove the selected entry.
IPv6 Protocol	It defines the IPv6 connection types for LAN interface. Possible types contain Link-Local, Static and DHCP-SLA. Except Link-Local, each type requires different parameter settings. **Link-Local**- Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address. **Static** –This type allows you to setup static IPv6 address for LAN. **DHCP-SLA**- DHCPv6 client mode would use IA_NA option of DHCPv6 protocol to obtain IPv6 address from server.
IPv6 Address	If **Static** is chosen as IPv6 Protocol, please type the IPv6 address in this field.
IPv6 Prefix Length	Display the IPv6 prefix length.
DHCPv6 SLA WAN Interface	If **DHCP-SLA** is chosen as IPv6 Protocol, please choose one of the WAN profiles in this field.
DHCPv6 SLA ID	The ID number set here is used by an individual organization to create its own local addressing hierarchy and to identify subnets.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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



DHCP

In the Vigor3900 router, there are some IP address settings for the LAN interface. The IP address/subnet mask is for private users or NAT users. The IP address of the default gateway on other local PCs should be set as the Vigor3900 server IP address. When the DSL connection between the DSL and the ISP has been established, each local PC can directly route to the Internet. The IP address/subnet mask can also be used to connect to other private users (PCs). On this page you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the route.

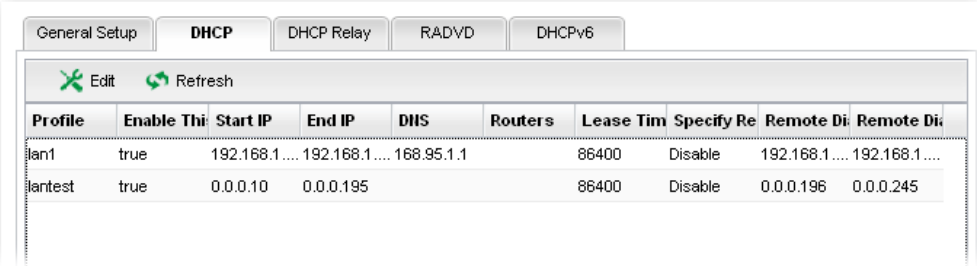
Each item will be explained as follows:

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.

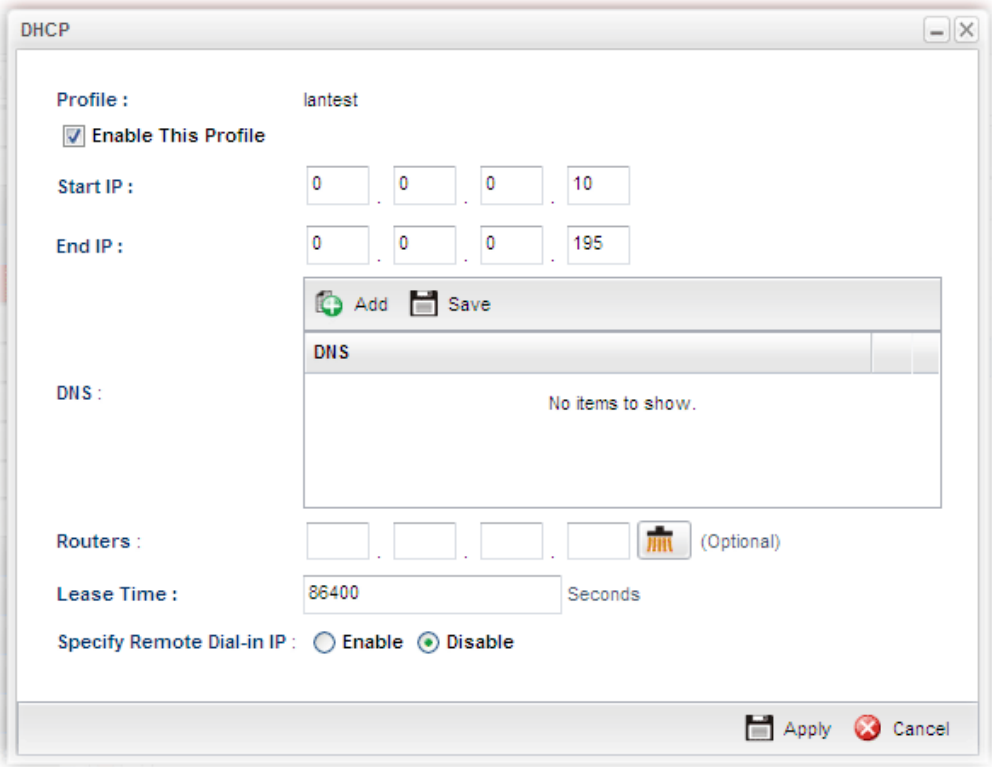
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Start IP	Display the starting IP address of the IP address pool for DHCP server.
End IP	Display the ending IP address of the IP address pool for DHCP server.
DNS	Display the IP address for DNS.
Routers	In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user.
Lease Time	Display the lease time for the DHCP server.
Specify Remote Dial-in IP	Display the status of remote dial-in function. Disable means disabled; Enable means enabled.
Remote Dial-in Start IP	Display the start IP address for an IP range. The DHCP server can assign an IP address for remote dial-in user from such IP range.
Remote Dial-in End IP	Display the end IP address for an IP range. The DHCP server can assign an IP address for remote dial-in user from such IP range.

How to edit a LAN profile for DHCP

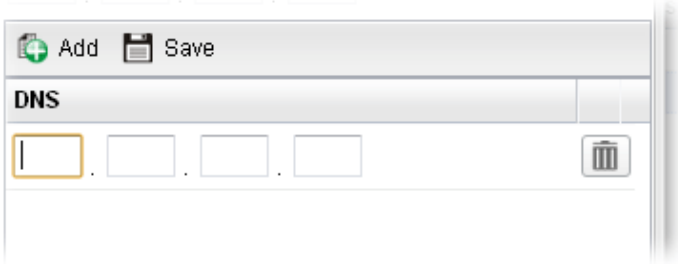
1. Open **LAN>>General Setup** and click the **DHCP** tab.



2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.



Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
Start IP	Set the starting IP address of the IP address pool for DHCP server.
End IP	Set the ending IP address of the IP address pool for DHCP server.
DNS	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. – click the icon to remove the selected entry.
Routers	In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user. However, if you want to use other gateway, please assign the IP address in this field.

	– click the icon to clear the IP setting.
Lease Time	Set a lease time for the DHCP server. The time unit is minute.
Specify Remote Dial-in IP	**Enable** – Enable this function that remote clients within the range specified below can access into Vigor3900 WUI. **Disable** – Disable this function.
Remote Dial-in Start IP	Specify the start IP address for an IP range. The DHCP server can assign an IP address for remote dial-in user from such IP range.
Remote Dial-in End IP	Specify the end IP address for an IP range. The DHCP server can assign an IP address for remote dial-in user from such IP range
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

5. The LAN profile has been edited.

DHCP Relay

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

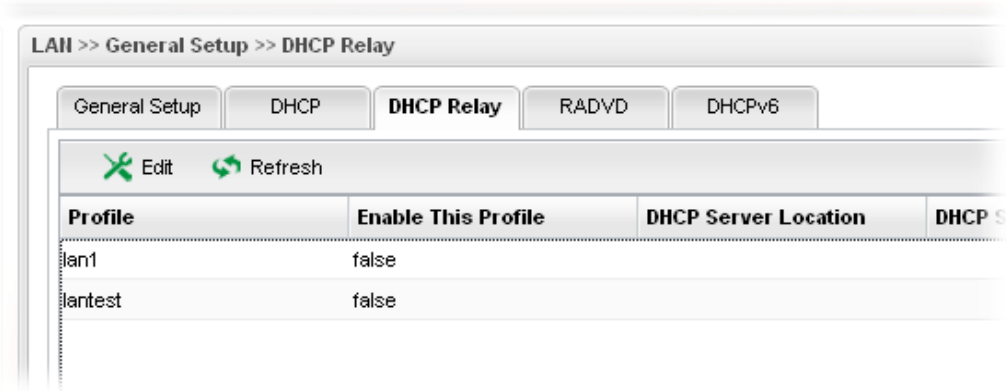
Each item will be explained as follows:

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

	rule.
Refresh	Renew current web page.
Profile	Display the name of the LAN profile.
Enable This Profile	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.

How to edit a LAN profile for DHCP Relay

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



2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.

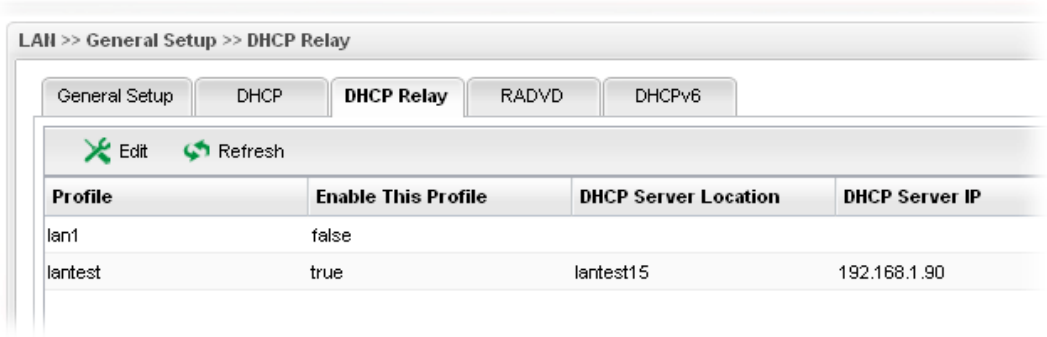
Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
DHCP Server Location	Type the LAN or WAN profile for the DHCP server
DHCP Server IP	Type the IP address of DHCP Server.
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.



RADVD

The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.

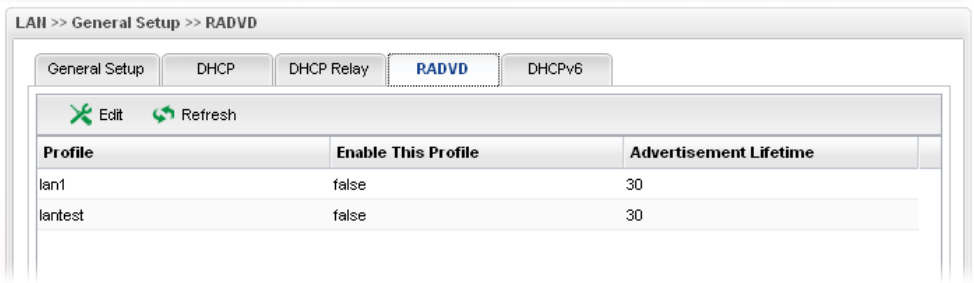
Each item will be explained as follows:

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

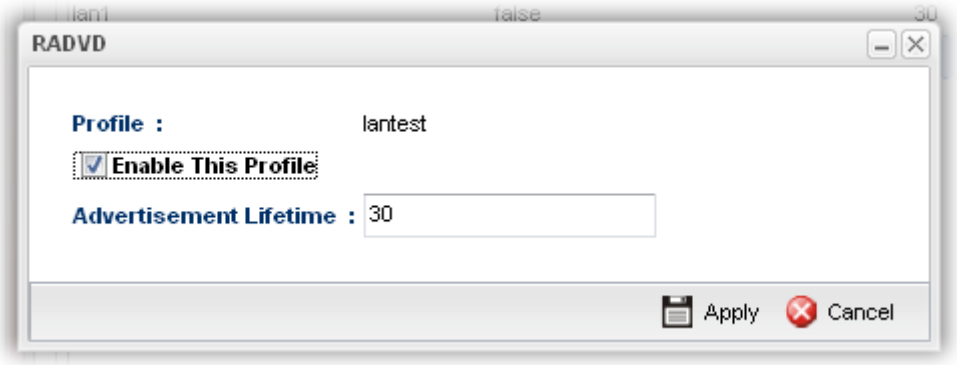
Profile	Display the name of the LAN profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Advertisement Lifetime	Display the lifetime value. The lifetime associated with the default router in units of minutes, ranging from 10 ~ 150. It is used to control the lifetime of the prefix. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.

How to edit a LAN profile for RADVD

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



2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.



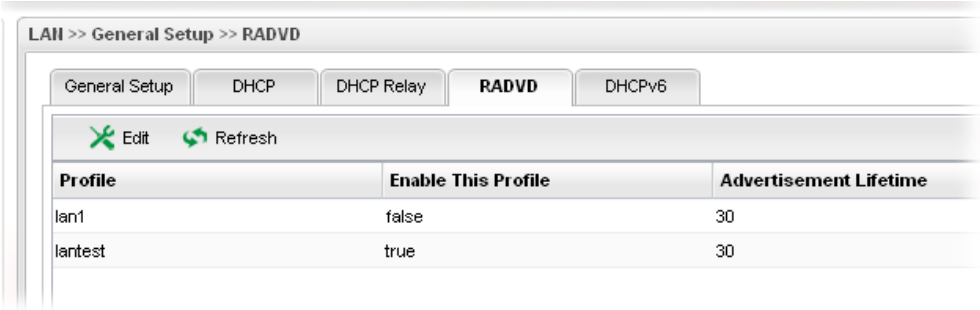
Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	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 **Appl**y to save the configuration and exit the dialog.

4. The LAN profile has been edited.



DHCP6

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

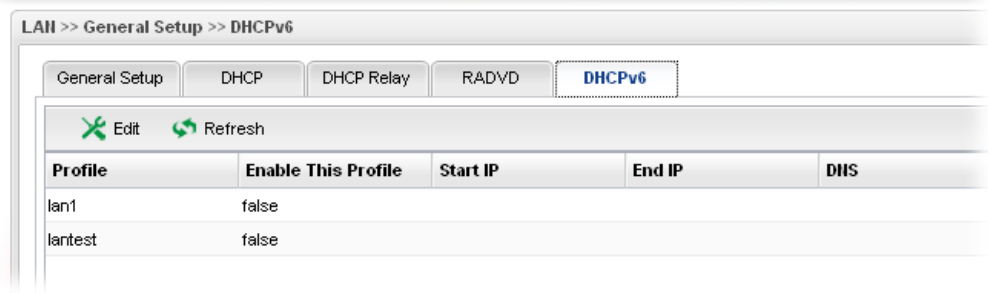
Each item will be explained as follows:

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

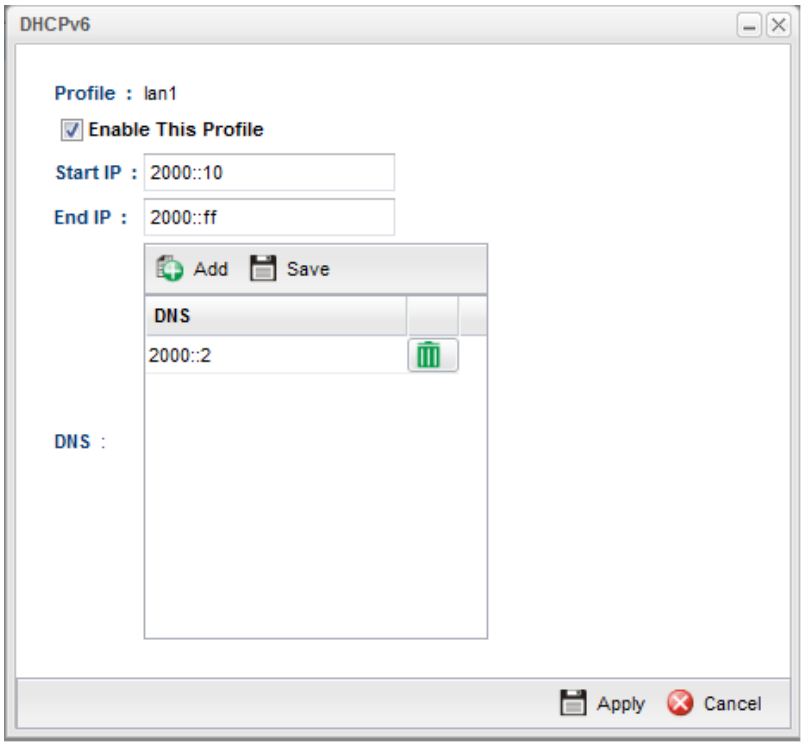
	means enabled.
Start IP	Display the starting IP address of the IP address pool for DHCP server.
End IP	Display the ending IP address of the IP address pool for DHCP server.
DNS	Display the private IP address for DNS server.

How to edit a LAN profile for DHCPv6

1. Open **LAN>>General Setup** and click the **DHCPv6** tab.

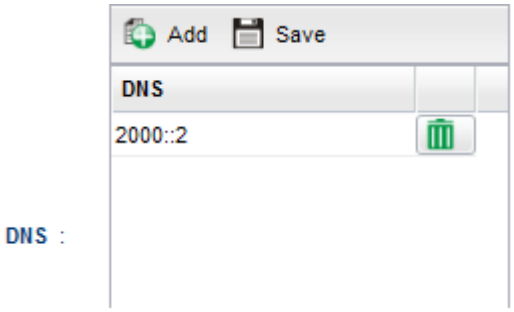


2. Choose one of the LAN profiles by clicking on it and click the **Edit** button to open the following dialog.



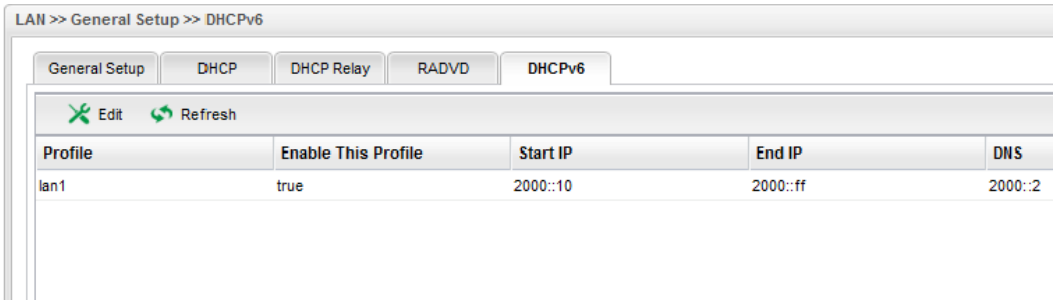
Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
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	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. – click the icon to remove the selected entry.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4. The LAN profile has been edited.



4.2.2 IP Routing

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

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

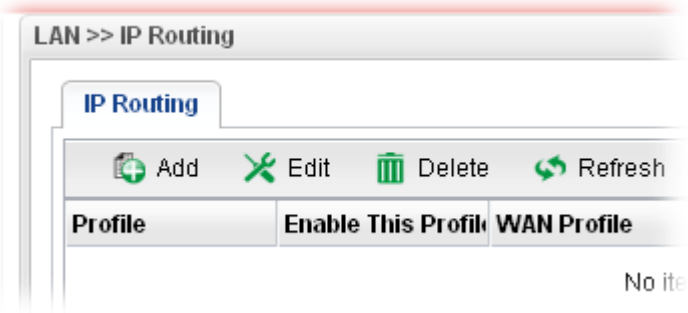
Each item will be explained as follows:

Item	Description
Add	Add a new IP Routing profile.
Edit	Modify the selected IP routing setting. To edit the IP routing 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 profile.
Delete	Remove the selected route setting. To delete a static route setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of such IP route profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display which WAN profile used for sending out the data packets.

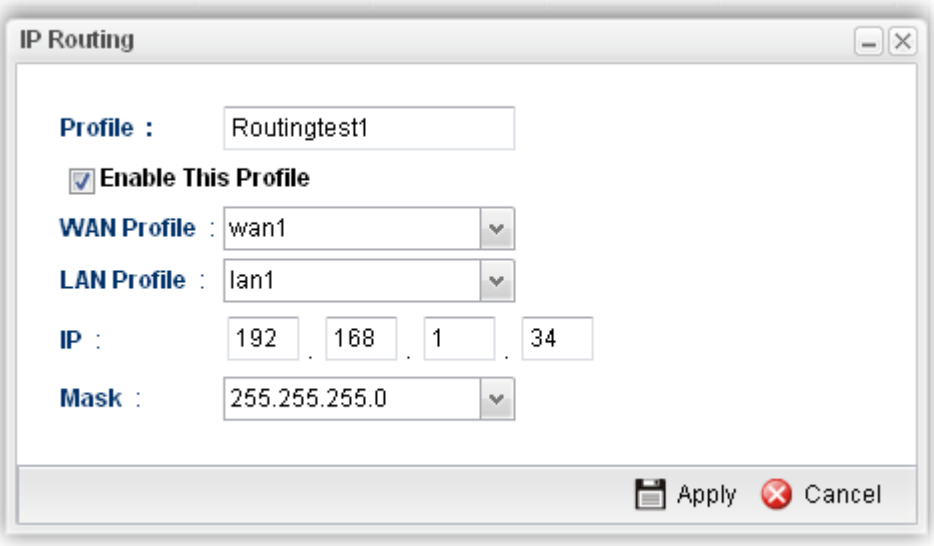
LAN Profile	Display which LAN profile used for the local device.
IP	Display the private IP address for such profile.
Mask	Display the subnet mask for such profile.

How to add a new IP Routing profile

1. Open **LAN>>IP Routing**.
2. Click the **Add** button.



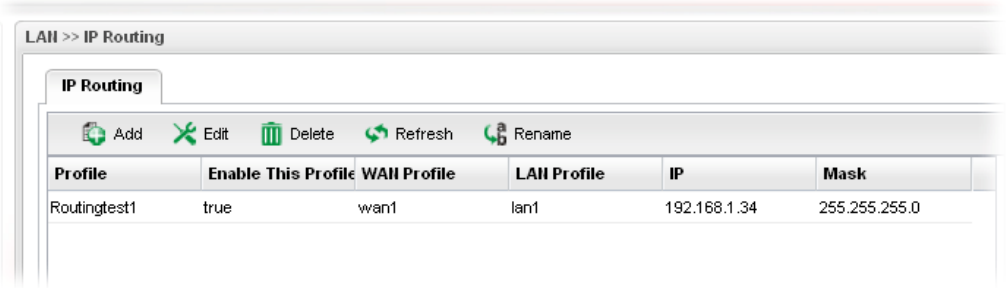
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IP routing profile.
Enable This Profile	Check this box to enable such IP routing profile.
WAN Profile	Choose one of WAN profiles for sending data out.
LAN Profile	Choose one of LAN profiles for the local device.
IP	Type the private IP address for such IP routing profile.
Mask	Type the subnet mask for such IP routing profile.

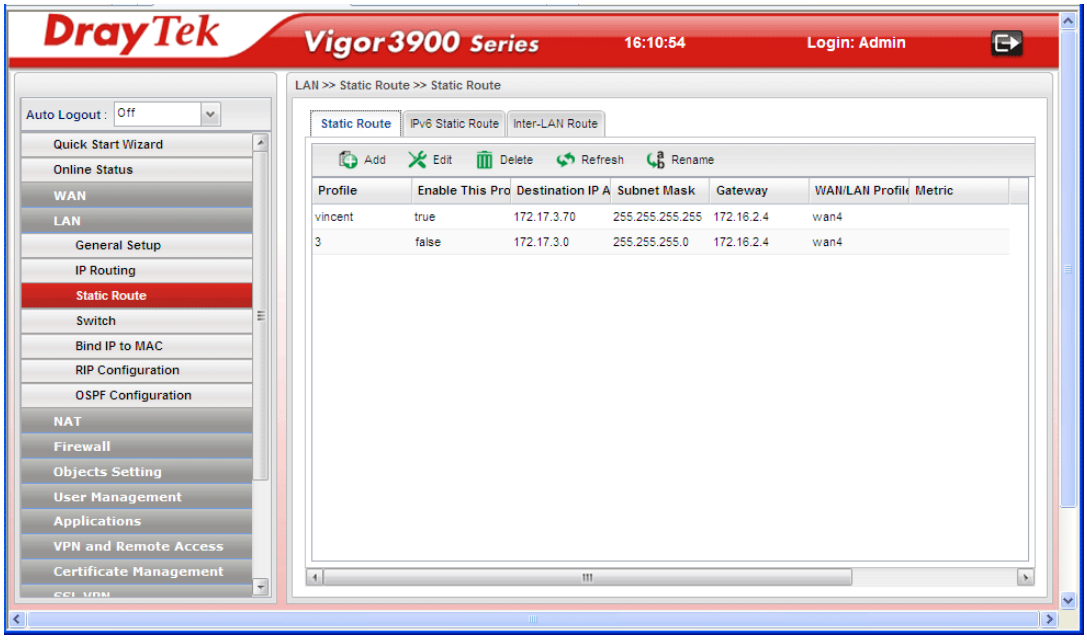
4. Enter all the settings and click **Apply**. The new profile will be added on the screen.



4.2.3 Static Route

When there are several subnets in LAN or WAN, a more effective and quicker way for connection is static route rather than other methods. Simply set rules to forward data to specified subnet through the specific gateway.

Static Route



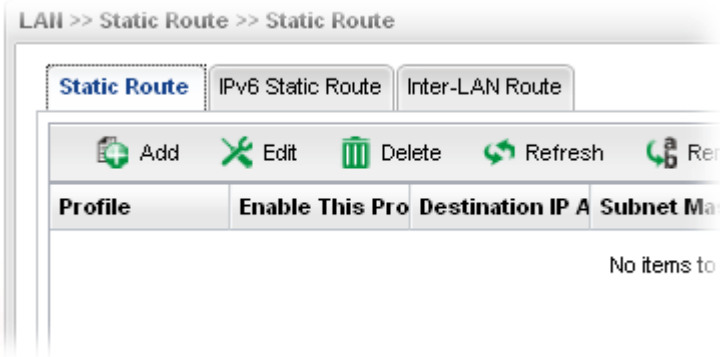
Each item will be explained as follows:

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

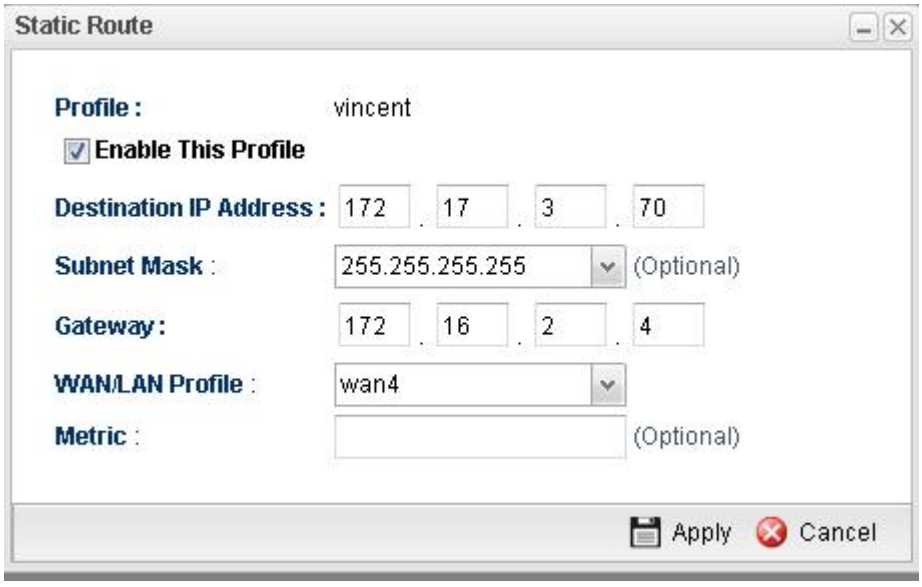
Profile	Display the name of such static route.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Destination IP Address	Display the IP address for such static route profile.
Subnet Mask	Display the subnet mask for such static route profile.
Gateway	Display 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 **LAN>>Static Routing** and click the **Static Route** tab.
2. Click the **Add** button.



3. The following dialog will appear.

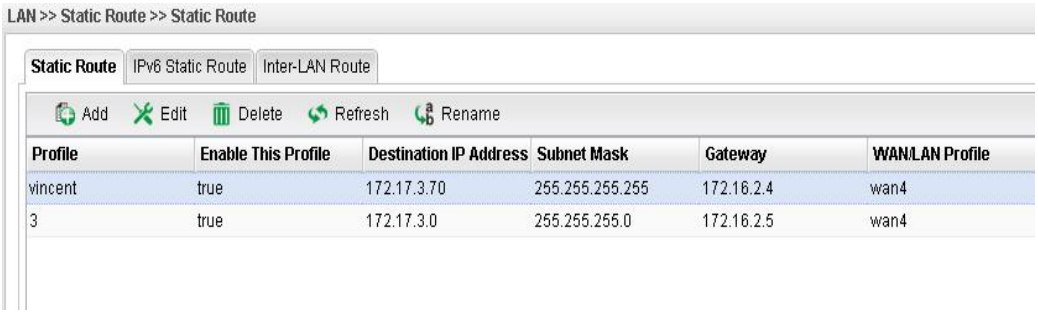


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the static route profile.
Enable This Profile	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 the settings and click **Apply**. The new profile will be added on the screen.



IPv6 Static Route

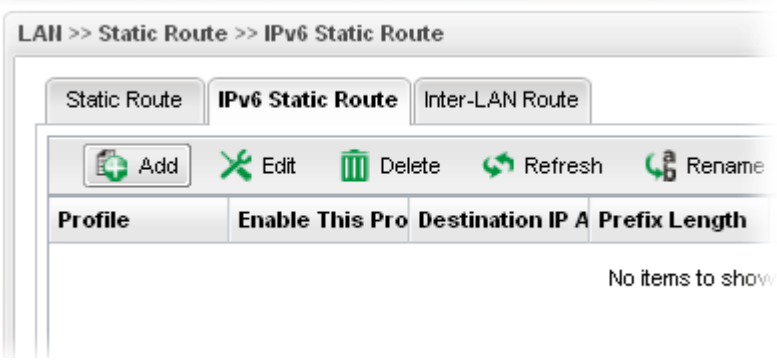
For IPv6 protocol, click the **IPv6 Static Route** tab to configure detailed settings.

Each item will be explained as follows:

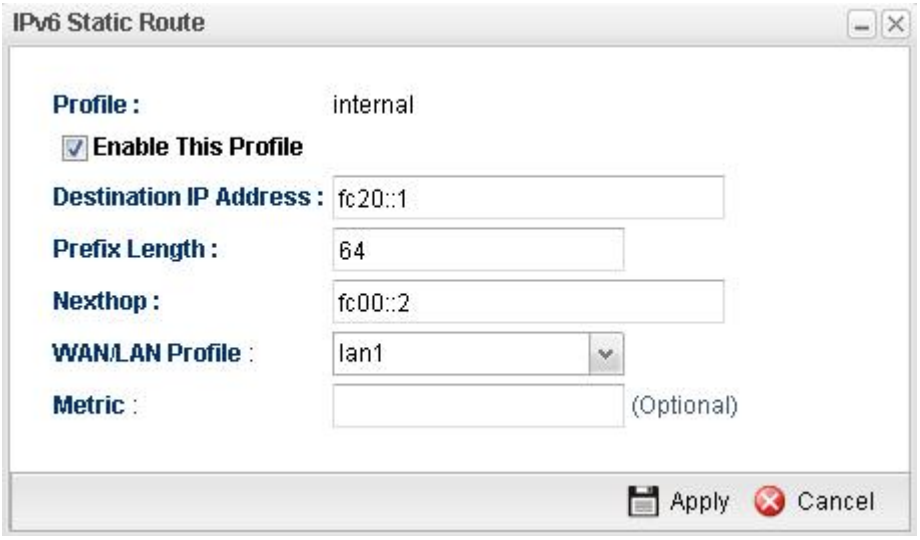
Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected static route setting. To delete a static route setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of such static route.
Enable This Profile	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 **LAN>>Static Route** and click the **IPv6 Static Route** tab.
2. Click the **Add** button.



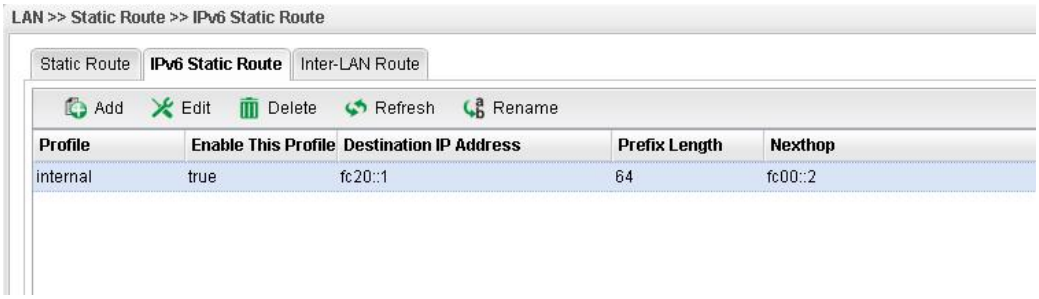
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile Name	Type the name of the static route profile.
Enable This Profile	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 the settings and click **Apply**. The new profile will be added on the screen.



Inter-LAN Route

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

4.2.4 Switch

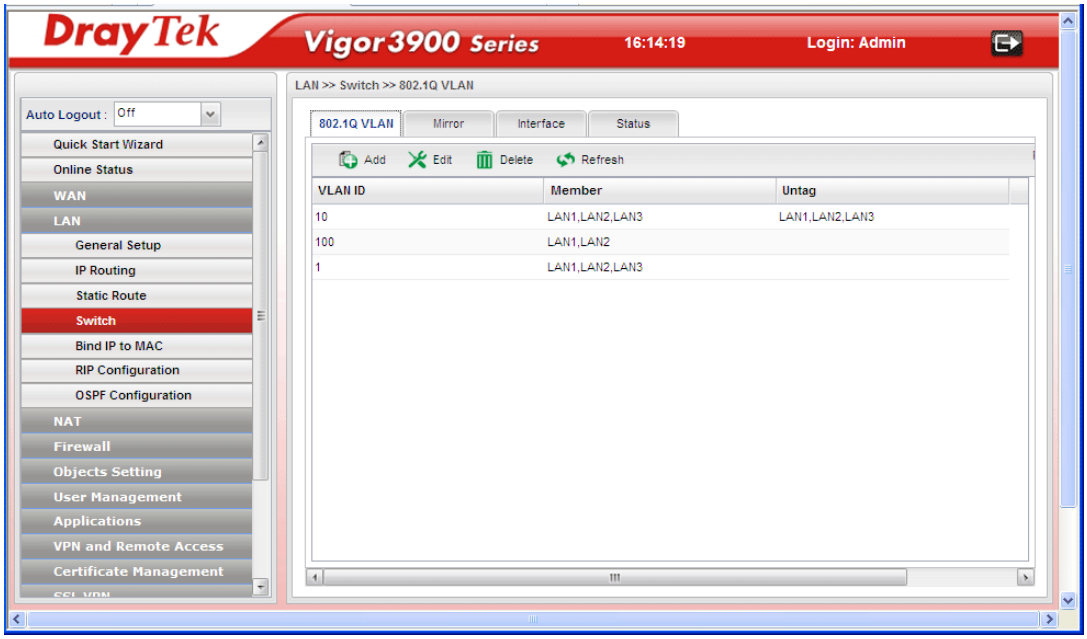
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable LAN interface, and configure 802.1Q VLAN ID for different LAN interfaces, and so on.

802.1Q VLAN

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

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

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



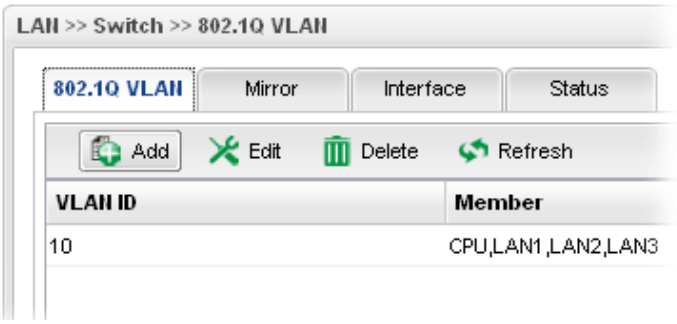
Each item will be explained as follows:

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

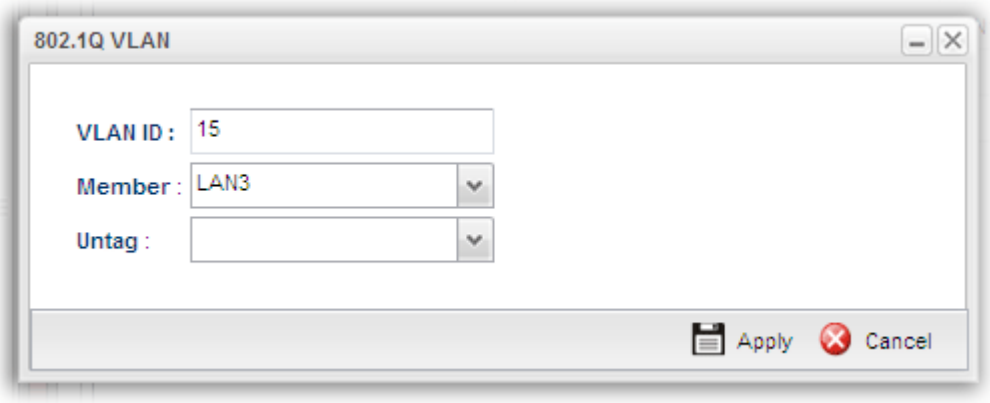
	selected rule.
Delete	Remove the selected VLAN ID setting. To delete a VLAN ID setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
VLAN ID	Display the VLAN ID number.
Member	Display the LAN interface that is used to access into Internet for such LAN profile with the VLAN ID number.
Untag	Display the LAN interface that packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or untagged.

How to add a new 802.1Q VLAN profile

1. Open **LAN>>Switch** and click the **802.1Q VLAN** tab.
2. Click the **Add** button.



3. The following dialog will appear.

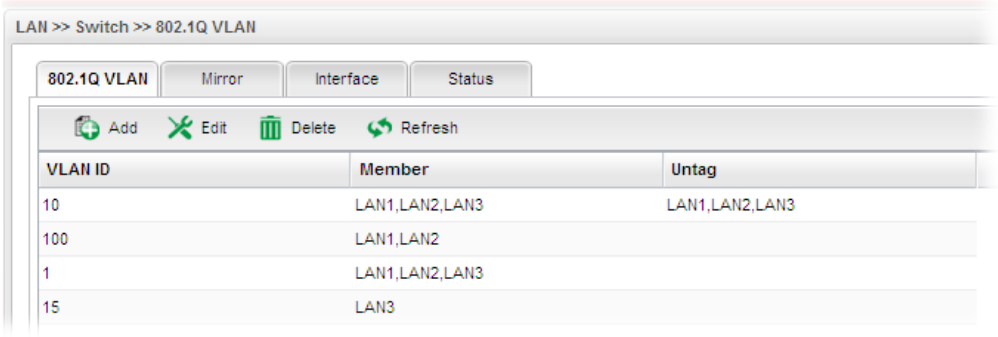


Available parameters are listed as follows:

Item	Description
VLAN ID	Type the number as the VLAN ID. Type a number used for identification on VLAN for your computer. Later, you have to type the same ID number for each PC which wants to be grouped within the same VLAN group.
Member	Determine which LAN interface can be used to access into

	Internet for such LAN profile with the VLAN ID number.
Untag	Determine if the packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or not.
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.

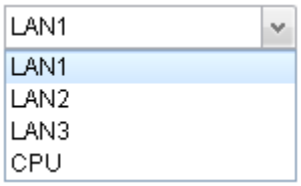
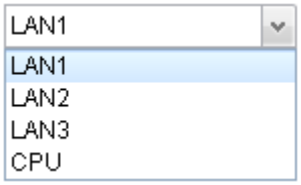


Mirror

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

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

Available parameters are listed as follows:

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

Interface

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

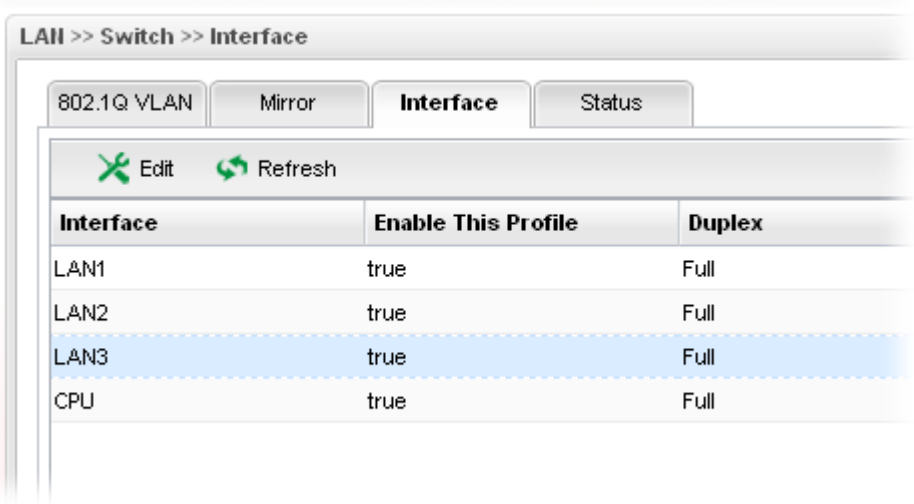
Each item will be explained as follows:

Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.

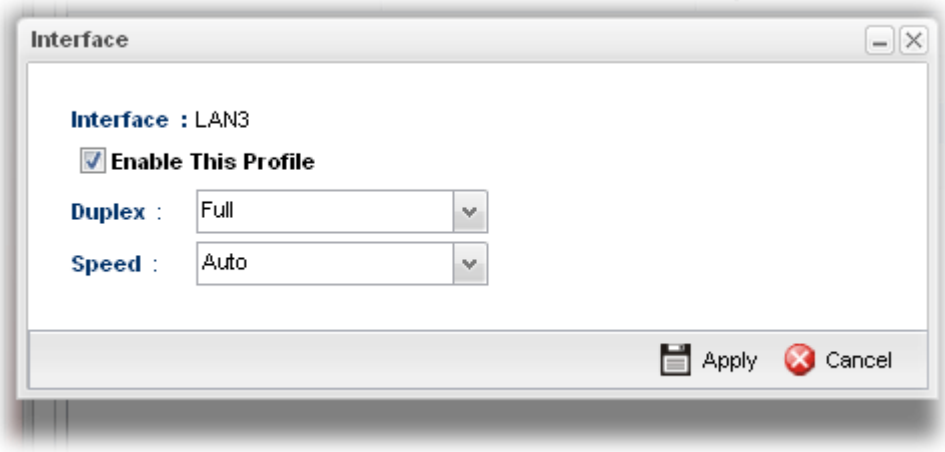
Refresh	Renew current web page.
Interface	Display the profile name of the interface.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Duplex	Display the duplex used (full or half) by such profile.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.

How to edit an Interface profile

1. Open **LAN>>Switch** and click the **Interface** tab.
2. Please select a profile and click the **Edit** button.



3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Interface	Display the name of LAN interface profile.
Enable This Profile	Check the box to enable the Mirror function for the switch.

Duplex	Use the drop down list to choose the duplex for such profile.
Speed	Use the drop down list to specify the transmission rate 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**. The profile has been edited.

Status

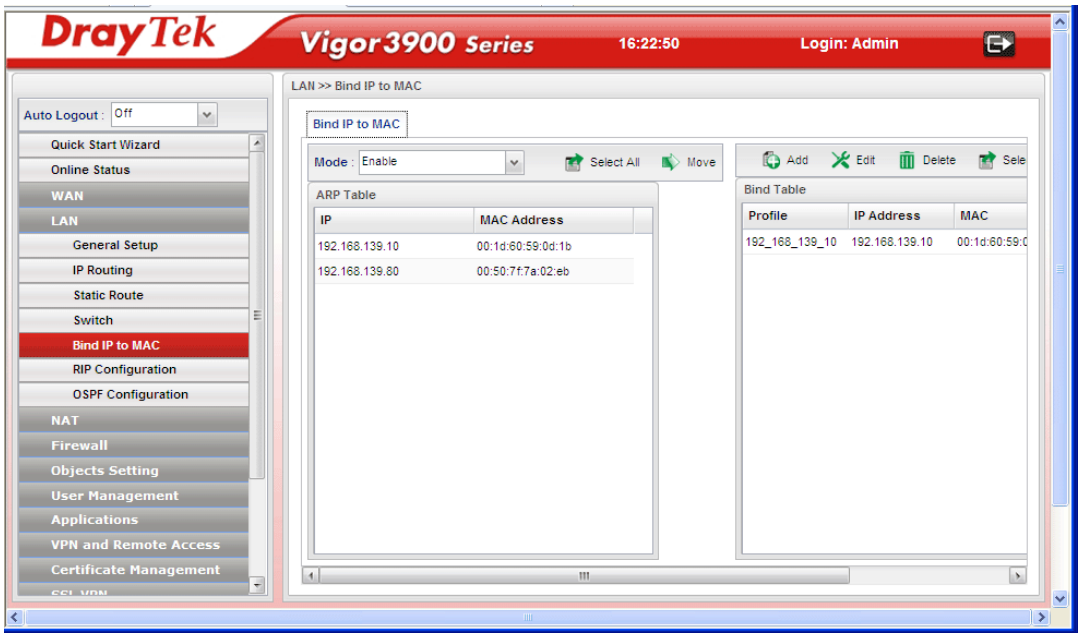
This page displays the status the status (enable / disable), speed(Auto,10M,100M,1000M) and duplex (Half/Full) of the LAN ports respectively.

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.
Interface	Display the profile name of the interface.
Status	Display the status (up or down) for the interface.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.
Duplex	Display the duplex used (full or half) by such profile.

4.2.5 Bind IP to MAC

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



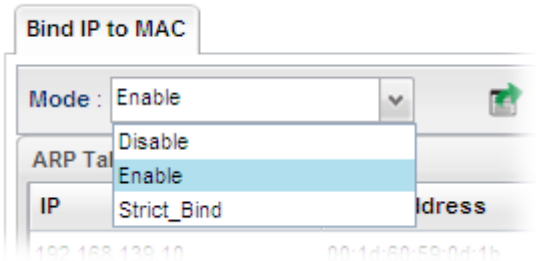
Each item will be explained as follows:

Item	Description
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.
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. **IP Address -** Display the IP address of one device. **MAC Address -** Display the MAC address of the device.
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.
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.
Rename	Allow to modify the selected profile name.
Bind Table	It displays a list for the IP bind to MAC information. **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.

How to configure Bind IP to MAC

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



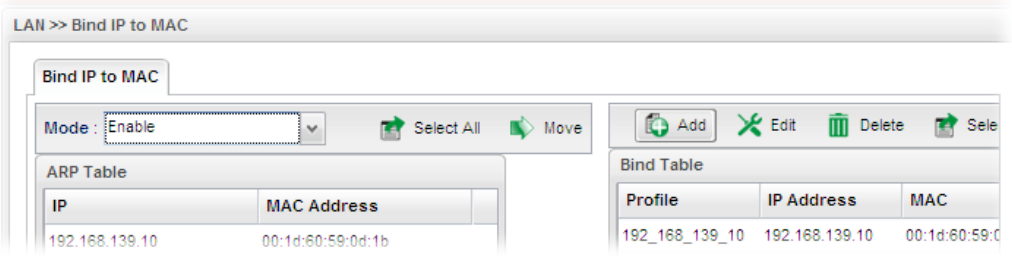
There are three modes offered for you to choose.

Disable – The function of Bind IP to MAC is disabled.

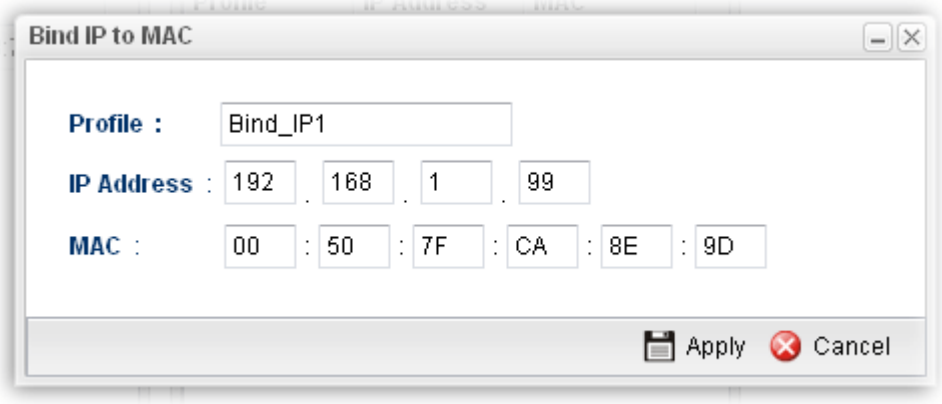
Enable – Specified IP addresses on the Bind Table will be reserved for the device with bind MAC address. Other devices which are not listed on the Bind Table shall still get the IP address from DHCP server.

Strict_Bind – Only specified IP addresses will be assigned to the device with bind MAC address. Other devices which are not listed on the Bind Table shall still **NOT** get the IP address from DHCP server.

3. Click **Add**.



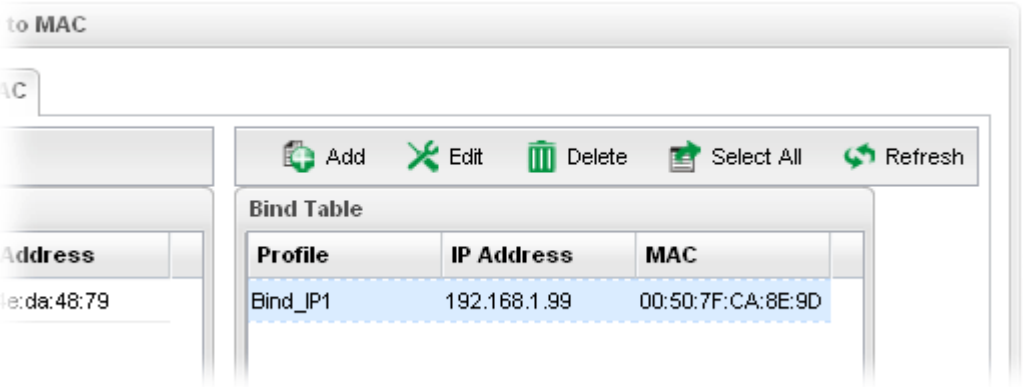
4. The following dialog appears.



Available parameters are listed as follows:

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

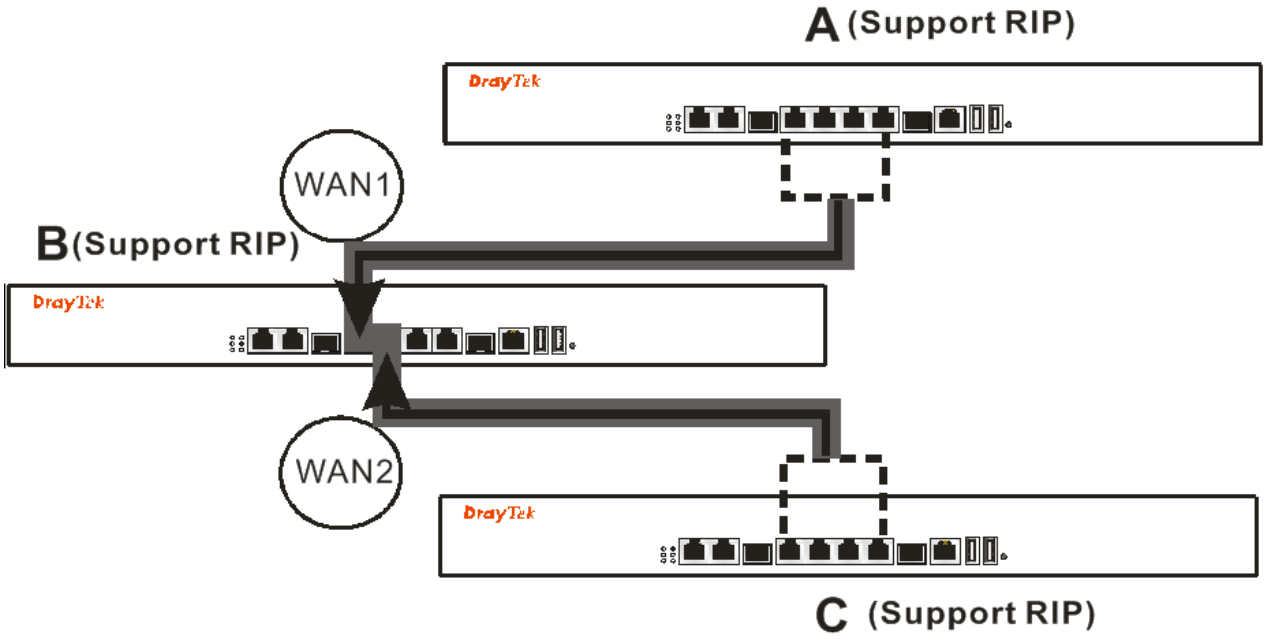
5. Enter all the settings and click **Apply**.
6. A new profile has been added onto **Bind Table**.



4.2.6 RIP Configuration

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

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



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

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

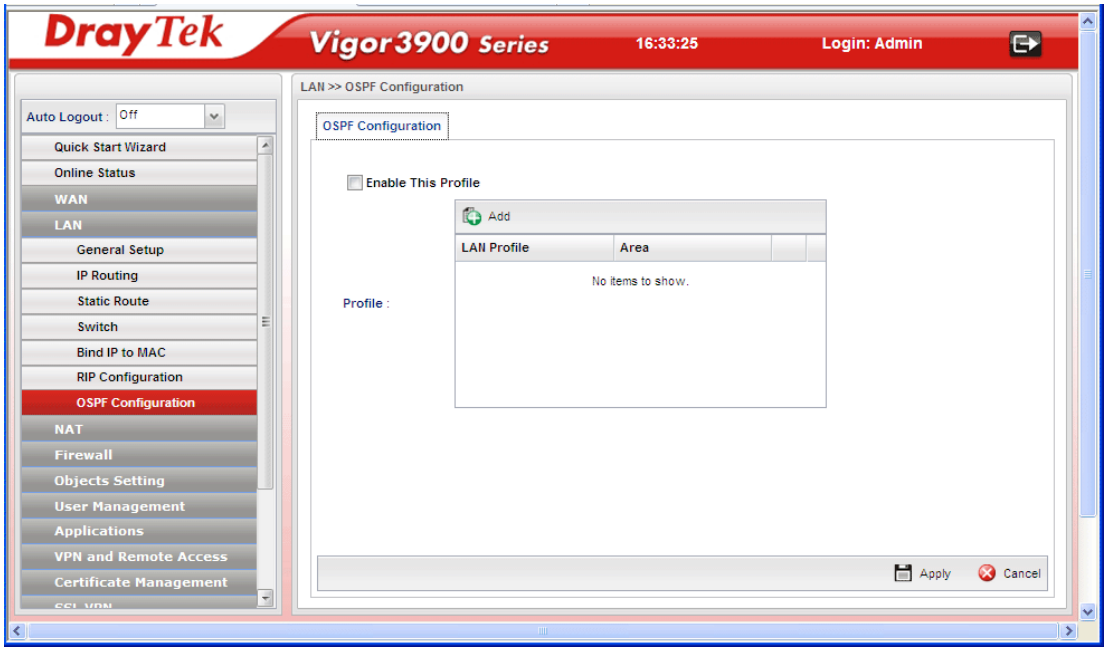
In another direction, C will do the same thing.

Available parameters are listed as follows:

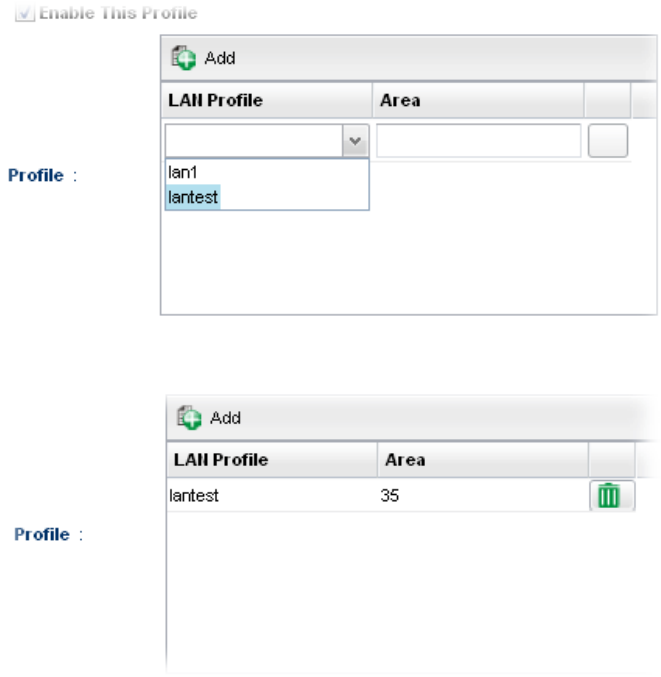
Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Profile	Choose one of the LAN profiles.
Apply	Click it to save the settings.
Cancel	Click it to discard the settings configured in this page.

4.2.7 OSPF Configuration

OSPF uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange.

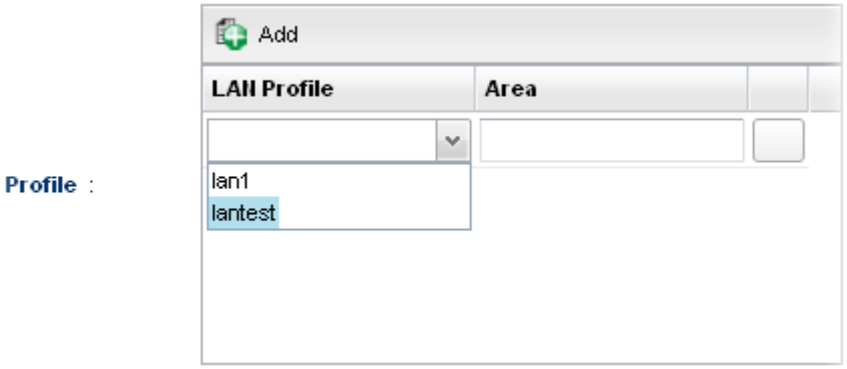


Available parameters are listed as follows:

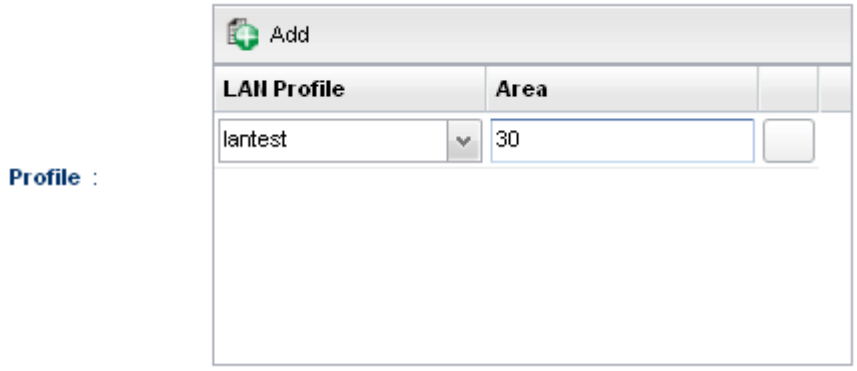
Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Profile	Type a new name for such profile. 
Apply	Click it to save the settings.
Cancel	Click it to cancel the settings configuration.

How to add a new profile

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

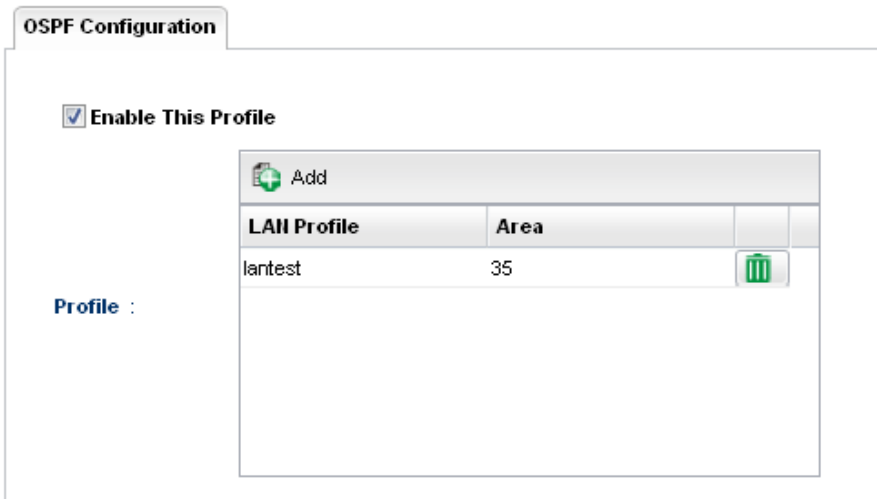


4. Use the drop down list of LAN Profile to choose the one you need. And specify the value of Area (either 0.0.0.0 ~ 255.255.255.255 or 0 ~ 4294967295) for that profile.



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

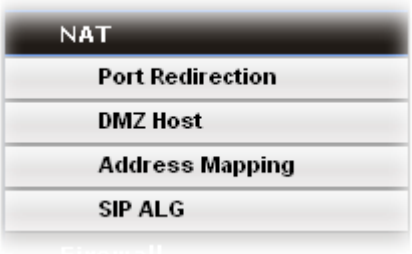
5. Click **Apply** to save the settings and exit the dialog. A new profile is created and displayed on the screen.



4.3 NAT

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

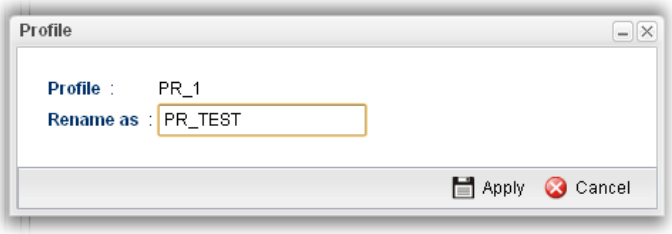
There are three functions that NAT provides – **Port Redirection**, **DMZ Host** and **Address Mapping**,.



4.3.1 Port Redirection

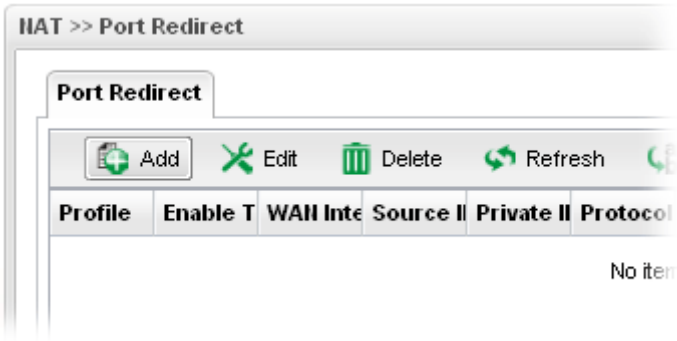
Port Redirection means port forwarding. It may be used to expose internal servers to the public domain or open a specific port to internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW and etc. The internal FTP server is running on the local host 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:

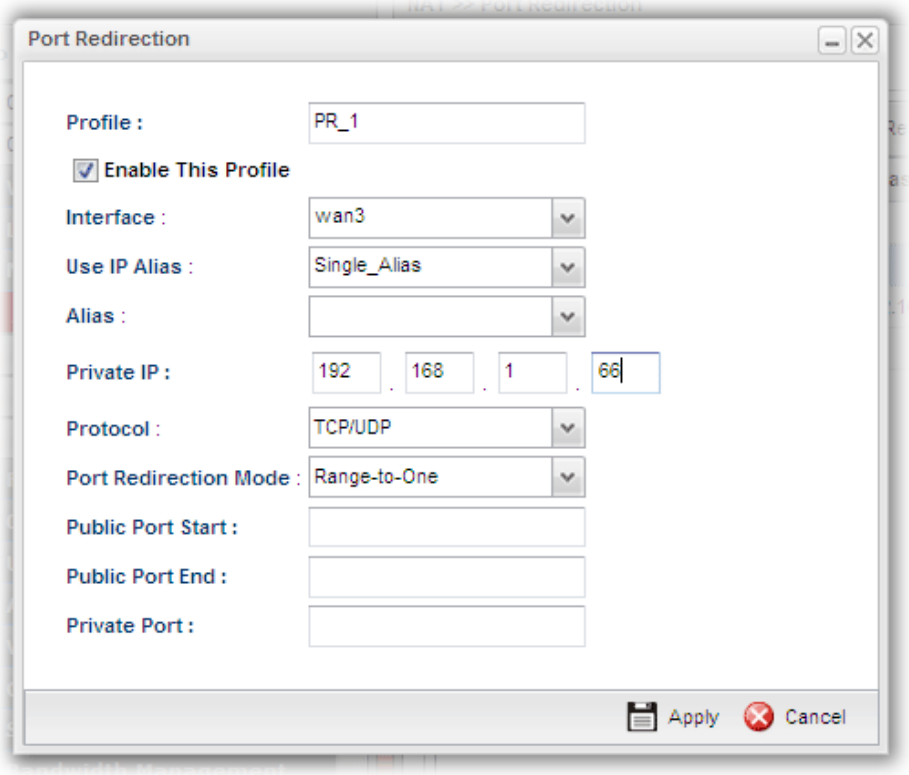
Item	Description
Add	Add a new port redirect profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name. 
Profile	Display the name of the profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Interface	Display the WAN interface of this profile.
Source IP	Display the source IP used for this entry.
Private IP	Display the private IP used for this entry.
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 Port	Display the number of the private port.
Public IP	Display what kind of IP is used.
IP Alias	Display the selected WAN IP address.

How to add a new Port Redirection profile

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

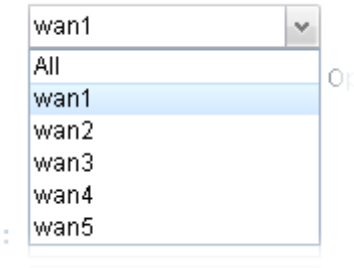
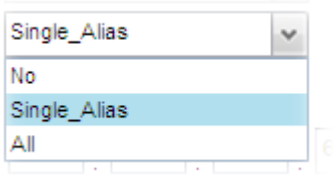
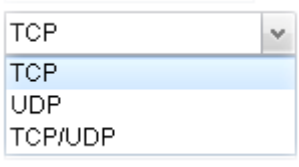
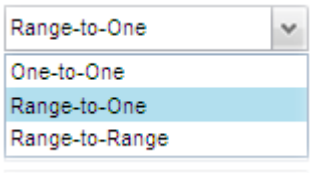


3. The following dialog will appear.

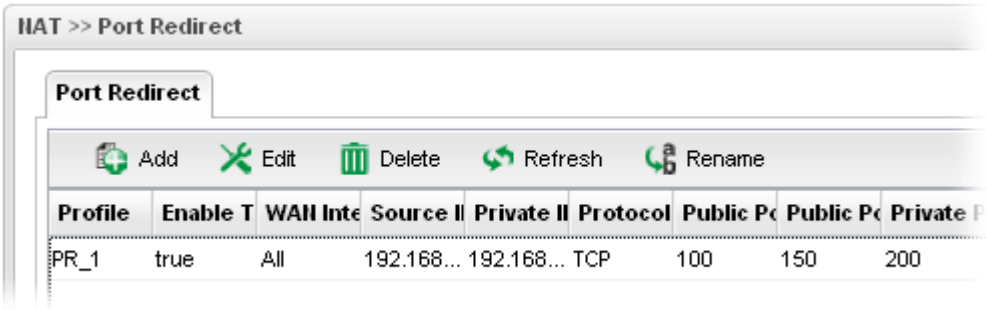


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check the box to enable this profile.
Interface	Specify the WAN profile for such profile.

	
Use IP Alias	Use the drop down list to select the one you want. 
IP 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.
Private IP	Specify the private IP address of the internal host providing the service. Simply type the private IP used for this entry.
Protocol	Choose the protocol used for the entry. 
Port Redirection Mode	Specify the direction for the port to be redirected. 
Public Port Start/ Public Port End	Type the starting/ending number of the public port.
Private Port	Specify the private port number of the service offered by the internal host.
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.

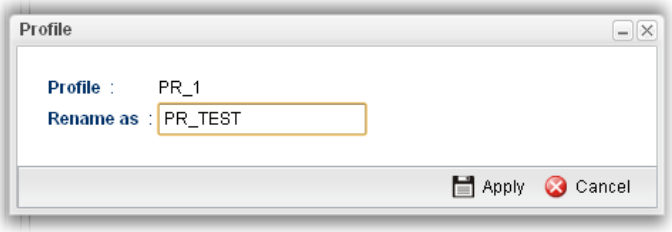


4.3.2 DMZ Host

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

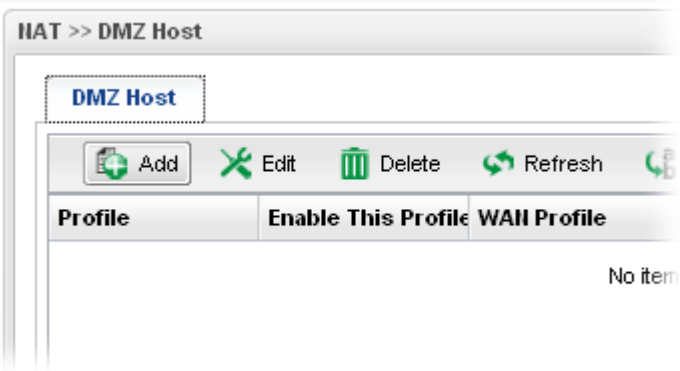
Each item will be explained as follows:

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

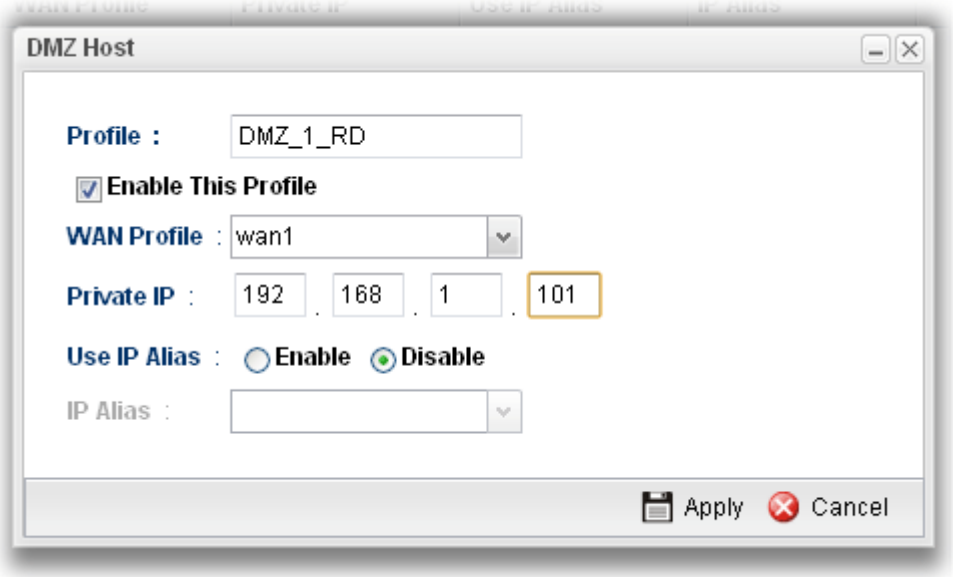
	rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name. 
Profile	Display the name of the profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN profile that such DMZ host profile will be applied to.
Private IP	Display the private IP used for this entry.
Use IP Alias	Display the using status (enabled or disabled) for WAN IP alias.
IP Alias	Display the selected WAN IP address.

How to add a new DMZ Host profile

1. Open **NAT>> DMZ Host**.
2. Simply click the **Add** button.



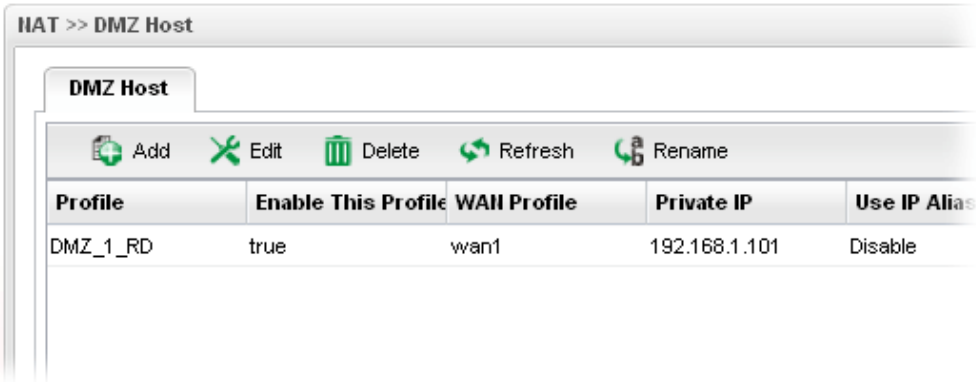
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check the box to enable the DMZ Host profile.
WAN Profile	Choose a WAN profile for such entry.
Private IP	Type the private IP used for this 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.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

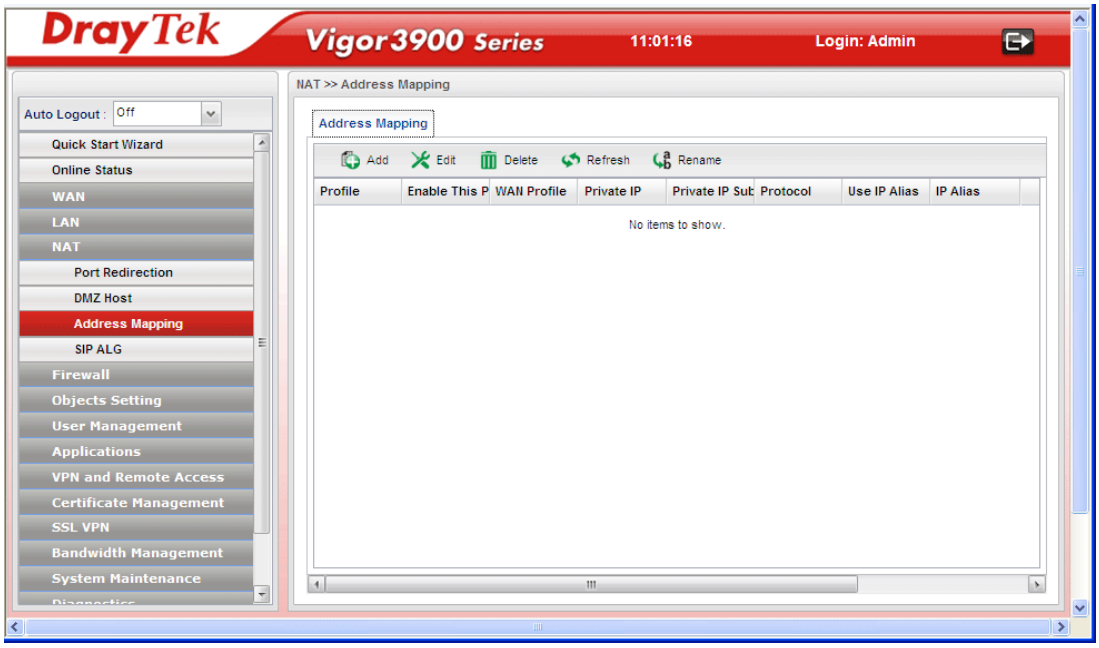


4.3.3 Address Mapping

This page is used to map specific private IP to specific WAN IP alias.

If you have "a group of IP Addresses" and want to apply to the router, please use WAN IP alias function to record these IPs first. Then, use address mapping function to map specific private IP to specific WAN IP alias.

For example, you have IP addresses ranging from 86.123.123.1 ~ 86.123.123.8. However, your router uses 86.123.123.1, and the rest of the IPs are recorded in WAN IP alias. You want that private IP 192.168.1.10 can use 86.123.123.2 as source IP when it sends packet out to Internet. You can use address mapping function to achieve this demand. Simply type 192.168.1.10 as the Private IP; and type 86.123.123.2 as the WAN IP.



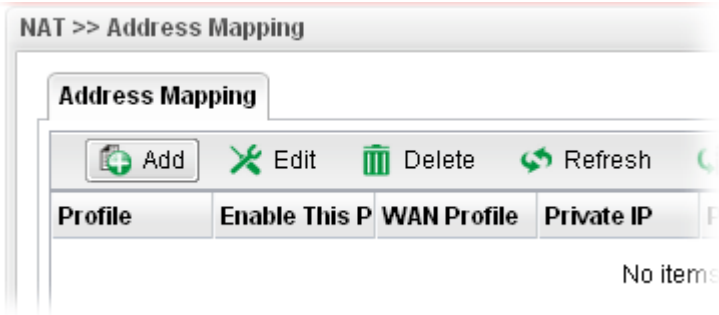
Each item will be explained as follows:

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.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN profile that such address mapping profile

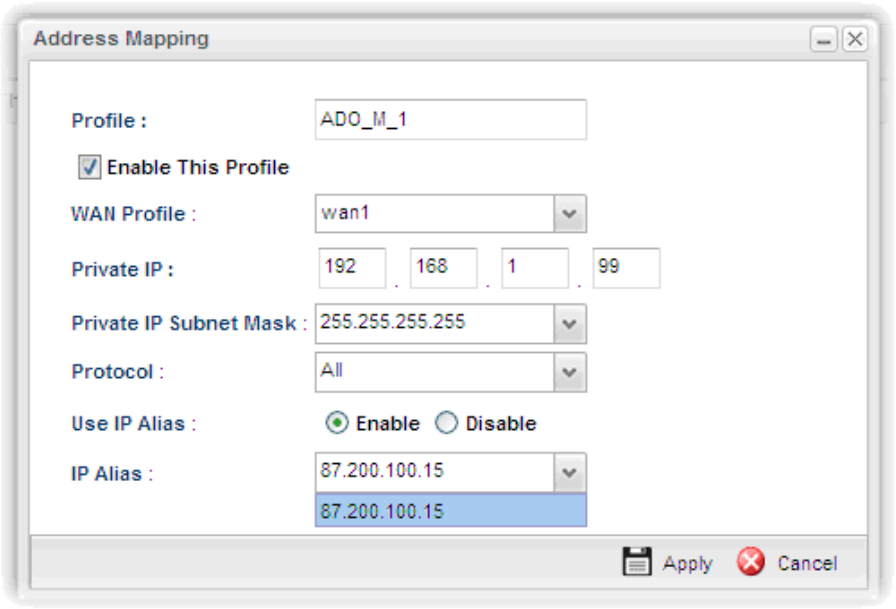
	will be applied to.
Private IP	Display the private IP used for this entry.
Private IP Subnet Mask	Display the subnet mask used for this entry.
Protocol	Display the protocol used for the entry.
Use IP Alias	Display the using status (enabled or disabled) for WAN IP alias.
IP Alias	Display the selected WAN IP address.

How to add a new Address Mapping profile

1. Open **NAT>> Address Mapping**.
2. Simply click the **Add** button.

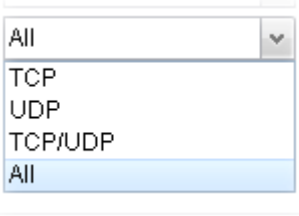


3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check the box to enable the Address Mapping profile.
WAN Profile	Choose a WAN profile for such entry.
Private IP	Type the private IP used for this entry.

Private IP subnet Mask	Type the subnet mask used for this entry.
Protocol	Choose the protocol used for the entry. 
Use IP Alias	Click **Enable** to invoke IP Alias function.
IP Alias	Select the Alias IP for this Address Mapping 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 **Address Mapping** table.

4.3.4 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.

Available parameters are listed as follows:

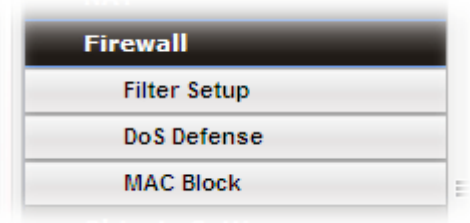
Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
LAN Interface	Choose one of the LAN profiles.
WAN Interface	Choose one of the WAN profiles.
Refresh	Renew current web page.
Apply	Click it to save the settings.

Click **Apply** to save the settings.

4.4 Firewall

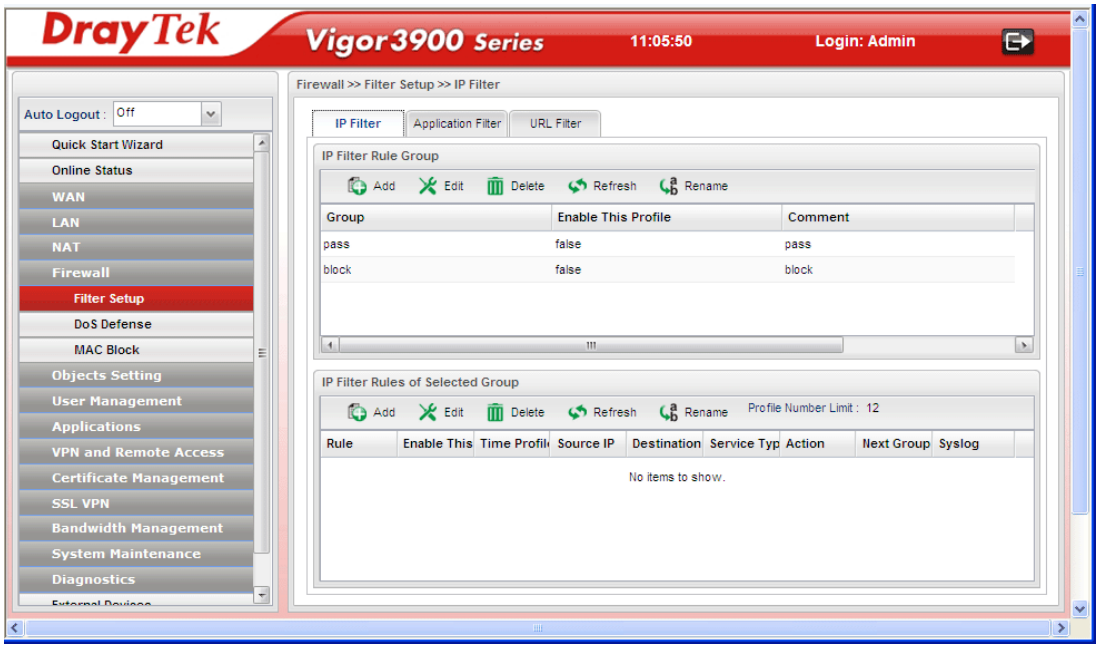
The firewall controls the allowance and denial of packets through the router. The **Firewall Setup** in the Vigor3900 Series mainly consists of packet filtering, Denial of Service (DoS) and URL (Universal Resource Locator) content filtering facilities. These firewall filters help to protect your local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

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



4.4.1 Filter Setup

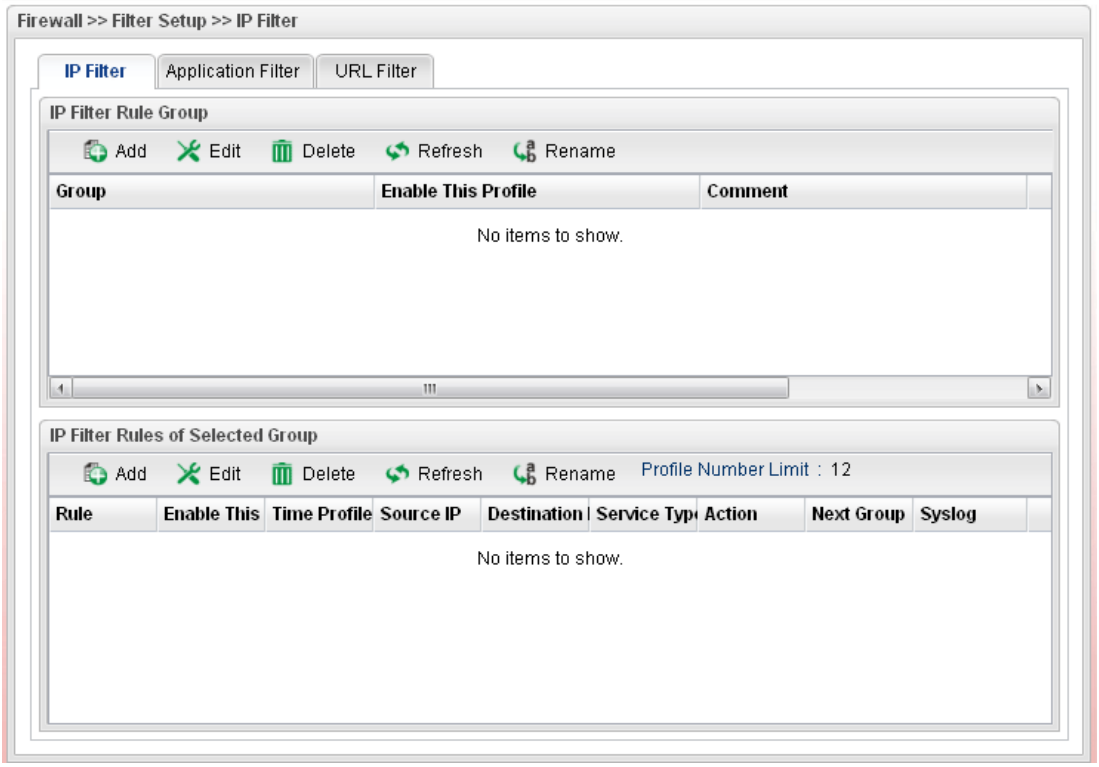
Vigor firewall will filter the packets based on the settings, including IP Filter, Application Filter and URL Filter configured under **Firewall>>Filter Setup**. These filters will group certain objects (e.g., IP Object, Service Object, Keyword Object, File Extension Object, IM Object, P2P Object, P2P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



IP Filter

This page allows you to create new IP filter rule(s) and group them for your request. The upper part displays the information of IP Filter Group(s); the lower part displays the information of IP Filter Rule(s).

You should create at least one IP filter rule and one group profile. The following will explain **IP Filter** functions with details.



Each item will be explained as follows:

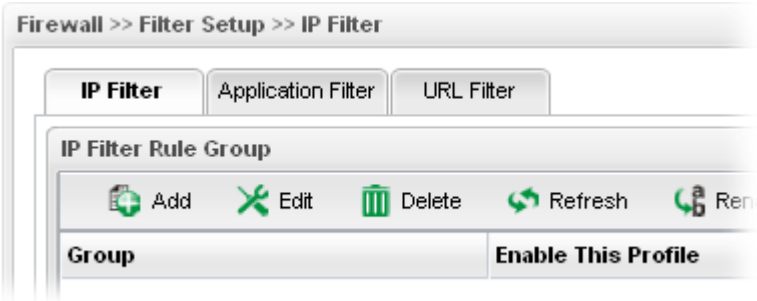
Item	Description
IP Filter Rule Group	
Add	Add a new group profile for IP filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
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.
Rename	Allow to modify the selected profile name.
Group	Display the name of the **IP filter group** profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.

Item	Description
Comment	Display the description for such profile.
IP Filter Rule Group of Selected Group	
Add	Add a new IP filter rule profile. Before you create an IP filter rule, you have to create an IP filter group first. Otherwise, you are not allowed to add any IP filter rule here.
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.
Rename	Allow to modify the selected profile name.
Rule	Display the name of the IP filter rule.
Enable The Profile	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 source IP object profile selected for each rule.
Destination IP	Display the destination IP object profile selected for each rule.
Service Type	Display the service type object profile selected for each rule.
Action	Display the action (pass or block) of such rule will use.
Next Group	Display the name for next group selected. If no group is chosen, **None** will be shown instead.
Syslog	Display the status (enable or disable) of the **Syslog** function.

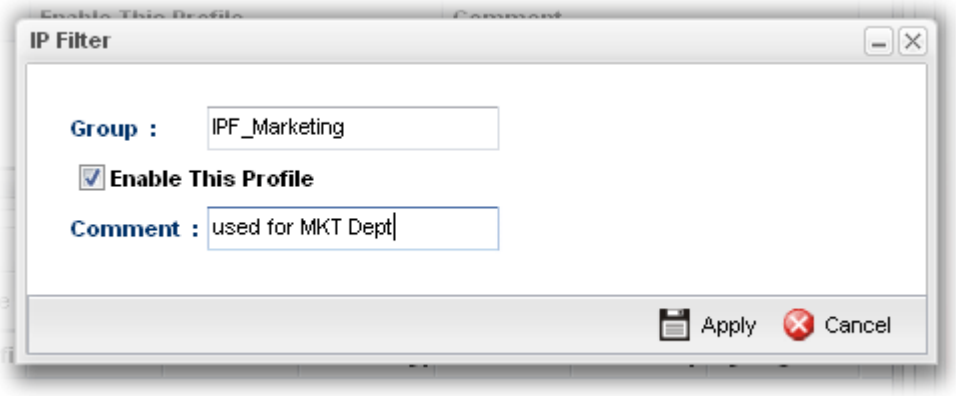
How to create an IP Filter group

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

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



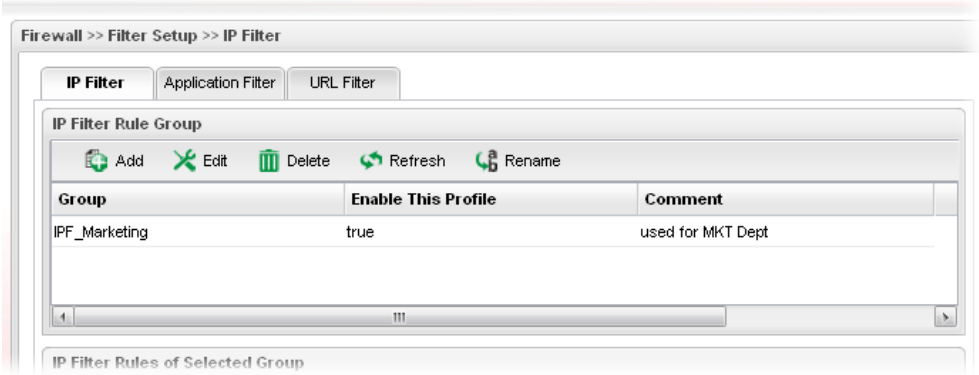
3. The following dialog will appear.



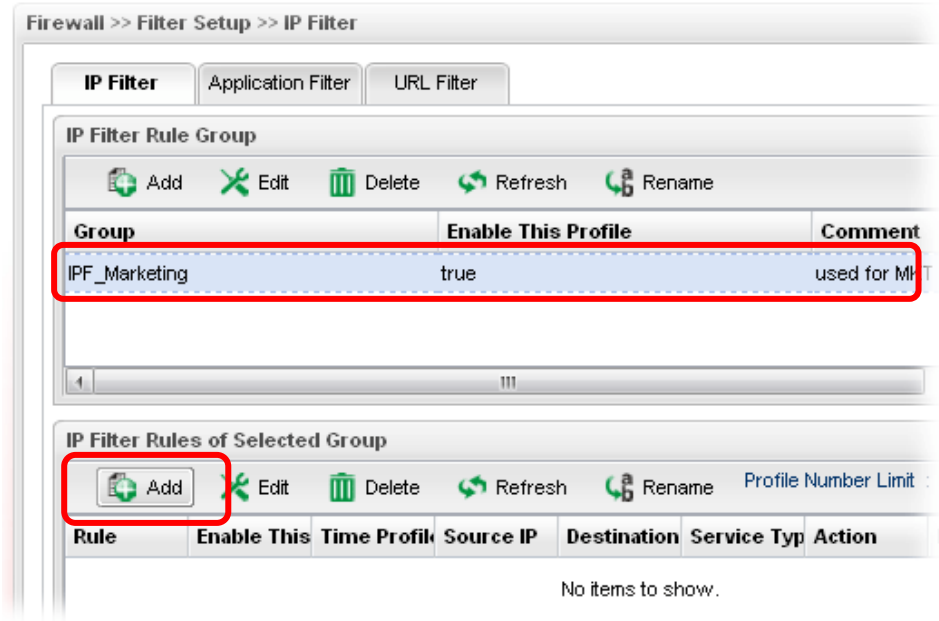
Available parameters are listed as follows:

Item	Description
Group	Type the name of the IP filter group.
Enable This Profile	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 onto **Address Mapping** table.



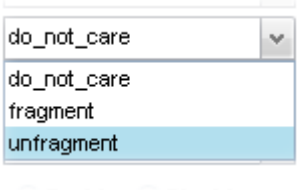
6. Choose the IP filter group first and then click the **Add** tab (the lower one in this page).

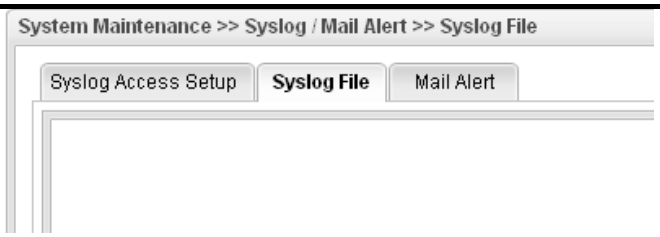


7. The following page for configuration will appear.

Available parameters are listed as follows:

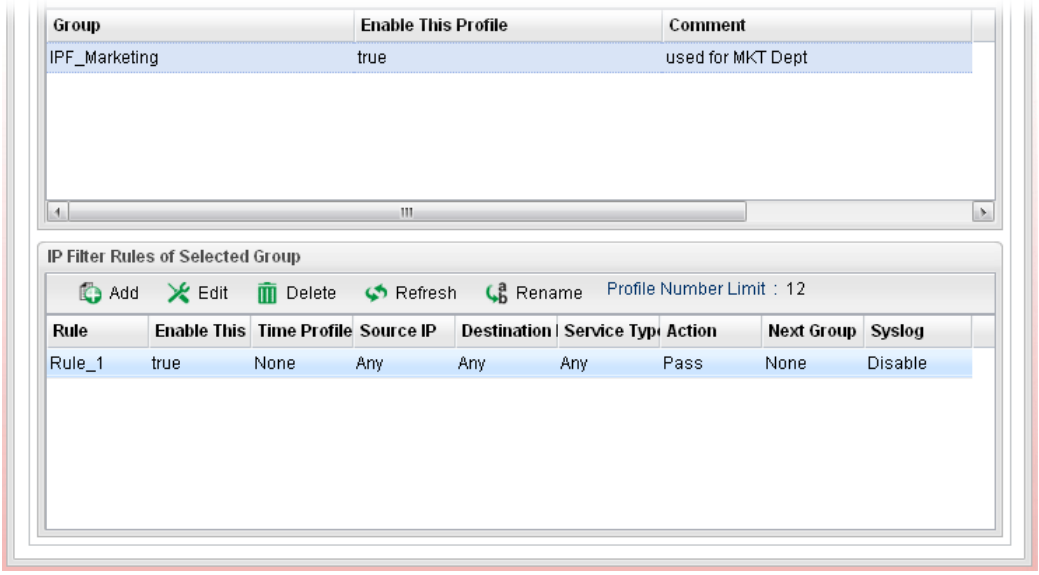
Item	Description
Rule	Type the name of the IP filter rule.
Enable This Profile	Check the box to enable this profile.

Time Profile	Choose a schedule profile to be applied on such rule. You can click to create another new time object profile.
Source IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source IP. You can click to create another new IP object profile.
Destination IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as destination IP. You can click to create another new IP object profile.
Service Type	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.
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.
Fragments	Specify the action for fragmented packets.  **do_not_care -**No action will be taken towards fragmented packets. **unfragment -** Apply the rule to unfragmented packets. **fragment -** Apply the rule to fragmented packets.
Action	The action to be taken when packets match the rule. **Block -** Packets matching the rule will be dropped immediately **Pass -** Packets matching the rule will be passed immediately. **Block_If_No_Further_Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Pass_If_No_Further_Match -** A packet matching the rule, and that does not match further rules, will be passed through.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance >> Syslog/Mail Alert** >> **Syslog File**.

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

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

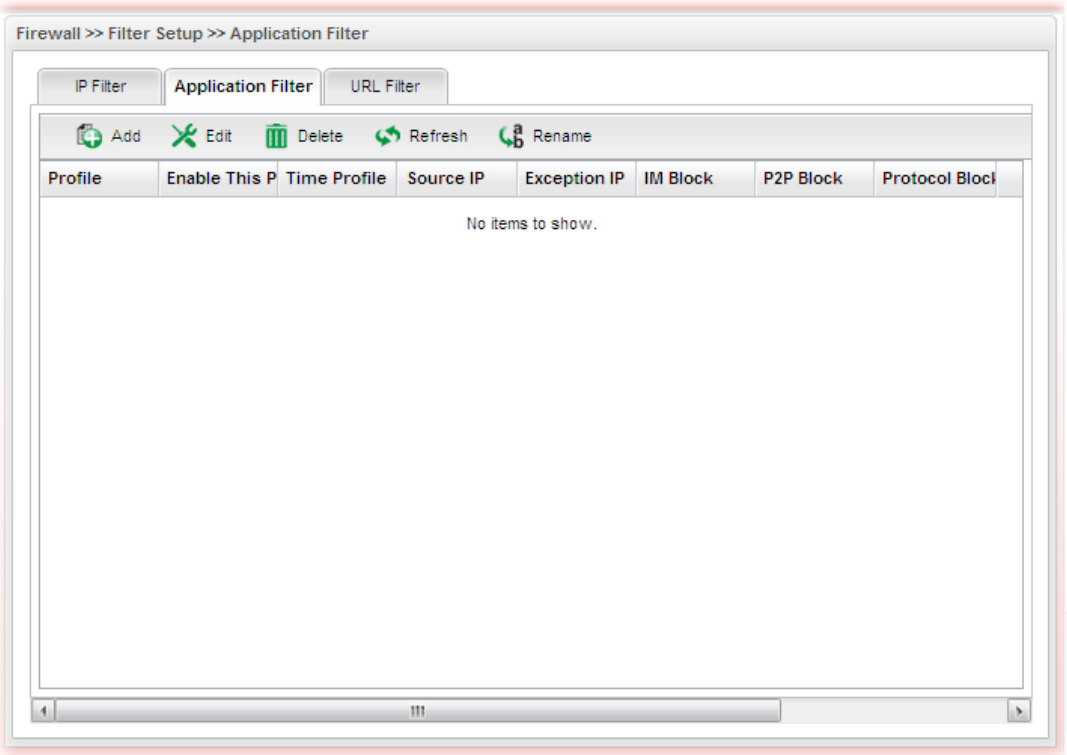
9. A new IP filter rule has been added onto **IP Filter Rules of Selected Group** table.



Note: You can create multiple IP filter groups. Each **IP Filter Rules of Selected Group** belongs to an **IP Filter Rule Group**. Click an **IP Filter Rule Group** to show its members in the lower display window.

Application Filter

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



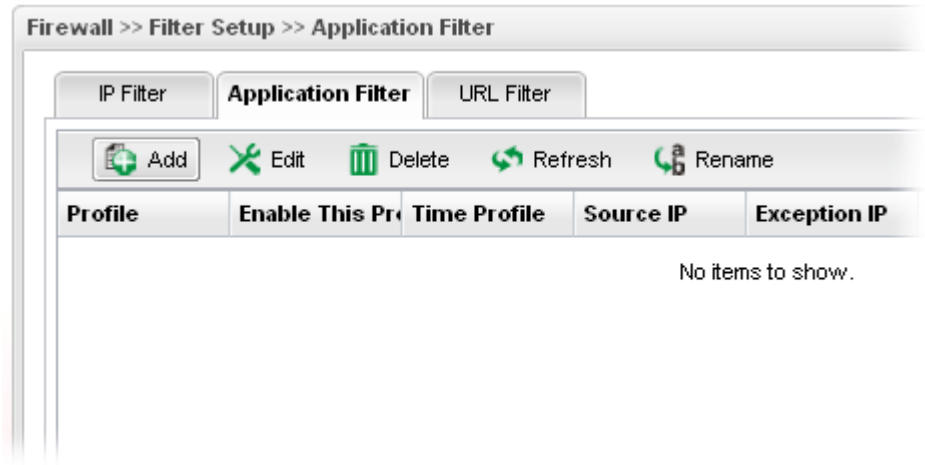
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for Application filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the application filter profile.
Enable The Profile	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 source IP object profile selected for such group.

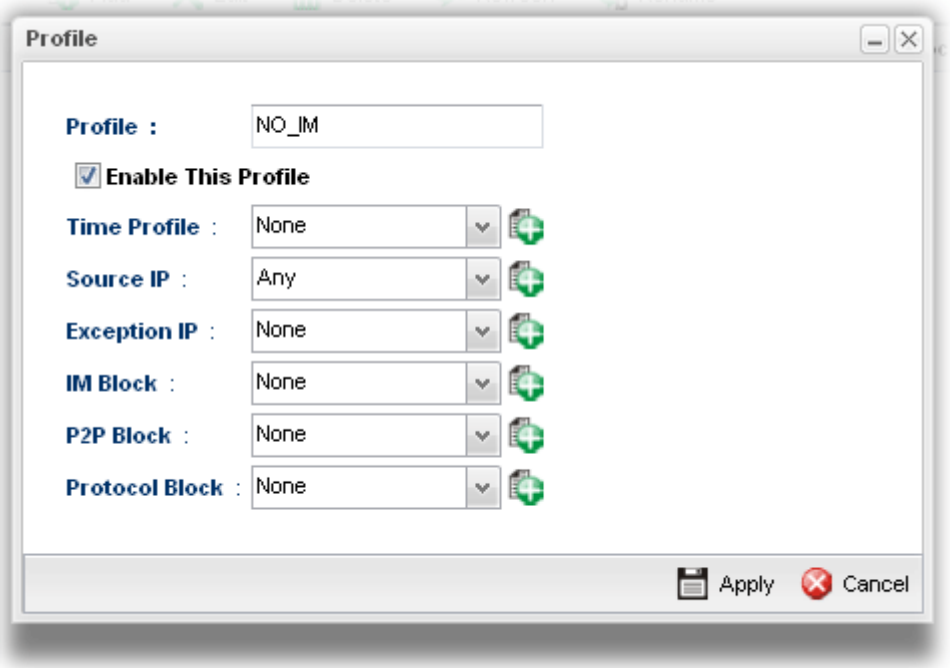
Item	Description
Exception IP	Display the IP object profile which will not be filtered by the router for such group.
IM Block	Display the IM object profile selected for such application profile.
P2P Block	Display the P2P object profile selected for such application profile.
Protocol Block	Display the protocol 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.



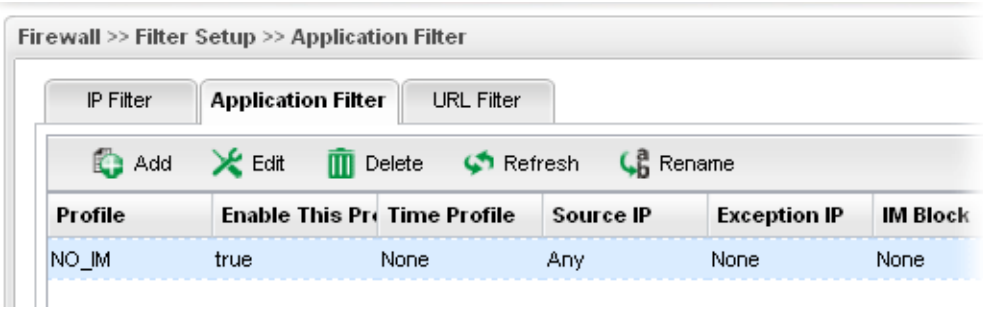
3. The following dialog will appear.



Available parameters are listed as follows:

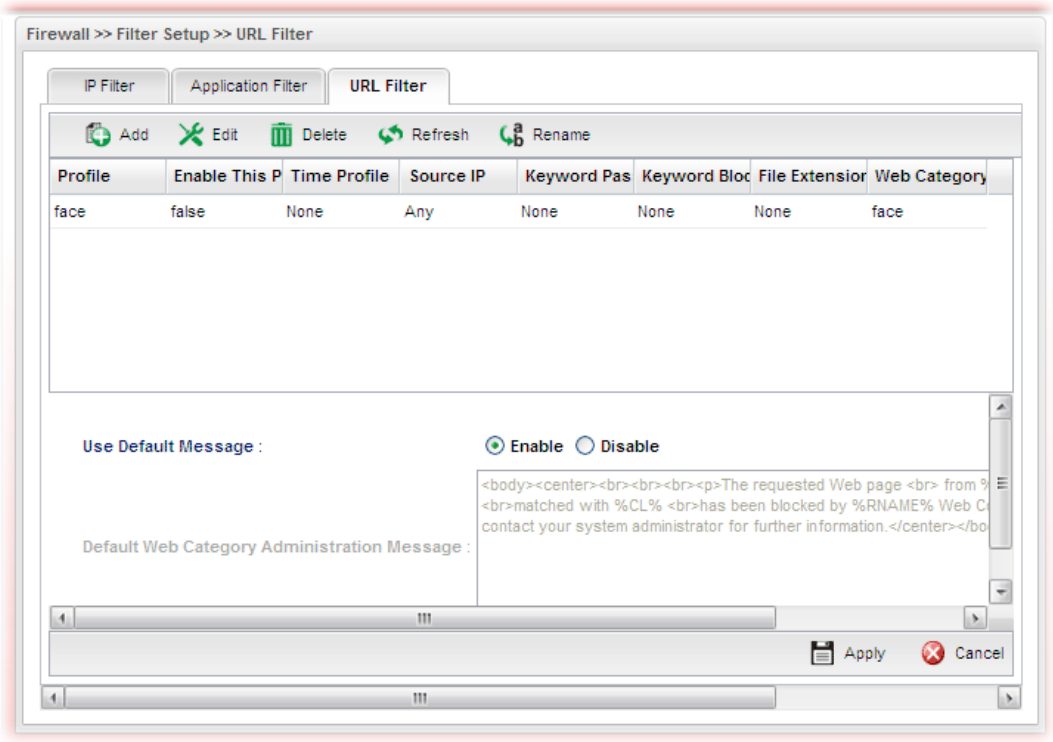
Item	Description
Profile	Type the name of the Application filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Choose a schedule profile to be applied on such rule. You can click to create another new time object profile.
Source IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source IP. You can click to create another new IP object profile.
Exception IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as exception IP which will not be filtered by the router for such group. You can click to create another new IP object profile.
IM Block	Choose one or more IM object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new IM object profile.
P2P Block	Choose one or more P2P object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new P2P object profile.
Protocol Block	Choose one or more Protocol object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new protocol 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.



URL Filter

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



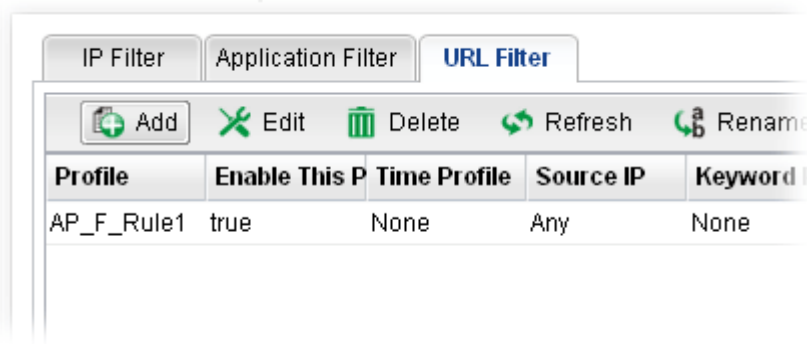
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the application filter profile.
Enable The Profile	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 source IP object profile selected for each rule.
Keyword Pass	Display the keyword object profile selected for each rule which is allowed to pass through the router.

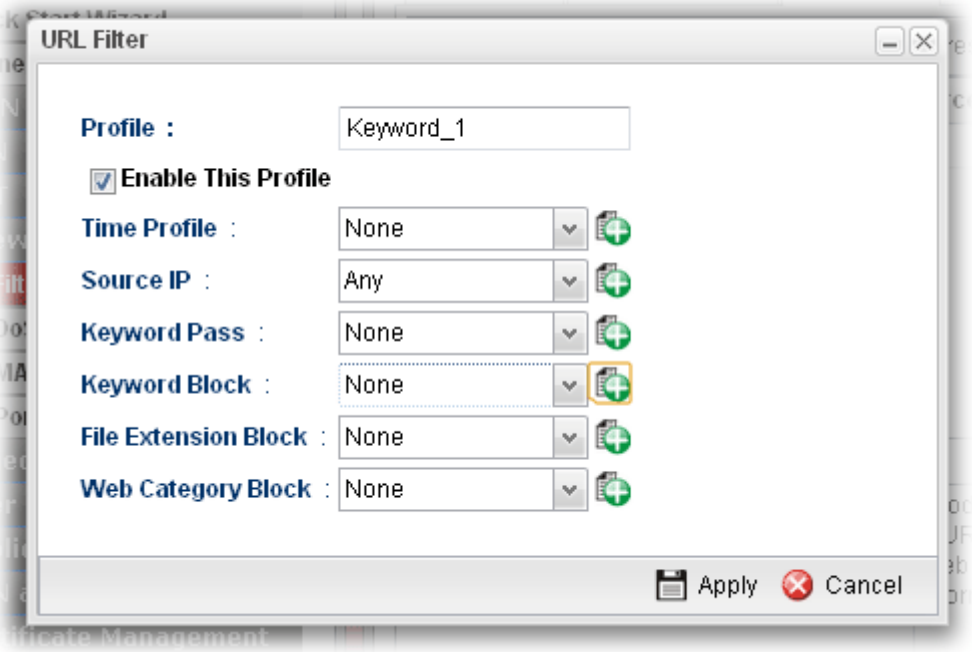
Item	Description
Keyword Block	Display the keyword object profile selected for each rule which is not allowed to pass through the router.
File Extension Block	Display the file extension object profile selected for each rule which is not allowed to pass through the router.
Web Category Block	Display the 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.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to create a URL Filter profile

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



3. The following dialog will appear.

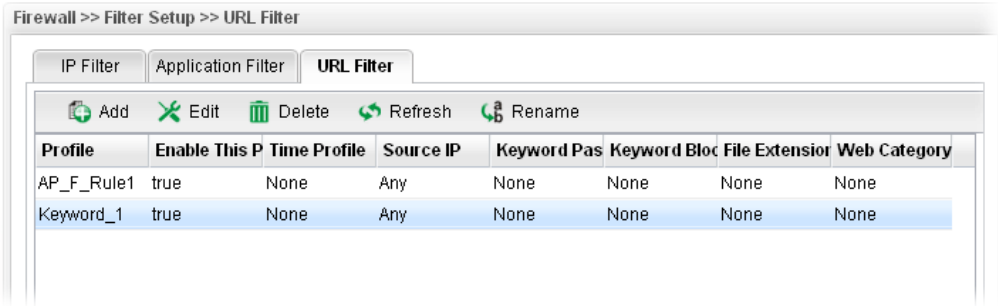


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the URL filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Choose a schedule profile to be applied on such rule. You can click to create another new time object profile.
Source IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source IP. You can click to create another new IP object profile.
Keyword Pass	Choose one or more keyword object profiles from the drop down list which will be allowed to pass through the router. You can click to create another new keyword object profile.
Keyword Block	Choose one or more keyword object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new keyword object profile.
File Extension Block	Choose one or more P2P object profiles from the drop down list which will not be allowed to pass through the router. You can click to create another new file extension object profile.
Web Category Block	Choose one or more WCF object profiles from the drop down list which will not be allowed to pass through the router.

Item	Description
	You can click to create another new WCF object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

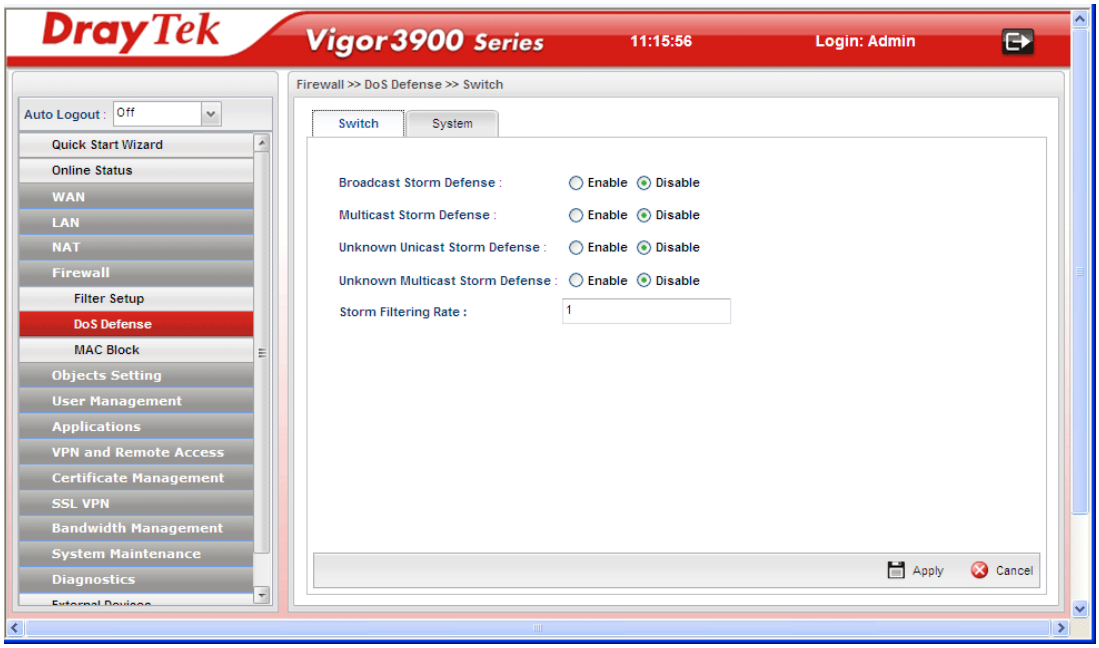
4. Enter all the settings and click **Apply**.
5. A new URL filter profile has been added.



4.4.2 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.

Switch



Available parameters are listed as follows:

Item	Description
Broadcast Storm Defense	Click **Enable** to block the packets attacks coming from broadcast storm.
Multicast Storm Defense	Click **Enable** to block the packets attacks coming from multicast storm.
Unknown Unicast Storm Defense	Click **Enable** to block the packets attacks coming from unknown unicast storm.
Unknown Multicast Storm Defense	Click **Enable** to block the packets attacks coming from unknown multicast storm.
Storm Filtering Rate	Type a number (1~4096, unit of 64Kpbs) as for the filtering rate.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

System

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

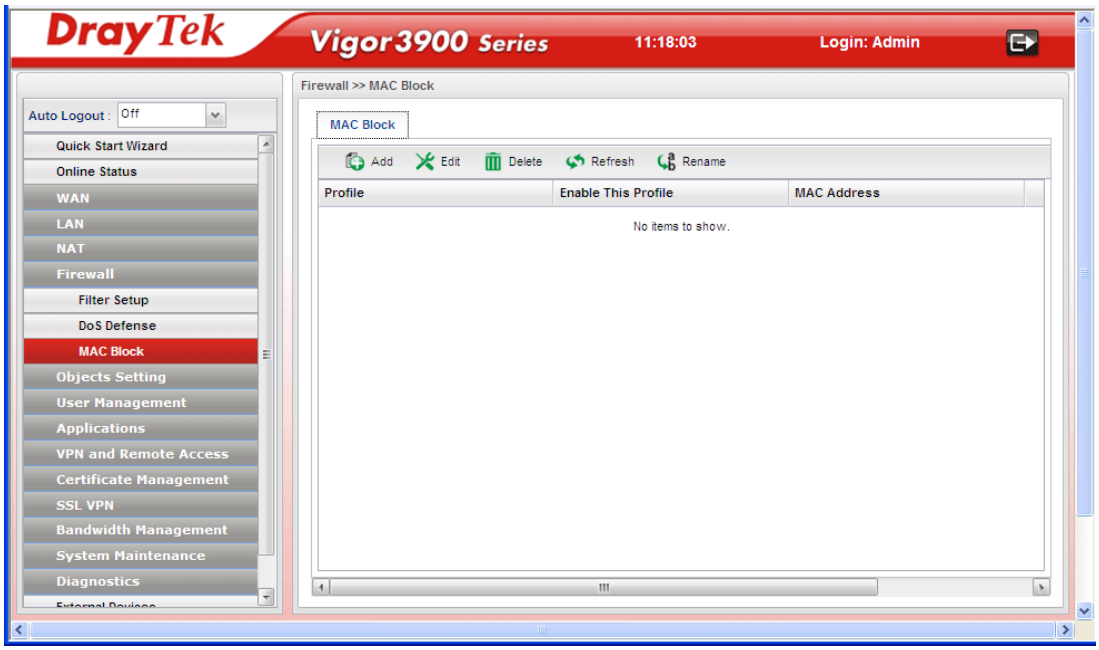
Available parameters are listed as follows:

Item	Description
Enable This Profile	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 **300** 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 **300** 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

Item	Description
	user-defined timeout period.
UDP Flood Threshold	The default setting for threshold is **300** packets per second.
UDP Flood Timeout	The default setting for timeout is **10** seconds.
Block Port Scan	Click **Enable** to activate the Port Scan detection function. Port scan sends packets with different port numbers to find available services, which respond. The router will identify it and report a warning message if the port scanning rate in packets per second exceeds the user-defined threshold value.
Port Scan Threshold	The default threshold is **300** 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.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

4.4.3 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.

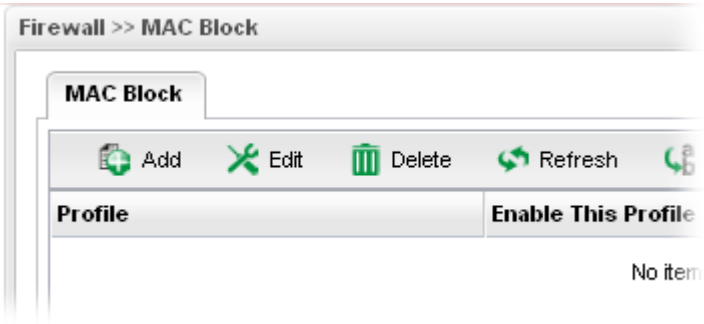


Each item will be explained as follows:

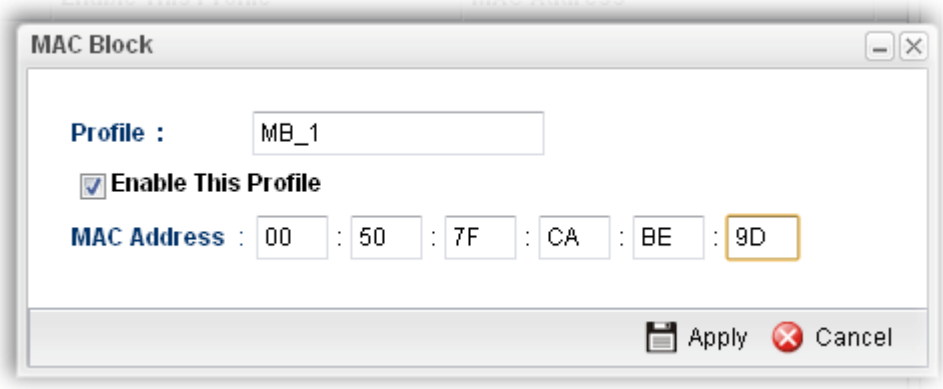
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new MAC Block profile

1. Open **Firewall>>MAC Block**.
2. Simply click the **Add** button.



3. The following dialog will appear.

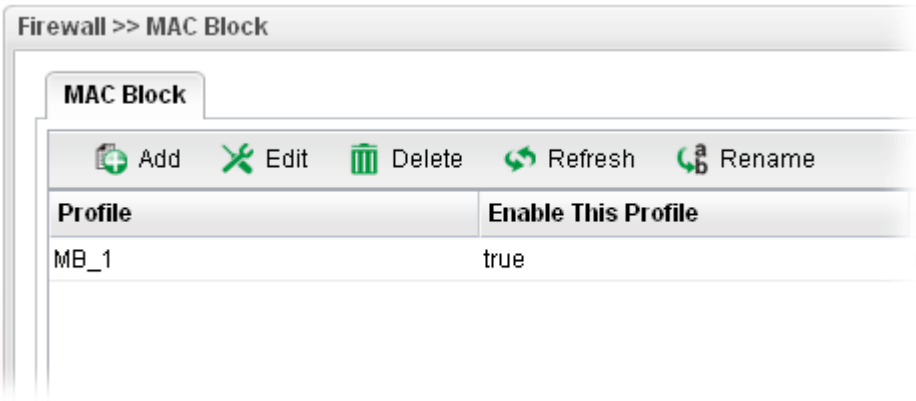


Available parameters are listed as follows:

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

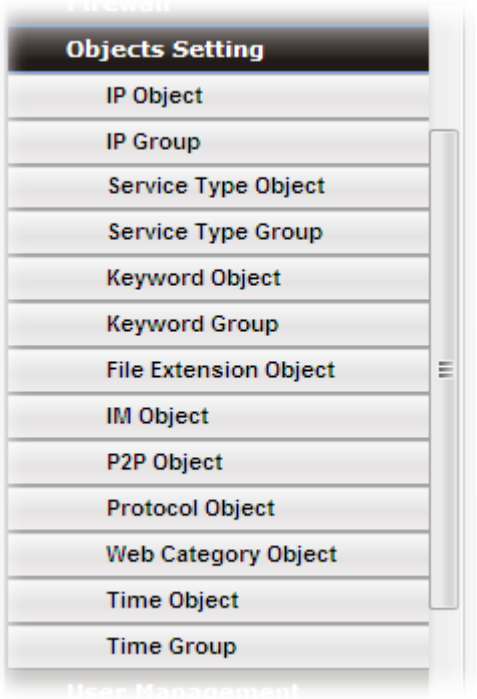
4. Enter all the settings and click **Apply**.

5. A new MAC Block profile has been created.



4.5 Objects Setting

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



4.5.1 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**.

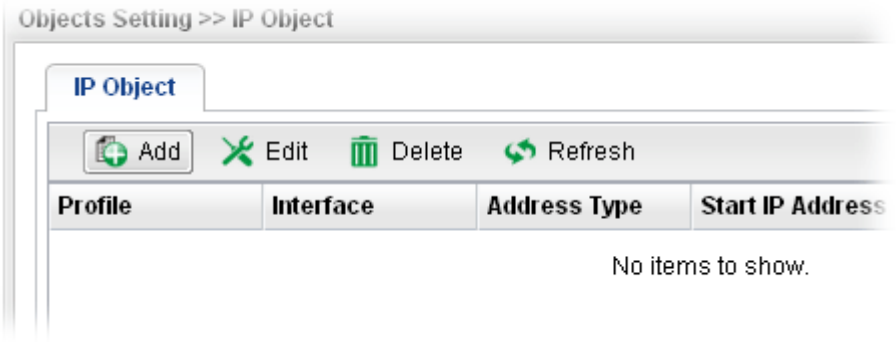
Each item will be explained as follows:

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.
Interface	Display the category (any, source or destination) of the IP Object.
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.

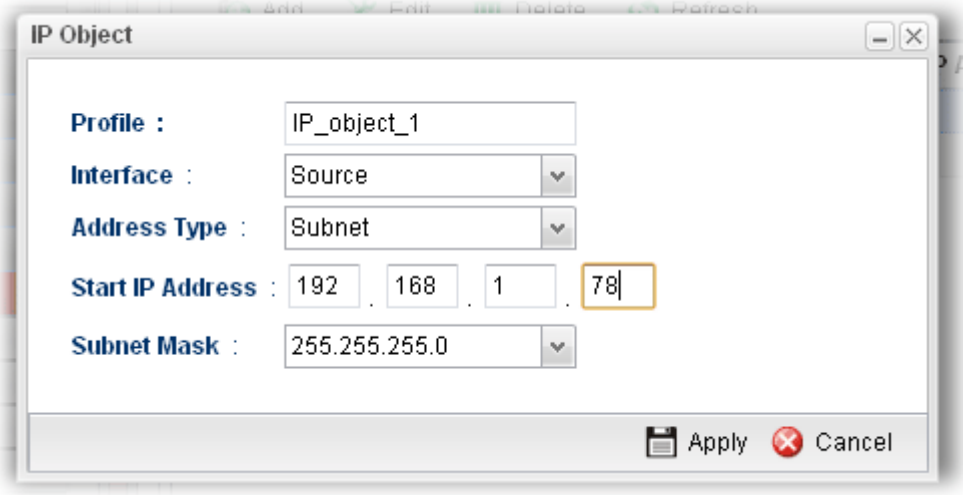
Item	Description
End IP Address	Display the IP address of the ending point for such profile. It will be joined with **Start IP Address** only when you choose **Range** as the **Address Type**.
Subnet Mask	Display the subnet mask for such profile.

How to create a new IP Object profile

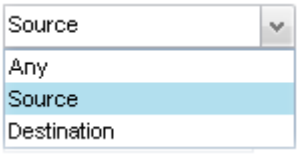
1. Open **Objects Setting>>IP Object.**
2. Simply click the **Add** button.

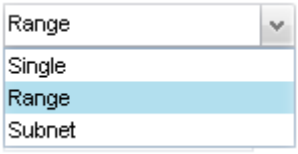


3. The following dialog will appear.



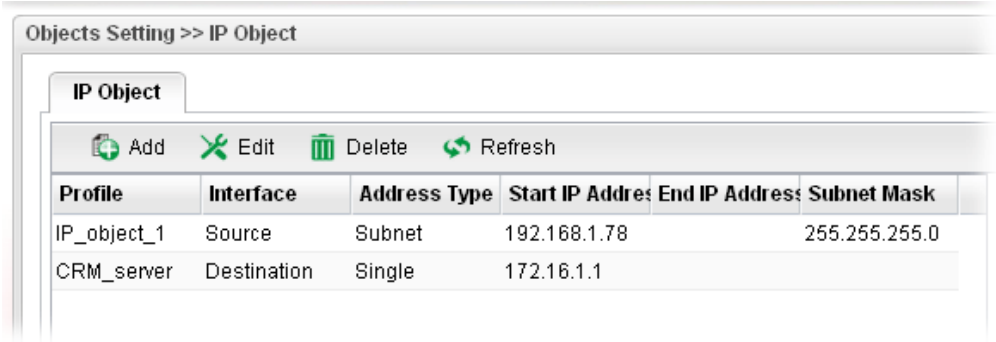
Available parameters are listed as follows:

Item	Description
Profile	Type the name of such profile.
Interface	Determine the category (any, source or destination) of this IP object. If an IP object is set to **Source**, it will only appear in the field of **Source IP** on **Firewall>>IP Filter Rule**. 

Item	Description
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.

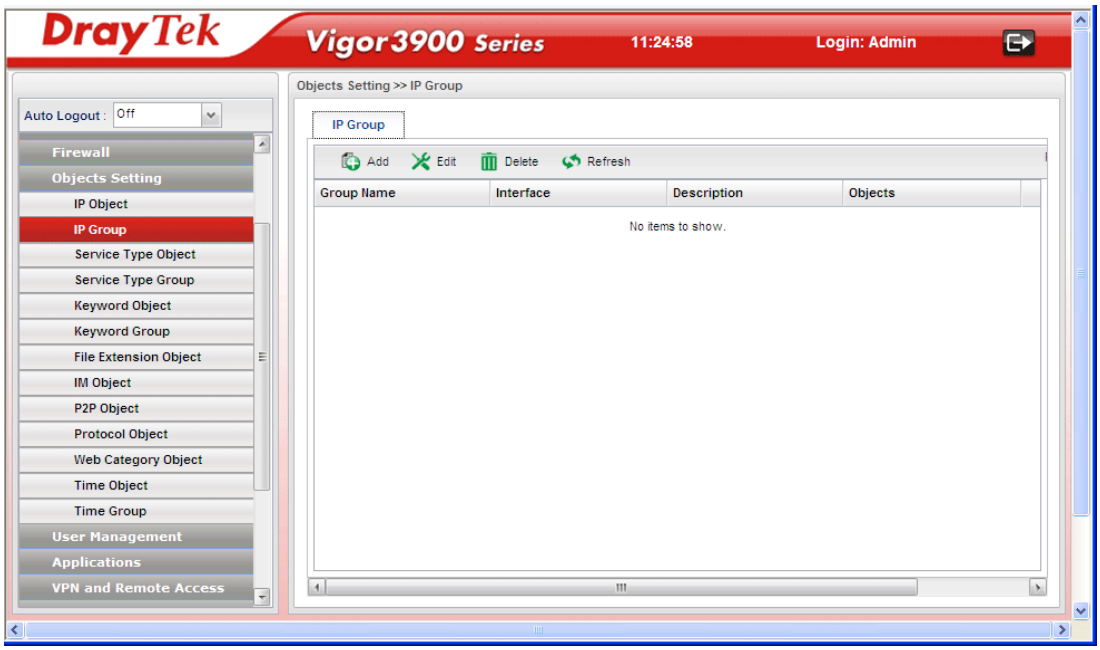
4. Enter all the settings and click **Apply**.

5. A new IP object profile has been created.



4.5.2 IP Group

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

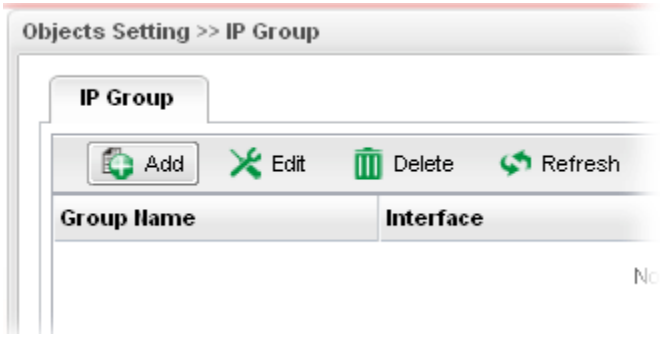


Each item will be explained as follows:

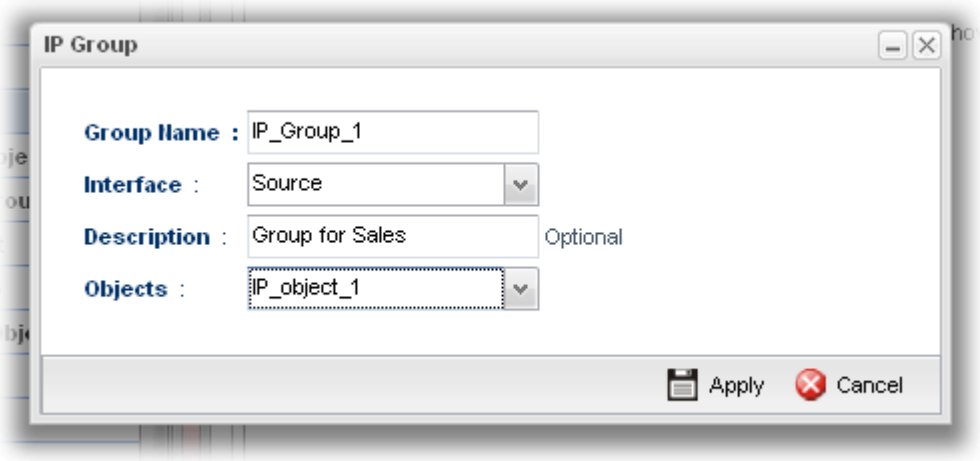
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete 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.
Interface	Display the category (any, source or destination) of the IP group.
Description	Display the description for such profile.
Objects	Display the object profiles grouped under such group.

How to create a new IP Group profile

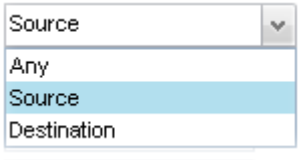
1. Open **Objects Setting>>IP Group.**
2. Simply click the **Add** button.



3. The following dialog will appear.



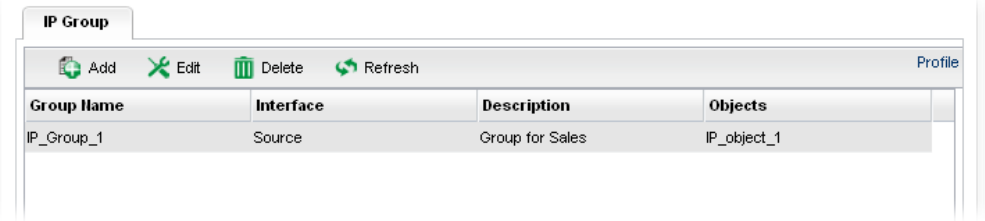
Available parameters are listed as follows:

Item	Description
Group Name	Type the name of the object group. The number of the characters allowed to be typed here is 10.
Interface	Determine the category (any, source or destination) of this IP group. If the group is set to **Source**, it will only appear in the field of **Source IP** on **Firewall>>IP Filter Rule**. 
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.
Apply	Click it to save the configuration.

Item	Description
Cancel	Click it to exit the dialog without saving anything.

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

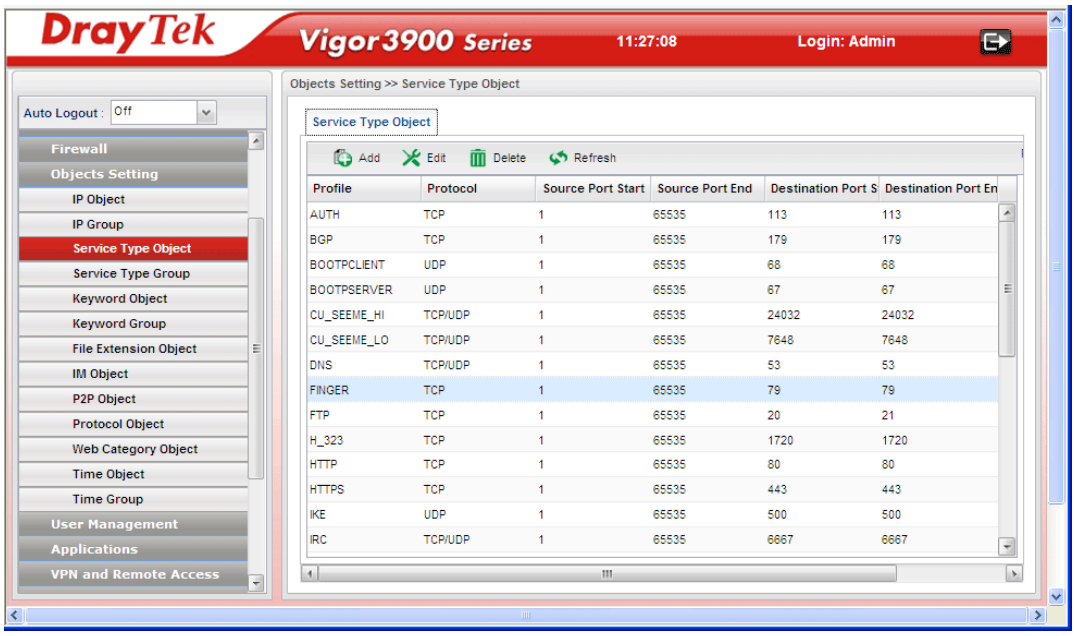
5. A new IP Group profile has been created.



4.5.3 Service Type Object

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

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



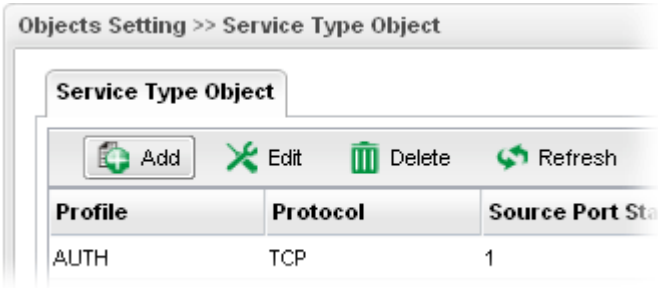
Each item will be explained as follows:

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

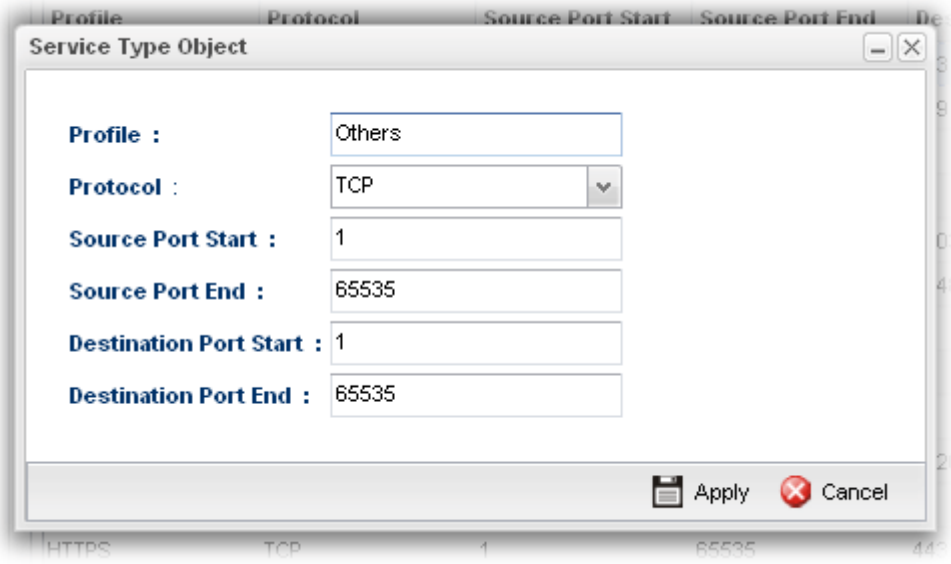
Item	Description
Refresh	Renew current web page.
Profile Number Limit	Display the total number (96) of the object profiles to be created.
Profile	Display the name of the service type object profile.
Protocol	Display the protocol selected for such profile.
Source Port Start	Display the starting source port for such profile.
Source Port End	Display the ending source port for such profile.
Destination Port Start	Display the starting destination port for such profile.
Destination Port End	Display the ending destination port for such profile.

How to create a new Service Type Object profile

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



3. The following dialog will appear.



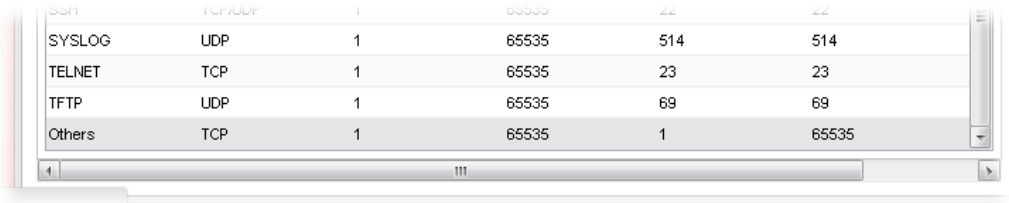
Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile. The number of the characters

Item	Description
	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**.

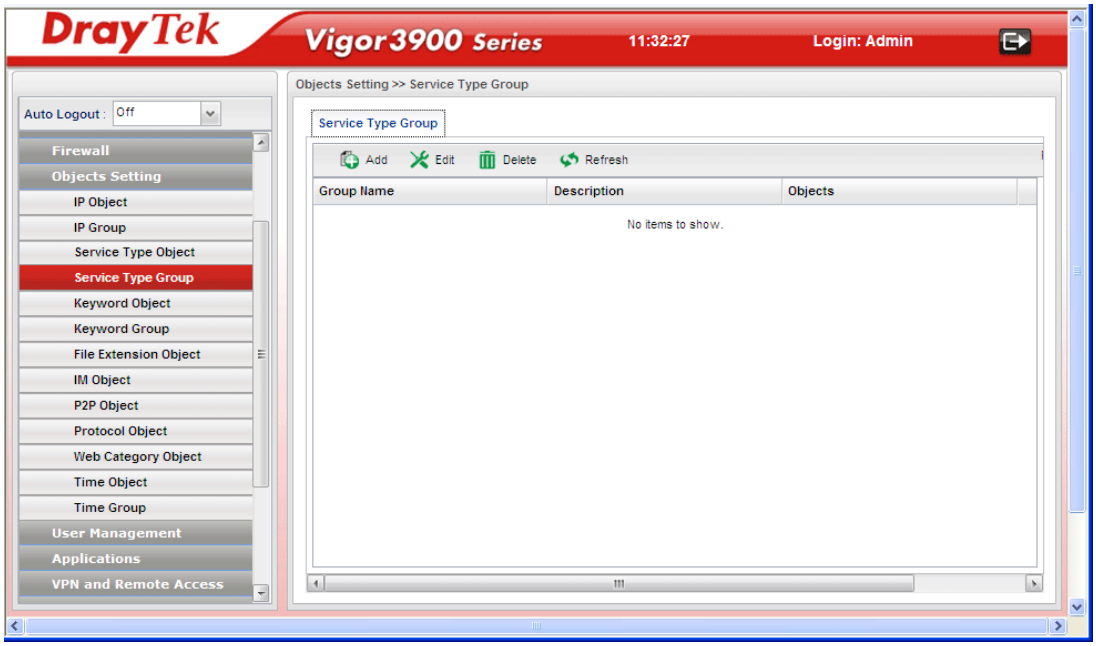
5. A new Service Type Object profile has been created.



4.5.4 Service Type Group

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

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

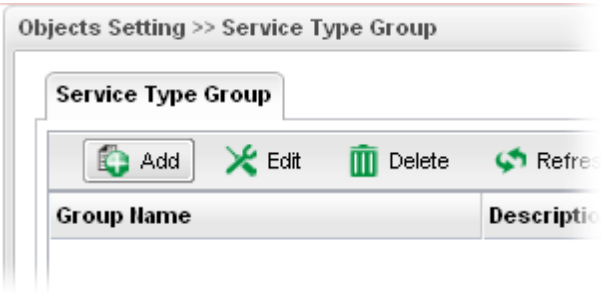


Each item will be explained as follows:

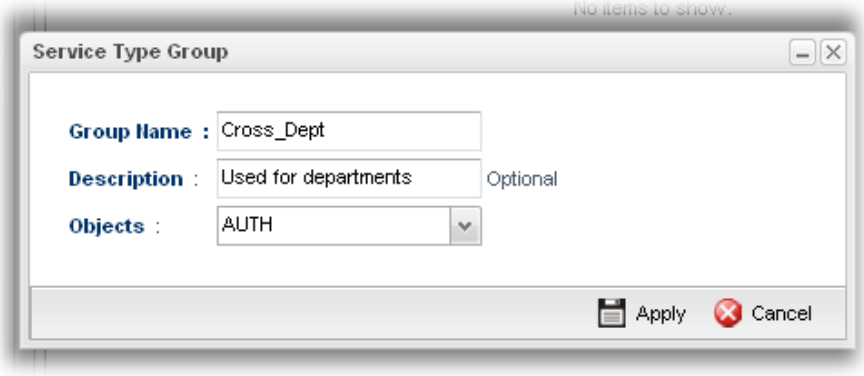
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new Service Type Group profile

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



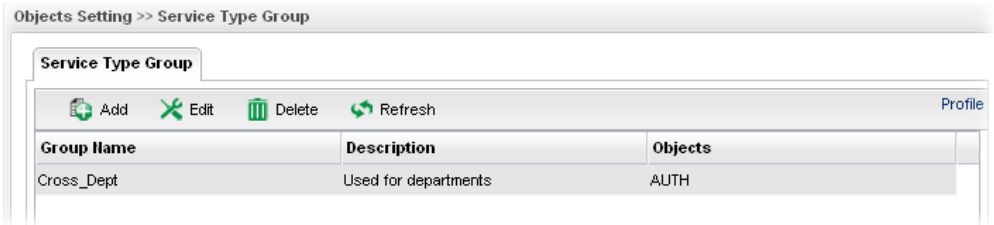
3. The following dialog will appear.



Available parameters are listed as follows:

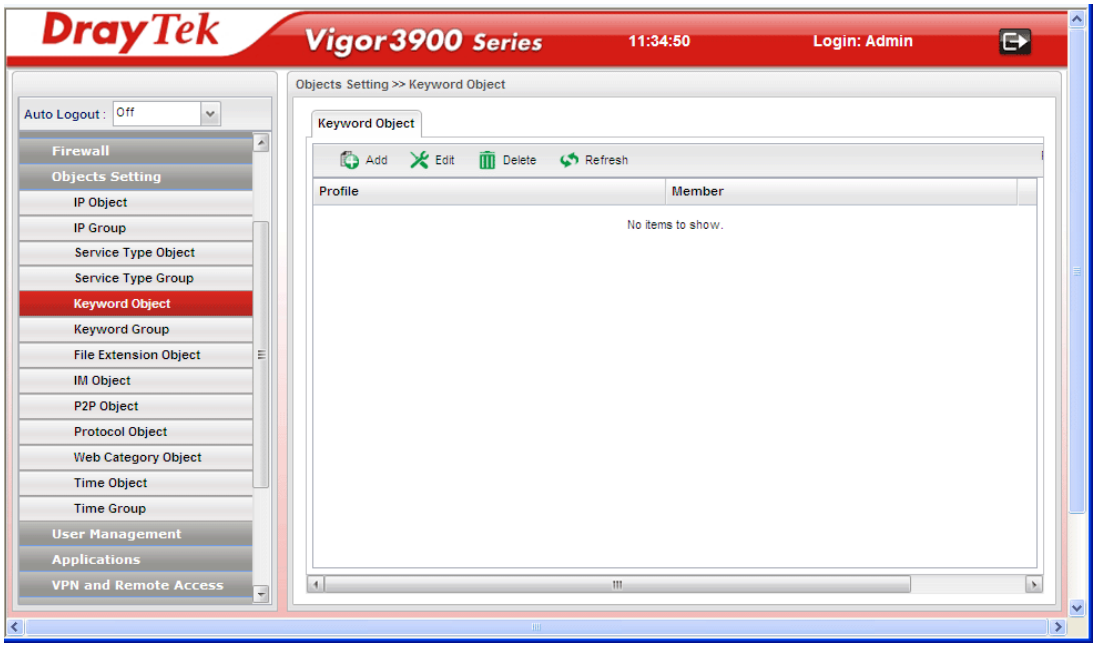
Item	Description
Group Name	Type the name of the service type object group. The number of the characters allowed to be typed here is 10.
Description	Type some words to describe such group.
Objects	Use the drop down list to check the service type object profiles under such group. All the available service type objects that you have added on **Objects Setting>>Service Type Object** will be seen here.
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.



4.5.5 Keyword Object

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

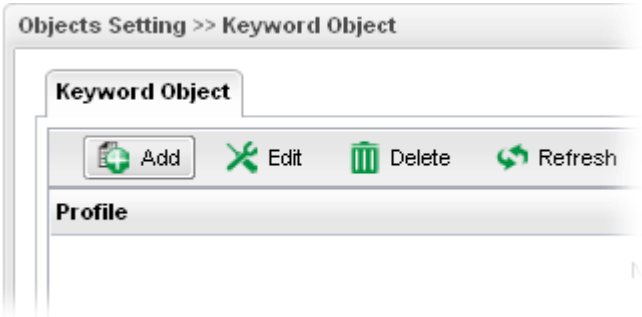


Each item will be explained as follows:

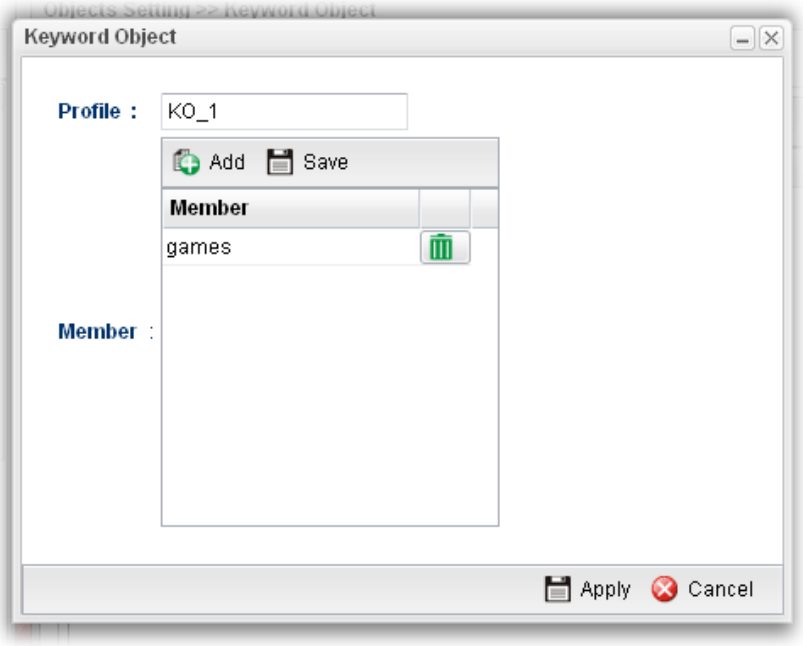
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new Keyword Object profile

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



3. The following dialog will appear.



Available parameters are listed as follows:

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

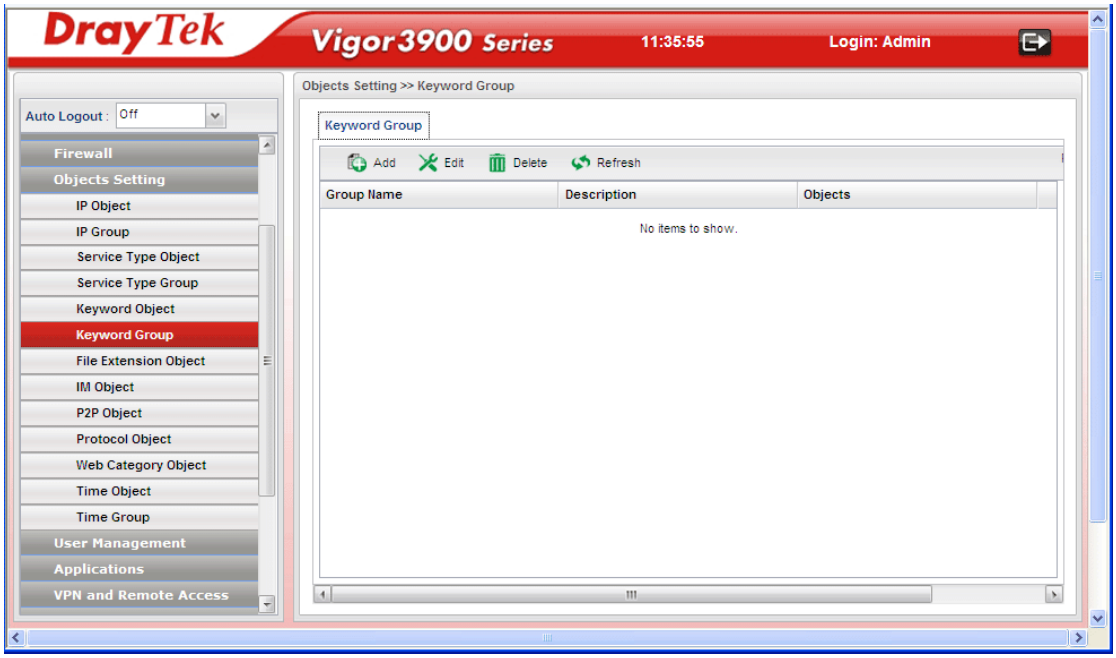
Item	Description
Cancel	Click it to exit the dialog without saving the configuration.

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

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

4.5.6 Keyword Group

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



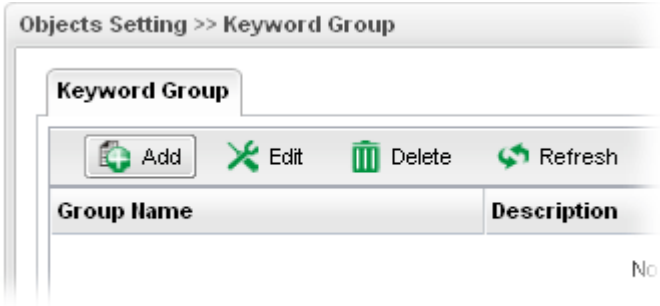
Each item will be explained as follows:

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.

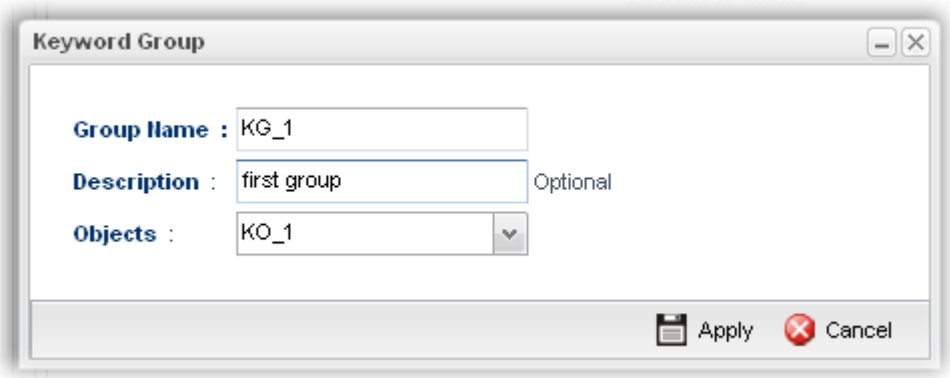
Item	Description
Profile Number Limit	Display the total number (16) of the object profiles to be created.
Group Name	Display the name of the service type group.
Description	Display the brief explanation for such profile.
Objects	Display the keyword object profiles grouped under such group.

How to create a new Keyword Group Profile

1. Open **Objects Setting>> Keyword Group.**
2. Simply click the **Add** button.



3. The following dialog will appear.

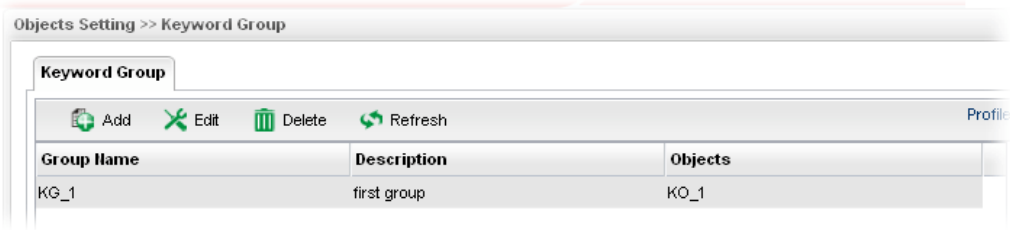


Available parameters are listed as follows:

Item	Description
Group Name	Type the name of the service type object group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the keyword object profiles under such group. All the available keyword objects that you have added on **Objects Setting>>Keyword Object** will be seen here.
Apply	Click it to save the configuration.

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

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



4.5.7 File Extension Object

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

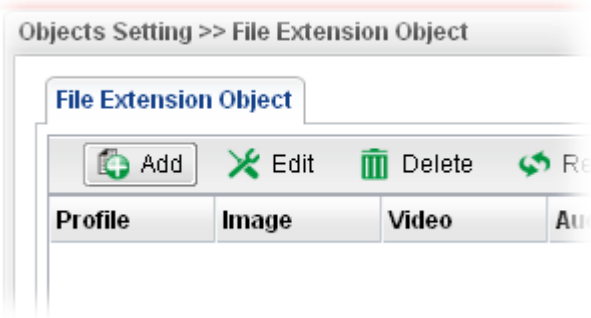
Each item will be explained as follows:

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

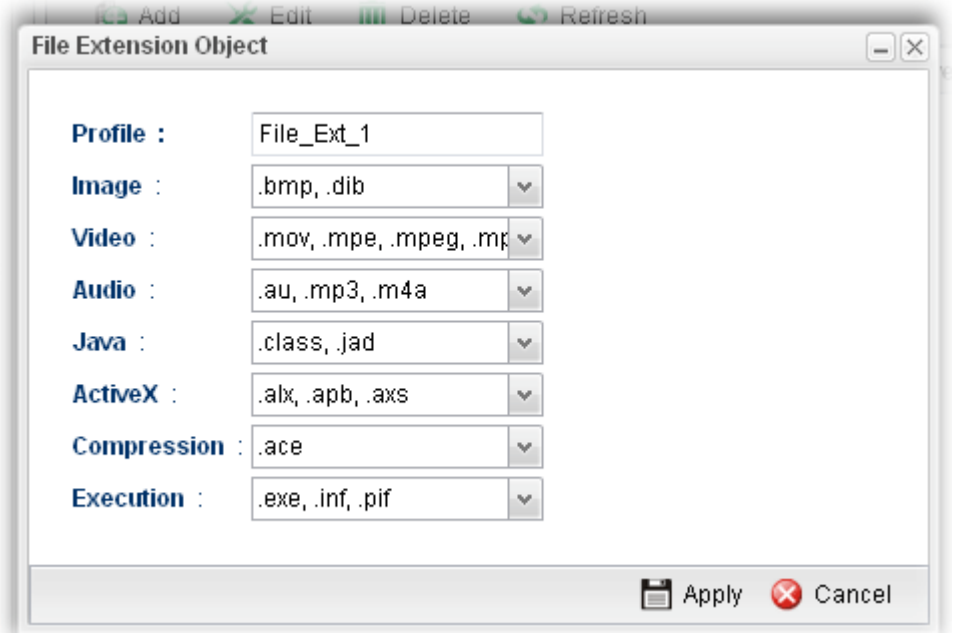
Item	Description
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Profile	Display the name of the profile.
Image	Display the selected file extension of image.
Video	Display the selected file extension of video.
Audio	Display the selected file extension of audio.
Java	Display the selected file extension of java.
ActiveX	Display the selected file extension of activeX.
Compression	Display the selected file extension of compression.
Execution	Display the selected file extension of execution.

How to create a new File Extension Object Profile

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



3. The following dialog will appear.

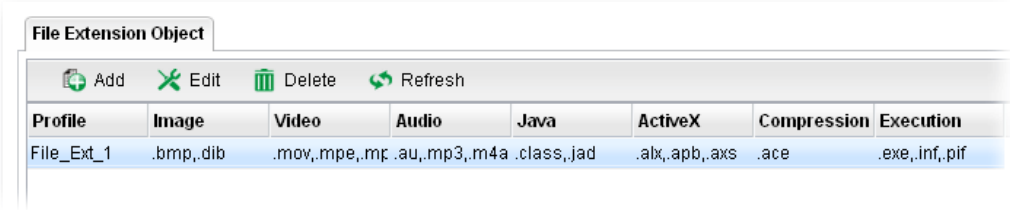


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the File Extension Object group. The number of the characters allowed to be typed here is 10.
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.

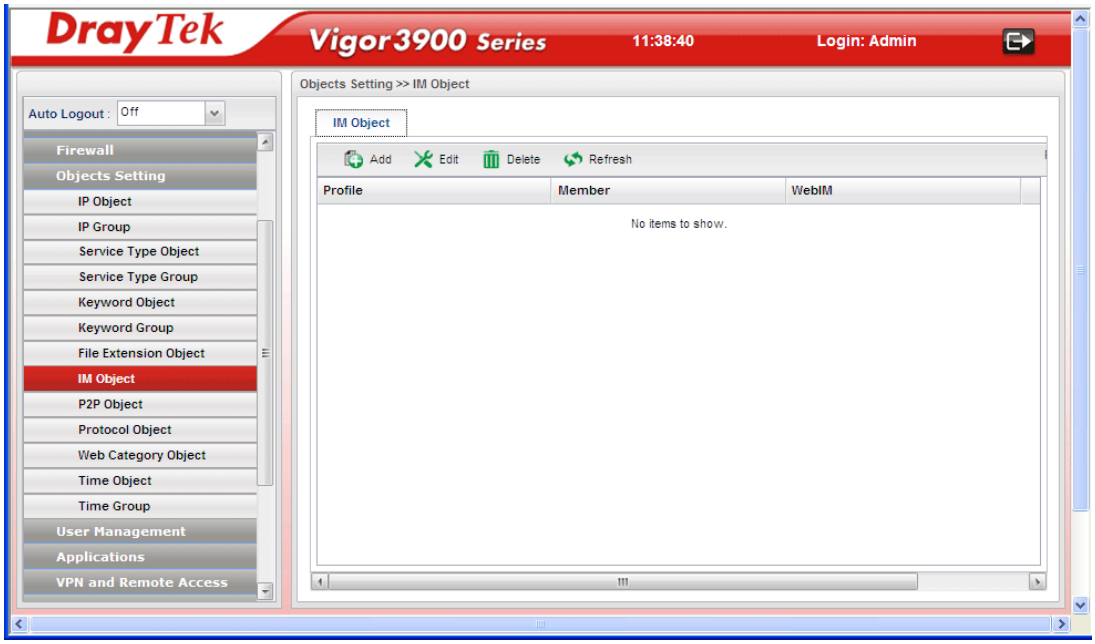
4. Enter all the settings and click **Apply**.

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



4.5.8 IM Object

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.

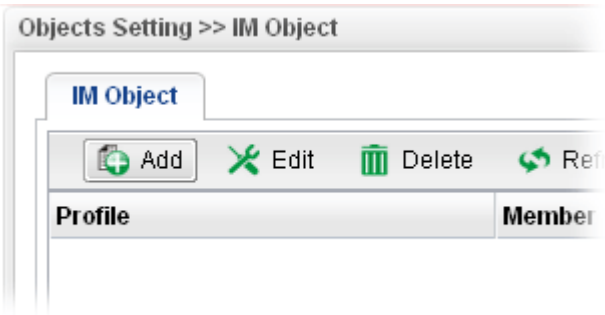


Each item will be explained as follows:

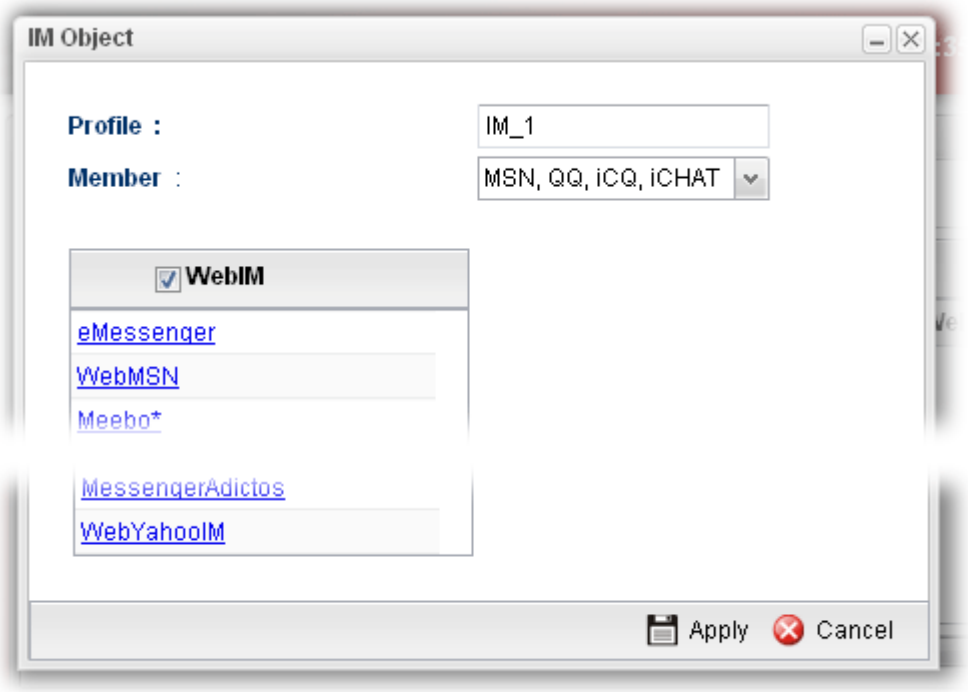
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete 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.
Profile	Display the name of the IM object profile.
Member	Display the IM application specified in such profile.
WebIM	Display the status of IM object whether including the specified set of web IM or not.

How to create a new IM Object Profile

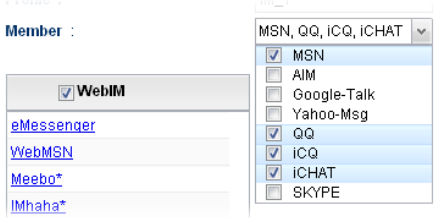
1. Open **Objects Setting>>IM Object.**
2. Simply click the **Add** button.



3. The following dialog will appear.

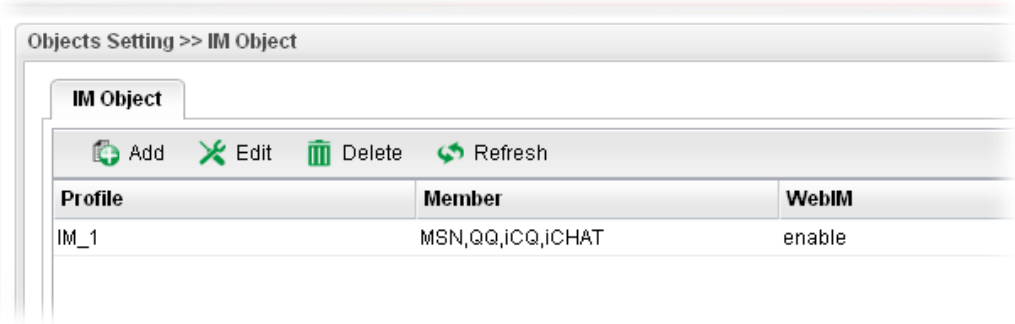


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IM object group. The number of the characters allowed to be typed here is 10.
Member	Several IM applications offered for you to choose. Check the one(s) you want to add for such profile. 

Item	Description
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.

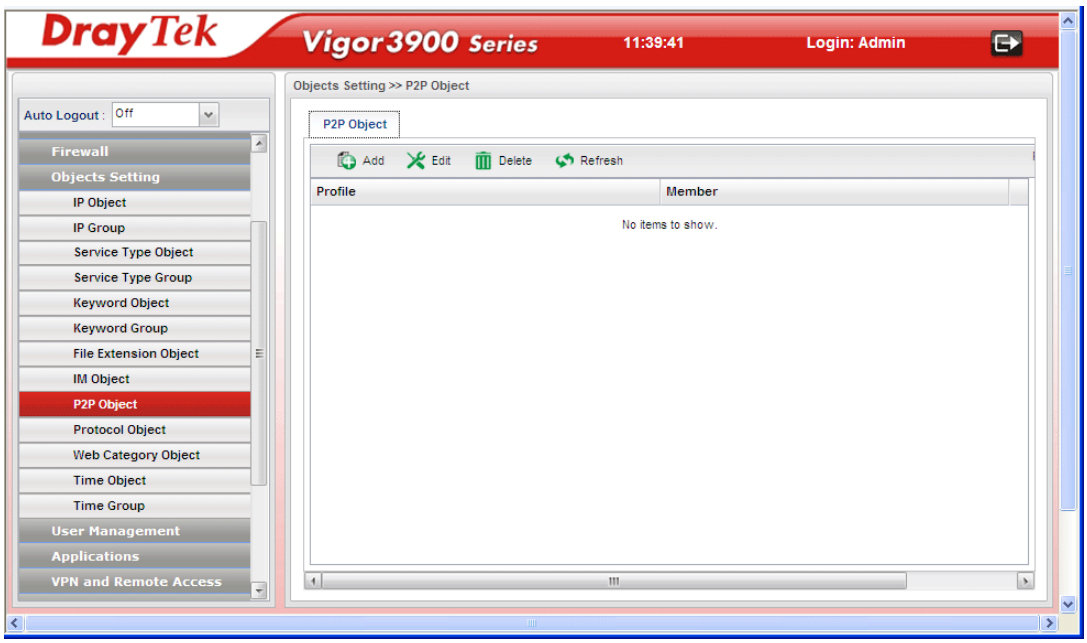
4. Enter all the settings and click **Apply**.
5. A new IM Object profile has been created.



4.5.9 P2P Object

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

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

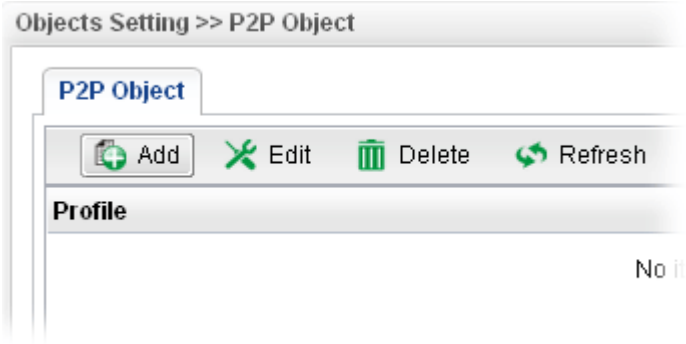


Each item will be explained as follows:

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.
Profile	Display the name of the IM object profile.
Member	Display the P2P application specified in such profile.

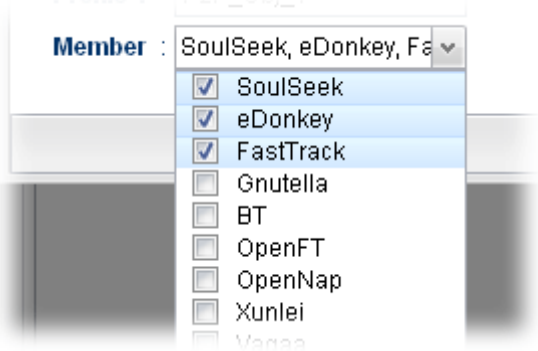
How to create a new P2P Object Profile

1. Open **Objects Setting>>P2P Object.**
2. Simply click the **Add** button.



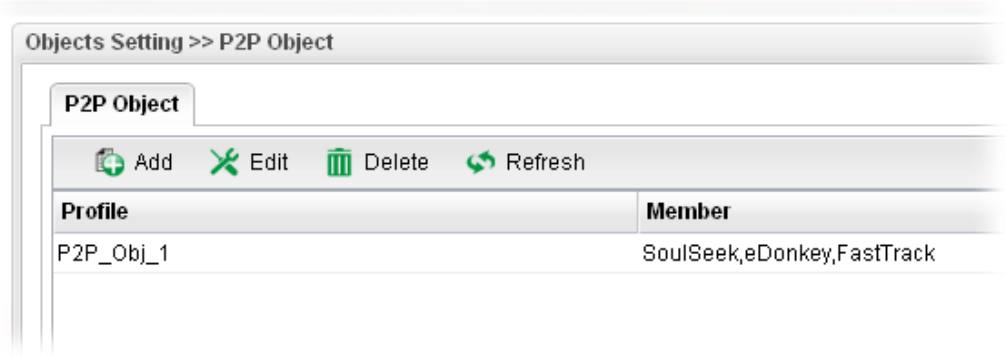
3. The following dialog will appear.

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IM object group. The number of the characters allowed to be typed here is 10.
Member	Several P2P applications offered for you to choose. Check the one(s) you want to add for such profile. 
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

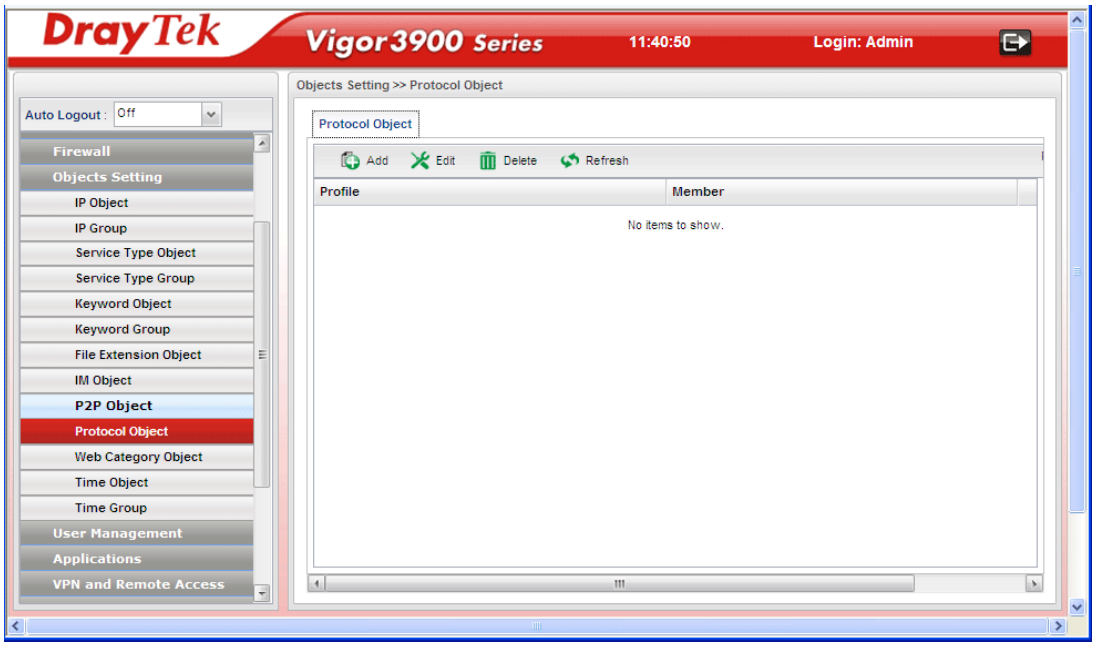
4. Enter all the settings and click **Apply**.

5. A new P2P Object profile has been created.



4.5.10 Protocol Object

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



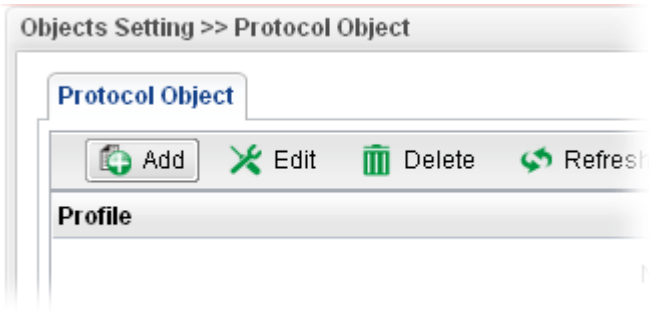
Each item will be explained as follows:

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

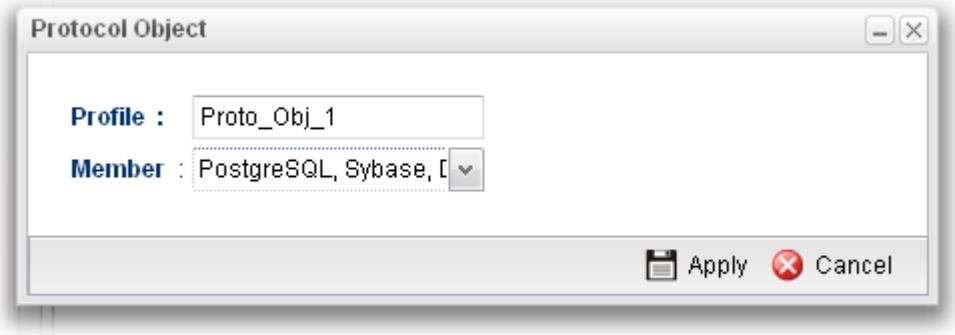
Item	Description
	created.
Profile	Display the name of the IM object profile.
Member	Display the protocol application specified in such profile.

How to create a new Protocol Object Profile

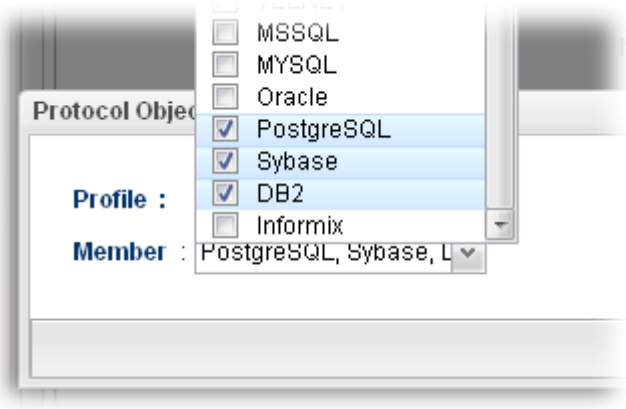
1. Open **Objects Setting>>Protocol Object.**
2. Simply click the **Add** button.



3. The following dialog will appear.

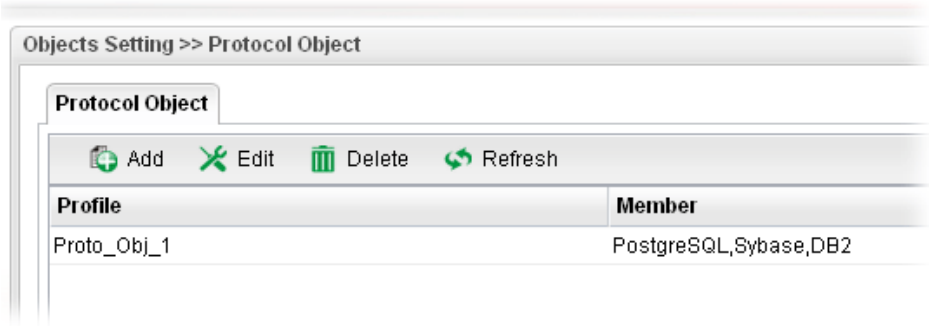


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the protocol object profile. The number of the characters allowed to be typed here is 10.
Member	Several protocols offered for you to choose. Check the one (s) you want to add for such 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 P2P Object profile has been created.



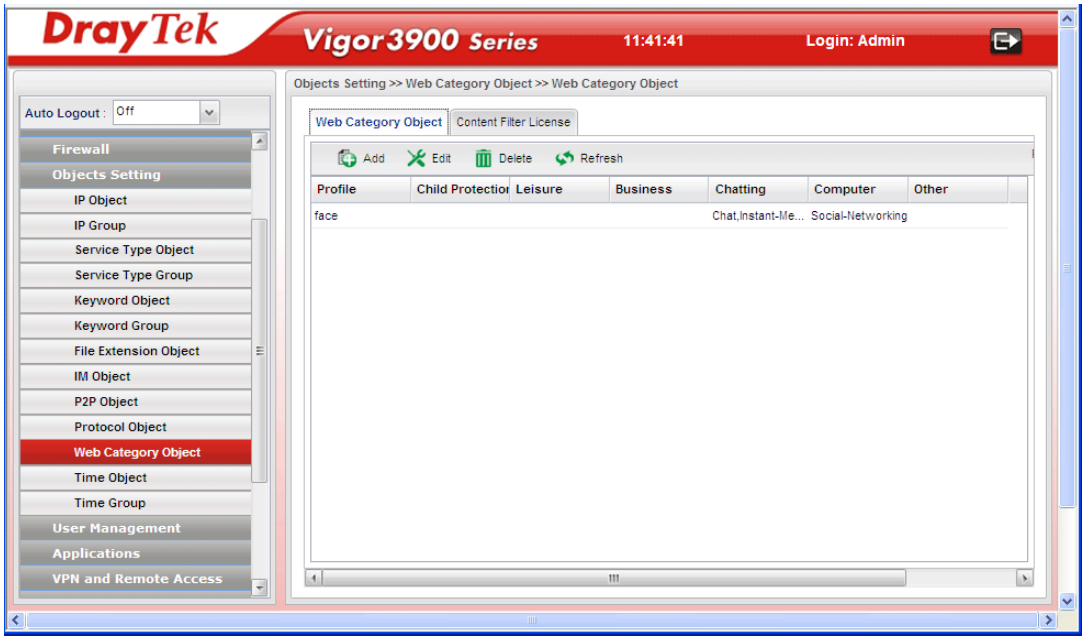
4.5.11 Web Category Object

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: 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.

Web Category Object



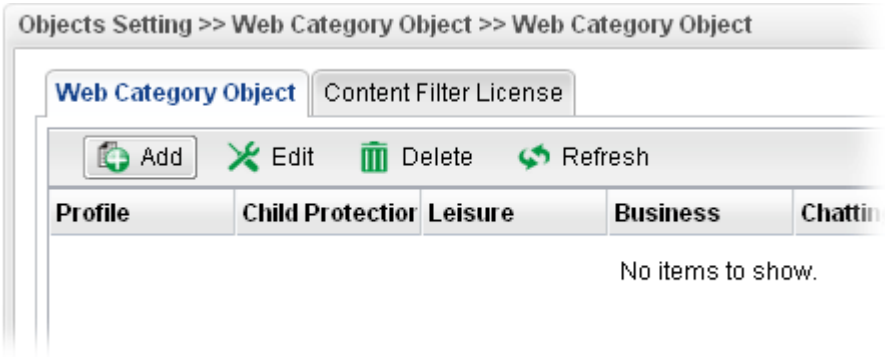
Each item will be explained as follows:

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

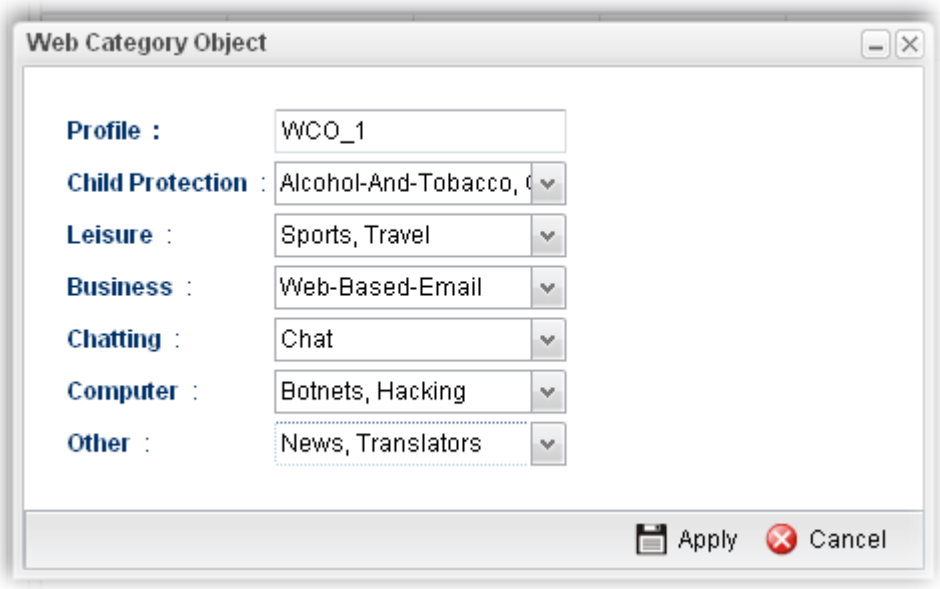
Item	Description
Other	Display the items under certain category that you choose to block.

How to create a new Web Category Object Profile

1. Open **Objects Setting>> Web Category Object** and click the **Web Category Object** tab**.**
2. Simply click the **Add** button.

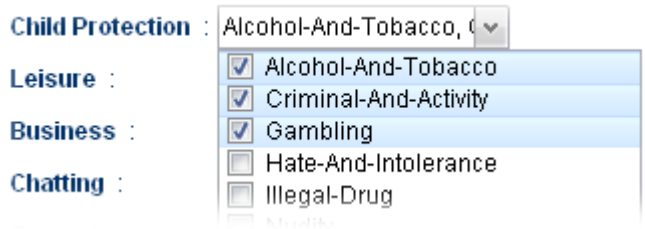


3. The following dialog will appear.

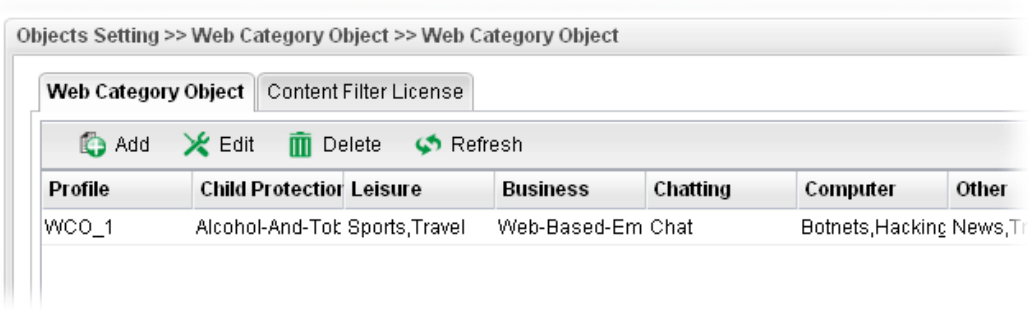


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the web category object profile. The number of the characters allowed to be typed here is 10.

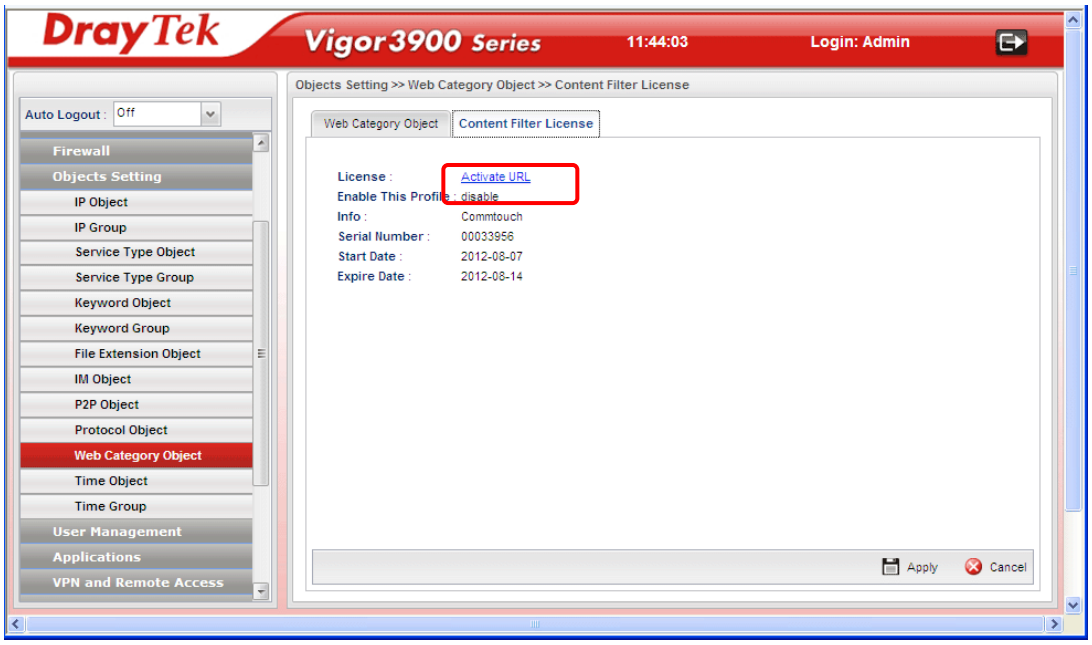
Child Protection	The web pages which are not suitable for children will be classified into different categories. Simply check the one(s) that you don't want the children to visit. 
Leisure	Simply check the one(s) that you don't want the user to visit.
Business	Simply check the one(s) that you don't want the user to visit.
Chatting	Simply check the one(s) that you don't want the user to use for gossip with remote people.
Computer	Simply check the one(s) that you don't want the user to visit.
Other	Simply check the one(s) that you don't want the user to visit.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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



Content Filter License

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



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

4.5.12 Time Object

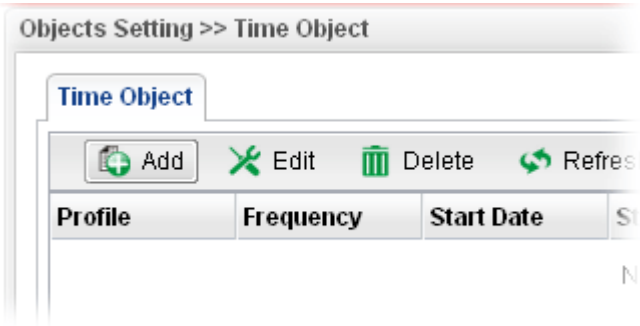
You restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions, e.g., Firewall.

Each item will be explained as follows:

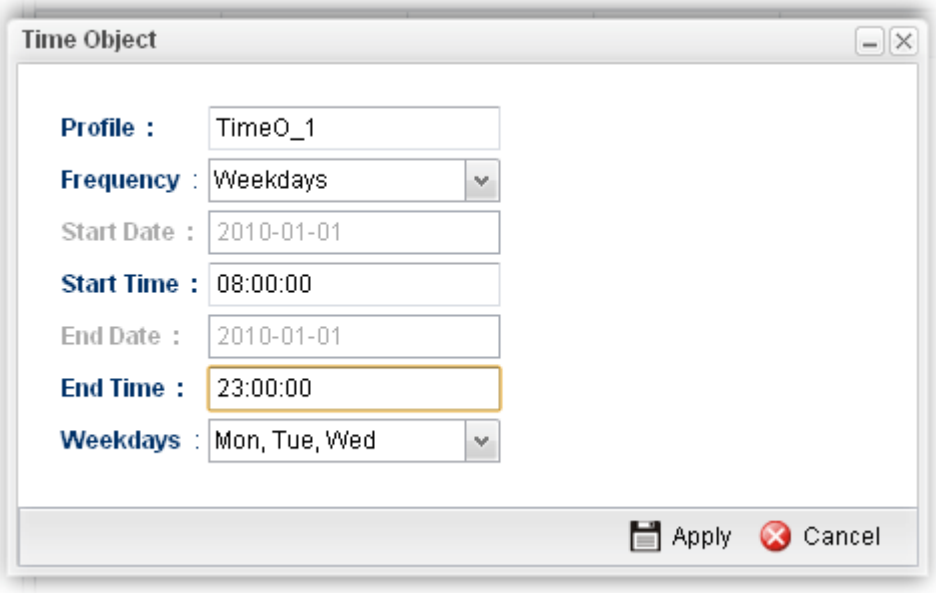
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new Time Object Profile

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

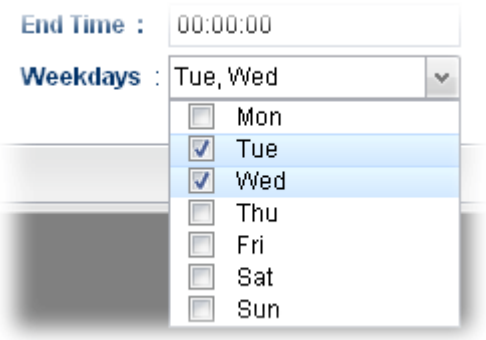


3. The following dialog will appear.



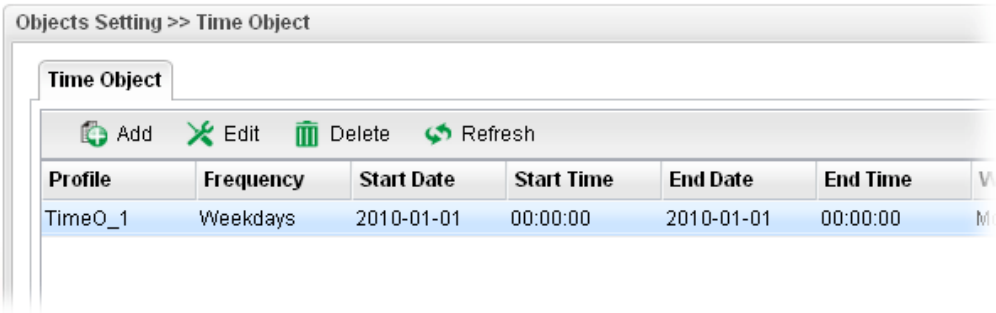
Available parameters are listed as follows:

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

Weekdays	Specify which days in one week should perform the schedule. 
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

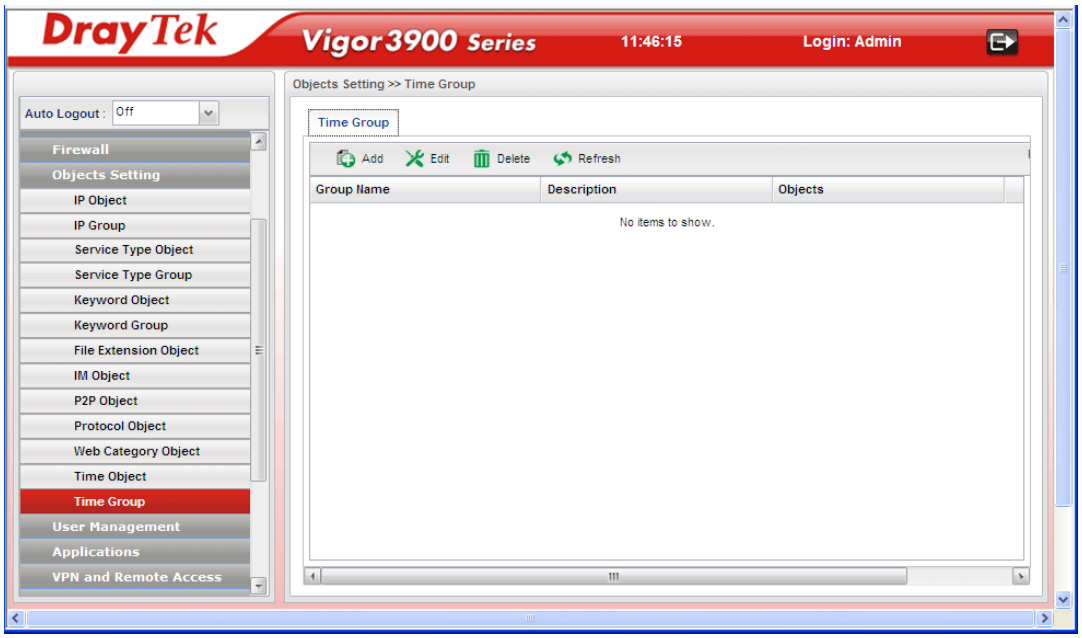
4. Enter all the settings and click **Apply**.

5. A new Time Object profile has been created.



4.5.13 Time Group

This page allows you to group several time object profiles.

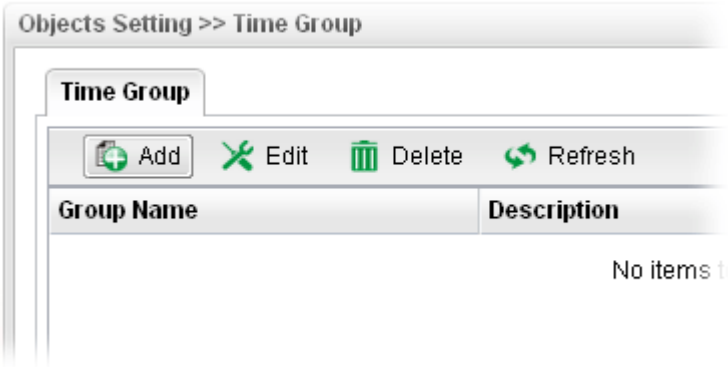


Each item will be explained as follows:

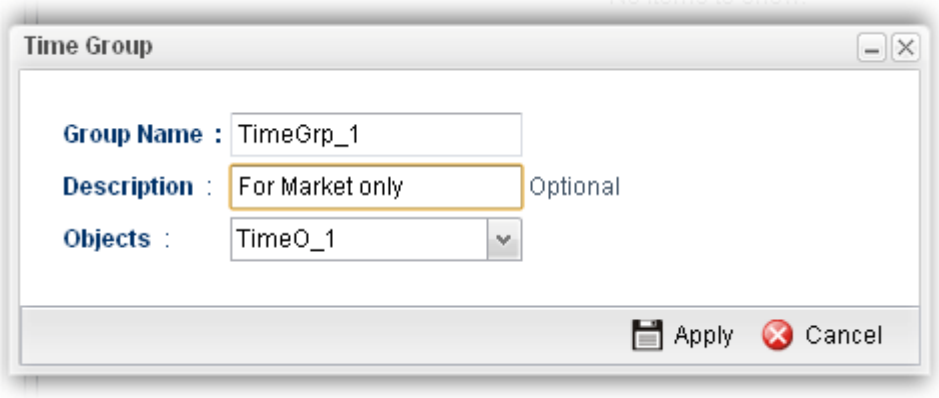
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new Time Group Profile

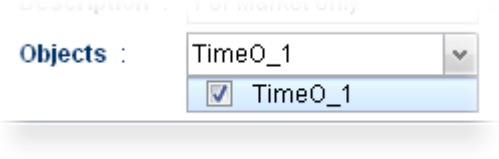
1. Open **Objects Setting>> Time Group.**
2. Simply click the **Add** button.



3. The following dialog will appear.

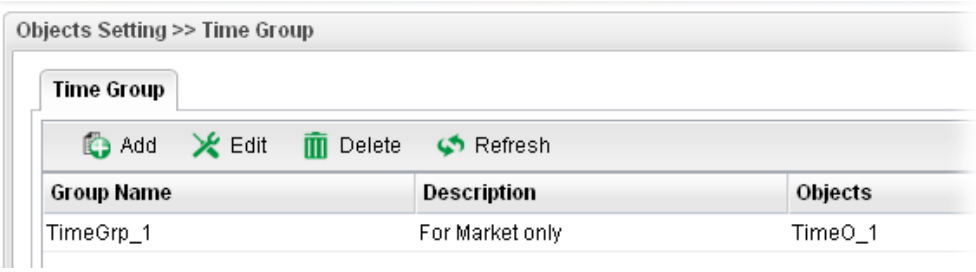


Available parameters are listed as follows:

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

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

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



4.6 User Management

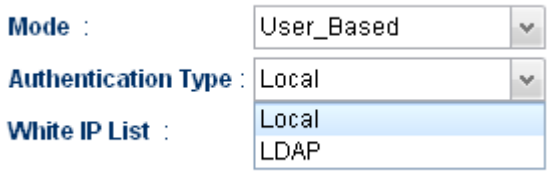
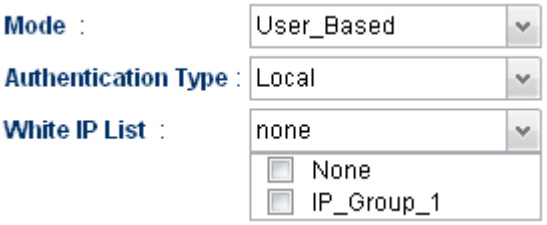
User Management can manage all the accounts (user profiles) to connect to Internet via different protocols.

4.6.1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.

Available parameters will be explained as follows:

Item	Description
Mode	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users

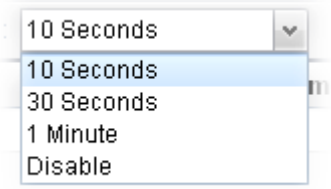
Item	Description
	involved. **User-Based** - If you choose such mode, the router will apply the filter rules configured in **User Management>>User Profile** to the users. **Rule-Based** –If you choose such mode, the router will apply the filter rules configured in **Firewall>>General Setup** and **Filter Rule** to the users.
Authentication Type	Under **User_Based** mode, please specify the authentication type. 
White IP List	Under **User_Based** mode, use the drop down list to choose IP object and/or IP group profiles. 

User-Based Firewall Status

The **User-Based Firewall Status** is a monitoring tool which only works after you choose **User_Based** as the **Mode** setting on **User Management>>General Setup**.

User authentication setup will launch if the router is running in **User_Based** mode. The **User-based Firewall Status** will start to record each authentication event of specified users including authentication failure or success, user's IP, when or how much time the user uses, and how much rest time for the user.

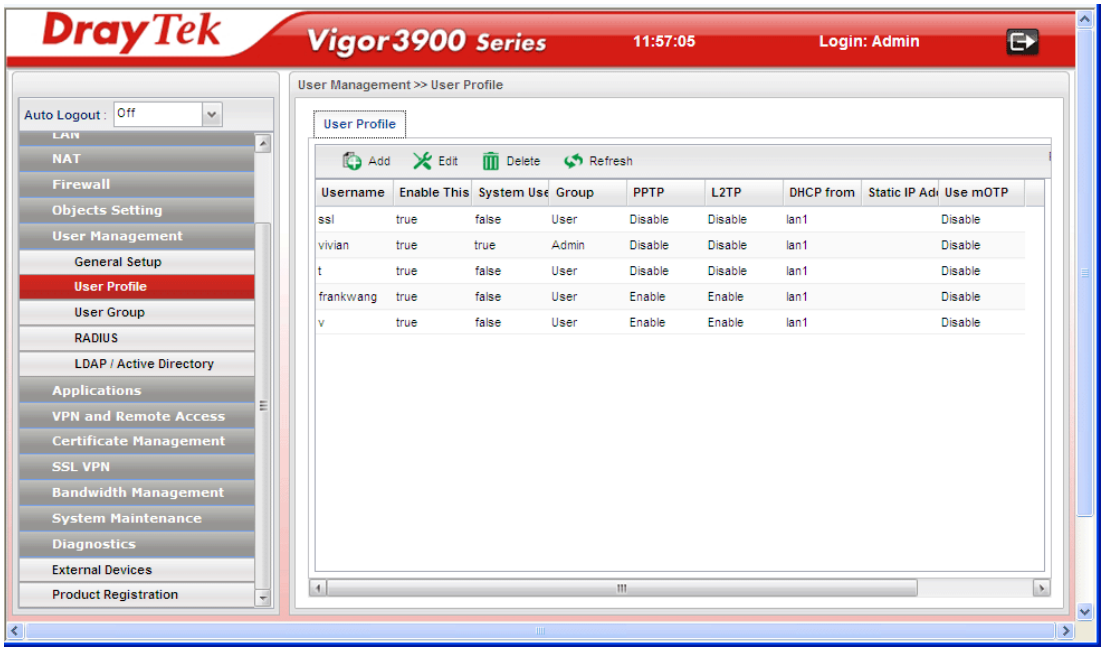
Available parameters will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked. 
User Name	Display the name of the client (wireless station) who accesses into Internet through the wireless connection.
IP	Display the IP address of the wireless station.
Allow Time	Display the total connection time allowed for the wireless station.
Start Time	Display the starting time of the wireless station.
End Time	Display the ending time of the wireless station.
Rest Time	Display the rest time for the wireless station to browse the Internet.
Delete	– It is available for the administrator to turn off a specific user's connection immediately.

Item	Description

4.6.2 User Profile

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



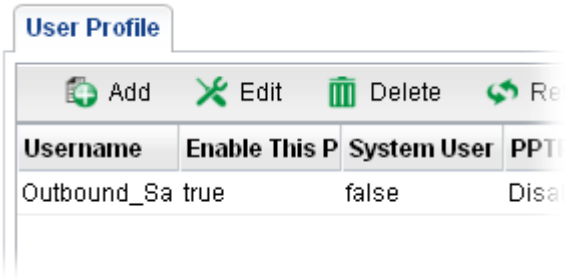
Each item will be explained as follows:

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.
Username	Display the name of the user.

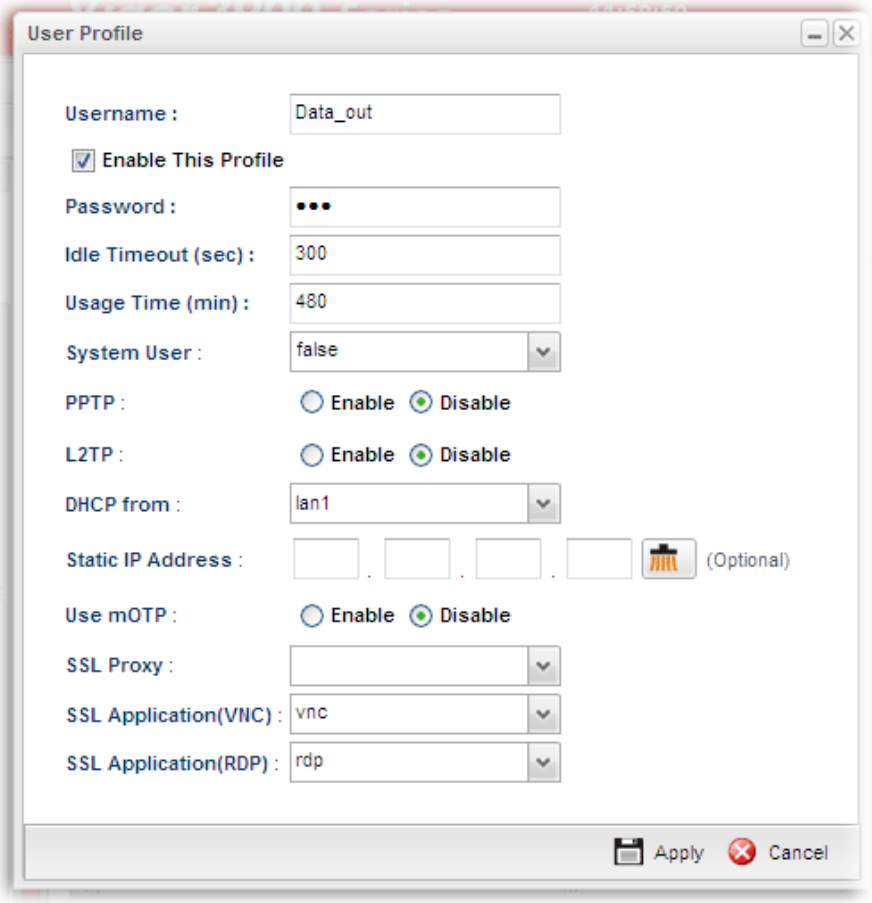
Item	Description
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
System User	Display the status of the System User. False means disabled; True means enabled.
PPTP	Display the status of PPTP/L2TP connection for such user profile.
L2TP	Display the LAN profile that such profile belongs to.
DHCP from	Display the LAN profile that DHCP server used for assigning IP address(es).
Static IP Address	Display the IP address for such user profile which accesses Internet with PPTP/L2TP connection.
Use mOTP	Display if mOTP is activated (enable or disable) or not.

How to create a new User Profile

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



3. The following dialog will appear.



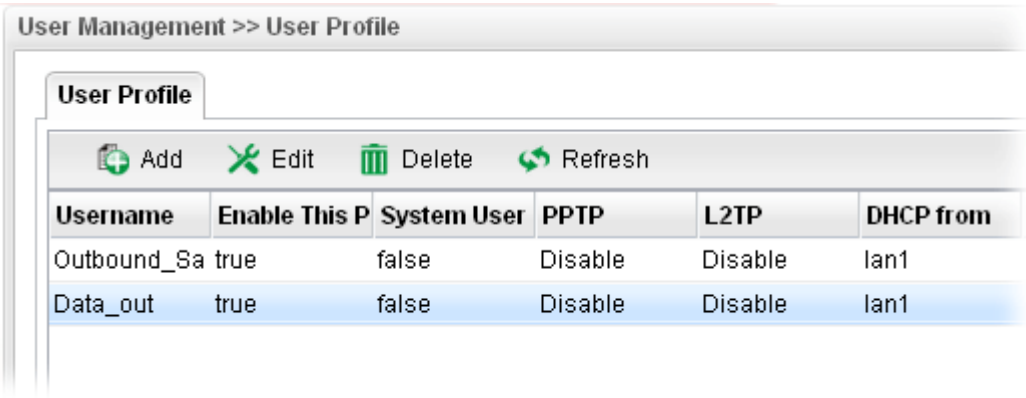
Available parameters are listed as follows:

Item	Description
Username	Type a name for such user profile (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the Username specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Enable This Profile	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.
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.

Usage Time (min)	It means the maximum usage duration for the user. By default, the Usage Time is 480 minutes.
System User	Choose **True** to allow the user accessing into WUI of Vigor3900 via the username and password above. If you choose **False**, you can set SSL for such profile.
PPTP/L2TP	Click **Enable** to make network connection through PPTP/L2TP protocol for users who access into Internet via such profile.
DHCP from	Choose a LAN profile for DHCP server.
Static IP Address	Type an IP address for such user profile which accesses Internet with PPTP/L2TP connection.
Use mOTP	Click **Enable** to make the authentication with mOTP function.
mOTP PIN Code	Type the code for authentication (e.g, 1234).
mOTP secret	Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
SSL Proxy	It is available when **System User** is set with **false**. The web proxy over SSL will be applied for VPN.
SSL Application (VNC)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (VNC) for applying into this profile.
SSL Application (RDP)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (RDP) for applying into this profile.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

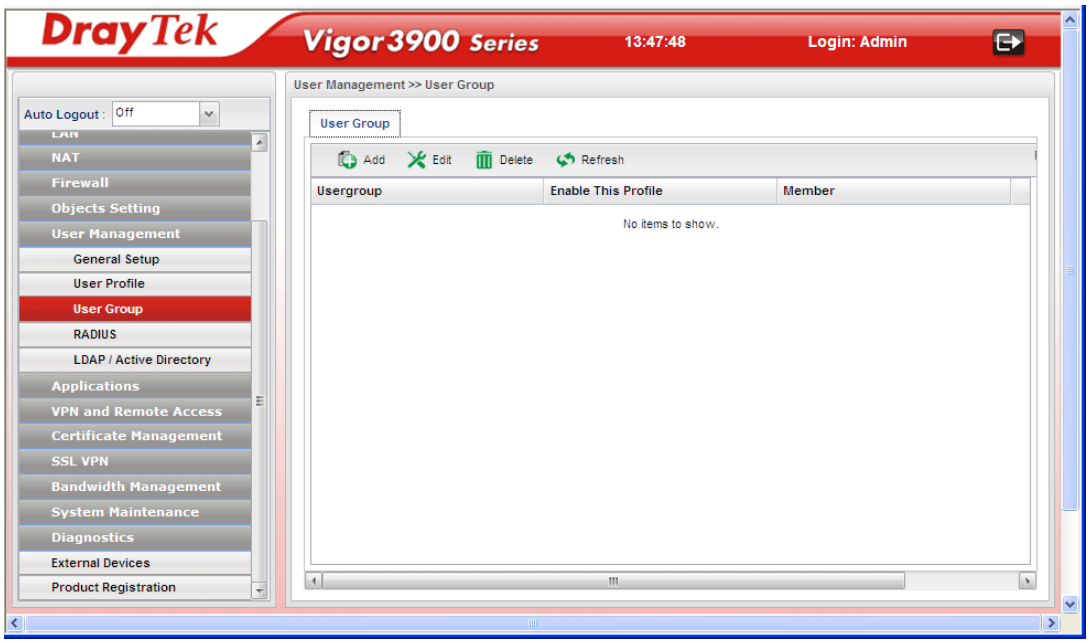
4. Enter all the settings and click **Apply**.

5. A new User Profile has been created.



4.6.3 User Group

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

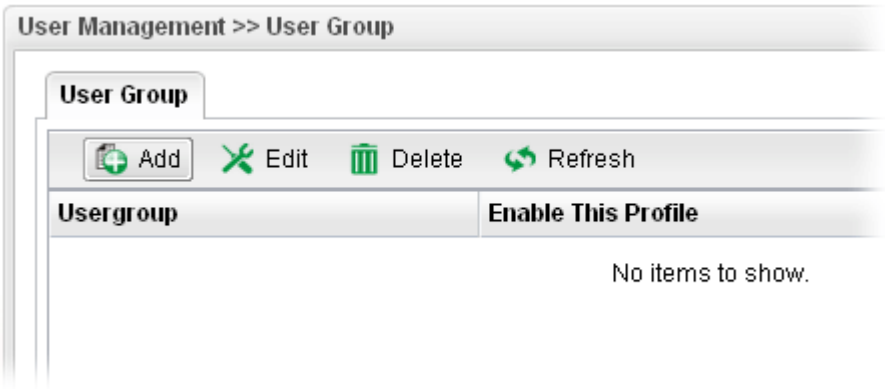


Each item will be explained as follows:

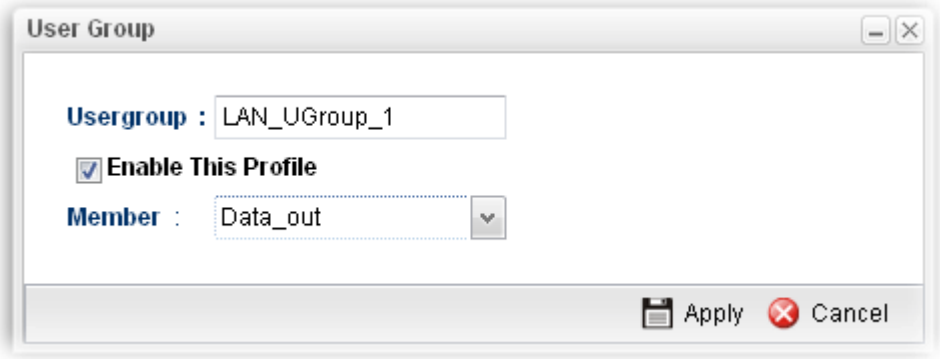
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete 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 (200) of the object profiles to be created.
Usergroup	Display the name of the user group.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Member	Display the user profiles under such group.

How to create a new User Group Profile

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



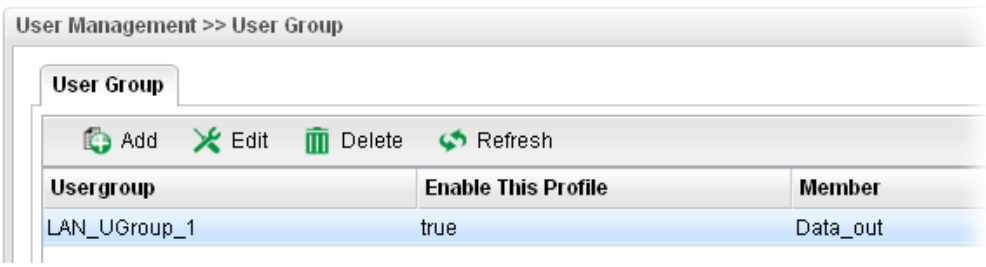
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Usergroup	Type the name of such profile.
Enable This Profile	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group.
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.



4.6.4 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.

Available parameters are listed as follows:

Item	Description
Enable This Profile	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.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

4.6.5 LDAP/Active Directory

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

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

Available parameters are listed as follows:

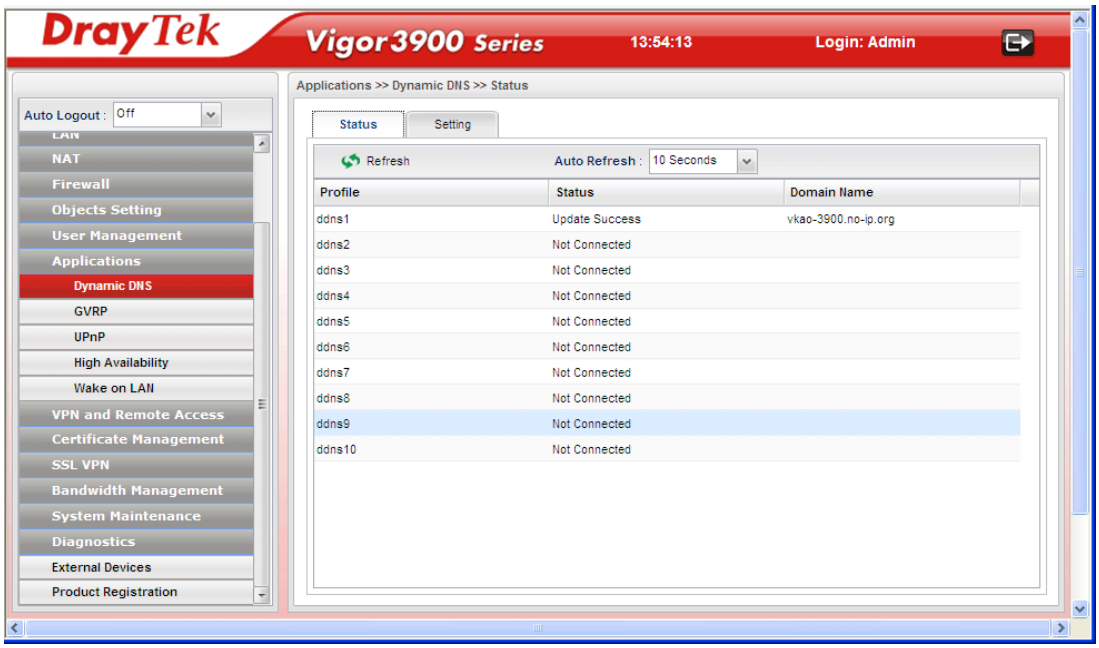
Item	Description
Enable This Profile	Check this box to enable such profile.
Server IP Address	Enter the IP address of RADIUS server.
Port	It means the port on TCP for establishing an LDAP session between clients and LDAP server. The default value is 389.
Base DN	It means "**Base Distinguished Name**". Type or edit the distinguished name used to look up entries on the LDAP server.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

4.7 Application

Below shows the menu items for Applications.

4.7.1 Dynamic DNS

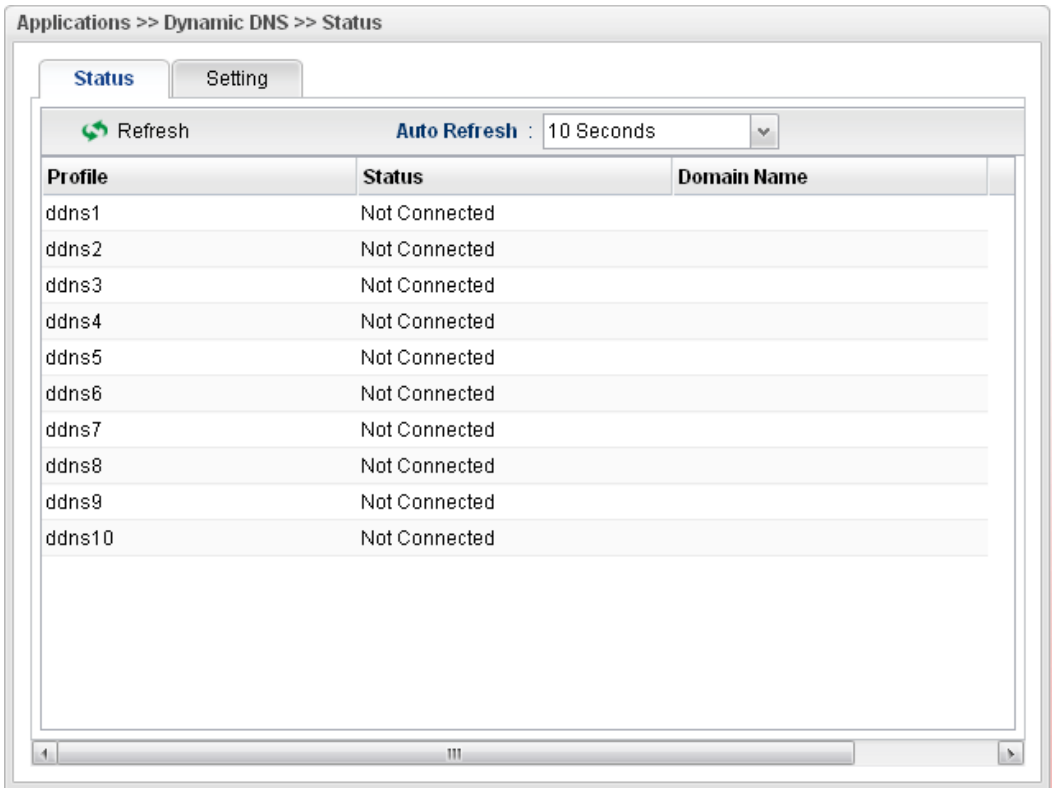
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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.



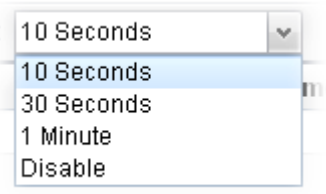
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to ten accounts from eight different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers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

Status

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

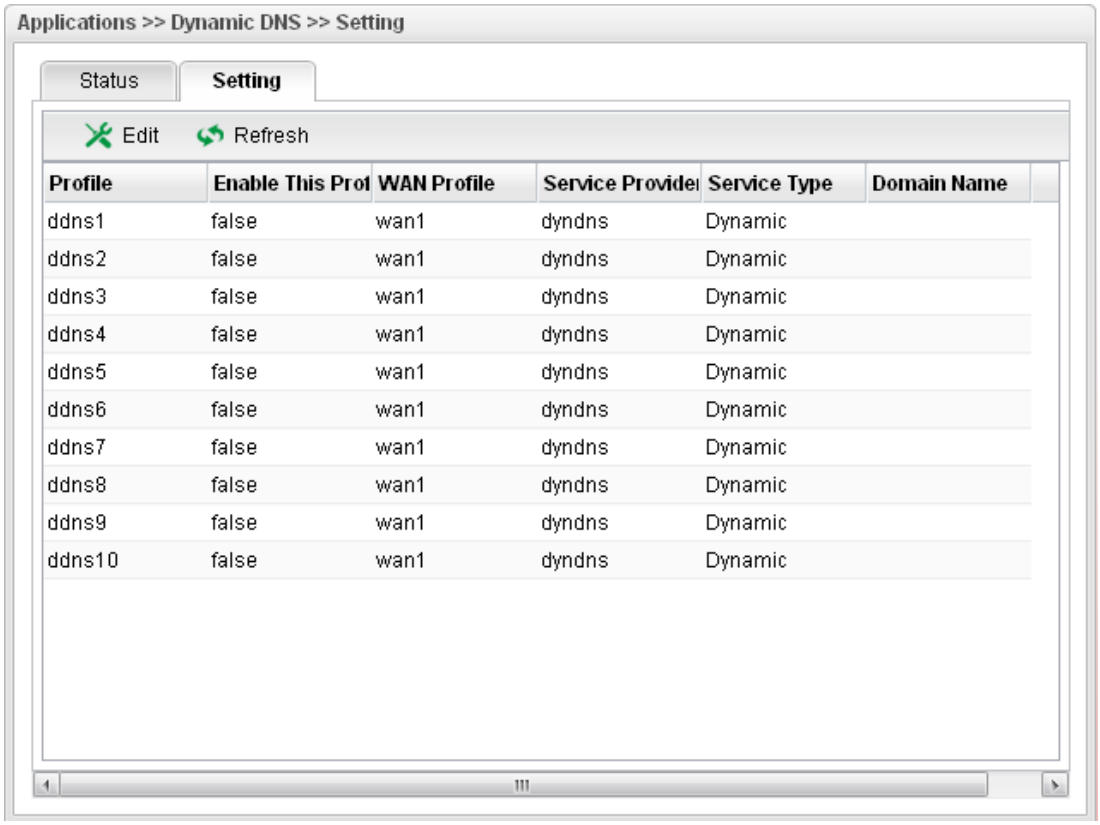


Each item will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked. 
Profile	Display the name of the DDNS.
Status	Display the connection status for the DDNS sever.
Domain Name	Display the domain name for the DDNS server.

Setting

This page allows you to configure DDNS profiles for your request.



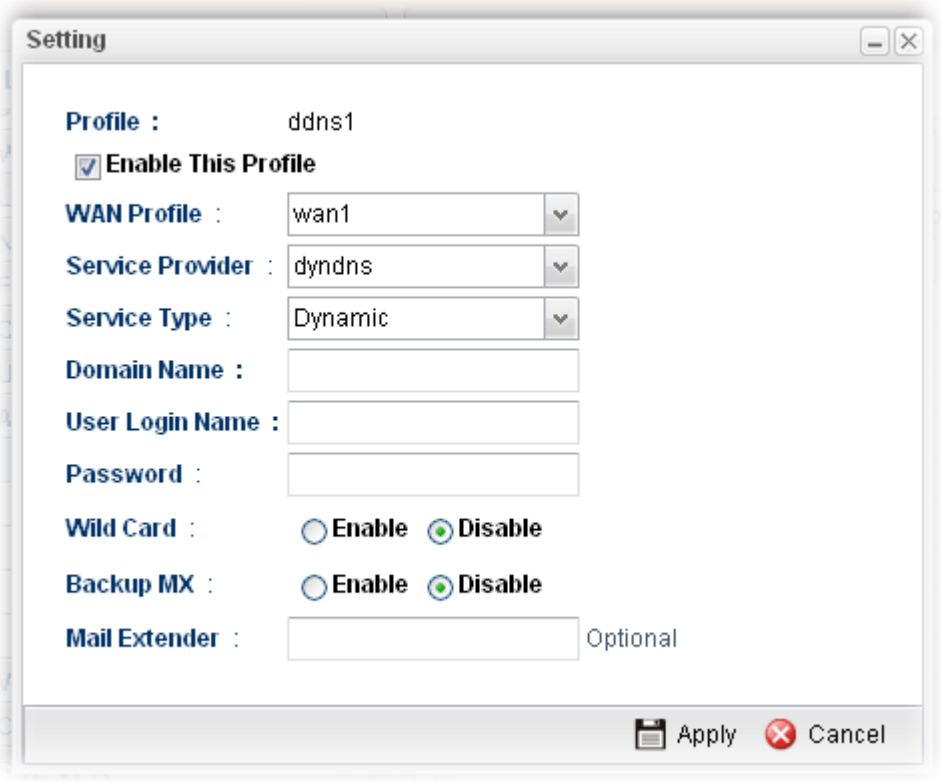
Each item will be explained as follows:

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

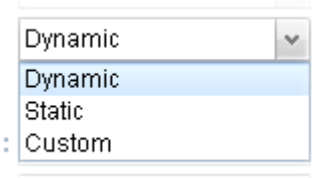
How to edit an existing DDNS Profile

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. Simply click the **Edit** button.

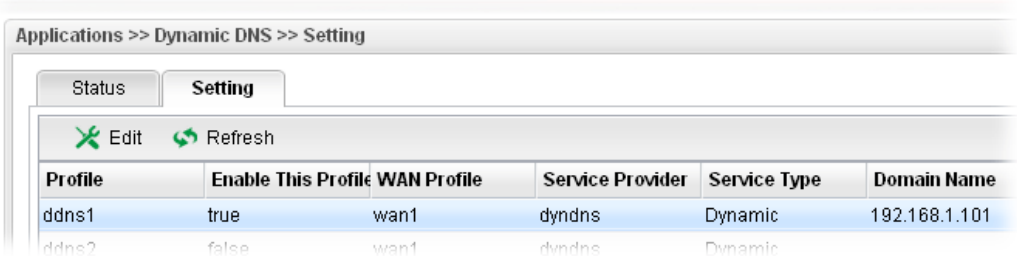


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable This Profile	Check this box to enable such profile.
WAN Profile	Choose a WAN profile that such profile will apply to.
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.
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.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

3. Enter all the settings and click **Apply**.
4. The DDNS Profile has been modified.



4.7.2 GVRP

This function can define the method for the changing the VLAN information among devices. With supporting GVRP, the device can receive the VLAN information coming from other devices.

Available parameters are listed as follows:

Item	Description
Enable This Profile	Check this box to enable GVRP function.
Interface	Choose a LAN or WAN profile.

Item	Description
Join Time	Define the time for the system to send GVRP packet to other device. The unit is second.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.7.3 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

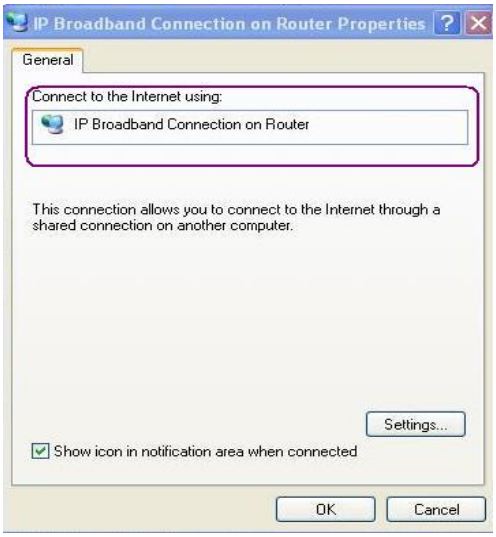
Available parameters are listed as follows:

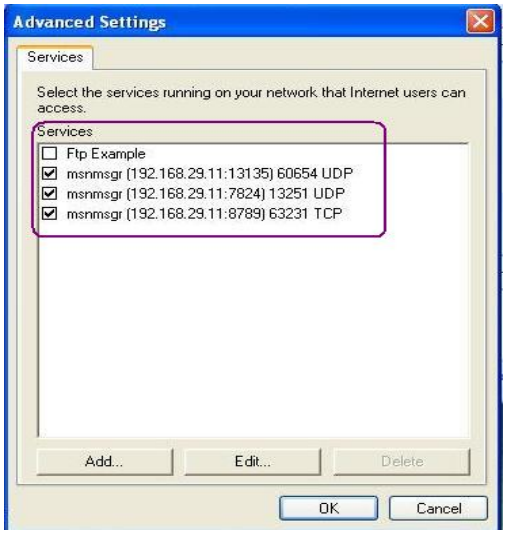
Item	Description
Enable This Profile	Check this box to enable UPnP function.
Download	Enter the maximum sustained WAN download speed in kilobits/second. Such information can be requested by UPnP clients.
Upload	Enter the maximum sustained WAN upload speed in kilobits/second. Such information can be requested by UPnP clients.
External Interface	Select a WAN profile for UPnP protocol.
Internal Interface	Select a LAN profile for UPnP protocol.

Item	Description
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.

After **enabling UPNP** service setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.





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.

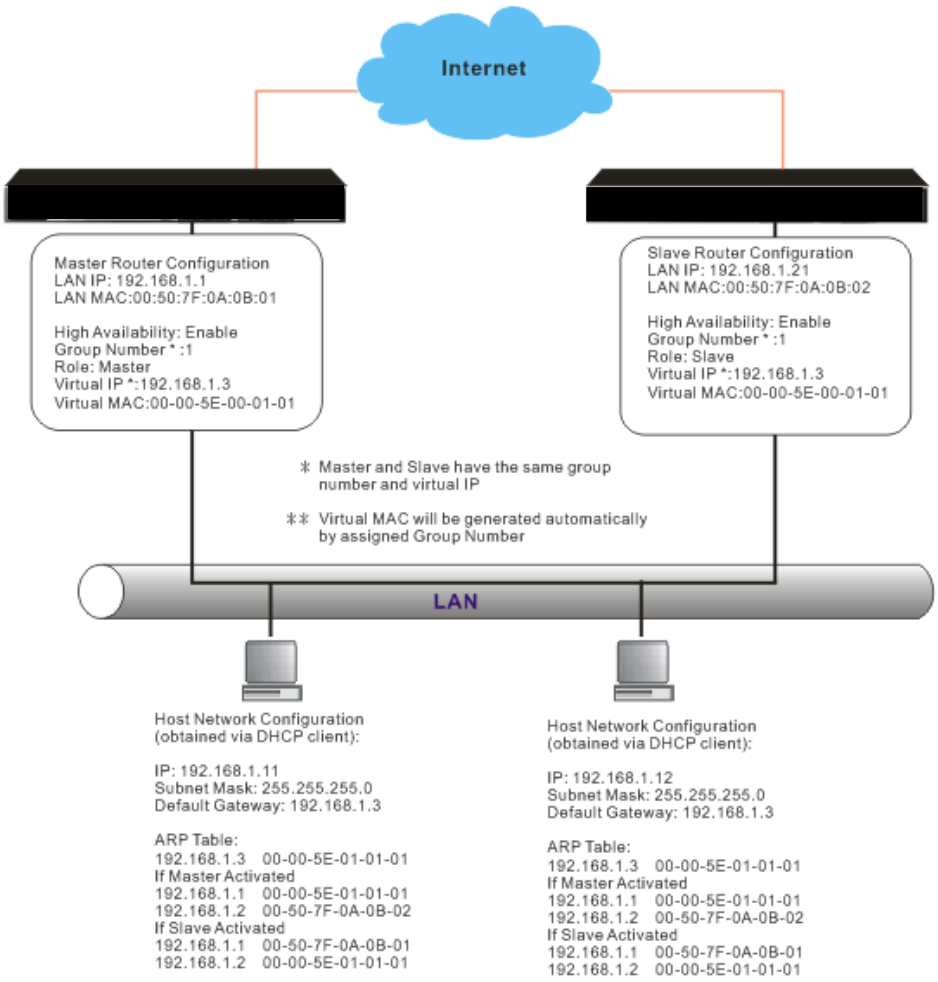
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

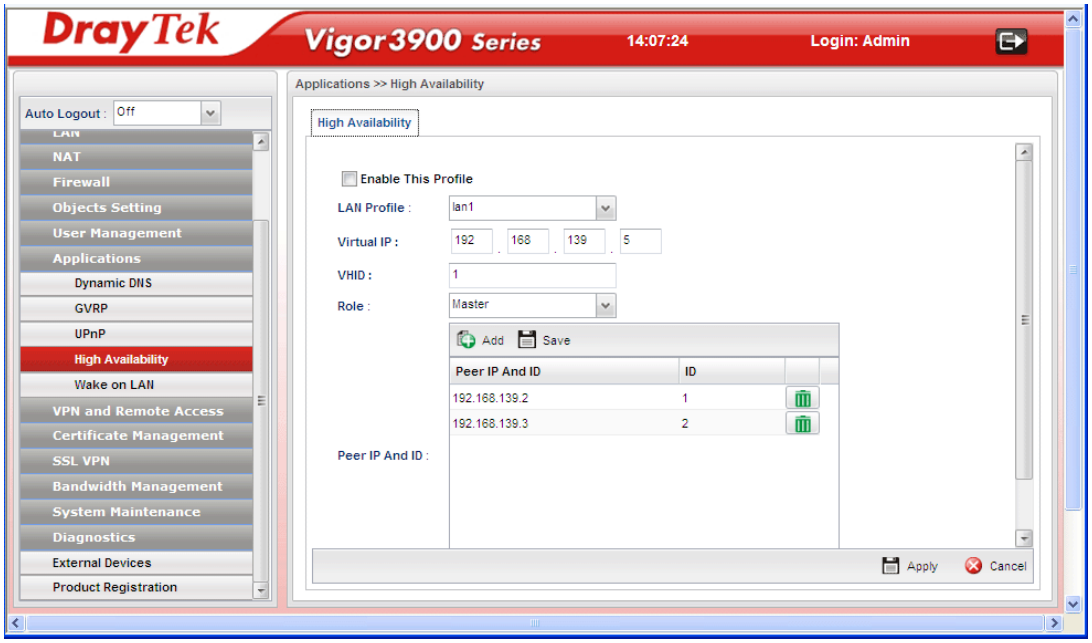
4.7.4 High Availability

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

The high availability of the V3900 Series is designed to avoid single points-of-failure. When failures occur, the failover process moves processing performed by the failed component (the "Master") to the backup component (the "Slave"). This process remains system-wide resources, recovers partial of failed transactions, and restores the system to normal within a matter of microseconds.

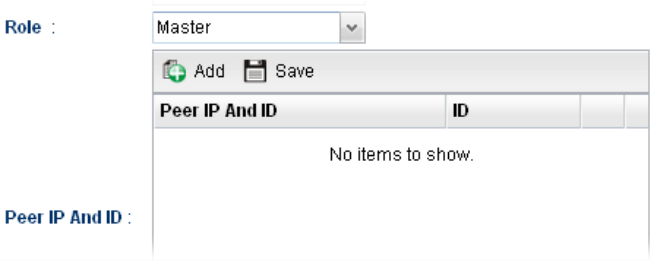
Take the following picture as an example. The left V3900 Series is regarded as Master device, the right V3900 Series is regarded as Slave device. When Master V3900 Series is broken down, the Slave (backup) device could replace the Master role to take over all jobs as soon as possible. However, once the original Master is working again, the Slave would be changed to original role to stand by.





Available parameters are listed as follows:

Item	Description
Enable This Profile	Check this box to enable UPnP function.

Item	Description
LAN Profile	Choose one of the LAN profiles that such function will be applied to.
Virtual IP	Assign an IP address as a virtual IP.
VHID	It means Virtual Host ID. Type a number as VHID for such function.
Role	Select a role for this device as Master or Backup. If you choose **Master**, the fields of **Peer IP** and **ID** will be hidden.  If you choose **Backup**, the field of **Peer IP and ID** will be hidden.
Peer IP	Type the IP address of the peer side. If **Master** is chosen as the role for Vigor3900, please type the LAN IP address of the backup device. If **Backup** is chosen as the role of Vigor3900, please type the LAN IP address of the master device.
ID	Type a number value here to represent the privilege of the peer IP.
Peer IP and ID	You can type several groups of Peer IP and ID for Vigor3900 (when it represents the Master device).
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.7.5 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.

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	Two types provide for you to wake up the binded 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.
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 binded PCs.
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 VPN and Remote Access

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

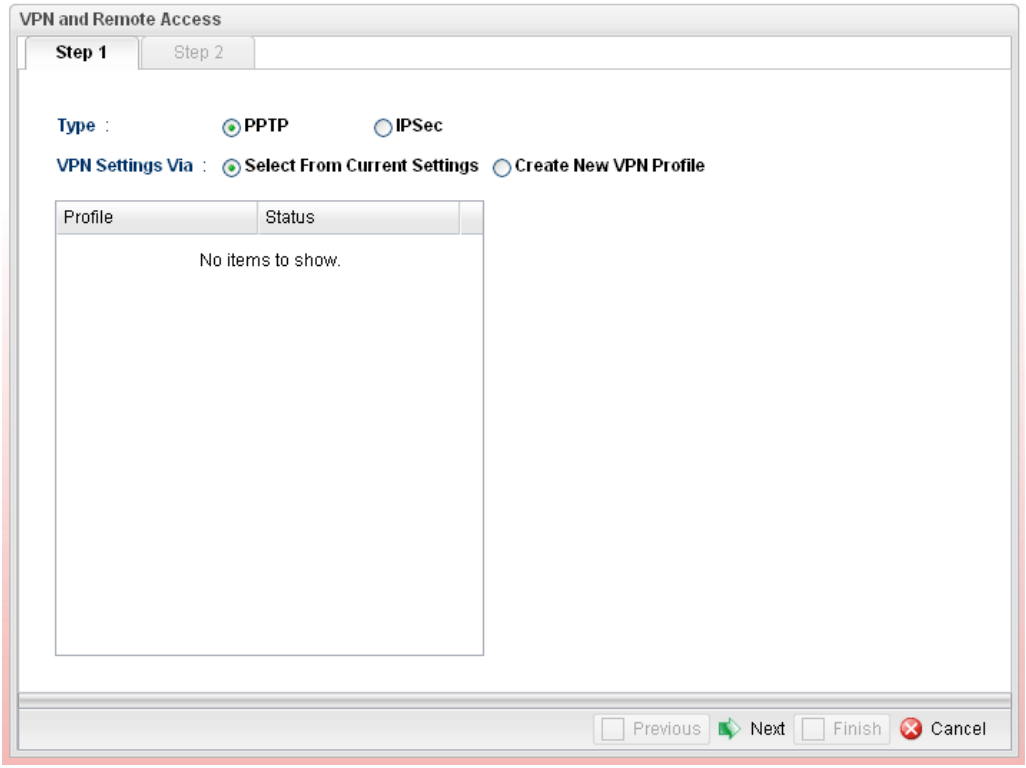
Below shows the menu items for VPN and Remote Access.

4.8.1 VPN Client Wizard

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

How to create LAN-to-LAN profile for VPN client (dial-out)

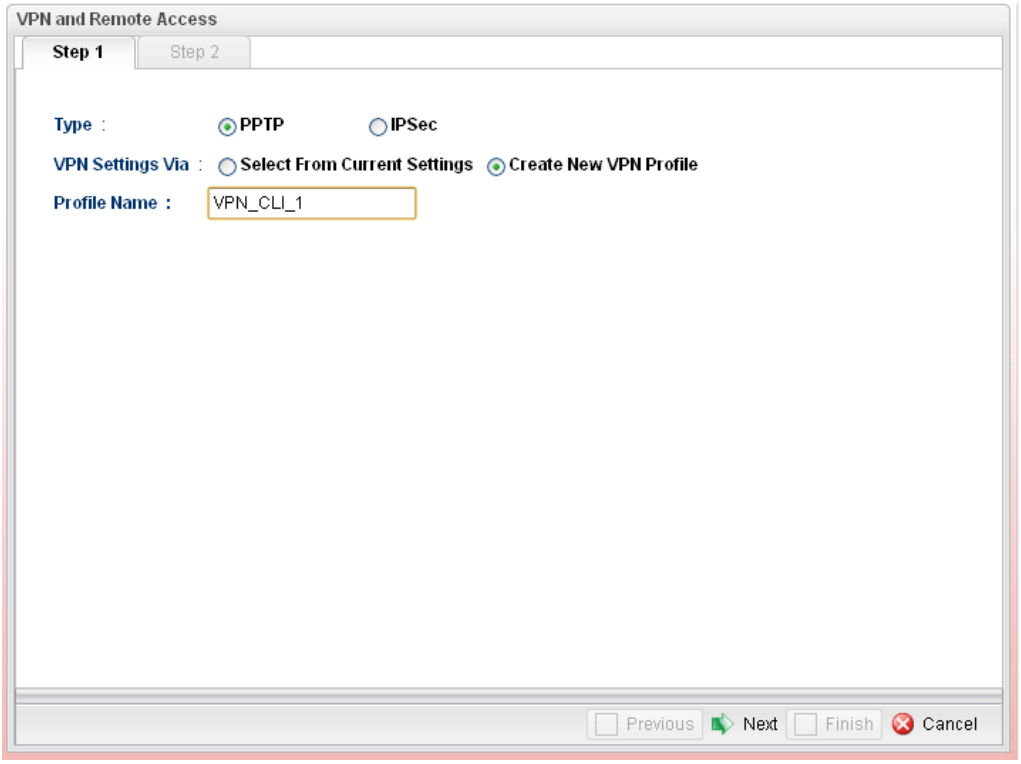
1. Open **VPN and Remote Access >> VPN Client Wizard.**
2. The following dialog will appear.



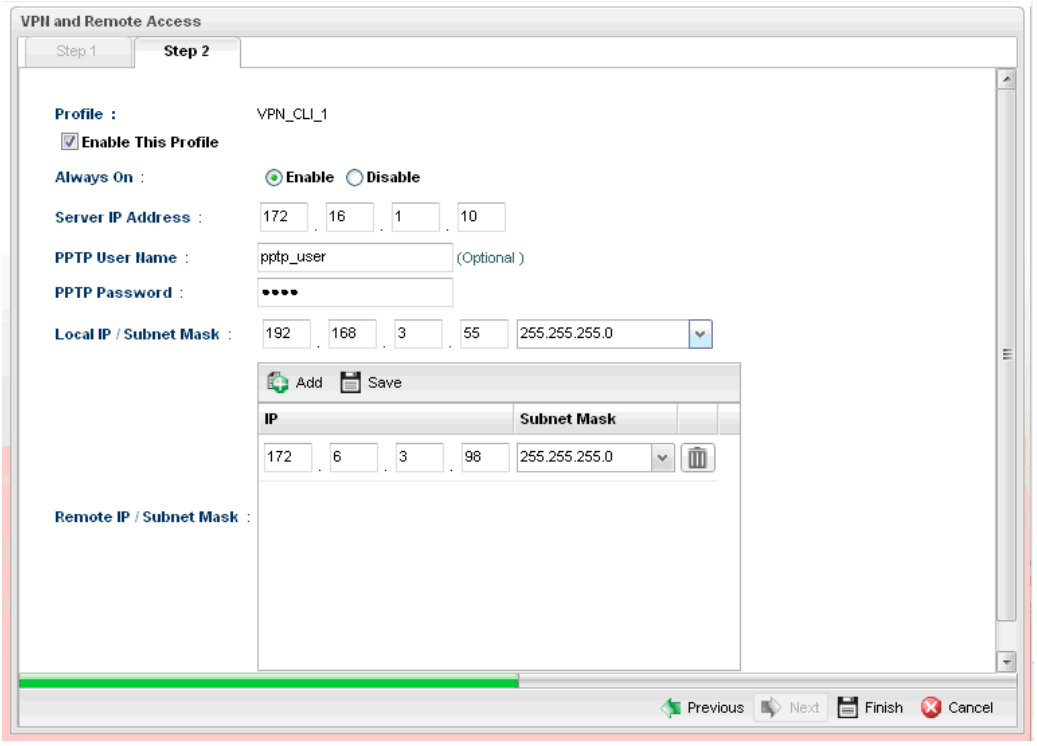
Available parameters are listed as follows:

Item	Description
Type	Specify which protocol (**PPTP** or **IPSec**) will be used for such VPN profile.
VPN Settings Via	**Select From Current Settings** - Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need. **Create New VPN Profile** – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of **Profile Name**. The field of Profile Name is available only when you click this setting.

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



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

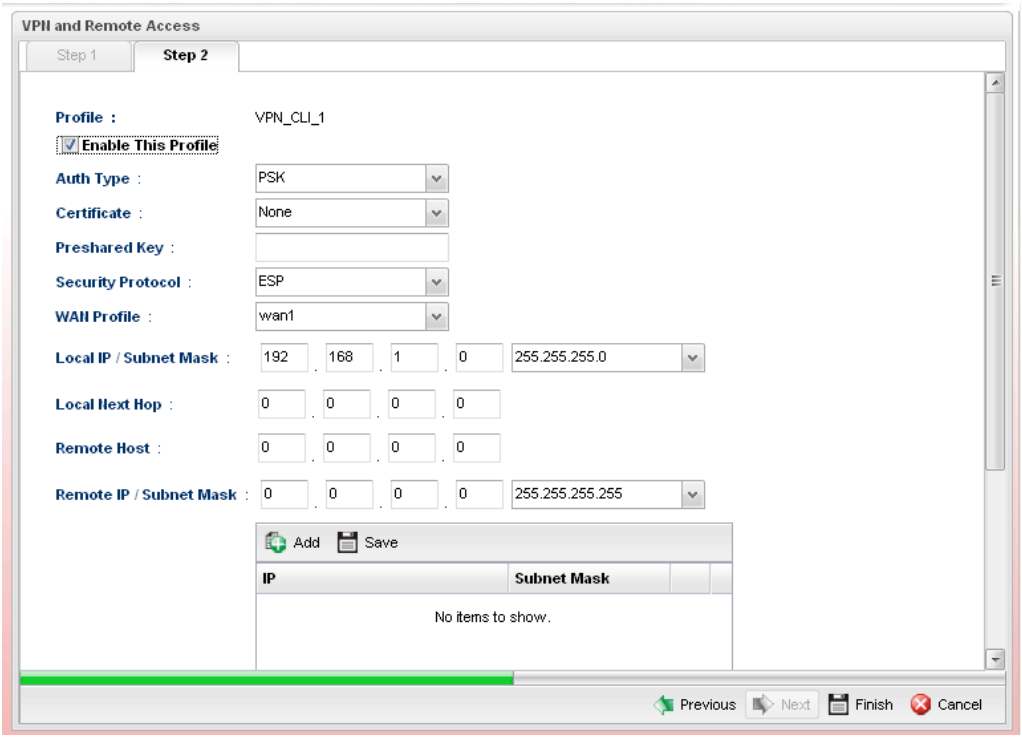


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.

Enable This Profile	Check this box to enable such profile.
Always On	Click Enable to make router always keeping connection.
Server IP Address	Type the IP address of PPTP server.
PPTP User Name	Type a user name for authentication in PPTP connection.
PPTP Password	Type a password for authentication in PPTP connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP/Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Route/NAT Mode	Specify the purpose for such profile.

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

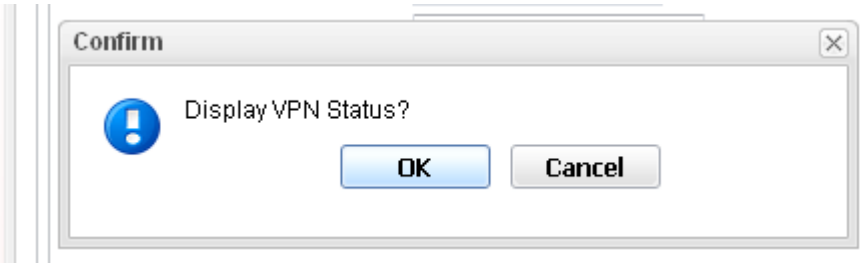


Available parameters are listed as follows:

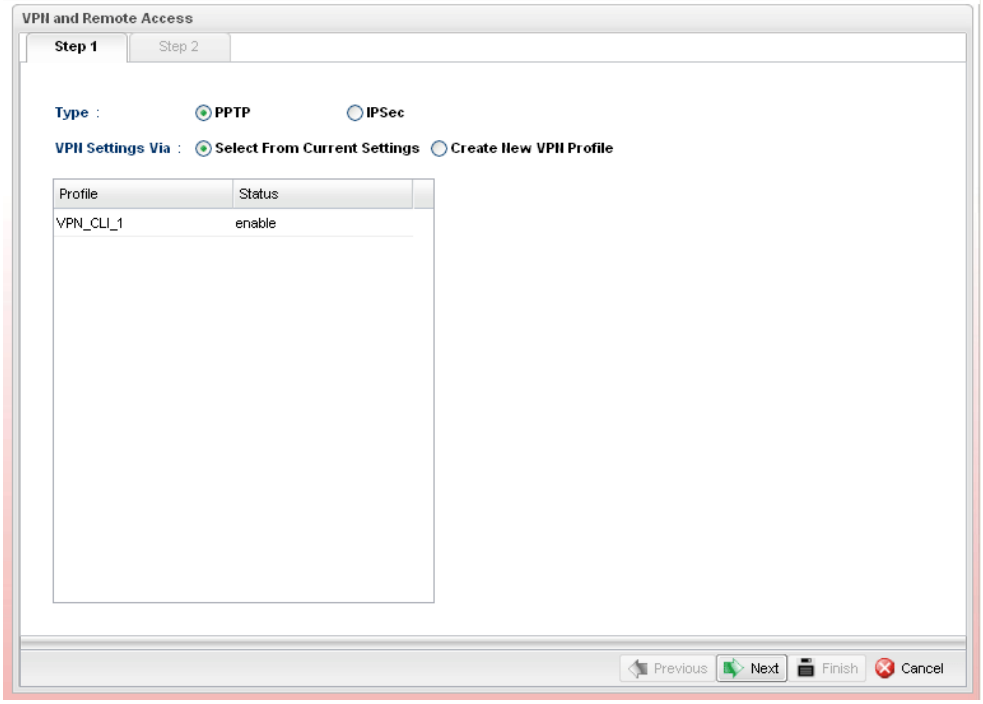
Item	Description
Profile	Display the name of the VPN profile.
Enable This Profile	Check this box to enable such profile.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list.
Preshared Key	Type a pre-shared key for authentication if PSK is selected

	as Auth Type.
Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
WAN Profile	Choose a WAN profile to be used by such profile.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
More Remote Subnet	Add more remote subnet in this field if required.
Local GRE IP	The virtual IP address of the router, specified for this tunnel.
Remote GRE IP	The virtual IP address of the remote client, specified for this tunnel.

5. Fill in the required information on this page and click **Finish**. Later, the system will ask if you want to display the new created VPN file.

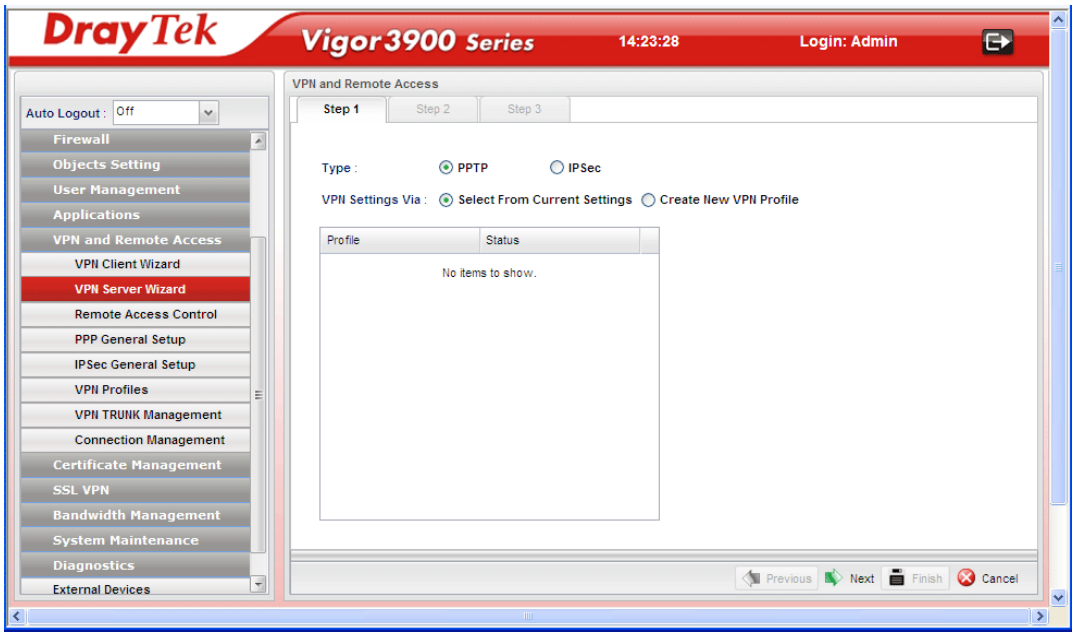


6. Click **OK**. A new profile has been created.



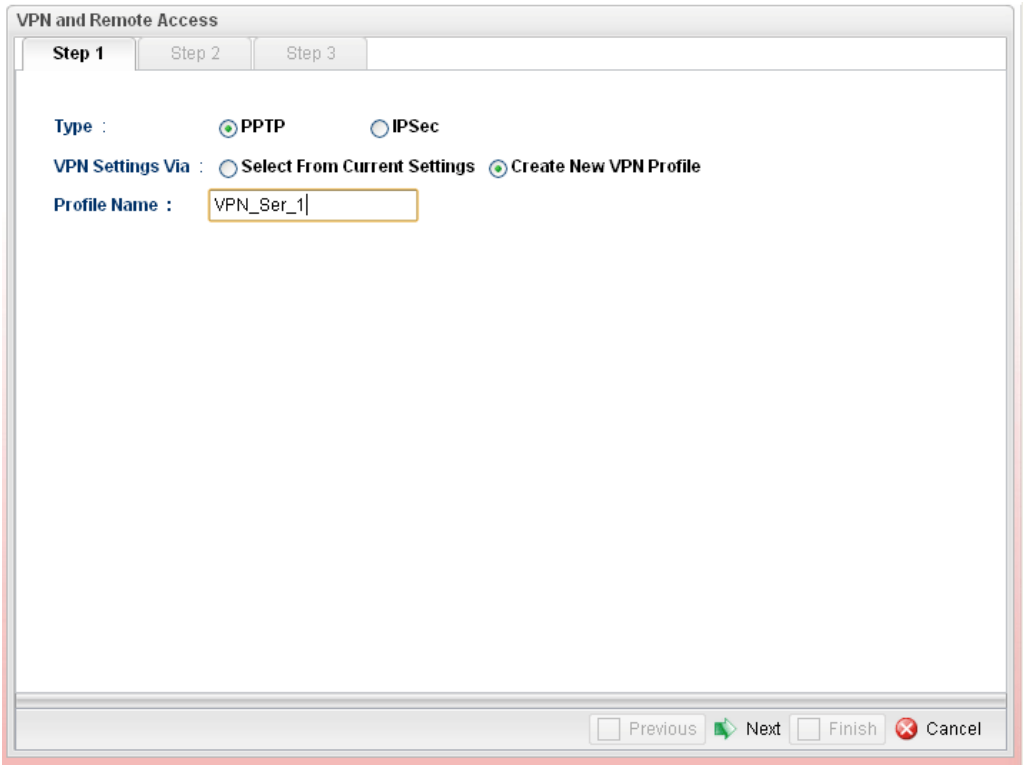
4.8.2 VPN Server Wizard

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



How to create LAN-to-LAN profile for VPN server

1. Open **VPN and Remote Access >> VPN Server Wizard.**
2. The following dialog will appear.

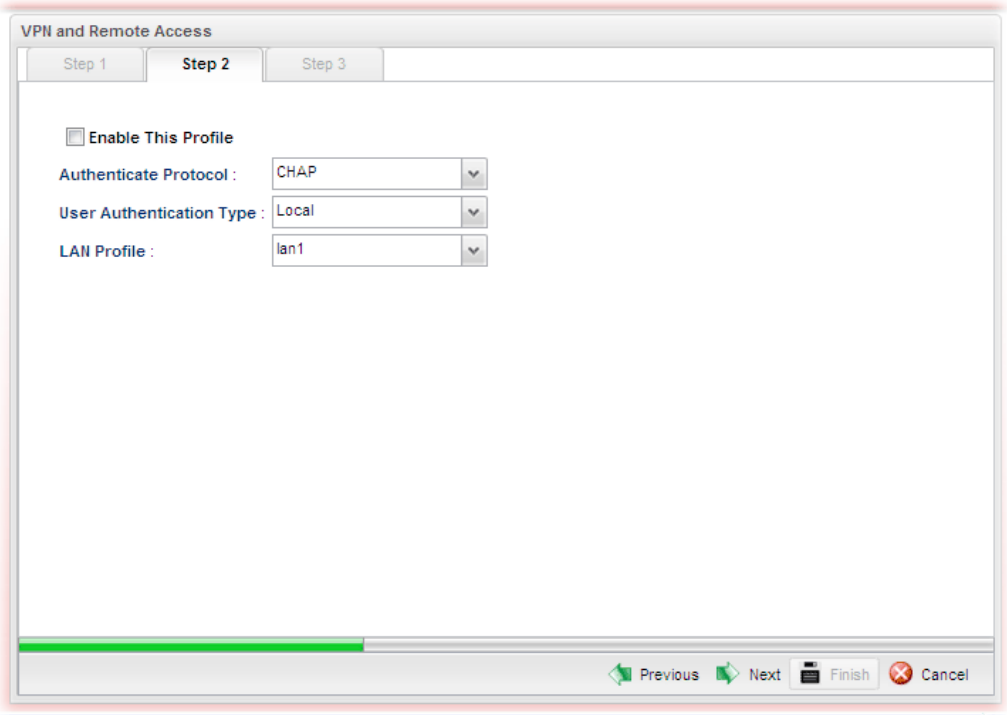


Available parameters are listed as follows:

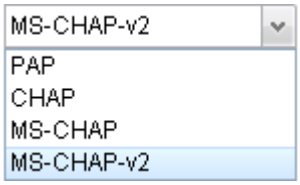
Item	Description

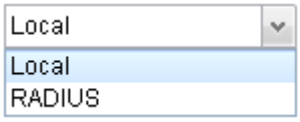
Type	Specify which protocol (**PPTP** or **IPSec**) will be used for such VPN profile.
VPN Settings Via	**Select From Current Settings** - Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need. **Create New VPN Profile** – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of **Profile Name**. The field of Profile Name is available only when you click this setting.
Profile Name	**Type a new name for such profile.**

3. Click **Create New VPN Profile** and type the name of the profile. Click **Next** to get the following page. Note that such page will be skipped if you choose **IPSec** as the **Type** in Step 1.

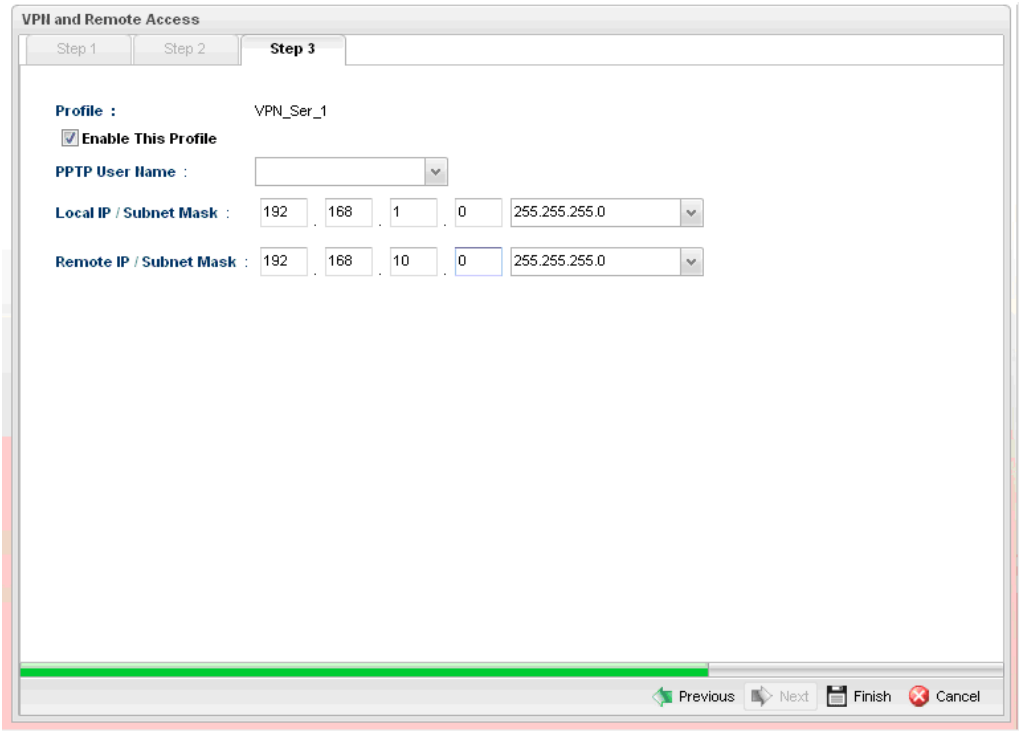


Available parameters are listed as follows:

Item	Description
Enable This Profile	Check this box to enable such profile.
Authentication Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate

	dial-in users with the CHAP protocol.
User Authentication Type	Set user authentication to **Local** server or **RADIUS** server. 
LAN Profile	Choose a LAN profile for PPTP Server if **Local** is selected as user authentication type.

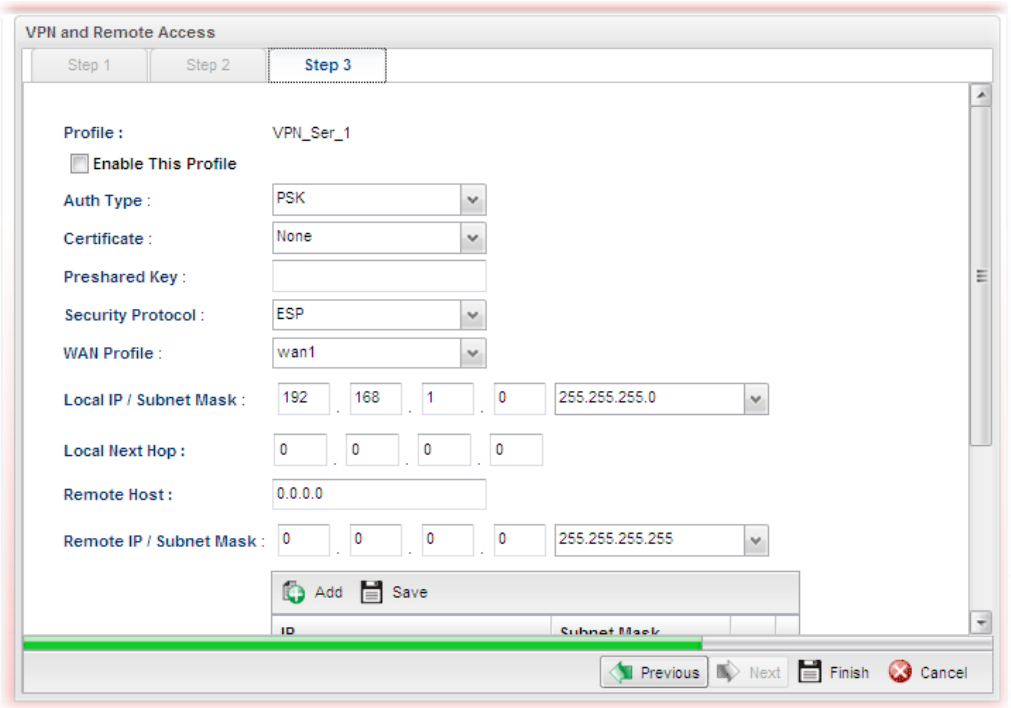
4. Fill in the required information on this page and click **Next** to go to next page.



Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable This Profile	Check this box to enable such profile.
PPTP User Name	Type a user name for authentication in PPTP connection. Such profile shall be created in **User Management>>User Profile** previously. Otherwise, there are no selections displayed here.
Local IP / Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.

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

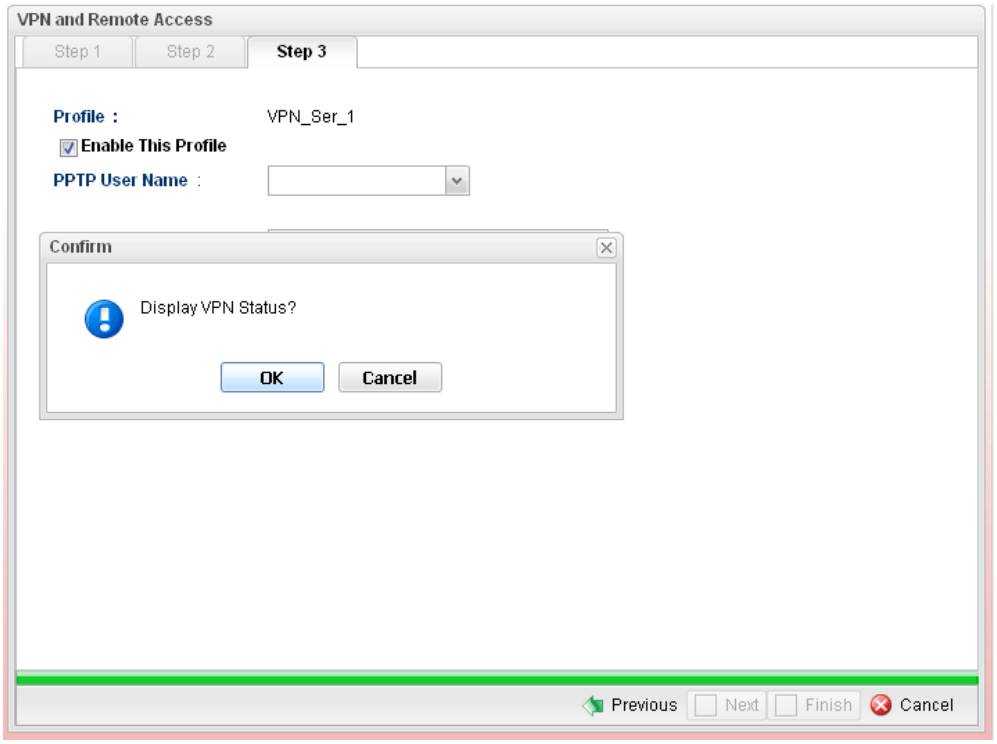


Available parameters are listed as follows:

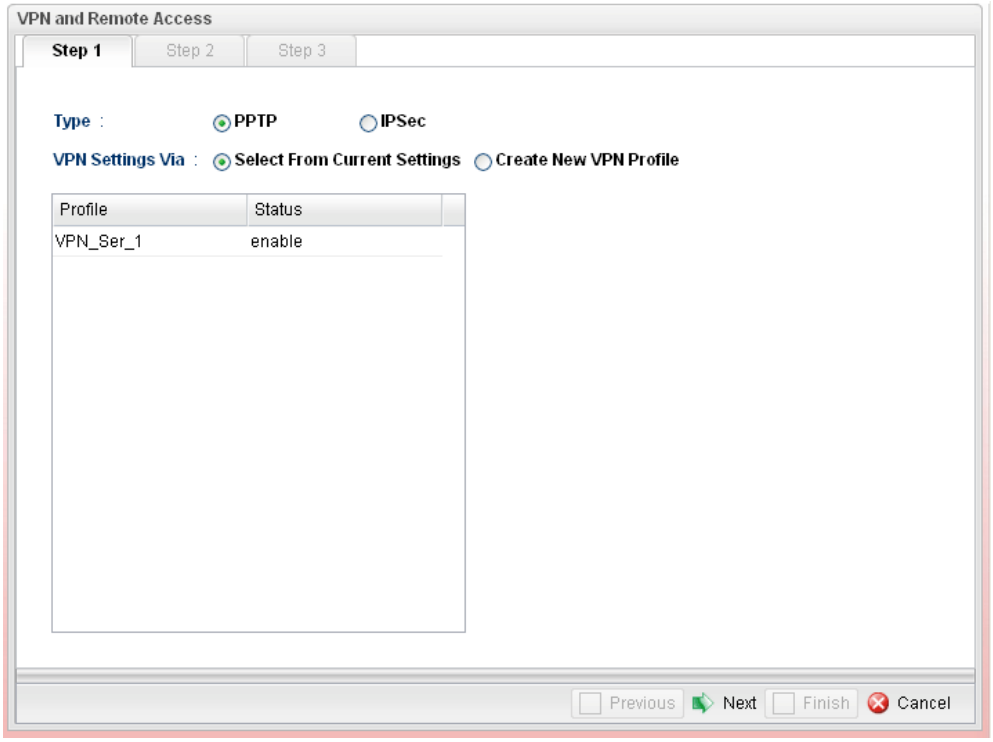
Item	Description
Profile	Display the name of the profile.
Enable This Profile	Check this box to enable such profile.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list.
Preshared Key	Type a pre-shared key for authentication if PSK is selected as Auth Type.
Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
WAN Profile	Choose a WAN profile to be used by such profile.
Local IP / Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Local GRE IP	The virtual IP address of the router, specified for this tunnel.

Remote GRE IP	The virtual IP address of the remote client, specified for this tunnel.

5. Fill in the required information on this page and click **Finish**.



6. After clicking **OK**, the new added VPN server profile will be displayed on the screen.



4.8.3 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service (e.g., PPTP VPN, IPSec VPN, L2TP VPN, SSL VPN, etc.) of Vigor Router to allow VPN tunnel pass through.

4.8.4 PPP General Setup

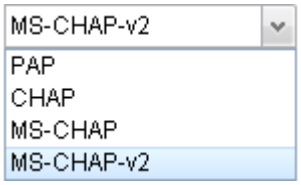
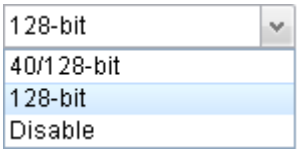
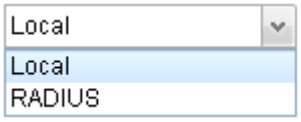
Remote users can connect to the site, host, server and etc. via VPN connection built between the router and the users by authentication procedure.

PPTP

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

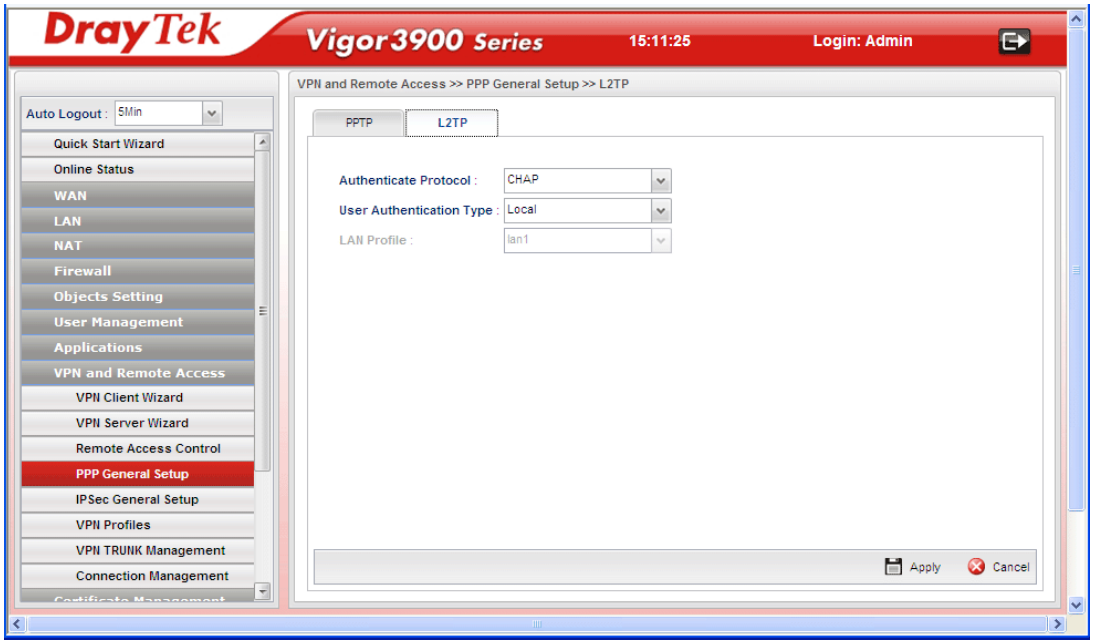
Available parameters are listed as follows:

Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol

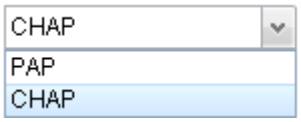
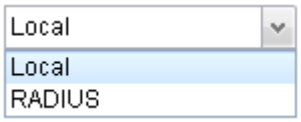
	selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
MPPE Encryption	Specify one of the encryptions for such server. It is available only when MS-CHAP or MS-CHAP_v2 is selected. 
User Authentication Type	Set user authentication to **Local** server or **RADIUS** server. 
LAN Profile	Choose a LAN profile for PPTP Server if **Local** is selected as user authentication type.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

L2TP

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



Available parameters are listed as follows:

Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP** - It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP** - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
User Authentication Type	Set user authentication to **Local** server or **RADIUS** server. 
LAN Profile	Choose a LAN profile for L2TP Server if **Local** is selected as user authentication type.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

4.8.5 IPSec General Setup

The IPSec services can provide access control, connectionless integrity, data origin authentication, rejection of replayed packets that is a form of partial sequence integrity, and confidentiality by encryption. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

Available parameters are listed as follows:

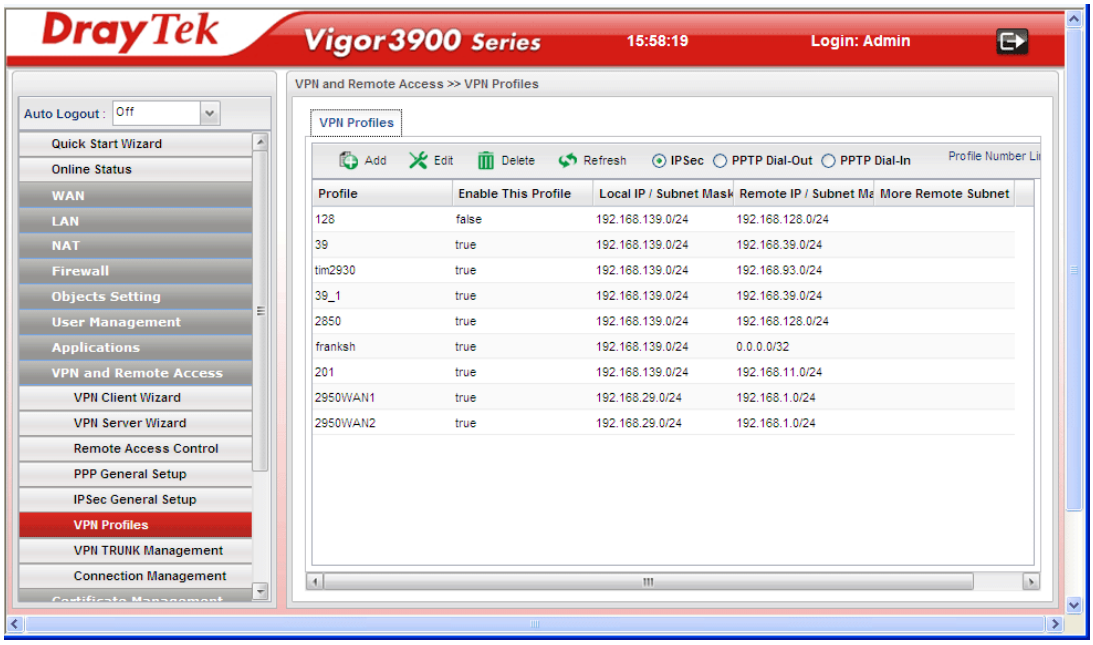
Item	Description

Preshared Key	Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key.
WAN Profile	Choose a WAN interface profile to be used.
DHCP LAN Profile	Choose one of the LAN profiles for VPN.
IKE Port	Type the UDP port number for Internet Key Exchange (IKE) traffic to the VPN server.
NAT-Port	Type the UDP port number for IPSec network address translator traversal (NAT-T) traffic.
IPSec MSS	Type the port number for IPSec MSS.
GRE over IPSec MSS	Type the port number for GRE over IPSec MSS.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.6 VPN Profiles

The router allows you to create VPN profiles via the protocol of IPSec or PPTP (dial-in or dial-out).

The router supports up to **500** VPN tunnels simultaneously. The following figure shows the summary table.



Each item will be explained as follows:

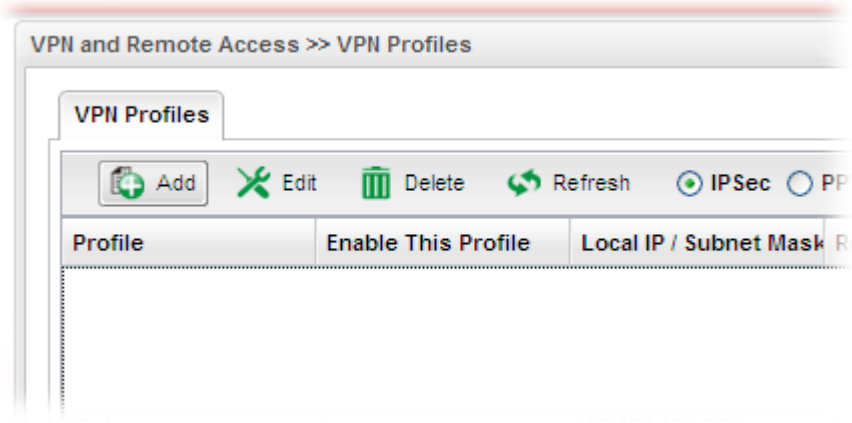
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected

	profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
IPSec	Display the LAN to LAN profile with IPSec policy.
PPTP Dial-out	Display the LAN to LAN profile with PPTP Dial-out policy.
PPTP Dial-in	Display the LAN to LAN profile with PPTP Dial-in policy.
Profile	Display the name of LAN to LAN profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Local IP / Subnet Mask	Display the LAN IP address with subnet mask of this profile.
Remote IP / Subnet Mask	Display the WAN IP address with subnet mask of this profile.
More Remote Subnet	Display other LAN IP addresses with subnet mask which can be used of this profile.

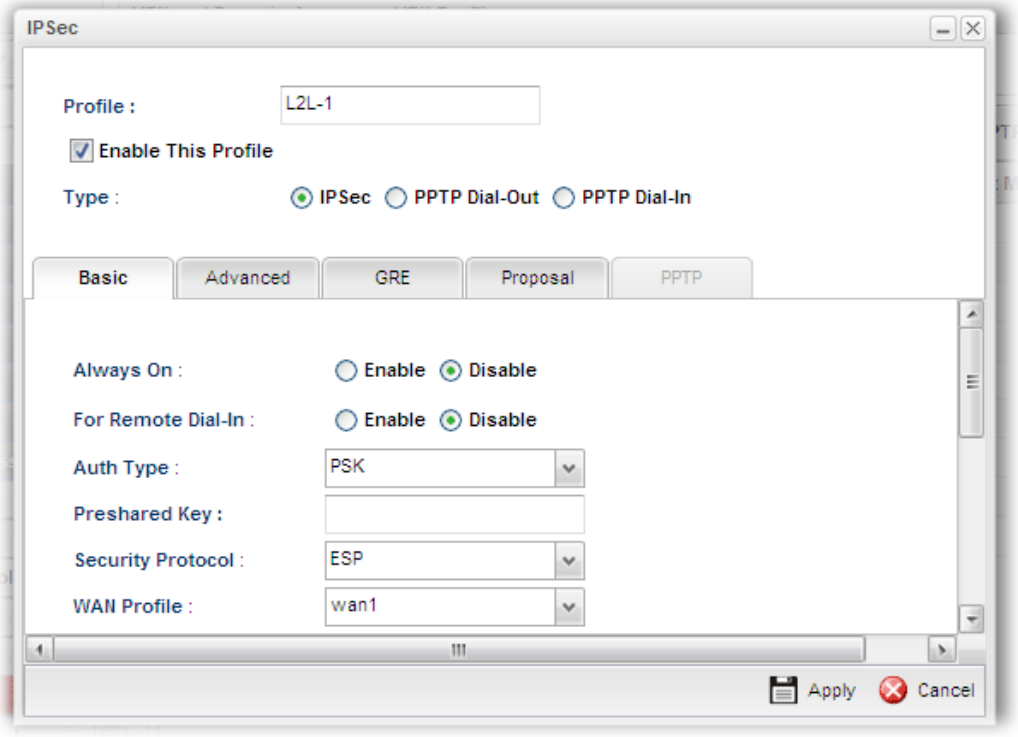
How to create an IPSec VPN profile

The IPSec services can provide access control, connectionless integrity, data origin authentication, rejection of replayed packets that is a form of partial sequence integrity, and confidentiality by encryption. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

1. Open **VPN and Remote Access >> LAN to LAN.**
2. Simply click the **Add** button.



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

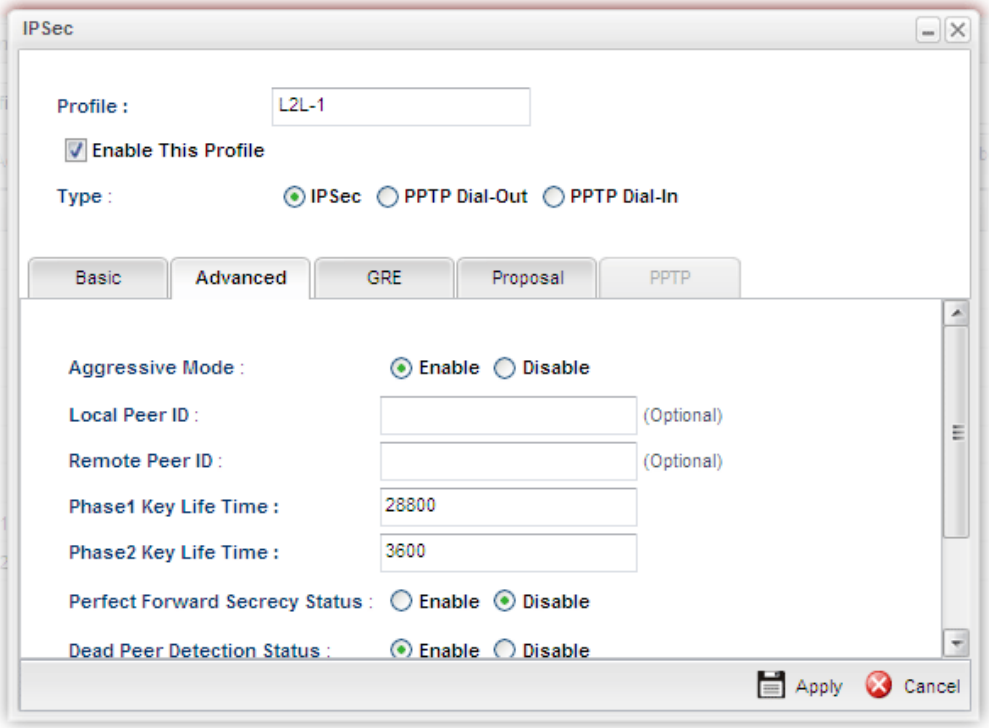


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **IPSec** for this case.
Basic	**Always On** – Click **Enable** to make router always keeping connection. **For Remote Dial-In** - Click **Enable** to allow the connection via IPSec remote dial-in host. **Auth Type -** The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile. **Preshared Key -** Type a pre-shared key for authentication if PSK is selected as Auth Type. **Security Protocol –** Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted. **WAN Profile-** Choose a wan profile to be used by such profile. **Local IP/Subnet Mask -** Type the IP address and subnet mask of local host. **Local Next Hop -** Specify the gateway for WAN interface.

	Usually, use the default setting (leave it in blank). **Remote Host -** Type the WAN IP address for the remote host. **Remote IP / Subnet Mask -** Type the LAN IP address and LAN subnet mask for the remote host. **More Remote Subnet** – Add more remote subnet in this field if required.

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

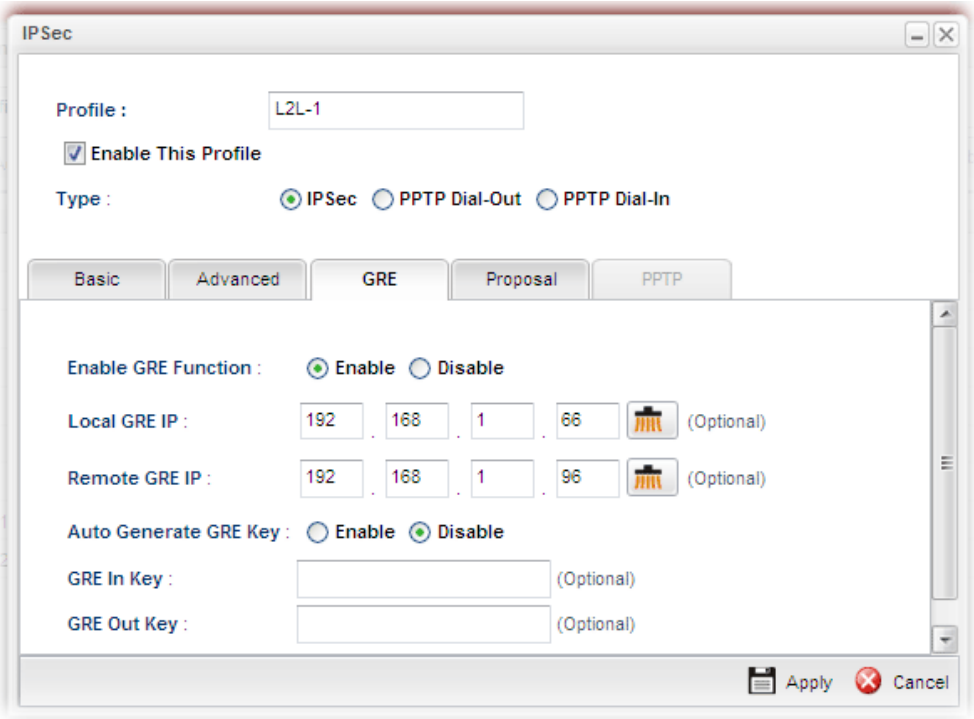


Available parameters are listed as follows:

Item	Description
Aggressive Mode	**Enable** – Click it to enable Aggressive Mode. **Disable** – Click it to disable Aggressive Mode.
Local Peer ID	Type the ID for Vigor3900 which can be configured by the remote end.
Remote Peer ID	Peer ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.
Phase 1 Key Life Time	The rekey-renegotiated period of the IKE Phase1 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).
Phase 2 Key Life Time	The rekey-renegotiated period of the IKE Phase 2 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).

Perfect Forward Secrecy Status	Enables the PFS function. A new Diffie-Hellman Key Exchange is included every time an encryption and/or authentication key are computed on PFS.
Dead Peer Detection Status	**Enable** – Click it to enable DPD. When there is no traffic through the IPSec tunnel, both server and the client will send the DPD packet to each other to ensure the IPSec tunnel connection is active still. **Disable** – Click it to disable DPD.
DPD Delay	The keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	The timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

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

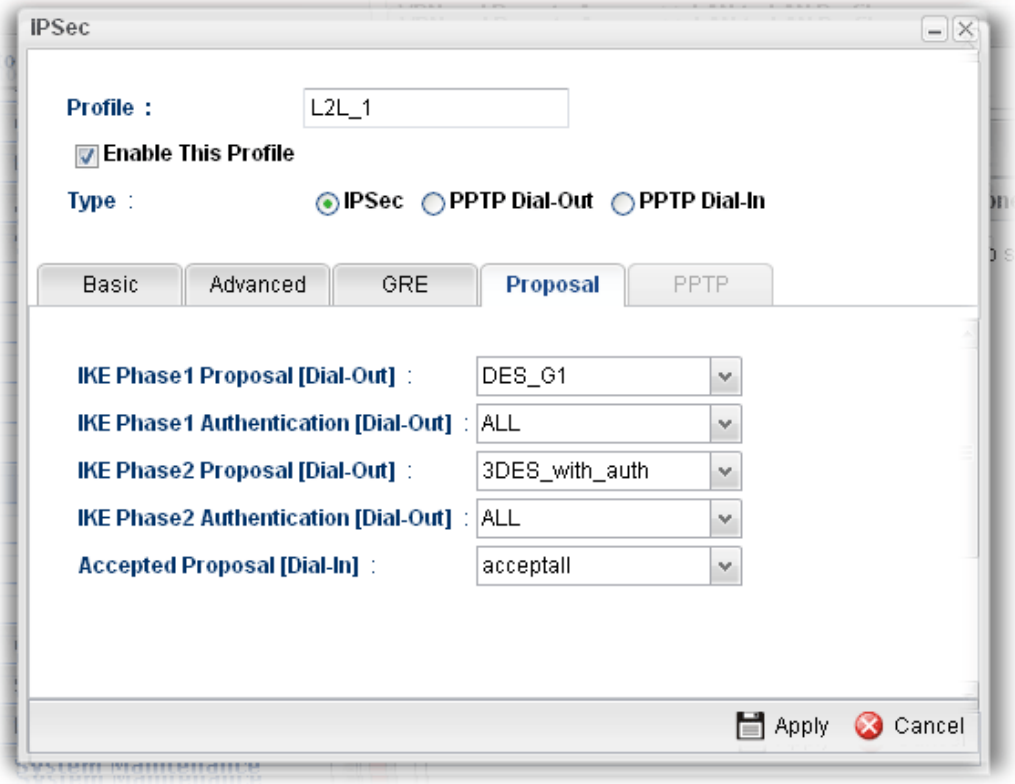


Available parameters are listed as follows:

Item	Description
Enable GRE Function	Check the box to enable the function.
Local GRE IP	The virtual IP address of the router, specified for this tunnel.
Remote GRE IP	The virtual IP address of the remote client, specified for this tunnel.
Auto Generate	Click **Enable** to generate the GRE key by the system

GRE Key	automatically. If you click **Disable**, you need to type GRE key manually.
GRE In Key	Type the hexadecimal number as GRE In Key. This value is used for the router to authenticate the source of the packet. The length is 4 bytes
GRE Out Key	Type the hexadecimal number as GRE Out Key. This value is used for the remote client to authenticate the source of the packet. The length is 4 bytes.

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



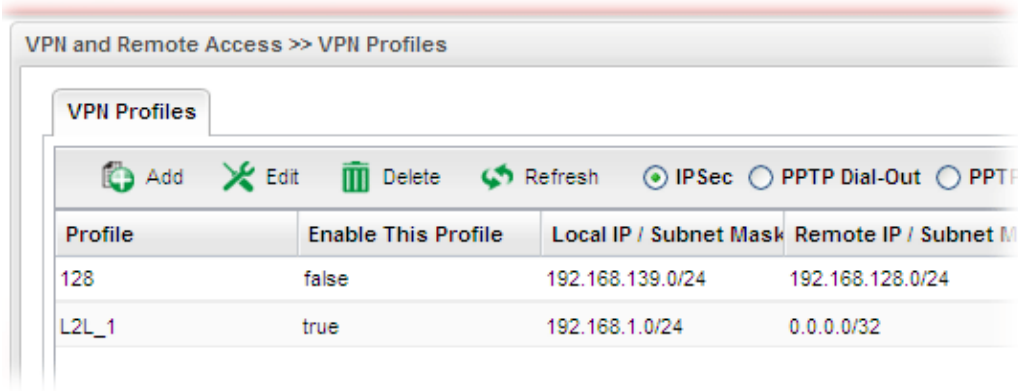
Available parameters are listed as follows:

Item	Description
IKE Phase1 Proposal (Dial-Out)	Propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase1 Authentication (Dial-Out)	Propose the local available algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase2 Proposal (Dial-Out)	Propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match.
IKE Phase2 Authentication (Dial-Out)	Propose the local available algorithms to the VPN peers, and get its feedback to find a match.

Accepted Proposal (Dial-In)	For the dial-in VPN user, please specify the limitation of the proposal. **Accept all supported proposal (acceptall)** - When the VPN tunnel is established, all the proposals supported by this device will be accepted and applied. **Only accept proposal listed above (acceptabove)** - When the VPN tunnel is established, only the selected proposal will be accepted and applied by this device.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving configuration.

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

8. A new IPSec LAN-to-LAN profile has been created.

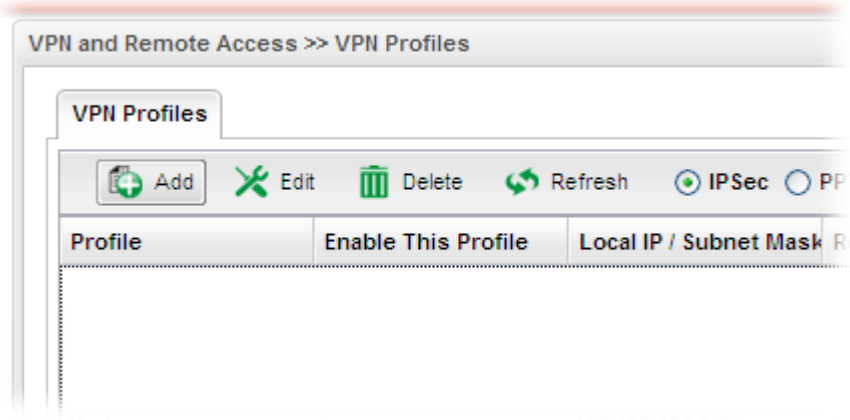


How to create a PPTP Dial-Out LAN to LAN profile

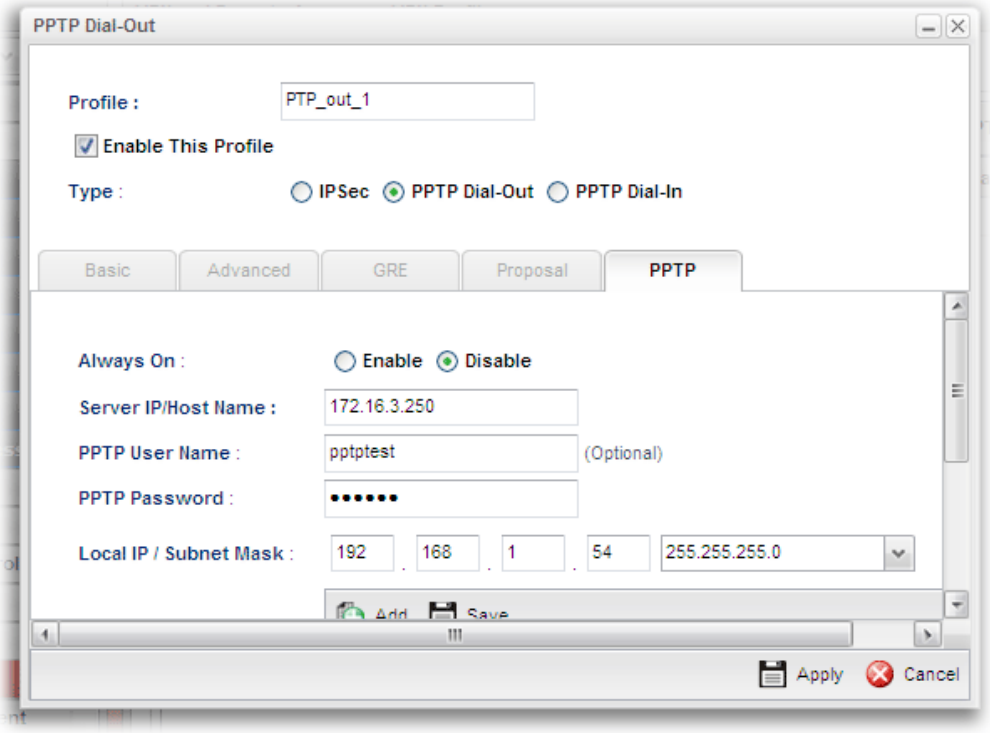
Below will guide you to create a PPTP dial-out profile for VPN connection:

1. Open **VPN and Remote Access >> VPN Profiles.**

2. Simply click the **Add** button.



3. The following dialog will appear.

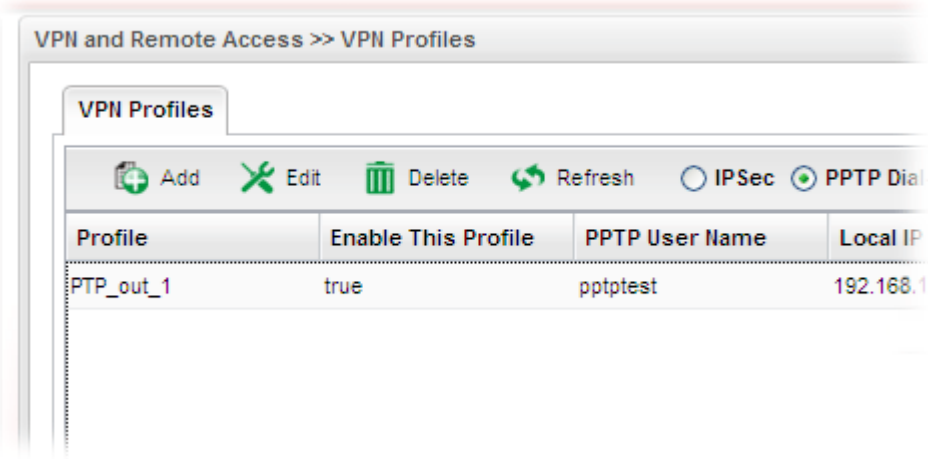


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **PPTP Dial-Out** for this case.
PPTP	**Always On -** Click **Enable** to make the profile being always on. **Server IP/Host Name -** Type the IP address or the host name of PPTP server. **PPTP User Name -** Type a user name for authentication in PPTP connection. **PPTP Password -** Type a password for authentication in PPTP connection. **Local IP/Subnet Mask -** Type the IP address and subnet mask of local host. **Remote IP / Subnet Mask -** Type the LAN IP address and LAN subnet mask for the remote host. **Route / NAT Mode -** Specify the purpose for such profile.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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

5. A new PPTP Dial-Out profile has been created.

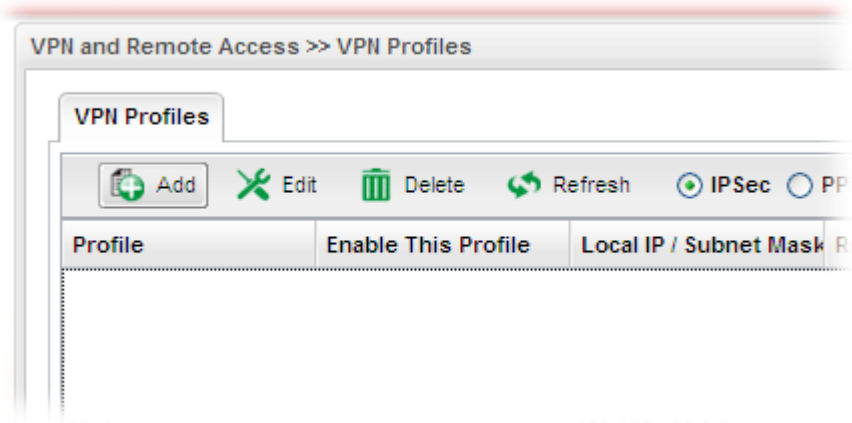


How to create a PPTP Dial-In LAN to LAN profile

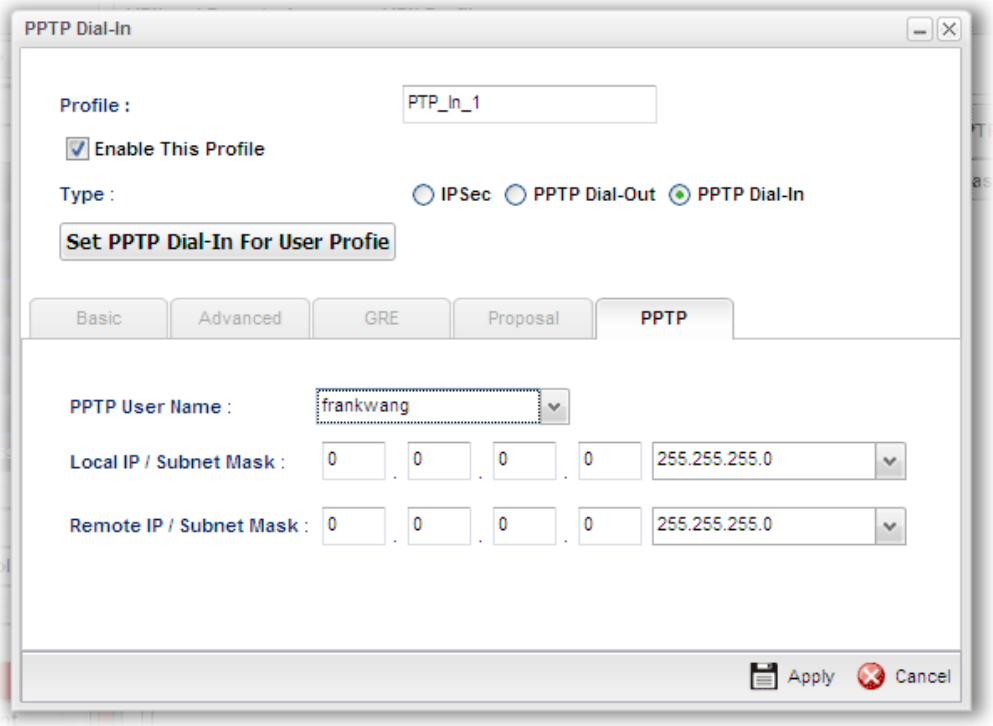
Below will guide you to create a PPTP dial-in profile for VPN connection:

1. Open **VPN and Remote Access >>VPN Profiles.**

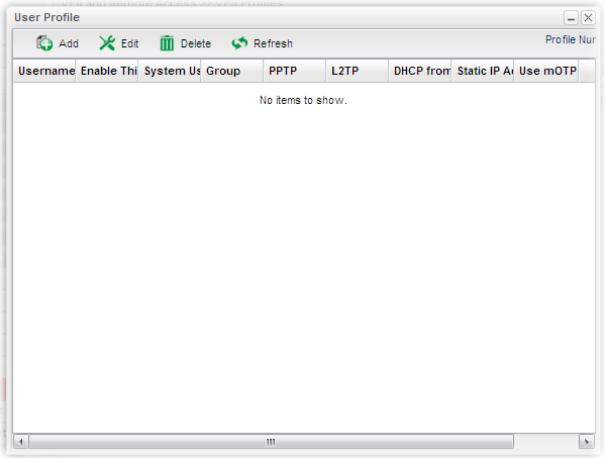
2. Simply click the **Add** button.



3. The following dialog will appear.

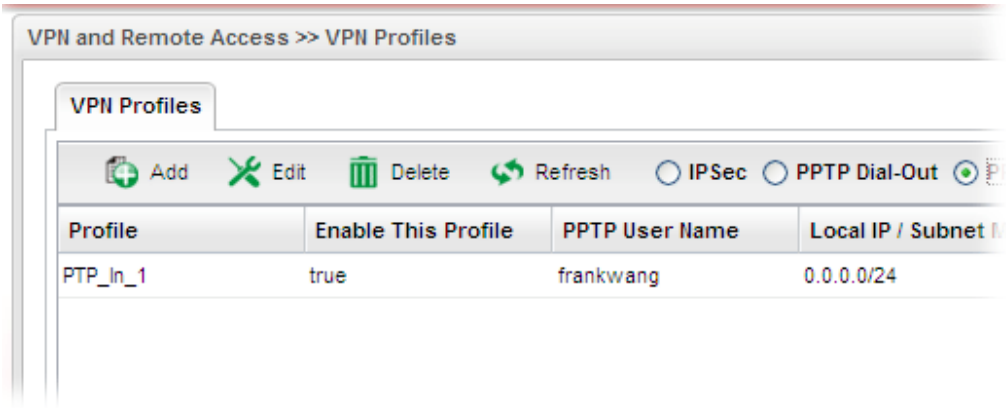


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable This Profile	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **PPTP Dial-In** for this case.
Set PPTP Dial-In For User Profile	Click it to create a new user profile or to modify an existing profile.  See the explanation later.
PPTP User Name	Choose a PPTP user profile for authentication in PPTP connection. Such profile shall be created in **User Management>>User**

	Profile previously. Otherwise, there are no selections displayed here.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

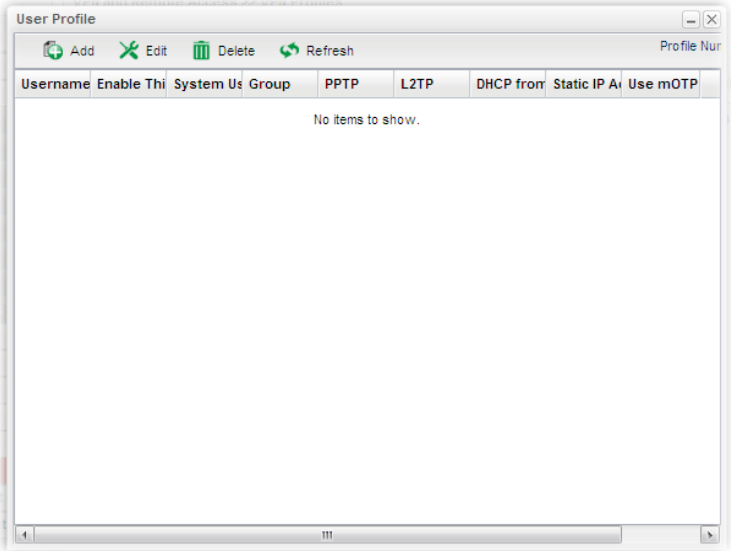
4. Enter all the settings and click **Apply**.
5. A new PPTP Dial-In profile has been created.



Set PPTP Dial-In For User Profile

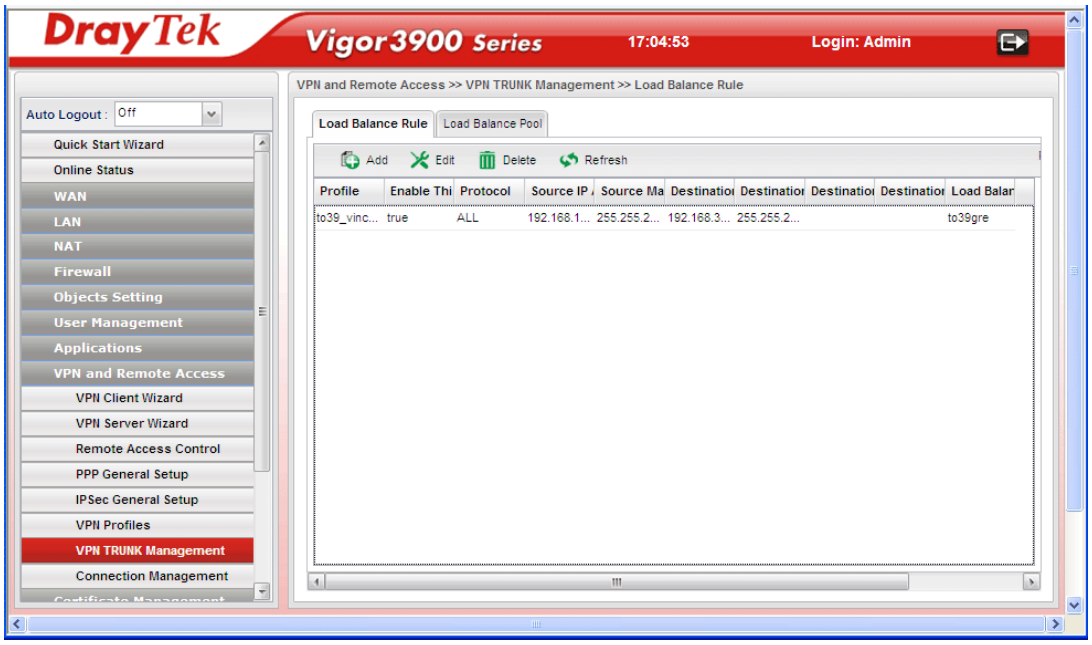
To set PPTP Dial-In connection, you have to create PPTP user profiles previously in **User Management>>User Profile**, or click **Set PPTP Dial-In For User Profile** in this page to configure a new one for choosing for authentication in PPTP connection.

Below shows the window of **Set PPTP Dial-In For User Profile.** For the configuration and detailed information, simply refer to **4.6.2 User Profile.**



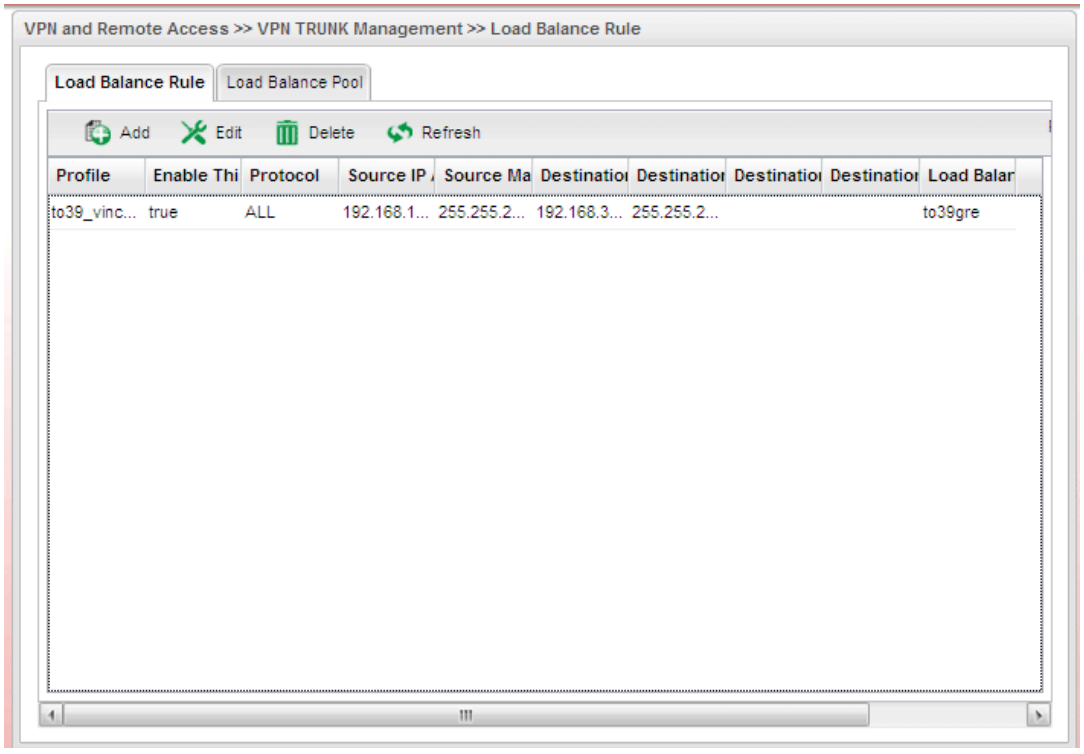
4.8.7 VPN Trunk Management

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



Load Balance Rule

To build VPN load balance connection with other router, you can define the load balance rule in this page.

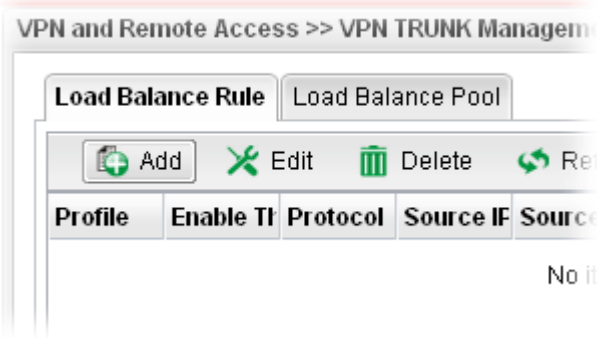


Each item will be explained as follows:

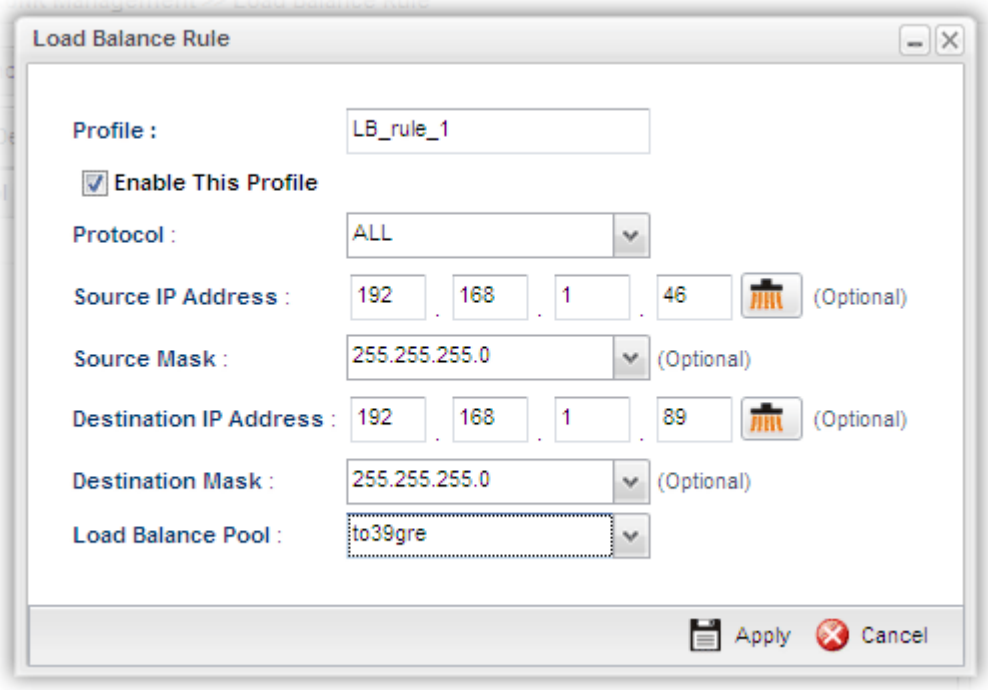
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Protocol	Display the protocol configured by such profile.
Source IP Address	Display the source IP address specified for this profile.
Source Mask	Display the subnet mask address specified for the source IP of this entry.
Destination IP Address	Display the destination IP address specified for this entry.
Destination Mask	Display the subnet mask address specified for the destination IP of this entry.
Destination Port Start	Display the start point specified in the **Dest Port Range** for this entry.
Destination Port End	Display the end point specified in the **Dest Port Range** for this entry.
Load Balance Pool	Display the selection of load balance pool.

How to add a Load Balance Rule profile

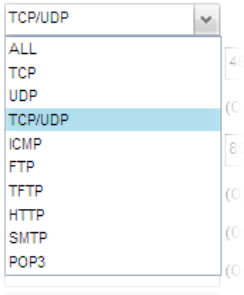
1. Open **VPN and Remote Access >>VPN TRUNK Management** and click the **Load Balance Rule** tab.
2. Simply click the **Add** button.



3. The following dialog will appear.



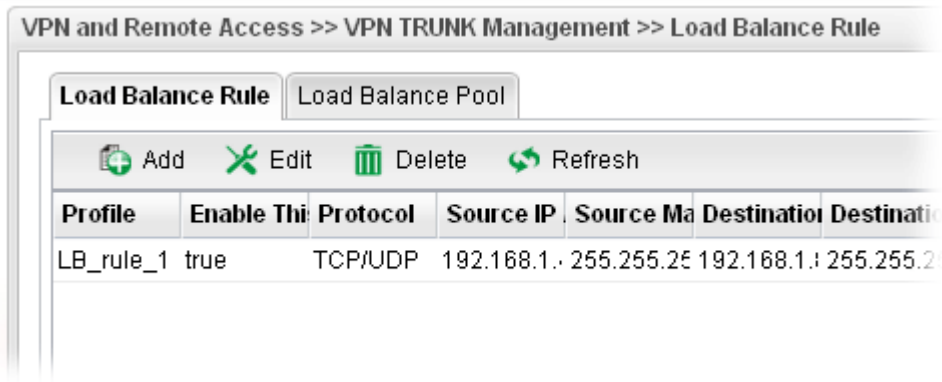
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable such profile.
Protocol	Choose the protocol for such profile. 
Source IP Address	Type the source IP address specified for this profile.
Source Mask	Type the subnet mask address specified for the source IP.
Destination IP Address	Type the destination IP address specified for this entry.
Destination Mask	Type the subnet mask address specified for the destination IP.
Destination Port Start	Type the start point.
Destination Port End	Type the end point.

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

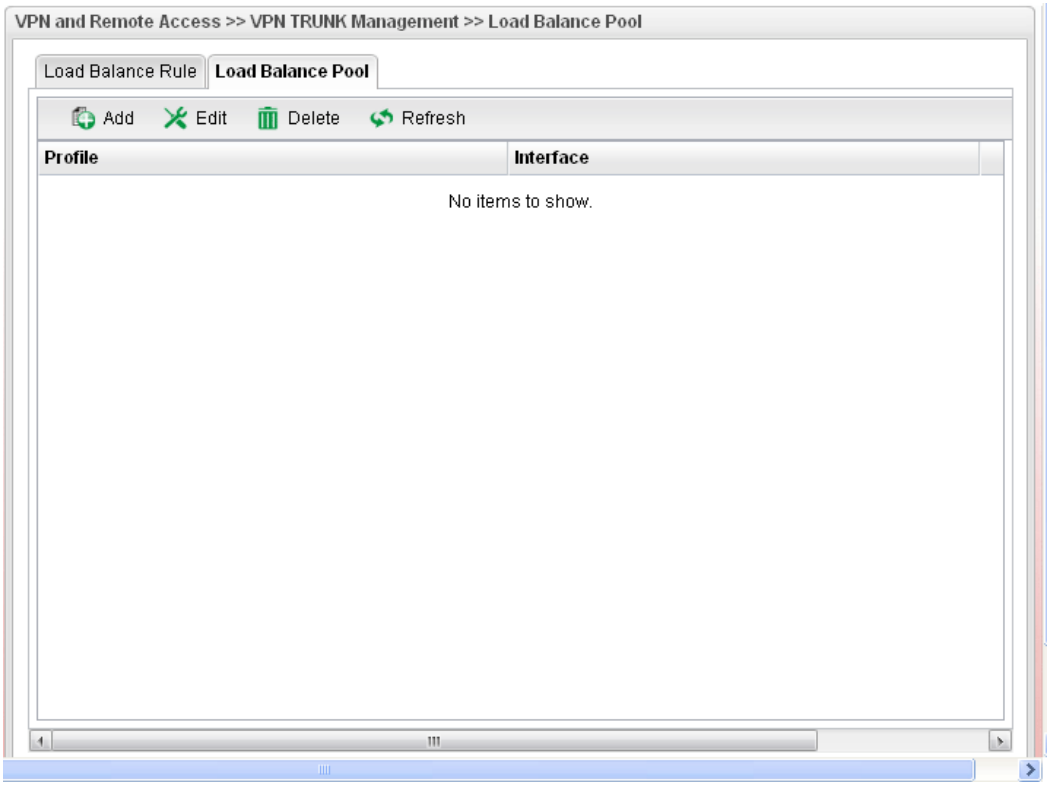
4. Enter all the settings and click **Apply**.

5. A new profile has been created.



Load Balance Pool

This page allows the user to integrate **several** VPN IPSec profiles as a pool profile for VPN Load Balance.



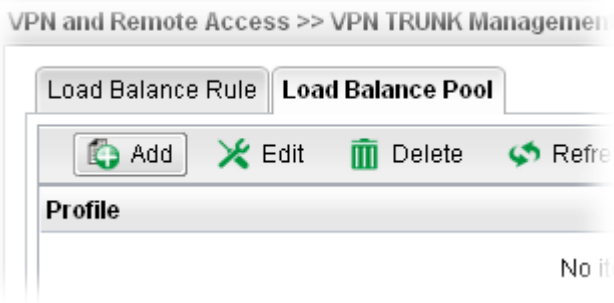
Each item will be explained as follows:

Item	Description

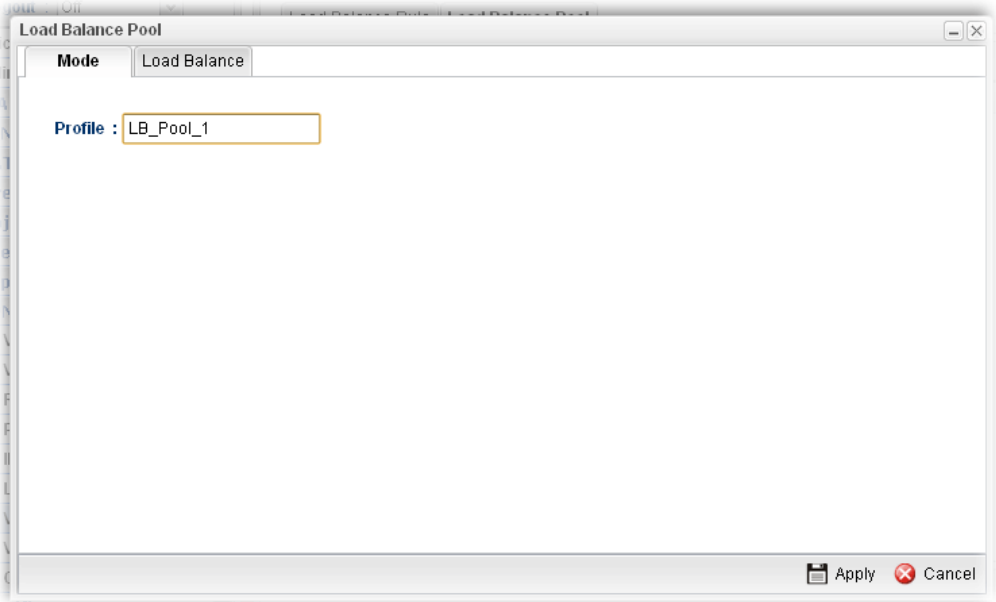
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Interface	Display the name of the Load Balance profile grouped under such pool profile.

How to add a Load Balance Pool Profile

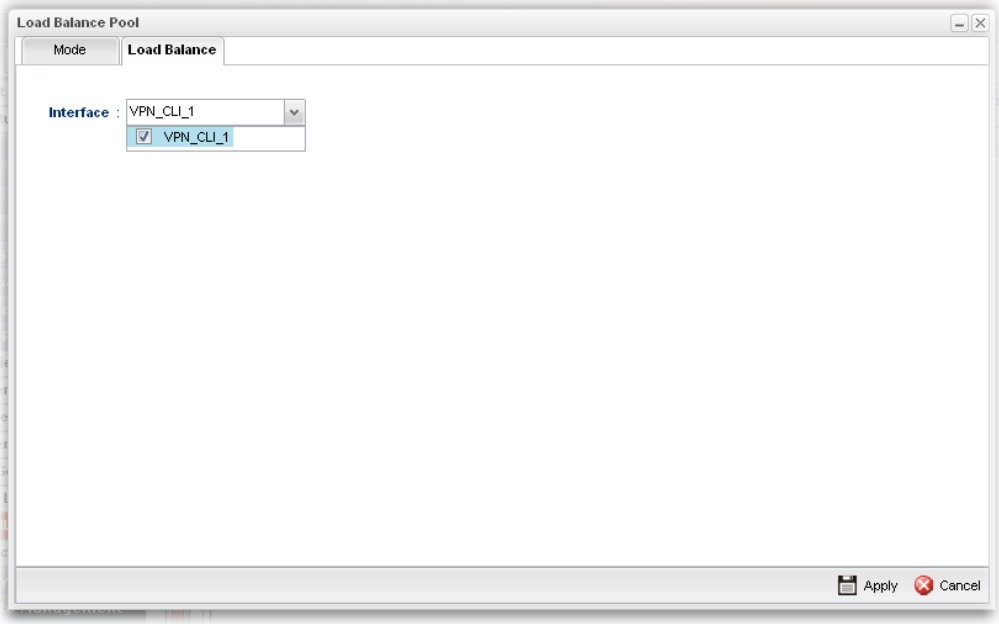
1. Open **VPN and Remote Access >>VPN TRUNK Management** and click the **Load Balance Pool** tab.
2. Simply click the **Add** button.



3. The following dialog will appear. Type the name of the profile (e.g., LB_Pool_1, within 10 characters including digit, letter, and underline) under the **Mode** tab.

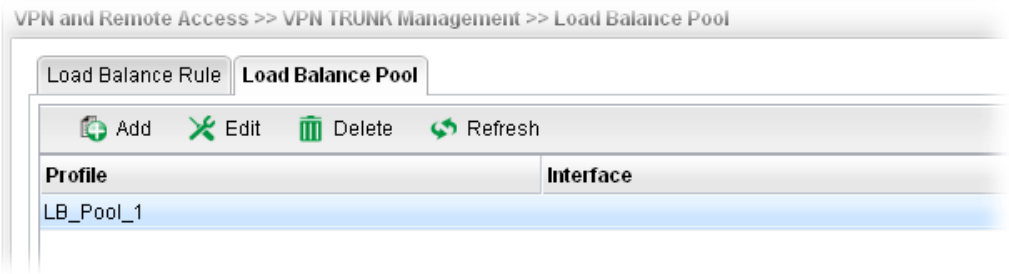


4. Click the **Load Balance** tab to open the following dialog.



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

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



Refer to Chapter 3, *How to Configure VPN Load Balance between Vigor3900 and Other Router* for getting more detailed information about Load Balance application.

4.8.8 Connection Management

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

Each item will be explained as follows:

Item	Description
Profile	This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.
Connect	Click this button to execute dial out function.
IPSec	Click it to perform IPSec VPN connection.
PPTP	Click it to perform PPTP VPN connection.
Refresh	Renew current web page.
Index	Display the item number of the VPN profile.
VPN	Display the name of VPN profile.
Type	Display the connection type (PPTP or IPSec) for such VPN profile.
Remote IP	Display the remote IP configure by VPN profile.
Virtual Network	Display the virtual network established by such VPN profile.
Up Time	Display the connection time of this VPN tunnel.
RX (Packets)	Display the total received packets through this VPN.
TX (Packets)	Display the total transmitted packets through this VPN.
Disconnect	Terminate the VPN connection.

4.9 Certificate Management

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

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

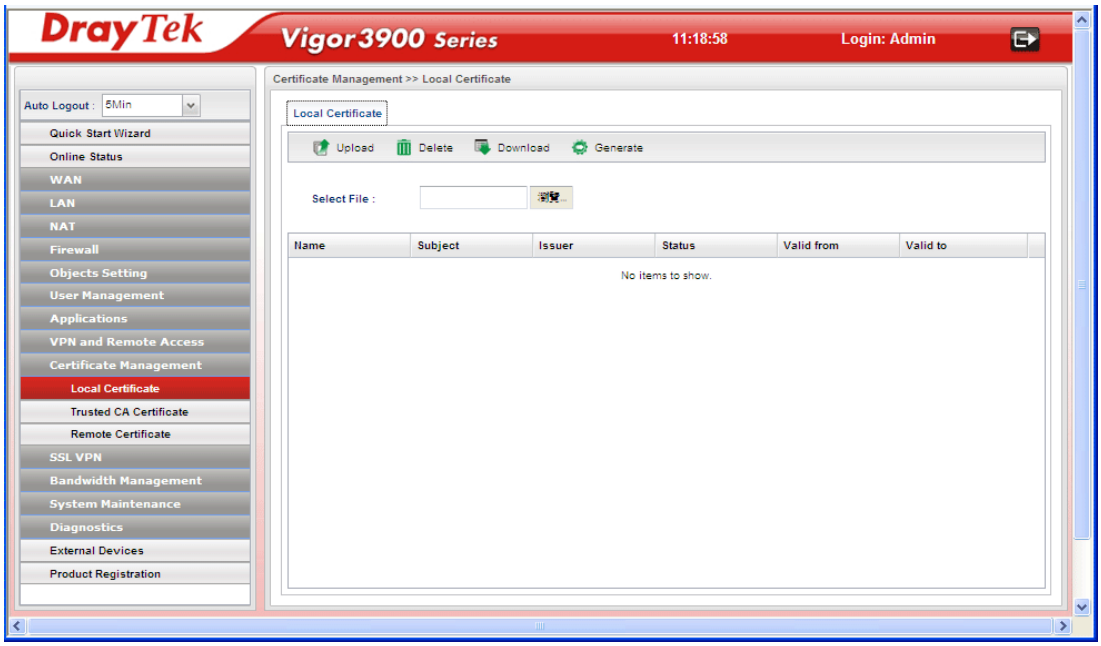
Below shows the menu items for Certificate Management.

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

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

4.9.1 Local Certificate

This page allows users to generate certificate based on different work requests. Local certificate can be signed by itself or signed by a root CA (e.g., root CA on Vigor3900).

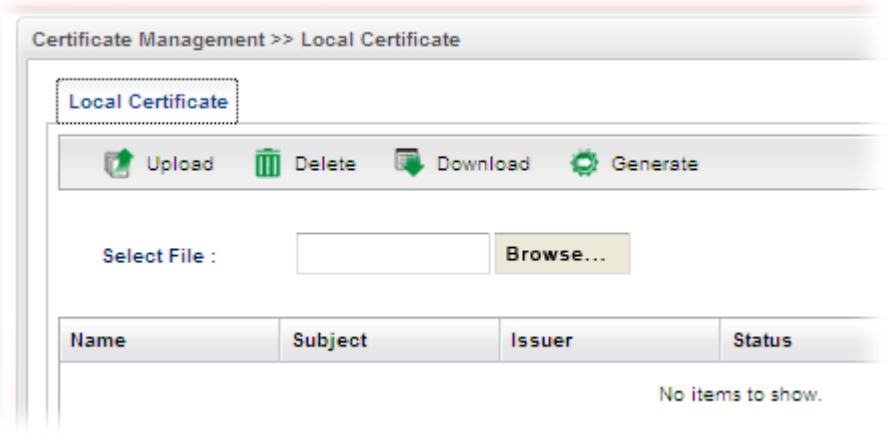


Each item will be explained as follows:

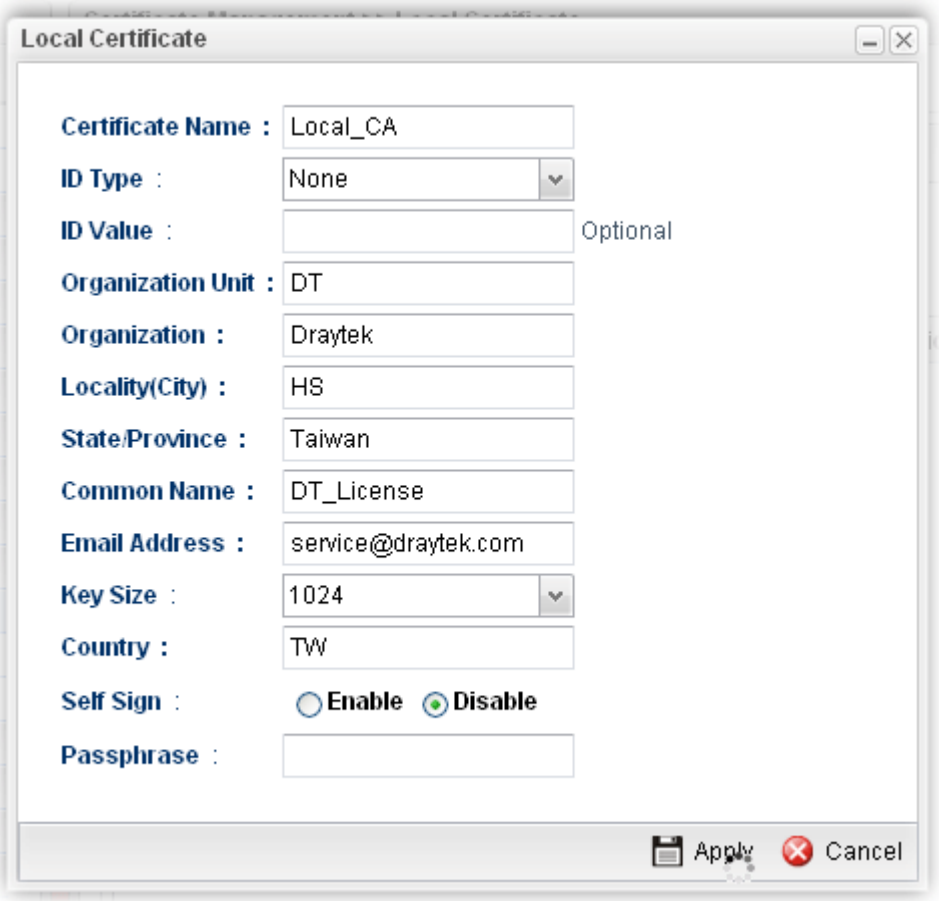
Item	Description
Upload	Allow you to upload current configuration to the host as a CA certificate.
Delete	Remove the selected item of Trusted CA listed below.
Download	Allow you to download an existing CA certificate to the router.
Generate	Open another web page for generating the local certificate.
Select File	Use the **Browse..** button to specify a file to be used as trusted CA certificate.
Name	Display the name of trusted CA built.
Subject	Display the subject of the trusted CA built.
Issuer	Display the issuer of the trusted CA built.
Status	Display the status of the trusted CA built.
Valid From	Display the starting point of the valid time of trusted CA.
Valid To	Display the end point of the valid time of trusted CA.

How to build a local certificate

1. Open **Certificate Management>> Local Certificate.**
2. Simply click the **Generate** button.

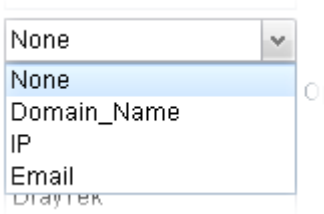


3. The following dialog will appear.

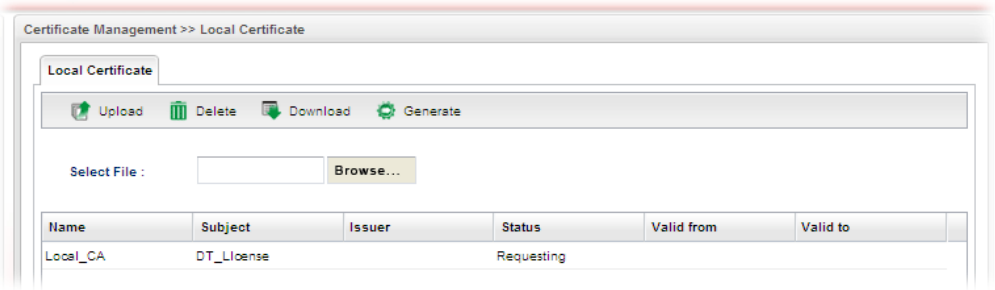


Available parameters are listed as follows:

Item	Description
Certificate Name	Type the name of the local certificate.
ID Type	The ID type for such certificate. There are four types:

	Domain Name: Certificated by domain name. **IP**: Certificated by IP address. **Email**: Certificated by email address. **None**: Do not enter an ID value. 
ID Value	The ID value is determined by the **ID Type** selected for such certificate. For example, if you choose **Domain_Name** as the ID Type, please type the domain name in this field.
Organization Unit	Type a description for the organization unit.
Organization	Type the name of the organization.
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state /province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
Key Size	Choose one of the key sizes for such certificate.
Country	Type the name of the country that such certificate located.
Self Sign	Click **Enable** to enable the self sign function. If the certificated has been signed by it self, it can not be approved or signed by other Root CA server any more. Click **Disable** to disable the self sign function. A certificate without self sign can be approved or signed by a Root CA server, e.g., Vigor3900.
Passphase	Such string will be used for confirmation while signing remote CA. It is similar to a password but generally it is longer for security.
Apply	Click it to create a new local certificate based on the configuration here.
Cancel	Click it to exit the web page without saving the configuration.

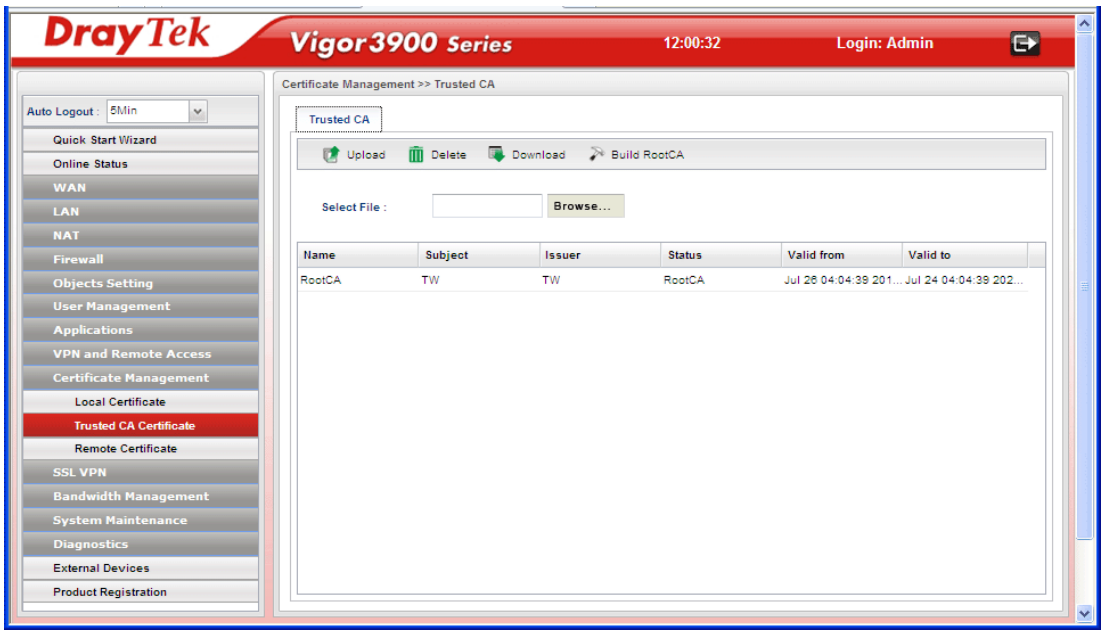
4. Enter all the settings and click **Apply**.
5. A new generated Local Certificate has been created.



4.9.2 Trusted Certificate

This page allows you to build a RootCA certificate for Vigor3900.

RootCA can be deleted but not edited. If you want to modify the settings for a RootCA, please delete the one and create another one by clicking **Build RootCA**.



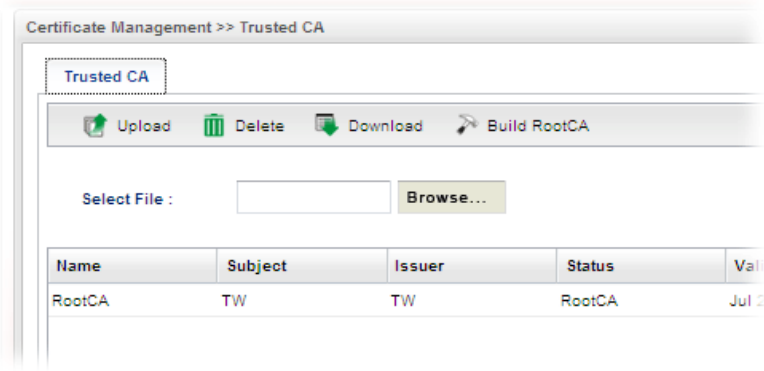
Each item will be explained as follows:

Item	Description
Upload	Allow you to upload current configuration to the host as a CA certificate.
Delete	Remove the selected item of trusted CA listed below.
Download	Allow you to download an existing trusted CA certificate to the router.
Build RootCA	Allow to create a new CA certificate as Root CA.
Select File	Use the **Browse..** button to specify a file to be used as trusted CA certificate.
Name	Display the name of trusted certificate built.
Subject	Display the subject of trusted certificate built.
Issuer	Display the issuer of trusted certificate built.
Status	Display the status of trusted certificate built.

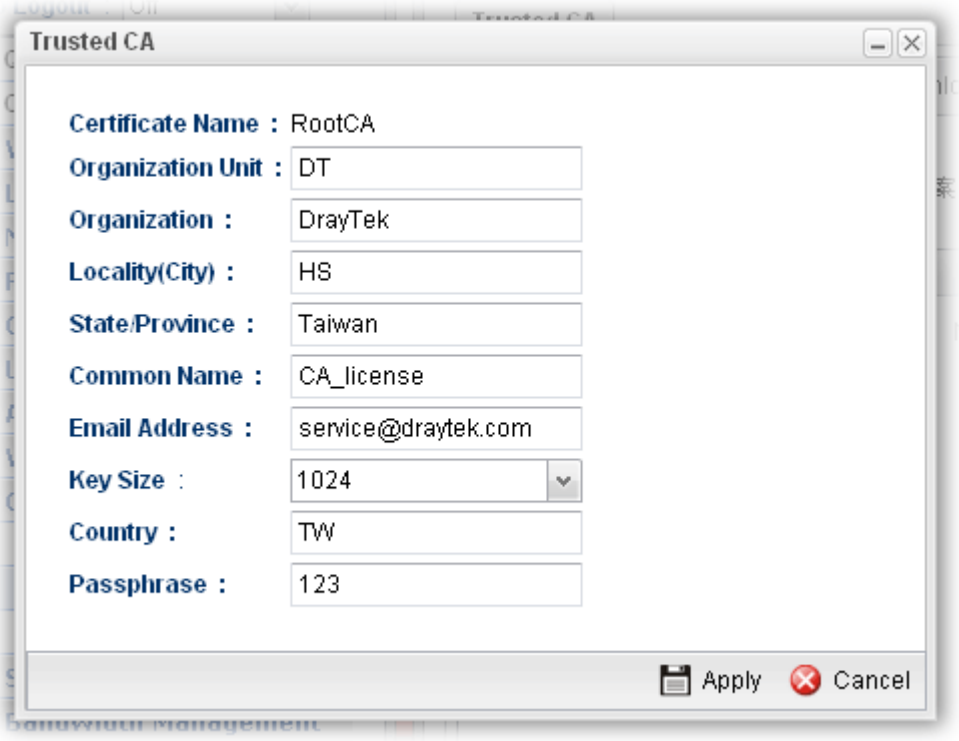
Valid From	Display the starting point of the valid time of trusted certificate.
Valid To	Display the end point of the valid time of trusted certificate.

How to build a trusted CA certificate

1. Open **Certificate Management>>Trusted CA Certificate.**
2. Simply click the **Build RootCA** button.



3. The following dialog will appear.

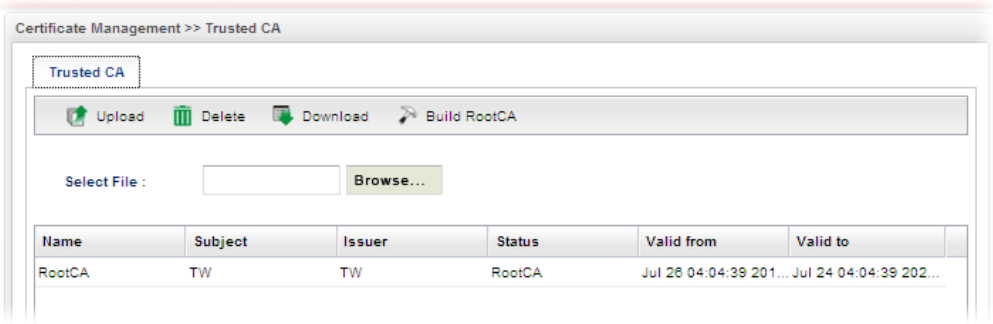


Available parameters are listed as follows:

Item	Description
Certificate Name	Display the name of the trusted CA certificate.
Organization Unit	Type a description for the organization unit.
Organization	Type the name of the organization.

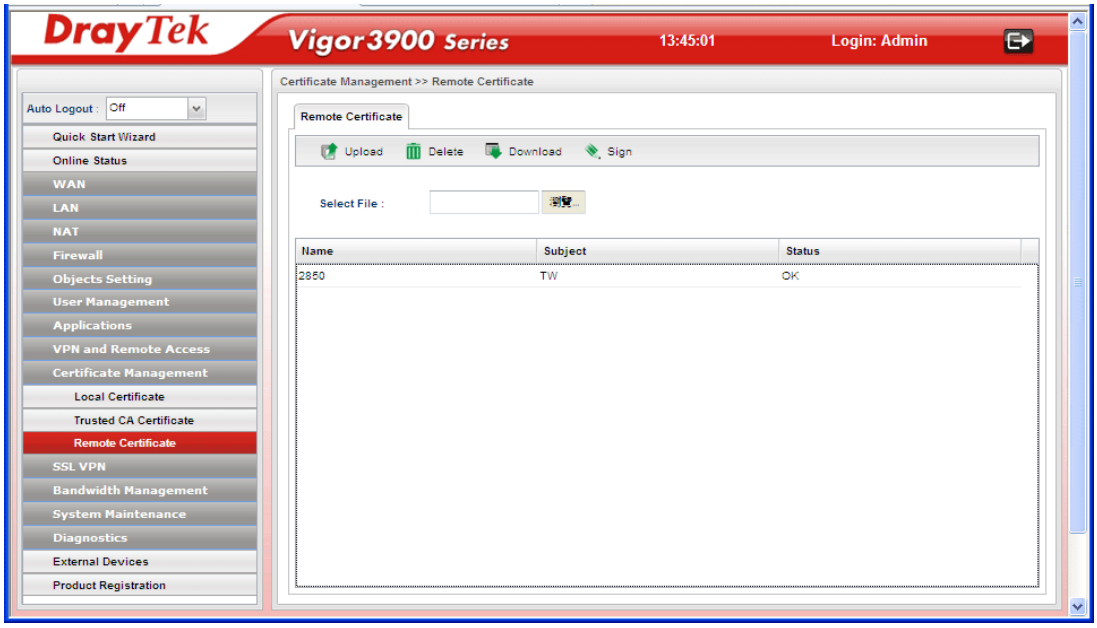
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state / province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
Key Size	Choose one of the key sizes for such certificate.
Country	Type the name of the country that such certificate located.
Passphase	Type the string for the new certificate.
Apply	Click it to create a new local certificate based on the configuration here.
Cancel	Click it to exit the web page without saving the configuration.

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



4.9.3 Remote Certificate

Vigor3900, as a Root CA, can sign any certificate coming from end users locally or remotely. The selected user-defined certificate must be uploaded to Root CA. Also, the processing result will be displayed on this page.



Each item will be explained as follows:

Item	Description
Upload	Allow you to upload current configuration to the host as a remote certificate.
Delete	Remove the selected item of remote certificate listed below.
Download	Allow you to download an existing certificate to the router.
Selected File	Use the **Browse..** button to specify a file to be used as trusted CA certificate.
Name	Display the name of remote certificate built.
Subject	Display the subject of remote certificate built.
Status	Display the status of remote certificate built.

4.10 SSL VPN

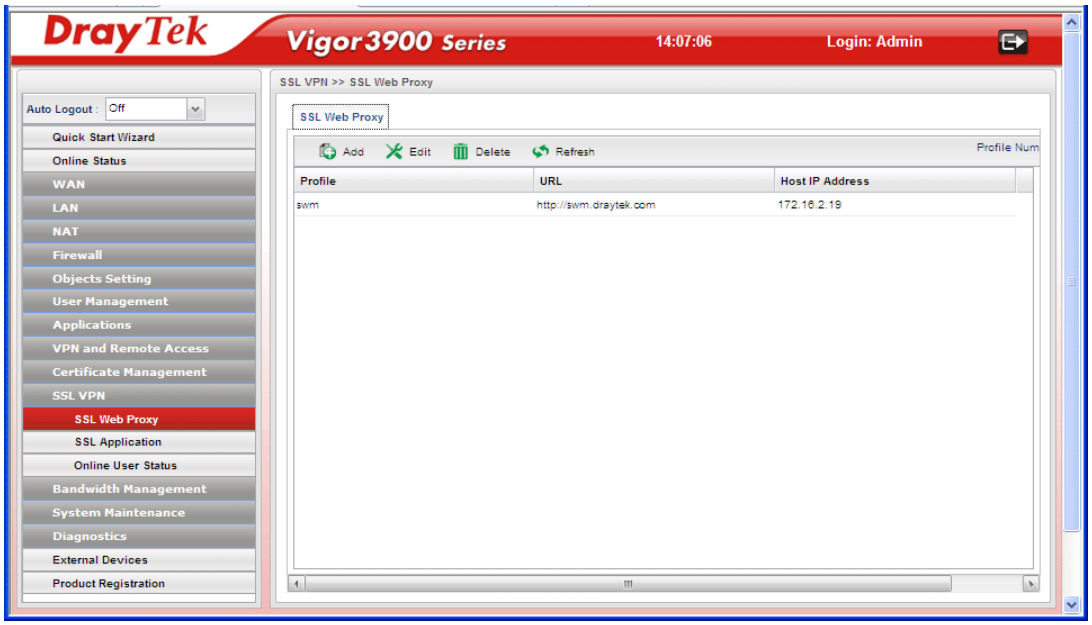
An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

There are two benefits that SSL VPN provides:

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

4.10.1 SSL Web Proxy

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



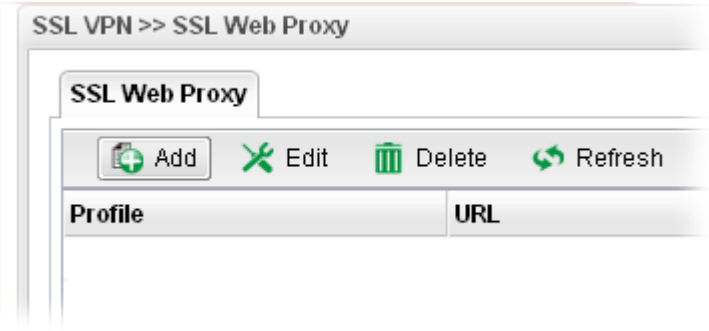
Each item will be explained as follows:

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

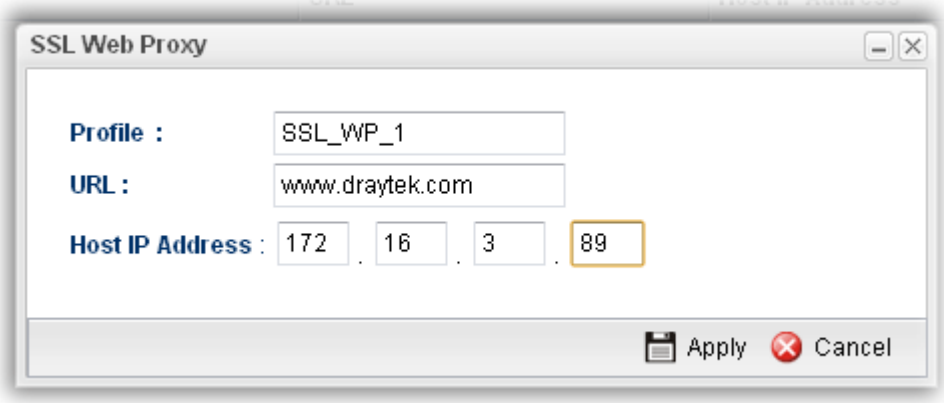
	To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the profile that you create.
URL	Display the URL.
Host IP Address	Display the IP address for the Host.

How to create a new SSL Web Proxy

1. Open **SSL VPN>> SSL Web Proxy.**
2. Simply click the **Add** button.



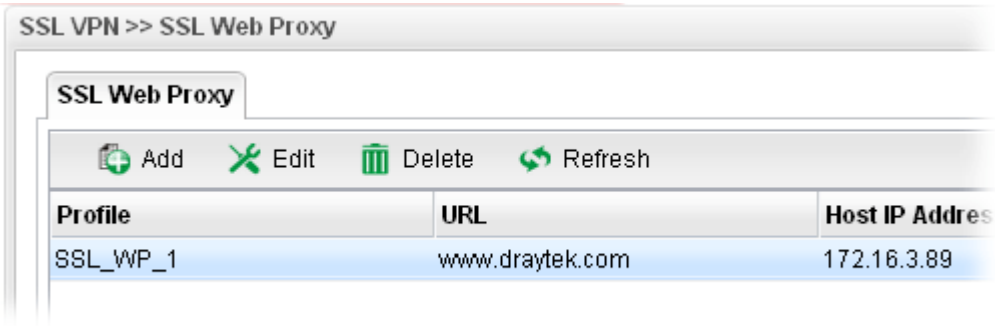
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type name of the profile.
URL	Type the address (function variation or IP address) or path of the proxy server.
Host IP Address	If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.

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

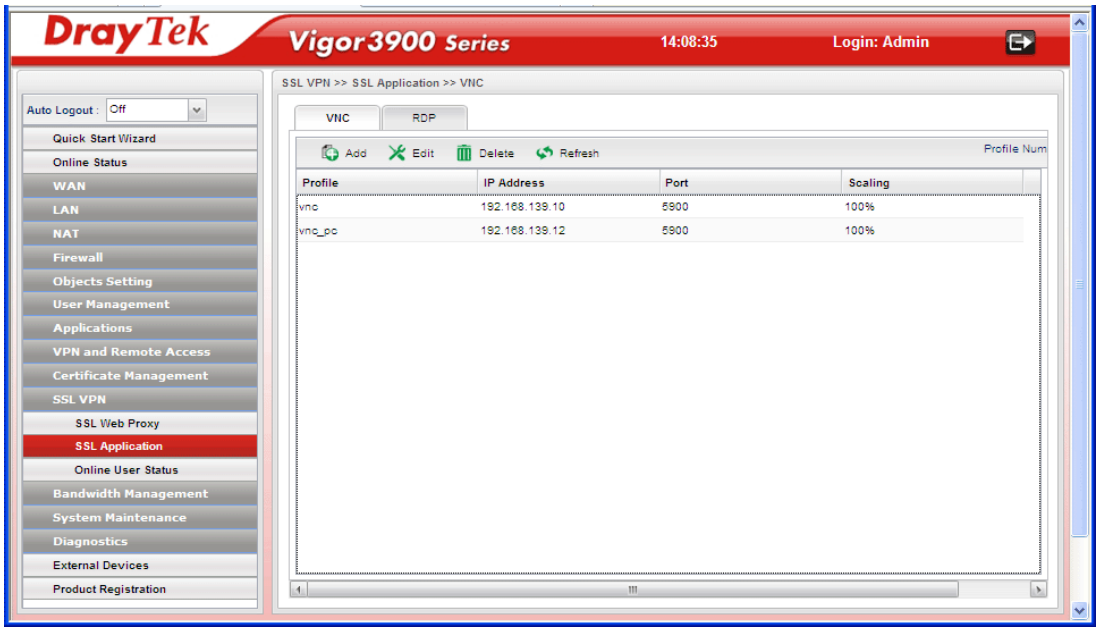


4.10.2 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) /SAMBA, to any remote user with access to Internet and a web browser.

VNC

VNC stands for **Virtual Network Computing.** It allows you to access and control a remote PC through VNC protocol.



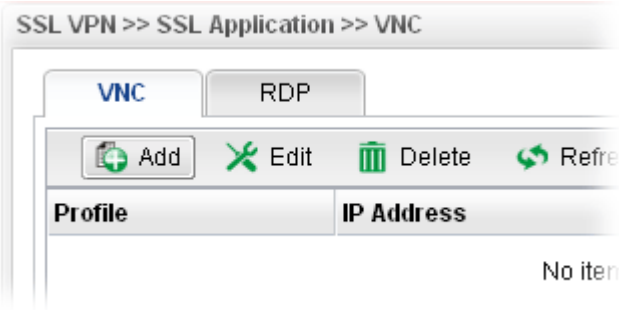
Each item will be explained as follows:

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

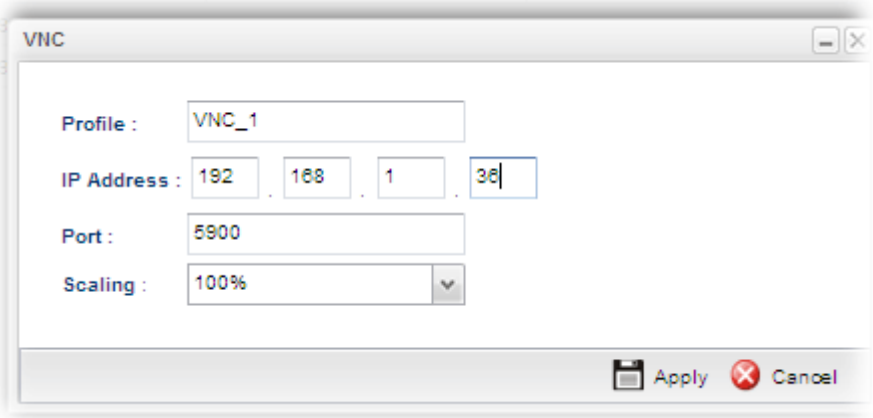
Refresh	Renew current web page.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.
Port	Display the port used for this protocol.
Scaling	Display the percentage for such application.

How to create a new SSL Application with VNC protocol

1. Open **SSL VPN>> SSL Application** and click the **VNC** tab.
2. Simply click the **Add** button.



3. The following dialog will appear.

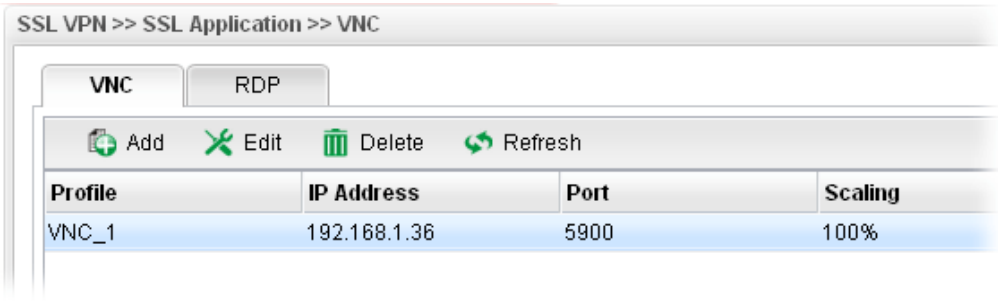


Available parameters are listed as follows:

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

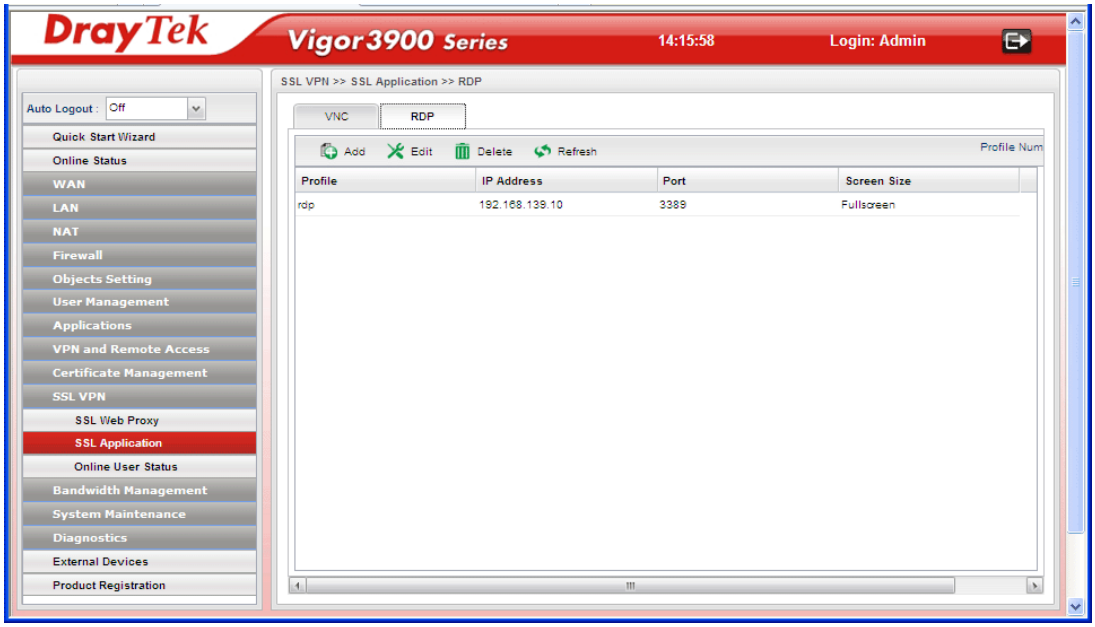
4. Enter all the settings and click **Apply**.

5. A new SSL Application profile has been created.



RDP

RDP stands for **Remote Desktop Protocol.** It allows you to access and control a remote PC through RDP protocol.



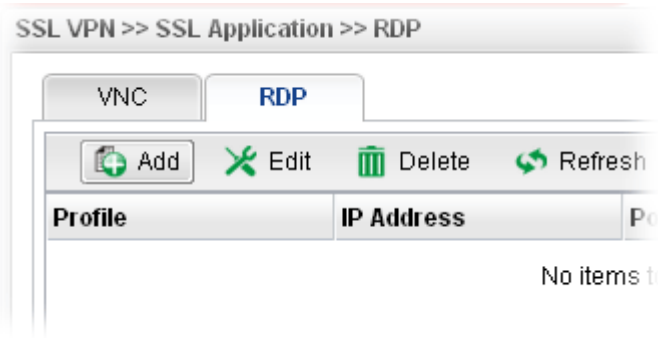
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.

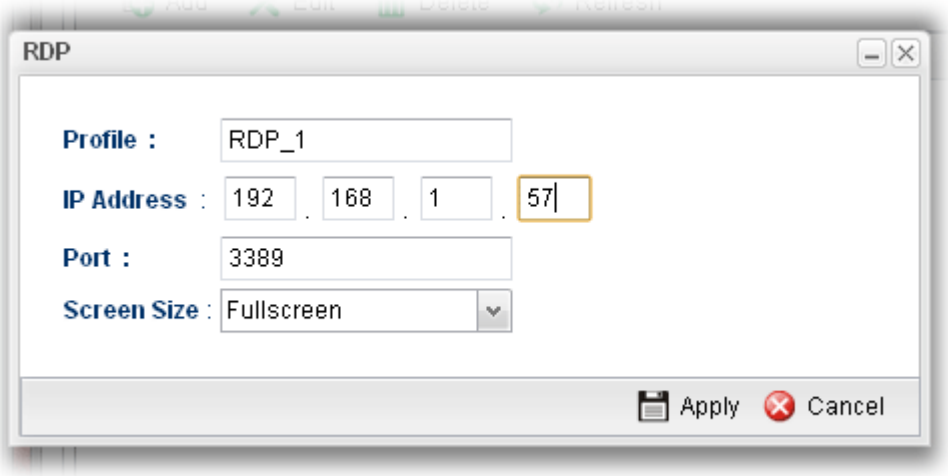
Port	Display the port used for this protocol.
Screen Size	Display the screen size for such application.

How to create a new SSL Application with RDP protocol

1. Open **SSL VPN>> SSL Application** and click the **RDP** tab.
2. Simply click the **Add** button.



3. The following dialog will appear.

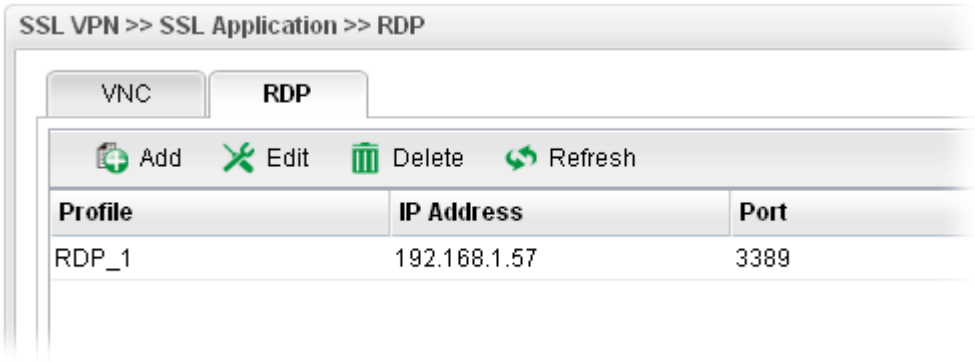


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile that you create.
IP Address	Type the IP address for this protocol.
Port	Specify the port used for this protocol.
Screen Size	Chose the screen size for such application.

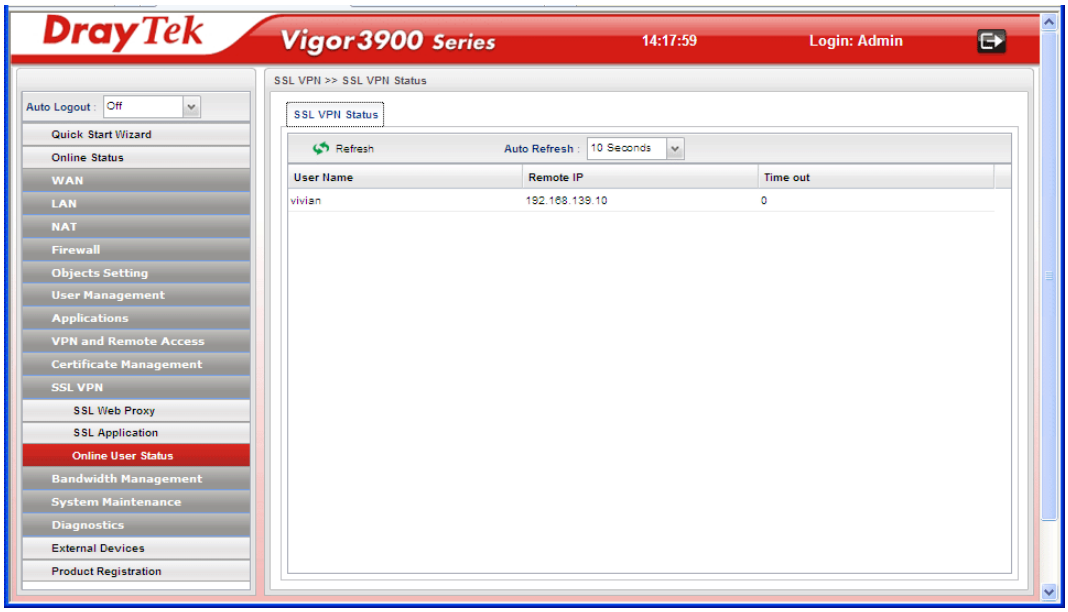
4. Enter all the settings and click **Apply**.

5. A new SSL Application profile has been created.



4.10.3 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into Draytek SSL VPN portal interface.

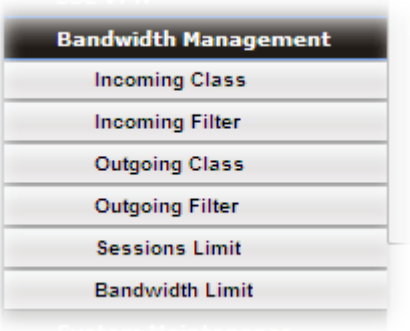


Each item will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
User Name	Display current user who visit SSL VPN server.
Remote IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.

4.11 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.

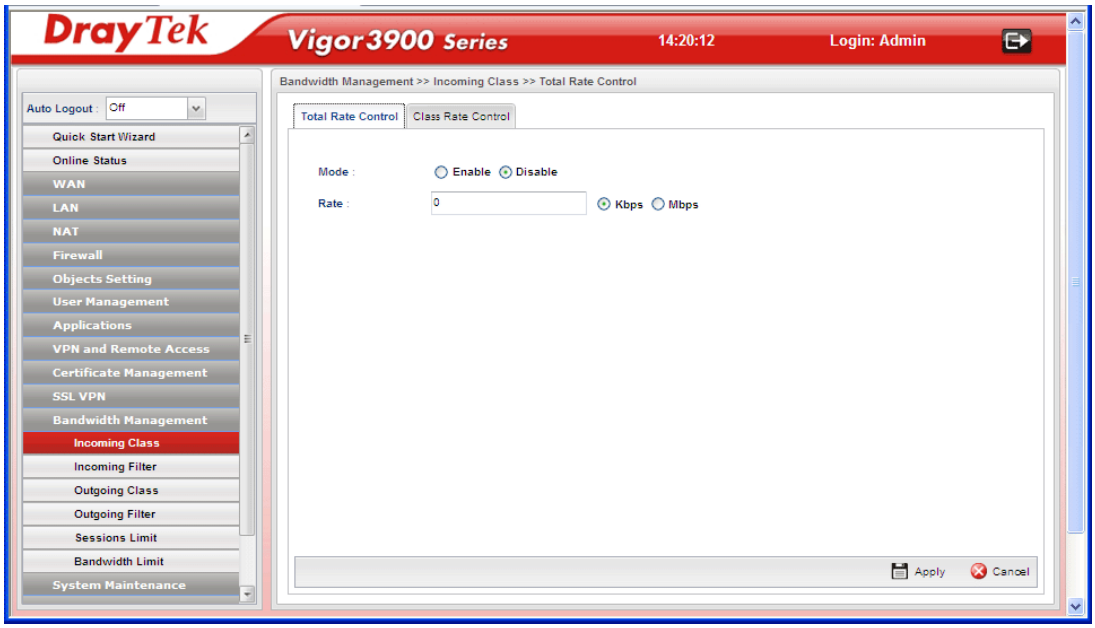
The QoS function handles incoming and outgoing classes independently. Users can configure incoming or outgoing separately without any impact on the other.

4.11.1 Incoming Class

Incoming Class Setup allows you to configure bandwidth percentage for data and voice signals transmission. Click the **Bandwidth Management** option and choose **Incoming Class.**

Total Rate Control

This page can set the total rate of incoming data for the QoS policer.

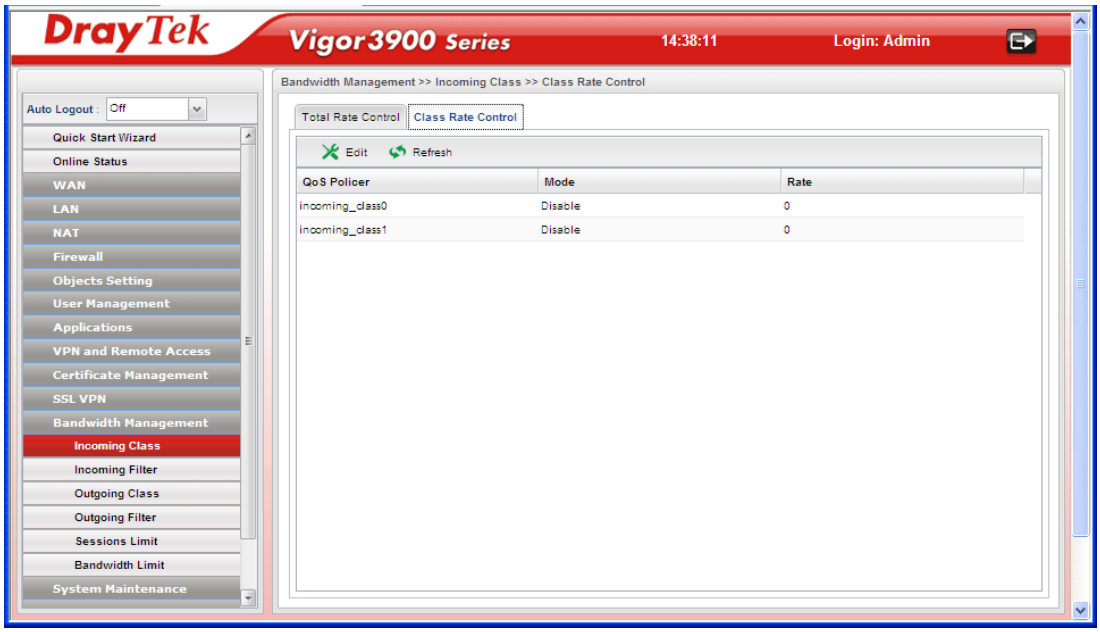


Available parameters are listed as follows:

Item	Description
Mode	Click **Enable** to enable such function.
Rate	Type the number as the total transmission rate for the incoming data.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

Class Rate Control

This page allows you to edit the incoming class rate for the QoS policer.

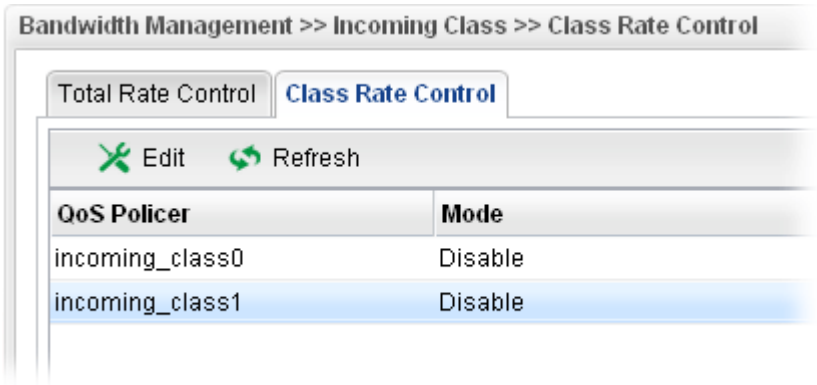


Each item will be explained as follows:

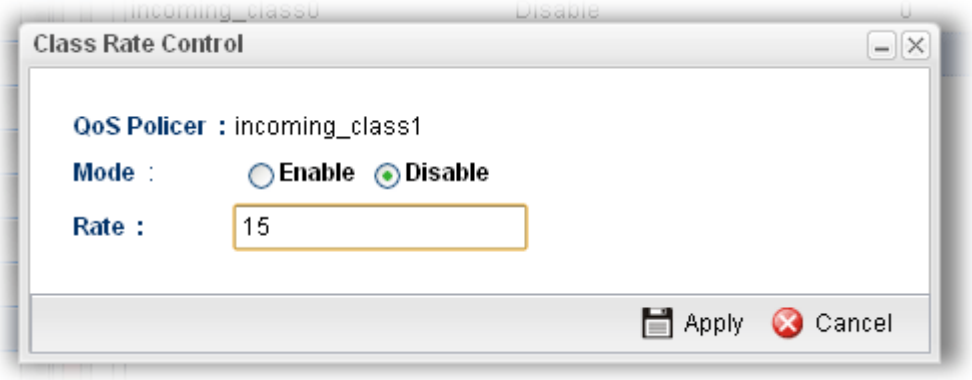
Item	Description
Edit	Modify the selected policy. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected policy.
Refresh	Renew current web page.
QoS Policer	Display the name of the QoS Policer.
Mode	Display the status of QoS Policer.
Rate	Display the rate of QoS Policer.

How to edit the incoming class rate for the QoS policer

1. Open **Bandwidth Management>> Incoming Class** and click the **Class Rate Control** tab**.**
2. Choose one of the incoming class rates and click the **Edit** button.



3. The following dialog will appear.

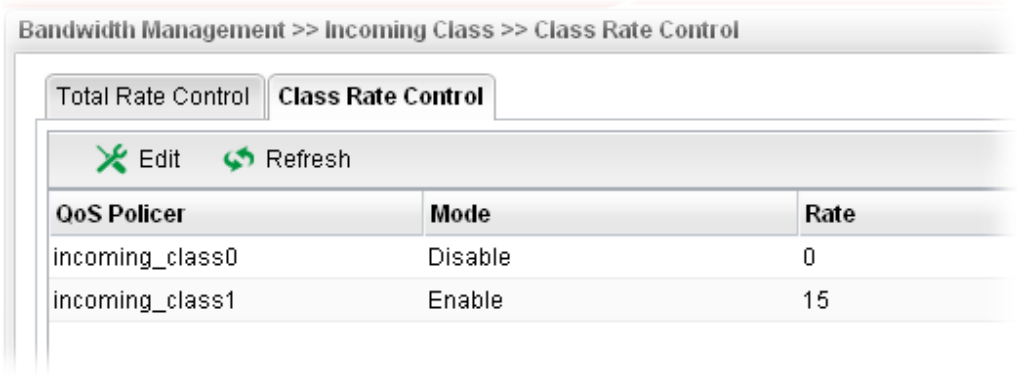


Available parameters are listed as follows:

Item	Description
QoS Policer	Display the name of the incoming class profile.
Mode	Click Enable to invoke such incoming class profile.
Rate	Type the number of rate for such profile.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

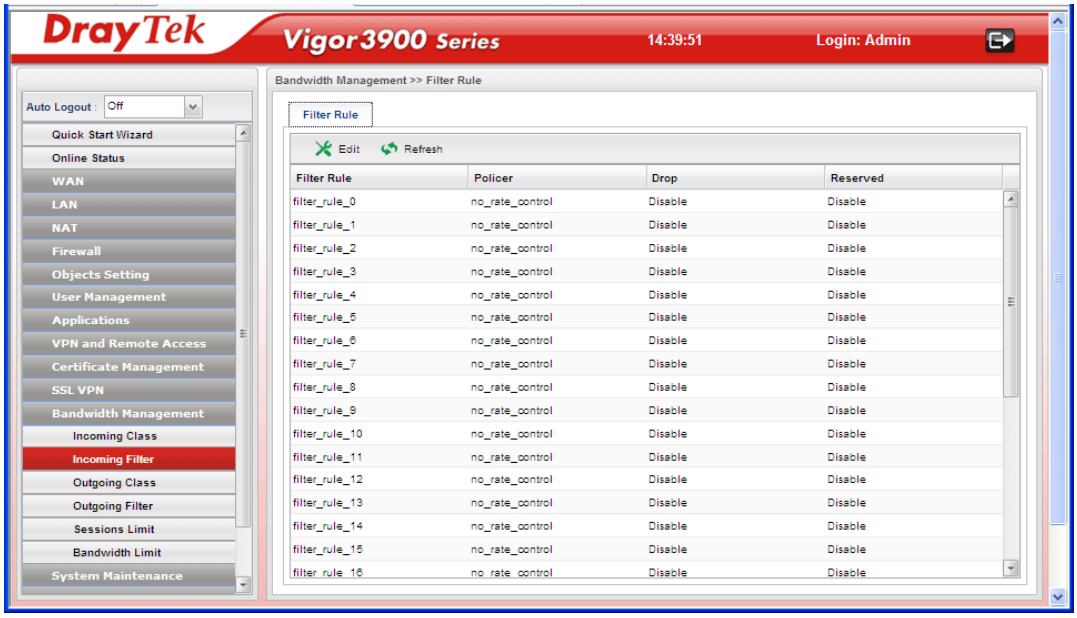
4. Enter all the settings and click **Apply**.

5. The **QoS Policer** profile has been modified.



4.11.2 Incoming Filter

There are 30 filter rules for incoming data that can be configured in such page.

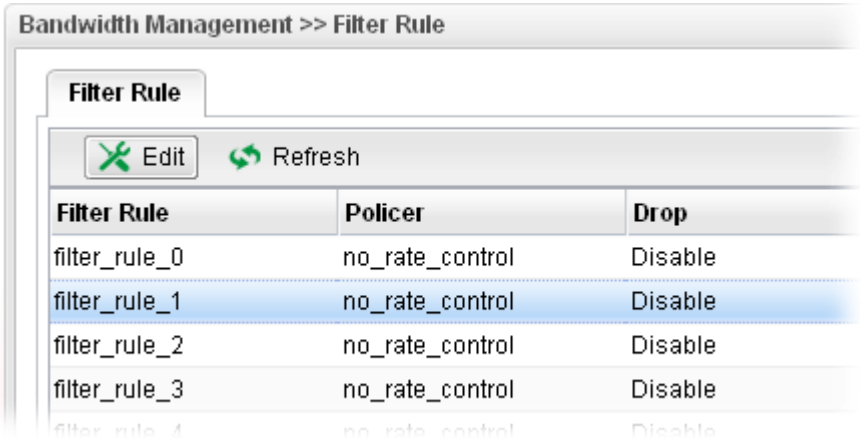


Each item will be explained as follows:

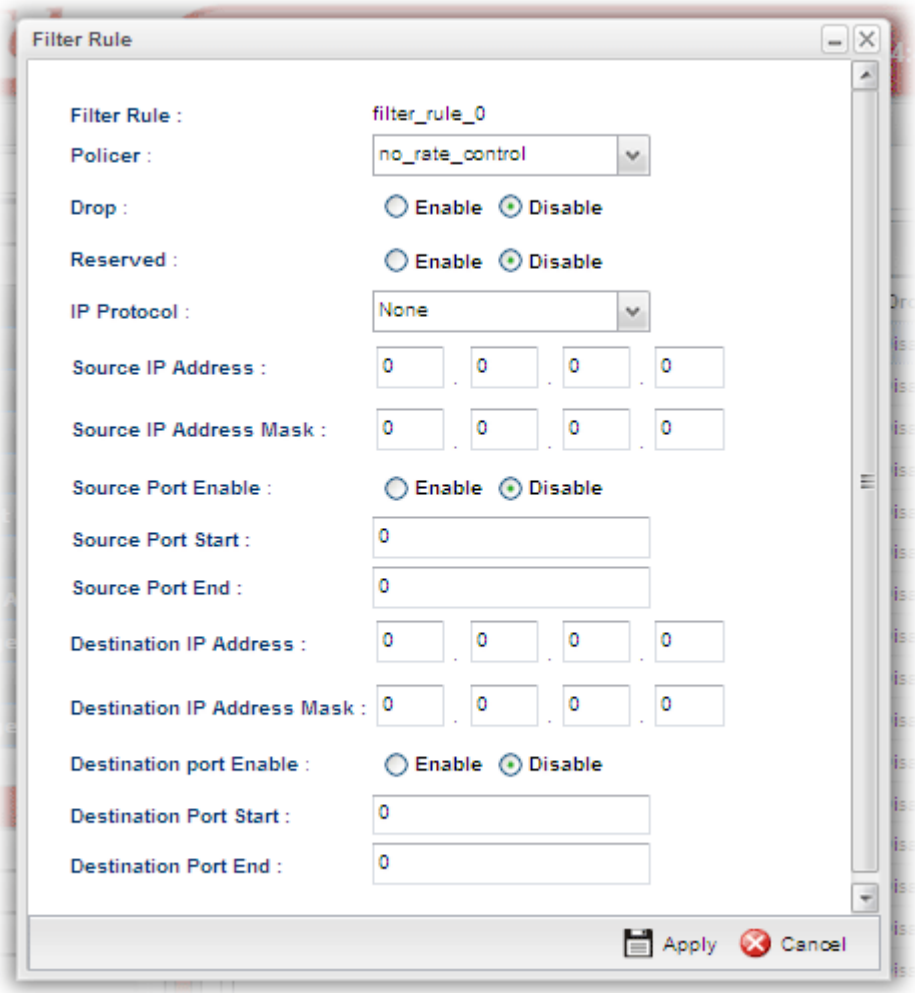
Item	Description
Edit	Modify the selected policy. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected policy.
Refresh	Renew current web page.
Filter Rule	Display the name of the filter rule.
Policer	Display the name of filter Policer.
Drop	Display the status for the packet to be discarded or not.
Reserved	Display the status for the packet to be kept in the buffer or not.

How to edit the incoming filter for the QoS policer

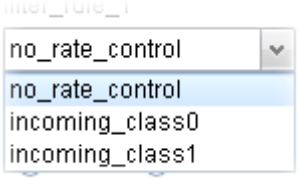
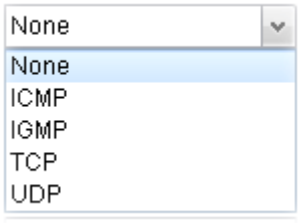
1. Open **Bandwidth Management>> Incoming Filter.**
2. Choose one of the filter rules and click the **Edit** button.



3. The following dialog will appear.

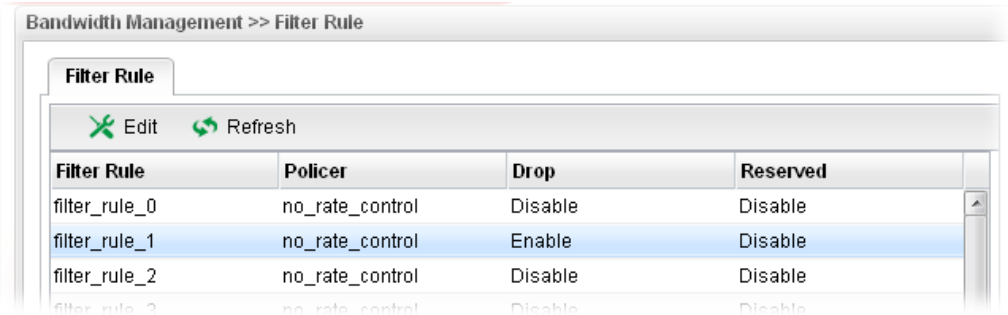


Available parameters are listed as follows:

Item	Description
Filter Rule	Display the profile name of the filter rule.
Policer	Choose the QoS Policer profile to apply to such filter rule. 
Drop	Choose **Enable** to discard the packets which satisfy the condition of the filter rule.
Reserved	Choose **Enable** to keep the packets which satisfy the condition of the filter rule, even the system is busy. When both **Drop** and **Reserved** are set to **Enable**, the priority of **Drop** is higher than **Reserved**.
IP Protocol	Choose a protocol for such filter rule. 
Source IP Address	Type the source IP address for such incoming filter rule.
Source IP Address Mask	Type the mask address for the source IP address.
Source Port Enable	Choose **Enable** to restrict the source port value.
Source Port Start	Type the starting port number (0 - 65535) in the range of the source port.
Source Port End	Type the ending port number (0 - 65535) in the range of the source port.
Destination IP Address	Type the destination IP address for such incoming filter rule.
Destination IP Address Mask	Type the mask address for the destination IP address.
Destination port Enable	Choose Enable to restrict the destination port value.
Destination Port Start	Type the starting port number (0 - 65535) in the range of the destination port.
Destination Port End	Type the ending port number (0 - 65535) in the range of the destination port.
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 incoming filter rule for **QoS Policer** has been modified.

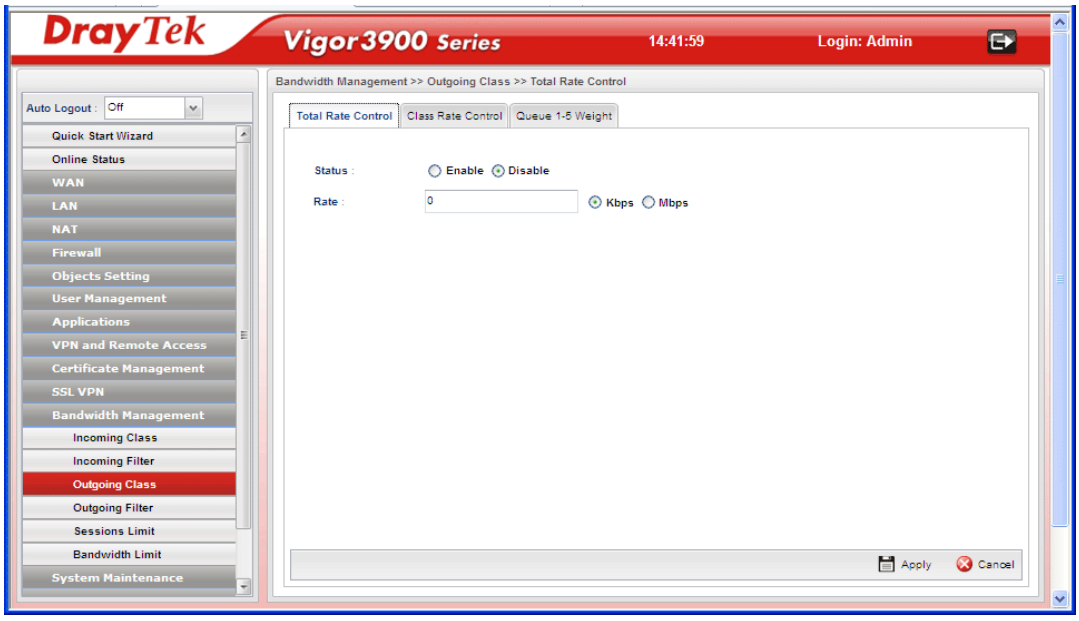


4.11.3 Outgoing Class

Outgoing Class Setup allows you to configure bandwidth percentage for data and voice signals transmission. Click the **Bandwidth Management** option and choose **Incoming Class.**

Total Rate Control

This page can set the total rate of outgoing data for the QoS policer.

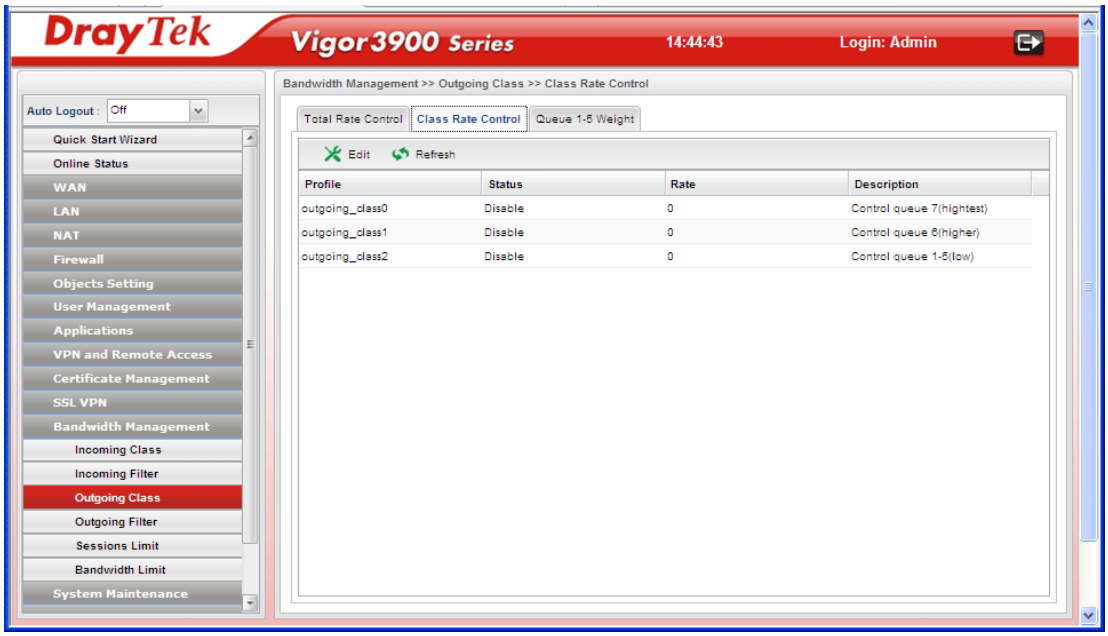


Available parameters are listed as follows:

Item	Description
Status	Click **Enable** to enable such function.
Rate	Type the rate for outgoing data. The range can be set from 64000 to 10000000.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to discard the settings configured in this page.

Class Rate Control

This page allows you to edit the outgoing class rate for different QoS policer.

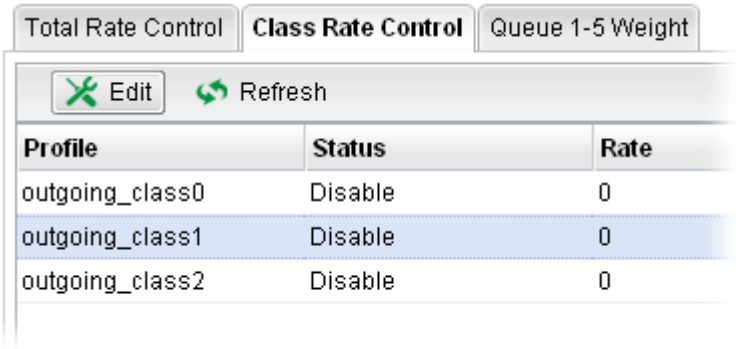


Each item will be explained as follows:

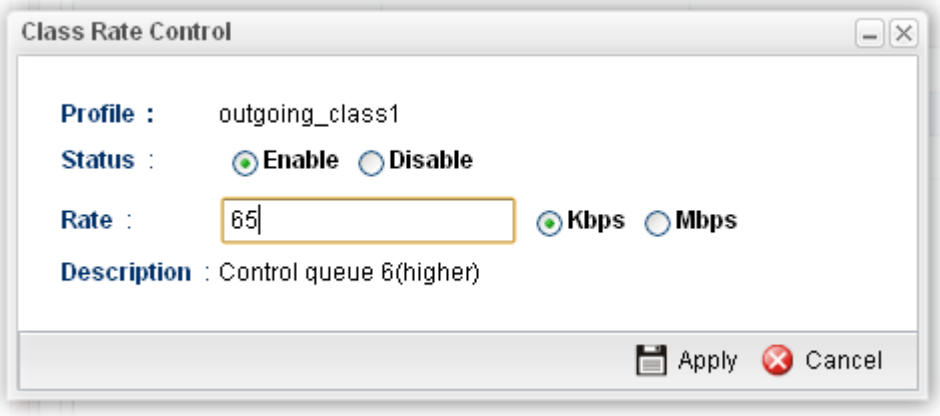
Item	Description
Edit	Modify the selected policy. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected policy.
Refresh	Renew current web page.
Profile	Display the name of the outgoing class rate profile.
Status	Display the status (enable or disable) of such profile.
Rate	Display the limitation (from 64000 to 10000000) for the rate of queue.
Description	Display the description for such profile.

How to edit the outgoing class rate for the QoS policer

1. Open **Bandwidth Management>> Outgoing Class** and click the **Class Rate Control** tab**.**
2. Choose one of the profiles and click the **Edit** button.



3. The following dialog will appear.

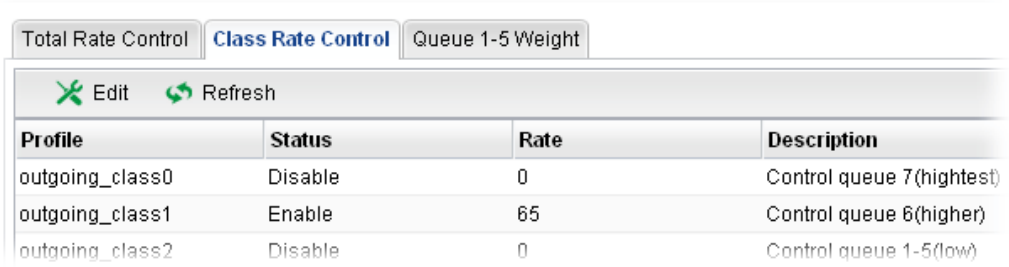


Available parameters are listed as follows:

Item	Description
Profile	Display the name of the QoS Shaper profile.
Status	Click **Enable** to enable such function.
Rate	Type the limitation for the rate of queue. Click the unit for such rate.
Description	Such information is offered by the system automatically. It is not necessary to change it.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

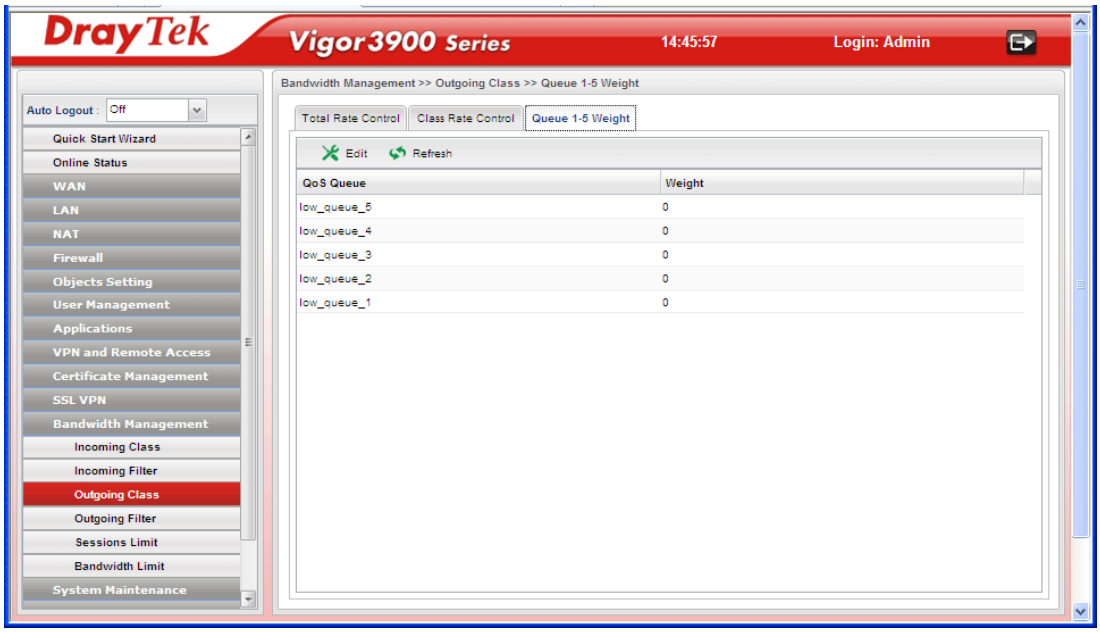
4. Enter all the settings and click **Apply**.

5. The outgoing class rate for **QoS Policer** has been modified.



Outgoing Queue 1- 5 Weight

There are several available outgoing queues, four shapers at varying levels, and five data queues with weights. 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.



Each item will be explained as follows:

Item	Description
Edit	Modify the selected policy. 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 policy.
Refresh	Renew current web page.
QoS Queue	Display the name of the QoS queue.
Weight	Display the weight of the QoS queue.

How to edit the outgoing queue 1- 5 weight for the QoS policer

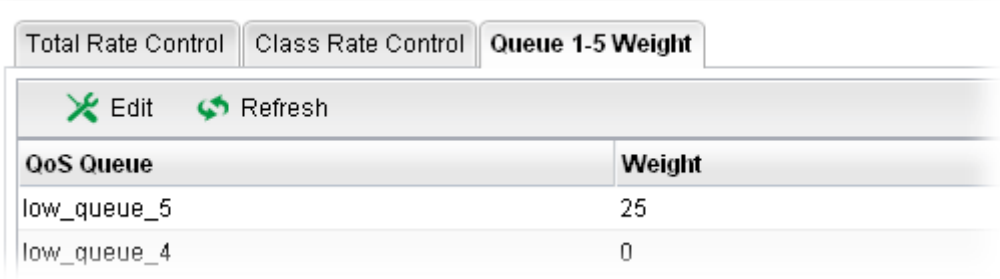
1. Open **Bandwidth Management>> Outgoing Class** and click the **Queue 1-5 Weight** tab**.**
2. Choose one of the profiles and click the **Edit** button.

3. The following dialog will appear.

Available parameters are listed as follows:

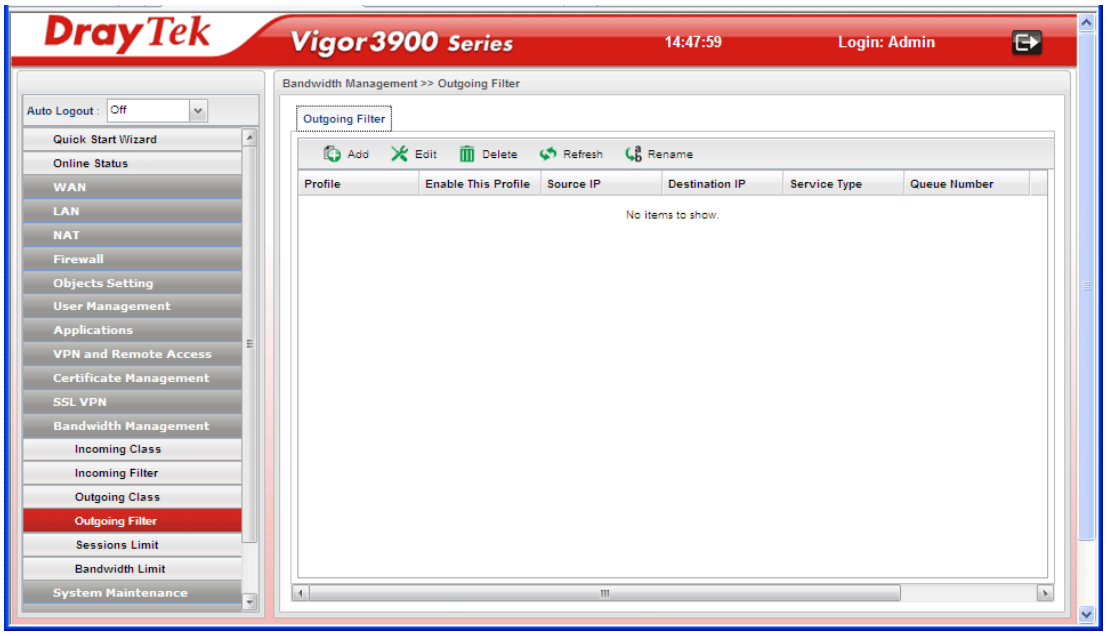
Item	Description
QoS Queue	Display the name of the QoS queue.
Weight	Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

4. Enter all the settings and click **Apply**.
5. The outgoing queue 1-5 weight for **QoS Policer** has been modified.



4.11.4 Outgoing Filter

There are 30 filter rules for outgoing data that can be configured in such page.

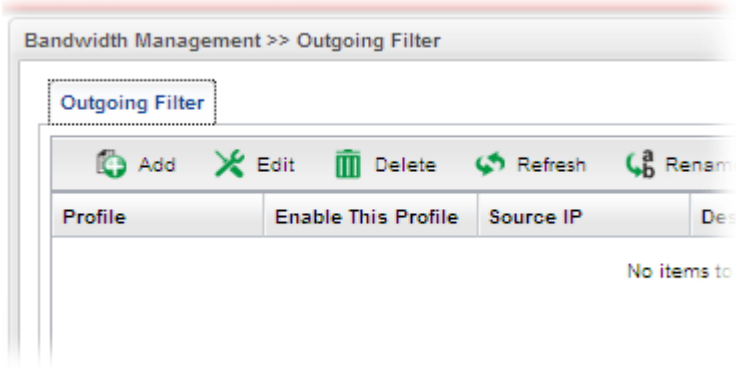


Each item will be explained as follows:

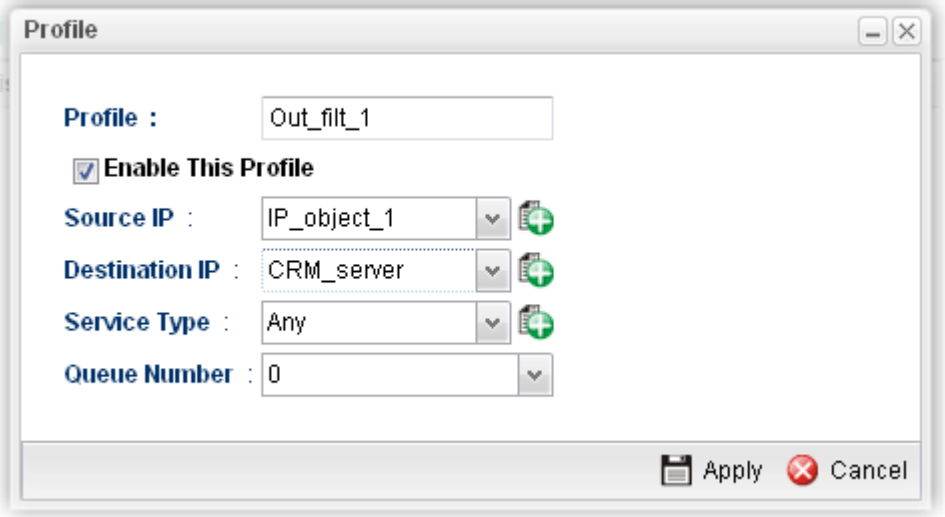
Item	Description
Add	Add a new filter profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile for the filter.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Source IP	Display the source IP address for the filter.
Destination IP	Display the destination IP address for the filter.
Service Type	Display the service type (e.g., IKE, HTTP, AUTH and etc) for the filter.
Queue Number	Display the queue number that such filter is categorized.

How to add an outgoing filter for the QoS policer

1. Open **Bandwidth Management>> Outgoing Filter.**
2. Simply click the **Add** button.

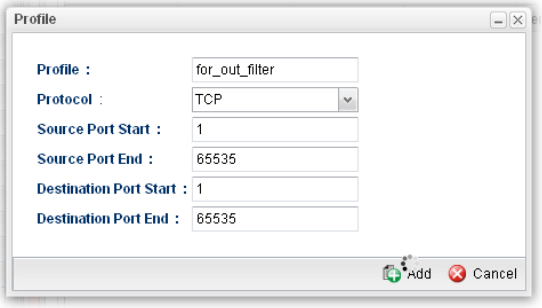
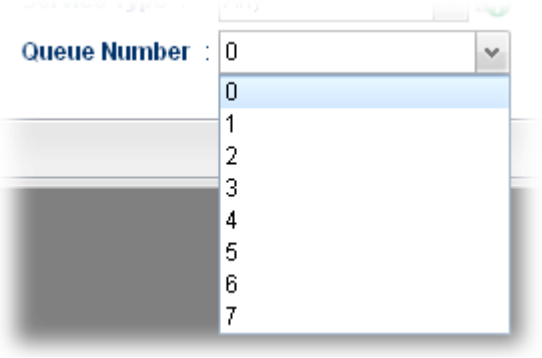


3. The following dialog will appear.

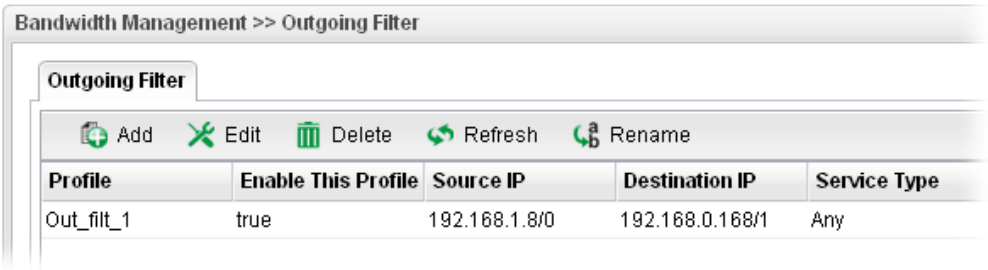


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the filter profile.
Enable This Profile	Check this box to enable such profile.
Source IP	Type the source IP address with subnet mask value to be applied for this filter.
Destination IP	Type the destination IP address with subnet mask value to be applied for this filter.
Service Type	Choose one of the service types from the drop down list. If you want to create a new service type, simply click to open the following dialog.

	 **Profile** – type a new name for such service type. **Protocol** –There are two options: **TCP**, **UDP** and **TCP/UDP**. Select the protocol that you want to use. **Source Port Start /End -** Type the start /end number for the port range of the source port for such filter. **Destination Port Start / End -** Type the start /end number for the port range of the destination port for such filter.
Queue Number	Choose a queue number to category the packets matching with the condition configured as above. Queue 7 is the highest; 0 is the lowest. 
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

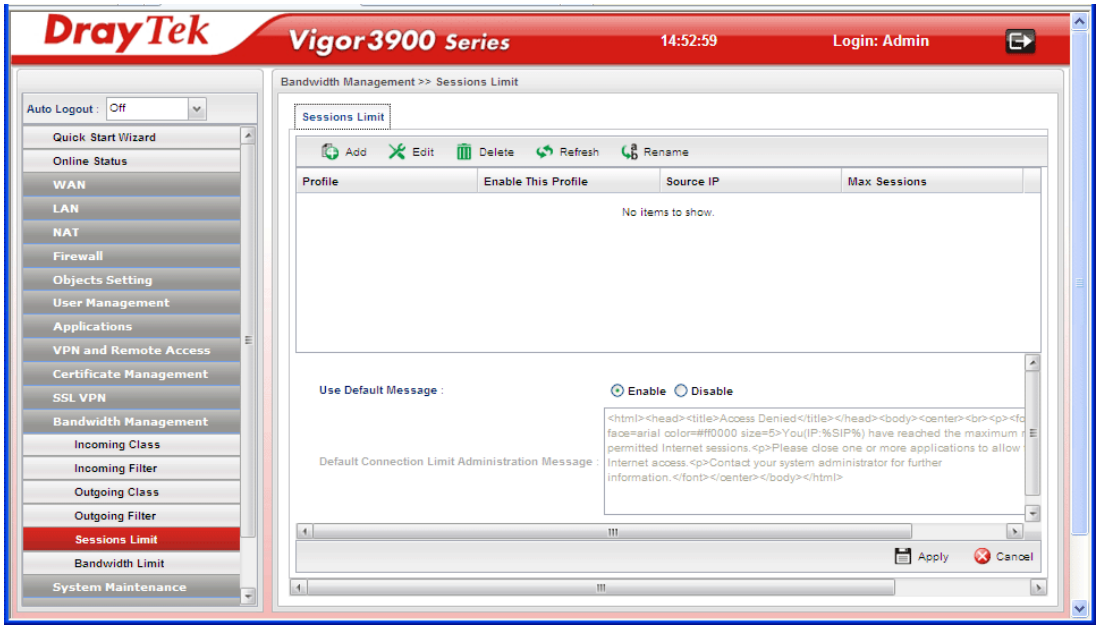
4. Enter all the settings and click **Apply**.
5. The outgoing filter for **QoS Policer** has been created.



4.11.5 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



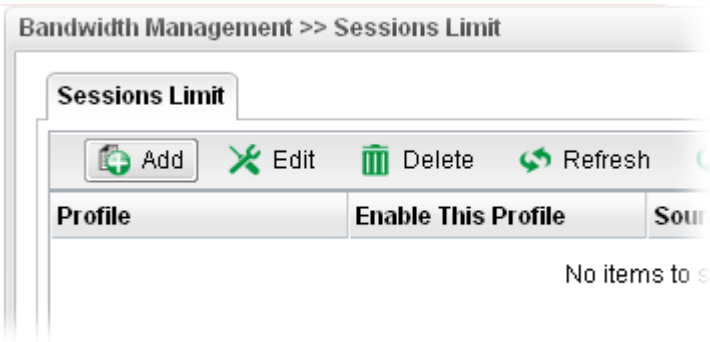
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Source IP	Display the IP address with subnet mask of the profile.
Max Sessions	Display the maximum sessions used by the profile.
Use Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page..

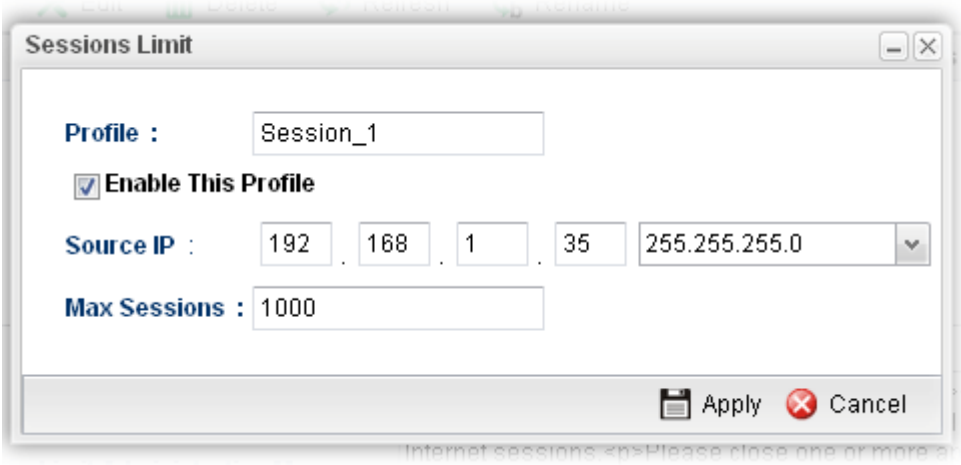
	Disable – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Web Category Administration Message	Such field is available when you disable the function of **Use Default Message**. The message will display on the user's browser when he/she tries to access the blocked web page.
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 for the QoS policer

1. Open **Bandwidth Management>> Sessions Limit.**
2. Simply click the **Add** button.



3. The following dialog will appear.

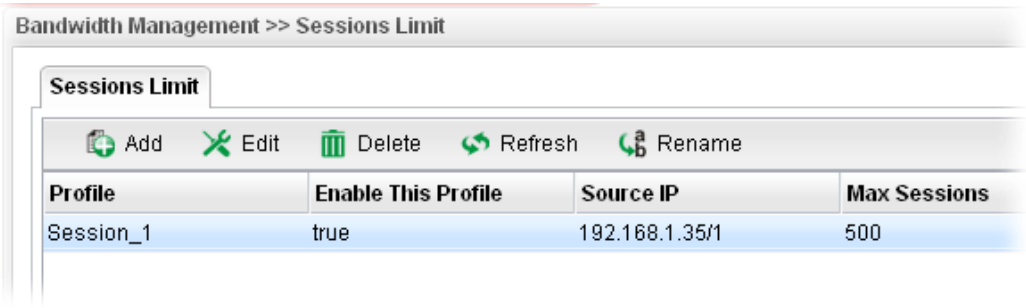


Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable such profile.
Source IP	Type the source IP address with subnet mask for limit session.
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.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

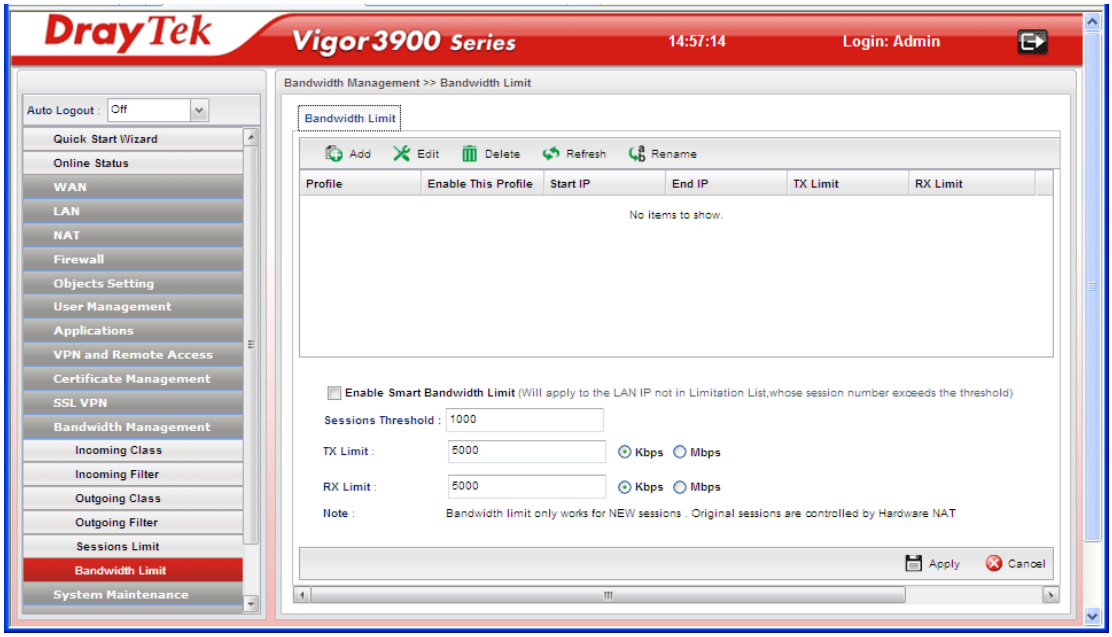
4. Enter all the settings and click **Apply**.
5. A session limit profile has been created.



4.11.6 Bandwidth Limit

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

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



Each item will be explained as follows:

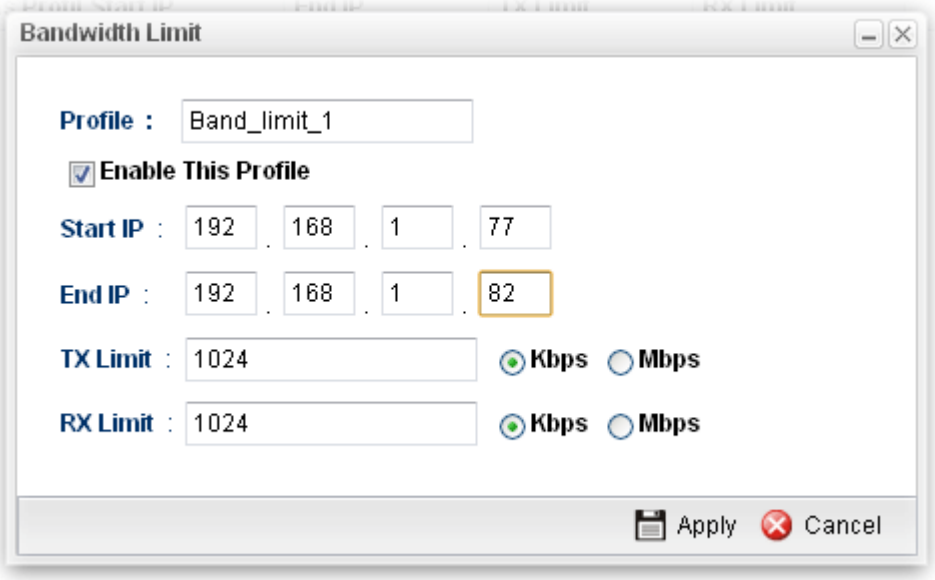
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for

	you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the bandwidth limitation profile.
Enable This Profile	Check the box to enable the Mirror function for the switch.
Start IP	Display the start IP address for the profile.
End IP	Display the end IP address for the profile.
TX Limit	Display the limitation for the speed of the upstream for the profile.
RX Limit	Display the limitation for the speed of the downstream for the profile.
Enable Smart Bandwidth Limit	Check this radio button to configure the default limitation for bandwidth for any LAN IP not included in the Limitation List.
Session Threshold	When session number exceeds the set threshold, Smart Bandwidth limit will work.
TX Limit	Define the default speed of the upstream for Smart Bandwidth Limit.
RX Limit	Define the default speed of the downstream for Smart Bandwidth Limit.
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 for the QoS policer

1. Open **Bandwidth Management>>Bandwidth Limit.**
2. Simply click the **Add** button.

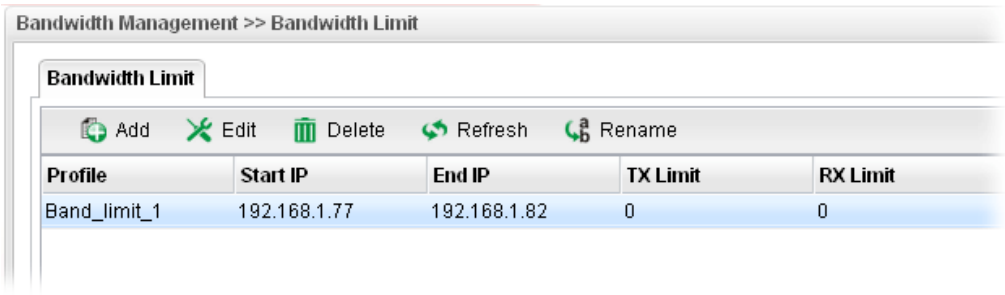
3. The following dialog will appear.



Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
TX Limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
RX Limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



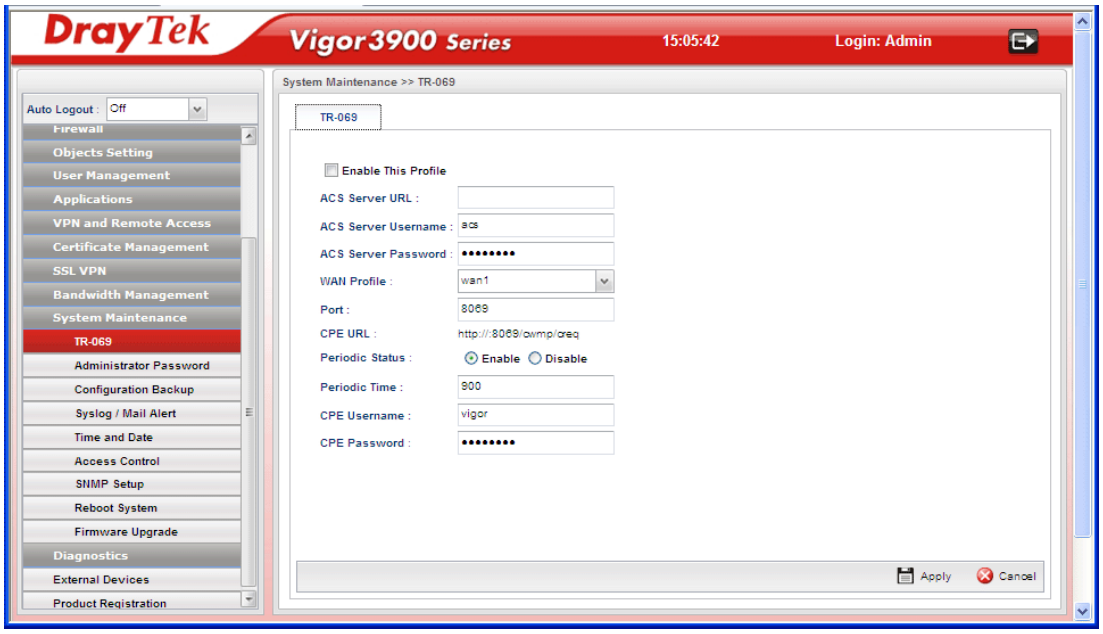
4.12 System Maintenance

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

Below shows the menu items for System Maintenance.

4.12.1 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



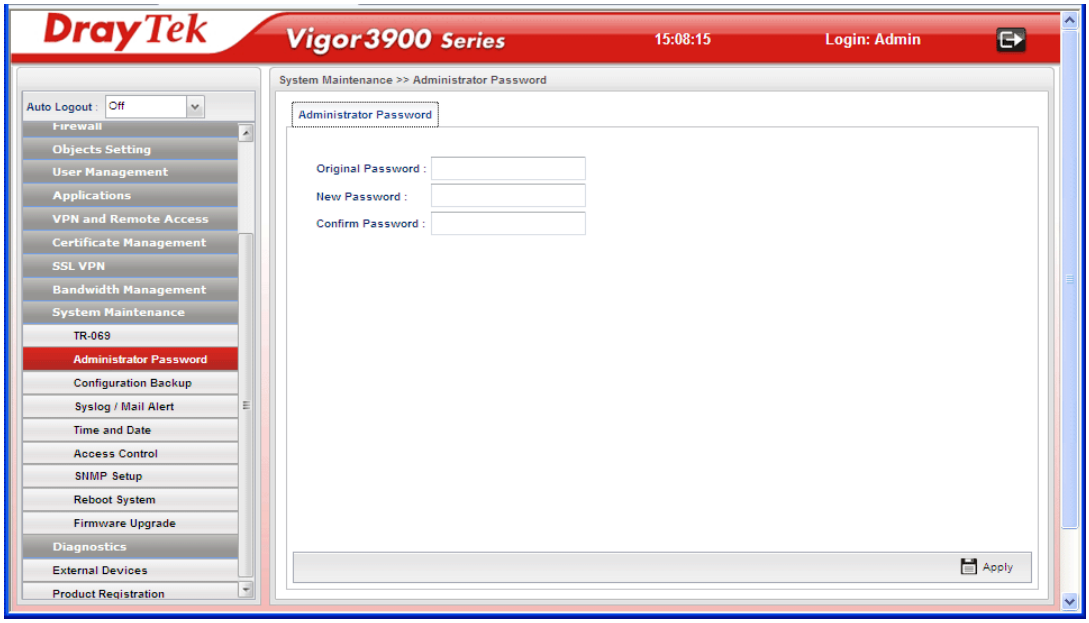
Each item will be explained as follows:

Item	Description
Enable This Profile	Check this box to enable such profile.
ACS Server URL/Username /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.

WAN Profile	Choose one of the WAN profiles which will be recognized by VigorACS.
Port	Type the port number for Vigor3900 which will be recognized by VigorACS.
CPE URL	Display the URL of such CPE.
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.
CPE Username	Type the user name for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
CPE Password	Type the password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.12.2 Administrator Password

This page allows you to set new password for accessing into the WUI of the router.



Each item will be explained as follows:

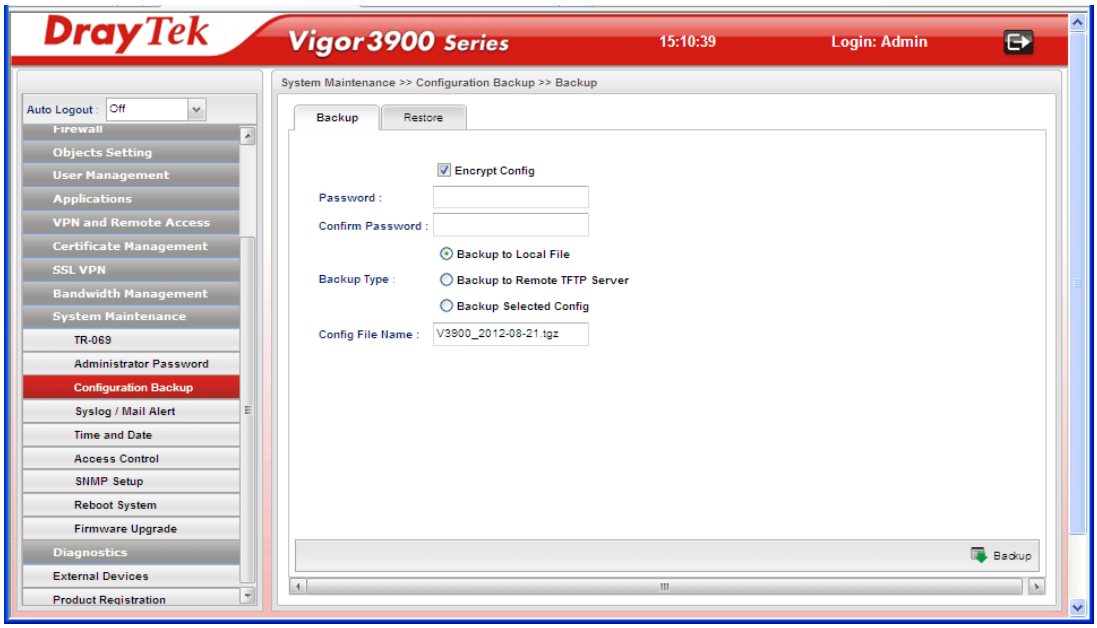
Item	Description
User Name	Display the name of the administrator.
Original Password	Type the old password.
New Password	Type the new password.
Confirm Password	Re-type the new password for confirmation.

Apply	Click this button to save the configuration and exit the web page.

4.12.3 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.

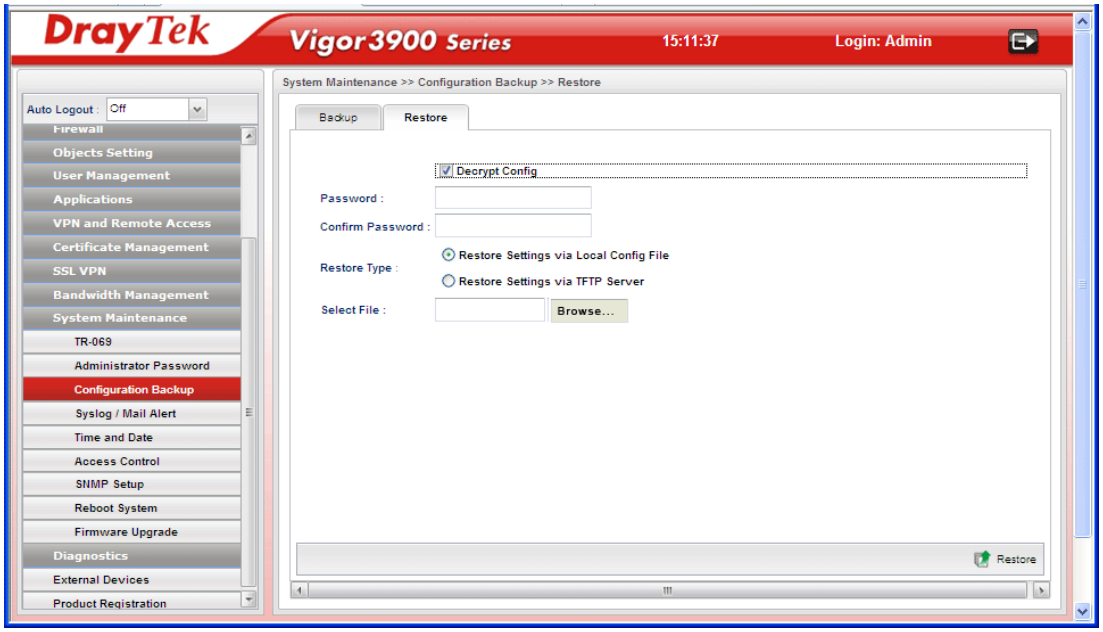
Backup



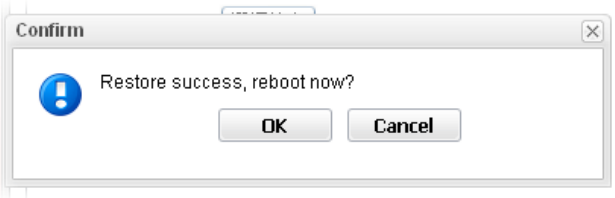
Each item will be explained as follows:

Item	Description
Encrypt Config	Check this box to encrypt the configuration file. **Password** – Type a password for encrypting the file. **Confirm Password –** Retype the password for confirmation.
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 configuration file name. You can change the name if required.
Backup	Execute the file downloading job to the computer.

Restore



Each item will be explained as follows:

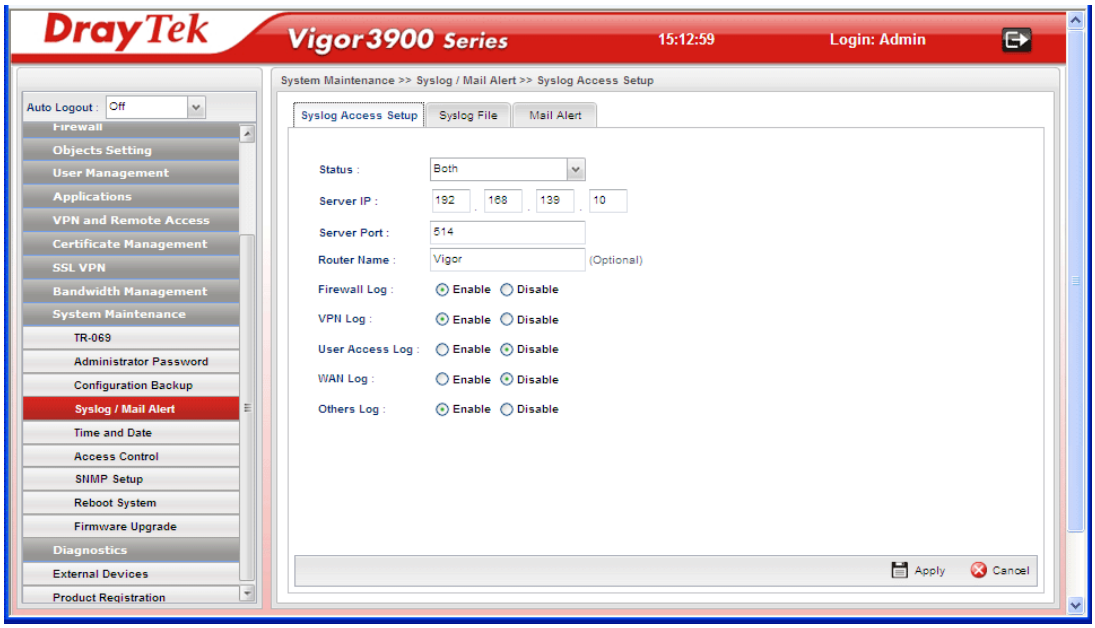
Item	Description
Decrypt Config	Check this box to decrypt an encrypted configuration file. You can specify a password for decrypting the file for restoring it for use next time. **Password** – Type a password for encrypting the file. **Confirm Password –** Retype the password for confirmation.
Restore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

4.12.4 Syslog / Mail Alert

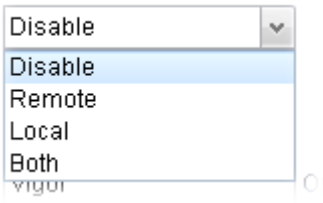
SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

Syslog Access Setup

To configure settings for Syslog, open **System Maintenance>>Syslog/Mail Alert** and click the **Syslog Access Setup** tab.

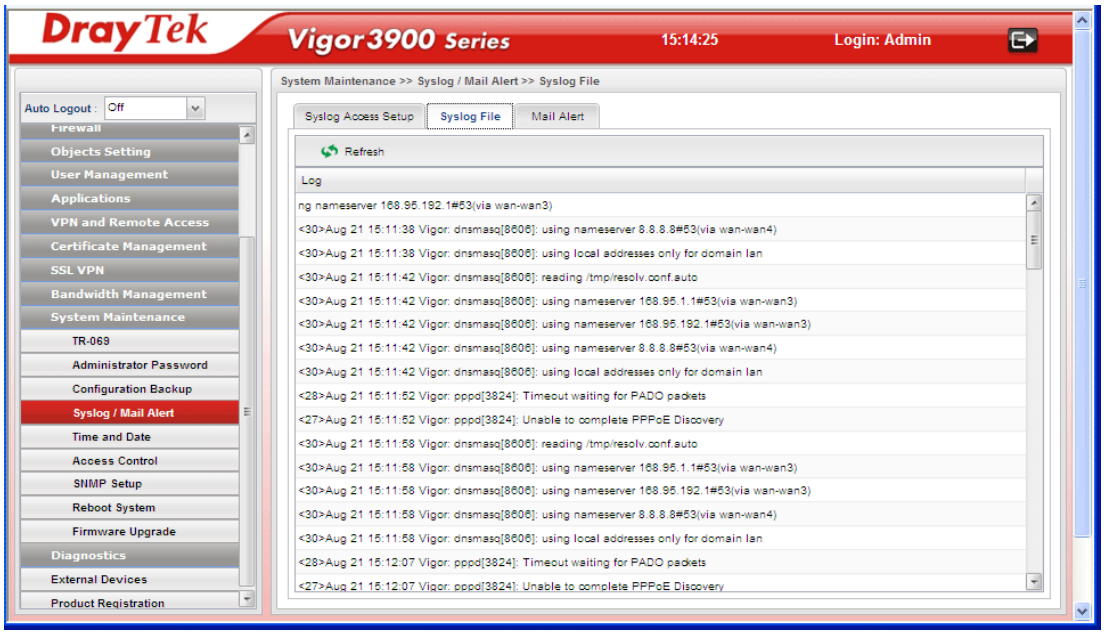


Available parameters are listed as follows:

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. 
Server IP	Type the IP address of the Syslog server.
Server Port	Type the port number for the Syslog server.
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.
VPN Log	Click **Enable** to make the VPN log recorded in the Syslog.
User Access Log	Click **Enable** to make the user access log recorded in the Syslog.

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

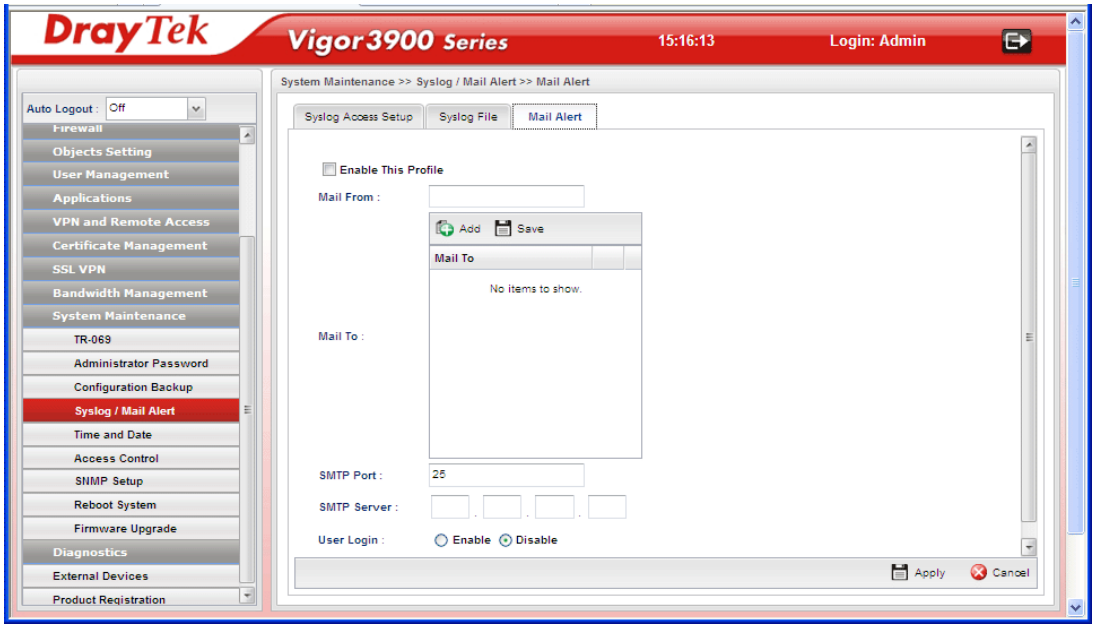
SysLog File



Available parameters are listed as follows:

Item	Description
Refresh	Renew the web page.

Mail Alert



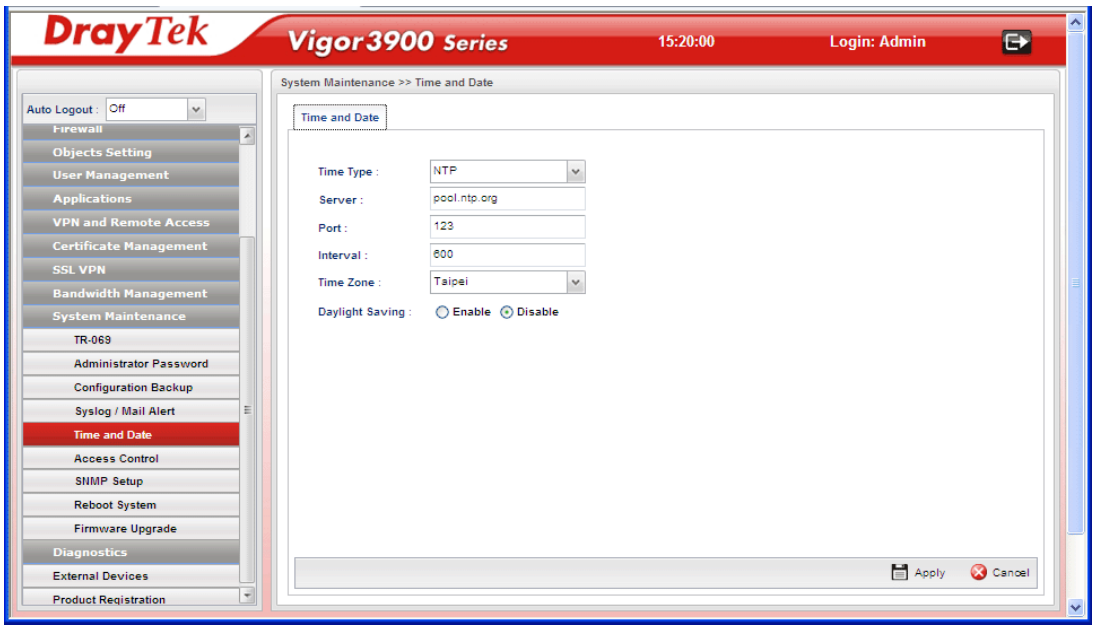
Available parameters are listed as follows:

Item	Description
Enable This Profile	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.
SMTP Port	Type the port number for SMTP server.
SMTP Server	Type the IP address for SMTP server.
User Login	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.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

4.12.5 Time and Date

This page allows you to specify where the time of the router should be inquired from.

As an NTP (Network Time Protocol) client, the router gets standard time from the time server. Some time-based functions cannot work properly until the system time functions run successfully. Typically, NTP achieves high accuracy and reliability with multiple redundant servers and diverse network paths.

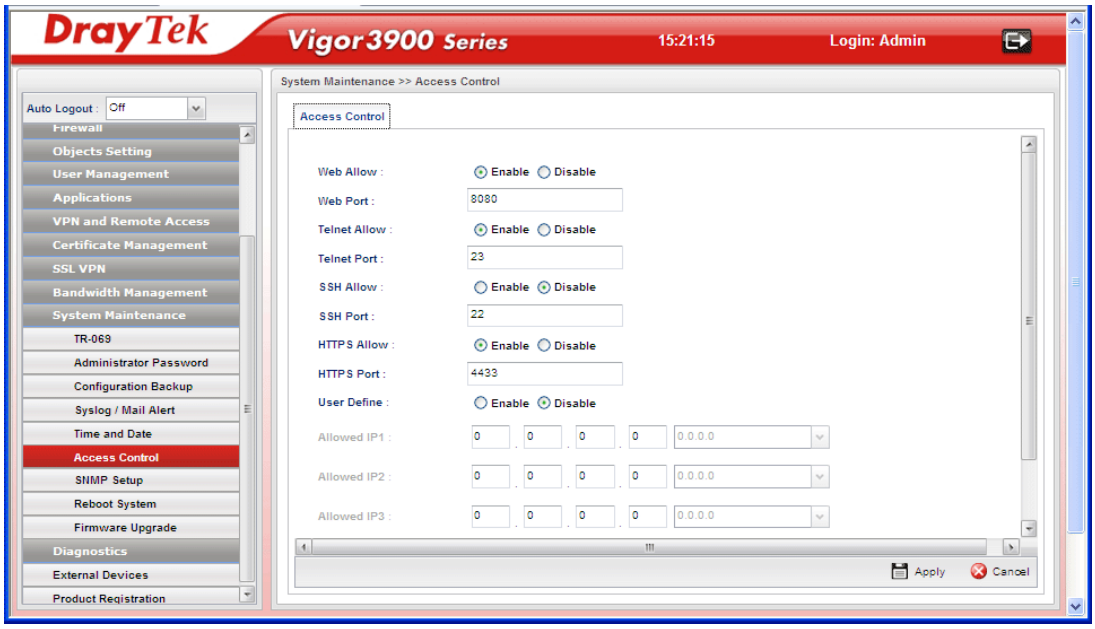


Available parameters are listed as follows:

Item	Description
Time Type	**NTP** – Select to inquire time information from Time Server on the Internet using assigned protocol. **Browser** - Select this option to use the browser time from the remote administrator PC host as router's system time.
Server	Type the domain name of the server.
Port	Type the port number for the time server.
Interval	Select a time interval for updating from the NTP server.
Time Zone	Select the time zone where the router is located.
Daylight Saving	Click **Enable** to enable the daylight saving. Such feature is available for certain area.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

4.12.6 Access Control

This page allows you to open or close the web configurator ofVigor3900 by using Telnet, SSH, HTTP, HTTPS… and etc…



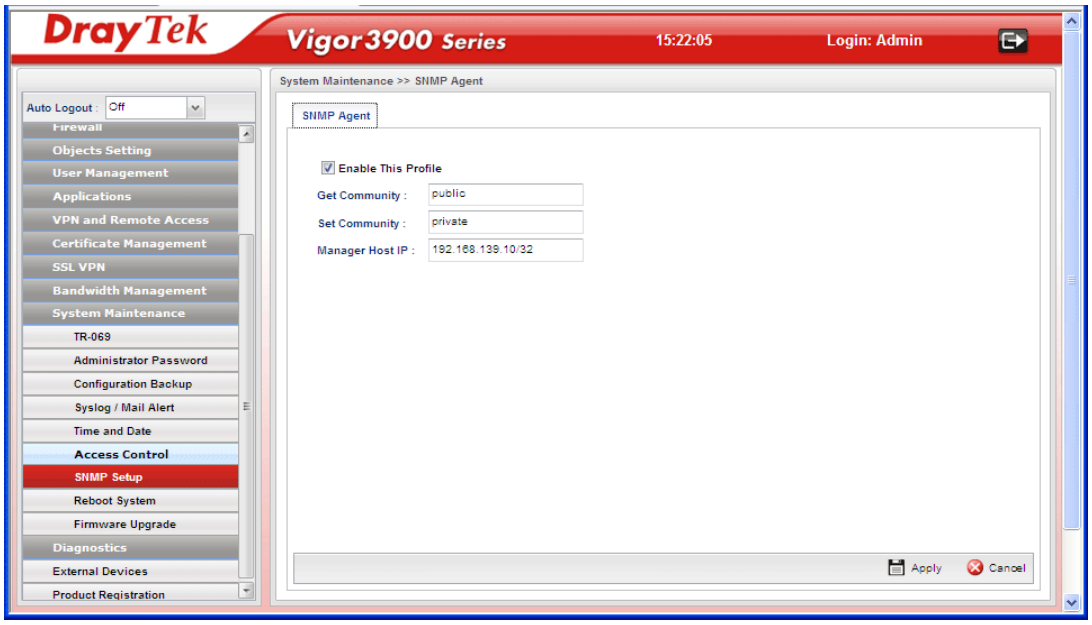
Available parameters are listed as follows:

Item	Description
Web Allow	Click **Enable** to allow system administrator to login from the Internet and management the web page of the router.
Web Port	Type the port number for the management through web page.
Telnet Allow	Click **Enable** to allow system administrator to login from the telnet and management the web page of the router.
Telnet Port	Type the port number for the management through telnet page.
SSH Allow	Click **Enable** to allow system administrator to login from the SSH server and management the web page of the router.
SSH Port	Type the port number for the management through SSH server.
HTTPS Allow	Click **Enable** to allow system administrator to login from the HTTPS server and management the web page of the router.
HTTPS Port	Type the port number for the management through HTTPS server.
User Define	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.
Allowed IP1 - Allowed IP3	Type the first IP address for the system administrator to login. The former box indicates an 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.
Allow Ping form LAN	Click **Enable** to allow system administrator to ping the router from LAN interface.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

4.12.7 SNMP Setup

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



Available parameters are listed as follows:

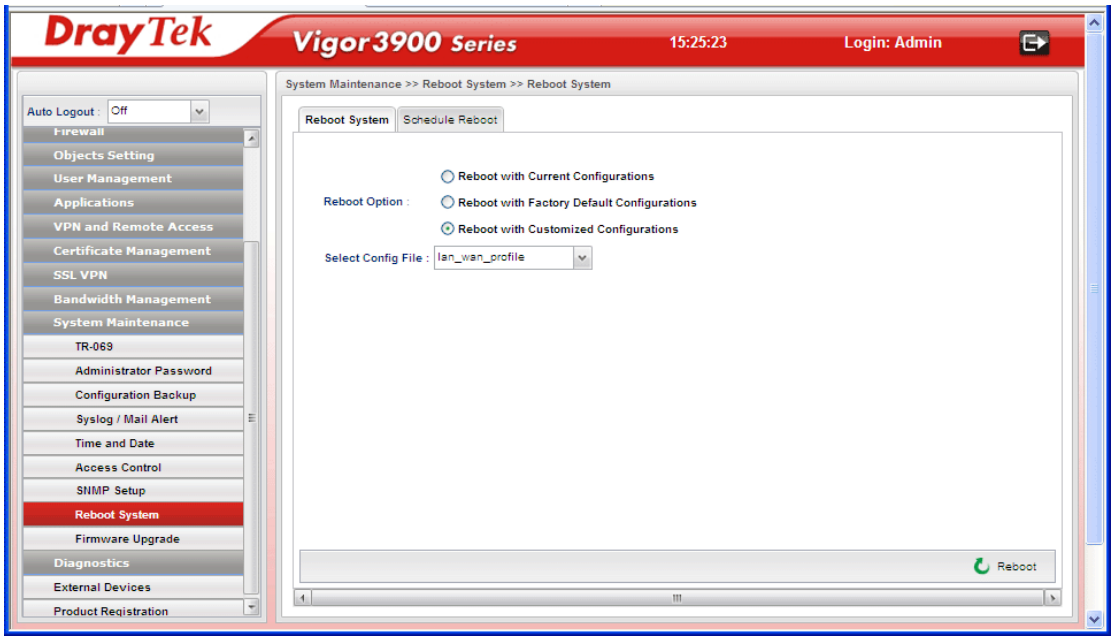
Item	Description
Enable This Profile	Check the box to enable such profile.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**
Set Community	Set community by typing a proper name. The default setting is **private.**
Manager Host IP	Type the IP address for the **manager host.**
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

4.12.8 Reboot System

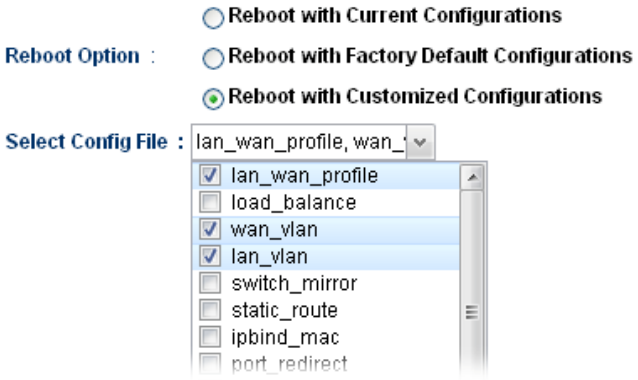
The Vigor router system can be restarted from a Web browser. You have to reboot the router to invoke the configured settings that you made before.

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.

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



Available parameters are listed as follows:

Item	Description
Reboot with Current Configurations	Click it to reboot the router using the current configuration. Then, click **Reboot**..
Reboot with Factory Default Configurations	Click it to reset the router settings to default values. Then, click **Reboot**.
Reboot with Customized Configurations	Click it to reboot the router using the current configuration (only the configuration settings listed and selected below). If you choose this option, **Select Config File** will be available for you to select. 

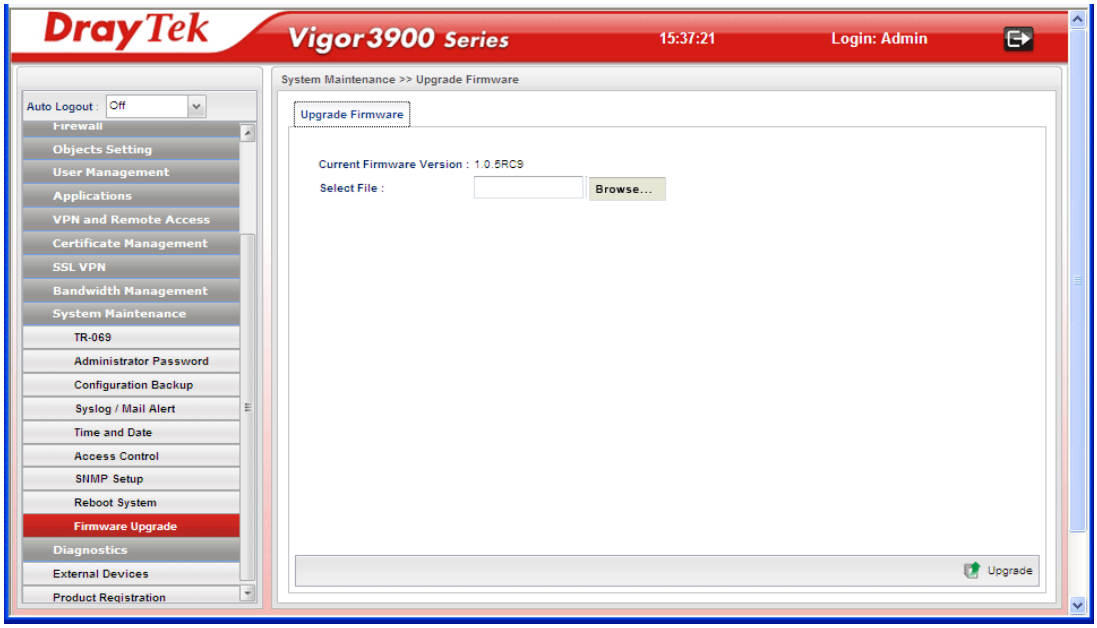
	After choosing the configuration files, click **Reboot**.
Reboot	Click this button to execute the rebooting job.

4.12.9 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 FTP site is ftp.DrayTek.com.

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

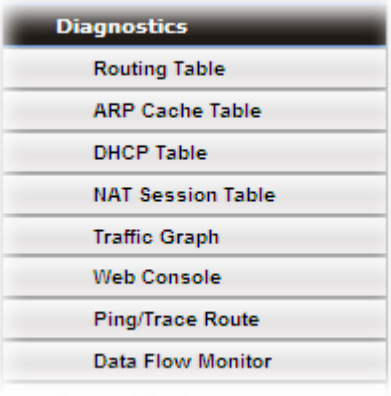


Available parameters are listed as follows:

Item	Description
Current Firmware Version	Display current version of the firmware.
Selected File	Use the **Browse..** button to locate and select the new firmware.
Upgrade	Click it to perform the firmware upgrade.

4.13 Diagnostics

In some cases, a user may need to know some information about the router, such as static or dynamic databases, or other routing information. The Vigor3900 supports five functions, **Routing Table**, **ARP Cache Table**, **DHCP Assignment Table**, **NAT Sessions Table** and **Traffic Graph** for the user to review such information.

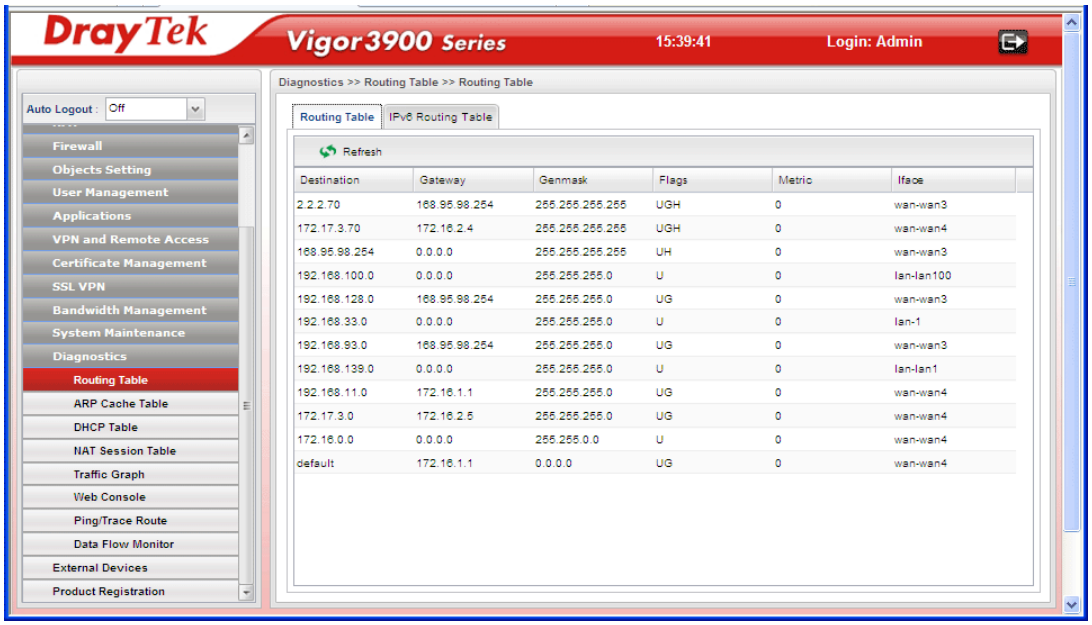


4.13.1 Routing Table

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

Routing Table

Display the information for each route.



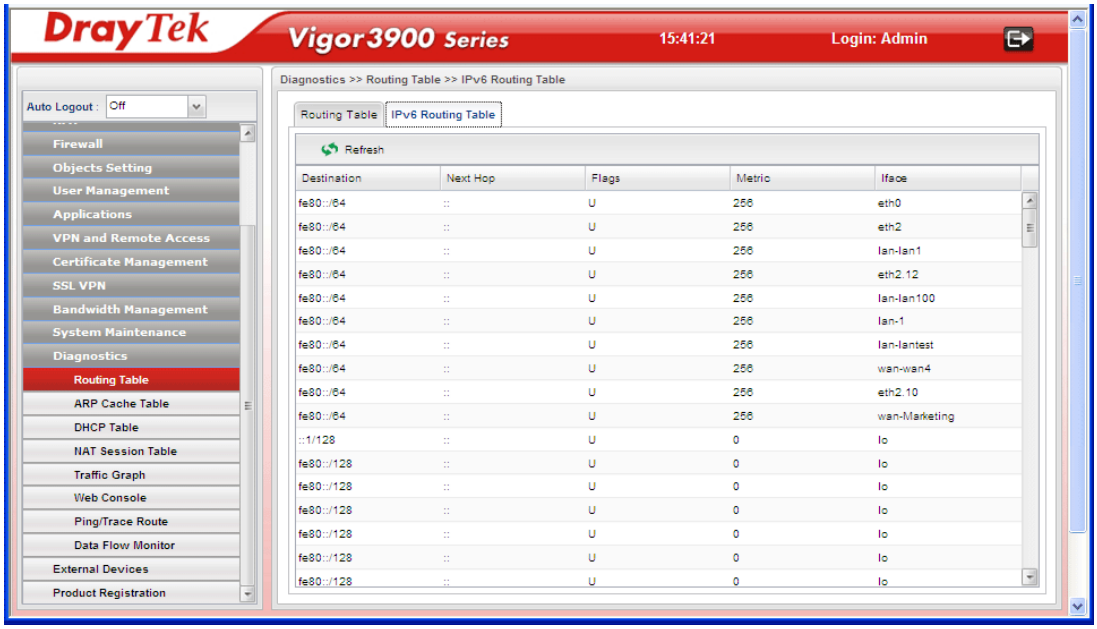
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
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).

IPv6 Routing Table

Display the information for each route with IPv6 protocol.



Each item will be explained as follows:

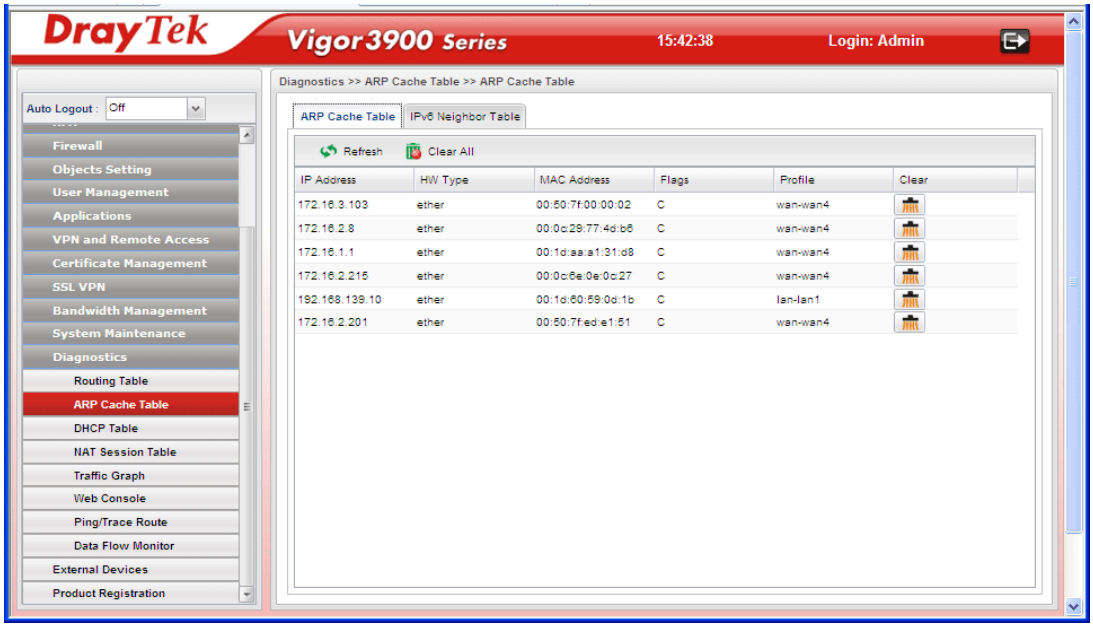
Item	Description
Refresh	Renew the web page.
Destination	Display the destination IP address for various routings.
Next Hop	Display the next hop address for such route ◦
Flags	Display the flag of the routing entry. Possible flags include: U (route is up) H (target is a host) G (use gateway)

	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).

4.13.2 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.

ARP Cache Table

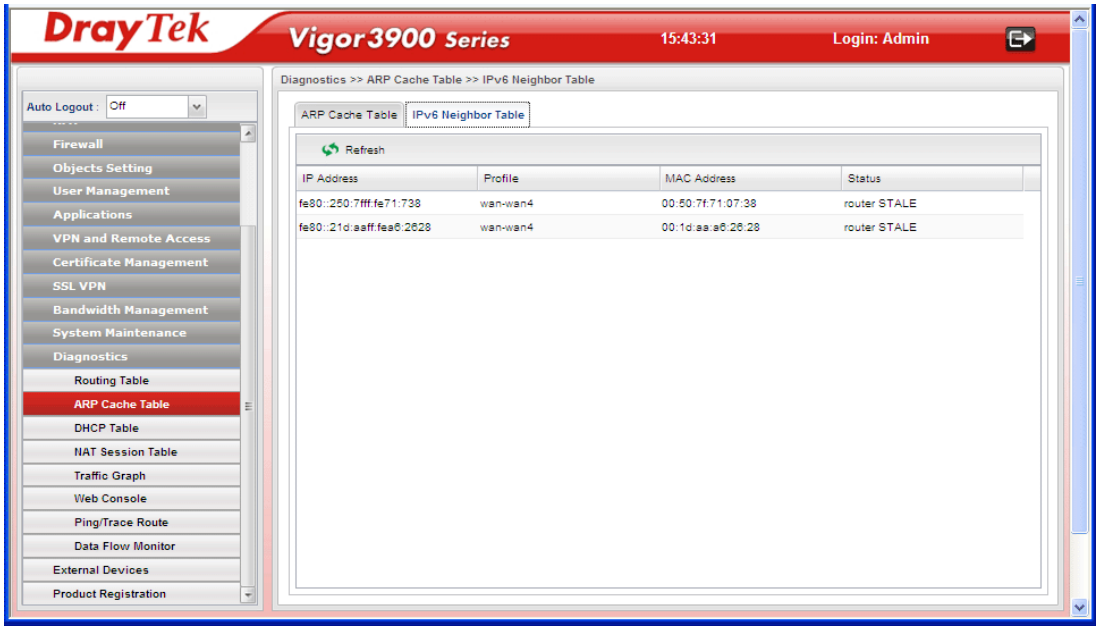


Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Clear All	Remove all of the information from this page.
IP Address	Display the IP address for different ARP cache.
HW type	Display the hardware type of the address from RFC 826.
MAC Address	Display the MAC address for different ARP cache.
Flags	Each complete entry in the ARP cache will be marked with the flag of 0x2. Permanent entries are marked with 0x4 and published entries have the 0x8 flag.
Profile	Display the direction of such route represented with

Item	Description
	LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).
Clear	Delete the selected profile.

IPv6 Neighbor Table



Each item will be explained as follows:

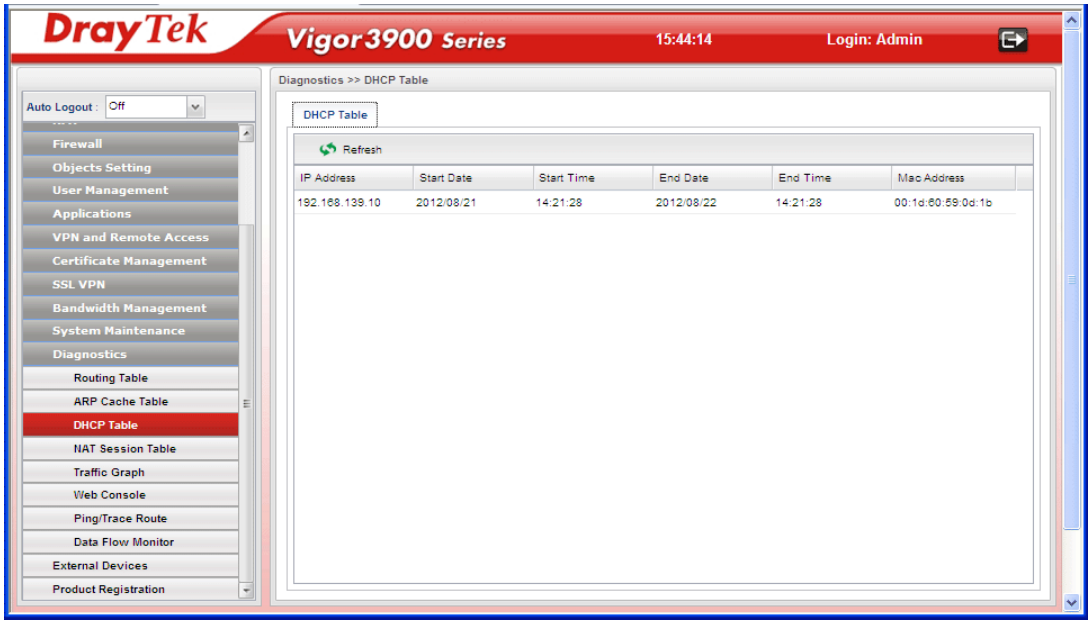
Item	Description
Refresh	Renew the web page.
IP Address	Display the IPv6 address of the neighbor.
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.
Status	Display the status for such neighbor. **INCOMPLETE** - Address resolution is in progress and the link-layer address of the neighbor has not yet been 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

Item	Description
	reachability.

4.13.3 DHCP Table

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

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

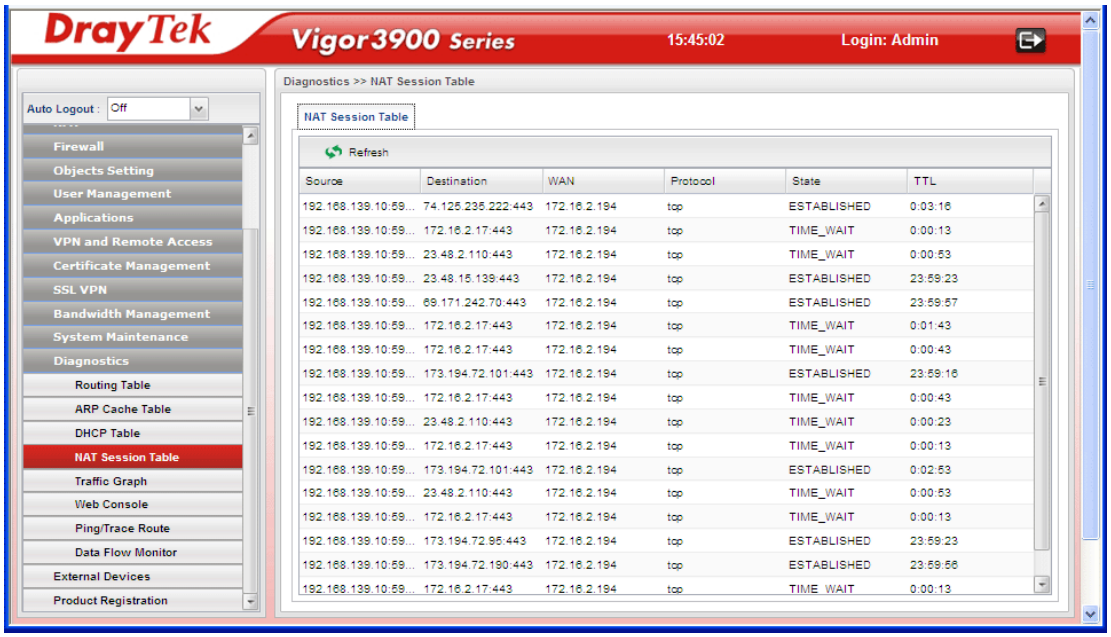


Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
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.

4.13.4 NAT Session Table

This table can display about 30000 sessions with 20 pages.

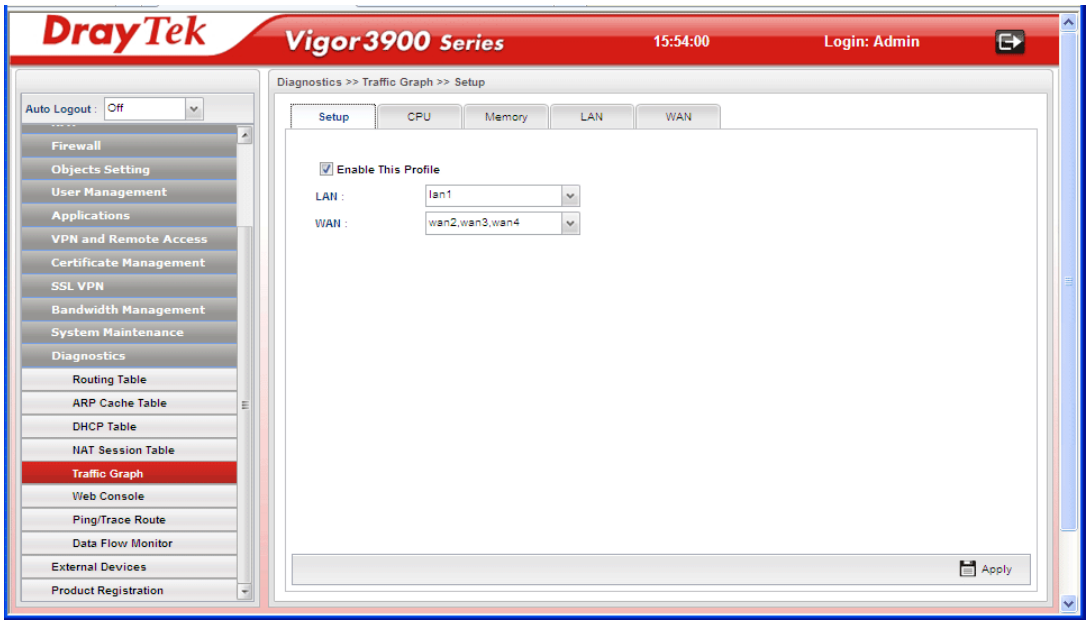


Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Source	Display the source IP address and port of local PC.
Destination	Display the destination IP address and port of remote host.
WAN	Display the WAN IP address of the router.
Protocol	Display the protocol of such NAT session used.
State	Display the actual state of the TCP connection.
TTL	Display how long the conntrack entry has to live.

4.13.5 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Specify LAN and WAN profiles to display corresponding graphs for CPU, Memory, LAN and WAN configurations. Click **Refresh** to renew the graph at any time.

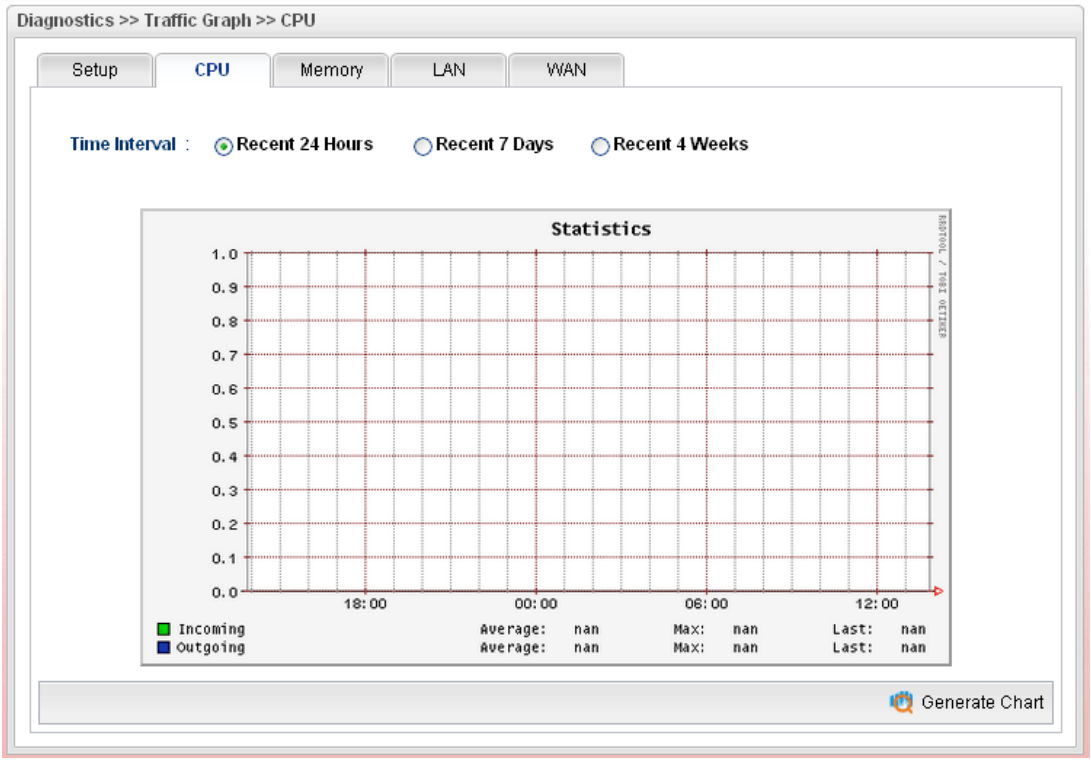


Each item will be explained as follows:

Item	Description
Setup	In this page, simply specify which LAN profile and WAN profile will be applied. The traffic graph will be drawn based on the profiles selected. **Enable This Profile** – 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. 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. **Network Interface** – Display the information of LAN operation.
WAN	Click the WAN tab. 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. **Network Interface** – Display the information of WAN operation.

Below show a graphic for CPU:

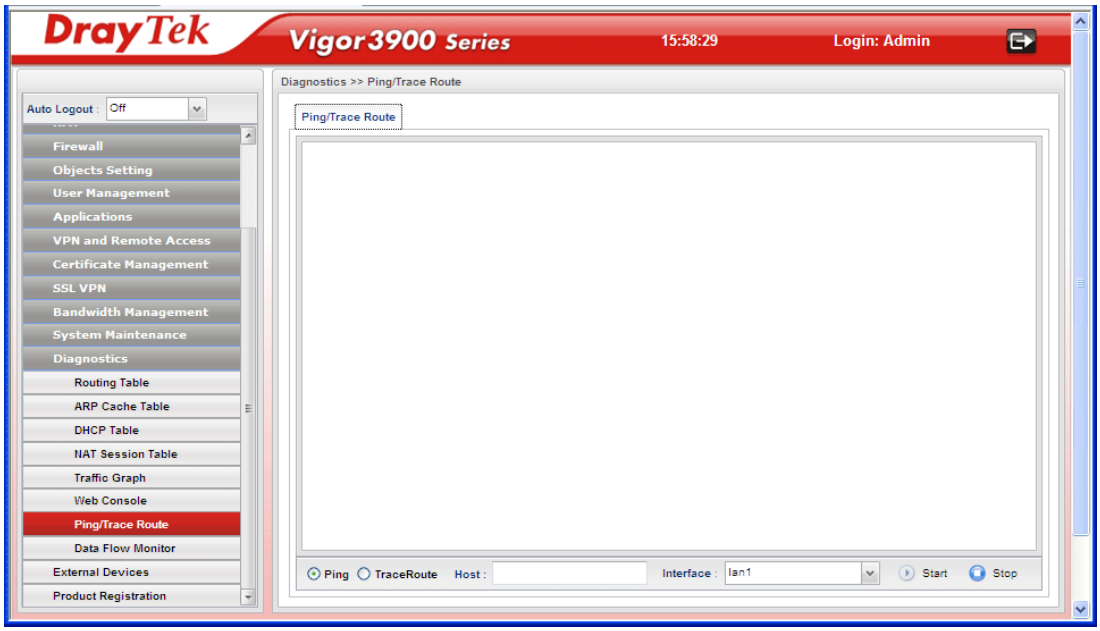


4.13.6 Web Console

Click **Diagnostics** and click **Web Console** to pen the web page for typing commands used in console connection. A remote user can operate Vigor3900 from this web page without installing and opening other connection utility.

4.13.7 Ping/Trace Route

This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

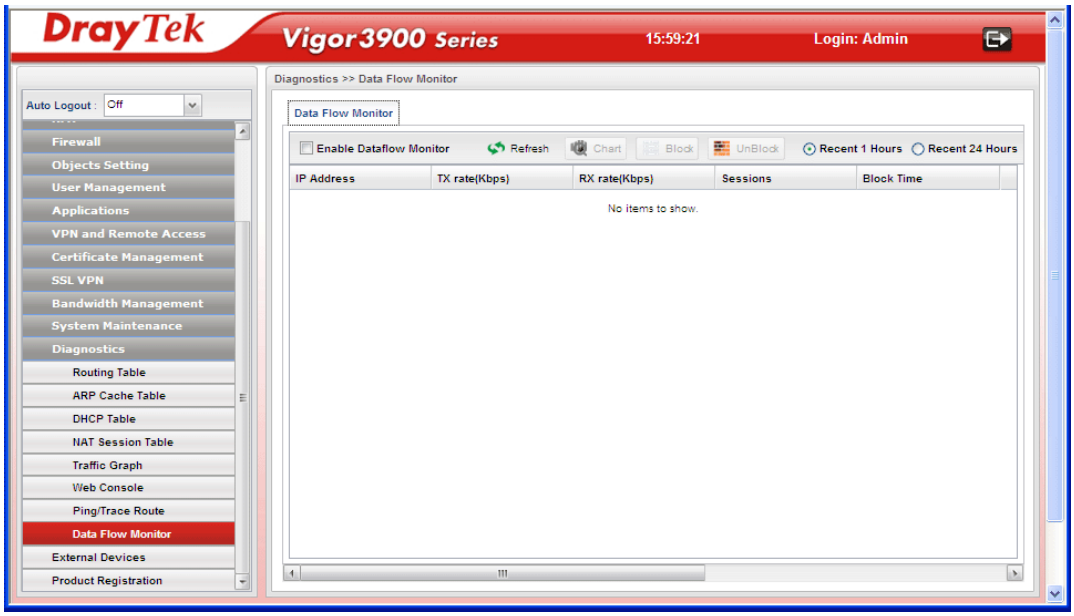


Each item will be explained as follows:

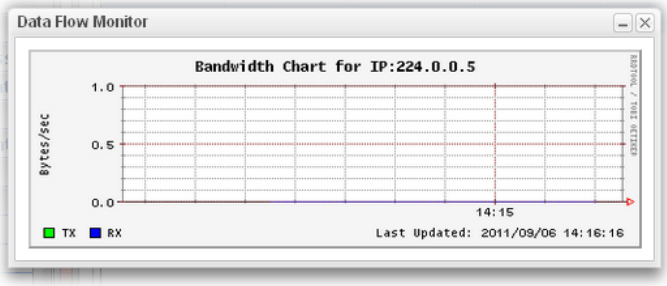
Item	Description
Ping / TraceRoute	Click **Ping** to perform ping function. Click **TraceRoute** to invoke trace router function.
Host	Type the IP address of the host.
Interface	Choose one of the LAN or WAN profile to be applied by such function.
Start	Click it to start the action of Ping or Trace Route.
Stop	Click it to terminate the action of Ping or Trace Route.

4.13.8 Data Flow Monitor

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



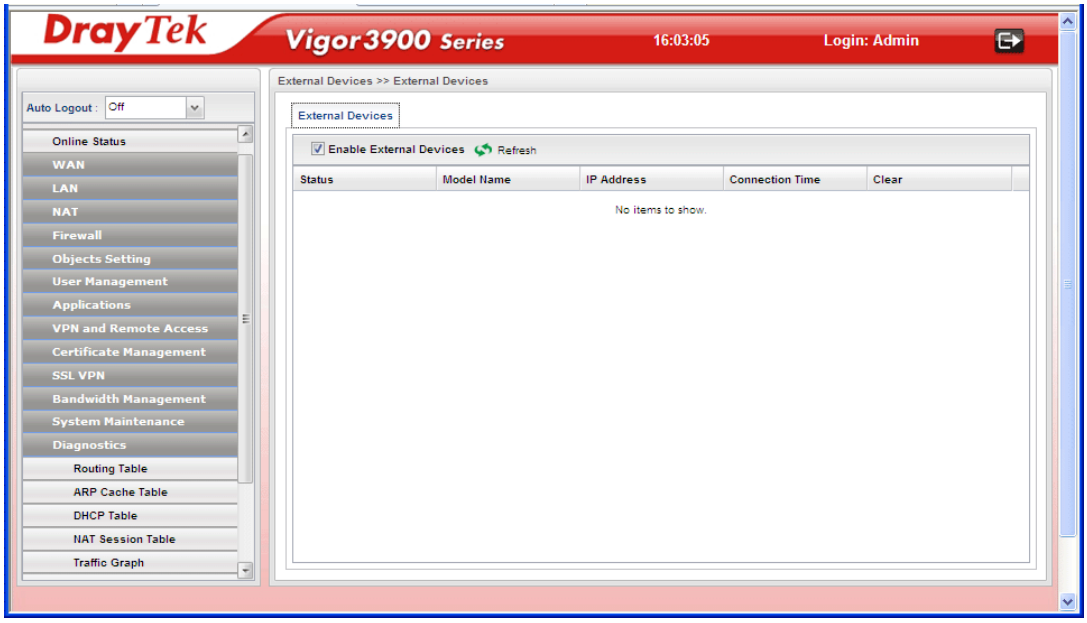
Each item will be explained as follows:

Item	Description
Enable Dataflow Monitor	Check this box to enable dataflow monitor performed by the router.
Refresh	Click it to renew the web page.
Chart	Click this button to illustrate data chart. Refer to the following figure as an example. 
Block	Prevent the specified PC accessing into Internet within 5 minutes.
UnBlock	Allow the specified PC accessing into Internet within 5 minutes.
Recent 1 Hour/ Recent 24 Hours / Recent 7 Days	Display the records with 1 hour/24 hours/7 days recently.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.

Item	Description
Enable Dataflow Monitor	Check this box to enable dataflow monitor performed by the router.
IP Address	Display the IP address of the monitored device.
TX rate (KBps)	Display the transmission speed of the monitored device.
RX rate (KBps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Block Time	Display the time for the duration of the block.

4.14 External Devices

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.



Each item will be explained as follows:

Item	Description
Enable External Devices	Check the box to detect the external device connected to Vigor3900.
Refresh	Click it to renew the web page.
Status	Display
Model Name	Display the model name of the external product.
IP Address	Display the IP address of the external product.
Connection Time	Display the connection time that the external product connecting to Vigor3900.
Clear	Allow to delete the selected profile.

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.

4.15 Product Registration

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

This page is left blank.

Chapter 5: Trouble Shooting

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

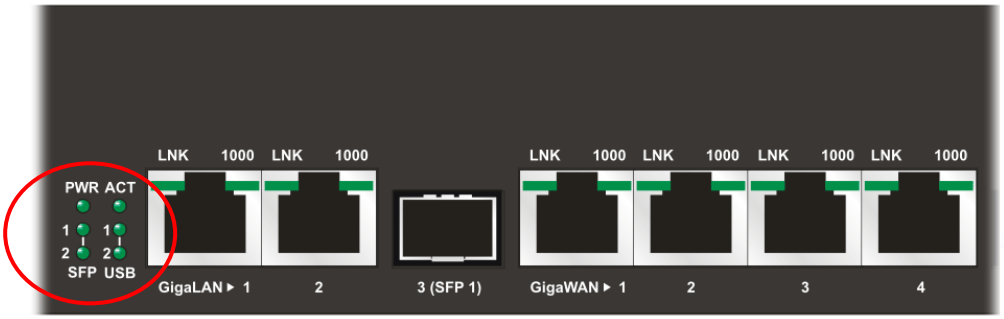
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check if the power line and WLAN/LAN cable connections is OK.
   If not, refer to "**1.3 Hardware Installation"** for reconnection.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

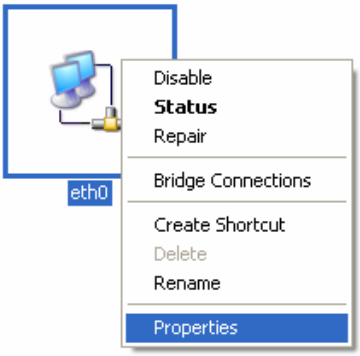
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

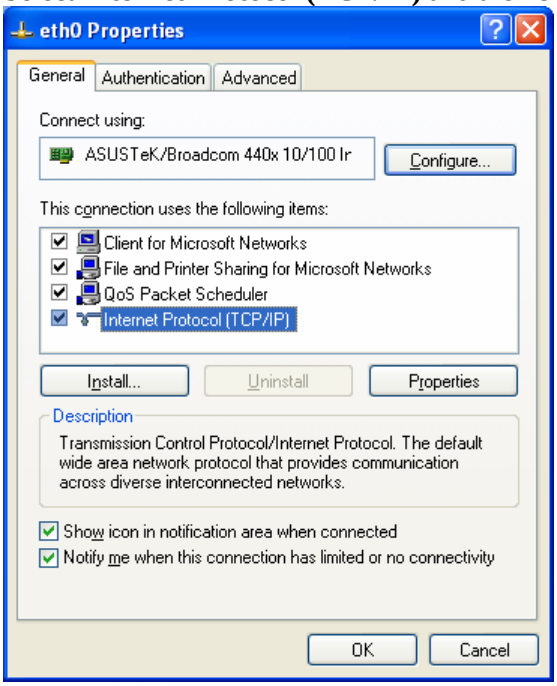
> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.

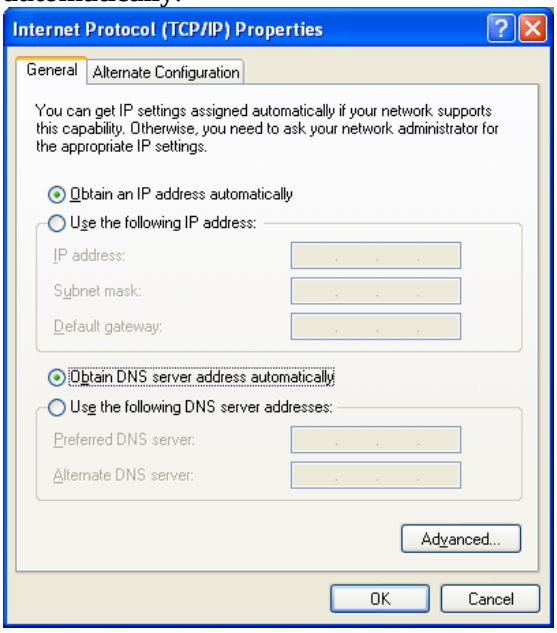
2. Right-click on **Local Area Connection** and click on **Properties**.



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

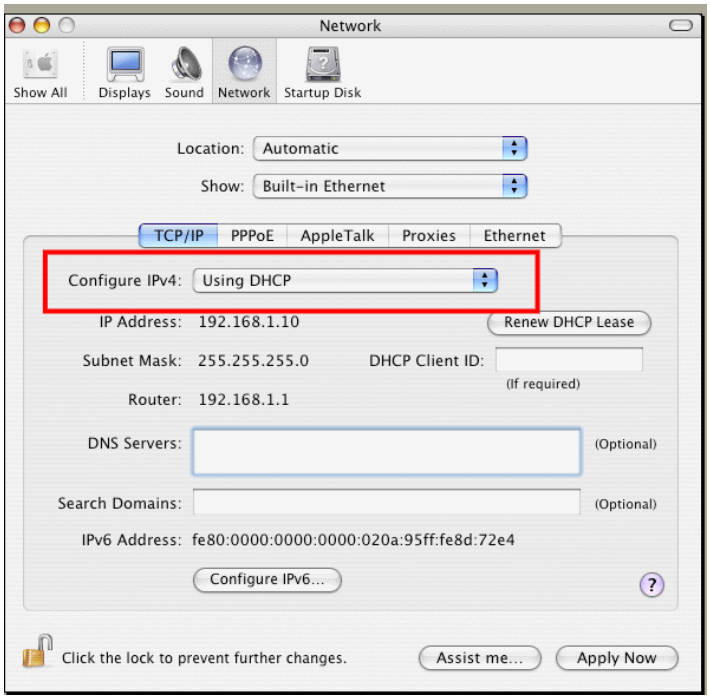


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For Mac OS

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



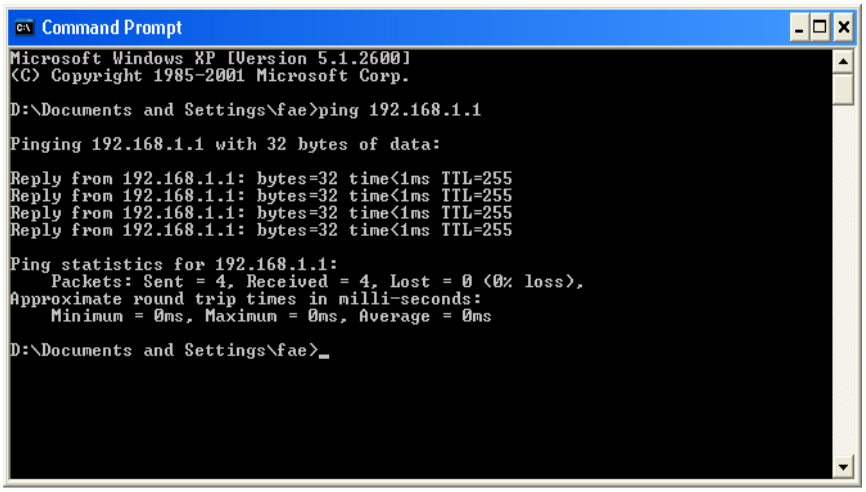
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

For Windows

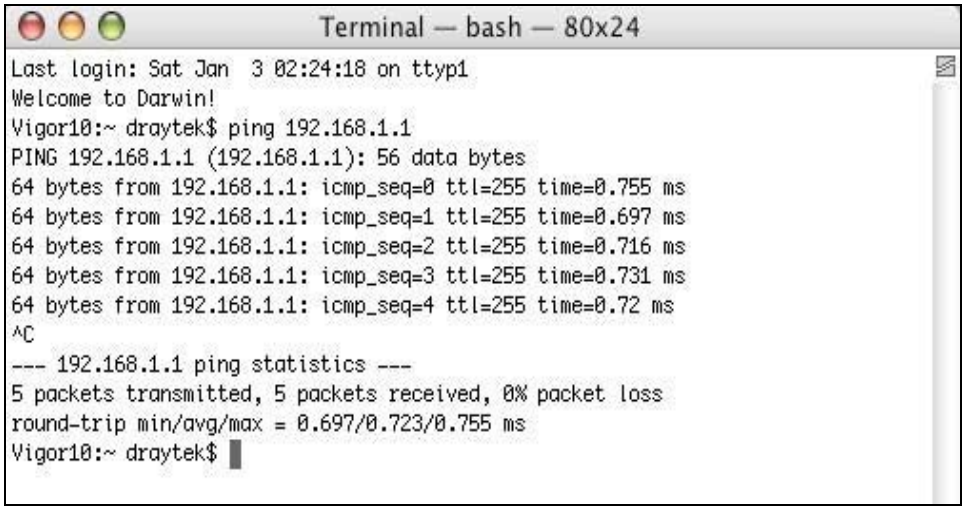
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

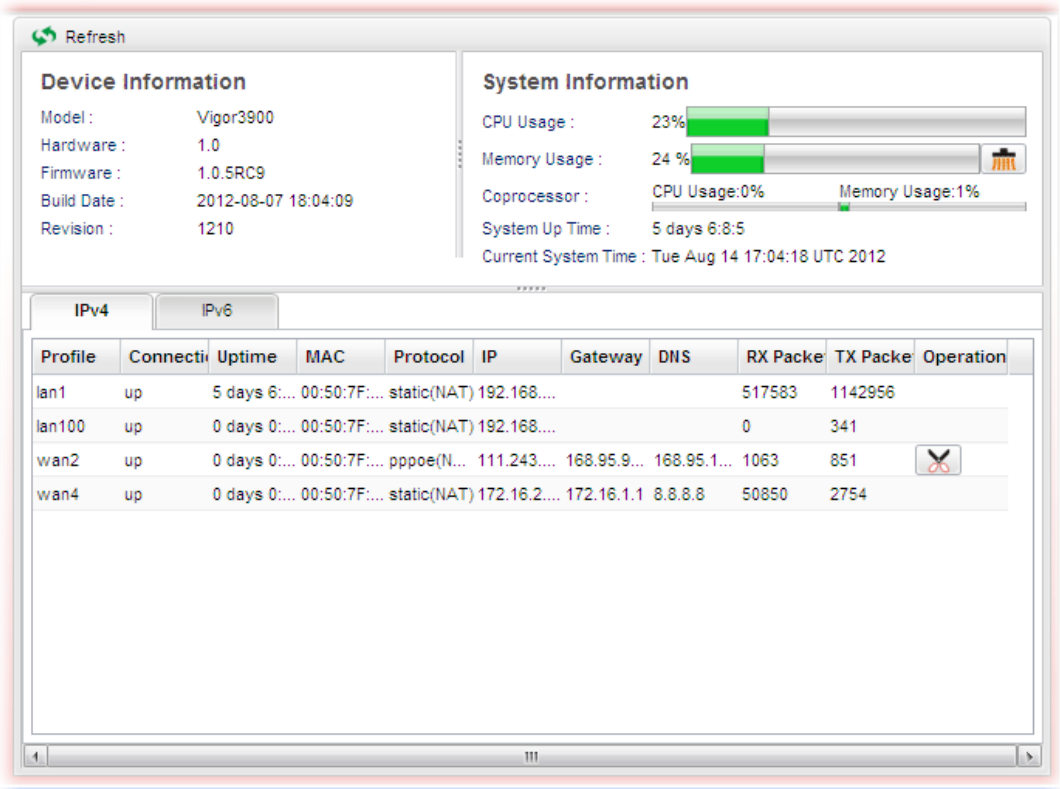
For Mac OS (Terminal)

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.



5.4 Checking If the ISP Settings are OK or Not

Open Online Status to check current network status. Be careful to check if the settings coming from your ISP have been typed correctly or not.



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

5.5 Backing to Factory Default Setting If Necessary

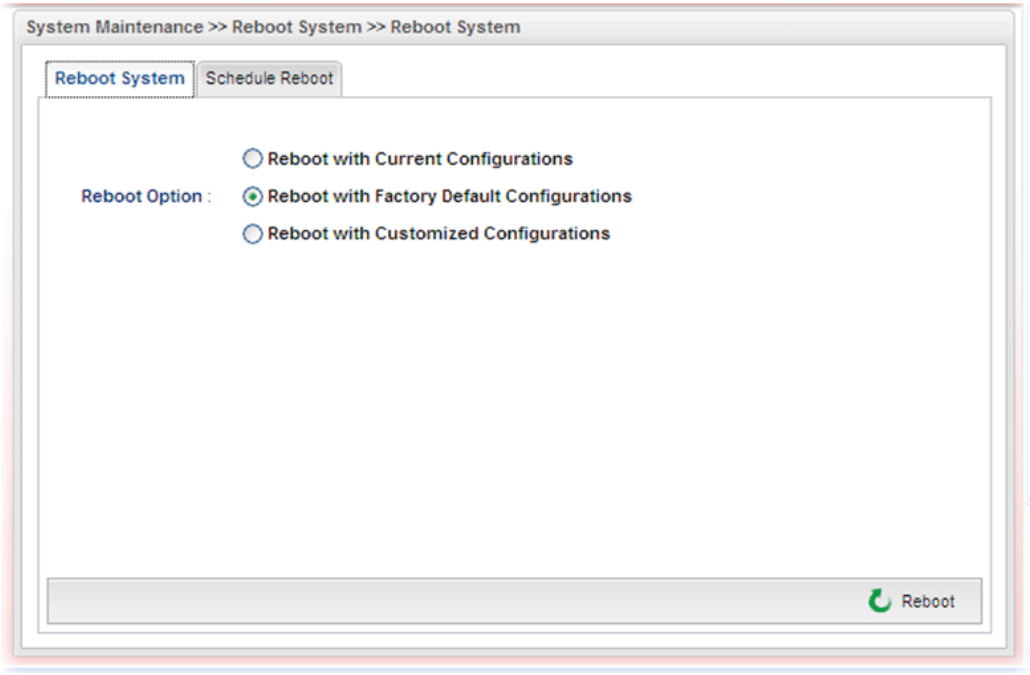
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of the factory default is null.

Software Reset

You can reset router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Reboot with Factory Default Configuration** and click **Reboot**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the ACT LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.

After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.6 Contacting Your Dealer

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**.