DrayTek

Vigor3900

Multi-WAN Security Appliance

Providing Productivity and Security for
Small, Medium and Large Businesses

Your reliable networking solutions partner

User's Guide

TAIWAN
EXCELLENCE
2012

V1.8

Vigor3900
Multi-WAN Security Appliance
User's Guide

Version: 1.8

Firmware Version: V1.0.8

(For future update, please visit DrayTek website)

Date: March 27, 2014

Copyright Information

Copyright Declarations

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

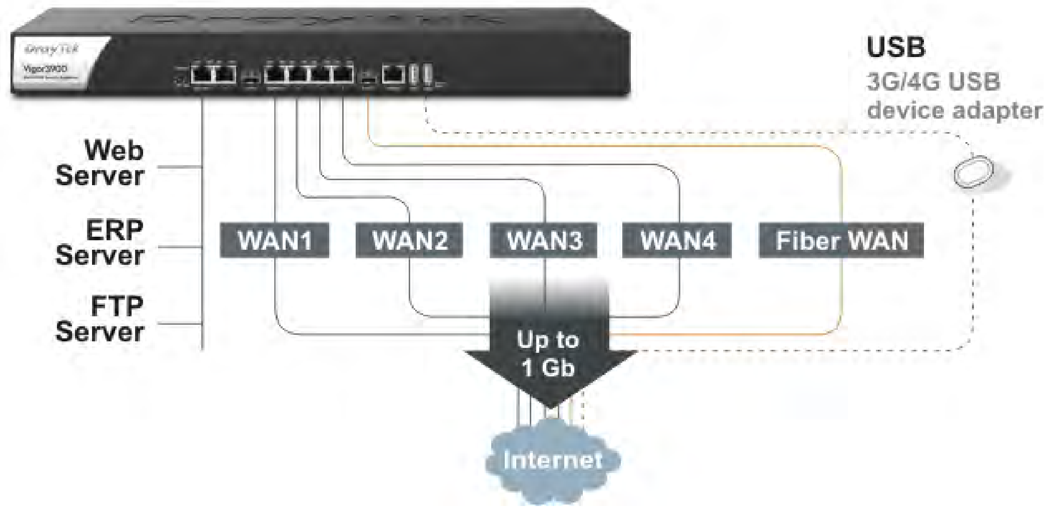
(2) This device may accept any interference received, including interference that may cause undesired operation.

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

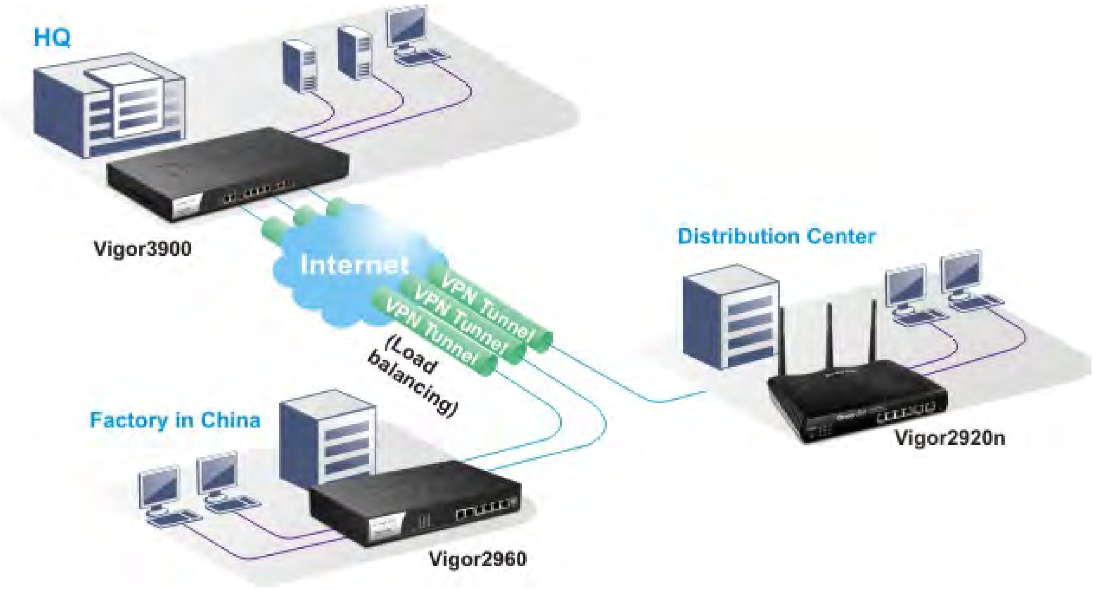
Table of Contents

Chapter 1: Introduction

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:

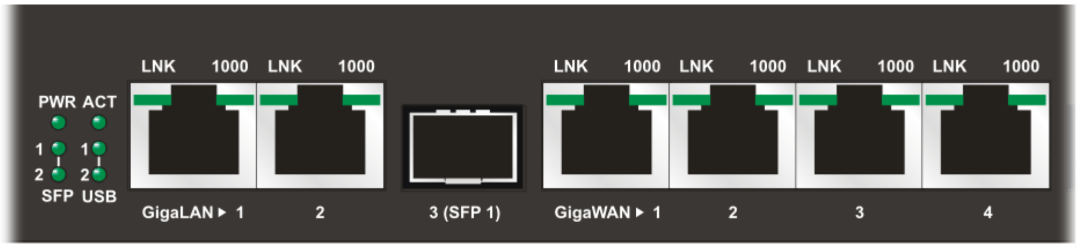
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

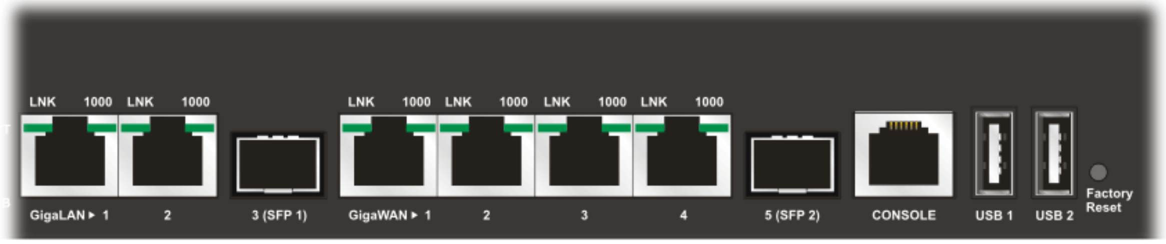
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

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.

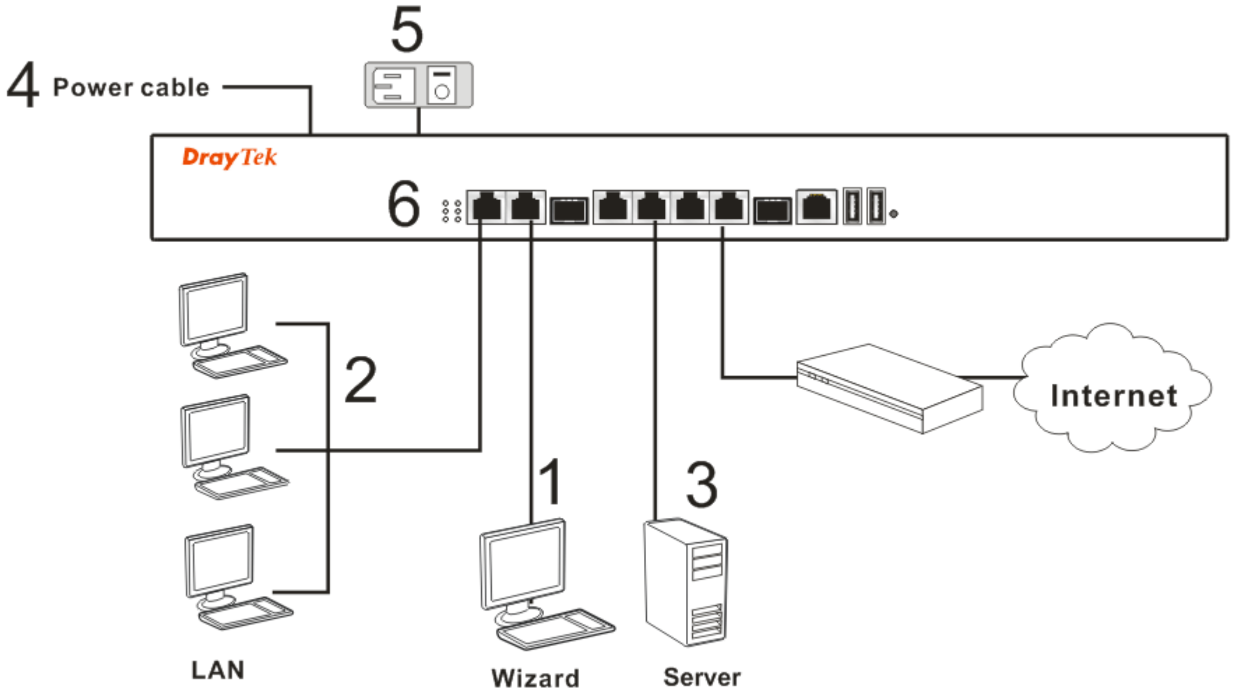
1.3 Hardware Installation

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.

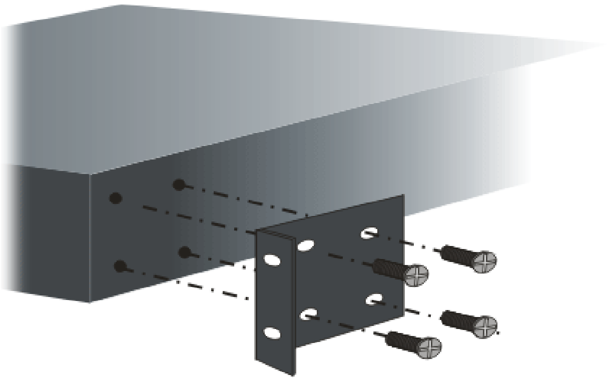
Below shows an outline of the hardware installation for your reference.



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.

DrayTek
Vigor3900
Multi-WAN Security Appliance
CONSOLE

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.

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.

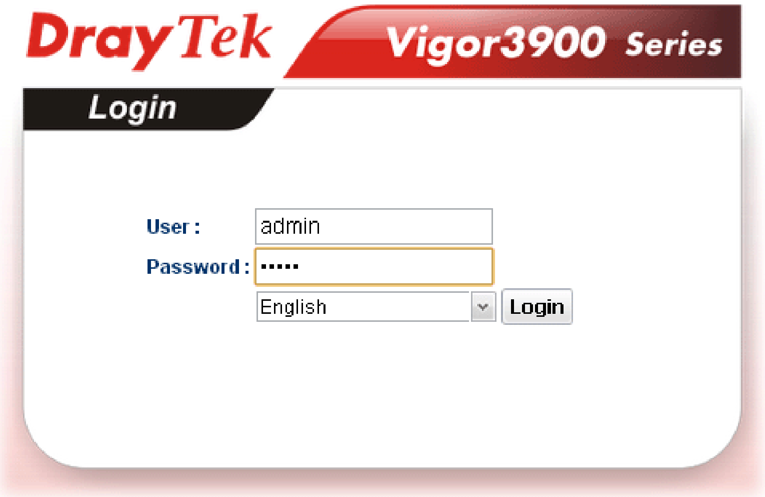
2.1 Changing Password

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.

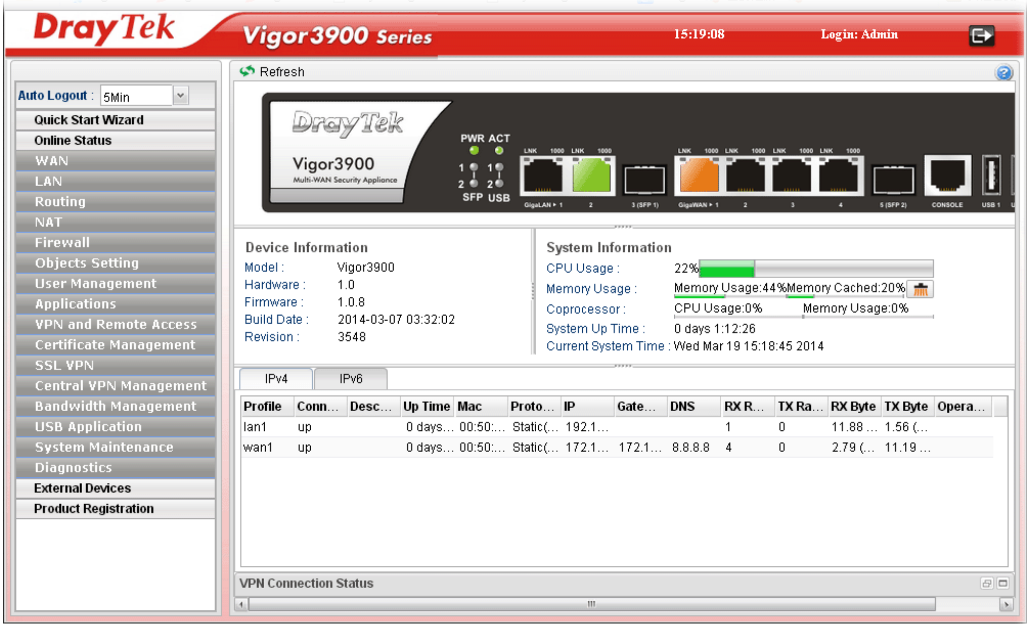
> **Notice:** You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of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



User : admin
Password : •••••
English

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



Device Information

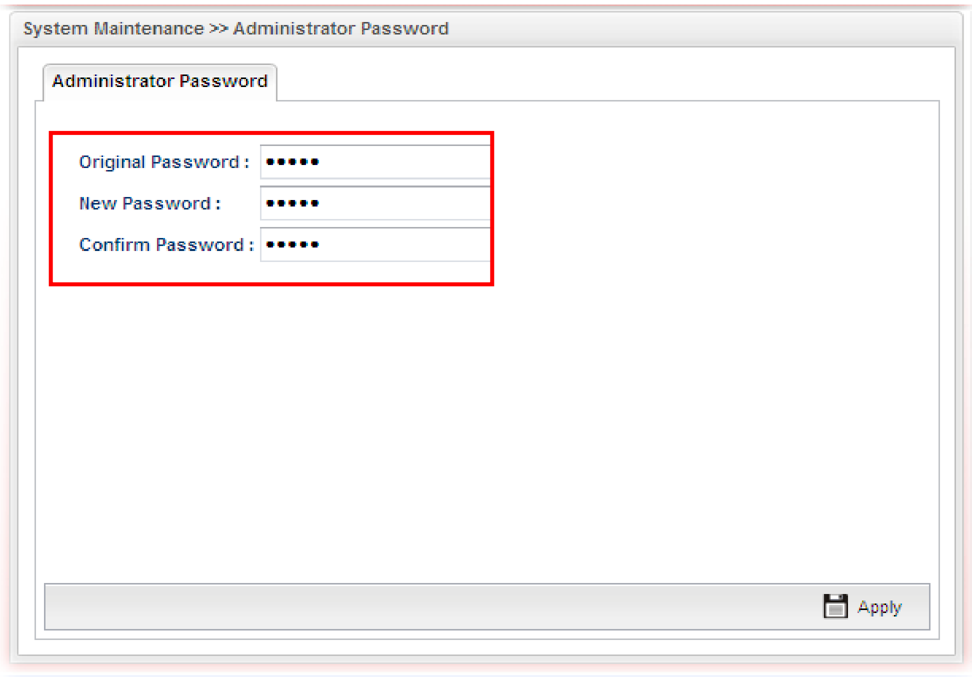
Model : Vigor3900
Hardware : 1.0
Firmware : 1.0.8
Build Date : 2014-03-07 03:32:02
Revision : 3548

System Information

CPU Usage : 22%
Memory Usage : Memory Usage:44% Memory Cached:20%
Coprocessor : CPU Usage:0% Memory Usage:0%
System Up Time : 0 days 1:12:26
Current System Time : Wed Mar 19 15:18:45 2014

Profile	Conn...	Desc...	Up Time	Mac	Proto...	IP	Gate...	DNS	RX R...	TX Ra...	RX Byte	TX Byte	Opera...
lan1	up		0 days...	00:50:...	Static(...	192.1...			1	0	11.88 ...	1.56 (...	
wan1	up		0 days...	00:50:...	Static(...	172.1...	172.1...	8.8.8.8	4	0	2.79 (...	11.19 ...	

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



Original Password : •••••
New Password : •••••
Confirm Password : •••••

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

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

2.2 Quick Start Wizard

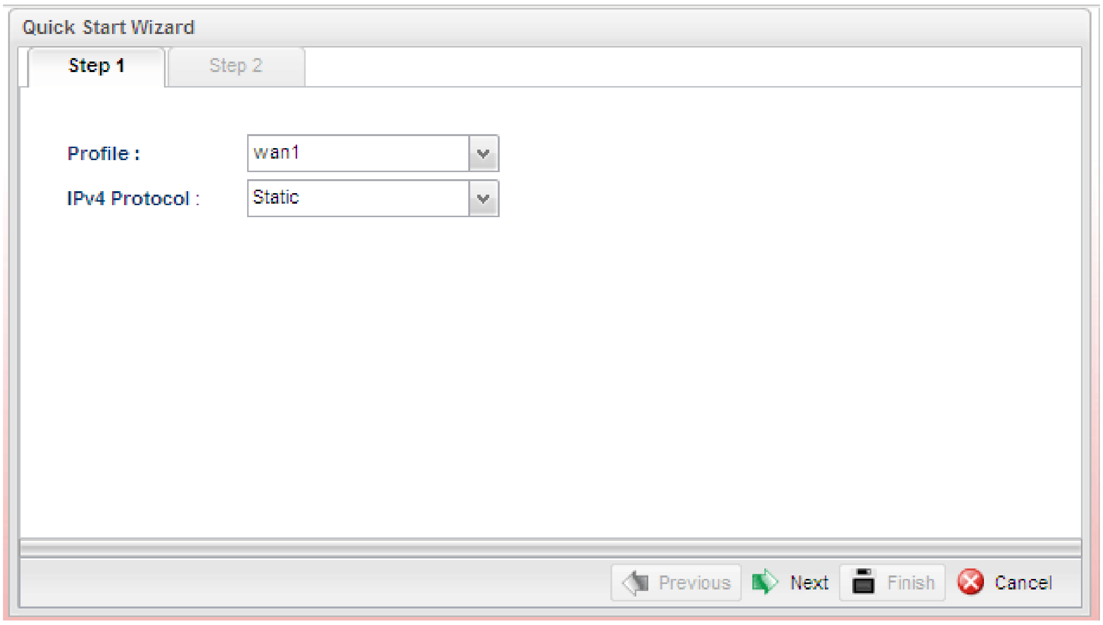
Quick Start Wizard is a wizard which is designed for configuring your router accessing Internet with simply steps. In the **Quick Start Wizard** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes.

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

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

2.2.1 Step 1 - Specifying the WAN Profile

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

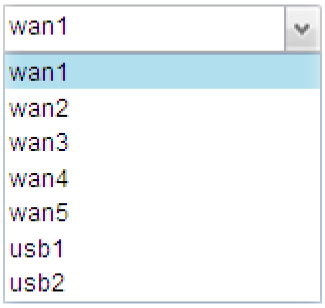


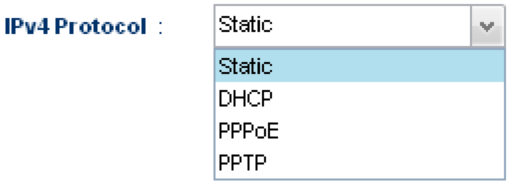
Quick Start Wizard

Profile : wan1

IPv4 Protocol : Static

Available settings are explained as follows:

Item	Description
Profile	Use the drop down list to choose one WAN profile.  wan1 wan1 wan2 wan3 wan4 wan5 usb1 usb2
IPv4 Protocol	Use the drop down list to choose a connection mode for such WAN profile.

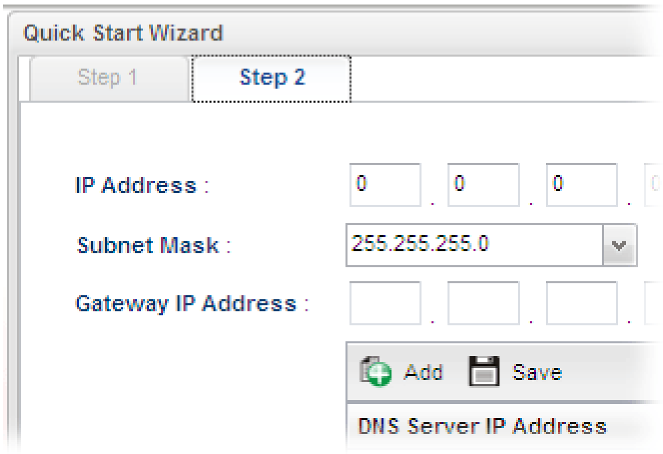
Item	Description
	 IPv4 Protocol : Static Static DHCP PPPoE PPTP **Static -** If **Static** is selected, you can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings. **DHCP -** It allows a user to obtain an IP address automatically from a DHCP 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

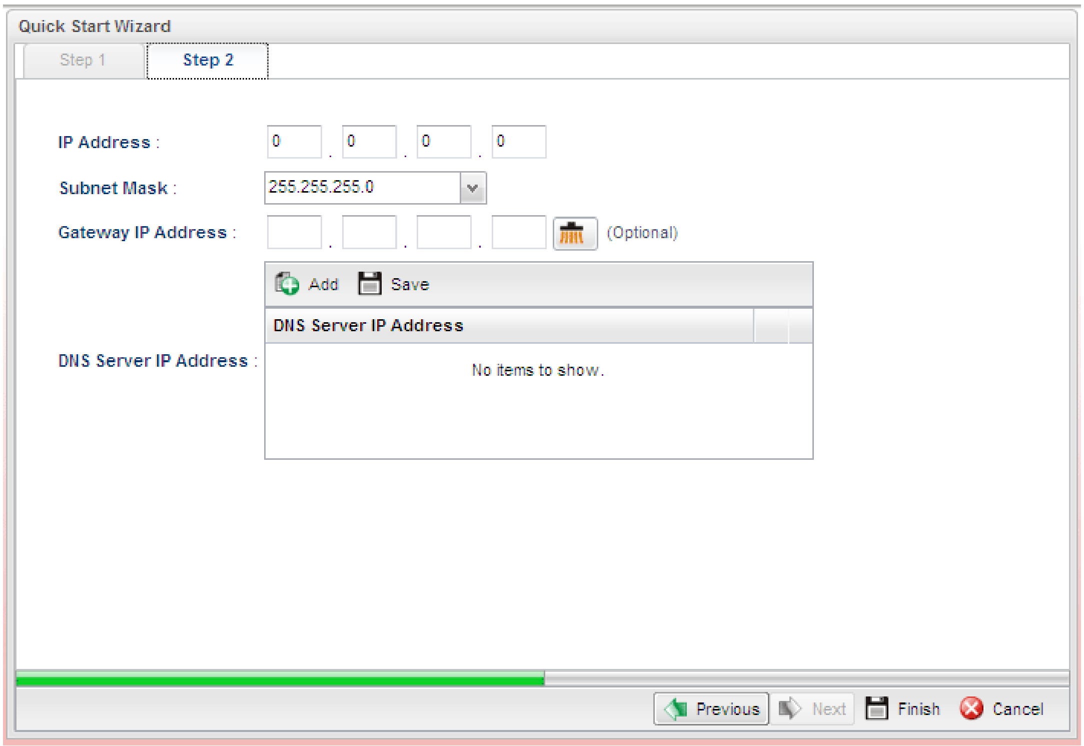
This page will be changed according to the **IPv4 Protocol Type** selected on last page.



IP Address : 0 . 0 . 0 .
Subnet Mask : 255.255.255.0
Gateway IP Address :

If Static is selected

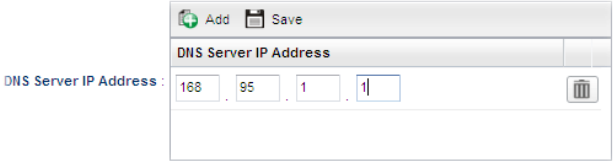
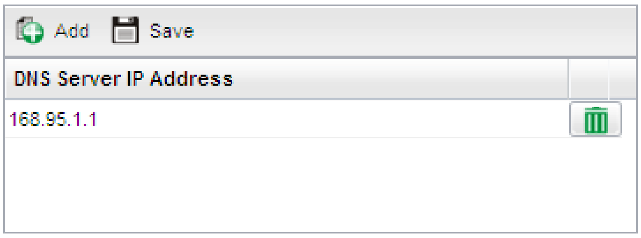
If **Static** is selected, the following screen will appear. You can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings.



IP Address : 0 . 0 . 0 . 0
Subnet Mask : 255.255.255.0
Gateway IP Address : . . . (Optional)
DNS Server IP Address : No items to show.

Available parameters are listed as follows:

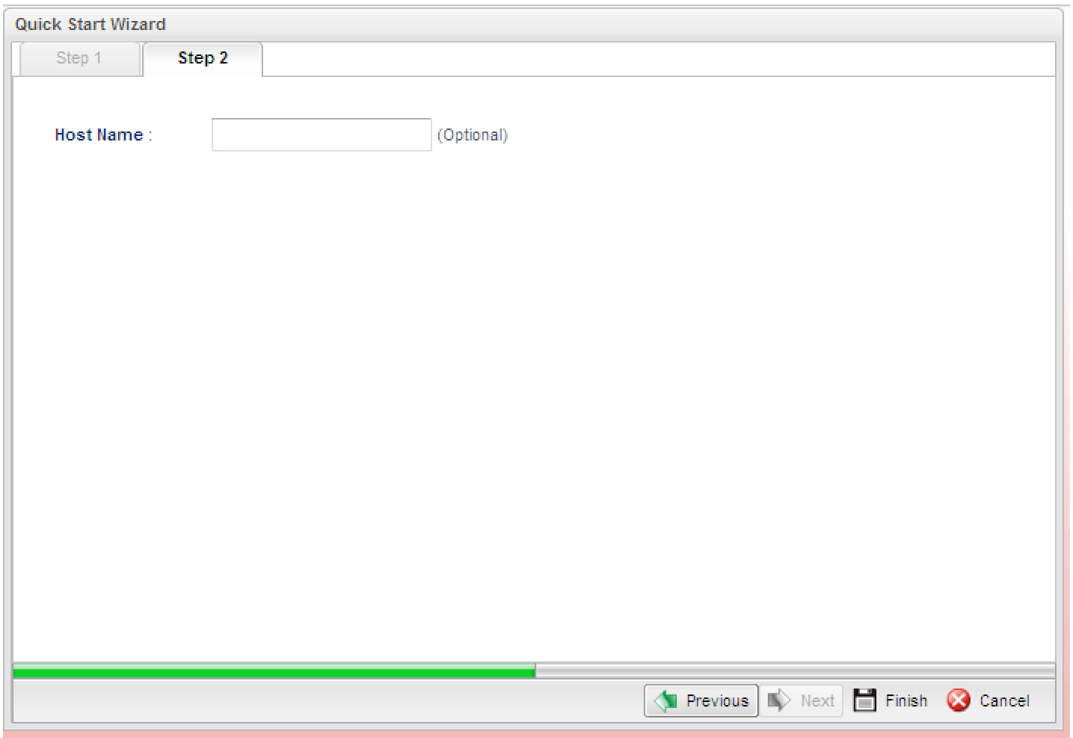
Item	Description
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile. - click it to remove the IP address if you are not satisfied with it.

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.  DNS Server IP Address : 168 . 95 . 1 . 1 **Save** – After finished the IP address configuration, click Save to save the setting onto the router.  168.95.1.1 🗑 – Click the icon to remove the selected entry.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

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

If DHCP is selected

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



Host Name : (Optional)

Available parameters are listed as follows:

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

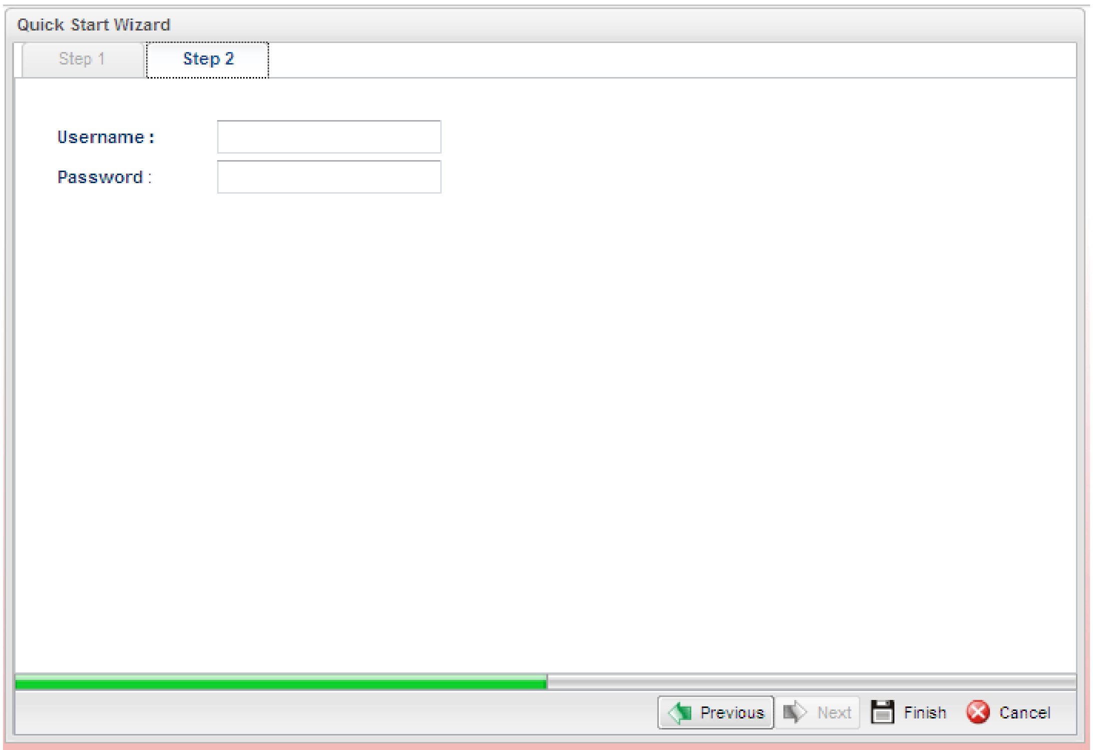
When you finished the above settings, please click **Finish**.

If PPPoE is selected

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

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

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



Quick Start Wizard

Step 1 | Step 2

Username :

Password :

Available parameters are listed as follows:

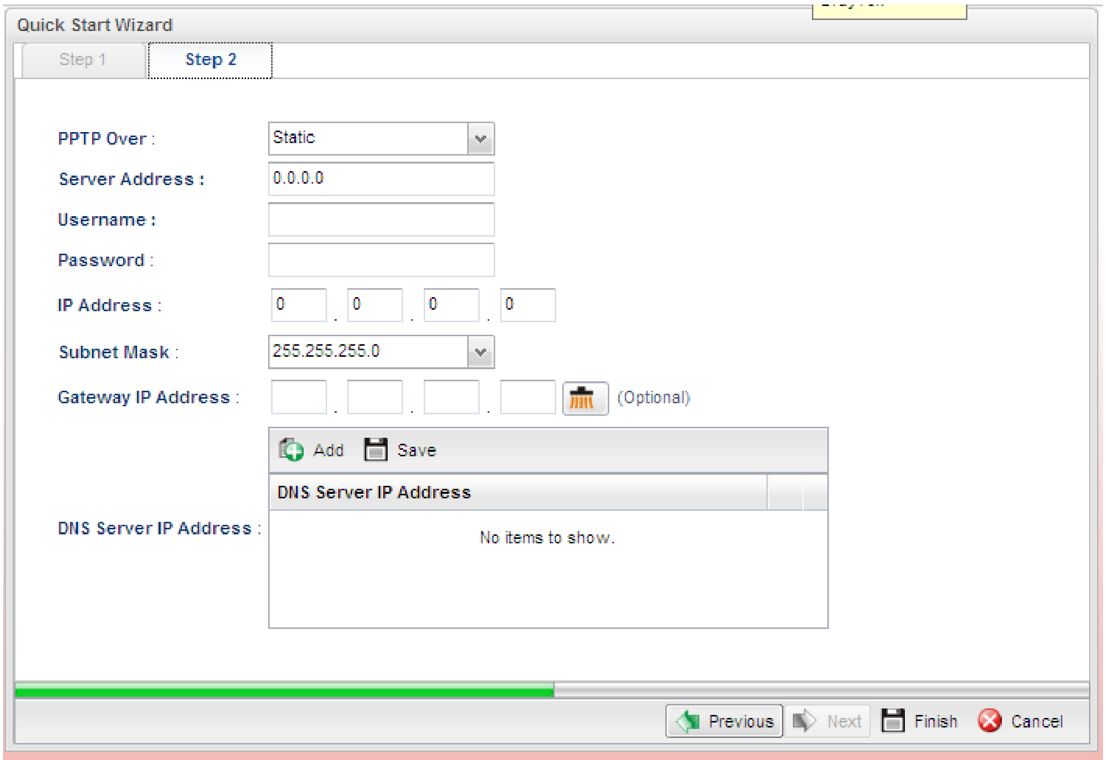
Item	Description
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

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

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.



PPTP Over : Static

Server Address : 0.0.0.0

Username :

Password :

IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255.255.255.0

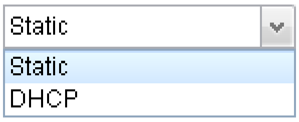
Gateway IP Address : . . . (Optional)

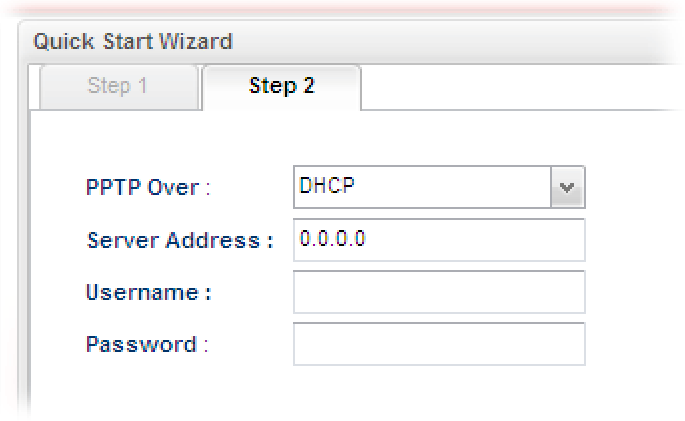
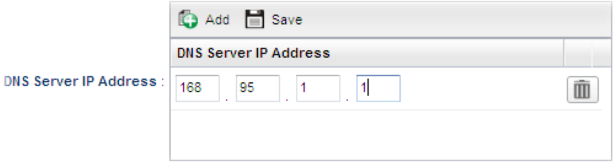
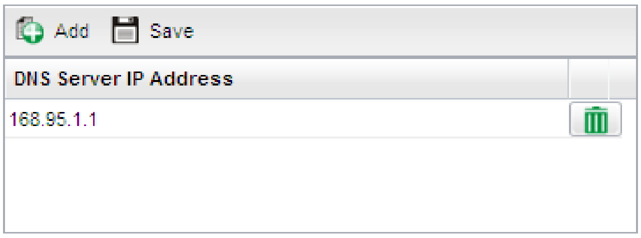
DNS Server IP Address :

DNS Server IP Address

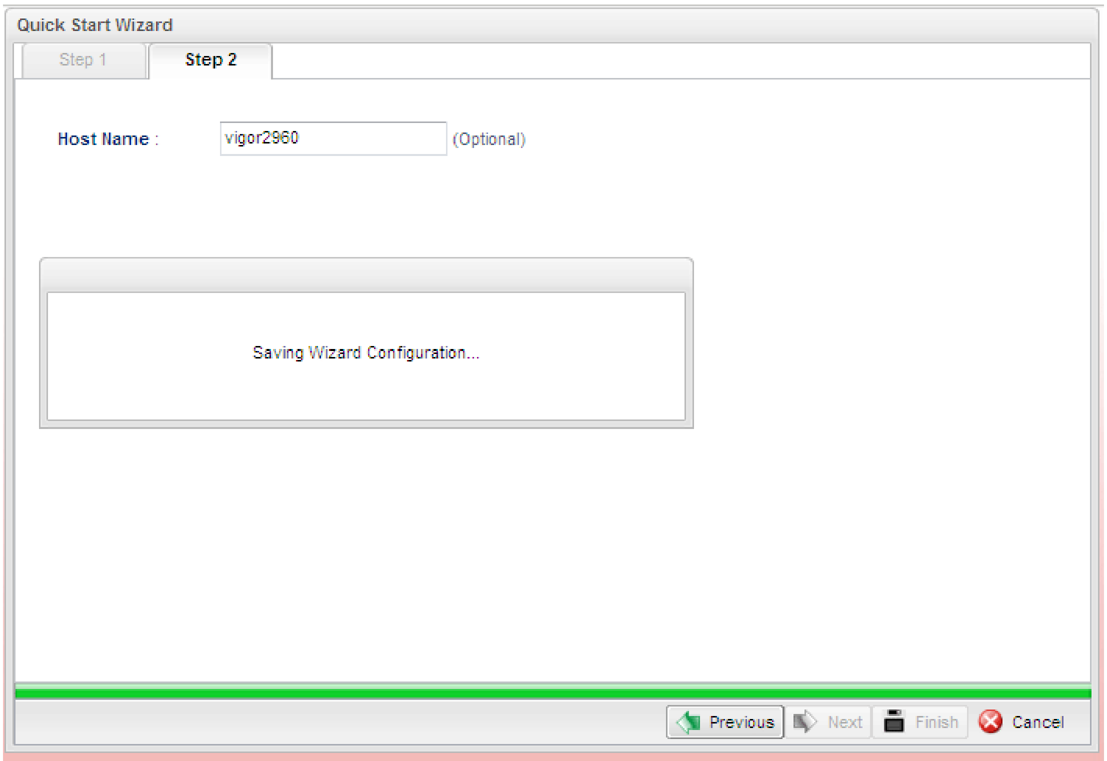
No items to show.

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 Static DHCP **Static** – specify the IP address. **DHCP** - obtain the IP address automatically.

	 Quick Start Wizard Step 1 / Step 2 PPTP Over : DHCP Server Address : 0.0.0.0 Username : Password :
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 Save DNS Server IP Address : 168 . 95 . 1 . 1 **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.  Add Save DNS Server IP Address 168.95.1.1 🗑 – Click the icon to remove the selected entry.
Previous	Click it to return to previous setting page.
Finish	Click it to finish the configuration.
Cancel	Click it to discard the settings configured in this page.

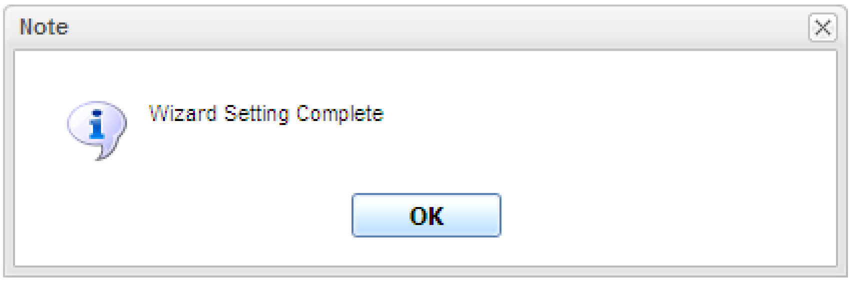
When you finished the above settings, please click **Finish**. Later, you can surf the Internet at any time.



Host Name : vigor2960 (Optional)

Saving Wizard Configuration...

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

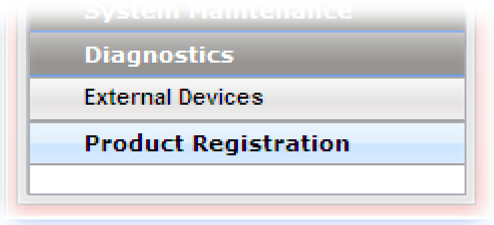


Wizard Setting Complete

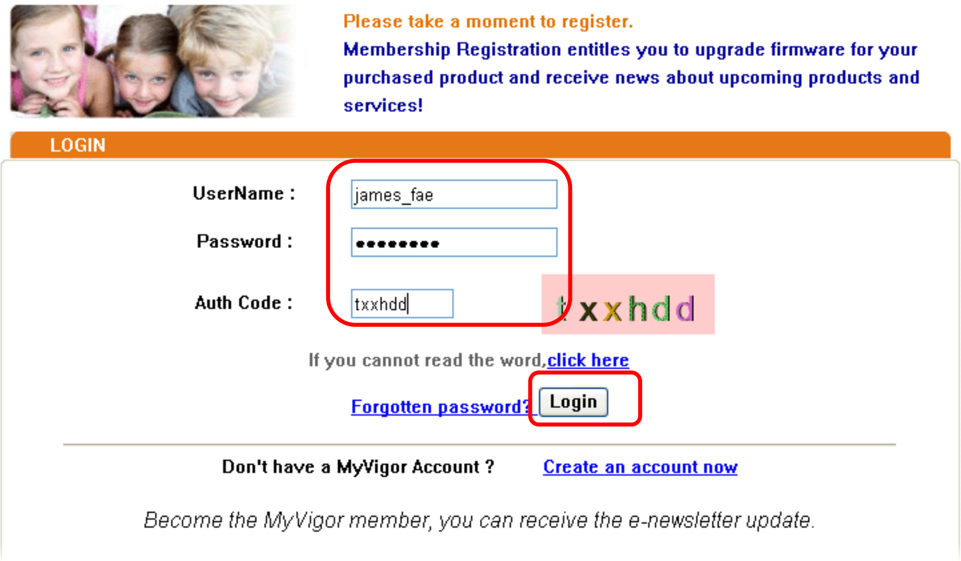
2.3 Register Vigor Router

Please follow the steps below to register the router.

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



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


Please take a moment to register.

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

LOGIN

UserName : james_fae

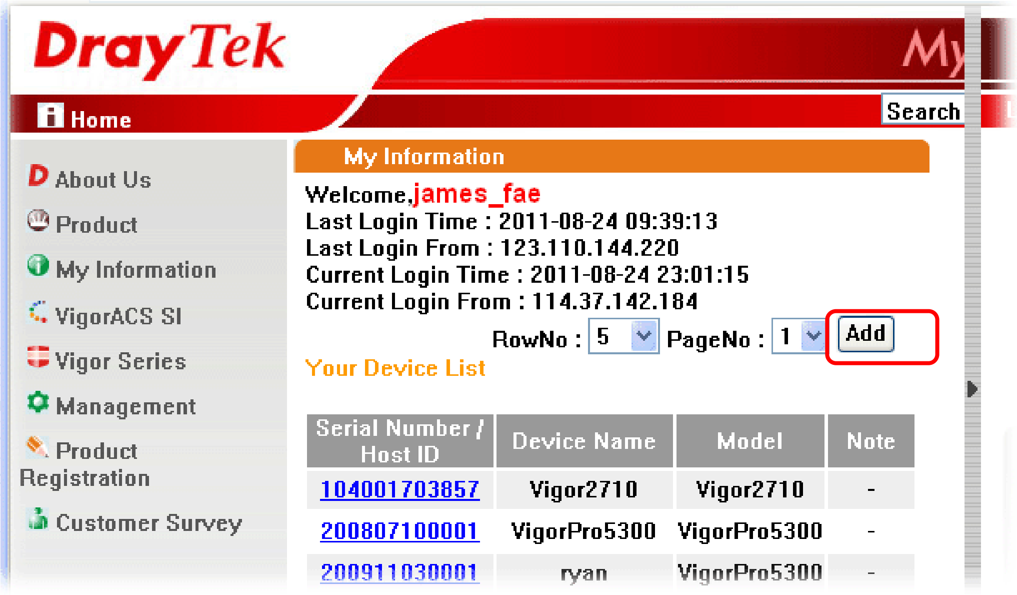
Password : ●●●●●●●●●

Auth Code : txxhdd

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

Become the MyVigor member, you can receive the e-newsletter update.

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



My Information

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

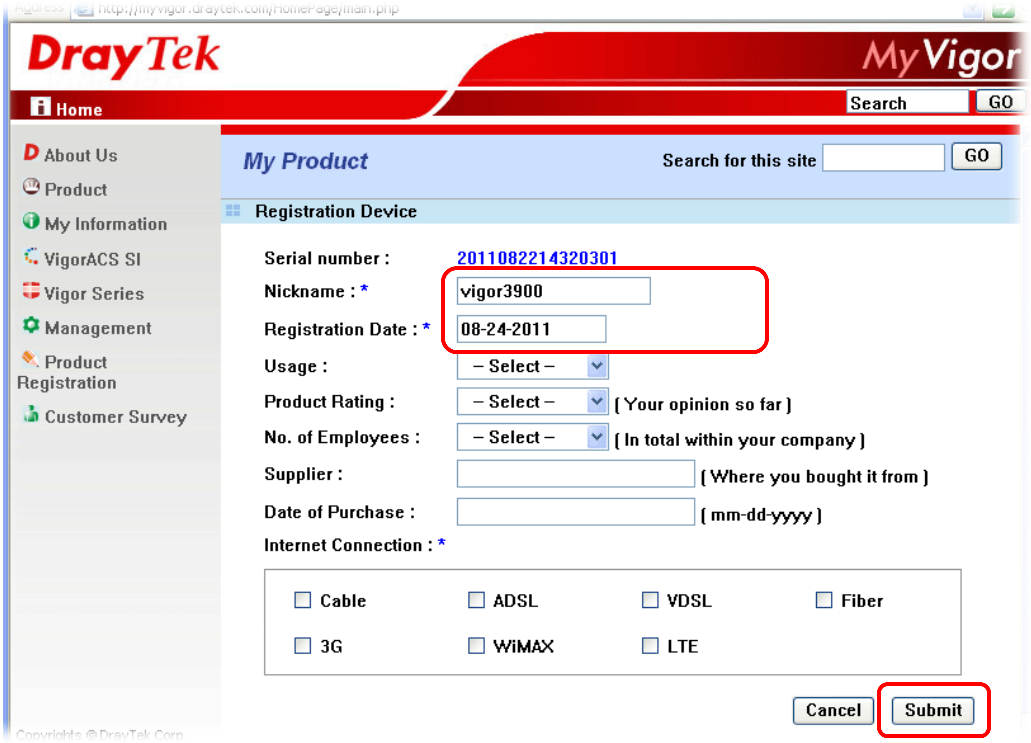
RowNo : 5 PageNo : 1

Your Device List

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

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

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



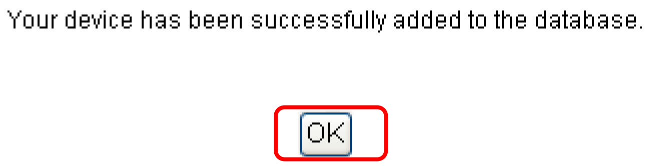
My Product

Registration Device

Serial number : 2011082214320301
Nickname : * vigor3900
Registration Date : * 08-24-2011
Usage : – Select –
Product Rating : – Select – (Your opinion so far)
No. of Employees : – Select – (In total within your company)
Supplier : (Where you bought it from)
Date of Purchase : (mm-dd-yyyy)
Internet Connection : *

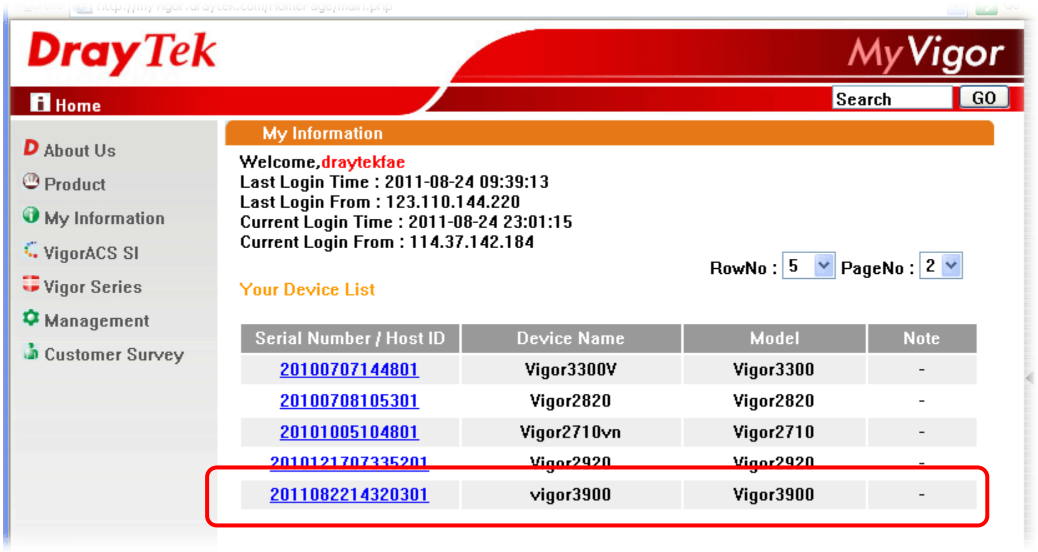
☐ Cable ☐ ADSL ☐ VDSL ☐ Fiber
☐ 3G ☐ WiMAX ☐ LTE

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



Your device has been successfully added to the database.

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



My Information

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

RowNo : 5 PageNo : 2

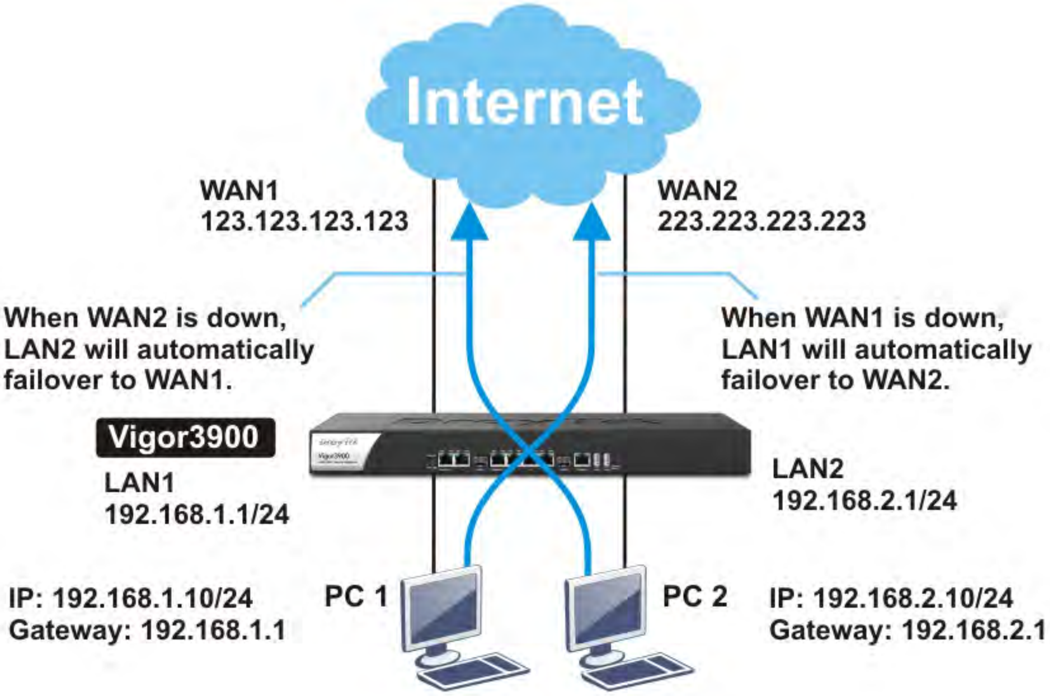
Your Device List

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

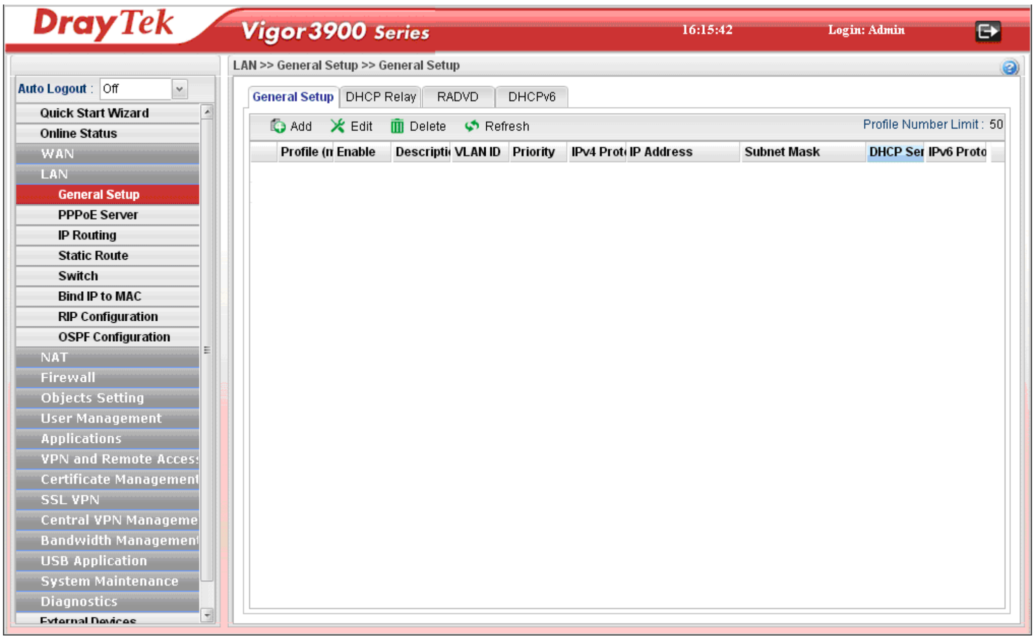
Chapter 3: Application and Tutorial

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

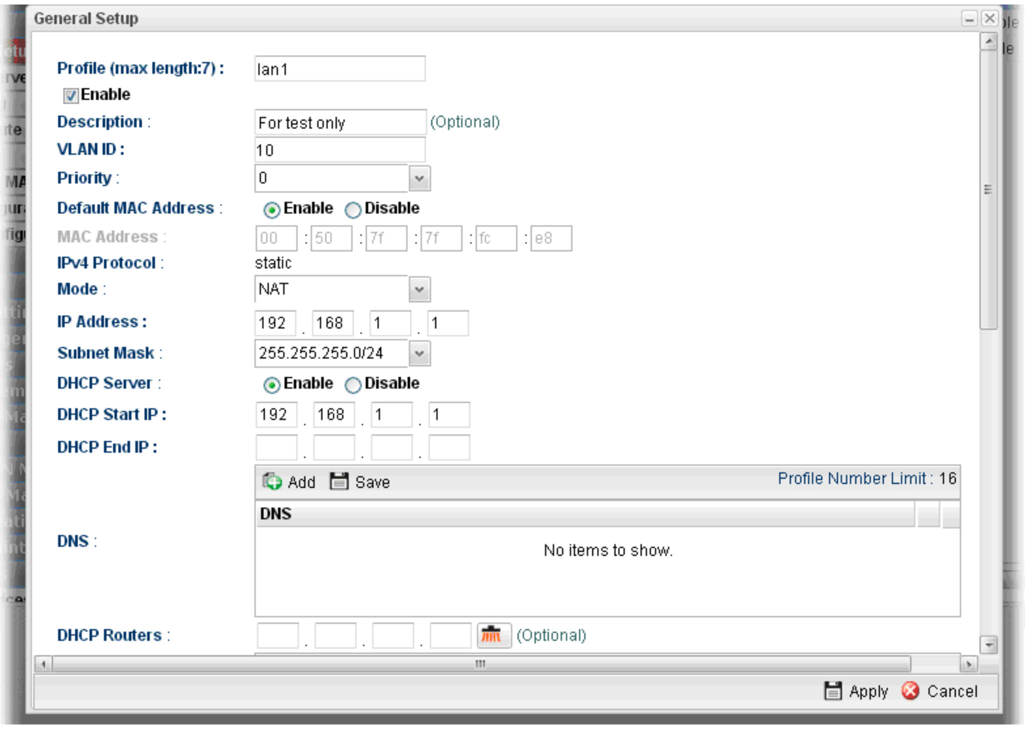
There are two different LANs configured in the following figure. One is for Sale (192.168.1.1/24) and the other is for FAE (192.168.2.1/24). Sale's LAN will be configured to go Internet always via WAN1. When WAN1 is down, Sale's LAN will automatically failover to WAN2. FAE's LAN will be configured to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



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



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



Profile (max length:7) : lan1

☑ Enable

Description : For test only (Optional)

VLAN ID : 10

Priority : 0

Default MAC Address : ● Enable ○ Disable

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

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 1 . 1

Subnet Mask : 255.255.255.0/24

DHCP Server : ● Enable ○ Disable

DHCP Start IP : 192 . 168 . 1 . 1

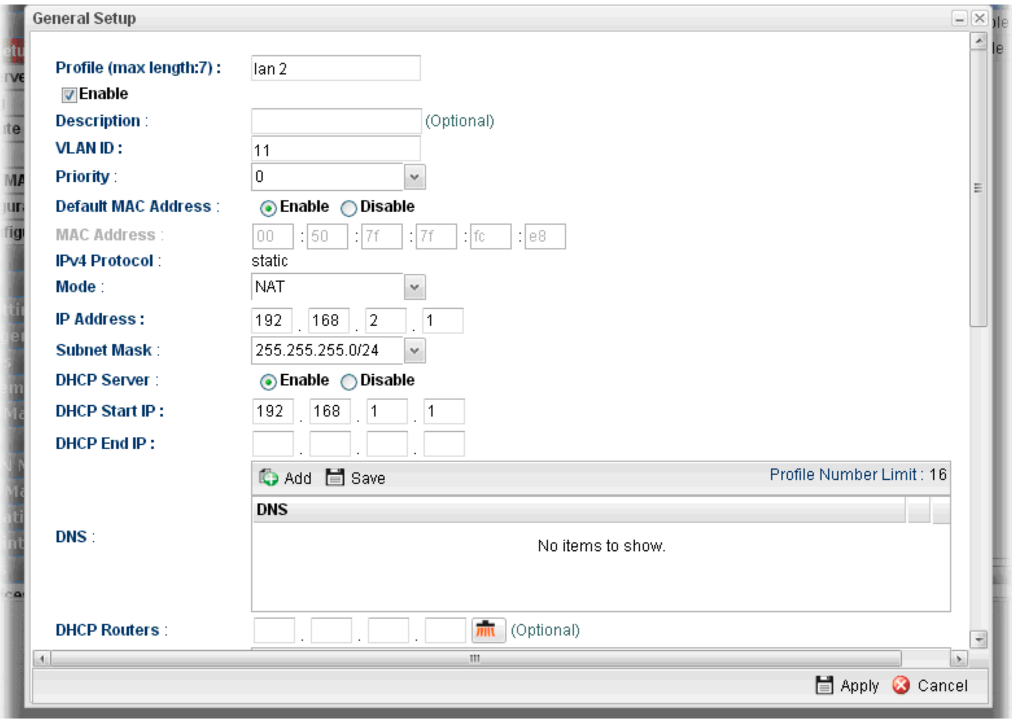
DHCP End IP : . . .

DNS :

DHCP Routers : . . . (Optional)

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).



General Setup

Profile (max length:7) : lan 2

☑ Enable

Description : (Optional)

VLAN ID : 11

Priority : 0

Default MAC Address : ● Enable ○ Disable

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

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 2 . 1

Subnet Mask : 255.255.255.0/24

DHCP Server : ● Enable ○ Disable

DHCP Start IP : 192 . 168 . 1 . 1

DHCP End IP : . . .

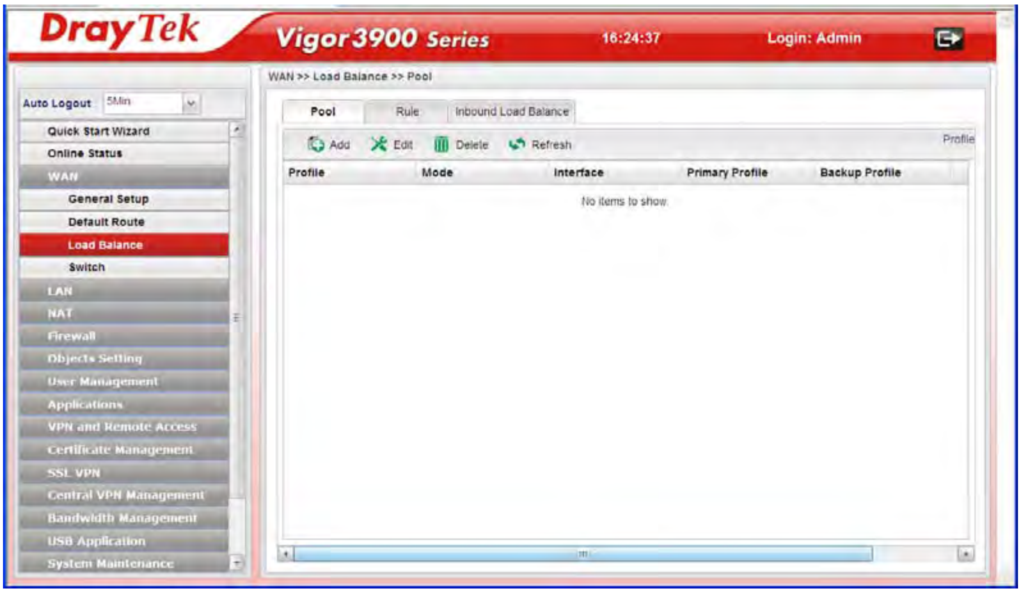
DNS : Add Save Profile Number Limit : 16

DNS
No items to show.

DHCP Routers : . . . (Optional)

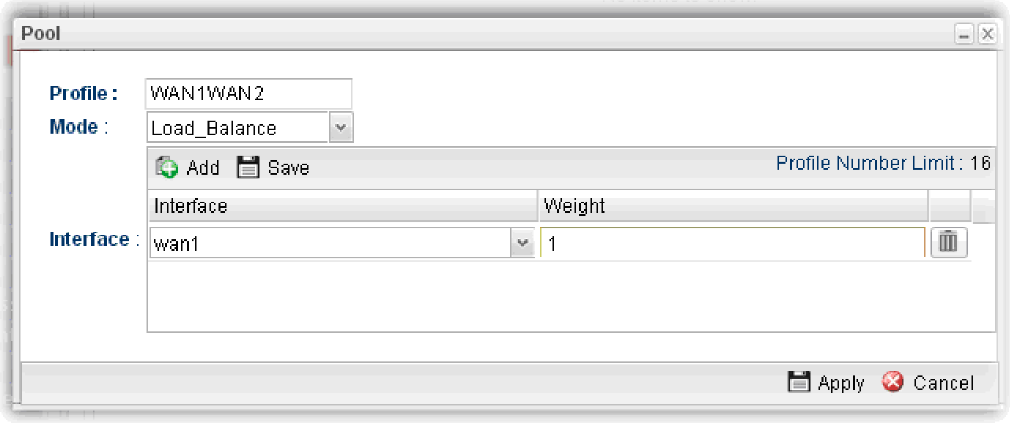
Type the information specified for LAN2 profile, then click **Apply** to save the settings and exit the screen.

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



Profile	Mode	Interface	Primary Profile	Backup Profile
No items to show				

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.



Profile : WAN1WAN2

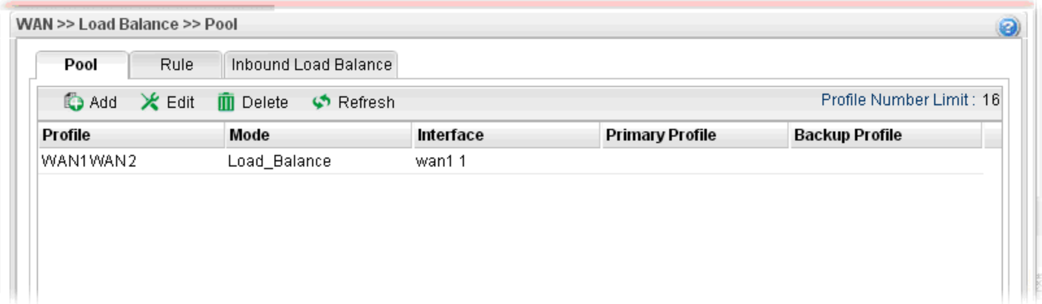
Mode : Load_Balance

Profile Number Limit : 16

Interface	Weight
wan1	1

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

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

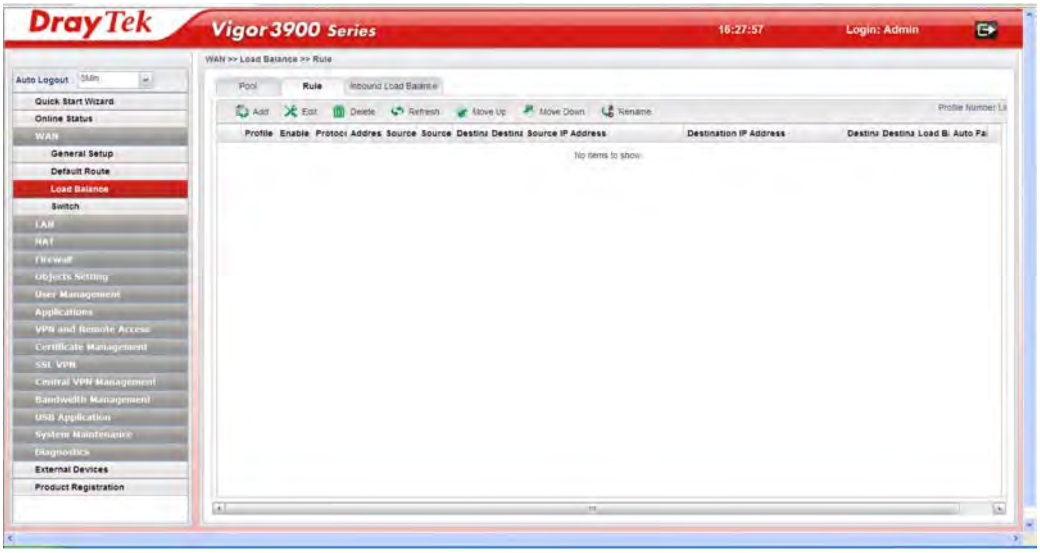


WAN >> Load Balance >> Pool

Profile Number Limit : 16

Profile	Mode	Interface	Primary Profile	Backup Profile
WAN1WAN2	Load_Balance	wan1 1		

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



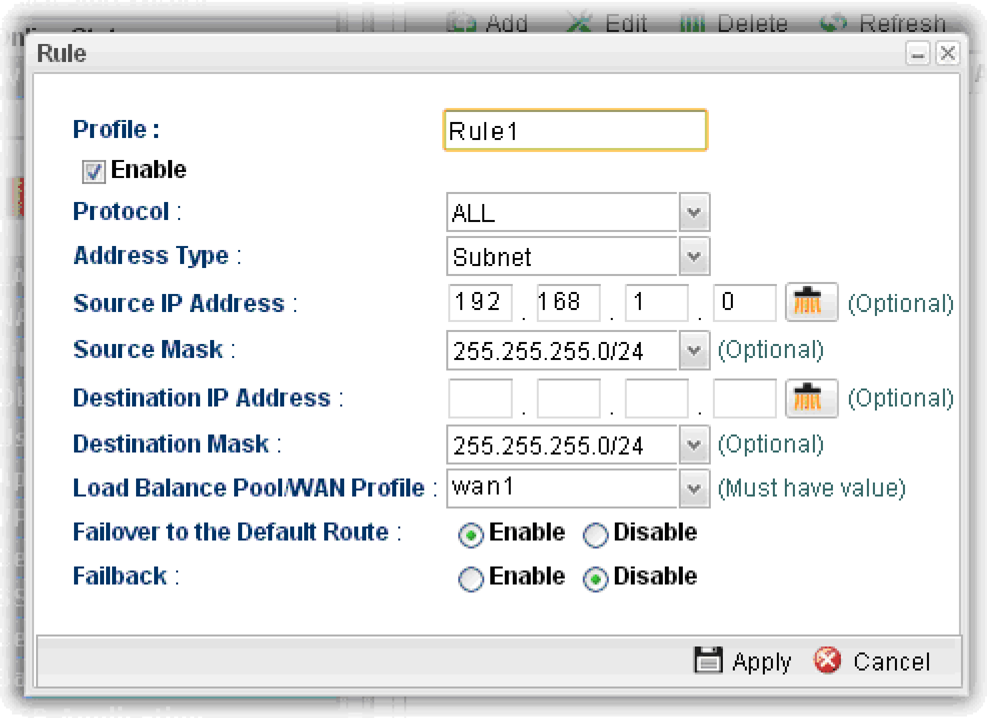
WAN >> Load Balance >> Rule

Profile	Enable	Protoc	Addres	Source	Source	Destin	Destin	Source IP Address	Destination IP Address	Destin	Destina	Load B	Auto Fa

No items to show

9. 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.



Rule

Profile : Rule1

☑ Enable

Protocol : ALL

Address Type : Subnet

Source IP Address : 192 . 168 . 1 . 0 (Optional)

Source Mask : 255.255.255.0/24 (Optional)

Destination IP Address : . . . (Optional)

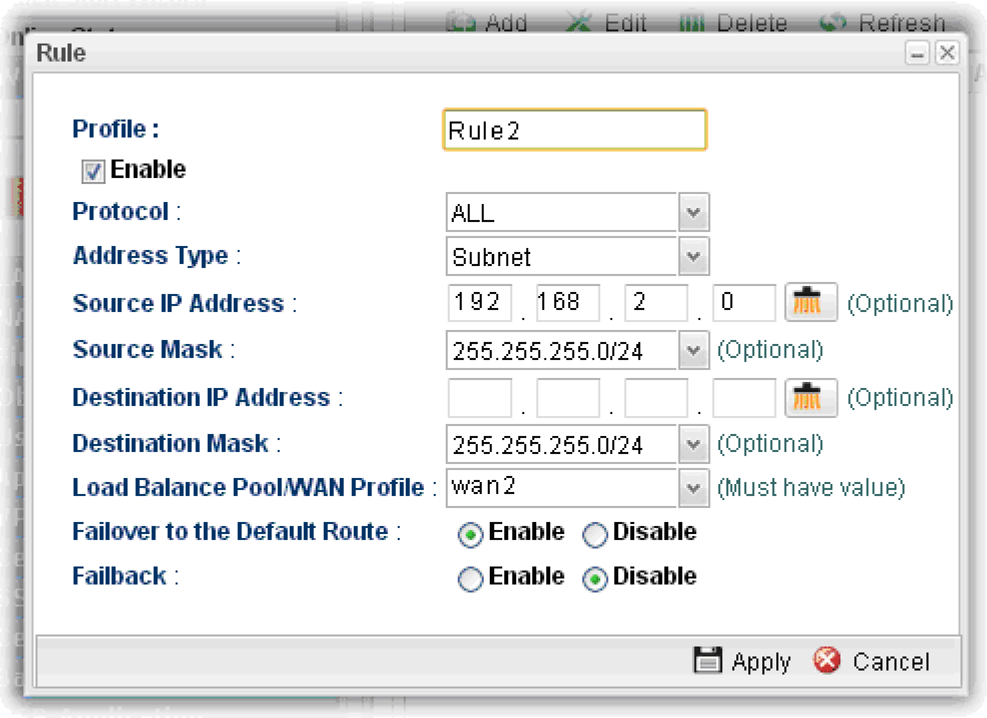
Destination Mask : 255.255.255.0/24 (Optional)

Load Balance Pool/WAN Profile : wan1 (Must have value)

Failover to the Default Route : ● Enable ○ Disable

Failback : ○ Enable ● Disable

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



Rule

Profile : Rule2

☑ Enable

Protocol : ALL

Address Type : Subnet

Source IP Address : 192 . 168 . 2 . 0 (Optional)

Source Mask : 255.255.255.0/24 (Optional)

Destination IP Address : . . . (Optional)

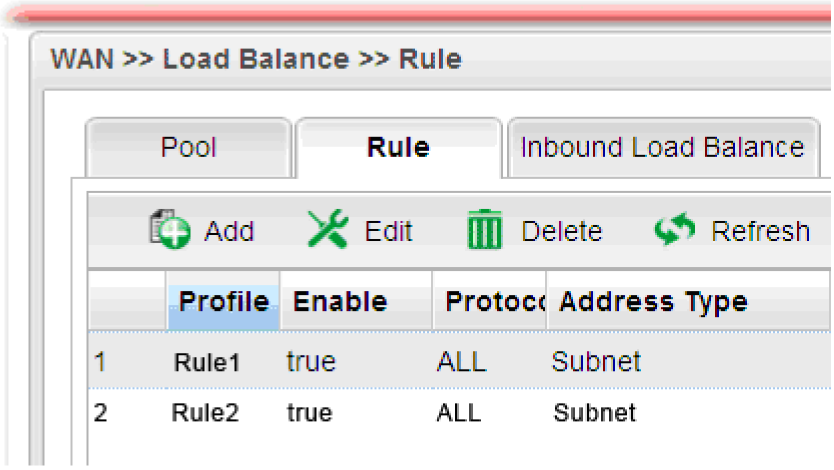
Destination Mask : 255.255.255.0/24 (Optional)

Load Balance Pool/WAN Profile : wan2 (Must have value)

Failover to the Default Route : ● Enable ○ Disable

Failback : ○ Enable ● Disable

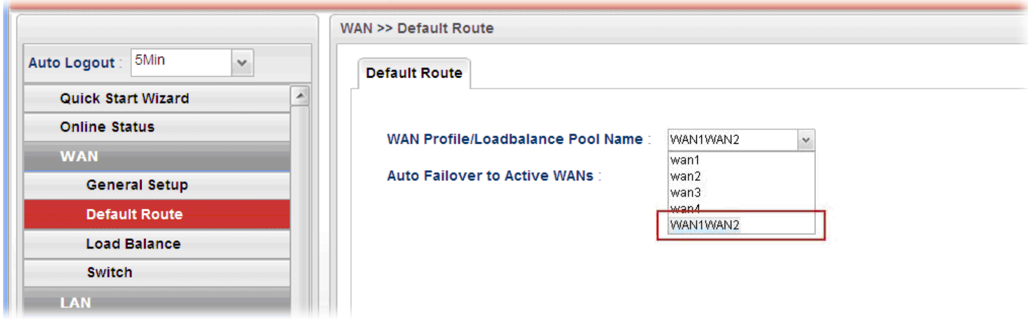
11. After clicking **Apply**, the created profiles will be shown on the screen.



WAN >> Load Balance >> Rule

	Profile	Enable	Protoco	Address Type
1	Rule1	true	ALL	Subnet
2	Rule2	true	ALL	Subnet

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



WAN >> Default Route

Auto Logout : 5Min

WAN Profile/Loadbalance Pool Name : WAN1WAN2

Auto Failover to Active WANs :

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.

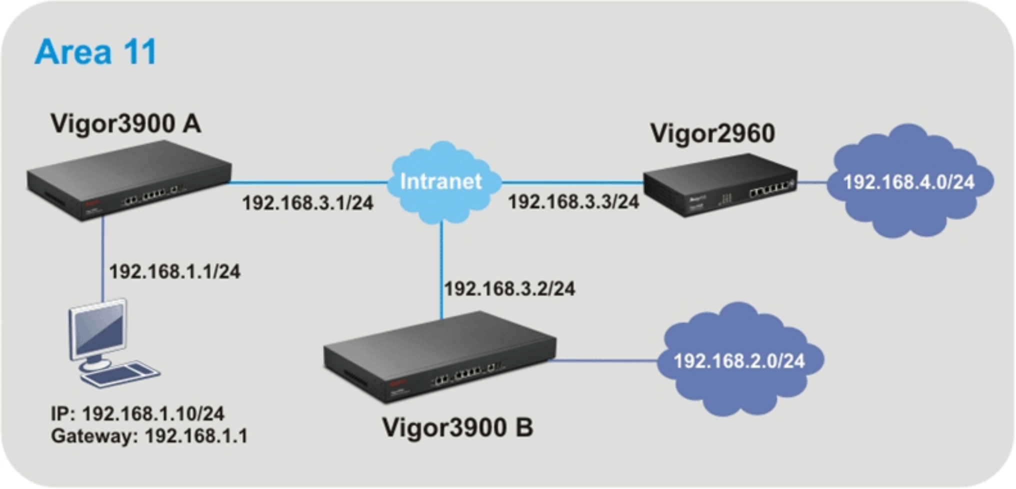
3.2 How to Configure OSPF?

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.

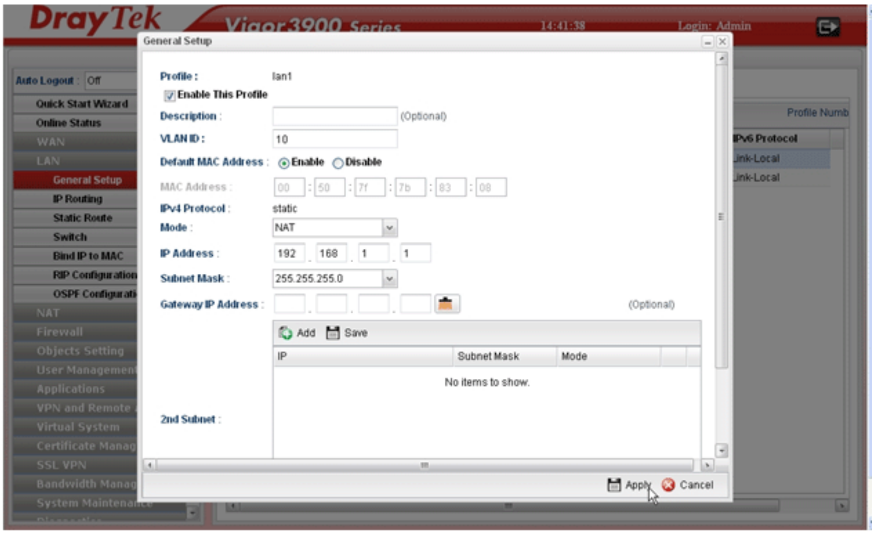


OSPF can place each router (e.g., Vigor3900A, Vigor3900B and Vigor2960 shown above) at the root of a tree and calculate the shortest path to each destination according to the cumulative cost to reach the destination.

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.



General Setup

Profile : lan1

☑ Enable This Profile

Description : (Optional)

VLAN ID : 10

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 50 : 7f : 7b : 83 : 08

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 1 . 1

Subnet Mask : 255.255.255.0

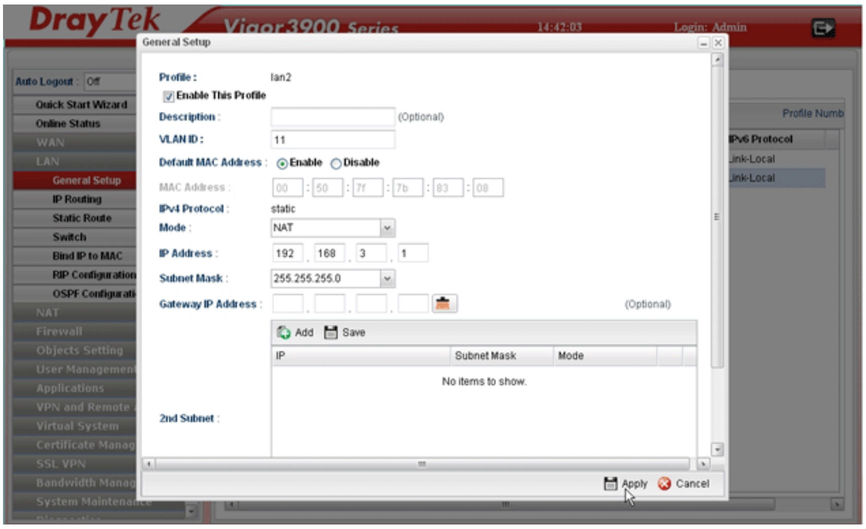
Gateway IP Address : (Optional)

2nd Subnet :

IP	Subnet Mask	Mode

No items to show.

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



General Setup

Profile : lan2

☑ Enable This Profile

Description : (Optional)

VLAN ID : 11

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 50 : 7f : 7b : 83 : 08

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 3 . 1

Subnet Mask : 255.255.255.0

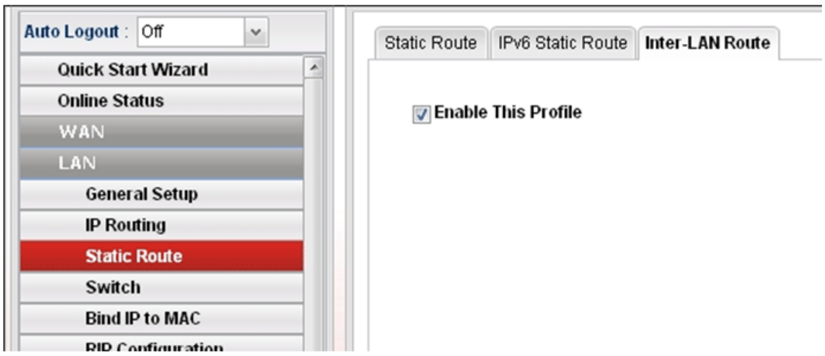
Gateway IP Address : (Optional)

2nd Subnet :

IP	Subnet Mask	Mode

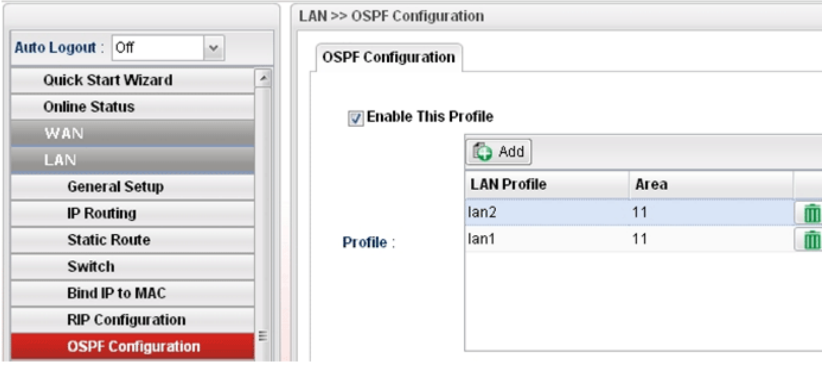
No items to show.

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



☑ Enable This Profile

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



LAN >> OSPF Configuration

OSPF Configuration

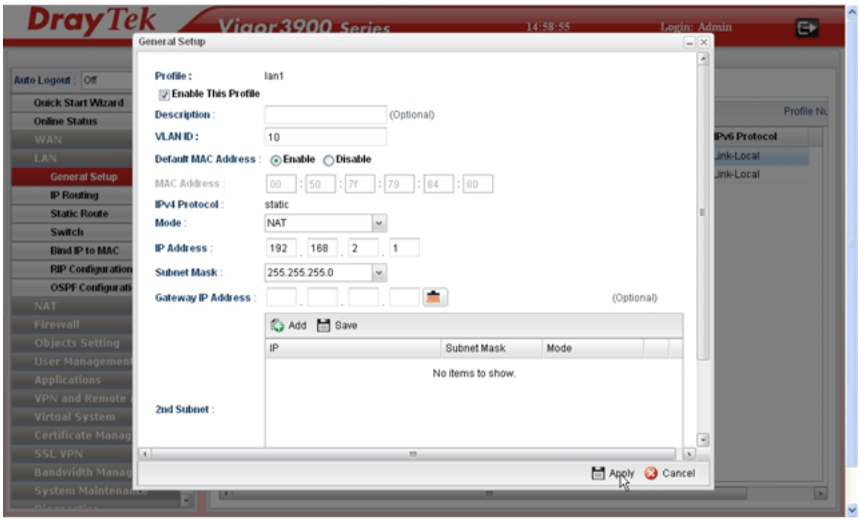
☑ Enable This Profile

Profile :

LAN Profile	Area
lan2	11
lan1	11

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.



General Setup

Profile : lan1

☑ Enable This Profile

Description : (Optional)

VLAN ID : 10

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 50 : 7f : 79 : 84 : 80

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 2 . 1

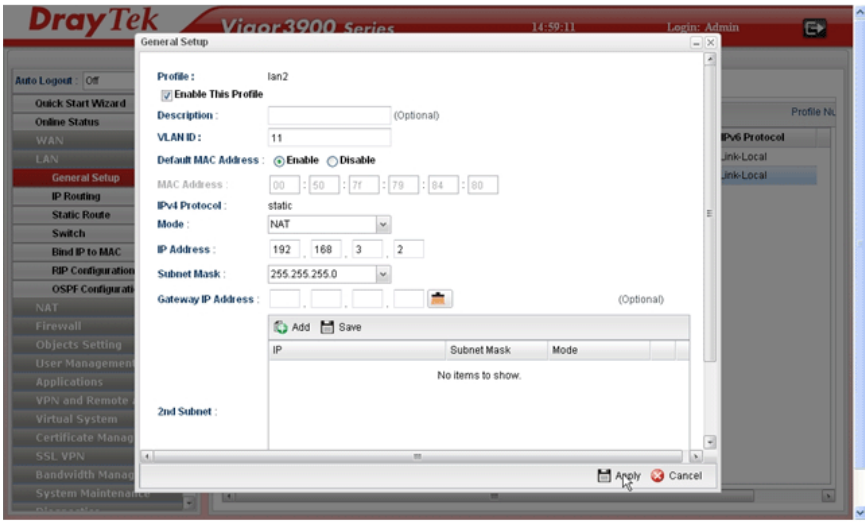
Subnet Mask : 255.255.255.0

Gateway IP Address : (Optional)

2nd Subnet :

IP	Subnet Mask	Mode
No items to show.		

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



General Setup

Profile : lan2

☑ Enable This Profile

Description : (Optional)

VLAN ID : 11

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 50 : 7f : 79 : 84 : 80

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 3 . 2

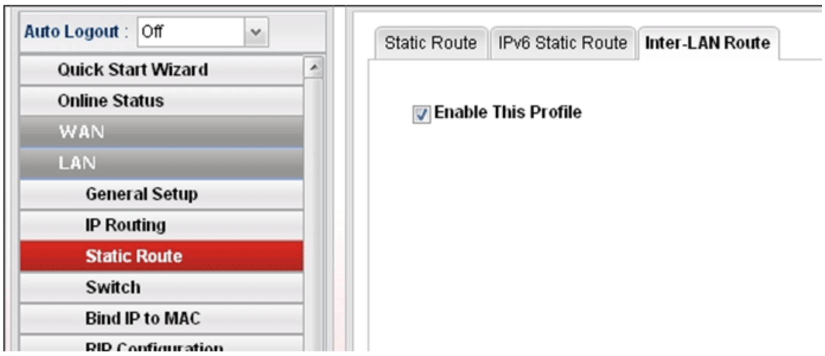
Subnet Mask : 255.255.255.0

Gateway IP Address : (Optional)

2nd Subnet :

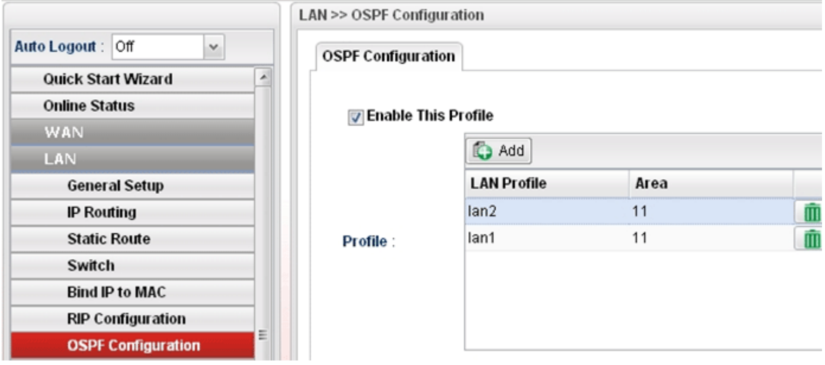
IP	Subnet Mask	Mode
No items to show.		

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



☑ Enable This Profile

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



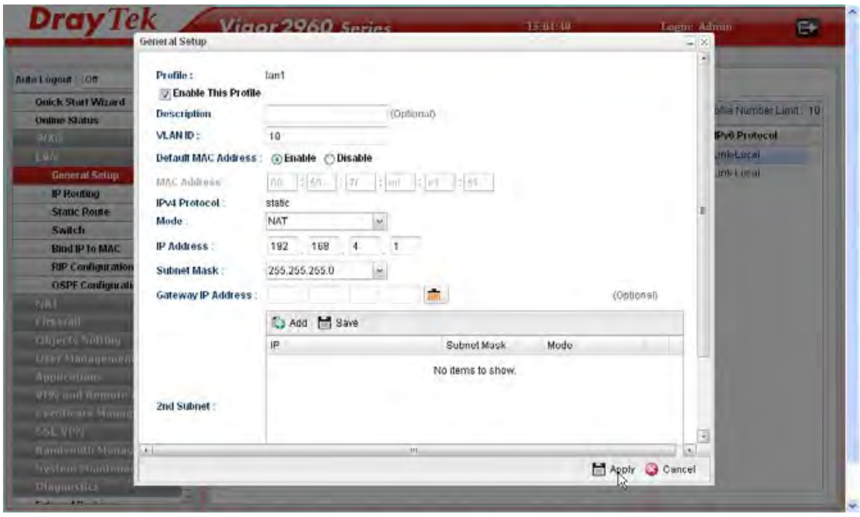
☑ Enable This Profile

Profile :

LAN Profile	Area
lan2	11
lan1	11

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.



Profile : lan1

☑ Enable This Profile

Description (Optional)

VLAN ID : 10

Default MAC Address : ● Enable ○ Disable

MAC Address

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 4 . 1

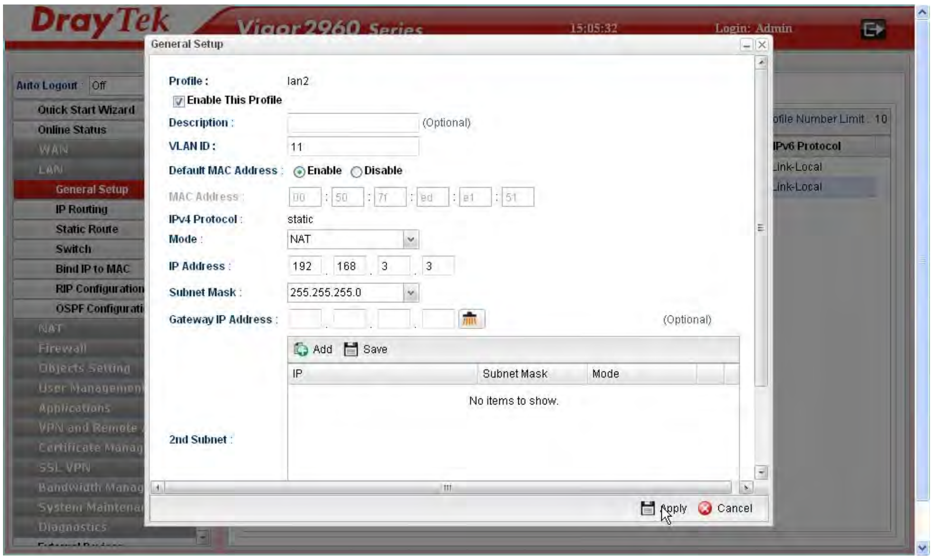
Subnet Mask : 255.255.255.0

Gateway IP Address : (Optional)

2nd Subnet :

IP	Subnet Mask	Mode
No items to show.		

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



General Setup

Profile : lan2

☑ Enable This Profile

Description : (Optional)

VLAN ID : 11

Default MAC Address : ● Enable ○ Disable

MAC Address : 00 : 50 : 7f : ed : e1 : 51

IPv4 Protocol : static

Mode : NAT

IP Address : 192 . 168 . 3 . 3

Subnet Mask : 255.255.255.0

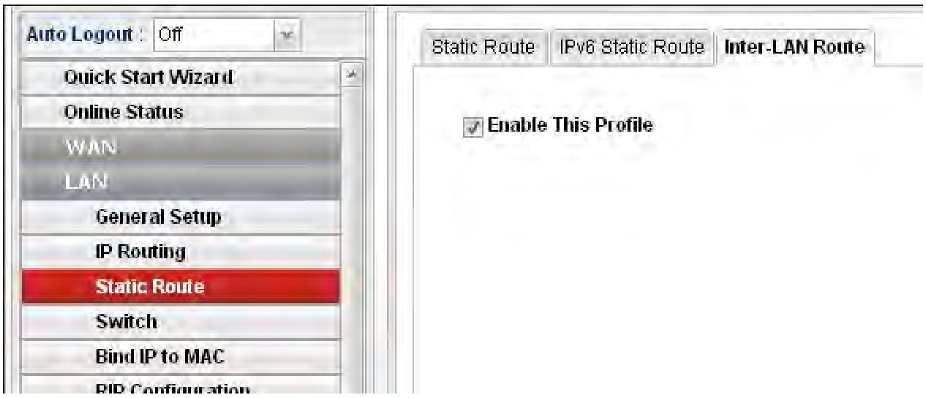
Gateway IP Address : . . . (Optional)

2nd Subnet :

IP	Subnet Mask	Mode

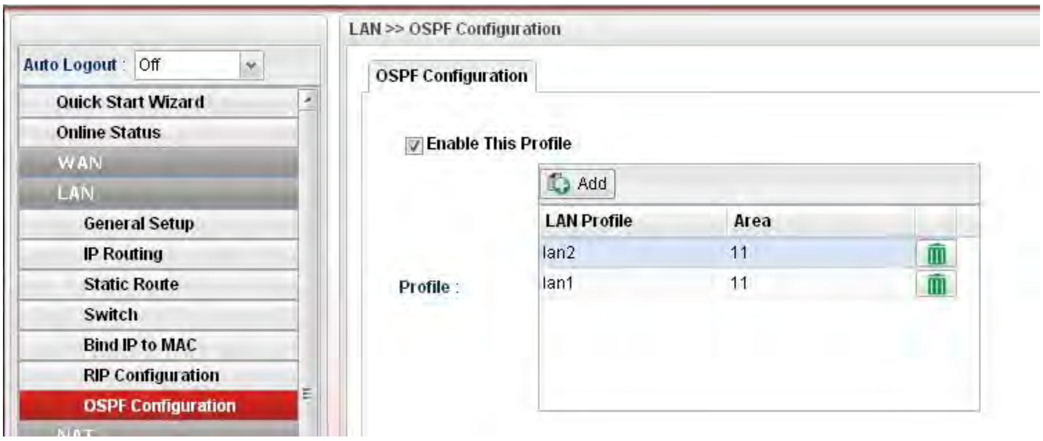
No items to show.

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



☑ Enable This Profile

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



LAN >> OSPF Configuration

OSPF Configuration

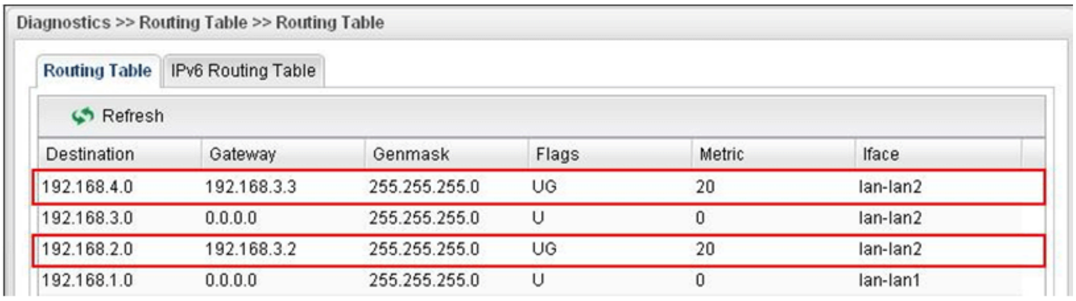
☑ Enable This Profile

Profile :

LAN Profile	Area
lan2	11
lan1	11

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

Routing information for Vigor3900 A



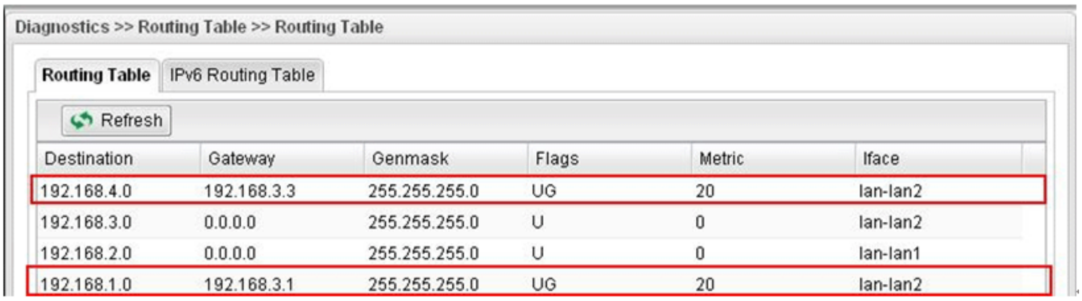
Diagnostics >> Routing Table >> Routing Table

Routing Table | IPv6 Routing Table

Refresh

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

Routing information for Vigor3900 B



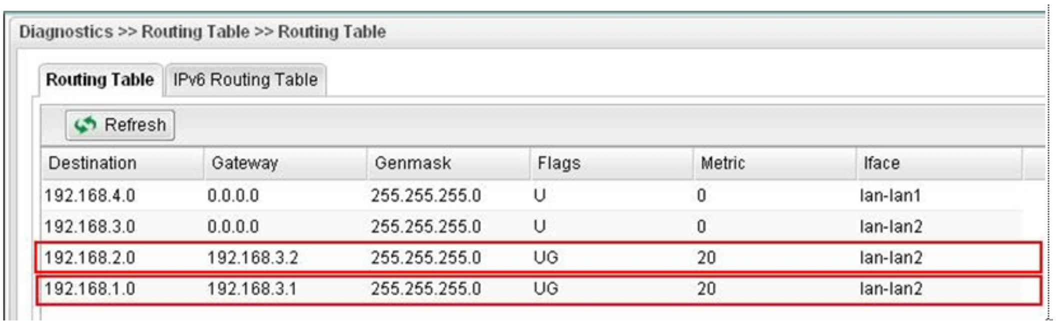
Diagnostics >> Routing Table >> Routing Table

Routing Table | IPv6 Routing Table

Refresh

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

Routing information for Vigor2960



Diagnostics >> Routing Table >> Routing Table

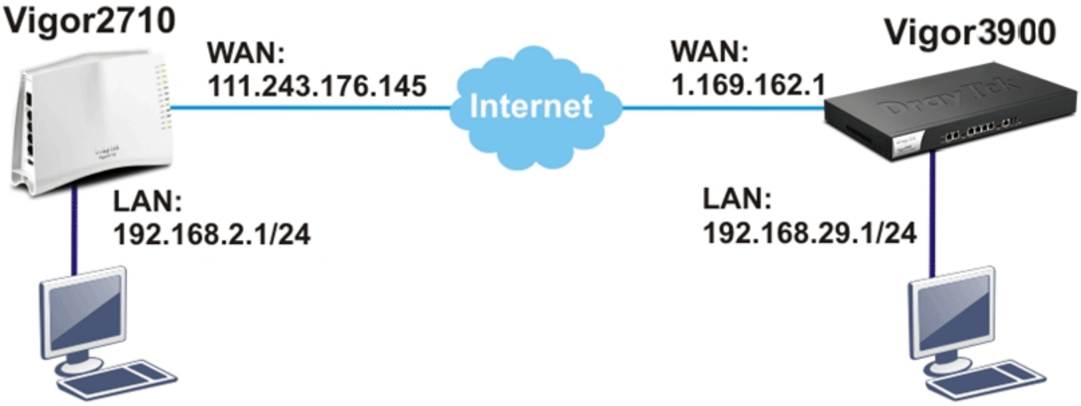
Routing Table | IPv6 Routing Table

Refresh

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

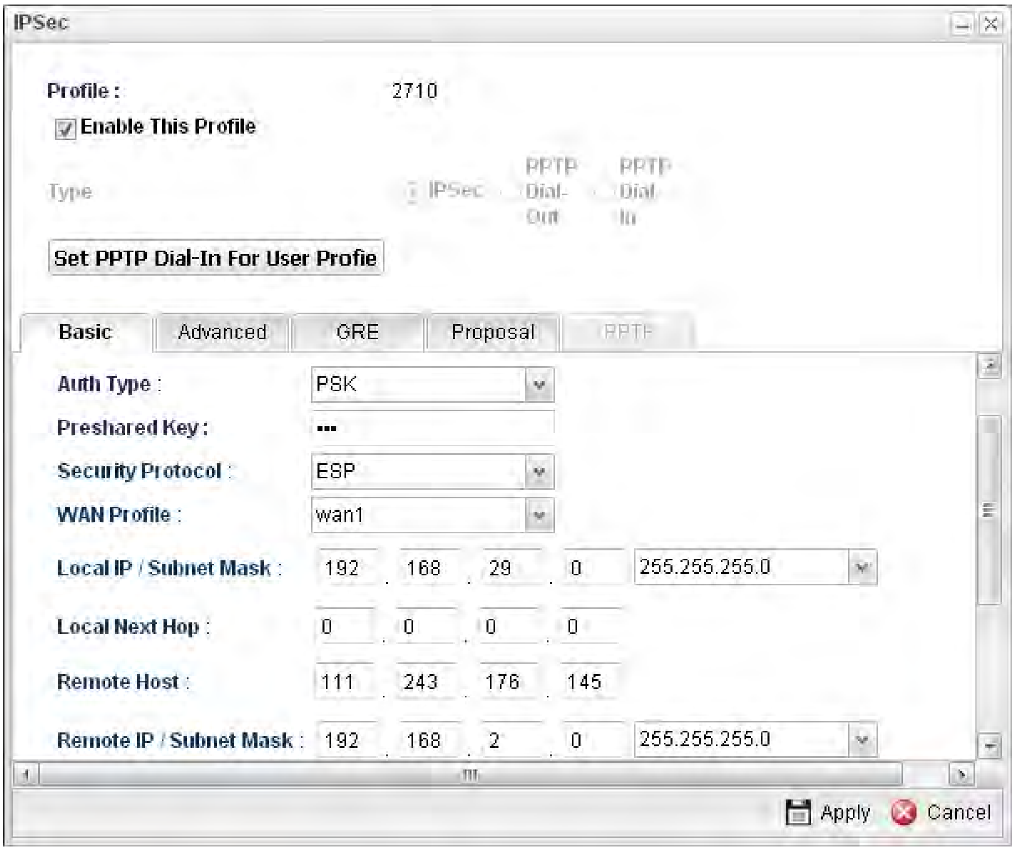
3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode)

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



Configuring Vigor3900

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



Profile : 2710

☑ Enable This Profile

Type ○ IPSec ○ PPTP Dial-Out ○ PPTP Dial-In

Auth Type : PSK

Preshared Key : •••

Security Protocol : ESP

WAN Profile : wan1

Local IP / Subnet Mask : 192 . 168 . 29 . 0 255.255.255.0

Local Next Hop : 0 . 0 . 0 . 0

Remote Host : 111 . 243 . 176 . 145

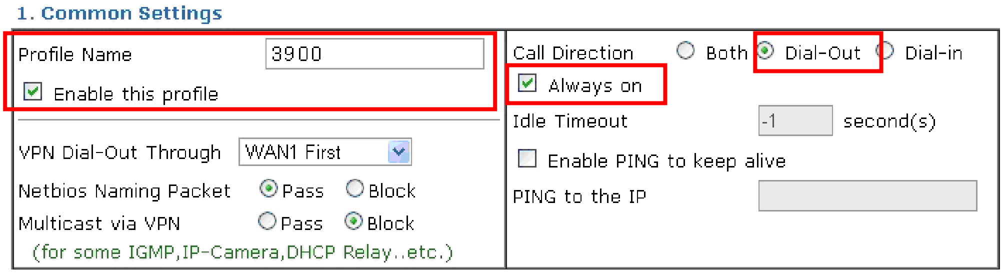
Remote IP / Subnet Mask : 192 . 168 . 2 . 0 255.255.255.0

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

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

Configuring Vigor2710

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



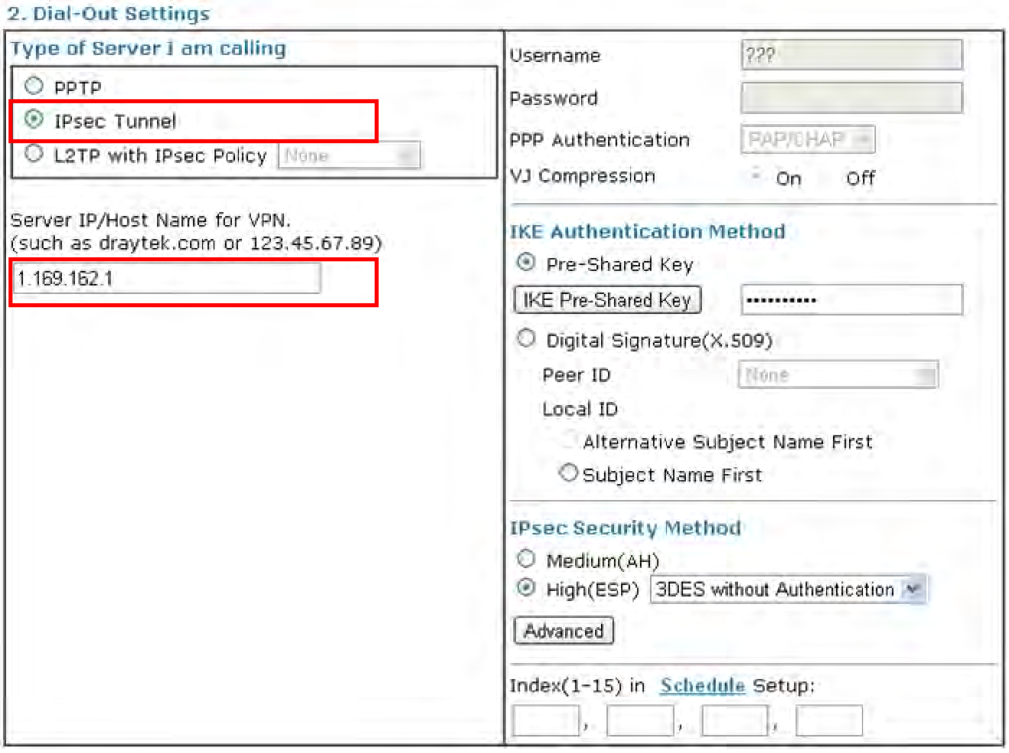
1. Common Settings

Profile Name: 3900
☑ Enable this profile
VPN Dial-Out Through: WAN1 First
Netbios Naming Packet: ● Pass ○ Block
Multicast via VPN: ○ Pass ● Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: ○ Both ● Dial-Out ○ Dial-in
☑ Always on
Idle Timeout: -1 second(s)
☐ Enable PING to keep alive
PING to the IP:

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

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



2. Dial-Out Settings

Type of Server I am calling
○ PPTP
● IPsec Tunnel
○ L2TP with IPsec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
1.169.162.1

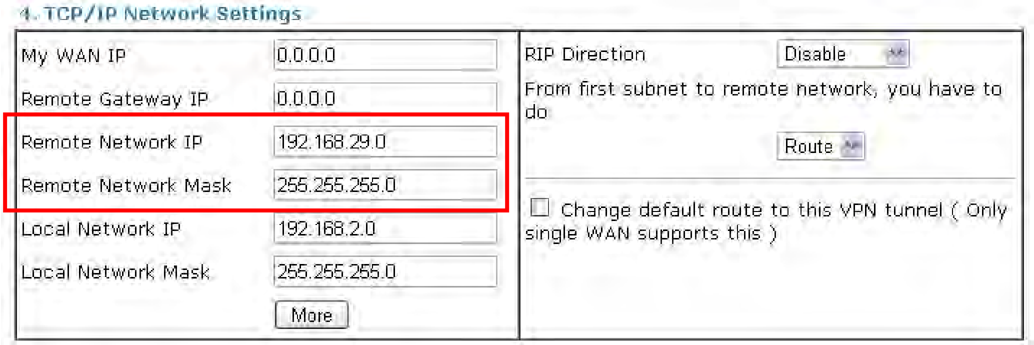
Username: ???
Password:
PPP Authentication: PAP/CHAP
VJ Compression: ○ On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key: ••••••••••
○ Digital Signature(X.509)
Peer ID: None
Local ID
○ Alternative Subject Name First
○ Subject Name First

IPsec Security Method
○ Medium(AH)
● High(ESP): 3DES without Authentication
Advanced

Index(1-15) in Schedule Setup: , , ,

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. TCP/IP Network Settings

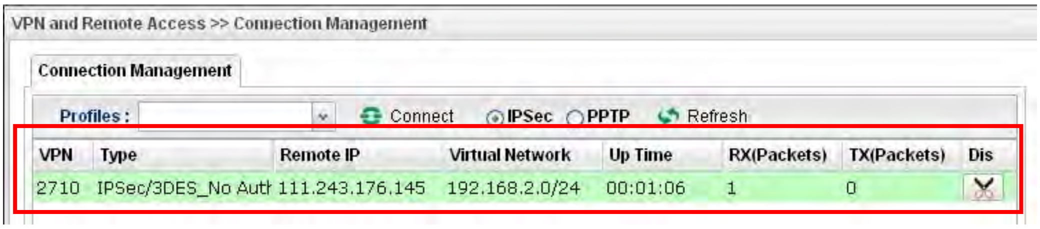
My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.29.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.2.0
Local Network Mask	255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

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.



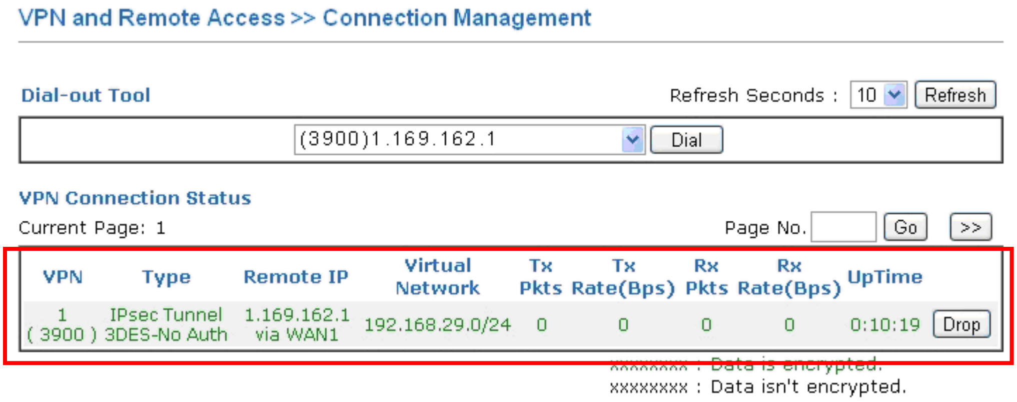
VPN and Remote Access >> Connection Management

Connection Management

Profiles : ▾ Connect ● IPSec ○ PPTP Refresh

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

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



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

(3900)1.169.162.1 Dial

VPN Connection Status

Current Page: 1

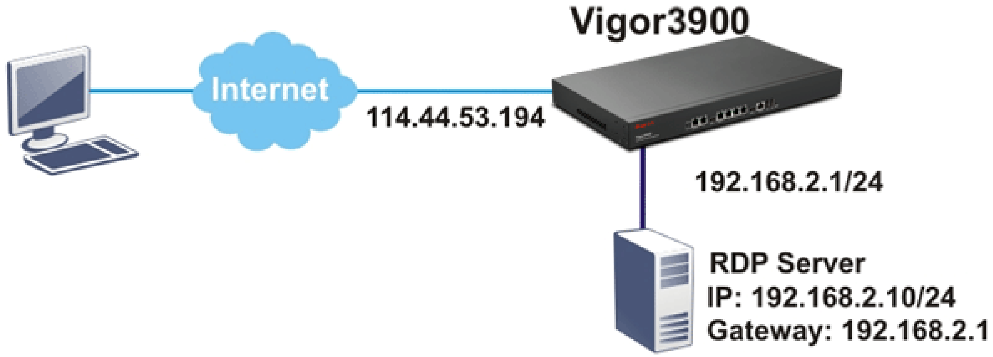
Page No. Go >>

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

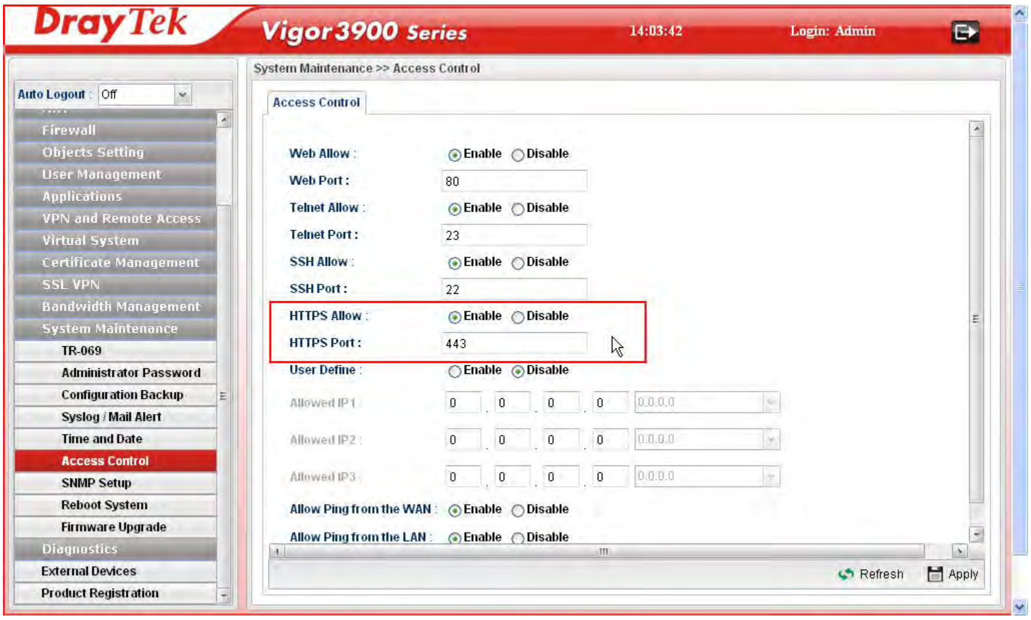
xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

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

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

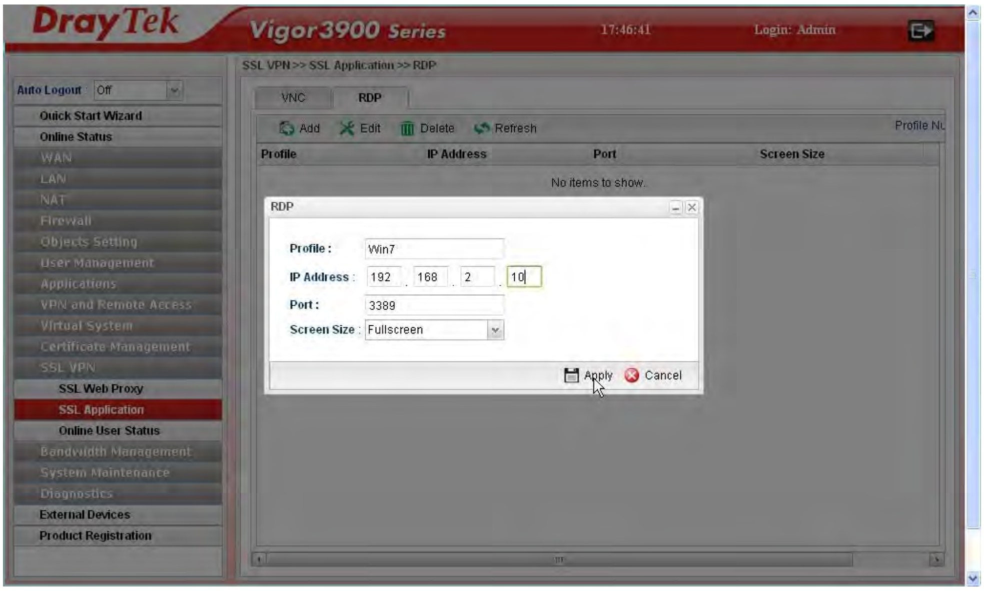


1. Open the Web User Interface of Vigor3900.
2. Enable the HTTPS service from **System Maintenance** >> **Access Control** by clicking **Enable** for **HTTPS Allow** and type **443** as the value of **HTTPS Port.**



Web Allow : ● Enable ○ Disable
Web Port : 80
Telnet Allow : ● Enable ○ Disable
Telnet Port : 23
SSH Allow : ● Enable ○ Disable
SSH Port : 22
HTTPS Allow : ● Enable ○ Disable
HTTPS Port : 443
User Define : ○ Enable ● Disable
Allowed IP1 : 0 . 0 . 0 . 0 0.0.0.0
Allowed IP2 : 0 . 0 . 0 . 0 0.0.0.0
Allowed IP3 : 0 . 0 . 0 . 0 0.0.0.0
Allow Ping from the WAN : ● Enable ○ Disable
Allow Ping from the LAN : ● Enable ○ Disable

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.



Profile	IP Address	Port	Screen Size

No items to show.

RDP

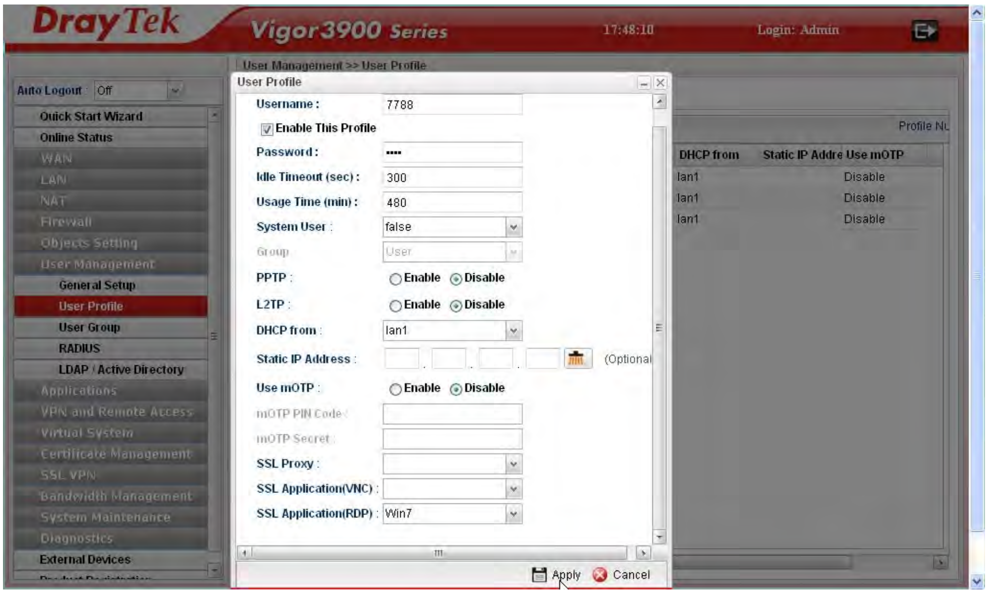
Profile : Win7

IP Address : 192 . 168 . 2 . 10

Port : 3389

Screen Size : Fullscreen

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**.



DHCP from	Static IP Addre	Use mOTP
lan1		Disable
lan1		Disable
lan1		Disable

User Profile

Username : 7788

☑ Enable This Profile

Password : ••••

Idle Timeout (sec) : 300

Usage Time (min) : 480

System User : false

Group : User

PPTP : ○ Enable ● Disable

L2TP : ○ Enable ● Disable

DHCP from : lan1

Static IP Address : . . . (Optional

Use mOTP : ○ Enable ● Disable

mOTP PIN Code :

mOTP Secret :

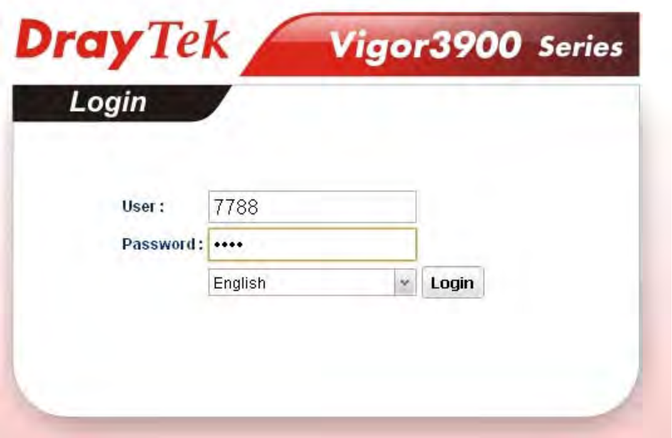
SSL Proxy :

SSL Application(VNC) :

SSL Application(RDP) : Win7

5. Logout Vigor3900.

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

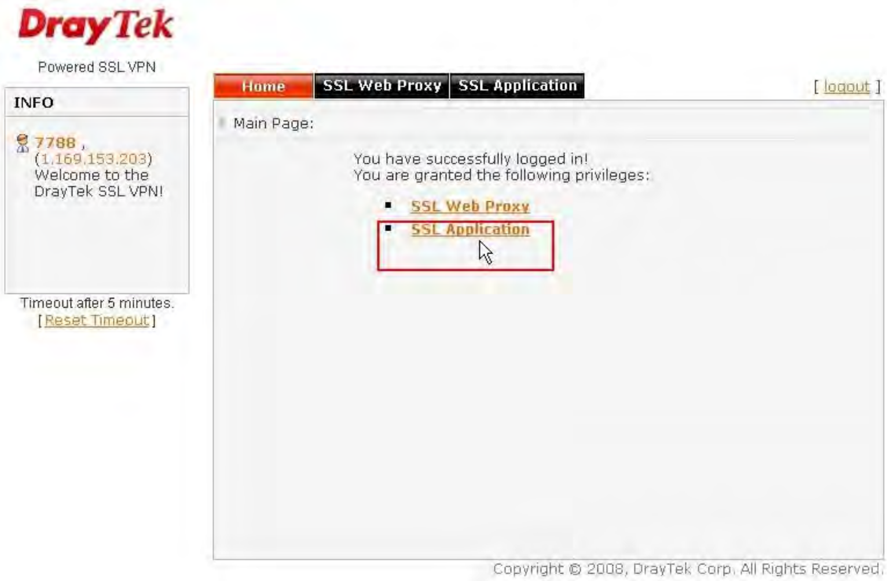


User : 7788

Password : ••••

English

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



INFO

7788 , (1.169.153.203) Welcome to the DrayTek SSL VPN!

Timeout after 5 minutes.
[Reset Timeout]

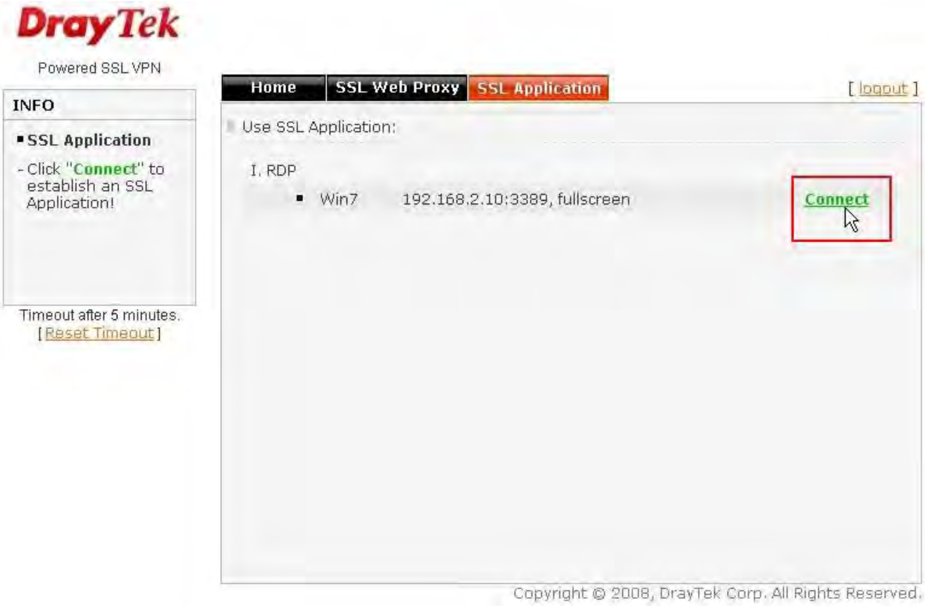
Main Page:

You have successfully logged in!
You are granted the following privileges:

- SSL Web Proxy
- SSL Application

Copyright © 2008, DrayTek Corp. All Rights Reserved.

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



INFO

- SSL Application

- Click "Connect" to establish an SSL Application!

Timeout after 5 minutes.
[Reset Timeout]

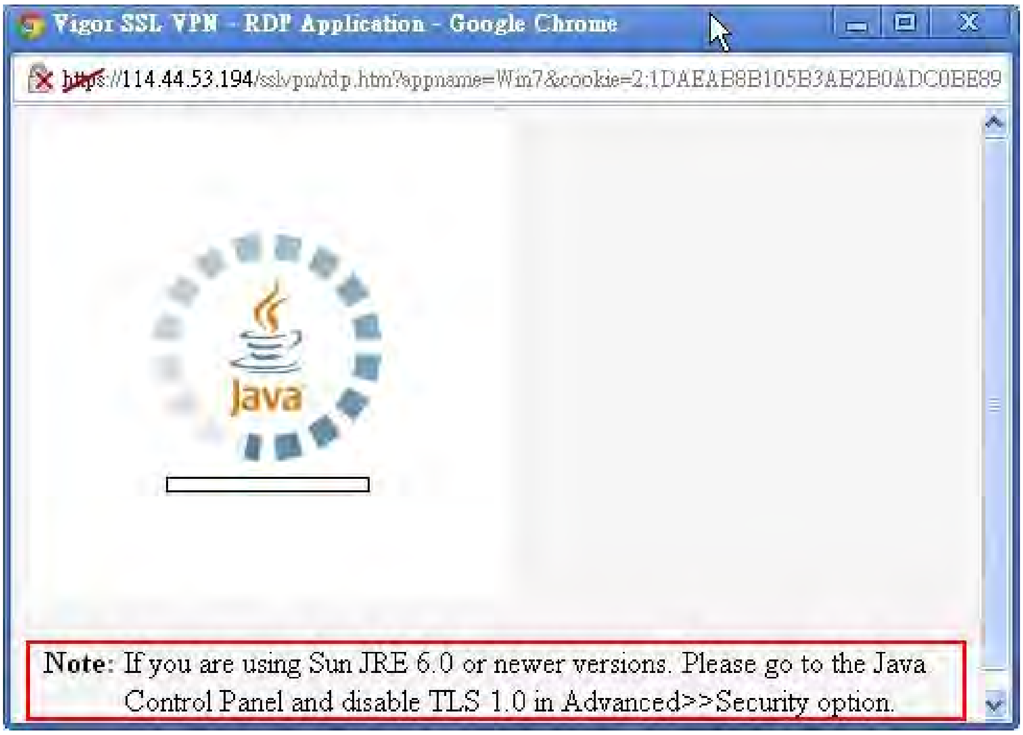
Use SSL Application:

I. RDP

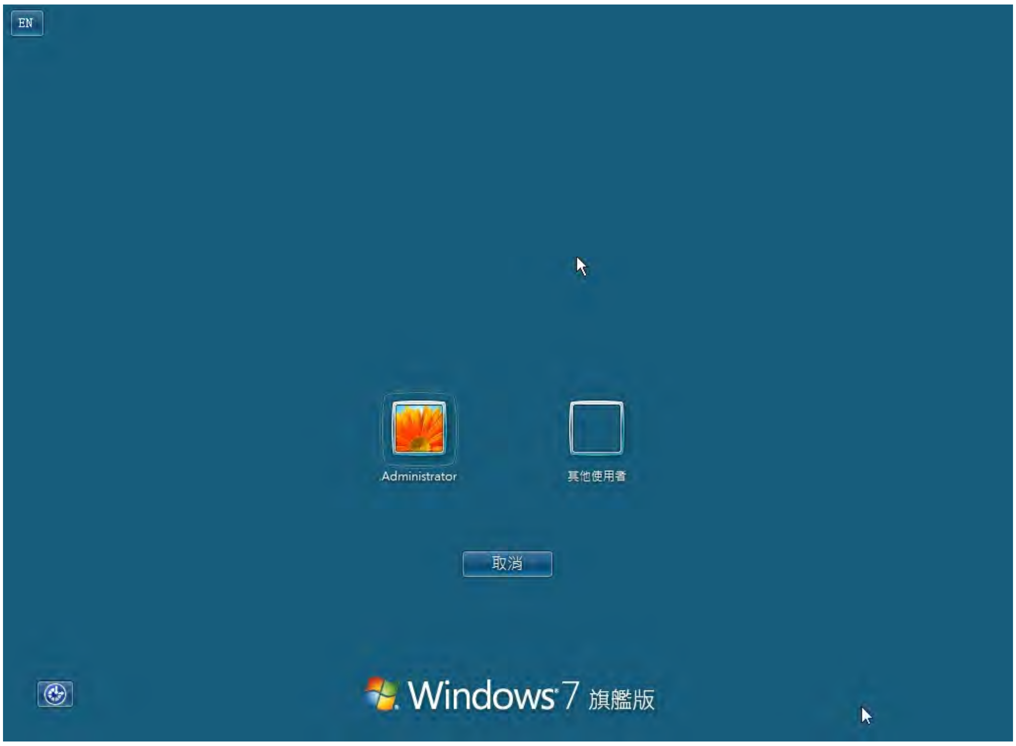
- Win7 192.168.2.10:3389, fullscreen Connect

Copyright © 2008, DrayTek Corp. All Rights Reserved.

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.

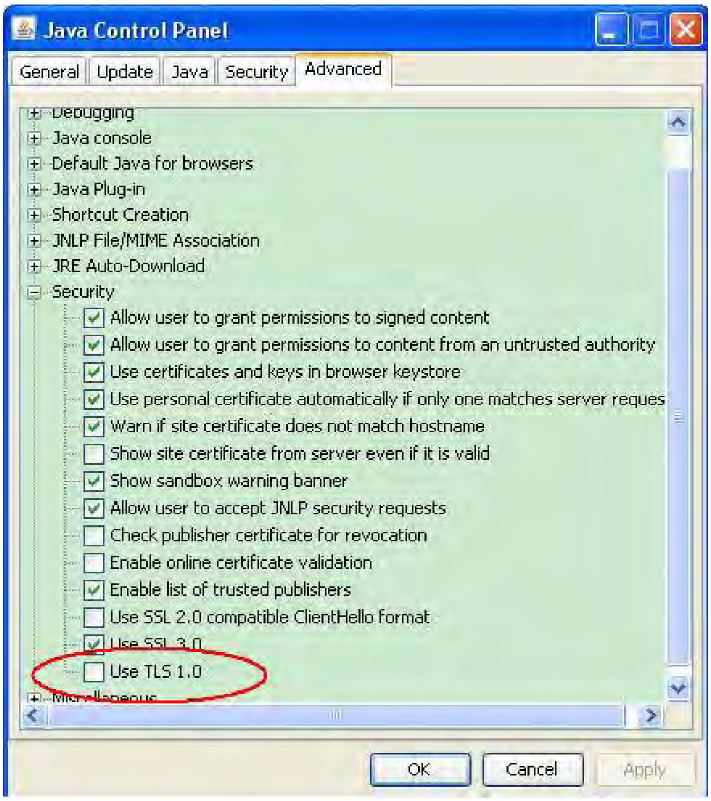

Vigor SSL VPN - RDP Application - Google Chrome
https://114.44.53.194/sslvpn/rdp.htm?appname=Win7&cookie=2:1DAEAB8B105B3AB2B0ADC0BE89
Java

Note: If you are using Sun JRE 6.0 or newer versions. Please go to the Java Control Panel and disable TLS 1.0 in Advanced>>Security option.



Troubleshooting

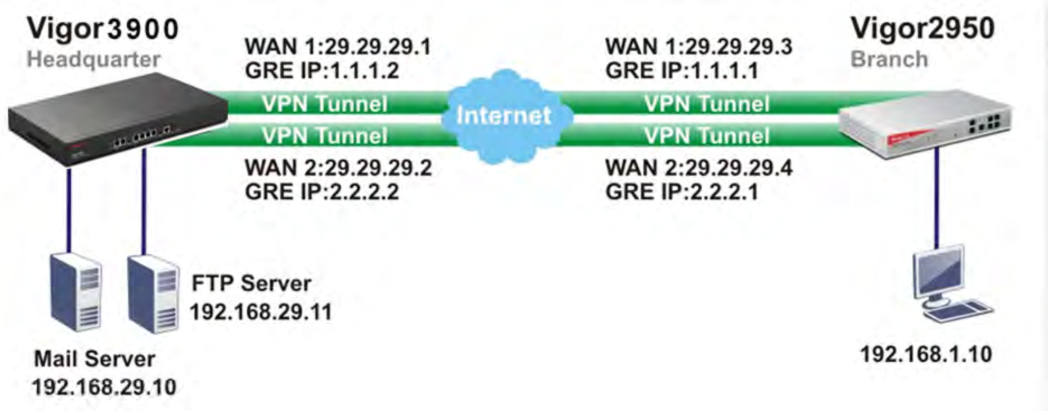
If you have installed Java Runtime Environment edition 6 but still cannot establish the connection, please make sure you have disabled “**Use TLS 1.0**” in the **Java Control Panel** as figure shown below. Then, try to connect again.



- ⊞ Debugging
- ⊞ Java console
- ⊞ Default Java for browsers
- ⊞ Java Plug-in
- ⊞ Shortcut Creation
- ⊞ JNLP File/MIME Association
- ⊞ JRE Auto-Download
- ⊟ Security
  - ☑ Allow user to grant permissions to signed content
  - ☑ Allow user to grant permissions to content from an untrusted authority
  - ☑ Use certificates and keys in browser keystore
  - ☑ Use personal certificate automatically if only one matches server reques
  - ☑ Warn if site certificate does not match hostname
  - □ Show site certificate from server even if it is valid
  - ☑ Show sandbox warning banner
  - ☑ Allow user to accept JNLP security requests
  - □ Check publisher certificate for revocation
  - □ Enable online certificate validation
  - ☑ Enable list of trusted publishers
  - □ Use SSL 2.0 compatible ClientHello format
  - ☑ Use SSL 3.0
  - □ Use TLS 1.0
- ⊞ Miscellaneous

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

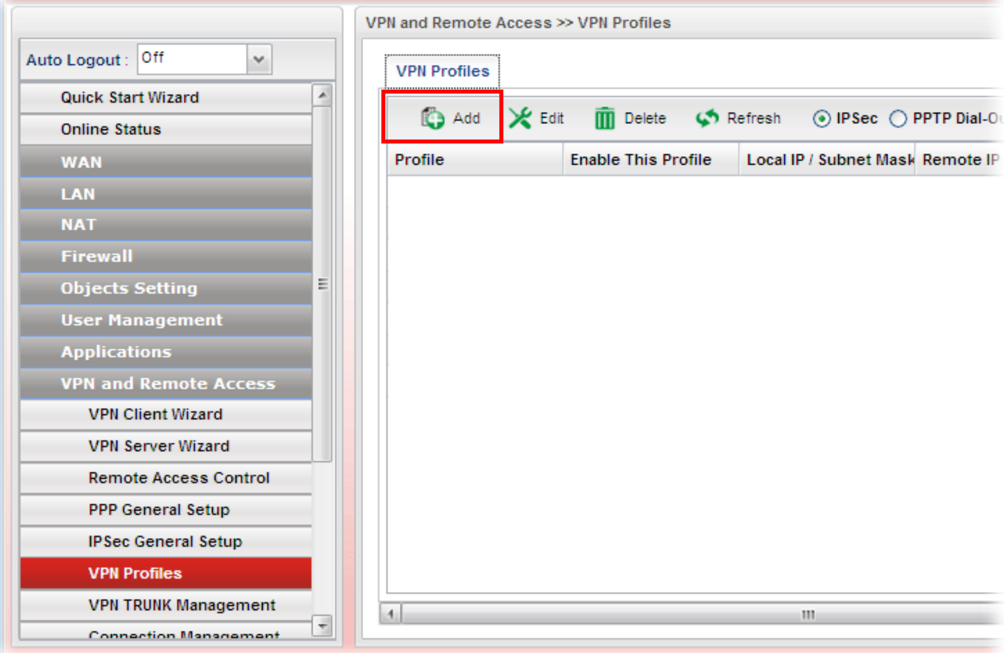
The staff in branch office can access into mail server/FTP server installed in the headquarters via VPN Load Balance tunnels. Refer to the following figure.



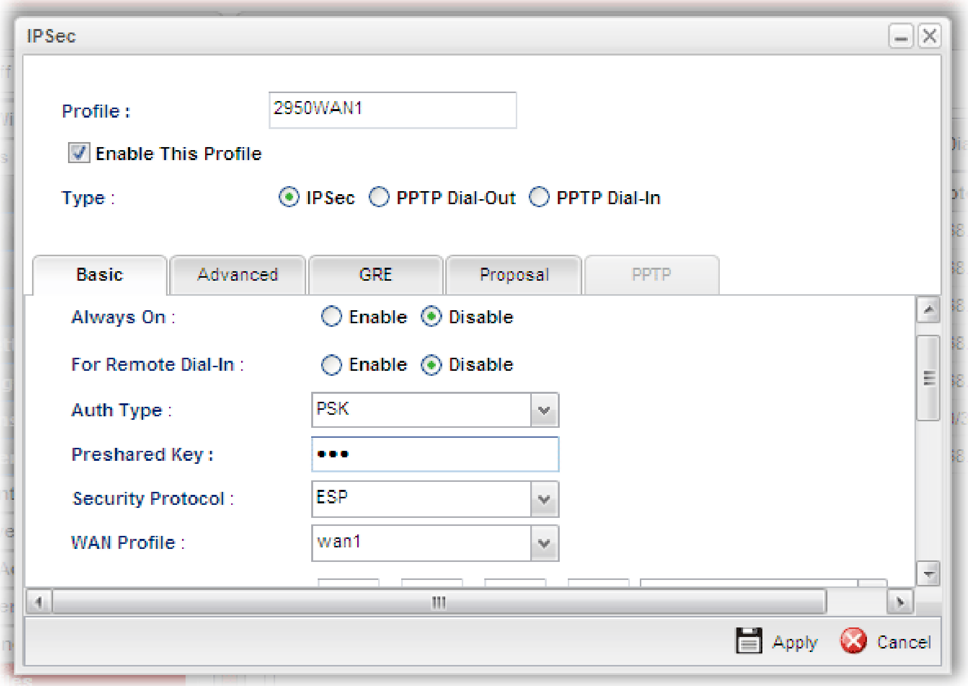
Vigor3900 allows users to build VPN load balance connection between Vigor3900 and other router. Take Vigor2950 for an example. There are two WANs on Vigor2950 and two WANs on Vigor3900. We will build VPN connection with load balance between Vigor3900 and two WANs of Vigor2950 respectively.

Configuring Vigor3900

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



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



IPSec

Profile : 2950WAN1

☑ Enable This Profile

Type : ● IPSec ○ PPTP Dial-Out ○ PPTP Dial-In

Basic | Advanced | GRE | Proposal | PPTP

Always On : ○ Enable ● Disable

For Remote Dial-In : ○ Enable ● Disable

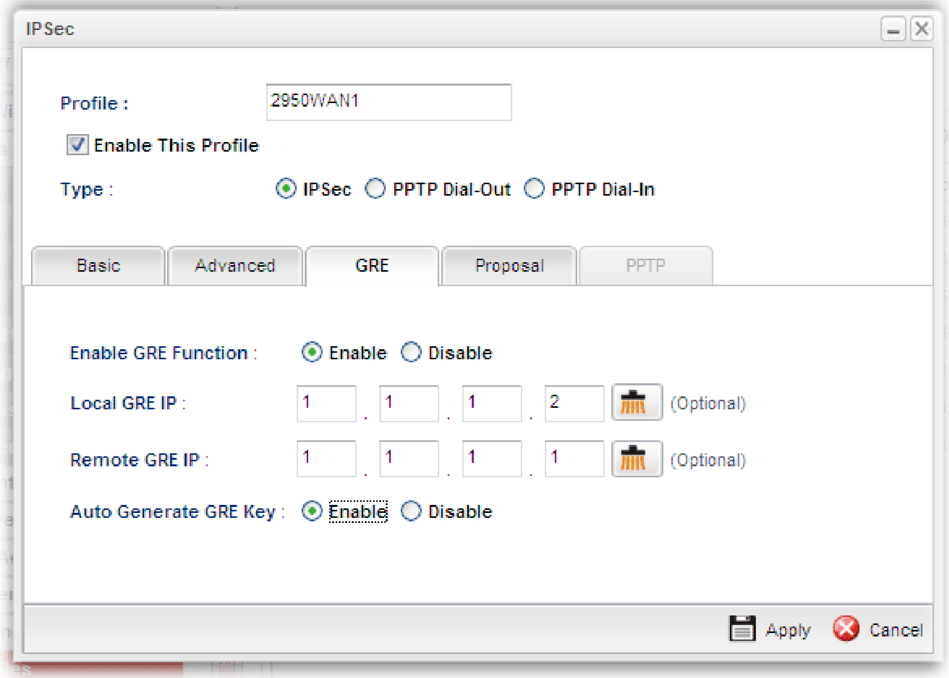
Auth Type : PSK

Preshared Key : •••

Security Protocol : ESP

WAN Profile : wan1

Apply Cancel



IPSec

Profile : 2950WAN1

☑ Enable This Profile

Type : ● IPSec ○ PPTP Dial-Out ○ PPTP Dial-In

Basic | Advanced | GRE | Proposal | PPTP

Enable GRE Function : ● Enable ○ Disable

Local GRE IP : 1 . 1 . 1 . 2 (Optional)

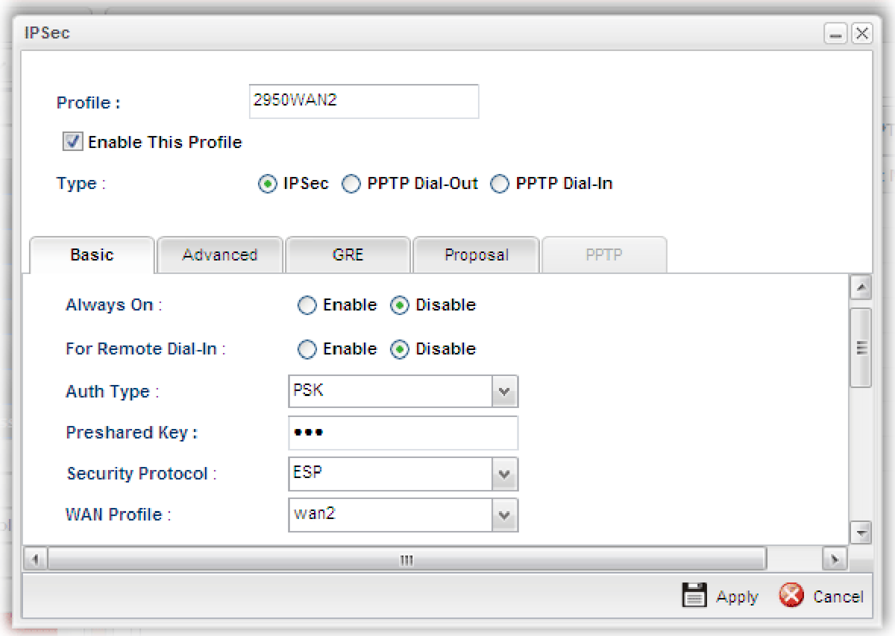
Remote GRE IP : 1 . 1 . 1 . 1 (Optional)

Auto Generate GRE Key : ● Enable ○ Disable

Apply Cancel

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

4. Create a profile for WAN 2 (named 2950WAN2).



IPSec

Profile : 2950WAN2

☑ Enable This Profile

Type : ● IPSec ○ PPTP Dial-Out ○ PPTP Dial-In

Always On : ○ Enable ● Disable

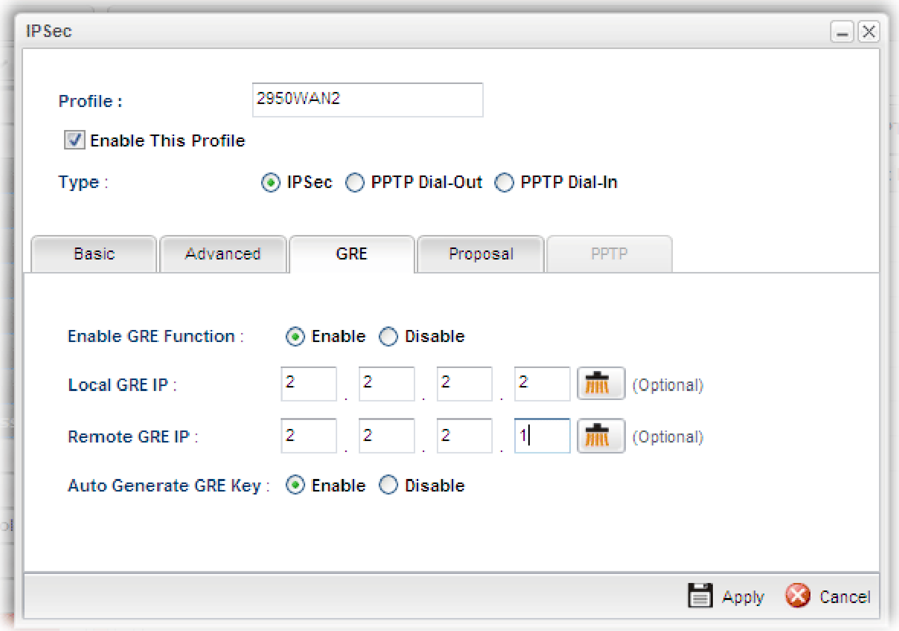
For Remote Dial-In : ○ Enable ● Disable

Auth Type : PSK

Preshared Key : •••

Security Protocol : ESP

WAN Profile : wan2



IPSec

Profile : 2950WAN2

☑ Enable This Profile

Type : ● IPSec ○ PPTP Dial-Out ○ PPTP Dial-In

Enable GRE Function : ● Enable ○ Disable

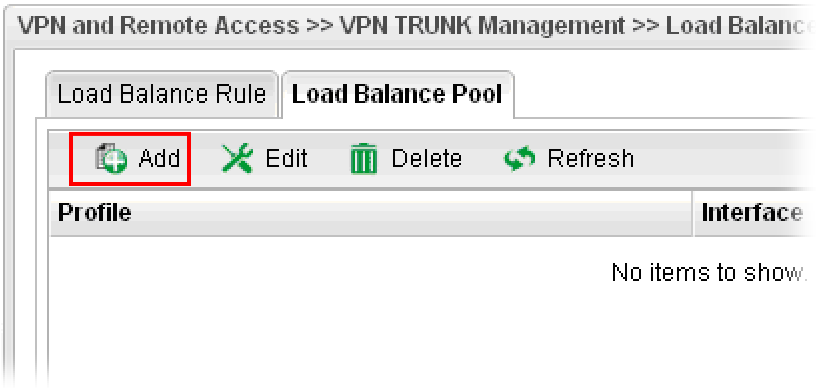
Local GRE IP : 2 . 2 . 2 . 2 (Optional)

Remote GRE IP : 2 . 2 . 2 . 1 (Optional)

Auto Generate GRE Key : ● Enable ○ Disable

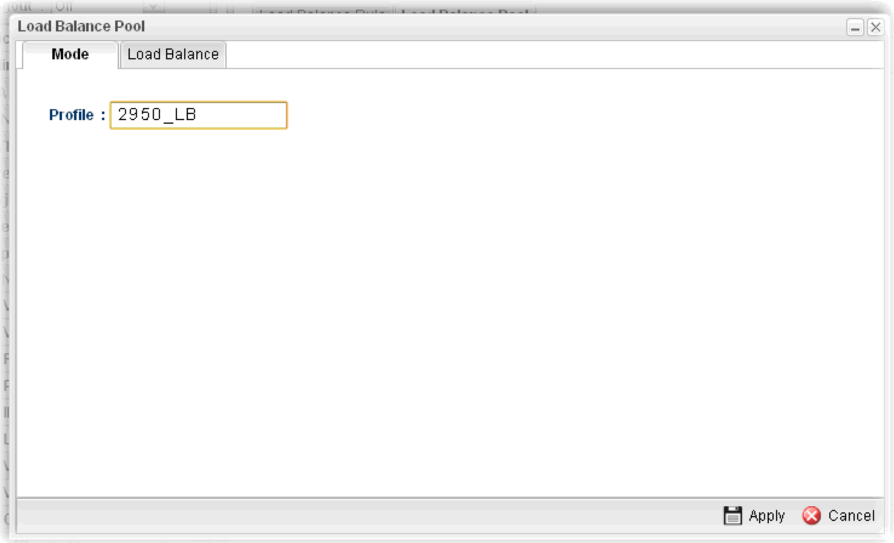
5. Click **Apply** to save the settings and exit the dialog.

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.


VPN and Remote Access >> VPN TRUNK Management >> Load Balanc

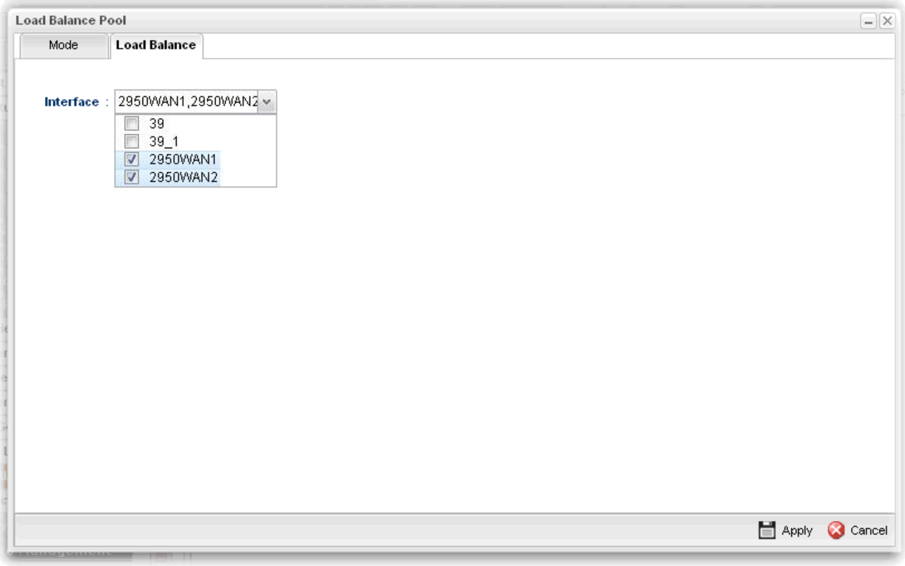
No items to show.

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



Profile : 2950_LB

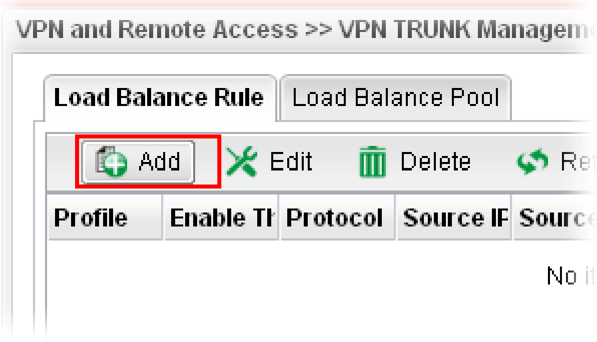
8. Click the **Load Balance** tab. Select the IPSec GRE profiles (e.g., 2950WAN1) set for Vigor2950 then click **Apply**.



Interface : 2950WAN1,2950WAN2

☐ 39
☐ 39_1
☑ 2950WAN1
☑ 2950WAN2

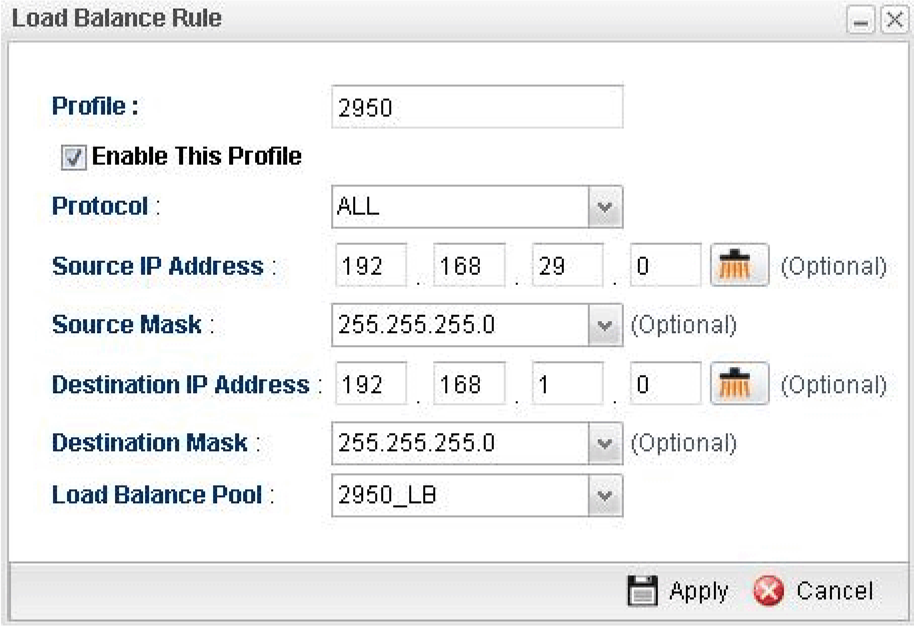
9. Click the **Load Balance Rule** tab and click **Add** to add a Load Balance rule profile.



VPN and Remote Access >> VPN TRUNK Managem

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.



Load Balance Rule

Profile : 2950

☑ Enable This Profile

Protocol : ALL

Source IP Address : 192 . 168 . 29 . 0 (Optional)

Source Mask : 255.255.255.0 (Optional)

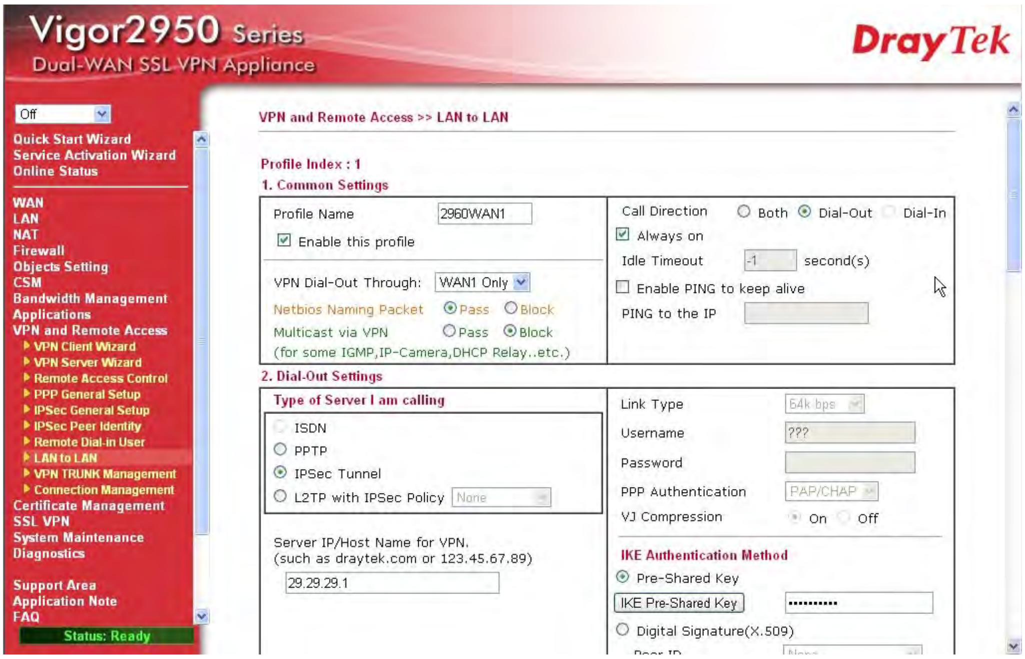
Destination IP Address : 192 . 168 . 1 . 0 (Optional)

Destination Mask : 255.255.255.0 (Optional)

Load Balance Pool : 2950_LB

Configuring Vigor2950

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



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: 2960WAN1

☑ Enable this profile

VPN Dial-Out Through: WAN1 Only

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction ○ Both ● Dial-Out ○ Dial-In

☑ Always on

Idle Timeout: -1 second(s)

☐ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

29.29.29.1

Link Type: 64k bps

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression ● On ○ Off

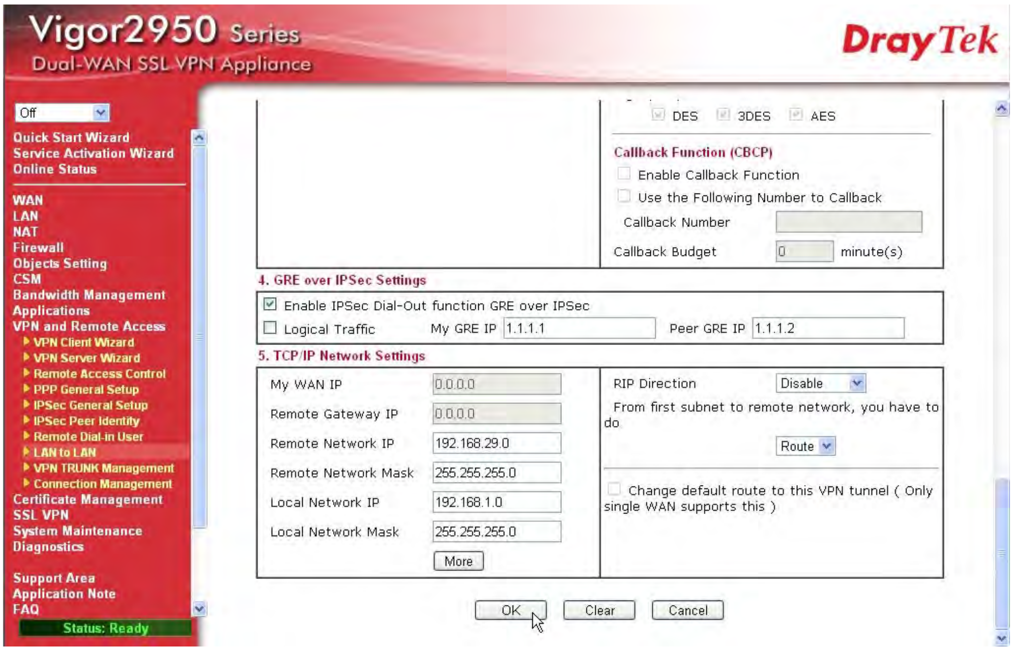
IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key: ••••••••••

○ Digital Signature(X.509)

- 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**.



☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number

Callback Budget 0 minute(s)

4. GRE over IPSec Settings

☑ Enable IPSec Dial-Out function GRE over IPSec

□ Logical Traffic My GRE IP 1.1.1.1 Peer GRE IP 1.1.1.2

5. TCP/IP Network Settings

My WAN IP 0.0.0.0

Remote Gateway IP 0.0.0.0

Remote Network IP 192.168.29.0

Remote Network Mask 255.255.255.0

Local Network IP 192.168.1.0

Local Network Mask 255.255.255.0

More

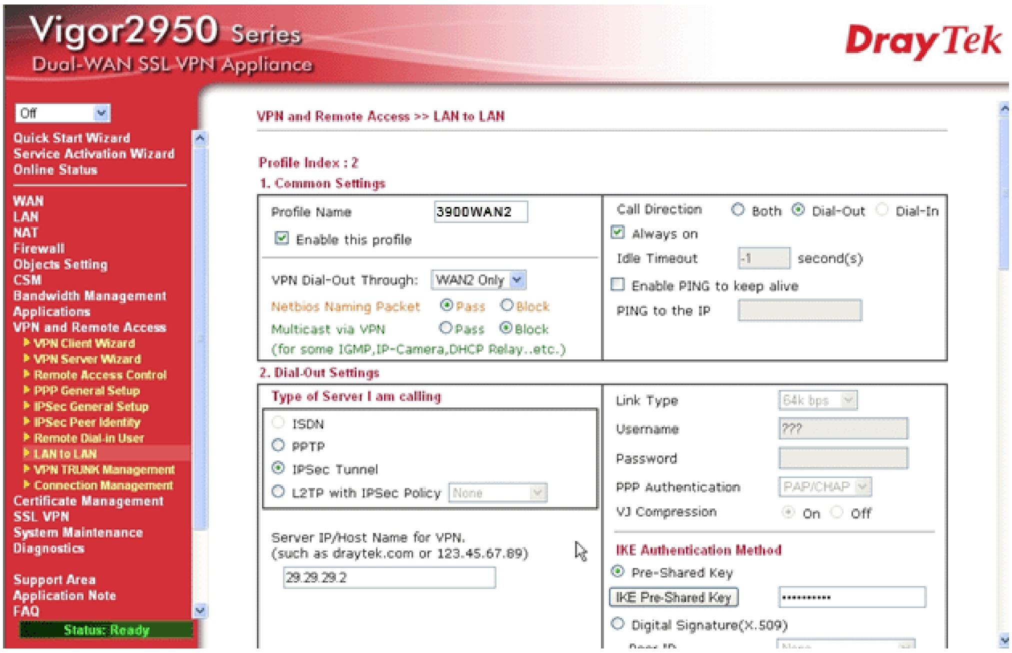
RIP Direction Disable

From first subnet to remote network, you have to do Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

- 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**.



VPN and Remote Access >> LAN to LAN

Profile Index : 2

1. Common Settings

Profile Name 3900WAN2

☑ Enable this profile

VPN Dial-Out Through: WAN2 Only

Netbios Naming Packet ● Pass ○ Block

Multicast via VPN ○ Pass ● Block

(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction ○ Both ● Dial-Out ○ Dial-In

☑ Always on

Idle Timeout -1 second(s)

□ Enable PING to keep alive

PING to the IP

2. Dial-Out Settings

Type of Server I am calling

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy None

Server IP/Host Name for VPN.

(such as draytek.com or 123.45.67.89)

29.29.29.2

Link Type 64k bps

Username ???

Password

PPP Authentication PAP/CHAP

VJ Compression ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

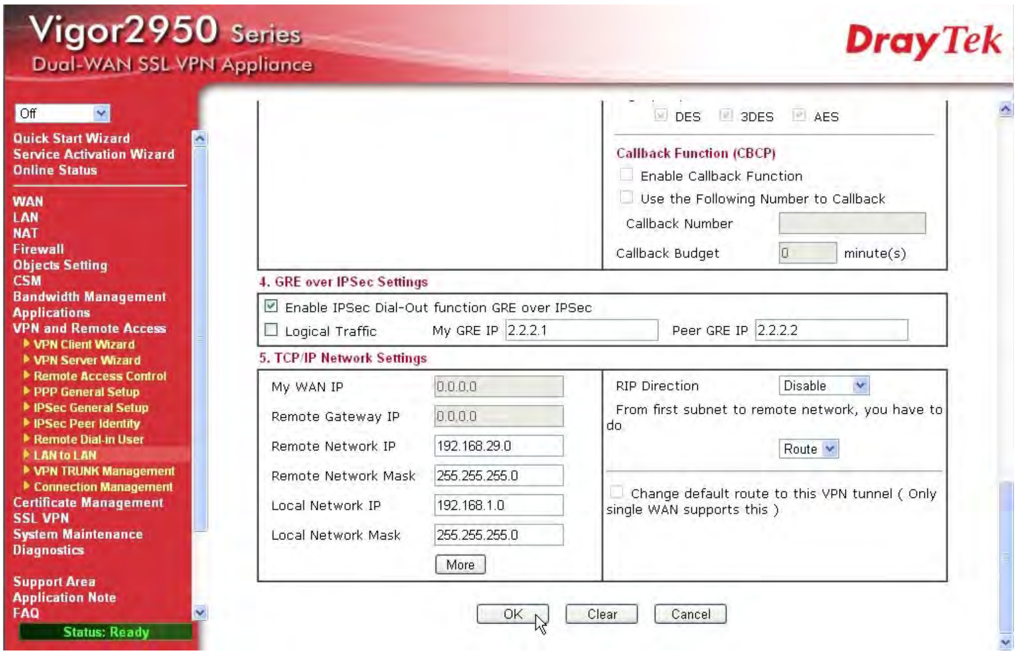
IKE Pre-Shared Key ••••••••••

○ Digital Signature(X.509)

- 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.



☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number

Callback Budget 0 minute(s)

4. GRE over IPSec Settings

☑ Enable IPSec Dial-Out function GRE over IPSec

□ Logical Traffic My GRE IP 2.2.2.1 Peer GRE IP 2.2.2.2

5. TCP/IP Network Settings

My WAN IP	0.0.0.0
Remote Gateway IP	0.0.0.0
Remote Network IP	192.168.29.0
Remote Network Mask	255.255.255.0
Local Network IP	192.168.1.0
Local Network Mask	255.255.255.0

More

RIP Direction Disable

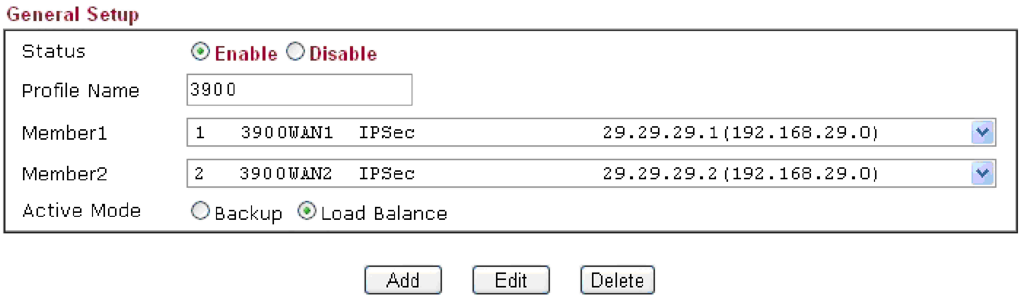
From first subnet to remote network, you have to do Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

OK Clear Cancel

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

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

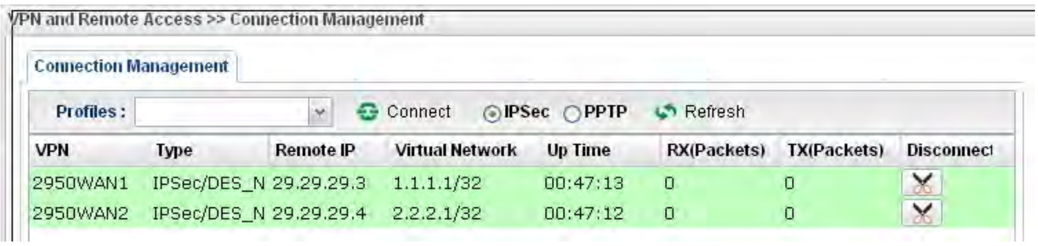


General Setup

Status	● Enable ○ Disable
Profile Name	3900
Member1	1 3900WAN1 IPSec 29.29.29.1(192.168.29.0)
Member2	2 3900WAN2 IPSec 29.29.29.2(192.168.29.0)
Active Mode	○ Backup ● Load Balance

Add Edit Delete

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



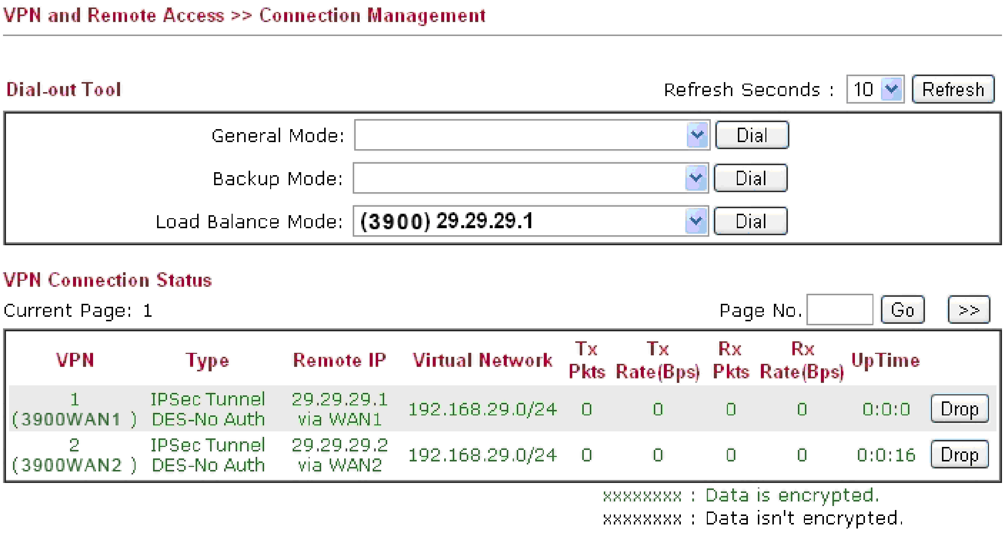
VPN and Remote Access >> Connection Management

Connection Management

Profiles : Connect ● IPSec ○ PPTP Refresh

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

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



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode:		Dial
Backup Mode:		Dial
Load Balance Mode:	(3900) 29.29.29.1	Dial

VPN Connection Status

Current Page: 1

Page No. Go >>

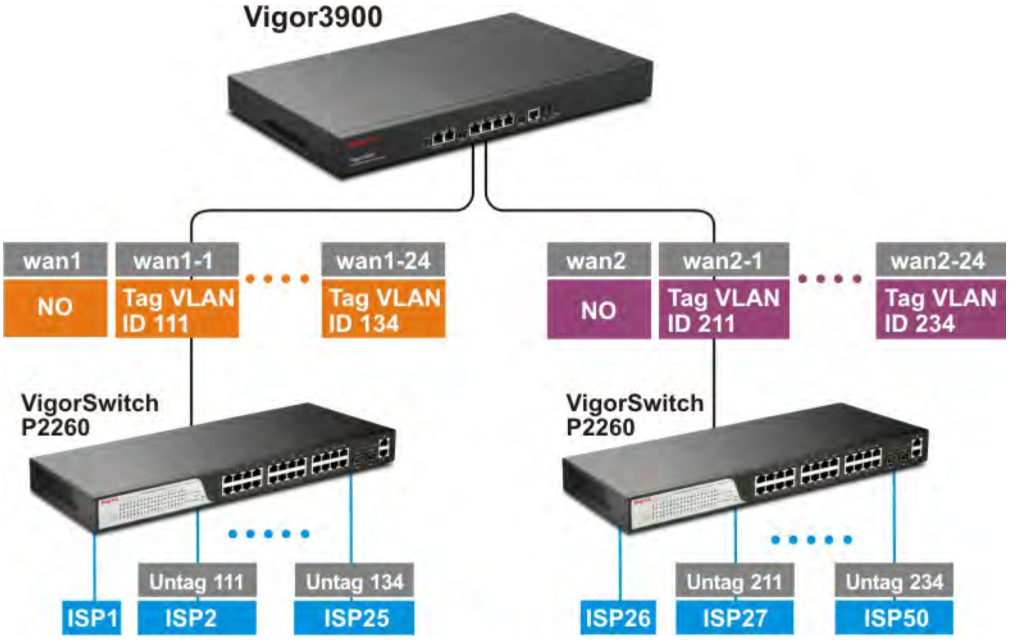
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (3900WAN1)	IPSec Tunnel DES-No Auth	29.29.29.1 via WAN1	192.168.29.0/24	0	0	0	0	0:0:0	Drop
2 (3900WAN2)	IPSec Tunnel DES-No Auth	29.29.29.2 via WAN2	192.168.29.0/24	0	0	0	0	0:0:16	Drop

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

3.6 How to Setup 50 WANs on Vigor3900

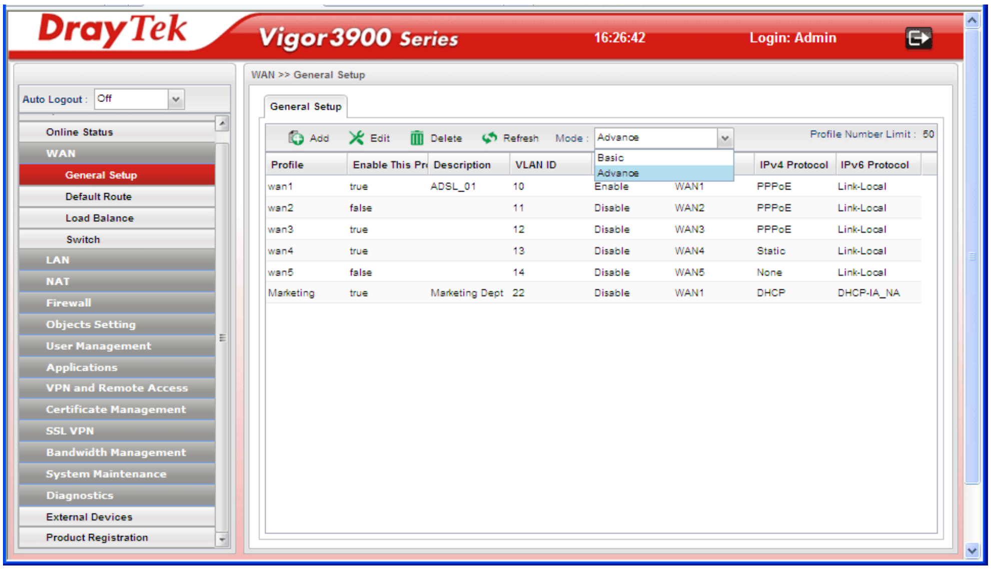
Vigor3900 has 5 physical WANs; however, it can be extended to 50 WANs at most by using VLAN Tagging technology.

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



Configuring 50 WAN profiles on Vigor3900

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

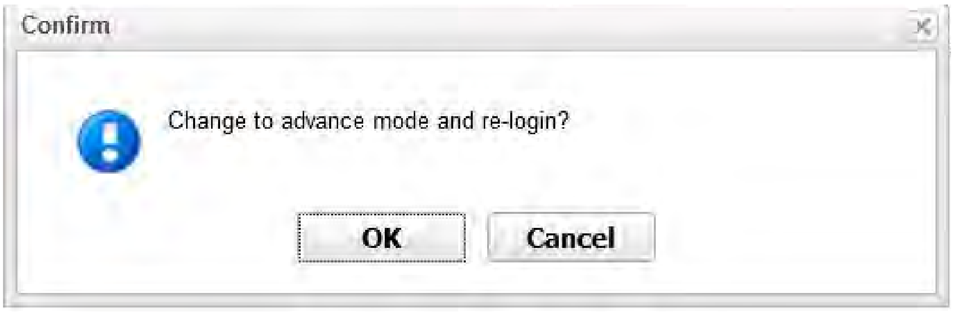


Mode : Advance

Profile Number Limit : 50

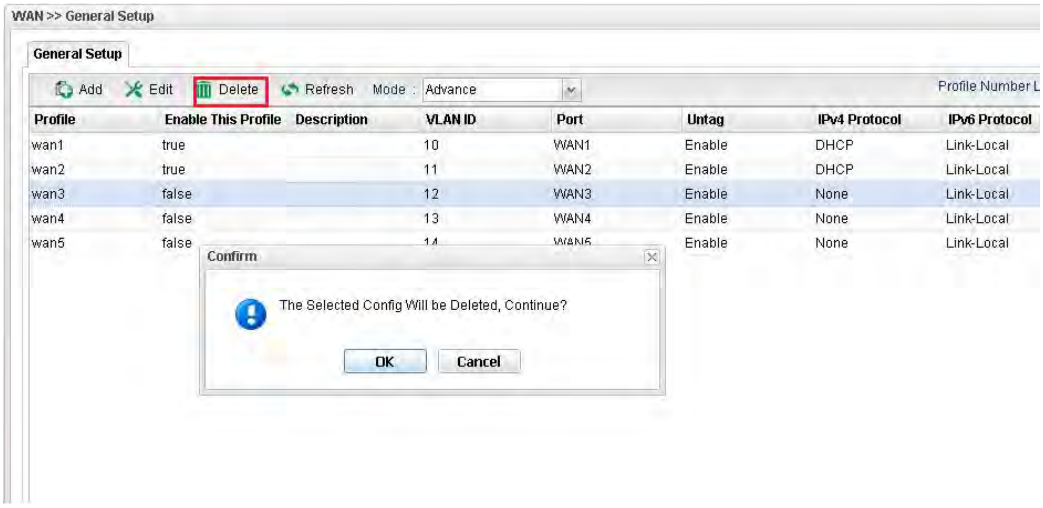
Profile	Enable This Pr	Description	VLAN ID			IPv4 Protocol	IPv6 Protocol
wan1	true	ADSL_01	10	Enable	WAN1	PPPoE	Link-Local
wan2	false		11	Disable	WAN2	PPPoE	Link-Local
wan3	true		12	Disable	WAN3	PPPoE	Link-Local
wan4	true		13	Disable	WAN4	Static	Link-Local
wan5	false		14	Disable	WAN5	None	Link-Local
Marketing	true	Marketing Dept	22	Disable	WAN1	DHCP	DHCP-IA_NA

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



Change to advance mode and re-login?

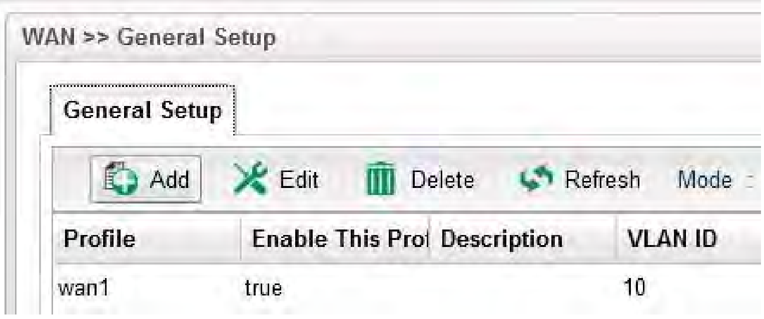
3. Delete default wan profiles for wan3, wan4 and wan5 by selecting the wan profile then click **Delete**.



Profile	Enable This Profile	Description	VLAN ID	Port	Untag	IPv4 Protocol	IPv6 Protocol
wan1	true		10	WAN1	Enable	DHCP	Link-Local
wan2	true		11	WAN2	Enable	DHCP	Link-Local
wan3	false		12	WAN3	Enable	None	Link-Local
wan4	false		13	WAN4	Enable	None	Link-Local
wan5	false		14	WAN5	Enable	None	Link-Local

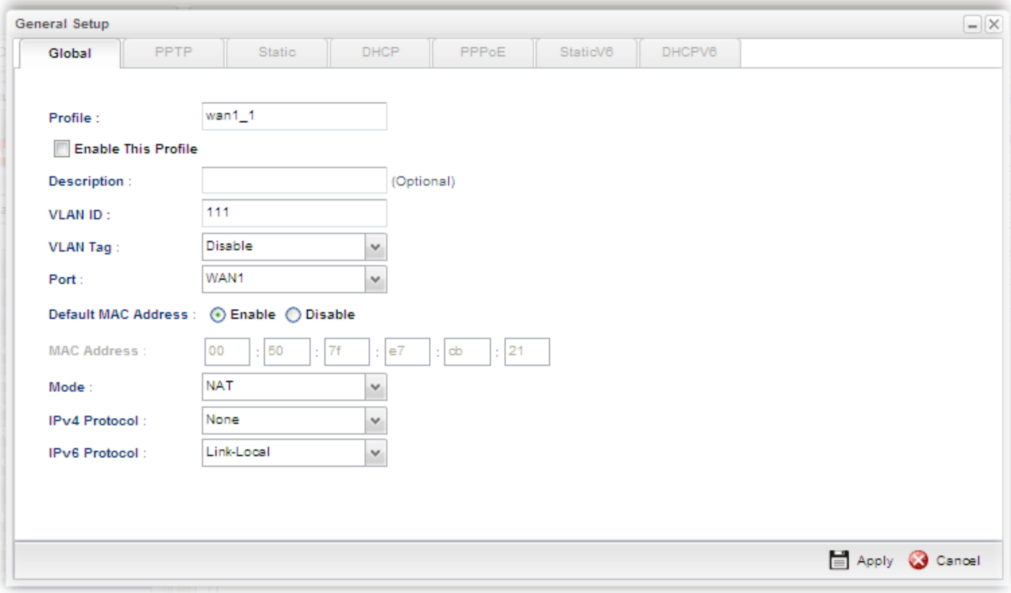
The Selected Config Will be Deleted, Continue?

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



Profile	Enable This Prof	Description	VLAN ID
wan1	true		10

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.



Profile : wan1_1

□ Enable This Profile

Description : (Optional)

VLAN ID : 111

VLAN Tag : Disable

Port : WAN1

Default MAC Address : ● Enable ○ Disable

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

Mode : NAT

IPv4 Protocol : None

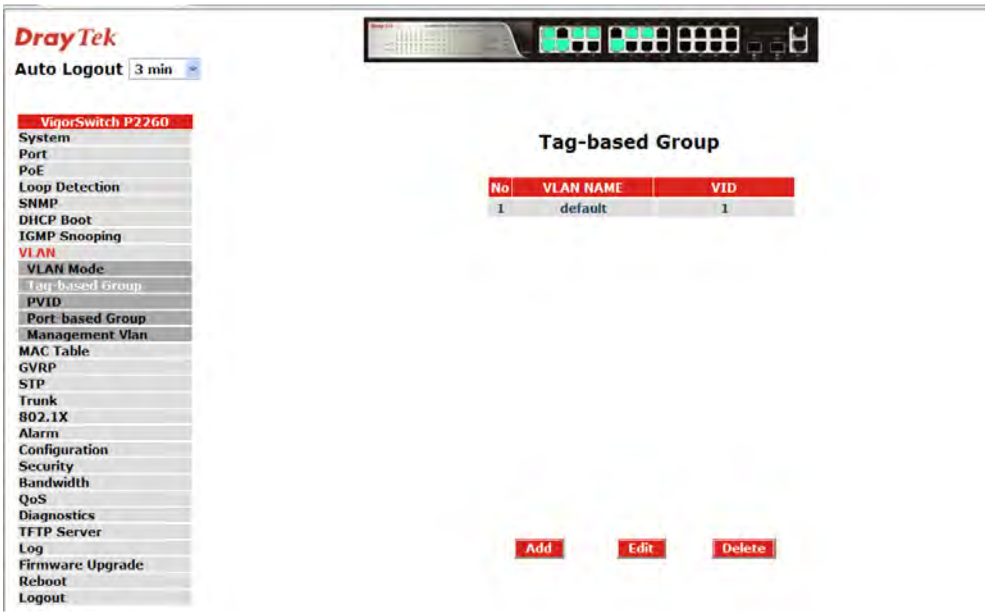
IPv6 Protocol : Link-Local

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**.

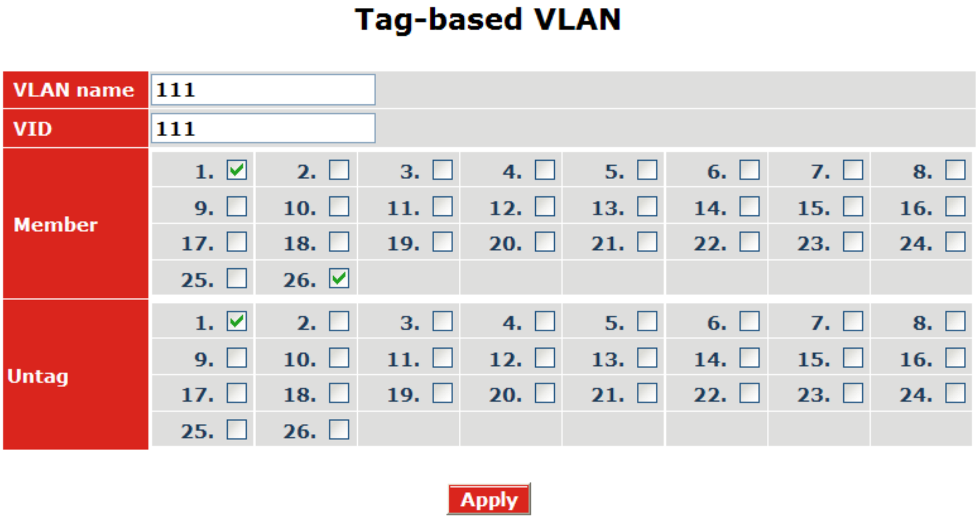
2. Click **Add** to create a New VLAN GROUP via **VLAN>>TAG-based Group** page.



Tag-based Group

No	VLAN NAME	VID
1	default	1

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



Tag-based VLAN

VLAN name	111
VID	111

Member

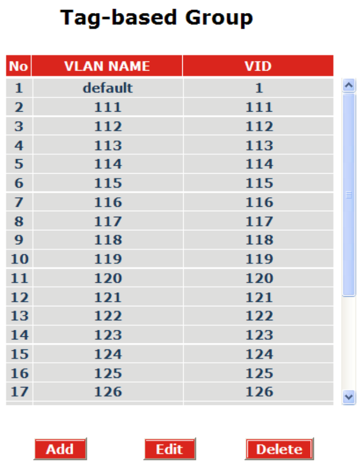
1. ☑	2. □	3. □	4. □	5. □	6. □	7. □	8. □
9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
25. □	26. ☑						

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. □						

- 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.

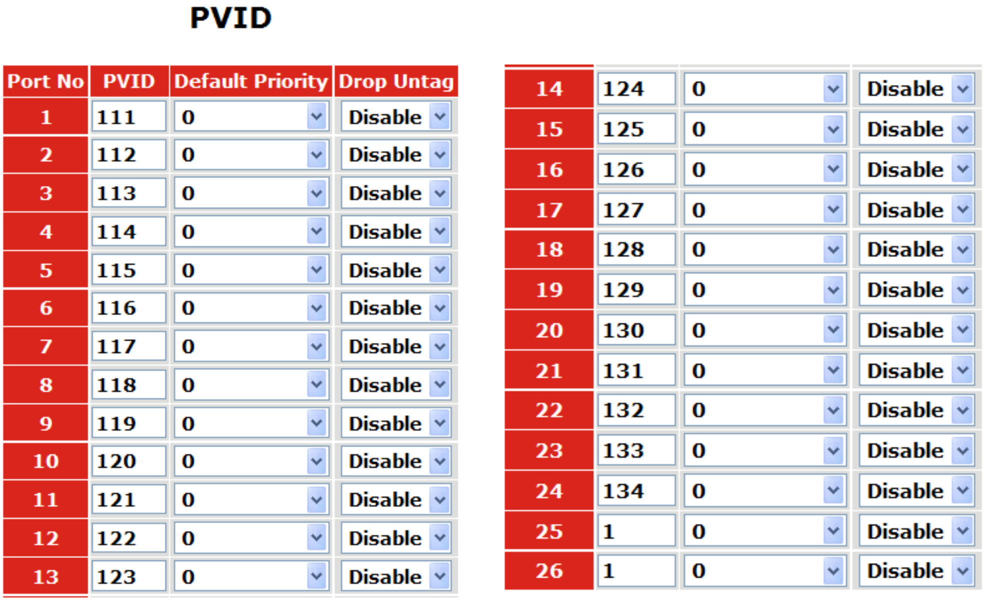
4. Create the rest VLAN Groups (total is 24) by referring to the following figure. Please notice that Port 26 must be selected as the member for each group, for it is the channel for any packets coming from Vigor3900. As to Untag, when you check Port 2 and Port 26, you have to untag Port 2; when you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

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



PVID

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

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

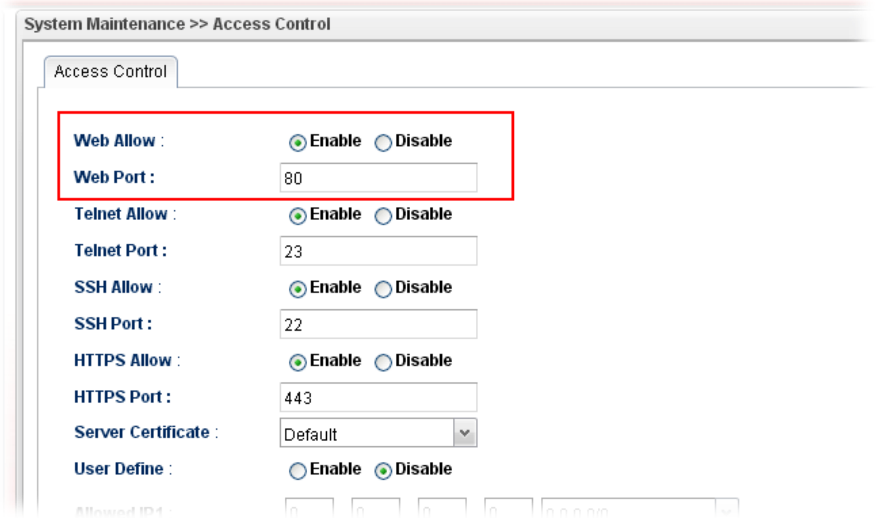
6. After finishing the configuration for one VigorSwitch, please set for another VigorSwitch with the same procedure. The file names shall be wan2_1~ wan2_24 and the VLAN ID shall be set as 211~ 234.

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

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

3.7.1 Configure Settings on Vigor3900

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

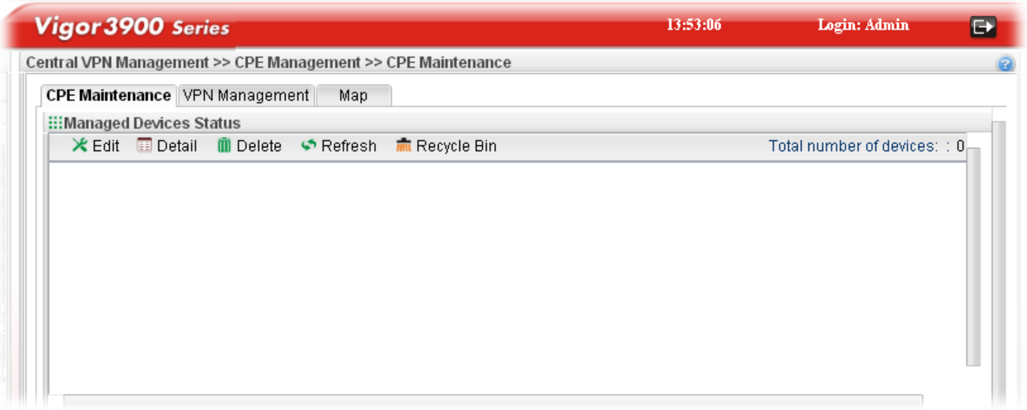


System Maintenance >> Access Control

Access Control

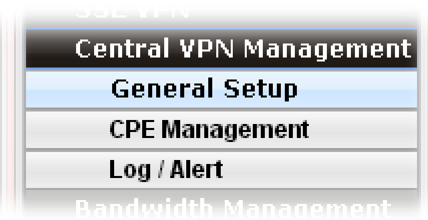
Web Allow :	● Enable ○ Disable
Web Port :	80
Telnet Allow :	● Enable ○ Disable
Telnet Port :	23
SSH Allow :	● Enable ○ Disable
SSH Port :	22
HTTPS Allow :	● Enable ○ Disable
HTTPS Port :	443
Server Certificate :	Default
User Define :	○ Enable ● Disable

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

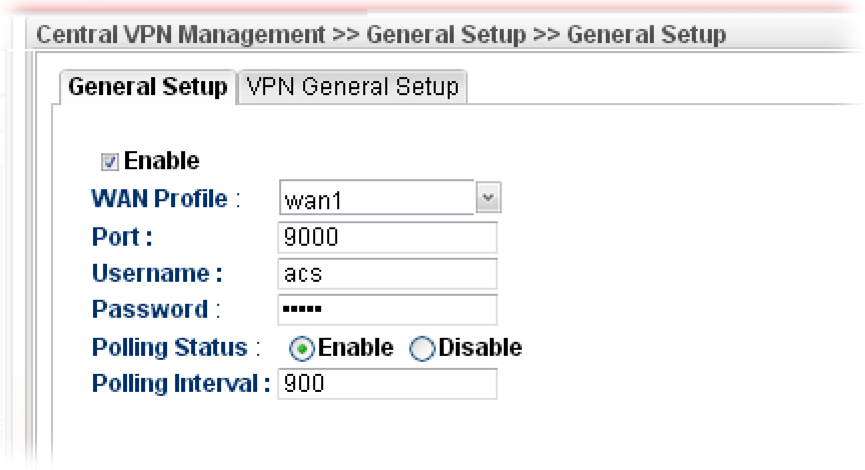


Total number of devices: : 0

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



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



Central VPN Management >> General Setup >> General Setup

General Setup | VPN General Setup

☑ Enable

WAN Profile : wan1

Port : 9000

Username : acs

Password : •••••

Polling Status : ● Enable ○ Disable

Polling Interval : 900

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

3.7.2 Configure Settings on CPE

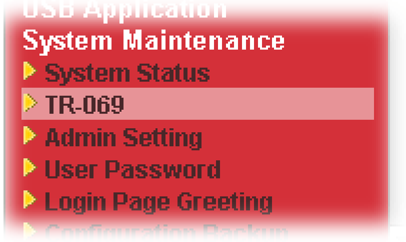
To manage CPEs through Vigor3900, you have to set ACS URL on CPE first and set username and password for Vigor3900.

1. Connect one CPE (e.g., Vigor2830 series) and get ready to access into the web user interface of the CPE.

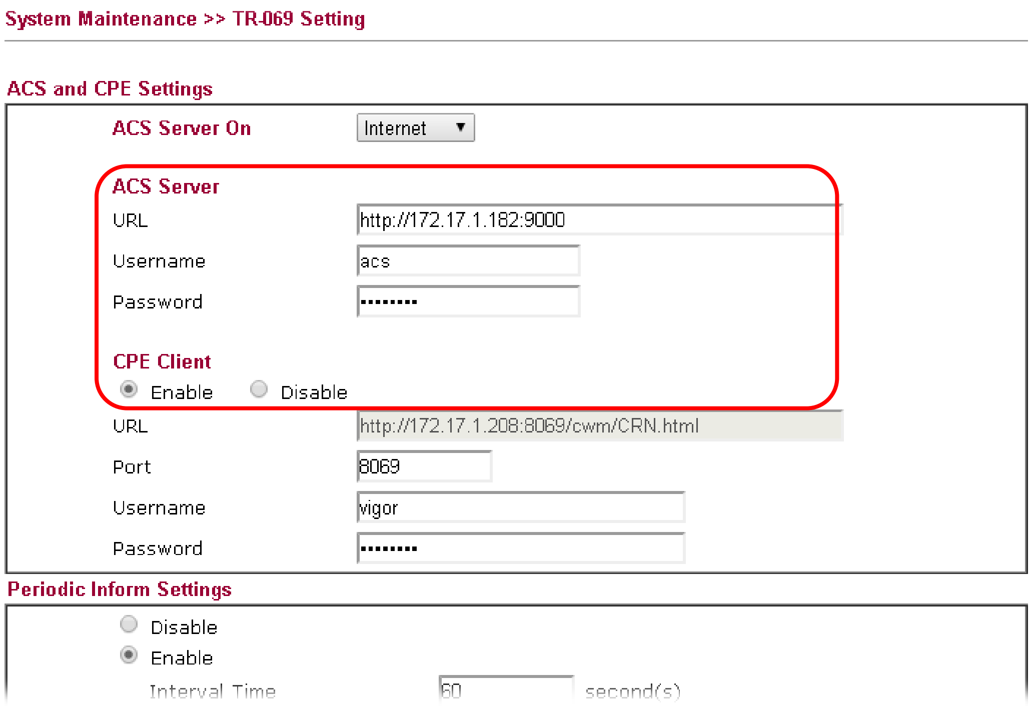
2. Open a web browser (for example, **IE**, **Mozilla Firefox** or **Netscape**) on your computer and type **http://192.168.1.1.**

3. Please type username and password on the window. If you don’t know the correct username and password, please consult our dealer to get them.

4. Open **System Maintenance** >> **TR-069**.



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



System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On: Internet ▼

ACS Server

URL: http://172.17.1.182:9000

Username: acs

Password: ••••••••

CPE Client

● Enable ○ Disable

URL: http://172.17.1.208:8069/cwm/CRN.html

Port: 8069

Username: vigor

Password: ••••••••

Periodic Inform Settings

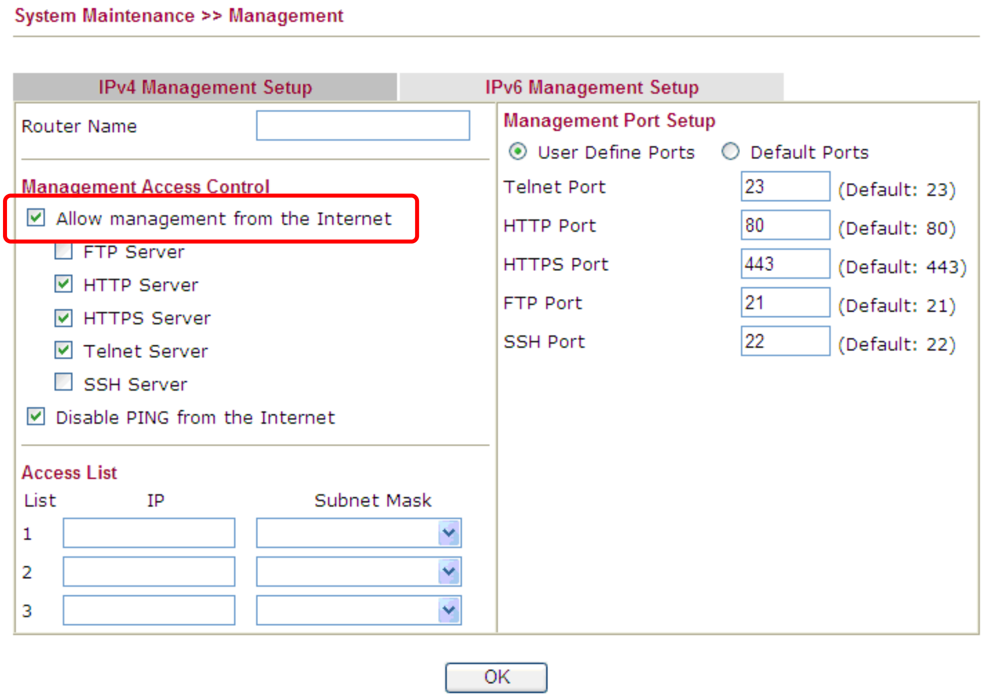
○ Disable

● Enable

Interval Time: 60 second(s)

3.7.3 Invoke Remote Management for CPE

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



System Maintenance >> Management

IPv4 Management Setup | IPv6 Management Setup

Router Name:

Management Access Control

☑ Allow management from the Internet

□ FTP Server

☑ HTTP Server

☑ HTTPS Server

☑ Telnet Server

□ SSH Server

☑ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1		
2		
3		

Management Port Setup

● User Define Ports ○ Default Ports

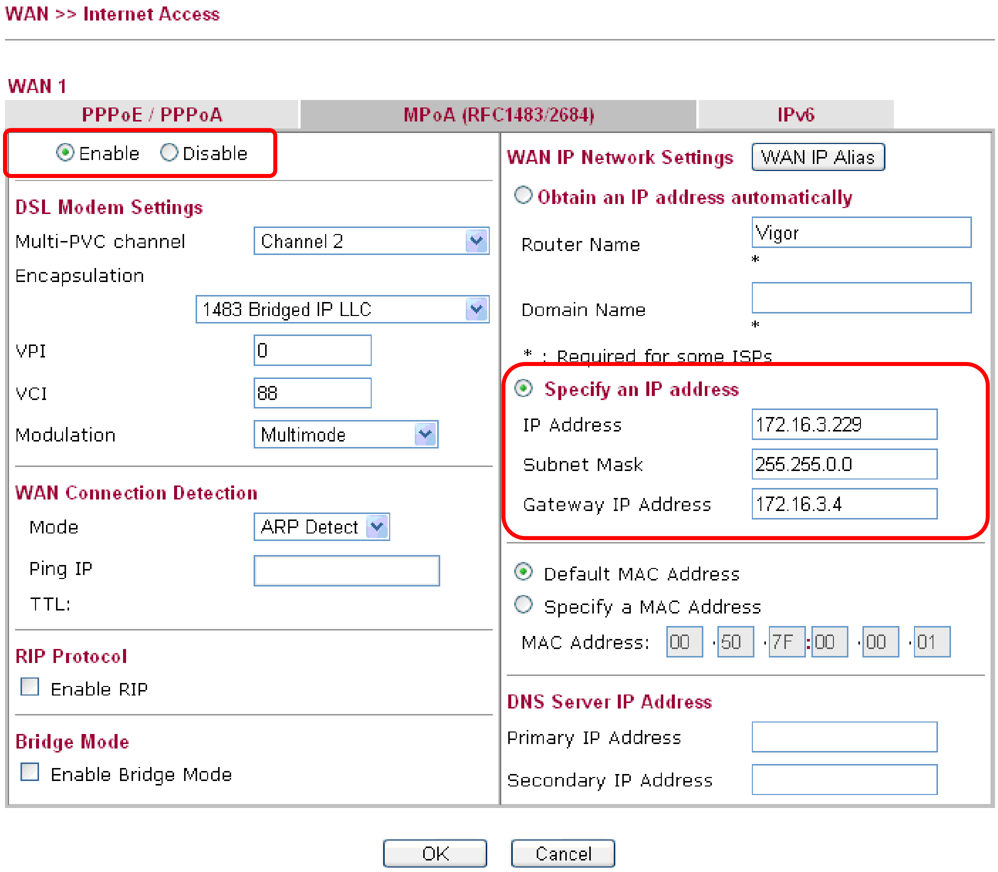
Telnet Port	23	(Default: 23)
HTTP Port	80	(Default: 80)
HTTPS Port	443	(Default: 443)
FTP Port	21	(Default: 21)
SSH Port	22	(Default: 22)

3.7.4 Enable WAN Connection on CPE

1. Login the web user interface of the CPE.

2. Open **WAN>>Internet Access.** Use the drop down list of **Access Mode** on WAN1 to select **MPoA** (RFC1483/2684). Then, click **Details Page**.

3. Click **Specify an IP address**. Type correct WAN IP address, subnet mask and gateway IP address for your CPE. Then click **OK**.



WAN >> Internet Access

WAN 1

PPPoE / PPPoA | MPoA (RFC1483/2684) | IPv6

● Enable ○ Disable

DSL Modem Settings

Multi-PVC channel: Channel 2

Encapsulation: 1483 Bridged IP LLC

VPI: 0

VCI: 88

Modulation: Multimode

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

RIP Protocol

□ Enable RIP

Bridge Mode

□ Enable Bridge Mode

WAN IP Network Settings [WAN IP Alias]

○ Obtain an IP address automatically

Router Name: Vigor *

Domain Name: *

* : Required for some ISPs

● Specify an IP address

IP Address: 172.16.3.229

Subnet Mask: 255.255.0.0

Gateway IP Address: 172.16.3.4

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 : 50 : 7F : 00 : 00 : 01

DNS Server IP Address

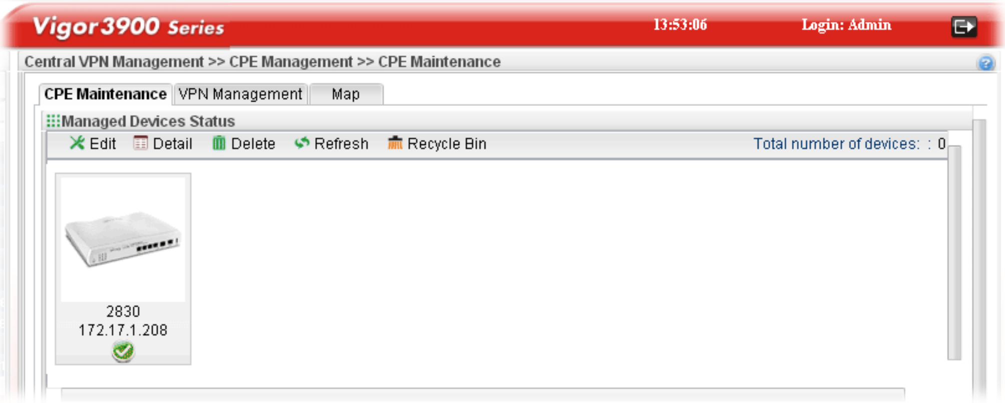
Primary IP Address:

Secondary IP Address:

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

3.7.5 Check CPE Maintenance Page

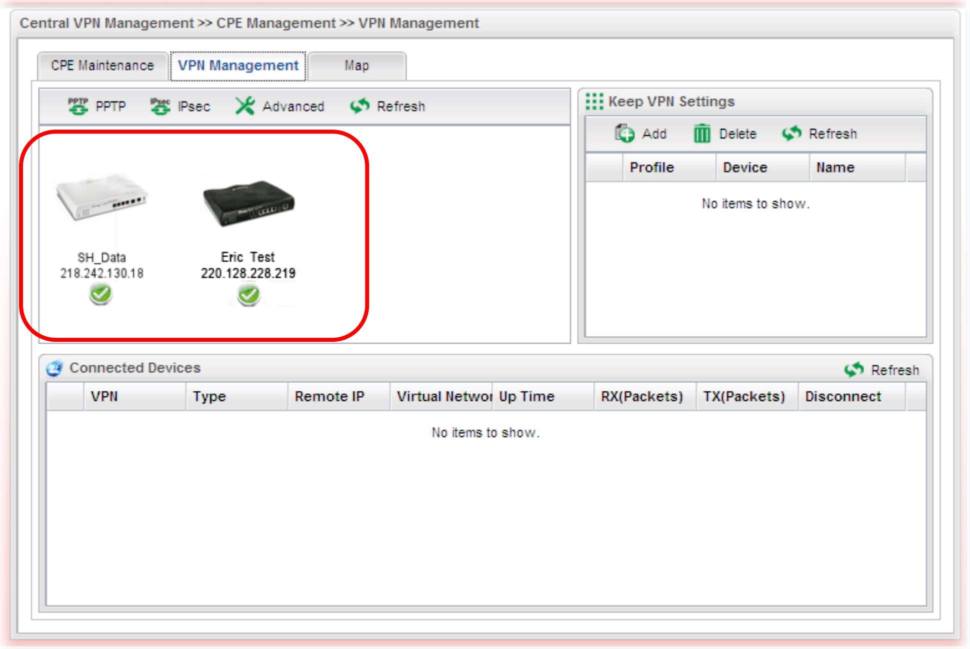
1. Return to the web user interface of Vigor3900.
2. Open **Central VPN Management>>CPE Management.**
3. Now there is one CPE managed (Vigor2830) by Vigor3900 on the page of **CPE Maintenance**.



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

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

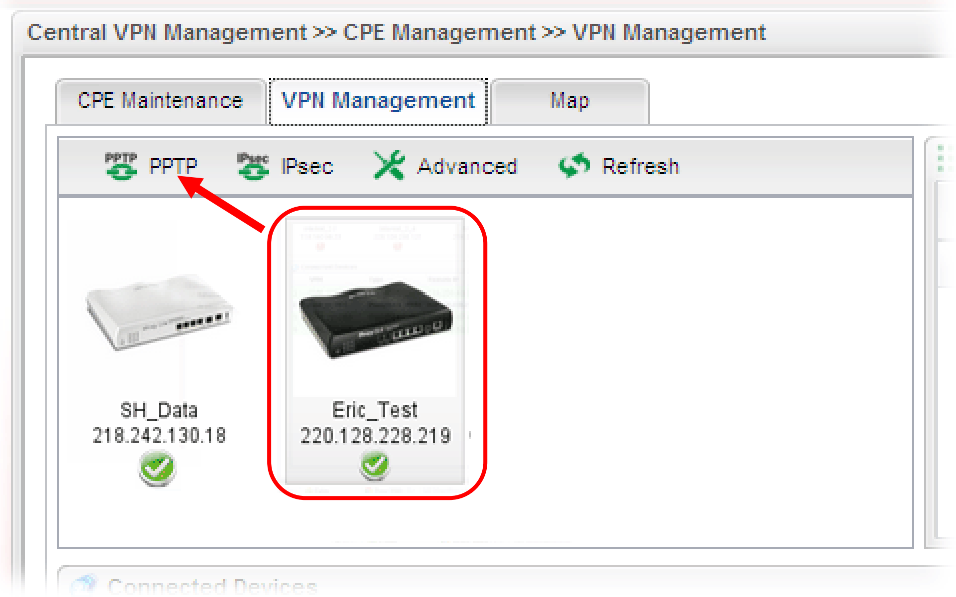
1. Access into the web user interface of Vigor3900 series.
2. Open **Central VPN Management>>CPE Management**. The icons displayed on the screen means the remote devices are ready for building VPN with Vigor3900.



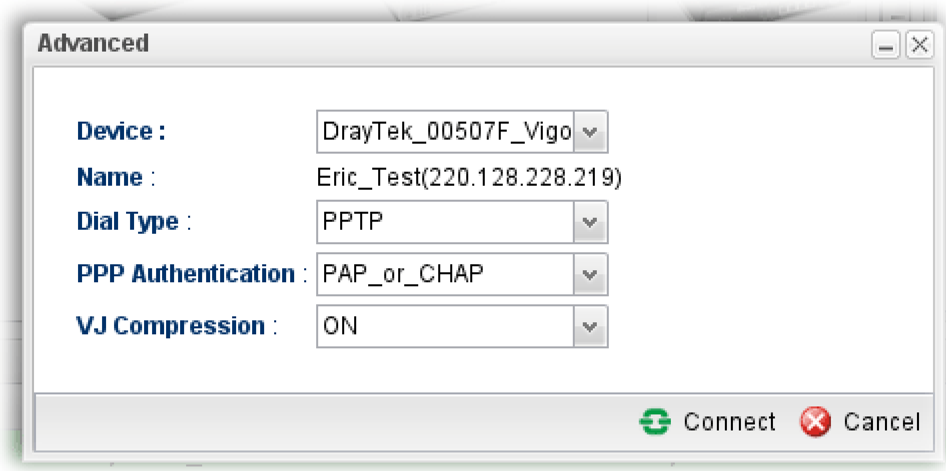
Profile	Device	Name
No items to show.		

VPN	Type	Remote IP	Virtual Networ	Up Time	RX(Packets)	TX(Packets)	Disconnect
No items to show.							

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



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



Advanced

Device : DrayTek_00507F_Vigo

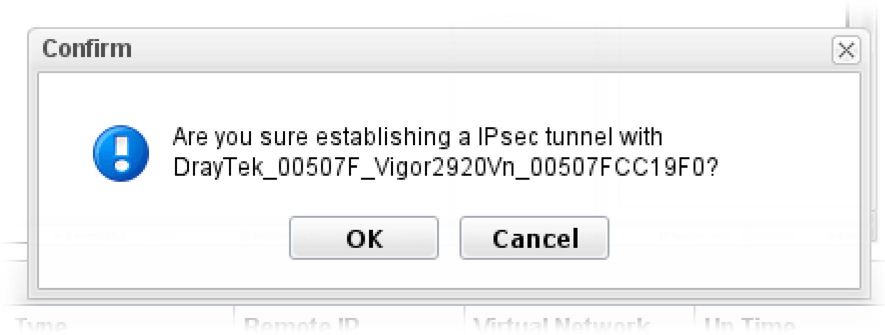
Name : Eric_Test(220.128.228.219)

Dial Type : PPTP

PPP Authentication : PAP_or_CHAP

VJ Compression : ON

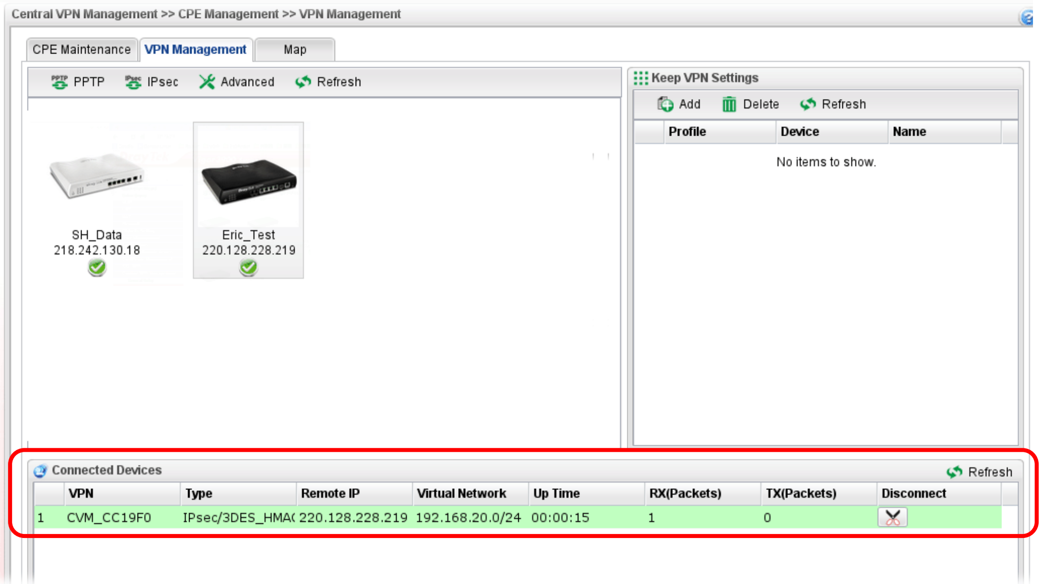
4. A confirmation dialog will appear. Click **OK** and wait for a moment.



Confirm

Are you sure establishing a IPsec tunnel with DrayTek_00507F_Vigor2920Vn_00507FCC19F0?

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



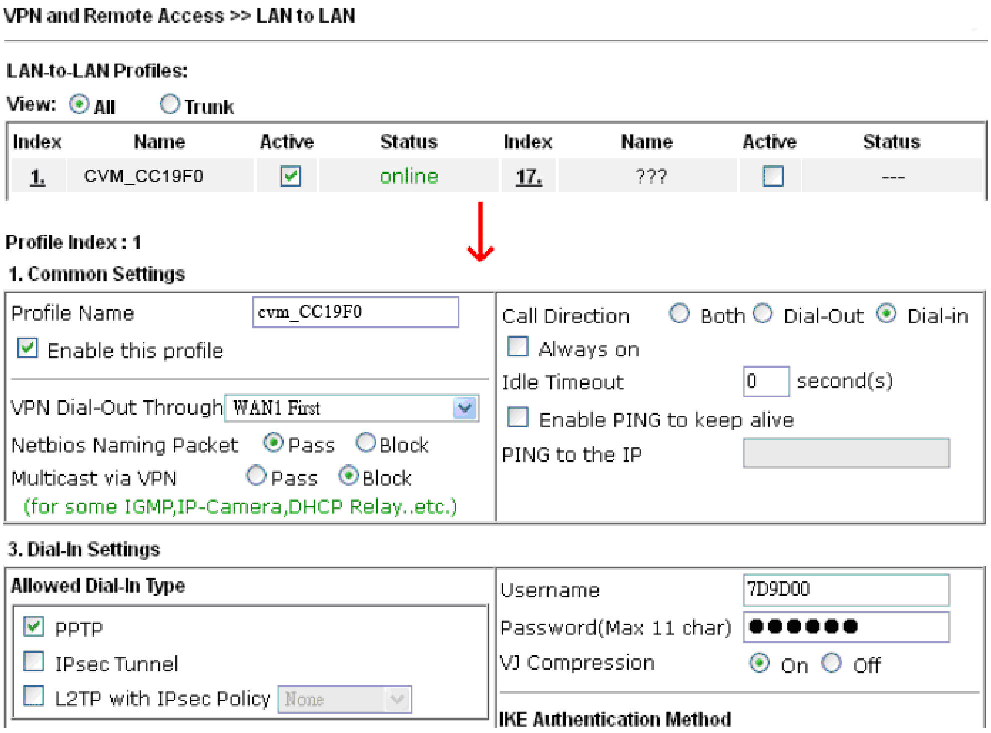
Profile	Device	Name

No items to show.

Connected Devices

	VPN	Type	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect
1	CVM_CC19F0	IPsec/3DES_HMA(	220.128.228.219	192.168.20.0/24	00:00:15	1	0	✕

6. A LAN to LAN profile for such VPN will be generated automatically. You can access into **VPN and Remote Access>>LAN to LAN** of the remote device for viewing the detailed information.



VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: ● All ○ Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	CVM_CC19F0	☑	online	17.	???	□	---

Profile Index : 1

1. Common Settings

Profile Name: cvm_CC19F0	Call Direction: ○ Both ○ Dial-Out ● Dial-in
☑ Enable this profile	□ Always on
VPN Dial-Out Through: WAN1 First	Idle Timeout: 0 second(s)
Netbios Naming Packet: ● Pass ○ Block	□ Enable PING to keep alive
Multicast via VPN: ○ Pass ● Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	PING to the IP

3. Dial-In Settings

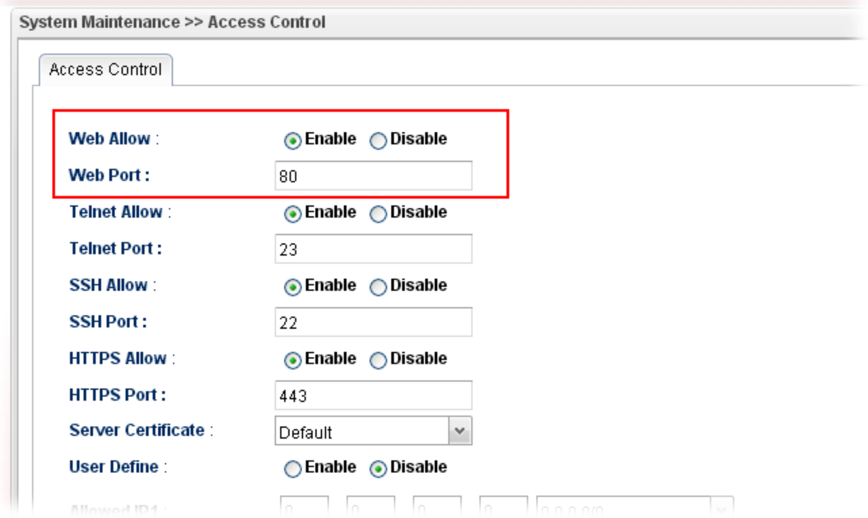
Allowed Dial-In Type	Username: 7D9D00
☑ PPTP	Password(Max 11 char): ●●●●●●
□ IPsec Tunnel	VJ Compression: ● On ○ Off
□ L2TP with IPsec Policy: None	IKE Authentication Method

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

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

3.9.1 Import firmware file from your PC to Vigor3900

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

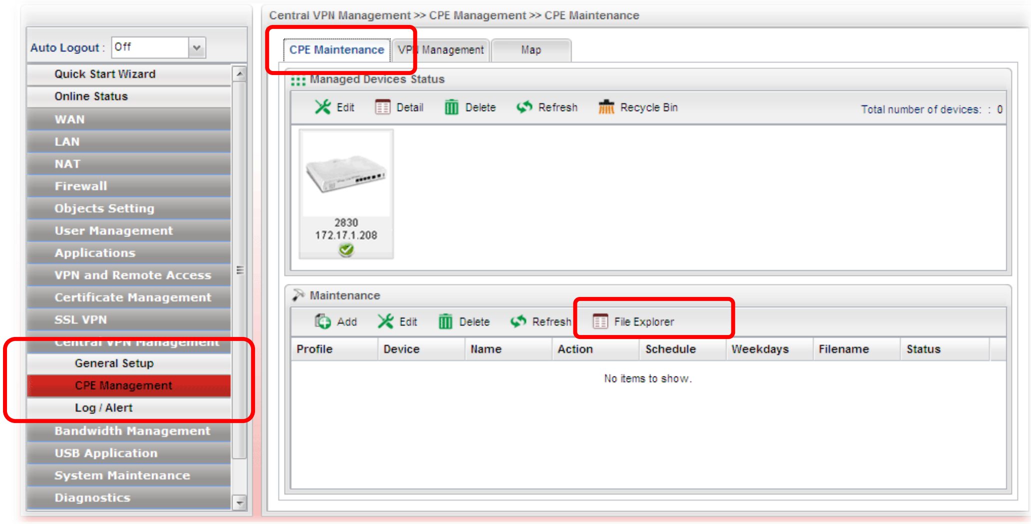


System Maintenance >> Access Control

Access Control

Web Allow :	● Enable ○ Disable
Web Port :	80
Telnet Allow :	● Enable ○ Disable
Telnet Port :	23
SSH Allow :	● Enable ○ Disable
SSH Port :	22
HTTPS Allow :	● Enable ○ Disable
HTTPS Port :	443
Server Certificate :	Default
User Define :	○ Enable ● Disable

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



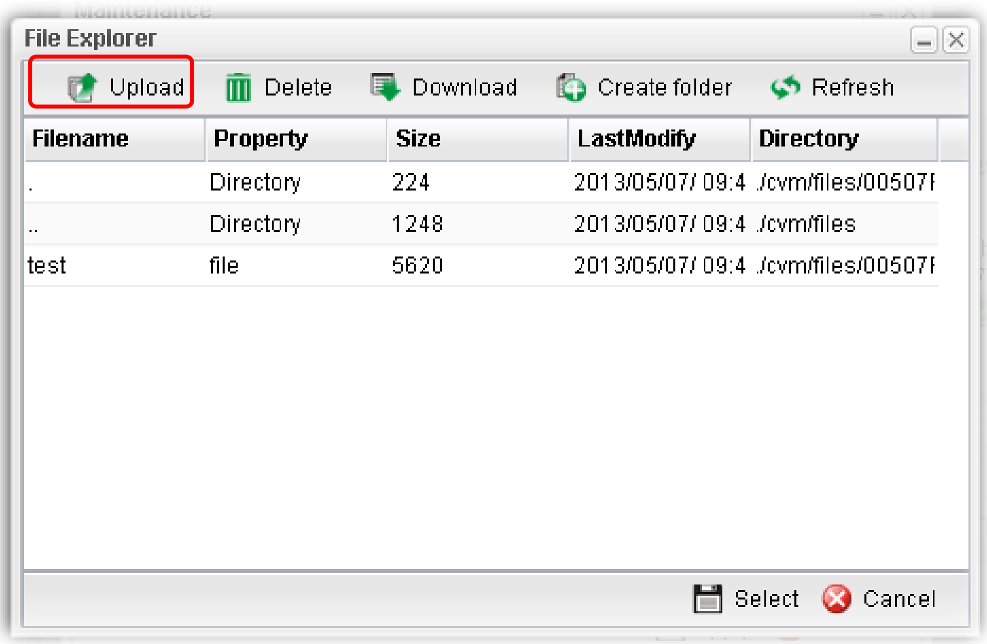
Central VPN Management >> CPE Management >> CPE Maintenance

Auto Logout : Off

Profile	Device	Name	Action	Schedule	Weekdays	Filename	Status

No items to show.

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

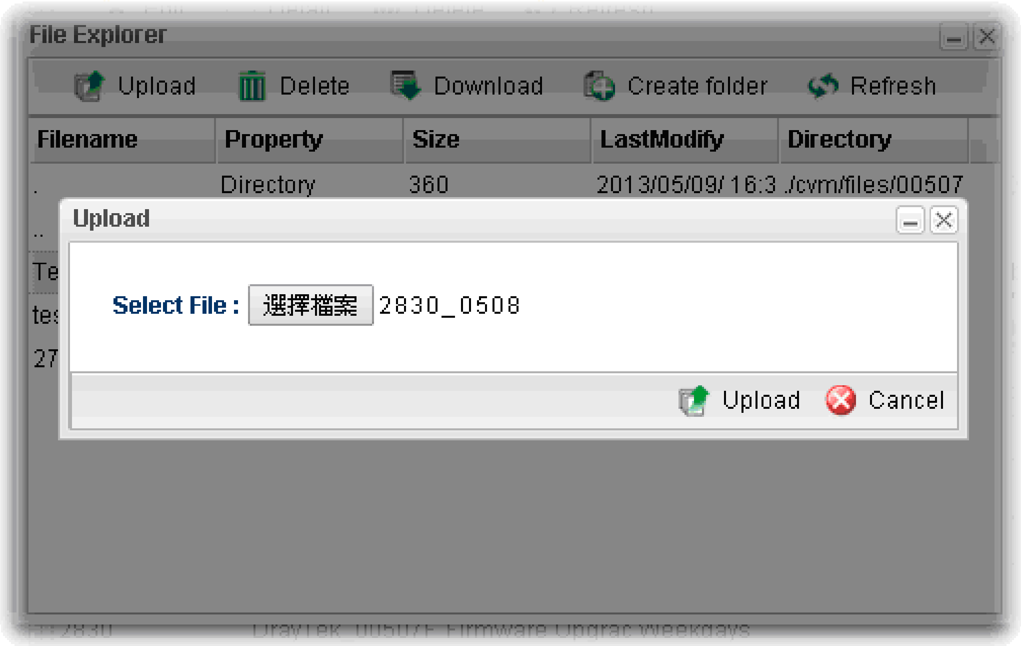


File Explorer

Upload | Delete | Download | Create folder | Refresh

Filename	Property	Size	LastModify	Directory
.	Directory	224	2013/05/07/ 09:4	./cvm/files/00507F
..	Directory	1248	2013/05/07/ 09:4	./cvm/files
test	file	5620	2013/05/07/ 09:4	./cvm/files/00507F

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



File Explorer

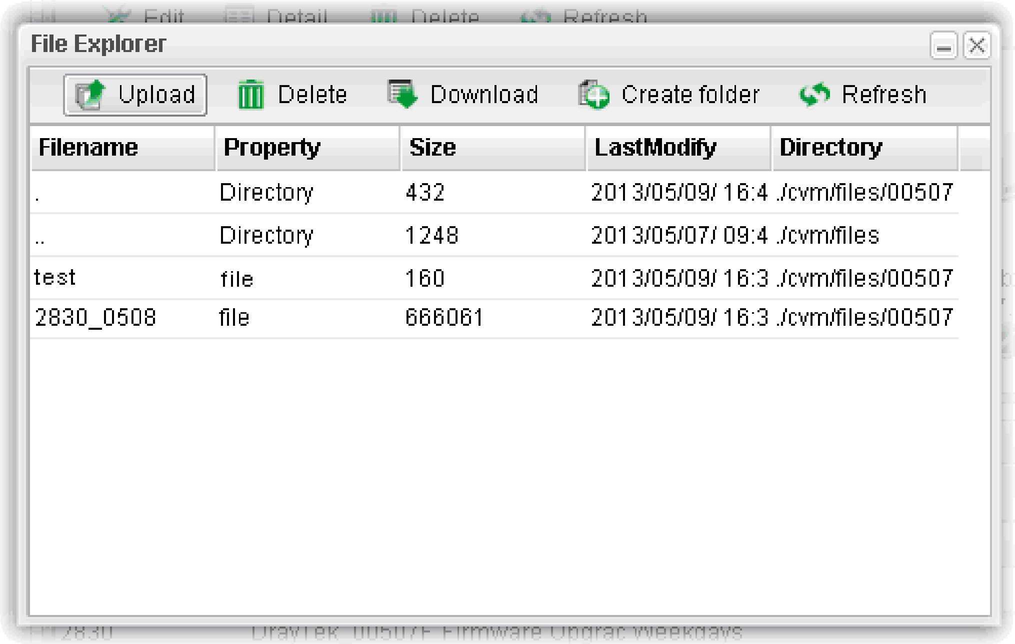
Upload | Delete | Download | Create folder | Refresh

Filename	Property	Size	LastModify	Directory
.	Directory	360	2013/05/09/ 16:3	./cvm/files/00507

Upload

Select File : 選擇檔案 2830_0508

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

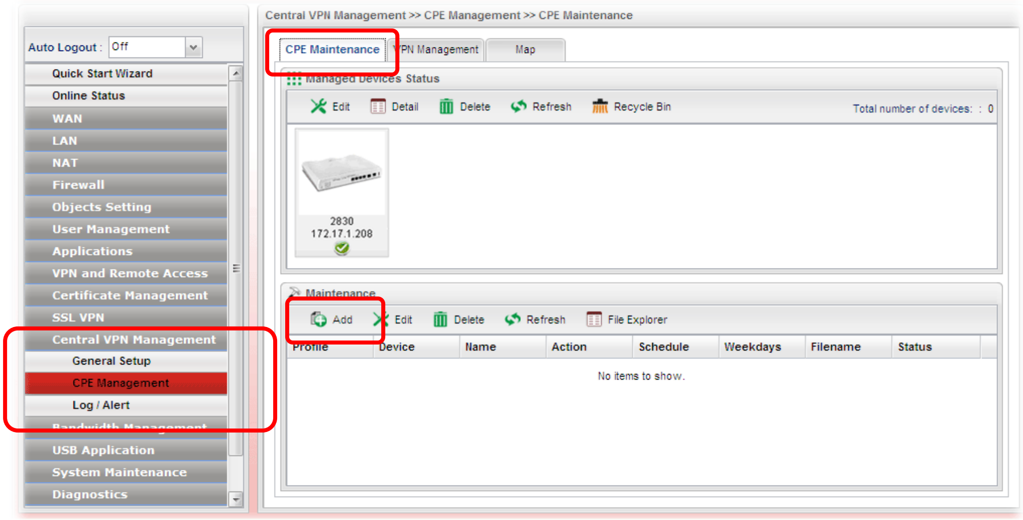


Filename	Property	Size	LastModify	Directory
.	Directory	432	2013/05/09/ 16:4	./cvm/files/00507
..	Directory	1248	2013/05/07/ 09:4	./cvm/files
test	file	160	2013/05/09/ 16:3	./cvm/files/00507
2830_0508	file	666061	2013/05/09/ 16:3	./cvm/files/00507

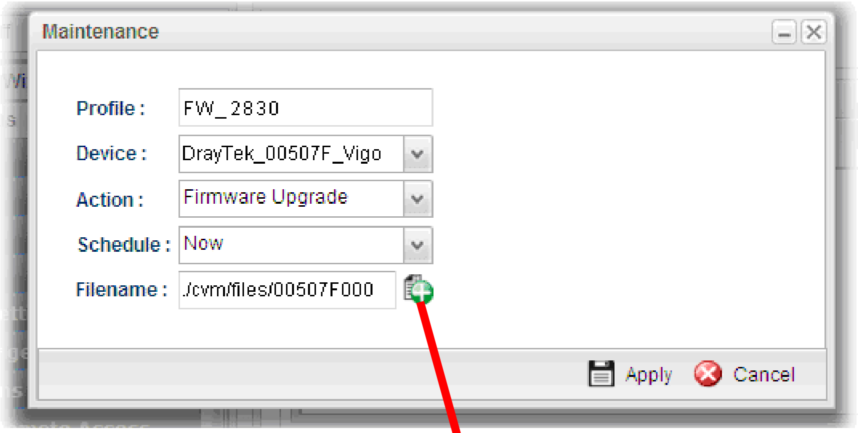
3.9.2 Set a new firmware upgrade profile

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

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



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


Maintenance

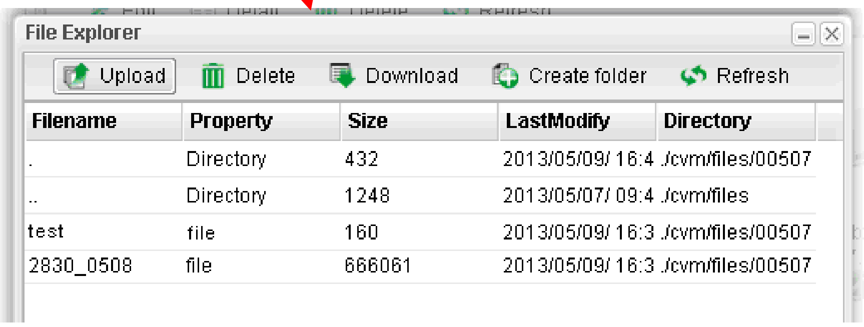
Profile : FW_2830

Device : DrayTek_00507F_Vigo

Action : Firmware Upgrade

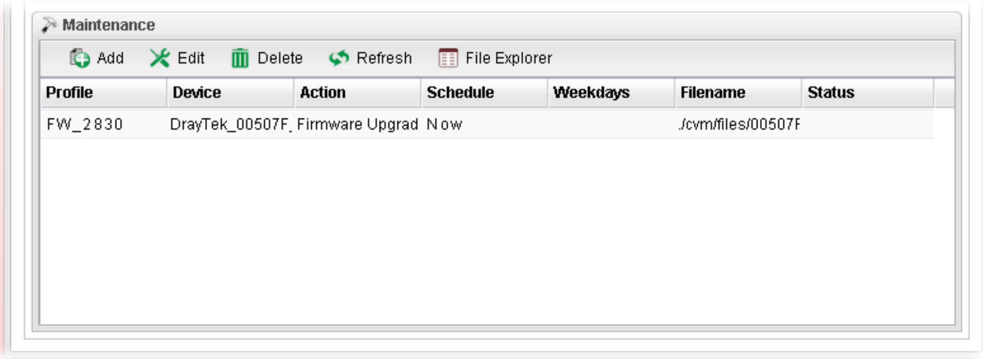
Schedule : Now

Filename : ./cvm/files/00507F000


File Explorer

Filename	Property	Size	LastModify	Directory
.	Directory	432	2013/05/09/ 16:4	./cvm/files/00507
..	Directory	1248	2013/05/07/ 09:4	./cvm/files
test	file	160	2013/05/09/ 16:3	./cvm/files/00507
2830_0508	file	666061	2013/05/09/ 16:3	./cvm/files/00507

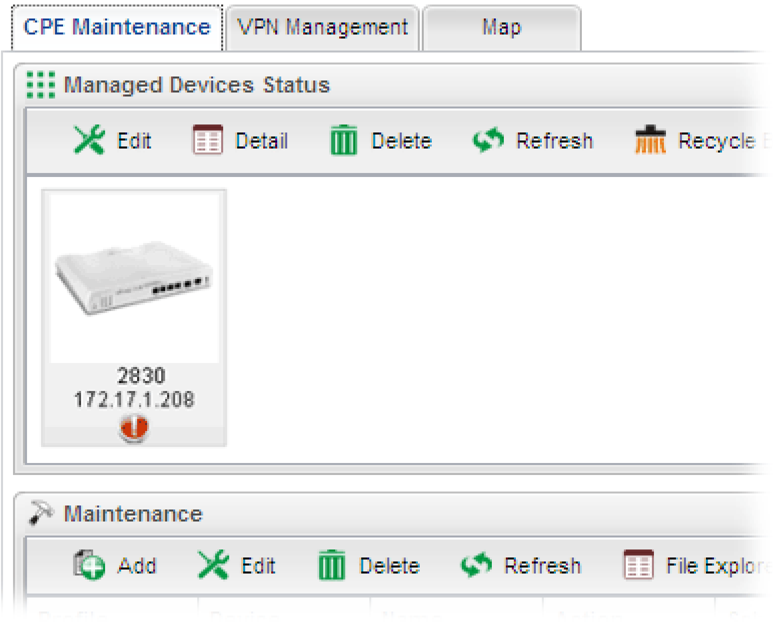
3. When you finished the above settings, click **Apply** to save them. The new maintenance profile has been created and displayed on the Maintenance area.



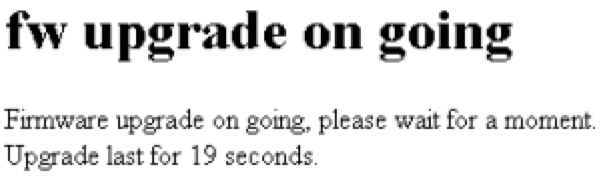
Profile	Device	Action	Schedule	Weekdays	Filename	Status
FW_2830	DrayTek_00507F_	Firmware Upgrad	Now		./cvm/files/00507F	

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

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



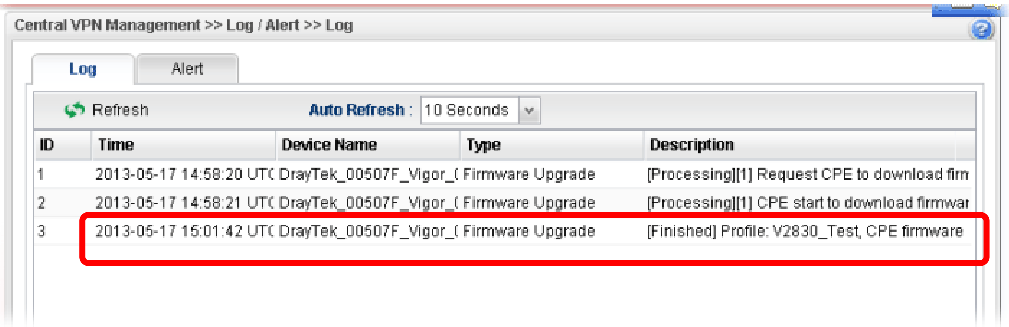
And, in the web user interface of client's CPE, the system will show you that firmware upgrade is on going.



fw upgrade on going

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

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



Central VPN Management >> Log / Alert >> Log

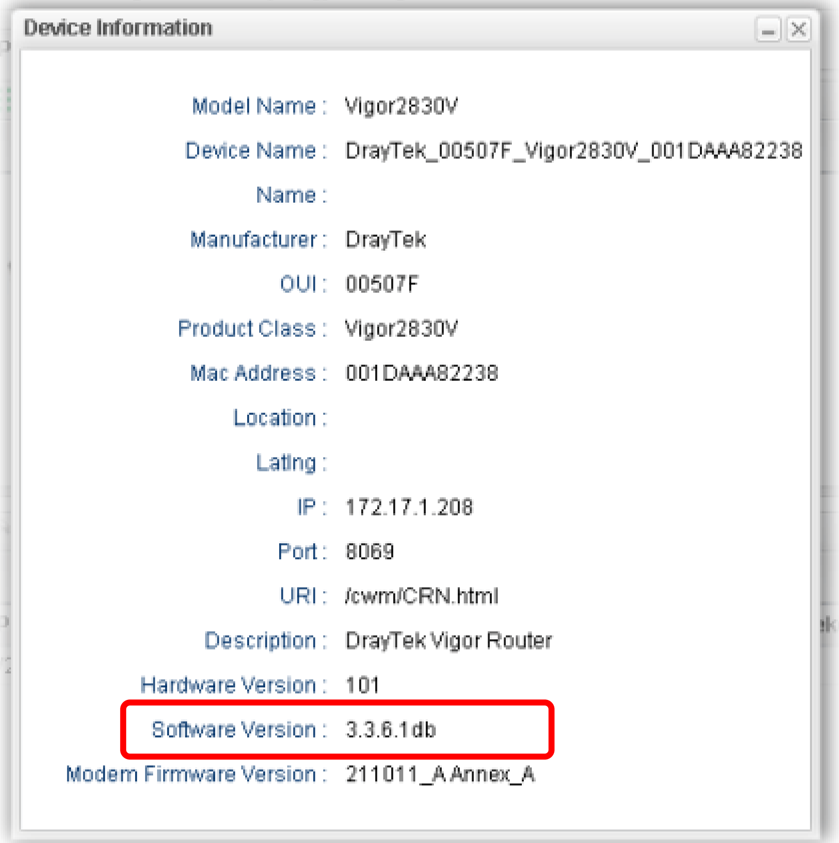
Auto Refresh : 10 Seconds

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

3.9.3 Check the Device Information

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

2. Check the software version field.



Device Information

Model Name : Vigor2830V

Device Name : DrayTek_00507F_Vigor2830V_001DAAA82238

Name :

Manufacturer : DrayTek

OUI : 00507F

Product Class : Vigor2830V

Mac Address : 001DAAA82238

Location :

Latlng :

IP : 172.17.1.208

Port : 8069

URI : /cwm/CRN.html

Description : DrayTek Vigor Router

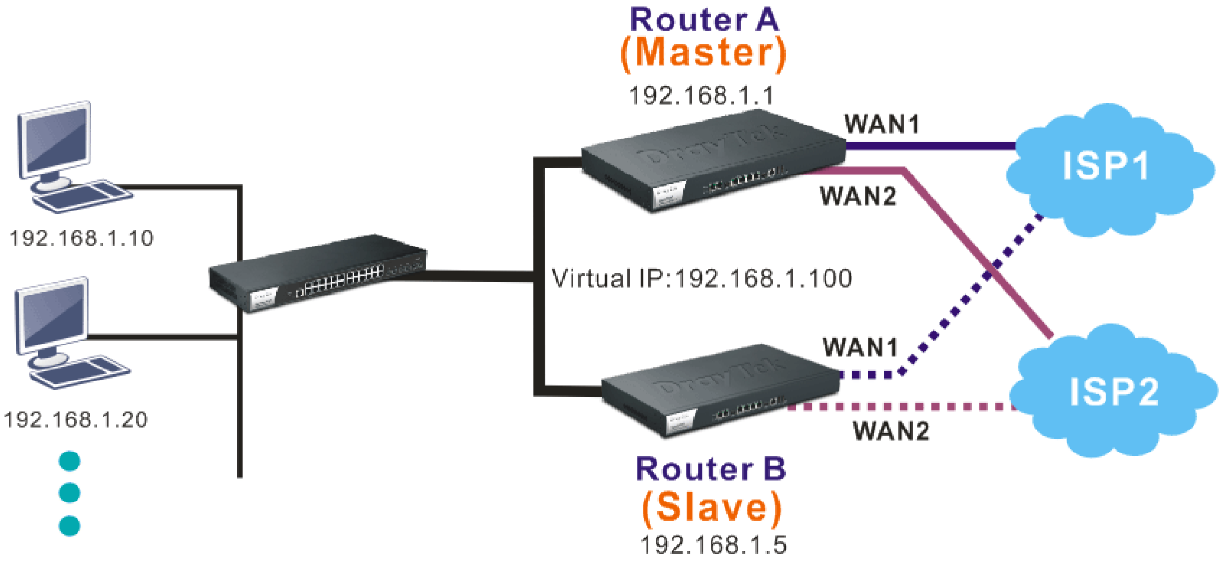
Hardware Version : 101

Software Version : 3.3.6.1db

Modem Firmware Version : 211011_A Annex_A

3.10 How to use High Availability for Vigor routers?

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



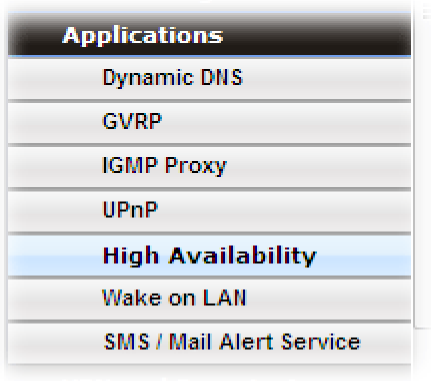
When the HA feature is enabled, the network administrator can set another Vigor3900(s) as the backup device(s) to deliver full routing services during the shutdown of the main Vigor3900. The network administrator can use a Virtual IP (e.g. 192.168.1.100) for both master device and backup device. During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

Note: Make sure the WAN interfaces for both Router A and Router B are well connected. Both routers can be used to access into Internet.

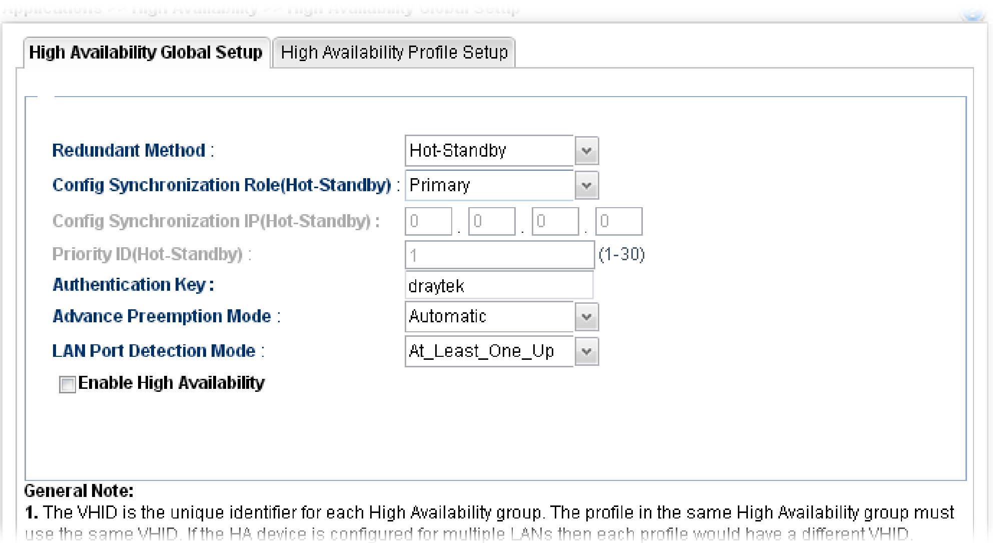
Note: For advanced applications, please refer to FAQ/Application Notes on www.draytek.com.

For router A

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



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



Applications >> High Availability >> High Availability Global Setup

High Availability Global Setup | High Availability Profile Setup

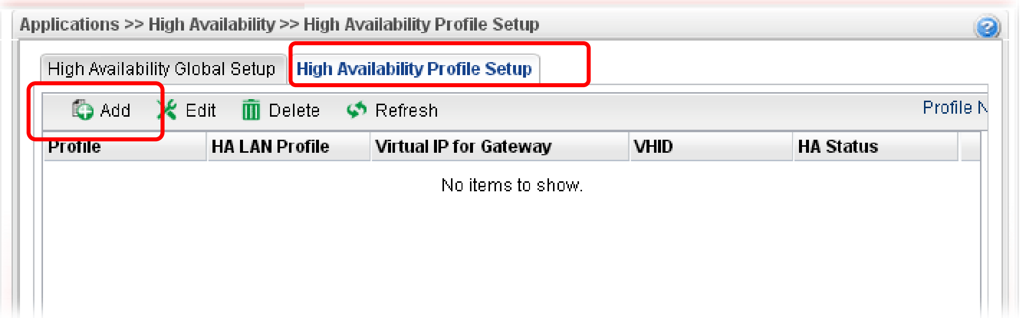
Redundant Method :	Hot-Standby
Config Synchronization Role(Hot-Standby) :	Primary
Config Synchronization IP(Hot-Standby) :	0 . 0 . 0 . 0
Priority ID(Hot-Standby) :	1 (1-30)
Authentication Key :	draytek
Advance Preemption Mode :	Automatic
LAN Port Detection Mode :	At_Least_One_Up

□ Enable High Availability

General Note:

1. The VHID is the unique identifier for each High Availability group. The profile in the same High Availability group must use the same VHID. If the HA device is configured for multiple LANs then each profile would have a different VHID.

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



Applications >> High Availability >> High Availability Profile Setup

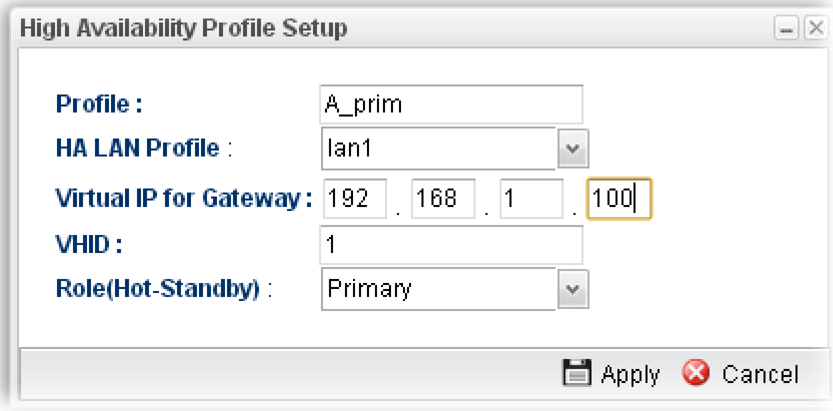
High Availability Global Setup | High Availability Profile Setup

Add | Edit | Delete | Refresh | Profile N

Profile	HA LAN Profile	Virtual IP for Gateway	VHID	HA Status

No items to show.

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



High Availability Profile Setup

Profile : A_prim

HA LAN Profile : lan1

Virtual IP for Gateway : 192 . 168 . 1 . 100

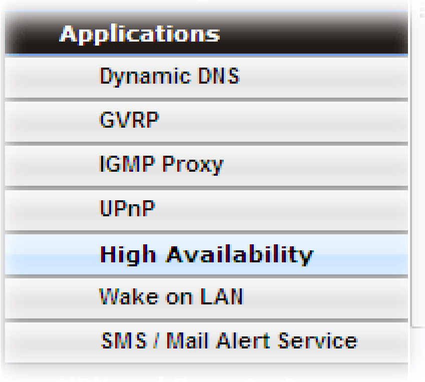
VHID : 1

Role(Hot-Standby) : Primary

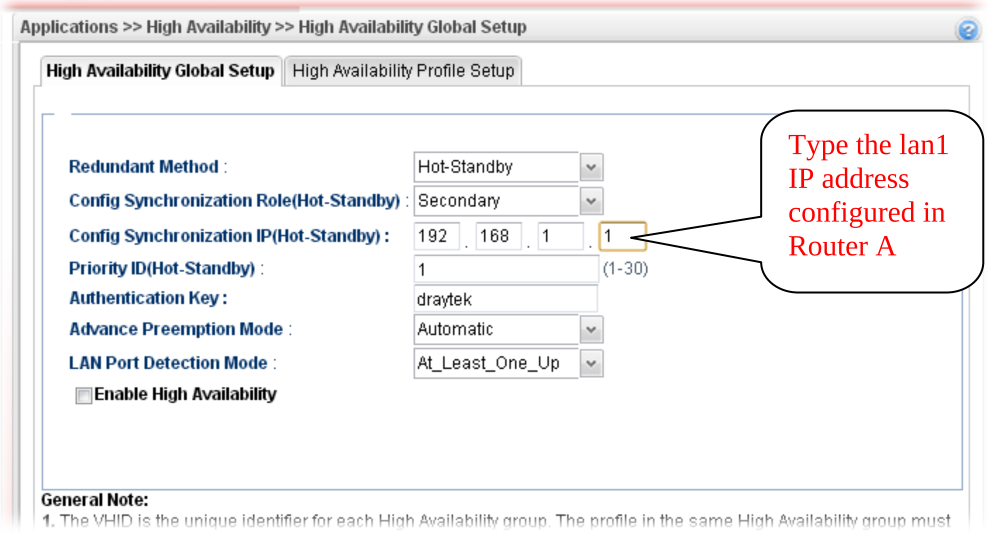
6. Now, the configuration for router A has been finished.

For router B

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



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



Applications >> High Availability >> High Availability Global Setup

High Availability Global Setup | High Availability Profile Setup

Redundant Method : Hot-Standby

Config Synchronization Role(Hot-Standby) : Secondary

Config Synchronization IP(Hot-Standby) : 192 . 168 . 1 . 1

Priority ID(Hot-Standby) : 1 (1-30)

Authentication Key : draytek

Advance Preemption Mode : Automatic

LAN Port Detection Mode : At_Least_One_Up

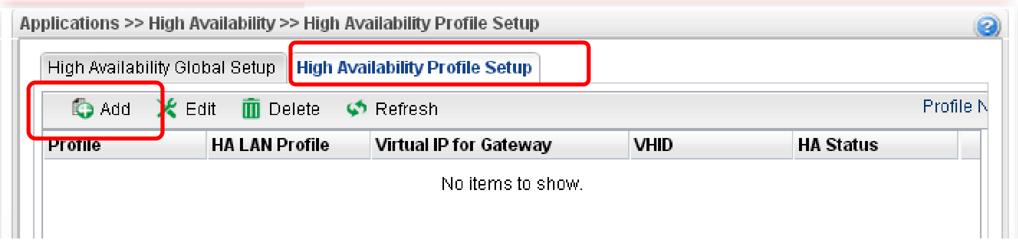
☐ Enable High Availability

General Note:

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

Type the lan1 IP address configured in Router A

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



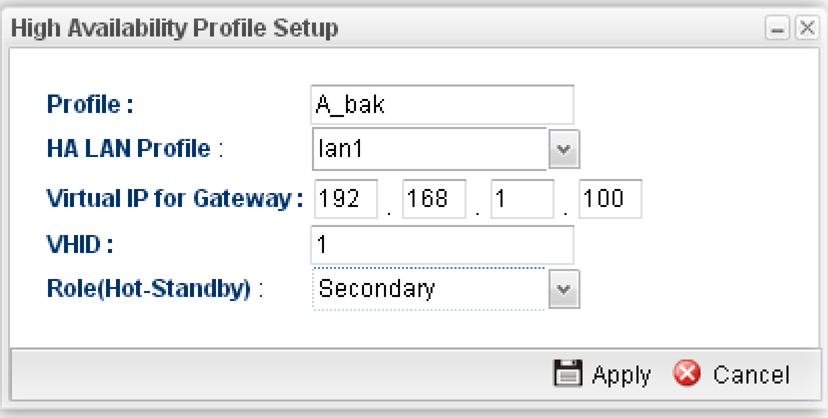
Applications >> High Availability >> High Availability Profile Setup

High Availability Global Setup | High Availability Profile Setup

Profile	HA LAN Profile	Virtual IP for Gateway	VHID	HA Status

No items to show.

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



High Availability Profile Setup

Profile : A_bak

HA LAN Profile : lan1

Virtual IP for Gateway : 192 . 168 . 1 . 100

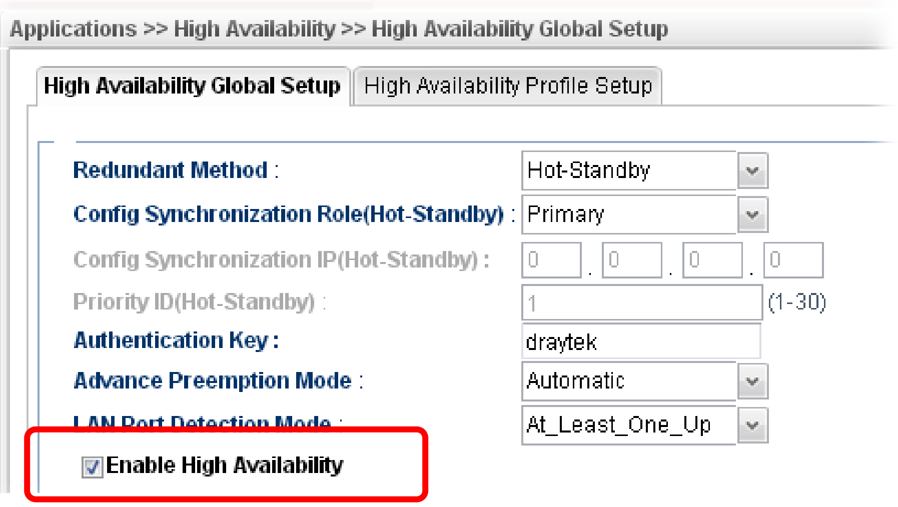
VHID : 1

Role(Hot-Standby) : Secondary

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

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

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



Applications >> High Availability >> High Availability Global Setup

High Availability Global Setup | High Availability Profile Setup

Redundant Method : Hot-Standby

Config Synchronization Role(Hot-Standby) : Primary

Config Synchronization IP(Hot-Standby) : 0 . 0 . 0 . 0

Priority ID(Hot-Standby) : 1 (1-30)

Authentication Key : draytek

Advance Preemption Mode : Automatic

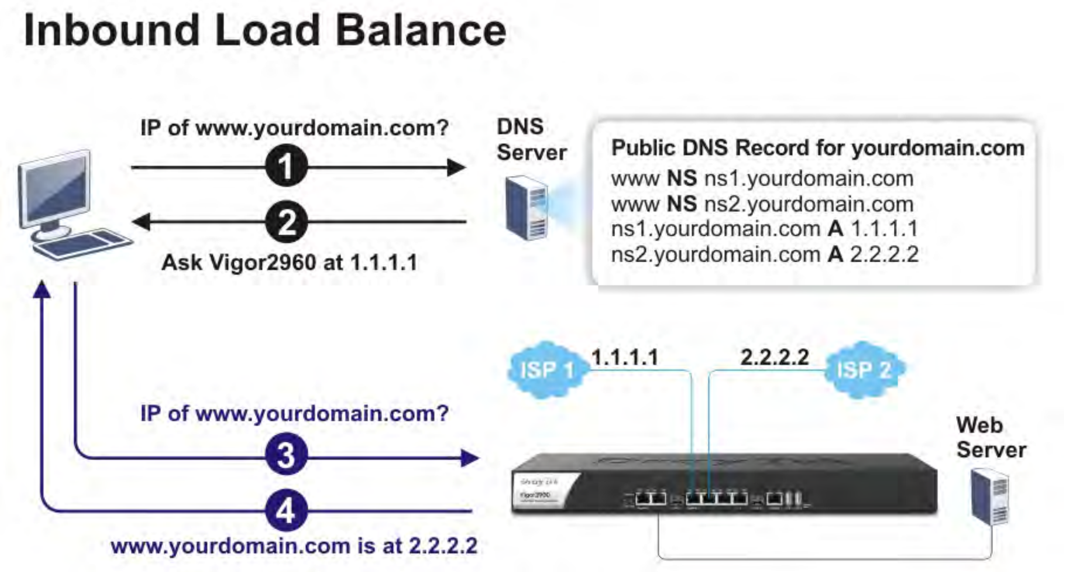
LAN Port Detection Mode : At_Least_One_Up

☑ Enable High Availability

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

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

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


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

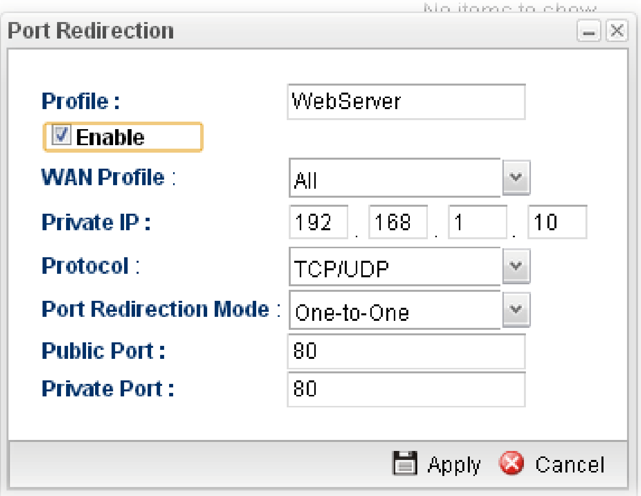
WAN1 IP Address: 1.1.1.1

WAN2 IP Address: 2.2.2.2

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

Enabling Web service on the Router

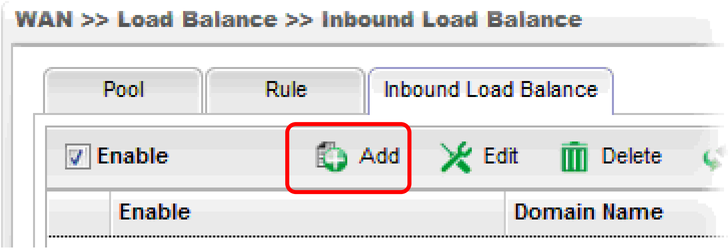
1. Open **NAT** >> **Port Redirection** to set up Port Redirection rules for the Web server. Click **Apply** to save the settings.



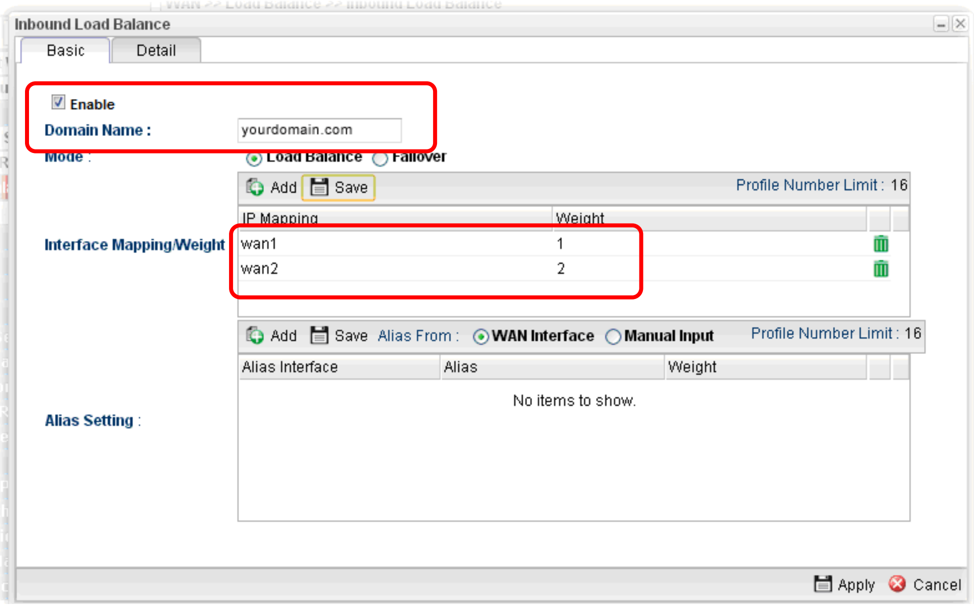
Port Redirection

Profile :	WebServer
☑ Enable	
WAN Profile :	All
Private IP :	192 . 168 . 1 . 10
Protocol :	TCP/UDP
Port Redirection Mode :	One-to-One
Public Port :	80
Private Port :	80

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



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



☑ Enable

Domain Name : yourdomain.com

Mode : ● Load Balance ○ Failover

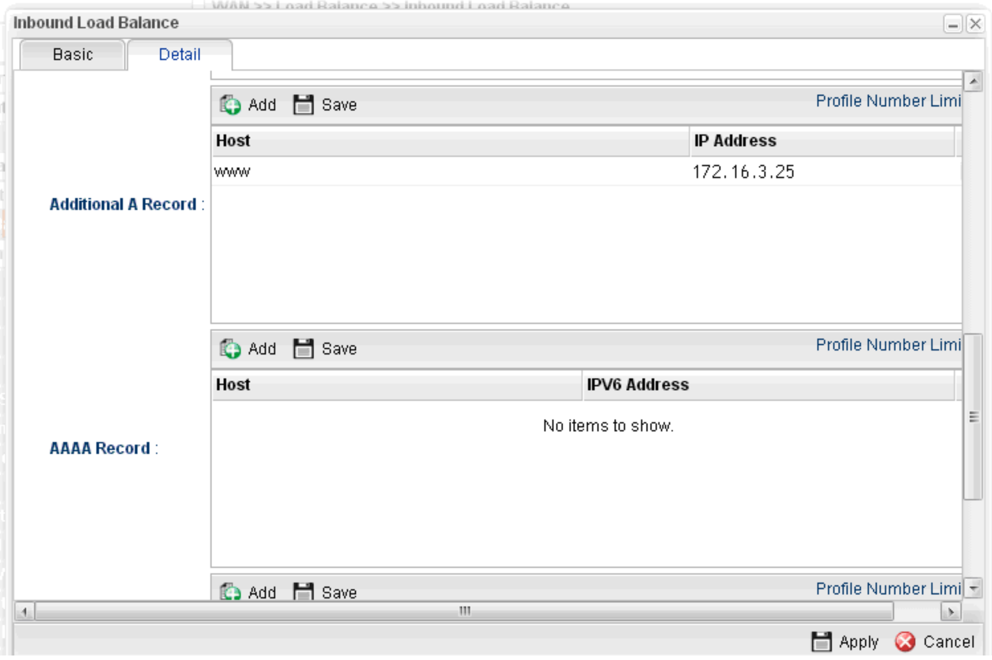
Interface Mapping/Weight

IP Mapping	Weight
wan1	1
wan2	2

Alias Setting : Alias From : ● WAN Interface ○ Manual Input

Alias Interface	Alias	Weight
No items to show.		

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



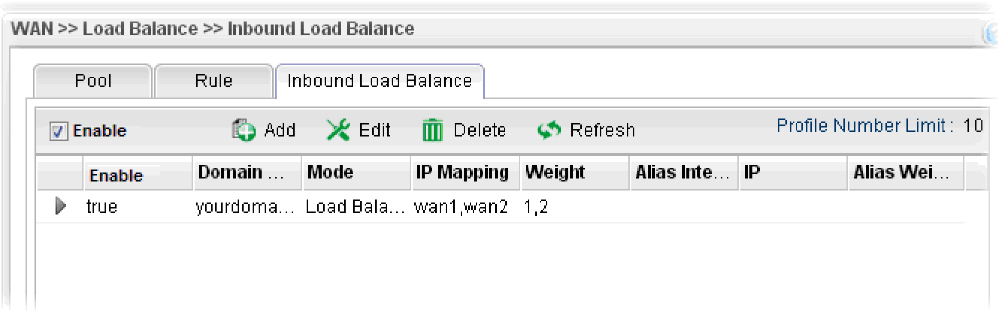
Additional A Record :

Host	IP Address
www	172.16.3.25

AAAA Record :

Host	IPV6 Address
No items to show.	

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



WAN >> Load Balance >> Inbound Load Balance

Profile Number Limit : 10

	Enable	Domain ...	Mode	IP Mapping	Weight	Alias Inte...	IP	Alias Wei...
▶	true	yourdoma...	Load Bala...	wan1,wan2	1,2			

Now, make a test for inbound load balance.

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

First DNS query

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

Second DNS query

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

Third DNS query

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

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

This page is left blank.

Chapter 4: Advanced Web Configuration

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

4.1 WAN Setup

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

Basics of Internet Protocol (IP) Network

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

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

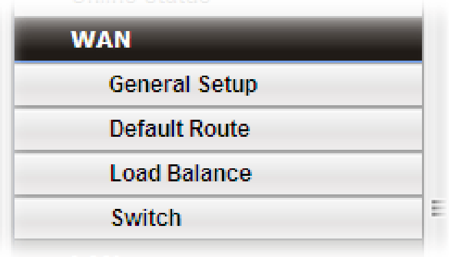
What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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



4.1.1 General Setup

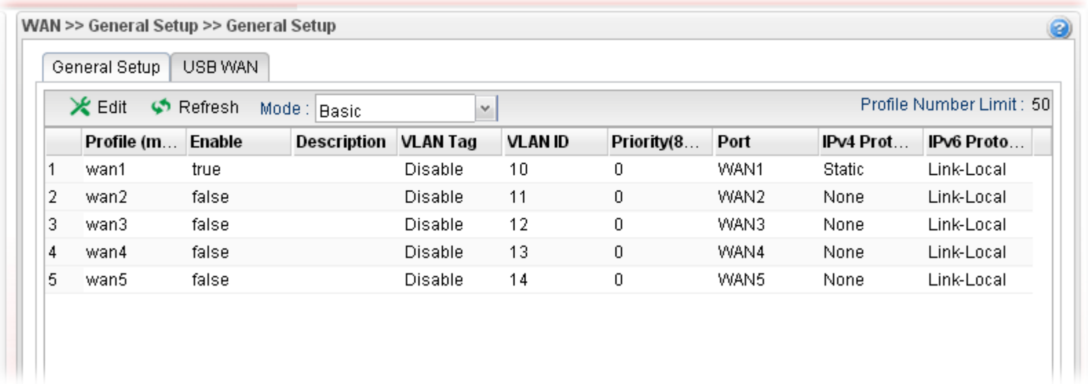
This section will introduce some general settings of Internet and explain the connection modes for WAN profiles in details.

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

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

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

Web Page in Basic Mode

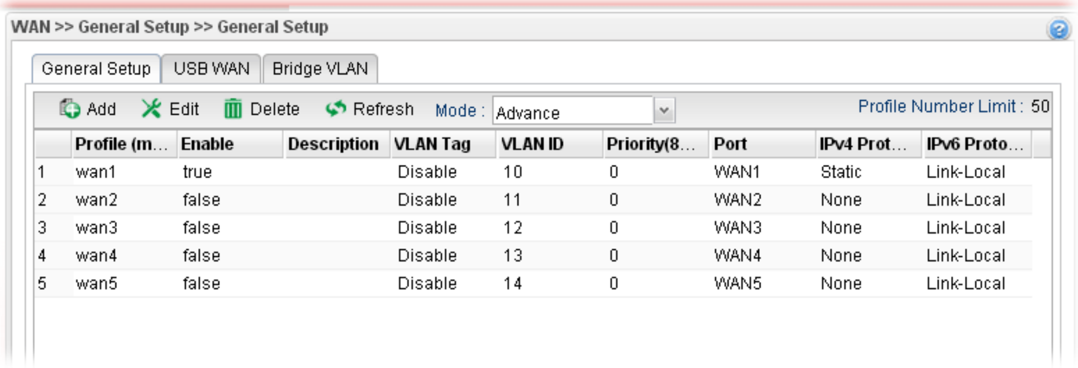


Mode : Basic

Profile Number Limit : 50

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

Web Page in Advance Mode



Mode : Advance

Profile Number Limit : 50

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

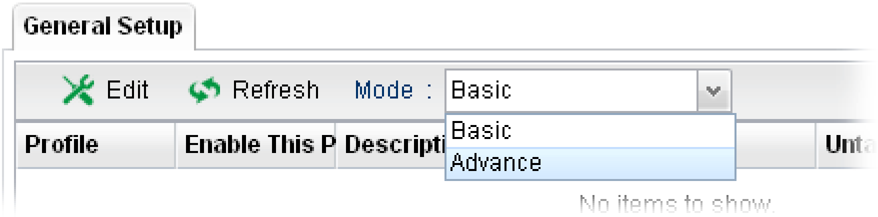
Each item will be explained as follows:

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

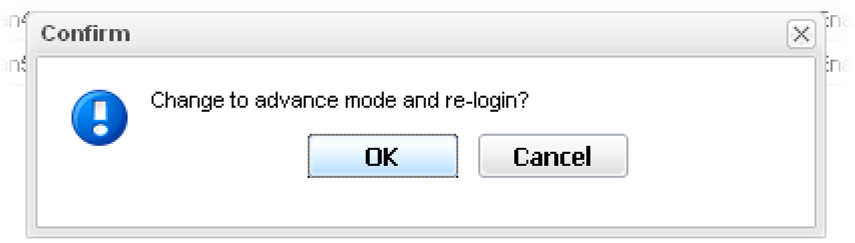
4.1.1.1 Ethernet WAN Profiles

How to add a new WAN profile:

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



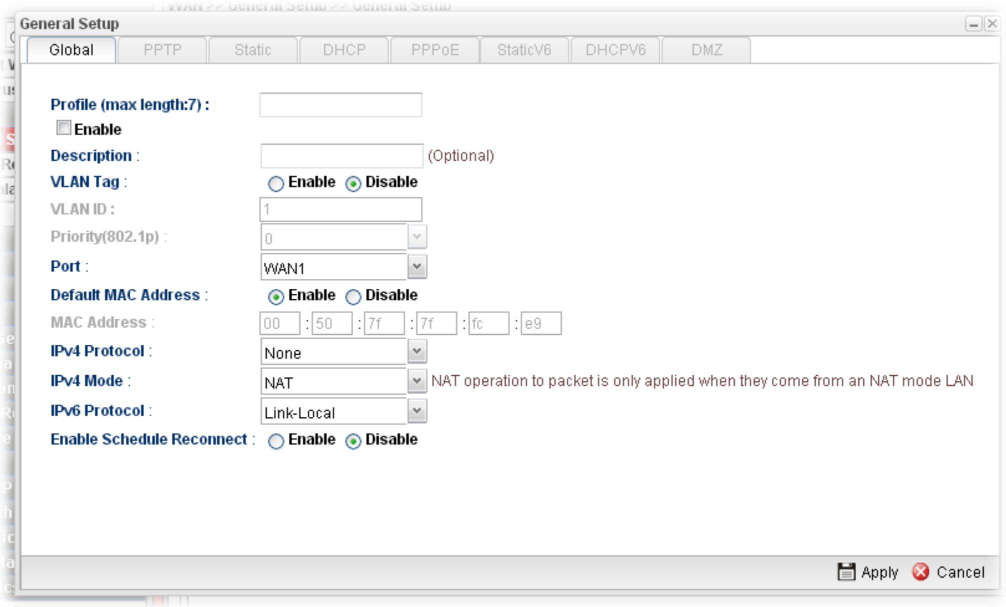
2. A confirmation dialog will appear. Click **OK** to apply the related settings for **Advance** mode.


Confirm

Change to advance mode and re-login?

3. Re-login the system.

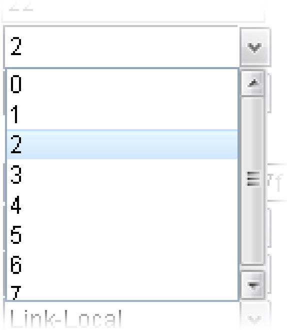
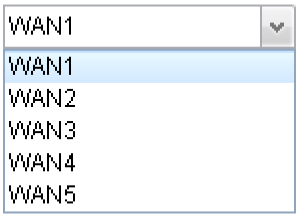
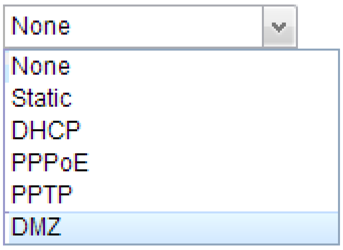
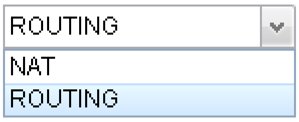
4. Open **WAN>>General Setup**. Click the **Add** button to open the following dialog. Different protocol type selected will bring up different configuration web page.

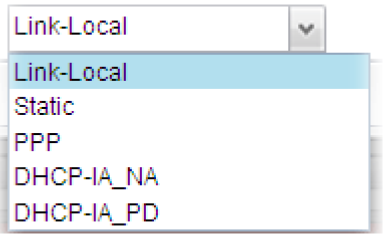


Profile (max length:7) :
□ Enable
Description : (Optional)
VLAN Tag : ○ Enable ● Disable
VLAN ID : 1
Priority(802.1p) : 0
Port : WAN1
Default MAC Address : ● Enable ○ Disable
MAC Address : 00 : 50 : 7f : 7f : fc : e9
IPv4 Protocol : None
IPv4 Mode : NAT NAT operation to packet is only applied when they come from an NAT mode LAN
IPv6 Protocol : Link-Local
Enable Schedule Reconnect : ○ Enable ● Disable

Available parameters are listed as follows:

Item	Description
Profile (max length:7)	Type a name (less than 7 characters) for such profile.

Enable	Check this box to enable such profile.
Description	Give the brief description for such profile.
VLAN Tag	Choose **Enable** to tag the packets passing through the port specified below.
VLAN ID	Type the VLAN ID number for such profile.
Priority(802.1p)	Type the packet priority number for such VLAN. The range is from 0 to 7. 
Port	Choose the physical WAN interface for such profile. 
Default MAC Address	**Enable** – Click it to enable the default MAC address for such profile. **Disable** – Click it to type the MAC address manually for such profile.
MAC Address	Specify the MAC address for such profile. In default, the system will determine it automatically.
IPv4 Protocol	There are several connection modes for you to specify for IPv4 protocol type. Each mode will bring up different web page.  The DMZ protocol is available for WAN4 profile only.
IPv4 Mode	Determine such profile will be used for. 

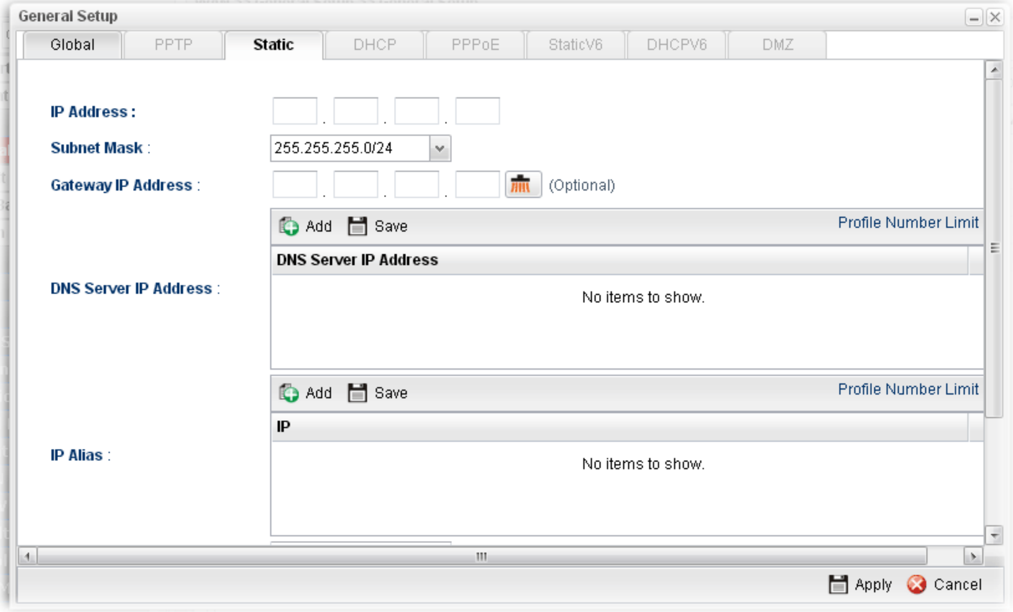
IPv6 Protocol	There are four connection modes for you to specify for IPv6 protocol type. Each mode will bring up different web page.  Link-Local Link-Local Static PPP DHCP-IA_NA DHCP-IA_PD
Enable Schedule Reconnect	**Enable** – Click it to enable the function of reconnecting the network automatically within the time schedule. **Disable** – Click it to disable the schedule reconnect function.
Schedule Time Object	Choose the time object profile to be applied by such WAN.

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

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

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

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



General Setup

IP Address : . . .

Subnet Mask : 255.255.255.0/24

Gateway IP Address : . . . (Optional)

DNS Server IP Address :

DNS Server IP Address

No items to show.

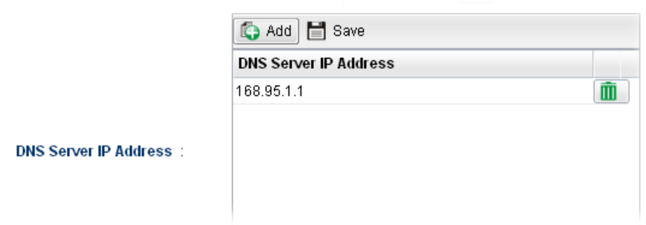
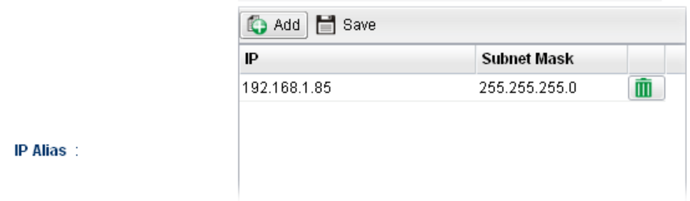
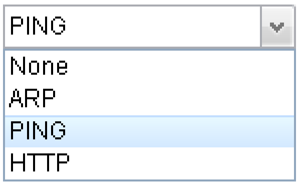
IP Alias :

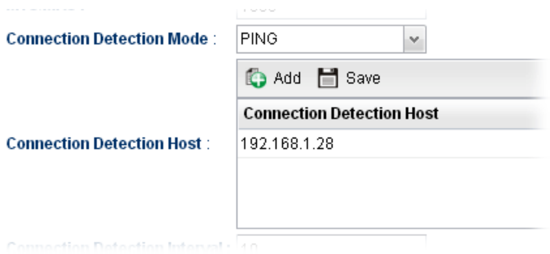
IP

No items to show.

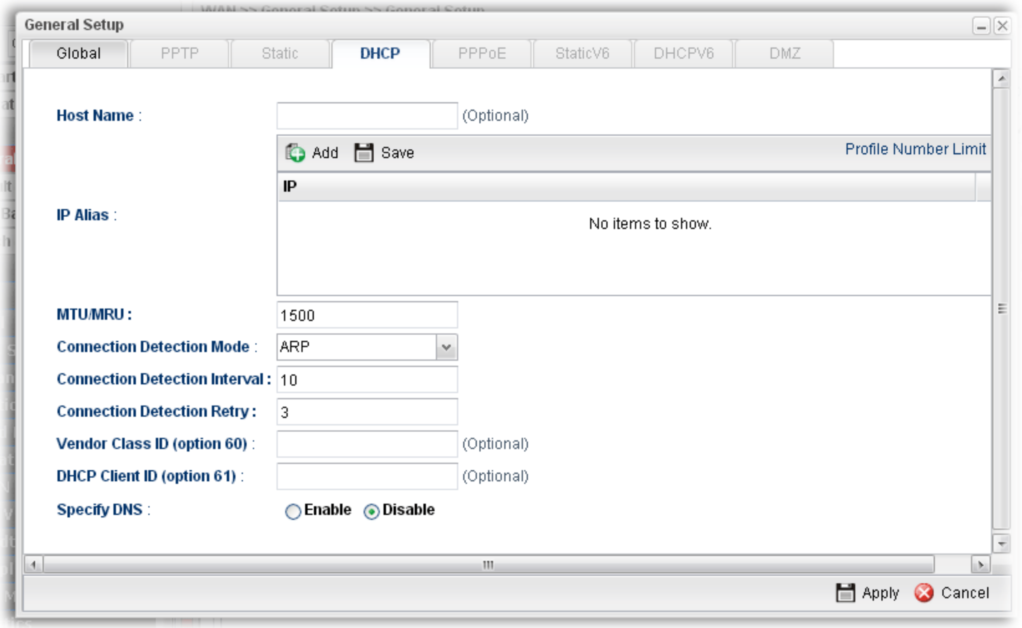
Available parameters are listed as follows:

Item	Description
IP Address	Type the IP address specified for such profile.
Subnet Mask	Use the drop down list to choose the subnet mask for such profile.

Gateway IP Address	Type the gateway address for such profile.
DNS Server IP Address	Type a public IP address as the primary DNS (Domain Name Server). To add a new IP address, simply place the mouse cursor on this filed. The following dialog will appear.  DNS Server IP Address : DNS Server IP Address 168.95.1.1 **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host**). 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.  IP Alias : IP / Subnet Mask 192.168.1.85 / 255.255.255.0 **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.  PING None ARP PING HTTP
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**.  Connection Detection Mode : PING Add Save Connection Detection Host Connection Detection Host : 192.168.1.28 **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:***



Host Name : (Optional)

IP Alias : IP — No items to show.

MTU/MRU : 1500

Connection Detection Mode : ARP

Connection Detection Interval : 10

Connection Detection Retry : 3

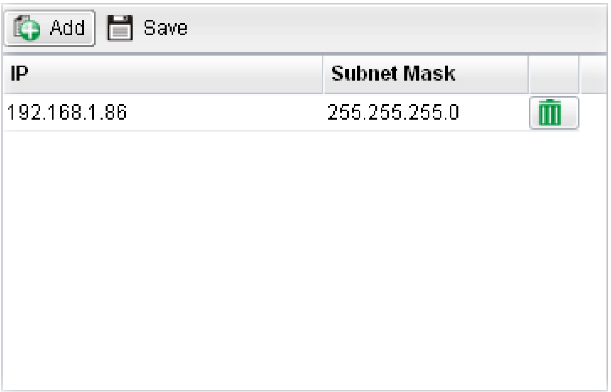
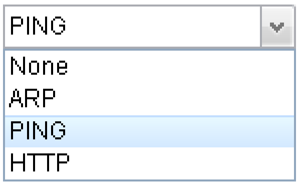
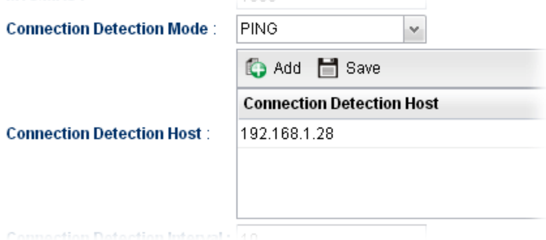
Vendor Class ID (option 60) : (Optional)

DHCP Client ID (option 61) : (Optional)

Specify DNS : ○ Enable ● Disable

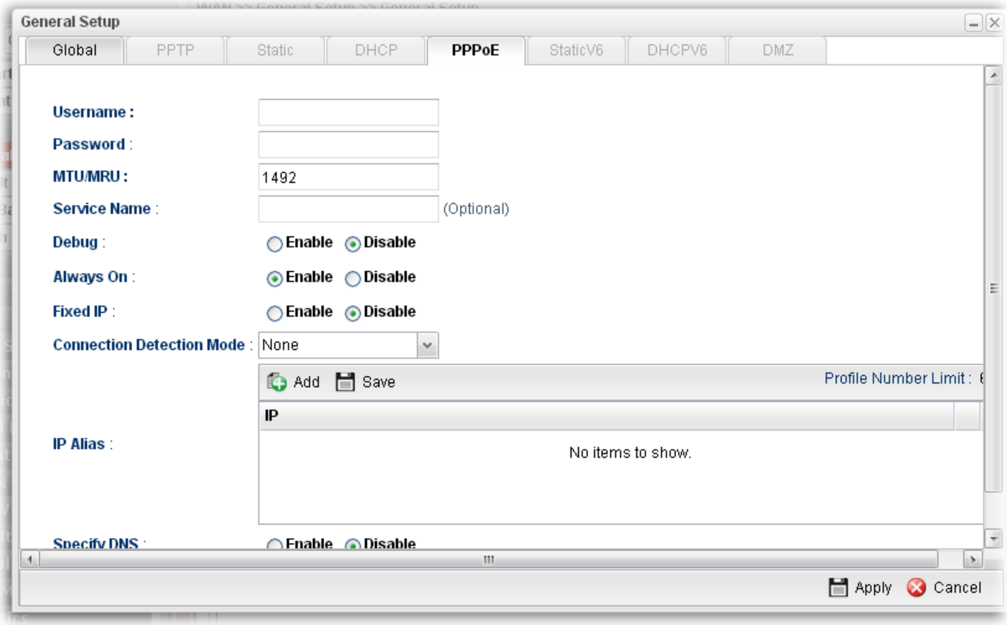
Available parameters are listed as follows:

Item	Description
Host Name (Optional)	Type a name as the host name for identification.

IP Alias	Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **NAT>>Port Redirection/DMZ Host)**. 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.  IP: 192.168.1.86 Subnet Mask: 255.255.255.0 **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**.  Connection Detection Mode : PING Connection Detection Host : 192.168.1.28 **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.
Vendor Class ID (option 60)	It is used to identify the vendor type and the configuration of a DHCP client.
DHCP Client ID (option 61)	It used to specify a DHCP client identifier in a host declaration, so that DHCP can find the host record by matching against the client identifier.
Specify DNS	**Enable** – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. **Disable** – Click it to disable the function of DNS specified.
DNS	**Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



General Setup

Username :

Password :

MTU/MRU : 1492

Service Name : (Optional)

Debug : ○ Enable ● Disable

Always On : ● Enable ○ Disable

Fixed IP : ○ Enable ● Disable

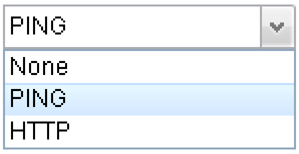
Connection Detection Mode : None

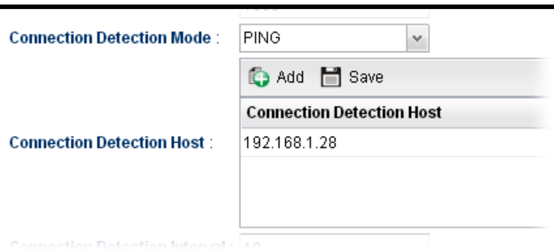
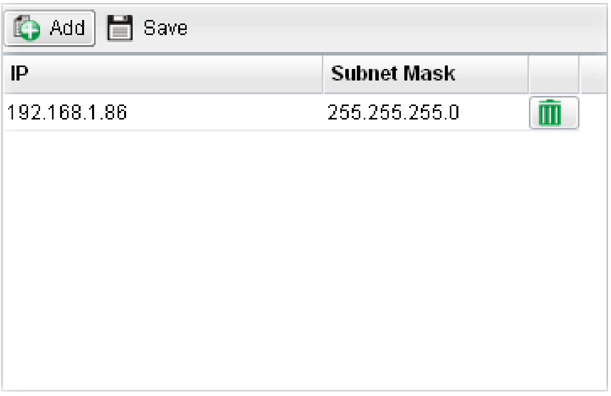
IP Alias :

IP
No items to show.

Specify DNS : ○ Enable ● Disable

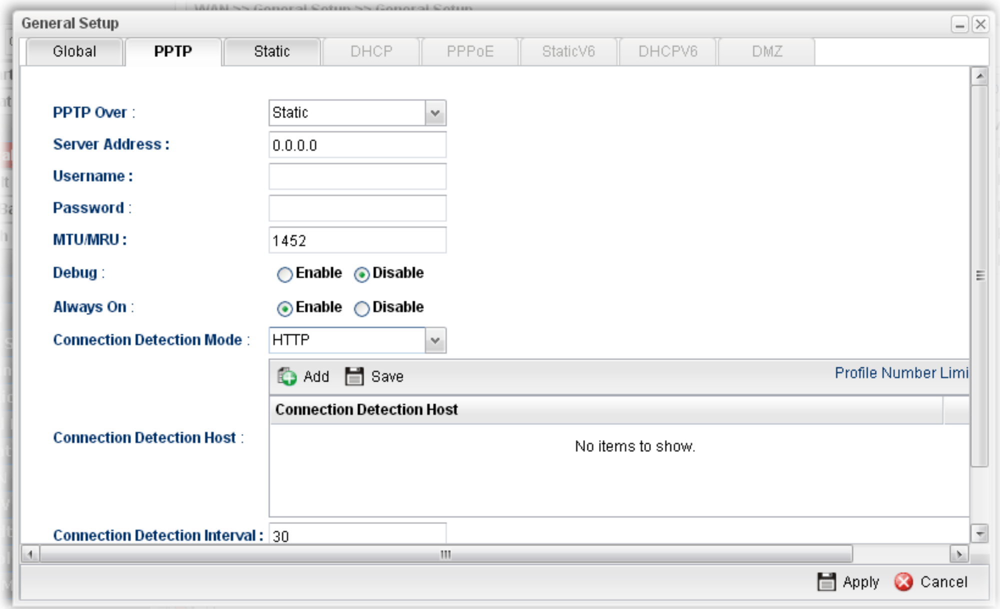
Available parameters are listed as follows:

Item	Description
Username	Type the user name offered by your ISP.
Password	Type the password offered by your ISP.
MTU/MRU	Type the value of MTU/MRU. The default value is 1492.
Service Name	This is an optional setting. Some ISP will offer such information and ask you to type the same data on this field.
Debug	Click **Enable** to display the PPPoE debug message in Syslog. The default setting is **Disable**.
Always On	**Enable** – Click it to enable the function of Always On. The router will keep network connection all the time. **Disable** – Click it to disable the function of Always On.
Fixed IP	**Enable** – Click it to enable the function of fixed IP. **Disable** – Click it to disable the function of fixed IP.
Fixed IP Address	Type the IP address in the boxes.
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways **PING** and **HTTP** supported in Vigor router for you to choose to send the request out.  PING None PING HTTP
Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection **host address** in this field. Use the default setting.

	 Connection Detection Mode : PING Add Save Connection Detection Host : 192.168.1.28 **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 Save IP: 192.168.1.86 Subnet Mask: 255.255.255.0 🗑 **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.
Specify DNS	Enable – Click it to enable the function of DNS specified. It is used for local service (e.g., NTP, ping diagnostic) or used for forwarding packets to PC on LAN/VPN. Disable – Click it to disable the function of DNS specified.
DNS	**Add** – click this button to have a field for adding a new IP

	address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



PPTP Over : Static

Server Address : 0.0.0.0

Username :

Password :

MTU/MRU : 1452

Debug : ○ Enable ● Disable

Always On : ● Enable ○ Disable

Connection Detection Mode : HTTP

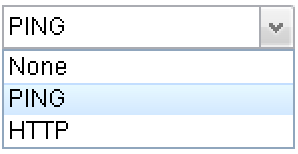
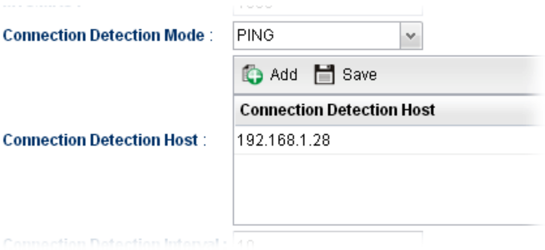
Connection Detection Host :

Connection Detection Host
No items to show.

Connection Detection Interval : 30

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	Select a detecting mode for this WAN interface. There are

Detection Mode	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.  Connection Detection Mode : PING Connection Detection Host : 192.168.1.28 **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.

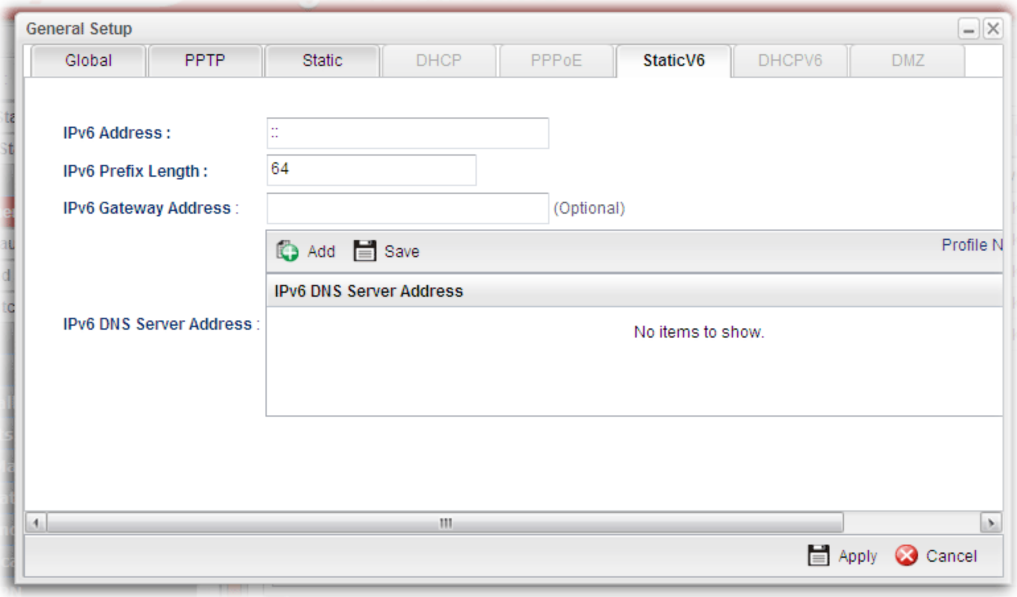
- ***If you choose Link-Local as IPv6 protocol type***

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 PPP as IPv6 protocol type***

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

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



General Setup

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

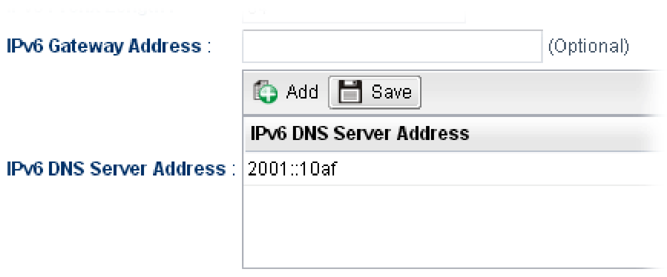
IPv6 Address : ::

IPv6 Prefix Length : 64

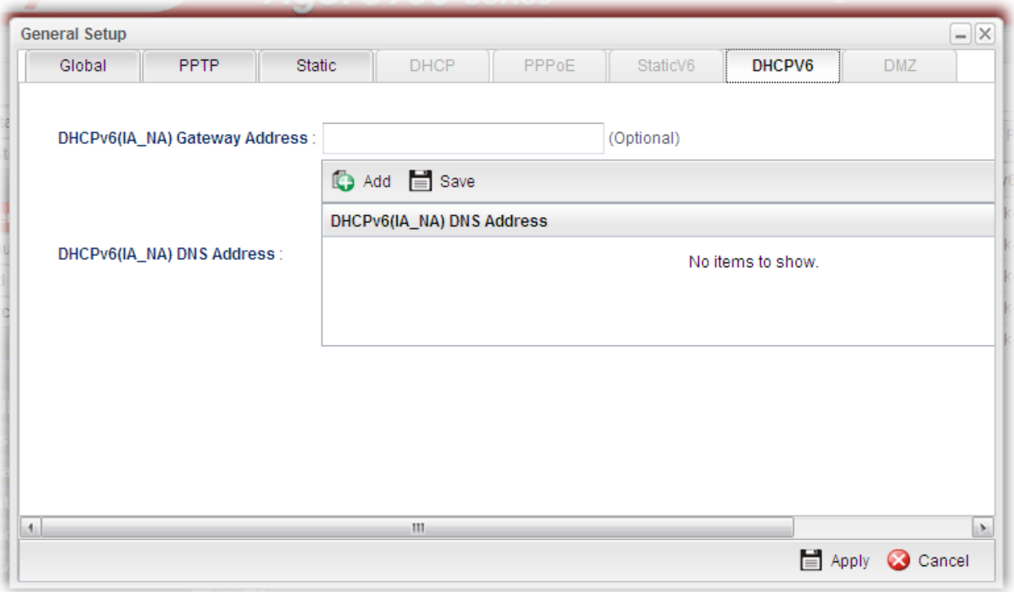
IPv6 Gateway Address : (Optional)

IPv6 DNS Server Address : No items to show.

Available parameters are listed as follows:

Item	Description
IPv6 Address	Type the IP address for such protocol.
IPv6 Prefix Length	Type your IPv6 address prefix length.
IPv6 Gateway Address	Type your IPv6 gateway address.
IPv6 DNS Server Address	Type your IPv6 primary DNS Server address.  IPv6 Gateway Address : (Optional) IPv6 DNS Server Address : 2001::10af **Add** – click this button to have a field for adding a new IP address. **Save** – click this button to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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



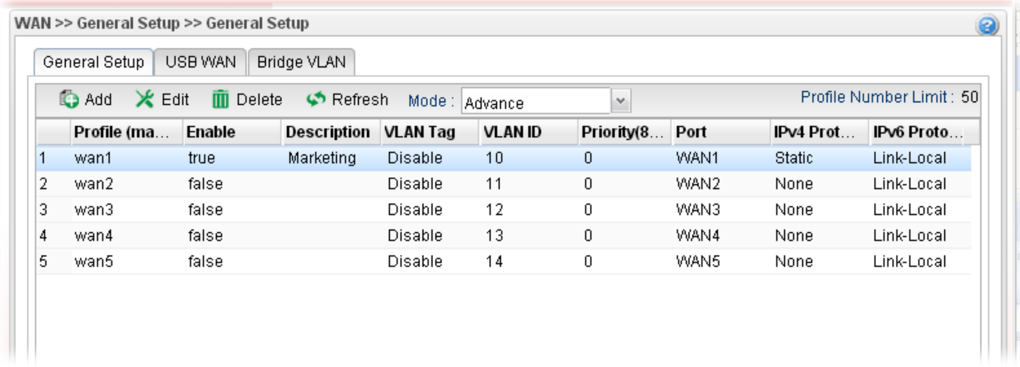
Available parameters are listed as follows:

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

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

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

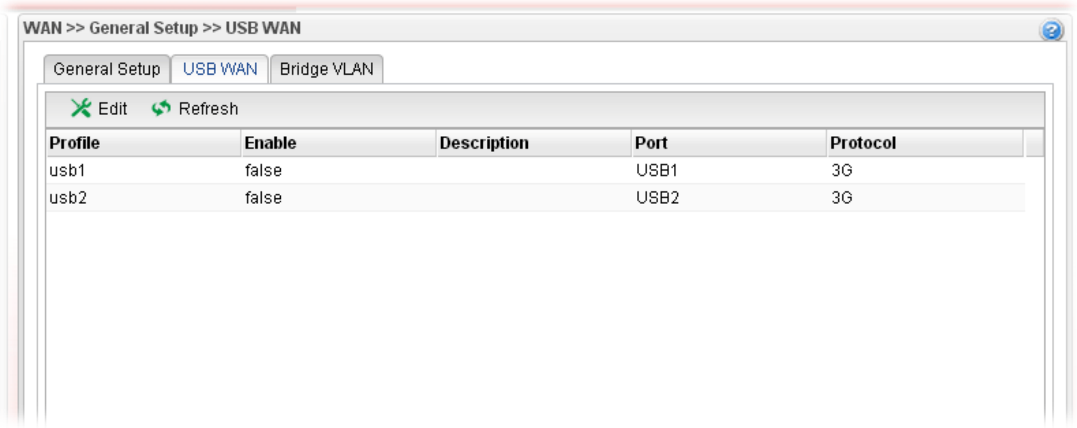
5. Enter all the settings and click **Apply**. The new added profile will be shown as below.



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

4.1.1.2 USB WAN Profiles

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



WAN >> General Setup >> USB WAN

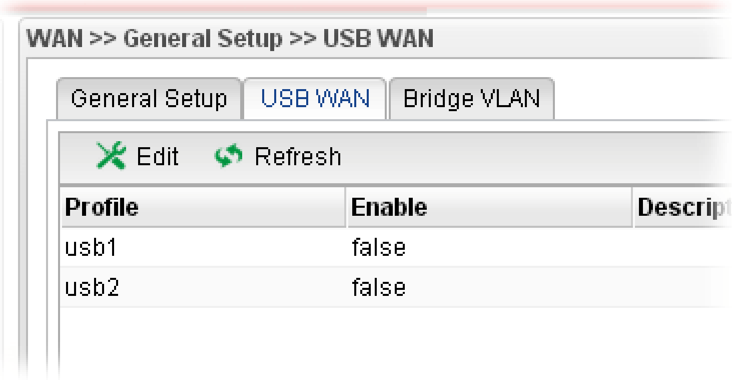
Profile	Enable	Description	Port	Protocol
usb1	false		USB1	3G
usb2	false		USB2	3G

Each item will be explained as follows:

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

How to edit a new USB WAN profile

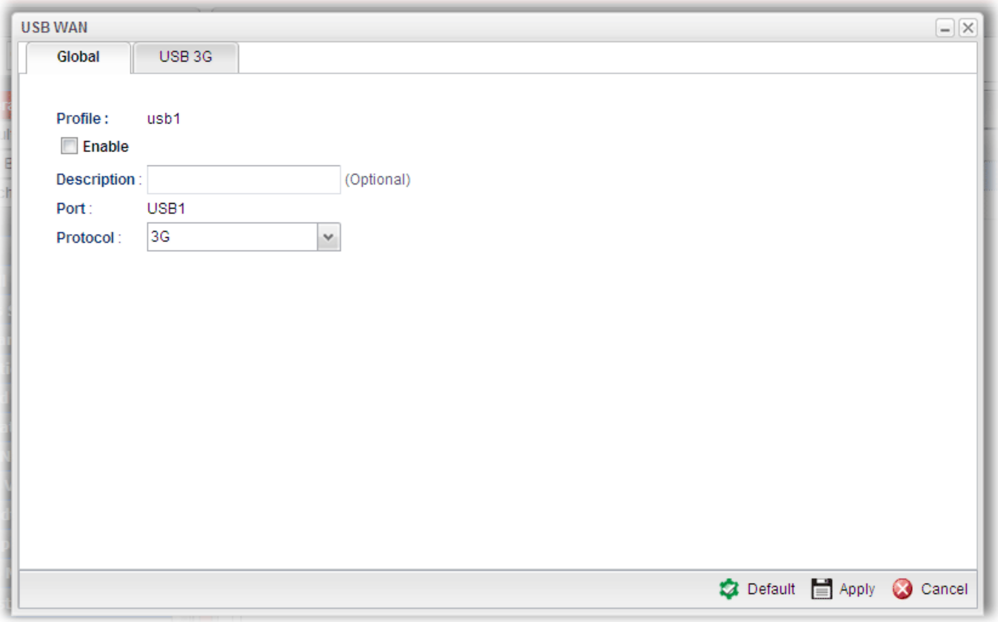
1. Choose one of the USB WAN profiles and click **Edit**.



WAN >> General Setup >> USB WAN

Profile	Enable	Descrip
usb1	false	
usb2	false	

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



Profile : usb1

□ Enable

Description : (Optional)

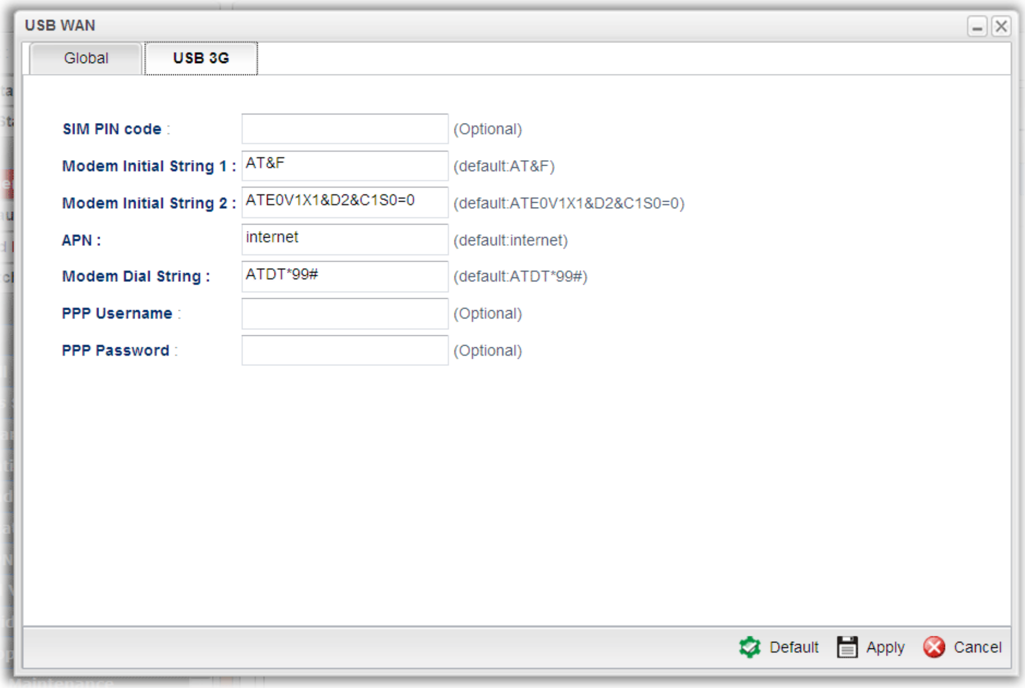
Port : USB1

Protocol : 3G

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the USB WAN profile.
Enable	Check it to enable the USB WAN profile.
Description	Give the brief description for such profile.
Port	Display the physical WAN interface for such profile.
Protocol	Choose the connection mode (e.g., 3G) for USB WAN.
Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

3. After finished the settings above, click the USB 3G tab to display the following page:



USB WAN

SIM PIN code : (Optional)

Modem Initial String 1 : AT&F (default:AT&F)

Modem Initial String 2 : ATE0V1X1&D2&C1S0=0 (default:ATE0V1X1&D2&C1S0=0)

APN : internet (default:internet)

Modem Dial String : ATDT*99# (default:ATDT*99#)

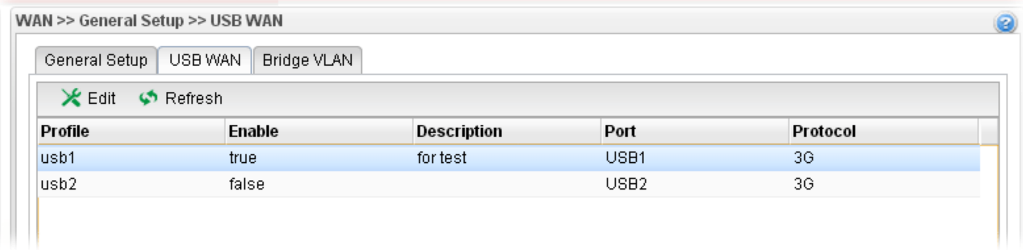
PPP Username : (Optional)

PPP Password : (Optional)

Available parameters are listed as follows:

Item	Description
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
Modem Initial String2	The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings.
APN	APN means Access Point Name which is provided and required by some ISPs. Type the name.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).
Default	Click it to restore the default settings.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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



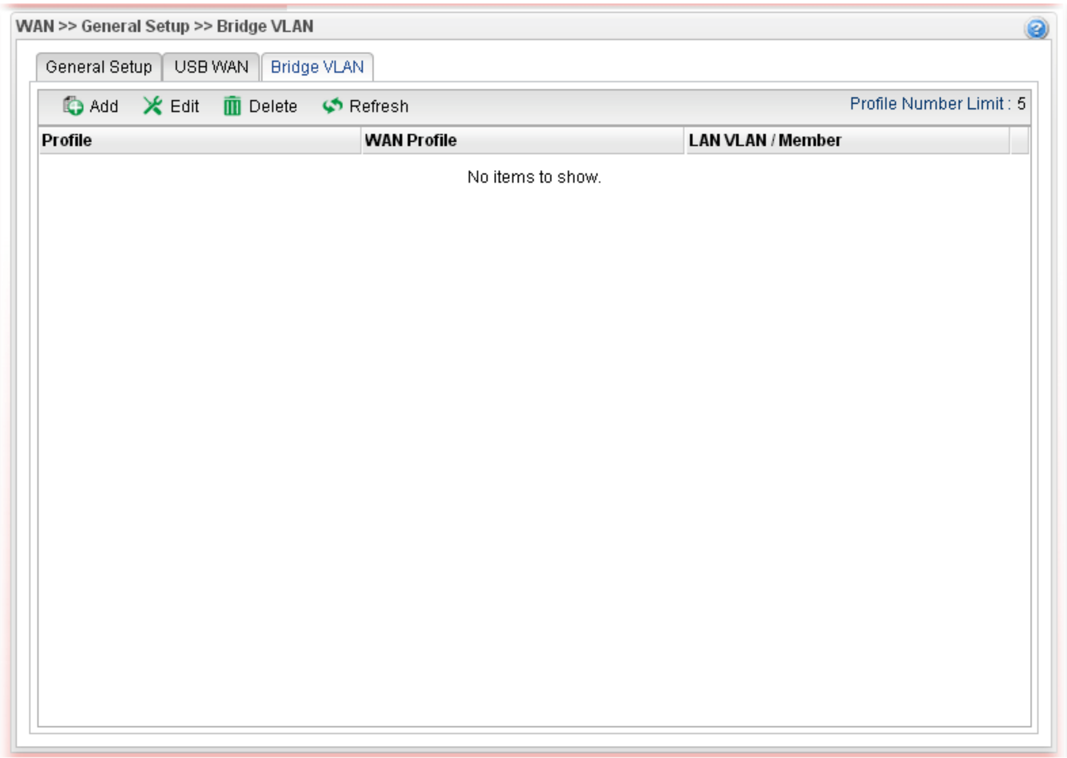
WAN >> General Setup >> USB WAN

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

4.1.1.3 Bridge VLAN Profiles

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

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



WAN >> General Setup >> Bridge VLAN

Profile	WAN Profile	LAN VLAN / Member

No items to show.

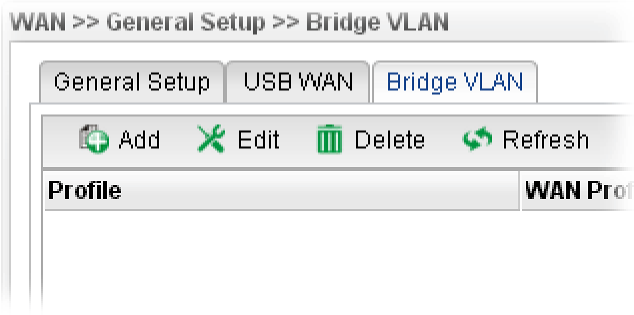
Each item will be explained as follows:

Item	Description
Add	Click to create a new profile.
Edit	Modify the selected USB WAN profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected WAN profile. Such function is available in Advance mode only. To delete a profile, simply select the one you want to delete and click the Delete button.

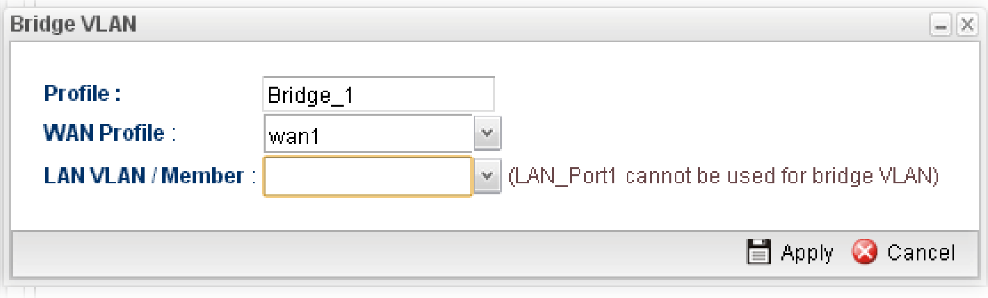
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the profile name.
WAN Profile	Display the WAN profile selected.
LAN VLAN/Member	Display VLAN ID number of the LAN port selected.

How to add a new bridge VLAN profile

1. Click **Add.**



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



Profile : Bridge_1

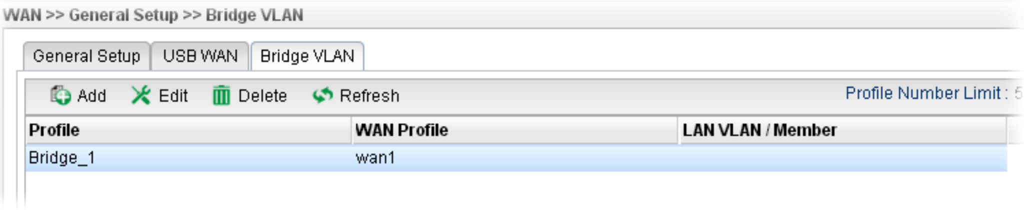
WAN Profile : wan1

LAN VLAN / Member : (LAN_Port1 cannot be used for bridge VLAN)

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
WAN Profile	Use the drop down list to choose the WAN interface.
LAN VLAN/Member	Choose a VLAN profile from the drop down list. You have to open **LAN>>Switch** page and click **802.1Q** VLAN for creating VLAN ID number bound with LAN port (802.1Q VLAN profile) first. Otherwise, no profiles will be displayed here for you to specify.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

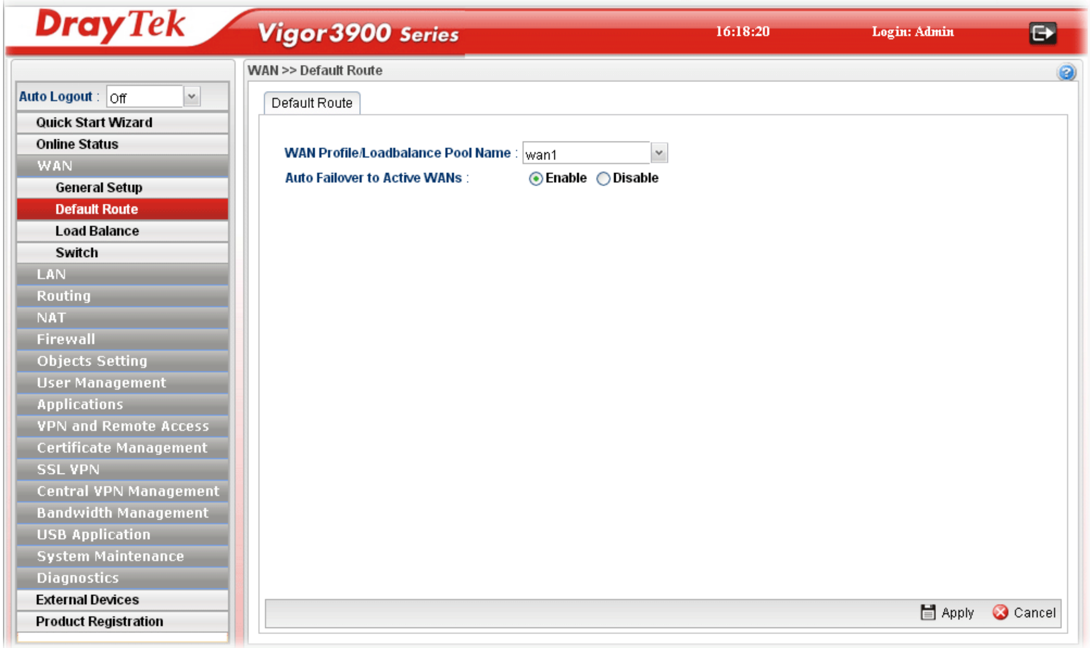


WAN >> General Setup >> Bridge VLAN

Profile	WAN Profile	LAN VLAN / Member
Bridge_1	wan1	

4.1.2 Default Route

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



WAN >> Default Route

WAN Profile/Loadbalance Pool Name : wan1

Auto Failover to Active WANs : ● Enable ○ Disable

Available parameters are listed as follows:

Item	Description
WAN Profile /Load Balance Pool Name	Display the WAN profiles for user to choose as a default route. In which, wan1 to wan5 are factory default settings.
Auto Failover to Active WANs	**Enable** – Check it to let the network connection being established through any active WAN interface. **Disable** – Check it to disable the function.
Apply	Click it to save the configuration.
Cancel	Discard current page modification.

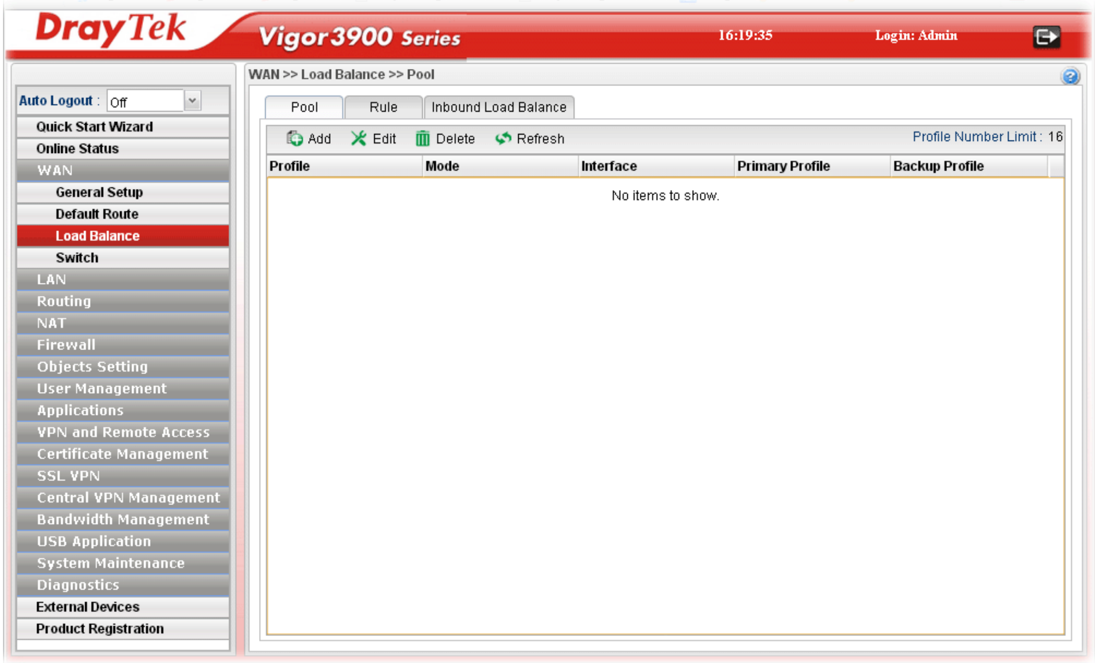
4.1.3 Load Balance

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** option.

4.1.3.1 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:

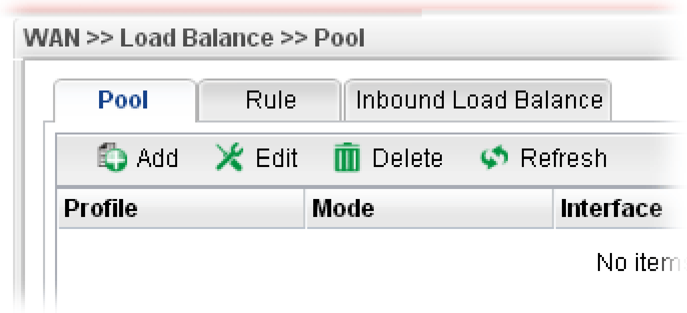
Item	Description
Add	Add a new pool profile.
Edit	Modify the selected pool profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected rule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

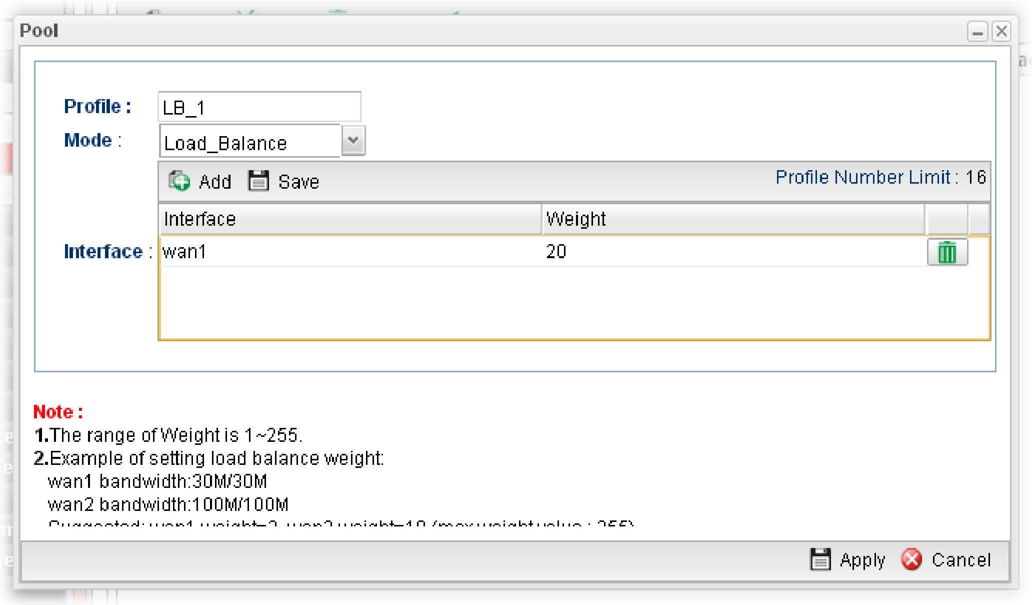


WAN >> Load Balance >> Pool

Profile	Mode	Interface

No item

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



Pool

Profile : LB_1

Mode : Load_Balance

Profile Number Limit : 16

Interface :

Interface	Weight
wan1	20

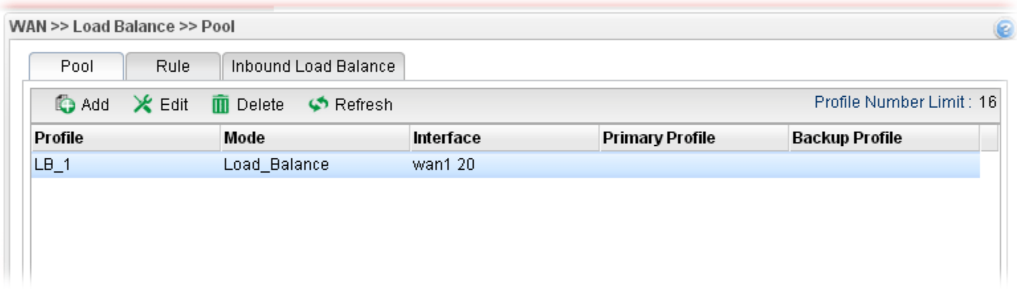
Note :
1.The range of Weight is 1~255.
2.Example of setting load balance weight:
wan1 bandwidth:30M/30M
wan2 bandwidth:100M/100M
Suggested: wan1 weight=3, wan2 weight=10 (max weight value : 255)

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.

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

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



WAN >> Load Balance >> Pool

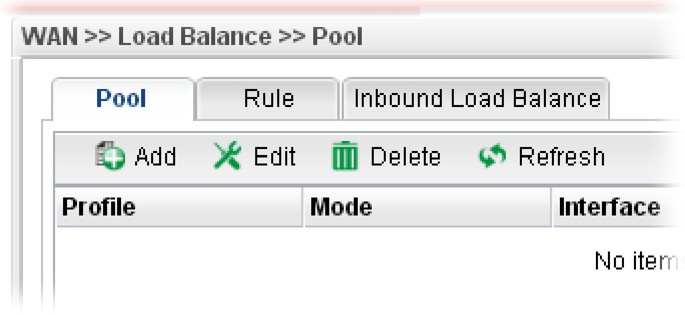
Profile Number Limit : 16

Profile	Mode	Interface	Primary Profile	Backup Profile
LB_1	Load_Balance	wan1 20		

How to add a Pool profile for Failover

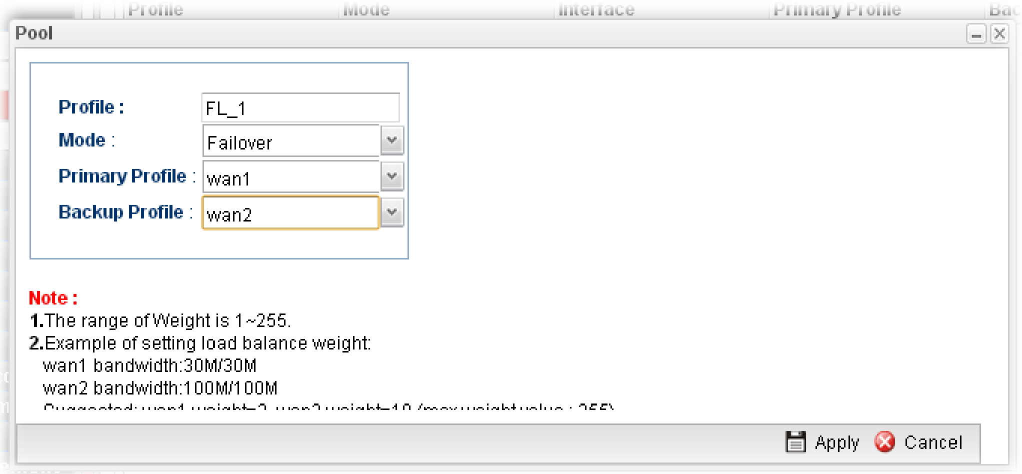
Such page allows you to set a backup profile which will be activated when the primary profile is invalid by any reason.

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



WAN >> Load Balance >> Pool

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



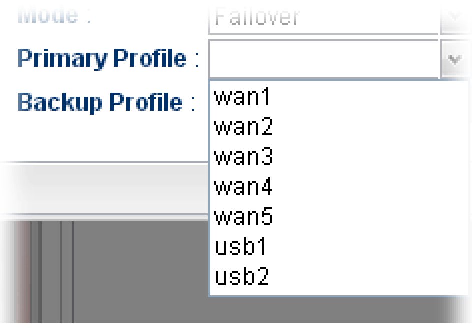
Pool

Profile : FL_1
Mode : Failover
Primary Profile : wan1
Backup Profile : wan2

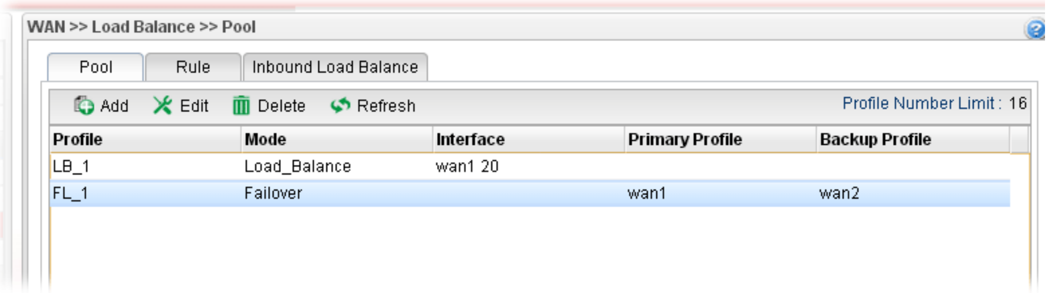
Note :
1.The range of Weight is 1~255.
2.Example of setting load balance weight:
wan1 bandwidth:30M/30M
wan2 bandwidth:100M/100M

Available parameters are listed as follows:

Item	Description

Profile	Type the name of the profile.
Mode	Choose **Failover** as the **Mode** selection.
Primary Profile	In default, the system will apply Primary Profile. If Primary Profile cannot be used any more, the Backup Profile will be used instead. Use the drop down list to choose the one you need.
Backup Profile	Use the drop down list to choose the one you need.  Mode : Failover Primary Profile : Backup Profile : wan1 wan2 wan3 wan4 wan5 usb1 usb2

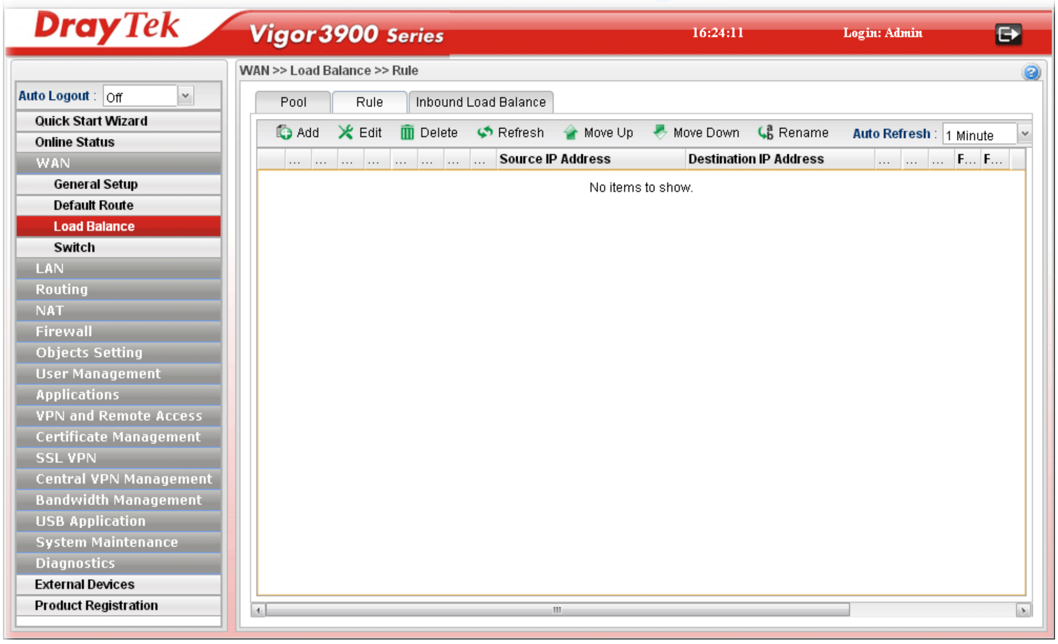
3. Click **Apply**. A new profile will be added on the page.



Profile	Mode	Interface	Primary Profile	Backup Profile
LB_1	Load_Balance	wan1 20		
FL_1	Failover		wan1	wan2

4.1.3.2 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. Simply click the **Rule** tab to open the following page:

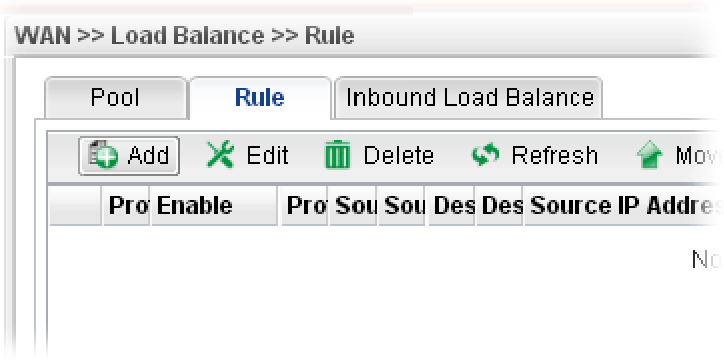


Each item will be explained as follows:

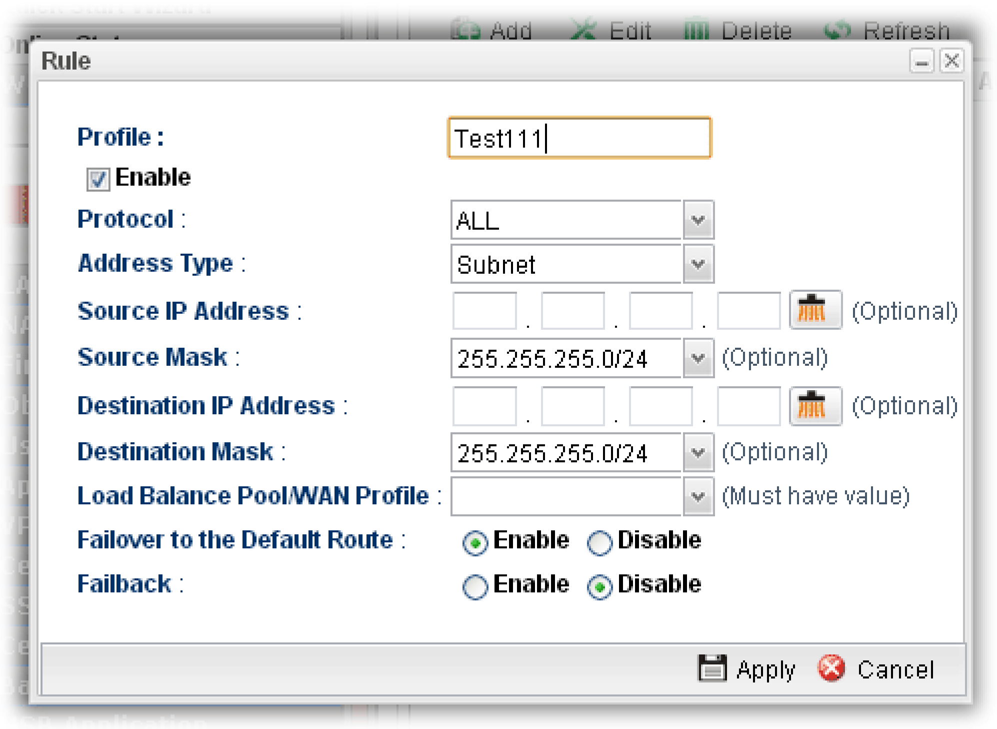
Item	Description
Add	Add a new rule profile.
Edit	Modify the selected rule profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected rule 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.
Rename	Allow to modify the selected profile name.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Profile	Display the name of the rule.
Enable	Display the status of the profile. False means disabled; True means enabled.
Protocol	Display the protocol of such rule.
Source IP Object	Display the name of the source object.
Source IP Group	Display the name of the source group.
Destination IP Object	Display the name of the destination object.
Destination IP Group	Display the name of the destination group.
Source IP Address	Display the source WAN IP address for such rule.
Destination IP Address	Display the destination WAN IP address for such rule.
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.
Failover Status	Display the status (enabled or disabled) of the function.
Failback	Display the status (enabled or disabled) of the function.

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.



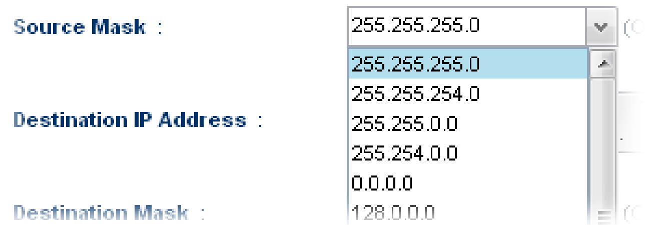
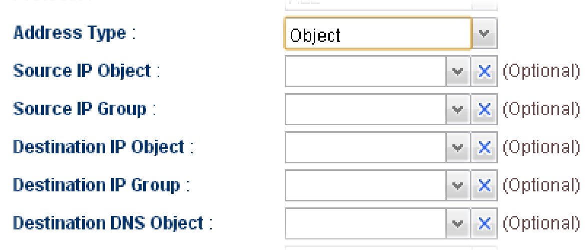
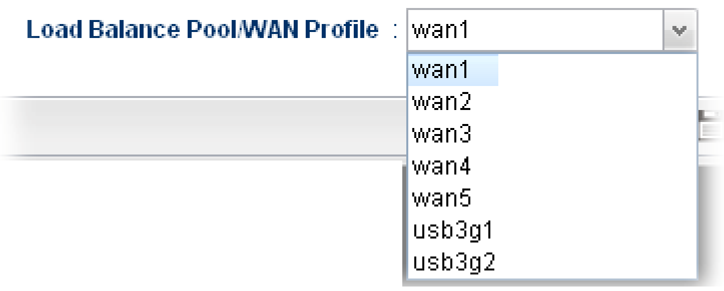
3. The following dialog will appear.



Profile :	Test111
☑ **Enable**	
Protocol :	ALL
Address Type :	Subnet
Source IP Address :	. . . (Optional)
Source Mask :	255.255.255.0/24 (Optional)
Destination IP Address :	. . . (Optional)
Destination Mask :	255.255.255.0/24 (Optional)
Load Balance Pool/WAN Profile :	(Must have value)
Failover to the Default Route :	● Enable ○ Disable
Failback :	○ Enable ● Disable

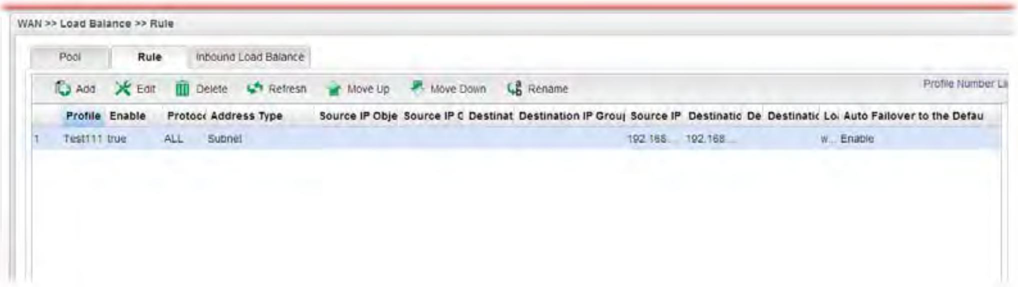
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the rule.
Enable	Check this box to enable such profile.
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.
Address Type	Choose the address type (Subnet or Object) for such rule. Each type will bring different settings for configuration.
Subnet	**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.

	 Source Mask : 255.255.255.0 255.255.255.0 255.255.254.0 255.255.0.0 255.254.0.0 0.0.0.0 128.0.0.0 Destination IP Address : Destination Mask : **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.
Object	**Source IP Object –** Use the drop down list to choose one of the source IP objects for such rule profile. **Source IP Group –**Use the drop down list to choose one of the source IP group for such rule profile. **Destination IP Object –** Use the drop down list to choose one of the destination IP objects for such rule profile. **Destination IP Group -** Use the drop down list to choose one of the destination IP group for such rule profile. **Destination DNS Object –** Use the drop down list to choose one of the DNS objects for such rule profile.  Address Type : Object Source IP Object : (Optional) Source IP Group : (Optional) Destination IP Object : (Optional) Destination IP Group : (Optional) Destination DNS Object : (Optional)
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.  Load Balance Pool/WAN Profile : wan1 wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2
Failover to the Default Route	When the specified interface disconnects due to some reason, the router can use the default route to perform data transmission.

	Enable – Click it to enable such function. **Disable** – Click it to disable such function.
Failback	When the specified interface re-connects, the traffic via other interface will be interrupted immediately. The router will use the specified interface for data transmission again. **Enable** – Click it to enable such function. **Disable** – Click it to disable such function.
Apply	Click it to save the configuration.
Cancel	Click it to return to the factory setting.

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

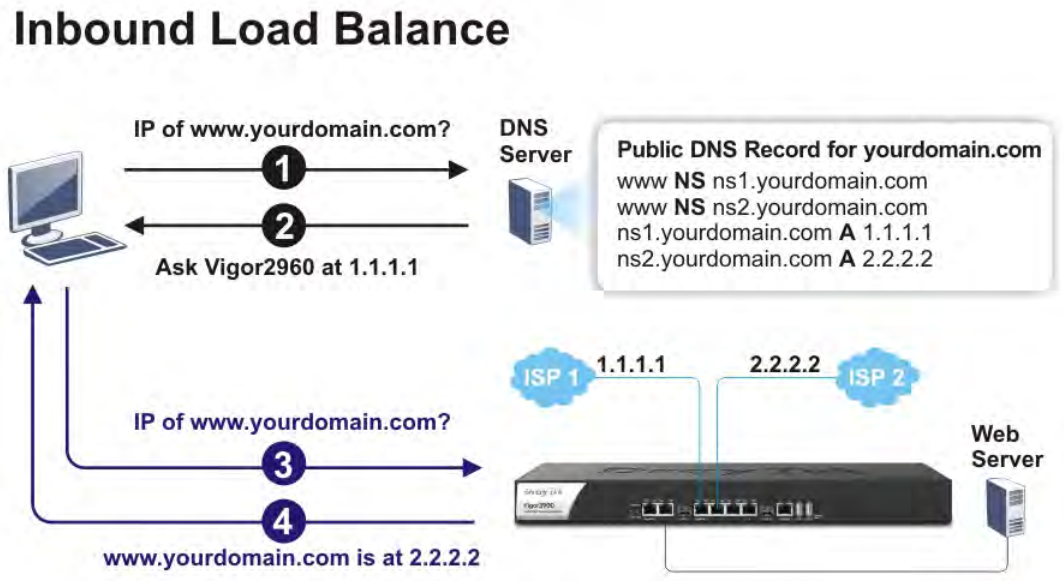


WAN >> Load Balance >> Rule

	Profile	Enable	Protoc	Address Type	Source IP Obje	Source IP C	Destinat	Destination IP Grou	Source IP	Destinatic	De	Destinatic	Lo	Auto Failover to the Defau
1	Test111	true	ALL	Subnet					192.168...	192.168...			w...	Enable

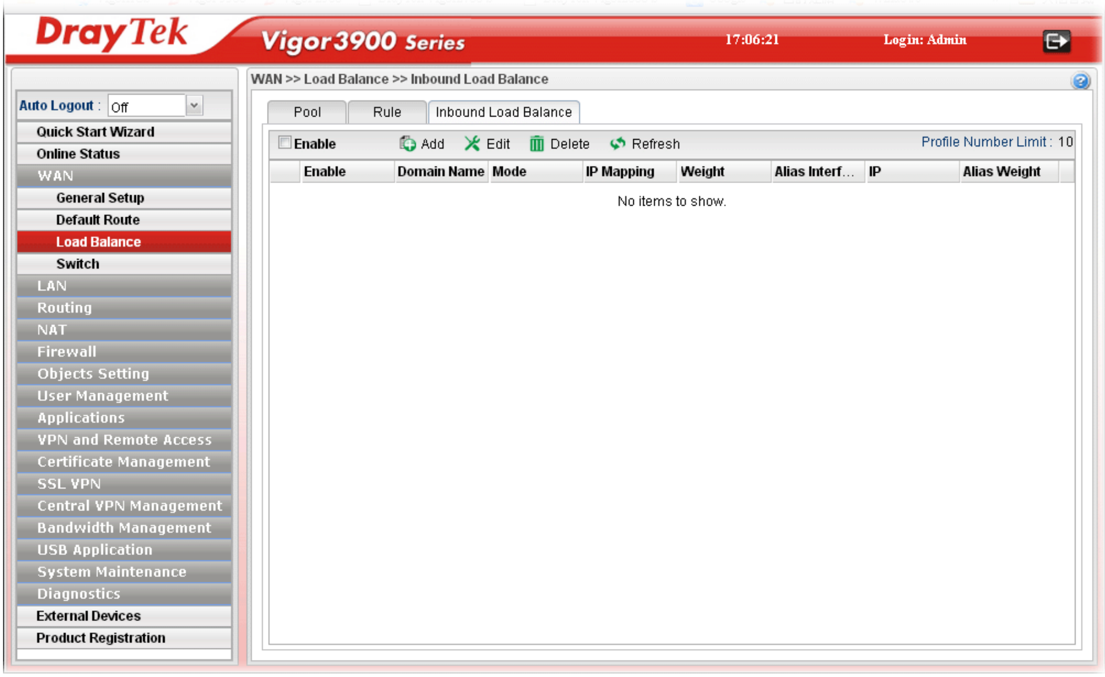
4.1.3.3 Inbound Load Balance

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



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

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



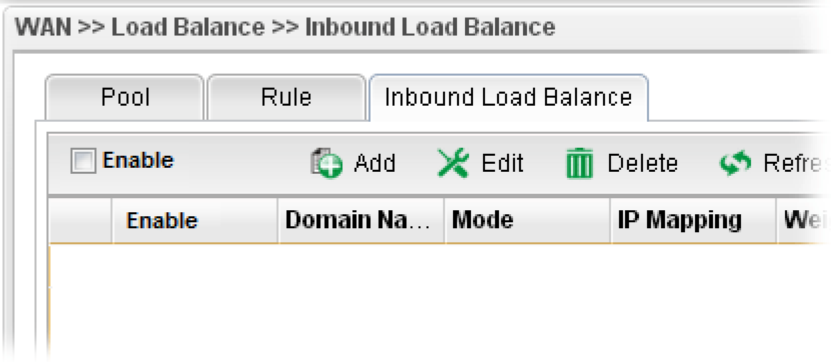
Each item will be explained as follows:

Item	Description
Enable	Check the box the enable inbound load balance function.
Add	Add a new WAN profile for inbound load balance.
Edit	Modify the selected WAN profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected WAN profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Enable	Display the status of the profile. False means disabled; True means enabled.
Domain Name	Display the domain name used by the profile.
Mode	Display the mode (failover or load balance) applied by the profile.
IP Mapping	Display the WAN interfaces used by the profile.
Weight	Display the weight(s) that WAN interface(s) used.
Alias Interface	Display the WAN interfaces used by the IP alias.
IP	Display the alias IP settings used by the profile.
Alias Weight	Display the weight that the above IP address used.

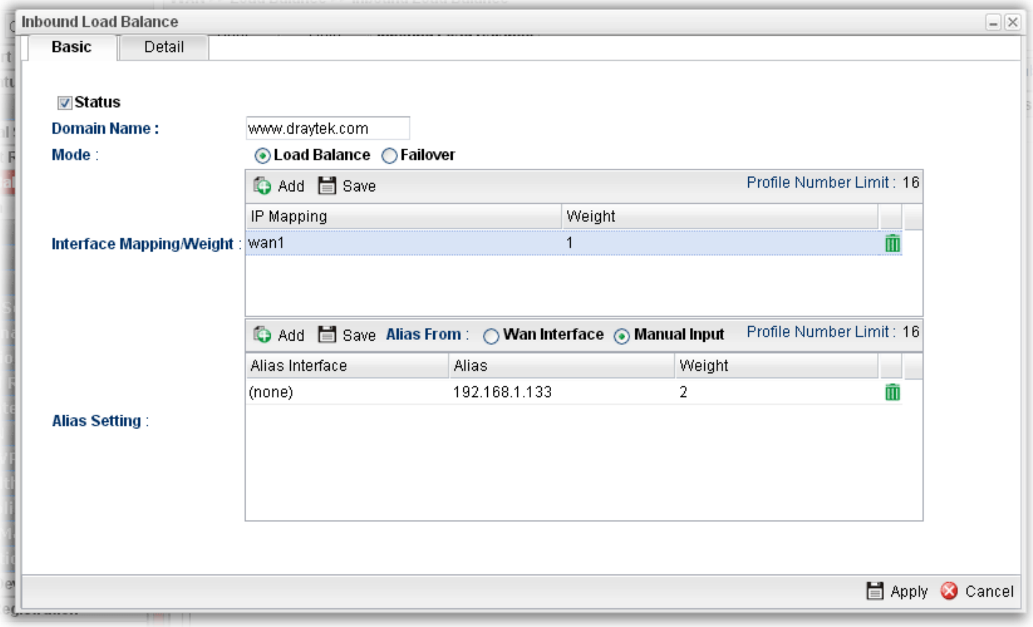
How to create a new Inbound Load Balance profile

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

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



2. Simply click the **Add** button to open the following dialog.



☑ Status

Domain Name : www.draytek.com

Mode : ● Load Balance ○ Failover

Interface Mapping/Weight : Profile Number Limit : 16

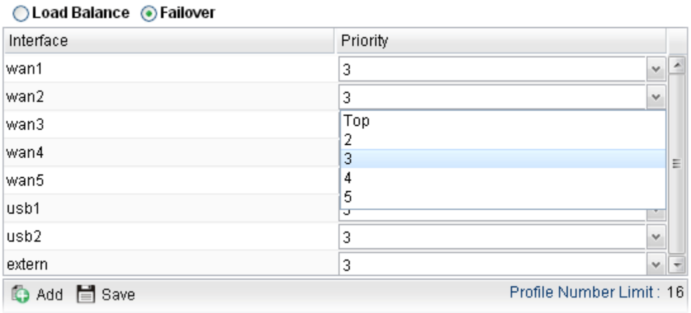
IP Mapping	Weight
wan1	1

Alias Setting : Alias From : ○ Wan Interface ● Manual Input Profile Number Limit : 16

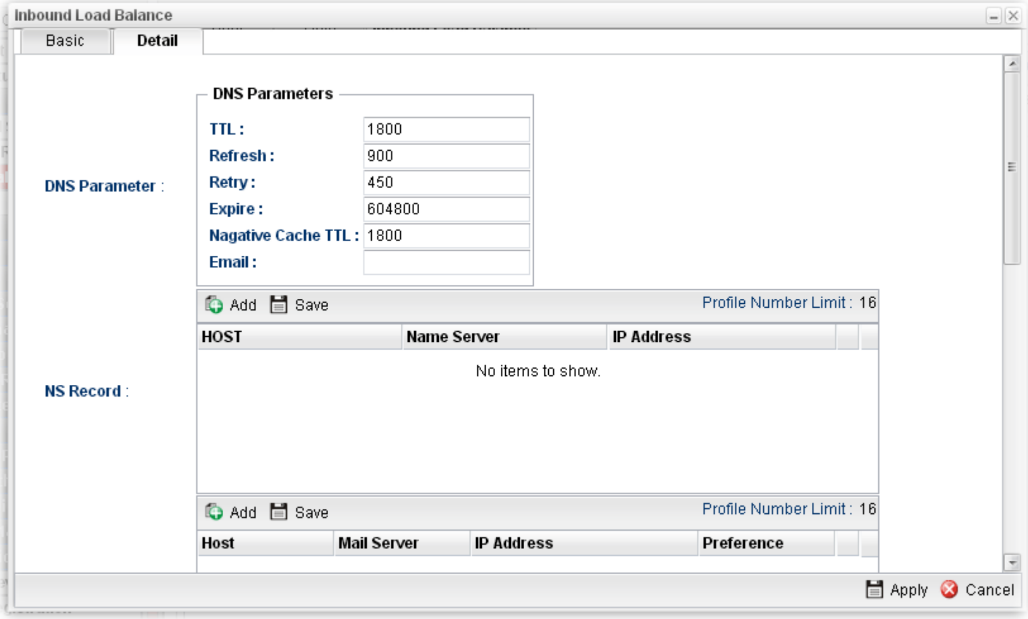
Alias Interface	Alias	Weight
(none)	192.168.1.133	2

Available parameters are listed as follows:

Item	Description
Status	Check this box to enable such profile.
Domain Name	Type an available domain name to serve the inbound load balance.
Mode	Specify the type (Load Balance or Failover) of the WAN profile for inbound load balance
Priority Setting	It is available only when Failover is selected as the Mode. There are five levels (Top, 2, 3, 4 and 5) which can be specified for WAN profiles (including default WAN profiles and user-defined WAN profiles).

	 ○ Load Balance ● Failover Interface / Priority wan1 3 wan2 3 wan3 wan4 wan5 usb1 usb2 3 extern 3 Top / 2 / 3 / 4 / 5 Add Save Profile Number Limit : 16
Interface Mapping/Weight	The domain name will inform the remote end with the IP address for DNS query asked by the remote end. The incoming query from the WAN interfaces specified in IP Mapping will be processed according to the weight value. **Add** – Click it to choose a WAN interface and weight. **Save** – Click it to save the settings. **IP Mapping** – Use the drop down list to choose a WAN interface profile which will be used by the domain. **Weight** – Use the drop down list to choose the one you want. 🗑 – click the icon to remove the selected entry.
Alias Setting	The purpose of such setting is to specify a WAN IP address from the WAN interface or by typing it manually to respond DNS query. **Add** – Click it to add a new IP address. **Save** – Click it to save the settings. **Alias From Wan Interface** – The alias IP setting can be specified from existed WAN IP alias. **Alias From Manual Input** – The alias IP setting can be specified manually. The Alias Interface is not necessary for such method. **Alias Interface** –Use the drop down list to choose a WAN interface profile for the alias IP setting. **Alias** – Use the drop down list to choose an alias IP setting (for **Alias From Wan Interface**) or type an IP address manually (for **Alias From Manual Input**). **Weight** –Use the drop down list to choose the one you want. 🗑 – click the icon to remove the selected entry.

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



DNS Parameter :

DNS Parameters

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

NS Record :

Profile Number Limit : 16

HOST	Name Server	IP Address

No items to show.

Profile Number Limit : 16

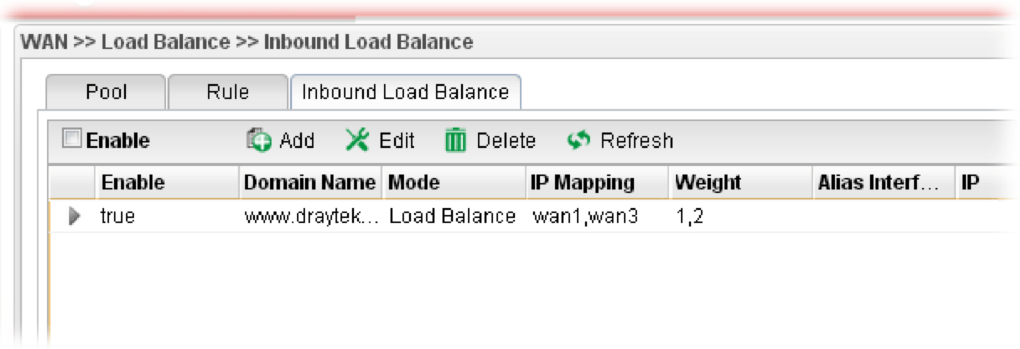
Host	Mail Server	IP Address	Preference

Available parameters are listed as follows:

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

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

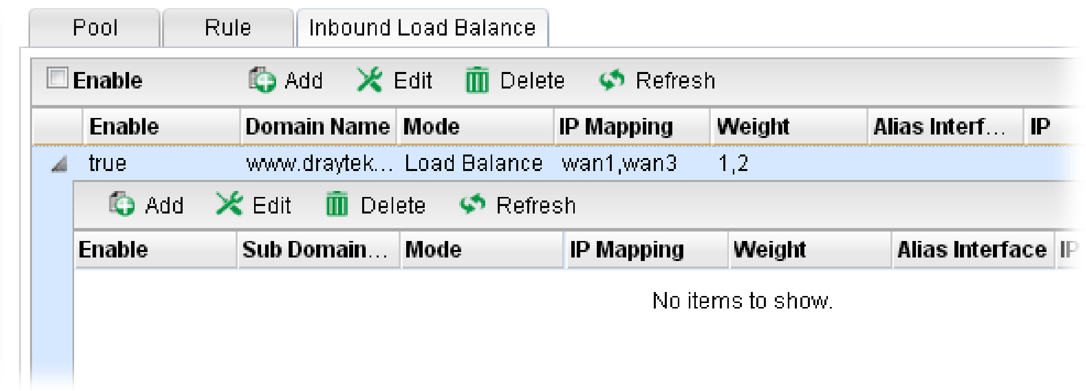
4. Click **Apply**. A new profile will be added on the page.



WAN >> Load Balance >> Inbound Load Balance

Enable	Domain Name	Mode	IP Mapping	Weight	Alias Interf...	IP
true	www.draytek...	Load Balance	wan1,wan3	1,2		

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



	Enable	Domain Name	Mode	IP Mapping	Weight	Alias Interf...	IP
◢	true	www.draytek...	Load Balance	wan1,wan3	1,2		

Enable	Sub Domain...	Mode	IP Mapping	Weight	Alias Interface	IP

No items to show.

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

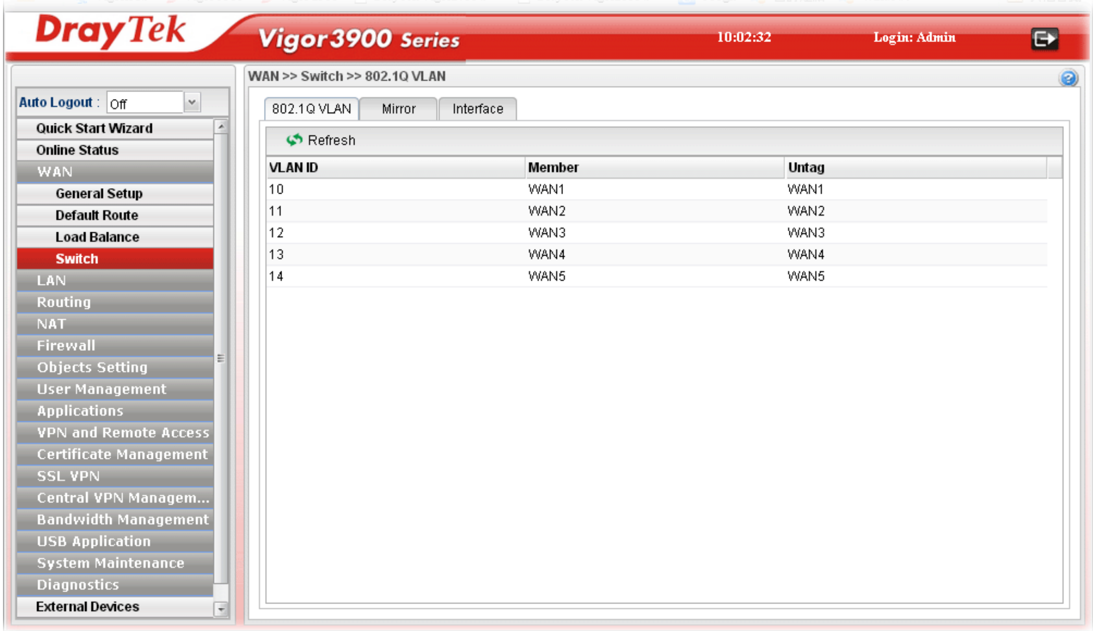
4.1.4 Switch

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

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

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



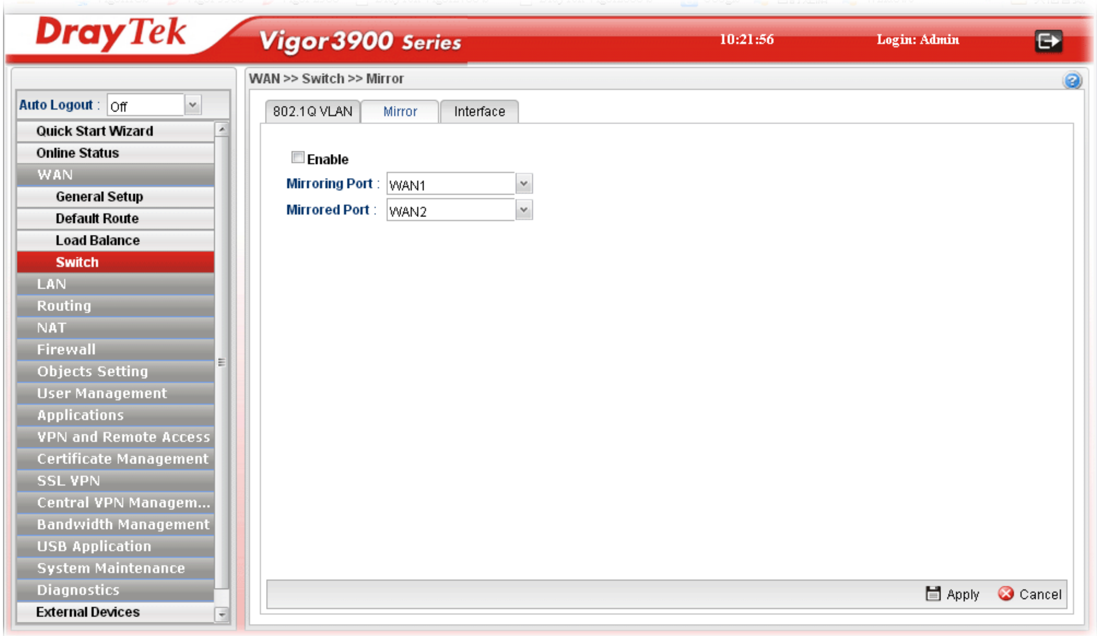
VLAN ID	Member	Untag
10	WAN1	WAN1
11	WAN2	WAN2
12	WAN3	WAN3
13	WAN4	WAN4
14	WAN5	WAN5

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.



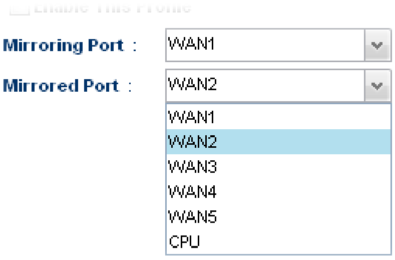
WAN >> Switch >> Mirror

□ Enable

Mirroring Port : WAN1

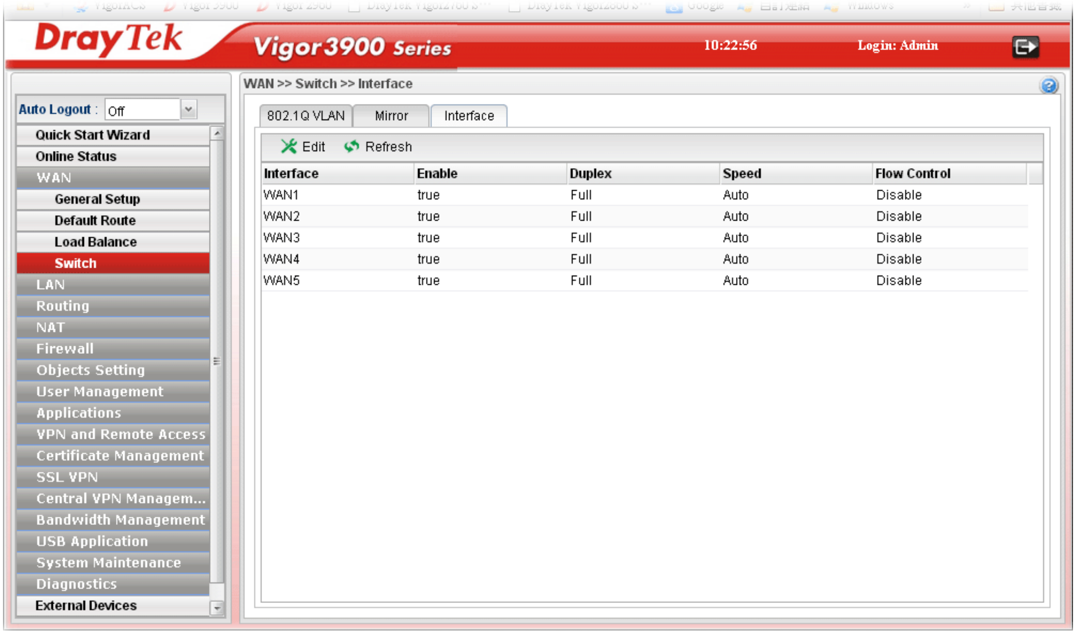
Mirrored Port : WAN2

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.  Mirroring Port : WAN1 Mirrored Port : WAN2
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

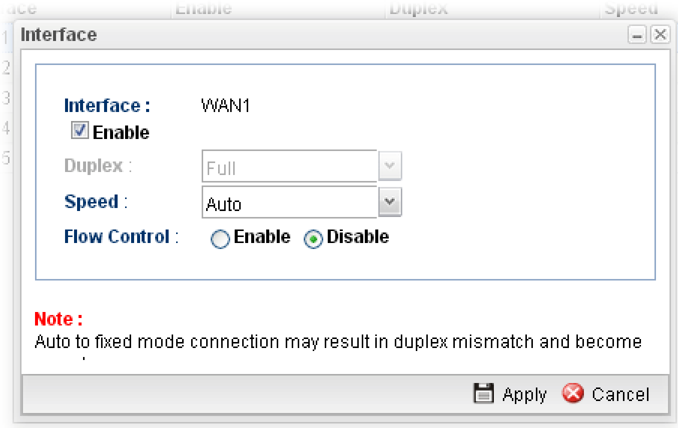
Interface Configuration

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



Interface	Enable	Duplex	Speed	Flow Control
WAN1	true	Full	Auto	Disable
WAN2	true	Full	Auto	Disable
WAN3	true	Full	Auto	Disable
WAN4	true	Full	Auto	Disable
WAN5	true	Full	Auto	Disable

Each item will be explained as follows:

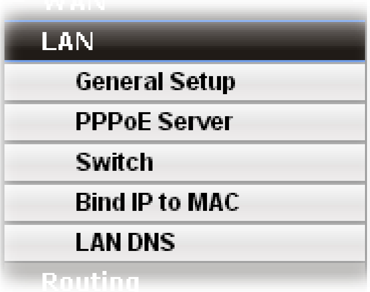
Item	Description
Edit	Choose the interface listed below and click the **Edit** button to modify the settings. A pop up window will appear for you to change the settings.  Interface : WAN1 ☑ Enable Duplex : Full Speed : Auto Flow Control : ○ Enable ● Disable Note : Auto to fixed mode connection may result in duplex mismatch and become **Interface** – Display the name of WAN interface. **Enable** – Check it to enable such interface. **Speed** – Use the drop down list to specify the transmission rate (**Auto, 10M, 100M** or **1000M**) for such interface. **Flow Control** – Click **Enable** to enable such function. When the data cache is approaching to full load, Vigor router will pause transmitting the packets till the system is able to accept new data again. It can avoid the network traffic congestion.

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

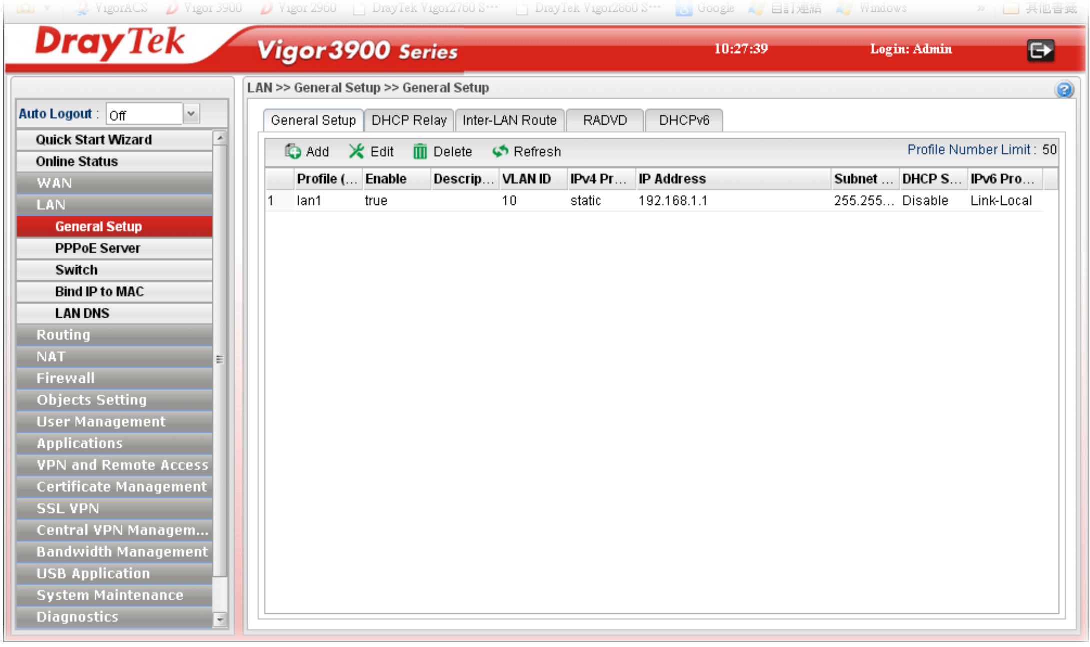


4.2.1 General Setup

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

4.2.1.1 General Setup

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



LAN >> General Setup >> General Setup

Profile Number Limit : 50

	Profile (...	Enable	Descrip...	VLAN ID	IPv4 Pr...	IP Address	Subnet ...	DHCP S...	IPv6 Pro...
1	lan1	true		10	static	192.168.1.1	255.255...	Disable	Link-Local

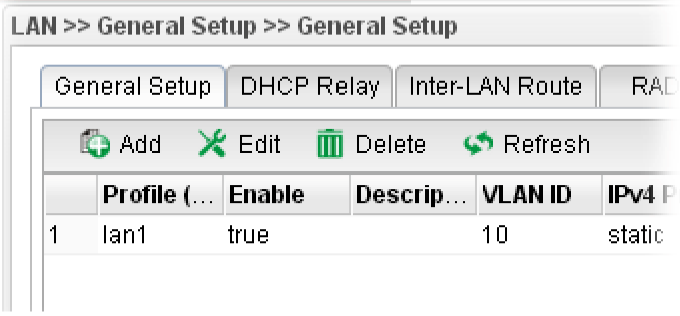
Each item will be explained as follows:

Item	Description
Add	Add a new LAN profile.

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

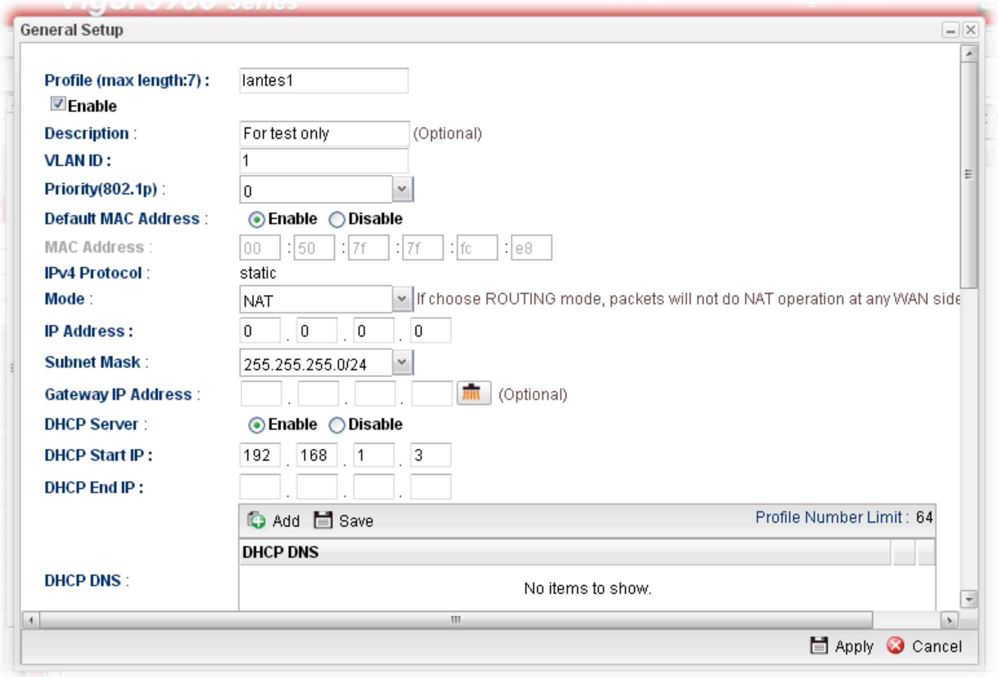
How to add a new LAN profile

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


LAN >> General Setup >> General Setup

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

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



General Setup

Profile (max length:7) : lantes1

☑ Enable

Description : For test only (Optional)

VLAN ID : 1

Priority(802.1p) : 0

Default MAC Address : ● Enable ○ Disable

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

IPv4 Protocol : static

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

IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255.255.255.0/24

Gateway IP Address : . . . (Optional)

DHCP Server : ● Enable ○ Disable

DHCP Start IP : 192 . 168 . 1 . 3

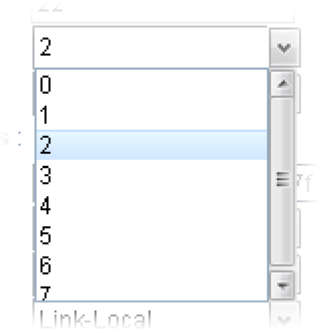
DHCP End IP : . . .

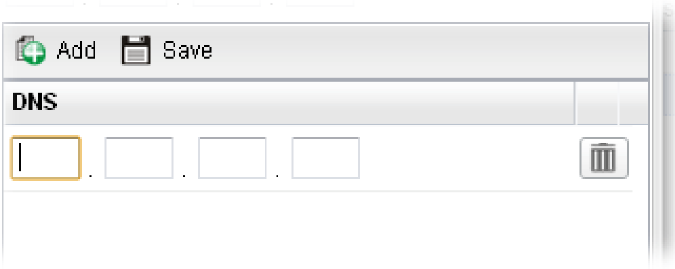
DHCP DNS : Add Save Profile Number Limit : 64

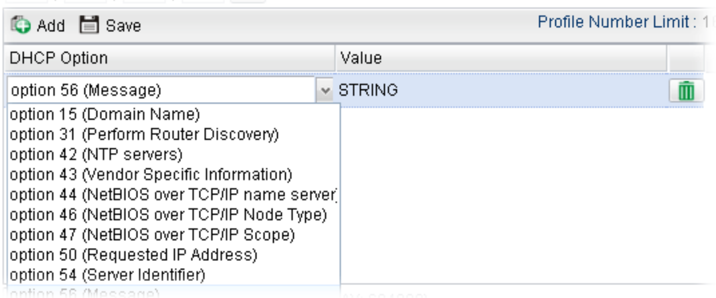
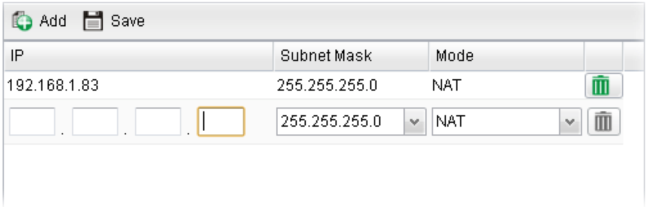
DHCP DNS
No items to show.

Apply Cancel

Available parameters are listed as follows:

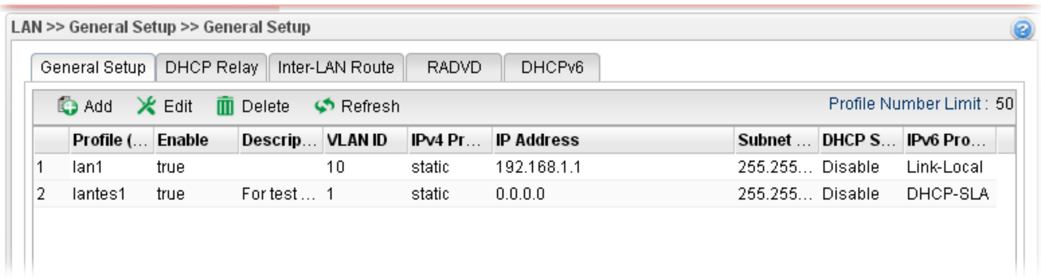
Item	Description
Profile (max length:7)	Type the name of the LAN profile.
Enable	Check this box to enable such profile.
Description	Type the description for the new LAN profile.
VLAN ID	Type a number as the VLAN ID to make the data be identified while performing data transmission.
Priority(802.1q)	Type the packet priority number for such profile. The range is from 0 to 7. 
Default MAC Address	**Enable** – Click it to enable the default MAC address for such profile. **Disable** – Click it to type the MAC address manually for such profile.
MAC Address	If Default MAC address is disabled, please specify a MAC address 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	Type the gateway IP address of the router for such LAN profile.
DHCP Server	Enable – Click it to enable the DHCP server. The DHCP server will assign the IP address randomly for the LAN user. The range of the IP addresses must be defined in DHCP Start IP and DHCP End IP. Disable – Click it to disable the DHCP server.
DHCP Start IP	Type an IP address as the starting point for DHCP server.
DHCP End IP	Type an IP address as the ending point for DHCP server.
DHCP DNS	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. 🗑 – click the icon to remove the selected entry.
DHCP Routers	In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user. However, if you want to use other gateway, please assign the IP address in this field. 🧹 – click the icon to clear the IP setting.
DHCP Options	DHCP packets can be processed by adding option number and data information when such function is enabled. Each DHCP option is composed by an option number with data. For example, Option number:100 Data: abcd When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.

	 Add Save Profile Number Limit : 1 DHCP Option | Value option 56 (Message) | STRING option 15 (Domain Name) option 31 (Perform Router Discovery) option 42 (NTP servers) option 43 (Vendor Specific Information) option 44 (NetBIOS over TCP/IP name server option 46 (NetBIOS over TCP/IP Node Type) option 47 (NetBIOS over TCP/IP Scope) option 50 (Requested IP Address) option 54 (Server Identifier) option 56 (Message) **Add** – Click it to add a new DHCP option profile. **Save** – Click it to save the setting. **DHCP Option** – Use the drop down list to choose the one you want. **Value** – Type the content of the data to be processed by the function of DHCP option. 🗑 – Click the icon to remove the selected entry.
DHCP IP Lease Time	Set a lease time for the DHCP server. The time unit is minute.
Specify Remote Dial-in IP	**Enable** – Check the box to enable this function. Remote clients within the range specified below can access into Vigor3900 WUI.
More Subnet	Specify other subnets which might be needed in the future.  Add Save IP | Subnet Mask | Mode 192.168.1.83 | 255.255.255.0 | NAT . . . | 255.255.255.0 | NAT **Add** – Click it to add a new subnet mask with IP address and specified mode. **Save** – Click it to save the settings. **IP** – Type the IP address if you click Add for adding a new entry. **Subnet Mask** – Use the drop down list to choose the one you want. **Mode** – Specify NAT or Routing as the mode. 🗑 – click the icon to remove the selected entry.
DNS Redirection	**Enable** – It can redirect DNS queries from such LAN profile to router's DNS Server. It must work with LAN DNS function.
IPv6 Protocol	It defines the IPv6 connection types for LAN interface. Possible types contain Link-Local, Static and DHCP-SLA. Except Link-Local, each type requires different parameter settings. **Link-Local**- Link-Local address is used for communicating with neighbouring nodes on the same link. It is defined by the address prefix **fe80::/10**. You don't need to setup Link-Local

	address manually for it is generated automatically according to your MAC Address. **Static** –This type allows you to setup static IPv6 address for LAN. **DHCP-SLA-** DHCPv6 client mode would use IA_NA option of DHCPv6 protocol to obtain IPv6 address from server.
IPv6 Address	If **Static** is chosen as IPv6 Protocol, please type the IPv6 address in this field.
IPv6 Prefix Length	Display the IPv6 prefix length.
DHCPv6 SLA WAN Interface	If **DHCP-SLA** is chosen as IPv6 Protocol, please choose one of the WAN profiles in this field.
DHCPv6 SLA ID	The ID number set here is used by an individual organization to create its own local addressing hierarchy and to identify subnets.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

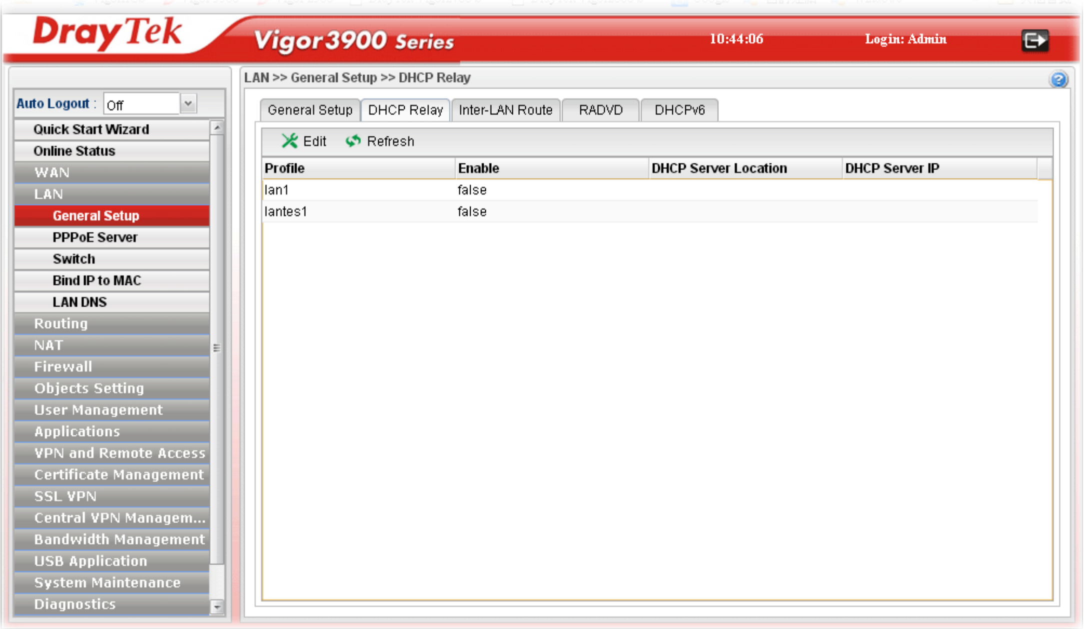


Profile Number Limit : 50

	Profile (...	Enable	Descrip...	VLAN ID	IPv4 Pr...	IP Address	Subnet ...	DHCP S...	IPv6 Pro...
1	lan1	true		10	static	192.168.1.1	255.255...	Disable	Link-Local
2	lantes1	true	For test ...	1	static	0.0.0.0	255.255...	Disable	DHCP-SLA

4.2.1.2 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.



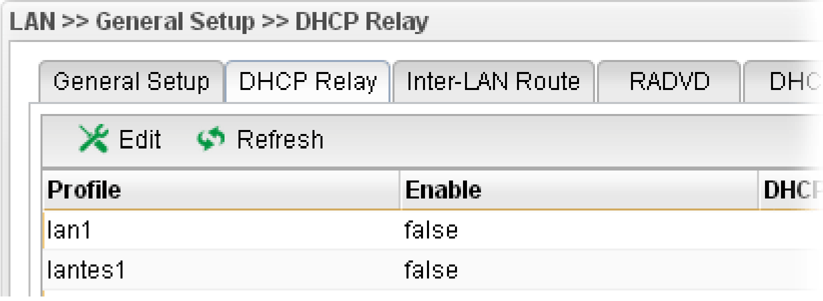
Profile	Enable	DHCP Server Location	DHCP Server IP
lan1	false		
lantes1	false		

Each item will be explained as follows:

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

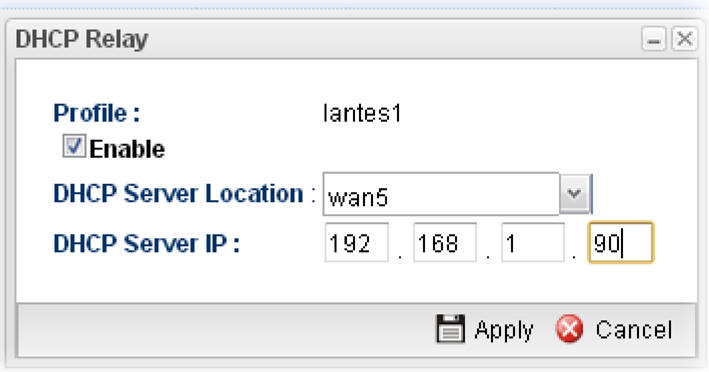
How to edit a LAN profile for DHCP Relay

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



Profile	Enable	DHC
lan1	false	
lantes1	false	

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



DHCP Relay

Profile : lantes1

☑ Enable

DHCP Server Location : wan5

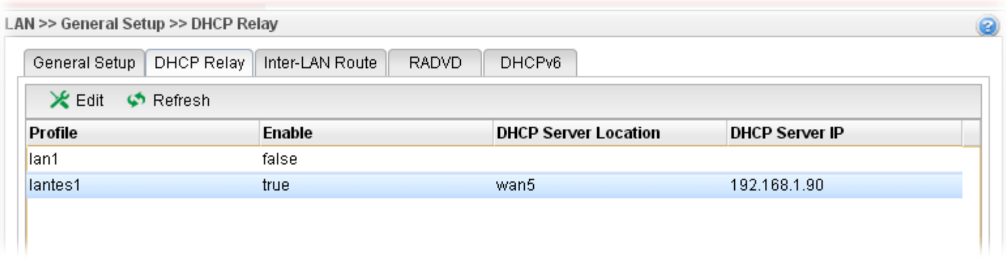
DHCP Server IP : 192 . 168 . 1 . 90

Available parameters are listed as follows:

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

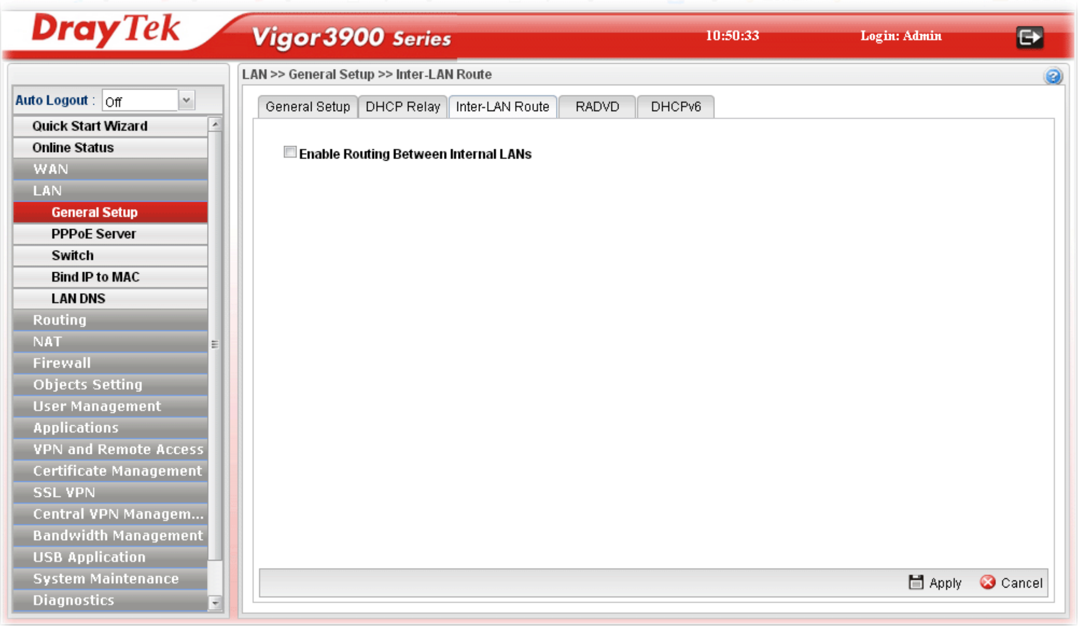


LAN >> General Setup >> DHCP Relay

Profile	Enable	DHCP Server Location	DHCP Server IP
lan1	false		
lantes1	true	wan5	192.168.1.90

4.2.1.3 Inter-LAN Route

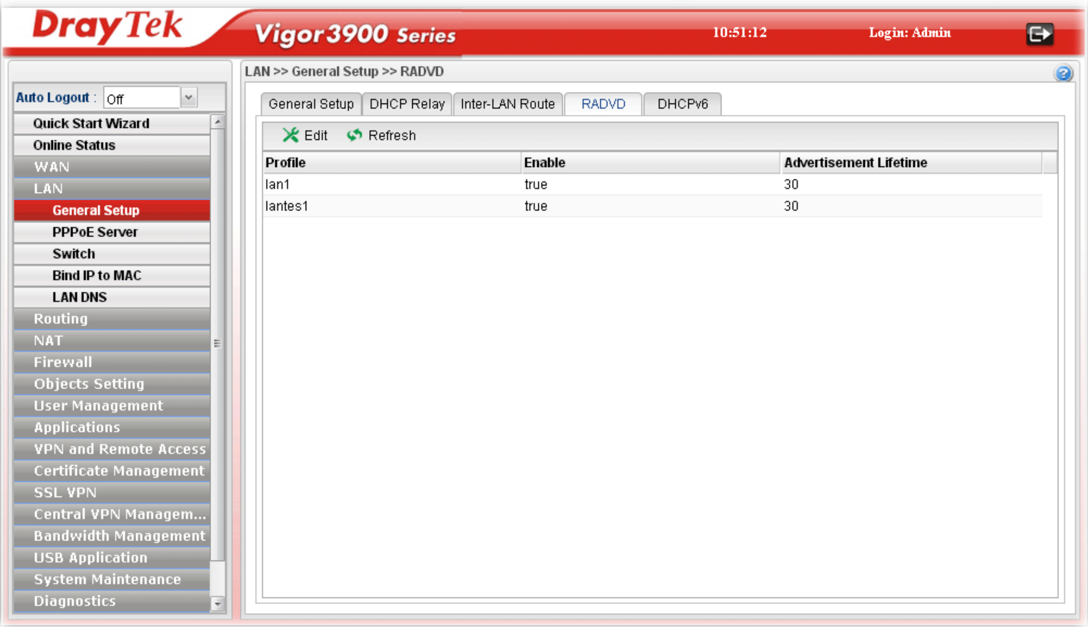
To make the users in different LAN communicating with each other, please check the box to enable Inter-LAN route function.



□ Enable Routing Between Internal LANs

4.2.1.4 RADVD

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



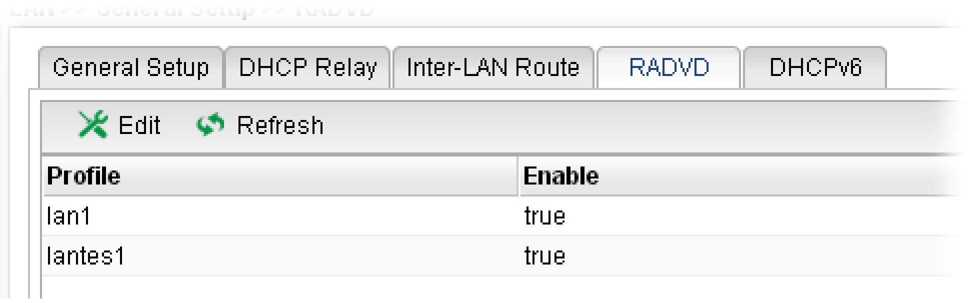
Profile	Enable	Advertisement Lifetime
lan1	true	30
lantes1	true	30

Each item will be explained as follows:

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

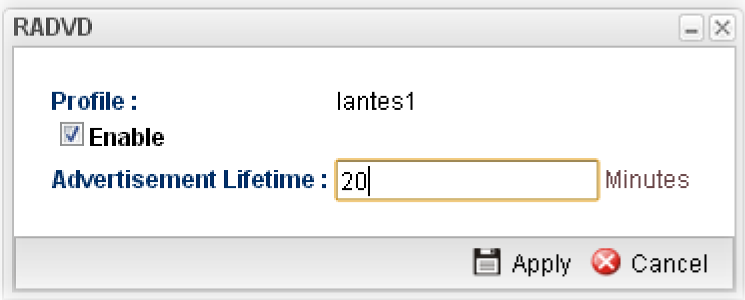
How to edit a LAN profile for RADVD

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



Profile	Enable
lan1	true
lantes1	true

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



Profile : lantes1

☑ Enable

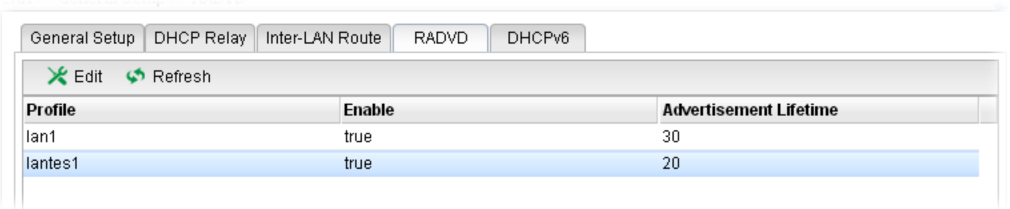
Advertisement Lifetime : 20 Minutes

Available parameters are listed as follows:

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

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

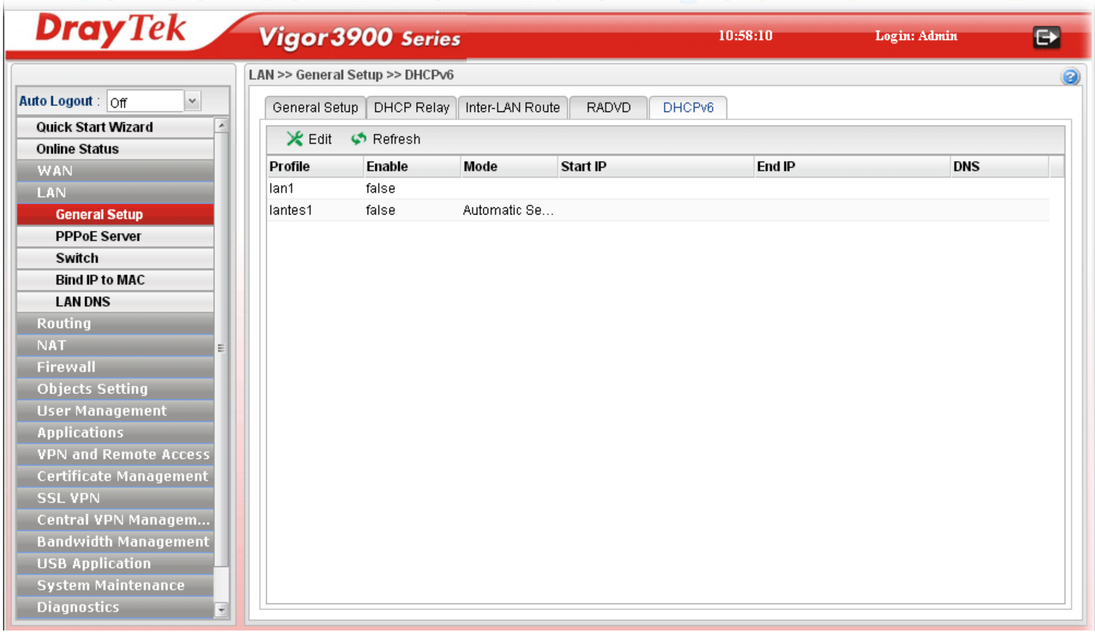
4. The LAN profile has been edited.



Profile	Enable	Advertisement Lifetime
lan1	true	30
lantes1	true	20

4.2.1.5 DHCP6

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



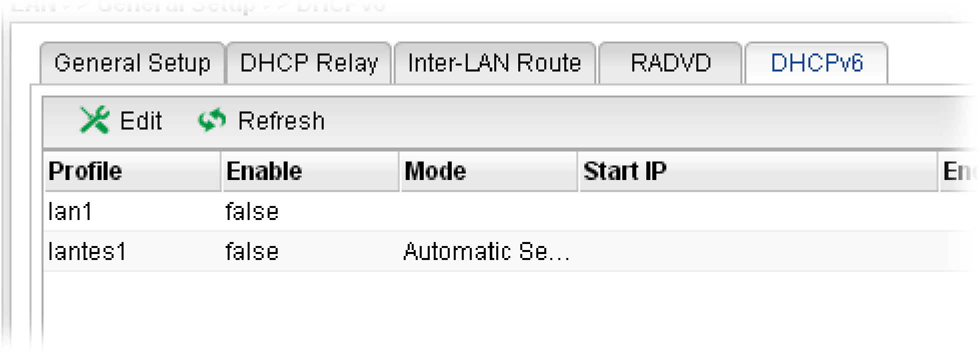
Profile	Enable	Mode	Start IP	End IP	DNS
lan1	false				
lantes1	false	Automatic Se...			

Each item will be explained as follows:

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

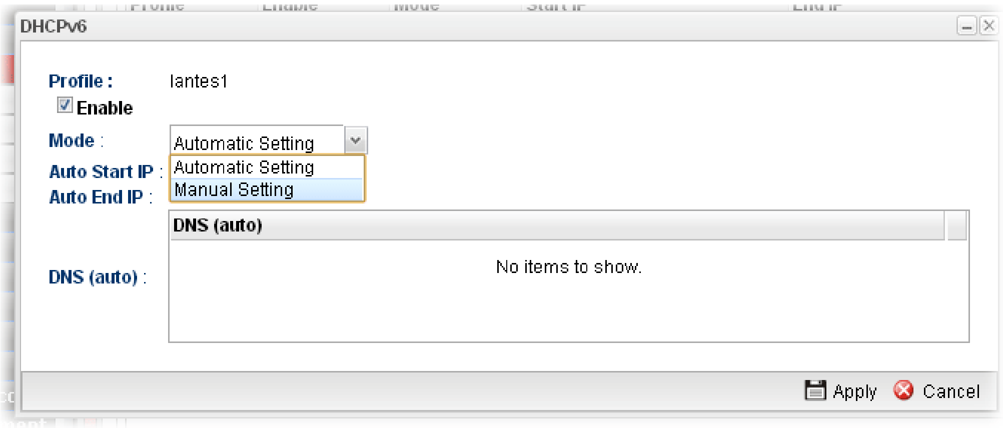
How to edit a LAN profile for DHCPv6

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



Profile	Enable	Mode	Start IP	En
lan1	false			
lantes1	false	Automatic Se...		

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



DHCPv6

Profile : lantes1

☑ Enable

Mode : Automatic Setting

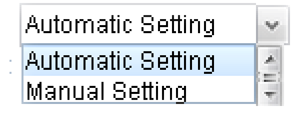
Auto Start IP :

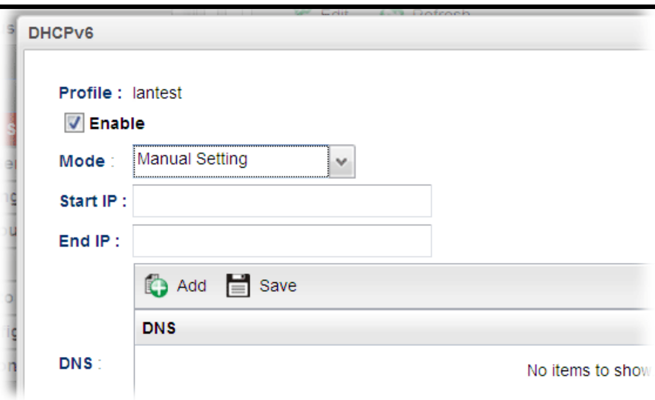
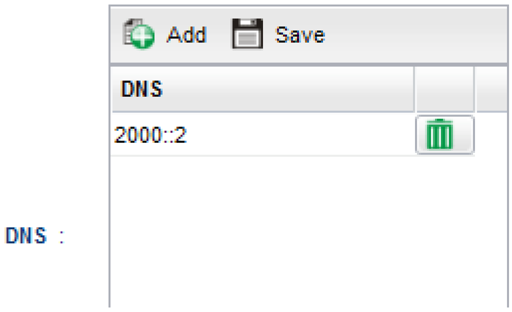
Auto End IP :

DNS (auto) :

DNS (auto)
No items to show.

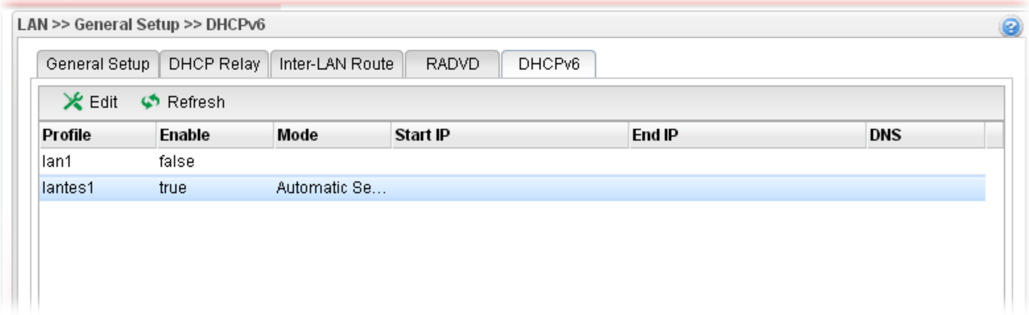
Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable	Check this box to enable this profile.
Mode	Choose **Automatic Setting** or **Manual Setting**.  Automatic Setting Automatic Setting Manual Setting **Automatic Setting** – It is not necessary to configure Start IP, End IP and DNS setting. The system will assign suitable address automatically. **Manual Setting** – You should type the Start IP address and End IP address manually.

	 DHCPv6 Profile : lantest ☑ Enable Mode : Manual Setting Start IP : End IP : Add Save DNS DNS : No items to show
Start IP	Set the starting IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.
End IP	Set the ending IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the following example: 2000:0000:0000:0000:0000:0000:0000:10 or 2000::10.
DNS	It is available when **Manual Setting** is selected as **Mode**. Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.  Add Save DNS 2000::2 DNS : **Add** – Click it to add a new IP address for DNS server. **Save** – Click it to save the setting. 🗑 – click the icon to remove the selected entry.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4. The LAN profile has been edited.


LAN >> General Setup >> DHCPv6

Profile	Enable	Mode	Start IP	End IP	DNS
lan1	false				
lantes1	true	Automatic Se...			

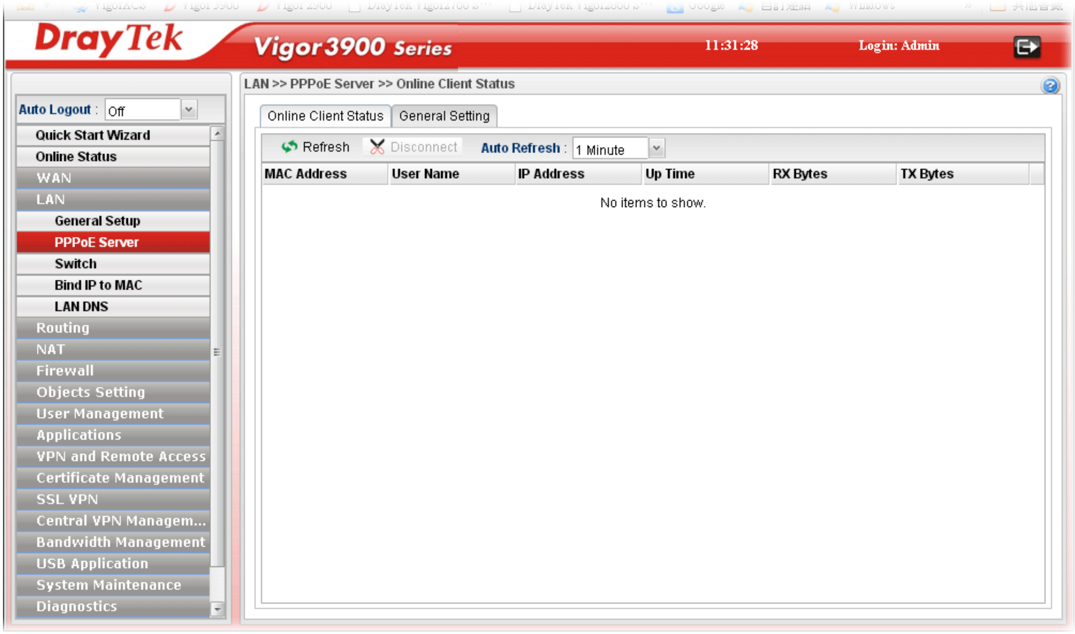
4.2.2 PPPoE Server

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

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

4.2.2.1 Online Client Status

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



LAN >> PPPoE Server >> Online Client Status

Auto Refresh : 1 Minute

MAC Address	User Name	IP Address	Up Time	RX Bytes	TX Bytes

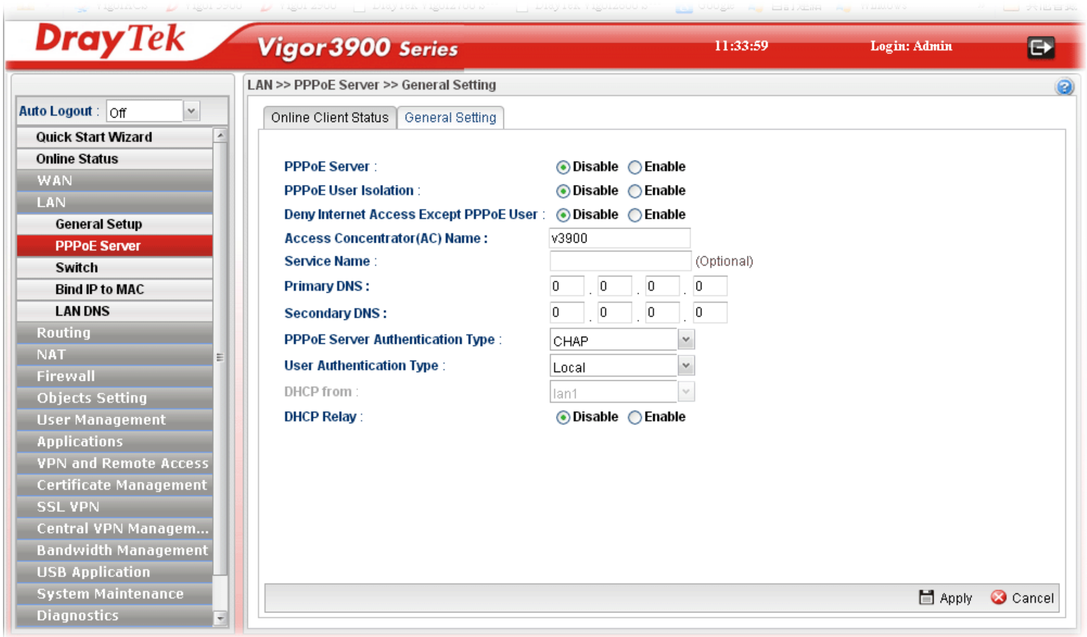
No items to show.

Each item will be explained as follows:

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

MAC Address	Display the MAC address of the client's host.
User Name	Display the user name used to access into the PPPoE server.
IP Address	Display the IP address of the client's host.
Up Time	Display the time that the PPPoE connection built.
RX Bytes	Display the total amount of received packets.
TX Bytes	Display the total amount of transmitted packets.

4.2.2.2 General Setting



LAN >> PPPoE Server >> General Setting

PPPoE Server : ● Disable ○ Enable

PPPoE User Isolation : ● Disable ○ Enable

Deny Internet Access Except PPPoE User : ● Disable ○ Enable

Access Concentrator(AC) Name : v3900

Service Name : (Optional)

Primary DNS : 0 . 0 . 0 . 0

Secondary DNS : 0 . 0 . 0 . 0

PPPoE Server Authentication Type : CHAP

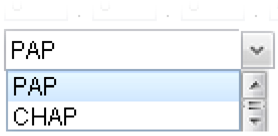
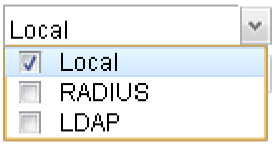
User Authentication Type : Local

DHCP from : lan1

DHCP Relay : ● Disable ○ Enable

Available parameters are listed as follows:

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

Secondary DNS	Type another IP address as secondary DNS.
PPPoE Server Authentication Type	Choose the authentication type for PPPoE server.  Any PPPoE user shall pass the authentication of PPPoE server and access into Internet.
User Authentication Type	Users in LAN can access into Internet through Vigor router with RADIUS, LDAP or local authentication. Specify the type for the users. 
LDAP Profile	It is available when **LDAP** is selected as User Authentication Type. If you choose LDAP as the authentication type, use the drop down list to specify the LDAP profile.
DHCP From	It is available when **RADIUS** is selected as User Authentication Type.
DHCP Relay	**Enable -** If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. **DHCP Server Location** – Choose one of the interfaces for DHCP server. **DHCP Server IP Address -** Set the IP address of the DHCP server you are going to use so DHCP Relay can help to forward the DHCP request to the DHCP server.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard current page modification.

4.2.3 Switch

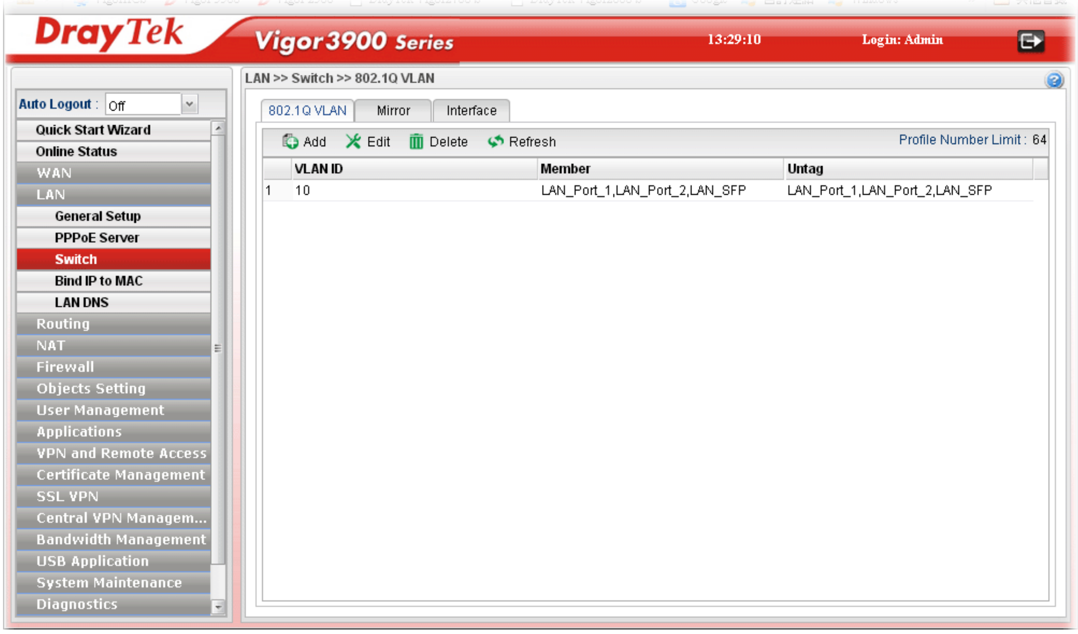
This page allows you to configure Mirroring Port, Mirrored Port, enable/disable LAN interface, and configure 802.1Q VLAN ID for different LAN interfaces, and so on.

802.1Q VLAN

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

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

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



	VLAN ID	Member	Untag
1	10	LAN_Port_1,LAN_Port_2,LAN_SFP	LAN_Port_1,LAN_Port_2,LAN_SFP

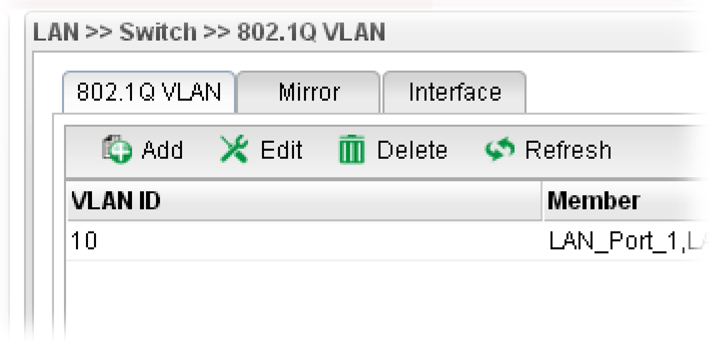
Each item will be explained as follows:

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

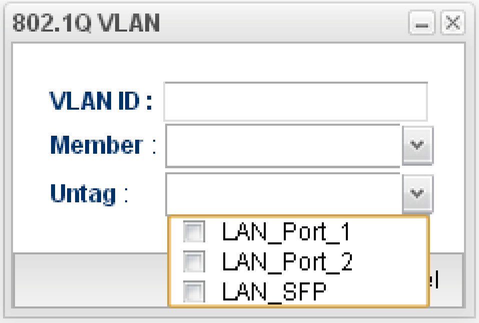
	selected rule.
Delete	Remove the selected VLAN ID setting. To delete a VLAN ID setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
VLAN ID	Display the VLAN ID number.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

How to add a new 802.1Q VLAN profile

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

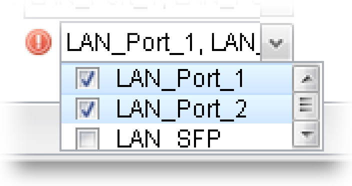


3. The following dialog will appear.

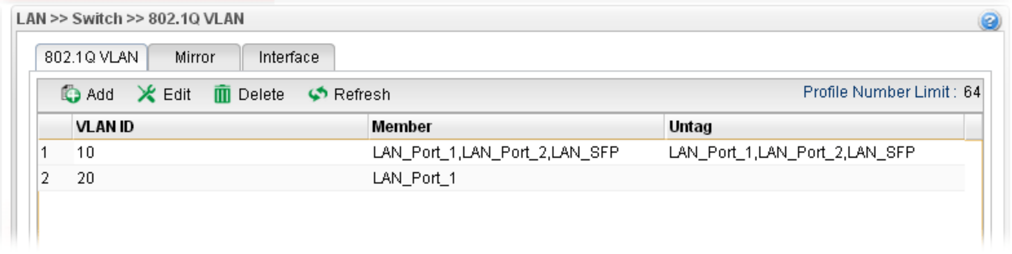


Available parameters are listed as follows:

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

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

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

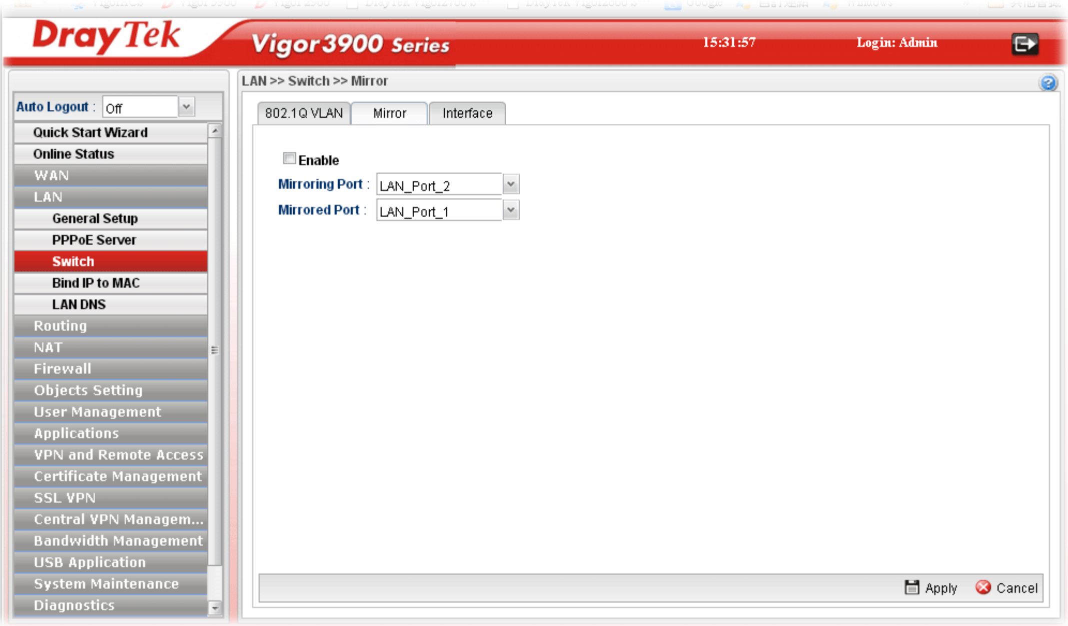


	VLAN ID	Member	Untag
1	10	LAN_Port_1,LAN_Port_2,LAN_SFP	LAN_Port_1,LAN_Port_2,LAN_SFP
2	20	LAN_Port_1	

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.

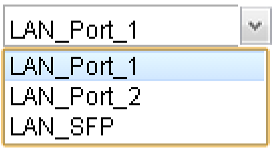
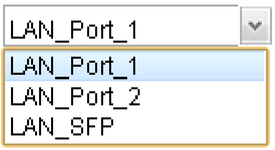


☐ Enable

Mirroring Port : LAN_Port_2

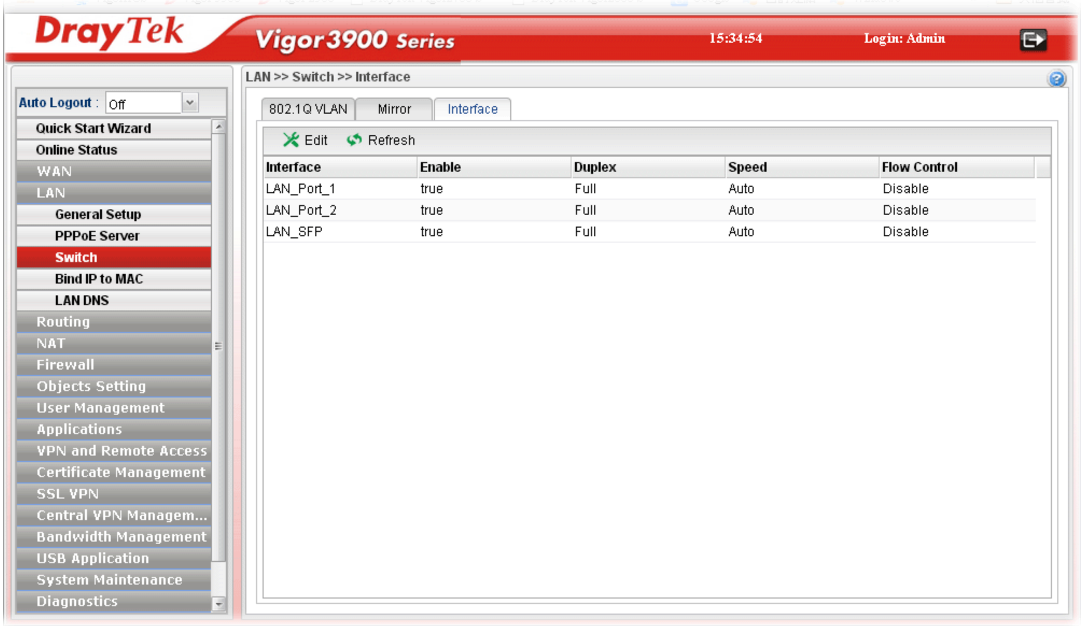
Mirrored Port : LAN_Port_1

Available parameters are listed as follows:

Item	Description
Enable This Profile	Check the box to enable the Mirror function for the switch.
Mirroring Port	Select a port to view traffic sent from mirrored ports.  LAN_Port_1 LAN_Port_1 LAN_Port_2 LAN_SFP
Mirrored Port	Select which port is necessary to be mirrored.  LAN_Port_1 LAN_Port_1 LAN_Port_2 LAN_SFP
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.



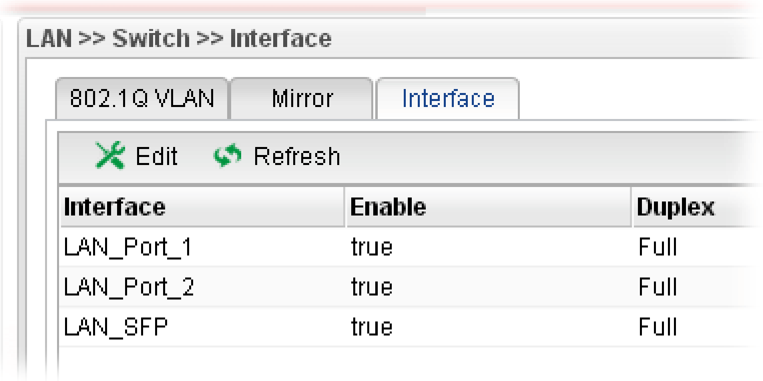
Interface	Enable	Duplex	Speed	Flow Control
LAN_Port_1	true	Full	Auto	Disable
LAN_Port_2	true	Full	Auto	Disable
LAN_SFP	true	Full	Auto	Disable

Each item will be explained as follows:

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

How to edit an Interface profile

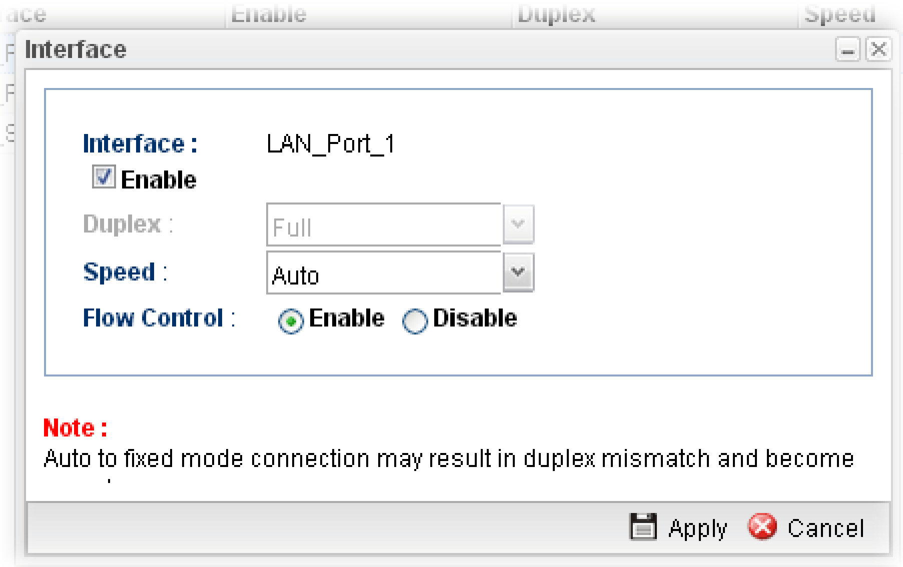
1. Open **LAN>>Switch** and click the **Interface** tab.
2. Please select a profile and click the **Edit** button.



LAN >> Switch >> Interface

Interface	Enable	Duplex
LAN_Port_1	true	Full
LAN_Port_2	true	Full
LAN_SFP	true	Full

3. The following dialog will appear.



Interface

Interface : LAN_Port_1

☑ Enable

Duplex : Full

Speed : Auto

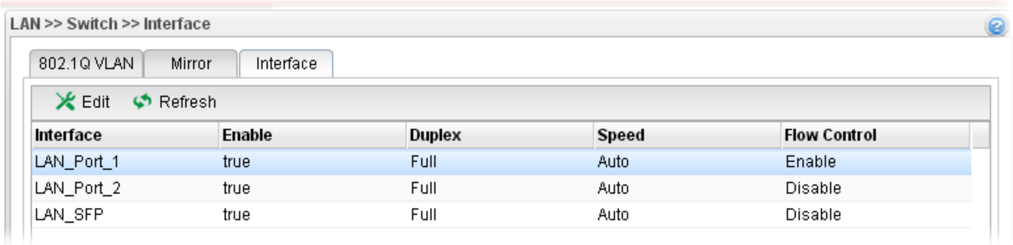
Flow Control : ● Enable ○ Disable

Note :
Auto to fixed mode connection may result in duplex mismatch and become

Available parameters are listed as follows:

Item	Description
Interface	Display the name of LAN interface profile.
Enable	Check the box to enable the Mirror function for the switch.
Speed	Use the drop down list to specify the transmission rate for such profile.
flow_control	Click **Enable** to enable such function. When the data cache is approaching to full load, Vigor router will pause transmitting the packets till the system is able to accept new data again. It can avoid the network traffic congestion.
Note	Display addition information for such interface.
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.

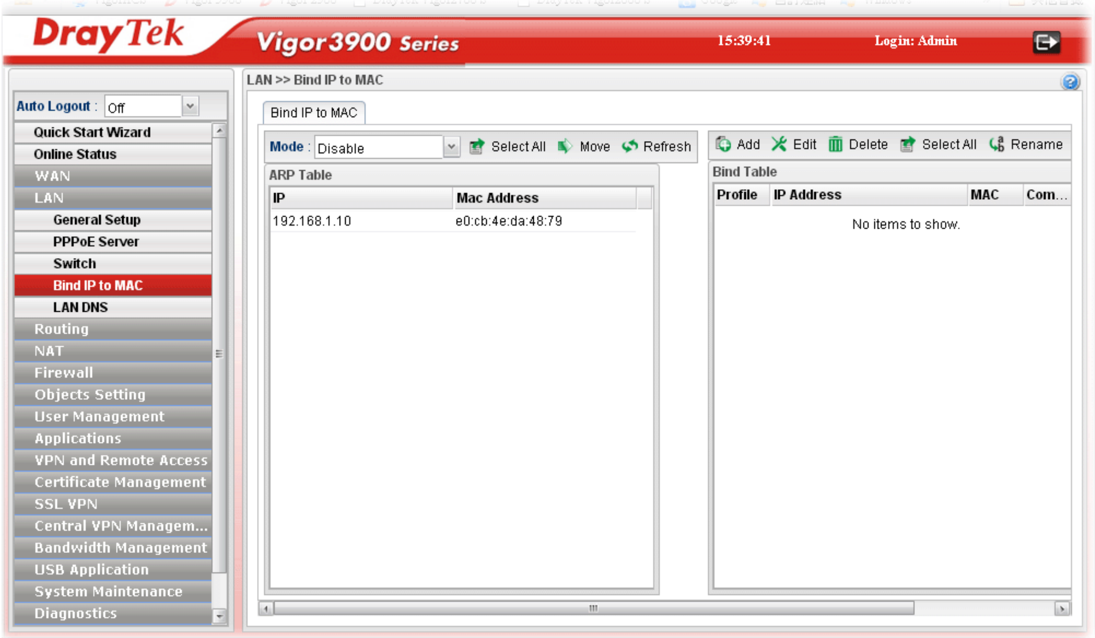


LAN >> Switch >> Interface

Interface	Enable	Duplex	Speed	Flow Control
LAN_Port_1	true	Full	Auto	Enable
LAN_Port_2	true	Full	Auto	Disable
LAN_SFP	true	Full	Auto	Disable

4.2.4 Bind IP to MAC

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



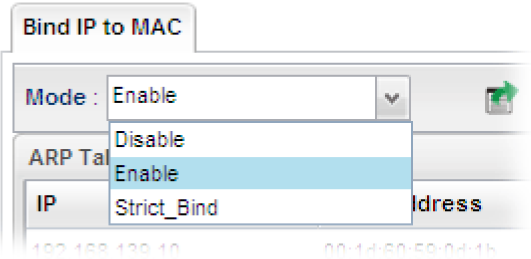
Each item will be explained as follows:

Item	Description
Mode	**Enable -** Choose it to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet. **Disable -** Choose it to disable this function. All the settings on this page will be invalid. **Strict Bind** – Choose it to lock the connection of the IP/MAC which is not listed in IP Bind List.
Select All	Allow you to choose all the items listed in ARP Table.
Move	Move the selected item to IP Bind List.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
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.
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. **Comment** – Display the brief description for such profile.

How to configure Bind IP to MAC

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



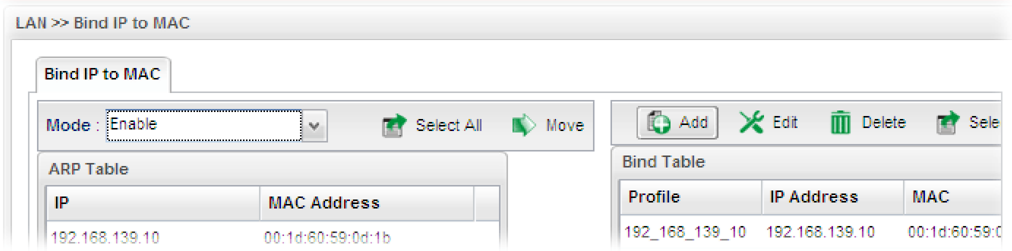
There are three modes offered for you to choose.

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

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

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

3. Click **Add**.



Mode : Enable

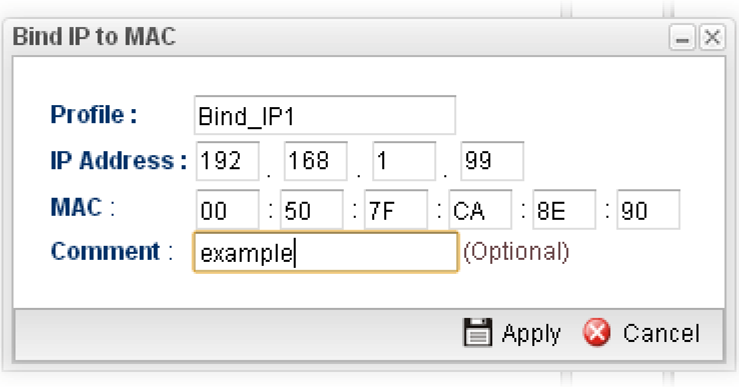
ARP Table

IP	MAC Address
192.168.139.10	00:1d:60:59:0d:1b

Bind Table

Profile	IP Address	MAC
192_168_139_10	192.168.139.10	00:1d:60:59:0

4. The following dialog appears.



Profile : Bind_IP1

IP Address : 192 . 168 . 1 . 99

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

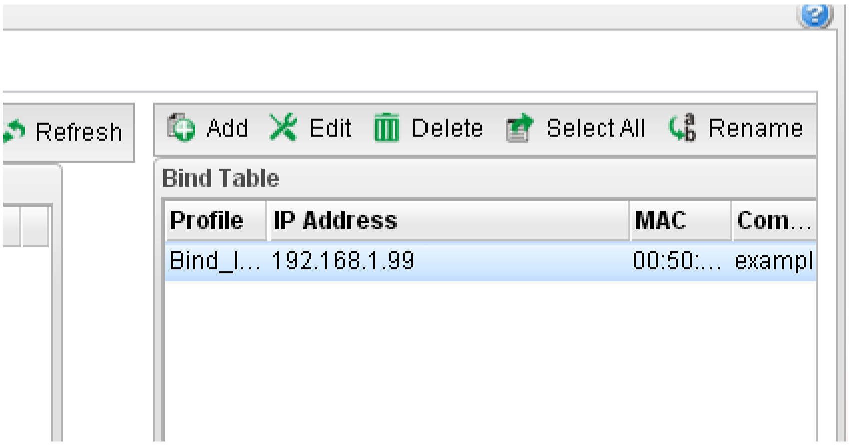
Comment : example (Optional)

Available parameters are listed as follows:

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

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

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

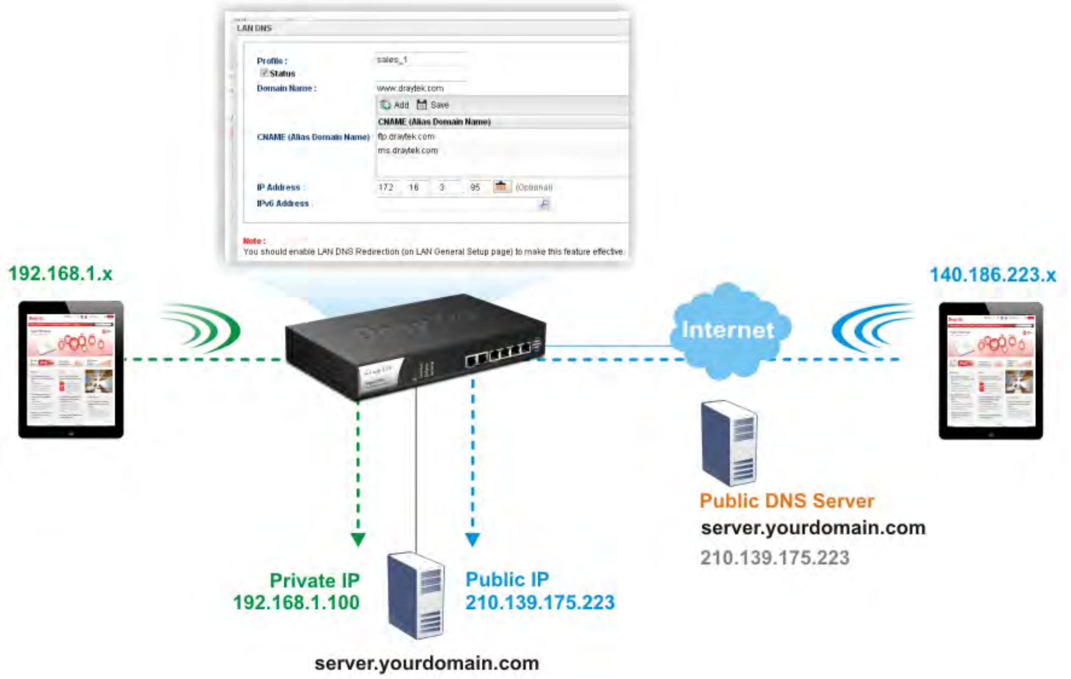


Bind Table

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

4.2.5 LAN DNS

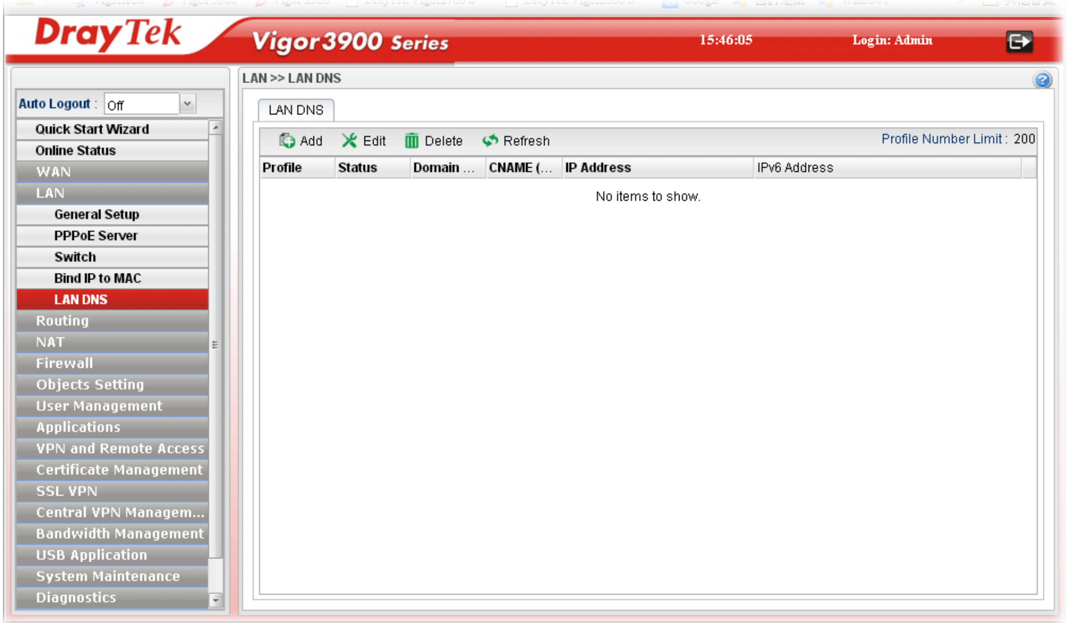
LAN DNS is a simple version of DNS server. It is not necessary for the user to build another DNS server in LAN. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.



LAN DNS

Profile : sales_1
☑ Status
Domain Name : www.draytek.com
CNAME (Alias Domain Name) :
CNAME (Alias Domain Name)
ftp.draytek.com
ms.draytek.com
IP Address : 172 . 16 . 3 . 95 (Optional)
IPv6 Address :

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



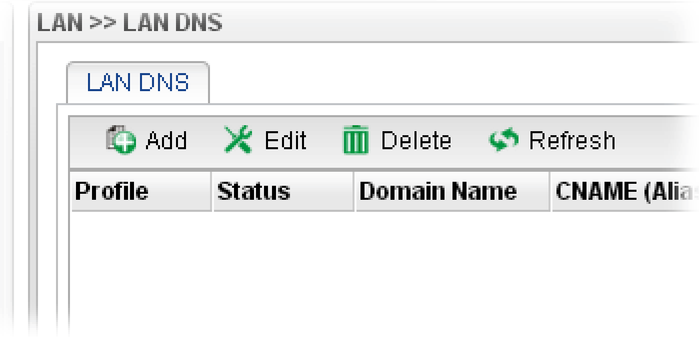
No items to show.

Each item will be explained as follows:

Item	Description
Add	Add a new VLAN ID setting.
Edit	Modify the selected VLAN ID setting. To edit VALN ID setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected VLAN ID setting. To delete a VLAN ID setting, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of the profile.
Status	Display if such profile is enabled (true) or disabled (false).
Domain Name	Display the domain name configured for such profile.
CNAME(Alias Domain Name)	Display the alias domain name for such profile.
IP Address	Display the IP address of the domain name.
IPv6 Address	Display the IPv6 address of the domain name.

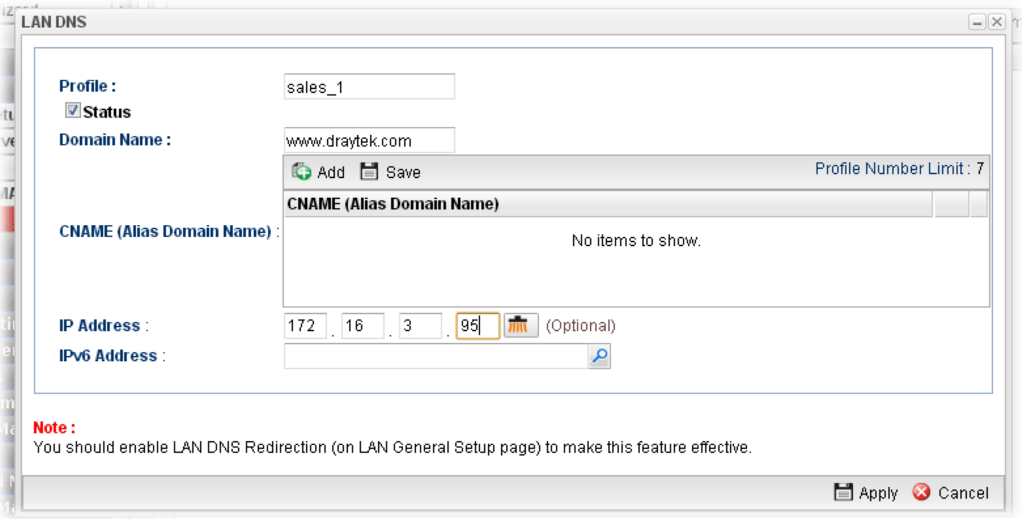
How to add a new LAN DNS profile

1. Open **LAN>>LAN DNS.**
2. Click the **Add** button.



Profile	Status	Domain Name	CNAME (Alia

3. The following dialog will appear.



Profile : sales_1

☑ Status

Domain Name : www.draytek.com

Profile Number Limit : 7

CNAME (Alias Domain Name) :

CNAME (Alias Domain Name)
No items to show.

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

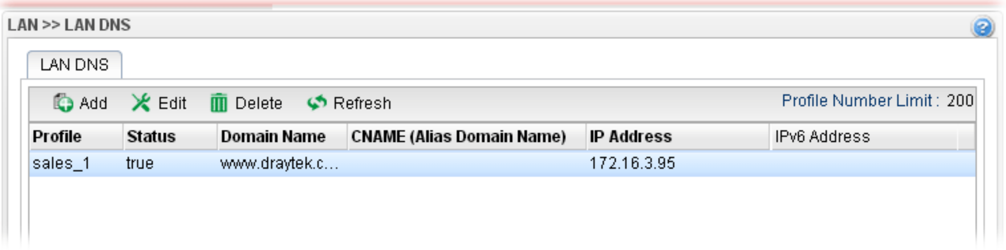
IPv6 Address :

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

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
Status	Check the box to enable such profile.
Domain Name	Type the domain name for such profile.
CNAME (Alias Domain Name)	Type several domain names in this field. LAN DNS will redirect both Domain name and CNAME to an assigned IP. For example, Domain Name is set with "www.draytek.com", and the CNAME is set as "www.dray.com". If the IP address is set with "192.168.1.123", then both "www.draytek.com" and "www.dray.com" will be directed to "192.168.1.123".
IP Address	The IP address will be used for mapping with the domain name specified above.
IPv6 Address	The IPv6 address will be used for mapping with the domain name specified above.

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



LAN >> LAN DNS

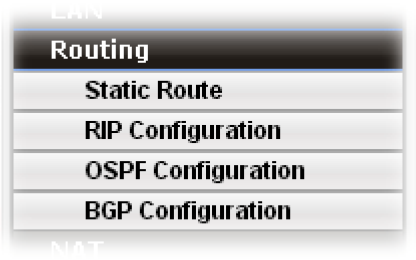
LAN DNS

Add | Edit | Delete | Refresh — Profile Number Limit : 200

Profile	Status	Domain Name	CNAME (Alias Domain Name)	IP Address	IPv6 Address
sales_1	true	www.draytek.c...		172.16.3.95	

4.3 Routing

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

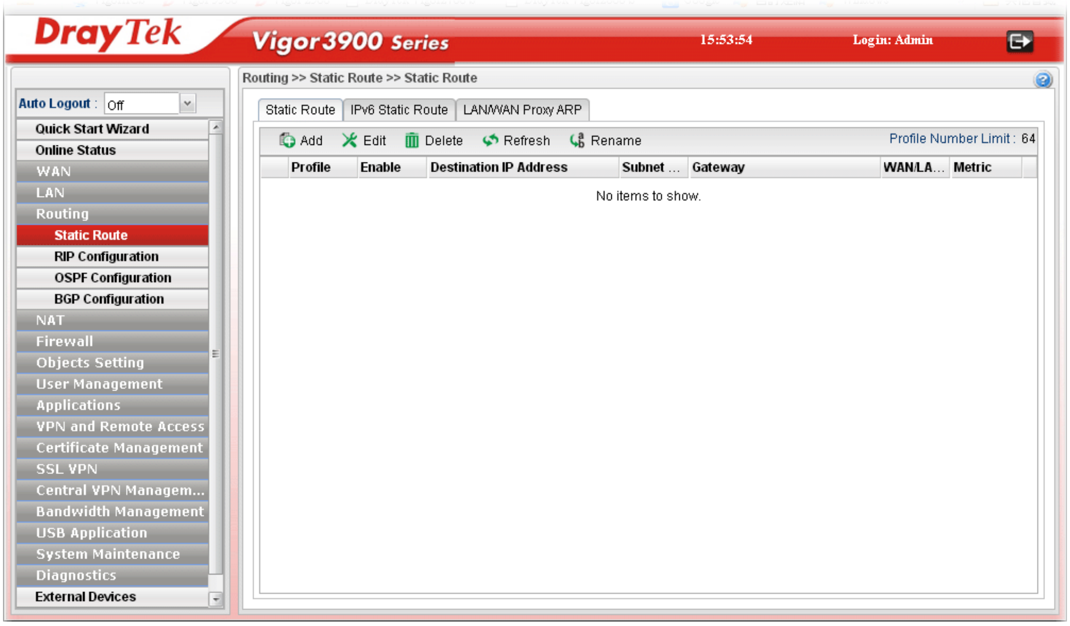


4.3.1 Static Route

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.

4.3.1.1 Static Route

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



Routing >> Static Route >> Static Route

Static Route | IPv6 Static Route | LAN/WAN Proxy ARP

Add | Edit | Delete | Refresh | Rename — Profile Number Limit : 64

Profile	Enable	Destination IP Address	Subnet ...	Gateway	WAN/LA...	Metric

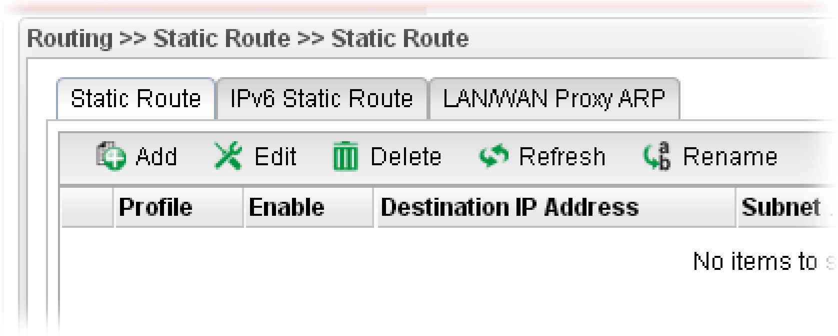
No items to show.

Each item will be explained as follows:

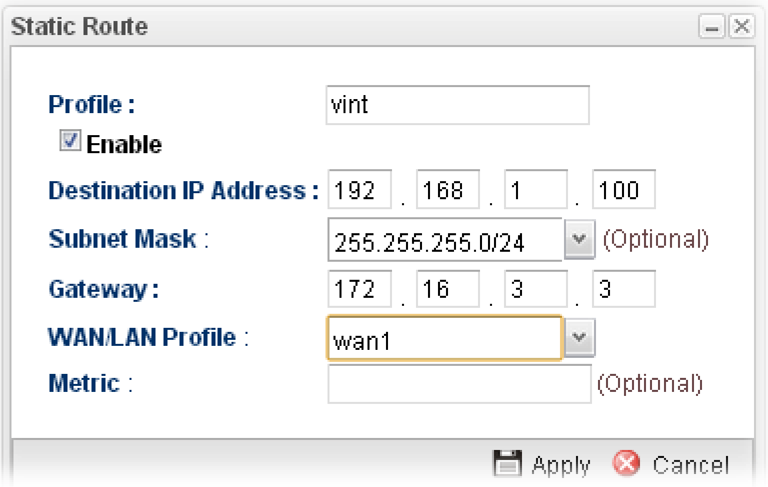
Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete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

How to add a new Static Route profile

1. Open **Routing>>Static Routing** and click the **Static Route** tab.
2. Click the **Add** button.



3. The following dialog will appear.



Static Route

Profile : vint

☑ Enable

Destination IP Address : 192 . 168 . 1 . 100

Subnet Mask : 255.255.255.0/24 (Optional)

Gateway : 172 . 16 . 3 . 3

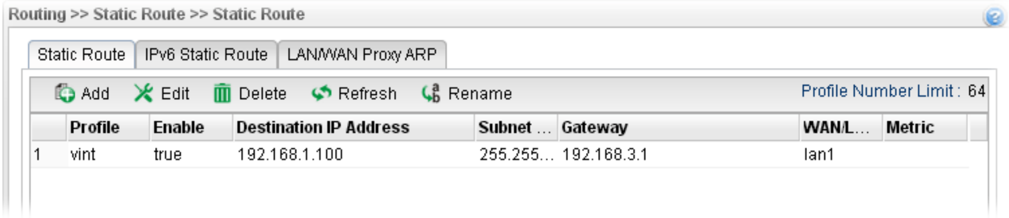
WAN/LAN Profile : wan1

Metric : (Optional)

Available parameters are listed as follows:

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

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



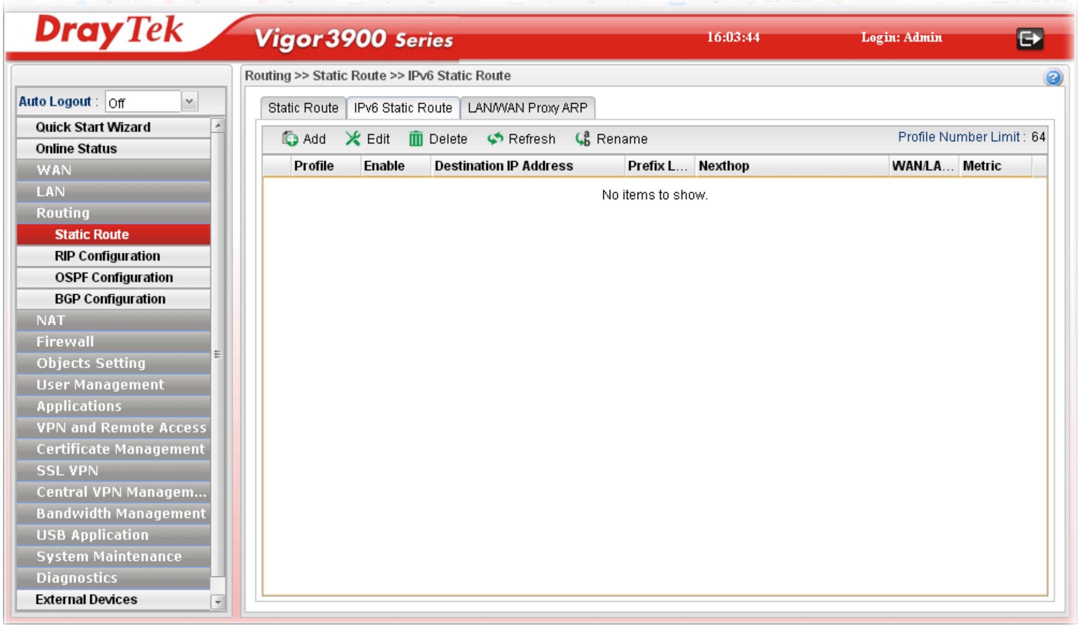
Routing >> Static Route >> Static Route

Profile Number Limit : 64

	Profile	Enable	Destination IP Address	Subnet ...	Gateway	WAN/L...	Metric
1	vint	true	192.168.1.100	255.255...	192.168.3.1	lan1	

4.3.1.2 IPv6 Static Route

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

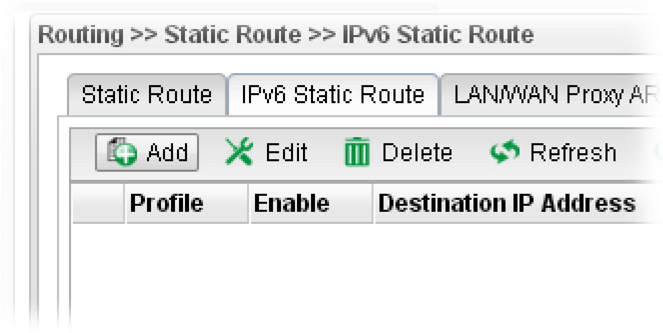


Each item will be explained as follows:

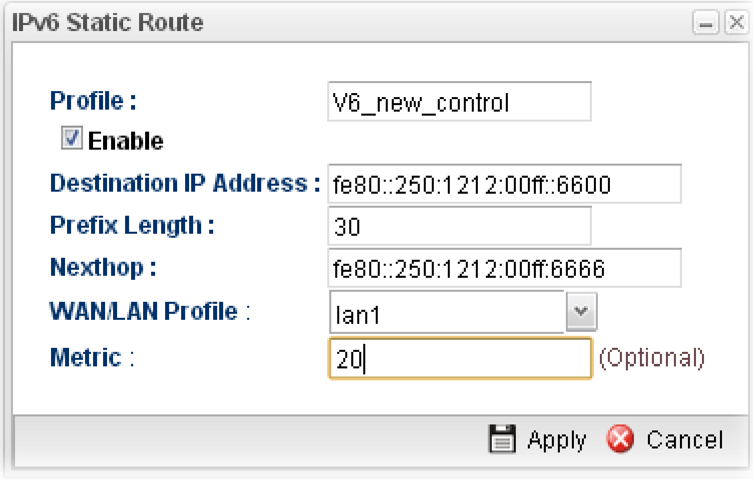
Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete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

How to add a new IPv6 Static Route profile

1. Open **Routing>>Static Route** and click the **IPv6 Static Route** tab.
2. Click the **Add** button.



3. The following dialog will appear.



Profile : V6_new_control

☑ Enable

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

Prefix Length : 30

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

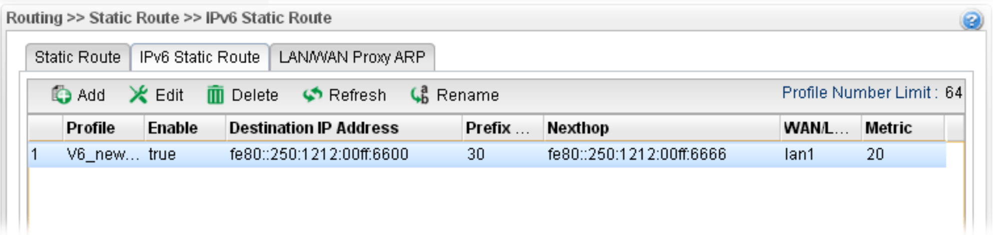
WAN/LAN Profile : lan1

Metric : 20 (Optional)

Available parameters are listed as follows:

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

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

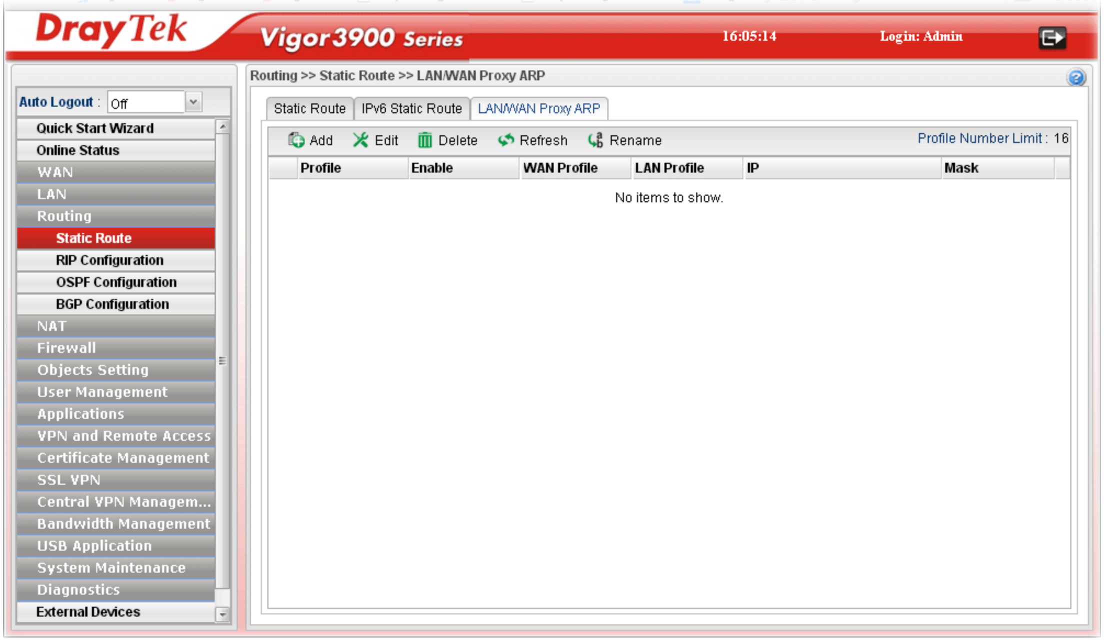


	Profile	Enable	Destination IP Address	Prefix ...	Nexthop	WAN/L...	Metric
1	V6_new...	true	fe80::250:1212:00ff:6600	30	fe80::250:1212:00ff:6666	lan1	20

4.3.1.3 LAN/WAN Proxy ARP

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

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



Profile	Enable	WAN Profile	LAN Profile	IP	Mask

No items to show.

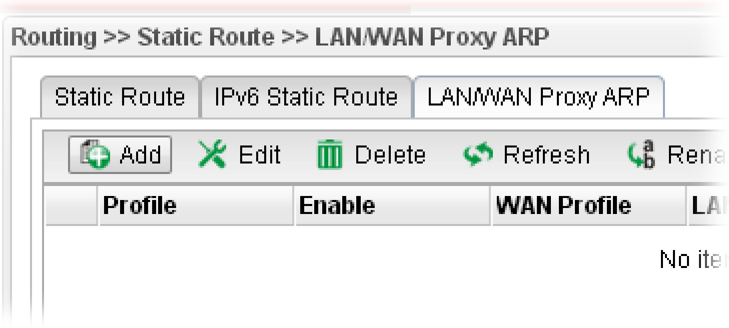
Each item will be explained as follows:

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

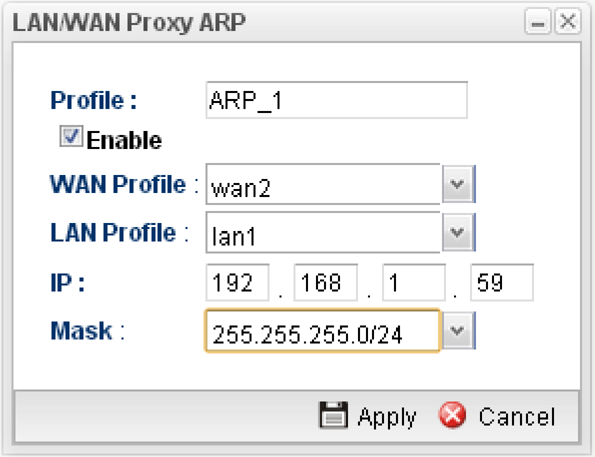
Rename	Allow to modify the selected profile name.
Profile Number Limit	Display the total number of the profiles to be created.
Profile	Display the name of such profile
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN profile used for such ARP profile.
LAN Profile	Display the LAN profile used for such ARP profile.
IP	Display the IP address used by such ARP profile.
Mask	Display the mask address used by such ARP profile.

How to add a new Proxy ARP profile

1. Open **Routing>>Static Route** and click the **LAN/WAN Proxy ARP** tab.
2. Click the **Add** button.



3. The following dialog will appear.



Profile : ARP_1

☑ Enable

WAN Profile : wan2

LAN Profile : lan1

IP : 192 . 168 . 1 . 59

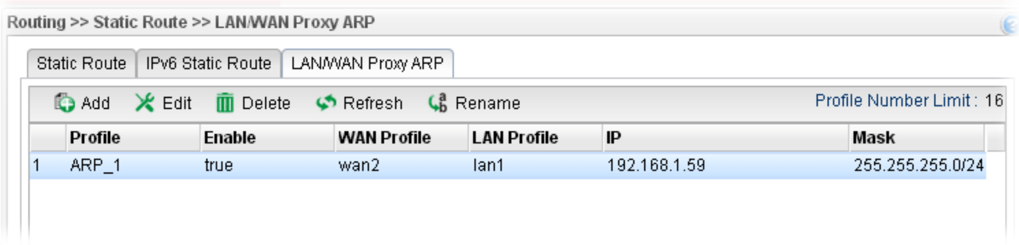
Mask : 255.255.255.0/24

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the static route profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose one of the WAN/USB profiles of the gateway for such profile.

LAN Profile	Choose one of the LAN profiles for such profile.
IP	Type an IP address for such profile.
Mask	Use the drop down menu to specify mask address.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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



Routing >> Static Route >> LAN/WAN Proxy ARP

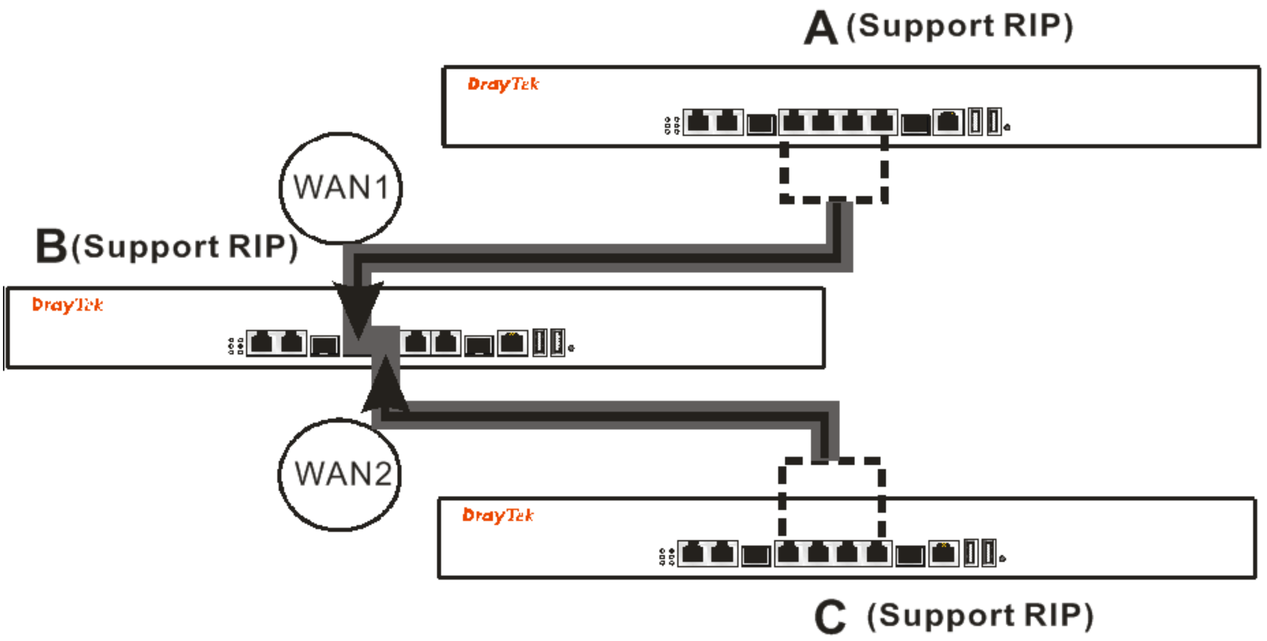
Profile Number Limit : 16

	Profile	Enable	WAN Profile	LAN Profile	IP	Mask
1	ARP_1	true	wan2	lan1	192.168.1.59	255.255.255.0/24

4.3.2 RIP Configuration

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

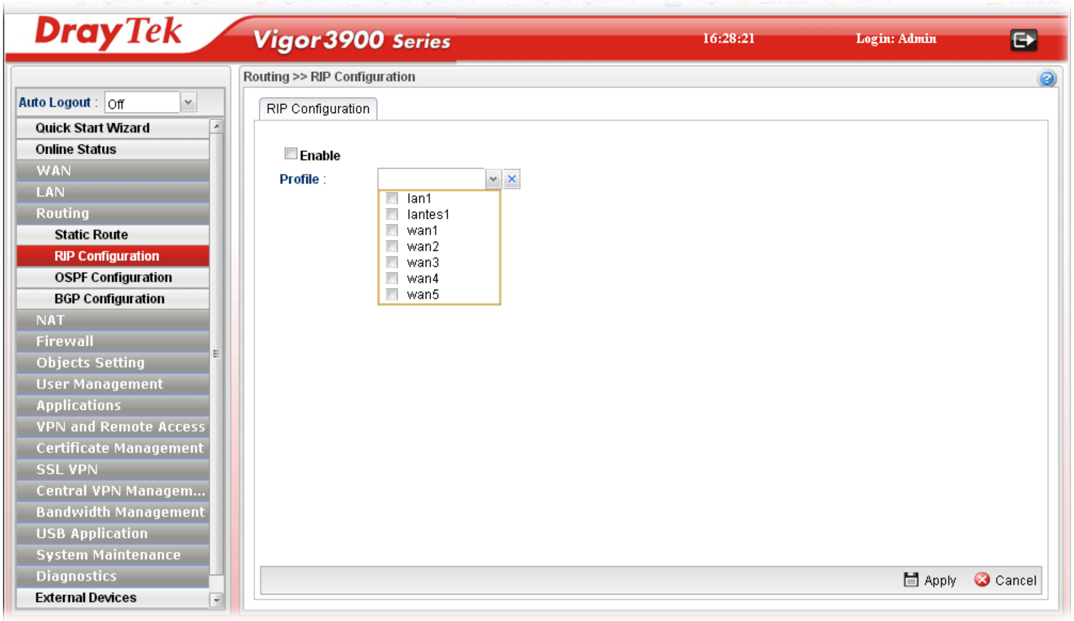
RIP can update the routing table automatically and find a route to send packet. See the following figure as an example:



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

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

In another direction, C will do the same thing.



Routing >> RIP Configuration

RIP Configuration

□ Enable

Profile :

- □ lan1
- □ lantes1
- □ wan1
- □ wan2
- □ wan3
- □ wan4
- □ wan5

Available parameters are listed as follows:

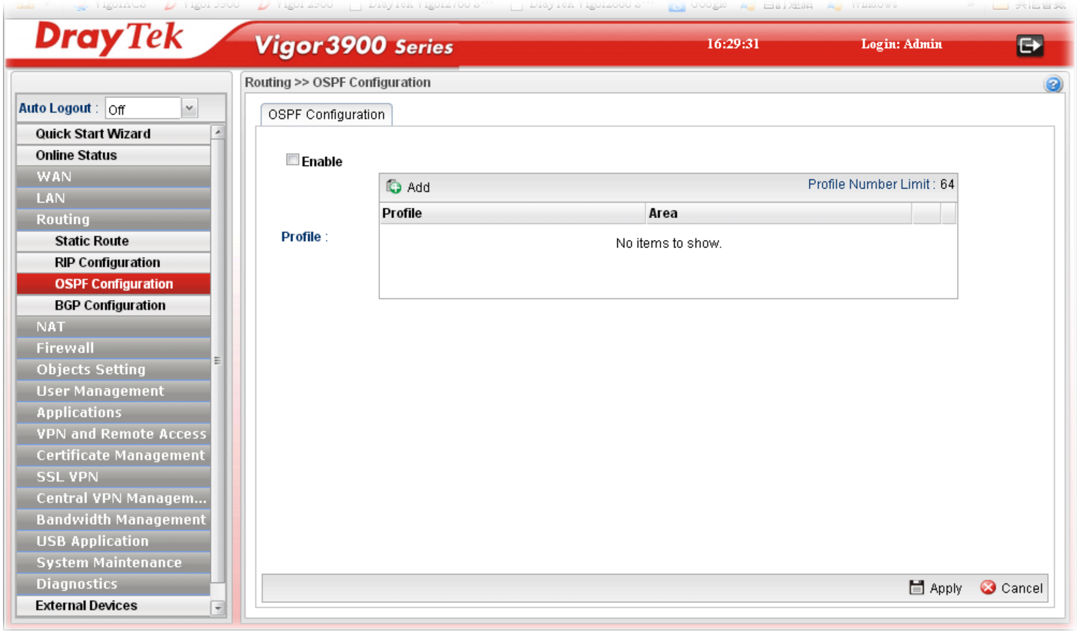
Item	Description
Enable	Check the box to enable the Mirror function for the switch.
Profile	Choose the LAN/WAN profile(s).
Apply	Click it to save the settings.
Cancel	Click it to exit the dialog without saving anything.

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

4.3.3 OSPF Configuration

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

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



Routing >> OSPF Configuration

OSPF Configuration

□ Enable

Profile :

Add   Profile Number Limit : 64

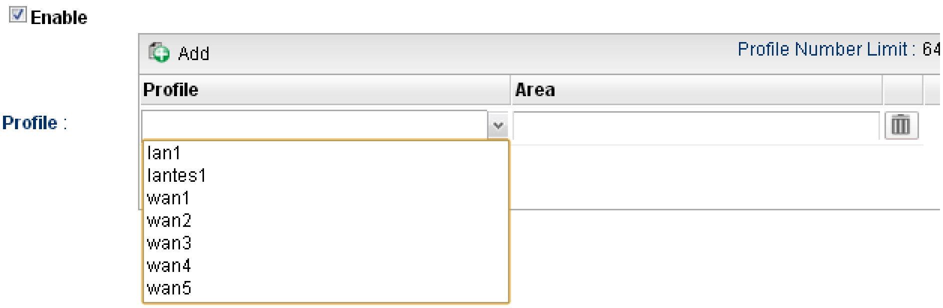
Profile	Area
No items to show.	

Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable the Mirror function for the switch.
Profile	Choose a LAN/WAN profile from the drop down list to apply for such configuration.
Apply	Click it to save the settings.
Cancel	Click it to discard the settings configured in this page.

How to add a new profile

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



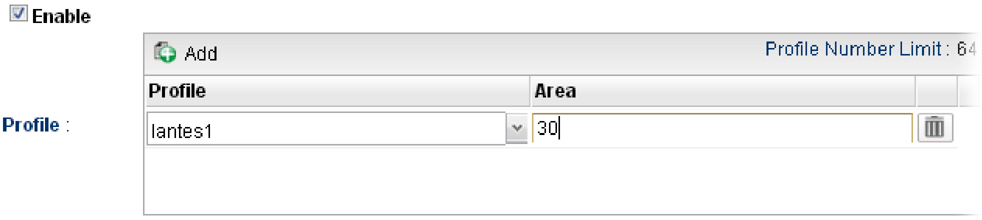
☑ Enable

Profile : Add — Profile Number Limit : 64

Profile	Area

lan1
lantes1
wan1
wan2
wan3
wan4
wan5

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



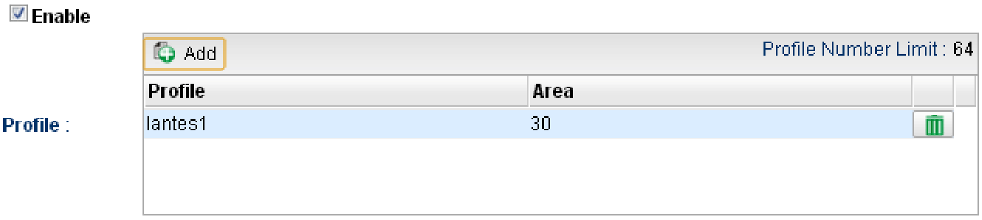
☑ Enable

Profile : Add — Profile Number Limit : 64

Profile	Area
lantes1	30

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

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



☑ Enable

Profile : Add — Profile Number Limit : 64

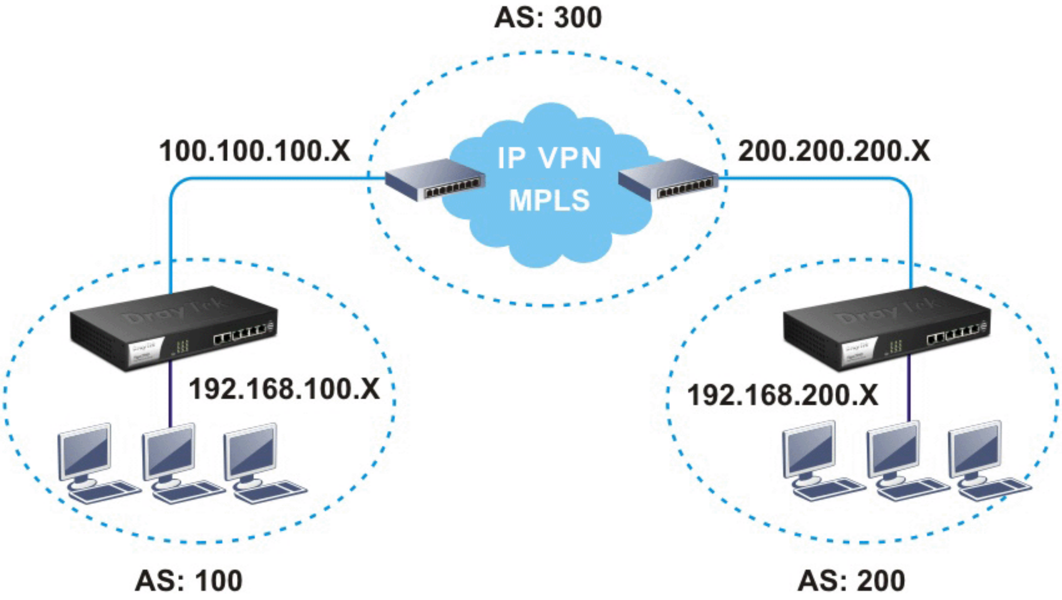
Profile	Area
lantes1	30

4.3.4 BGP Configuration

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

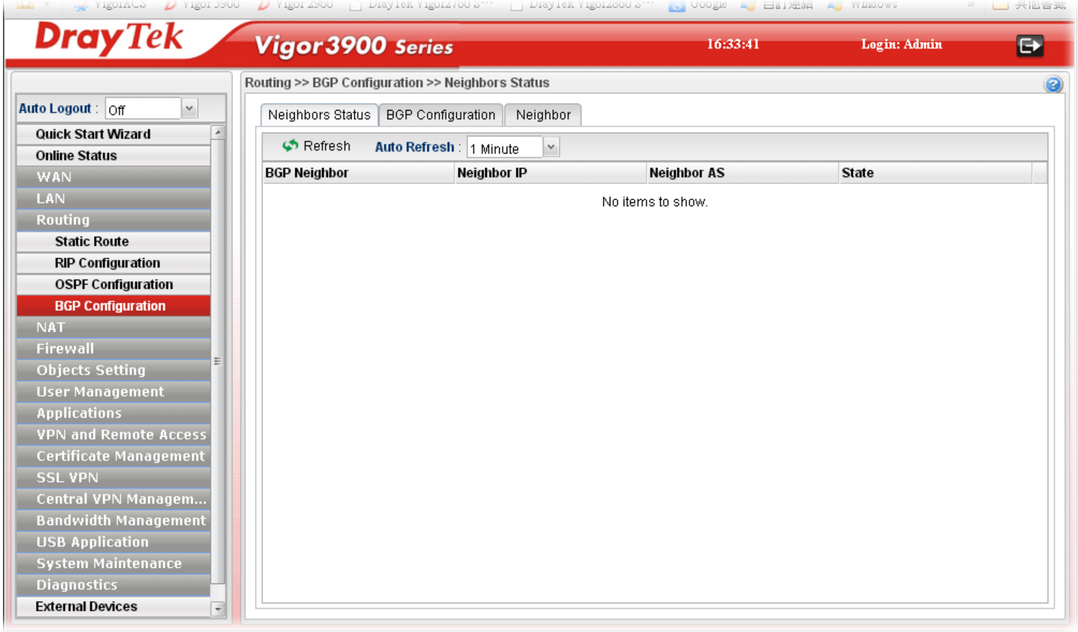
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the “neighbor” of other BGP routers. Define the IP address, AS number for the router is essential for TCP connection of BGP routing information exchange.

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



4.3.4.1 Neighbors Status

Such page displays current neighbors status in BGP routing environment.



Routing >> BGP Configuration >> Neighbors Status

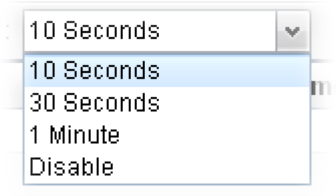
Auto Logout : Off

Auto Refresh : 1 Minute

BGP Neighbor	Neighbor IP	Neighbor AS	State

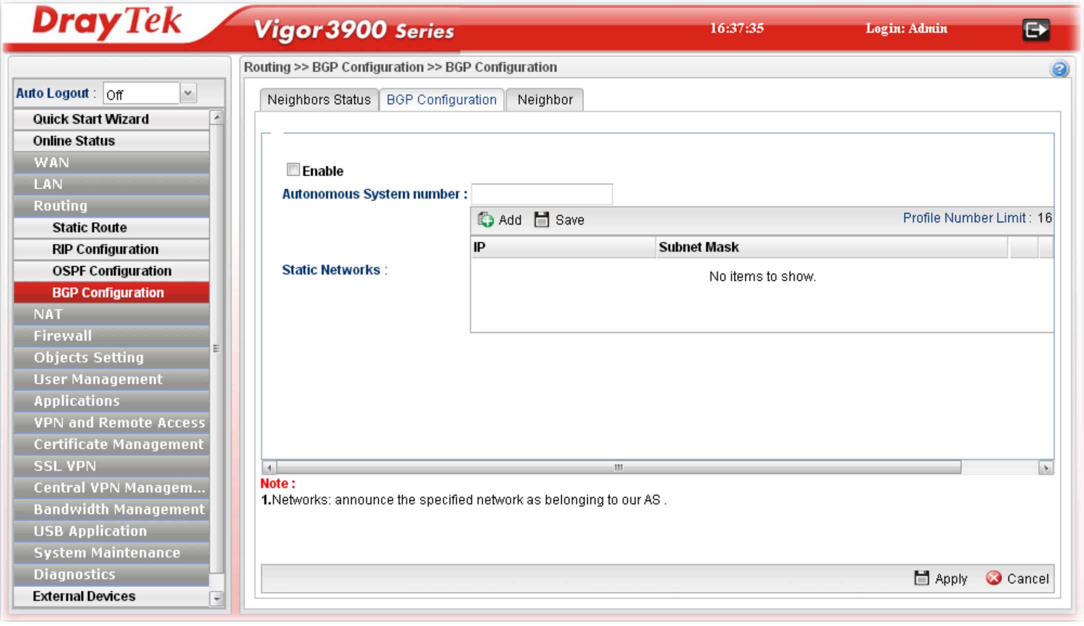
No items to show.

Available parameters are listed as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the **Refresh** button is clicked.  10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
BGP Neighbor	Display the neighbor profile name configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
Neighbor IP	Display the neighbor IP address configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
Neighbor AS	Display the autonomous system number of the neighbor configured successfully in the **Neighbor** tab in **Routing >>BGP configuration**.
State	Display the status of neighbor profile. If it is established successfully, "Established (time)" will be shown in this field.

4.3.4.2 BGP Configuration

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



Routing >> BGP Configuration >> BGP Configuration

□ Enable

Autonomous System number :

Static Networks :

Profile Number Limit : 16

IP	Subnet Mask

No items to show.

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

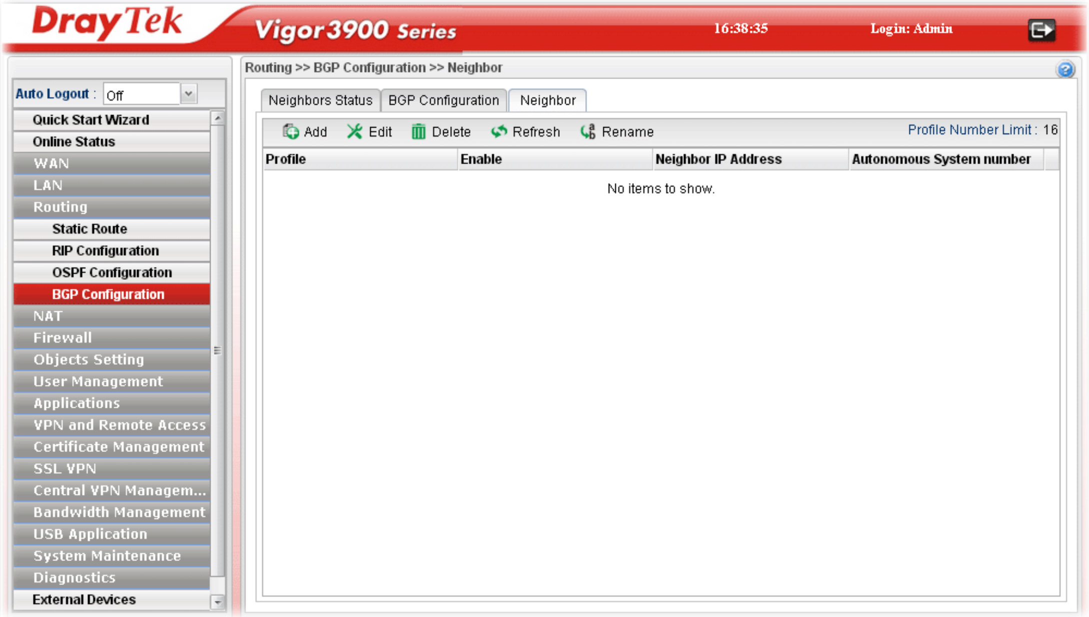
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable BGP function.
Autonomous System number	Type the autonomous system number for the host in BGP application.
Static Networks	Define the IP addresses (forming network range) which allow to be connected by other clients through static route. **Add** – Click it to add a specified IP address and subnet mask. **Save** – Click it to save the settings. **Profile Number Limit -** Display the total number of the profiles to be created. **IP** – Type the IP address. **Subnet Mask** – Display subnet mask for the IP address automatically.

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

4.3.4.3 Neighbor

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



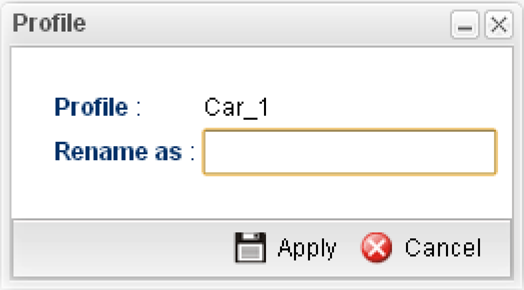
Routing >> BGP Configuration >> Neighbor

Profile Number Limit : 16

Profile	Enable	Neighbor IP Address	Autonomous System number

No items to show.

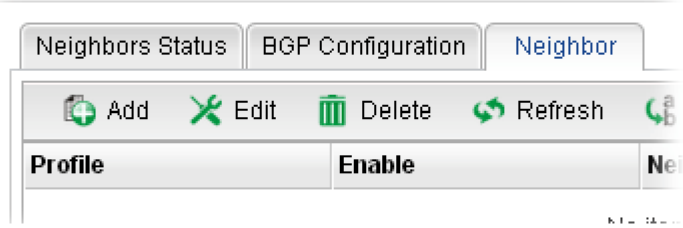
Available parameters are listed as follows:

Item	Description
Add	Add a new port redirect profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.  Profile : Car_1 Rename as : Before using such function, there is one profile existed at least.
Profile	Display the name of the profile.

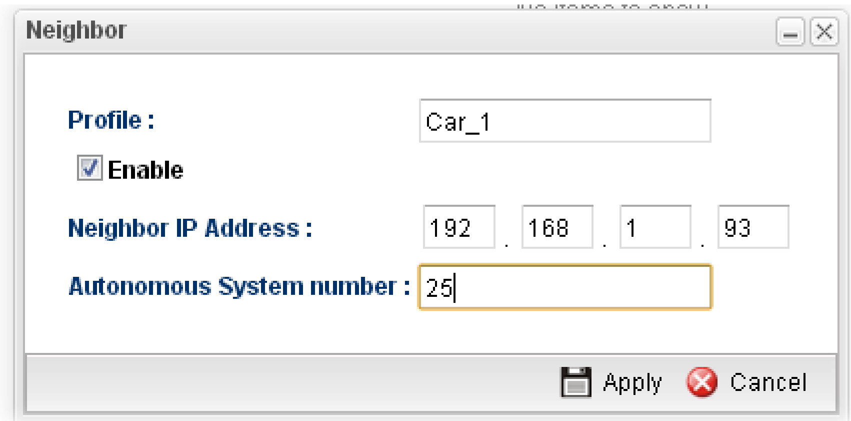
Enable	Display the status of the profile. False means disabled; True means enabled.
Neighbor IP Address	Display the IP address of the neighbor**.**
Autonomous System Number	Display the autonomous system number of the neighbor in BGP application.

How to add a new BGP profile

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



3. The following dialog will appear.



Profile : Car_1

☑ Enable

Neighbor IP Address : 192 . 168 . 1 . 93

Autonomous System number : 25

Available parameters are listed as follows:

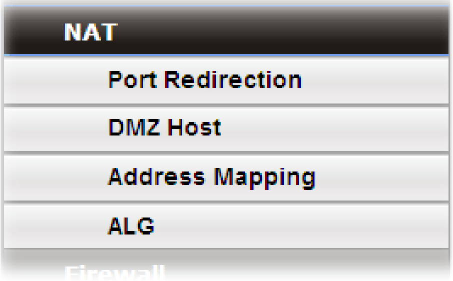
Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
Neighbor IP Address	Type the private IP used for this profile.
Autonomous System number	Type the autonomous system number for the neighbor in BGP application.
Apply	Click it to save and exit the dialog.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

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

4.4 NAT

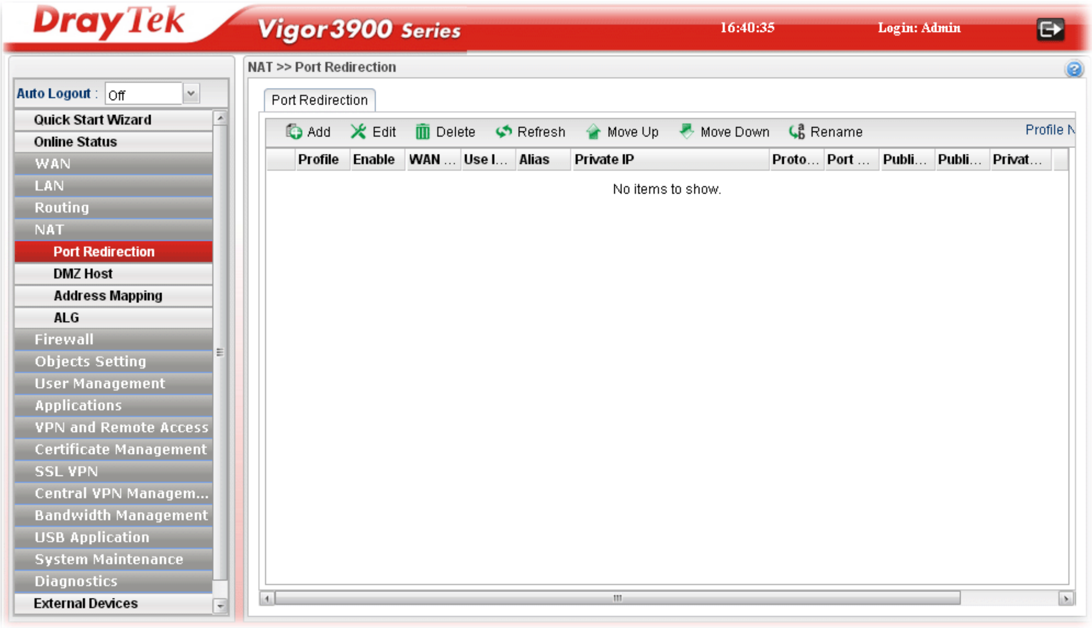
NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services. It allows the internal IP addresses of many computers on a LAN to be translated to one public address to save costs and resources of multiple public IP addresses.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

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



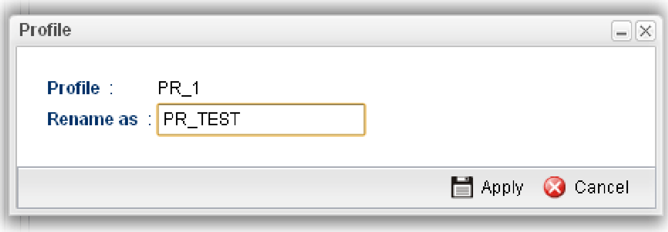
4.4.1 Port Redirection

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



No items to show.

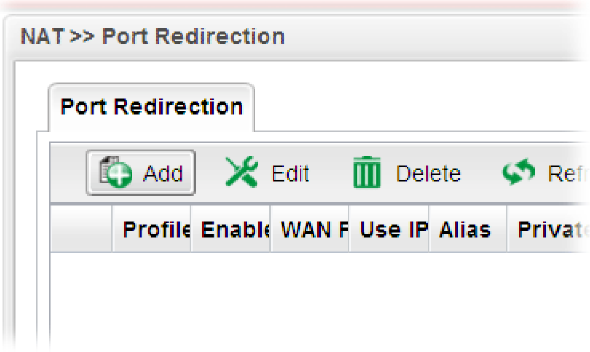
Each item will be explained as follows:

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.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.  Profile : PR_1 Rename as : PR_TEST
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display the WAN interface of this profile.
Use IP Alias	Display the type (no, Single_Alias, All) the IP Alias used.

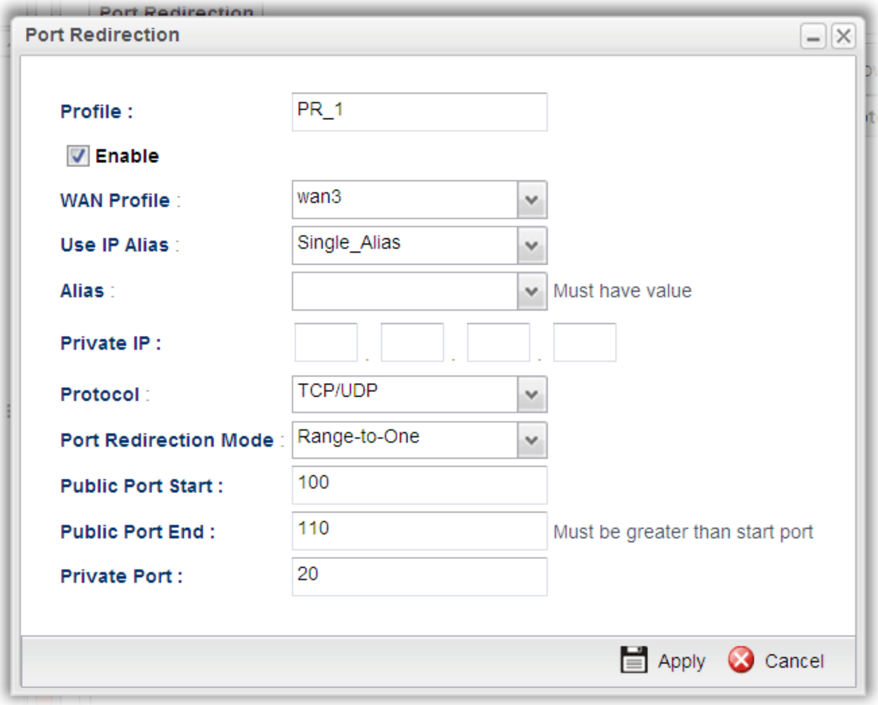
Alias	Display the selected WAN IP address.
Private IP	Display the private IP used for this entry.
Protocol	Display the protocol used for the entry.
Port Redirection Mode	Display the direction for the port to be redirected.
Public Port Start	Display the starting number of the public port.
Public Port End	Display the ending number of the public port.
Private Port	Display the number of the private port.

How to add a new Port Redirection profile

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



3. The following dialog will appear.



Port Redirection

Profile : PR_1

☑ Enable

WAN Profile : wan3

Use IP Alias : Single_Alias

Alias : Must have value

Private IP : . . .

Protocol : TCP/UDP

Port Redirection Mode : Range-to-One

Public Port Start : 100

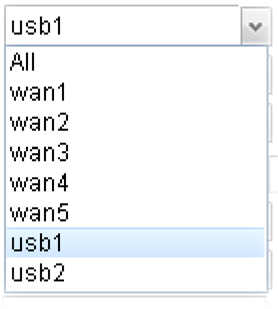
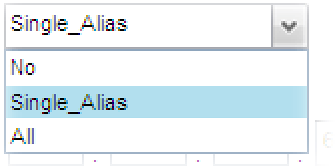
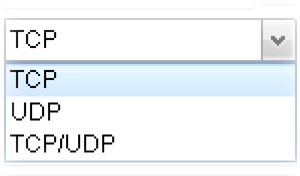
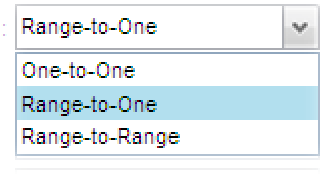
Public Port End : 110 Must be greater than start port

Private Port : 20

Apply Cancel

Available parameters are listed as follows:

Item	Description

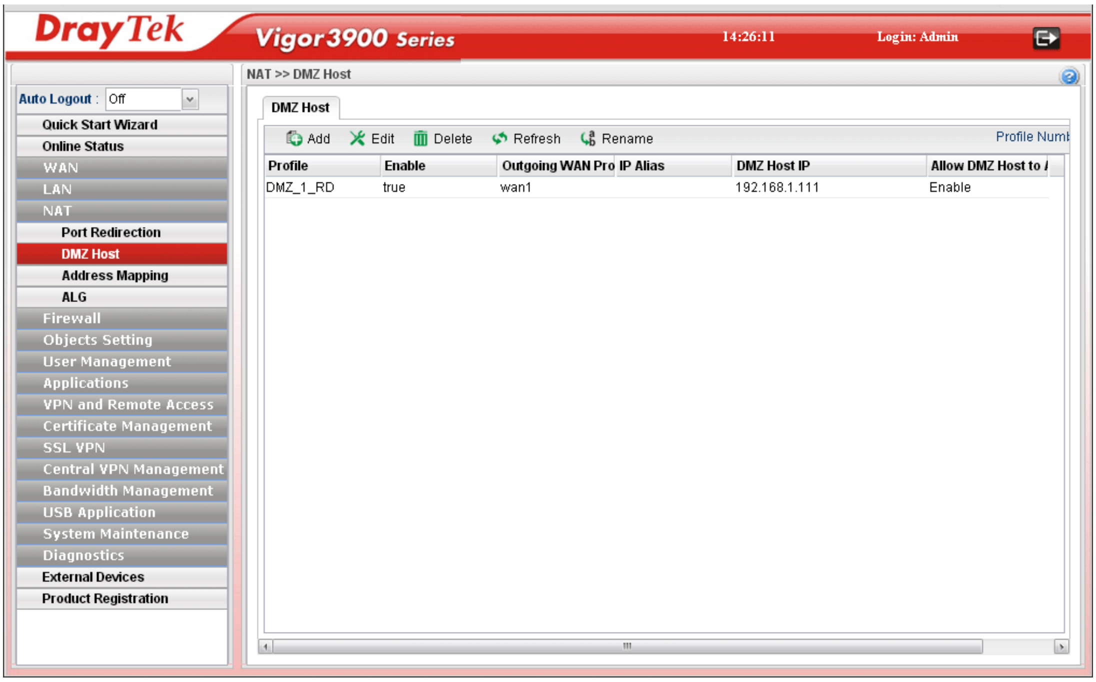
Profile	Type the name of the profile.
Enable	Check the box to enable this profile.
WAN Profile	Specify the WAN profile for such profile.  usb1 All wan1 wan2 wan3 wan4 wan5 usb1 usb2
Use IP Alias	When **All** is selected as **WAN Profile**, such feature is unavailable. Use the drop down list to select the type you want.  **Single_Alias** – You have to type one IP address used for IP Alias. **All** – All the IP address can be treated as IP Alias.
Alias	WAN IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
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.  Range-to-One One-to-One Range-to-One Range-to-Range
Public Port Start/ Public Port End	It is available when **Range-to-One** or **Range-to-Range** is selected as Port Redirection Mode. Type the starting/ending number of the public port.

	For Range-to-One, set both Start and End values with the same value.
Private 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.

4.4.2 DMZ Host

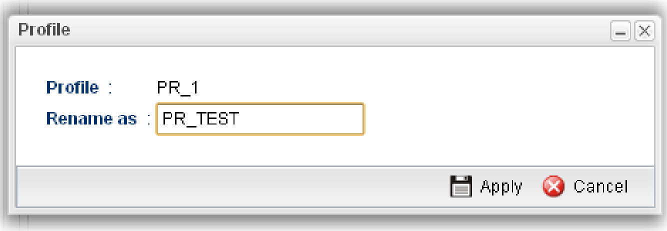
In computer networks, a DMZ (De-Militarized Zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to company network. A DMZ is an optional and more secure approach to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



Profile	Enable	Outgoing WAN Pro	IP Alias	DMZ Host IP	Allow DMZ Host to /
DMZ_1_RD	true	wan1		192.168.1.111	Enable

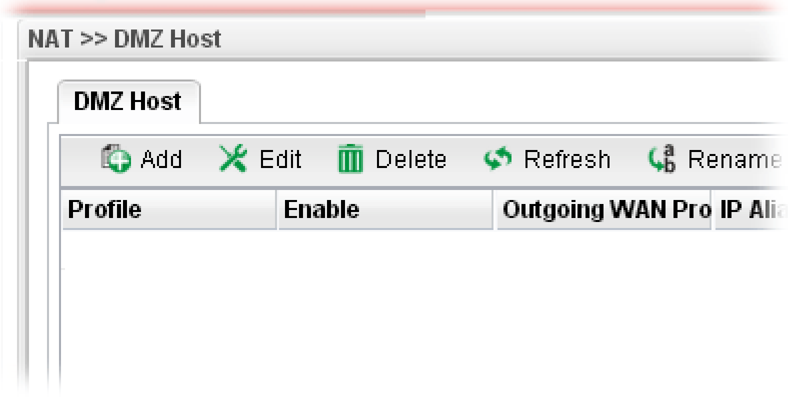
Each item will be explained as follows:

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.

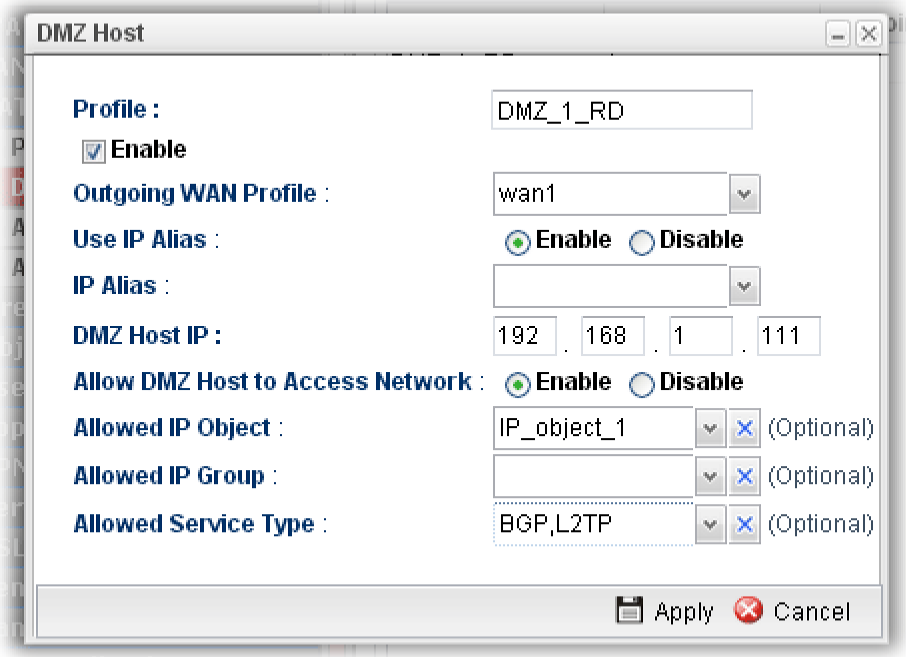
	 Profile Profile : PR_1 Rename as : PR_TEST Apply Cancel
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Outgoing WAN Profile	Display the WAN profile that such DMZ host profile will be applied to.
IP Alias	Display the selected WAN IP address if Use IP Alias is enabled.
DMZ Host IP	Display the IP address of the DMZ host.
Allow DMZ Host to Access Network	Display if such function is enabled or disabled.

How to add a new DMZ Host profile

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



3. The following dialog will appear.



DMZ Host

Profile : DMZ_1_RD

☑ Enable

Outgoing WAN Profile : wan1

Use IP Alias : ● Enable ○ Disable

IP Alias :

DMZ Host IP : 192 . 168 . 1 . 111

Allow DMZ Host to Access Network : ● Enable ○ Disable

Allowed IP Object : IP_object_1 (Optional)

Allowed IP Group : (Optional)

Allowed Service Type : BGP,L2TP (Optional)

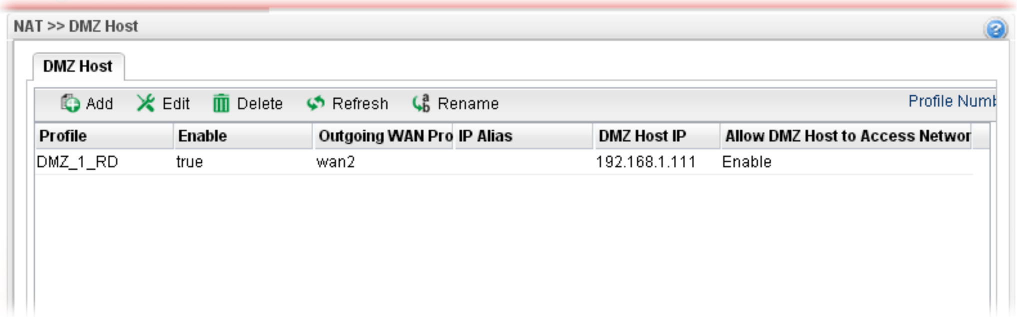
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable the DMZ Host profile.
Outgoing WAN Profile	Choose a WAN profile for such entry.
Use IP Alias	Click **Enable** to invoke IP Alias function.
IP Alias	IP alias that can be selected and used for port redirection. Before using it, please go to **WAN>>General Setup** and enable the **wan1** profile. Add several IP addresses under **Static** mode for wan1.
DMZ Host IP	Type the IP address of the DMZ host.
Allow DMZ Host to Access Network	Click Enable to make DMS host accessing network.
Allowed IP Object	This is an optional setting. Use the drop down list to choose the IP object profile(s) to apply to such profile.
Allowed IP Group	This is an optional setting. Use the drop down list to choose the IP group profile(s) to apply to such profile.
Allowed Service Type	This is an optional setting. Use the drop down list to choose the type(s) to apply to such profile.
Apply	Click it to save and exit the dialog.

Cancel	Click it to exit the dialog without saving anything.

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

5. A new profile has been added onto **DMZ Host** table.



NAT >> DMZ Host

DMZ Host

Add Edit Delete Refresh Rename Profile Numb

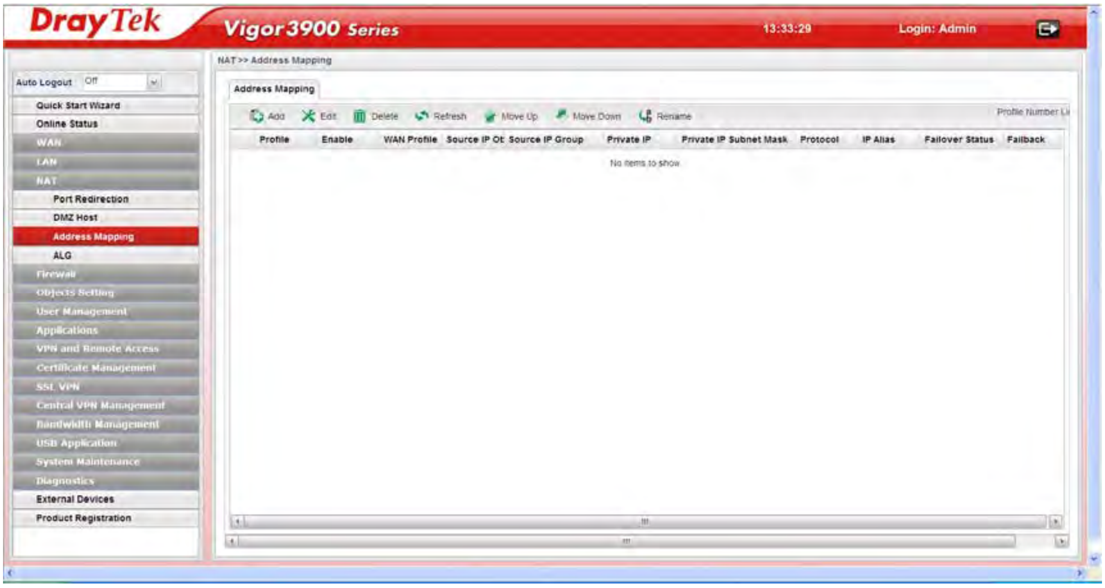
Profile	Enable	Outgoing WAN Pro	IP Alias	DMZ Host IP	Allow DMZ Host to Access Networ
DMZ_1_RD	true	wan2		192.168.1.111	Enable

4.4.3 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.



Profile	Enable	WAN Profile	Source IP Ot	Source IP Group	Private IP	Private IP Subnet Mask	Protocol	IP Alias	Failover Status	Fallback

No items to show

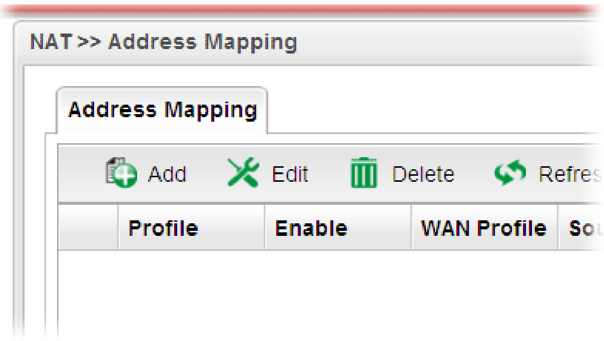
Each item will be explained as follows:

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

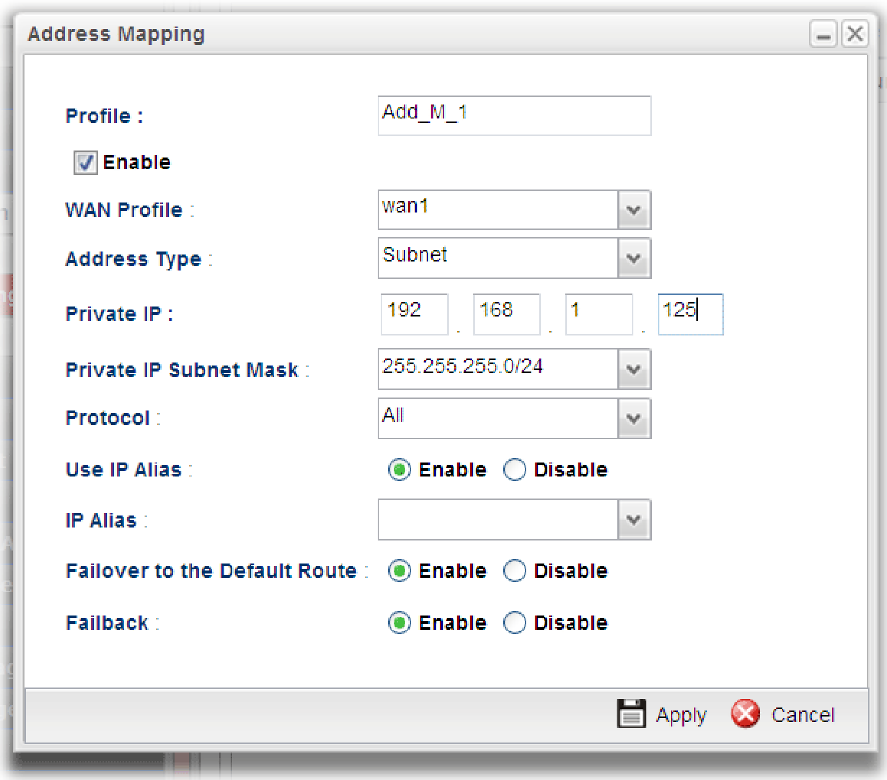
WAN Profile	Display the WAN profile that such address mapping profile will be applied to.
Source IP Object	Display the source IP object profile name.
Source IP Group	Display the source IP group profile name.
Private IP	Display the private IP used for this entry.
Private IP Subnet Mask	Display the subnet mask used for this entry.
Protocol	Display the protocol used for the entry.
IP Alias	Display the selected WAN IP address.
Failover Status	Display if failover to the default route is enabled or disabled.
Failback	Display if the function of Failback is enabled or disabled.

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.



Address Mapping

Profile : Add_M_1

☑ Enable

WAN Profile : wan1

Address Type : Subnet

Private IP : 192 . 168 . 1 . 125

Private IP Subnet Mask : 255.255.255.0/24

Protocol : All

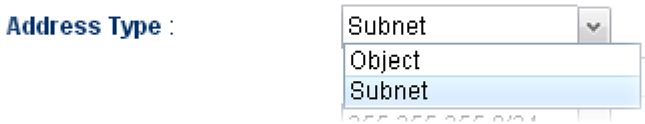
Use IP Alias : ● Enable ○ Disable

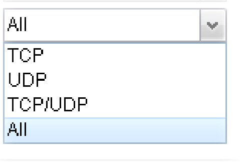
IP Alias :

Failover to the Default Route : ● Enable ○ Disable

Failback : ● Enable ○ Disable

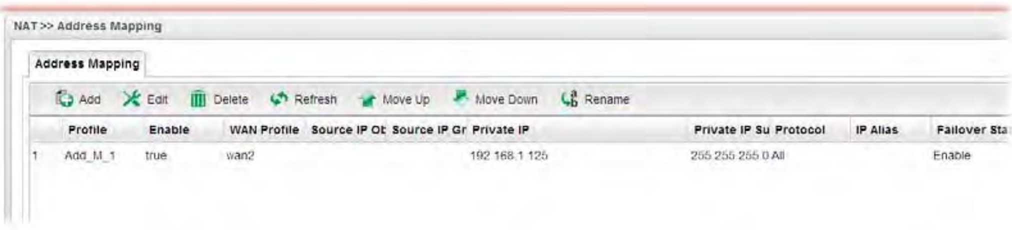
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check the box to enable the Address Mapping profile.
WAN Profile	Choose the active WAN interface for such entry.
Address Type	Choose **Subnet** or **Object** as the address type. Related setting options will be displayed later.  Address Type : Subnet Object Subnet
Private IP	It is available when Subnet is selected as Address Type. Type the private IP used for this entry.
Private IP subnet Mask	It is available when Subnet is selected as Address Type. Type the subnet mask used for this entry.
Source IP Object	It is available when **Object** is selected as Address Type. Use the drop down list to specify one IP object for such profile. If there is nothing to be specified, simply open **Object Settings** to create the one you want.
Source IP Group	It is available when Object is selected as Address Type. Use the drop down list to specify one IP group for such profile. If there is nothing to be specified, simply open **Object Settings** to create the one you want.
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.
Failover to the Default Route	**Enable -** When the specified WAN profile is down, the data traffic will be transmitted by suing default route. **Disable -** When the specified WAN profile is down, the data traffic will be blocked.
Failback	**Enable** – The connection session made by default route will be redirected with the specified route configured in Address Mapping. **Disable -** The connection session made by default route will be kept. Only the new session will be processed by the route configured in Address Mapping.
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.

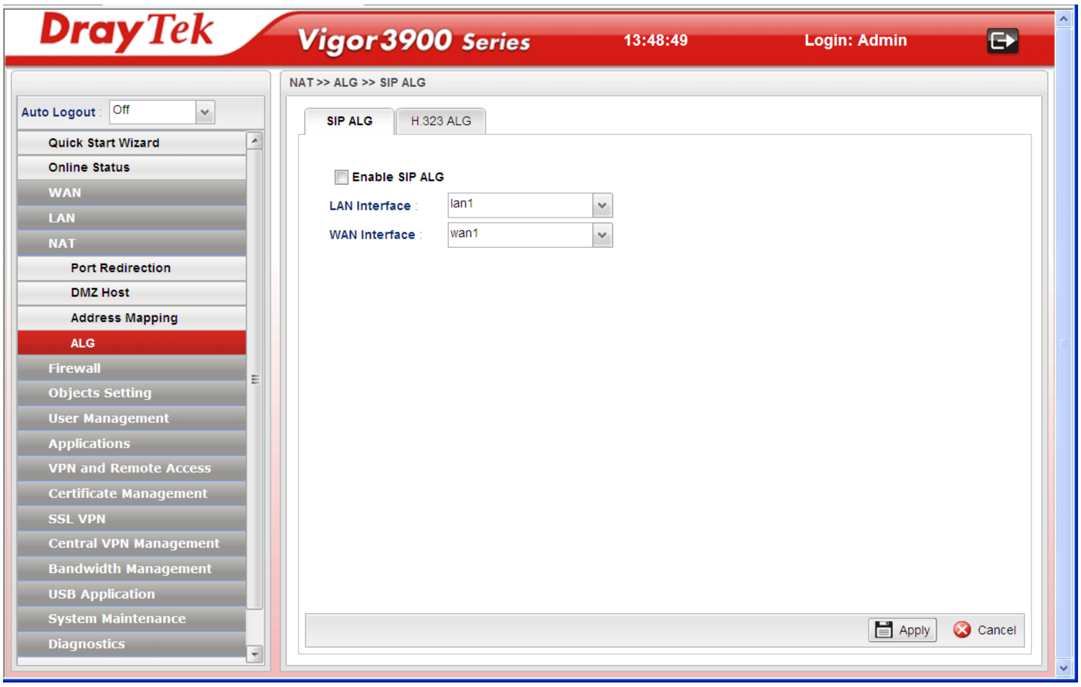


	Profile	Enable	WAN Profile	Source IP Ob	Source IP Gr	Private IP	Private IP Su	Protocol	IP Alias	Failover Sta
1	Add_M_1	true	wan2			192.168.1.125	255.255.255.0	All		Enable

4.4.4 ALG

4.4.4.1 SIP ALG

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



NAT >> ALG >> SIP ALG

□ Enable SIP ALG

LAN Interface : lan1

WAN Interface : wan1

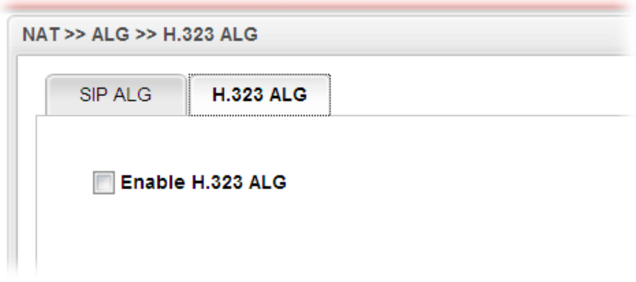
Available parameters are listed as follows:

Item	Description
Enable SIP ALG	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.

4.4.4.2 H.323 ALG

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



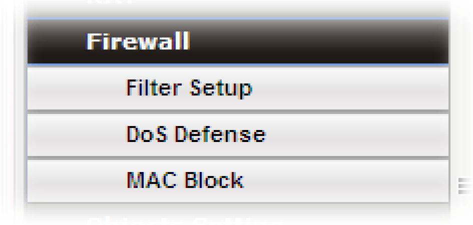
NAT >> ALG >> H.323 ALG

□ Enable H.323 ALG

4.5 Firewall

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

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

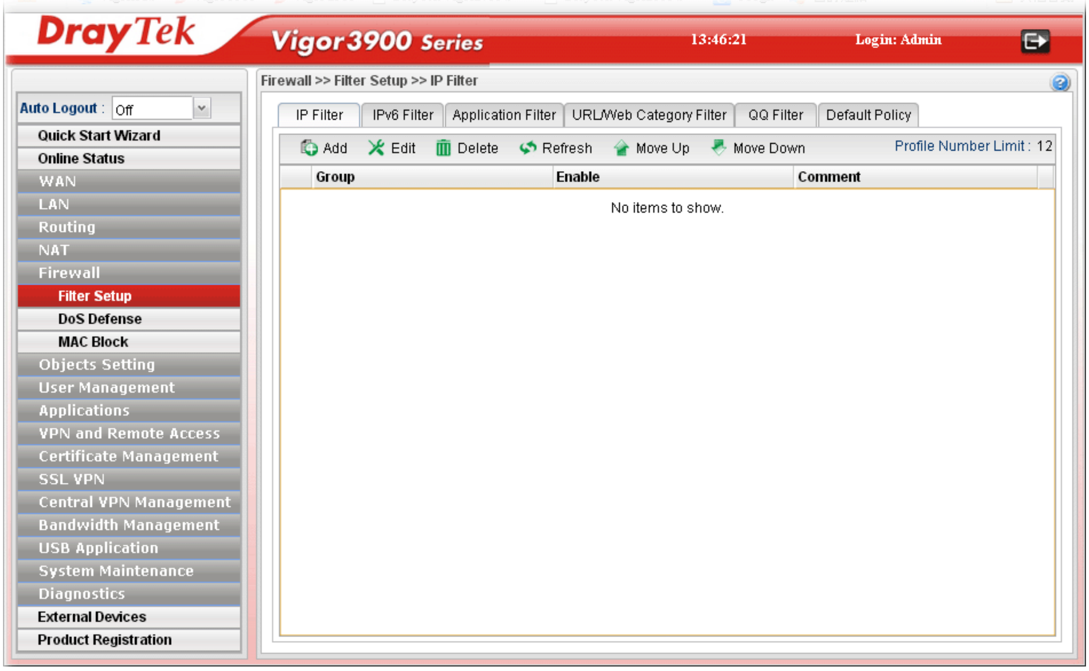


4.5.1 Filter Setup

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

4.5.1.1 IP Filter

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



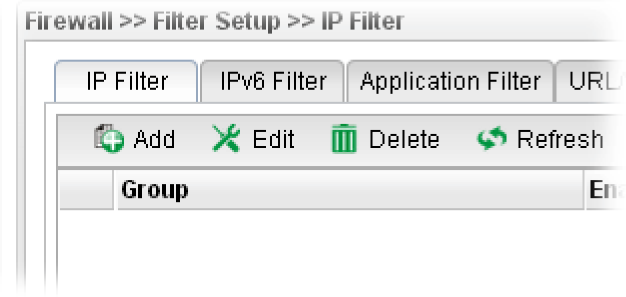
Each item will be explained as follows:

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

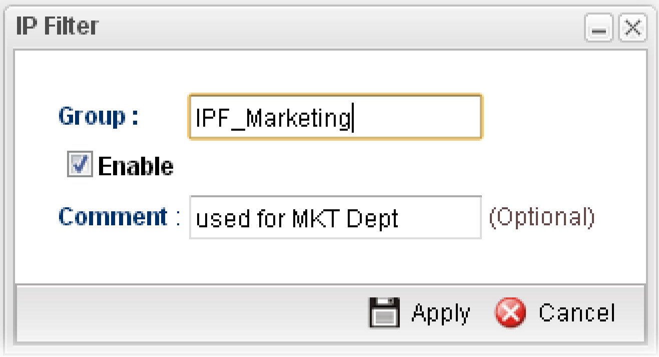
How to create an IP Filter group

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

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



3. The following dialog will appear.



Group : IPF_Marketing

☑ Enable

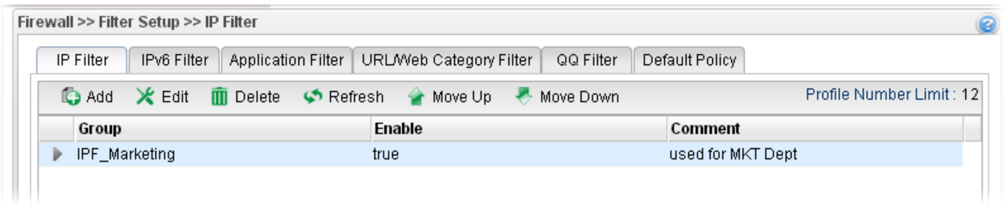
Comment : used for MKT Dept (Optional)

Available parameters are listed as follows:

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

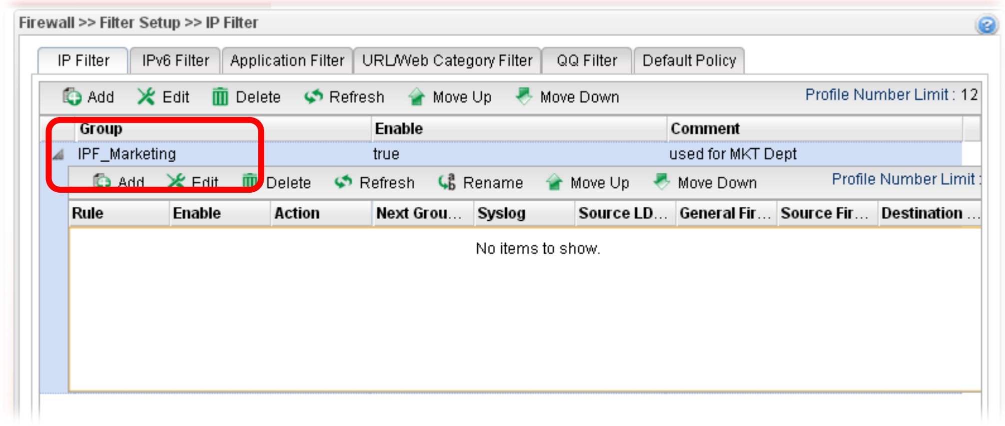
4. Enter all the settings and click **Apply**.

5. A new filter group has been added.



Group	Enable	Comment
IPF_Marketing	true	used for MKT Dept

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

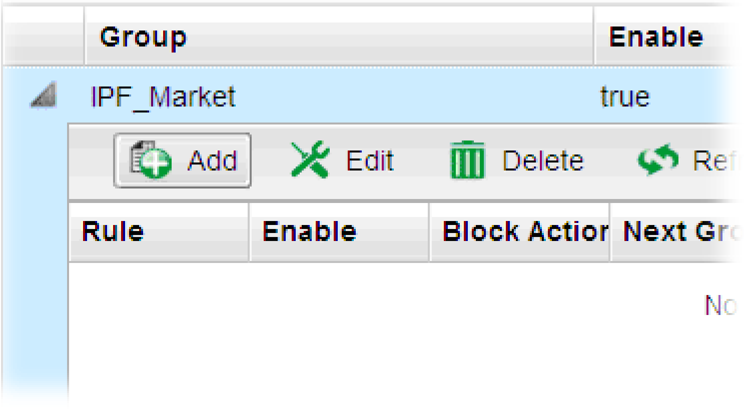


Group	Enable	Comment
IPF_Marketing	true	used for MKT Dept

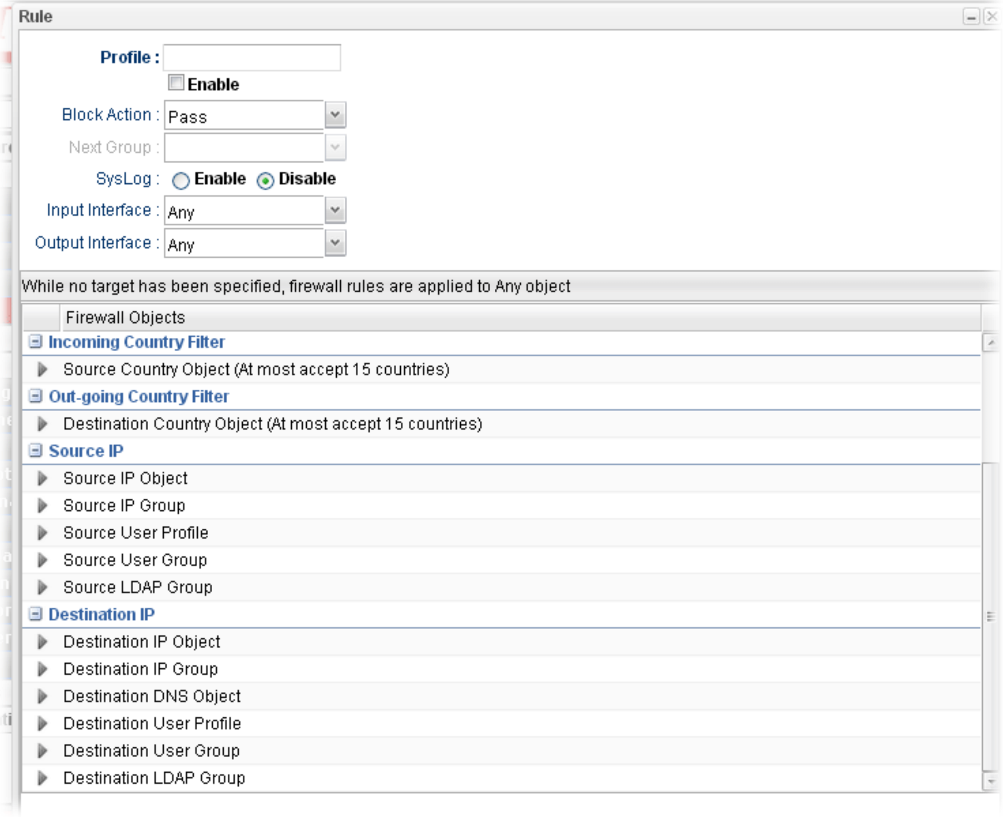
Rule	Enable	Action	Next Grou...	Syslog	Source LD...	General Fir...	Source Fir...	Destination ...

No items to show.

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



8. The following page for configuration will appear.



Rule

Profile :

□ Enable

Block Action : Pass

Next Group :

SysLog : ○ Enable ● Disable

Input Interface : Any

Output Interface : Any

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

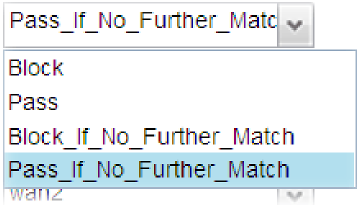
⊟ Incoming Country Filter
- Source Country Object (At most accept 15 countries)

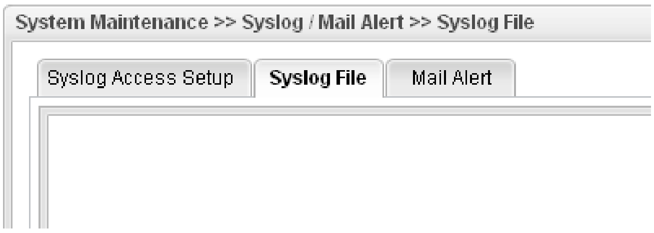
⊟ Out-going Country Filter
- Destination Country Object (At most accept 15 countries)

⊟ Source IP
- Source IP Object
- Source IP Group
- Source User Profile
- Source User Group
- Source LDAP Group

⊟ Destination IP
- Destination IP Object
- Destination IP Group
- Destination DNS Object
- Destination User Profile
- Destination User Group
- Destination LDAP Group

Available parameters are listed as follows:

Item	**Description**
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Block Action	The action to be taken when packets match the rule. **Block -** Packets matching the rule will be dropped immediately **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.  Pass_If_No_Further_Matc Block Pass Block_If_No_Further_Match Pass_If_No_Further_Match wan2
Next Group	When you choose **Block_If_No_Further_Match** or **Pass_If_No_Further_Match** as **Block Action**, you have to specify next IP filter group for further matching.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance** >> **Syslog/Mail**

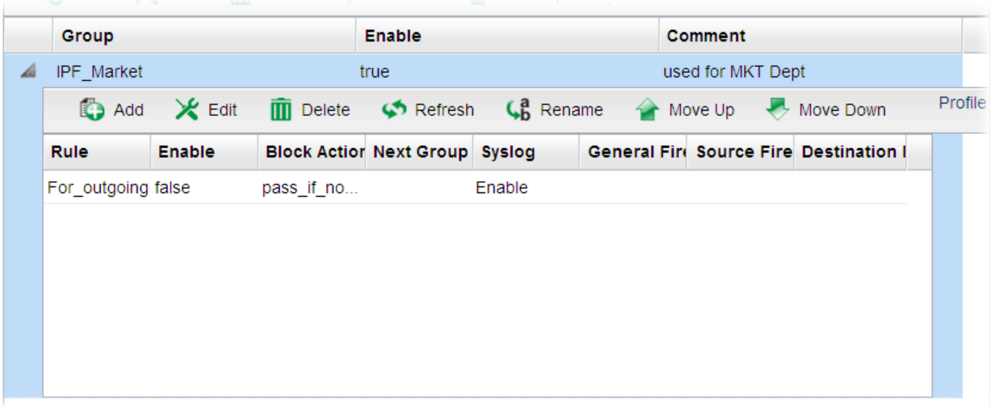
	Alert >> **Syslog File**.  System Maintenance >> Syslog / Mail Alert >> Syslog File Syslog Access Setup Syslog File Mail Alert
Input Interface	Choose one of the LAN or WAN profiles as data receiving interface.
Output Interface	Choose one of the LAN or WAN profiles as data transmitting interface.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
Service Protocol	**Service Type Object** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type object profiles from the drop down list. The selected profile will be treated as service type. You can click ⊕ to create another new service type object profile. **Service Type Group** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type group profiles from the drop down list. The selected profile will be treated as service type. You can click ⊕ to create another new service type group profile.
Incoming Country Filter	**Source Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an incoming country filter. You can click ⊕ to create another new filter profile.
Outgoing Country Filter	**Destination Country Object (At most accept 15 countries) -** Click the triangle icon ▶ to display the profile selection box. Choose one or more country object profiles from the drop down list. The selected profile will be treated as an outgoing country filter. You can click ⊕ to create another new filter profile.
Destination IP	**Destination IP Object-** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected profile will be treated as destination target. You can click ⊕ to create another new IP object profile. **Destination IP Group -** Click the triangle icon ▶ to

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

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

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

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



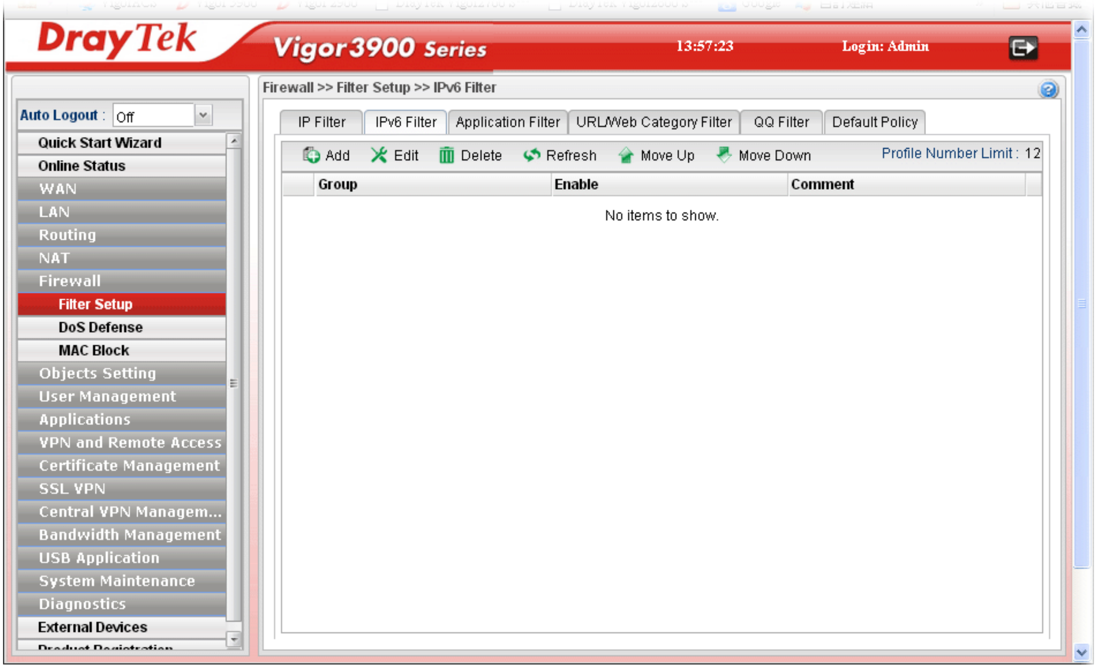
Group	Enable	Comment
IPF_Market	true	used for MKT Dept

Rule	Enable	Block Actior	Next Group	Syslog	General Fir	Source Fire	Destination I
For_outgoing	false	pass_if_no...		Enable			

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

4.5.1.2 IPv6 Filter

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



Each item will be explained as follows:

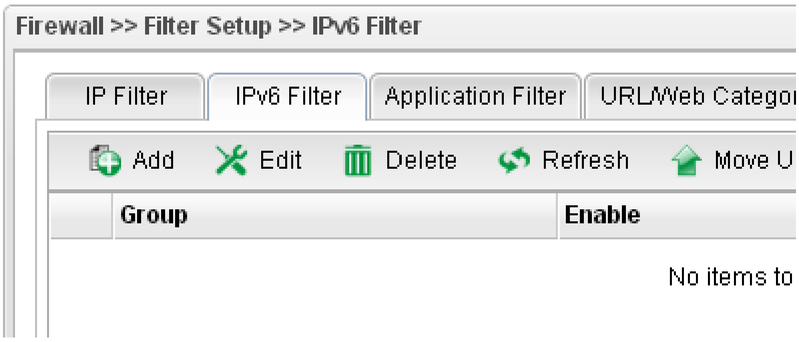
Item	Description
Add	Add a new group profile for IPv6 filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify

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

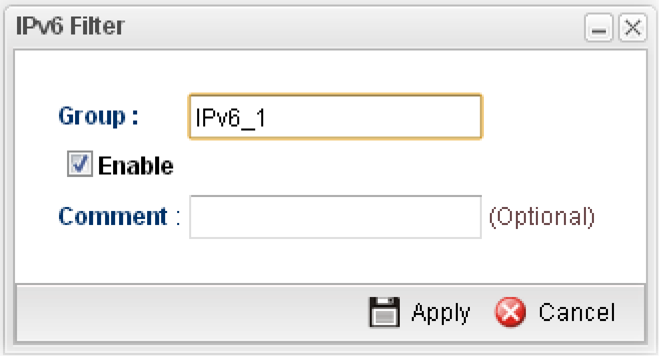
How to create an IPv6 Filter group

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

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



3. The following dialog will appear.



Group : IPv6_1

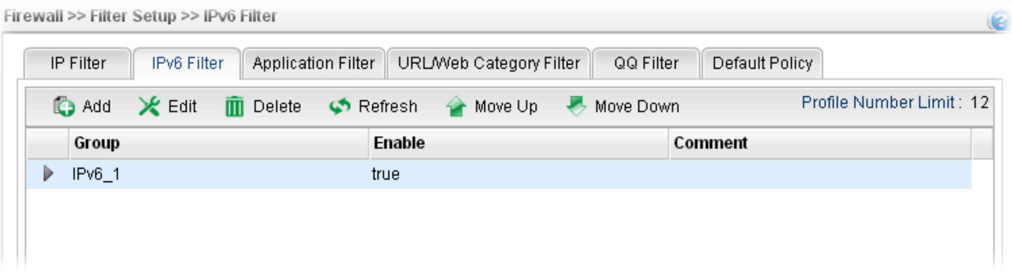
☑ Enable

Comment : (Optional)

Available parameters are listed as follows:

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

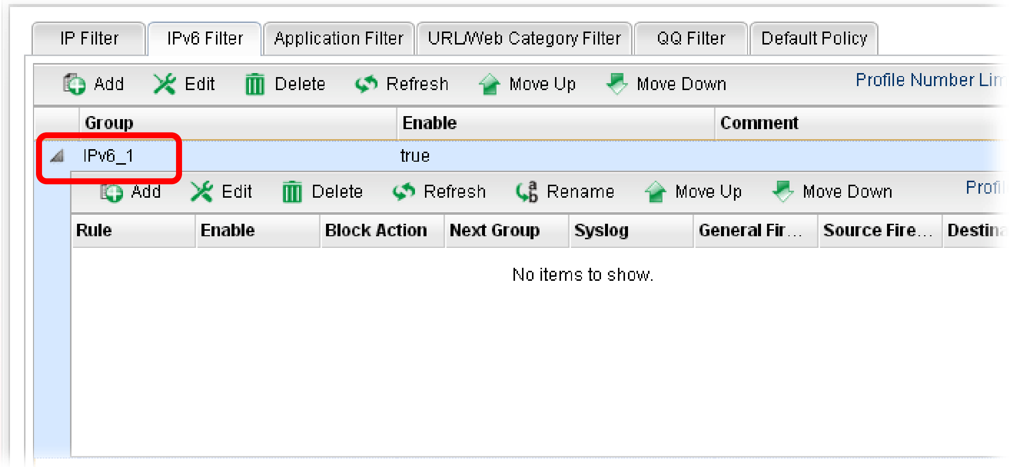
4. Enter all of the settings and click **Apply**.
5. A new filter group has been added.



Profile Number Limit : 12

Group	Enable	Comment
IPv6_1	true	

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



IP Filter | IPv6 Filter | Application Filter | URL/Web Category Filter | QQ Filter | Default Policy

Add | Edit | Delete | Refresh | Move Up | Move Down | Profile Number Lir

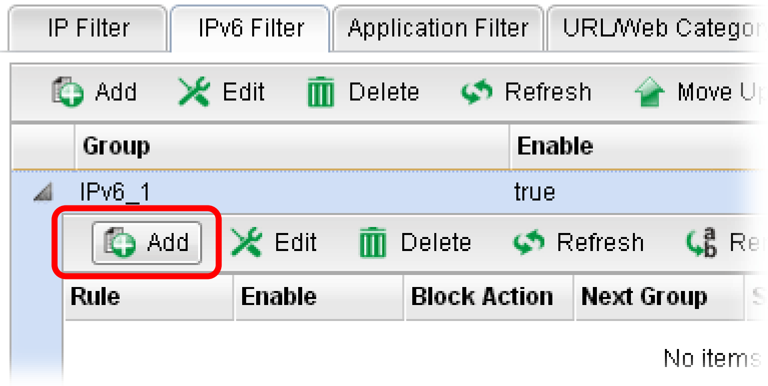
Group	Enable	Comment
IPv6_1	true	

Add | Edit | Delete | Refresh | Rename | Move Up | Move Down | Profi

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

No items to show.

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



IP Filter | IPv6 Filter | Application Filter | URL/Web Categor

Add | Edit | Delete | Refresh | Move U

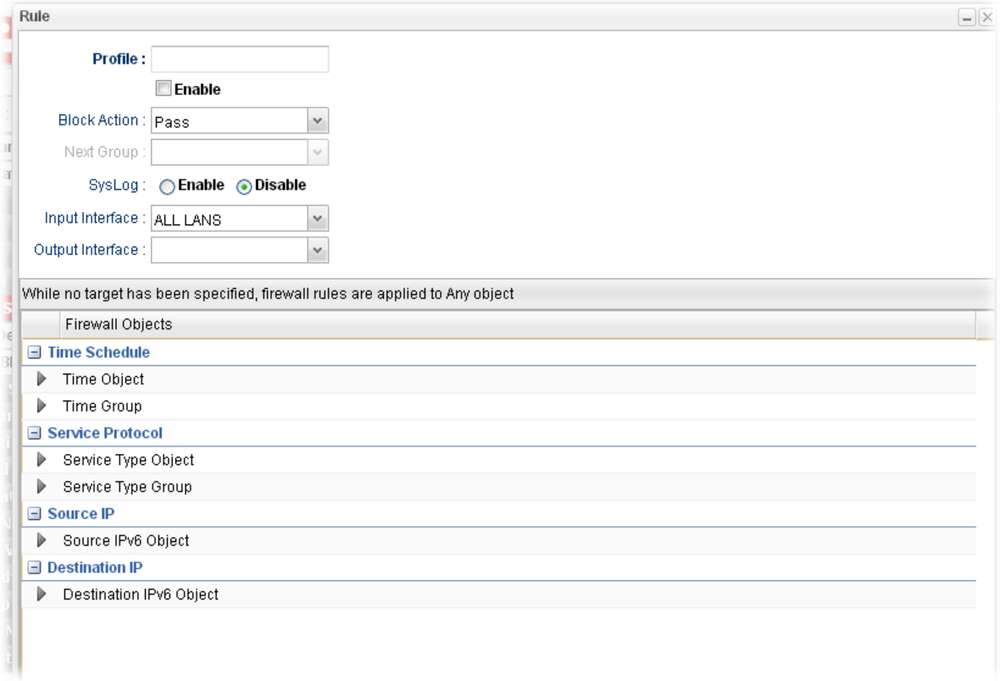
Group	Enable
IPv6_1	true

Add | Edit | Delete | Refresh | Re

Rule	Enable	Block Action	Next Group

No items

8. The following page for configuration will appear.



Rule

Profile :

□ Enable

Block Action : Pass

Next Group :

SysLog : ○ Enable ● Disable

Input Interface : ALL LANS

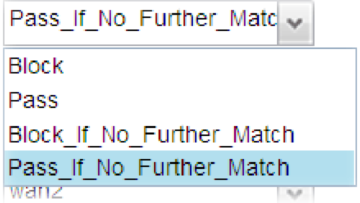
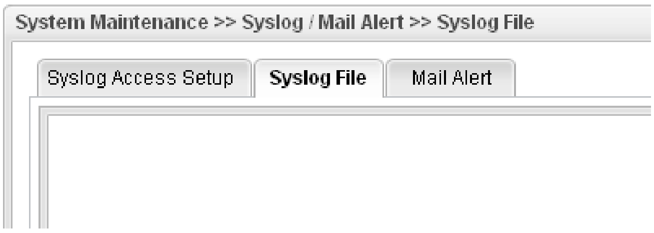
Output Interface :

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

- Time Schedule
  - Time Object
  - Time Group
- Service Protocol
  - Service Type Object
  - Service Type Group
- Source IP
  - Source IPv6 Object
- Destination IP
  - Destination IPv6 Object

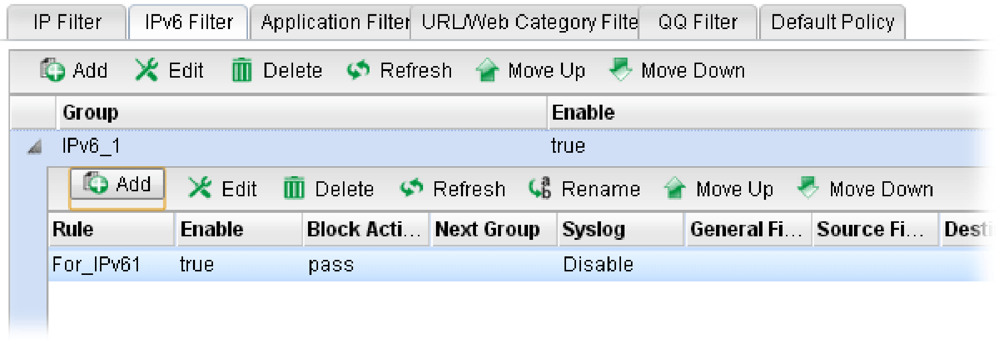
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the IP filter rule.
Enable	Check the box to enable this profile.
Block Action	The action to be taken when packets match the rule. **Block -** Packets matching the rule will be dropped immediately **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.  Pass_If_No_Further_Matc Block Pass Block_If_No_Further_Match Pass_If_No_Further_Match wan2
Next Group	When you choose **Block_If_No_Further_Match** or **Pass_If_No_Further_Match** as **Block Action**, you have to specify next IP filter group for further matching.
Syslog	Click **Enable** to make the history of firewall actions appearing on the **System Maintenance** >> **Syslog/Mail Alert** >> **Syslog File**.  System Maintenance >> Syslog / Mail Alert >> Syslog File Syslog Access Setup Syslog File Mail Alert
Input Interface	Choose one of the LAN or WAN profiles as data receiving interface.
Output Interface	Choose one of the LAN or WAN profiles as data transmitting interface.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
Service Protocol	**Service Type Object** –Click the triangle icon ▶ to display the profile selection box. Choose one or more service type object profiles from the drop down list. The selected profile

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

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

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



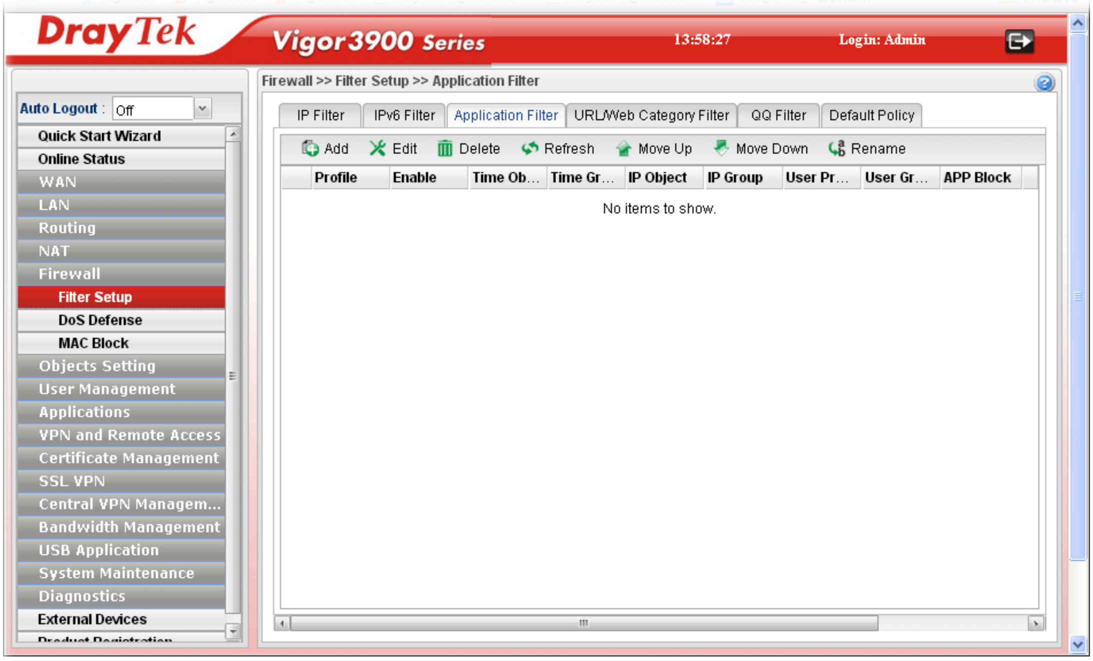
Group	Enable
IPv6_1	true

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

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

4.5.1.3 Application Filter

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



Firewall >> Filter Setup >> Application Filter

Profile	Enable	Time Ob...	Time Gr...	IP Object	IP Group	User Pr...	User Gr...	APP Block

No items to show.

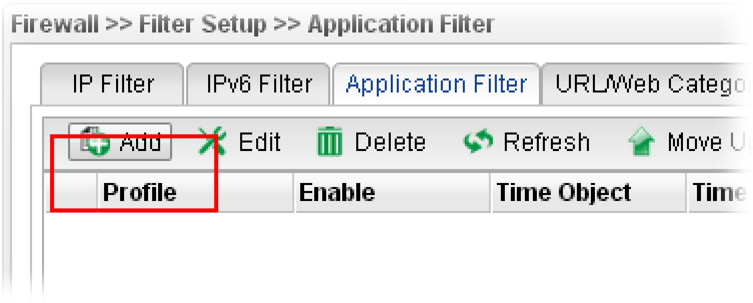
Each item will be explained as follows:

Item	Description
Add	Add a new group profile for Application filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application

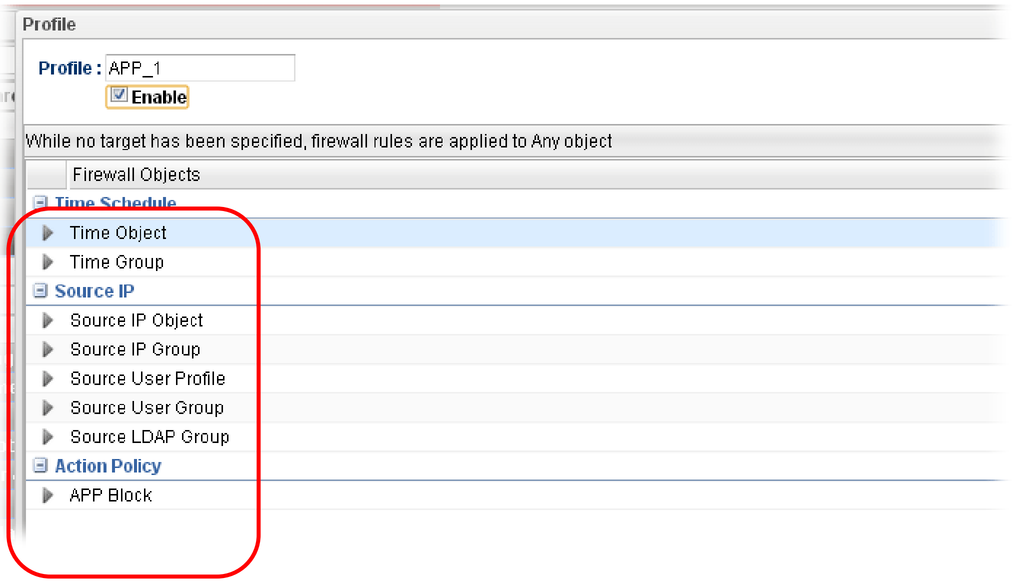
Item	Description
	profile.
IP Object	Display the IP object profile selected for such application profile.
IP Group	Display the IP group profile selected for such application profile.
User Profile	Display the user object profile selected for such application profile.
User Group	Display the user group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

How to create an Application Filter profile

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



3. The following dialog will appear. Click the triangle icon ▶ to display the profile selection box (red rectangle).



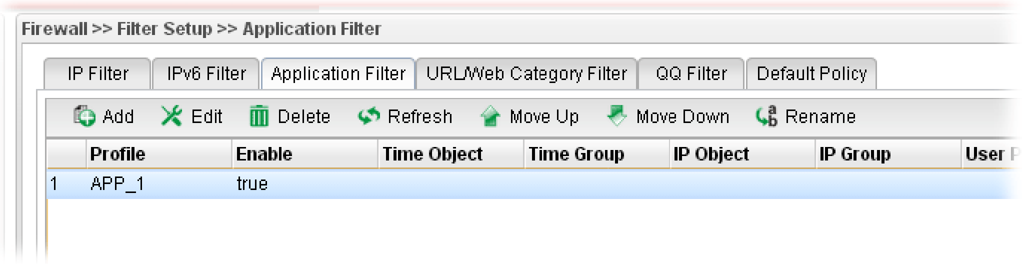
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the application filter profile.
Enable	Check the box to enable this profile.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click ⊕ to create another new time object profile, or you can click the edit icon ✎ to modify the existed object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile, or you can click the edit icon ✎ to modify the existed group profile. **IP Object -** Click the triangle icon ▶ to display the profile selection box. **C**hoose one or more IP object profiles from the drop down list. The selected IP will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new IP object profile. **IP Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new IP group profile, or you can click the edit icon ✎ to modify the existed group profile. **User Profile -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user profiles from the drop down list. The user specified in the selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new user profile, or you can click the edit icon ✎ to modify the existed user profile. **User Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user group profiles from the drop down list. The users within the selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new user group profile, or you can click the edit icon ✎ to modify the existed group profile.
Source IP	**Source IP Object -** Click the triangle icon ▶ to display the profile selection box. **C**hoose one or more IP object profiles from the drop down list. The selected IP will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new IP object profile. **Source IP Group -** Click the triangle icon ▶ to display the

	profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new IP group profile, or you can click the edit icon ✂ to modify the existed group profile. **Source User Profile -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user profiles from the drop down list. The user specified in the selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new user profile, or you can click the edit icon ✂ to modify the existed user profile. **Source User Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user group profiles from the drop down list. The users within the selected profile will be filtered by the router when such application filter profile is applied. You can click ⊕ to create another new user group profile, or you can click the edit icon ✂ to modify the existed group profile. **Source LDAP Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user LDAP profiles from the drop down list. The selected profile will be treated as source target. You can click ⊕ to create another new LDAP group profile.
Action Policy	**APP Block -** Click the triangle icon ▶ to display the profile selection box. Choose one or more APP object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click ⊕ to create another new APP object profile, or you can click the edit icon ✂ to modify the existed object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

5. A new Application filter profile has been added.

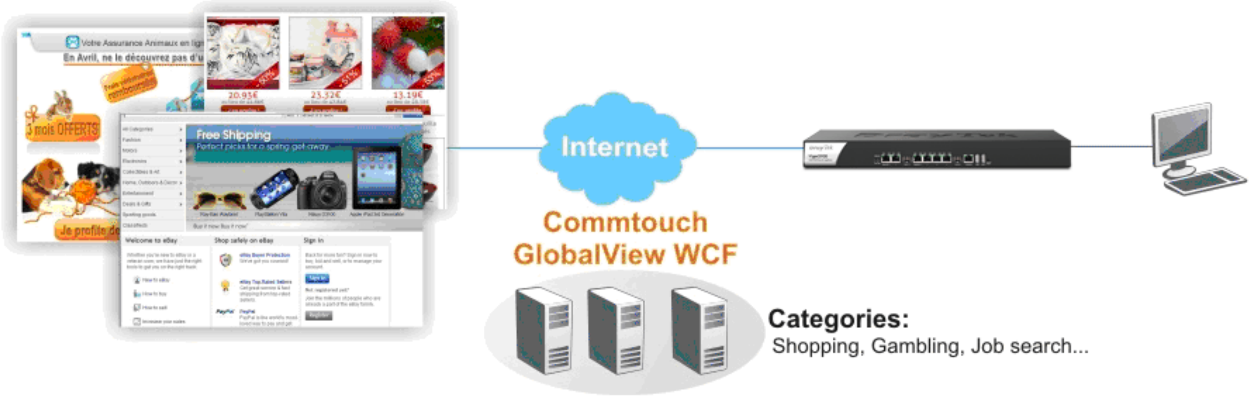


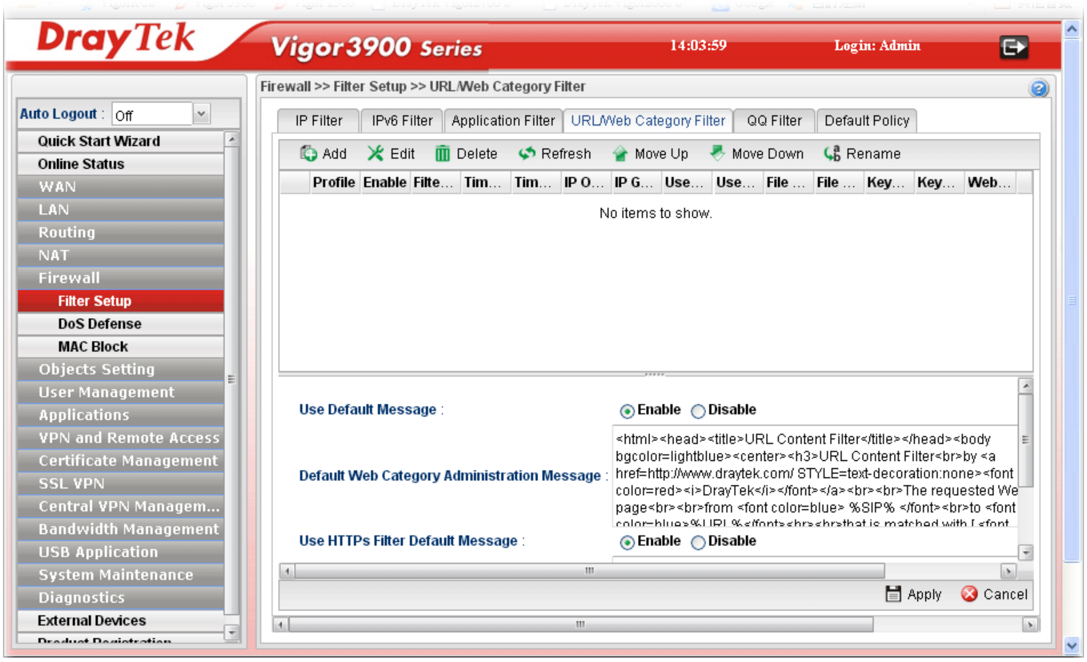
Firewall >> Filter Setup >> Application Filter

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

4.5.1.4 URL/Web Category Filter

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





No items to show.

Use Default Message : ● Enable ○ Disable

Default Web Category Administration Message : <html><head><title>URL Content Filter</title></head><body bgcolor=lightblue><center><h3>URL Content Filter
by <a href=http://www.draytek.com/ STYLE=text-decoration:none><font color=red><i>DrayTek</i></font></a>

The requested We page

from <font color=blue> %SIP% </font>
to <font color=blue>%URL %</font>

that is matched with [<font

Use HTTPs Filter Default Message : ● Enable ○ Disable

Each item will be explained as follows:

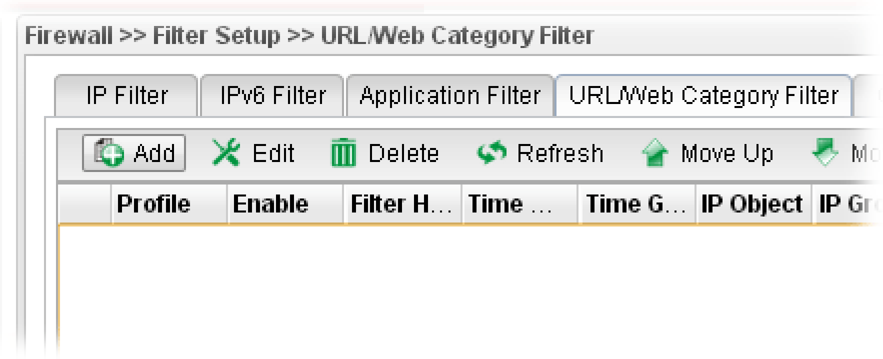
Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected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

Item	Description
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Profile Number Limit	Display the total number of the object profiles to be created.
Profile	Display the name of the application filter profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Filter Https	Display if the HTTPs filter is enabled or not.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application profile.
IP Object	Display the IP object profile selected for each rule.
IP Group	Display the IP group profile selected for each rule.
User Profile	Display the user object profile selected for each rule.
User Group	Display the user group profile selected for each rule.
File Extension Pass	Display the file extension object profile selected for each rule which is allowed to pass through the router.
File Extension Block	Display the file extension object profile selected for each rule which is not allowed to pass through the router.
Keyword Pass	Display the keyword object profile selected for each rule which is allowed to pass through the router.
Keyword Block	Display the keyword object profile selected for each rule which is not allowed to pass through the router.
Web Category Block	Display the web category object profile selected for each rule which is not allowed to pass through the router.
China Web Category	Display the China web category object profile selected for each rule which is not allowed to pass through the router.
Use Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page.. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Web Category Administration Message	Such field is available when you disable the function of **Use Default Message**. The message will display on the user's browser when he/she tries to access the blocked web page.
Use HTTPs Filter Default Message	**Enable** – Use the default message to display on the page that the user tries to access into the blocked web page through HTTPs. **Disable** – Type the message manually to display on the page that the user tries to access into the blocked web page through HTTPs.
Default HTTPS WebSite	The message will display on the user's browser when he/she

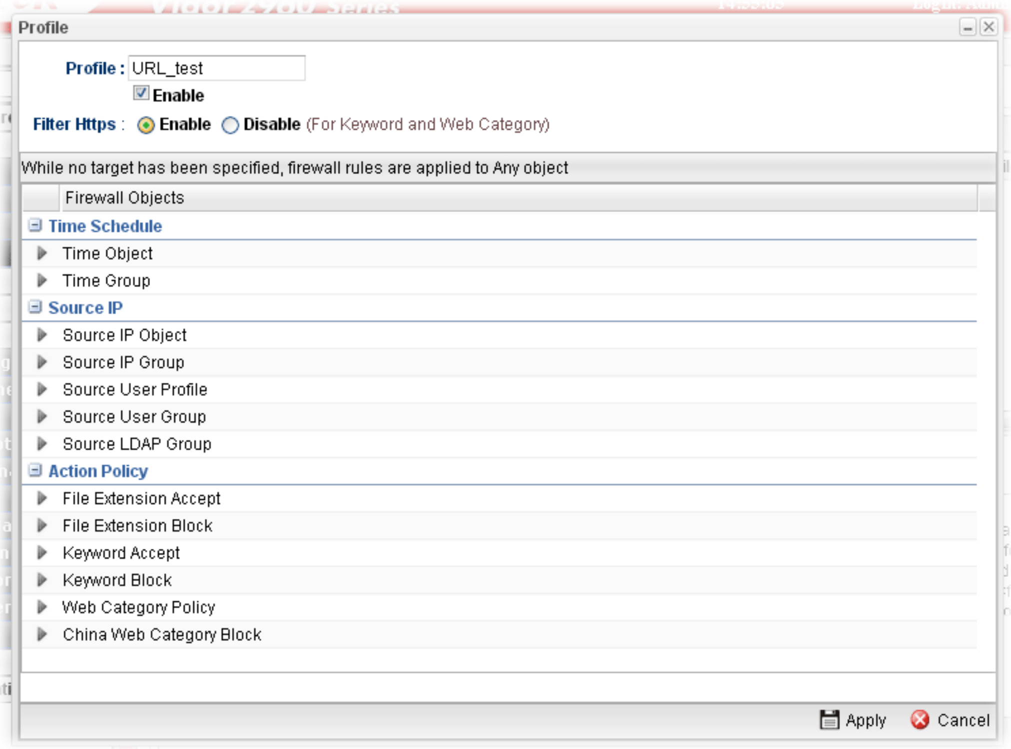
Item	Description
Filter Message	tries to access the blocked web page through HTTPs.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to create a URL Filter profile

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



3. The following dialog will appear.



Profile

Profile : URL_test

☑ Enable

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

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

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

Available parameters are listed as follows:

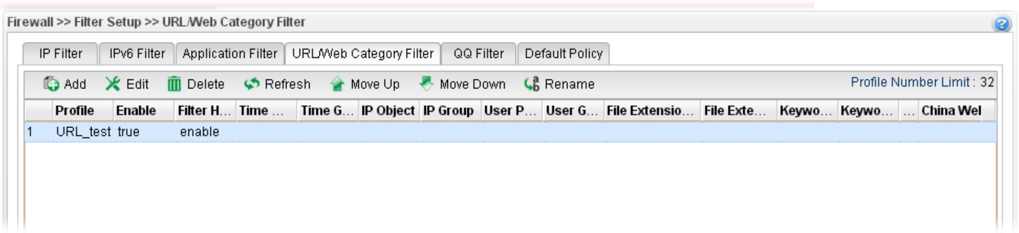
Item	Description
Profile	Type the name of the URL filter profile.
Enable	Check the box to enable this profile.
Filter https	**Enable** – Click it to enable the HTTPS filtering job.

Item	Description
	Disable – When only keyword and web category are selected for such rule, choose Disable.
Time Schedule	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the filtering job based on the time object selected. You can click ⊕ to create another new time object profile, or you can click the edit icon ✎ to modify the existed object profile. **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile, or you can click the edit icon ✎ to modify the existed group profile.
Source IP	**Source IP Object -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected IP will be filtered by the router when such URL filter profile is applied. You can click ⊕ to create another new IP object profile. **Source IP Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be filtered by the router when such URL filter profile is applied. You can click ⊕ to create another new IP group profile, or you can click the edit icon ✎ to modify the existed group profile. **Source User Profile -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user profiles from the drop down list. The user specified in the selected profile will be filtered by the router when such URL filter profile is applied. You can click ⊕ to create another new user profile, or you can click the edit icon ✎ to modify the existed user profile. **Source User Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user group profiles from the drop down list. The users within the selected profile will be filtered by the router when such URL filter profile is applied. You can click ⊕ to create another new user group profile, or you can click the edit icon ✎ to modify the existed group profile. **Source LDAP Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more user LDAP profiles from the drop down list. The selected profile will be treated as source target. You can click ⊕ to create another new LDAP group profile.
Action Policy	**File Extension Accept / File Extension Block -** Click the

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

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

5. A new URL filter profile has been added.



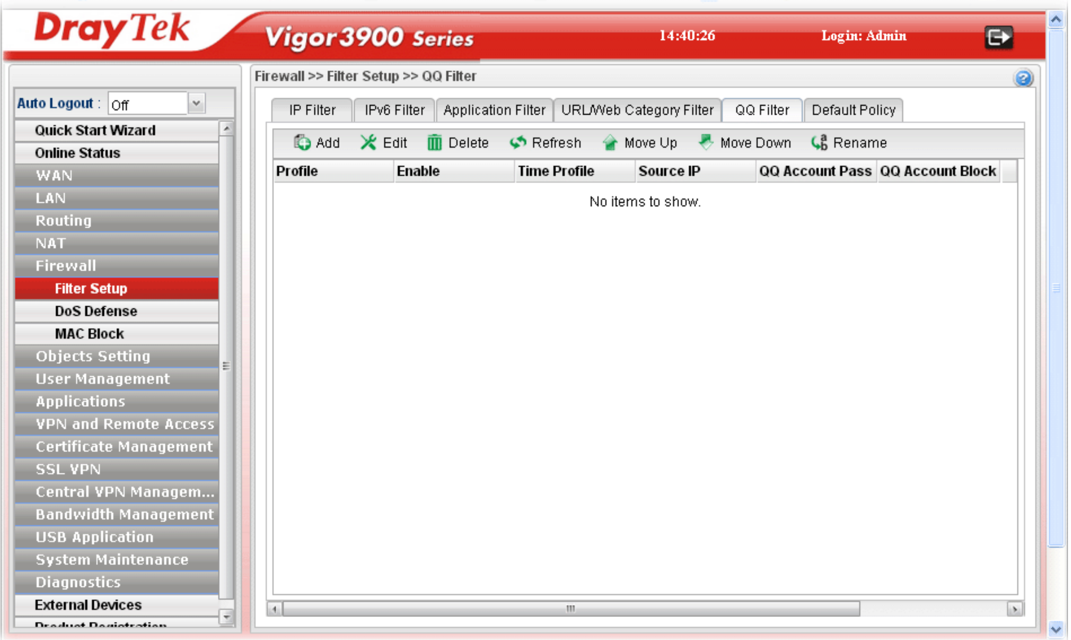
Firewall >> Filter Setup >> URL/Web Category Filter

Profile Number Limit : 32

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

4.5.1.5 QQ Filter

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



Profile	Enable	Time Profile	Source IP	QQ Account Pass	QQ Account Block

No items to show.

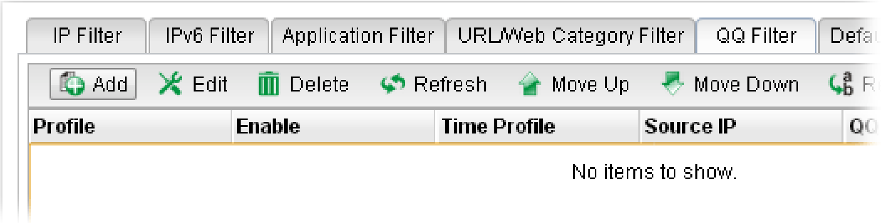
Each item will be explained as follows:

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

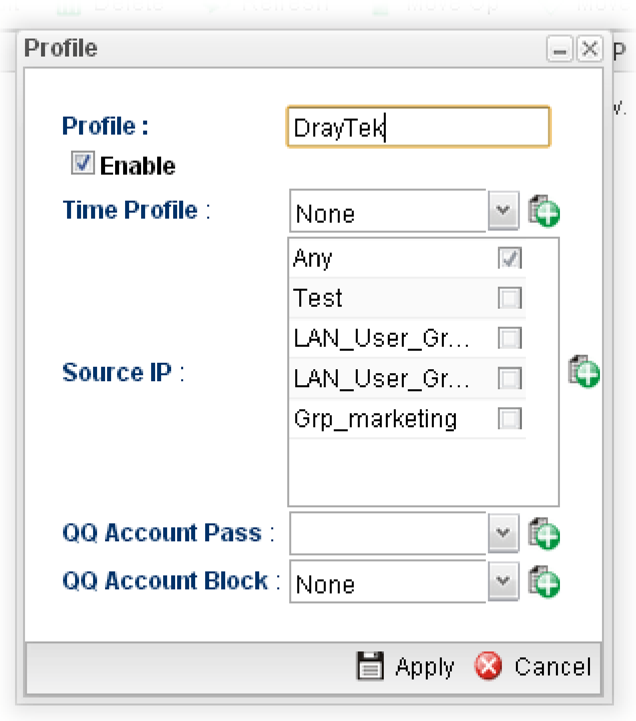
Item	Description
	selected QQ profile is enabled.
QQ Account Block	Display the account name which will be blocked if the selected QQ profile is enabled.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to create a QQ Filter profile

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



3. The following dialog will appear.



Profile : DrayTek

☑ Enable

Time Profile : None

Source IP :
Any ☑
Test □
LAN_User_Gr... □
LAN_User_Gr... □
Grp_marketing □

QQ Account Pass :

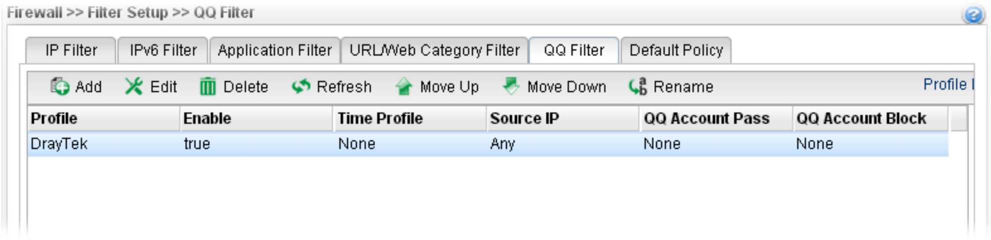
QQ Account Block : None

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the QQ filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Use the drop down list to specify a time profile for such profile.

Item	Description
	You can click to create another new time object profile.
Source IP	Specify user profiles for such profile. Users within the source IP will be filtered by Vigor router when such profile is applied.
QQ Account Pass	Use the drop down list to specify a QQ account profile for such profile. The select account will not be blocked by Vigor router. You can click to create another new QQ account.
QQ Account Block	Use the drop down list to specify a QQ account profile for such profile. The select account will be blocked by Vigor router. You can click to create another new QQ account.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

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

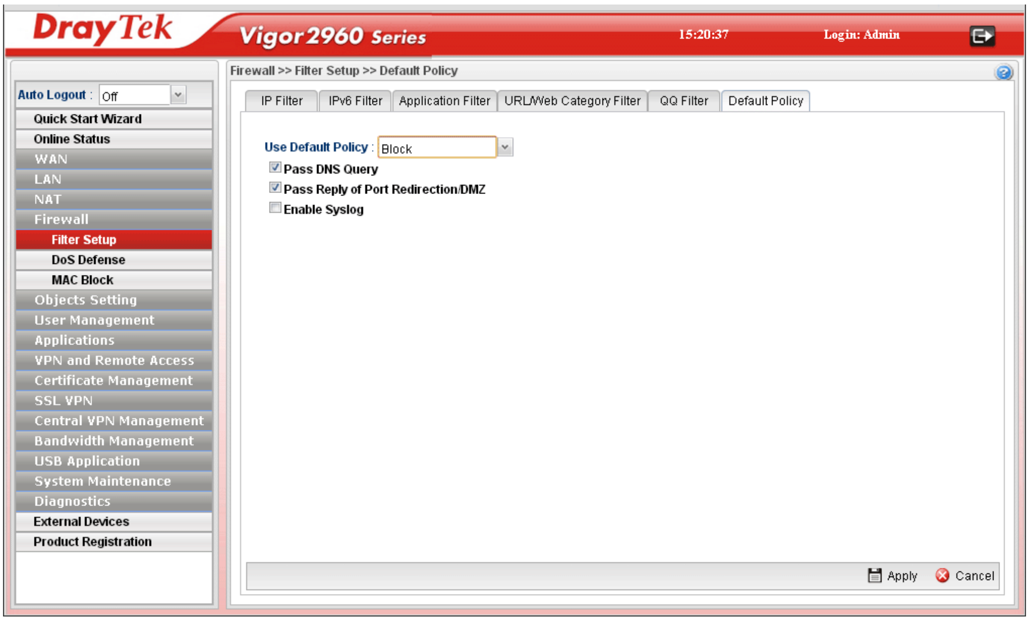


Firewall >> Filter Setup >> QQ Filter

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

4.5.1.6 Default Policy

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



Firewall >> Filter Setup >> Default Policy

Use Default Policy : Block

☑ Pass DNS Query

☑ Pass Reply of Port Redirection/DMZ

□ Enable Syslog

Available parameters are listed as follows:

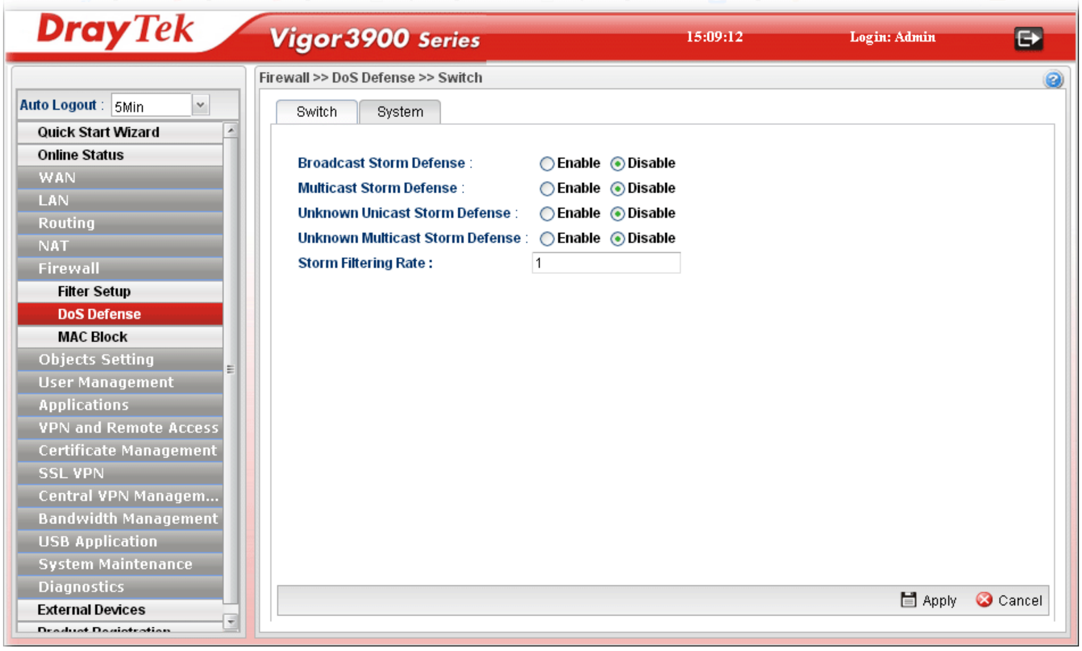
Item	Description
Use Default Policy	**Pass** – All of the incoming packets can pass through Vigor router without any filtering. **Block** – All of the incoming packets will be blocked except the following rules. ● **Pass DNS Query** – Check the box to make the DNS query passing through Vigor router's firewall. ● **Pass Reply of Port Redirection /DMZ** – Check the box to make the **outgoing** packets processed by Port Redirection/DMZ passing through Vigor router's firewall. ● **Enable Syslog** – Check the box to make related information for the blocked packets being recorded in Syslog. The above three policies also can be configured in **Firewall>>Filter Setup>>IP Filter/Application Filter.**
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.5.2 DoS Defense

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

4.5.2.1 Switch



Broadcast Storm Defense : ○ Enable ⦿ Disable

Multicast Storm Defense : ○ Enable ⦿ Disable

Unknown Unicast Storm Defense : ○ Enable ⦿ Disable

Unknown Multicast Storm Defense : ○ Enable ⦿ Disable

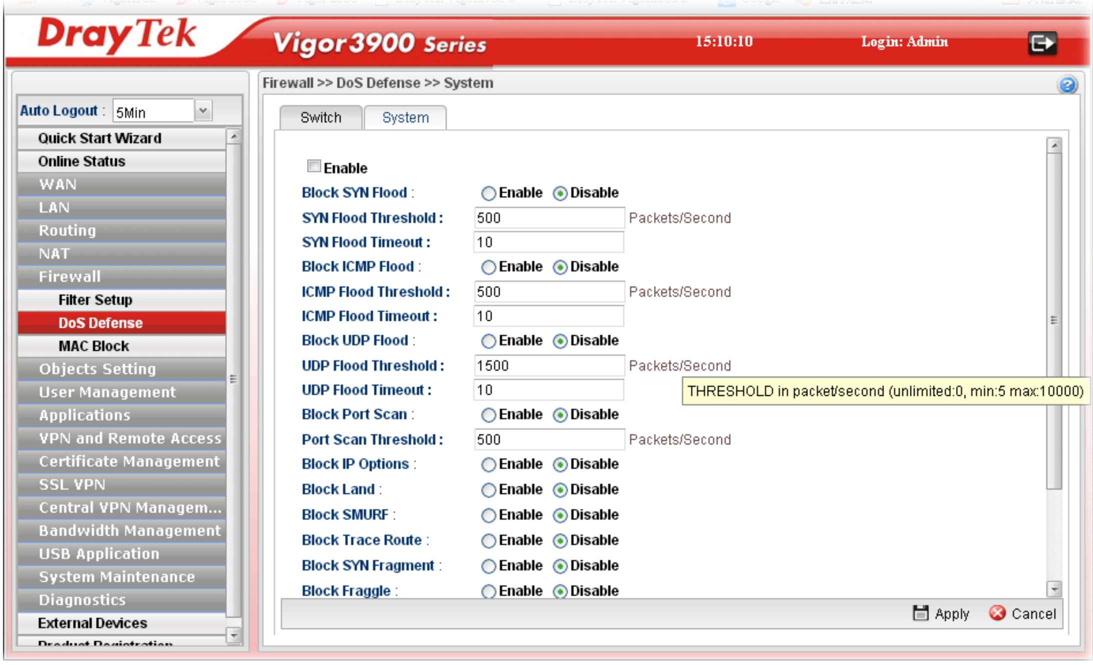
Storm Filtering Rate : 1

Available parameters are listed as follows:

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

4.5.2.2 System

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



Firewall >> DoS Defense >> System

□ Enable

Block SYN Flood :	○ Enable ● Disable	
SYN Flood Threshold :	500	Packets/Second
SYN Flood Timeout :	10	
Block ICMP Flood :	○ Enable ● Disable	
ICMP Flood Threshold :	500	Packets/Second
ICMP Flood Timeout :	10	
Block UDP Flood :	○ Enable ● Disable	
UDP Flood Threshold :	1500	Packets/Second
UDP Flood Timeout :	10	
Block Port Scan :	○ Enable ● Disable	
Port Scan Threshold :	500	Packets/Second
Block IP Options :	○ Enable ● Disable	
Block Land :	○ Enable ● Disable	
Block SMURF :	○ Enable ● Disable	
Block Trace Route :	○ Enable ● Disable	
Block SYN Fragment :	○ Enable ● Disable	
Block Fraggle :	○ Enable ● Disable	

THRESHOLD in packet/second (unlimited:0, min:5 max:10000)

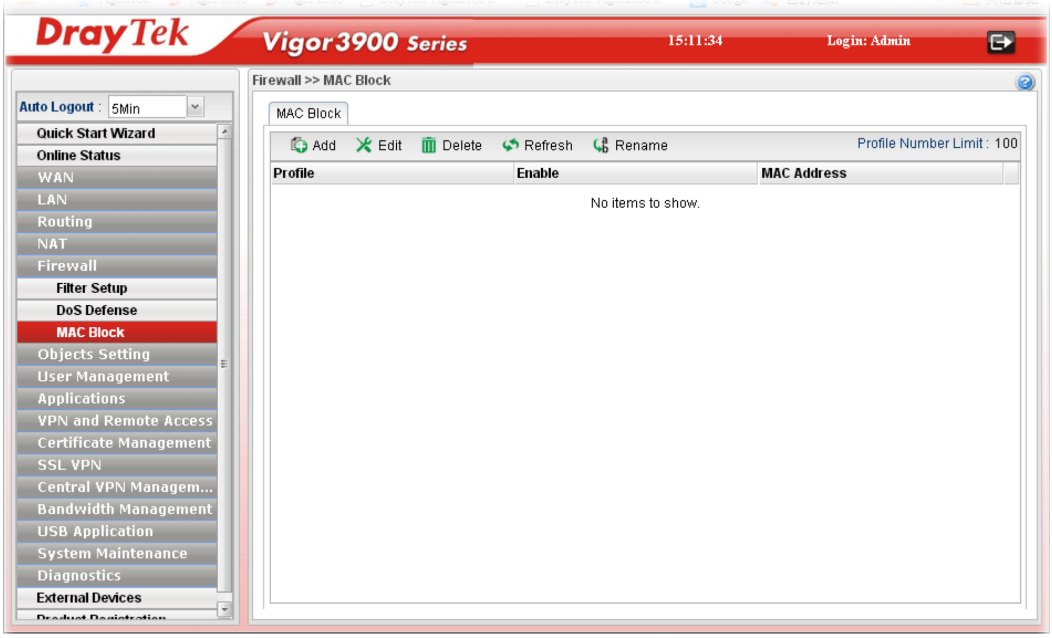
Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable this profile.
Block SYN Flood	Click **Enable** to activate the SYN flood defense function. If the amount of TCP SYN packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN packets within the user-defined timeout period.
SYN Flood Threshold	The default setting for threshold is **500** 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 **500** 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 **1500** 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 **500** pps (packets per second).
Block IP Options	Click **Enable** to activate the Block IP options function. The router will ignore any IP packets with IP option field appearing in the datagram header.
Block Land	Click **Enable** to activate the Block Land function. A Land attack occurs when an attacker sends spoofed SYN packets with identical source address, destination addresses and port number as those of the victim.
Block SMURF	Click **Enable** to activate the Block Smurf function. The router will reject any ICMP echo request destined for the broadcast address.
Block Trace Route	Click **Enable** to activate the Block Trace Route function.
Block SYN Fragment	Click **Enable** to activate the Block SYN fragment function. Any packets having the SYN flag and fragmented bit sets will be dropped.
Block Fraggle	Click **Enable** to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet are blocked.
Block Tear Drop	Click **Enable** to activate the Block Tear Drop function. This attack involves the perpetrator sending overlapping packets to the target hosts so that target host will hang once they re-construct the packets. The routers will block any packets resembling this attacking activity.
Block Ping of Death	Click **Enable** to activate the Block Ping of Death function. Many machines may crash when receiving an ICMP datagram that exceeds the maximum length. The router will block any fragmented ICMP packets with a length greater than 1024 octets.
Block ICMP Fragment	Click **Enable** to activate the Block ICMP fragment function. Any ICMP packets with fragmented bit sets are dropped.
Block Unknown Protocol	Click **Enable** to activate the Block Unknown Protocol function. The router will block any packets with unknown protocol types.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.5.3 MAC Block

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



Auto Logout : 5Min

Profile Number Limit : 100

Profile	Enable	MAC Address

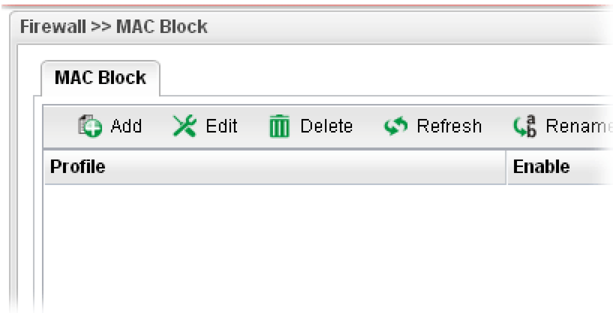
No items to show.

Each item will be explained as follows:

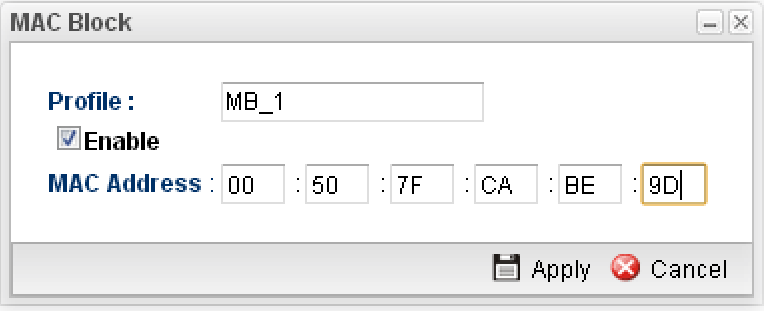
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new MAC Block profile

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



3. The following dialog will appear.

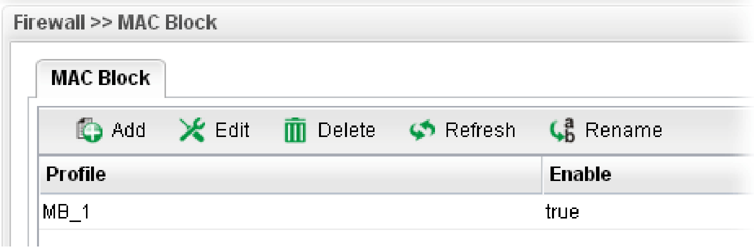


Profile : MB_1
☑ Enable
MAC Address : 00 : 50 : 7F : CA : BE : 9D

Available parameters are listed as follows:

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

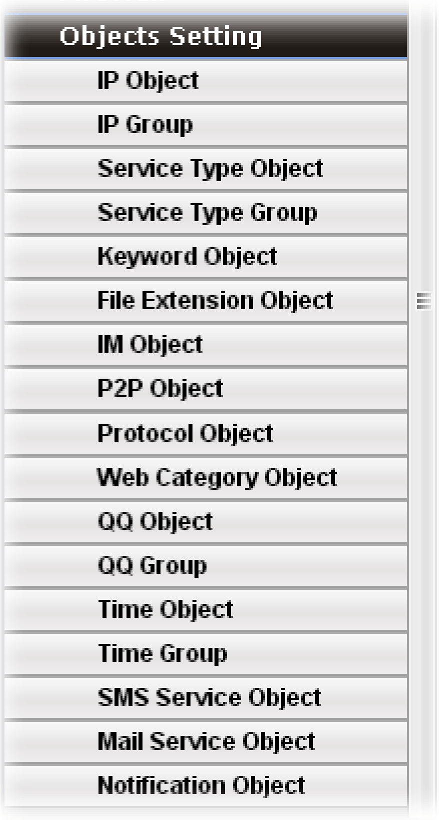
4. Enter all the settings and click **Apply**.
5. A new MAC Block profile has been created.



Profile	Enable
MB_1	true

4.6 Objects Setting

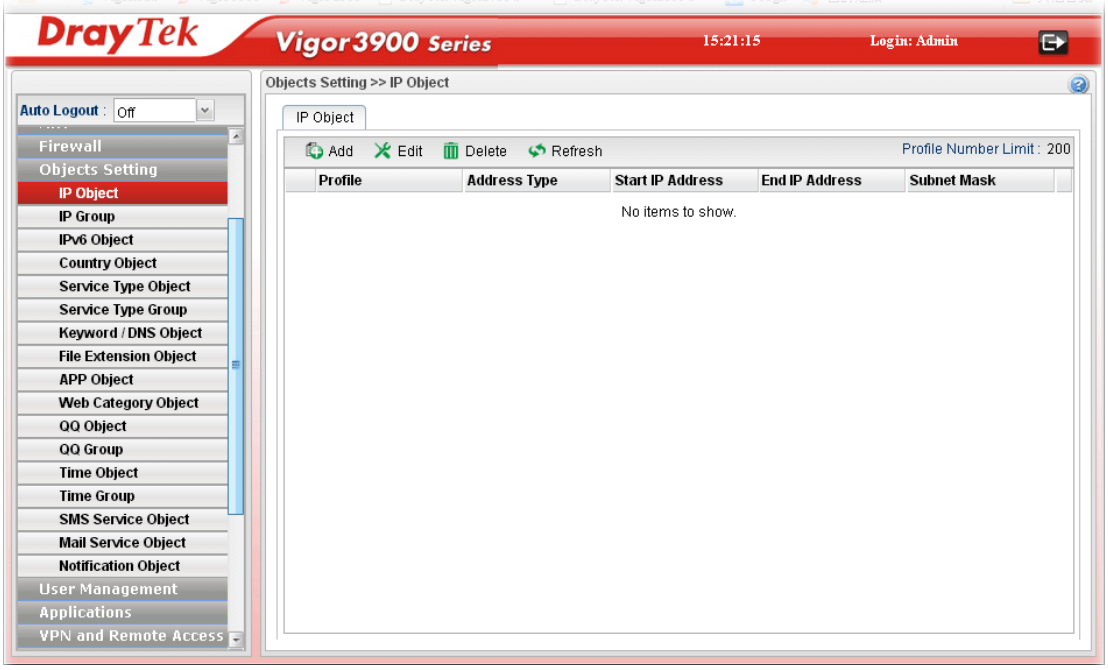
Vigor3900 allows users to set different filter profiles based on IP, service type, keyword, file extension, instant message application, P2P application, protocol application, web category, QQ application, time setting, SMS service, mail service and notification. These objects setting profiles can be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



4.6.1 IP Object

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

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



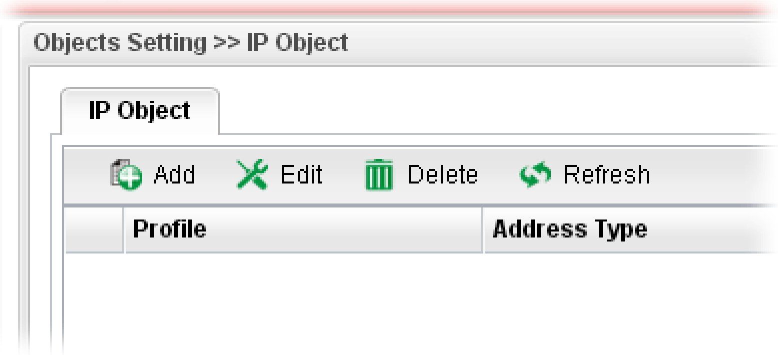
Each item will be explained as follows:

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

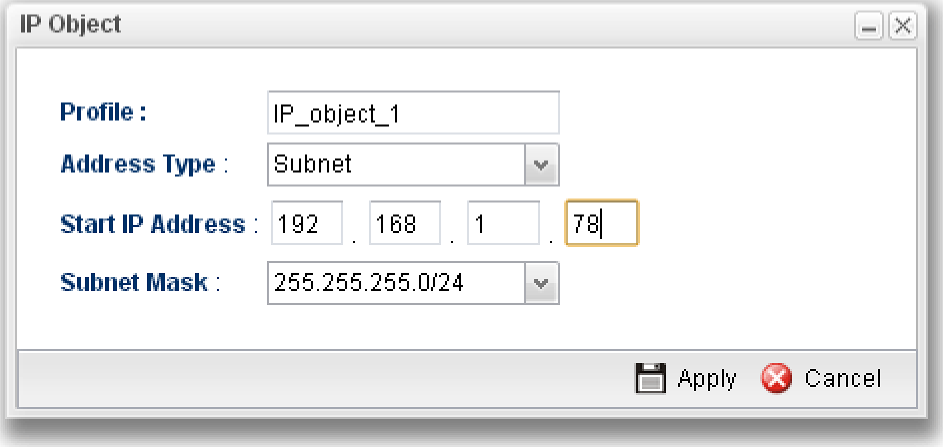
Item	Description
	It will be joined with **Start IP Address** only when you choose **Range** as the **Address Type**.
Subnet Mask	Display the subnet mask for such profile.

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.



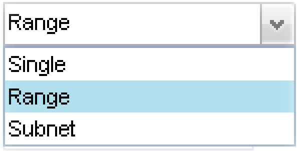
Profile : IP_object_1

Address Type : Subnet

Start IP Address : 192 . 168 . 1 . 78

Subnet Mask : 255.255.255.0/24

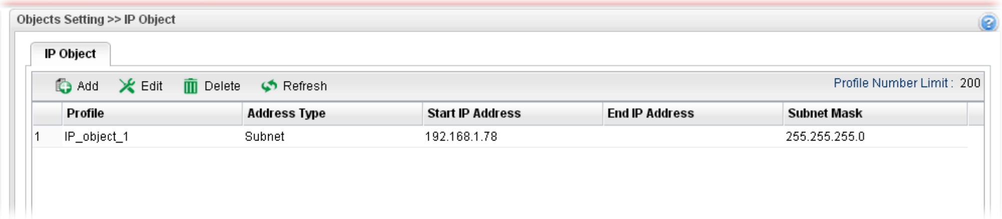
Available parameters are listed as follows:

Item	Description
Profile	Type the name of such profile.
Address Type	Choose the address type (Single / Range /Subnet) for such profile. 
Start IP Address	Type the IP address of the starting point for such profile.
End IP Address	Type the IP address of the ending point for such profile if

Item	Description
	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**.

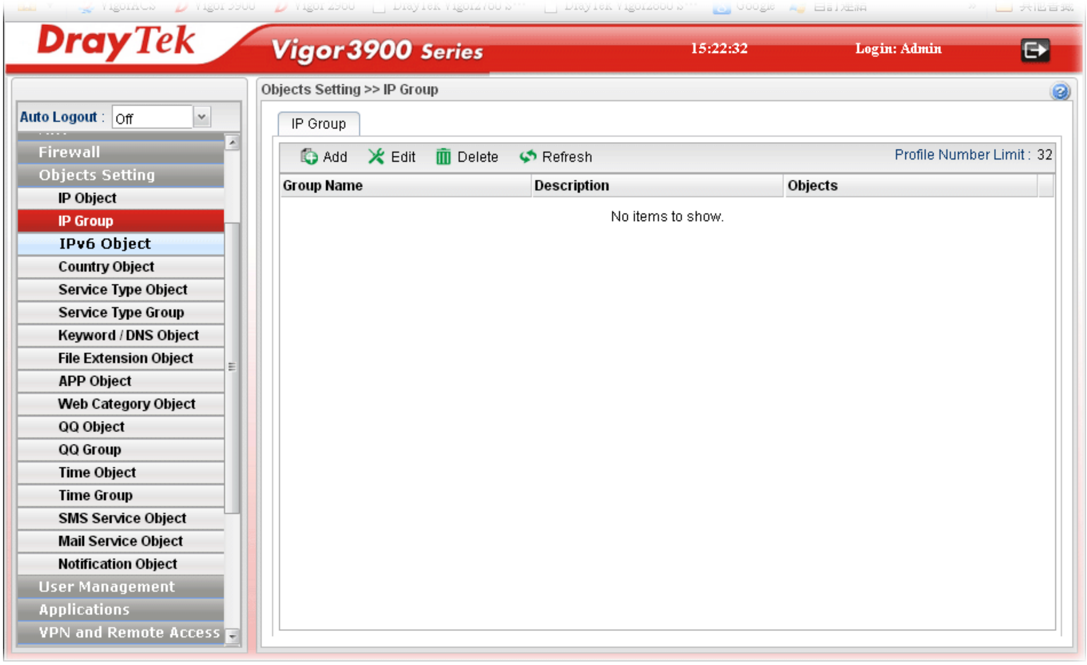
5. A new IP object profile has been created.



	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
1	IP_object_1	Subnet	192.168.1.78		255.255.255.0

4.6.2 IP Group

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

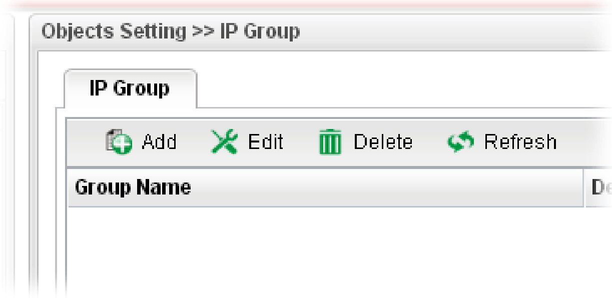


Each item will be explained as follows:

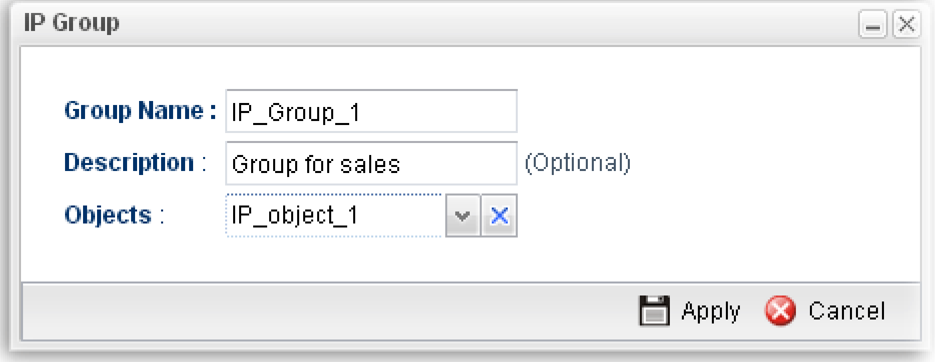
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new IP group profile

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



3. The following dialog will appear.



Group Name : IP_Group_1

Description : Group for sales (Optional)

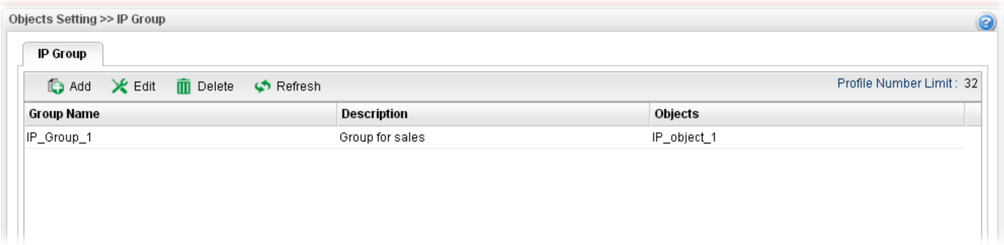
Objects : IP_object_1

Available parameters are listed as follows:

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

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

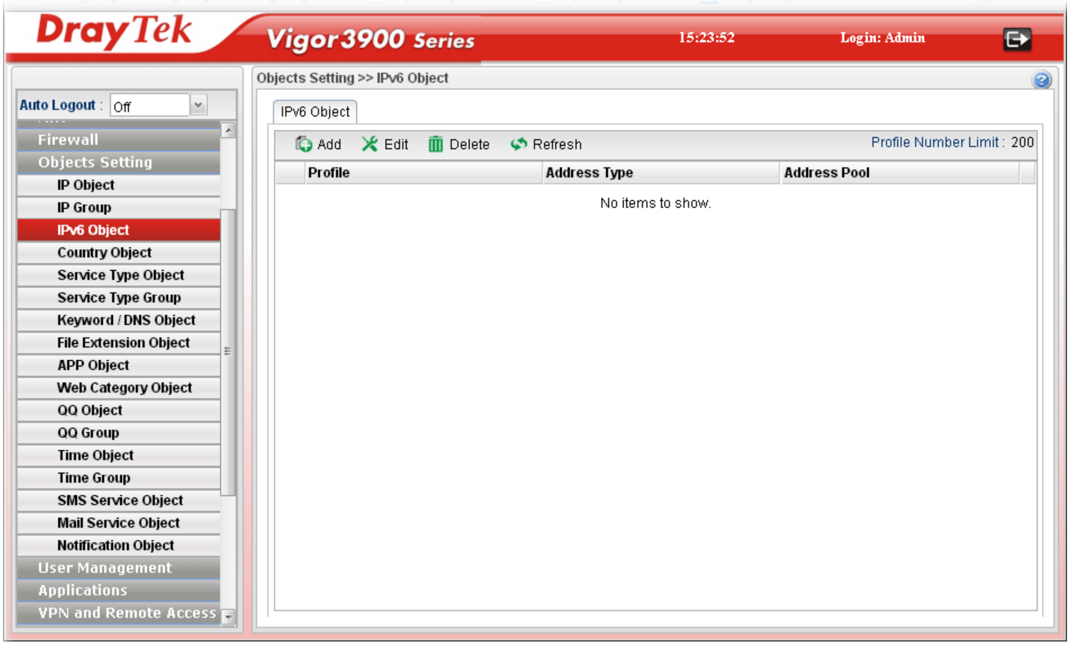
5. A new IP Group profile has been created.



Group Name	Description	Objects
IP_Group_1	Group for sales	IP_object_1

4.6.3 IPv6 Object

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



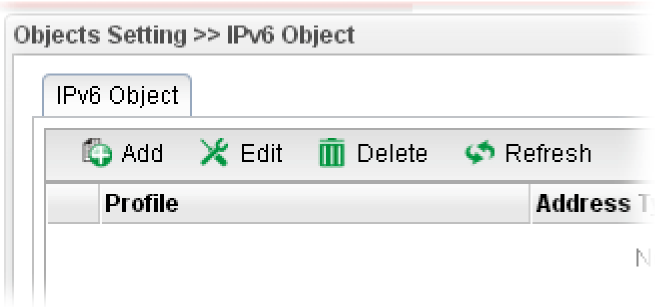
Each item will be explained as follows:

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

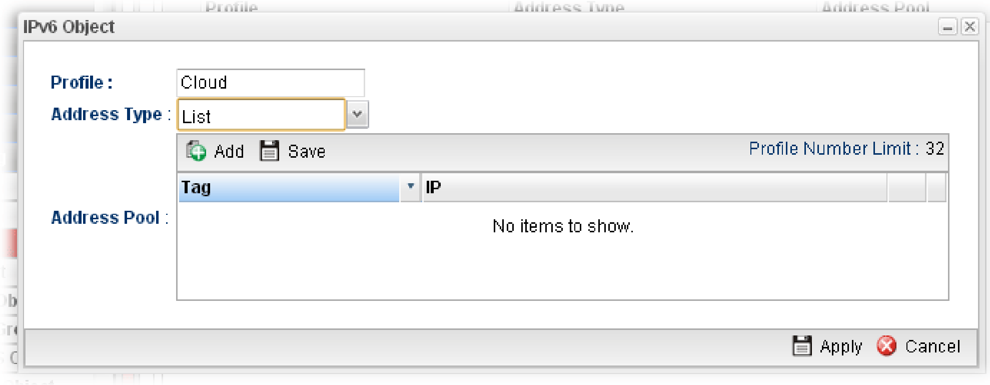
Item	Description
Address Pool	Display the IP address/ IP range /subnet of the object.

How to create a new IPv6 Object profile

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



3. The following dialog will appear.


IPv6 Object

Profile : Cloud

Address Type : List

Available parameters are listed as follows:

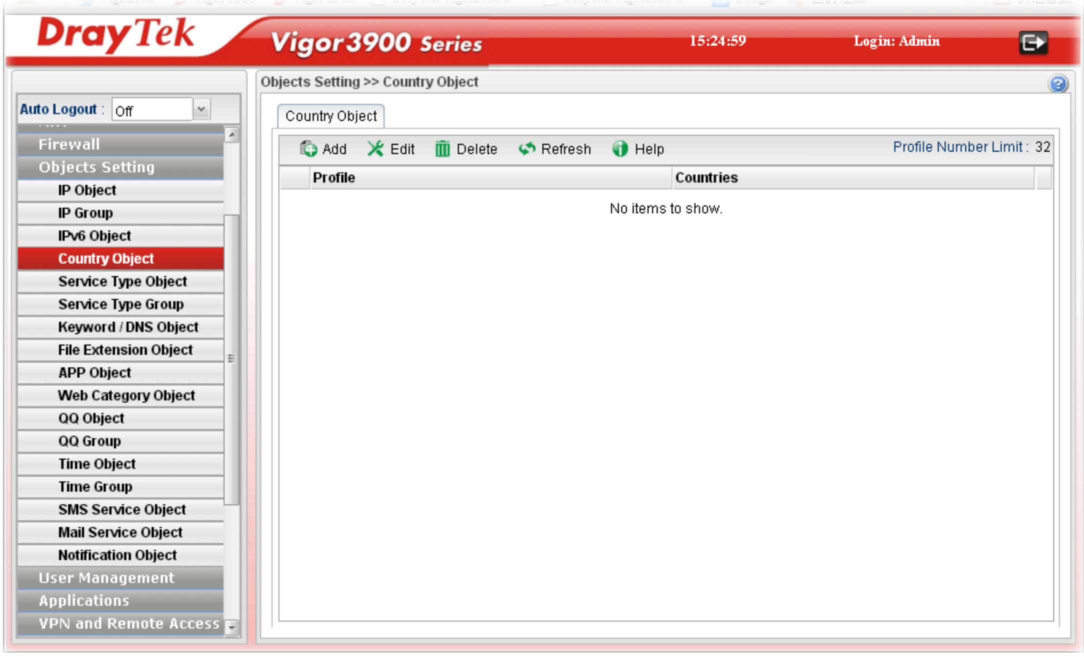
Item	Description
Profile	Type the name of the object.
Address Type	There are three types: **List** – Allow to specify IP address. **Range** – Allow to specify a range of IP addresses. **Subnet** – Allow to specify subnet mask.
Address Pool	This field allows you to type IP address, specify Tag number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

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

   A new IPv6 Object profile has been created.

4.6.4 Country Object

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

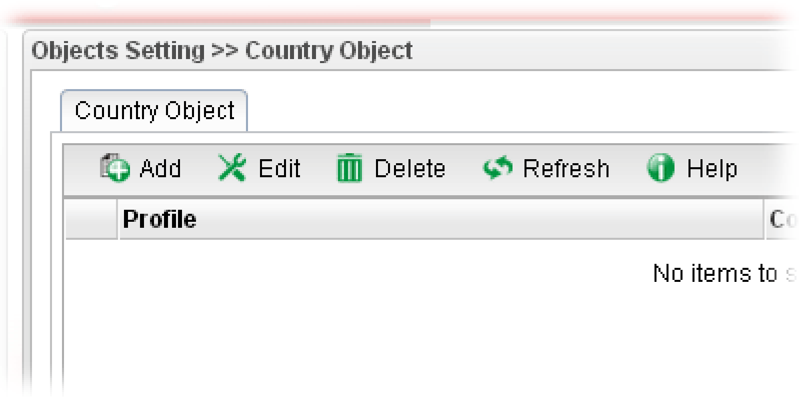


Each item will be explained as follows:

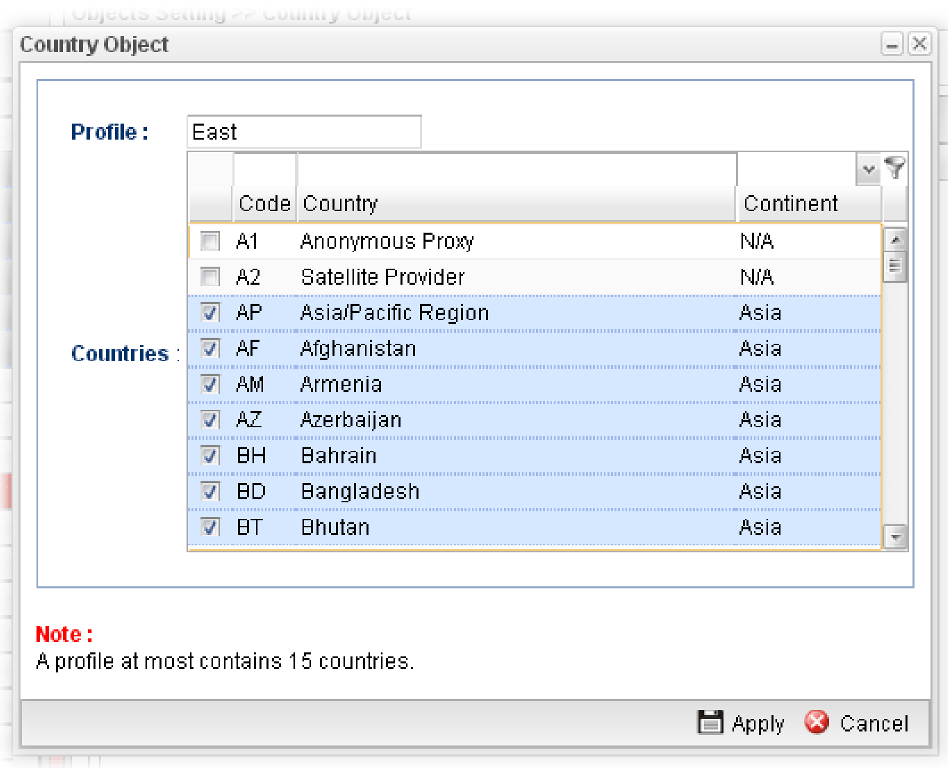
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new Country Object profile

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



3. The following dialog will appear.



Profile : East

Countries :

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

Note :
A profile at most contains 15 countries.

Available parameters are listed as follows:

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

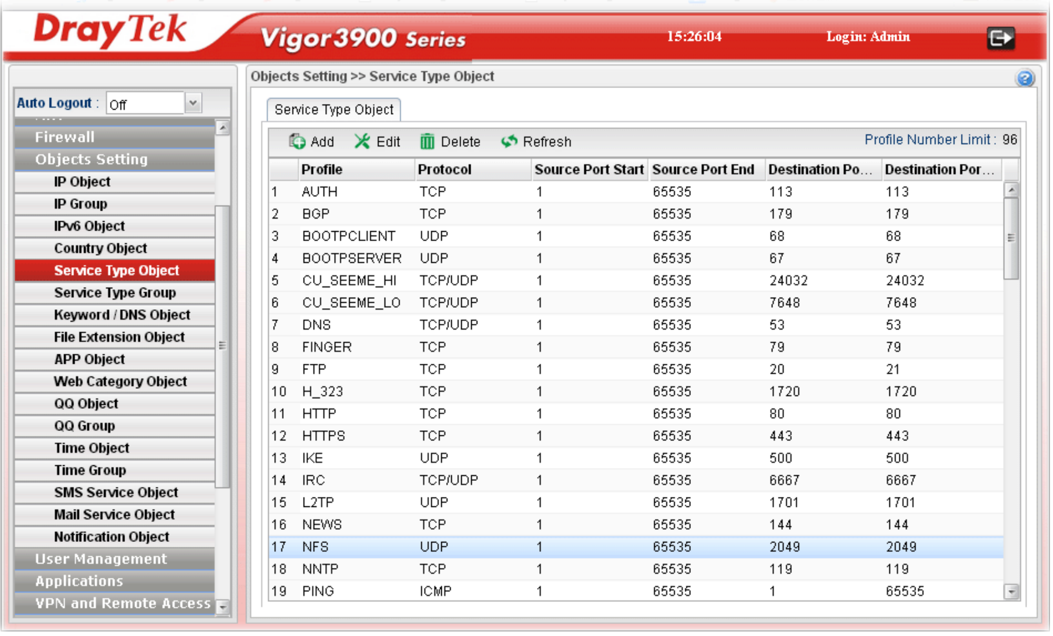
4. Enter all of the settings and click **Apply**.

5. A new Country Object profile has been created.

4.6.5 Service Type Object

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

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



Objects Setting >> Service Type Object

Profile Number Limit : 96

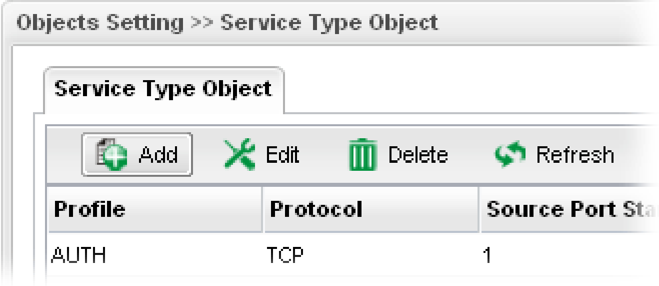
	Profile	Protocol	Source Port Start	Source Port End	Destination Po...	Destination Por...
1	AUTH	TCP	1	65535	113	113
2	BGP	TCP	1	65535	179	179
3	BOOTPCLIENT	UDP	1	65535	68	68
4	BOOTPSERVER	UDP	1	65535	67	67
5	CU_SEEME_HI	TCP/UDP	1	65535	24032	24032
6	CU_SEEME_LO	TCP/UDP	1	65535	7648	7648
7	DNS	TCP/UDP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

Each item will be explained as follows:

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

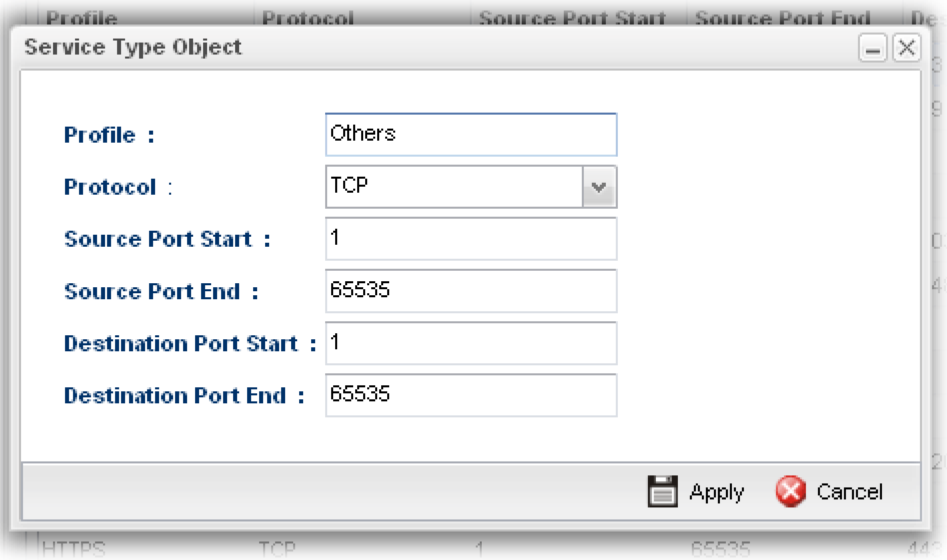
How to create a new service type object profile

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



Profile	Protocol	Source Port Sta
AUTH	TCP	1

3. The following dialog will appear.



Profile : Others

Protocol : TCP

Source Port Start : 1

Source Port End : 65535

Destination Port Start : 1

Destination Port End : 65535

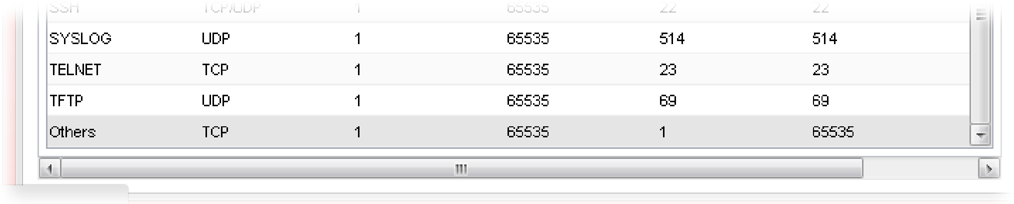
Available parameters are listed as follows:

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

Item	Description
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.

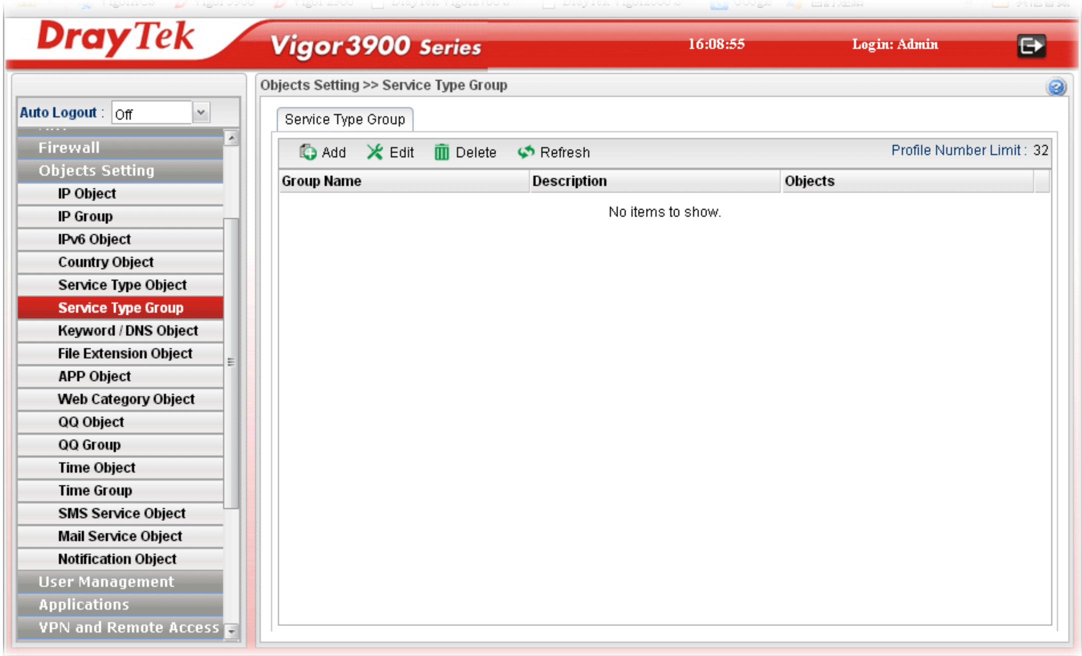


SSH	TCP/UDP	1	65535	22	22
SYSLOG	UDP	1	65535	514	514
TELNET	TCP	1	65535	23	23
TFTP	UDP	1	65535	69	69
Others	TCP	1	65535	1	65535

4.6.6 Service Type Group

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

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



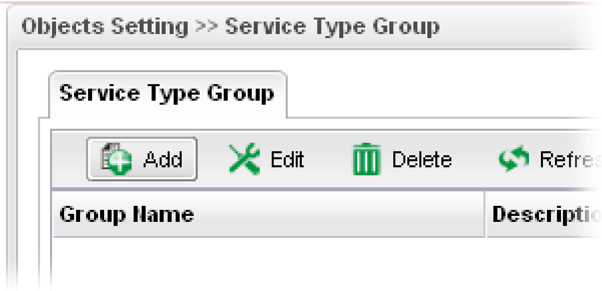
No items to show.

Each item will be explained as follows:

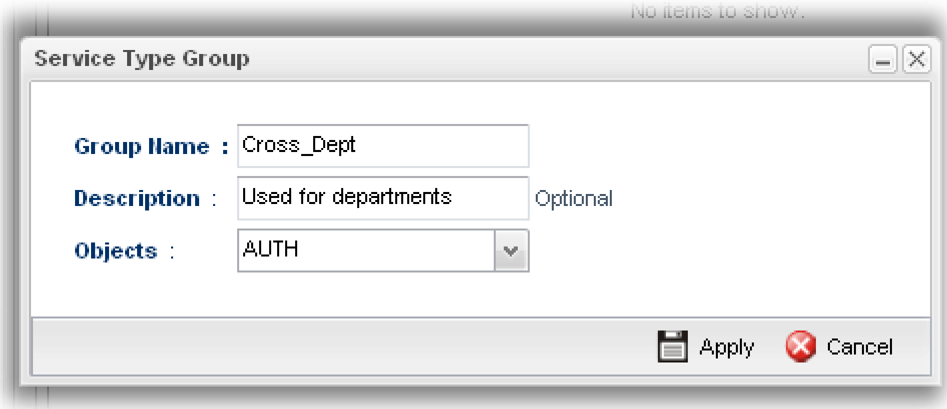
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new service type group profile

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



3. The following dialog will appear.



Group Name : Cross_Dept

Description : Used for departments Optional

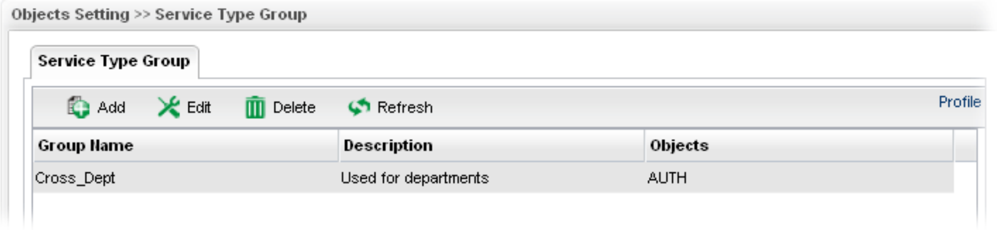
Objects : AUTH

Available parameters are listed as follows:

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

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

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



Objects Setting >> Service Type Group

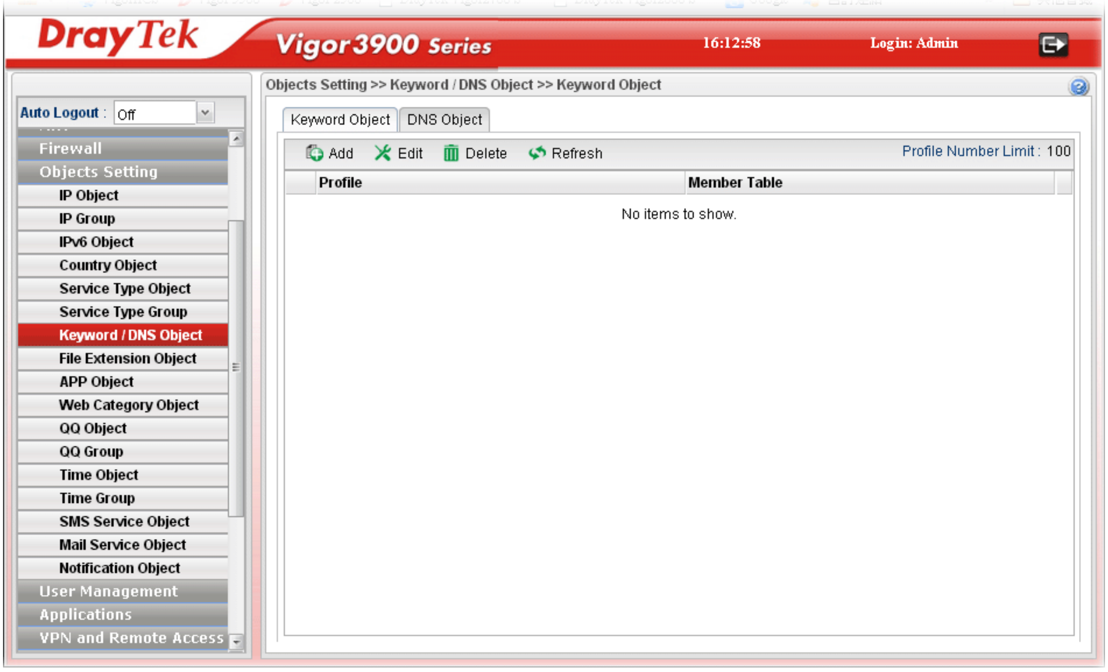
Service Type Group

Group Name	Description	Objects
Cross_Dept	Used for departments	AUTH

4.6.7 Keyword /DNS Object

4.6.7.1 Keyword Object

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



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

Profile Number Limit : 100

Profile	Member Table

No items to show.

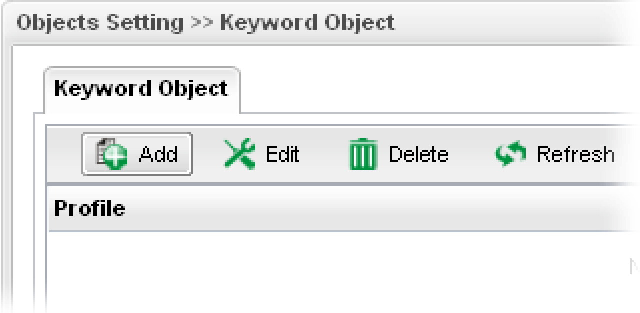
Each item will be explained as follows:

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

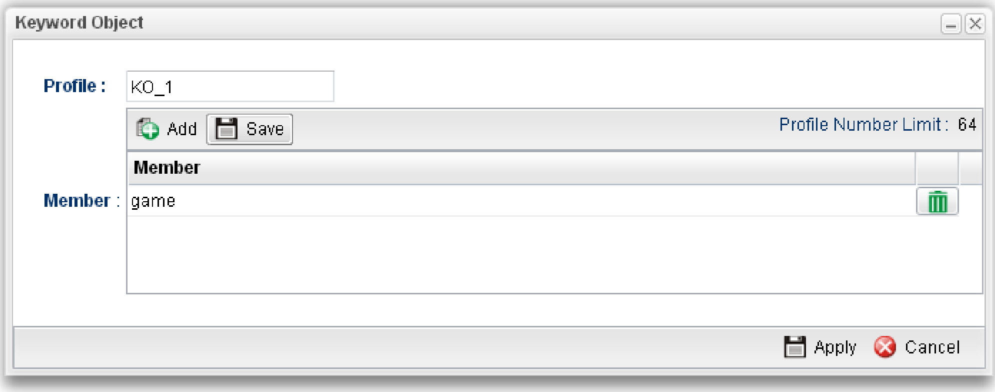
Item	Description
	created.
Profile	Display the name of the keyword object profile.
Member	Display the words specified in such profile.

How to create a new keyword object profile

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



3. The following dialog will appear.



Profile : KO_1

Profile Number Limit : 64

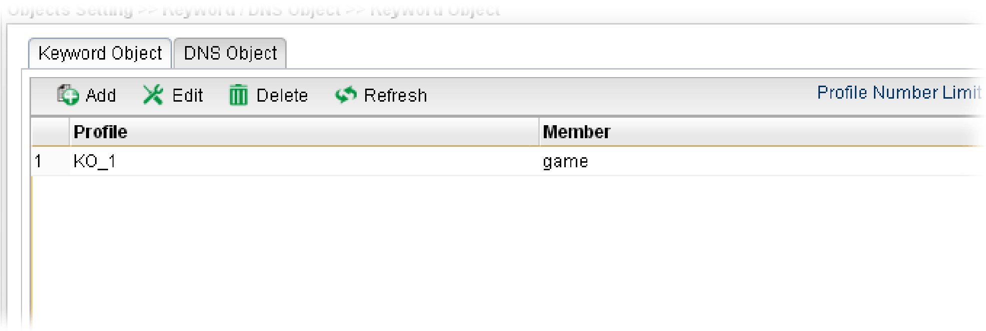
Member : game

Available parameters are listed as follows:

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

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

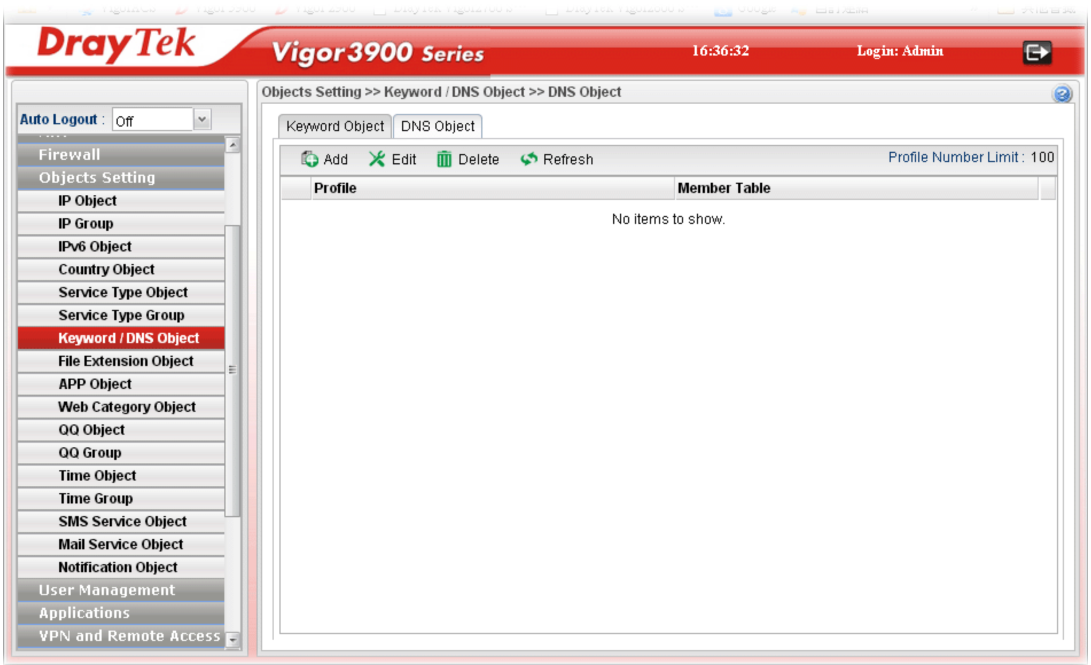
5. A new **Keyword Object** profile has been created.



	Profile	Member
1	KO_1	game

4.6.7.2 DNS Object

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



No items to show.

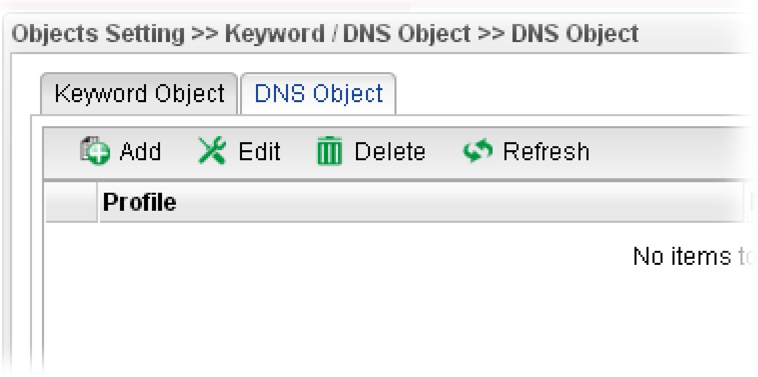
Each item will be explained as follows:

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

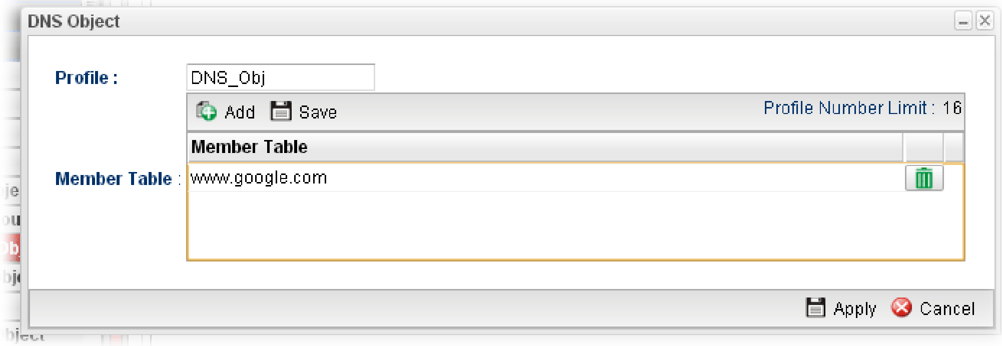
Item	Description
	created.
Profile	Display the name of the keyword object profile.
Member Table	Display the words specified in such profile.

How to create a new DNS Object profile

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



3. The following dialog will appear.


DNS Object

Profile : DNS_Obj

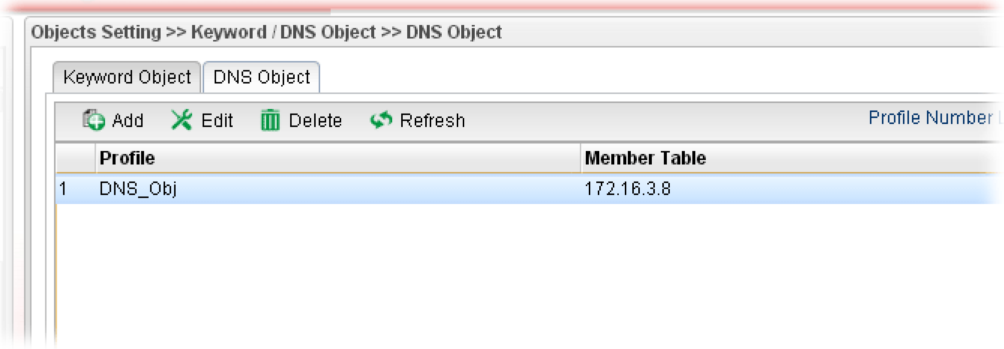
Member Table : www.google.com

Available parameters are listed as follows:

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

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

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

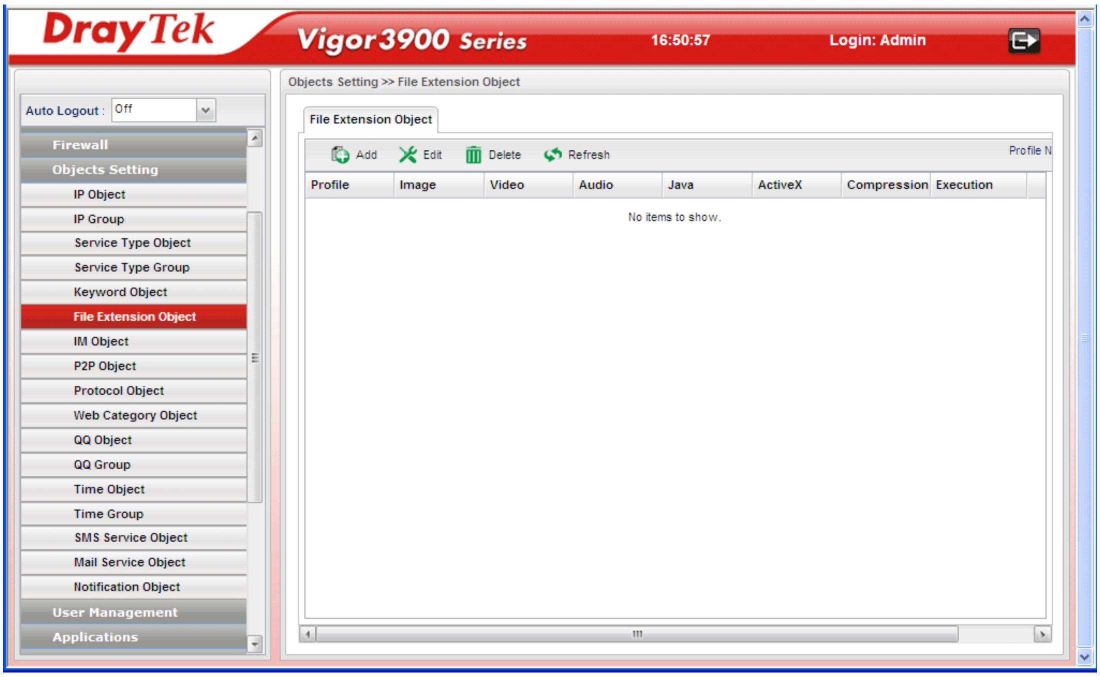


Objects Setting >> Keyword / DNS Object >> DNS Object

	Profile	Member Table
1	DNS_Obj	172.16.3.8

4.6.8 File Extension Object

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



Profile	Image	Video	Audio	Java	ActiveX	Compression	Execution

No items to show.

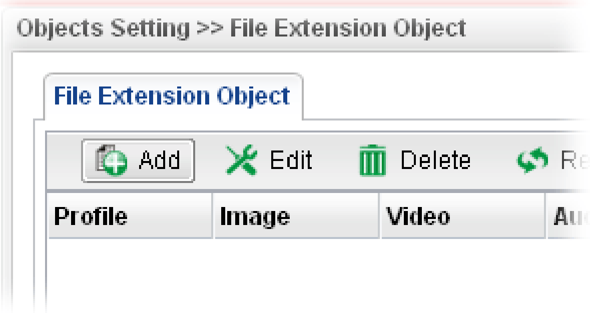
Each item will be explained as follows:

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

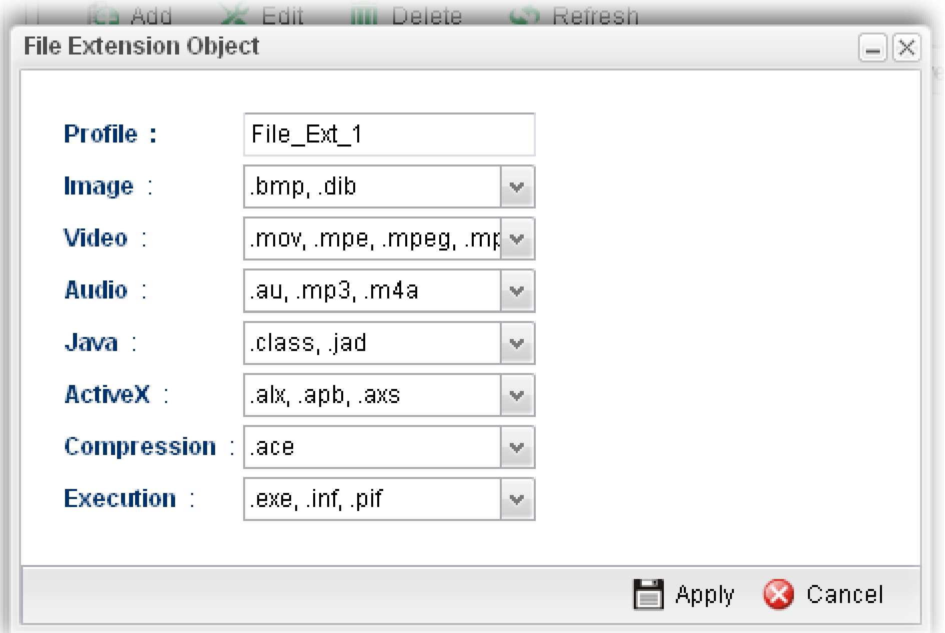
Item	Description
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Profile	Display the name of the profile.
Image	Display the selected file extension of image.
Video	Display the selected file extension of video.
Audio	Display the selected 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.



File Extension Object

Profile : File_Ext_1

Image : .bmp, .dib

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

Audio : .au, .mp3, .m4a

Java : .class, .jad

ActiveX : .alx, .apb, .axs

Compression : .ace

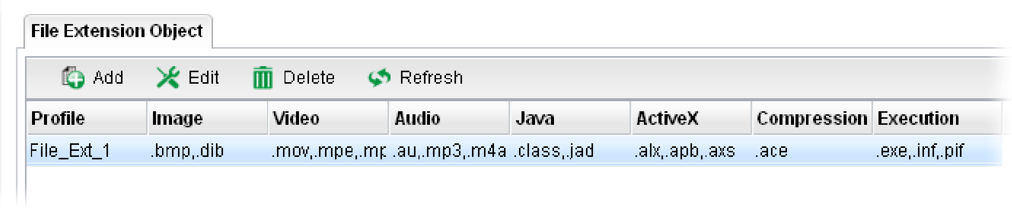
Execution : .exe, .inf, .pif

Available parameters are listed as follows:

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

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

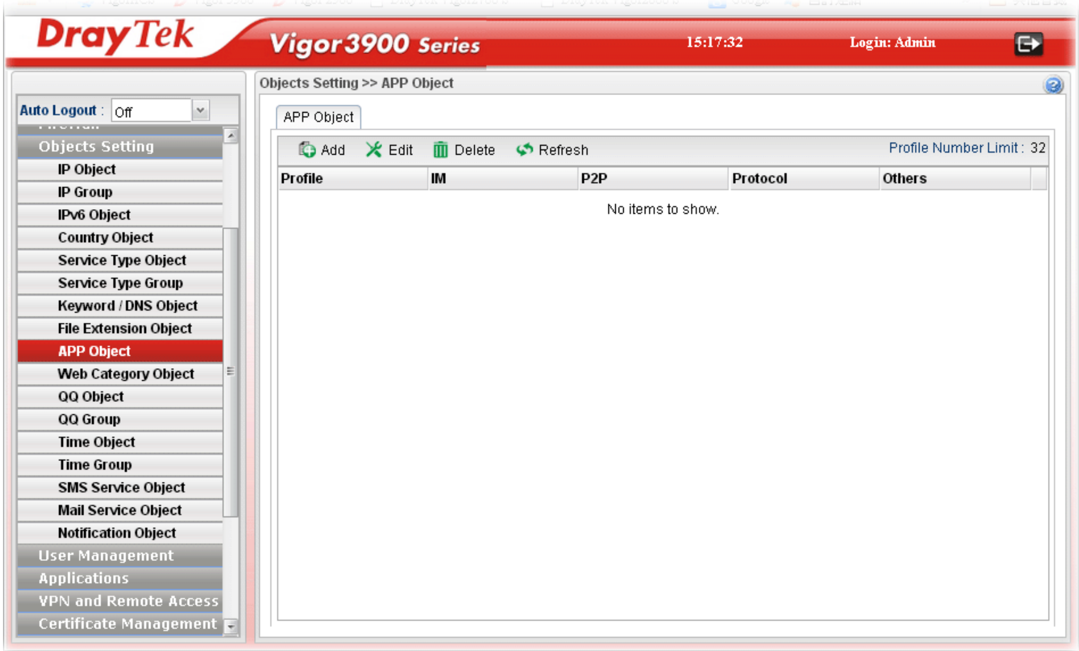
5. A new File Extension Object profile has been created.



Profile	Image	Video	Audio	Java	ActiveX	Compression	Execution
File_Ext_1	.bmp,.dib	.mov,.mpe,.mp	.au,.mp3,.m4a	.class,.jad	.alx,.apb,.axs	.ace	.exe,.inf,.pif

4.6.9 APP Object

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



Auto Logout : Off

Objects Setting >> APP Object

Profile Number Limit : 32

Profile	IM	P2P	Protocol	Others

No items to show.

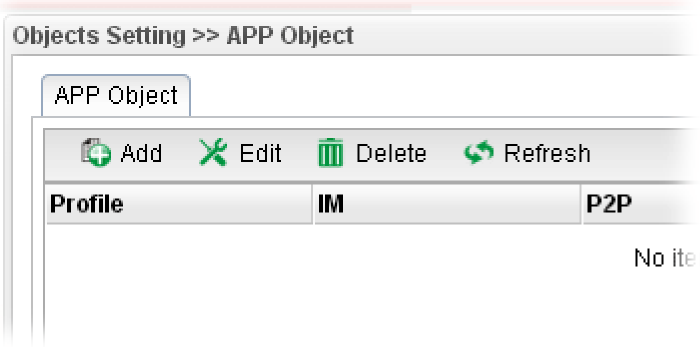
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Profile	Display the name of the IM object profile.
IM	Display the IM application specified in such profile.
P2P	Display the P2P specified in such profile.
Protocol	Display the protocol specified in such profile.
Others	Display other types specified in such profile.

How to create a new APP Object Profile

1. Open **Objects Setting>>APP Object.**

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



Objects Setting >> APP Object

APP Object

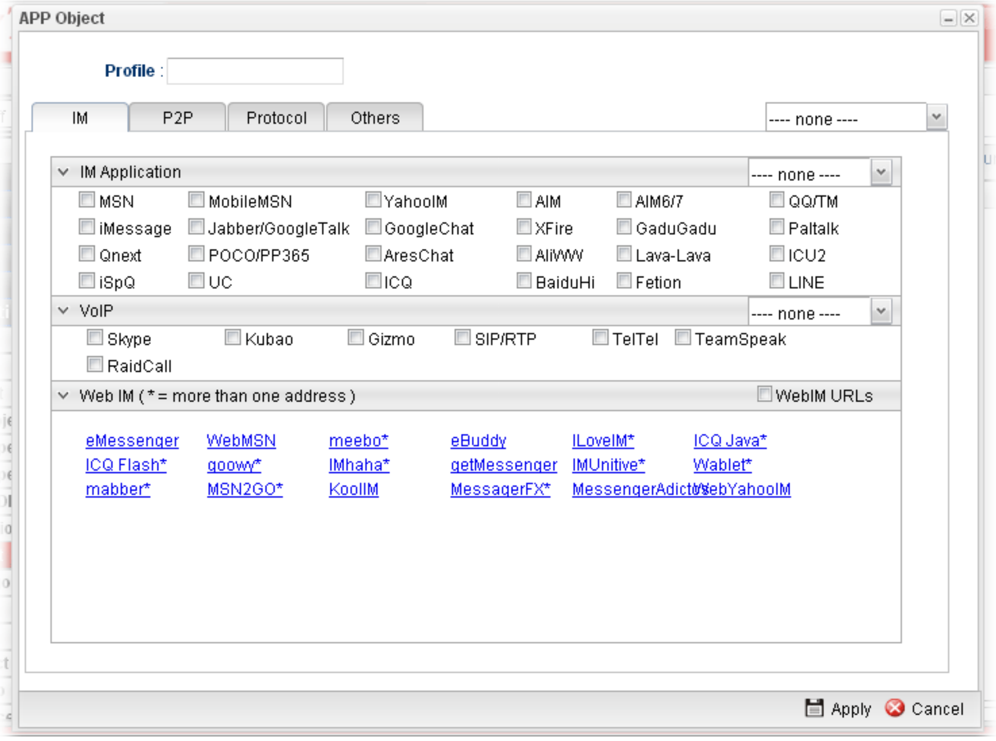
Add | Edit | Delete | Refresh

Profile	IM	P2P

No ite

3. The following dialog will appear.

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



APP Object

Profile :

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

IM Application ---- none ----

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

VoIP ---- none ----

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

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

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

Apply | Cancel

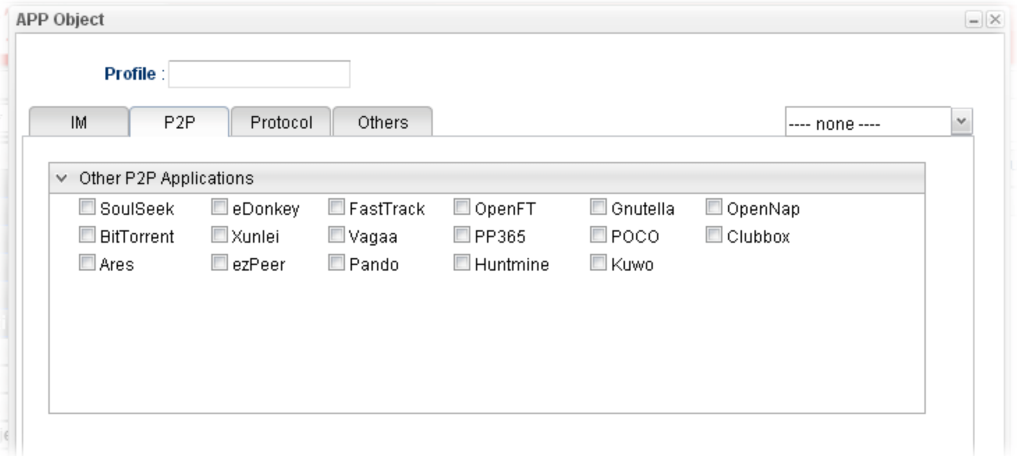
Available parameters are listed as follows:

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

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

Click **P2P** to get the following page. 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.



APP Object

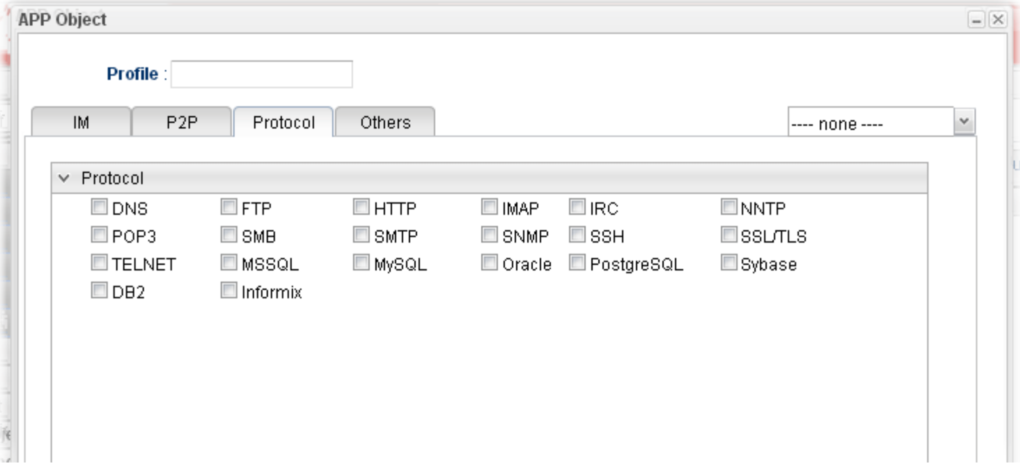
Profile :

Other P2P Applications

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

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

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



APP Object

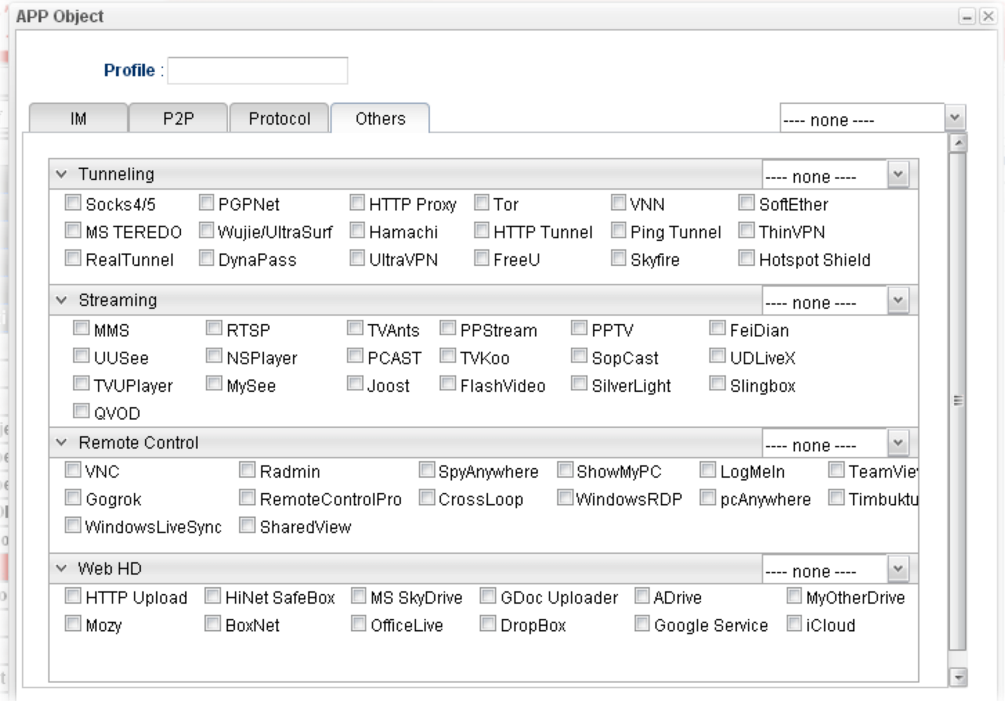
Profile :

Protocol

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

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

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



APP Object

Profile :

IM | P2P | Protocol | Others

---- none ----

Tunneling ---- none ----

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

Streaming ---- none ----

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

Remote Control ---- none ----

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

Web HD ---- none ----

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

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

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

5. A new APP Object profile has been created.

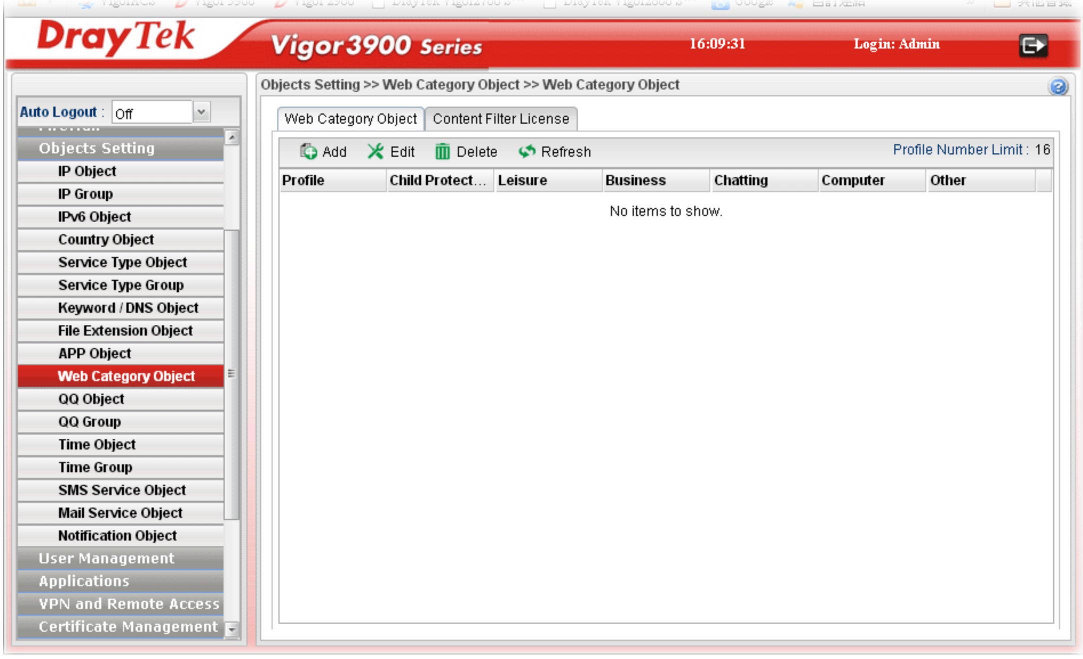
4.6.10 Web Category Object

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

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

powered by **Commtouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.
Note 2: Commtouch is merged by Cyren and GlobalView services will be continued to deliver powerful cloud-based information security solutions! Refer to: http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

4.6.10.1 Web Category Object



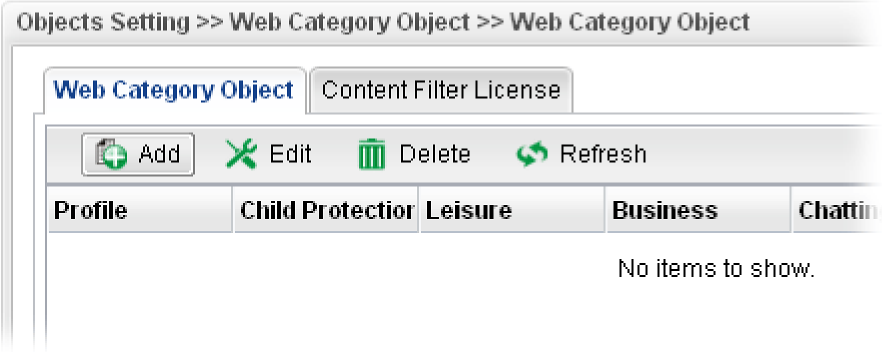
Each item will be explained as follows:

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

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

How to create a new web category object profile

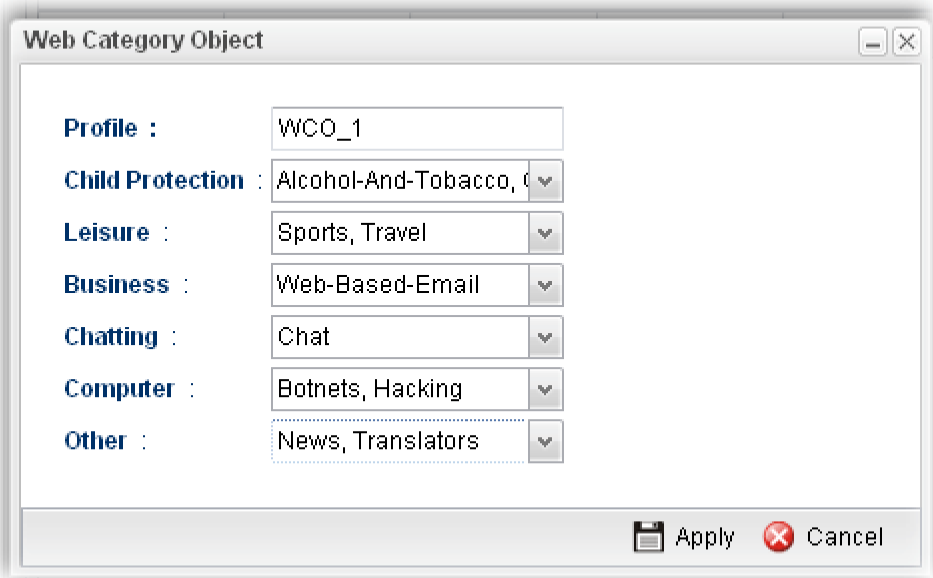
1. Open **Objects Setting>> Web Category Object** and click the **Web Category Object** tab**.**
2. Simply click the **Add** button.



Objects Setting >> Web Category Object >> Web Category Object

No items to show.

3. The following dialog will appear.



Web Category Object

Profile : WCO_1

Child Protection : Alcohol-And-Tobacco, (

Leisure : Sports, Travel

Business : Web-Based-Email

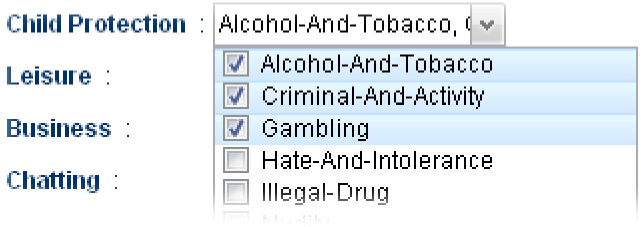
Chatting : Chat

Computer : Botnets, Hacking

Other : News, Translators

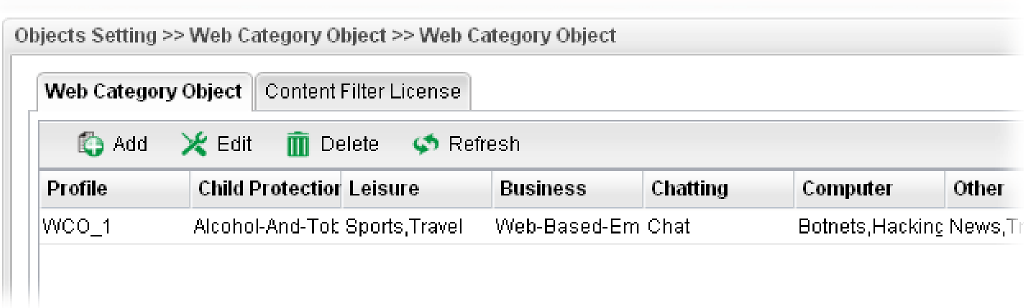
Available parameters are listed as follows:

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

	 Child Protection : Alcohol-And-Tobacco, (Leisure : Business : Chatting : ☑ Alcohol-And-Tobacco ☑ Criminal-And-Activity ☑ Gambling □ Hate-And-Intolerance □ Illegal-Drug
Leisure	Simply check the one(s) that you don’t want the user to visit.
Business	Simply check the one(s) that you don’t want the user to visit.
Chatting	Simply check the one(s) that you don’t want the user to use for gossip with remote people.
Computer	Simply check the one(s) that you don’t want the user to visit.
Other	Simply check the one(s) that you don’t want the user to visit.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

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

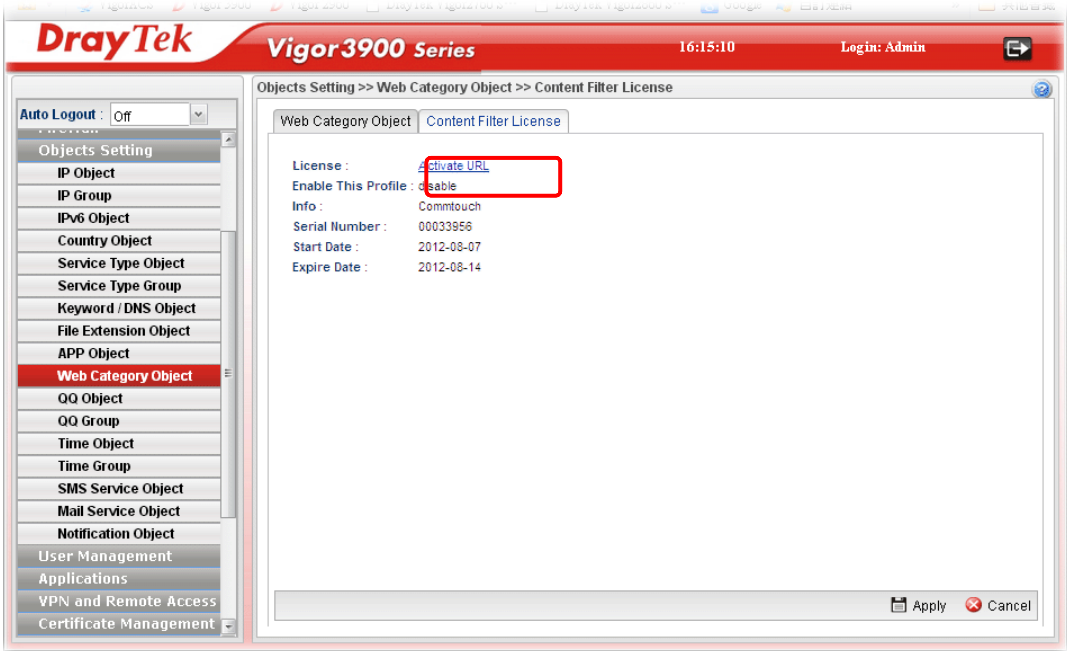


Objects Setting >> Web Category Object >> Web Category Object

Profile	Child Protectior	Leisure	Business	Chatting	Computer	Other
WCO_1	Alcohol-And-Tok	Sports,Travel	Web-Based-Em	Chat	Botnets,Hacking	News,Tr

4.6.10.2 Content Filter License

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



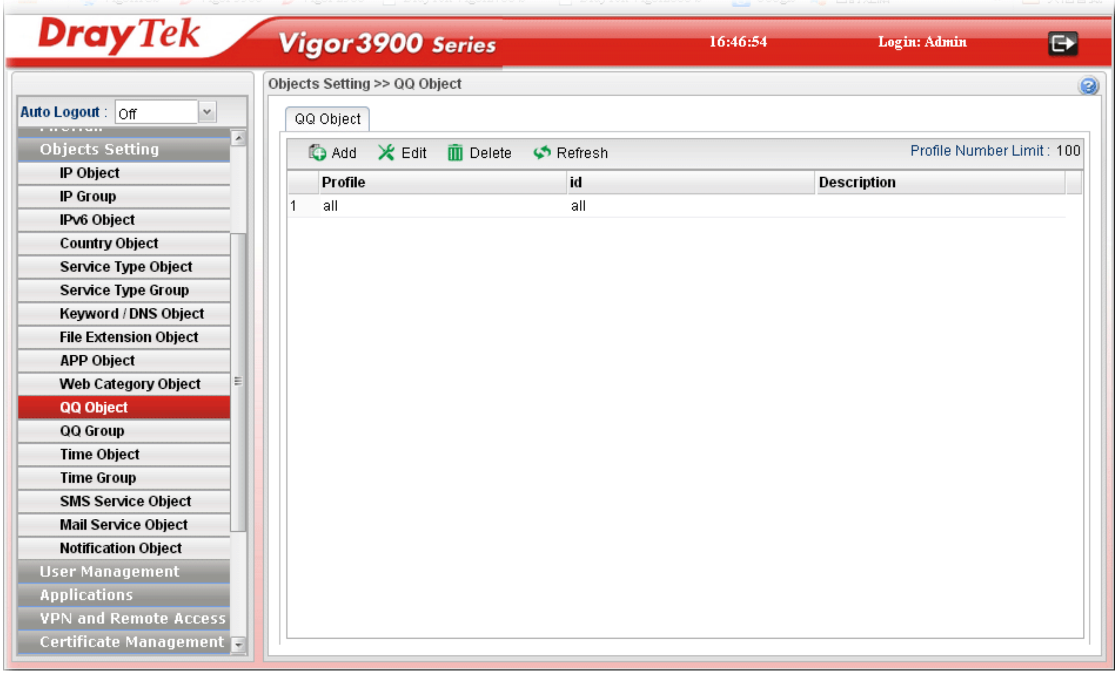
Objects Setting >> Web Category Object >> Content Filter License

License : Activate URL
Enable This Profile : disable
Info : Commtouch
Serial Number : 00033956
Start Date : 2012-08-07
Expire Date : 2012-08-14

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

4.6.11 QQ Object

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



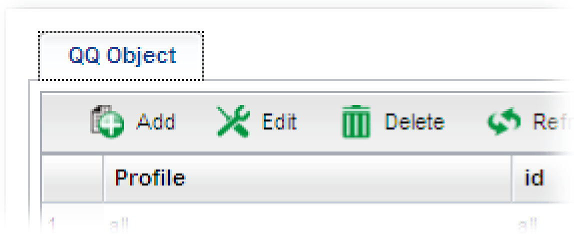
	Profile	id	Description
1	all	all	

Each item will be explained as follows:

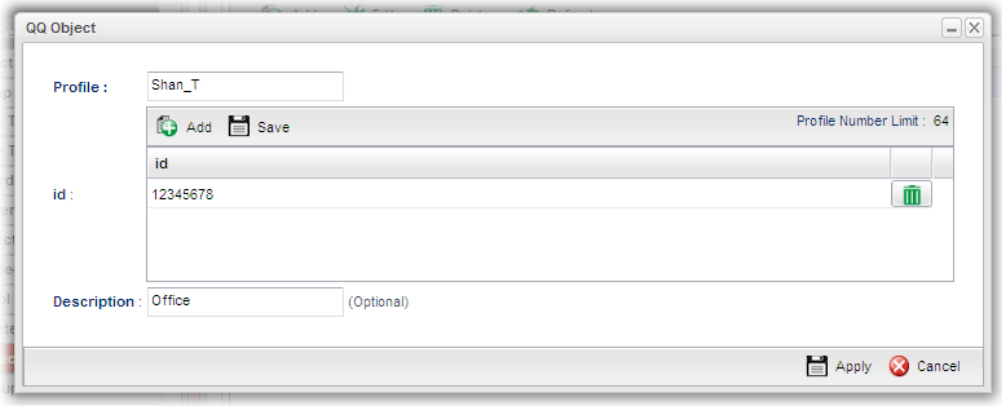
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new QQ object profile

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



3. The following dialog will appear.


QQ Object

Profile : Shan_T

Add | Save | Profile Number Limit : 64

id : 12345678

Description : Office (Optional)

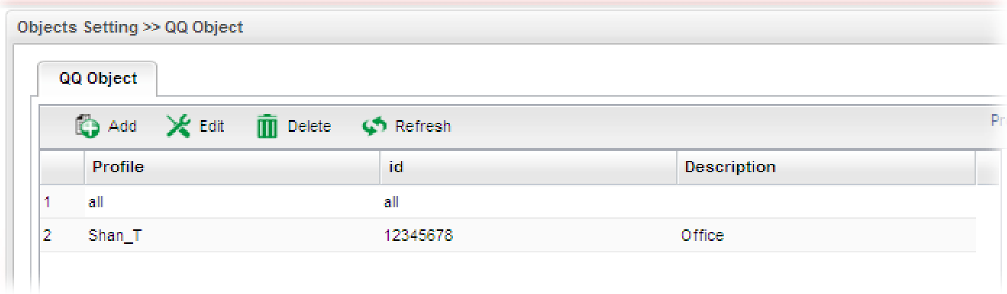
Apply | Cancel

Available parameters are listed as follows:

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

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

5. A new QQ Object profile has been created.

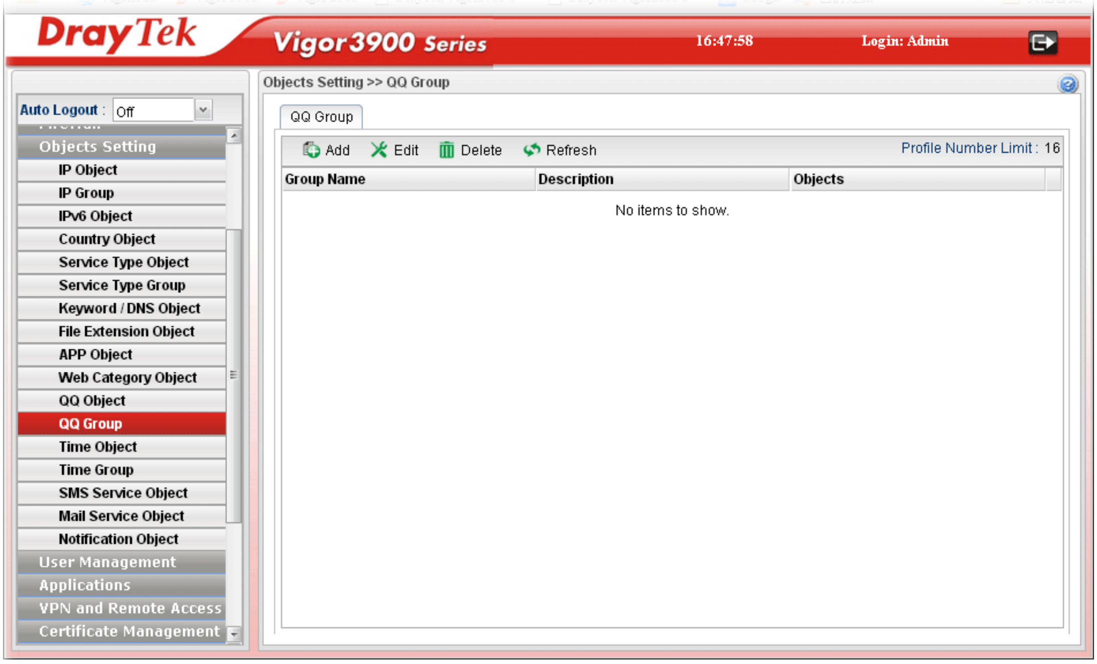


Objects Setting >> QQ Object

	Profile	id	Description
1	all	all	
2	Shan_T	12345678	Office

4.6.12 QQ Group

This page allows you to group several QQ object profiles.



Profile Number Limit : 16

Group Name	Description	Objects

No items to show.

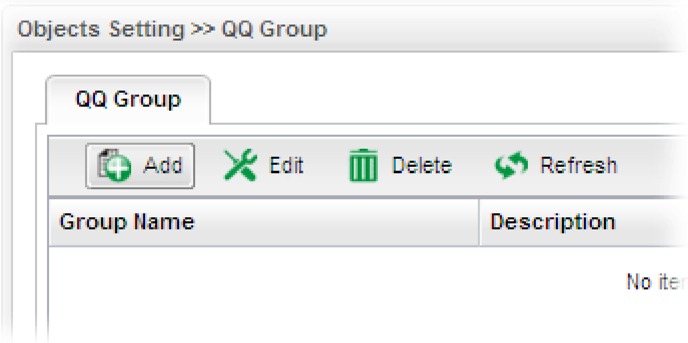
Each item will be explained as follows:

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

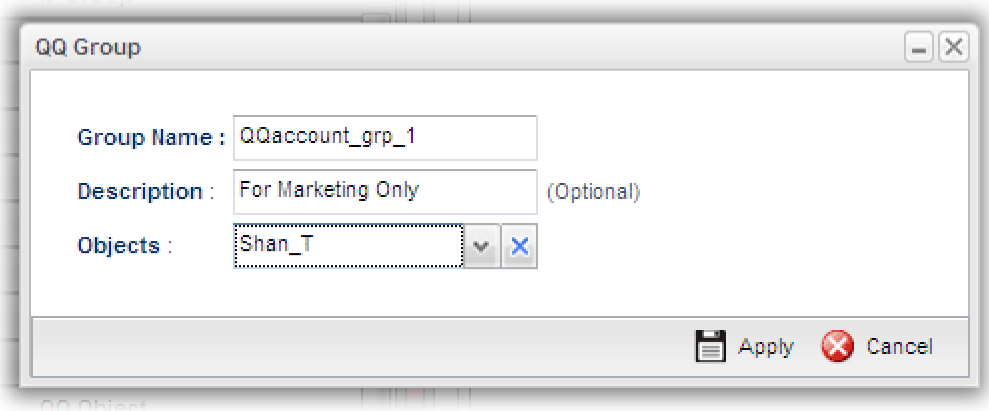
Item	Description
Description	Display the brief explanation for such group.
Objects	Display the time objects selected by such group.

How to create a new QQ group profile

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



3. The following dialog will appear.



Group Name : QQaccount_grp_1

Description : For Marketing Only (Optional)

Objects : Shan_T

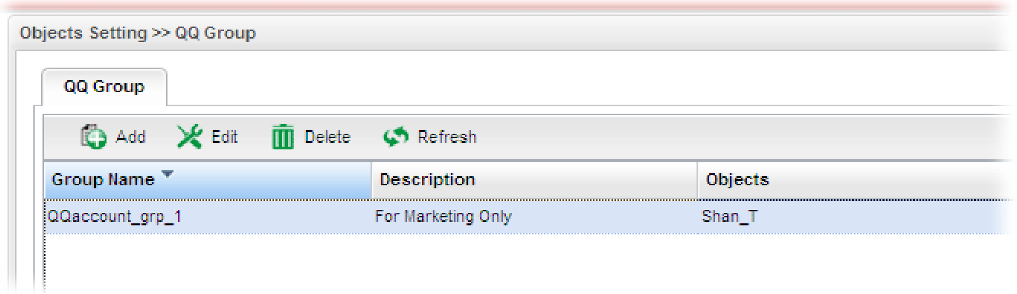
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the time group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to select the object profiles under such group. All the available objects that you have added on **Objects Setting>>QQ Object** will be seen here. To clear the selected one, click ✕ to remove current object selections.
Apply	Click it to save the configuration.

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

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

5. A new QQ group profile has been created.

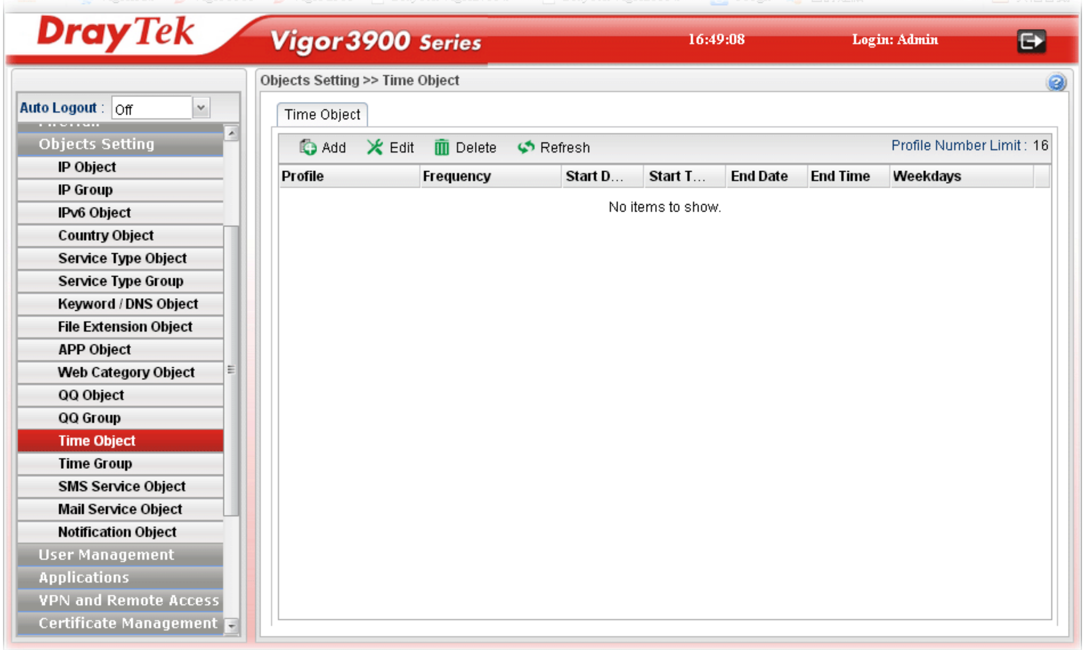


Objects Setting >> QQ Group

Group Name	Description	Objects
QQaccount_grp_1	For Marketing Only	Shan_T

4.6.13 Time Object

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

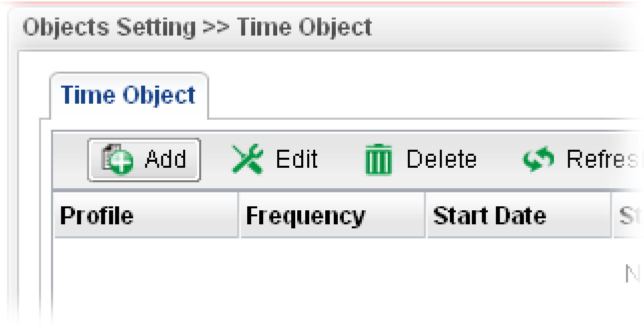


Each item will be explained as follows:

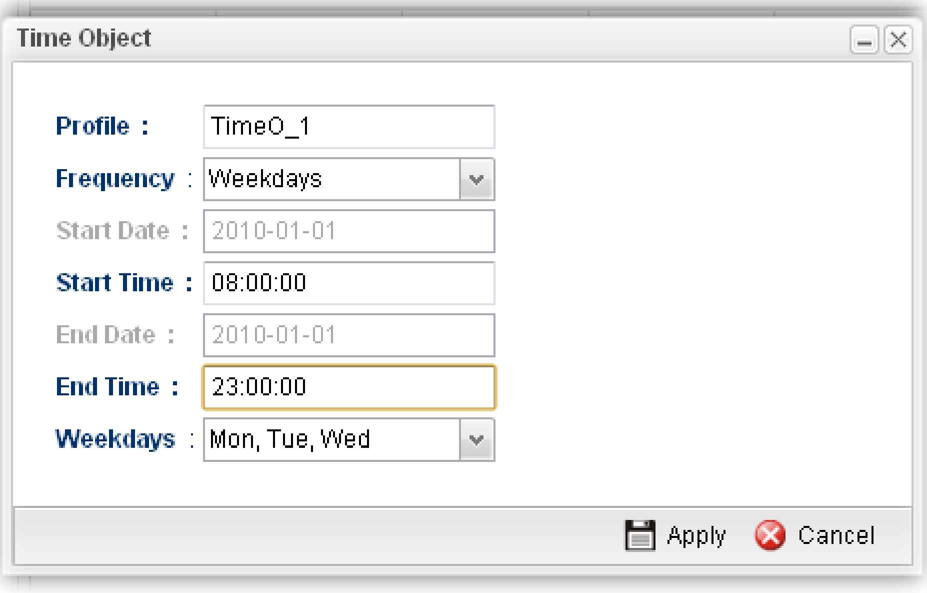
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new time object profile

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



3. The following dialog will appear.



Profile : TimeO_1

Frequency : Weekdays

Start Date : 2010-01-01

Start Time : 08:00:00

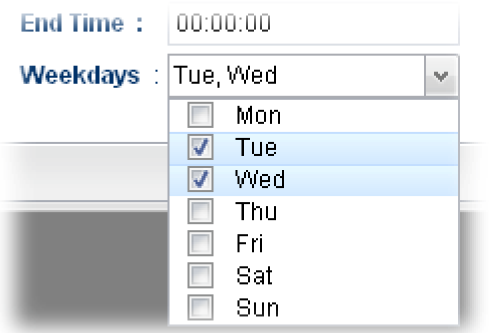
End Date : 2010-01-01

End Time : 23:00:00

Weekdays : Mon, Tue, Wed

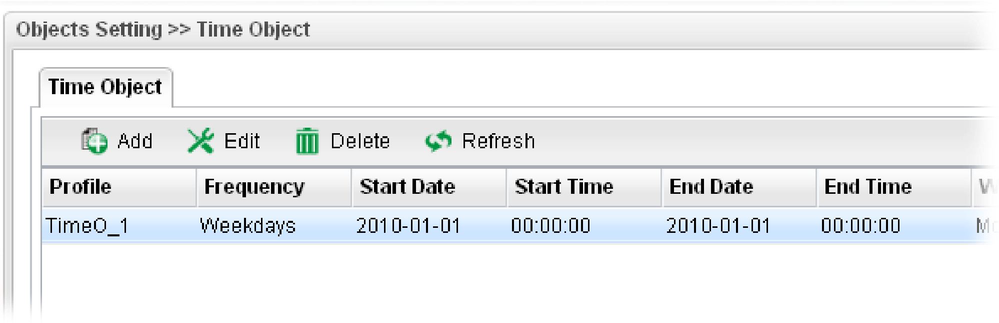
Available parameters are listed as follows:

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

Weekdays	Specify which days in one week should perform the schedule.  End Time : 00:00:00 Weekdays : Tue, Wed ☐ Mon ☑ Tue ☑ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A new Time Object profile has been created.

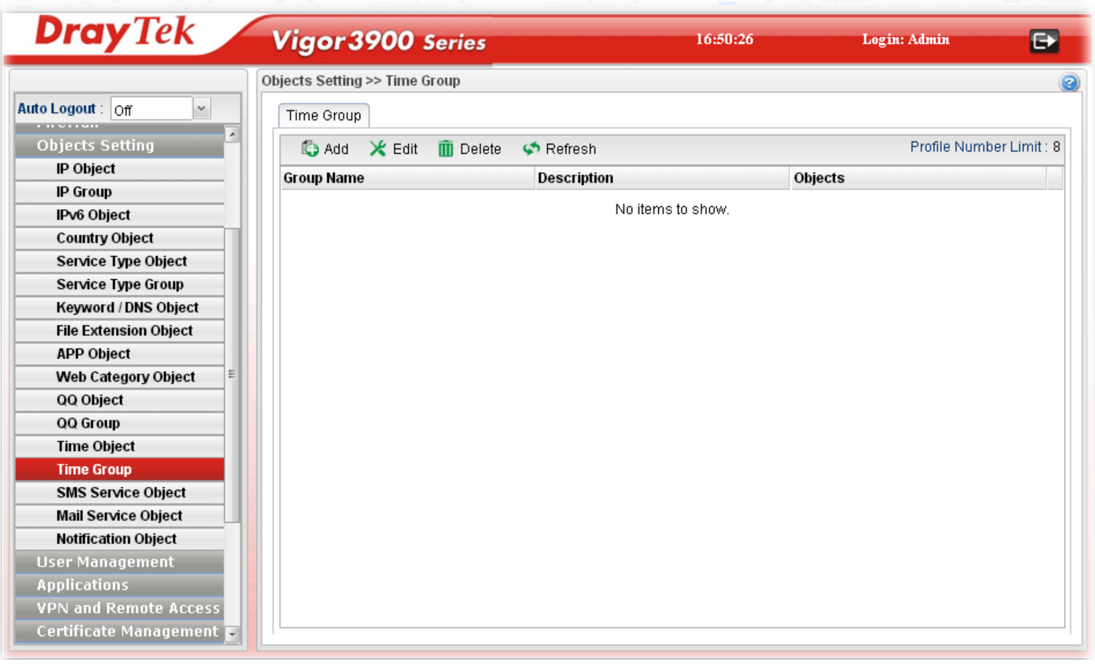


Objects Setting >> Time Object

Profile	Frequency	Start Date	Start Time	End Date	End Time	V
TimeO_1	Weekdays	2010-01-01	00:00:00	2010-01-01	00:00:00	M

4.6.14 Time Group

This page allows you to group several time object profiles.



Profile Number Limit : 8

Group Name	Description	Objects

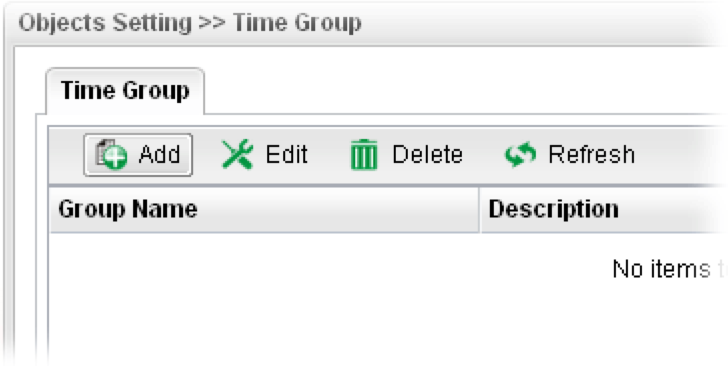
No items to show.

Each item will be explained as follows:

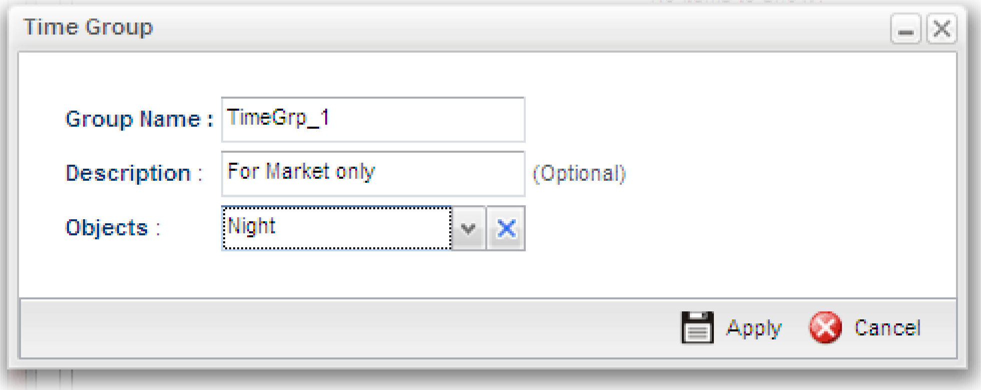
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete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

How to create a new time group profile

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



3. The following dialog will appear.



Group Name : TimeGrp_1

Description : For Market only (Optional)

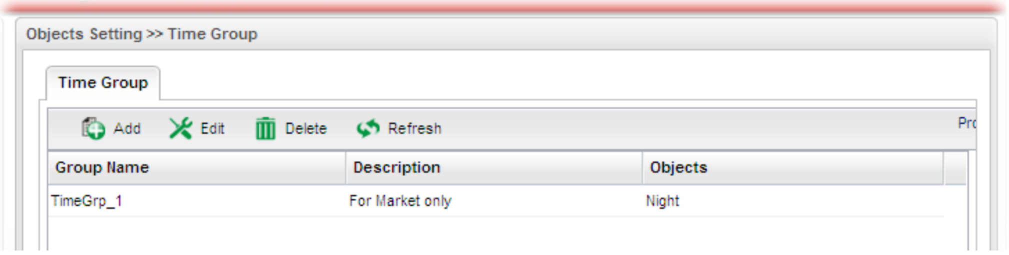
Objects : Night

Available parameters are listed as follows:

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

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

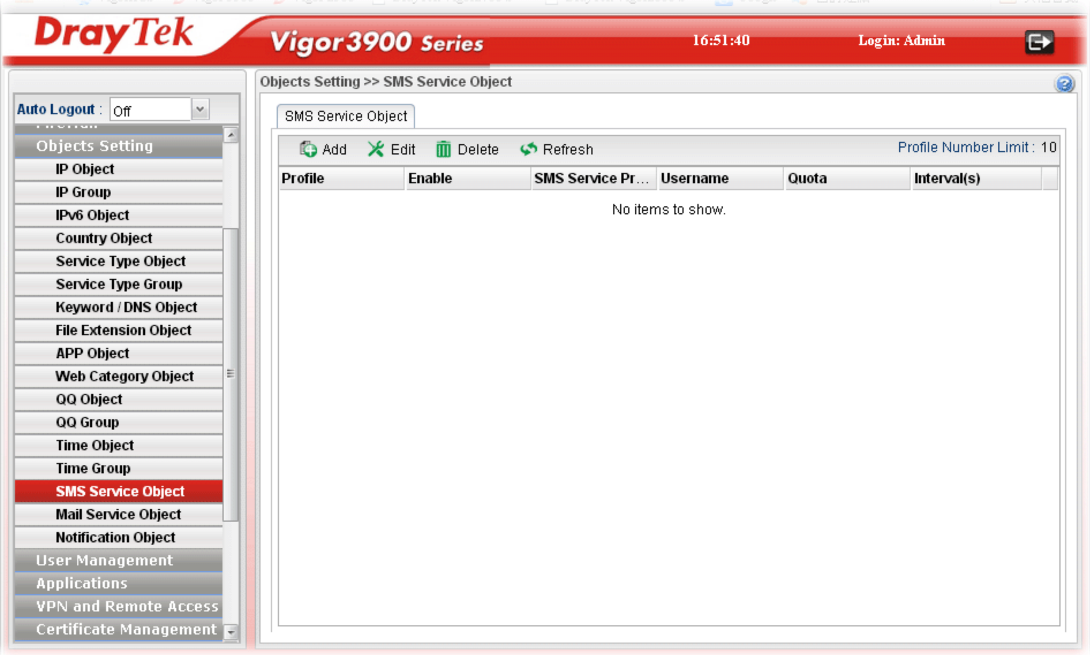
5. A new time group profile has been created.



Group Name	Description	Objects
TimeGrp_1	For Market only	Night

4.6.15 SMS Service Object

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



Profile	Enable	SMS Service Pr...	Username	Quota	Interval(s)

No items to show.

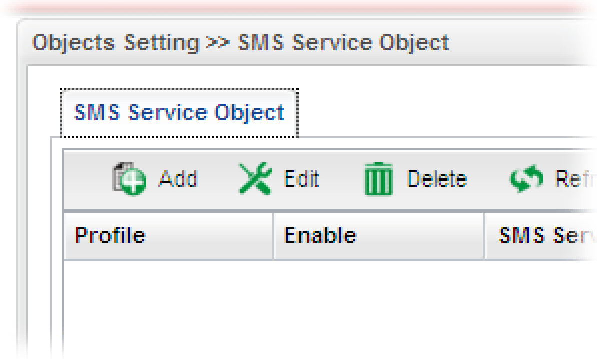
Each item will be explained as follows:

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

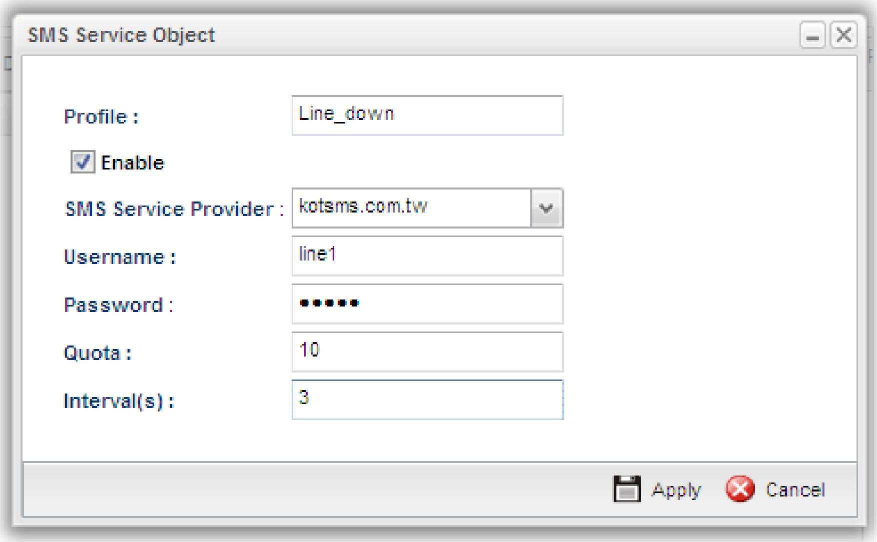
Item	Description
Enable	Display the status of the profile. False means disabled; True means enabled.
SMS Service Provider	Display the service provider which offers SMS service.
Username	Display the user name that the sender can use to register to selected SMS provider.
Quota	Display the number of the credit that you purchase from the service provider
Interval(s)	Display the time interval for sending the SMS.

How to create a new SMS service profile

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



3. The following dialog will appear.



Profile : Line_down

☑ Enable

SMS Service Provider : kotsms.com.tw

Username : line1

Password : •••••

Quota : 10

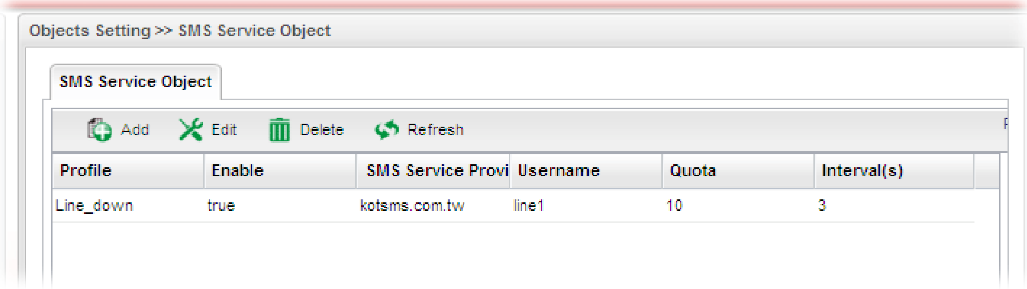
Interval(s) : 3

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such SMS profile. The maximum length of the name you can set is 20 characters.

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

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

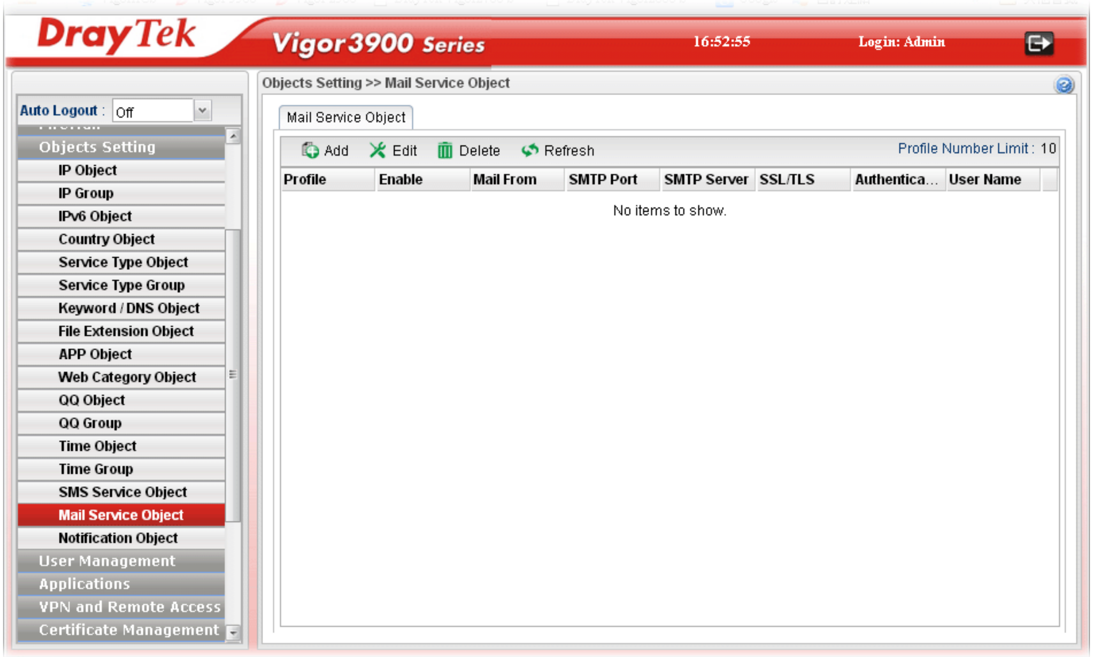


Objects Setting >> SMS Service Object

Profile	Enable	SMS Service Provi	Username	Quota	Interval(s)
Line_down	true	kotsms.com.tw	line1	10	3

4.6.16 Mail Service Object

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



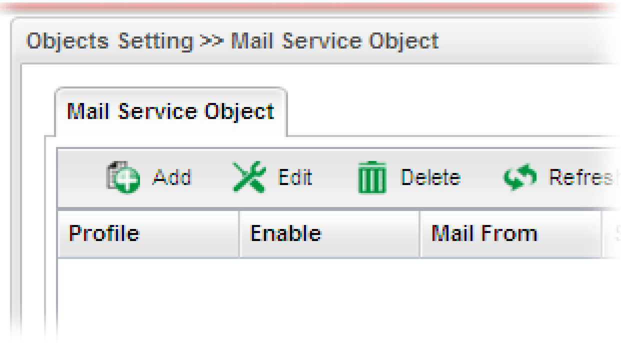
Each item will be explained as follows:

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

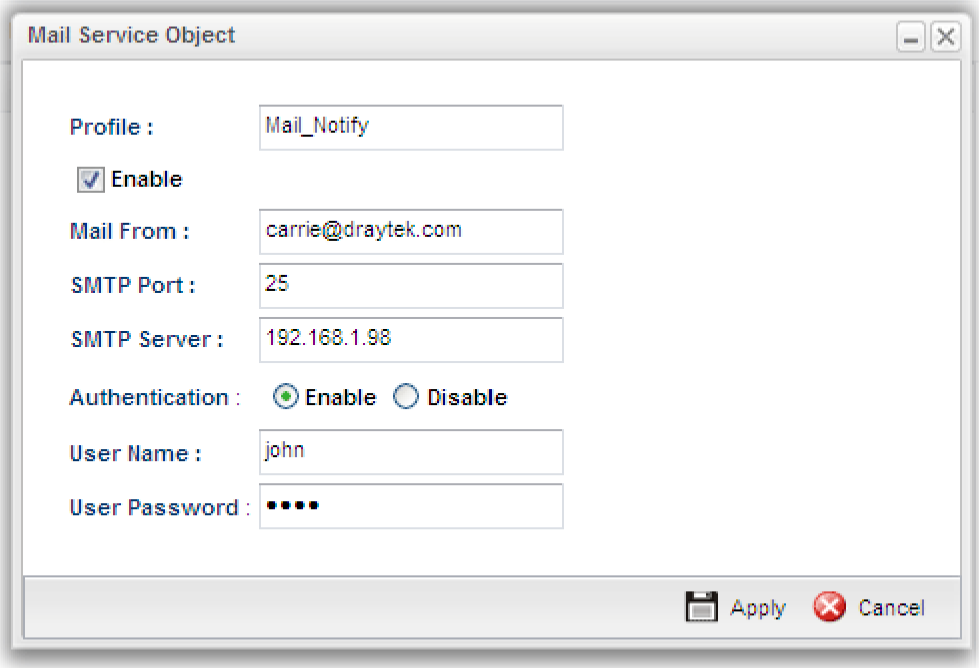
Item	Description
	Disable means such profile will not be authenticated by the server.
User Name	Display the name used for authentication.

How to create a new mail service profile

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



3. The following dialog will appear.


Mail Service Object

Profile : Mail_Notify

☑ Enable

Mail From : carrie@draytek.com

SMTP Port : 25

SMTP Server : 192.168.1.98

Authentication : ● Enable ○ Disable

User Name : john

User Password : ••••

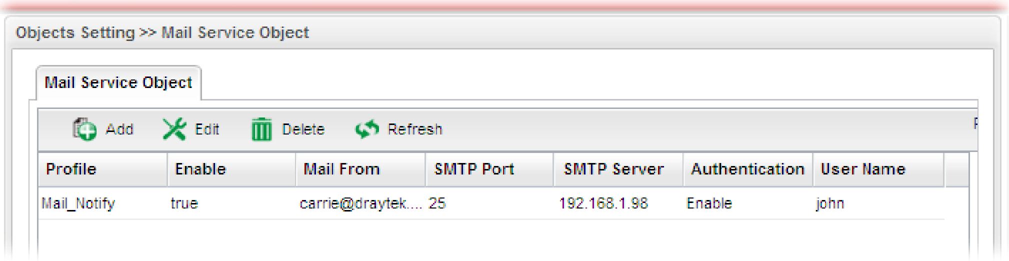
Available parameters are listed as follows:

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

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

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

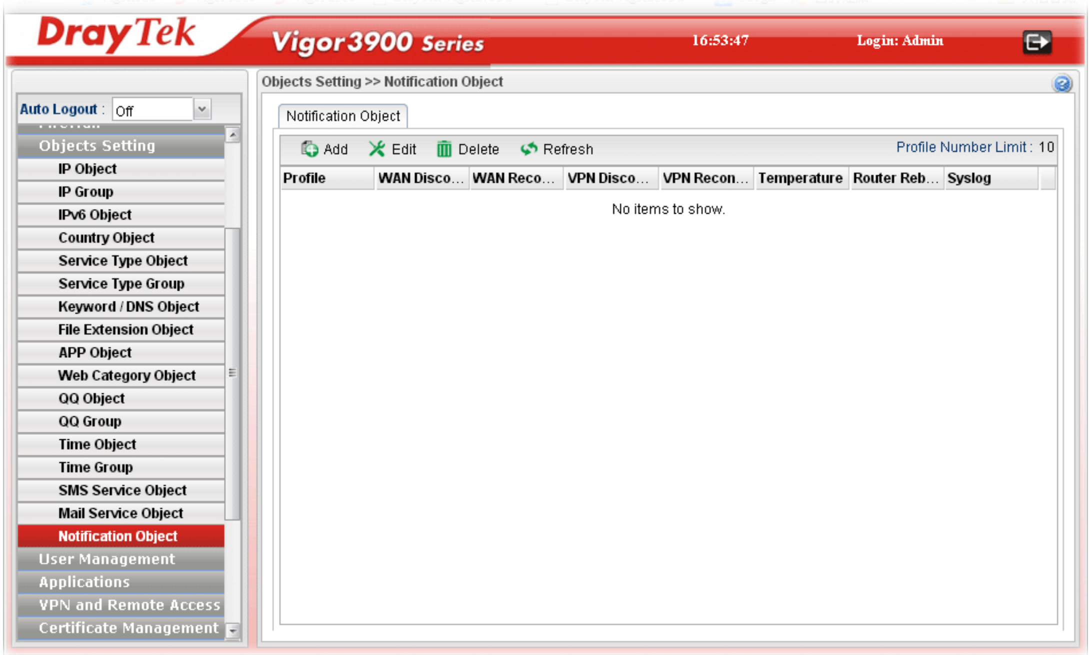
5. A new mail service object profile has been created.



Profile	Enable	Mail From	SMTP Port	SMTP Server	Authentication	User Name
Mail_Notify	true	carrie@draytek....	25	192.168.1.98	Enable	john

4.6.17 Notification Object

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



Objects Setting >> Notification Object

Notification Object

Profile Number Limit : 10

Profile	WAN Disco...	WAN Reco...	VPN Disco...	VPN Recon...	Temperature	Router Reb...	Syslog

No items to show.

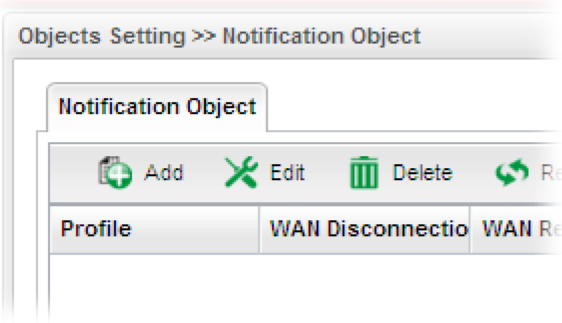
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Profile	Display the name of the profile.
WAN Disconnection	Display if such function is enabled or disabled.
WAN Reconnection	Display if such function is enabled or disabled.
VPN Disconnection	Display if such function is enabled or disabled.
VPN Reconnection	Display if such function is enabled or disabled.
Temperature	Display if such function is enabled or disabled.
Router Reboot	Display if such function is enabled or disabled.

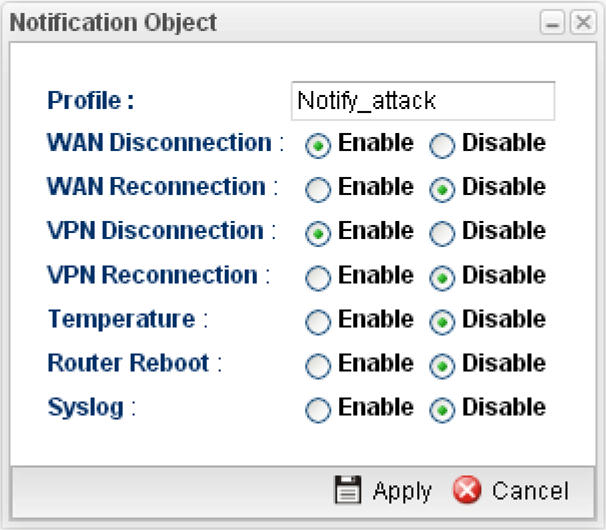
Item	Description
Syslog	Display if such function is enabled or disabled.

How to create a new notification profile

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



3. The following dialog will appear.


Notification Object

Profile : Notify_attack

WAN Disconnection : ● Enable ○ Disable

WAN Reconnection : ○ Enable ● Disable

VPN Disconnection : ● Enable ○ Disable

VPN Reconnection : ○ Enable ● Disable

Temperature : ○ Enable ● Disable

Router Reboot : ○ Enable ● Disable

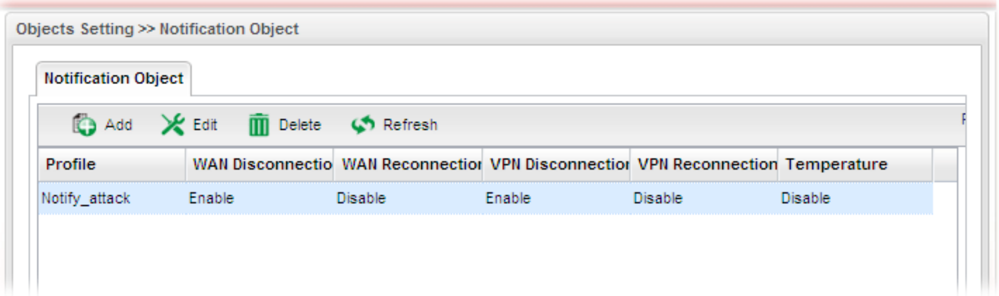
Syslog : ○ Enable ● Disable

Available parameters are listed as follows:

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

VPN Reconnection	**Enable** - When reconnection happened to a VPN tunnel, the router system will send the alert message to the recipient.
Temperature	**Enable** - When the temperature is out of range, the router system will send the alert message to the recipient.
Router Reboot	**Enable** - When the router reboots, the router system will send the alert message to the recipient.
Syslog	**Enable** – Such notification will be recorded in Syslog.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

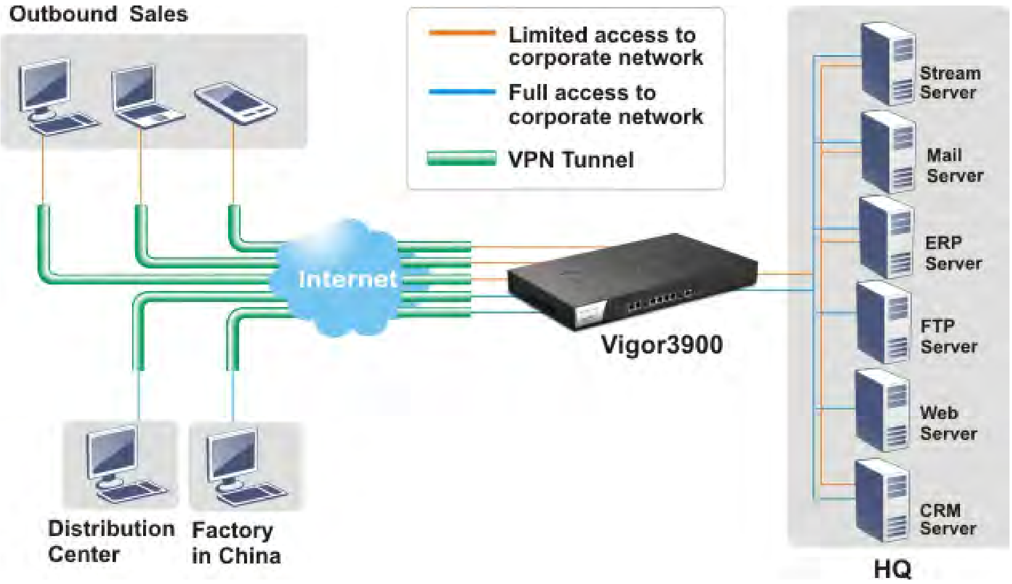
4. Enter all the settings and click **Apply**.
5. A new notification object profile has been created.



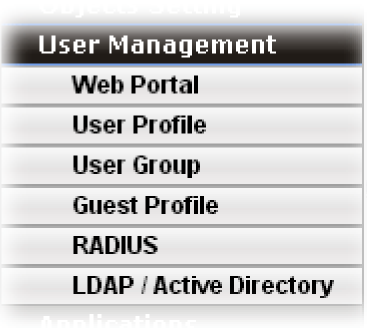
Profile	WAN Disconnectio	WAN Reconnectior	VPN Disconnectior	VPN Reconnection	Temperature
Notify_attack	Enable	Disable	Enable	Disable	Disable

4.7 User Management

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



Below shows the menu items for User Management:



4.7.1 Web Portal

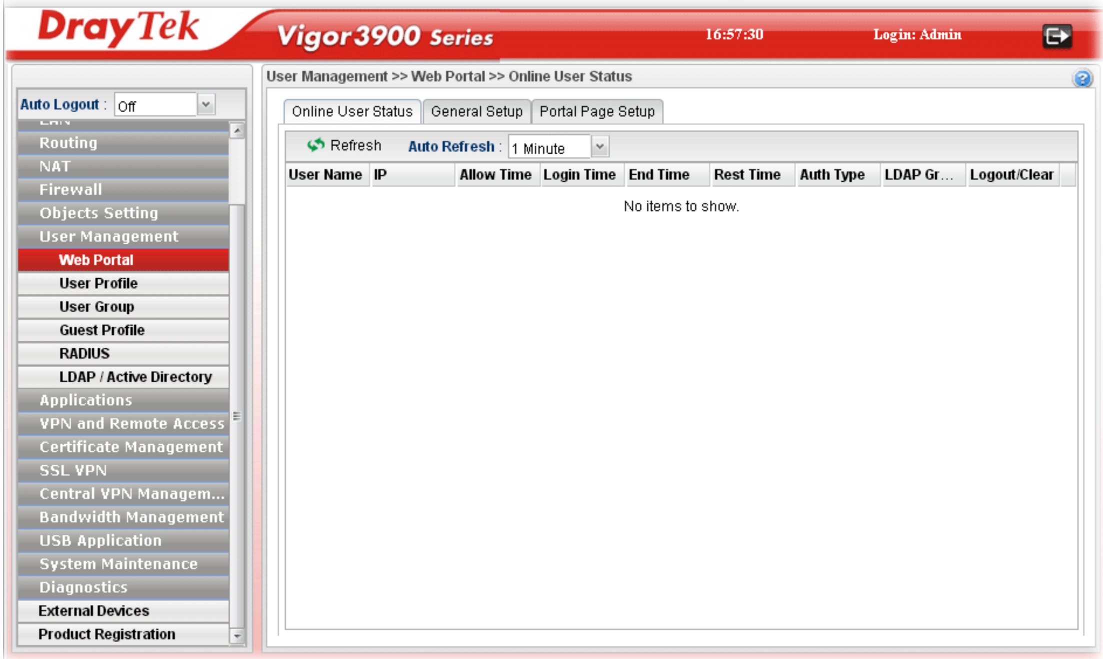
Web Portal is a gateway which organizes the network access of LAN hosts. The identity of LAN host can be recognized by web portal mechanism and then be managed for functions like firewall or load balance.

This page can determine the general rule for the users controlled by User Management. The mode selected in this page will influence the contents of the filter rule(s) applied to every user.

4.7.1.1 Online User Status

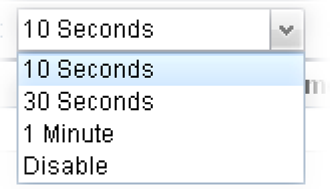
The **Online User Status** is a monitoring tool which only works after you choose **HTTP** or **HTTPS** as the **Mode** setting on **General Setup** page of **User Management>>Web Portal**.

Refer to section 4.7.1.2 General Setup to get more detailed information of setting web portal.



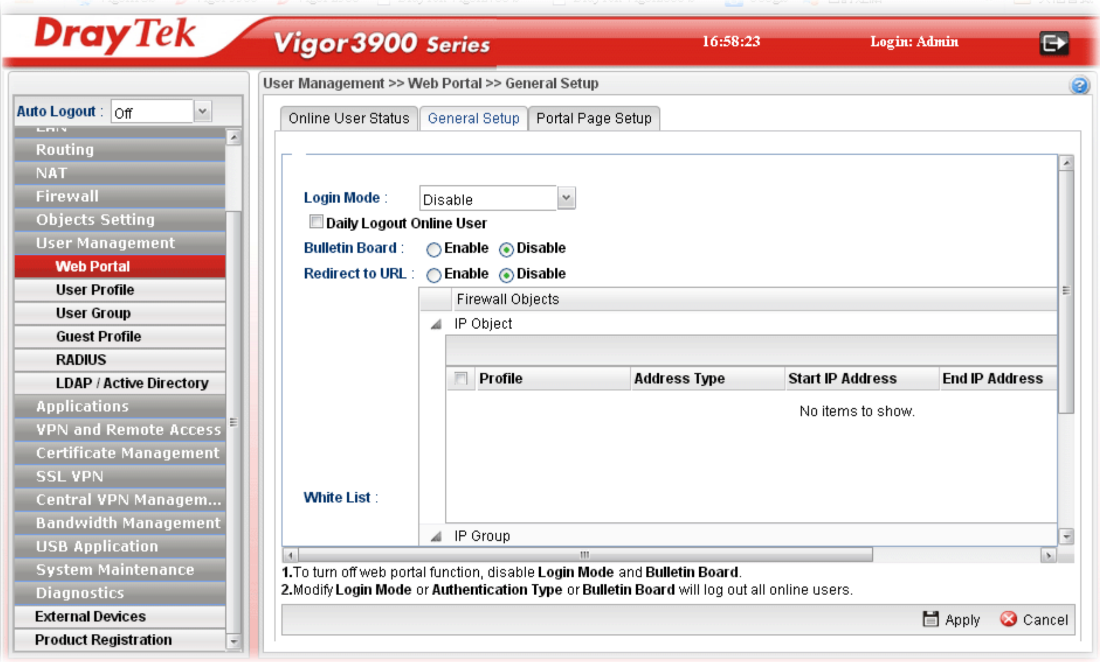
Available parameters will be explained as follows:

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

Item	Description
	 10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
User Name	Display the name information for the user who logs into the WUI of Vigor3900.
IP	Display the IP address of the user who logs into the WUI of Vigor3900.
Allow Time	Display the total network connection time allowed for the log-in user.
Start Time	Display the starting time of the network connection.
End Time	Display the ending time of the network connection.
Rest Time	Display the rest time of the network connection.
Auth Type	Display the authentication type (local, RADIUS, LDAP, Login Disable, Guest) used by such user.
LDAP Group	Display the LDAP group used by such user.
Logout/Clear	It is a button which is used to disconnect the connection manually.

4.7.1.2 General Setup

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



Login Mode : Disable

□ Daily Logout Online User

Bulletin Board : ○ Enable ● Disable

Redirect to URL : ○ Enable ● Disable

White List :

Firewall Objects

IP Object

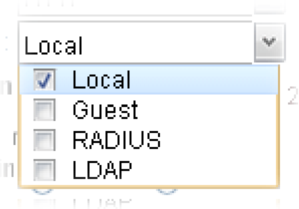
□	Profile	Address Type	Start IP Address	End IP Address

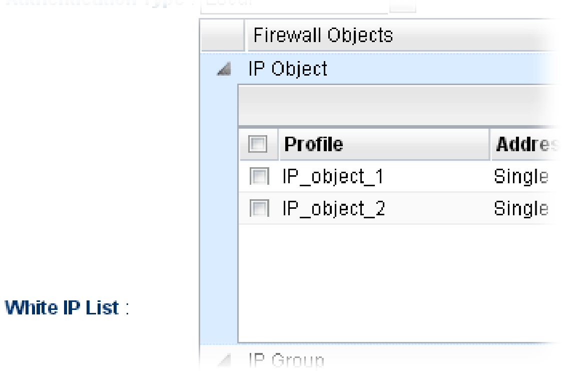
No items to show.

IP Group

1.To turn off web portal function, disable **Login Mode** and **Bulletin Board**.
2.Modify **Login Mode** or **Authentication Type** or **Bulletin Board** will log out all online users.

Available parameters will be explained as follows:

Item	Description
Login Mode	There are several login modes offered here for you to choose. **Disable** – The web portal function is disabled. **HTTP/HTTPS-** If you choose such mode, the user can access into Vigor router by HTTP or HTTPS.
Authentication Type	This option is available when the Login Mode is set as HTTP or HTTPS. Note that the authentication sequence adopted by the system will be Local first, Guest second, RADIUS third and LDAP the last.  **LDAP Profiles -** It is available when **LDAP** is selected as **Authentication Type**. You have to specify one profile (defined in User Management>>LDAP/Active Directory) from the drop down list for LDAP authentication.
Daily Logout Online User	Check the box to force the online user logging out the web user interface of Vigor router everyday.
Time to Logout	It is available when **Daily Logout Online User** is enabled. Type that time setting (HH:MM) for the router to force online user leaving Vigor router.
Also Recharge Time Quota	It is available when **Daily Logout Online User** is enabled. The time quota of all local users will be recharged whenever Daily Logout Online User is executed.
Bulletin Board	**Disable –** The function of Bulletin Board is disabled. **Enable –** The function of Bulleting Board is enabled. The message on the Bulleting Board will be displayed on the screen when the user logs into the web user interface of Vigor router. **Show Bulletin in Login Page –** It is available when **Bulletin Board** is enabled. It is used to determine showing bulletin in web portal login page or not.
Redirect to URL	**Disable –** The function of URL redirection is disabled. **Enable** – Click it to force users to visit the specified web page after passing through web portal. Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit. **URL** – Type the URL of specified web page for redirection.
White List	Select the source IP objects/groups that are ignored by web portal function.

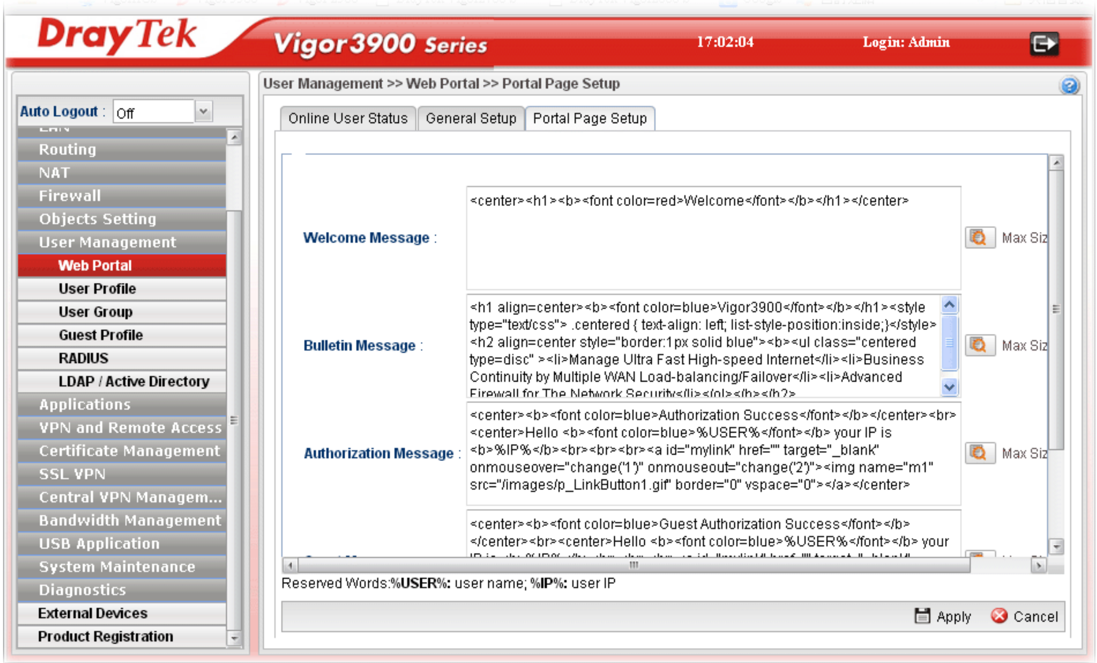
Item	Description
	 White IP List : Firewall Objects IP Object IP Group □ Profile | Addre □ IP_object_1 | Single □ IP_object_2 | Single
LDAP Profiles	It is available when **LDAP** is selected as **Authentication Type**. You have to specify one profile from the drop down list for authentication.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

4.7.1.3 Portal Page Setup

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

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



User Management >> Web Portal >> Portal Page Setup

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

Bulletin Message : `<h1 align=center><b><font color=blue>Vigor3900</font></b></h1><style type="text/css"> .centered { text-align: left; list-style-position:inside;}</style><h2 align=center style="border:1px solid blue"><b><ul class="centered type=disc" ><li>Manage Ultra Fast High-speed Internet</li><li>Business Continuity by Multiple WAN Load-balancing/Failover</li><li>Advanced Firewall for The Network Security</li></ol></b></h2>`

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

<a id="mylink" href="" target="_blank" onmouseover="change('1')" onmouseout="change('2')"><img name="m1" src="/images/p_LinkButton1.gif" border="0" vspace="0"></a></center>`

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

Reserved Words:%**USER%:** user name; %**IP%:** user IP

Available parameters will be explained as follows:

Item	Description
Welcome Message	Type words or sentences here. The message will be displayed on the top of the login page.
Bulletin Message	The bulletin message is shown at bottom of login page or authorization page. In login page, it can be disabled by Show Bulletin In Login Page.
Authorization Message	The welcome message is shown in authorization page which is the page after a user passing the authentication successfully.
Guest Message	The welcome message is shown in authorization page which is the page after a guest passing the authentication successfully.
Login Page Preview	Click it to have a preview of login page (including welcome message, and bulletin message).
Reset All to Default	Reset the above message fields to default settings. Check the box and then press **Apply**.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

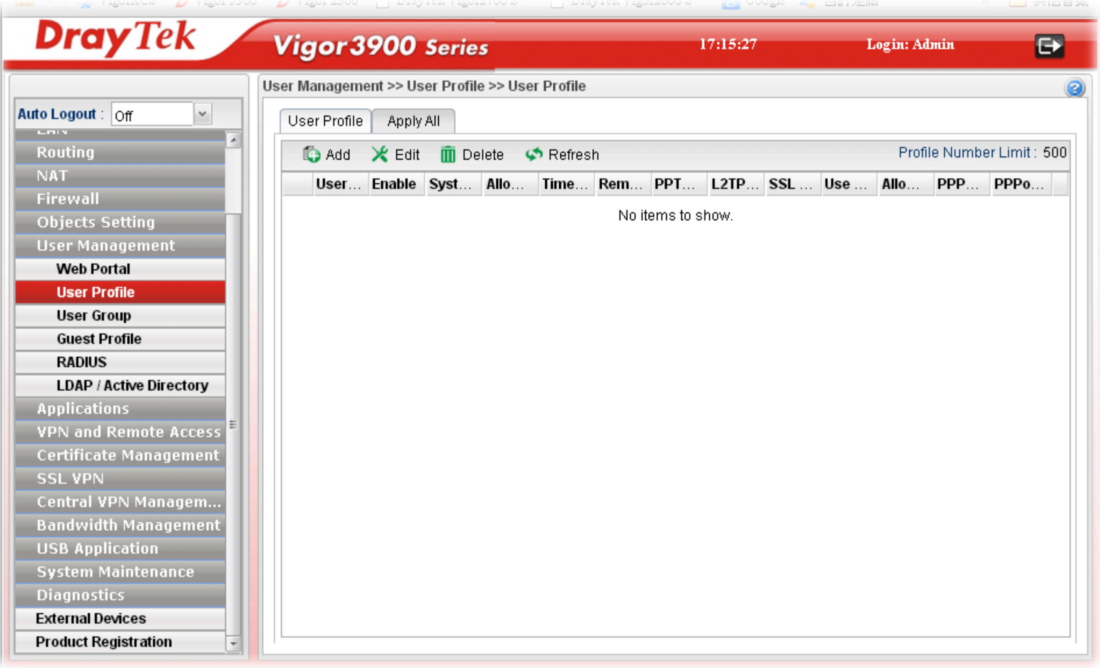
After finished the above settings, click **Apply** to save the configuration.

4.7.2 User Profile

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

4.7.2.1 User Profile

User profile is used to configure different authorities, including web portal, VPN dial-in, PPPoE server, System Administration, etc., for different users.



User Management >> User Profile >> User Profile

Auto Logout : Off

Profile Number Limit : 500

No items to show.

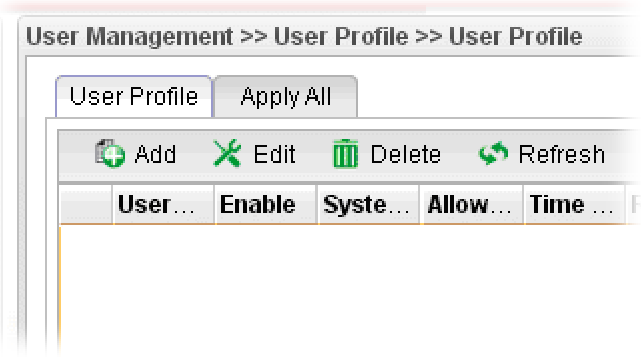
Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number of the user profiles to be created.
Username	Display the name of the user.
Enable	Display the status of the profile. False means disabled; True means enabled.
System User	Display the status of the System User. False means disabled; True means enabled.
Allow Web Portal Login	Display the status (Enable/Disable) of the account usage for

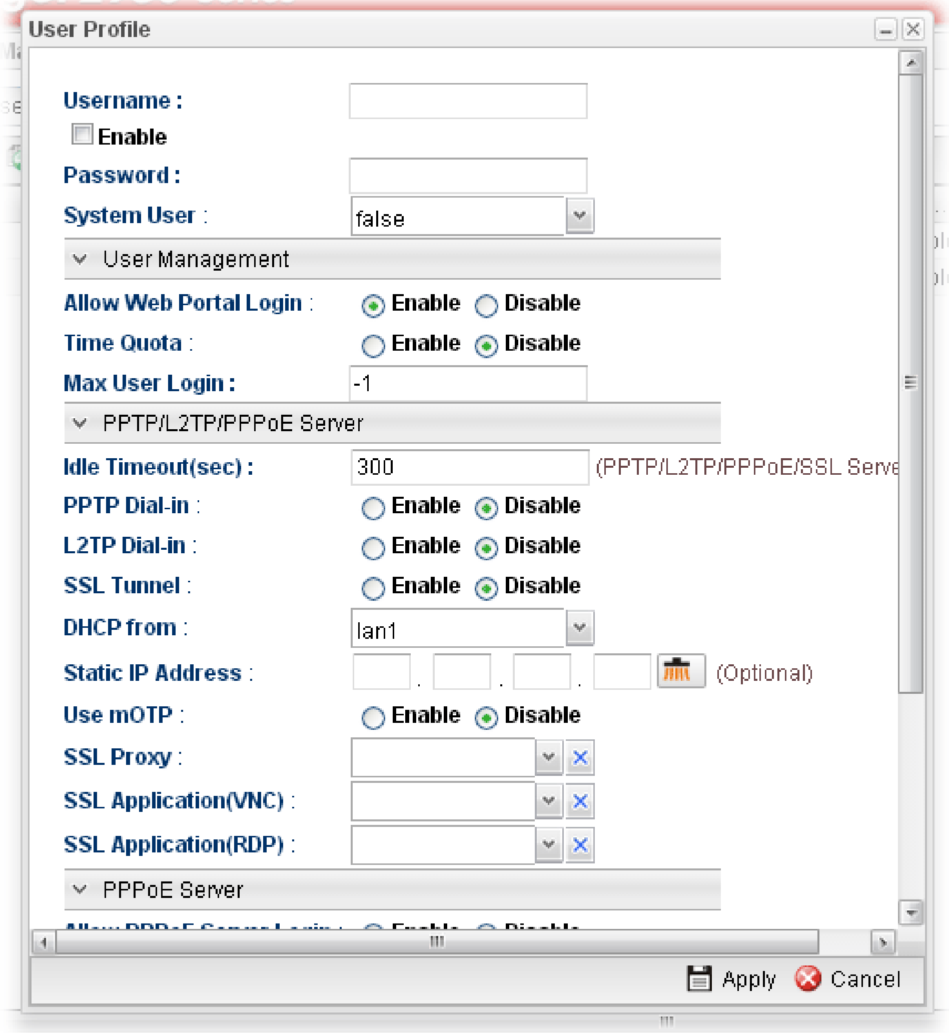
Item	Description
	web portal login.
Time Quota	Display the status (Enable/Disable) of time quota mechanism for web portal use.
Remaining Time	Display the remaining time for the user profile. **Recharge** – It can recharge the remaining time quota of the user on-the-fly (will not log out online users)**.**
PPTP Dial-in	Display the status of PPTP connection for such user profile.
L2TP Dial-in	Display the status of L2TP connection for such user profile.
SSL Tunnel	Display if SSL Tunnel is activated (enable or disable) or not.
Use mOTP	Display if mOTP is activated (enable or disable) or not.
Allow PPPoE Server Login	Display the status of PPPoE connection for such user profile. (enable or disable)
PPPoE Time Quota(min)	Display the current PPPoE time quota usage portion for such user.
PPPoE Traffic Quota(MB)	Display the current PPPoE traffic quota usage portion for such user.

How to create a new User Profile

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



3. The following dialog will appear.



User Profile

Username :

□ Enable

Password :

System User : false

User Management

Allow Web Portal Login : ● Enable ○ Disable

Time Quota : ○ Enable ● Disable

Max User Login : -1

PPTP/L2TP/PPPoE Server

Idle Timeout(sec) : 300 (PPTP/L2TP/PPPoE/SSL Serve

PPTP Dial-in : ○ Enable ● Disable

L2TP Dial-in : ○ Enable ● Disable

SSL Tunnel : ○ Enable ● Disable

DHCP from : lan1

Static IP Address : . . . (Optional)

Use mOTP : ○ Enable ● Disable

SSL Proxy :

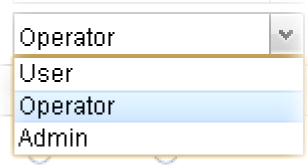
SSL Application(VNC) :

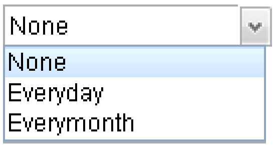
SSL Application(RDP) :

PPPoE Server

Available parameters are listed as follows:

Item	Description
Username	Type a name for such user profile (e.g., *LAN_User_Group_1*, *WLAN_User_Group_A*, *WLAN_User_Group_B*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the Username specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Enable	Check this box to enable such profile.
Password	Type a password for such profile (e.g., *lug123*, *wug123,wug456*, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.

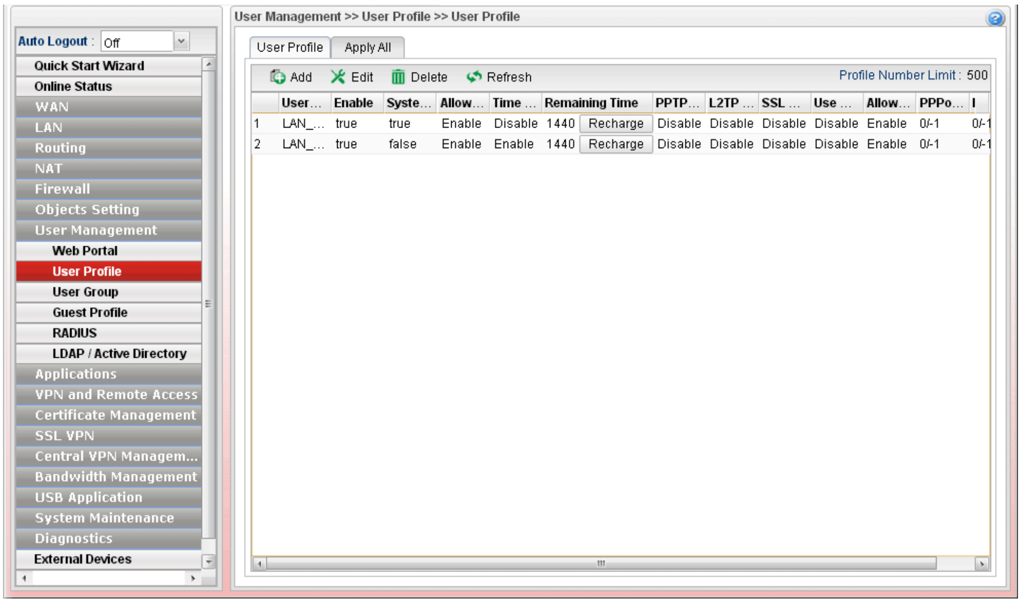
System User	Only the user profile with privilege level has the right to operate the function of the router as the administrator of the router. **False –** Choose it to disable the function of System User. Such user profile does not have the right to operate the router’s function. **True –** Choose it to enable the function of System User. **Privilege Level –** If true is selected for **System User**, you have to specify the privilege level (User/Operator/Admin) for such profile.  **Admin** has the greatest authority for router operation; **User** has the smallest authority for router operation.
User Management	
Allow Web Portal Login	**Enable** – Click it to enable web portal login with such profile. **Disable** – Click it to disable the option.
Time Quota	**Enable** – Click it to enable time quota function. **Disable** – Click it to disable the function. **Set Time Quota (min)** – Type the time value. **Remaining Time** – Display the remaining time for the user profile.
Max User Login	It means the maximum online number of clients logging with this profile. The range is from 1 to 255. -1 means not limit; 0 means No access.
PPTP/L2TP/PPPoE Server	
Idle Timeout (sec)	If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.
PPTP Dial-in / L2TP Dial-in / **SSL Tunnel**	Click **Enable** to make network connection through PPTP/L2TP/SSL Tunnel protocol for users who access into Internet via such profile.
DHCP from	Choose a LAN profile for DHCP server IP dispatching. Remote clients using this profile to do PPTP/L2TP dial-in will be assigned IP addresses according to this DHCP pool.
Static IP Address	Type an IP address for such user profile which accesses Internet with PPTP/L2TP connection.

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. To clear the selected one, click ☒ to remove current object selections.
SSL Application (VNC)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (VNC) for applying into this profile. To clear the selected one, click ☒ to remove current object selections.
SSL Application (RDP)	It is available when **System User** is set with **false**. Choose one of the SSL Application profiles (RDP) for applying into this profile. To clear the selected one, click ☒ to remove current object selections.
PPPoE Server	
Allow PPPoE Server Login	Click **Enable** to activate related PPPoE configuration.
Quota Reset Frequency	It is used to configure the cycle time for PPPoE quota. Note that each time when the quota is reset, the value of Current Time Used/Current Traffic Quota will be reset to initial situation (0). **Everyday** – The quota for PPPoE will be reset every day. **Everymonth** – The quota for PPPoE will be reset every month.  None None Everyday Everymonth
Time Quota (min)	Type a time quota for PPPoE connection.
Current Time Used (min)	Display the cumulative amount of time that the user used. **Reset -** Click it to reset the setting to default value (0).
Traffic Quota(MB)	It is used to set the maximum traffic (MB) for such user profile.
Current Traffic Quota (MB)	Display the cumulative amount of data traffic that the user used. **Reset -** Click it to reset the setting to default value (0).

MAC Binding	Specify a MAC address which is limited and used for such PPPoE account. **Enable –** Click it to enable the function. **MAC Address** – If MAC Binding is enabled, simply type the MAC address of the router in this field.
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.



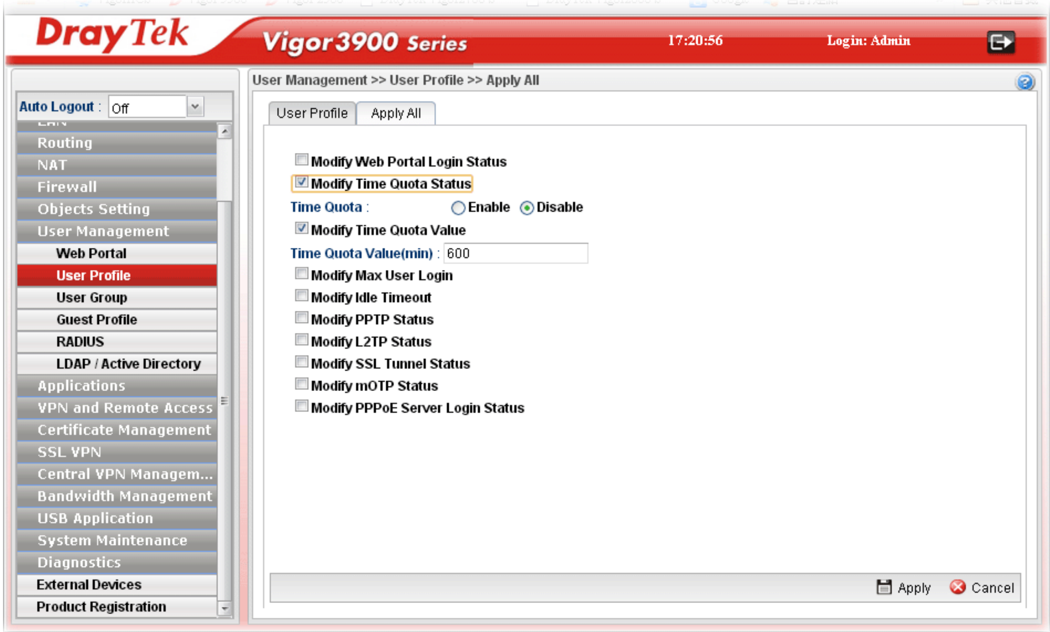
Profile Number Limit : 500

	User...	Enable	Syste...	Allow...	Time ...	Remaining Time		PPTP...	L2TP ...	SSL ...	Use ...	Allow...	PPPo...	I
1	LAN_...	true	true	Enable	Disable	1440	Recharge	Disable	Disable	Disable	Disable	Enable	0/-1	0/-1
2	LAN_...	true	false	Enable	Enable	1440	Recharge	Disable	Disable	Disable	Disable	Enable	0/-1	0/-1

4.7.2.2 Apply All

This page allows you to modify many options for **ALL** user profiles in one apply operation. It is useful for administrator to edit the options of all users without opening profile one by one.

You can click **Apply** to save the settings and apply all of the modifications to all user profiles.



User Management >> User Profile >> Apply All

□ Modify Web Portal Login Status

☑ Modify Time Quota Status

Time Quota : ○ Enable ● Disable

☑ Modify Time Quota Value

Time Quota Value(min) : 600

□ Modify Max User Login

□ Modify Idle Timeout

□ Modify PPTP Status

□ Modify L2TP Status

□ Modify SSL Tunnel Status

□ Modify mOTP Status

□ Modify PPPoE Server Login Status

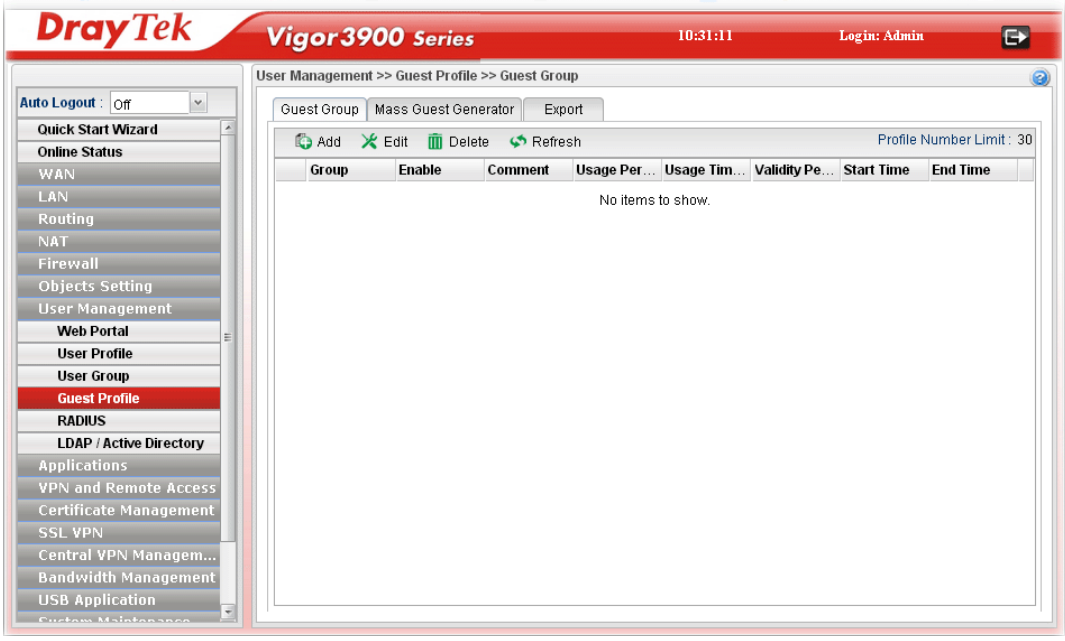
Available parameters are listed as follows:

Item	Description
Modify Web Portal Login Status	Check the box to configure detailed setting. **Enable –** Click it to enable the web portal login function for remote client.
Modify Time Quota Status	Check the box to configure detailed setting. **Enable –** Click it to enable the time quota function for all user profiles.
Modify Time Quota Value	Check the box to configure detailed setting. You have to check this box and type the time quota value in **Time Quota Value(min)**.
Modify Max User Login	-1 means not limit; 0 means No access.
Modify Idle Timeout	If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.
Modify PPTP Status /Modify L2TP Status **/Modify SSL Tunnel Status**	Check the box to configure detailed setting. **Enable –** Click it to enable the PPTP/L2TP/SSL tunnel network connection all user profiles.
Modify mOTP Status	Check the box to configure detailed setting. **Enable –** Click it to enable the moTP function all user profiles.
Modify PPPoE Server Login Status	Check the box to configure detailed setting. **Enable –** Click it to enable the PPPoE authentication function all user profiles.

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

4.7.3 User Group

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



Group	Enable	Comment	Usage Per...	Usage Tim...	Validity Pe...	Start Time	End Time

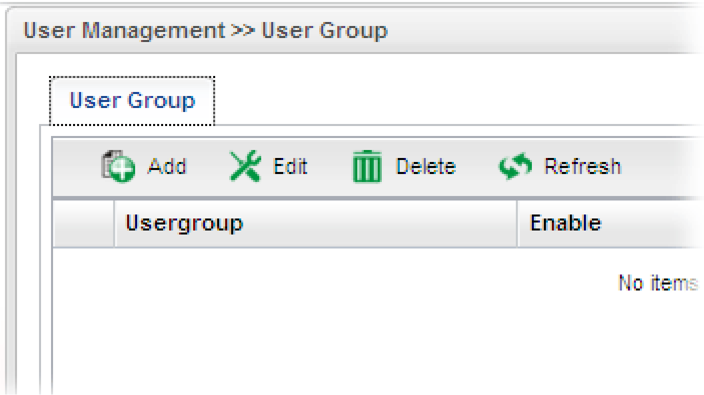
No items to show.

Each item will be explained as follows:

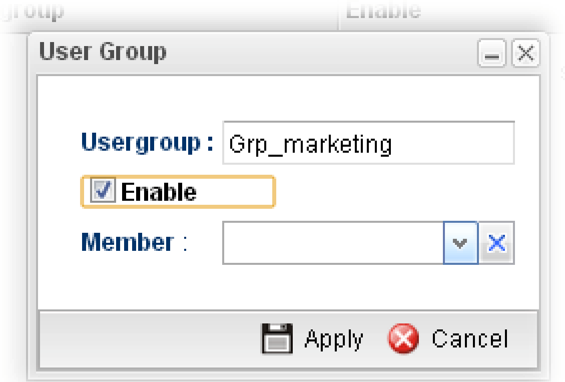
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (30) of the object profiles to be created.
Usergroup	Display the name of the user group.
Enable	Display the status of the profile. False means disabled; True means enabled.
Member	Display the user profiles under such group.

How to create a new User Group Profile

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



3. The following dialog will appear.



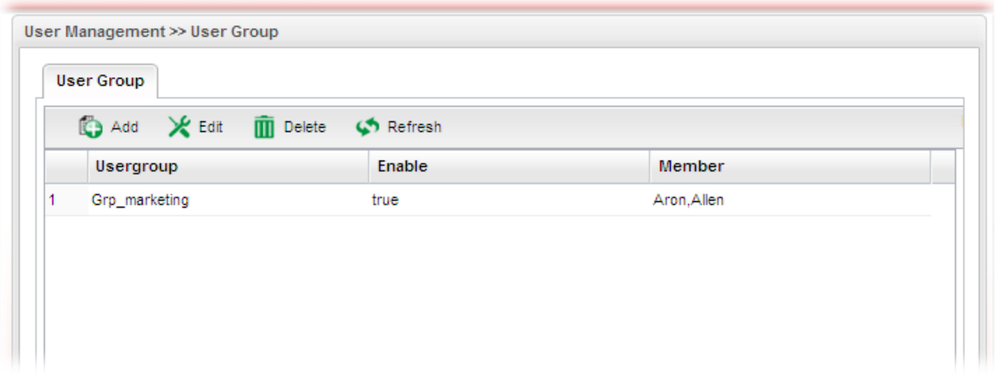
Usergroup : Grp_marketing

☑ Enable

Available parameters are listed as follows:

Item	Description
Usergroup	Type the name of such profile.
Enable	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group. To clear the selected one, click ☒ to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

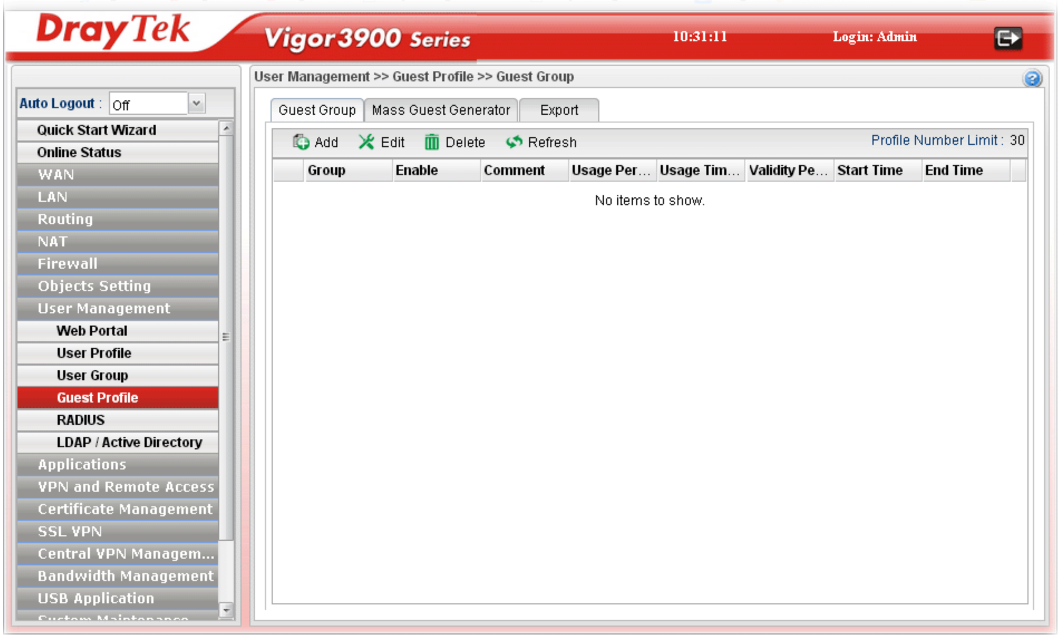


	Usergroup	Enable	Member
1	Grp_marketing	true	Aron,Allen

4.7.4 Guest Profile

Guest Profile allows the users to access Internet within validity period and limit the user accessing into the specified URL configured by web portal.

4.7.4.1 Guest Group



Group	Enable	Comment	Usage Per...	Usage Tim...	Validity Pe...	Start Time	End Time

No items to show.

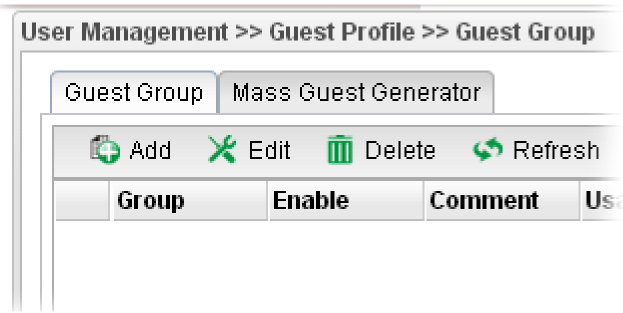
Available parameters are listed as follows:

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

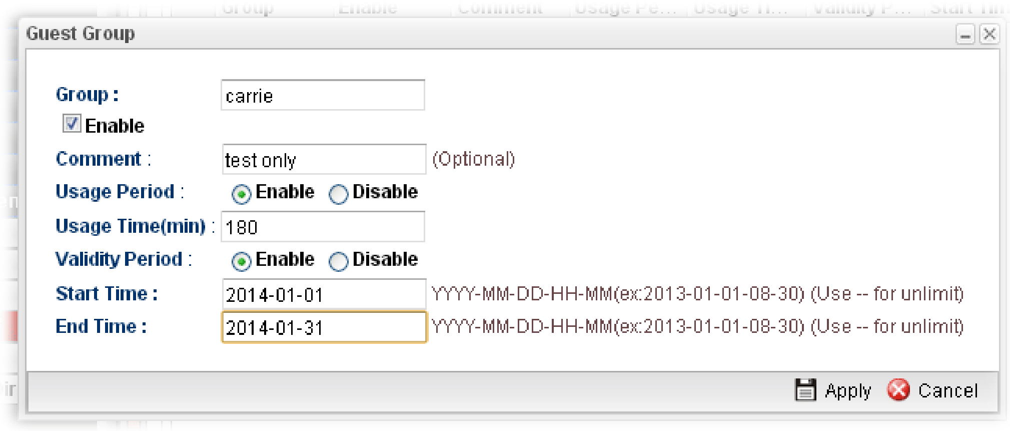
Item	Description
Profile Number Limit	Display the total number (30) of the profiles to be created.
Group	Display the name of the guest group.
Enable	Check this box to enable such profile.
Comment	Display the description for the profile.
Usage Period	Display the status (Enable/Disable) for the function of usage time.
Usage Time(min)	Display the usage time for the guest accessing into Internet each time.
Validity Period	Display the valid period for the guest accessing into Internet.
Start Time/ End Time	Display the detailed time setting (starting and ending).

How to create a new Guest Group Profile

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



3. The following dialog will appear.



Group : carrie
☑ Enable
Comment : test only (Optional)
Usage Period : ● Enable ○ Disable
Usage Time(min) : 180
Validity Period : ● Enable ○ Disable
Start Time : 2014-01-01 YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)
End Time : 2014-01-31 YYYY-MM-DD-HH-MM(ex:2013-01-01-08-30) (Use -- for unlimit)

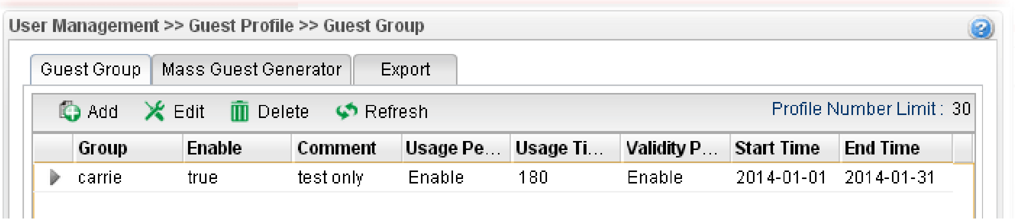
Available parameters are listed as follows:

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

Usage Period	It determines the usage time for the guest accessing into Internet each time. Click **Enable** to enable such option. **Usage Time(min)-** Determines the connection time allowed for accessing Internet every time. The default setting is 180 minutes. When the time is up, the user will be forced to exit Internet.
Validity Period	Validity Period determines the effective time for the user account/guest. Within the period of the validity, the user/guest can access into Internet whenever he wants. **Start Time/End Time** – Specify the valid period by typing the time with the format of YYYY-MM-DD-HH-MM. When it is set with "--", that means such time setting is no limit.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

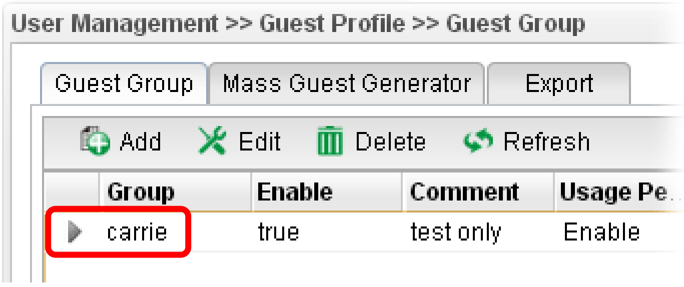
5. A new guest profile has been created.



User Management >> Guest Profile >> Guest Group

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

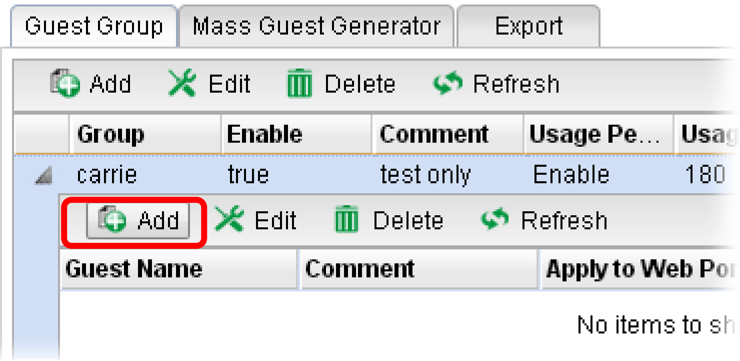
6. You can create several guest names by clicking ▶ on the left side of the selected guest group profile. A setting page will appear for you to add new guest list.



User Management >> Guest Profile >> Guest Group

	Group	Enable	Comment	Usage Pe...
▶	carrie	true	test only	Enable

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

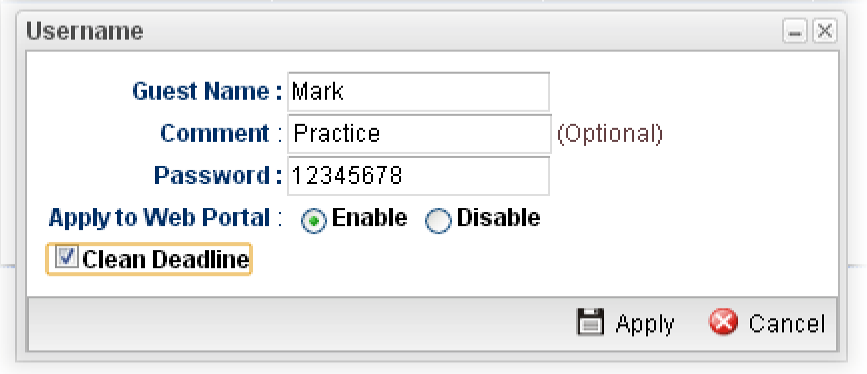


	Group	Enable	Comment	Usage Pe...	Usag
◢	carrie	true	test only	Enable	180

Guest Name	Comment	Apply to Web Po

No items to sh

8. The following page for configuration will appear.



Username

Guest Name : Mark

Comment : Practice (Optional)

Password : 12345678

Apply to Web Portal : ● Enable ○ Disable

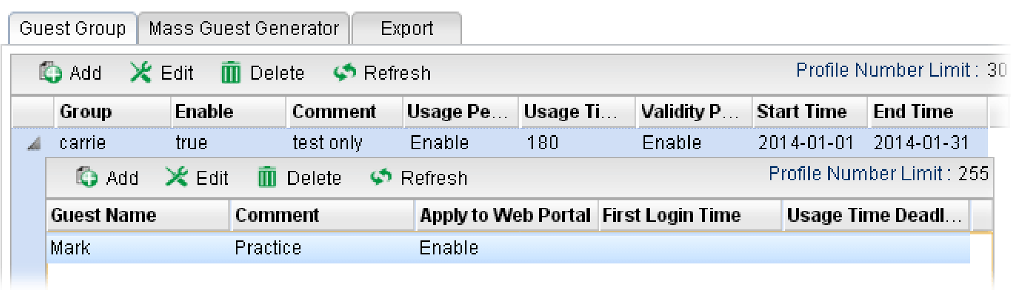
☑ Clean Deadline

Available parameters are listed as follows:

Item	Description
Guest Name	Type the name of the guest under the guest group.
Comment	Give a brief description for the guest.
Apply to Web Portal	**Enable** – Click it to make such profile being applied to web portal. Disable – Click it to disable the option.
Clean Deadline	The guest profile can be unlocked to be used by other users.

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

10. A new guest has been added under the Guest Group (named Carrie in this case).



Profile Number Limit : 30

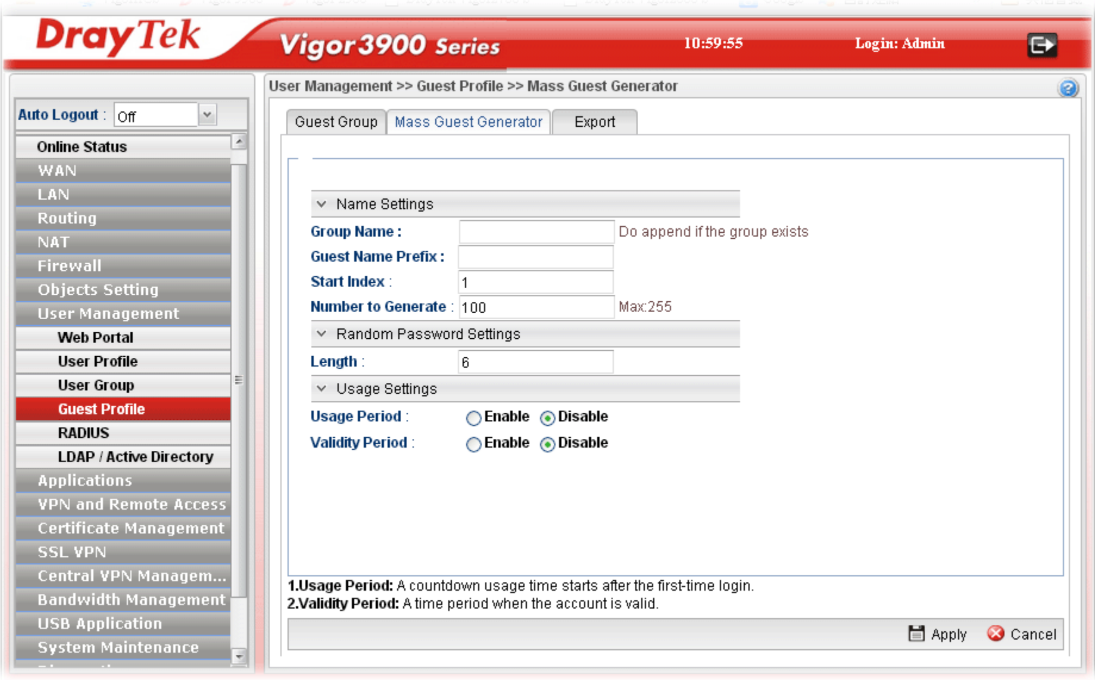
Group	Enable	Comment	Usage Pe...	Usage Ti...	Validity P...	Start Time	End Time
carrie	true	test only	Enable	180	Enable	2014-01-01	2014-01-31

Profile Number Limit : 255

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

4.7.4.2 Mass Guest Generator

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



User Management >> Guest Profile >> Mass Guest Generator

Name Settings

Group Name : Do append if the group exists

Guest Name Prefix :

Start Index : 1

Number to Generate : 100 Max:255

Random Password Settings

Length : 6

Usage Settings

Usage Period : ○ Enable ● Disable

Validity Period : ○ Enable ● Disable

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

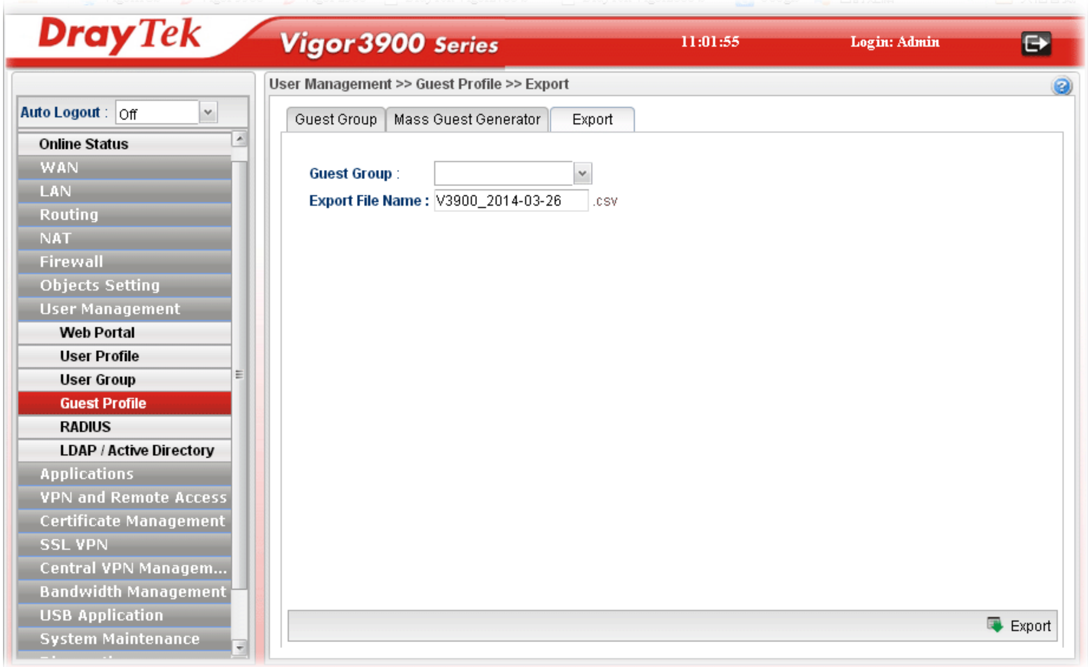
Available parameters are listed as follows:

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

Item	Description
Usage Settings	**Usage Period** –It determines the usage time for the guest accessing into Internet each time. Click **Enable** to enable such option. ● **Usage Time(min)**-The default setting is 180 minutes. **Validity Period** –It determines the valid period for the guest accessing into Internet. That is, the guest cannot access into the Internet anytime outside the valid period. Click **Enable** to enable such option. ● **Start Time/End Time** – Specify the valid period by typing the time with the format of YYYY-MM-DD-MM.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.7.4.3 Export

This function is used to export the guest profile names and random passwords.



User Management >> Guest Profile >> Export

Guest Group :

Export File Name : V3900_2014-03-26 .csv

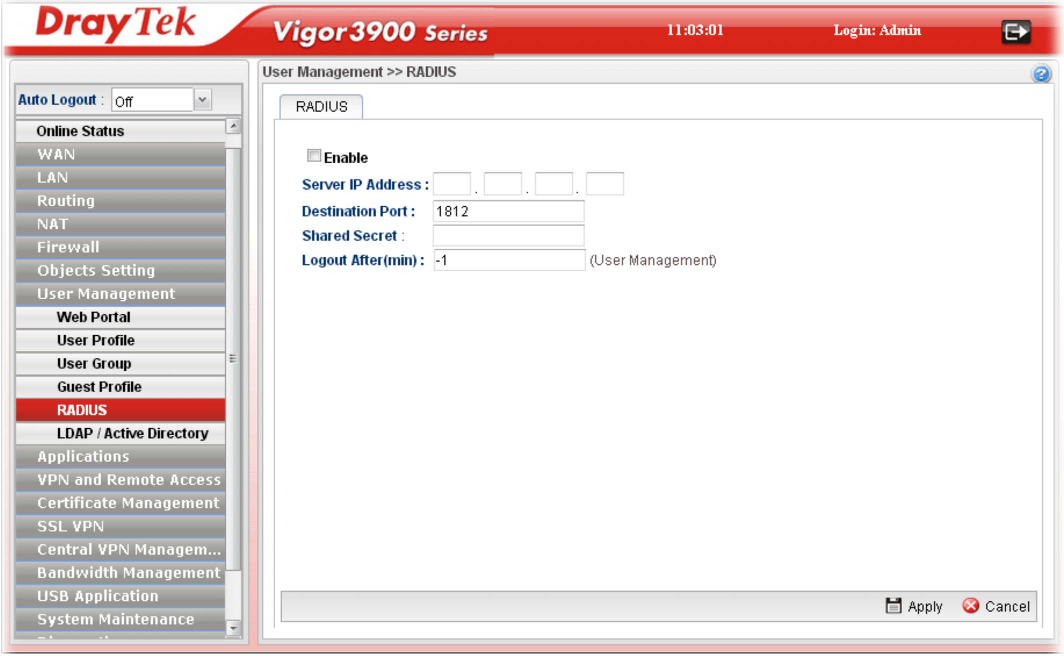
Available parameters are listed as follows:

Item	Description
Guest Group	Choose a group that you want to export the settings, including guest profile names and random passwords as a file for reference.

4.7.5 RADIUS

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

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



□ Enable

Server IP Address : . . .

Destination Port : 1812

Shared Secret :

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

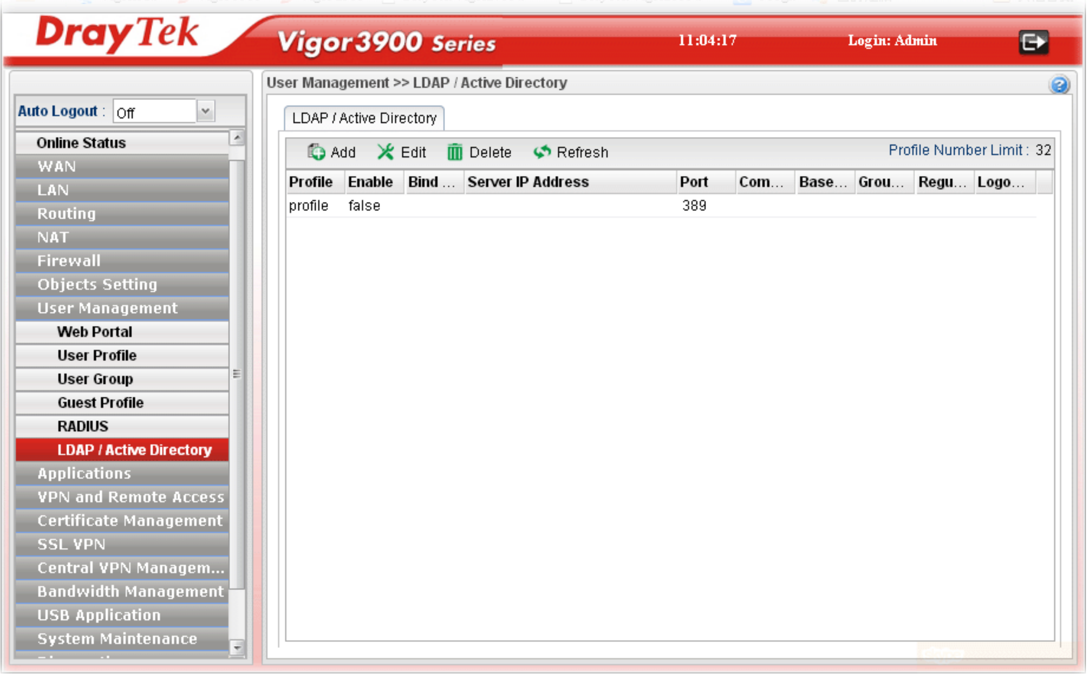
Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
Server IP Address	Enter the IP address of RADIUS server.
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Logout After(min)	It means the maximum usage duration for RADIUS authentication.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.7.6 LDAP/Active Directory

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

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



Profile	Enable	Bind ...	Server IP Address	Port	Com...	Base...	Grou...	Regu...	Logo...
profile	false			389					

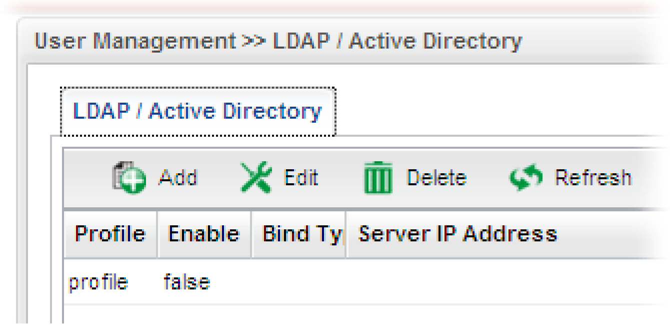
Available parameters are listed as follows:

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

Item	Description
Bind Type	Display the type setting selected for such profile.
Server IP Address	Display the IP address of the LDAP server.
Port	Display the port number set for such profile.
Common Name Identifier	Display the name for identification.
Base DN	Display the configured Base DN if Bind Type is set with Simple Mode.
Group DN	Display the configured Group DN if Bind Type is set with Simple Mode.
Regular DN	Display the configured regular DN if Bind Type is set with Regular Mode.
Logout After(min)	Display the maximum usage duration for RADIUS authentication.

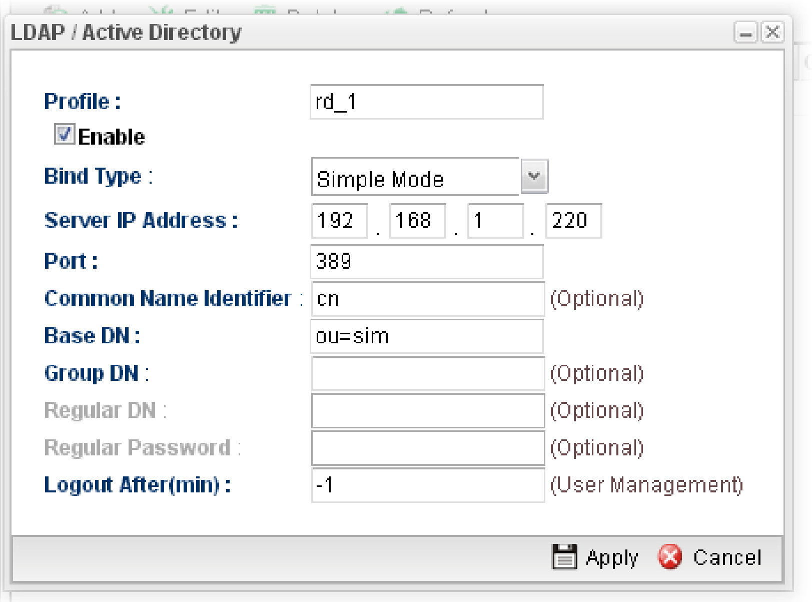
How to create a new LDAP/Active Directory Profile

1. Open **User Management>>LDAP/Active Directory.**
2. Simply click the **Add** button.



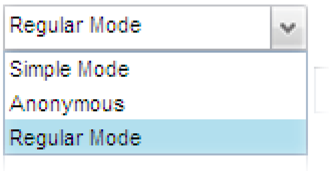
Profile	Enable	Bind Ty	Server IP Address
profile	false		

3. The following dialog will appear.

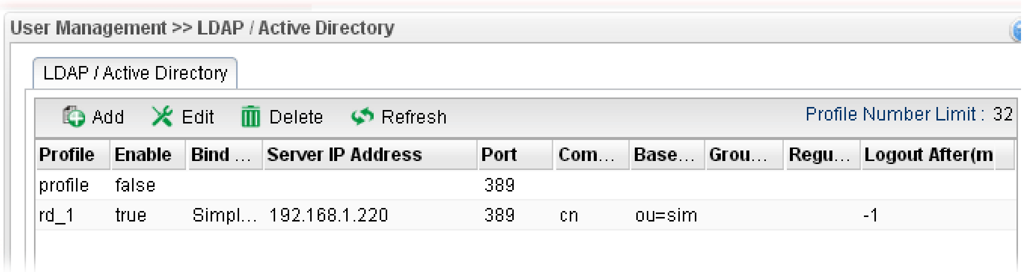


Profile :	rd_1	
☑ Enable		
Bind Type :	Simple Mode	
Server IP Address :	192 . 168 . 1 . 220	
Port :	389	
Common Name Identifier :	cn	(Optional)
Base DN :	ou=sim	
Group DN :		(Optional)
Regular DN :		(Optional)
Regular Password :		(Optional)
Logout After(min) :	-1	(User Management)

Available parameters are listed as follows:

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

4. Enter all the settings and click **Apply**.
5. A new LADP/Active Directory Profile has been created.



User Management >> LDAP / Active Directory

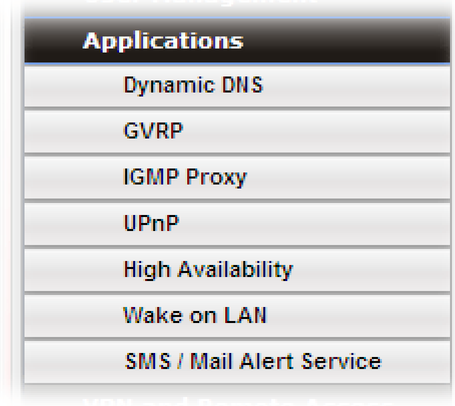
LDAP / Active Directory

Profile Number Limit : 32

Profile	Enable	Bind ...	Server IP Address	Port	Com...	Base...	Grou...	Regu...	Logout After(m
profile	false			389					
rd_1	true	Simpl...	192.168.1.220	389	cn	ou=sim			-1

4.8 Application

Below shows the menu items for Applications.



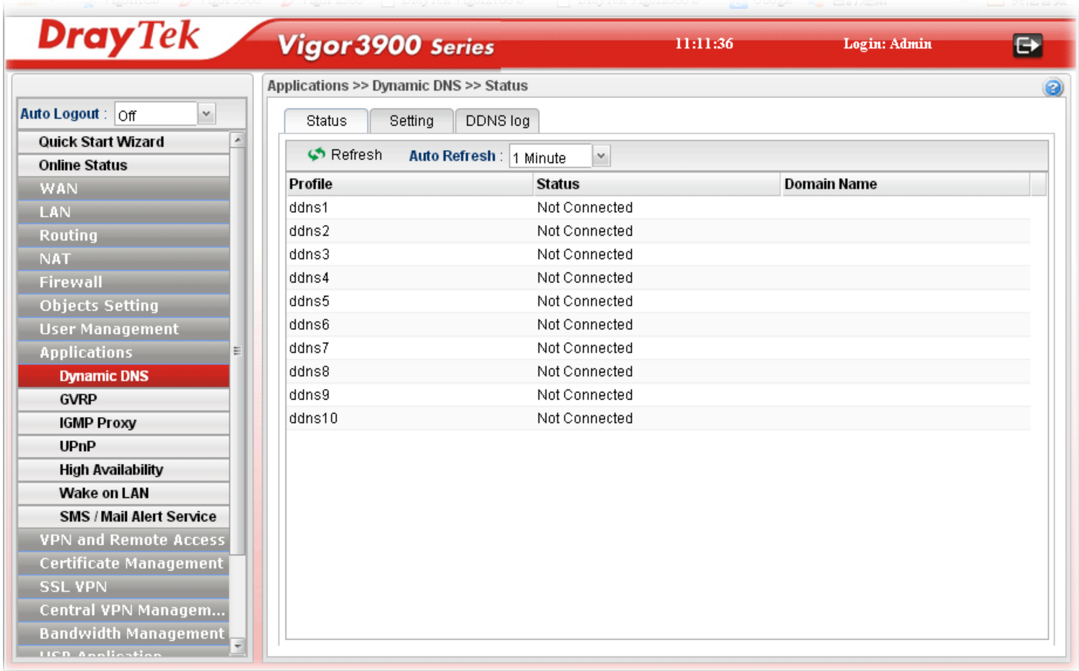
4.8.1 Dynamic DNS

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

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

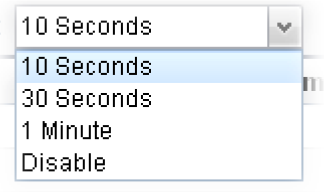
4.8.1.1 Status

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



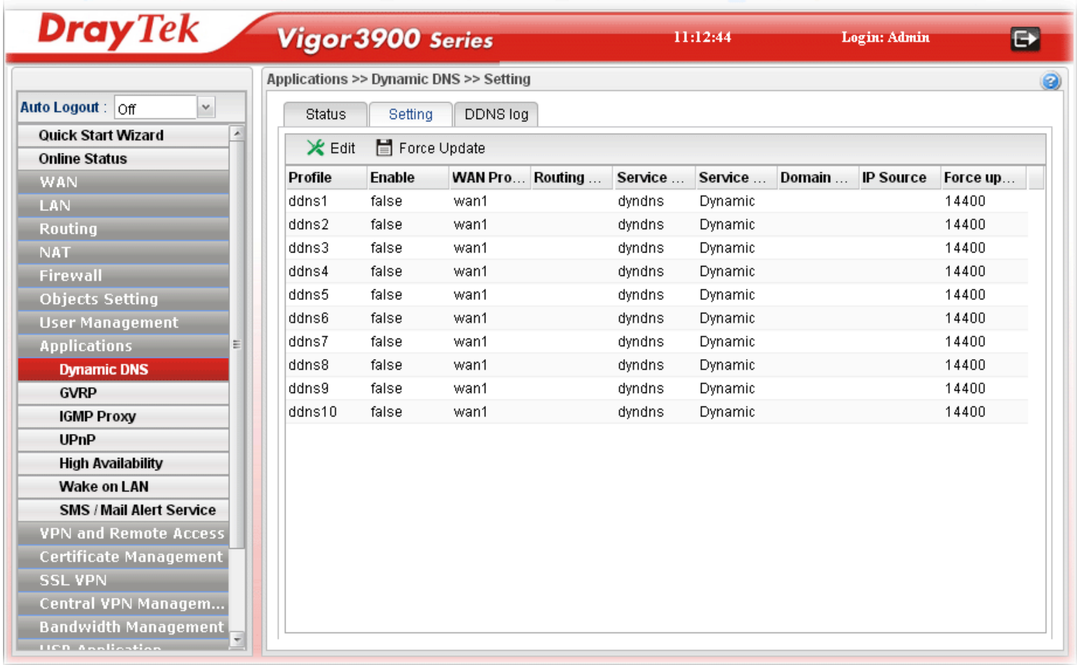
Profile	Status	Domain Name
ddns1	Not Connected	
ddns2	Not Connected	
ddns3	Not Connected	
ddns4	Not Connected	
ddns5	Not Connected	
ddns6	Not Connected	
ddns7	Not Connected	
ddns8	Not Connected	
ddns9	Not Connected	
ddns10	Not Connected	

Each item will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.  10 Seconds 10 Seconds 30 Seconds 1 Minute Disable
Profile	Display the name of the DDNS.
Status	Display the connection status for the DDNS sever.
Domain Name	Display the domain name for the DDNS server.

4.8.1.2 Setting

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



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

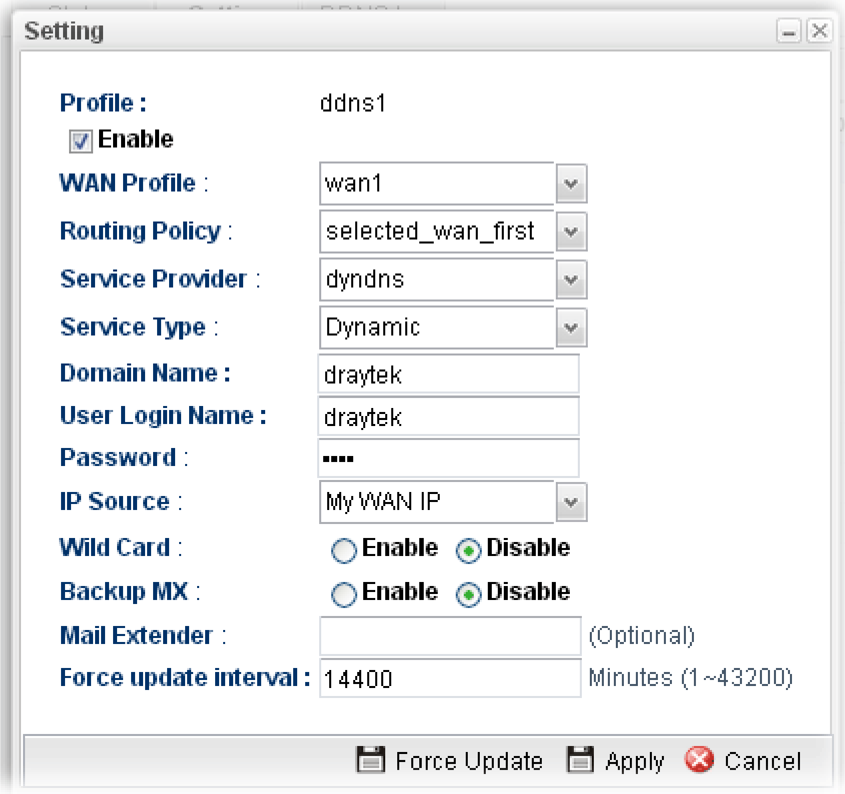
Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Force Update	Force the router updates its information to DDNS server immediately.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display current WAN profile used by such DDNS profile.
Routing Policy	Display the routing policy used by such DDNS profile.
Service Provider	Display the name of service provider used by such profile.
Service Type	Display the type for such profile.
Domain Name	Display the domain name of such profile.
IP Source	Display the interface (My WAN IP or My Internet IP) selected by such DDNS profile.
Force update interval	Display the interval setting to refresh the data for such profile.

How to edit a DDNS Profile

There are 10 sets of DDNS server offered for you to modify and configure. Please choose any one of them and click **Edit** to open the following page for modification.

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



Setting

Profile : ddns1

☑ Enable

WAN Profile : wan1

Routing Policy : selected_wan_first

Service Provider : dyndns

Service Type : Dynamic

Domain Name : draytek

User Login Name : draytek

Password : ••••

IP Source : My WAN IP

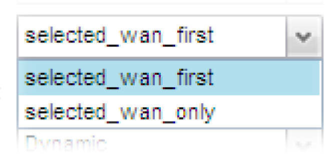
Wild Card : ○ Enable ● Disable

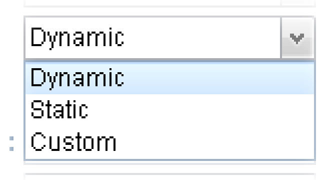
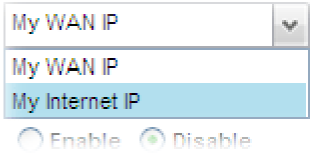
Backup MX : ○ Enable ● Disable

Mail Extender : (Optional)

Force update interval : 14400 Minutes (1~43200)

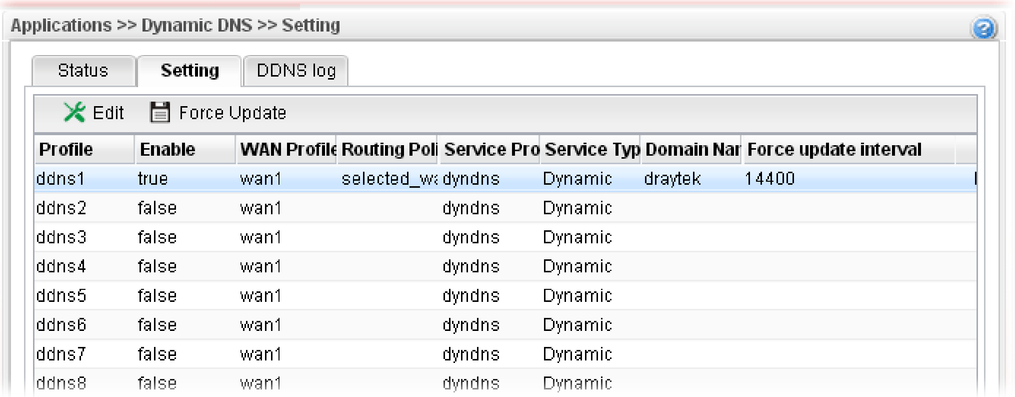
Available parameters are listed as follows:

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

Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field. 
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
User Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
IP Source	Choose My WAN IP or My Internet IP as the source for the DDNS profile.  My WAN IP My WAN IP My Internet IP Enable Disable
Wildcard and Backup MX	The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	Type the IP/Domain name of the mail server.
Force update interval	Set the time for the router to perform auto update for DDNS service.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

4. The DDNS Profile has been modified.

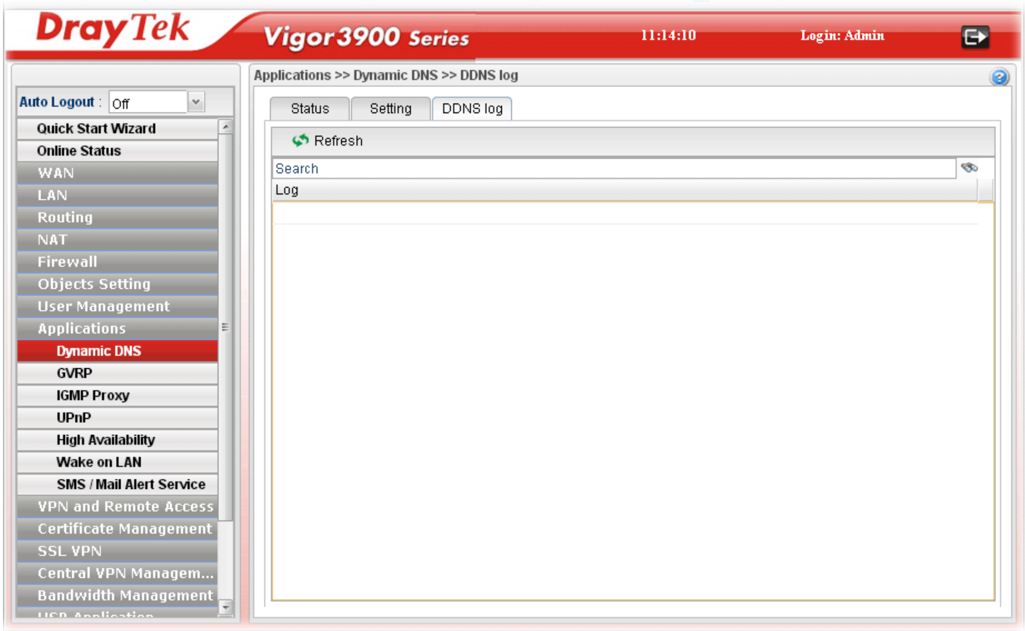


Applications >> Dynamic DNS >> Setting

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

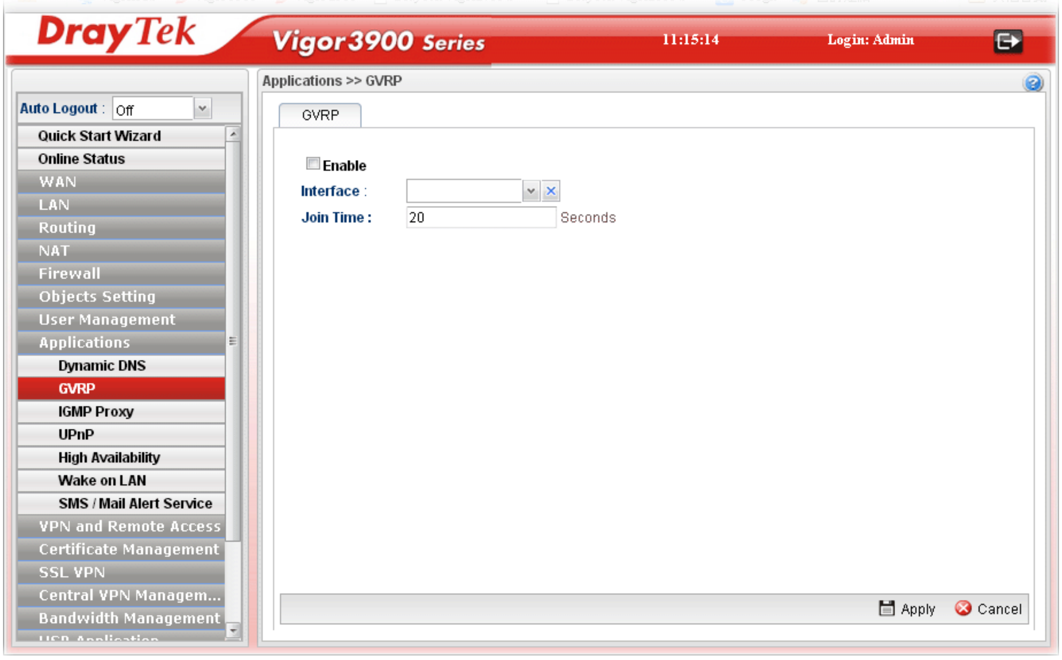
4.8.1.3 DDNS Log

This page displays the information related to all DDNS.



4.8.2 GVRP

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



□ Enable

Interface :

Join Time : 20 Seconds

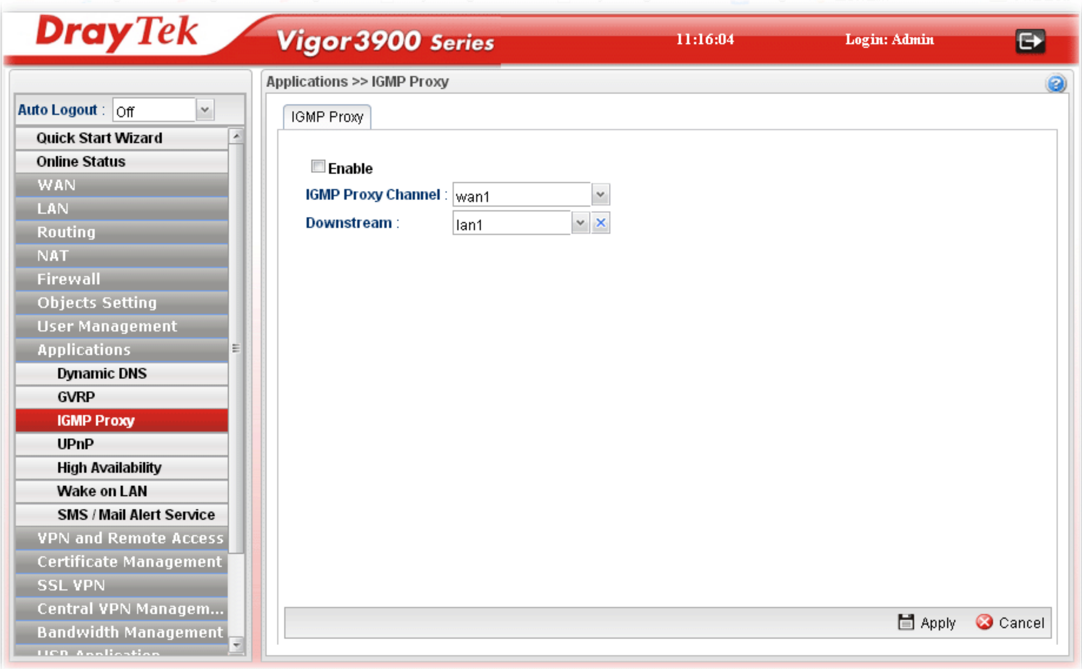
Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable GVRP function.

Item	Description
Interface	Choose LAN and/or WAN profiles. To clear the selected one, click ✕ to remove current object selections.
Join Time	Define the time for the system to send GVRP packet to other device. The unit is second.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.3 IGMP Proxy

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.



Applications >> IGMP Proxy

IGMP Proxy

□ Enable

IGMP Proxy Channel : wan1

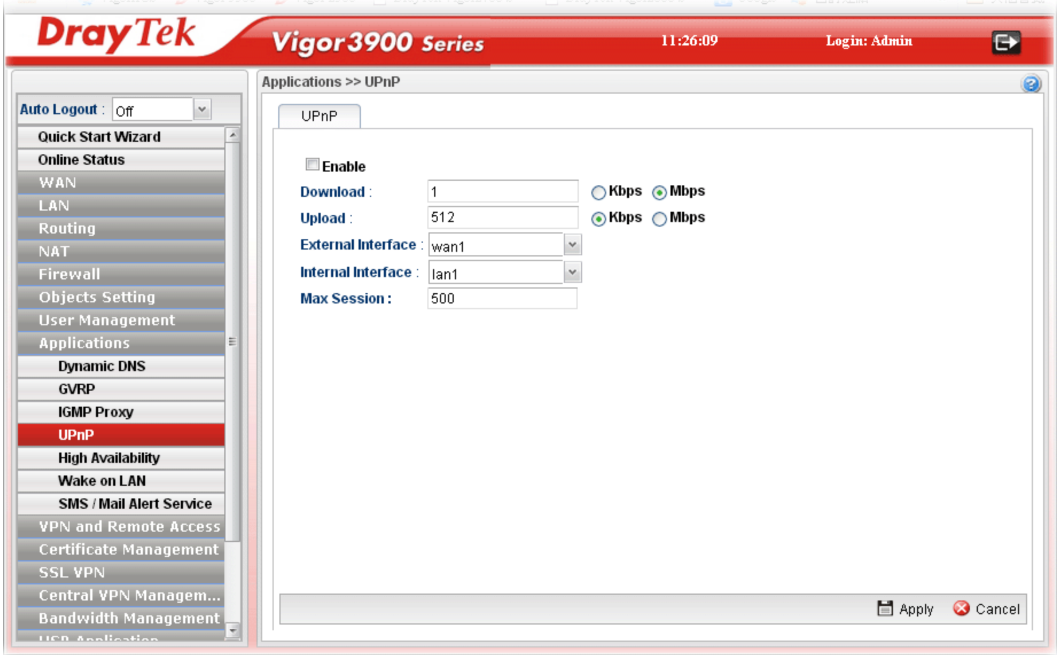
Downstream : lan1

Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable IGMP proxy function.
IGMP Proxy Channel	The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.
Downstream	Use the drop down list to specify the LAN profile as the destination of data coming from WAN interface (defined in IGMP Proxy Channel).
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.8.4 UPnP

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



□ Enable

Download : 1 ○ Kbps ● Mbps

Upload : 512 ● Kbps ○ Mbps

External Interface : wan1

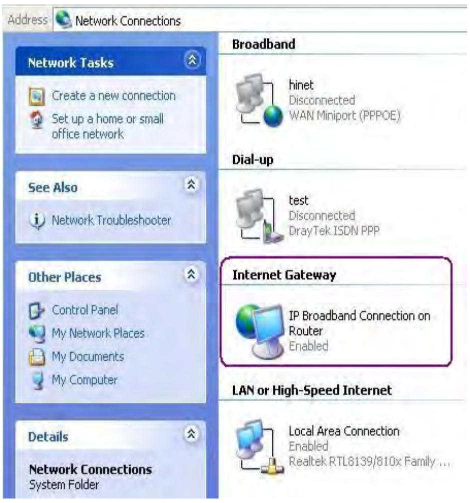
Internal Interface : lan1

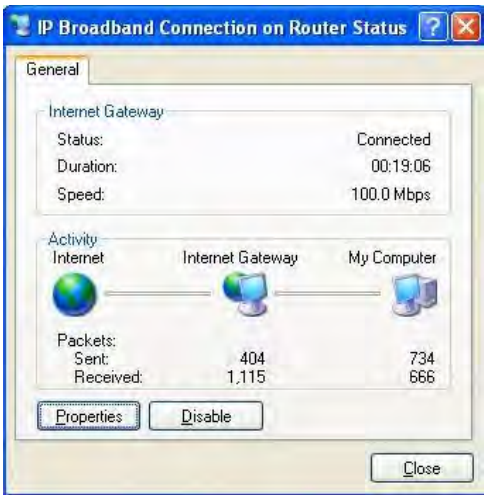
Max Session : 500

Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable UPnP function.
Download	Enter the maximum sustained WAN download speed in kilobits/second. Such information can be requested by UPnP clients.
Upload	Enter the maximum sustained WAN upload speed in kilobits/second. Such information can be requested by UPnP clients.
External Interface	Select a WAN profile for UPnP protocol.
Internal Interface	Select a LAN profile for UPnP protocol.
Max Session	Determine the maximum session number for UPnP function.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

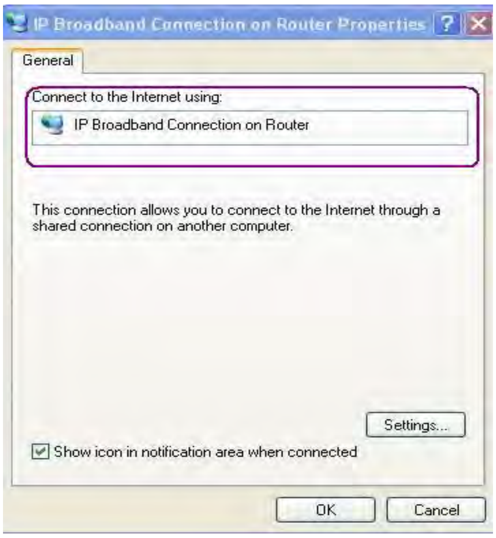
After **enabling UPNP** service setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This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





Status:		Connected
Duration:		00:19:06
Speed:		100.0 Mbps
Packets:		
Sent:	404	734
Received:	1,115	666

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.

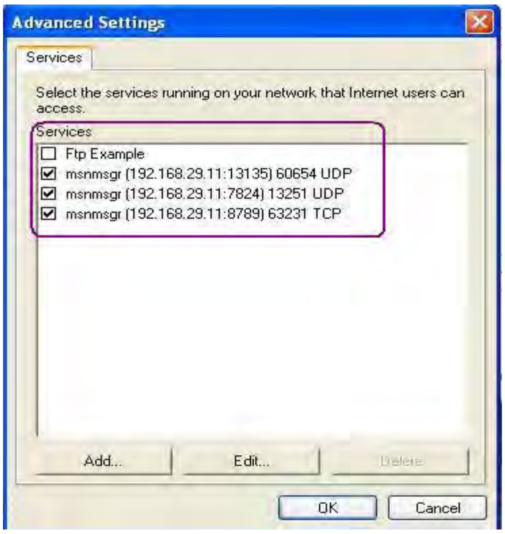


Connect to the Internet using:

IP Broadband Connection on Router

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected



Select the services running on your network that Internet users can access.

Services

☐ Ftp Example
☑ msnmsgr (192.168.29.11:13135) 60654 UDP
☑ msnmsgr (192.168.29.11:7824) 13251 UDP
☑ msnmsgr (192.168.29.11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

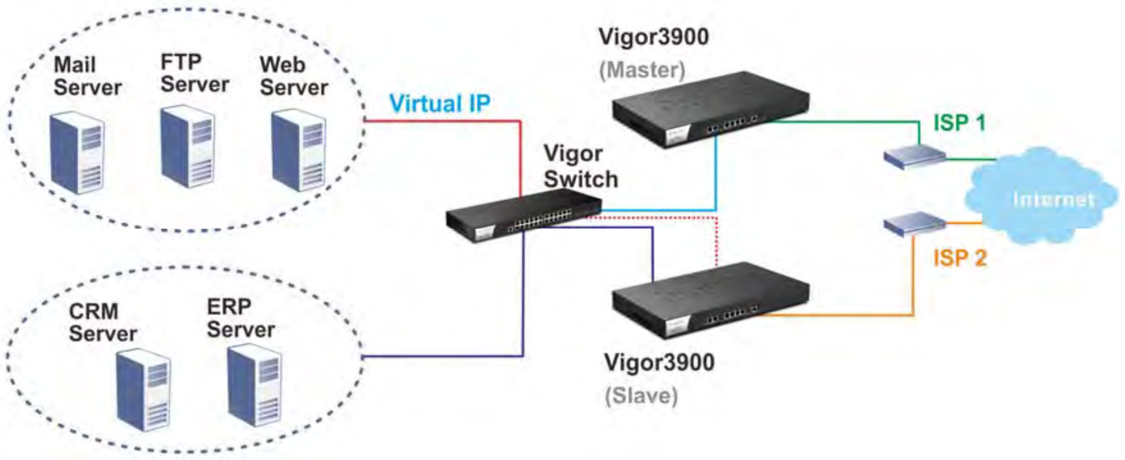
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

4.8.5 High Availability

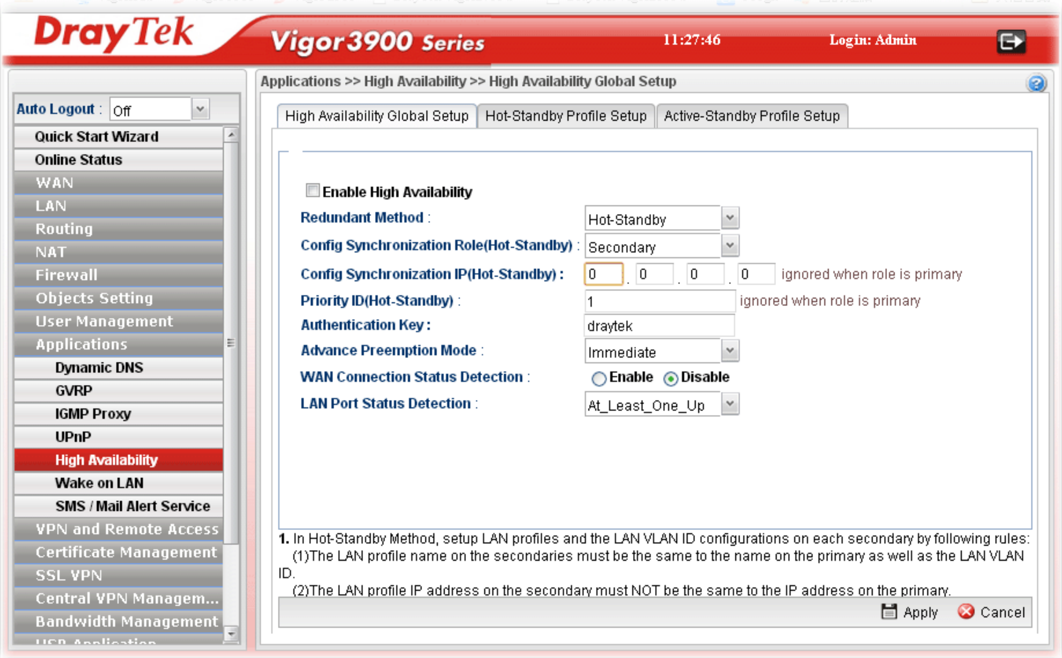
The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, provides nearly full-time availability, typically have redundant hardware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



4.8.5.1 High Availability Global Setup



Applications >> High Availability >> High Availability Global Setup

High Availability Global Setup | Hot-Standby Profile Setup | Active-Standby Profile Setup

□ Enable High Availability

Redundant Method : Hot-Standby

Config Synchronization Role(Hot-Standby) : Secondary

Config Synchronization IP(Hot-Standby) : 0 . 0 . 0 . 0 ignored when role is primary

Priority ID(Hot-Standby) : 1 ignored when role is primary

Authentication Key : draytek

Advance Preemption Mode : Immediate

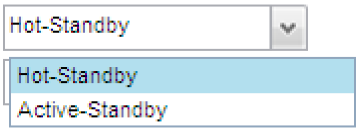
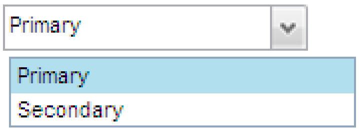
WAN Connection Status Detection : ○ Enable ● Disable

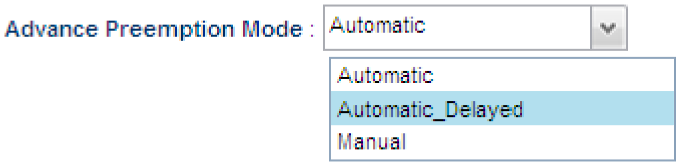
LAN Port Status Detection : At_Least_One_Up

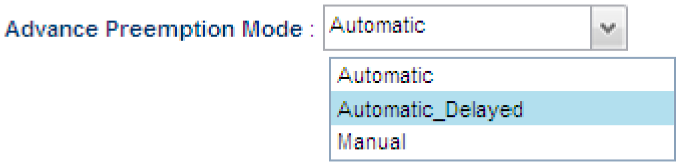
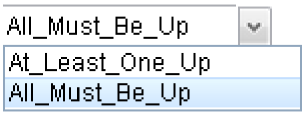
1. In Hot-Standby Method, setup LAN profiles and the LAN VLAN ID configurations on each secondary by following rules:
(1)The LAN profile name on the secondaries must be the same to the name on the primary as well as the LAN VLAN ID.
(2)The LAN profile IP address on the secondary must NOT be the same to the IP address on the primary.

Apply Cancel

Available parameters are listed as follows:

Item	Description
Enable High Availability	Check this box to enable HA function.
Redundant Method	Choose Hot-Standby or Active-Standby as the method for HA.  **Hot –Standby** –Hot-Standby is a redundant method of having several secondary service nodes running standby with another identical primary service node. Upon failure of the primary node, the system immediately elects one from all secondary nodes to replace the failure one and take over the service. While in the standby status, the secondary nodes are still mirrored the configuration of primary in real time, thus the whole systems are assured of having identical configuration. **Active-Standby** –Active-Standby is a redundant method of having the access points configured independently by participating in HA session with individual LAN interface. As an active gateway LAN, it routes user's traffic while others stay in standby status.
Settings under Hot-Standby	**Config Synchronization Role(Hot-Standby)** – Specify the role for such Vigor router. 
	Primary – It means such Vigor router is treated as the primary

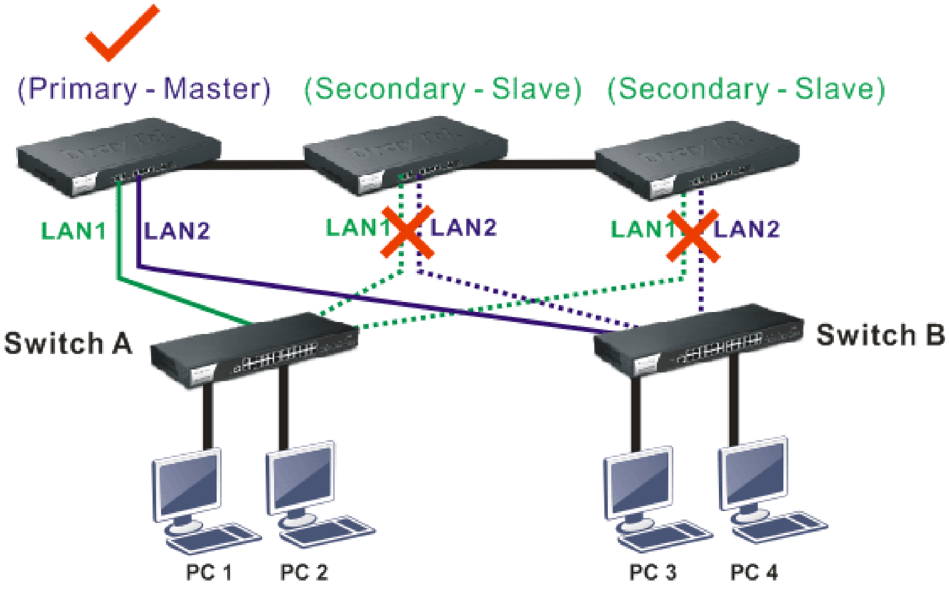
Item	Description
	device (master device).
	Authentication Key – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack. **Advance Preemption Mode** – Specify a mode for changing the Config Synchronization Role.  Advance Preemption Mode : Automatic ● **Automatic** – The router will be restored to primary (master) router once the service is restored. ● **Automatic_Delayed** – The router must wait for a period of time to restore to primary (master) router when the service is restored. **Delayed Interval:** Specify the time for waiting. ● **Manual** – Restoring must be done according to the setting of **Manual Preemption Status**. **Manual Preemption Status** – Click Active or Inactive. **Manual Mode Threshold** – Set a period of time for the system to determine the master router when there is no master router detected. If the router is set as Primary (Master) router, and you change the Manual Preemption Status from Active to Inactive. Once the router (Primary) detects that it is in Inactive state, it will not take preemption. However, if there is no secondary router taking over the service, all the data traffic would be terminated. To solve the problem, two methods can be executed: 1. Simply reset Manual Preemption Status from Inactive to Active and then click **Apply** to save the settings. 2. Set the value for Manual Mode Threshold. After passing the time configured in Manual Mode Threshold, if the system detects no master router (primary) router existing, then Manual Preemption Status will be reset to Active to locate the master router.
	Secondary – It means such Vigor router is treated as the secondary device (slave device). The secondary router will copy the configuration from the primary router to make itself as primary.
	Authentication Key – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack. **Advance Preemption Mode** – Specify a mode for changing the Config Synchronization Role.

Item	Description
	 Advance Preemption Mode : Automatic Automatic Automatic_Delayed Manual ● **Automatic** – The router will be restored to primary (master) router once the service is restored. ● **Automatic_Delayed** – The router must wait for a period of time to restore to primary (master) router when the service is restored. **Delayed Interval:** Specify the time for waiting. ● **Manual** – Restoring must be done according to the setting of **Manual Preemption Status**. **Manual Preemption Status** – Click Active or Inactive. **Manual Mode Threshold** – Set a period of time for the system to determine the master router when there is no master router detected. If the router is set as Primary (Master) router, and you change the Manual Preemption Status from Active to Inactive. Once the router (Primary) detects that it is in Inactive state, it will not take preemption. However, if there is no secondary router taking over the service, all the data traffic would be terminated. To solve the problem, two methods can be executed: 1. Simply reset Manual Preemption Status from Inactive to Active and then click **Apply** to save the settings. 2. Set the value for Manual Mode Threshold. After passing the time configured in Manual Mode Threshold, if the system detects no master router (primary) router existing, then Manual Preemption Status will be reset to Active to locate the master router.
	LAN Port Detection Mode – The router (with the role of Primary - Master) will detect if there is malfunction on LANs automatically. This function will force the master router to failover to other backups if any failure of LAN is detected. There are two schemes to determine the failure of LAN ports:  ● At_Least_One_Up - The master router can own its position only if one LAN port is connecting. ● All_Must_Be_Up - The master router can own its position only when all of LAN ports are connecting. **Enable High Availability –** Check the box to enable HA function.
	WAN Connection Status Detection –Click **Enable** to make the router detecting WAN connection status. It is similar to "LAN Port Detection Mode" but will detect connection status of all enabled WAN profiles. If connection status of all enabled

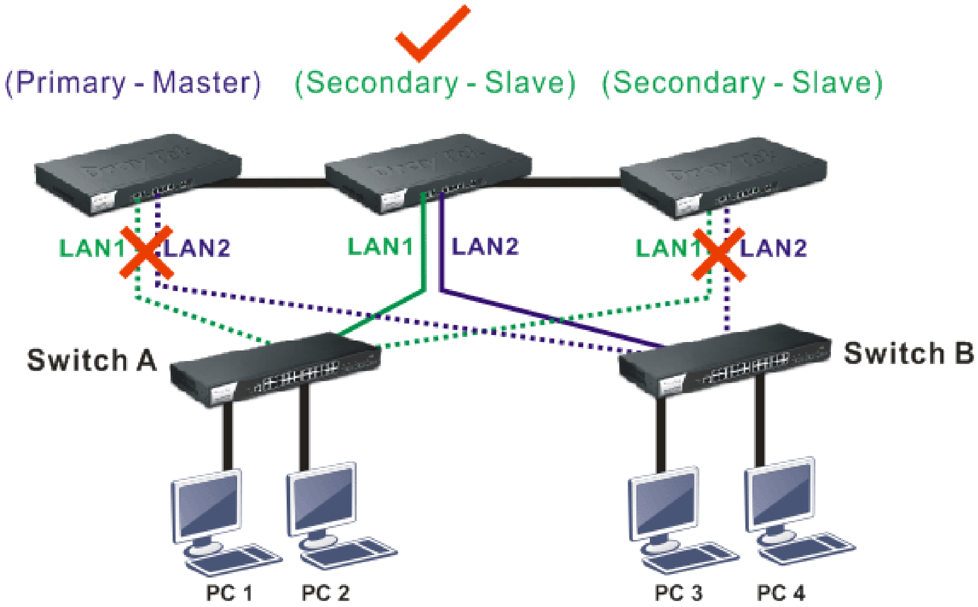
Item	Description
	WAN profiles are **down**, the master router hands off its position.
Settings under Active-Standby	**Authentication Key** – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack. **WAN Connection Status Detection –** Click **Enable** to make the router detecting WAN connection status**.** It is similar to "LAN Port Detection Mode" but will detect connection status of all enabled WAN profiles. If connection status of all enabled WAN profiles are **down**, the master router hands off its position.

4.8.5.2 Hot-Standby Mechanism

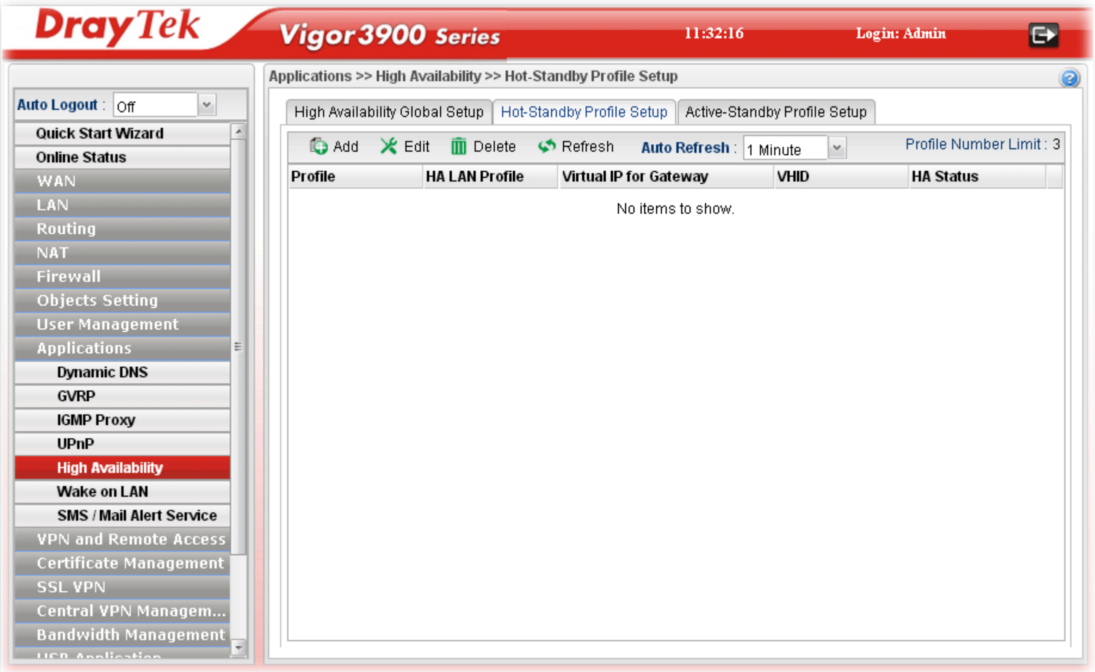
The hot-standby mechanism is that each secondary access point will be a backup device for the primary access point (router). When the primary device fails, one of the rest ones will be elected as the new master device.



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



The following page is used to create Hot-Standby profiles.



Profile	HA LAN Profile	Virtual IP for Gateway	VHID	HA Status

No items to show.

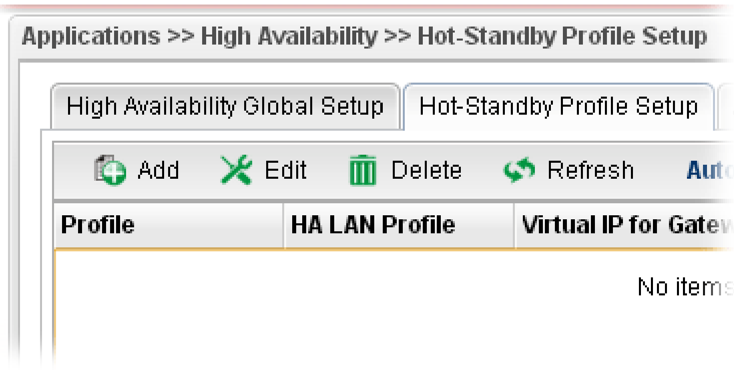
Available parameters are listed as follows:

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

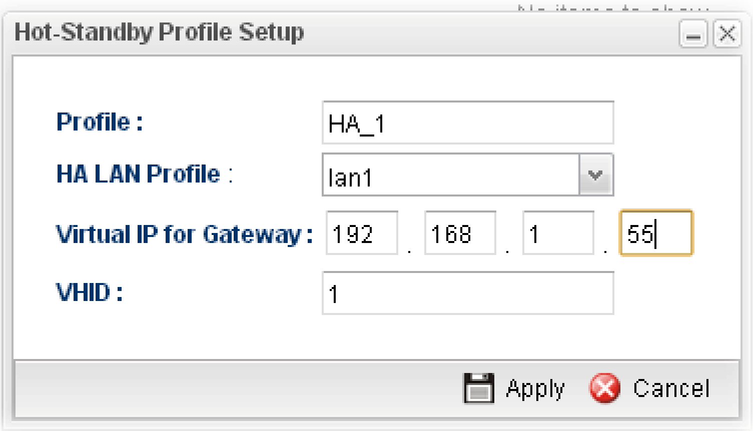
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Profile Number Limit	Display the total number (3) of the object profiles to be created.
Profile	Display the name of the HA profile.
HA LAN Profile	Display the LAN profile used by such HA.
Virtual IP for Gateway	Display the IP address of the gateway.
VHID	Display the virtual host ID number of the profile.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.

How to create a new HA Hot-Standby Profile

1. Open **Applications>>High Availability** and click the **Hot-Standby Profile Setup** tab.
2. Simply click the **Add** button.


Applications >> High Availability >> Hot-Standby Profile Setup
High Availability Global Setup
Hot-Standby Profile Setup
Add
Edit
Delete
Refresh
Aut
Profile
HA LAN Profile
Virtual IP for Gatev
No items

3. The following dialog will appear.



Profile : HA_1

HA LAN Profile : lan1

Virtual IP for Gateway : 192 . 168 . 1 . 55

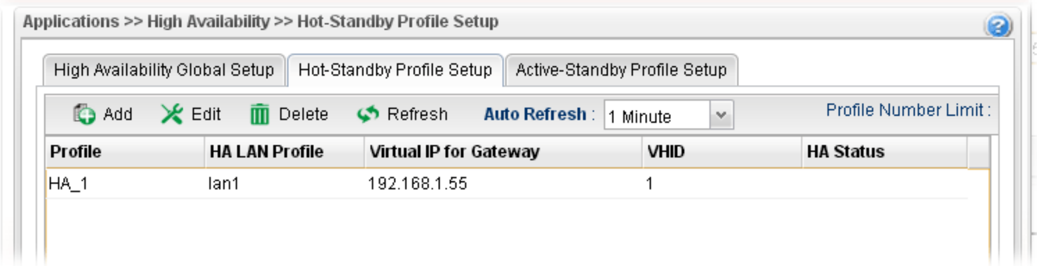
VHID : 1

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.

HA LAN Profile	Choose one of the LAN profiles that such function will be applied to.
Virtual IP for Gateway	Assign an IP address as a virtual IP.
VHID	It means Virtual Host ID. Type a number as VHID for such function. VHID is used for Backup router to identify which Master will be backed up.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

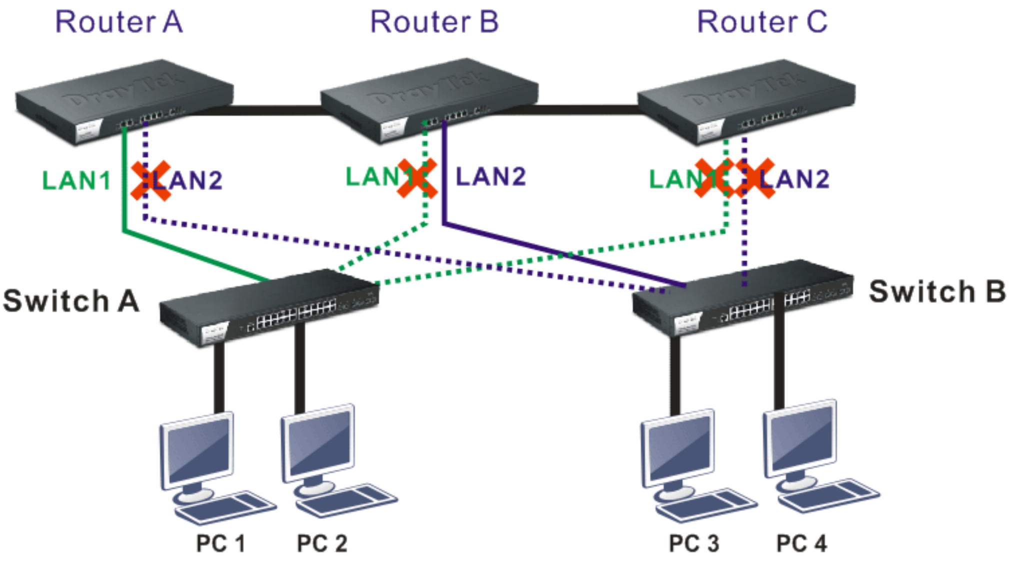


Applications >> High Availability >> Hot-Standby Profile Setup
High Availability Global Setup
Hot-Standby Profile Setup
Active-Standby Profile Setup
Add
Edit
Delete
Refresh
Auto Refresh :
1 Minute
Profile Number Limit :

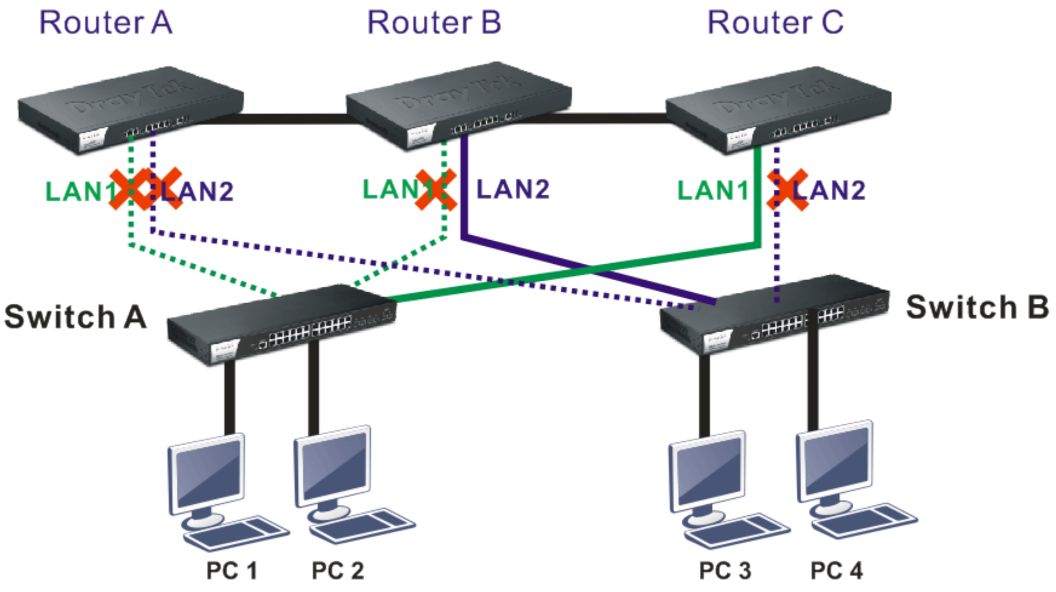
Profile	HA LAN Profile	Virtual IP for Gateway	VHID	HA Status
HA_1	lan1	192.168.1.55	1	

4.8.5.3 Active-Standby Mechanism

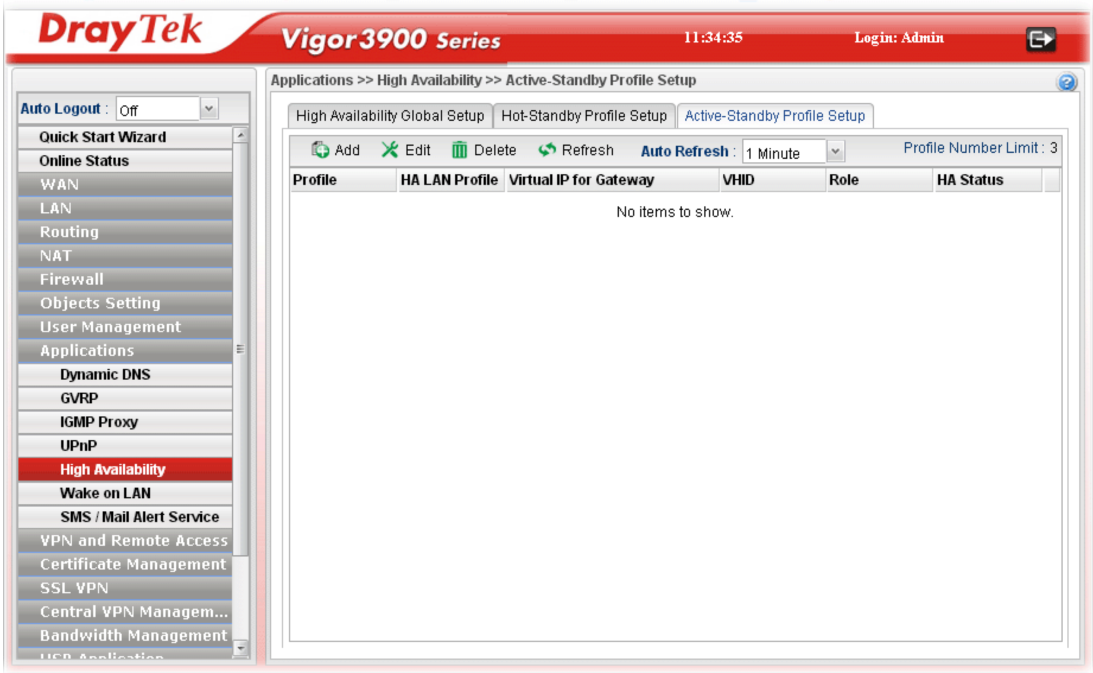
The active-standby Mechanism is that each access point in LAN will participate in different high availability sessions. All the WAN interfaces can be active which provide more flexible utilization of network service.



When LAN1 in Router A fails, one of the available line connections (e.g., LAN1 in Router C) will be selected to offer the network service for all the connected PCs.



The following page is used to create Hot-Standby profiles.



Applications >> High Availability >> Active-Standby Profile Setup

Auto Logout : Off

Auto Refresh : 1 Minute

Profile Number Limit : 3

Profile	HA LAN Profile	Virtual IP for Gateway	VHID	Role	HA Status

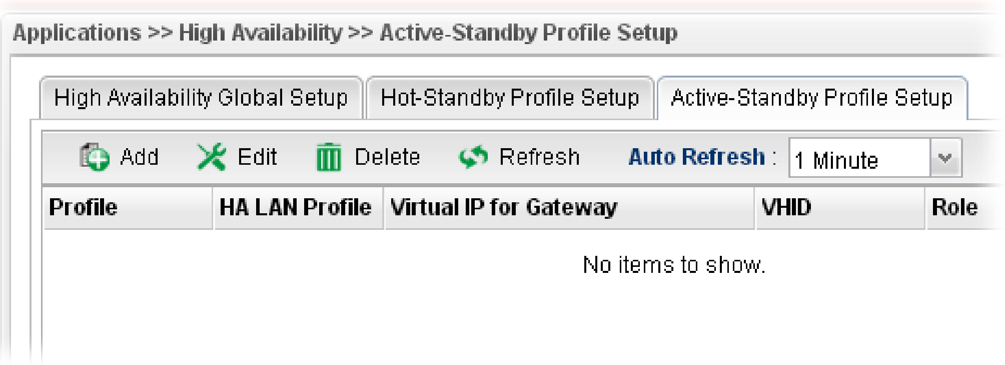
No items to show.

Available parameters are listed as follows:

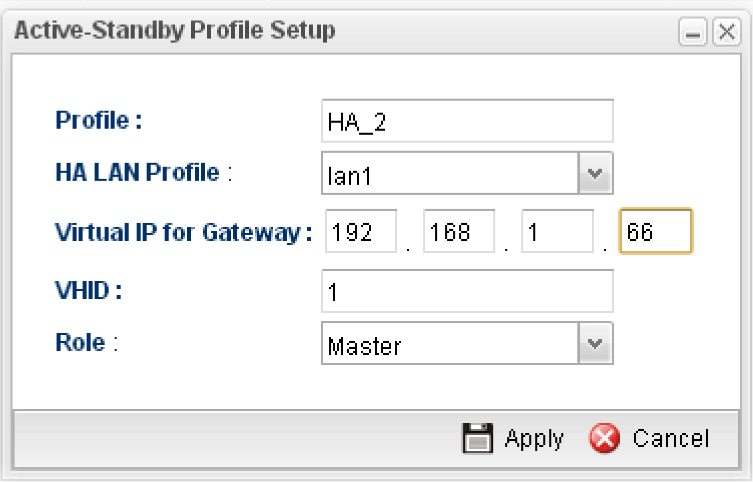
Item	Description
Add	Add a new HA profile.
Edit	Modify the selected HA profile. To edit the profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected HA profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Profile Number Limit	Display the total number (3) of the object profiles to be created.
Profile	Display the name of the HA profile.
HA LAN Profile	Display the LAN profile used by such HA.
Virtual IP for Gateway	Display the IP address of the gateway.
VHID	Display the virtual host ID number of the profile.
Role	Display the role of this profile in the corresponding HA group.
HA Status	Display the online status (Master, Backup, LAN_failed and WAN_Failed) of such HA profile.

How to create a new Active-Standby Profile

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


Applications >> High Availability >> Active-Standby Profile Setup
High Availability Global Setup
Hot-Standby Profile Setup
Active-Standby Profile Setup
Add
Edit
Delete
Refresh
Auto Refresh :
1 Minute
Profile
HA LAN Profile
Virtual IP for Gateway
VHID
Role
No items to show.

3. The following dialog will appear.



Profile : HA_2

HA LAN Profile : lan1

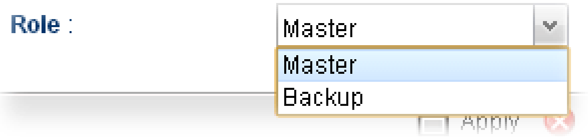
Virtual IP for Gateway : 192 . 168 . 1 . 66

VHID : 1

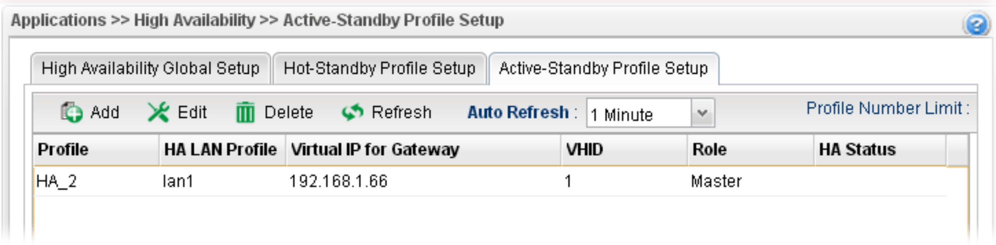
Role : Master

Available parameters are listed as follows:

Item	Description
Profile	Type a name for such profile.
HA LAN Profile	Choose one of the LAN profiles that such function will be applied to.
Virtual IP for Gateway	Assign an IP address as a virtual IP.
VHID	It means Virtual Host ID. Type a number as VHID for such function. VHID is used for Backup router to identify which Master will be backed up.
Role	LAN profiles configured for HA application can run independently and will not interfere with each other. Therefore, LAN1 (Backup) of router A can be the backup of LAN1 (Master) of router B; LAN2 (Backup) of router B can the backup of LAN2 of router A(Master). Each HA LAN profile (configured under the same router) must

	be specified a role as Master or Backup. 
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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



Applications >> High Availability >> Active-Standby Profile Setup

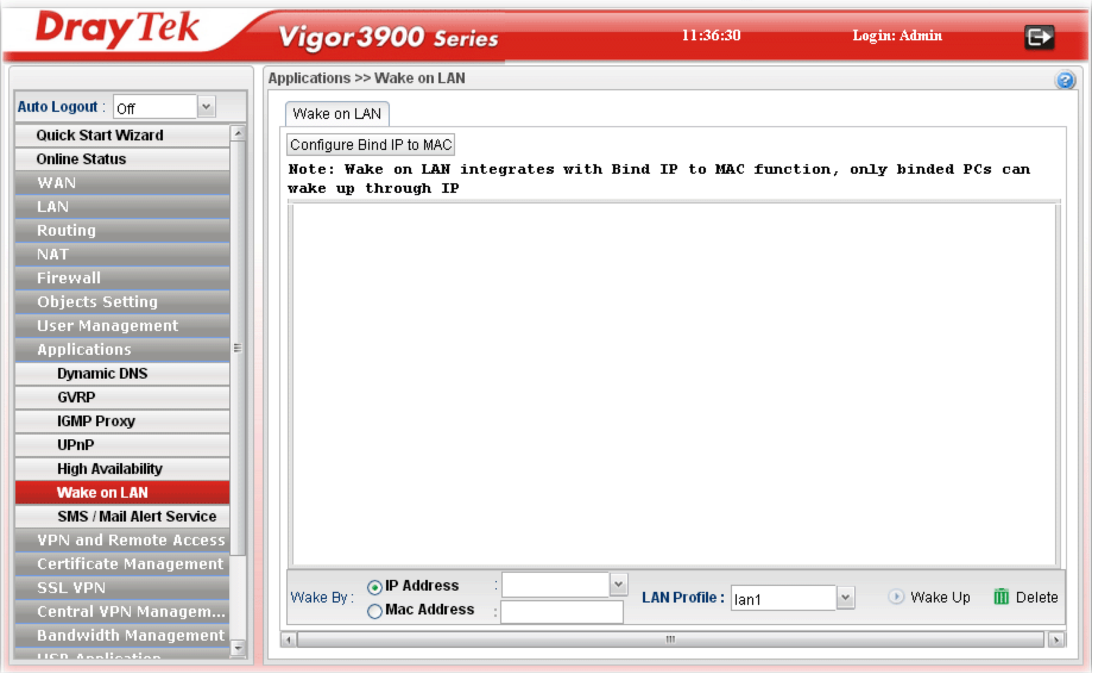
High Availability Global Setup
Hot-Standby Profile Setup
Active-Standby Profile Setup
Add
Edit
Delete
Refresh
Auto Refresh :
1 Minute
Profile Number Limit :

Profile	HA LAN Profile	Virtual IP for Gateway	VHID	Role	HA Status
HA_2	lan1	192.168.1.66	1	Master	

4.8.6 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting.



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

Wake By : ● IP Address : ○ Mac Address : LAN Profile : lan1 Wake Up Delete

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 bind PCs. **LAN Profile** – Use the drop down list to choose one of the LAN profiles.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.
Delete	Click this button to remove all the settings.

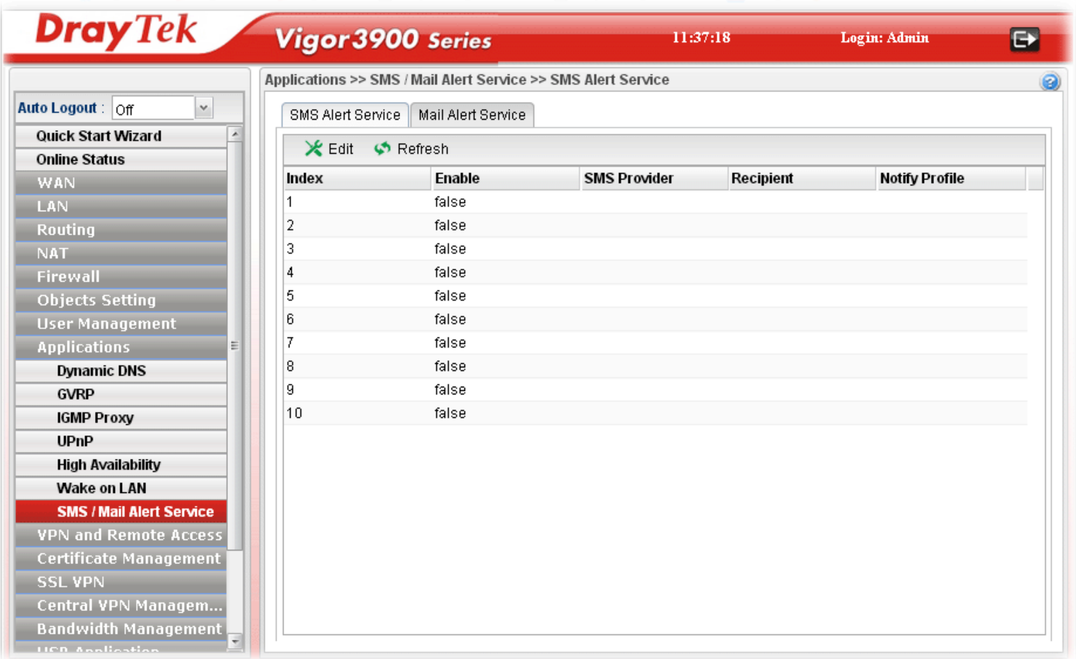
4.8.7 SMS / Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

4.8.7.1 SMS Alert Service

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.



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

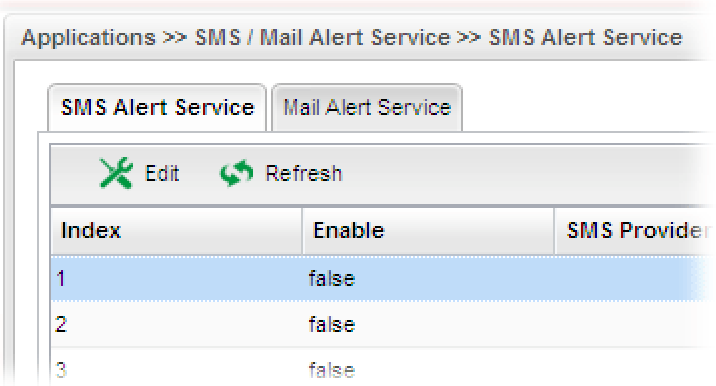
Index	Enable	SMS Provider	Recipient	Notify Profile
1	false			
2	false			
3	false			
4	false			
5	false			
6	false			
7	false			
8	false			
9	false			
10	false			

Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
SMS Provider	Display the name of the SMS provider.
Recipient	Display the one who will receive the SMS.
Notify Profile	Display the name of the notify profile.

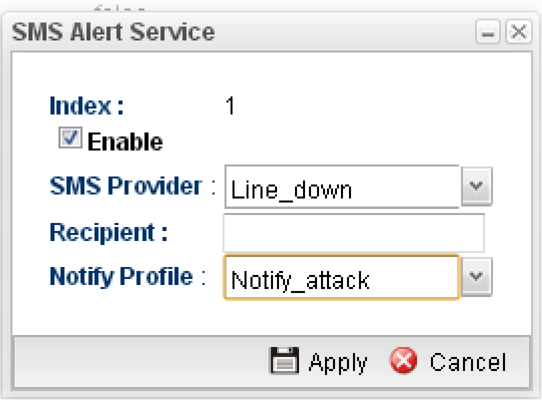
How to edit the SMS alert service profile

1. Open **Applications>> SMS/Mail Alert Service** and click the **SMS Alert Service** tab**.**
2. Choose one of the index numbers and click the **Edit** button.


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

Index	Enable	SMS Provide
1	false	
2	false	
3	false	

3. The following dialog will appear.



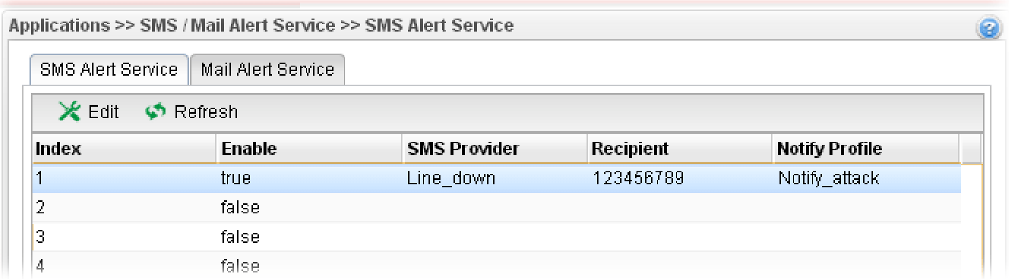
Index : 1
☑ Enable
SMS Provider : Line_down
Recipient :
Notify Profile : Notify_attack

Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
SMS Provider	Choose the SMS provider object profile from the drop down list. Such profiles can be created from **Object Setting>>SMS Service Object**.
Recipient	Type the cell phone number to receive the SMS.
Notify Profile	Choose a profile (specify the timing for sending SMS) from the drop down list. Such profiles can be created from **Object Setting>>Notification Object**.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

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

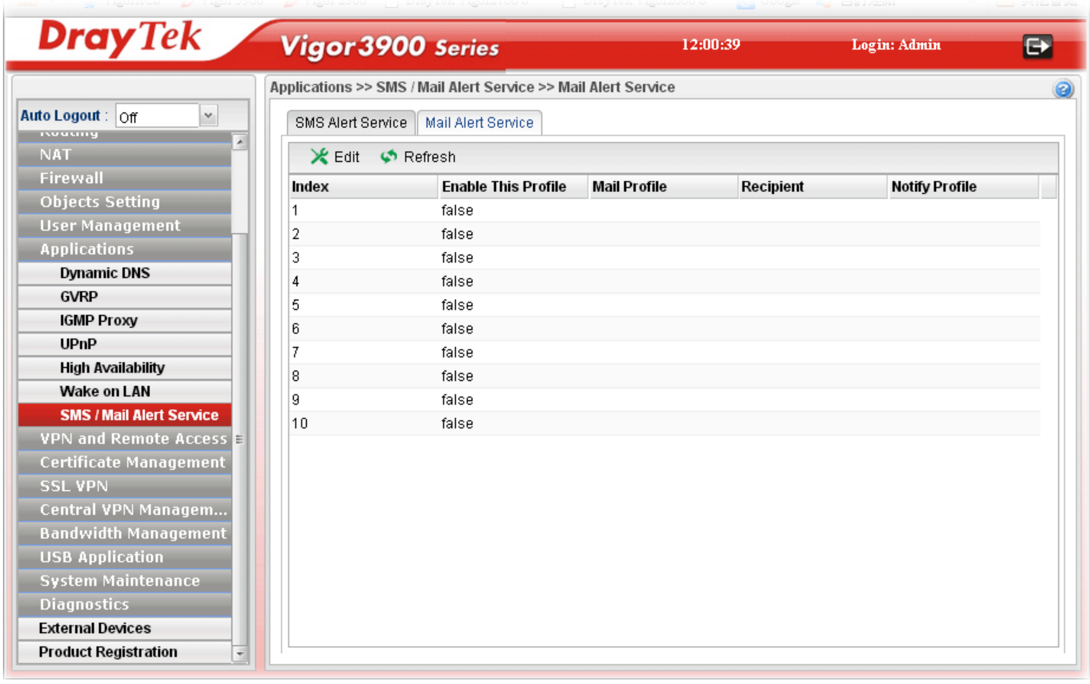
5. The SMS alert service profile has been modified.


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

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

4.8.7.2 Mail Alert Service

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.



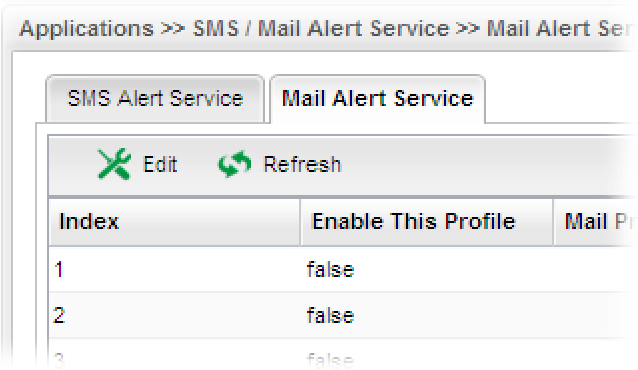
Index	Enable This Profile	Mail Profile	Recipient	Notify Profile
1	false			
2	false			
3	false			
4	false			
5	false			
6	false			
7	false			
8	false			
9	false			
10	false			

Each item will be explained as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Mail Profile	Display the name of the mail profile.
Recipient	Display the one who will receive the mail alert.
Notify Profile	Display the name of the notify profile.

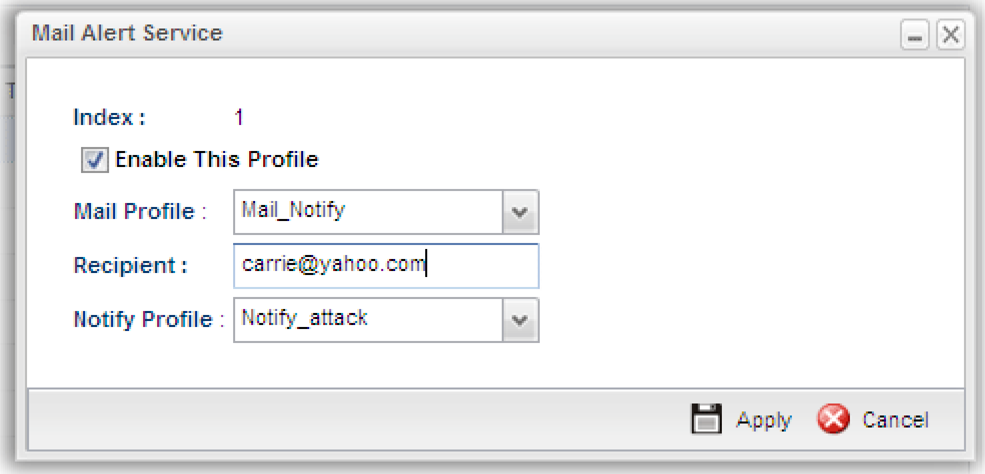
How to edit the mail alert service profile

1. Open **Applications>> SMS/Mail Alert Service** and click the **Mail Alert Service** tab**.**
2. Choose one of the index numbers and click the **Edit** button.



Index	Enable This Profile	Mail P
1	false	
2	false	
3	false	

3. The following dialog will appear.



Index : 1

☑ Enable This Profile

Mail Profile : Mail_Notify

Recipient : carrie@yahoo.com

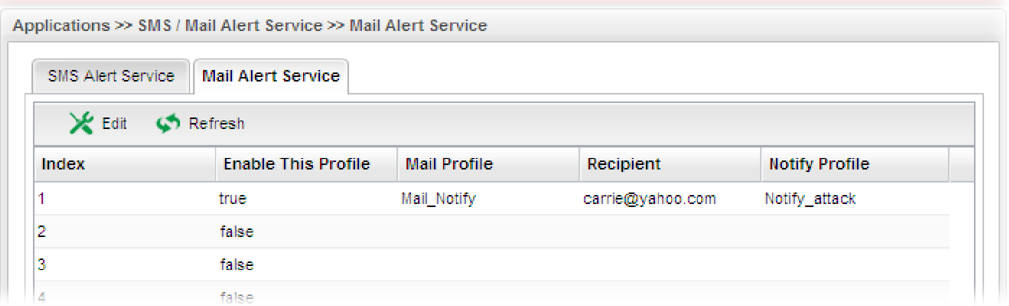
Notify Profile : Notify_attack

Available parameters are listed as follows:

Item	Description
Enable This Profile	Check this box to enable such profile.
Mail Profile	Choose the mail service object profile from the drop down list. Such profiles can be created from **Object Setting>>Mail Service Object**.
Recipient	Type the e-mail address for receiving the mail.
Notify Profile	Choose a profile (specify the timing for sending SMS) from the drop down list. Such profiles can be created from **Object Setting>>Notification Object**.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. The mail alert service profile has been modified.



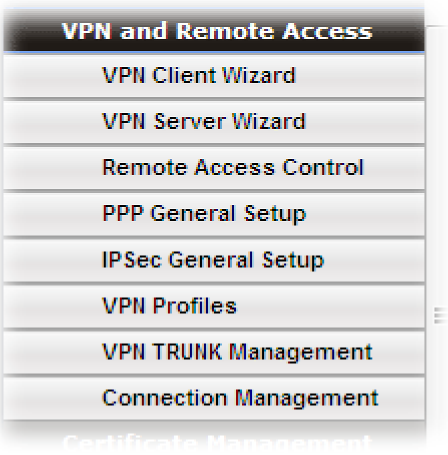
Applications >> SMS / Mail Alert Service >> Mail Alert Service

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

4.9 VPN and Remote Access

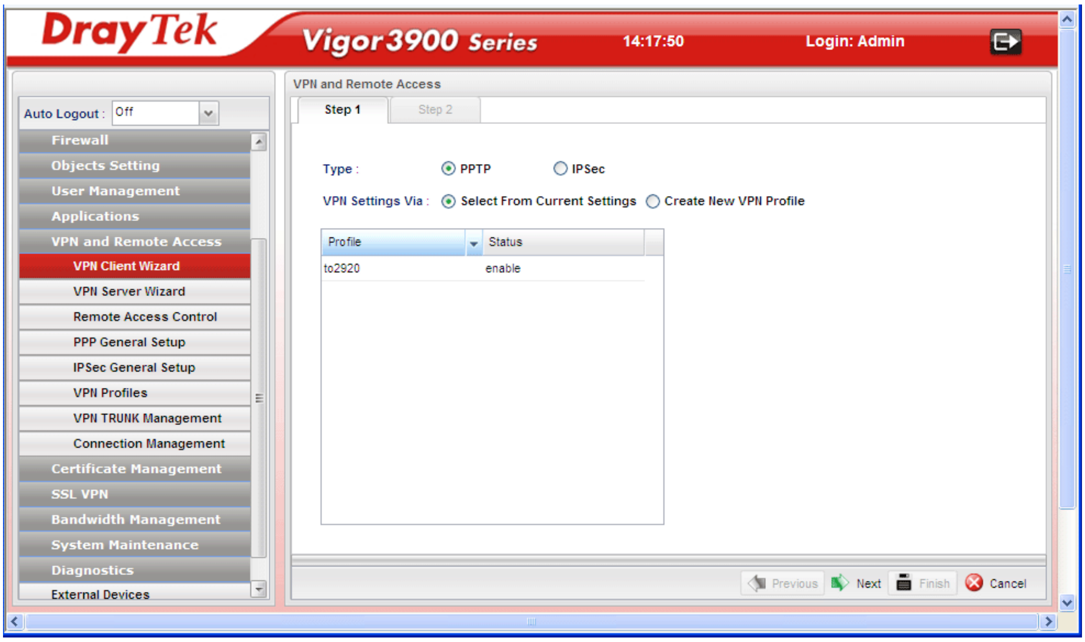
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



4.9.1 VPN Client Wizard

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



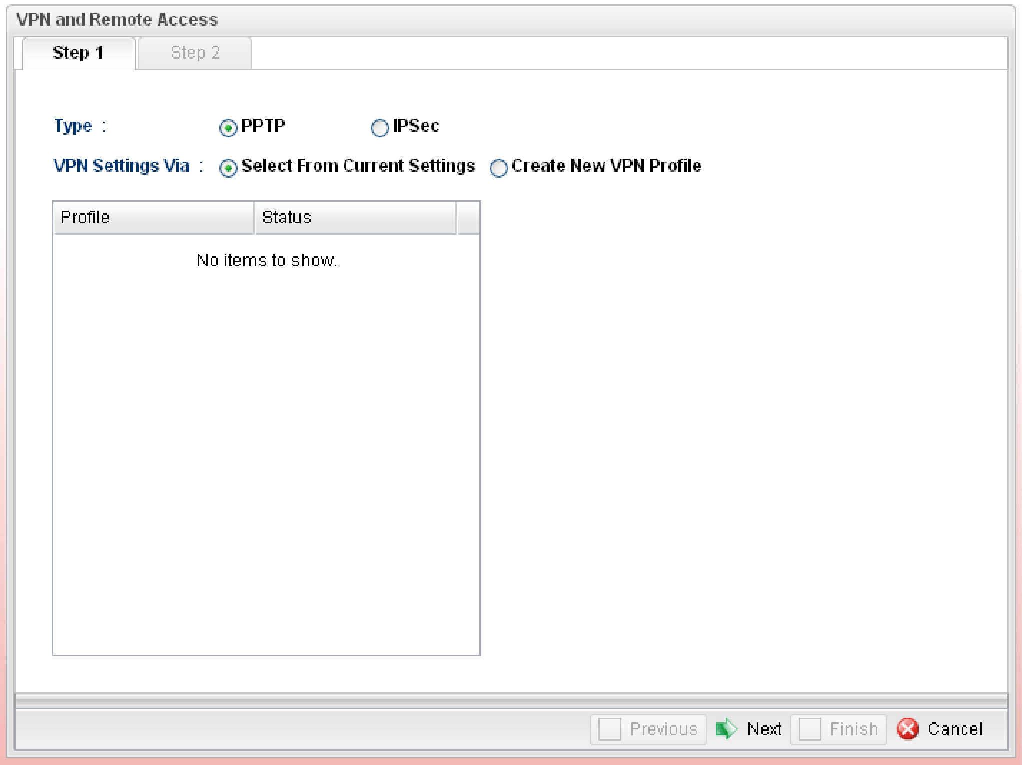
Type : ● PPTP ○ IPSec

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

Profile	Status
to2920	enable

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.



Type : ● PPTP ○ IPSec

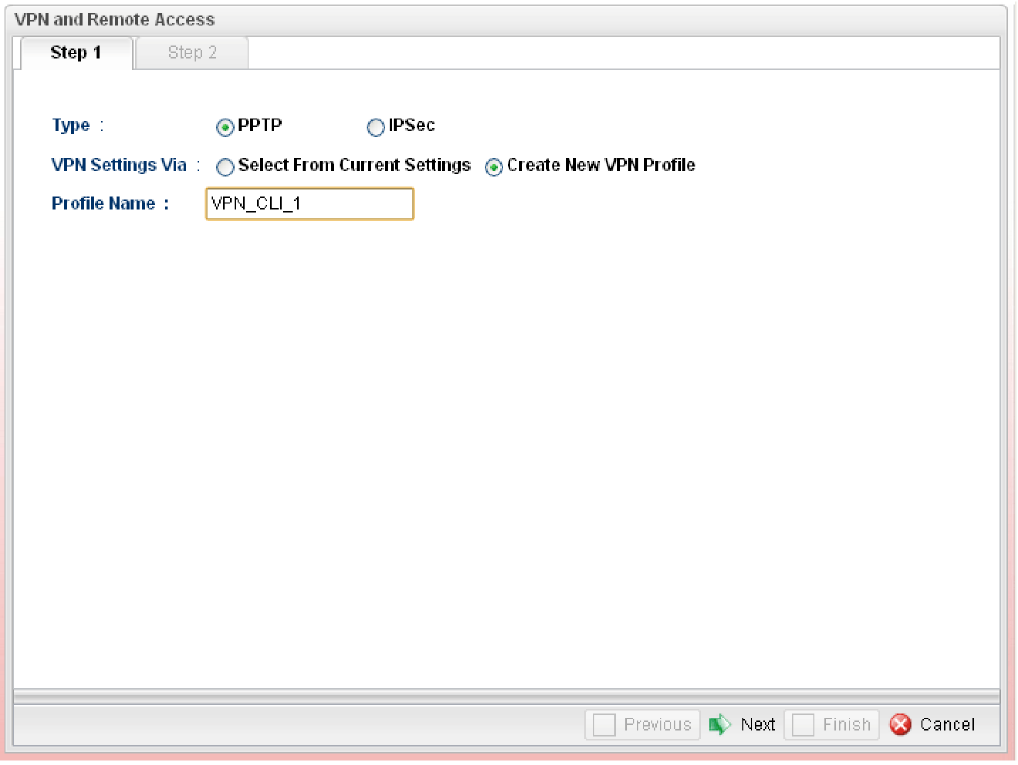
VPN Settings Via : ● Select From Current Settings ○ Create New VPN Profile

Profile	Status
No items to show.	

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**.

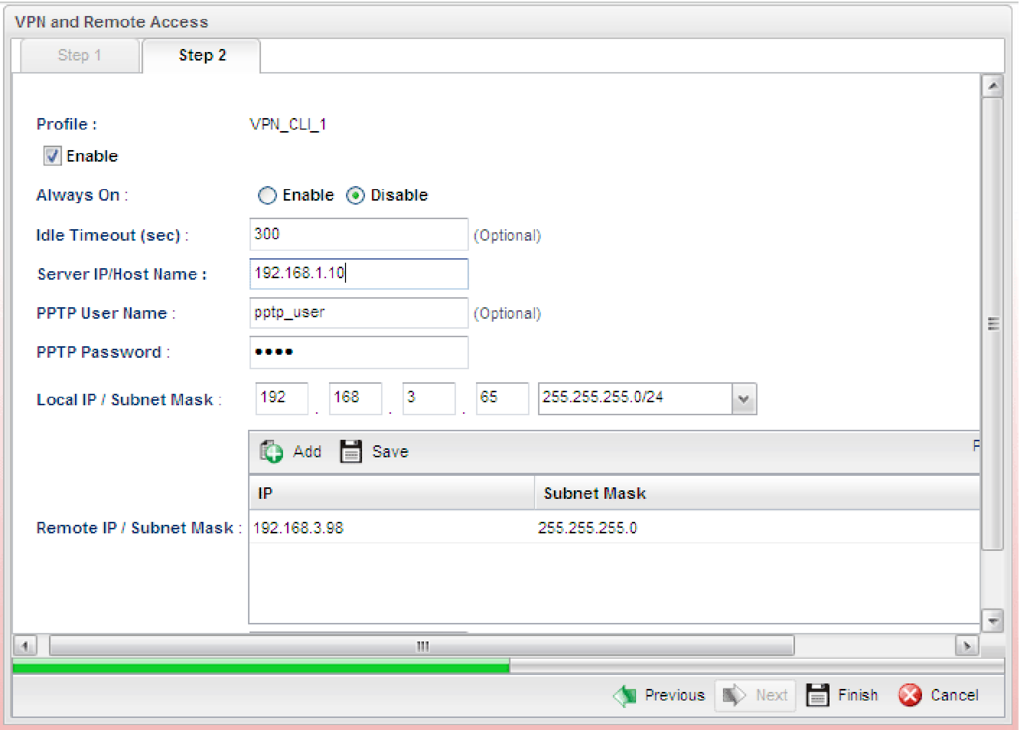


Type : ● PPTP ○ IPSec

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

Profile Name : VPN_CLI_1

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



Profile : VPN_CLI_1

☑ Enable

Always On : ○ Enable ● Disable

Idle Timeout (sec) : 300 (Optional)

Server IP/Host Name : 192.168.1.10

PPTP User Name : pptp_user (Optional)

PPTP Password : ••••

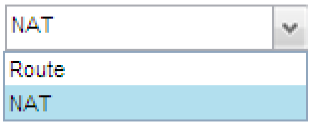
Local IP / Subnet Mask : 192 . 168 . 3 . 65 255.255.255.0/24

Remote IP / Subnet Mask :

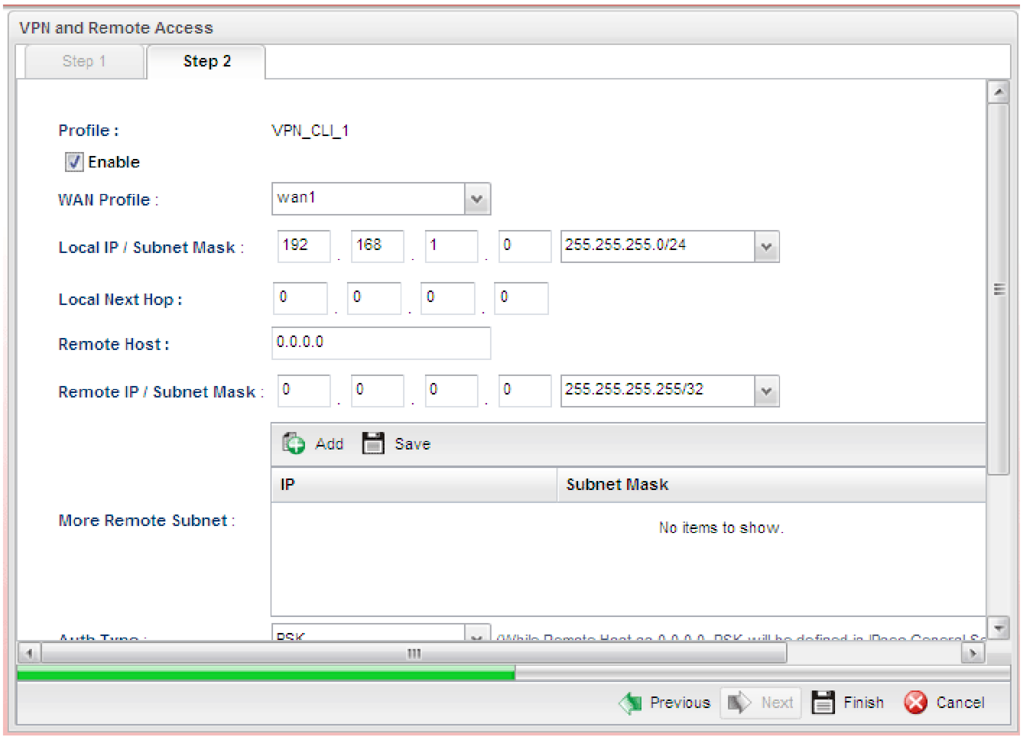
IP	Subnet Mask
192.168.3.98	255.255.255.0

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.
Idle Timeout	When Always On is disabled, you have to type the value for terminating the network connection.
Server IP/Host Name	Type the IP address or host name of PPTP server.
PPTP User Name	Type a user name for authentication in PPTP connection.
PPTP Password	Type a password for authentication in PPTP connection.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Remote IP/Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
Route/NAT Mode	Specify the purpose for such profile.  NAT Route NAT

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



VPN and Remote Access

Profile : VPN_CLI_1

☑ Enable

WAN Profile : wan1

Local IP / Subnet Mask : 192 . 168 . 1 . 0 255.255.255.0/24

Local Next Hop : 0 . 0 . 0 . 0

Remote Host : 0.0.0.0

Remote IP / Subnet Mask : 0 . 0 . 0 . 0 255.255.255.255/32

More Remote Subnet :

IP	Subnet Mask
No items to show.	

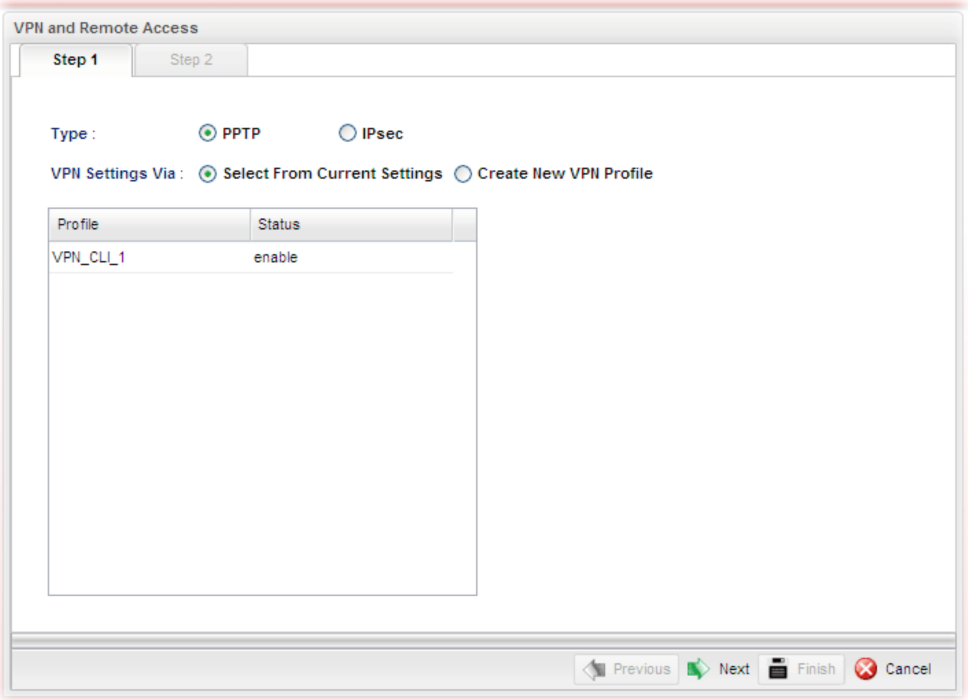
Auth Type : PSK (While Remote Host as 0.0.0.0, PSK will be defined in IPsec General Se

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose a WAN profile to be used by such profile.

Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
More Remote Subnet	Add more remote subnet in this field if required.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list if RSA is selected as Auth Type.
Preshared Key	Type a pre-shared key for authentication if PSK is selected as Auth Type.
Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
DPD Delay	DPD means dead peer detection. It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

5. Fill in the required information on this page and click **Finish**. A new profile has been created.



VPN and Remote Access

Step 1 | Step 2

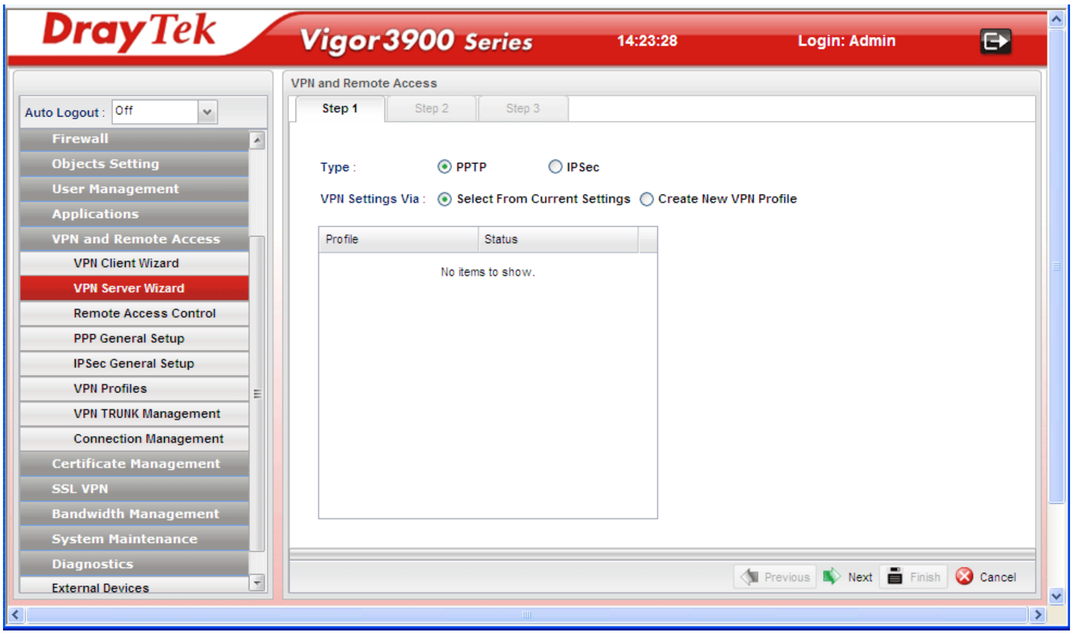
Type : ● PPTP ○ IPsec

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

Profile	Status
VPN_CLI_1	enable

4.9.2 VPN Server Wizard

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



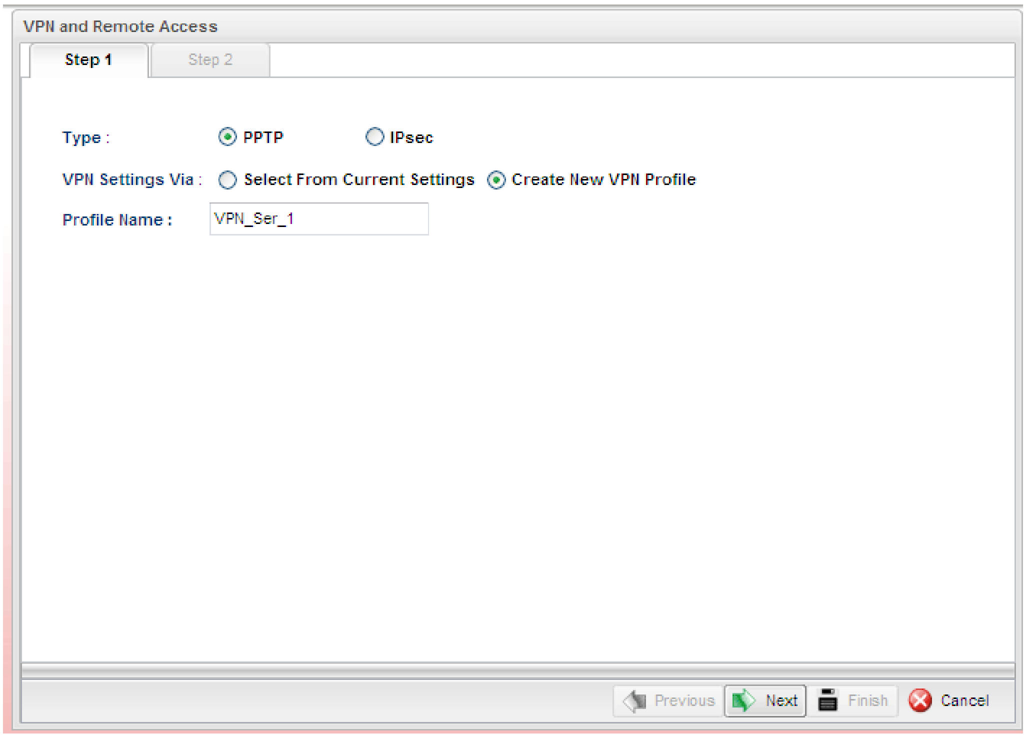
Type : ● PPTP ○ IPSec

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

Profile	Status
No items to show.	

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.



Type : ● PPTP ○ IPsec

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

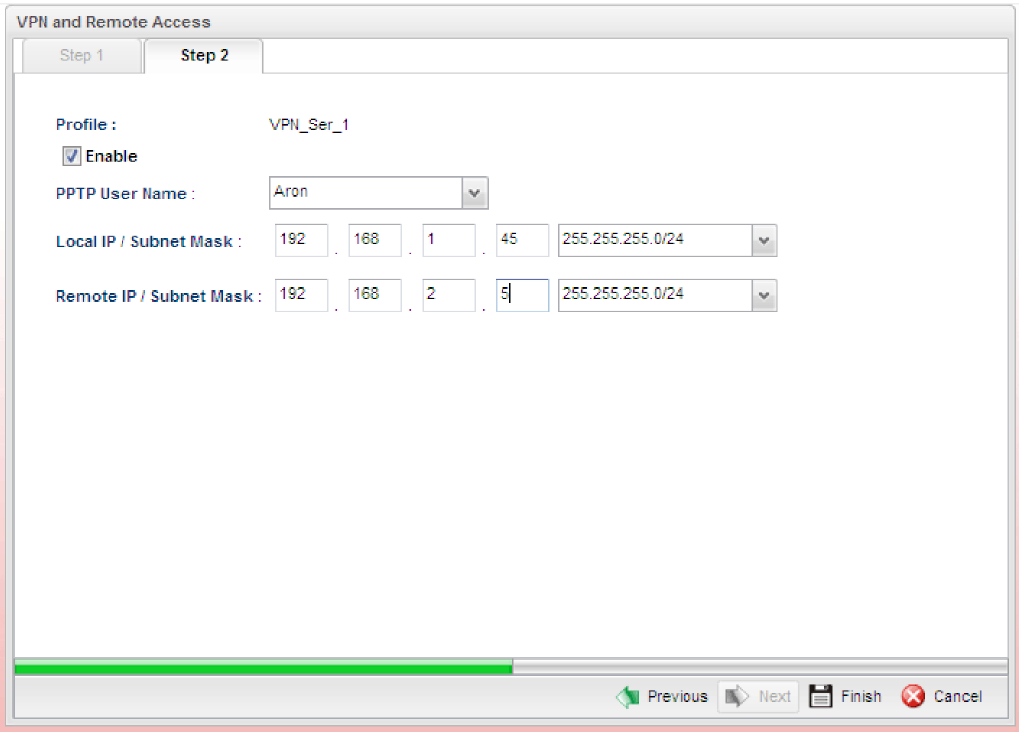
Profile Name : VPN_Ser_1

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**.**
Next	Go to next page.
Cancel	Cancel the configuration and return to the home page of such function.

3. Click **Create New VPN Profile** and type the name of the profile. Click **Next** to get into next page. Note that if you choose **PPTP** as the **Type** in Step 2, you will see the page as below:



Profile : VPN_Ser_1

☑ Enable

PPTP User Name : Aron

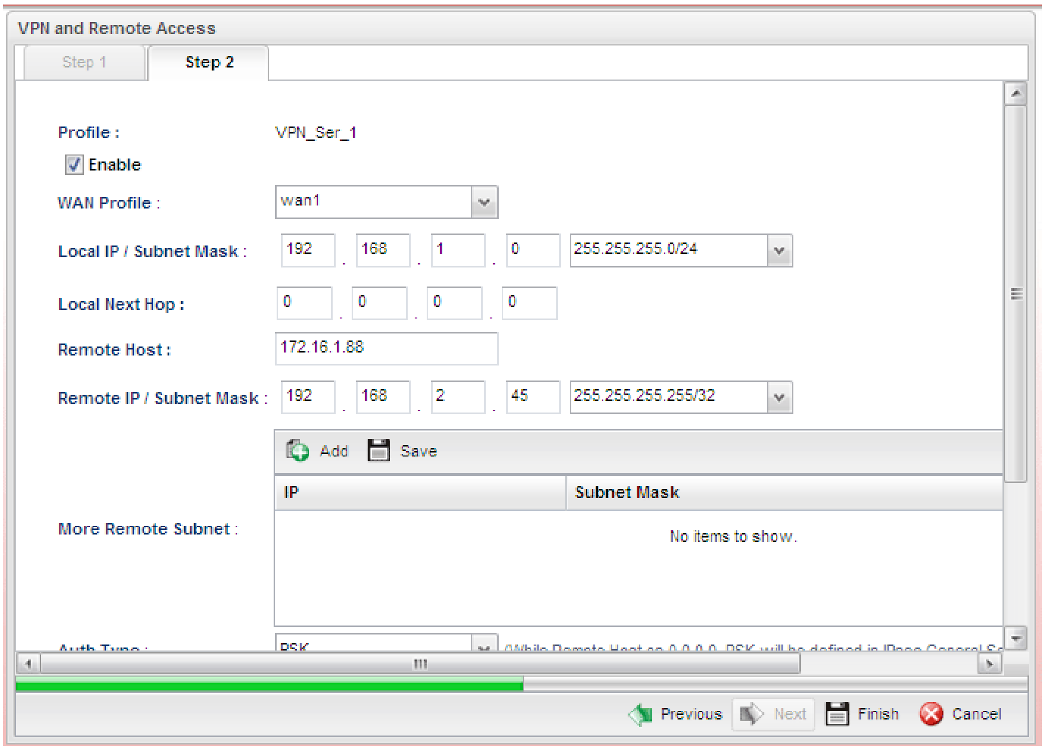
Local IP / Subnet Mask : 192 . 168 . 1 . 45 255.255.255.0/24

Remote IP / Subnet Mask : 192 . 168 . 2 . 5 255.255.255.0/24

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

Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.

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



VPN and Remote Access

Step 1 | Step 2

Profile : VPN_Ser_1

☑ Enable

WAN Profile : wan1

Local IP / Subnet Mask : 192 . 168 . 1 . 0 255.255.255.0/24

Local Next Hop : 0 . 0 . 0 . 0

Remote Host : 172.16.1.88

Remote IP / Subnet Mask : 192 . 168 . 2 . 45 255.255.255.255/32

IP	Subnet Mask
No items to show.	

More Remote Subnet :

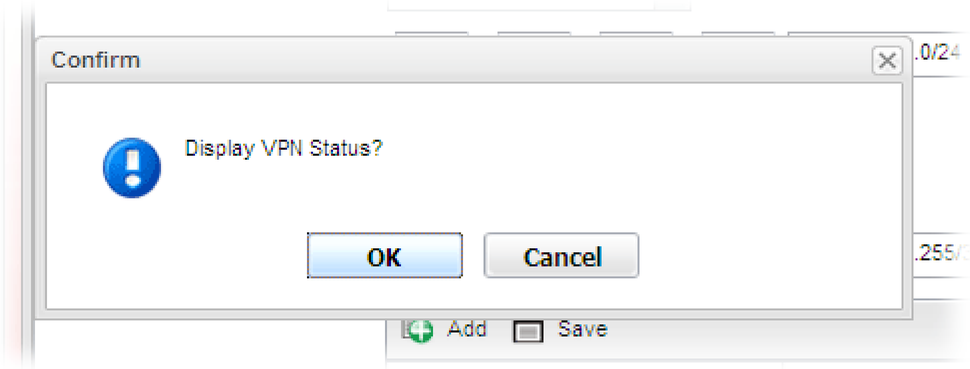
Auth Type : PSK (While Remote Host as 0.0.0.0, PSK will be defined in IPsec General Se

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the VPN profile.
Enable	Check this box to enable such profile.
WAN Profile	Choose a WAN profile to be used by such profile.
Local IP/Subnet Mask	Type the IP address and subnet mask of local host.
Local Next Hop	Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).
Remote Host	Type the WAN IP address for the remote host.
Remote IP / Subnet Mask	Type the LAN IP address and LAN subnet mask for the remote host.
More Remote Subnet	Add more remote subnet in this field if required.
Auth Type	The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile.
Certificate	Choose a local certificate from the drop down list if RSA is selected as Auth Type.
Preshared Key	Type a pre-shared key for authentication if PSK is selected as Auth Type.

Security Protocol	Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
DPD Delay	DPD means dead peer detection. It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.
DPD Timeout	It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

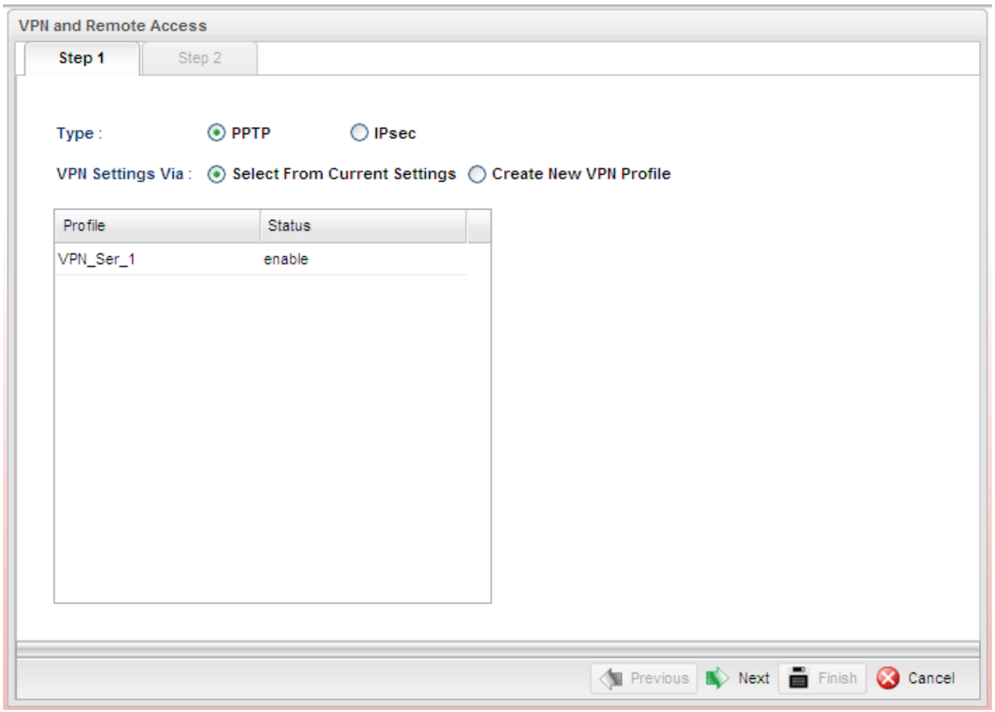
4. Fill in the required information on this page and click **Finish**. A pop-up window will appear.



Confirm

Display VPN Status?

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



VPN and Remote Access

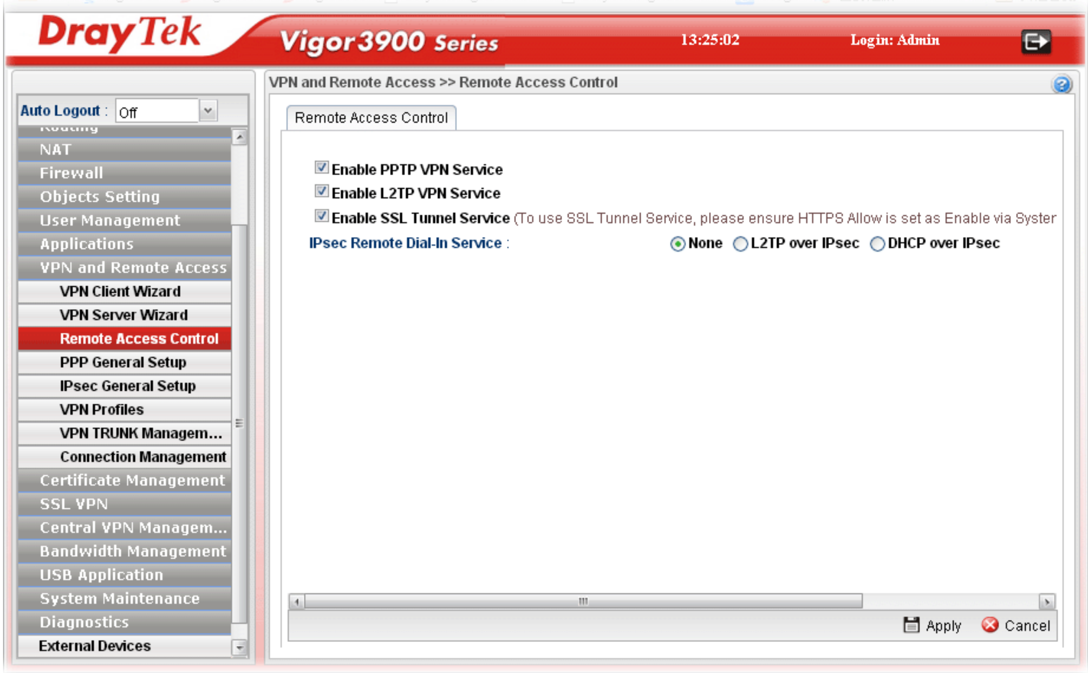
Type : ● PPTP ○ IPsec

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

Profile	Status
VPN_Ser_1	enable

4.9.3 Remote Access Control

Enable the necessary VPN service as you need. In default, PPTP VPN Service and L2TP VPN Service are enabled. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through.



VPN and Remote Access >> Remote Access Control

Remote Access Control

☑ Enable PPTP VPN Service

☑ Enable L2TP VPN Service

☑ Enable SSL Tunnel Service (To use SSL Tunnel Service, please ensure HTTPS Allow is set as Enable via Syster

IPsec Remote Dial-In Service : ● None ○ L2TP over IPsec ○ DHCP over IPsec

Available parameters are listed as follows:

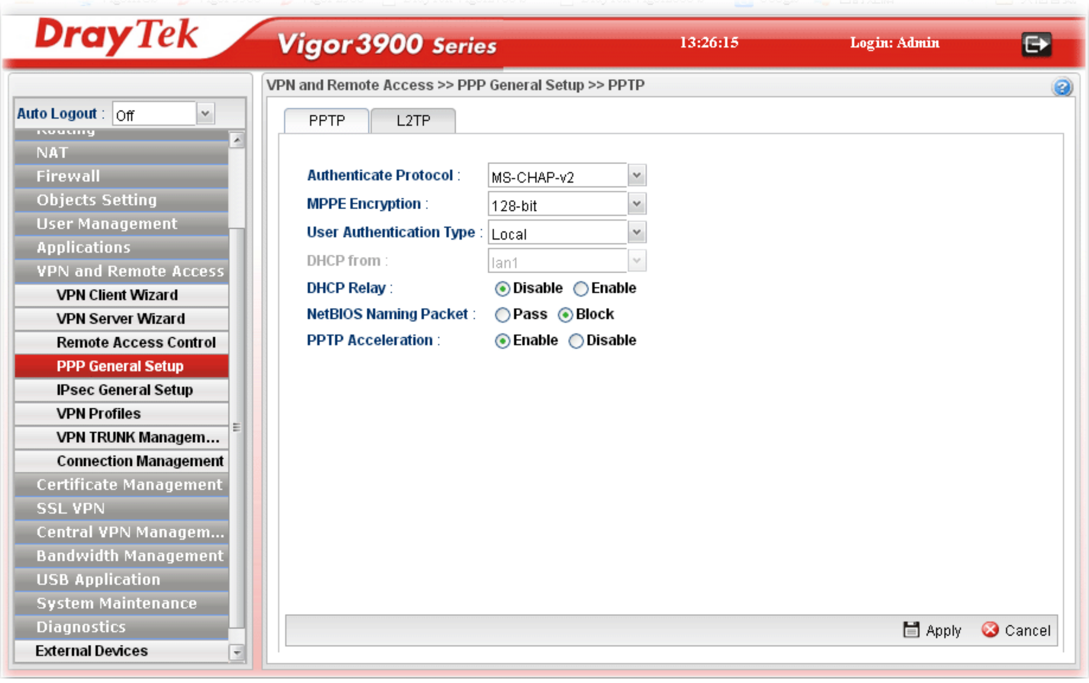
Item	Description
Enable PPTP VPN Service / **Enable L2TP VPN Service/** **Enable SSL Tunnel Service**	Check the box(es) to enable the service.
IPSec Remote Dial-In Service	Choose one of the services by clicking on the radio button.
Apply	Click it to save the configuration.
Cancel	Click it to discard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

4.9.4 PPP General Setup

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

4.9.4.1 PPTP

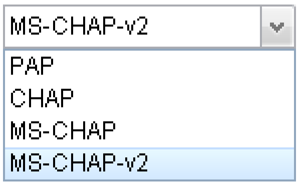
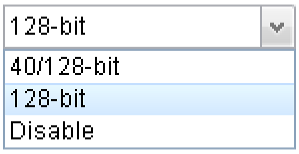
This page display current status for VPN tunnel built with PPTP protocol.

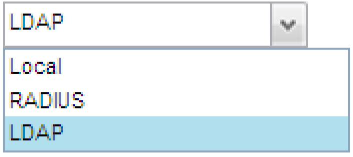


VPN and Remote Access >> PPP General Setup >> PPTP

Authenticate Protocol : MS-CHAP-v2
MPPE Encryption : 128-bit
User Authentication Type : Local
DHCP from : lan1
DHCP Relay : ● Disable ○ Enable
NetBIOS Naming Packet : ○ Pass ● Block
PPTP Acceleration : ● Enable ○ Disable

Available parameters are listed as follows:

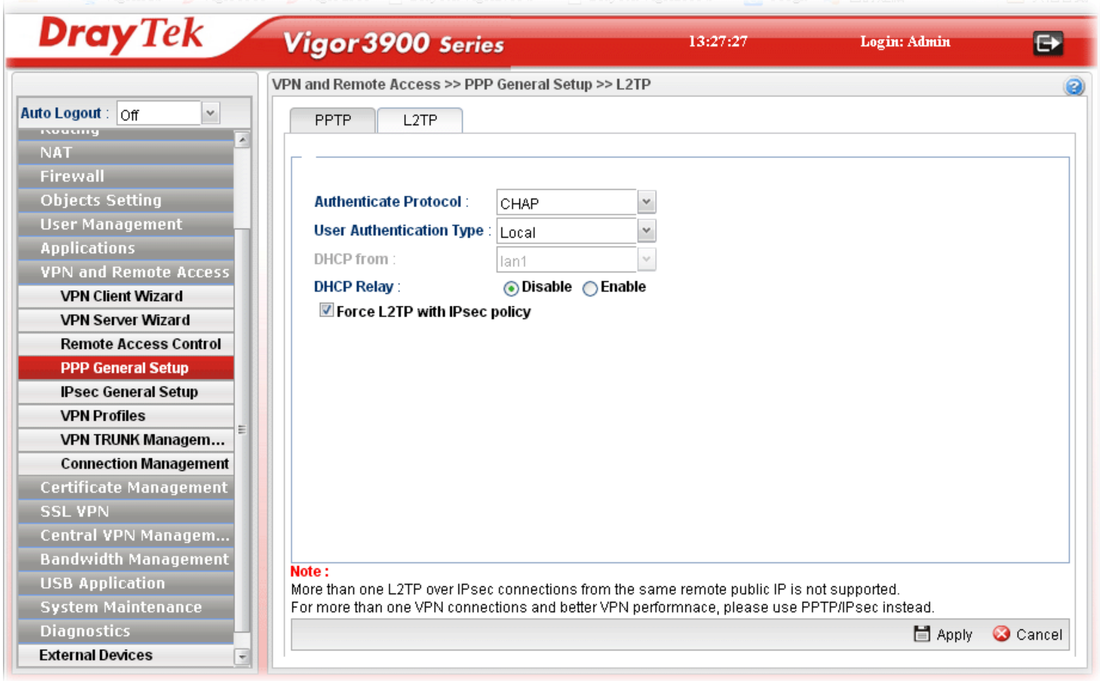
Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  MS-CHAP-v2 PAP CHAP MS-CHAP MS-CHAP-v2 **PAP -** It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP -** It means the router will attempt to 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.  128-bit 40/128-bit 128-bit Disable
User Authentication Type	Set user authentication to **Local** server, **RADIUS** server or **LDAP** server.

	
LDAP profiles	Choose a LDAP profile for PPTP Server if **LDAP** is selected as user authentication type. To clear the selected one, click × to remove current object selections.
LAN Profile	Choose a LAN profile for PPTP Server if **RADIUS** or **LDAP** is selected as user authentication type.
NetBIOS Naming Packet	**Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
PPTP Acceleration	**Enable –** Click it to make PPTP acceleration for VPN.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.9.4.2 L2TP

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



VPN and Remote Access >> PPP General Setup >> L2TP

Authenticate Protocol : CHAP

User Authentication Type : Local

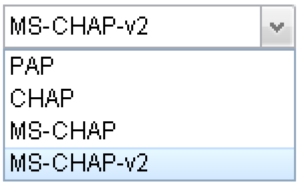
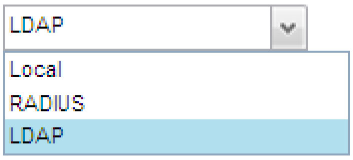
DHCP from : lan1

DHCP Relay : ● Disable ○ Enable

☑ Force L2TP with IPsec policy

Note :
More than one L2TP over IPsec connections from the same remote public IP is not supported.
For more than one VPN connections and better VPN performnace, please use PPTP/IPsec instead.

Available parameters are listed as follows:

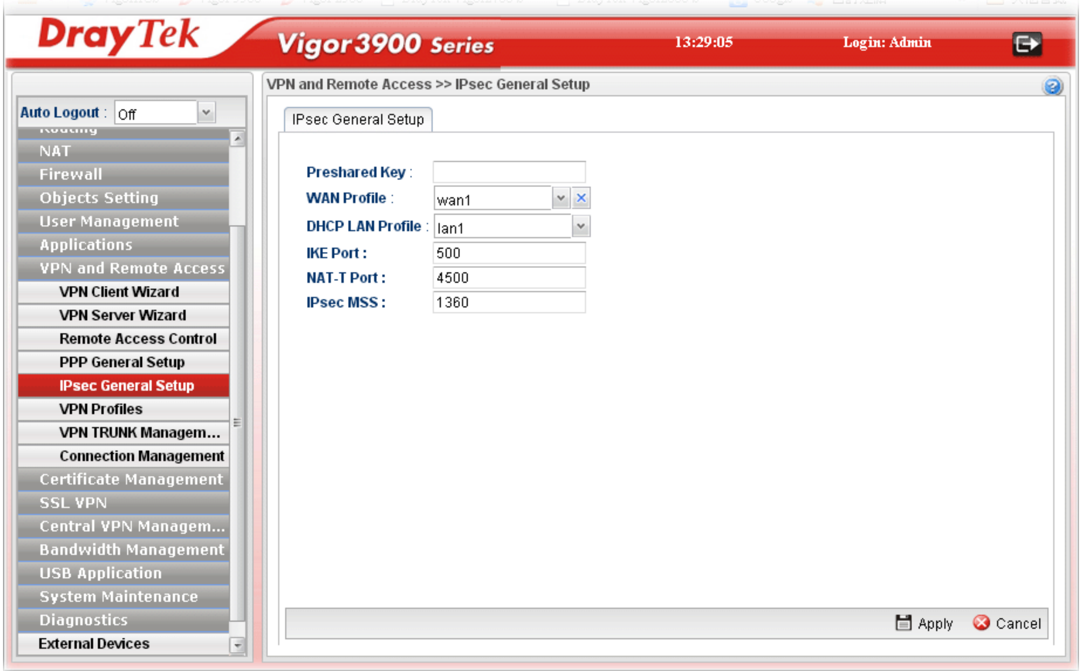
Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here.  **PAP -** It means the router will attempt to authenticate dial-in users with the PAP protocol. **CHAP -** It means the router will attempt to authenticate dial-in users with the CHAP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

DHCP Relay	**Enable -** Let the router assign IP address to every host in the LAN. **Disable -** Let you manually assign IP address to every host in the LAN.
DHCP Server Location	Choose the WAN/LAN interface for the DHCP server.
DHCP Server IP Address	It is available when **DHCP Relay** is enabled. Set the IP address of the DHCP server you are going to use so the relay agent can help to forward the DHCP request to the DHCP server.
Force L2TP with IPsec policy	If it is checked, the router will use L2TP with IPsec policy for VPN connection.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

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

4.9.5 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.



Preshared Key :
WAN Profile : wan1
DHCP LAN Profile : lan1
IKE Port : 500
NAT-T Port : 4500
IPsec MSS : 1360

Available parameters are listed as follows:

Item	Description
Preshared Key	Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key.

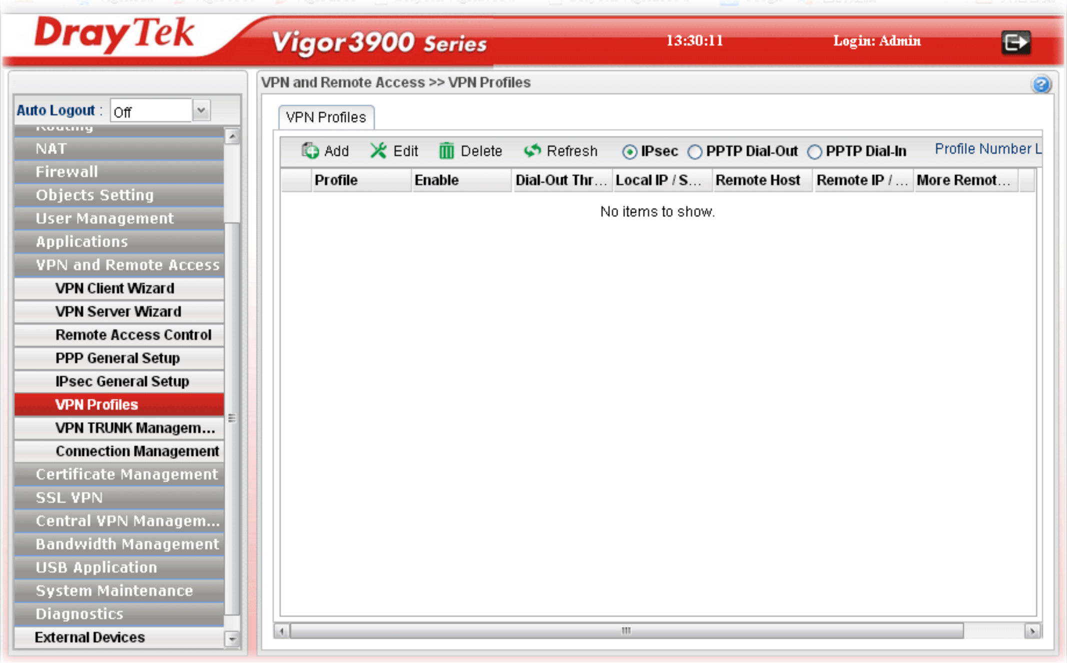
WAN Profile	Choose a WAN interface profile to be used. To clear the selected one, click ☒ to remove current profile selections.
DHCP LAN Profile	Choose one of the LAN profiles for VPN.
IKE Port	Type the UDP port number for Internet Key Exchange (IKE) traffic to the VPN server.
NAT-Port	Type the UDP port number for IPSec network address translator traversal (NAT-T) traffic.
IPSec MSS	Type the port number for IPSec MSS.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.9.6 VPN Profiles

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

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



Each item will be explained as follows:

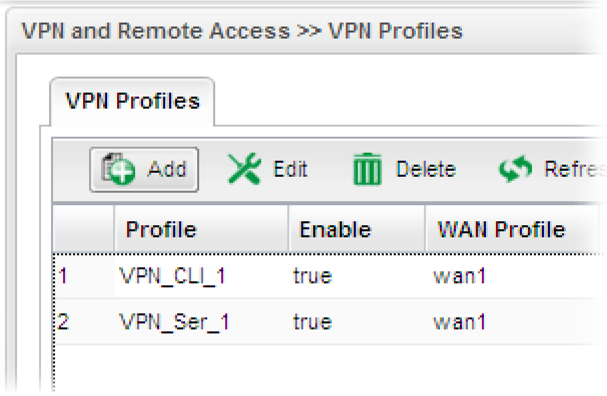
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected

	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 Number Limit	Display the total number (500) of the object profiles to be created.
Profile	Display the name of LAN to LAN profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Dial-Out Through	Display the WAN interface selected for the profile.
Local IP / Subnet Mask	Display the LAN IP address with subnet mask of this profile.
Remote Host	Display the name of the remote host of this profile.
Remote IP / Subnet Mask	Display the WAN IP address with subnet mask of this profile.
More Remote Subnet	Display other LAN IP addresses with subnet mask which can be used of this profile.

How to create an IPSec VPN profile

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

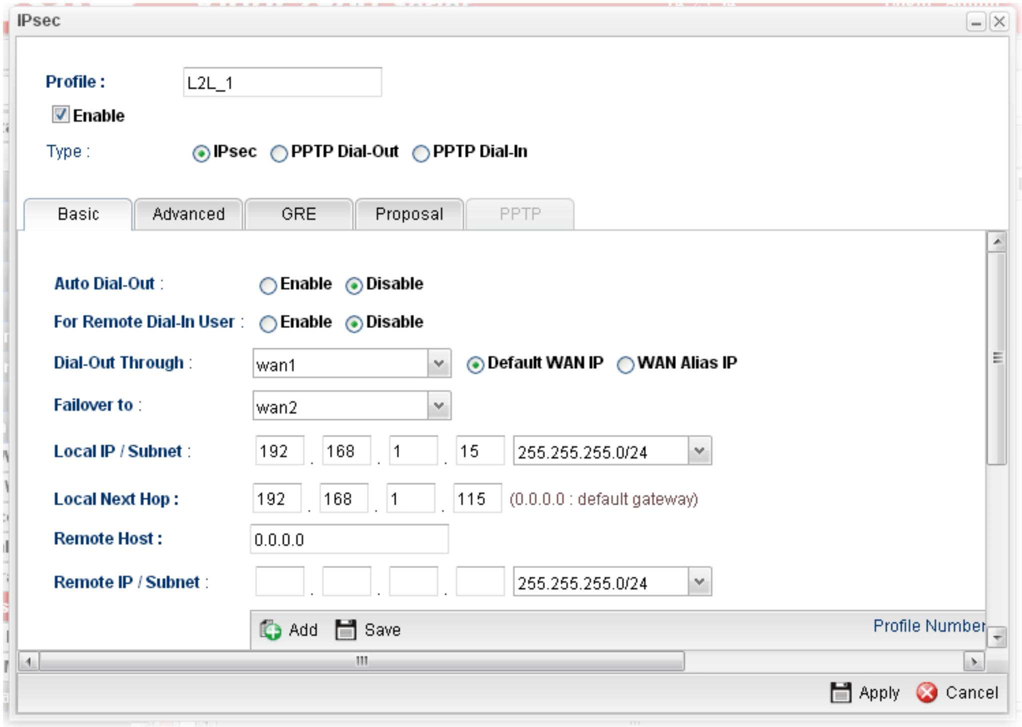
1. Open **VPN and Remote Access >> LAN to LAN.**
2. Simply click the **Add** button.



VPN and Remote Access >> VPN Profiles

	Profile	Enable	WAN Profile
1	VPN_CLI_1	true	wan1
2	VPN_Ser_1	true	wan1

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



Profile : L2L_1

☑ Enable

Type : ● IPsec ○ PPTP Dial-Out ○ PPTP Dial-In

Auto Dial-Out : ○ Enable ● Disable

For Remote Dial-In User : ○ Enable ● Disable

Dial-Out Through : wan1 ● Default WAN IP ○ WAN Alias IP

Failover to : wan2

Local IP / Subnet : 192 . 168 . 1 . 15 255.255.255.0/24

Local Next Hop : 192 . 168 . 1 . 115 (0.0.0.0 : default gateway)

Remote Host : 0.0.0.0

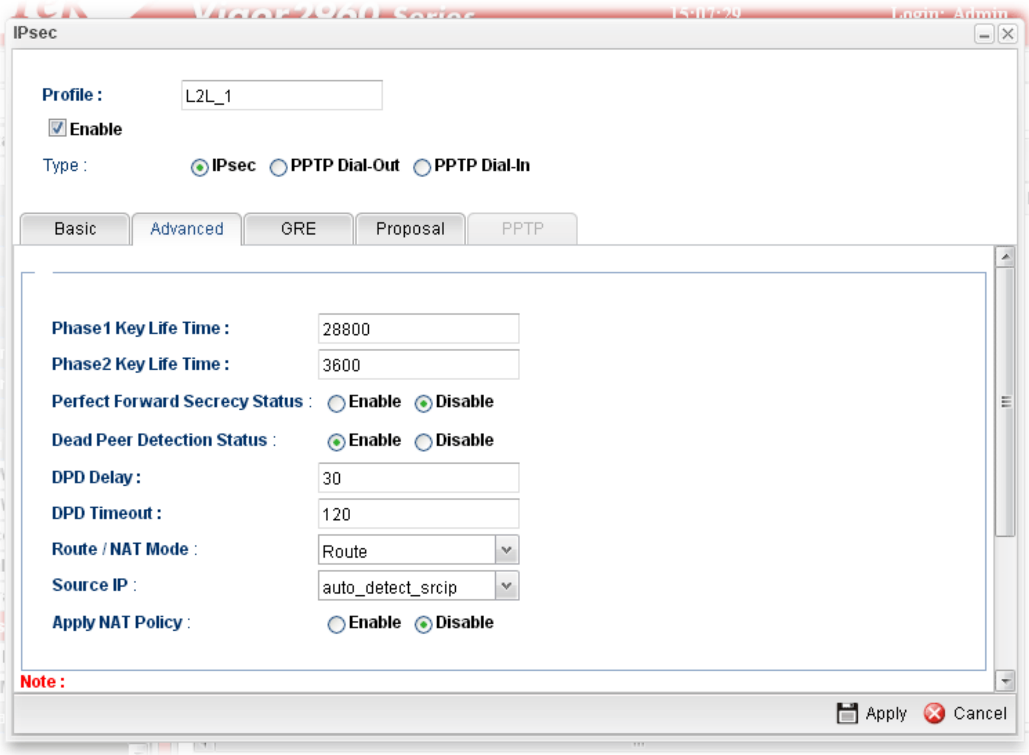
Remote IP / Subnet : . . . 255.255.255.0/24

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **IPSec** for this case.
Basic	**Always On** – Click **Enable** to make router always keeping connection. **For Remote Dial-In User-** Click **Enable** to allow the connection via IPSec remote dial-in host. **Dial-Out Through-** Choose a wan profile to be used by such profile. **Failover to** – Choose a wan profile which will lead the data passing through other WAN automatically when the selected WAN interface (in **Dial-Out Through**) is failover. **Local IP/Subnet -** Type the IP address and subnet mask of local host. **Local Next Hop -** Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank). **Remote Host -** Type the WAN IP address for the remote host. **Remote IP / Subnet Mask -** Type the LAN IP address and LAN subnet mask for the remote host. **More Remote Subnet** – Add more remote subnet in this

	field if required. **IKE Phase 1 -** Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode. **Auth Type -** The authentication to be used by Pre-Shared Key or RSA Signature. Choose **PSK** or **RSA** for such profile. **Local Certificate -** Choose a local certificate from the drop down list if RSA is selected as Auth Type. **Local Peer ID** –Type the ID for Vigor3900 which can be configured by the remote end. It is available for Aggressive Mode enabled only. **Remote Peer ID –** Peer ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters. It is available for Aggressive Mode enabled only. **Preshared Key** – Specify a key for IKE authentication if PSK is selected as Auth Type. **Security Protocol –** Choose **ESP** to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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



Profile : L2L_1

☑ Enable

Type : ● IPsec ○ PPTP Dial-Out ○ PPTP Dial-In

Phase1 Key Life Time : 28800

Phase2 Key Life Time : 3600

Perfect Forward Secrecy Status : ○ Enable ● Disable

Dead Peer Detection Status : ● Enable ○ Disable

DPD Delay : 30

DPD Timeout : 120

Route / NAT Mode : Route

Source IP : auto_detect_srcip

Apply NAT Policy : ○ Enable ● Disable

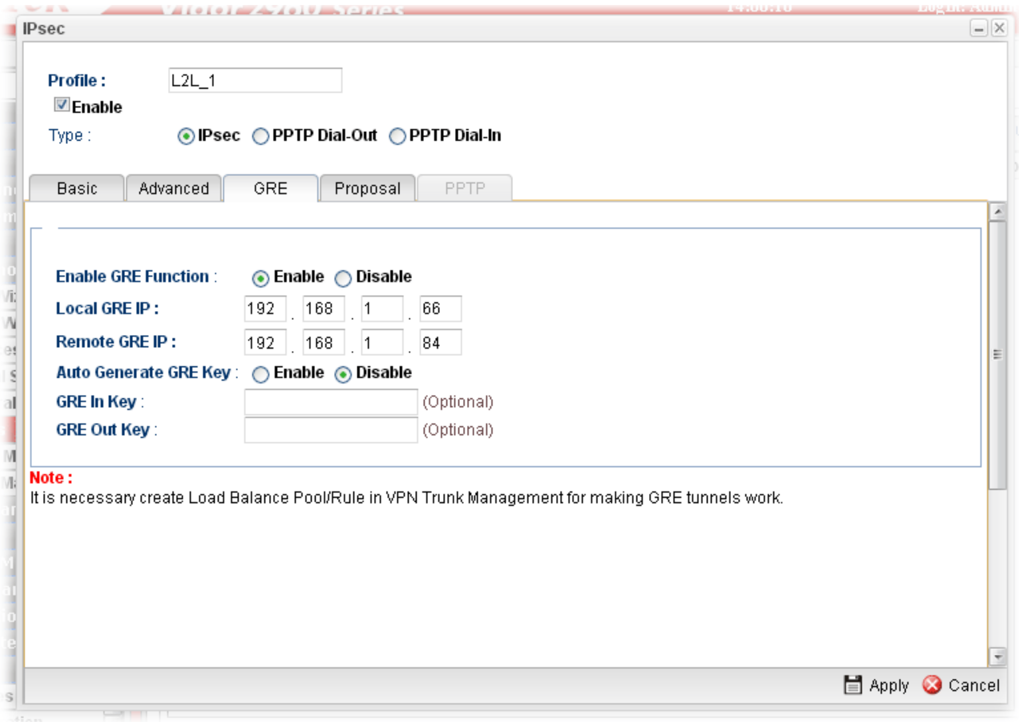
Note :

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. It is available only when Aggressive Mode is enabled.
Remote Peer ID	Peer ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters. It is available only when Aggressive Mode is enabled.
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.
Route/NAT Mode	If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.
Source IP	Choose one of the LAN profiles as a source IP.
Apply NAT Policy	**Enable** – This option allows for performing one-to-one NAT for all traffic flowing across the VPN. **Translated Local Network** – Specify the IP address with subnet mask of the network that all traffic will be translated into.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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



Profile : L2L_1

☑ Enable

Type : ● IPsec ○ PPTP Dial-Out ○ PPTP Dial-In

Enable GRE Function : ● Enable ○ Disable

Local GRE IP : 192 . 168 . 1 . 66

Remote GRE IP : 192 . 168 . 1 . 84

Auto Generate GRE Key : ○ Enable ● Disable

GRE In Key : (Optional)

GRE Out Key : (Optional)

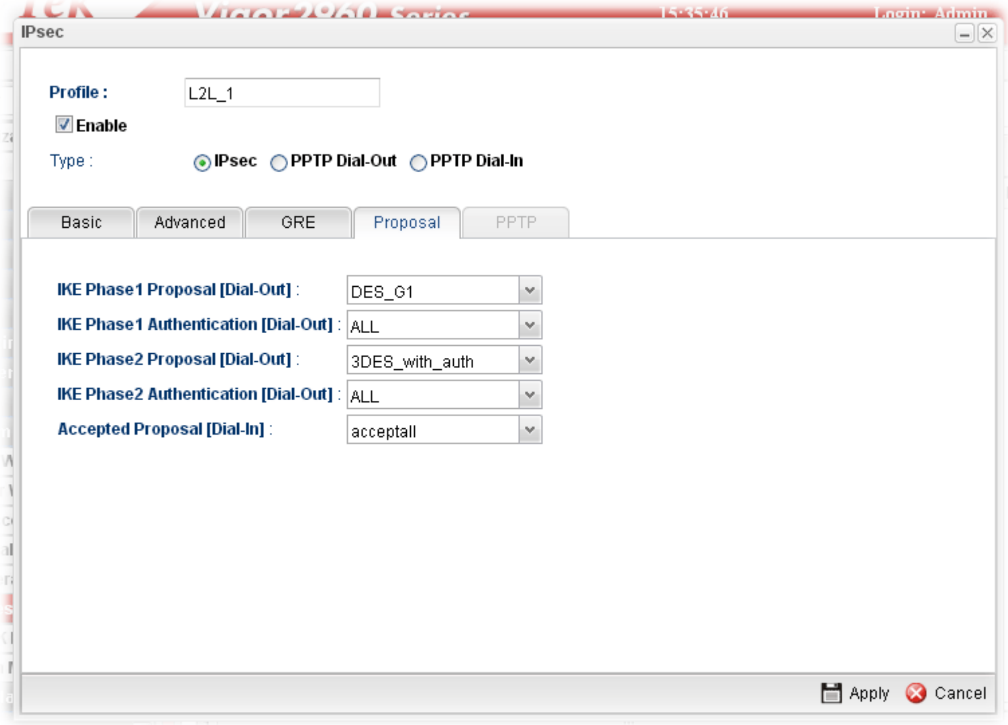
Note :
It is necessary create Load Balance Pool/Rule in VPN Trunk Management for making GRE tunnels work.

Available parameters are listed as follows:

Item	Description
Enable GRE Function	Check the box to enable the function.

Local GRE IP	The virtual IP address of the router, specified for this tunnel.
Remote GRE IP	The virtual IP address of the remote client, specified for this tunnel.
Auto Generate GRE Key	Click **Enable** to generate the GRE key by the system automatically. If you click **Disable**, you need to type GRE key manually.
GRE In Key	Type the hexadecimal number as GRE In Key. This value is used for the router to authenticate the source of the packet. The length is 4 bytes.
GRE Out Key	Type the hexadecimal number as GRE Out Key. This value is used for the remote client to authenticate the source of the packet. The length is 4 bytes.

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



Profile : L2L_1

☑ Enable

Type : ● IPsec ○ PPTP Dial-Out ○ PPTP Dial-In

IKE Phase1 Proposal [Dial-Out] : DES_G1

IKE Phase1 Authentication [Dial-Out] : ALL

IKE Phase2 Proposal [Dial-Out] : 3DES_with_auth

IKE Phase2 Authentication [Dial-Out] : ALL

Accepted Proposal [Dial-In] : acceptall

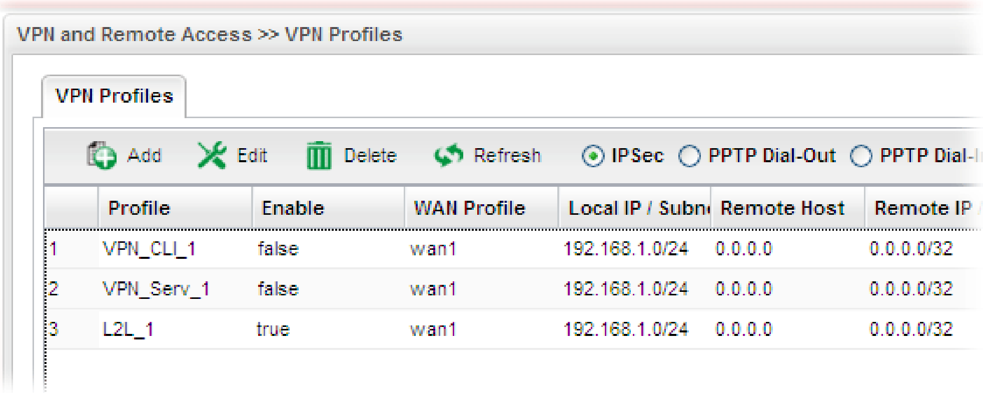
Available parameters are listed as follows:

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.

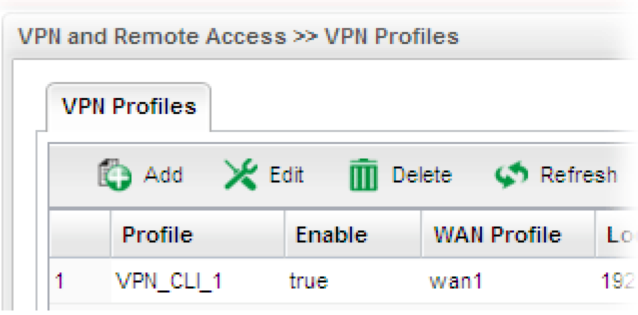


	Profile	Enable	WAN Profile	Local IP / Subn	Remote Host	Remote IP /
1	VPN_CLI_1	false	wan1	192.168.1.0/24	0.0.0.0	0.0.0.0/32
2	VPN_Serv_1	false	wan1	192.168.1.0/24	0.0.0.0	0.0.0.0/32
3	L2L_1	true	wan1	192.168.1.0/24	0.0.0.0	0.0.0.0/32

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

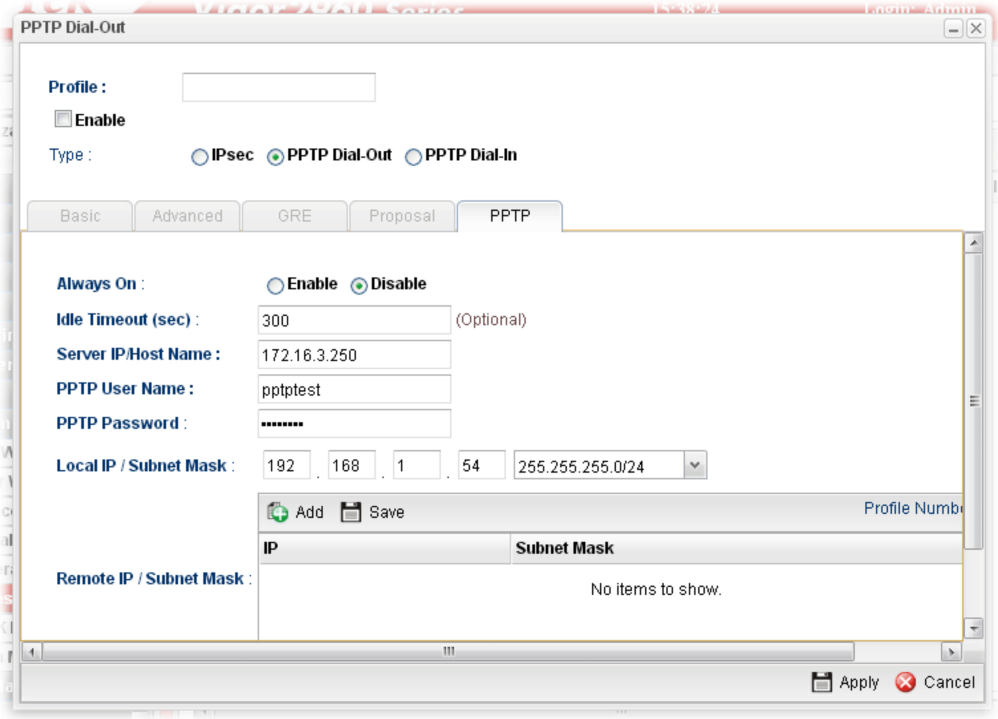
Below will guide you to create a PPTP dial-out profile for VPN connection:

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



	Profile	Enable	WAN Profile	Lo
1	VPN_CLI_1	true	wan1	192

3. The following dialog will appear.



PPTP Dial-Out

Profile :

□ Enable

Type : ○ IPsec ● PPTP Dial-Out ○ PPTP Dial-In

Always On : ○ Enable ● Disable

Idle Timeout (sec) : 300 (Optional)

Server IP/Host Name : 172.16.3.250

PPTP User Name : pptptest

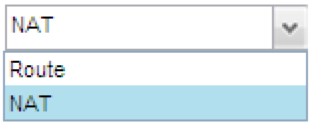
PPTP Password : ••••••••

Local IP / Subnet Mask : 192 . 168 . 1 . 54 255.255.255.0/24

Remote IP / Subnet Mask :

IP	Subnet Mask
No items to show.	

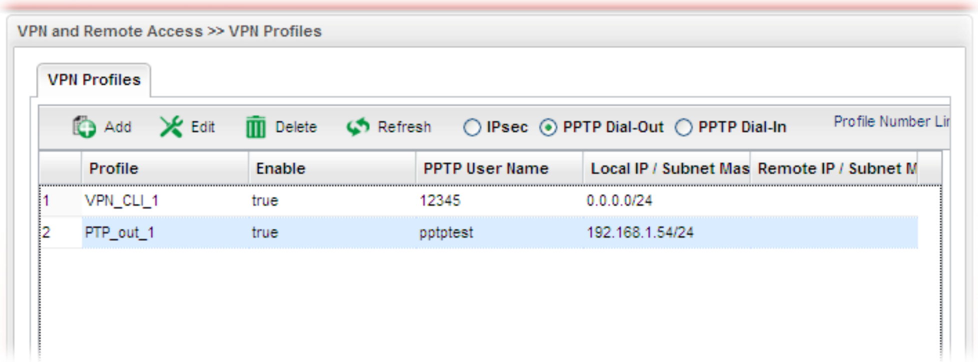
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **PPTP Dial-Out** for this case.
PPTP	**Always On** - Click **Enable** to make the profile being always on. **Idle Timeout (sec)** - If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds. **Server IP/Host Name** - Type the IP address or the host name of PPTP 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.



VPN and Remote Access >> VPN Profiles

VPN Profiles

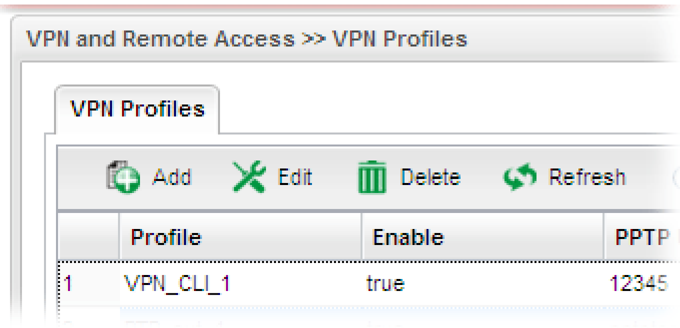
Add Edit Delete Refresh ○ IPsec ● PPTP Dial-Out ○ PPTP Dial-In Profile Number Lir

	Profile	Enable	PPTP User Name	Local IP / Subnet Mas	Remote IP / Subnet M
1	VPN_CLI_1	true	12345	0.0.0.0/24	
2	PTP_out_1	true	pptptest	192.168.1.54/24	

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.



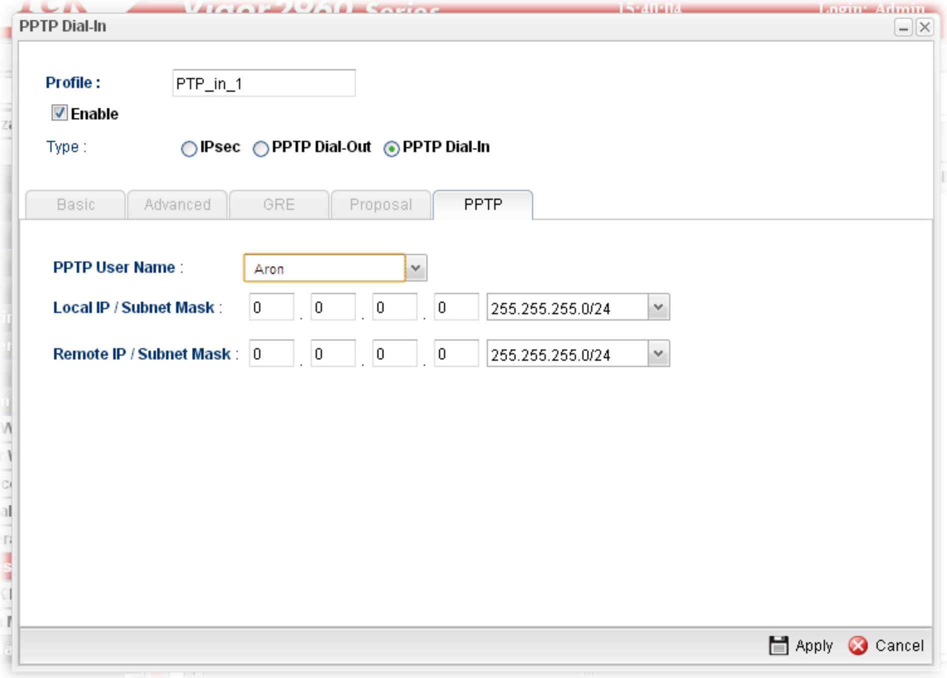
VPN and Remote Access >> VPN Profiles

VPN Profiles

Add Edit Delete Refresh

	Profile	Enable	PPTP
1	VPN_CLI_1	true	12345

3. The following dialog will appear.



PPTP Dial-In

Profile : PTP_in_1

☑ Enable

Type : ○ IPsec ○ PPTP Dial-Out ● PPTP Dial-In

PPTP User Name : Aron

Local IP / Subnet Mask : 0 . 0 . 0 . 0 255.255.255.0/24

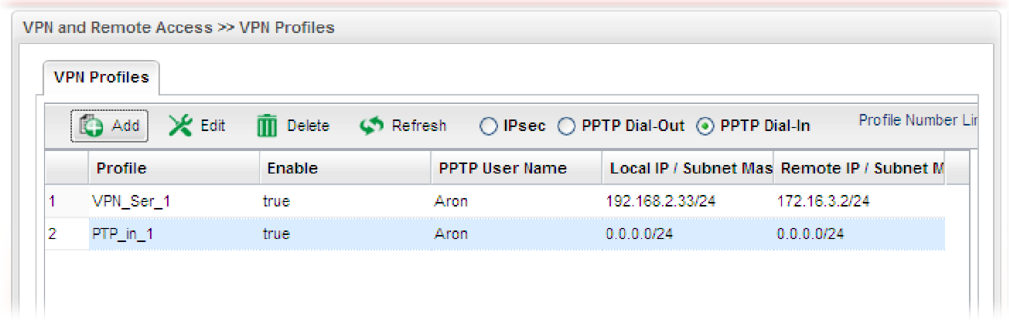
Remote IP / Subnet Mask : 0 . 0 . 0 . 0 255.255.255.0/24

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable this profile.
Type	There are three types offered here for you to choose. Please choose **PPTP Dial-In** for this case.
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.


VPN and Remote Access >> VPN Profiles

VPN Profiles

Add Edit Delete Refresh ○ IPsec ○ PPTP Dial-Out ● PPTP Dial-In Profile Number Lir

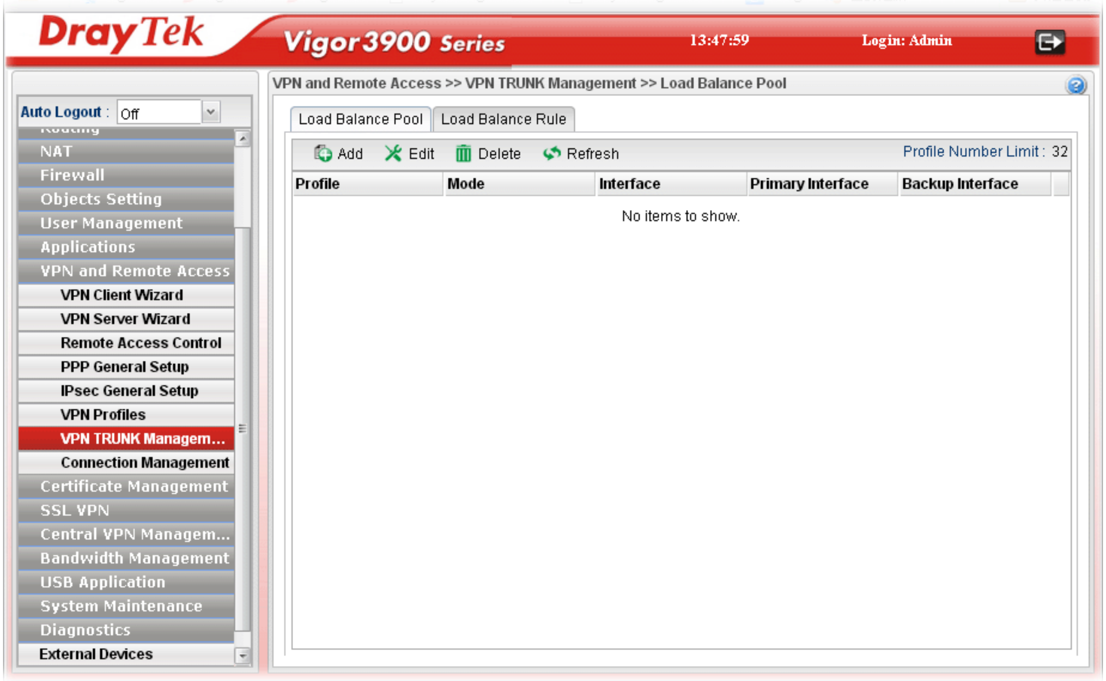
	Profile	Enable	PPTP User Name	Local IP / Subnet Mas	Remote IP / Subnet M
1	VPN_Ser_1	true	Aron	192.168.2.33/24	172.16.3.2/24
2	PTP_in_1	true	Aron	0.0.0.0/24	0.0.0.0/24

4.9.7 VPN Trunk Management

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

4.9.7.1 Load Balance Pool

This page allows the user to integrate **several** WAN profiles as a pool profile specified with the function of load balance or failover.



VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool

Load Balance Pool | Load Balance Rule

Add Edit Delete Refresh Profile Number Limit : 32

Profile	Mode	Interface	Primary Interface	Backup Interface

No items to show.

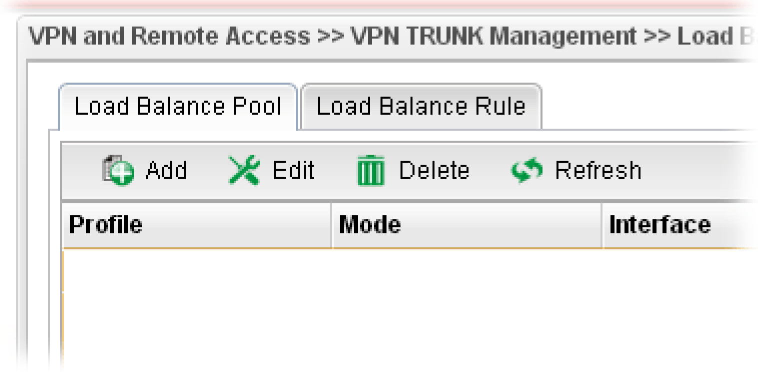
Each item will be explained as follows:

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

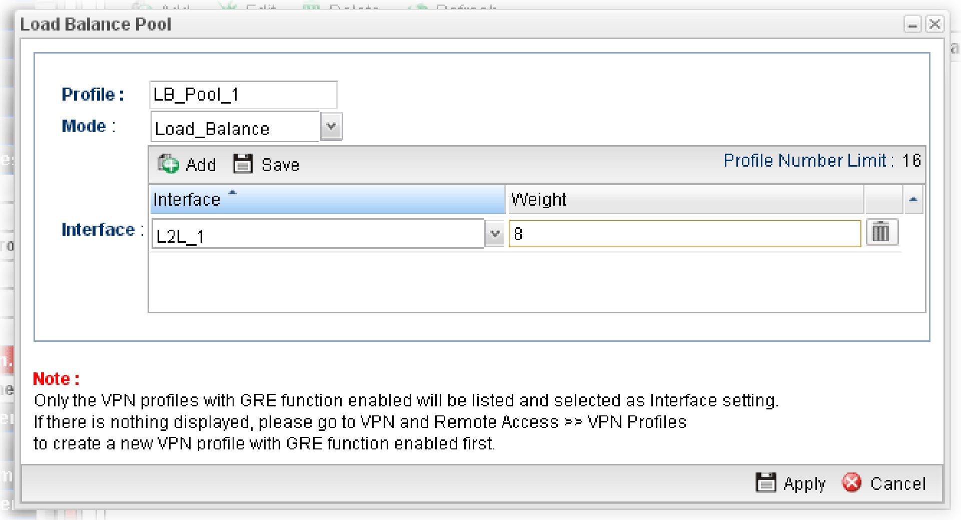
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Profile	Display the name of the profile.
Mode	Display which mode (load_balance or failover) is selected.
Interface	Display the name of the Load Balance profile grouped under such pool profile.
Primary Interface	Display the primary interface for failover.
Backup Interface	Display the backup interface for failover.

How to add a Load Balance Pool Profile

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



3. The following dialog will appear.



Profile : LB_Pool_1

Mode : Load_Balance

Profile Number Limit : 16

Interface : L2L_1 | Weight: 8

Note :
Only the VPN profiles with GRE function enabled will be listed and selected as Interface setting.
If there is nothing displayed, please go to VPN and Remote Access >> VPN Profiles
to create a new VPN profile with GRE function enabled first.

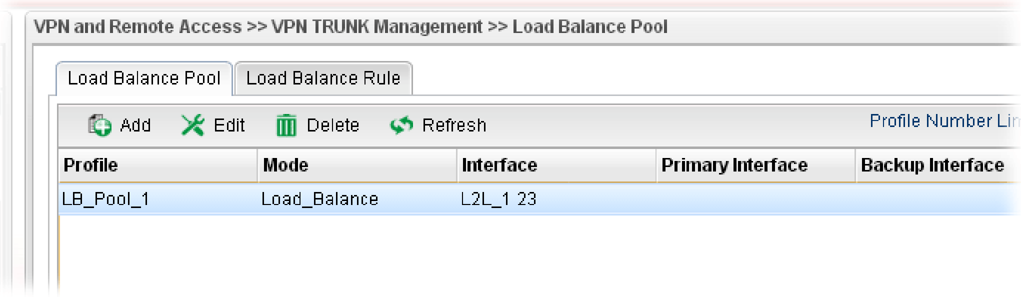
Available settings are listed below:

Item	Description
Profile	Type the name of the profile (e.g., LB_Pool_1, within 10 characters including digit, letter, and underline).
Mode	Choose Load_Balance or Failover. **Load_Balance** **Interface** – Choose VPN profile(s) as the interface. Note: Only the VPN profiles with GRE function enabled will be listed and selected as Interface setting. If there is nothing displayed, please go to VPN and Remote Access>>VPN Profiles to create a new VPN profile with GRE function enabled first. **Weight** – Type a value in such field. **Failover** **Primary Interface / Backup Interface -** Use the drop down list to specify the VPN profiles for Primary Interface and Backup Interface respectively.

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

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

5. A new profile has been created.



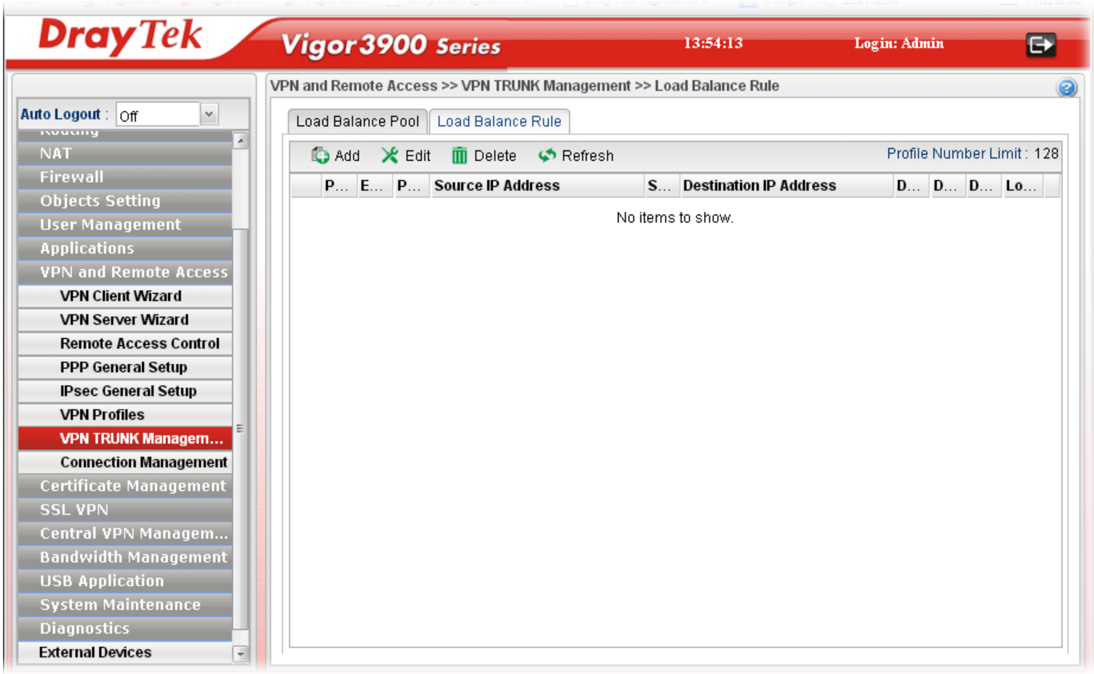
VPN and Remote Access >> VPN TRUNK Management >> Load Balance Pool

Profile	Mode	Interface	Primary Interface	Backup Interface
LB_Pool_1	Load_Balance	L2L_1 23		

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

4.9.7.2 Load Balance Rule

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



Each item will be explained as follows:

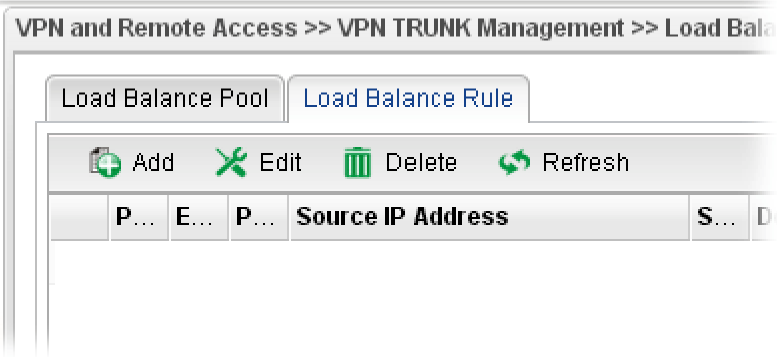
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (128) of the profiles to be created.
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Protocol	Display the protocol configured by such profile.
Source IP Address	Display the source IP address specified for this profile.
Source Mask	Display the subnet mask address specified for the source IP of this entry.
Destination IP Address	Display the destination IP address specified for this entry.

Destination Mask	Display the subnet mask address specified for the destination IP of this entry.
Destination Port Start	Display the start point specified in the **Dest Port Range** for this entry.
Destination Port End	Display the end point specified in the **Dest Port Range** for this entry.
Load Balance Pool	Display the selection of load balance pool.

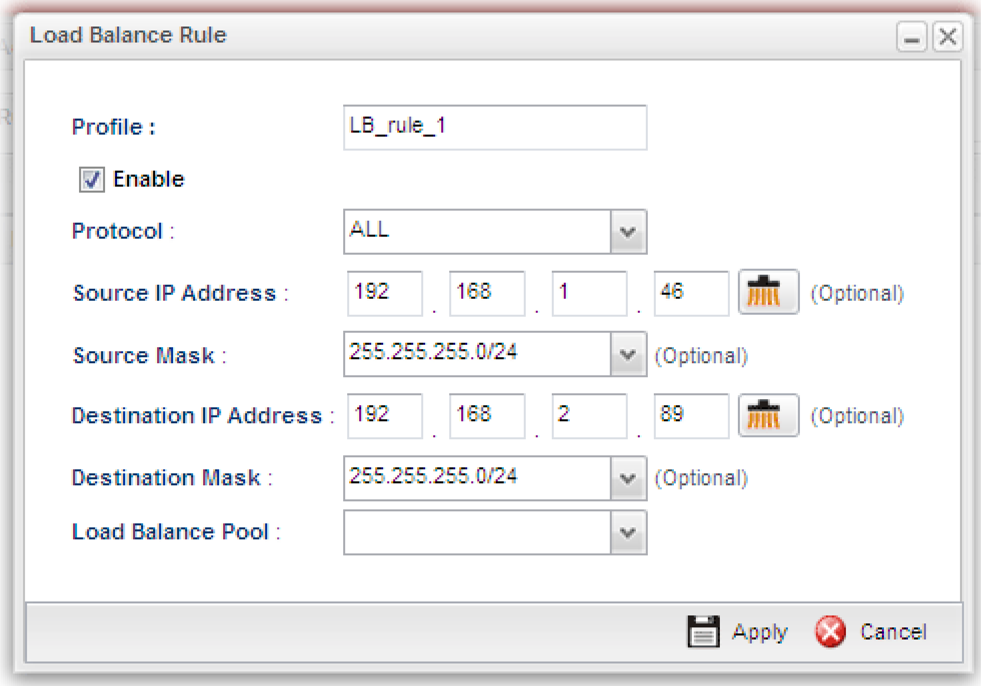
How to add a Load Balance Rule profile

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

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



3. The following dialog will appear.


Load Balance Rule

Profile : LB_rule_1

☑ Enable

Protocol : ALL

Source IP Address : 192 . 168 . 1 . 46 (Optional)

Source Mask : 255.255.255.0/24 (Optional)

Destination IP Address : 192 . 168 . 2 . 89 (Optional)

Destination Mask : 255.255.255.0/24 (Optional)

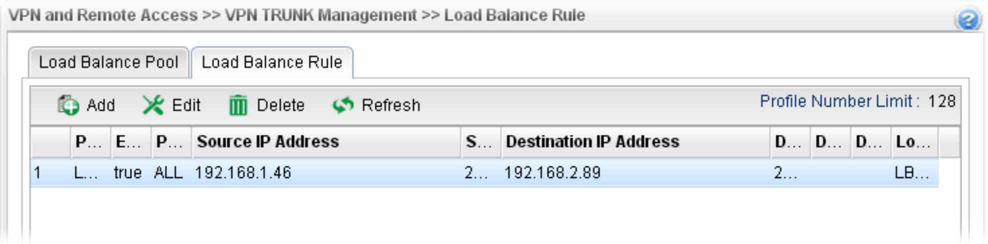
Load Balance Pool :

Available parameters are listed as follows:

Item	Description

Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
Protocol	Choose the protocol for such profile.
Source IP Address	Type the source IP address specified for this profile.
Source Mask	Type the subnet mask address specified for the source IP.
Destination IP Address	Type the destination IP address specified for this entry.
Destination Mask	Type the subnet mask address specified for the destination IP.
Destination Port Start	Type the start point.
Destination Port End	Type the end point.
Load Balance Pool	Use the drop down list to choose one profile configured in load balance pool. Then, such rule will be applied by the pool.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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



VPN and Remote Access >> VPN TRUNK Management >> Load Balance Rule

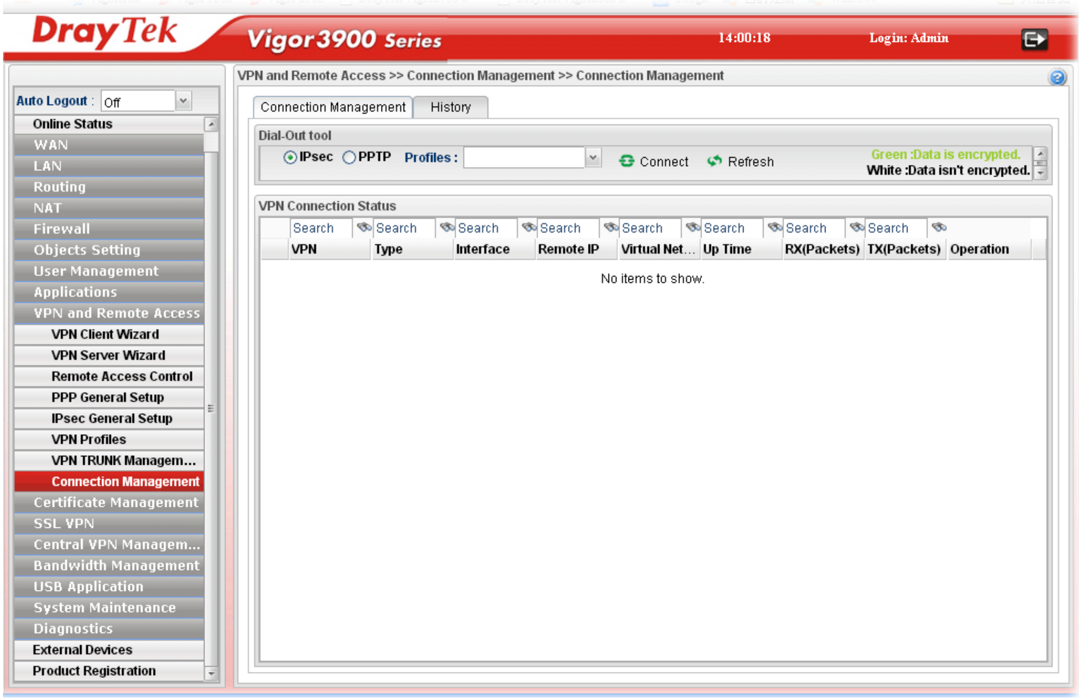
Profile Number Limit : 128

	P...	E...	P...	Source IP Address	S...	Destination IP Address	D...	D...	D...	Lo...
1	L...	true	ALL	192.168.1.46	2...	192.168.2.89	2...			LB...

4.9.8 Connection Management

4.9.8.1 Connection Management

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



Auto Logout : Off

VPN and Remote Access >> Connection Management >> Connection Management

Dial-Out tool

● IPsec ○ PPTP Profiles :

Green :Data is encrypted.
White :Data isn't encrypted.

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Net...	Up Time	RX(Packets)	TX(Packets)	Operation

No items to show.

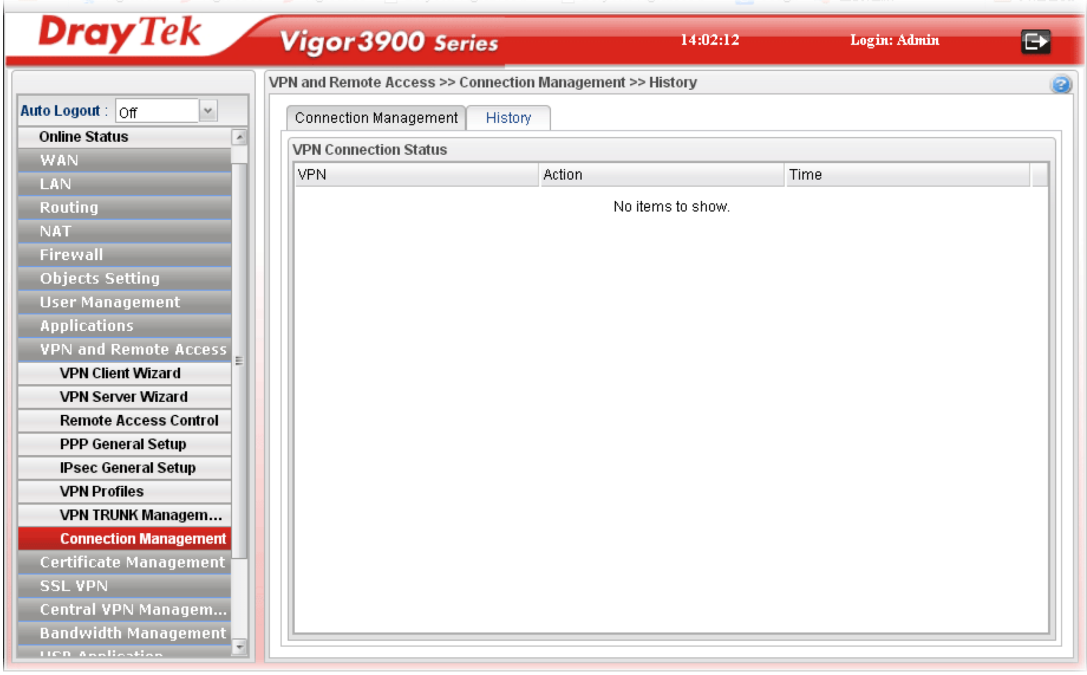
Each item will be explained as follows:

Item	Description
IPSec	Click it to perform IPSec VPN connection.
PPTP	Click it to perform PPTP VPN connection.
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.
Refresh	Renew current web page.
VPN	Display the name of VPN profile.
Type	Display the connection type (PPTP or IPSec) for such VPN profile.
Interface	Display the WAN interface for such VPN profile.
Remote IP	Display the remote IP configure by VPN profile.
Virtual Network	Display the virtual network established by such VPN profile.
Up Time	Display the connection time of this VPN tunnel.
RX (Packets)	Display the total received packets through this VPN.
TX (Packets)	Display the total transmitted packets through this VPN.

Disconnect	Terminate the VPN connection.
Operation	Display the icons to terminate / view the VPN profile.

4.9.8.2 History

This page displays the history of VPN connection.



VPN and Remote Access >> Connection Management >> History

VPN Connection Status

VPN	Action	Time

No items to show.

Each item will be explained as follows:

Item	Description
VPN	Display the name of VPN profile.
Action	Display the connection status (UP or DOWN) of VPN profile.
Time	Display the time the VPN profile connects/disconnects.

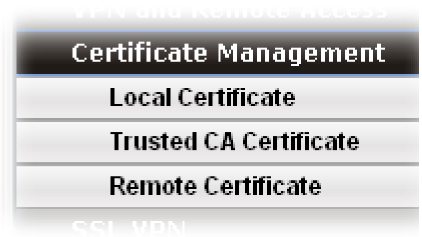
4.10 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.

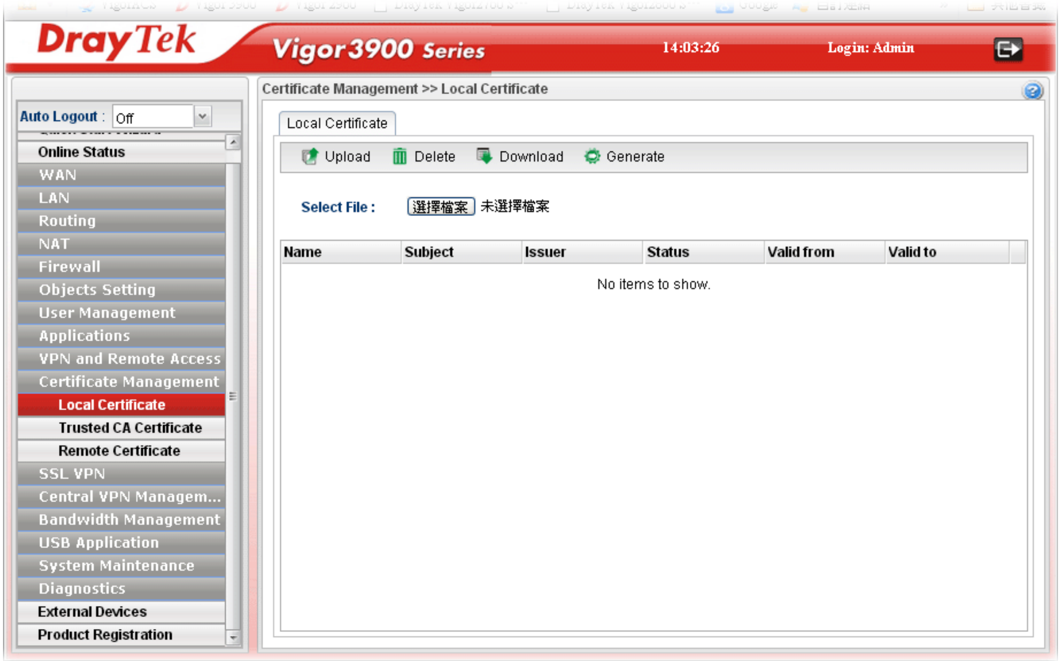


Local certificate is created by the end user and must be signed by a trusted CA center. Vigor3900 can serve as a trusted CA and is called with “Root CA”. Therefore, any user can ask for certificate signed by Vigor3900.

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

4.10.1 Local Certificate

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



Name	Subject	Issuer	Status	Valid from	Valid to

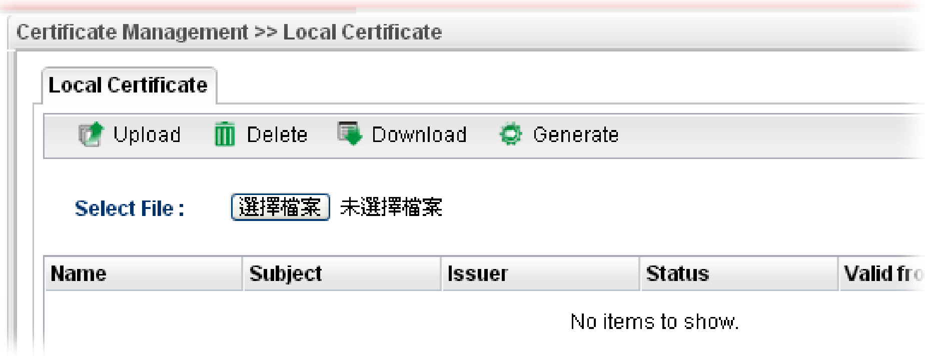
No items to show.

Each item will be explained as follows:

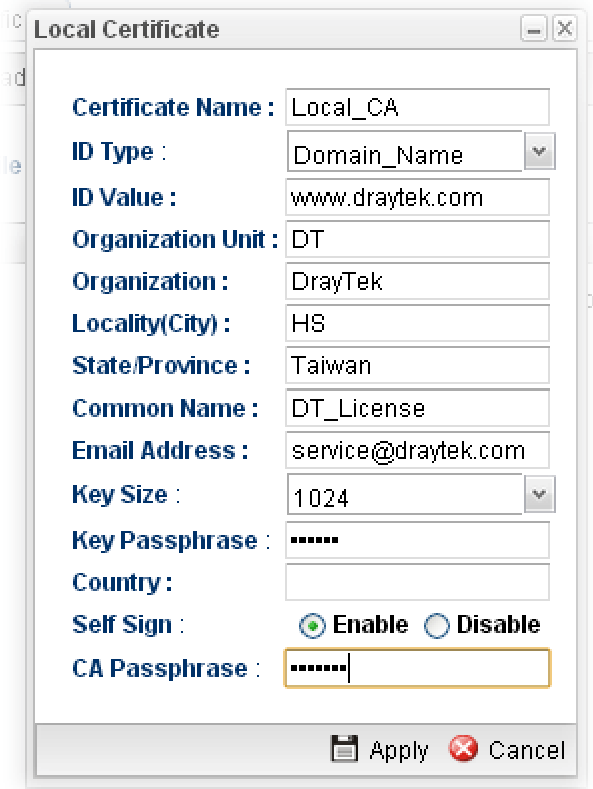
Item	Description
Upload	Allow you to upload current configuration to the host as a CA certificate.
Delete	Remove the selected item of Trusted CA listed below.
Download	Allow you to download an existing CA certificate to the router.
Generate	Open another web page for generating the local certificate.
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.



Certificate Name : Local_CA

ID Type : Domain_Name

ID Value : www.draytek.com

Organization Unit : DT

Organization : DrayTek

Locality(City) : HS

State/Province : Taiwan

Common Name : DT_License

Email Address : service@draytek.com

Key Size : 1024

Key Passphrase : ••••••

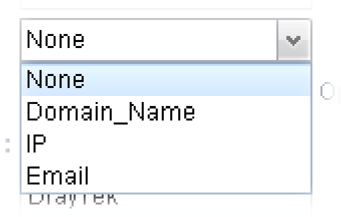
Country :

Self Sign : ● Enable ○ Disable

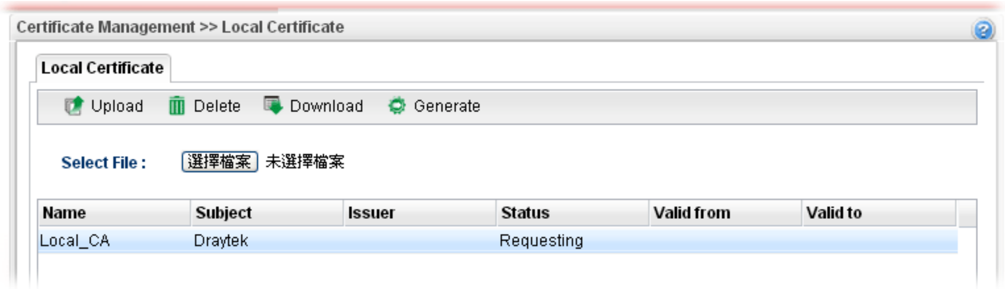
CA Passphrase : •••••••

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.

	 None None Domain_Name IP Email
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.
Key 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.
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.
CA 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.



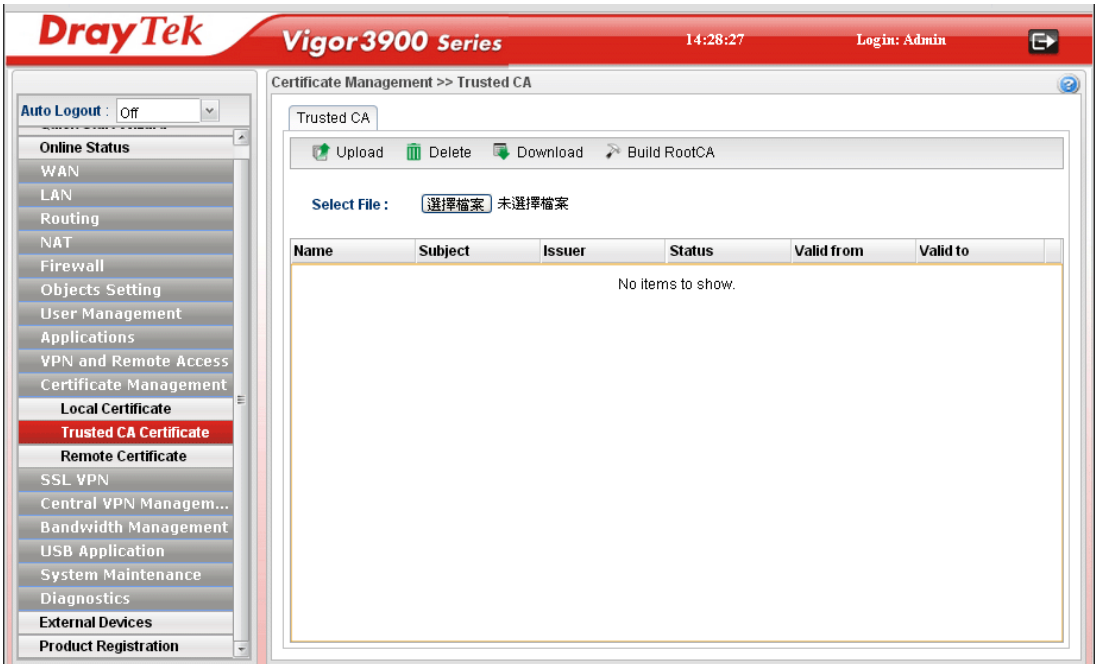
Select File : 選擇檔案 未選擇檔案

Name	Subject	Issuer	Status	Valid from	Valid to
Local_CA	Draytek		Requesting		

4.10.2 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**.



Select File : 選擇檔案 未選擇檔案

Name	Subject	Issuer	Status	Valid from	Valid to

No items to show.

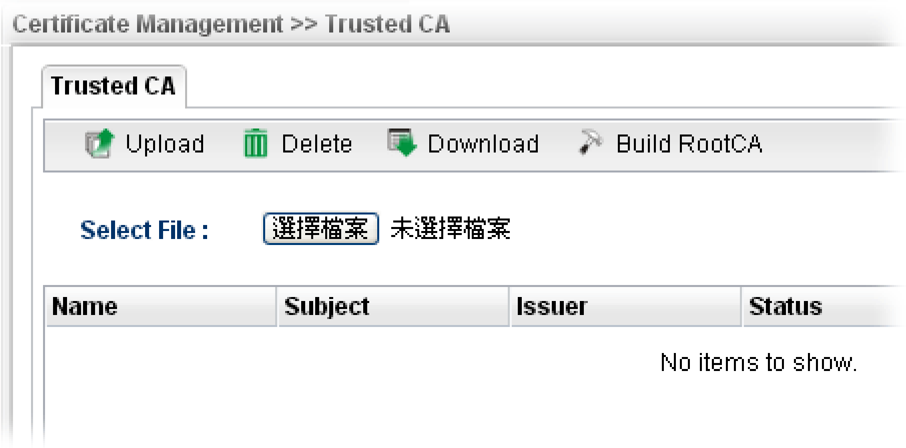
Each item will be explained as follows:

Item	Description
Upload	After choosing the certificate file, click this button to upload onto the router.
Delete	Remove the selected item of trusted CA listed below.
Download	Allow you to download an existing trusted CA certificate to the router.
Build RootCA	Allow to create a new CA certificate as Root CA.
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.



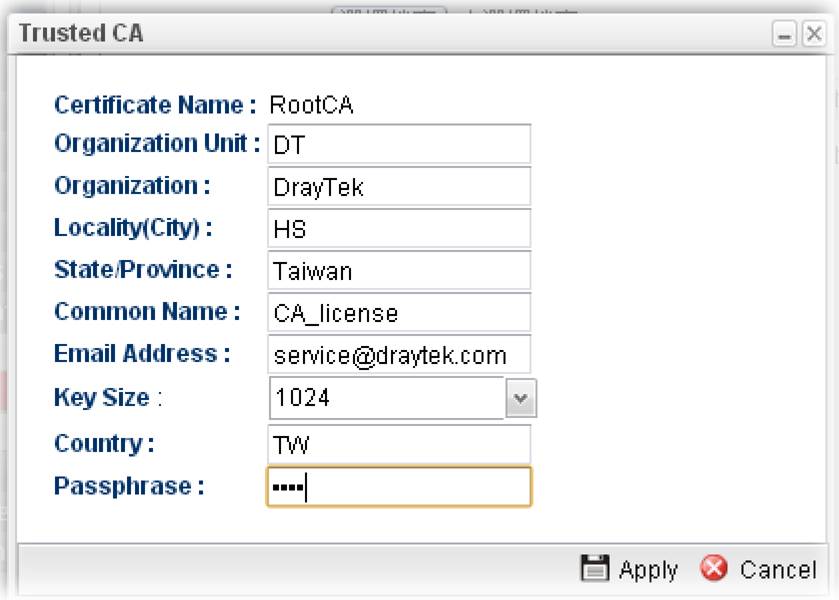
Certificate Management >> Trusted CA

Select File : 選擇檔案 未選擇檔案

Name	Subject	Issuer	Status

No items to show.

3. The following dialog will appear.



Trusted CA

Certificate Name :	RootCA
Organization Unit :	DT
Organization :	DrayTek
Locality(City) :	HS
State/Province :	Taiwan
Common Name :	CA_license
Email Address :	service@draytek.com
Key Size :	1024
Country :	TW
Passphrase :	••••

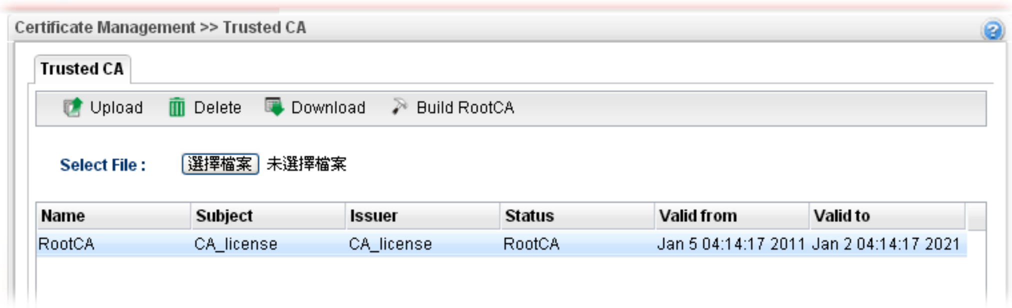
Available parameters are listed as follows:

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.

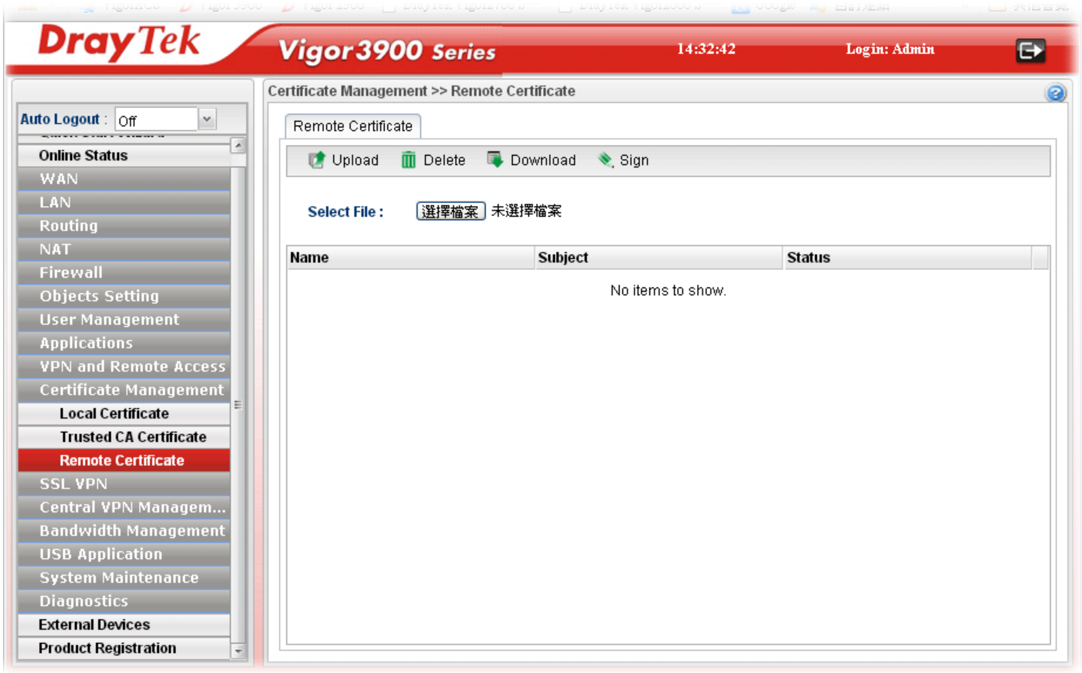


Select File : 選擇檔案 未選擇檔案

Name	Subject	Issuer	Status	Valid from	Valid to
RootCA	CA_license	CA_license	RootCA	Jan 5 04:14:17 2011	Jan 2 04:14:17 2021

4.10.3 Remote Certificate

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



Select File : 未選擇檔案

Name	Subject	Status

No items to show.

Each item will be explained as follows:

Item	Description
Upload	Allow you to upload current configuration to the host as a remote certificate.
Delete	Remove the selected item of remote certificate listed below.
Download	Allow you to download an existing certificate to the router.
Sign	Allow you to sign a requested certificate.
Select 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.

4.11 SSL VPN

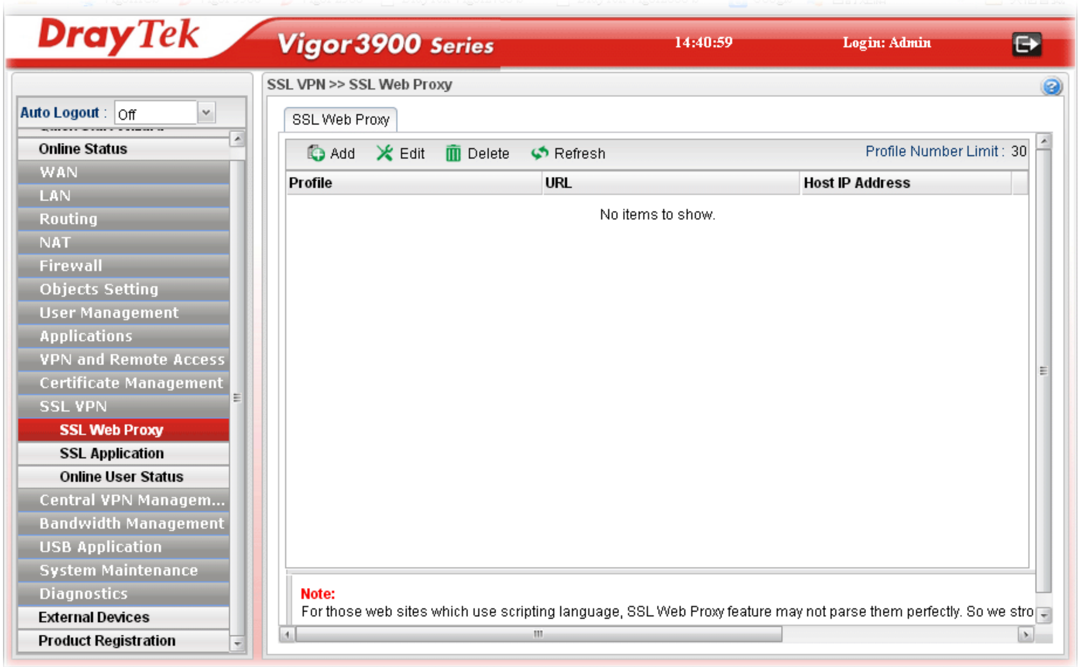
An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

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.

4.11.1 SSL Web Proxy

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



No items to show.

Note:
For those web sites which use scripting language, SSL Web Proxy feature may not parse them perfectly. So we stro

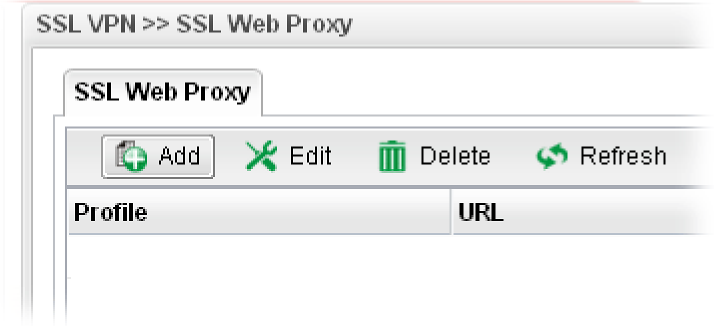
Each item will be explained as follows:

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

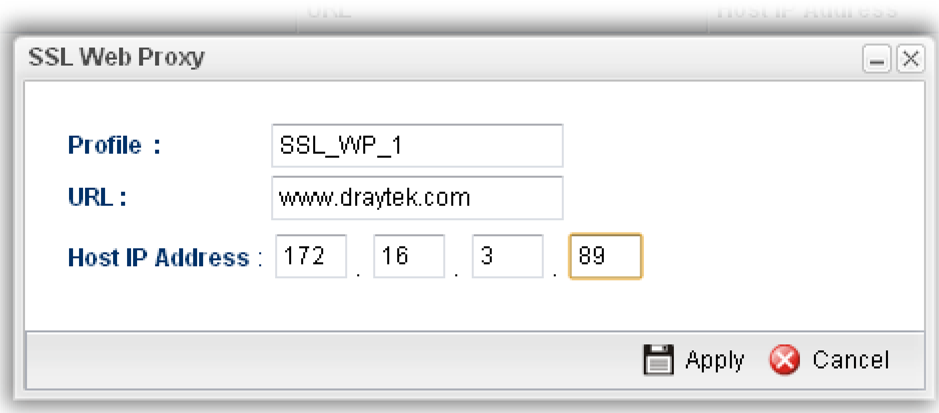
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (10) of the profiles to be created.
Profile	Display the name of the profile that you create.
URL	Display the URL.
Host IP Address	Display the IP address for the Host.

How to create a new SSL Web Proxy

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



3. The following dialog will appear.



Profile : SSL_WP_1

URL : www.draytek.com

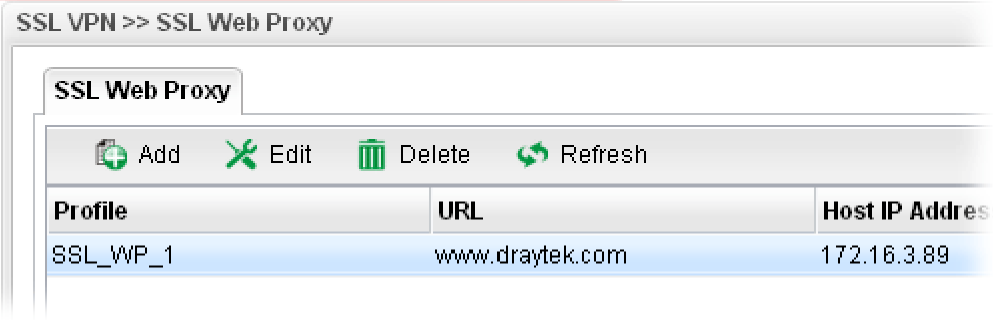
Host IP Address : 172 . 16 . 3 . 89

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.



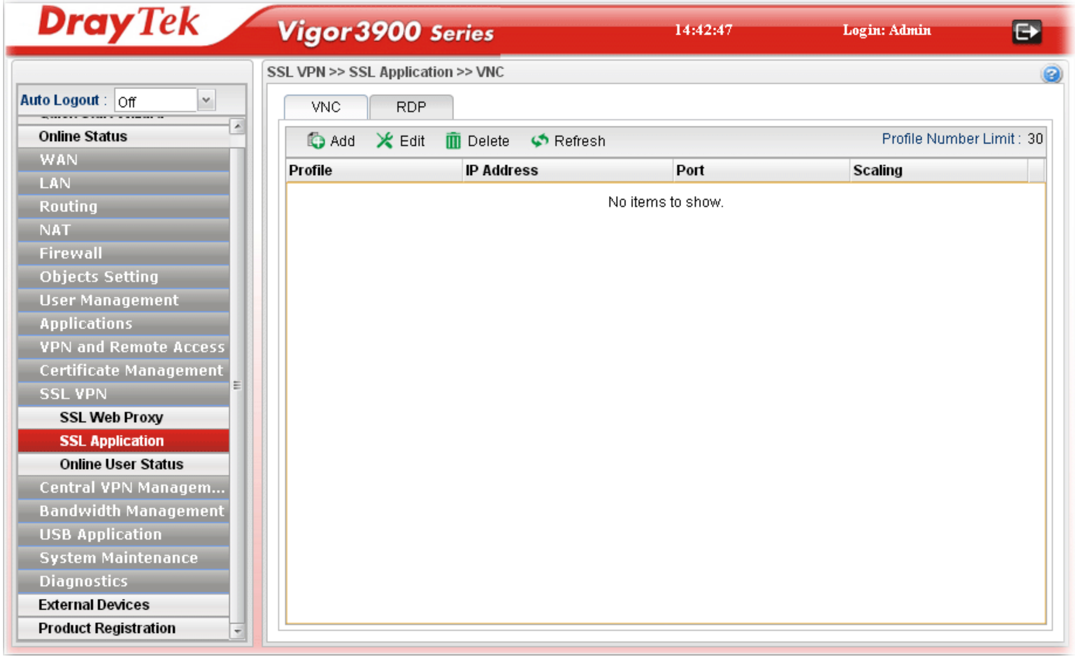
Profile	URL	Host IP Addres
SSL_WP_1	www.draytek.com	172.16.3.89

4.11.2 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.

4.11.2.1 VNC

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



Profile	IP Address	Port	Scaling

No items to show.

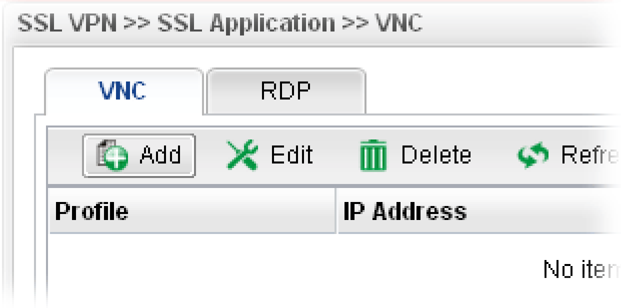
Each item will be explained as follows:

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

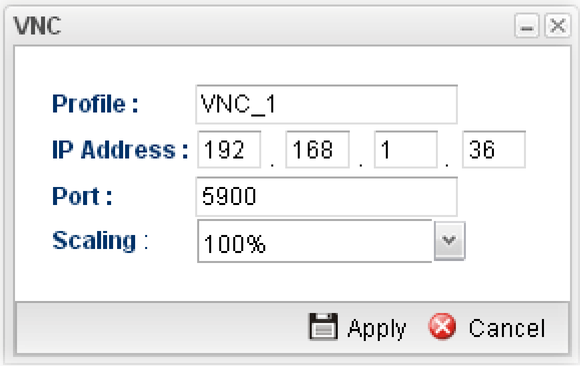
	To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (10) of the profiles to be created.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.
Port	Display the port used for this protocol.
Scaling	Display the percentage for such application.

How to create a new SSL Application with VNC protocol

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



3. The following dialog will appear.



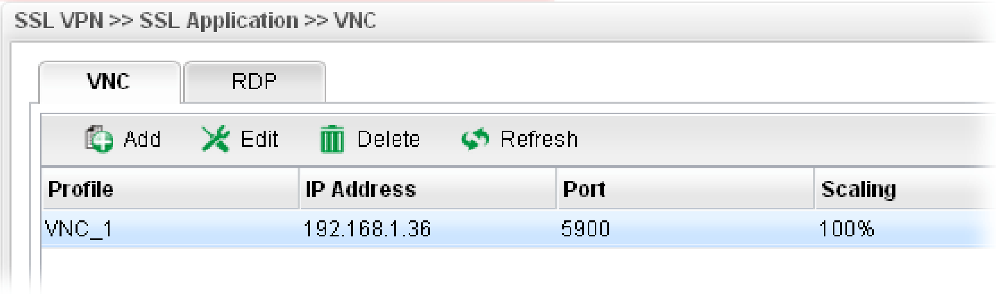
Profile : VNC_1
IP Address : 192 . 168 . 1 . 36
Port : 5900
Scaling : 100%

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile that you create.
IP Address	Type the IP address for this protocol.
Port	Specify the port used for this protocol. The default setting is 5900.
Scaling	Chose the percentage (100%, 80%, 60) for such application.
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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

5. A new SSL Application profile has been created.

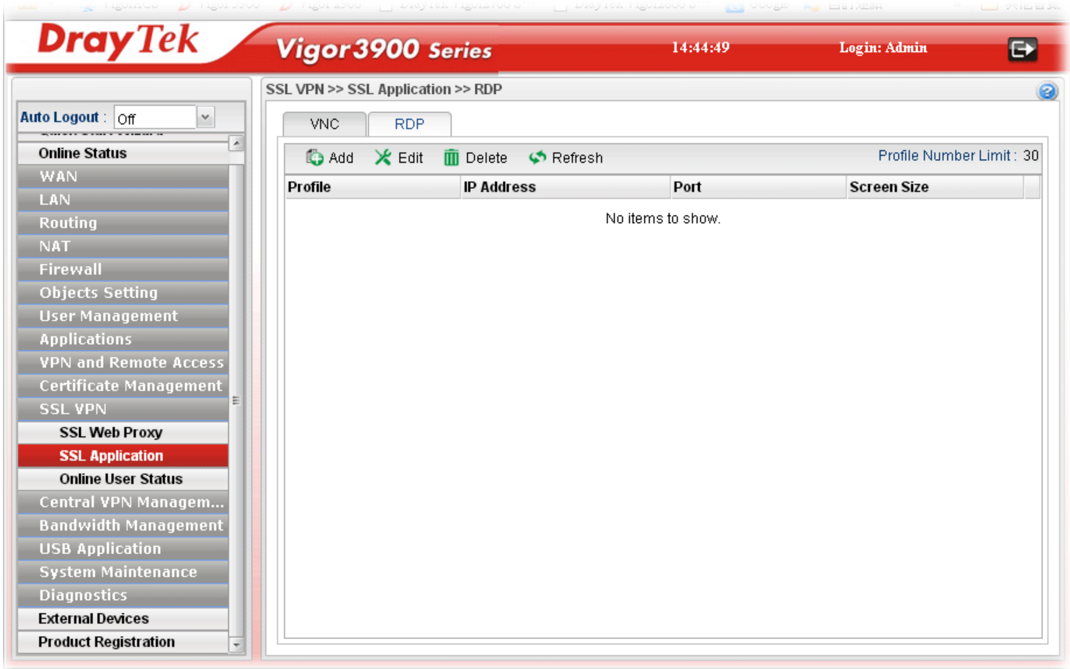


SSL VPN >> SSL Application >> VNC

Profile	IP Address	Port	Scaling
VNC_1	192.168.1.36	5900	100%

4.11.2.2 RDP

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



SSL VPN >> SSL Application >> RDP

Auto Logout : Off

Profile Number Limit : 30

Profile	IP Address	Port	Screen Size

No items to show.

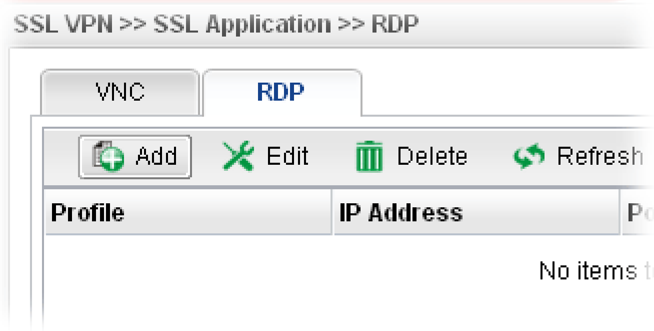
Each item will be explained as follows:

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

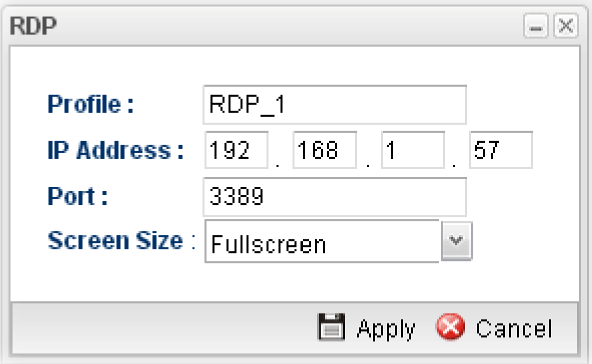
Profile Number Limit	Display the total number (10) of the profiles to be created.
Profile	Display the name of the profile that you create.
IP Address	Display the IP address for this protocol.
Port	Display the port used for this protocol.
Screen Size	Display the screen size for such application.

How to create a new SSL Application with RDP protocol

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



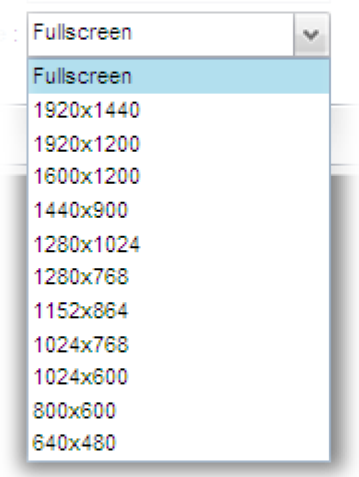
3. The following dialog will appear.



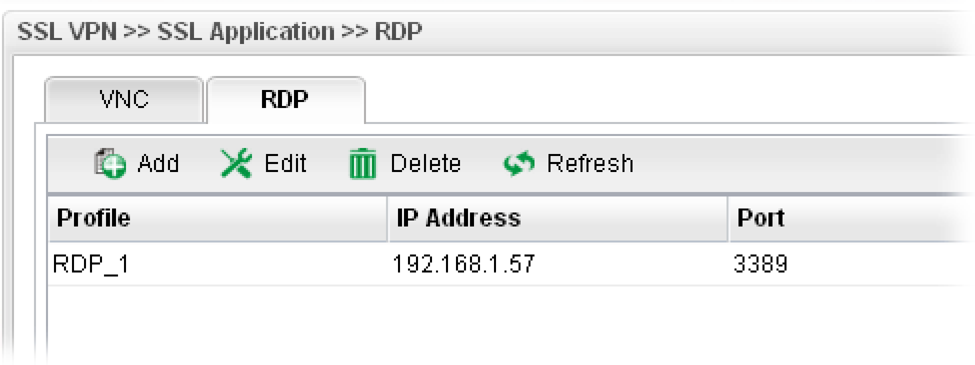
Profile : RDP_1
IP Address : 192 . 168 . 1 . 57
Port : 3389
Screen Size : Fullscreen

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.

	 Fullscreen Fullscreen 1920x1440 1920x1200 1600x1200 1440x900 1280x1024 1280x768 1152x864 1024x768 1024x600 800x600 640x480
Apply	Click it to save the configuration.
Cancel	Click it to exit the page without saving the configuration.

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

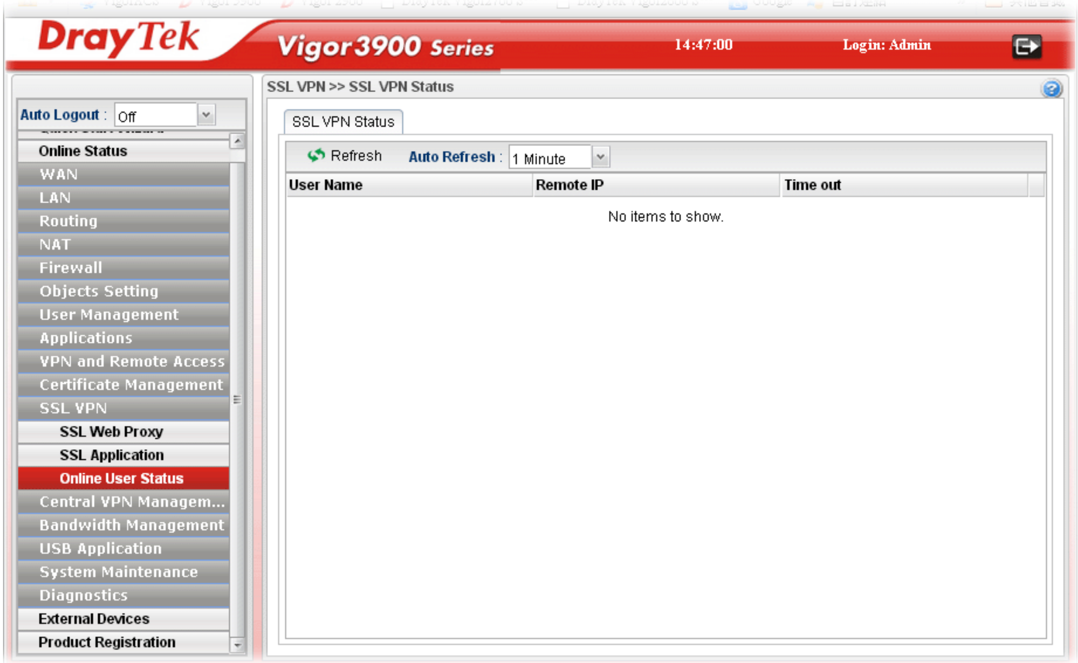


SSL VPN >> SSL Application >> RDP

Profile	IP Address	Port
RDP_1	192.168.1.57	3389

4.11.3 Online User Status

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

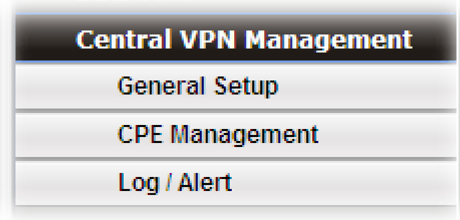


Each item will be explained as follows:

Item	Description
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.

4.12 Central VPN Management

Vigor3900 can build virtual private network (VPN) between itself and any other TR-069 CPE by the function of central VPN management. In addition, it can be treated as a server (called CVM server) which can manage TR-069 CPE for periodical firmware upgrade, configuration backup and restoring configuration.



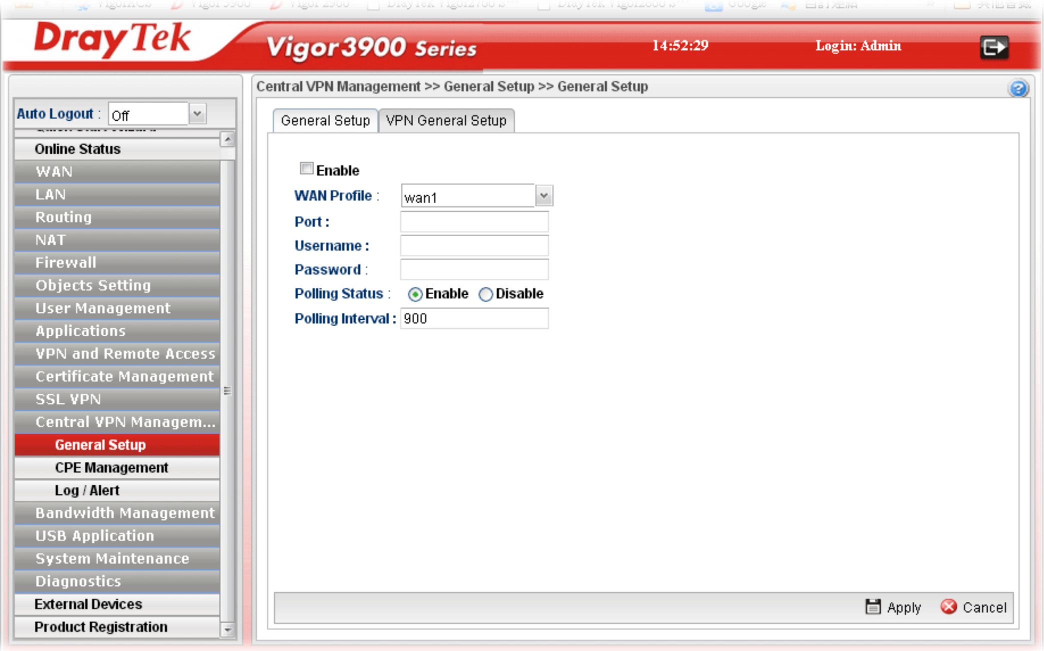
Note: 1. Such menu can manage the CPE connected through WAN only.

2. Up to 16 devices can be managed.

4.12.1 General Setup

4.12.1.1 General Setup

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



□ Enable

WAN Profile : wan1

Port :

Username :

Password :

Polling Status : ● Enable ○ Disable

Polling Interval : 900

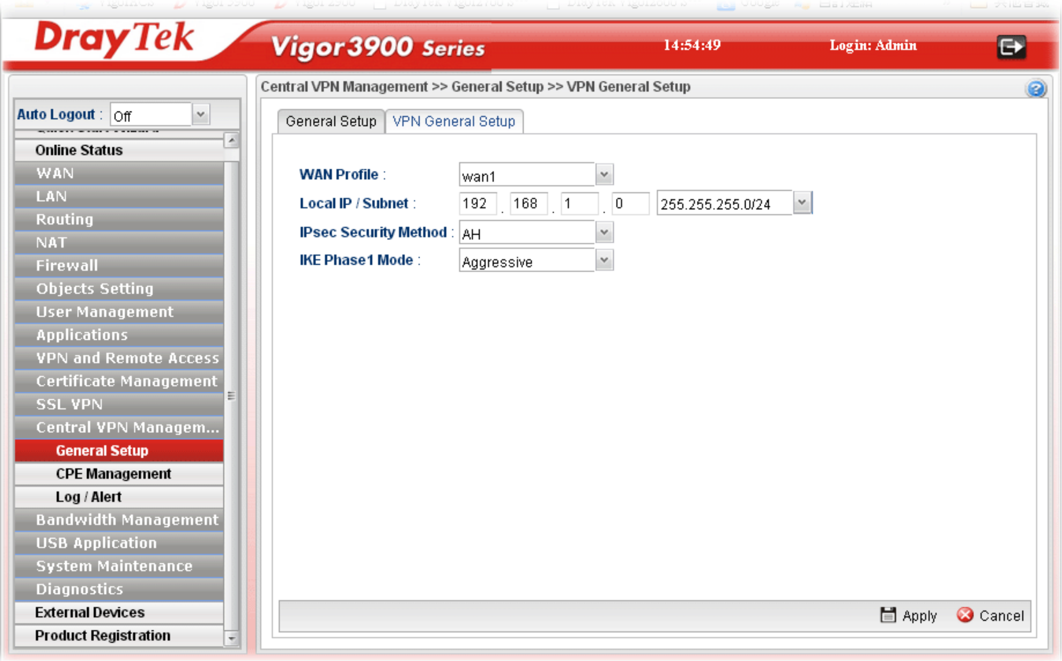
Available parameters are listed as follows:

Item	Description
Enable	Check it to enable the settings.
WAN Profile	Specify an interface for VPN management.
Port	Type a port number for Vigor3900.
Username	Type a username which will be used by any CPE tried to connect to Vigor router.

Password	Type a password which will be used by any CPE tried to connect to Vigor router.
Polling Status	**Enable** – Click it to enable the polling function. **Disable** – Click it to disable the polling function.
Polling Interval	Type the time value (unit is second). The range is from 60 ~ 86400.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.12.1.2 VPN General Setup

This page allows you to configure the basic settings for the VPN tunnel of Vigor3900.



Central VPN Management >> General Setup >> VPN General Setup

WAN Profile : wan1

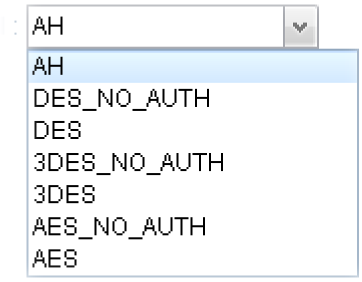
Local IP / Subnet : 192 . 168 . 1 . 0 255.255.255.0/24

IPsec Security Method : AH

IKE Phase1 Mode : Aggressive

Available parameters are listed as follows:

Item	Description
WAN Profile	Choose a WAN interface profile to be used.
Local IP/Subnet	Type the IP address and subnet mask of local host.
IPsec Security Method	Choose one of the following methods for the security of data transmission. For example, choose **AH** to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.

	 AH AH DES_NO_AUTH DES 3DES_NO_AUTH 3DES AES_NO_AUTH AES
IKE Phase1 Mode	Choose **Aggressive** or **Main** as the IKE Phase1 Mode.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

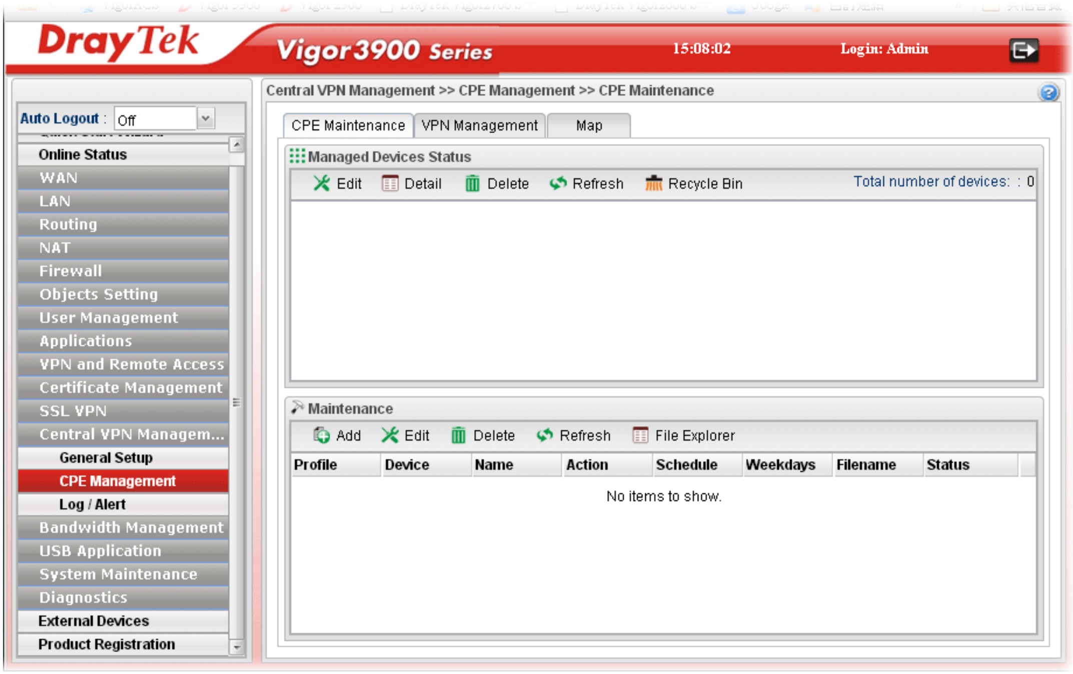
4.12.2 CPE Management

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

4.11.2.1 CPE Maintenance

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

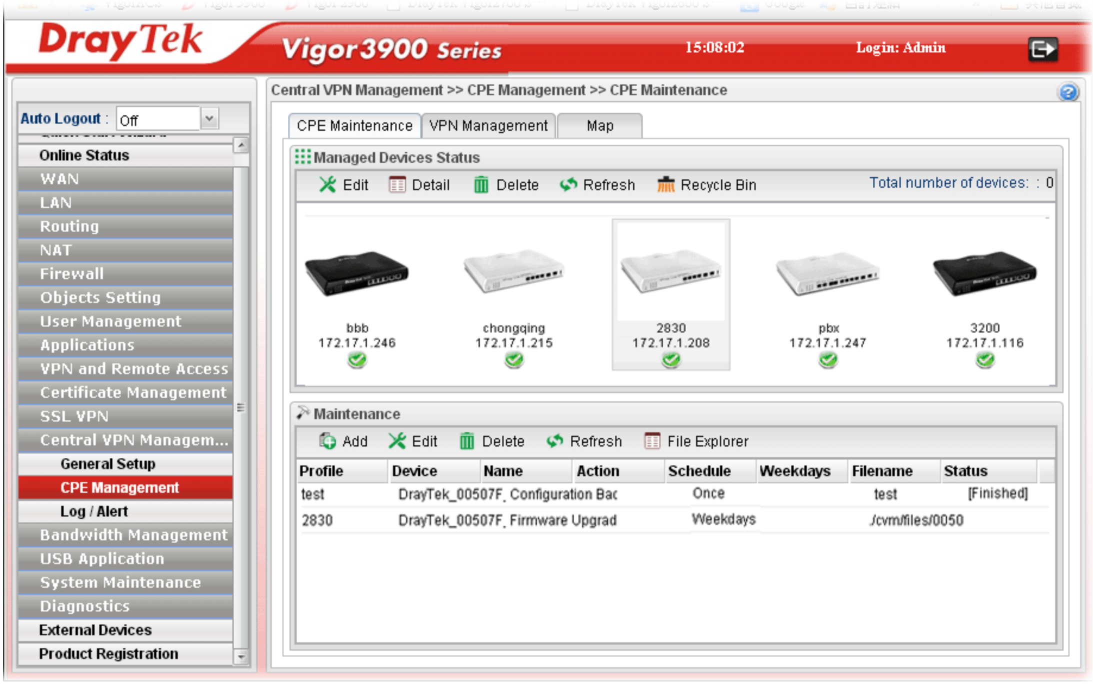
- Page without CPE connected



Profile	Device	Name	Action	Schedule	Weekdays	Filename	Status

No items to show.

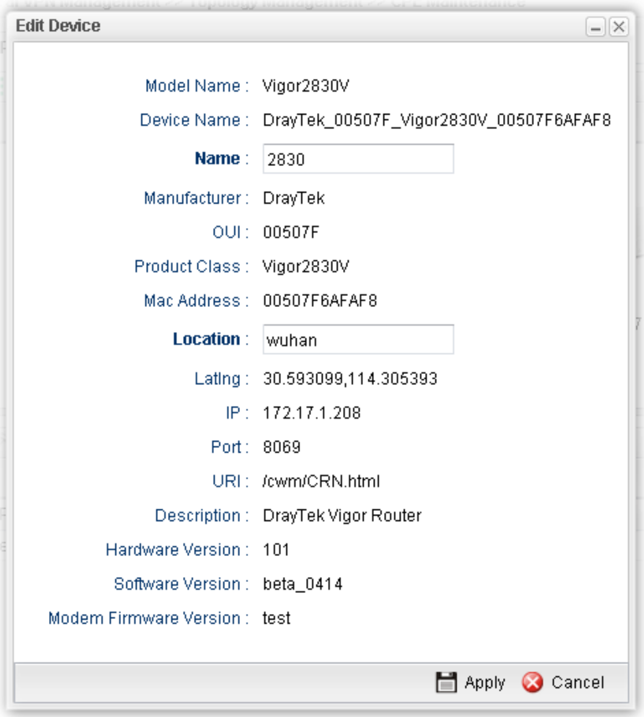
- Page with CPE connected

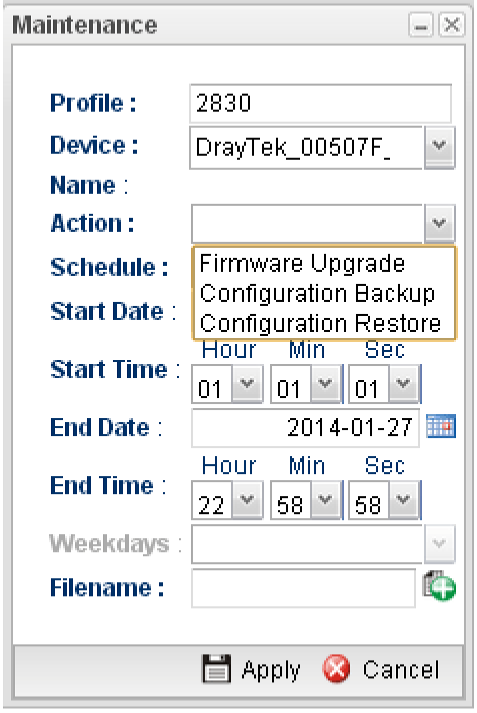


Profile	Device	Name	Action	Schedule	Weekdays	Filename	Status
test	DrayTek_00507F_	Configuration Bac		Once		test	[Finished]
2830	DrayTek_00507F_	Firmware Upgrad		Weekdays		/cvm/files/0050	

Available parameters are listed as follows:

Item	Description

Managed Devices Status	This area displays icons for the CPE managed by Vigor3900. **Edit** – To modify the name and location of specific CPE, click the one you want and click the **Edit** button. A pop up window will appear. Simply change the name (for identification) and/or location manually.  Edit Device Model Name : Vigor2830V Device Name : DrayTek_00507F_Vigor2830V_00507F6AFAF8 **Name** : 2830 Manufacturer : DrayTek OUI : 00507F Product Class : Vigor2830V Mac Address : 00507F6AFAF8 **Location** : wuhan Latlng : 30.593099,114.305393 IP : 172.17.1.208 Port : 8069 URI : /cwm/CRN.html Description : DrayTek Vigor Router Hardware Version : 101 Software Version : beta_0414 Modem Firmware Version : test **Detail** – It displays the same content as the Edit button. However, it cannot be used to modify name or location. **Delete** – To disconnect the management of any CPE, click the CPE icon you want and click the Delete button. **Refresh** – Click it to refresh current page. **Recycle Bin** – All the deleted CPEs will be stored in a temporary place for the administrator to retrieve. It is useful especially for the CPEs deleted carelessly. If you want to retrieve some CPE, click it to open another window. Deleted CPEs containing related information will be displayed on the window. Choose the one you want to retrieve and click Restore. Later, the selected one will appear on the **Managed Devices Status** area again.
Maintenance	This area displays all the profiles which are created for applying to the managed device. **Add** – To add a new profile, simply click it to open a pop up window.



Profile : 2830

Device : DrayTek_00507F_

Name :

Action :

Firmware Upgrade
Configuration Backup
Configuration Restore

Schedule :

Start Date :

Start Time : Hour 01 Min 01 Sec 01

End Date : 2014-01-27

End Time : Hour 22 Min 58 Sec 58

Weekdays :

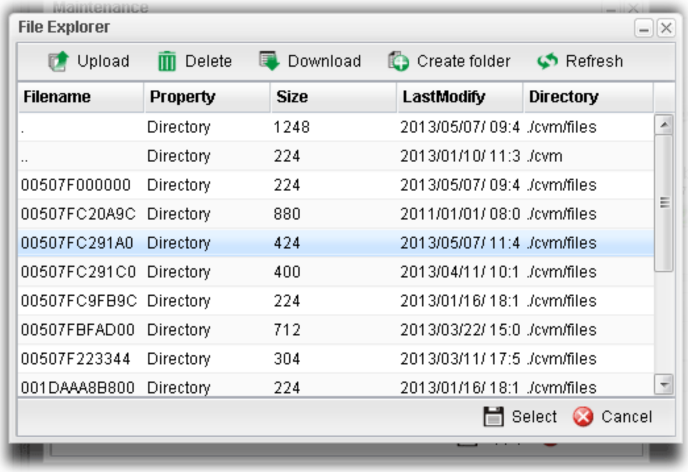
Filename :

Edit – To modify existed profile, choose the one you want to change and click this button to open the pop up window.

Delete – To discard any existed profile, simply choose one you want and click this button to delete the profile.

Refresh – Click it to refresh current page.

File Explorer – Click it to open a file explorer. The available firmware will be displayed in such page.



Filename	Property	Size	LastModify	Directory
.	Directory	1248	2013/05/07/ 09:4	./cvm/files
..	Directory	224	2013/01/10/ 11:3	./cvm
00507F000000	Directory	224	2013/05/07/ 09:4	./cvm/files
00507FC20A9C	Directory	880	2011/01/01/ 08:0	./cvm/files
00507FC291A0	Directory	424	2013/05/07/ 11:4	./cvm/files
00507FC291C0	Directory	400	2013/04/11/ 10:1	./cvm/files
00507FC9FB9C	Directory	224	2013/01/16/ 18:1	./cvm/files
00507FBFAD00	Directory	712	2013/03/22/ 15:0	./cvm/files
00507F223344	Directory	304	2013/03/11/ 17:5	./cvm/files
001DAAA8B800	Directory	224	2013/01/16/ 18:1	./cvm/files

Profile – Display the name of the profile.

Device – Display the name (named by Vigor3900) of the devices selected by such profile.

Name – Display the name (can be modified by the administrator) of the device.

Action – Display the action specified for such profile.

Schedule – Display the frequency of for such profile which will be performed by Vigor router.

Weekdays – Display the day(s) chosen for such profile.

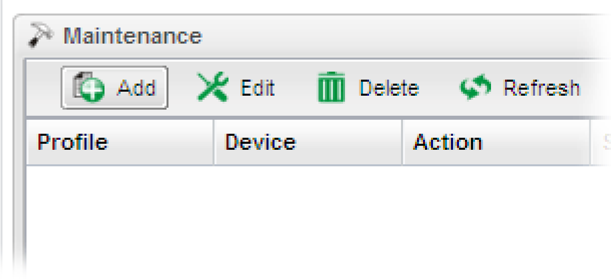
	Filename – Display the filename of the firmware. **Status** – Display current status of the profile has been finished or not.

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

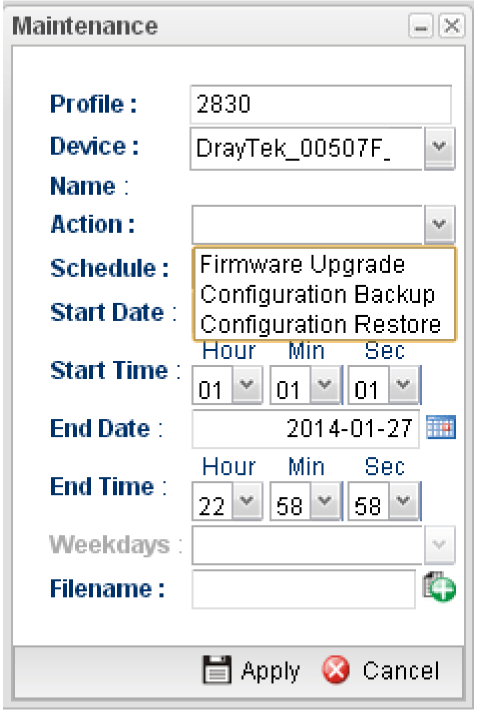
How to add a new Maintenance Profile

Follow the steps below to create a new maintenance profile.

6. Click **Add** from the **Maintenance** area



2. The Maintenance dialog appears.



Profile : 2830

Device : DrayTek_00507F_

Name :

Action :

Firmware Upgrade
Configuration Backup
Configuration Restore

Schedule :

Start Date :

Start Time : Hour 01 Min 01 Sec 01

End Date : 2014-01-27

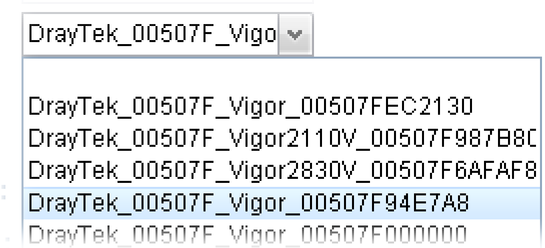
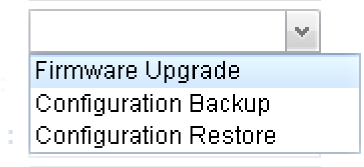
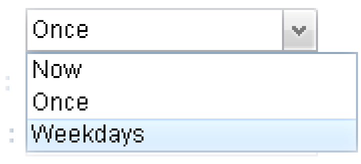
End Time : Hour 22 Min 58 Sec 58

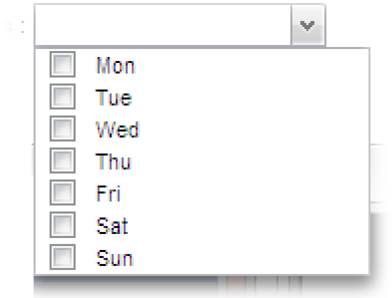
Weekdays :

Filename :

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the maintenance profile.
Device	The drop down list will display all the devices detected by Vigor3900. Choose the one which will be applied with such new created profile.

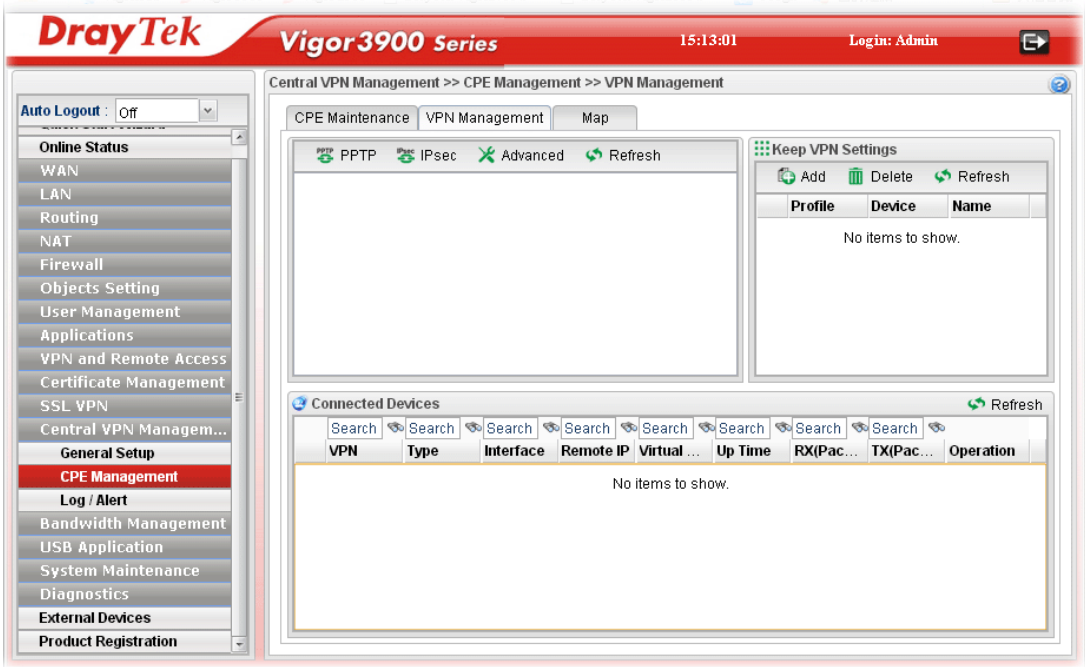
	 DrayTek_00507F_Vigo DrayTek_00507F_Vigor_00507FEC2130 DrayTek_00507F_Vigor2110V_00507F987B8C DrayTek_00507F_Vigor2830V_00507F6AFAF8 DrayTek_00507F_Vigor_00507F94E7A8 DrayTek_00507F_Vigor_00507F000000 Usually, the name of the device will be assigned by Vigor3900 automatically. If you want to give a name easy for easy recognition, refer to 4.11.2.1 CPE Maintenance to specify another name for the device additionally.
Name	Display the name (can be modified by the administrator) of the device.
Action	There are three actions for you to choose for such profile.  Firmware Upgrade Configuration Backup Configuration Restore **Firmware Upgrade** – It means such profile will be used for firmware upgrade. **Configuration Backup** – It means such profile will be used for configuration backup of the selected CPE. **Configuration Restore** – It means such profile will be used for restoring the configuration of the selected CPE.
Schedule	The new created profile can be applied to the selected CPE based on the schedule configured here.  **Now** – The action will be performed for the selected CPE immediately. **Once** – The action will be performed for the selected CPE at the specified time, and will be done for once. **Weekdays** – The action will be performed for the selected CPE at the time and date specified below every week.
Start Date / **End Date**	It is available only when **Once** is selected as **Schedule**. Specify the starting date /ending time with the format YYYY-MM-DD.
Start Time / **End Time**	It is available only when **Once** is selected as **Schedule**. Specify the starting date /ending date with the format YYYY-MM-DD.
Weekdays	It is available only when **Weekdays** is selected as **Schedule**. Simply check the day you want.

	
Filename	Type the name string of the file which will be used for firmware upgrade, configuration backup or configuration restore.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.12.2.2 VPN Management

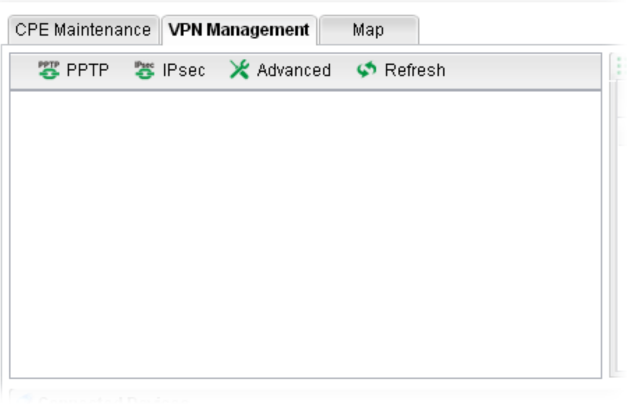
An easy method is offered to configure VPN settings for building VPN connection between Vigor3900 (treated as VPN server) and other Vigor router (treated as CPE device, i.e., VPN client).



Available parameters are listed as follows:

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

appear instead.



PPTP

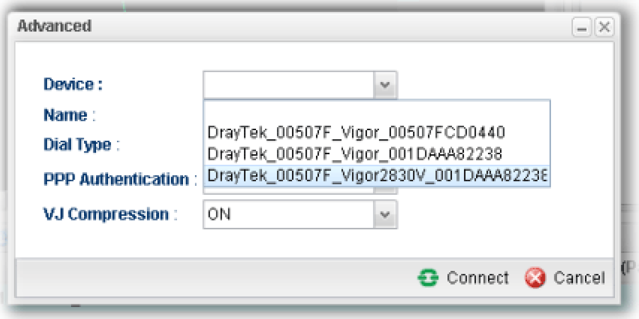
To build a quick VPN connection with **PPTP**, simply click the remote CPE (waiting for the icon to be bigger) first and then click it. If the connection is built successfully, a green line will appear.

IPsec

To build a quick VPN connection with **IPsec**, simply click the remote CPE (waiting for the icon to be bigger) first and then click it. If the connection is built successfully, a blue line will appear.

Advanced

To build a VPN connection with detailed configuration (such as PPP authentication and VJ compression), click **Advanced** tool.



Device :

Name :
DrayTek_00507F_Vigor_00507FCD0440
DrayTek_00507F_Vigor_001DAA82238
DrayTek_00507F_Vigor2830V_001DAA8223ε

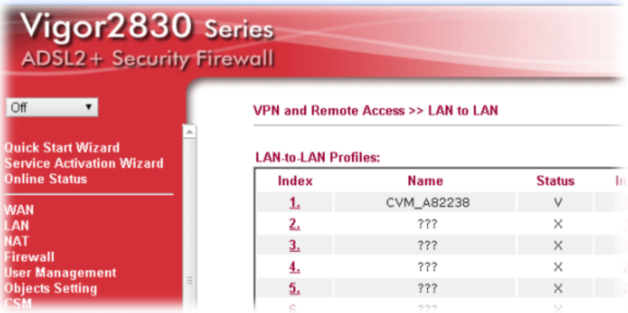
Dial Type :

PPP Authentication :

VJ Compression : ON

Specify the CPE from the Device drop down list; choose the name of the CPE; select PPTP or IPsec as the Dial Type; choose PAP_only or PAP_or_CHAP as PPP authentication; enable or disable VJ Compression; then click **Connect** to build the VPN connection.

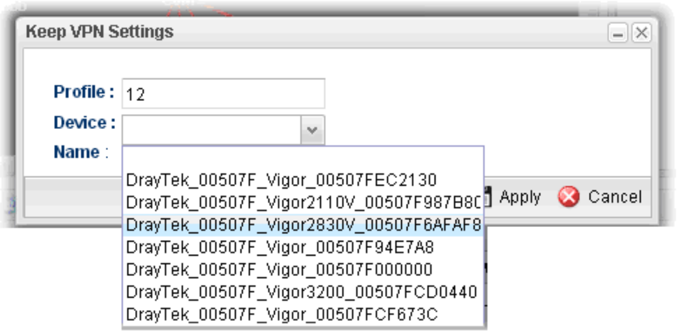
Note: If the VPN connection has been established successfully, a new ***LAN to LAN profile*** will be created for the CPE automatically. See the following example.



VPN and Remote Access >> LAN to LAN

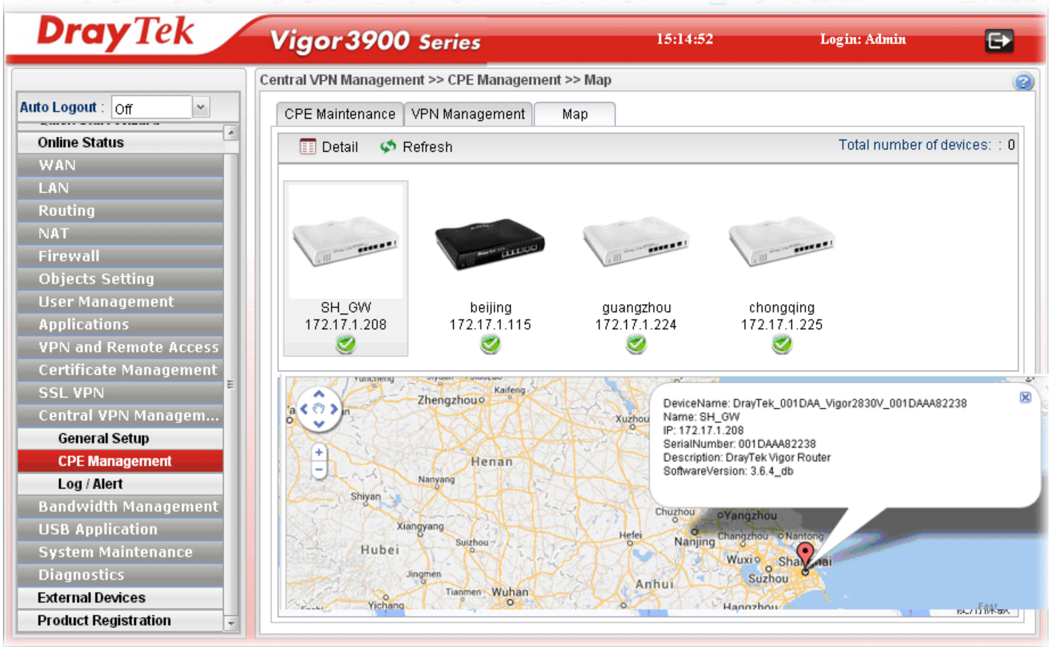
LAN-to-LAN Profiles:

Index	Name	Status
1.	CVM_A82238	V
2.	???	X
3.	???	X
4.	???	X
5.	???	X

Keep VPN Settings	To avoid the VPN be disconnected due to the settings changed by the client, the connection status can be kept by specified by such feature. **Add** – Click it to open the following dialog. Type the name of the profile and choose the CPE from the Device drop down list. Then, click Apply to save the settings. Such profile will be applied to the device connecting to Vigor3900 with VPN.  Keep VPN Settings Profile : 12 Device : Name : DrayTek_00507F_Vigor_00507FEC2130 DrayTek_00507F_Vigor2110V_00507F987B8C DrayTek_00507F_Vigor2830V_00507F6AFAF8 DrayTek_00507F_Vigor_00507F94E7A8 DrayTek_00507F_Vigor_00507F000000 DrayTek_00507F_Vigor3200_00507FCD0440 DrayTek_00507F_Vigor_00507FCF673C **Delete** – Click it to delete the profile. The VPN between the router and the client might not be guaranteed. **Refresh** – Click it to refresh current page. **Profile** – Display of the profile used now. **Device** – Display the name of the CPE connected to Vigor router via VPN. **Name** – Display the name (can be modified by the administrator) of the device. Refer to 4.11.2.1 CPE Maintenance for detailed information.
Connected Devices	Once the VPN is established successfully, the basic information such as the connection type, IP address, RX/RX will be displayed on this field. **Refresh** – Click it to refresh current page. **VPN –** Display the name of the VPN. **Type –** Display the type of the connection mode. **Interface** – Display the WAN interface. **Remote IP –** Display the IP address of the remote end. **Virtual Network –** Display the IP address of Vigor3900. **Up Time –**Display the connection time of such VPN. **RX(Packets) /TX(Packets) –**Display the number of the packets exchanged in such VPN. **Disconnect –** Click it to disconnect the VPN.

4.12.2.3 Map

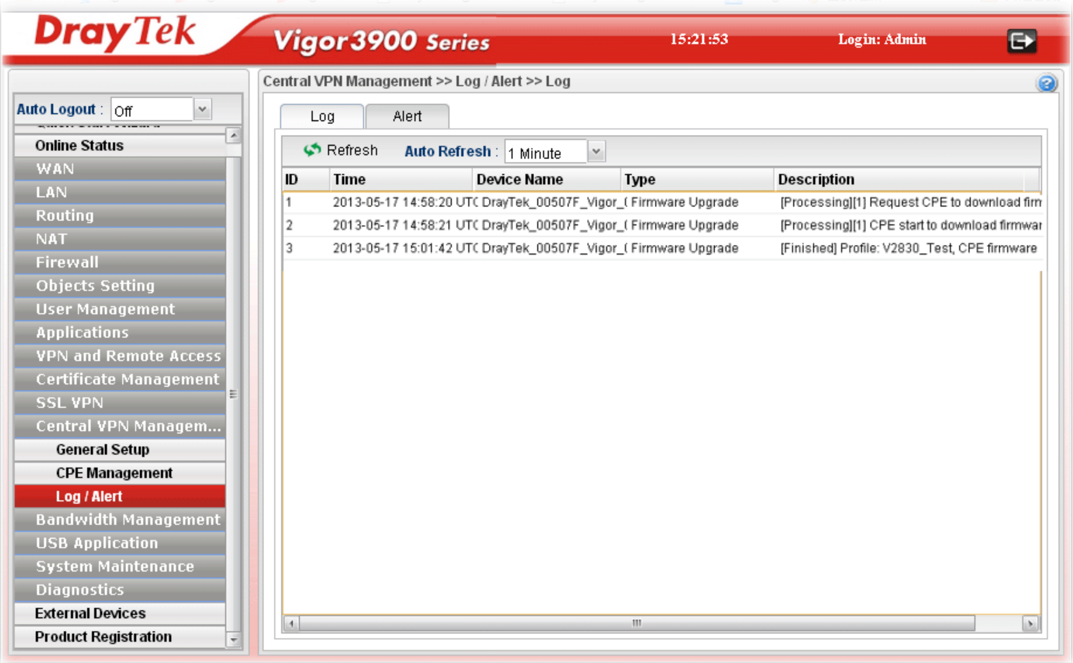
To display the **location** of the selected CPE with a bird's eye view, open **Central VPN Management>>CPE Management** and click the tab of **Map**.



DeviceName: DrayTek_001DAA_Vigor2830V_001DAAA82238
Name: SH_GW
IP: 172.17.1.208
SerialNumber: 001DAAA82238
Description: DrayTek Vigor Router
SoftwareVersion: 3.6.4_db

4.12.3 Log/Alert

The Log page offers brief information to identify the CPE connected to Vigor3900.



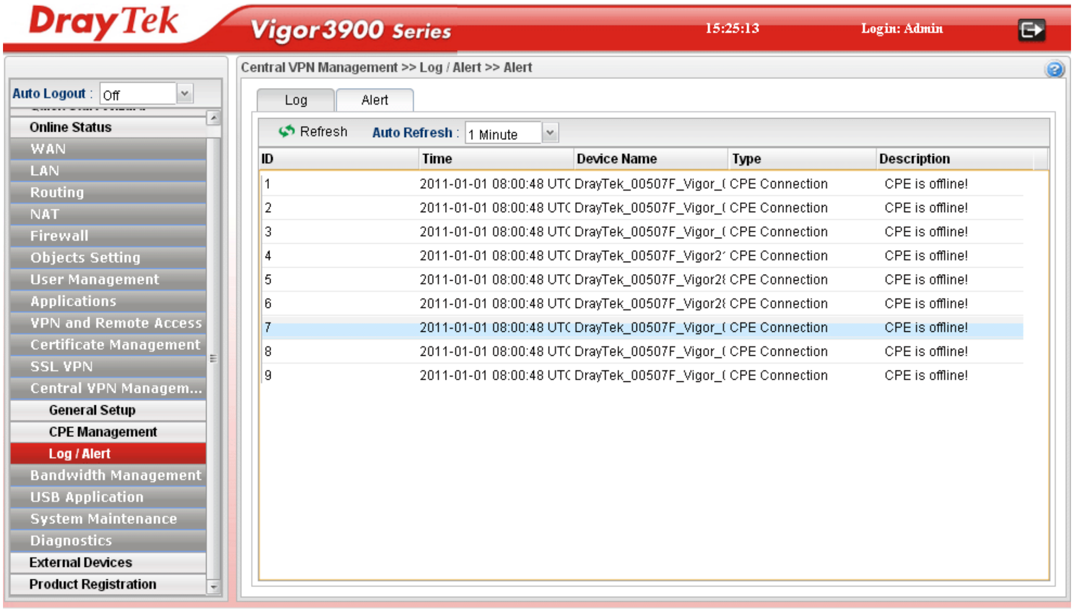
Central VPN Management >> Log / Alert >> Log

Auto Logout : Off

Auto Refresh : 1 Minute

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

The Alert page offers brief information to identify the CPE connected to Vigor3900.



Central VPN Management >> Log / Alert >> Alert

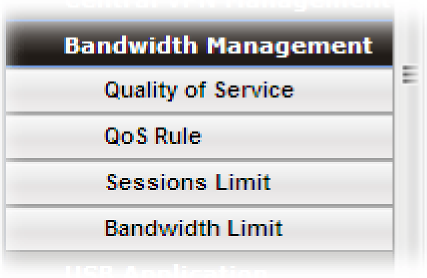
Auto Logout : Off

Auto Refresh : 1 Minute

ID	Time	Device Name	Type	Description
1	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!
2	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!
3	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!
4	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor2'	CPE Connection	CPE is offline!
5	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor2{	CPE Connection	CPE is offline!
6	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor2{	CPE Connection	CPE is offline!
7	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!
8	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!
9	2011-01-01 08:00:48 UT(	DrayTek_00507F_Vigor_(	CPE Connection	CPE is offline!

4.13 Bandwidth Management

Below shows the menu items for Bandwidth Management.



The QoS (Quality of Service) guaranteed technology in the Vigor router allows the network administrator to monitor, analyze, and allocate bandwidth for various types of network traffic in real-time and/or for business-critical traffic. Thus, timing-sensitive applications will not be impacted by web surfing traffic or other non-critical applications, such as file transfer. Without QoS-guaranteed control, there would be virtually no way to prioritize users/services or guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications.

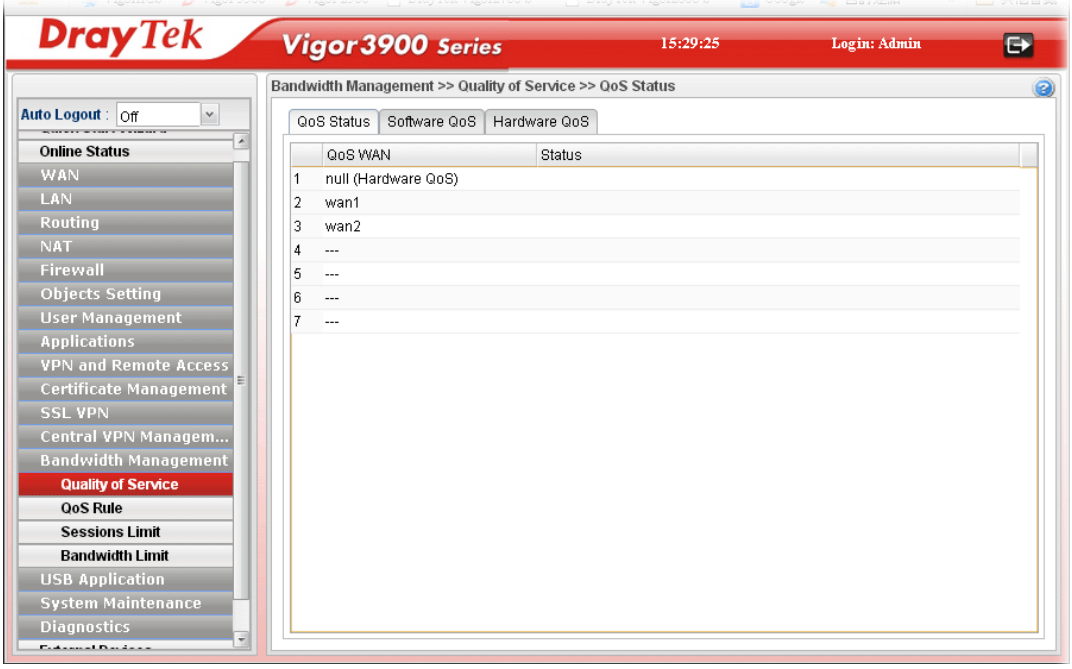
Differentiated quality of service is therefore one of the most important issues over the Internet infrastructure. In Vigor router, DSCP (Differentiated Service Code Point) support is also taken into consideration in the design of the QoS-guaranteed control module.

4.13.1 Quality of Service

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

4.13.1.1 QoS Status

This page displays current QoS Status.

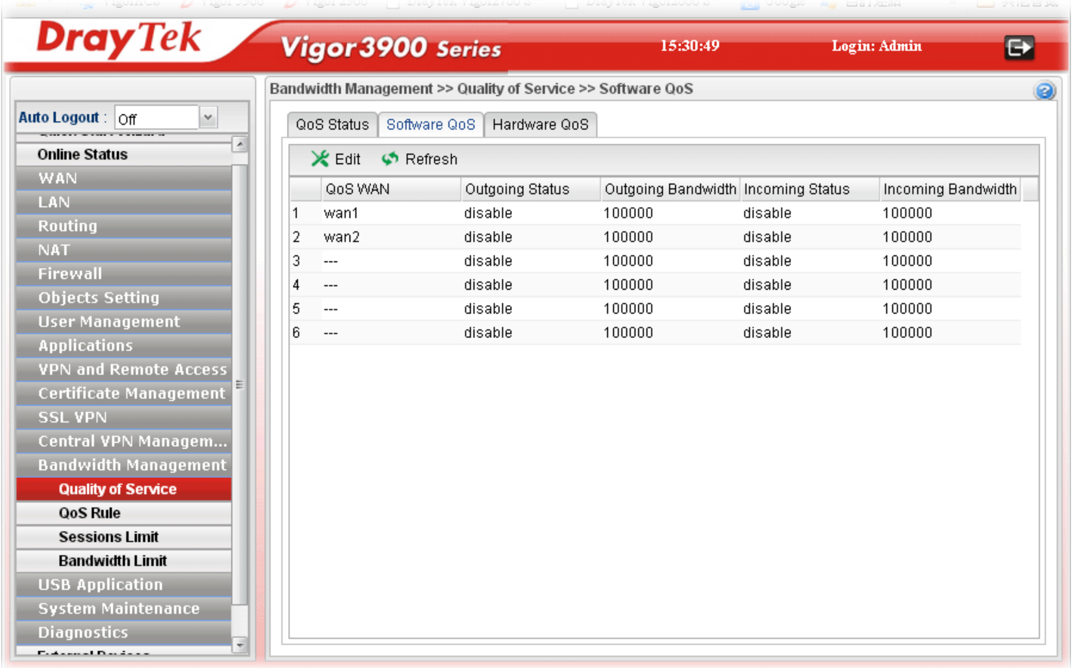


Bandwidth Management >> Quality of Service >> QoS Status

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

4.13.1.2 Software QoS

This page displays current software QoS status and allows you to edit related settings, including bandwidth, queue (high, medium, normal and low) for each QoS WAN.



Bandwidth Management >> Quality of Service >> Software QoS

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

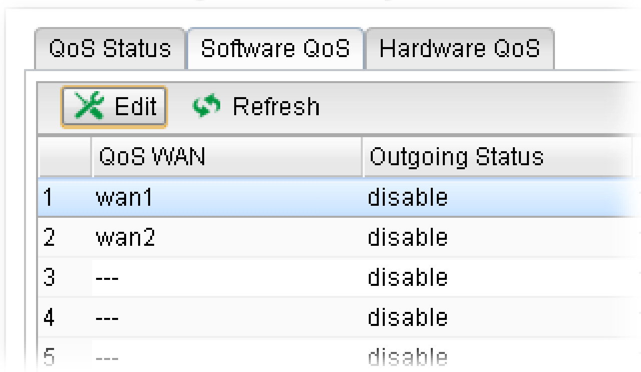
Available parameters are listed as follows:

Item	Description
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
QoS WAN	Display the WAN interface used for QoS.
Outgoing Status	Display bandwidth for the outgoing data is enabled or disabled.
Outgoing Bandwidth	Display the total number of transmission rate for the outgoing data.
Incoming Status	Display the total number of transmission rate for the incoming data.
Incoming Bandwidth	Display bandwidth for the incoming data is enabled or disabled.

How to edit a QoS Profile

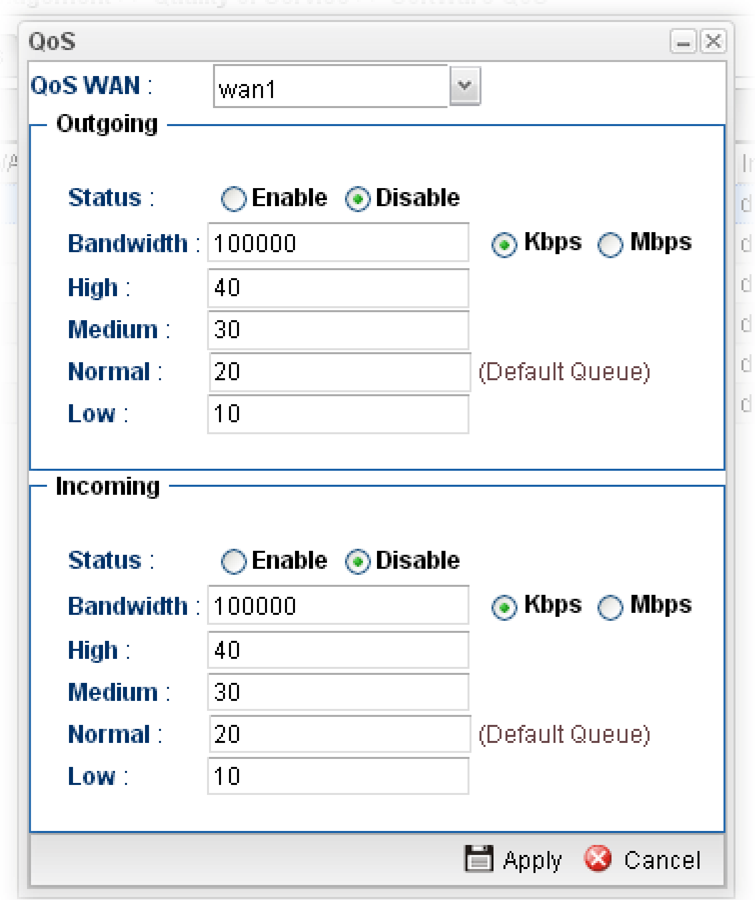
Follow the steps below to create a new maintenance profile.

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



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

3. The QoS settings page appears.



QoS

QoS WAN : wan1

Outgoing

Status : ○ Enable ● Disable

Bandwidth : 100000 ● Kbps ○ Mbps

High : 40

Medium : 30

Normal : 20 (Default Queue)

Low : 10

Incoming

Status : ○ Enable ● Disable

Bandwidth : 100000 ● Kbps ○ Mbps

High : 40

Medium : 30

Normal : 20 (Default Queue)

Low : 10

Available parameters are listed as follows:

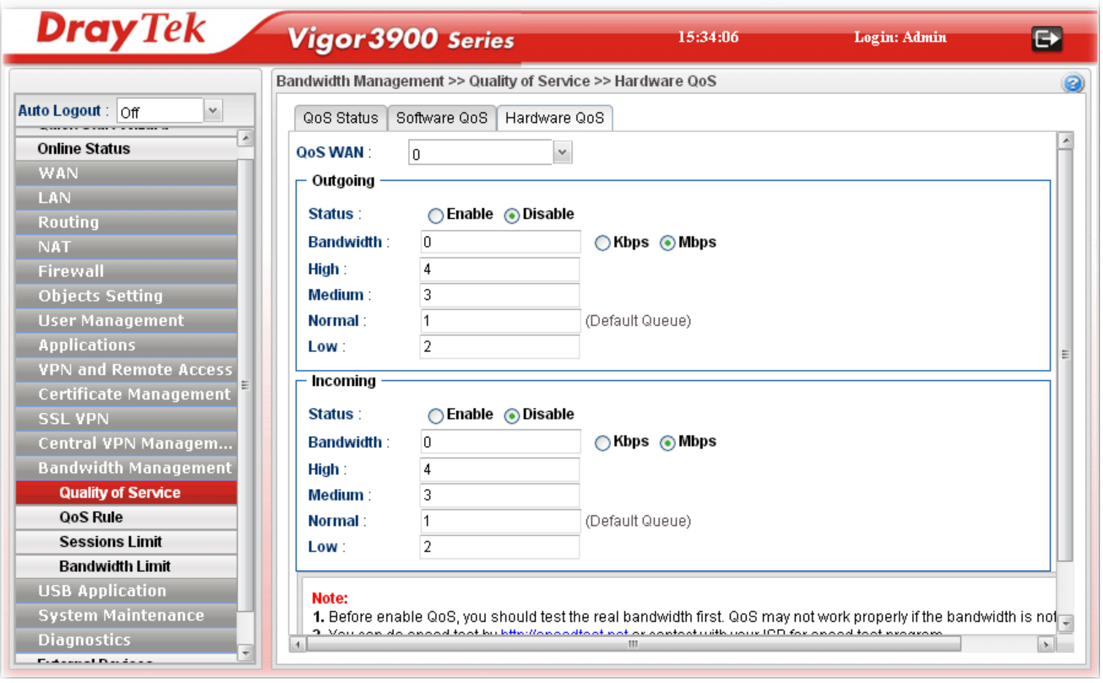
Item	Description
QoS WAN	Use the drop down list to set WAN interface for QoS by choosing one of the WAN interfaces.
Status	Enable – Click it to enable such profile. Disable – Click it to disable the QoS profile.
Bandwidth	Type the number as the total transmission rate for the outgoing /incoming data. The range can be set from 64000 to 10000000. Click the unit (Kbps or Mbps) for such rate.
High/Medium/ Normal/Low	There are several available outgoing queues. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.13.1.3 Hardware QoS

This page allows you to configure bandwidth of data and voice signals transmission for outgoing data and incoming data through hardware interface.

Note: The difference between Hardware QoS and Software QoS is that only one WAN interface is supported by Hardware QoS. However, there are six WAN interfaces supported by Software QoS.



QoS WAN : 0

Outgoing

Status : ○ Enable ● Disable

Bandwidth : 0 ○ Kbps ● Mbps

High : 4

Medium : 3

Normal : 1 (Default Queue)

Low : 2

Incoming

Status : ○ Enable ● Disable

Bandwidth : 0 ○ Kbps ● Mbps

High : 4

Medium : 3

Normal : 1 (Default Queue)

Low : 2

Note:

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

2. You can do speed test by http://speedtest.net or contact with your ISP for speed test program.

Available parameters are listed as follows:

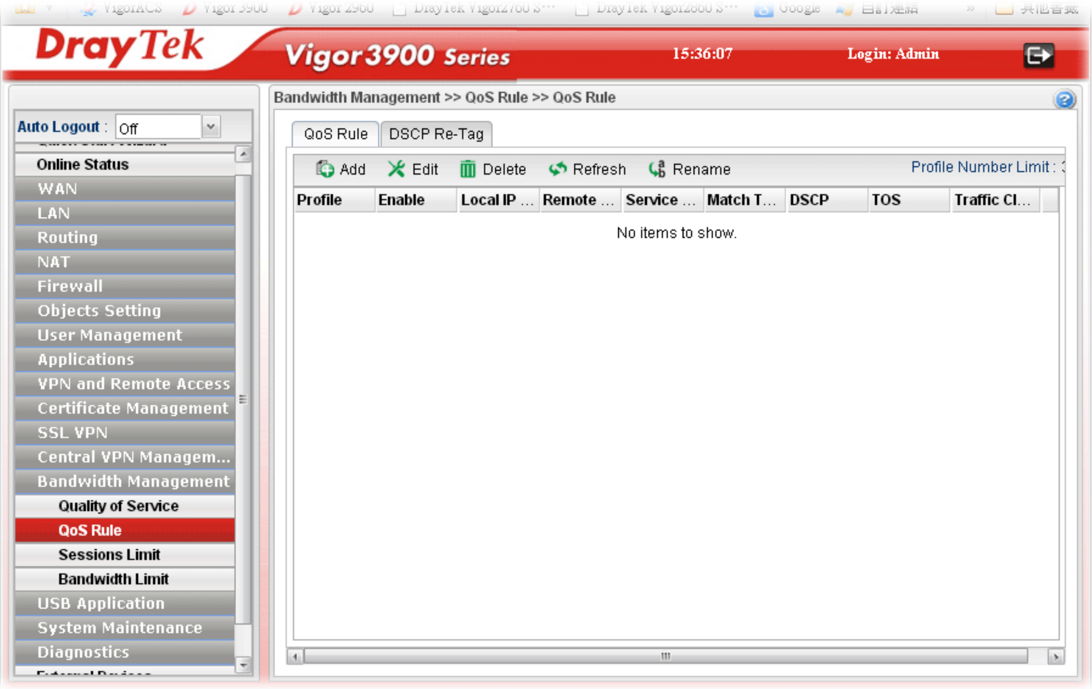
Item	Description
QoS WAN	Use the drop down list to choose the WAN interface to apply hardware QoS.
Status	**Enable** – Click it to enable QoS for outgoing/incoming traffic. **Disable** – Click it to disable QoS for outgoing/incoming traffic.
Bandwidth	Type the number as the total transmission rate for the outgoing /incoming data. The range can be set from 64 to 1000000 kbps. Click the unit (Kbps or Mbps) for such rate.
High/Medium/ Normal/Low	It determines the weight for each queue. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. Type the weight of queues in bytes, range from 0 to 1000000.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

4.13.2 QoS Rule

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

4.12.2.1 QoS Rule



No items to show.

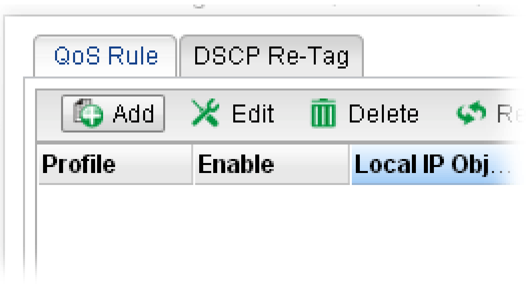
Available parameters are listed as follows:

Item	Description
Add	Add a new rule profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile for the filter.
Profile Number Limit	Display the total number (32) of the profiles to be created.
Enable	Display the status of the profile. False means disabled; True means enabled.
Local IP Object	Display the source IP address for the filter.
Remote IP Object	Display the destination IP address for the filter.
Service Type	Display the service type (e.g., IKE, HTTP, AUTH and etc) for the filter.

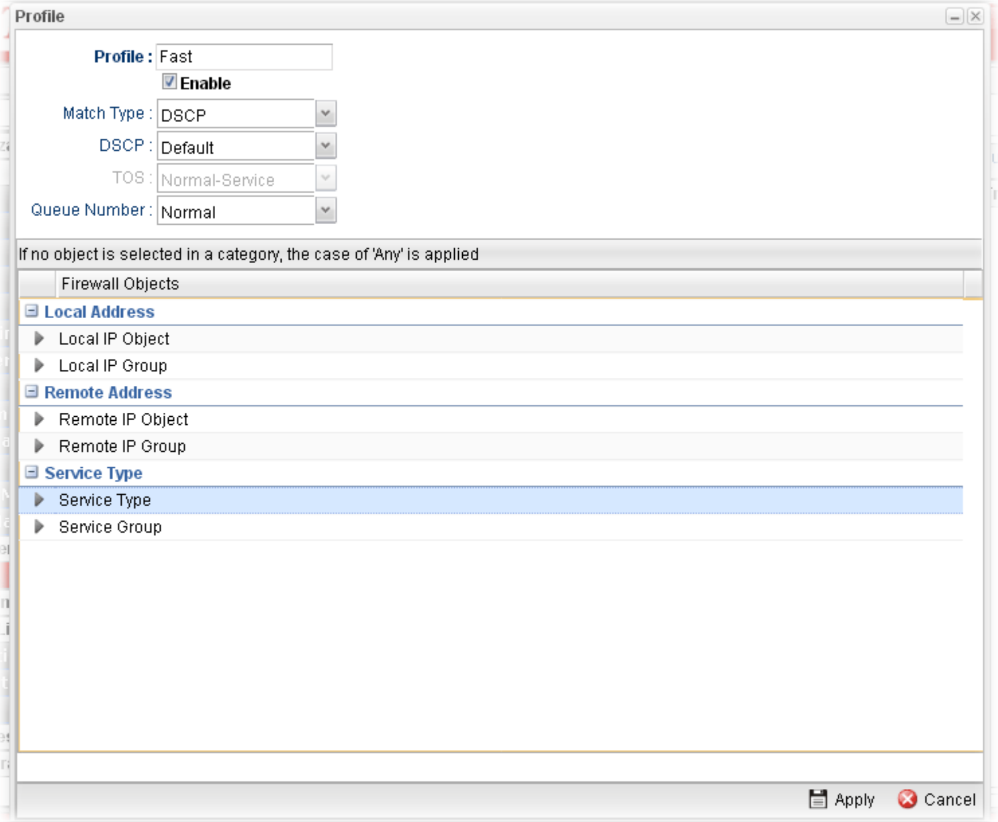
Match Type	Display the match type (e.g., TOS or DSCP) for the filter.
DSCP	Display the setting of DSCP.
TOS	Display the setting of TOS.
Traffic Class	Display the queue number that such filter is categorized.

How to add a QoS rule profile

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



3. The following dialog will appear.

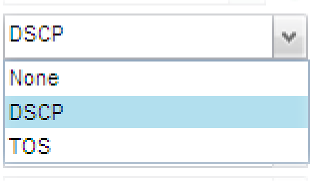
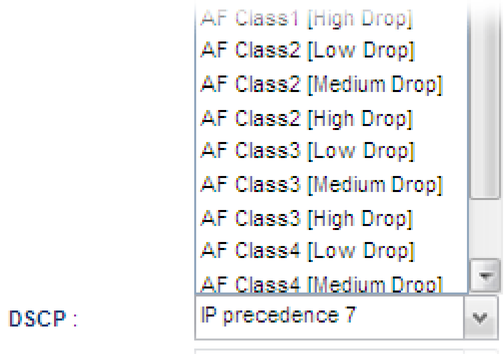
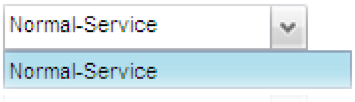
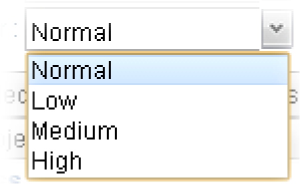
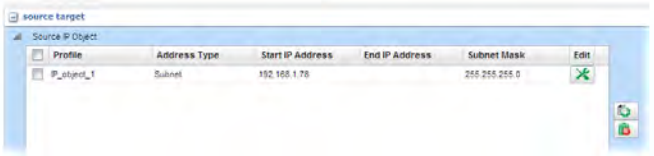


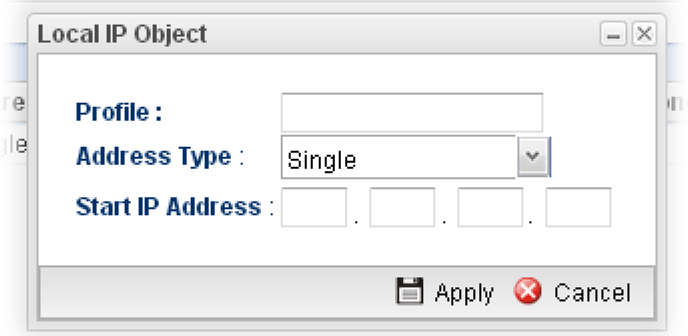
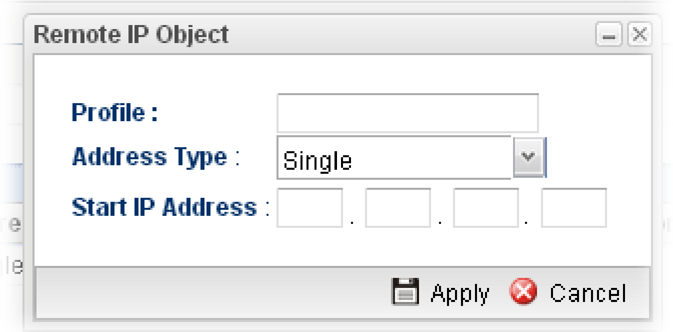
Profile : Fast
☑ Enable
Match Type : DSCP
DSCP : Default
TOS : Normal-Service
Queue Number : Normal

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

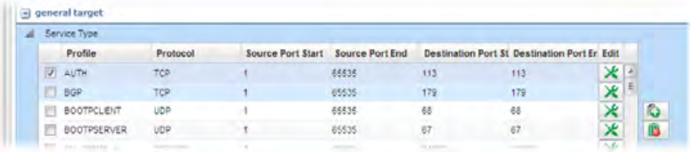
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the filter profile.
Enable	Check this box to enable such profile.

<table>
<tr><td><b>Match Type</b></td><td>Use the drop down list to specify a suitable match type.

DSCP
None
DSCP
TOS</td></tr>
<tr><td><b>DSCP</b></td><td>It is available when DSCP is selected as the Match type.

AF Class1 [High Drop]
AF Class2 [Low Drop]
AF Class2 [Medium Drop]
AF Class2 [High Drop]
AF Class3 [Low Drop]
AF Class3 [Medium Drop]
AF Class3 [High Drop]
AF Class4 [Low Drop]
AF Class4 [Medium Drop]
DSCP : IP precedence 7</td></tr>
<tr><td><b>TOS</b></td><td>It is available when TOS is selected as the Match type.

Normal-Service
Normal-Service</td></tr>
<tr><td><b>Queue Number</b></td><td>Choose a queue number to category the packets matching with the condition configured as above. High is the highest; Normal is the lowest.

Normal
Normal
Low
Medium
High</td></tr>
<tr><td><b>Local Address</b></td><td>Click ▶ on the left side of the <b>Source IP Object/Source IP Group</b> profile. Check the object profile(s) as the source target.

source target
Source IP Object
<table><tr><th>□</th><th>Profile</th><th>Address Type</th><th>Start IP Address</th><th>End IP Address</th><th>Subnet Mask</th><th>Edit</th></tr><tr><td>□</td><td>IP_object_1</td><td>Subnet</td><td>192.168.1.78</td><td></td><td>255.255.255.0</td><td></td></tr></table>
<b>Local IP Object –</b> Use the drop down list to choose one of the IP objects for such rule profile.
<b>Local IP Group –</b> Use the drop down list to choose one of the IP group for such rule profile.
If you want to create a new IP object, simply click ⊕ to open the following dialog.</td></tr>
</table>

	 Local IP Object Profile : Address Type : Single Start IP Address : . . . Apply Cancel ● **Profile** – type a new name for such IP object. ● **Address Type** –Choose the address type (Single or Range) for such rule. Each type will bring different settings for configuration. ● **Start IP Address -** Type the IP address of the starting point for such profile. ● **End IP Address -** Type the IP address of the ending point for such profile if you choose **Range** as **Address Type**. ● **Subnet Mask** – Choose the subnet mask from the drop down list if you choose **Subnet** as **Address Type**.
Remote Address	Click ▶ on the left side of the **Remote IP Object/ Remote IP Group** profile. Check the object profile(s) as the destination target. **Remote IP Object –** Use the drop down list to choose one of the destination IP objects for such rule profile. **Remote IP Group –** Use the drop down list to choose one of the destination IP group for such rule profile. If you want to create a new IP object, simply click ⊕ to open the following dialog.  Remote IP Object Profile : Address Type : Single Start IP Address : . . . Apply Cancel ● **Profile** – Type a new name for such IP object. ● **Address Type** – Choose the address type (Single or Range) for such rule. Each type will bring different settings for configuration. ● **Start IP Address -** Type the IP address of the starting point for such profile. ● **End IP Address -** Type the IP address of the ending point for such profile if you choose **Range** as **Address**

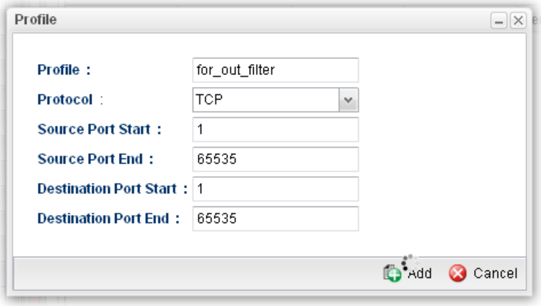
<table>
<tr><td></td><td><b>Type</b>.<ul><li><b>Subnet Mask</b> – Choose the subnet mask from the drop down list if you choose <b>Subnet</b> as <b>Address Type</b>.</li></ul></td></tr>
<tr><td><b>Service Type</b></td><td><b>Service Type -</b> Choose one of the service types from the drop down list.



general target
Service Type

<table>
<tr><th></th><th>Profile</th><th>Protocol</th><th>Source Port Start</th><th>Source Port End</th><th>Destination Port St</th><th>Destination Port Er</th><th>Edit</th></tr>
<tr><td>☑</td><td>AUTH</td><td>TCP</td><td>1</td><td>65535</td><td>113</td><td>113</td><td></td></tr>
<tr><td>□</td><td>BGP</td><td>TCP</td><td>1</td><td>65535</td><td>179</td><td>179</td><td></td></tr>
<tr><td>□</td><td>BOOTPCLIENT</td><td>UDP</td><td>1</td><td>65535</td><td>68</td><td>68</td><td></td></tr>
<tr><td>□</td><td>BOOTPSERVER</td><td>UDP</td><td>1</td><td>65535</td><td>67</td><td>67</td><td></td></tr>
</table>

If you want to create a new service type, simply click to open the following dialog.

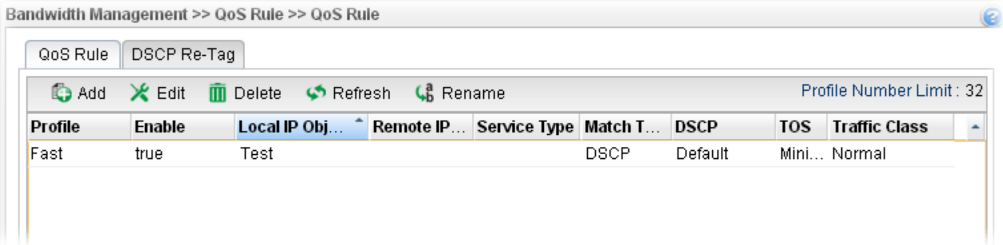


Profile
Profile : for_out_filter
Protocol : TCP
Source Port Start : 1
Source Port End : 65535
Destination Port Start : 1
Destination Port End : 65535
Add Cancel

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

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

5. A QoS rule profiler has been created.



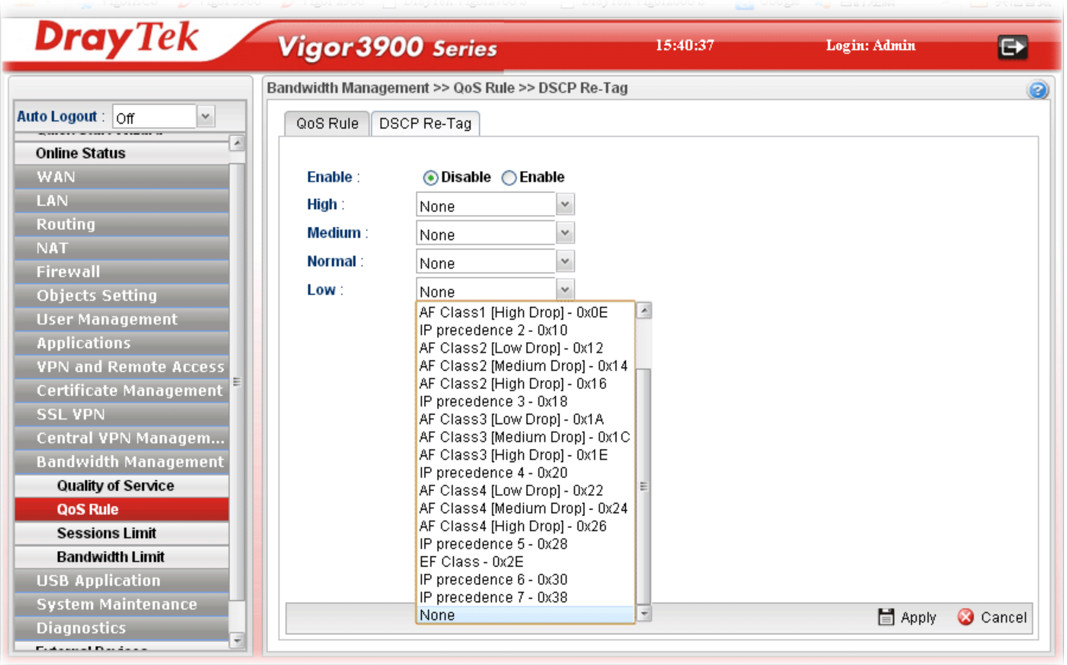
Bandwidth Management >> QoS Rule >> QoS Rule

Profile Number Limit : 32

Profile	Enable	Local IP Obj...	Remote IP...	Service Type	Match T...	DSCP	TOS	Traffic Class
Fast	true	Test			DSCP	Default	Mini...	Normal

4.13.2.2 DSCP Re-Tag

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.



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

Enable : ● Disable ○ Enable
High : None
Medium : None
Normal : None
Low : None

AF Class1 [High Drop] - 0x0E
IP precedence 2 - 0x10
AF Class2 [Low Drop] - 0x12
AF Class2 [Medium Drop] - 0x14
AF Class2 [High Drop] - 0x16
IP precedence 3 - 0x18
AF Class3 [Low Drop] - 0x1A
AF Class3 [Medium Drop] - 0x1C
AF Class3 [High Drop] - 0x1E
IP precedence 4 - 0x20
AF Class4 [Low Drop] - 0x22
AF Class4 [Medium Drop] - 0x24
AF Class4 [High Drop] - 0x26
IP precedence 5 - 0x28
EF Class - 0x2E
IP precedence 6 - 0x30
IP precedence 7 - 0x38
None

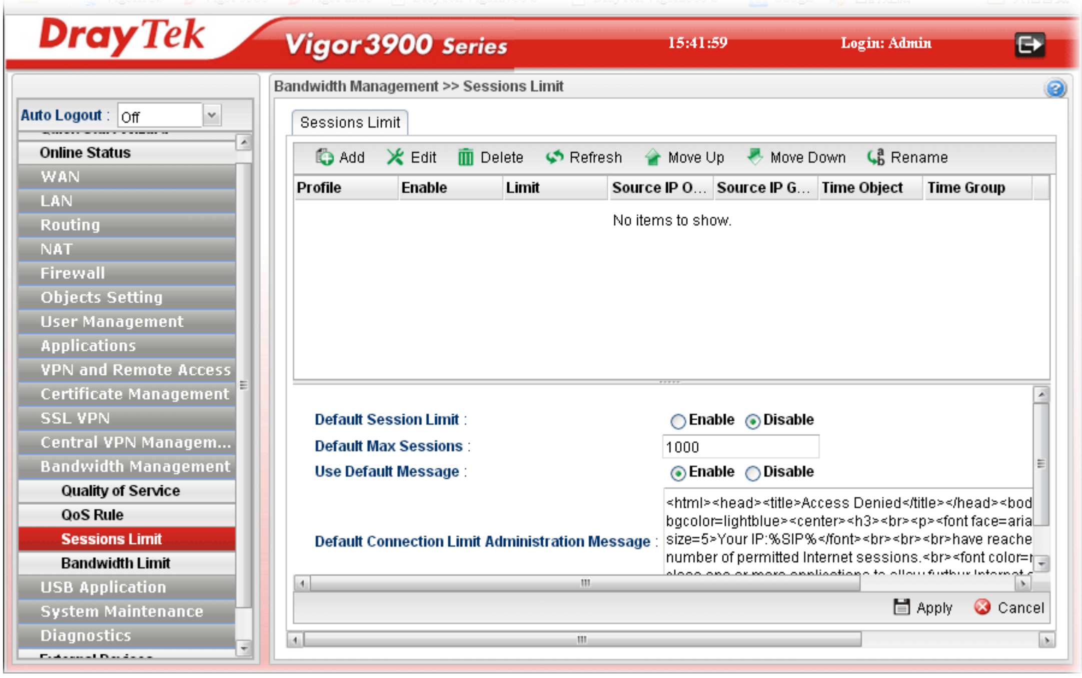
Each item will be explained as follows:

Item	Description
Enable	Enable – Click it to enable DSCP Re-Tag function.
High / Medium / Normal / Low	There are four queues allowed for QoS control. Use the drop down list to specify the heading for each queue which will be applied to the packets tagged.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

4.13.3 Sessions Limit

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

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



Profile	Enable	Limit	Source IP O...	Source IP G...	Time Object	Time Group

No items to show.

Default Session Limit : ○ Enable ● Disable

Default Max Sessions : 1000

Use Default Message : ● Enable ○ Disable

Default Connection Limit Administration Message : <html><head><title>Access Denied</title></head><bod bgcolor=lightblue><center><h3>
<p><font face=aria size=5>Your IP:%SIP%</font>

have reache number of permitted Internet sessions.
<font color=r

Each item will be explained as follows:

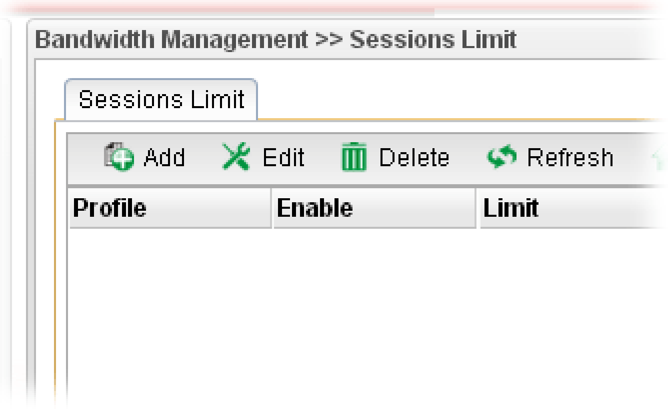
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To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

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

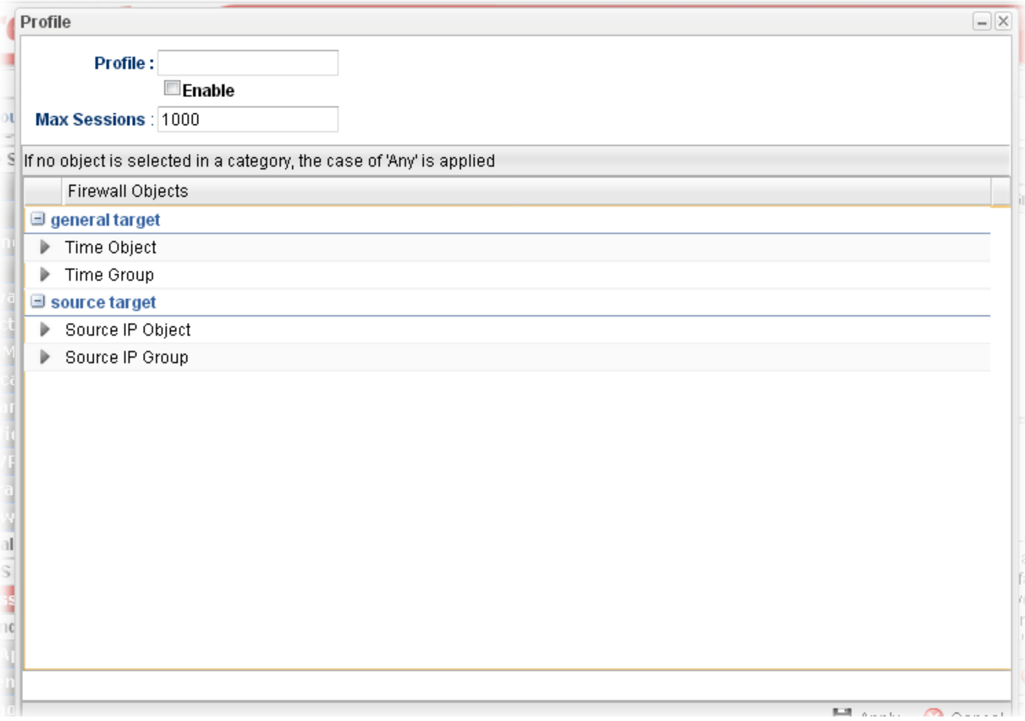
How to add a session limit profile

1. Open **Bandwidth Management>> Sessions Limit.**

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



3. The following dialog will appear.



Profile

Profile :

□ Enable

Max Sessions : 1000

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

Firewall Objects

⊟ general target

▶ Time Object

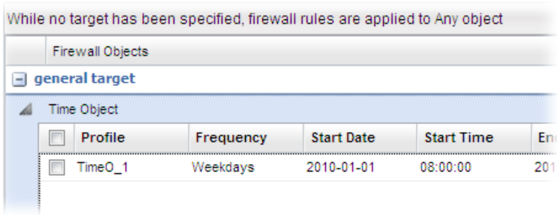
▶ Time Group

⊟ source target

▶ Source IP Object

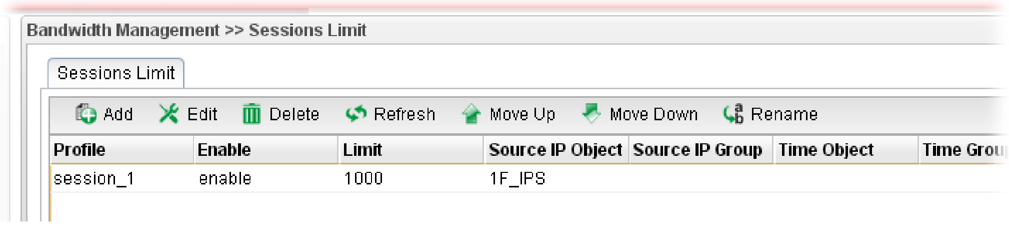
▶ Source IP Group

Available parameters are listed as follows:

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

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

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



Bandwidth Management >> Sessions Limit

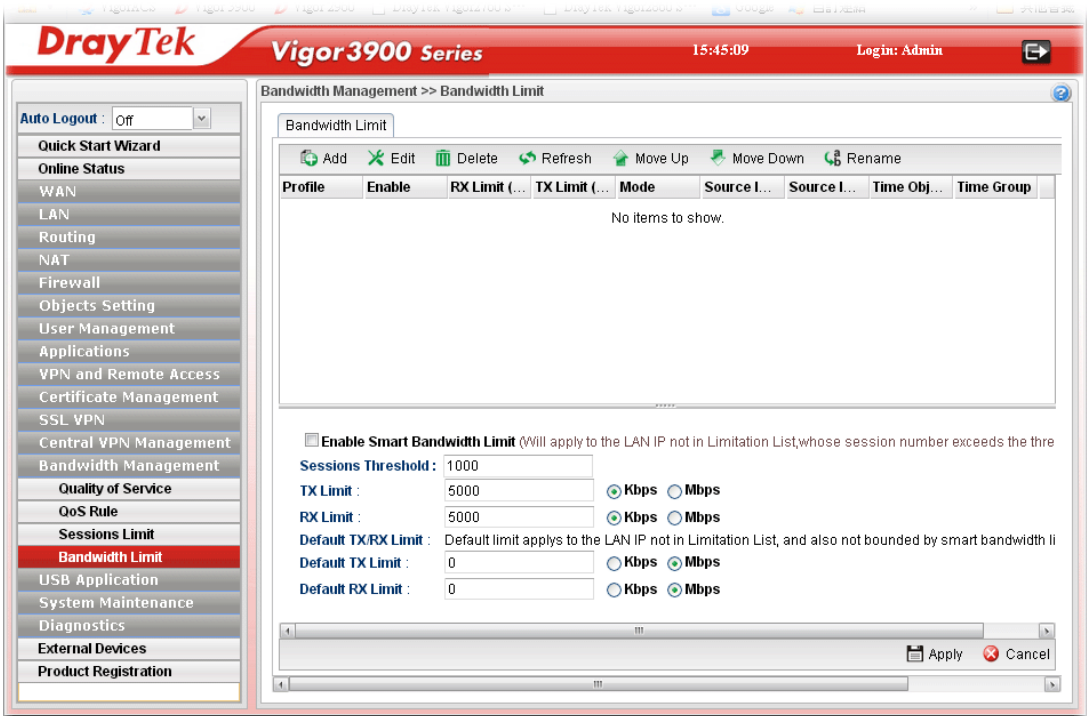
Sessions Limit

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

4.13.4 Bandwidth Limit

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

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



Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

Profile	Enable	RX Limit (...	TX Limit (...	Mode	Source I...	Source I...	Time Obj...	Time Group

No items to show.

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

Sessions Threshold : 1000

TX Limit : 5000 ● Kbps ○ Mbps

RX Limit : 5000 ● Kbps ○ Mbps

Default TX/RX Limit : Default limit applys to the LAN IP not in Limitation List, and also not bounded by smart bandwidth li

Default TX Limit : 0 ○ Kbps ● Mbps

Default RX Limit : 0 ○ Kbps ● Mbps

Each item will be explained as follows:

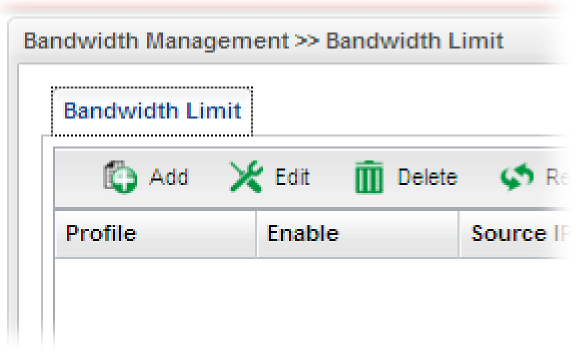
Item	Description

Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Move Up	Change the order of selected profile by moving it up.
Move Down	Change the order of selected profile by moving it down.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the bandwidth limitation profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
RX Limit	Display the limitation for the speed of the downstream.
TX Limit	Display the limitation for the speed of the upstream.
Mode	Display the mode selection (Each/Shared) of the selected profile.
Source IP Object	Display the source IP object profile name.
Source IP Group	Display the source IP group profile name.
Time Object	If no time schedule is set, **None** will be shown in this field.
Time Group	Display the Time group profile selected for such application profile.
Enable Smart Bandwidth Limit	Check this radio button to configure the default limitation for bandwidth for any LAN IP not included in the Limitation List.
Session Threshold	When session number exceeds the set threshold, Smart Bandwidth limit will work.
TX Limit	Define the speed of the upstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission.
RX Limit	Define the speed of the downstream for Smart Bandwidth Limit. If you do not set the limit in this field, the system will use the default speed for the data transmission
Default TX/RX Limit	The default limit will apply to LAN IP(s) not in the above configuration profiles **Default TX Limit** – Define the limitation for the speed of the upstream. **Default RX Limit** –Define the limitation for the speed of the upstream.

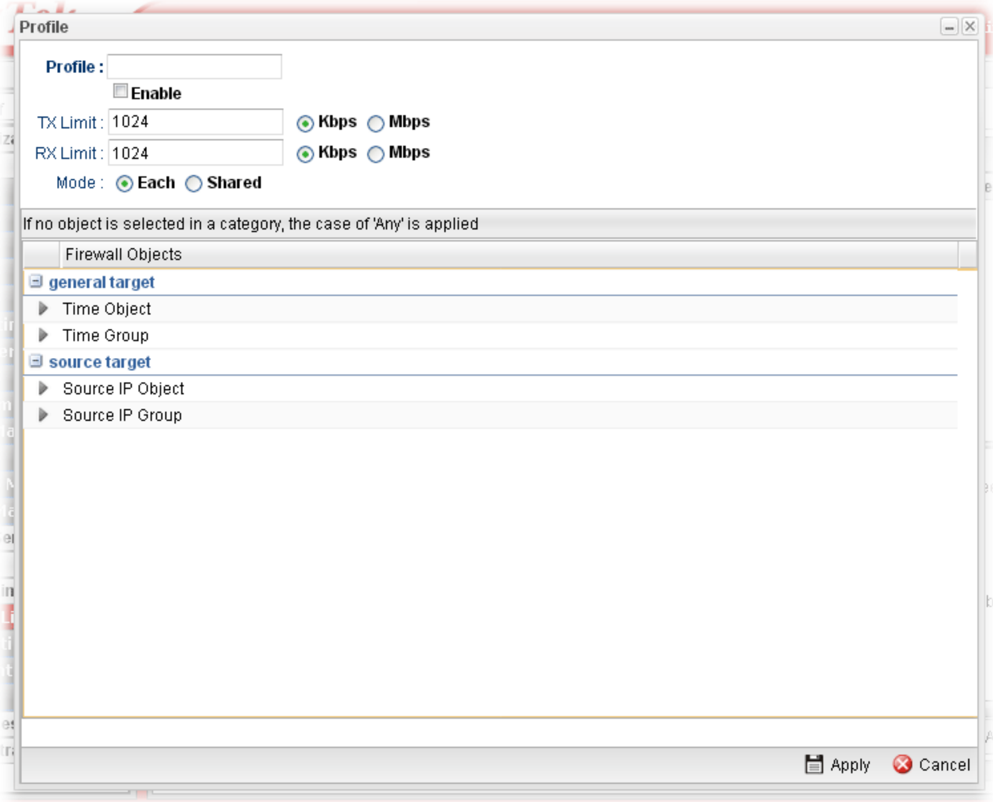
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to add a bandwidth limit profile

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



3. The following dialog will appear.



Profile :

□ Enable

TX Limit : 1024 ● Kbps ○ Mbps

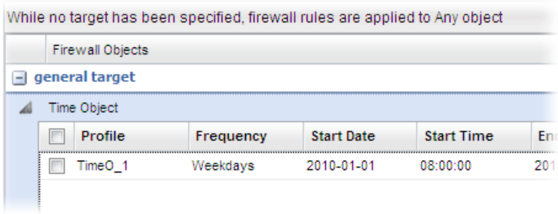
RX Limit : 1024 ● Kbps ○ Mbps

Mode : ● Each ○ Shared

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

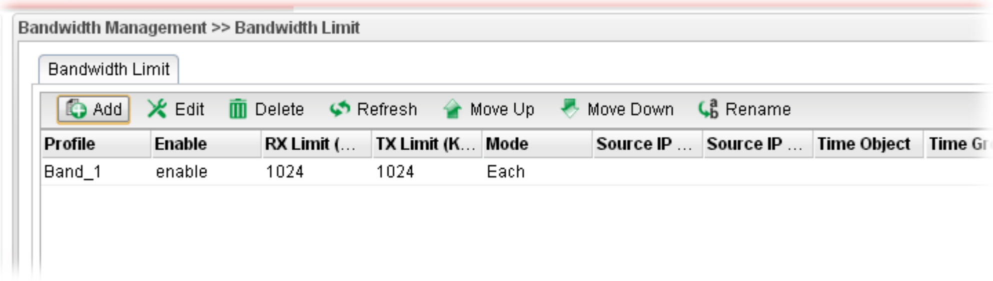
Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable such profile.
TX Limit(Kbps)	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default

	speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
RX Limit(Kbps)	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. Do not type the value with “0”, otherwise the profile cannot be saved.
Mode	Select **Each** to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select **Shared** to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.
general target	**Time Object -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click ⊕ to create another new time object profile.  While no target has been specified, firewall rules are applied to Any object Firewall Objects ⊟ general target Time Object □ Profile | Frequency | Start Date | Start Time | En □ TimeO_1 | Weekdays | 2010-01-01 | 08:00:00 | 201 **Time Group -** Click the triangle icon ▶ to display the profile selection box. Choose a schedule group profile to be applied on such rule. You can click ⊕ to create another new time group profile.
source target	**Source IP Object -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source target. You can click ⊕ to create another new IP object profile. **Source IP Group -** Click the triangle icon ▶ to display the profile selection box. Choose one or more IP group profiles from the drop down list. The selected profile will be treated as source target. You can click ⊕ to create another new IP group profile.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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

5. A bandwidth limit profile has been created.



Bandwidth Management >> Bandwidth Limit

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

4.14 USB Application

4.14.1 Temperature Sensor

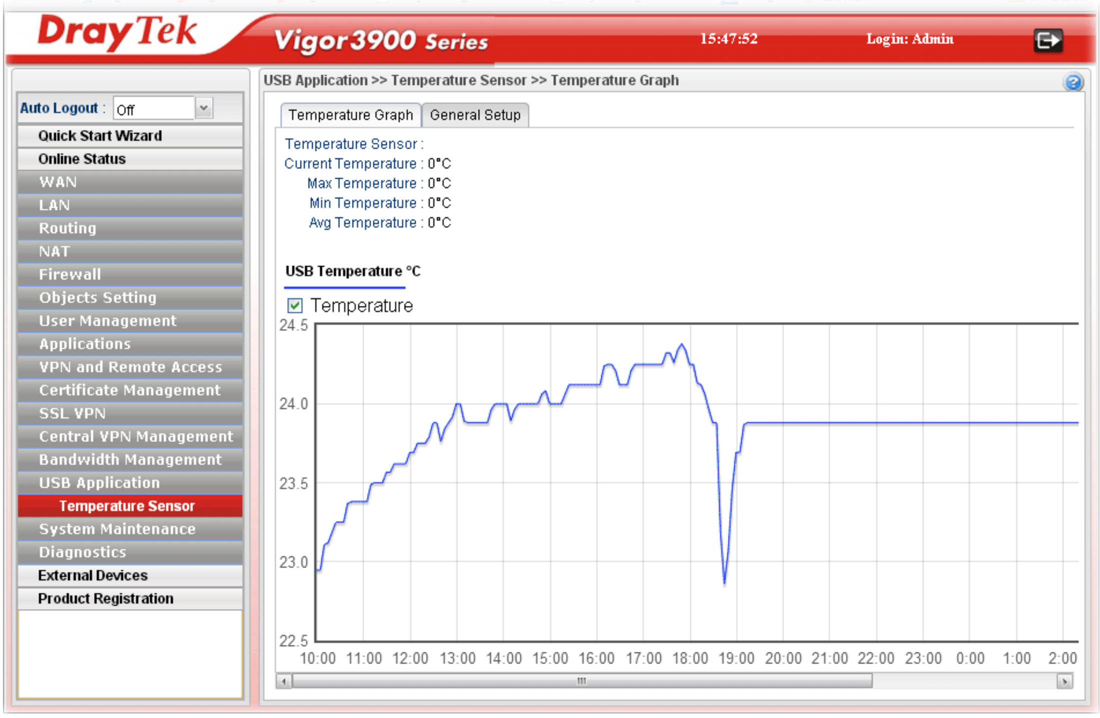
A USB Thermometer is now available that complements your installed DrayTek router installations that will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

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

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

4.14.1.1 Temperature Graph

Below shows an example of temperature graph:



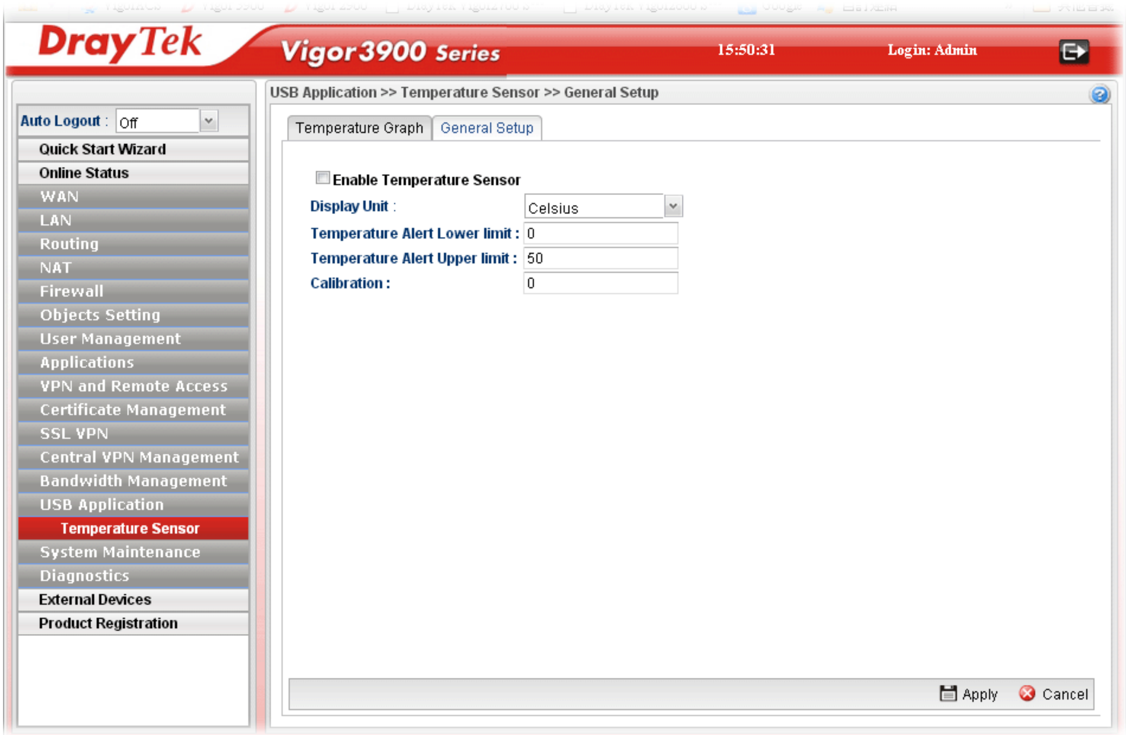
USB Application >> Temperature Sensor >> Temperature Graph

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

Available settings are explained as follows:

Item	Description
Enable Temperature Sensor	Check this box to enable such function.
Display Unit	Choose **Celsius** or **Fahrenheit** as the display unit.
Temperature Alert Lower limit / Temperature Alert Upper limit	Type the upper limit and lower limit for the system to send out temperature alert.
Calibration	Type a value used for correcting the temperature error.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

4.14.1.2 General Setup



USB Application >> Temperature Sensor >> General Setup

□ Enable Temperature Sensor

Display Unit : Celsius

Temperature Alert Lower limit : 0

Temperature Alert Upper limit : 50

Calibration : 0

Available settings are explained as follows:

Item	Description
Enable Temperature Sensor	Check this box to enable such function.
Display Unit	Choose **Celsius** or **Fahrenheit** as the display unit.
Temperature Alert Lower limit / Temperature Alert Upper limit	Type the upper limit and lower limit for the system to send out temperature alert.
Calibration	Type a value used for correcting the temperature error.
Apply	Click it to save the configuration and exit the dialog.

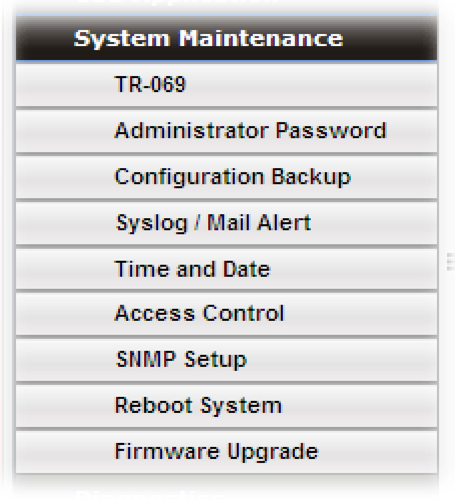
Cancel	Click it to exit the dialog without saving the configuration.

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

4.15 System Maintenance

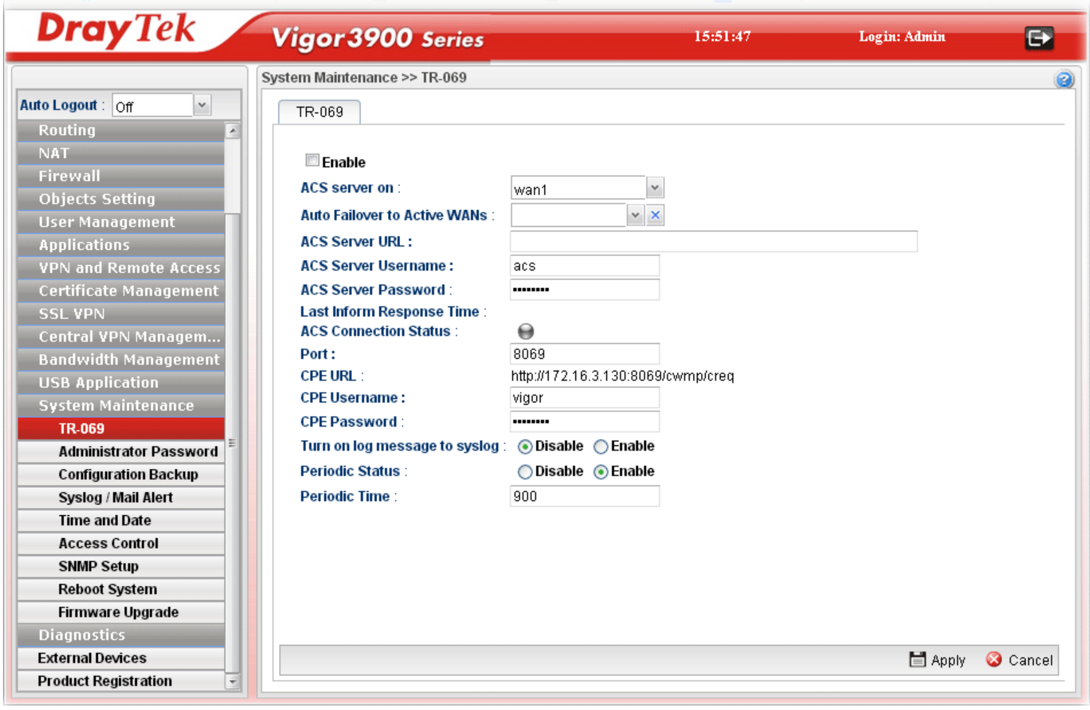
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog/Mail Alert, Time and Date, Access Control, SNMP Setup, Reboot System, Firmware Upgrade and Upload Language File.

Below shows the menu items for System Maintenance.



4.15.1 TR-069

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



System Maintenance >> TR-069

TR-069

□ Enable

ACS server on : wan1

Auto Failover to Active WANs :

ACS Server URL :

ACS Server Username : acs

ACS Server Password : ••••••••

Last Inform Response Time :

ACS Connection Status :

Port : 8069

CPE URL : http://172.16.3.130:8069/cwmp/creq

CPE Username : vigor

CPE Password : ••••••••

Turn on log message to syslog : ● Disable ○ Enable

Periodic Status : ○ Disable ● Enable

Periodic Time : 900

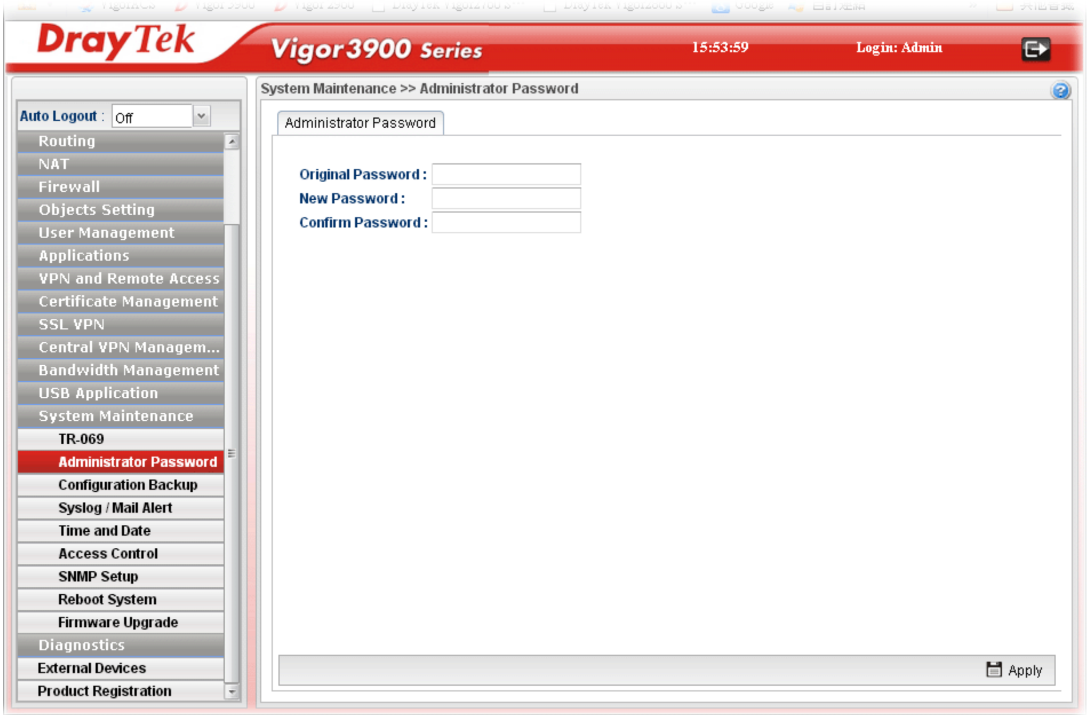
Each item will be explained as follows:

Item	Description
Enable	Check this box to enable such profile.
ACS server on	Choose one of the WANlLAN profiles which will be recognized by VigorACS.
Auto Failover to Active WANs	Specify the WAN interface to take over the job of network connection when the original WAN interface fails.
ACS Server URL/ **ACS Server Username /** **ACS Server Password**	Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
Last Inform Response Time	Display the response time informed by VigorACS.
ACS Connection Status	When it lights in green, it means the router has been detected and can be managed by VigorACS.
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.
Turn on log message to syslog	The default setting **Disable**. Click **Enable** to make the log message being recorded by Syslog.
Periodic Status	The default setting is **Enable**. Please set periodic time for VigorACS to send notification to CPE. Or click **Disable** to close the mechanism of notification.
Periodic Time	Set the time for VigorACS to send notification to CPE.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

4.15.2 Administrator Password

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



Each item will be explained as follows:

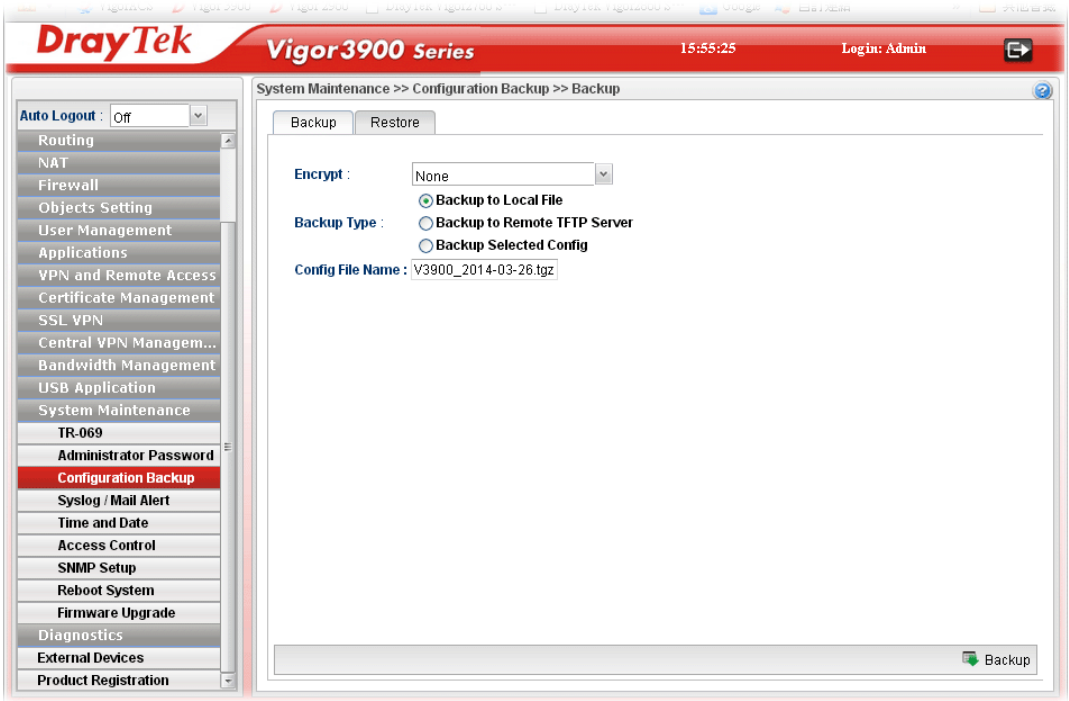
Item	Description
User Name	Display the name of the administrator.
Original Password	Type the old password.
New Password	Type the new password.
Confirm Password	Re-type the new password for confirmation.
Apply	Click this button to save the configuration and exit the web page.

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

4.15.3 Configuration Backup

Most of the settings can be saved locally as a configuration file, and can be applied to another router. The router supports functions of **restore and backup** for the configuration file.

4.15.3.1 Backup



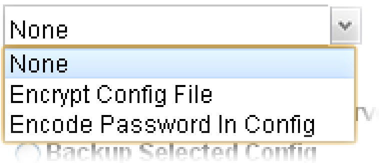
System Maintenance >> Configuration Backup >> Backup

Encrypt : None

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

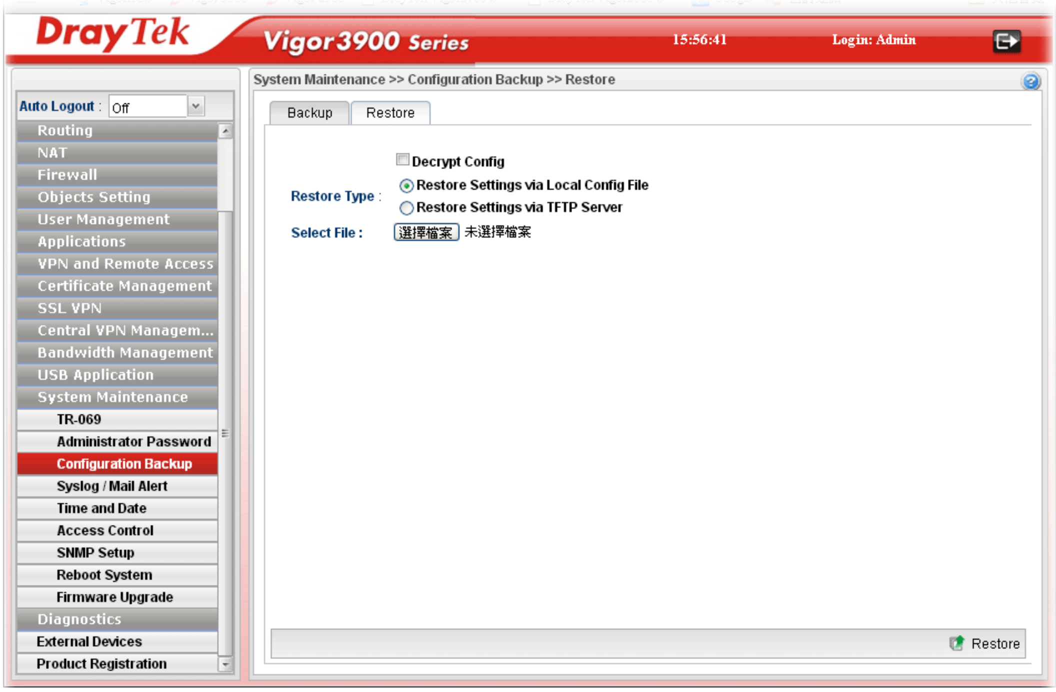
Config File Name : V3900_2014-03-26.tgz

Each item will be explained as follows:

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

	stored with an existing file in local host. You must select which file you want to store.
Config File Name	Display the default configuration file name. You can change the name if required.
Backup	Execute the file downloading job to the computer.

4.15.3.2 Restore



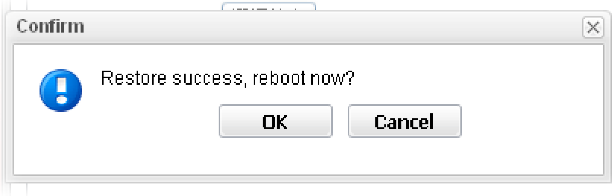
☐ Decrypt Config

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

Select File : 選擇檔案 未選擇檔案

Each item will be explained as follows:

Item	Description
Decrypt Config	Check this box to decrypt an encrypted configuration file. You can specify a password for decrypting the file for restoring it for use next time. **Password** – Type a password for encrypting the file. **Confirm Password –** Retype the password for confirmation.
Restore Type	Choose one of the types to determine where the file will be downloaded from. **Restore Settings via Local Config File** – Click it to restore the configuration settings through a configuration file stored locally. **Restore Settings via TFTP Server** – Click it to restore the configuration settings through TFTP server.
Select File	Use the ... **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.

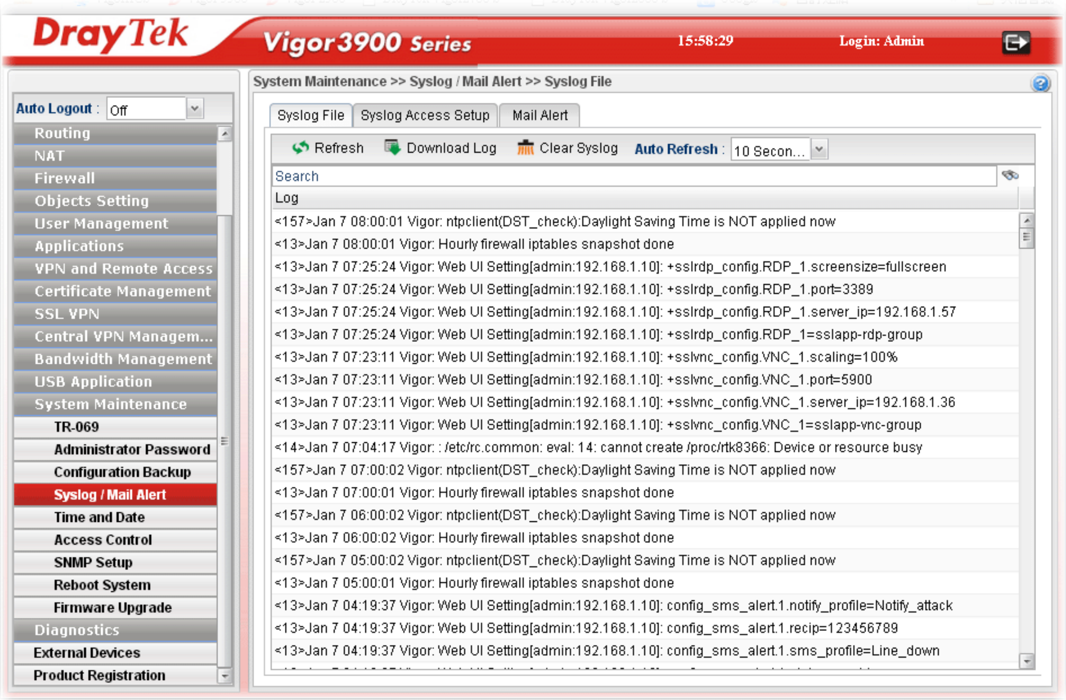
	 Confirm Restore success, reboot now? OK Cancel

4.15.4 Syslog / Mail Alert

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

4.15.4.1 SysLog File

This page displays all the operation logs for the router.

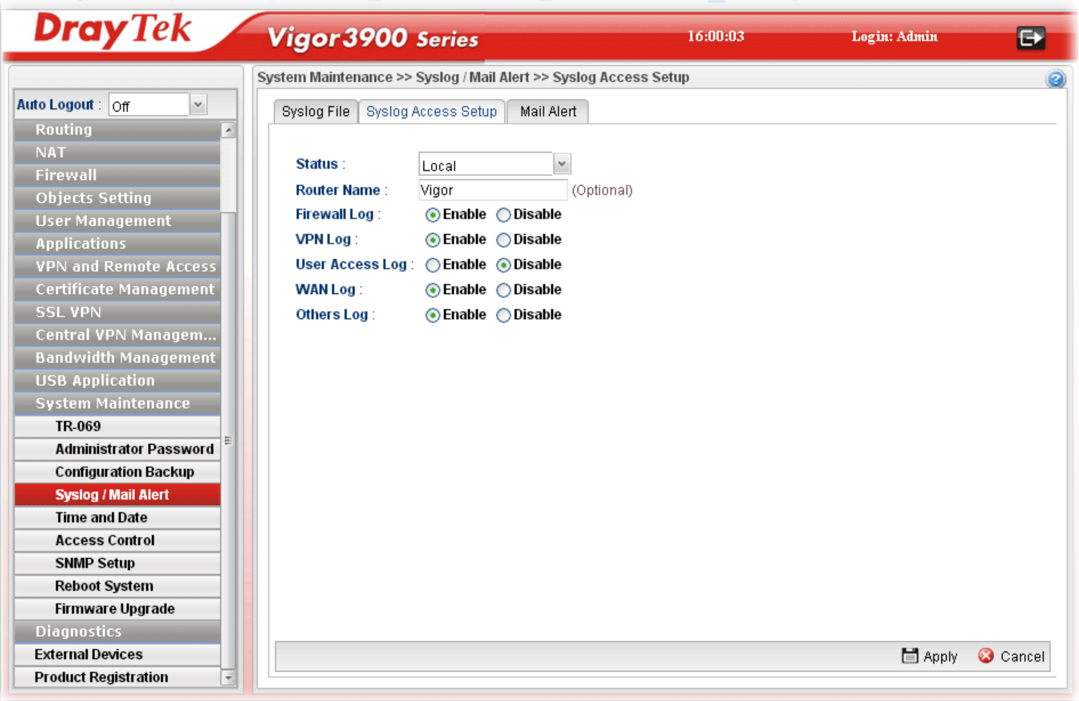


```
<157>Jan 7 08:00:01 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
<13>Jan 7 08:00:01 Vigor: Hourly firewall iptables snapshot done
<13>Jan 7 07:25:24 Vigor: Web UI Setting[admin:192.168.1.10]: +sslrdp_config.RDP_1.screensize=fullscreen
<13>Jan 7 07:25:24 Vigor: Web UI Setting[admin:192.168.1.10]: +sslrdp_config.RDP_1.port=3389
<13>Jan 7 07:25:24 Vigor: Web UI Setting[admin:192.168.1.10]: +sslrdp_config.RDP_1.server_ip=192.168.1.57
<13>Jan 7 07:25:24 Vigor: Web UI Setting[admin:192.168.1.10]: +sslrdp_config.RDP_1=sslapp-rdp-group
<13>Jan 7 07:23:11 Vigor: Web UI Setting[admin:192.168.1.10]: +sslvnc_config.VNC_1.scaling=100%
<13>Jan 7 07:23:11 Vigor: Web UI Setting[admin:192.168.1.10]: +sslvnc_config.VNC_1.port=5900
<13>Jan 7 07:23:11 Vigor: Web UI Setting[admin:192.168.1.10]: +sslvnc_config.VNC_1.server_ip=192.168.1.36
<13>Jan 7 07:23:11 Vigor: Web UI Setting[admin:192.168.1.10]: +sslvnc_config.VNC_1=sslapp-vnc-group
<14>Jan 7 07:04:17 Vigor: : /etc/rc.common: eval: 14: cannot create /proc/rtk8366: Device or resource busy
<157>Jan 7 07:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
<13>Jan 7 07:00:01 Vigor: Hourly firewall iptables snapshot done
<157>Jan 7 06:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
<13>Jan 7 06:00:02 Vigor: Hourly firewall iptables snapshot done
<157>Jan 7 05:00:02 Vigor: ntpclient(DST_check):Daylight Saving Time is NOT applied now
<13>Jan 7 05:00:01 Vigor: Hourly firewall iptables snapshot done
<13>Jan 7 04:19:37 Vigor: Web UI Setting[admin:192.168.1.10]: config_sms_alert.1.notify_profile=Notify_attack
<13>Jan 7 04:19:37 Vigor: Web UI Setting[admin:192.168.1.10]: config_sms_alert.1.recip=123456789
<13>Jan 7 04:19:37 Vigor: Web UI Setting[admin:192.168.1.10]: config_sms_alert.1.sms_profile=Line_down
```

Available parameters are listed as follows:

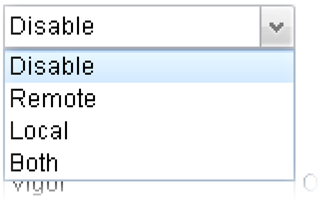
Item	Description
Refresh	Renew the web page.
Download Log	Save or open the Syslog file.
Clear Syslog	Remove all of the records.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.

4.15.4.2 Syslog Access Setup



Status : Local
Router Name : Vigor (Optional)
Firewall Log : ● Enable ○ Disable
VPN Log : ● Enable ○ Disable
User Access Log : ○ Enable ● Disable
WAN Log : ● Enable ○ Disable
Others Log : ● Enable ○ Disable

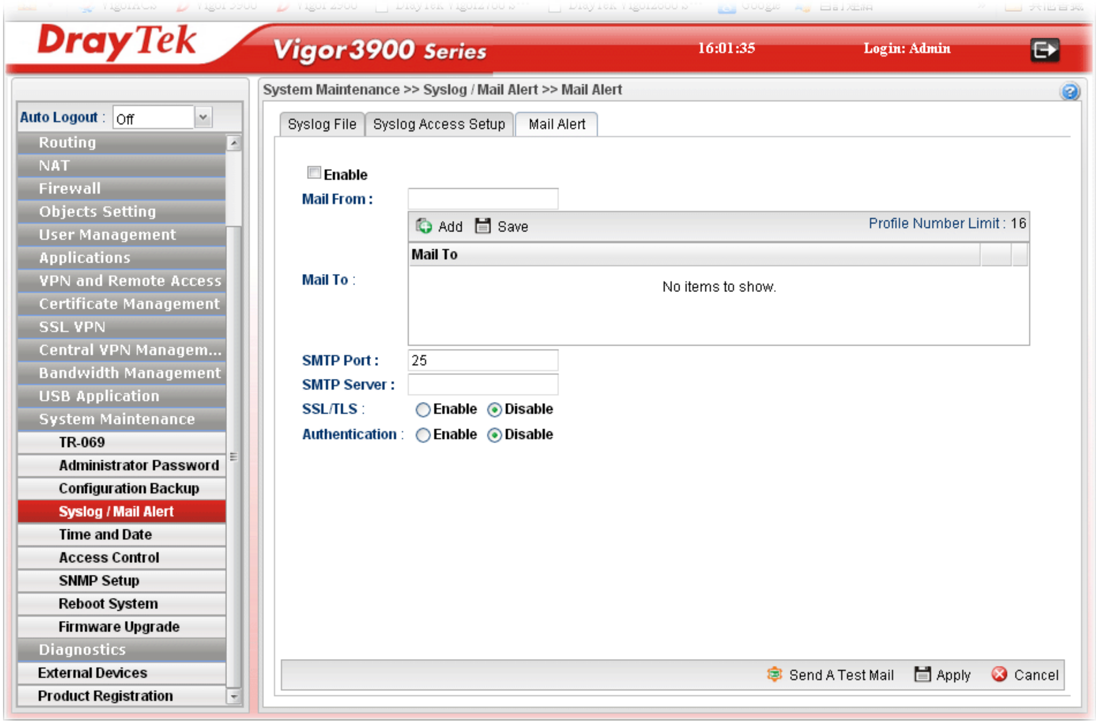
Available parameters are listed as follows:

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

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

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

4.15.4.3 Mail Alert



□ Enable

Mail From :

Mail To : No items to show.

SMTP Port : 25

SMTP Server :

SSL/TLS : ○ Enable ● Disable

Authentication : ○ Enable ● Disable

Available parameters are listed as follows:

Item	Description
Enable	Check the box to enable such profile.
Mail From	Type a mail address for the mail sender.
Mail To	Assign a mail address for the mail receiver. **Add** – Click this button to display a field for adding e-mail address. **Save** – After finished the address configuration, click Save to save the setting onto the router.
SMTP Port	Type the port number for SMTP server.
SMTP Server	Type the IP address for SMTP server.
SSL/TLS	Click Enable to activate SSL/TLS server.
Authentication	Click **Enable** to make any user logging into the mail server. If you click **Enable**, you have to type user name and user password on the below fields.
User Name	Type the user name for authentication.
User Password	Type the password for authentication.
Send A Test Mail	Click it to send a test mail to the specified address.

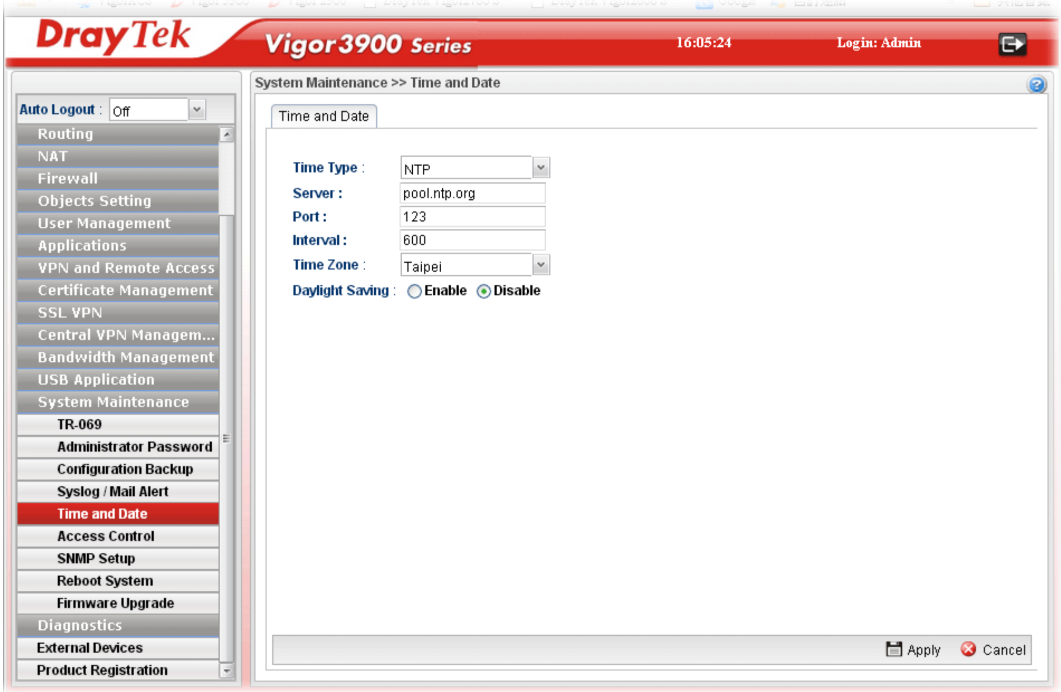
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

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

4.15.5 Time and Date

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

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



Time Type : NTP
Server : pool.ntp.org
Port : 123
Interval : 600
Time Zone : Taipei
Daylight Saving : ○ Enable ● Disable

Available parameters are listed as follows:

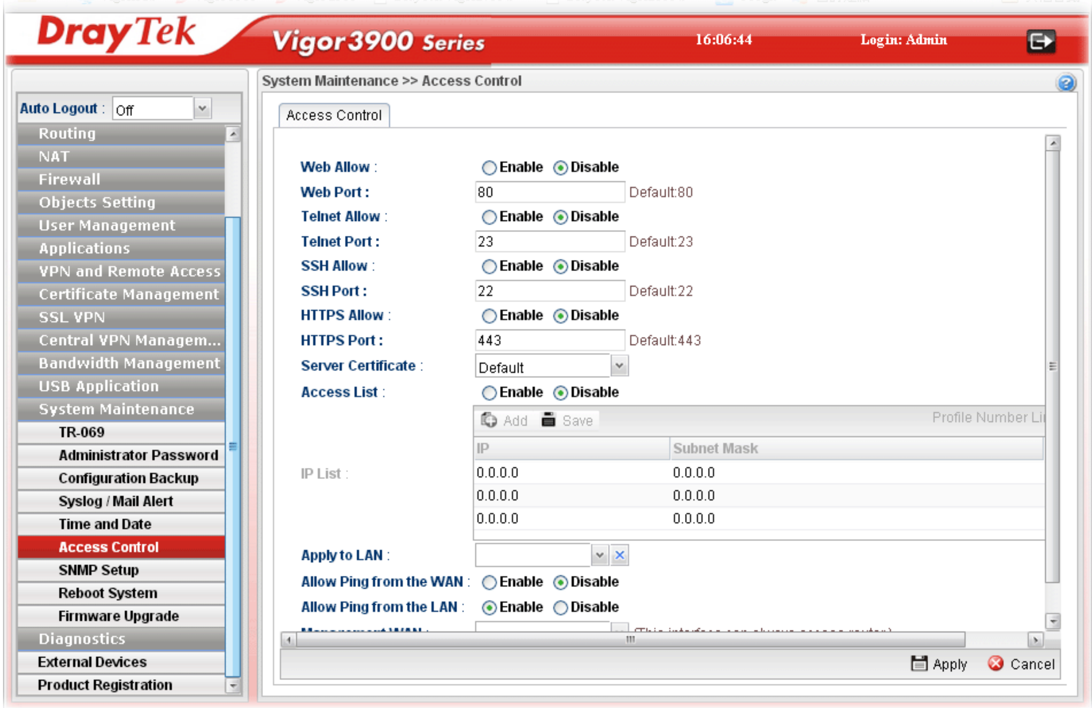
Item	Description
Time Type	**NTP** – Select to inquire time information from Time Server on the Internet using assigned protocol. **Browser -** Select this option to use the browser time from the remote administrator PC host as router's system time.
Server	Type the domain name of the server.
Port	Type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

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

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

4.15.6 Access Control

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



Web Allow : ○ Enable ● Disable

Web Port : 80 Default:80

Telnet Allow : ○ Enable ● Disable

Telnet Port : 23 Default:23

SSH Allow : ○ Enable ● Disable

SSH Port : 22 Default:22

HTTPS Allow : ○ Enable ● Disable

HTTPS Port : 443 Default:443

Server Certificate : Default

Access List : ○ Enable ● Disable

IP List :

IP	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

Apply to LAN :

Allow Ping from the WAN : ○ Enable ● Disable

Allow Ping from the LAN : ● Enable ○ Disable

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.
Server Certificate	Use the default setting.

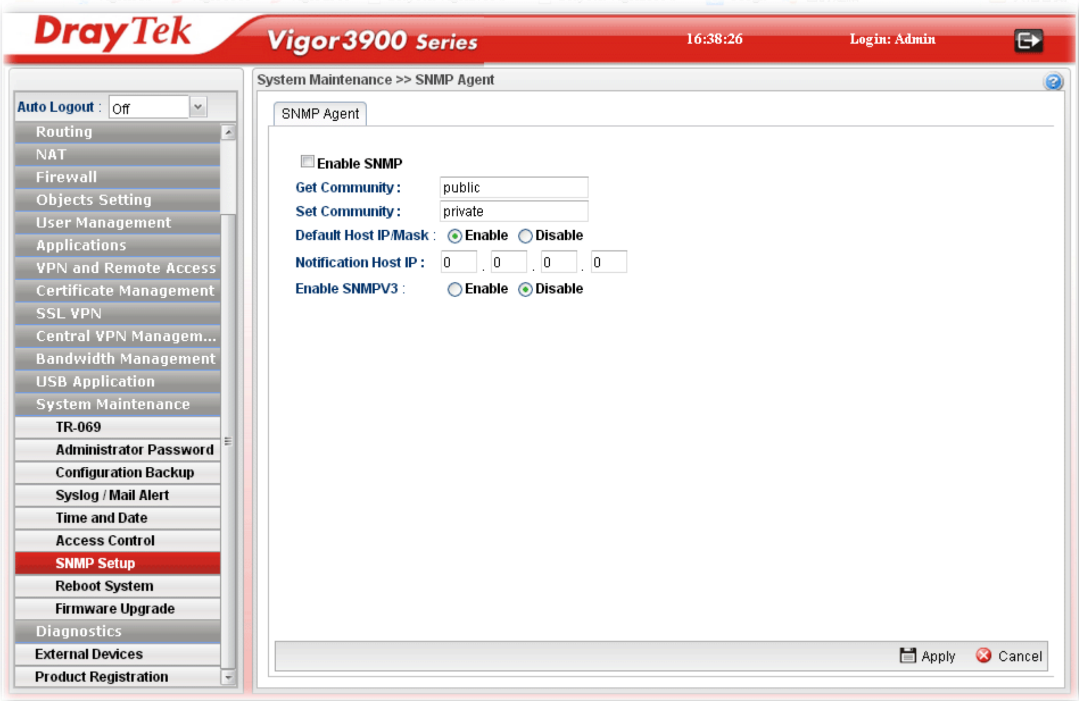
Access List	Click **Enable** to allow system administrator to login from the user defined IP address and management the web page of the router. If you enable such function, the system can be managed by these three IP addresses via WAN.
IP List	Type the first IP address for the system administrator to login. The former boxes indicate the IP address allowed to login to the router, and the later box indicates a subnet mask allowed to login to the router.
Apply to LAN	Choose the LAN profile(s) that the IPs controlled under such profile are allowed to access into the web user interface of Vigor3900.
Allow Ping from WAN	Click **Enable** to allow system administrator to ping the router from WAN interface.
Block LAN Profile	Choose the LAN profile(s) that the IPs controlled under such profile will be blocked by Vigor3900.
Management WAN	Only the interface selected here can be used to access into this router.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

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

4.15.7 SNMP Setup

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

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.



System Maintenance >> SNMP Agent

SNMP Agent

□ Enable SNMP

Get Community : public

Set Community : private

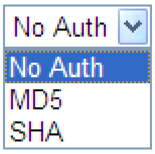
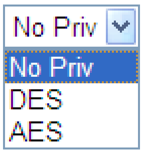
Default Host IP/Mask : ● Enable ○ Disable

Notification Host IP : 0 . 0 . 0 . 0

Enable SNMPV3 : ○ Enable ● Disable

Apply Cancel

Available parameters are listed as follows:

Item	Description
Enable	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.**
Default Host IP/Mask	Click **Enable** to use the default IP and mask of the host as the SNMP agent. If you click **Disable,** you need to type the IP address and choose the mask manually in related fields.
Notification Host IP	Type the IP address of the host for notification.
Enable SnmpV3	Click **Enable** to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

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

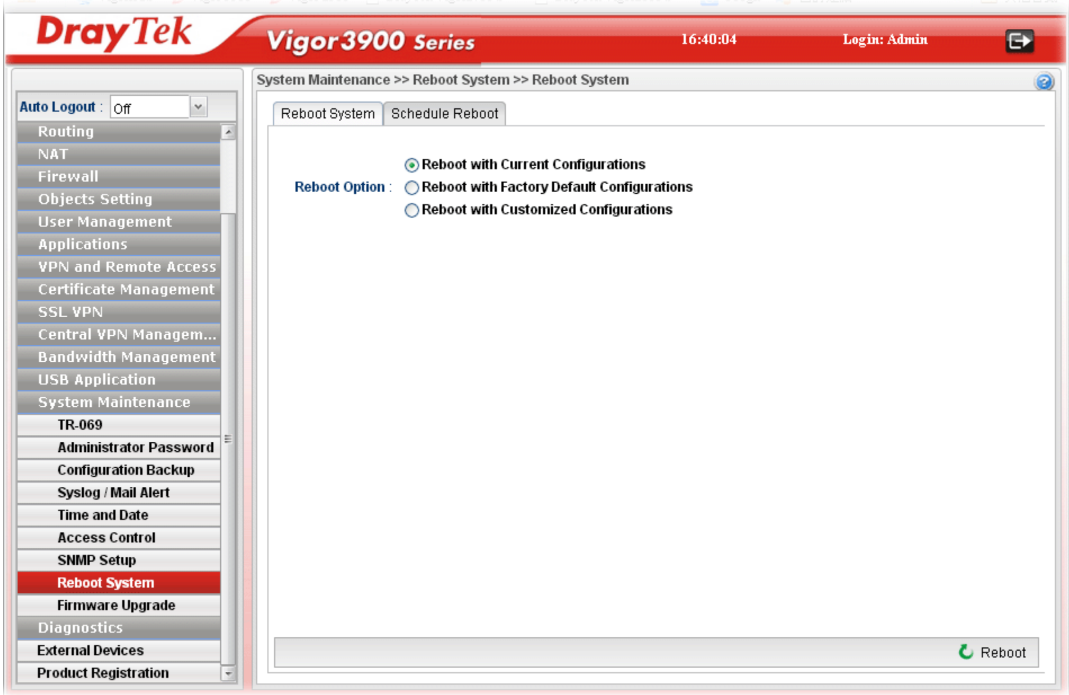
4.15.8 Reboot System

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

If you want to reboot the router using the current configuration, choose **Reboot with Current Configurations** and click **Reboot**. To reset the router settings to default values, click **Reboot with Factory Default Configurations** and click **Reboot**. The router will take a period of time to reboot the system.

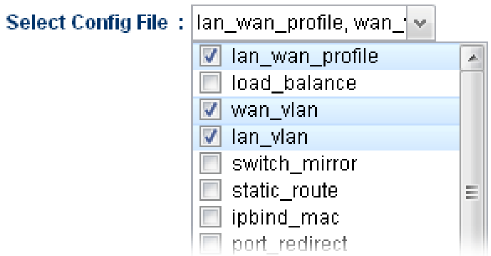
4.15.8.1 Reboot System

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



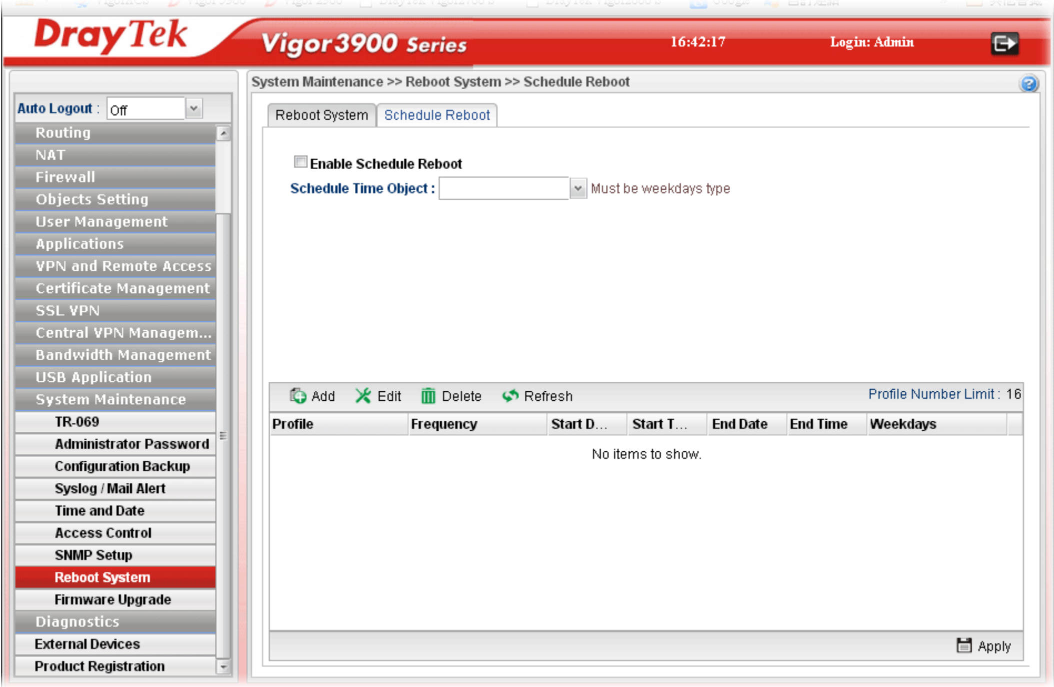
Reboot Option : ● Reboot with Current Configurations
○ Reboot with Factory Default Configurations
○ Reboot with Customized Configurations

Available parameters are listed as follows:

Item	Description
Reboot with Current Configurations	Click it to reboot the router using the current configuration. Then, click **Reboot**..
Reboot with Factory Default Configurations	Click it to reset the router settings to default values. Then, click **Reboot**.
Reboot with Customized Configurations	Click it to reboot the router using the current configuration (only the configuration settings listed and selected below). If you choose this option, **Select Config File** will be available for you to select.  Select Config File : lan_wan_profile, wan_ ☑ lan_wan_profile □ load_balance ☑ wan_vlan ☑ lan_vlan □ switch_mirror □ static_route □ ipbind_mac □ port_redirect

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

4.15.8.2 Schedule Reboot



□ Enable Schedule Reboot

Schedule Time Object : Must be weekdays type

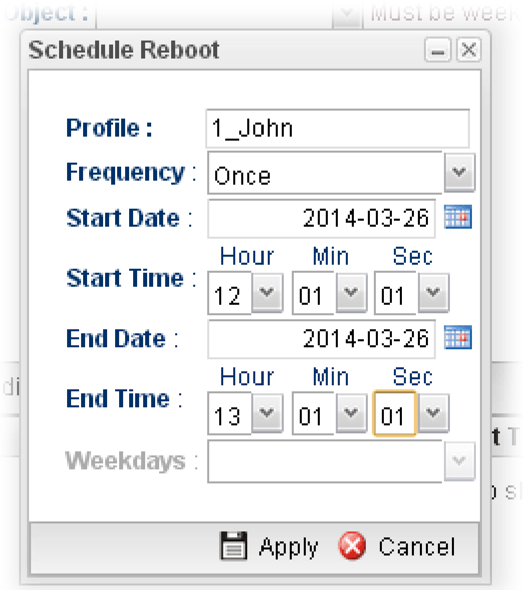
Available parameters are listed as follows:

Item	Description
Enable Schedule Reboot	Check the box to enable such option.
Schedule Time Object	Use the drop down list to choose one of the time objects to perform the schedule reboot.
Add	Add a new profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the **Edit** button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the **Delete** button.
Refresh	Renew current web page.
Profile	Display the name of the schedule profile.
Frequency	Display the type (Once or Weekdays) of frequency selected for the profile.
Start Date	Display the starting date of the profile.
Start Time	Display the starting time of the profile.

End Date	Display the ending date of the profile.
End Time	Display the ending time of the profile.
Weekdays	Display which day in a week shall perform the reboot job.

How to add a schedule profile

1. Open **System Maintenance>>Schedule Reboot.**
2. Simply click the **Add** button.
3. The following dialog will appear.



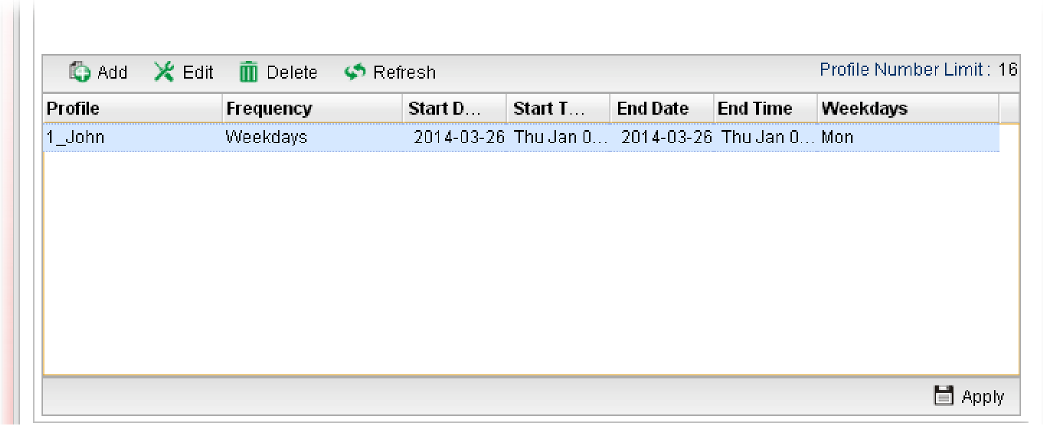
Profile : 1_John
Frequency : Once
Start Date : 2014-03-26
Start Time : Hour 12 Min 01 Sec 01
End Date : 2014-03-26
End Time : Hour 13 Min 01 Sec 01
Weekdays :

Available parameters are listed as follows:

Item	**Description**
Profile	Type the name of the profile.
Frequency	Specify how often the schedule will be applied. **Once** -The schedule will be applied just once **Weekdays** -Specify which days in one week should perform the schedule.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
End Date	Specify the ending date of the schedule.
End Time	Specify the ending time of the schedule.

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

5. A schedule profile has been created.



Profile Number Limit : 16

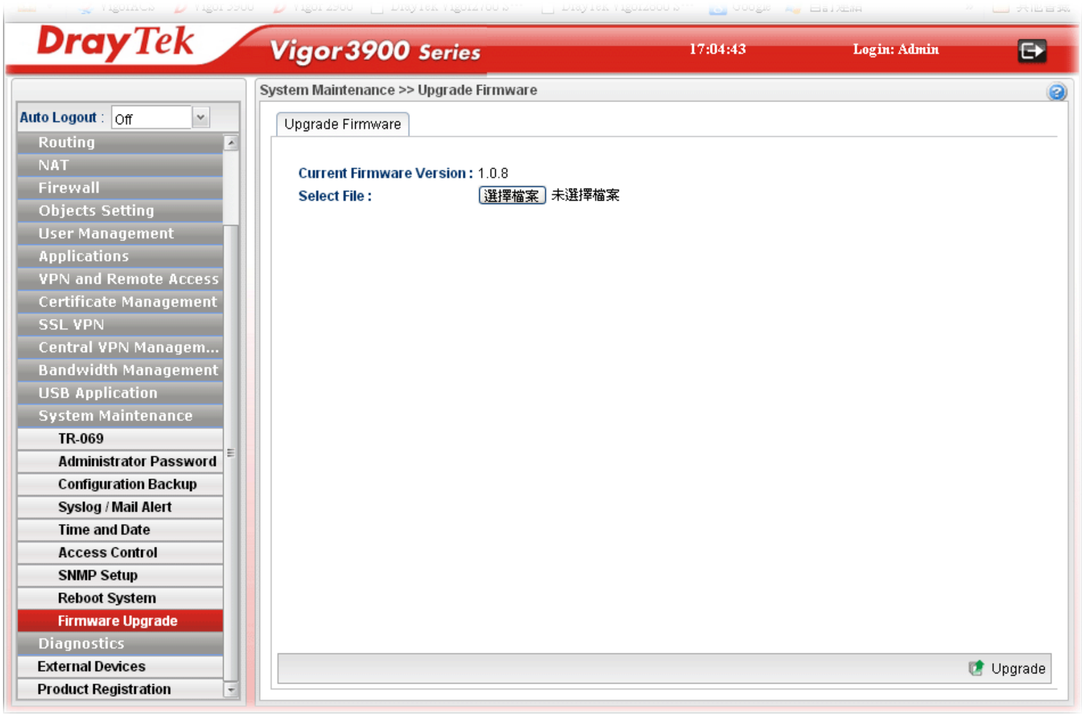
Profile	Frequency	Start D...	Start T...	End Date	End Time	Weekdays
1_John	Weekdays	2014-03-26	Thu Jan 0...	2014-03-26	Thu Jan 0...	Mon

4.15.9 Firmware Upgrade

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

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

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



Current Firmware Version : 1.0.8

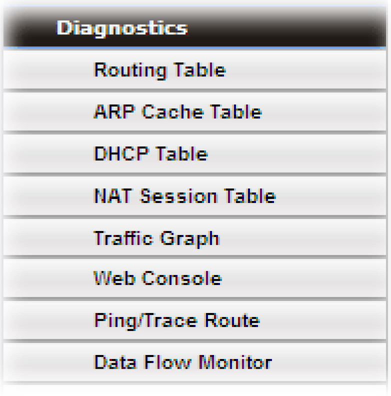
Select File : 選擇檔案 未選擇檔案

Available parameters are listed as follows:

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

4.16 Diagnostics

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

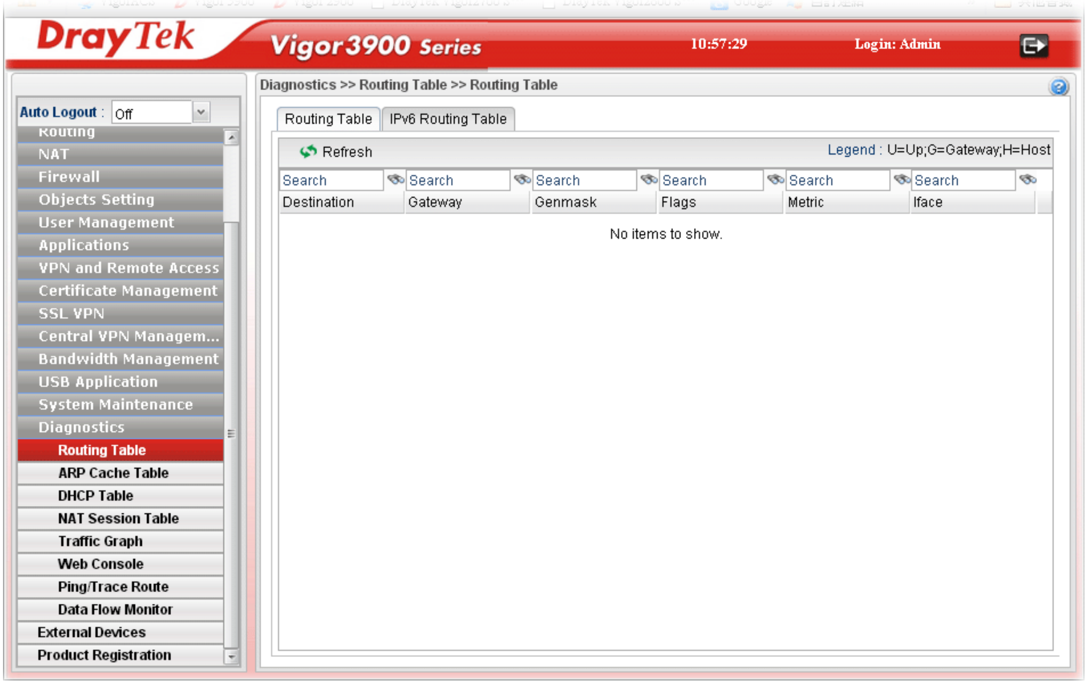


4.16.1 Routing Table

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

4.16.1.2 Routing Table

Display the information for each route.



Diagnostics >> Routing Table >> Routing Table

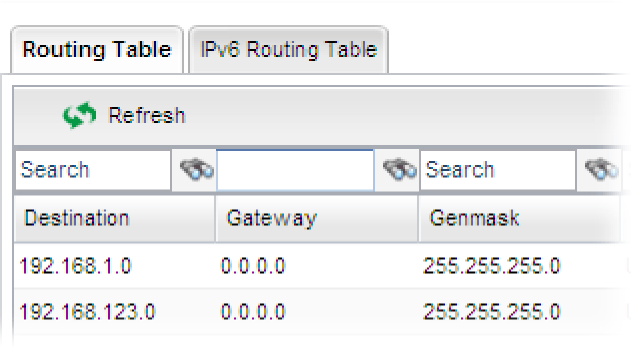
Legend : U=Up;G=Gateway;H=Host

Destination	Gateway	Genmask	Flags	Metric	Iface

No items to show.

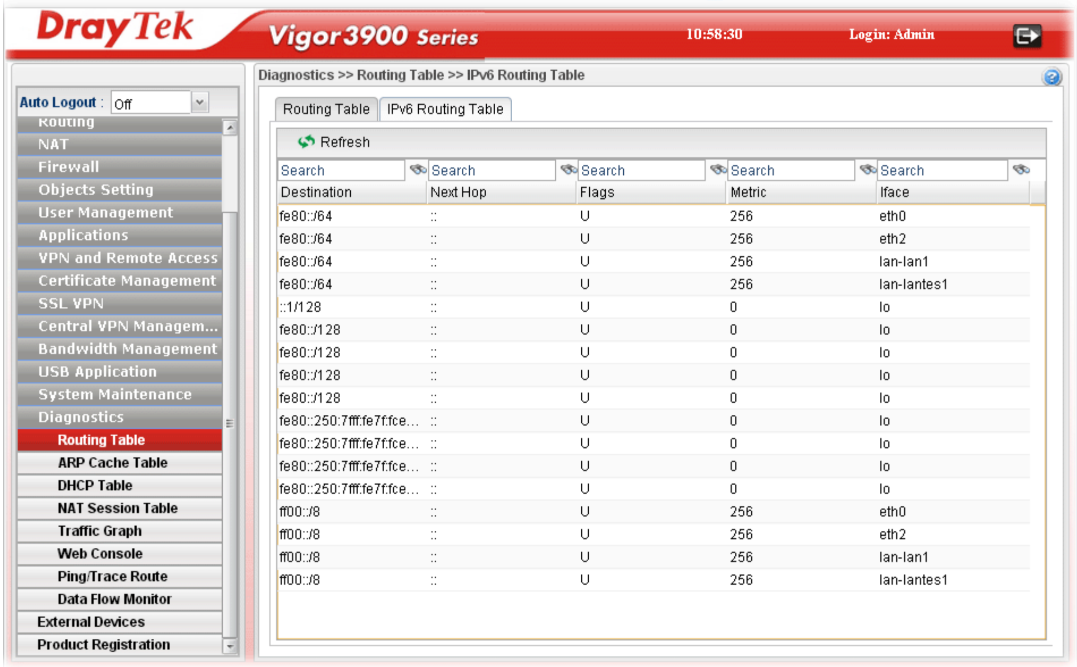
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The

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

4.16.1.2 IPv6 Routing Table

Display the information for each route with IPv6 protocol.



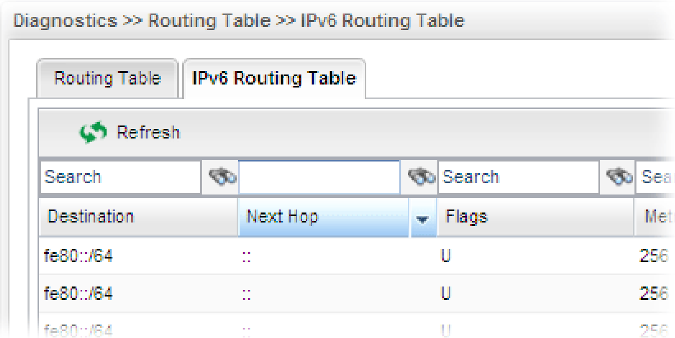
Diagnostics >> Routing Table >> IPv6 Routing Table

Routing Table | IPv6 Routing Table

Refresh

Destination	Next Hop	Flags	Metric	Iface
Search	Search	Search	Search	Search
fe80::/64	::	U	256	eth0
fe80::/64	::	U	256	eth2
fe80::/64	::	U	256	lan-lan1
fe80::/64	::	U	256	lan-lantes1
::1/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::250:7fff:fe7f:fce...	::	U	0	lo
fe80::250:7fff:fe7f:fce...	::	U	0	lo
fe80::250:7fff:fe7f:fce...	::	U	0	lo
fe80::250:7fff:fe7f:fce...	::	U	0	lo
ff00::/8	::	U	256	eth0
ff00::/8	::	U	256	eth2
ff00::/8	::	U	256	lan-lan1
ff00::/8	::	U	256	lan-lantes1

Each item will be explained as follows:

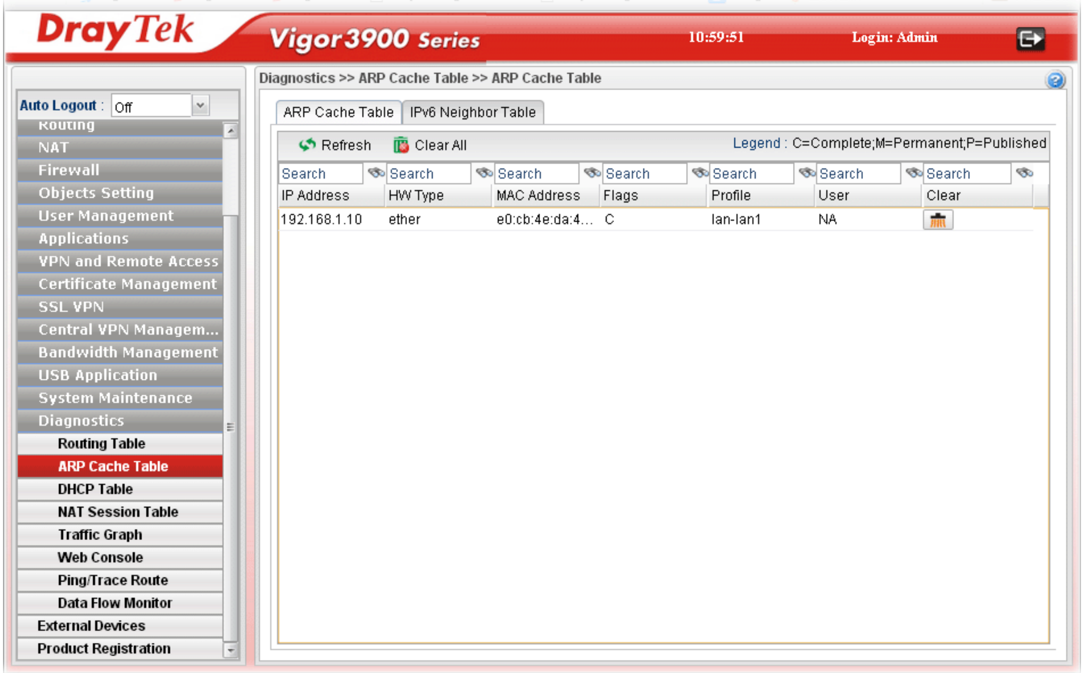
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> Routing Table >> IPv6 Routing Table Routing Table | IPv6 Routing Table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

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

4.16.2 ARP Cache Table

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

4.16.2.1 ARP Cache Table



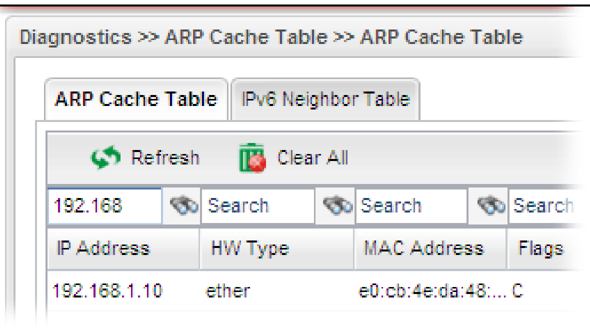
Diagnostics >> ARP Cache Table >> ARP Cache Table

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

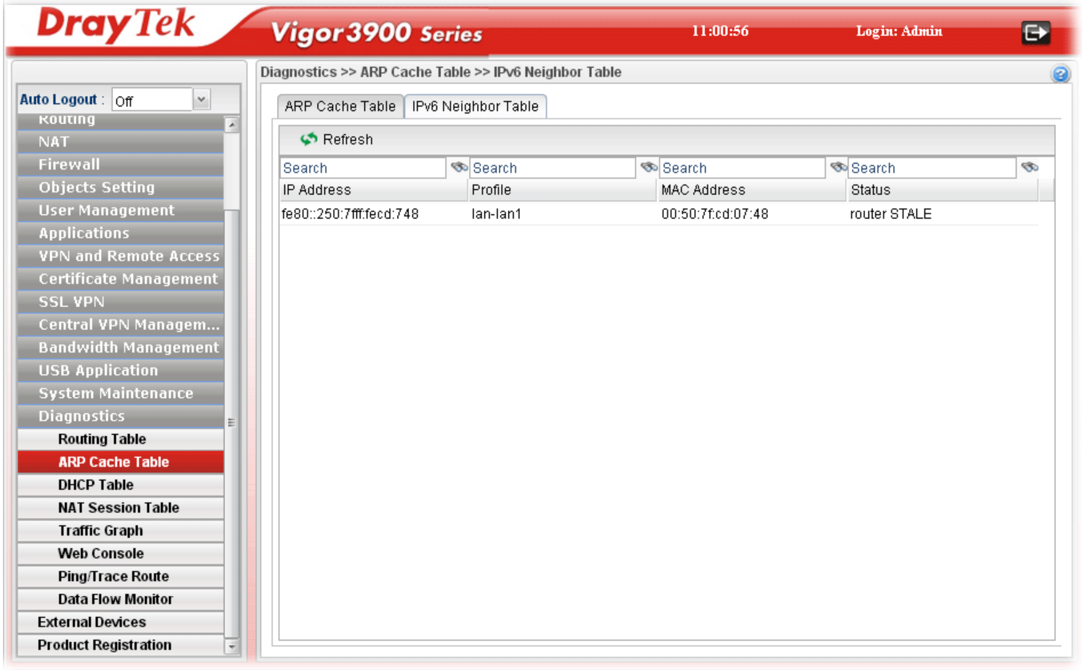
IP Address	HW Type	MAC Address	Flags	Profile	User	Clear
192.168.1.10	ether	e0:cb:4e:da:4...	C	lan-lan1	NA	

Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Clear All	Remove all of the information from this page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.

Item	Description
	 Diagnostics >> ARP Cache Table >> ARP Cache Table ARP Cache Table / IPv6 Neighbor Table Refresh / Clear All 192.168 / Search / Search / Search IP Address / HW Type / MAC Address / Flags 192.168.1.10 / ether / e0:cb:4e:da:48:... / C
IP Address	Display the IP address for different ARP cache.
HW type	Display the hardware type of the address from RFC 826.
MAC Address	Display the MAC address for different ARP cache.
Flags	C means complete entry. M means permanent entries. P means published entries.
Profile	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).
User	Display the identity of the user.
Clear	Delete the selected profile.

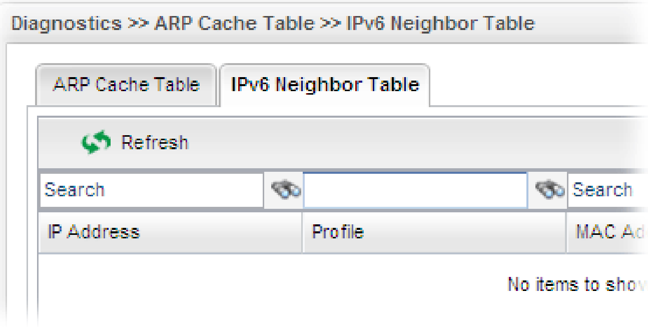
4.16.2.2 IPv6 Neighbor Table



Diagnostics >> ARP Cache Table >> IPv6 Neighbor Table

IP Address	Profile	MAC Address	Status
fe80::250:7fff:fecd:748	lan-lan1	00:50:7f:cd:07:48	router STALE

Each item will be explained as follows:

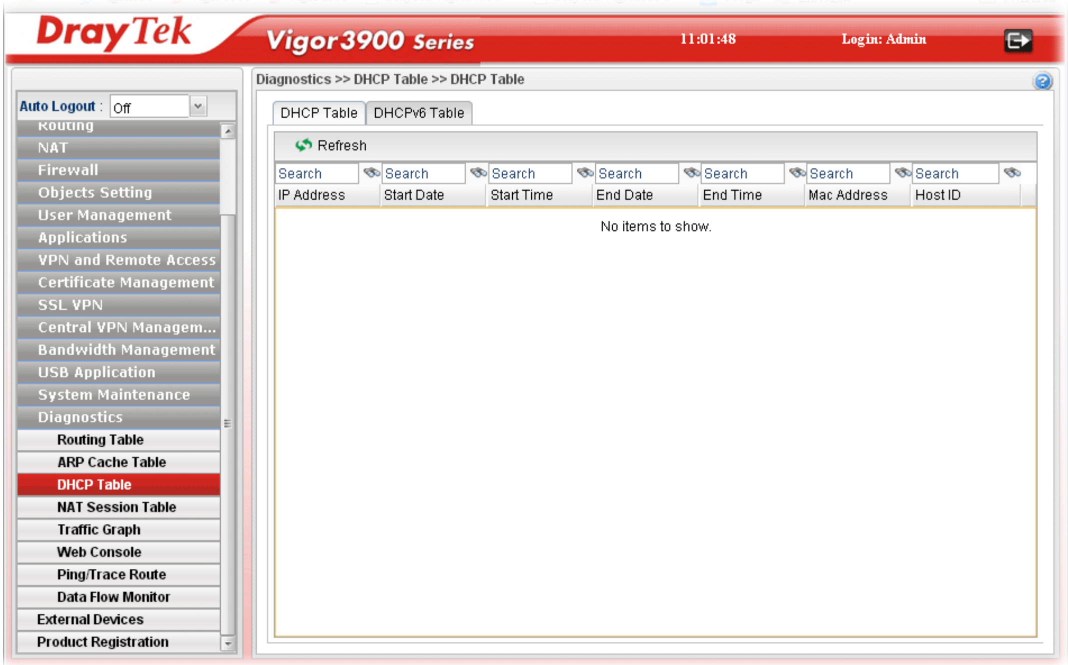
Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> ARP Cache Table >> IPv6 Neighbor Table ARP Cache Table IPv6 Neighbor Table Refresh Search Search IP Address Profile MAC Ad No items to sho
IP Address	Display the IPv6 address of the neighbor.
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.
Status	Display the status for such neighbor. **INCOMPLETE -** Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. **REACHABLE -** The neighbor is reachable recently (within tens of seconds ago). **STALE-**The neighbor is no longer to be reachable. Yet, until traffic is sent to the neighbor, no attempt should be made to verify its reachability. **DELAY -** The neighbor is no longer to be reachable, and the traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, delay sending probes for a short while in order to give upper layer protocols a chance to provide reachability confirmation. **PROBE -** The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

4.16.3 DHCP Table

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

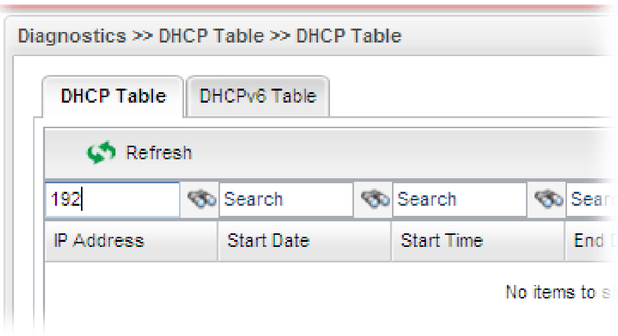
4.16.3.1 DHCP Table

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



No items to show.

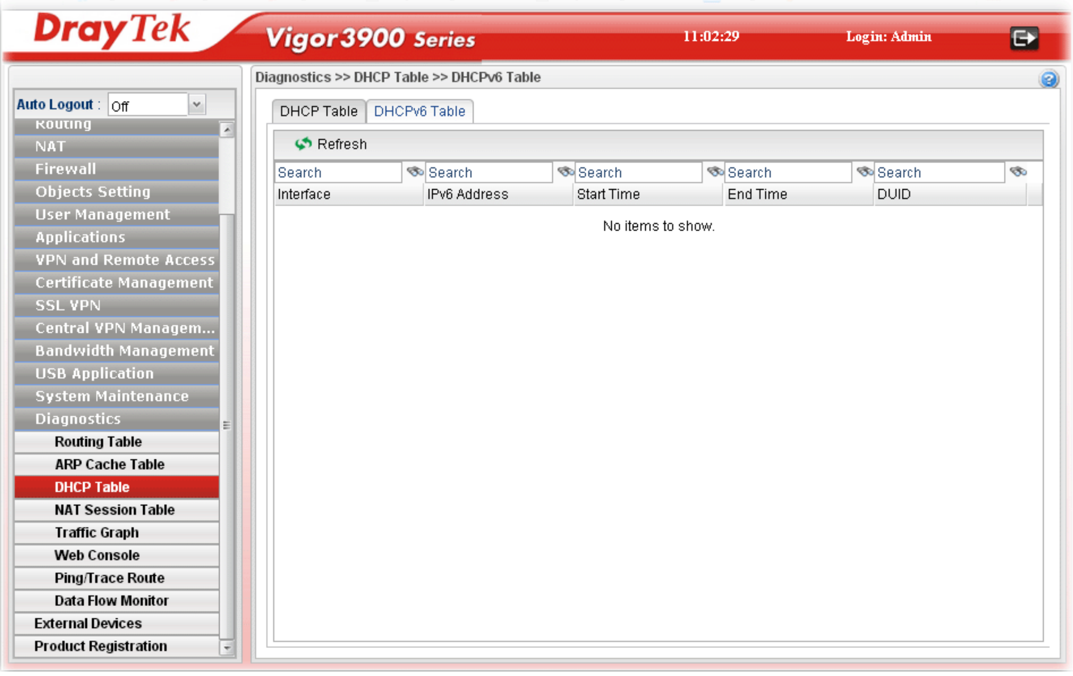
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> DHCP Table >> DHCP Table DHCP Table DHCPv6 Table Refresh 192 Search Search Sear IP Address Start Date Start Time End No items to s
IP Address	Display the IP address of the static DHCP server.
Start Date	Display the starting date that DHCP server is activated.
Start Time	Display the starting time that DHCP server is activated.
End Date	Display the end date that DHCP server is closed.

Item	Description
End Time	Display the end time that DHCP server is closed.
Mac Address	Display the MAC address of the static DHCP server.

4.16.3.2 DHCPv6 Table

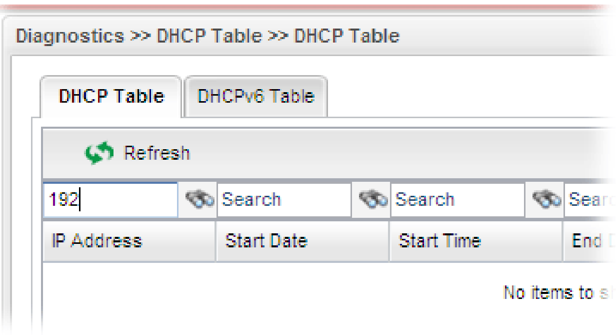
Click **DHCPv6 Table** to open the web page.



Interface	IPv6 Address	Start Time	End Time	DUID

No items to show.

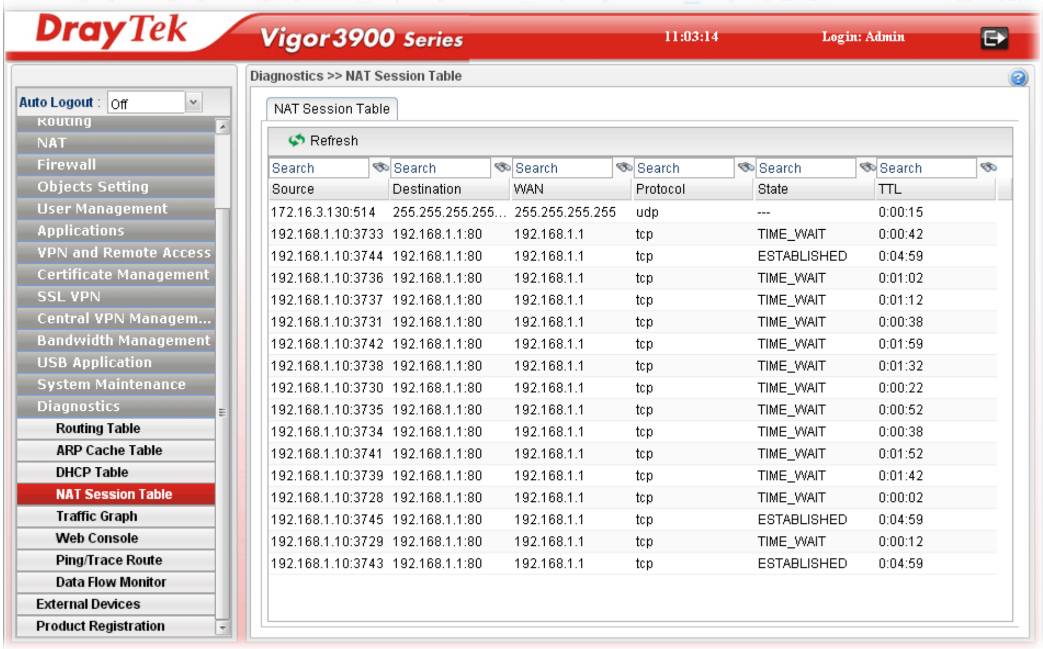
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> DHCP Table >> DHCP Table DHCP Table DHCPv6 Table Refresh 192 Search Search Sear IP Address Start Date Start Time End No items to s
Interface	Display the interface used by the DHCP server.
IPv6 Address	Display the IPv6 address of the static DHCP server.
Start Time	Display the starting time that DHCP server is activated.
End Time	Display the end time that DHCP server is closed.

Item	Description
DUID	Display the detailed information for DUID.

4.16.4 NAT Session Table

This table can display about 30000 sessions with 20 pages.



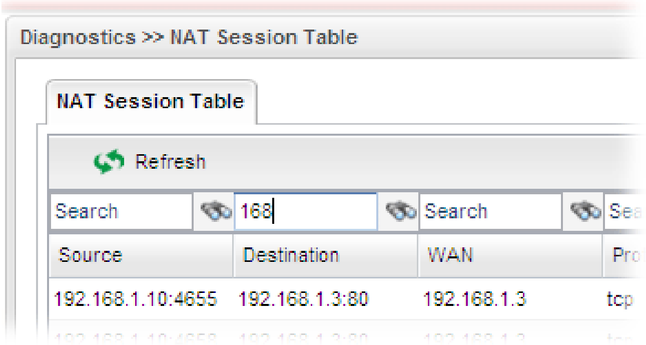
Diagnostics >> NAT Session Table

NAT Session Table

Refresh

Search	Search	Search	Search	Search	Search
Source	Destination	WAN	Protocol	State	TTL
172.16.3.130:514	255.255.255.255...	255.255.255.255	udp	---	0:00:15
192.168.1.10:3733	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:42
192.168.1.10:3744	192.168.1.1:80	192.168.1.1	tcp	ESTABLISHED	0:04:59
192.168.1.10:3736	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:02
192.168.1.10:3737	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:12
192.168.1.10:3731	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:38
192.168.1.10:3742	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:59
192.168.1.10:3738	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:32
192.168.1.10:3730	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:22
192.168.1.10:3735	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:52
192.168.1.10:3734	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:38
192.168.1.10:3741	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:52
192.168.1.10:3739	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:01:42
192.168.1.10:3728	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:02
192.168.1.10:3745	192.168.1.1:80	192.168.1.1	tcp	ESTABLISHED	0:04:59
192.168.1.10:3729	192.168.1.1:80	192.168.1.1	tcp	TIME_WAIT	0:00:12
192.168.1.10:3743	192.168.1.1:80	192.168.1.1	tcp	ESTABLISHED	0:04:59

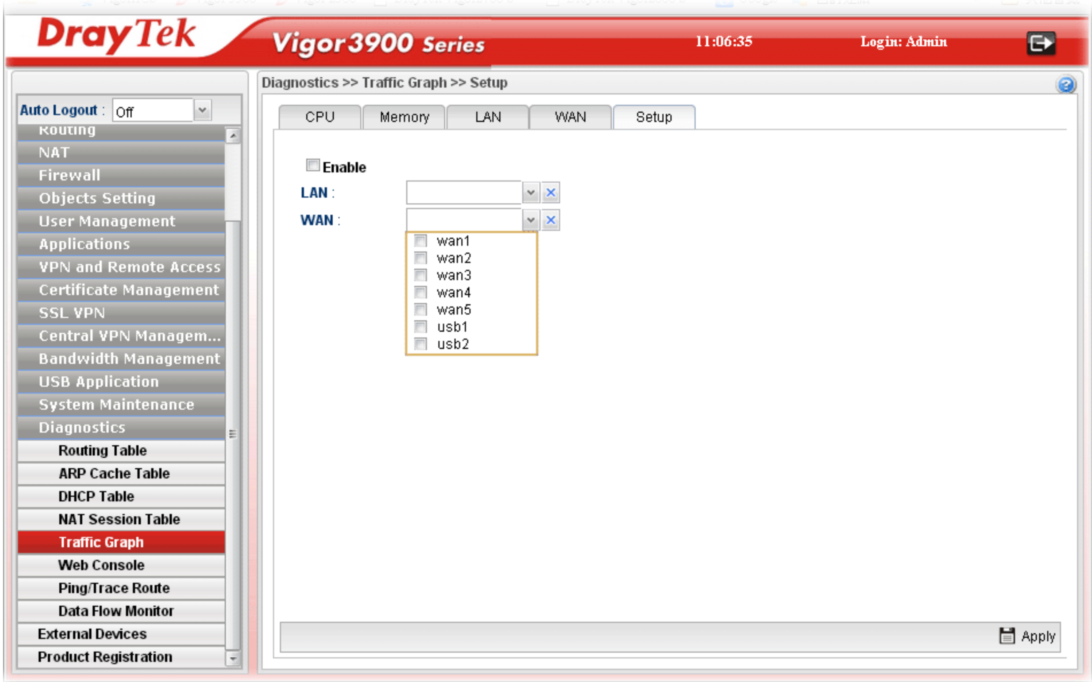
Each item will be explained as follows:

Item	Description
Refresh	Renew the web page.
Search	Move the mouse cursor onto the box of Search. Click the mouse button and type the keyword inside the box. The system will display the records relating to the keyword.  Diagnostics >> NAT Session Table NAT Session Table Refresh Search | 168 | Search | Se Source | Destination | WAN | Pro 192.168.1.10:4655 | 192.168.1.3:80 | 192.168.1.3 | tcp
Source	Display the source IP address and port of local PC.
Destination	Display the destination IP address and port of remote host.
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.

Item	Description
TTL	Display how long the conntrack entry has to live.

4.16.5 Traffic Graph

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



Diagnostics >> Traffic Graph >> Setup

□ Enable

LAN :

WAN :

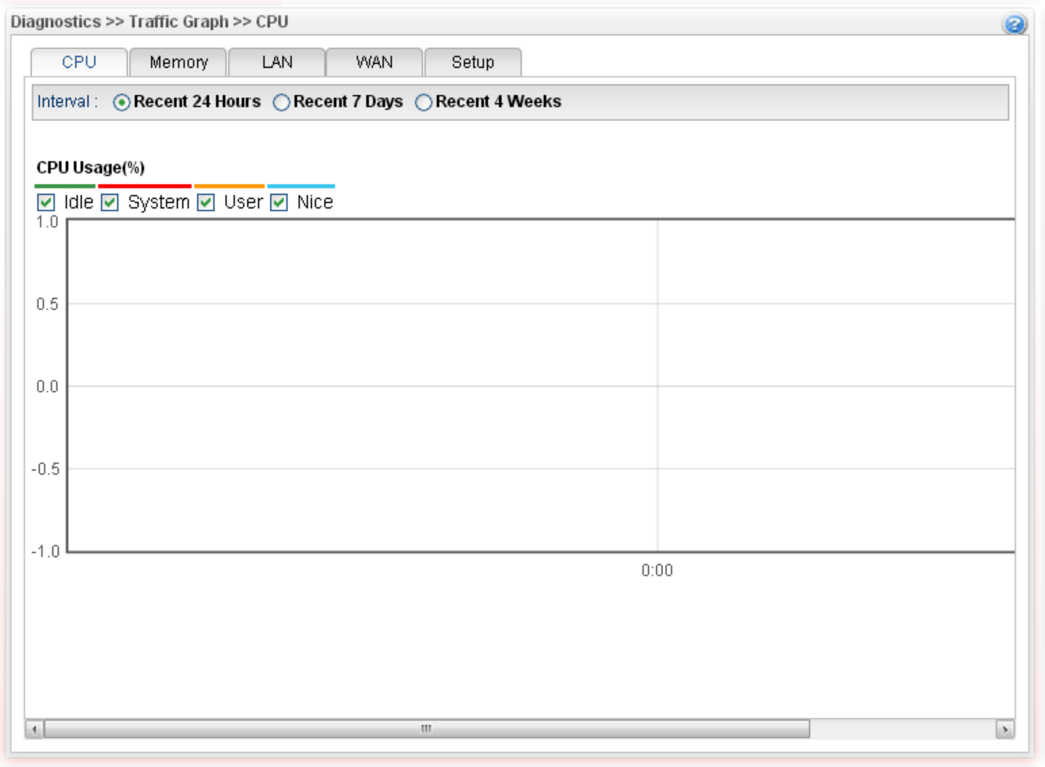
□ wan1
□ wan2
□ wan3
□ wan4
□ wan5
□ usb1
□ usb2

Each item will be explained as follows:

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

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

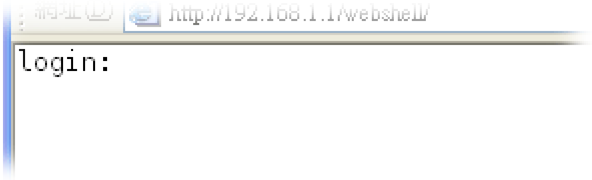
Below show a graphic for CPU:


Diagnostics >> Traffic Graph >> CPU
CPU
Memory
LAN
WAN
Setup
CPU Usage(%)
☑ Idle ☑ System ☑ User ☑ Nice
1.0
0.5
0.0
-0.5
-1.0
0:00

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

4.16.6 Web Console

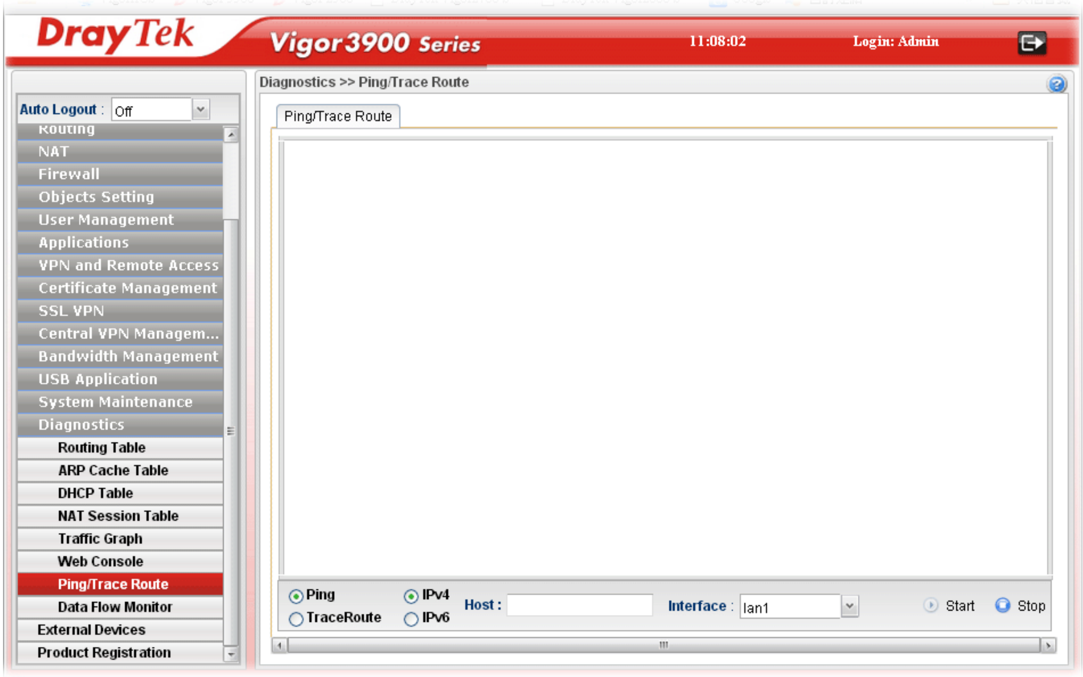
Click **Diagnostics** and click **Web Console** to pen the web page for typing commands used in console connection. A remote user can operate Vigor3900 from this web page without installing and opening other connection utility.



```
login:
```

4.16.7 Ping/Trace Route

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



Diagnostics >> Ping/Trace Route

Auto Logout : Off

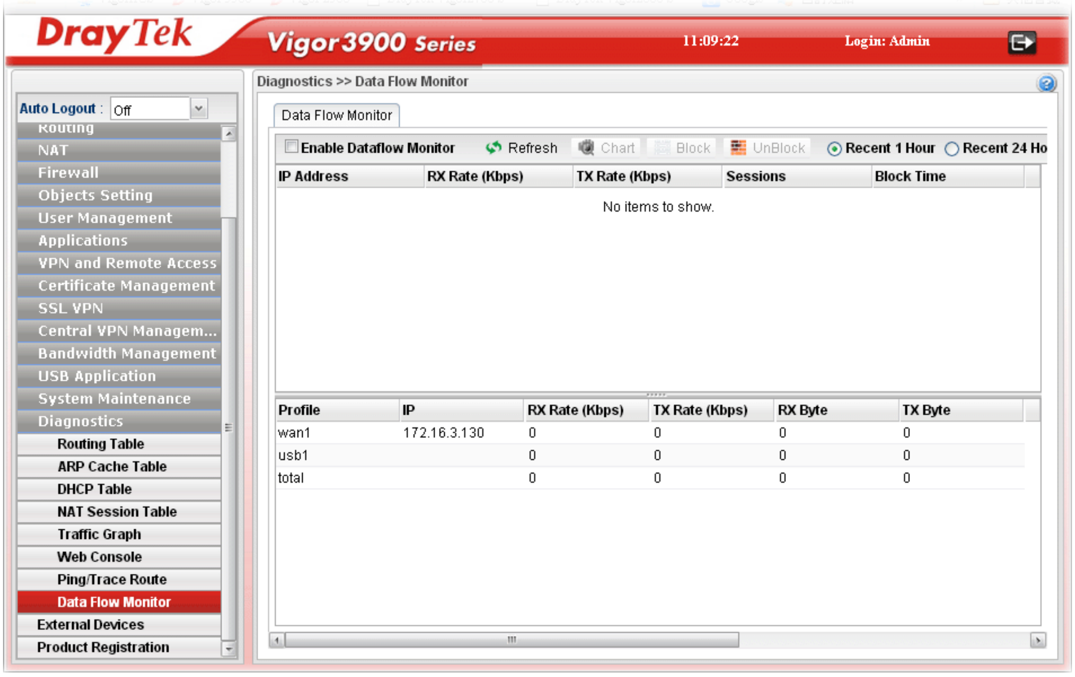
● Ping ○ TraceRoute ● IPv4 ○ IPv6 Host : Interface : lan1

Each item will be explained as follows:

Item	Description
Ping / TraceRoute	Click **Ping** to perform ping function. Click **TraceRoute** to invoke trace router function.
IPv4 / IPv6	Click IPv4 /IPv6 to determine the format of the IP address that you can type.
Host	Type the IP address of the host.
Interface	Choose one of the LAN or WAN profile to be applied by such function.
Start	Click it to start the action of Ping or TraceRoute.
Stop	Click it to terminate the action of Ping or TraceRoute.

4.16.8 Data Flow Monitor

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



DrayTek Vigor3900 Series 11:09:22 Login: Admin

Auto Logout : Off

Routing
NAT
Firewall
Objects Setting
User Management
Applications
VPN and Remote Access
Certificate Management
SSL VPN
Central VPN Managem...
Bandwidth Management
USB Application
System Maintenance
Diagnostics
Routing Table
ARP Cache Table
DHCP Table
NAT Session Table
Traffic Graph
Web Console
Ping/Trace Route
Data Flow Monitor
External Devices
Product Registration

Diagnostics >> Data Flow Monitor

Data Flow Monitor

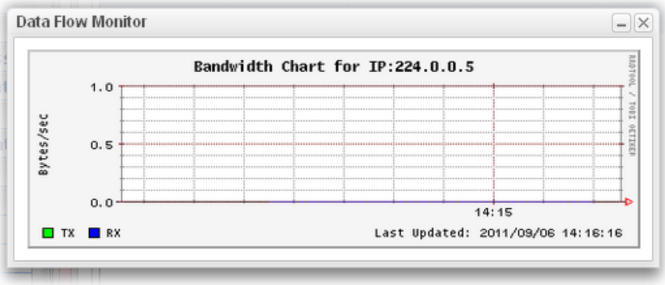
□ Enable Dataflow Monitor | Refresh | Chart | Block | UnBlock | ● Recent 1 Hour ○ Recent 24 Ho

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

No items to show.

Profile	IP	RX Rate (Kbps)	TX Rate (Kbps)	RX Byte	TX Byte
wan1	172.16.3.130	0	0	0	0
usb1		0	0	0	0
total		0	0	0	0

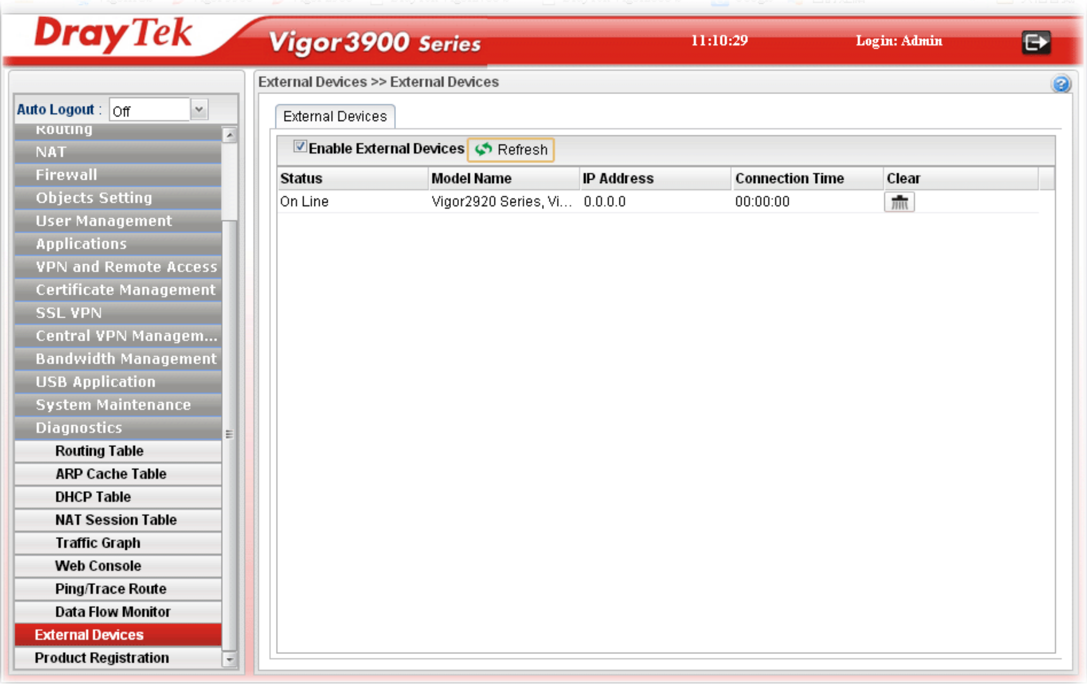
Each item will be explained as follows:

Item	Description
Enable Dataflow Monitor	Check this box to enable dataflow monitor performed by the router.
Refresh	Click it to renew the web page.
Chart	Click this button to illustrate data chart. Refer to the following figure as an example.  Data Flow Monitor Bandwidth Chart for IP:224.0.0.5 Bytes/sec 1.0 0.5 0.0 14:15 TX RX Last Updated: 2011/09/06 14:16:16
Block	Prevent the specified PC accessing into Internet within 5 minutes.
UnBlock	Allow the specified PC accessing into Internet within 5 minutes.
Recent 1 Hour/ Recent 24 Hours / Recent 7 Days	Display the records with 1 hour/24 hours/7 days recently.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh

	button is clicked.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Block Time	Display the time for the duration of the block.
Profile	Display the WAN interface.
IP	Display the IP address of the WAN interface.
RX Rate	Display the rate of data received.
TX Rate	Display the rate of data transmitted.
RX byte	Display the file size of data received.
TX byte	Display the file size of data transmitted.

4.17 External Devices

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



☑ Enable External Devices

Status	Model Name	IP Address	Connection Time	Clear
On Line	Vigor2920 Series, Vi...	0.0.0.0	00:00:00	🗑

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.

Item	Description
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.

4.18 Product Registration

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

Chapter 5: Trouble Shooting

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

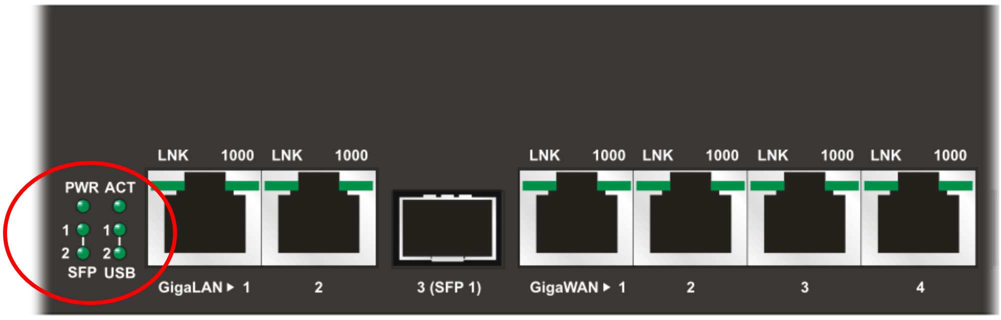
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

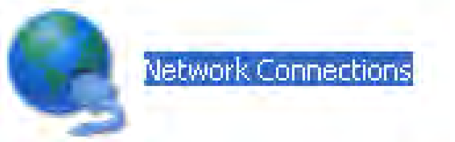
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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

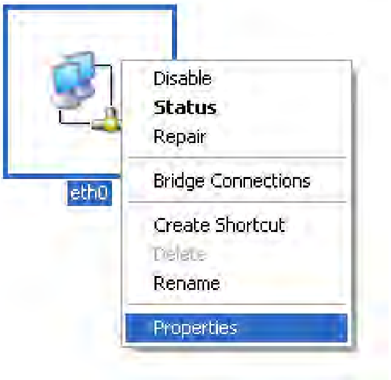
For Windows

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

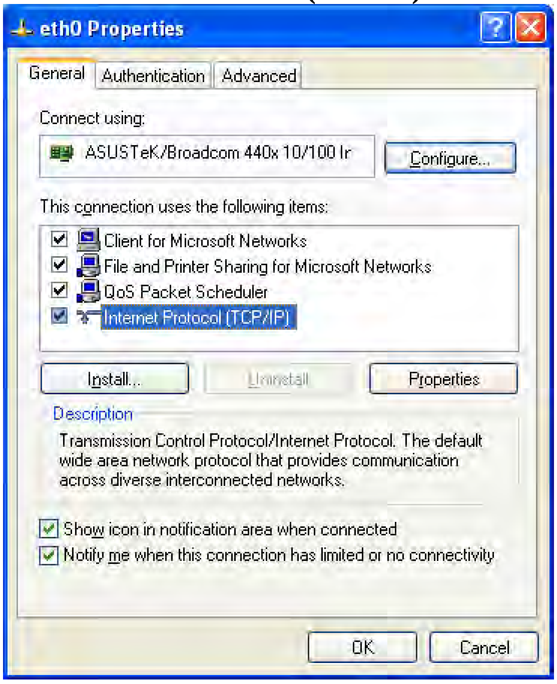
1. Go to **Control Panel** and then double-click on **Network Connections**.



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



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



eth0 Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

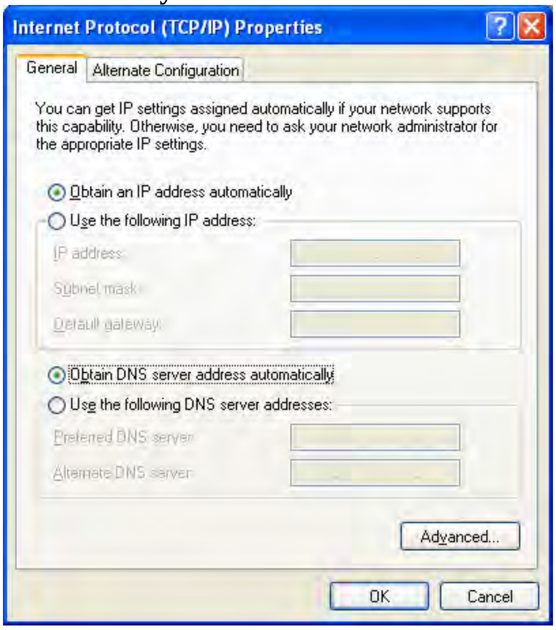
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

OK | Cancel

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



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

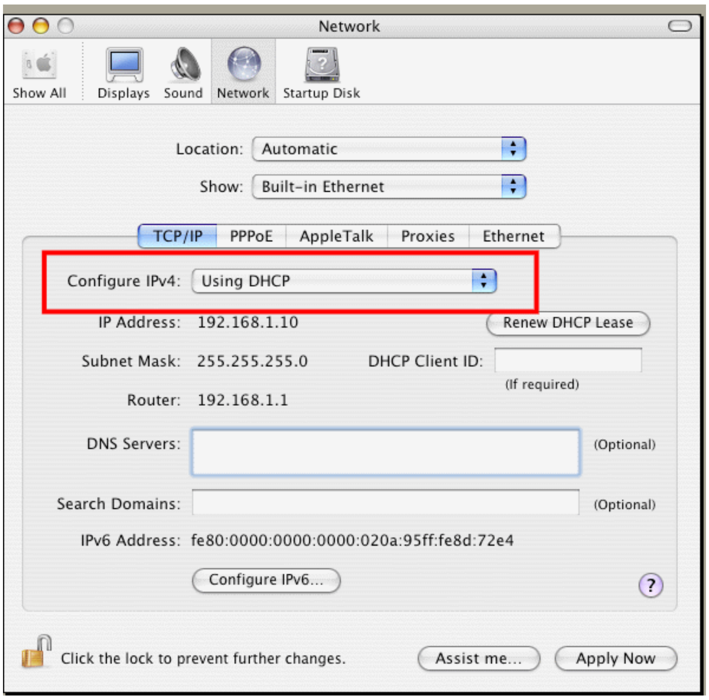
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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.



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

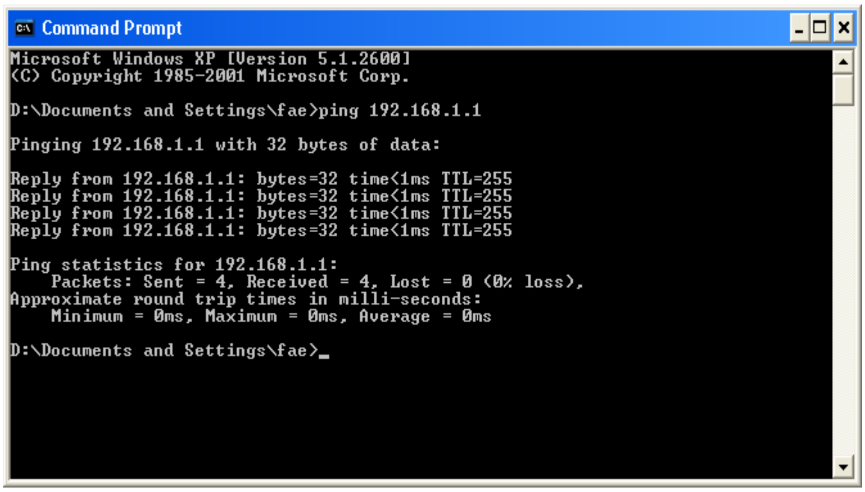
5.3 Pinging the Router from Your Computer

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.

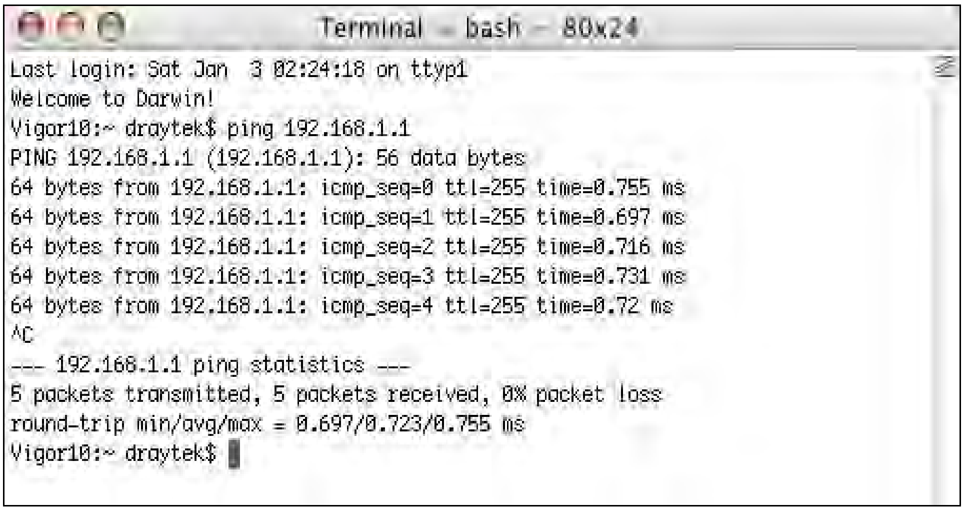


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.1:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

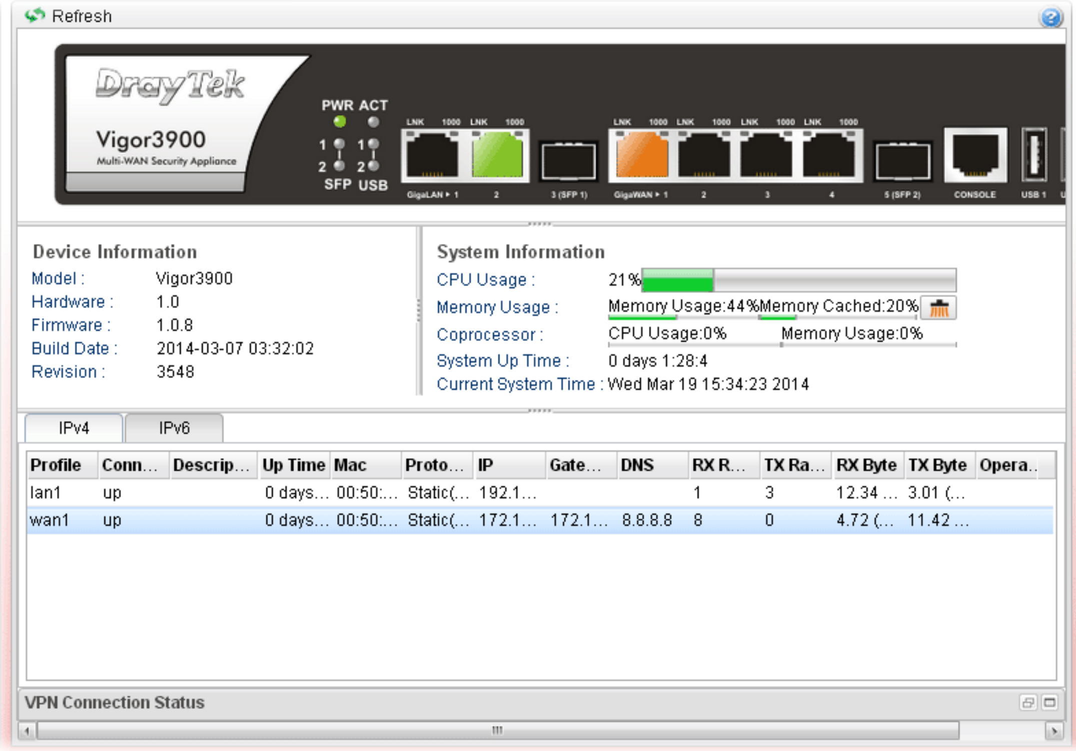
1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.



```
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

5.4 Checking If the ISP Settings are OK or Not

Open Online Status to check current network status. Be careful to check if the settings coming from your ISP have been typed correctly or not.



Device Information

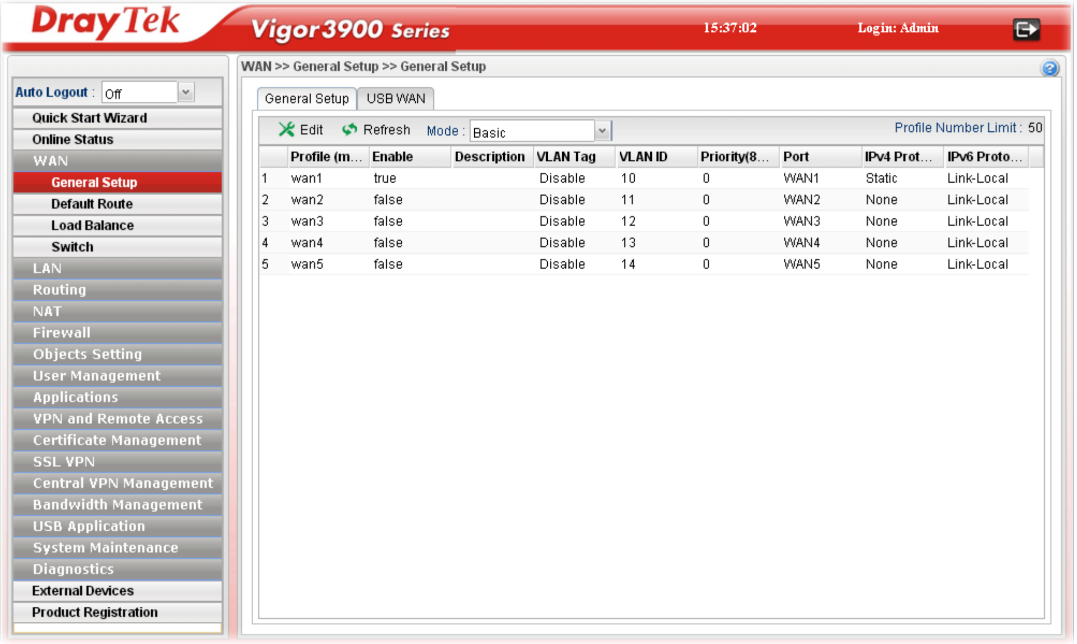
Model :	Vigor3900
Hardware :	1.0
Firmware :	1.0.8
Build Date :	2014-03-07 03:32:02
Revision :	3548

System Information

CPU Usage :	21%
Memory Usage :	Memory Usage:44%Memory Cached:20%
Coprocessor :	CPU Usage:0% Memory Usage:0%
System Up Time :	0 days 1:28:4
Current System Time :	Wed Mar 19 15:34:23 2014

Profile	Conn...	Descrip...	Up Time	Mac	Proto...	IP	Gate...	DNS	RX R...	TX Ra...	RX Byte	TX Byte	Opera...
lan1	up		0 days...	00:50:...	Static(...	192.1...			1	3	12.34 ...	3.01 (...	
wan1	up		0 days...	00:50:...	Static(...	172.1...	172.1...	8.8.8.8	8	0	4.72 (...	11.42 ...	

If there is something wrong with the configuration, please go to **WAN** page and choose **General Setup** again to modify the WAN connection.



WAN >> General Setup >> General Setup

Mode : Basic

Profile Number Limit : 50

	Profile (m...	Enable	Description	VLAN Tag	VLAN ID	Priority(8...	Port	IPv4 Prot...	IPv6 Proto...
1	wan1	true		Disable	10	0	WAN1	Static	Link-Local
2	wan2	false		Disable	11	0	WAN2	None	Link-Local
3	wan3	false		Disable	12	0	WAN3	None	Link-Local
4	wan4	false		Disable	13	0	WAN4	None	Link-Local
5	wan5	false		Disable	14	0	WAN5	None	Link-Local

5.5 Backing to Factory Default Setting If Necessary

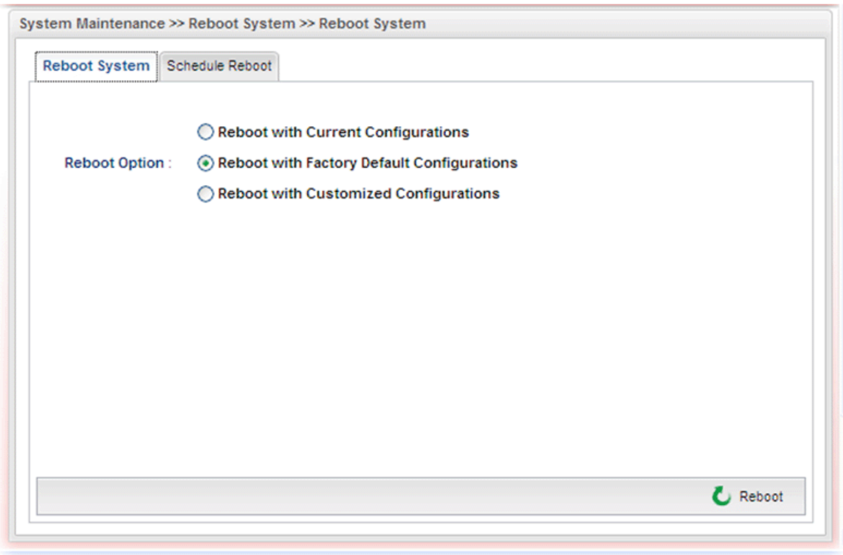
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of the factory default is null.

Software Reset

You can reset router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Reboot with Factory Default Configuration** and click **Reboot**. After few seconds, the router will return all the settings to the factory settings.

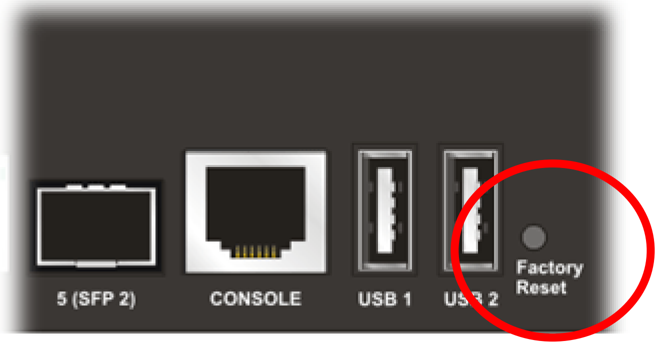


System Maintenance >> Reboot System >> Reboot System

Reboot Option : ○ Reboot with Current Configurations
● Reboot with Factory Default Configurations
○ Reboot with Customized Configurations

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**.

This page is left blank.

Appendix I Release Note

Firmware Version: 1.0.8

New Features

- Same WAN VLAN ID can be used in different WAN interfaces. (WAN >> General Setup Mode: Advance, Switch Mode: Double Tag)
- Support QoS for multiple WANs.
- Support SNMP v3.
- Support country block for Firewall.
- Support WCF white list.
- Support LAN DNS server.
- Support BGP routing protocol.
- Support SSL VPN tunnel mode (up to 20 tunnels).
- Support Web Portal and Hotspot (Guest profile) in User Management.
- Support PPTP acceleration for PPTP WAN/Remote Dial-in/LAN to LAN (125Mbps with MPPE, greater than 900Mbps without MPPE).
- Support QoS retag option.
- Support VPN dial-out failover if WAN disconnected.
- Support VPN LAN to LAN for overlap/duplicate subnets.
- Display the last UP/DOWN log of VPN profile.
- Add default policy for Firewall and default block policy can be applied.
- Add IPv6 firewall settings.
- Add DNS object.
- Add a remote capture telnet command (rc), for traffic monitor and wireshark remote capture.
- Add front panel and VPN status on the dashboard.

Improvement

Web User Interface Change

- Change the menu item “User Management>>General Setup” into “User Management>>Web Portal”.
- Move IP Routing from LAN to Static Route and rename as LAN/WAN Proxy ARP.
- Move Inter-LAN Route from LAN>>Static Route to LAN>>General Setup.
- Move status page to the first tab of each function menu.

Others

- Improved: Support RADIUS, LDAP, Local authentication in User Management.
- Improved: Support NAT option for IPsec LAN to LAN.
- Improved: Support LDAP profile in Firewall.
- Improved: Support ratio configuration for VPN Load Balancing.
- Improved: Port number setting for Access Control in WAN IP alias can be passed to LAN by default.
- Improved: Notification object can be recorded on Syslog through the configuration on Applications>>SMS/Mail Alert Service page.
- Improved: Support Local/RADIUS/LDAP authentication for PPTP/L2TP/PPPoE server at the same time.
- Improved: Change the priority of Inter-LAN route, that IP filter can do further control.
- Improved: Support connection failover for TR-069.
- Improved: Display router name in web page title.
- Improved: IPsec VPN dial-in connection with all WANs is supported in default.
- Improved: Support RFC3021.
- Improved: Combine IM/P2P/Protocol object to App Object for blocking more Apps.
- Improved: The number of Management Access Control List is increased up to 16.
- Improved: Support peer identity for IPsec RSA authentication.
- Improved: Support password encode option for configuration backup.
- Improved: Support more special characters in username for user profile.
- Improved: The number of SSL web proxy/VNC/RDP profile is increased up to 30.
- Improved: Support customized DDNS.
- Improved: Support acceleration of fragmented UDP packets (maximum 1628 bytes).
- Improved: Support DHCP option 95 (LDAP server), 161(FTP server), and 162 (File path) for DHCP server.
- Improved: Support more subnet DHCP servers in Bind IP to MAC.
- Improved: Support DHCP relay over LAN/Non-Direct-Connected LAN.
- Improved: Support DHCP relay settings for PPTP/L2TP/PPPoE.
- Improved: Support open port to the host in remote VPN network.
- Fixed: Default route cannot work well when two WAN IPs are in the same IP network.