

## Vigor3900 Multi-WAN Security Appliance

Dray Tel

Providing Productivity and Security for Small, Medium and Large Businesses

Your reliable networking solutions partner

# User's Guide



## Vigor3900 Multi-WAN Security Appliance User's Guide

Version: 1.71 Firmware Version: V1.0.7 (For future update, please visit DrayTek website) Date: 07/11/2013



## **Copyright Information**

Copyright Declarations	Copyright 2013 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	<ul> <li>The following trademarks are used in this document:</li> <li>Microsoft is a registered trademark of Microsoft Corp.</li> <li>Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.</li> <li>Apple and Mac OS are registered trademarks of Apple Inc.</li> <li>Other products may be trademarks or registered trademarks of their respective manufacturers.</li> </ul>

### Safety Instructions and Approval

Safety	• Read the installation guide thoroughly before you set up the router.								
Instructions	• 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.								
	• 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								
	• When you want to dispose of the router, please follow local regulations on								
Warranty									
	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								
	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.								
	<ul> <li>authorized and qualified personnel. Do not try to open or repair the router yourself.</li> <li>Do not place the router in a damp or humid place, e.g. a bathroom.</li> <li>The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.</li> <li>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.</li> <li>Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.</li> <li>Keep the package out of reach of children.</li> <li>When you want to dispose of the router, please follow local regulations on conservation of the environment.</li> <li>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 repair or replace met 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 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 register your Vigor router via http://www.draytek.com.</li> </ul>								
	http://www.draytek.com								



#### **European Community Declarations**

Manufacturer:	DrayTek Corp.
Address:	No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu County, Taiwan
	303
Product:	Vigor3900

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

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

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

#### **Regulatory Information**

Federal Communication Commission Interference Statement

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

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

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

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

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

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



### Table of Contents

Chapter 1: Preface	1
1.1 Web Configuration Buttons Explanation	2
1.2 LED Indicators and Connectors	2
1.3 Hardware Installation	5
1.3.1 Network Connection         1.3.2 Rack-Mounted Installation	
Chapter 2: Initialing Settings	7
2.1 Changing Password	7
2.2 Quick Start Wizard	9
2.2.1 Step 1 - Specifying the WAN Profile 2.2.2 Step 2 - Configuring the Selected Protocol	
2.3 Register Vigor Router	18
Chapter 3: Application and Tutorial	21
3.1 How to Configure Load Balance with Multi-WAN on Vigor3900?	21
3.2 How to Configure OSPF?	27
3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Ma	
3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server?	
3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router	41
3.6 How to Setup 50 WANs on Vigor3900	50
3.7 CVM Application - How to manage the CPE (router) through Vigor3900?	55
3.8 CVM Application - How to build the VPN between remote devices and Vigor3900?	60
3.9 CVM Application - How to upgrade CPE firmware through Vigor3900?	63
3.10 How to use High Availability for Vigor routers?	69
Chapter 4: Advanced Web Configuration	73
4.1 WAN Setup	73
4.1.1 General Setup	
4.1.2 Default Route 4.1.3 Load Balance	
4.1.4 Switch	
4.2 LAN	112
4.2.1 General Setup	
4.2.2 PPPoE Server 4.2.3 IP Routing	
4.2.4 Static Route	130
4.2.5 Switch 4.2.6 Bind IP to MAC	
4.2.6 Bind IP to MAC	
4.2.8 OSPF Configuration	148



4.3 NAT	149
4.3.1 Port Redirection	149
4.3.2 DMZ Host	
4.3.3 Address Mapping	
4.3.4 ALG	161
4.4 Firewall	162
4.4.1 Filter Setup	162
4.4.2 DoS Defense	
4.4.3 MAC Block	182
4.5 Objects Setting	184
4.5.1 IP Object	
4.5.2 IP Group	
4.5.3 Service Type Object	
4.5.4 Service Type Group	
4.5.5 Keyword Object 4.5.6 File Extension Object	
4.5.7 IM Object	
4.5.8 P2P Object	
4.5.9 Protocol Object	
4.5.10 Web Category Object	
4.5.11 QQ Object	
4.5.12 QQ Group 4.5.13 Time Object	
4.5.13 Time Object	
4.5.15 SMS Service Object	
4.5.16 Mail Service Object	
4.5.17 Notification Object	228
4.6 User Management	230
-	
4.6.1 General Setup 4.6.2 User Profile	231 234
4.6.1 General Setup 4.6.2 User Profile 4.6.3 User Group	231 234 239
<ul> <li>4.6.1 General Setup</li> <li>4.6.2 User Profile</li></ul>	231 234 239 241
<ul> <li>4.6.1 General Setup</li></ul>	231 234 239 241 242
<ul> <li>4.6.1 General Setup</li></ul>	231 234 239 241 242 246
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application .</li> <li>4.7.1 Dynamic DNS</li> </ul>	231 234 239 241 242 246 246
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile</li></ul>	231 234 249 241 242 246 251
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application.</li> <li>4.7.1 Dynamic DNS</li> <li>4.7.2 GVRP</li> <li>4.7.3 IGMP Proxy</li> </ul>	231 234 249 241 242 246 246 251 253
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application.</li> <li>4.7.1 Dynamic DNS.</li> <li>4.7.2 GVRP</li> <li>4.7.3 IGMP Proxy</li> <li>4.7.4 UPnP</li> </ul>	231 234 249 241 242 246 246 251 253 253
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application.</li> <li>4.7.1 Dynamic DNS</li> <li>4.7.2 GVRP</li> <li>4.7.3 IGMP Proxy</li> </ul>	231 234 249 241 242 246 246 251 253 253 256
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application.</li> <li>4.7.1 Dynamic DNS.</li> <li>4.7.2 GVRP</li> <li>4.7.3 IGMP Proxy.</li> <li>4.7.4 UPnP</li> <li>4.7.5 High Availability</li> </ul>	231 234 249 241 242 246 246 251 253 253 256 264
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li> <li>4.6.5 LDAP/Active Directory.</li> <li>4.7 Application.</li> <li>4.7.1 Dynamic DNS.</li> <li>4.7.2 GVRP</li> <li>4.7.3 IGMP Proxy.</li> <li>4.7.4 UPnP</li> <li>4.7.5 High Availability</li></ul>	231 234 249 241 242 246 246 251 253 253 256 264 265
<ul> <li>4.6.1 General Setup</li></ul>	231 234 249 241 242 246 251 253 253 256 264 265 270
<ul> <li>4.6.1 General Setup.</li> <li>4.6.2 User Profile.</li> <li>4.6.3 User Group.</li> <li>4.6.4 RADIUS</li></ul>	231 234 249 241 242 246 246 253 253 256 264 265 270 270
<ul> <li>4.6.1 General Setup</li></ul>	231 234 249 241 242 246 251 253 253 256 264 265 270 270 270 276
<ul> <li>4.6.1 General Setup</li></ul>	231 234 249 241 242 246 246 253 253 256 264 265 264 270 270 276 280
<ul> <li>4.6.1 General Setup</li></ul>	231 234 242 242 242 246 253 253 256 264 265 264 265 270 270 270 276 280 281 284
<ul> <li>4.6.1 General Setup</li></ul>	231 234 242 242 246 246 253 253 256 264 265 264 265 270 270 270 276 280 281 284 285
<ul> <li>4.6.1 General Setup</li></ul>	231 234 242 242 246 246 253 253 253 256 264 265 270 270 270 270 270 280 281 284 285 296
4.6.1 General Setup	231 234 242 242 242 246 246 253 253 256 264 265 264 265 270 270 270 270 270 280 281 284 285 296 303
<ul> <li>4.6.1 General Setup</li></ul>	231 234 239 241 242 246 251 253 253 256 264 265 270 270 270 270 270 270 270 280 281 284 285 296 303 304
4.6.1 General Setup	231 234 249 242 246 246 251 253 253 256 264 265 264 265 270 270 270 270 270 281 284 285 296 303 304 305

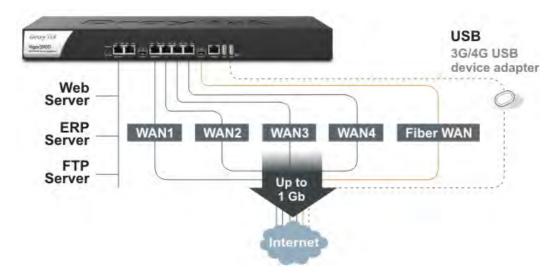


	4.9.3 Remote Certificate	311
	4.10 SSL VPN	312
	4.10.1 SSL Web Proxy	312
	4.10.2 SSL Application	
	4.10.3 Online User Status	
	4.11 Central VPN Management	
	4.11.1 General Setup	
	4.11.2 CPE Management 4.11.3 Log/Alert	
	4.12 Bandwidth Management	
	4.12.1 Quality of Service	
	4.12.2 QoS Rule	
	4.12.3 Sessions Limit	341
	4.12.4 Bandwidth Limit	344
	4.13 USB Application	348
	4.13.1 Temperature Sensor	348
	4.14 System Maintenance	350
	4.14.1 TR-069	
	4.14.2 Administrator Password	
	4.14.3 Configuration Backup	
	4.14.4 Syslog / Mail Alert 4.14.5 Time and Date	
	4.14.6 Access Control.	
	4.14.7 SNMP Setup	
	4.14.8 Reboot System	
	4.14.9 Firmware Upgrade	
	4.15 Diagnostics	363
	4.15.1 Routing Table	
	4.15.2 ARP Cache Table	
	4.15.3 DHCP Table	
	4.15.4 NAT Session Table 4.15.5 Traffic Graph	
	4.15.6 Web Console	
	4.15.7 Ping/Trace Route	
	4.15.8 Data Flow Monitor	
	4.16 External Devices	377
	4.17 Product Registration	378
Chap	oter 5: Trouble Shooting	379
	5.1 Checking If the Hardware Status Is OK or Not	379
	5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	380
	5.3 Pinging the Router from Your Computer	382
	5.4 Checking If the ISP Settings are OK or Not	383
	5.5 Backing to Factory Default Setting If Necessary	384
	5.6 Contacting Your Dealer	385

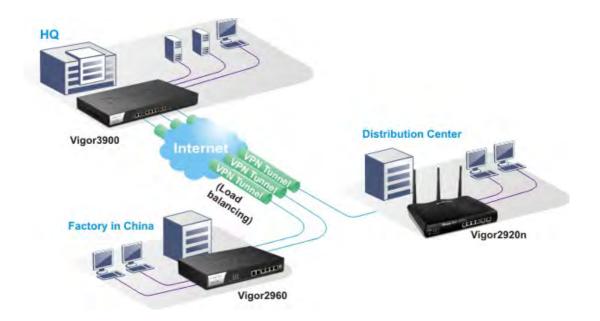


## **Chapter 1: Preface**

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



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



#### **1.1 Web Configuration Buttons Explanation**

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.
<b>Note:</b> For the ot explanation.	her buttons shown on the web pages, please refer to Chapter 4 for detailed

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

#### **1.2 LED Indicators and Connectors**

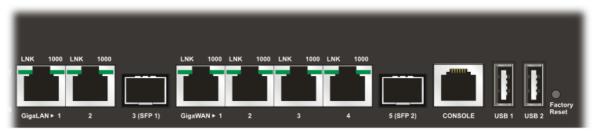
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly.

### **Description for LED**

	LNK	1000	LNK	1000		LNK	1000	LNK	1000	LNK	1000	LNK	1000
PWR ACT								Ľ					
SFP USB	GigaLA	N► 1	2	2	3 (SFP 1)	GigaW	AN ► 1	2	2	3	3		4

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.
	LNK	On	The Ethernet link is established on corresponding port.
GigaLAN1		Blinking	The data transmission is done through the corresponding port.
/LAN 2)		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.
	LNK	On	The Ethernet link is established.
Giga WAN1/2/3/4		Blinking	The data transmission is done through the corresponding port.
WIN(1/2/3/1		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 <b>ACT</b> LED begins to blink, release the button. Then the router will restart with the factory default configuration.
	Connecter for a power cord. ON/OFF - Power switch.

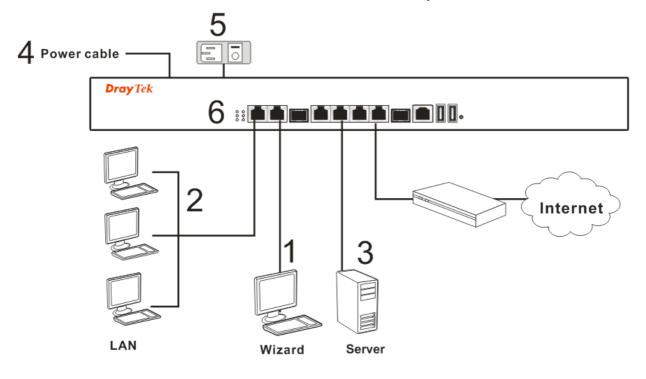
### **1.3 Hardware Installation**

#### **1.3.1 Network Connection**

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

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

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

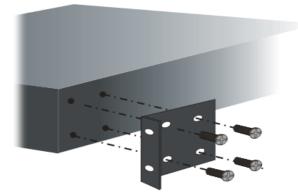


#### **1.3.2 Rack-Mounted Installation**

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



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



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



#### **Desktop Type Installation**

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



## **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.

<b>Dray</b> Tel	k Vi	gor3900 s	eries
Login			
lleese	admin		
User :	admin		
Password :			
	English	<ul> <li>Login</li> </ul>	

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

<b>Dray</b> Tek		Vigor 3900 Series						11:58:45			Login: Admin				
	🖨 Re	fresh													
uto Logout : Off 🛛 👻	Dev	ice l	Inform	ation	n			Syste	m Inform	atior	n				
Quick Start Wizard	Model			Vigor3	8900			CPU Us	age :	20%					
Online Status	Hardv			1.0				Memory	Usage :	Mem	ory Usag	e:41%	Memory	y Cached:1	6%
WAN	Firmw Build D			1.0.7_	RC12 08-27 15:	22-26		Coproc	essor :	CPU	Usage:0	%	Men	nory Usage	
LAN	Revisi			2013-0	00-27 13.	22.30			Up Time :	0 da	vs 0:10:4	5		-	
NAT									System Time				1		
Firewall	IF	v4		IPv6											
Objects Setting															
User Management			onnec D	escrij	•		Protoc		Gatewa D				-	TX byte	Operatio
Applications	lan1	up						192.1					228.7		
VPN and Remote Access	lantest			ist f				0.0.0.0			-	0	-	0	
Certificate Management	wan2	up			0 day	00:50:	Static(	. 172.1	172.1 8.8	3.8.8	11406	2396	131.2	22.28	
SSL VPN															
Central VPN Management															
Bandwidth Management															
USB Application															
System Maintenance															
Diagnostics															
External Devices															
Product Registration															

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

tem Maintenance >> Ad	ministrator Password		
Administrator Passwore	d		
		1	
Original Password :	•••••		
New Password :	•••••		
Confirm Password :	•••••		
			Apply

- 5. Enter the login password (admin) on the field of **Original Password.** Type a new one in the field of **New Password** and retype it on the field of **Confirm Password**. Then click **Apply** to continue.
- 6. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this router.



#### 2.2 Quick Start Wizard

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

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

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

#### 2.2.1 Step 1 - Specifying the WAN Profile

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

Quick Start Wizard		
Step 1 St	ep 2	
Profile :	wan1	<b>~</b>
IPv4 Protocol :	Static	*
		In Previous Next Trinish Strange
L		

Available settings are explained as follows:

Item	Description		
Profile	Use the drop down list to choose one WAN profile.		
	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			
	IP address to the V	d, you can manually assign a stati WAN interface and complete the applying the settings.		
	<b>DHCP</b> - It allows a user to	o obtain an IP address automatical		
	<b>DHCP</b> mode, the assign a dynamic automatically. It is any setting. (Host	ver on the Internet. If you choose DHCP server of your ISP will IP address for Vigor3900 s not necessary for you to assign Name and Domain Name are		
	required for some			
	DSL modem with service provider w and authentication <b>PPTP</b> as the proto	er get the IP group information by PPTP service from ISP. Your will give you user name, password n mode for a PPTP setting. Click pcol. Type in all the information vides for this protocol.		
	Tunneling Protoco this router. Next, e	you <b>PPTP</b> (Point-to-Point ol) mode, please select <b>PPTP</b> for enter the required information ISP on the web page.		
	<b>PPPoE</b> - PPPoE stands for	r Point-to-Point Protocol over		
	Ethernet. It relies PPP and Ethernet. Ethernet to the Int medium, such as a	s on two widely accepted standard It connects users through an ernet with a common broadband a single DSL line, wireless device All the users over the Ethernet can		
	local users can sha accessing the Inter	most of DSL modem users. All are one PPPoE connection for rnet. Your service provider will mation about user name, password mode.		
	Protocol over Ethe <b>PPPoE</b> for this ro	les you the <b>PPPoE</b> (Point-to-Point ernet) connection, please select uter to get the following page. <b>ne</b> and <b>password</b> provided by you		

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

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

#### 2.2.2 Step 2 - Configuring the Selected Protocol

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

Quick Start Wizard	
Step 1 Step 2	
IP Address :	0.0.0
Subnet Mask :	255.255.255.0 🗸
Gateway IP Address :	
	🏠 Add 💾 Save
	DNS Server IP Address

#### If Static is selected

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

k Start Wizard	
Step 1 Step 2	
IP Address :	0 . 0 . 0 . 0
Subnet Mask :	255.255.255.0 🗸
Gateway IP Address :	(Optional)
	🕼 Add 🗎 Save
	DNS Server IP Address
DNS Server IP Address :	No items to show.
	🕥 Previous ា Next 📑 Finish 🔇 Can

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		
Autress	one by one.	aressi rype are in address on	the ung cones
		dd 💾 Save	
	DNS S	erver IP Address	
	DNS Server IP Address : 168	95 . 1 . 1	Î
	<b>Save</b> – After finish to save the setting of	ed the IP address configuration onto the router.	on, click Save
	🚯 Add 💾 Save		
	DNS Server IP Addres	S	
	168.95.1.1		â
	$\mathbf{\hat{III}}$ – Click the ico	n to remove the selected entry	<i>.</i>
Previous	Click it to return to	previous setting page.	
Finish	Click it to finish th	e configuration.	
Cancel	Click it to discard t	he settings configured in this	page.

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

#### If DHCP is selected

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

Step 1 Step 2	-
Host Name : (Optional)	
🔊 Previous 🛋 Next 📑 Finish 🔇 Cancel	

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 Wiza	rd					
Step 1	Step 2					
Username : Password :		]				
			🔇 Previous	Next	Finish	🔇 Cancel

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.

Quick Start Wizard			
Step 1 Step 2			
PPTP Over :	Static v		
Server Address :	0.0.0.0		
Username :			
Password :			
IP Address :	0 . 0 . 0 . 0		
Subnet Mask :	255.255.255.0 🗸		
Gateway IP Address :			
	🕼 Add 🗎 Save		
	DNS Server IP Address		
DNS Server IP Address	No items to show.		
	Mu Previnus 🗈	Next 📙 Finish	Cancel
			U Ganoor

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. <b>Please contact your ISP before you want to use this</b> <b>function.</b>
	Static 🗸
	Static
	DHCP
	Static – specify the IP address.
	<b>DHCP</b> - 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
	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
	$\mathbf{I}$ – 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.

Quick Start Wizard	
Step 1	Step 2
Host Name :	vigor2960 (Optional)
	Saving Wizard Configuration
	🔄 Previous 🔊 Next 📑 Finish 😵 Cancel

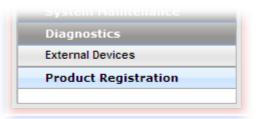
When the following screen appears, it means you have finished the Quick Start Wizard configuration.

Note	٩	ĸ
•	Wizard Setting Complete	
	ОК	

### 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 <b>x x h d d</b>
lf y	you cannot read the word, <u>click here</u>
	Forgotten password
Don't have a	MyVigor Account ? <u>Create an account now</u>
Become the MyVigo	or 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**.

<b>Dray</b> Tek				М
i Home				Searc
<ul> <li>About Us</li> <li>Product</li> <li>My Information</li> <li>VigorACS SI</li> <li>Vigor Series</li> </ul>	My Information Welcome, james Last Login Time : Last Login From : Current Login Tim Current Login From Your Device List	_ <mark>fae</mark> 2011-08-24 09:3 123.110.144.22 e : 2011-08-24 2	0 :3:01:15 84	Add
<ul> <li>Management</li> <li>Product</li> <li>Registration</li> <li>Customer Survey</li> </ul>	Serial Number / Host ID 104001703857 200807100001 200911030001	Device Name Vigor2710 VigorPro5300 ryan	Model Vigor2710 VigorPro5300 VigorPro5300	Note - -

**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**.

	iytek.com/nomePage/main.php				
<b>Dray</b> Tek	(			My	∕igo
i Home				Search	G
D About Us	My Product		Search for t	his site	GO
My Information	Registration Device				
VigorACS SI	Serial number : Nickname : *	20110822143	20301	)	
🗣 Vigor Series 🌻 Management	Registration Date : *	vigor3900 08-24-2011			
Product Registration	Usage : Product Rating :	– Select –	Your opinion so	farl	
🌡 Customer Survey	No. of Employees :	– Select –	( In total within yo	•	
	Supplier :		(Where	e you bought it from )	
	Date of Purchase : Internet Connection : *		( mm-d	d-уууу )	
	Cable	ADSL	VDSL	🗌 Fiber	
	🗖 3G	Wimax	🗌 LTE		
Copyrights © DrayTek Corp.				Cancel	bmit

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.

OK
----

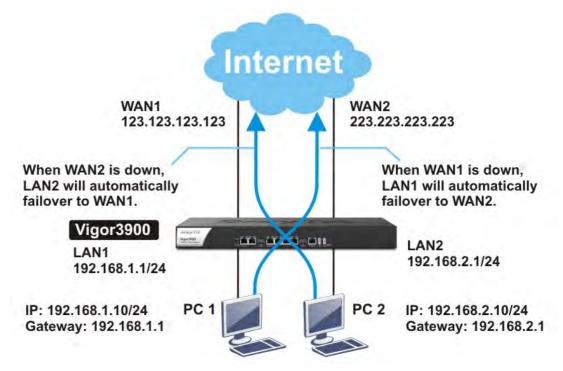
6 Take a look at the page of My Information, the new added Vigor3900 is listed under **Your Device List**.

<b>Dray</b> Tek		MyVig		
E Home			Se	arch G(
	My Information			
D About Us Product My Information	Welcome, <mark>draytekfae</mark> Last Login Time : 2011-08-24 Last Login From : 123.110.14 Current Login Time : 2011-08 Current Login From : 114.37.1	4.220 24 23:01:15		
VigorACS SI Vigor Series	, i i i i i i i i i i i i i i i i i i i	42.184	RowNo : 5 💌 Pa	igeNo : 🛛 💌
Uigor Series	Your Device List	42.184	RowNo : 5 💌 Pa	ogeNo : 2 💌
Vigor Series	, i i i i i i i i i i i i i i i i i i i	42.184 Device Name	RowNo : 5 💌 Pa	ngeNo : 2 💌 Note
Vigor Series Management	Your Device List			
Vigor Series Management	Your Device List	Device Name	Model	
Vigor Series Management	Your Device List Serial Number / Host ID <u>20100707144801</u>	Device Name Vigor3300V	Model Vigor3300	
Vigor Series	Your Device List Serial Number / Host ID 20100707144801 20100708105301	Device Name Vigor3300V Vigor2820	Model Vigor3300 Vigor2820	

## 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).

<b>Dray</b> Tek	Vigor 3900 s	ieries	16:15:	42 L	ogin: Admin 🗧
	LAN >> General Setup >> (	General Setup			
Auto Logout : Off 🛛 🗸	General Setup DHCP	Relay RADVD DHCPv6			
Quick Start Wizard					Des file Mussik and Justika
Online Status	🕼 Add 🔀 Edit	🔟 Delete 🛭 Ϛ Refresh			Profile Number Limit :
WAN	Profile (n Enable	Descripti VLANID Priority	IPv4 Prot(IP Address	Subnet Mask	DHCP Ser IPv6 Proto
LAN					
General Setup					
PPPoE Server					
IP Routing					
Static Route					
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Acces:					
Certificate Management					
SSL VPN					
Central VPN Manageme					
Bandwidth Managemen					
USB Application					
System Maintenance					
Diagnostics					

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 :		
	🕼 Add  Save	Profile Number Limit : 16
	DNS	
DNS :	No items to show.	
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).

lan 2 (Optional)	
(Optional)	
11	
0 🗸	
Enable      Disable	
00 :50 :7f :7f :fc :e8	
static	
NAT	
192 168 2 1	
255.255.255.0/24 👻	
Enable      Disable	
192 168 1 1	
🕼 Add 🛗 Save	Profile Number Limit : 16
DNS	
No items to show.	
(Optional)	
	0
	00       :50       :7f       :fc       :e8         static       NAT       ✓         192       .168       .2       .1         255.255.255.0/24       ✓       ✓         ● Enable ● Disable       192       .168       1         192       .168       .1       .1         .       .       .       .       .         MAT       ✓       .       .       .         .       .       .       .       .       .         .       .       .       .       .       .       .         .       .       .       .       .       .       .       .         .<

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

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



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

ol				-
Profile :	WAN1WAN2			
Mode :	Load_Balance 👻			
	🕼 Add   Save			Profile Number Limit : 1
	Interface		Weight	
Interface :	wan1	~	1	Î
				🛗 Apply 🛛 Qancel

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

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

Pool R	ule Inbound Load Balar	nce		
🕼 Add 🛛 🗶 B	Edit 🗻 Delete 🛭 🐼 Refri	esh		Profile Number Limit : 1
rofile	Mode	Interface	Primary Profile	Backup Profile
/AN1WAN2	Load_Balance	wan1 1		

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

Dray Tek	Vigor 3900 Series	16:27:57	Login: Admin 🕞
	WAN >> Load Batance >> Rule		
uto Logout Shim e	Pool Rule Incound Load Badmine		
Quick Start Wizard			Profile Number
Online Status	🖏 Add 🔆 Edit 🛄 Delete 🗢 Refresh 💣 Alove Up 🤌 Move Down 📢 Rename		Australia Manuset
WAN	Profile Enable Protoci Addres Source Source Destina Destina Source IP Address	Destination IP Address	Destina Destina Load B. Auto Pa
General Setup	No nems to show		
Default Route			
Load Balance			
Switch			
LAH			
HAT			
(Include			
Objects Setting			
User Management			
Applications			
VPN and Remote Access			
Certificate Management			
SSL VIN			
Central VPN Management			
Bandwelth Management			
USB Application			
System Maintenance			
Elagitostics			
External Devices			
Product Registration			
	(4)		1 10

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**;



×
~
*
~
168 . 1 . 0 📠 (Optional
5.255.0/24 💌 (Optional)
5.255.0/24 🗸 (Optional)
<ul> <li>(Must have value)</li> </ul>
ble 🔿 Disable
al

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

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.

ule2 LL ubnet 92 _ 168 _ 55.255.255.0/2	2 24 2	0 🚠 (Opt	tion
ubnet 92 <sub>.</sub> 168 .	2.	0 🟦 (Opt	tion
ubnet 92 <sub>.</sub> 168 .	2.	0 🟦 (Opt	tion
92 <sub>.</sub> 168.	2.	0 📠 (Opt	tion
	· ·		tion
55.255.255.0/2	24 🗸	(Optional)	
		(Opt	tion
55.255.255.0/2	24 👻	(Optional)	
an2	~	(Must have value	e)
)Enable 🔿 🛛	Disable	_	
) Enable 💿 🛛	)isable		
	an2 )Enable ()[	an2 v	an 2 v (Must have value Enable ODisable

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



	Pool	Rule	e In	bound Load Balanc
	🚯 Add	🔀 Edit	D D	elete 🛛 🗳 Refres
	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 🗸	Default Route	
Quick Start Wizard		
Online Status	WAN Profile/Loadbalance Pool Name	WAN1WAN2
WAN		wan1
General Setup	Auto Failover to Active WANs :	wan2 wan3
Default Route		wan4 WAN1WAN2
Load Balance		
Switch		
LAN		

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

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

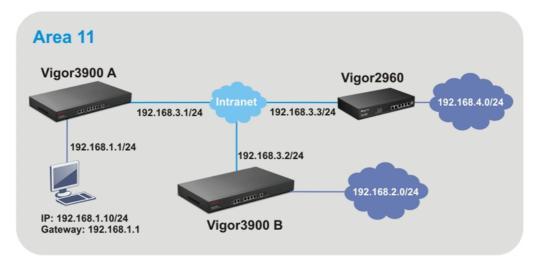
#### 3.2 How to Configure OSPF?

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

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

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

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



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

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



#### Configuration for Vigor3900 A,

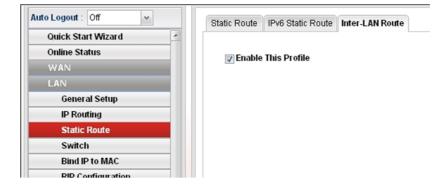
1. Open **LAN** >> **General Setup** to create a LAN (192.168.1.1/24) profile named lan1 with the settings shown below.

<b>Dray</b> Tel		or 3900 Series	14:41:38	Logir		min 🕞
	General Setup				- X	
Auto Logout : Off	Profile : [7] Enable This Profile	lan1			•	
Quick Start Wizard	Description :	(Optional)				Profile Numb
Online Status						
WAN	VLAN ID :	10				Pv6 Protocol
LAN	Default MAC Address :	Enable      Disable				Jink-Local
General Setup	MAC Address :	00 : 50 : 7f : 7b : 83 : 08				Jink-Local
IP Routing	IPv4 Protocol :	static				
Static Route	Mode :	NAT			Ε	
Switch						
Bind IP to MAC	IP Address :	192 168 1 1				
RIP Configuration	Subnet Mask :	255.255.255.0 ~				
OSPF Configurati	Gateway IP Address :	<b>i</b>		(Optional)		
Firewall		🖏 Add 🛗 Save				
Objects Setting		IP Subnet Mask	Mode			
User Management		No items to show				
Applications		No items to show	Ψ.			
VPN and Remote (	2nd Subnet :					
Virtual System	Zhd Subnet :					
Certificate Manag					-	
	( )	12				
Bandwidth Manag				🛗 Apply 🙆 Canc	el	
System Maintenand				нg		

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

Dray Tek	or 3900 Series 14:43		min 🕞
General Setup		- ×	
Auto Logout : Off Profile :	lan2 le	*	
Ouick Start Wizard	(Optional)		Profile Numb
Online Status			
WAN VLANID:	11		IPv6 Protocol
LAN Default MAC Addres	s: <ul> <li>Enable</li> <li>Disable</li> </ul>		Jink-Local
General Setup MAC Address :	00 : 50 : 7f : 7b : 83 : 08		Jink-Local
IP Routing IPv4 Protocol :	static		
Static Route Mode :	NAT	E	
Switch			
Bind IP to MAC IP Address :	192 168 3 1		
RIP Configuration Subnet Mask :	255.255.255.0 ¥		
OSPF Configurati Gateway IP Address		(Optional)	
NAT		(Optional)	
Firewall	🕼 Add 🛗 Save		
Objects Setting	IP Subnet Mask M	tode	
User Management			
Applications	No items to show.		
VPN and Remote a 2nd Subnet :			
Virtual System			
Certificate Manag			
SSL VPN			
Bandwidth Manag		💾 Apply 🛛 Cancel	
System Maintenance		13	

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



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

	LAN >> OSPF Config	uration		
Auto Logout : Off 🛛 👻	OSPF Configurat	ion		
Quick Start Wizard				
Online Status	🔽 Enable Thi	is Profile		
WAN				
LAN		bbA 🕼		
General Setup		LAN Profile	Area	
IP Routing		lan2	11	Ŵ
Static Route	Profile :	lan1	11	Ē
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration				

# Configuration for Vigor3900 B,

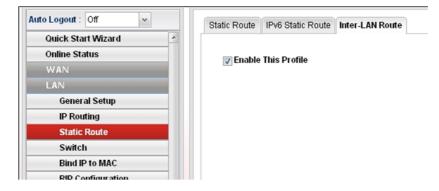
1. Open **LAN** >> **General Setup** to create a LAN (192.168.2.1/24) profile named lan1 with the settings shown below.

Description:     (Optional)       WAN     VAN ID:       UAN     10       WAN     VAN ID:       ID     0       General Schup     Defcuit MAC Address:       General Schup     MAC       Bind Pro Mark     ID:       Static Roze     MAC       Switch     PA Address:       Dorf Configuration     Op: 100: 77: 70: 84: 800       Bind Pro Mark     ID:       Bind Pro Mark     ID:       Switch     MAC       Bind Pro Mark     ID: 25525255.0       Gateway IP Address:	<b>Dray</b> Tek	Vige	or 3900 Series	14:58:55	Log	in: Ad	min 💽
Logont of Datck Start Witzed Others Status WAN LAN General Schup IP Roating IP Subnet Mask IP Subnet Mask Mode IP Subnet Mask Mode IP Subnet Mask Mode IP Subnet Mask Mode IP Subnet Mask Mode	Ger	neral Setup					
Order Status       Conduct Status       Description:       (Copbona)       Profile         WAN       Description:       (Copbona)       Profile         WAN       Default MAC Address:       © Enable       Discription:       Profile         Canno       Default MAC Address:       © Enable       Discription:       Profile         Status       Default MAC Address:       © Enable       Discription:       Profile         Canno       Default MAC Address:       © Enable       Discription:       Profile         Status Route       MAC Address:       © : [0 : [7 : 72 : 84 : 80       Profile       Inic Local         Status Route       MAC Address:       192 : 168 2 : 1       Inic Local       Inic Local       Inic Local         Status Route       Right Catinguation       Statuset Mask:       255: 255: 0 : 0       Gateway IP Address:	Laura Car	Profile :	lan1			1	
Outline Status     Description:     © optional)     Profile       WAN     VLND:     10     Px0file       LAN     Default MAC Address:     © Enable     Disable       General Schop     MAC Address:     © 0 : 50 : 77 : 79 : 64 : 60     Px0file       PR conting     Px1 Protocol:     static       Static Route     MAC Address:     192 : 168 : 2     1       Bind Pro MAC     Px Address:     192 : 168 : 2     1       OSPF Configuration     OSFF Configuration     Gateway IP Address:		Finable This Profile					
Other is status     VLAN D:     10       WAN     VLAN D:     10       LAN     Default MAC Address:     © Enable       Default MAC Address:     0:50:17:29:84:80       BP Routing     Bodies:     10:50:21       Static Route     MAC Address:     0:50:17:29:84:80       Static Route     Bodies:     10:20:17:20:84:100       Brid P to MAC     MAT     m       Brid P to MAC     Static Route     Static Route       Static Route     NAT     m       Brid P to MAC     Static Route     Static Route       Static Route     NAT     m       P Address:     192:188:2.1     Static Route       Static Route     Static Route     Gateway IP Address:       Objects Setting     Add Save     No items to show.       VPN and Remote     Znd Statient:     Znd Statient:       Static Yuhana     T     =		Description :	(Optional)				Profile N
Convertal Schop     Default MAC Address:     Obisable     IntelCocal       IP Routing     MAC Address:     Obisable     IntelCocal       Static Route     Static Route     NAT     IntelCocal       Static Route     NAT     IntelCocal     IntelCocal       Bind Pto BAAC     Hodees:     192     168     IntelCocal       Bind Pto BAAC     Subnet Mask:     255252550     IntelCocal     IntelCocal       OSFF Consignation     Gateway IP Address:     IntelCocal     IntelCocal       Objects Setting     User Management Applications     No items to show.     IntelCocal       Virtual System     Zind Statinet :     IntelCocal     IntelCocal	Online Status						Pv6 Protocol
Center al Setup     MCC Addess :     OC : FO : T : Z0 : Edit     D       IP Routing     MCC Addess :     OC : FO : T : Z0 : Edit     D       Static Route     MCC Addess :     OC : FO : T : Z0 : Edit     D       Static Route     MACC Addess :     D     Edit       Static Route     MACC Addess :     D     Edit       Gold IP to SARC     P Address :     D     Image: Content of Content	TYPEN						and the second sec
MAC Address : 00 : 50 : 77 : 70 : 84 : 80 MAC Address : 00 : 50 : 77 : 70 : 84 : 80 MAC Address : 00 MAC Add	Canadal Salam						and the second se
Static Route     PA 4 Potocci:     static       Switch     Mode:     NAT       Bind P to MAC     P Address:     192       IBP Configuration     Stather Mask:     252.255.255.0 w       OOSPC Configuration     Gateway IP Address:     (Optional)       PAdd ID Save     (Optional)       IP     Subnet Mask     Mode       Objects Setting     IP     Subnet Mask     Mode       Virtual System     Add ID Save     No items to show.       Virtual System     Confificate Manage     IP       StL VPN     T     T		MAC Address :	00 : 50 : 71 : 79 : 84 :	80			
Switch       Mode :       NAT       Image: Configuration         Bind Pto MAC       P Address :       192       168       2       1         BPC configuration       Subnet Mask :       255.255.250       Image: Configuration       Image:		IPv4 Protocol :					
Bind IP to MAC       IP Address :       192 [168 ] 2 [1]         RIP Configuration OSPF Configuration OSPF Configuration OSPF Configuration OSPF Configuration OSPF Configuration Firewall       Gateway IP Address :       (Optional)         Firewall       Image: Image		Mode :	NAT 👻				
OSPF Configuration     Configuration       NAT     Gateway IP Address :       Configuration     Configuration       Objects Setting     IP       Subnet Mask     Mode       VPN and Remote     P       Virtual System     Zind Subnet :       SSL VPN     r		IP Address :	192 168 2 1				
NAT     GutewaylP Address :     (Optional)       Firewall     Image: Constraint of the same interval of the sam	RIP Configuration	Subnet Mask :	255.255.255.0 ¥				
NAT     Outering in volunts:     Image: Comparison of the compariso	OSPF Configurati	Cataway ID Address			(Optional)		
Objects Setting User Management Applications VPN and Remote Virtual System SSL VPN	NAT	Gateway IP Address .			(Optional)	. 11	
User Management Applications VPN and Remote Virtual System SSL VPN IT I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			🕼 Add 🔚 Save				
Applications No items to show. VPN and Remote Virtual System Currificate Manage SSL VPN T Constraints of the Constraint			IP Su	onet Mask Mode			
Applications VPN and Remote   VPN and Remote   VPN and State SSL VPN It			No ite	ms to show			
Virtual System 2nd Subnet : Certificate Manag SSL VPN It IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII							
SSL VPN		2nd Subnet					
SSL VPN	Virtual System	and control :					
	Certificate Manag						
Bandwidth Manag			70				
	Bandwidth Manag				🛗 Apply 🛛 😡 Car	icel	

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

Dray Tek	or 3900 Series	14:59:11 Log	in: Admin 🕞
General Setup			- ×
Auto Logout : Off Profile :	lan2		4
Ouick Start Wizard			
Online Status Description :	(Optional)		Profile NL
WAN VLANID:	11		Pv6 Protocol
LAN Default MAC Address :	Enable Obisable		Jink-Local
General Setup MAC Address :	00 : 50 : 71 : 79 : 84 : 80		_ink-Local
IP Routing IPv4 Protocol :	static		
Static Route Mode :	NAT v		-
Switch Bind IP to MAC IP Address :	192 168 3 2		
RIP Configuration Subnet Mask :	255.255.255.0 ~		
OSPF Configurati NAT Gateway IP Address :		(Optional)	
Firewall	🚯 Add 🛗 Save		
Objects Setting	IP Subnet Mask	Mode	
User Management	No items to show.		
Applications	NO BERIS ID SHOW.		
VPN and Remote - 2nd Subnet :			
Virtual System			
Certificate Manag			•
SSL VPN			
Bandwidth Manag		💾 Apply 🔞 Can	
System Maintenance		-	

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



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

	l	AN >> OSPF Configura	ntion		
Auto Logout : Off 🛛 👻		OSPF Configuration			
Quick Start Wizard Online Status		👽 Enable This F	Profile		
LAN			bbA 🕼		
General Setup			LAN Profile	Area	
IP Routing			lan2	11	Ŵ
Static Route		Profile :	lan1	11	Ŵ
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					

## 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.

Dray Tel	eneral Setup	pr 2960 Series	35304640-		Admin Et
n Lùgout :0ff	Profile :	lan1			
Onich Start Wizard	Description	(Optional)			e Number Limit: 10
Online Statizs	VLANID :	10			Pvő Protocol
Lak	Default MAC Address	Enable      Disable			unik-Lacal
General Selup	MAC Address	00 2(60 )/77 2 mil 2 mil 2 mil			unisk on al
IP Routing		100 14 (20 17) 21 14 14 14 14 14 14 15 15 15 15 15 15 15 15 15 15 15 15 15			
Static Route	Mode .	NAT			9
Switch Bind IP to MAC	IP Address	192 168 4 1			
RIP Configuration					
OSPF Configurati	Subnet Mask :	255,255.255.0			
NAL	Gateway IP Address :	an .		(Optional)	
r feavoitt		add 🛗 Save			
Digects withing		IP Subnet Ma	sk Mode		
User Management Applications		No items to si	how.		-
wine and formula					
recticate biomet	2nd Subnet :				
COL VPN				_	<b>a</b>
		111			
reston Hantmin			3	🗄 Apply 🥥 Cance	C

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

General Setup	15:05:		egin: Admin
Logout Off Profile :	lan2		
Ouick Start Wizard			ofile Number Limit 10
Online Status Description :	(Optional)		
WAN VLANID:	11		IPv6 Protocol
Default MAC Addres	s:		Link-Local
General Setup MAC Address	00 : 50 : 71 : ed : e1 : 51		_ink-Local
IP Routing Static Route IPv4 Protocol :	static		-
Switch Mode :	NAT		
Bind IP to MAC IP Address :	192 168 3 3		
RIP Configuration Subnet Mask :	255,255,255,0 *		
OSPE Configurati			
Gateway IP Address		(Optional)	
-irewa))	🕼 Add   Save		
Dijects Setting	IP Subnet Mask Mo	ie	
Jsør Managemoni	No items to show.		
Applications	No none to onow.		
/PN and Remote / 2nd Subnet :			
SSL VPN			
Sandwidth Manag	inf.		
System Maintenar		E Coply 🥝 C	a harring

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

Auto Logout : Off 🛛 👻	Static Route IPv6 Static Route Inter-LAN Route
Quick Start Wizard	
Online Status	This Profile
WAN	
LAN	
General Setup	
IP Routing	
Static Route	
Switch	
Bind IP to MAC	
RID Configuration	

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

o Logout : Off 🛛 👻	OSPF Configurat	tion		
Online Status	Enable Th	is Profile		
WAN	V Lindoje ili			
LAN		C Add		
General Setup		LAN Profile	Area	
IP Routing		lan2	11	m
Static Route	Profile :	lan1	11	m
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration	Ę.			

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

# Routing information for Vigor3900 A

Routing Table	IPv6 Routing Table				
🖨 Refres	h				
Destination	Gateway	Genmask	Flags	Metric	lface
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	255,255,255,0	Ū	0	lan-lan1

# Routing information for Vigor3900 B

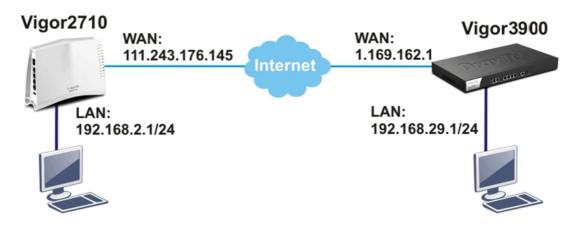
Routing Table	IPv6 Routing Table				
S Refrest	1				
Destination	Gateway	Genmask	Flags	Metric	lface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	0.0.00	255.255.255.0	U	0	lan-lan1
192,168,1.0	192,168,3,1	255,255,255,0	UG	20	lan-lan2

# **Routing information for Vigor2960**

Routing Table	IPv6 Routing Table				
S Refrest	n				
Destination	Gateway	Genmask	Flags	Metric	lface
192.168.4.0	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.

IPSec							×
Profile : Profile This Profile Type		2710 IP	Sec D		PPTF Dial In		
Set PPTP Dial-In For Use	r Profie						
Basic Advanced	GRE		Proposal	F	HTH-		_
Auth Type :	PSK		1.				1
Preshared Key :							
Security Protocol	ESP						
WAN Profile :	wan1						
Local IP / Subnet Mask :	192	168	29	0	255.255.255.0	*	
Local Next Hop :	D	0	. 0	Ū			
Remote Host :	111	243	176	. 145	C		
Remote IP / Subnet Mask	192	168	2	0	255.255.255.0	~	1
1			III				
						Apply 🙆	Cancel

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	Call Direction 🛛 🔿 Both 💿 Dial-Out 🗘 Dial-in
Enable this profile	Always on
	Idle Timeout -1 second(s)
VPN Dial-Out Through WAN1 First 💌	Enable PING to keep alive
Netbios Naming Packet 💿 Pass 🔘 Block	PING to the IP
Multicast via VPN 🛛 🔿 Pass 💿 Block	
(for some IGMP,IP-Camera,DHCP Relayetc.)	

- 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.

Type of Server I am calling	Username ???
O PPTP	Password
IPsec Tunnel	
C L2TP with IPsec Policy None	VJ Compression On Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method  Pre-Shared Key
1.169.162.1	[IKE Pre-Shared Key]
	O Digital Signature(X.509)
	Peer ID
	Local ID
	Alternative Subject Name First
	O Subject Name First
	IPsec Security Method
	O Medium(AH)
	High(ESP) 3DES without Authentication >>
	Advanced
	Index(1-15) in <u>Schedule</u> 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.

My WAN IP	0.0.0.0	RIP Direction Disable 👐
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to
Remote Network IP	192.168.29.0	Route 2
Remote Network Mask	255.255.255.0	
Local Network IP	192.168.2.0	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	
	More	

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.

Conne	ection Management						
Pro	files :	👻 🙃 Conn	ect  IPSec  I	PPTP 🦛 Re	resh		
					and the second sec		
VPN	Туре	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Dis

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

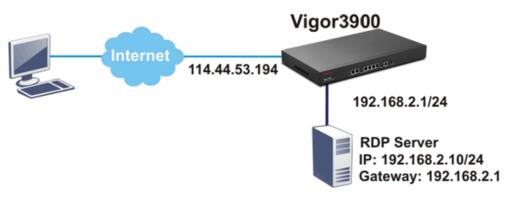
#### VPN and Remote Access >> Connection Management

Dial-out	Tool				R	efresł	n Seconds :	10 💌 🕻	Refresh
		(3900	1)1.169.162.1		<b>v</b> [	ial			
VPN Con Current F	nection Statu Page: 1	IS				F	Page No.	Go	>>
VPN	Туре	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
					~~~~~		<del>ita is encryp</del>	ited.	

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.**

1	System Maintenance >> Acces	es Control	
o Logout : Off	Access Control		
Firewall Objects Setting User Management Applications VPN and Remote Access VPN and Remote Access VPN Setting Certificate Management SSL VPN Bandwidth Management System TR069	Web Allow : Web Port : Teinet Allow : Teinet Port : SSH Allow : SSH Port : HTTPS Allow : HTTPS Port :	<ul> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> <li>Enable Disable</li> </ul>	Ē
Administrator Password	User Define :	⊖Enable ⊙Disable	
Configuration Backup ≣ Syslog / Mail Alert	Allowed IP1	0.0.0	
Time and Date	Allowed IP2	0 0 0 0.0.0.0 *	
Access Control SNMP Setup	Allowed IP3	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,	
Reboot System Firmware Upgrade		N: ⊛Enable ⊜Disable : ⊛Enable ⊜Disable	
Diagnostics	Allow Pillg If offit 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.

DrayTek	Vigor 3900 Series	17:46:41	Login: Admin	ex.
	SSL VPN>> SSL Application >> RDP			
uto Logout 🗌 Off	VNC RDP			
Ouick Start Wizard	🕼 Add 💥 Edit 🏢 Delete 👒 Refresh			Profile Nu
Online Status				TTOMO TR
	Profile IP Address	Port	Screen Size	
		No items to show.		
	RDP	- X		
Firewall				
Objects Setting	Profile : Win7			
User Management	IP Address : 192 168 2 10	1		
Applications		1		
VPN and Remote Access	Port: 3389			
Virtual System	Screen Size : Fullscreen 🛩			
Certificate Management				
SSL VPN		💾 Apply 🔕 Cancel		
SSL Web Proxy		<u>↓</u> .		
SSL Application				
Online User Status				
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				
	0			1

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.

	Vigor 3900				and the second	e,
	User Management >> Use User Profile	er Profile	- X	-		
Logont: Off   Logont: Off  Logont: Off  Collick Start Wizard  Collick Start Wizard  Collick Start Wizard  VA N  LAN  VAN  LAN  User Start  Coneral Setup  User Group  Rabits  LDAP / Active Directory  Applications  VPN and Remote Access  VPN and Remote Access		7788 7788 300 480 false • • © Enable © Disable lan1 • • © Enable © Disable	E (Optional	DHCP from lant lant lant lant	Static IP Addre Use mOTF Disable Disable Disable	Profile N
Certificaté Management SSL VPN Bandwidth Management System Maintenairce Diagnostics Systema Davices	SSL Proxy : SSL Application(VNC) : SSL Application(RDP) :	Possi				

5. Logout Vigor3900.

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

ay Tel	/			
User :	7788			
Password:	••••			
	English	*	Login	

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



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



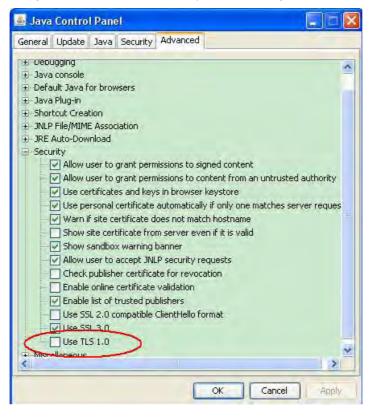


9. After that, you can access into Windows 7 via a browser. Note the message below the window. In which, TLS means Transport Layer Security.



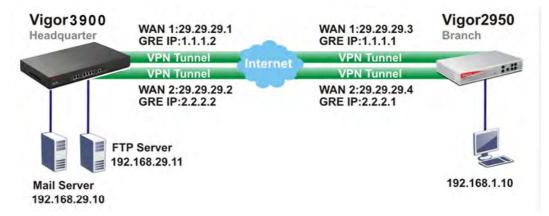
# Troubleshooting

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



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

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



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

# **Configuring Vigor3900**

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

		VPN and Remo	te Access	>> VPN Profiles			
Auto Logout : Off		VPN Profile	s				
Quick Start Wizard	*		100			<u> </u>	
Online Status		🕼 🖓	i 🔀 Edi	t 🇰 Delete (	S Refresh	⊙ IPSec ◯ I	PPTP Dial-0
WAN		Profile		Enable This Profil	e Local I	P / Subnet Mask	Remote I
LAN							
NAT							
Firewall							
Objects Setting	E						
User Management							
Applications							
VPN and Remote Access							
VPN Client Wizard							
VPN Server Wizard							
Remote Access Control							
PPP General Setup							
IPSec General Setup							
VPN Profiles							
VPN TRUNK Management		4					
Connection Management	-						

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

PSec					_ X
Profile :	2950WAN1				
Enable This Profile					
Туре :	💿 IPSec 🔘 PPTF	P Dial-Out 🔘 PP	TP 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	~			
4					
				Apply	🔇 Cancel

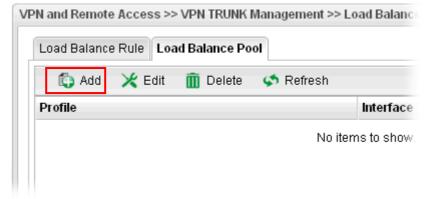
Profile :	2950WAN1	
Enable This Profil		
Type :	IPSec OPTP Dial-Out OPTP Dial-In	
Basic Advan	GRE Proposal PPTP	
Enable GRE Function	:      • Enable      O Disable	
Local GRE IP :	1 . 1 . 2 mm (Optional)	
Remote GRE IP :	1 . 1 . 1 . (Optional)	
Auto Generate GRE	ey : 💿 Enable 🔘 Disable	

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

IPSec					=×
Profile :	2950WAN2				
Туре :	IPSec OPPTI	P Dial-Out 🔘 PPT	P Dial-In		
Basic Advance	ed GRE	Proposal	PPTP		
Always On :	🔵 Enable 🧕	Disable			^
For Remote Dial-In :	🔵 Enable 🧕	Disable			E
Auth Type :	PSK	~			
Preshared Key :	•••				
Security Protocol :	ESP	*			
WAN Profile :	wan2	*			-
4	I				>
				🗎 Apply (	🔇 Cancel

IPSec				-×
Profile :	2950WAN2			
Enable This Prof	le			
Type :	IPSec OPPTP	Dial-Out 🔵 PP1	TP Dial-In	
Basic Adva	nced GRE	Proposal	рртр	
Enable GRE Functio	n: 💿 Enable 🔘 D	isable		
Local GRE IP :	2 . 2	. 2 . 2	(Optional)	
Remote GRE IP :	2 . 2	. 2 . 1	(Optional)	
Auto Generate GRE	Key: 💿 Enable 🔘 D	isable		
			📑 Apply 🔇	Cancel

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



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

jour : joii	Y	
Load Balance	e Pool	_×
Mode	Load Balance	
Profile :	2950_LB	
1		
	🖬 Apply	🔇 Cancel

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

l Balance I	2001	-
Mode	Load Balance	
Interface	: 2950WAN1,2950WAN2 -	
interrace	39	
	39_1 2950WAN1	
	2950WAN2	
		💾 Apply 🛛 🔇 Car

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



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

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

Profile :	2950						
🔽 Enable This Profile							
Protocol :	ALL			~			
Source IP Address	192	. 168	. 29		0	IIII	) (Optiona
Source Mask :	255.25	55.255.0		*	(Opti	onal)	
Destination IP Address :	192	. 168	. 1	].	0	m	) (Optiona
Destination Mask :	255.25	55.255.0		¥	(Opti	onal)	
Load Balance Pool :	2950_	LB		~	1		

## **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**.

Vigor2950 Dual-WAN SSL VPN A		<b>Dray</b> Tek
Off  Quick Start Wizard Service Activation Wizard Online Status	VPN and Remote Access >> LAN to LAN Profile Index : 1 1. Common Settings	
WAN LAN NAT Firewall Objects Setting CSM Bandwidth Management Applications VPN and Remote Access • VPN Cient Wizard	Profile Name     2960WAN1     ✓ Enable this profile            VPN Dial-Out Through:         WAN1 Only ♥           Netbios Naming Packet	Call Direction O Both O Dial-Out Dial-In Always on Idle Timeout 1 second(s) Enable PING to keep alive
VPN Server Wizard Remote Access Control	2. Dial-Out Settings	
PPP General Setup     PiPScc General Setup     PiPScc Peer identity     Remote Dial-in User     LAN to LAN     VPN TRUNK Management     Connection Management     Connection Management     Stystem Maintenance     Diagnostics     Support Area     Application Note     FAQ     Status: Ready	Type of Server Lam calling ISDN PPTP IPSec Tunnel L2TP with IPSec Policy Name Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 29.29.29.1	Link Type Edik bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression On Off IKE Authentication Method Pre-Shared Key

- 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 0 30	es 🖻 aes
Start Wizard e Activation Wizard			Callback Function (CB	CP)
Status			🗌 Enable Callback F	unction
			🗌 Use the Following	Number to Callback
			Callback Number	
ill			Callback Budget	0 minute(s)
s Setting	1 005 000 000		Comback budget	
vidth Management	4. GRE over IPSec Setting	A		
ations	🗹 Enable IPSec Dial-Ou			
nd Remote Access	Logical Traffic	My GRE IP 1.1.1.1	Peer GRE IP	1.1.1.2
V Server Wizard	5. TCP/IP Network Settings	s		
note Access Control	My WAN IP	nnnn	RIP Direction	Disable 💌
P General Setup ec General Setup		levere.	From first subnet to r	emote network, you have to
ec Peer Identity	Remote Gateway IP	0.0,0.0	do	emote network, you have to
note Dial-in User I to LAN	Remote Network IP	192.168.29.0		Route M
TRUNK Management	Remote Network Mask	255.255.255.0	-	
nection Management		Percipative con	🗆 Change default rou	te to this VPN tunnel ( Only
ate Management	Local Network IP	192.168.1.0	single WAN supports th	iis )
Maintenance	Local Network Mask	255.255.255.0		
stics	the second se			

- 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**.

Vigor2950 Dual-WAN SSL VPN A		<b>Dray</b> Tek
Off	VPN and Remote Access >> LAN to LAN Profile Index : 2 1. Common Settings	
LAN NAT Firewall Objects Setting CSM Bandwidth Management Applications VPN and Remote Access > VPN and Remote Access > VPN client Wizard > VPN Server Wizard	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 Relayetc.)	Call Direction  Both  Dial-Out Dial-In Callways on Idle Timeout -1 second(s) Enable PING to keep alive PING to the IP
Remote Access Control     PPP General Setup     IPSec General Setup     IPSec Deer Identity     Remote Dials in User     LAN to LAN     VPN TRUMM Management     Controlion Management     SSL VPN     System Maintenance     Diagnostics     Support Area     Application Note     FAQ     Status: Ready	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 V Username ??? Password PPP Authentication PAPICHAP V V3 Compression © On Off IKE Authentication Method © Pre-Shared Key

- 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.

ff 🛛 💌			DES 030	DES 🖻 AES	
uick Start Wizard ervice Activation Wizard Iline Status			Callback Function (CB		
AN IN			Callback Number	Number to Callback	
AT rewall sjects Setting			Callback Budget	0 minute(s)	
M Indwidth Management	4. GRE over IPSec Setting				
plications N and Remote Access VPN Client Wizard	Enable IPSec Dial-Ou	t function GRE over IP My GRE IP 2.2.2.1	Sec Peer GRE IP	2.2.2.2	
VPN Server Wizard	5. TCP/IP Network Settings	5			
Remote Access Control PPP General Setup	My WAN IP	0.0.0.0	RIP Direction	Disable 💌	
IPSec General Setup IPSec Peer Identity	Remote Gateway IP	0.0.0.0	From first subnet to do	remote network, you have to	
Remote Dial-in User LAN to LAN	Remote Network IP	192.168.29.0		Route 💌	
VPN TRUNK Management Connection Management	Remote Network Mask	255.255.255.0		and the second second	
tificate Management	Local Network IP	192.168.1.0	single WAN supports the	ite to this VPN tunnel ( Only nis )	
VPN tem Maintenance	Local Network Mask	255.255.255.0			
gnostics	the second se	More			

- 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		

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.

Add

Connection N	lanagement						
Profiles :		× 9	Connect 💿 IPS	ec OPPTP	🦛 Refresh		
VPN	Туре	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect
2950WAN1	IPSec/DES_N	29.29.29.3	1.1.1/32	00:47:13	0	0	X
2950WAN2	IPSec/DES N	29.29.29.4	2.2.2.1/32	00:47:12	a	0	X

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

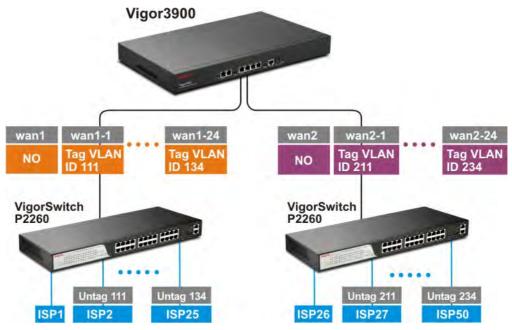
VPN Connection Current Page:						Don	e No.	Go	
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	D	Du		
1 (3900WAN1 )	IPSec Tunnel DES-No Auth	29.29.29.1 via WAN1	192.168.29.0/24		0	0	0	0:0:0	Drop
2 (3900WAN2)	IPSec Tunnel DES-No Auth	29.29.29.2 via WAN2	192.168.29.0/24	0	0	0	0	0:0:16	Drop

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:

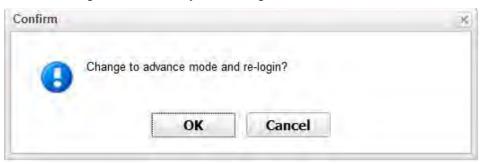


### Configuring 50 WAN profiles on Vigor3900

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

<b>Dray</b> Tek	2.6		900 Sei	100		16:26:42		Login: Admir	
		WAN >> General \$	Setup						
ito Logout : Off		General Setup							
Online Status		🕼 Add	🗶 Edit 🗴 🕅	Delete 🛛 🗳 F	Refresh Mode :	Advance	*	Profi	le Number Limit : 50
WAN General Setup		Profile	Enable This Pro	Description	VLAN ID	Basic		IPv4 Protocol	IPv6 Protocol
Default Route		wan1	true	ADSL_01	10	Enable	WAN1	PPPoE	Link-Local
Load Balance		wan2	false		11	Disable	WAN2	PPPoE	Link-Local
Switch		wan3	true		12	Disable	WAN3	PPPoE	Link-Local
LAN		wan4	true		13	Disable	WAN4	Static	Link-Local
		wan5	false		14	Disable	WAN5	None	Link-Local
NAT Firewall		Marketing	true	Marketing Dept	22	Disable	WAN1	DHCP	DHCP-IA_NA
Objects Setting	E								
User Management									
Applications									
VPN and Remote Access									
Certificate Management									
SSL VPN									
Bandwidth Management									
System Maintenance									
Diagnostics									
External Devices									

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



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

🚺 Add	🔀 Edit	Delete	Refresh Mod	le : Advance	*			Profile Number
Profile	Enab	le 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	Confirm		14	MANE	Enable	None	Link-Local
		0	The Selected Confi	g Will be Deleted, C	ontinue?			

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

General Setu	p	
🚺 Add	💥 Edit 🔟 Del	lete 🗳 Refresh Mode
Profile	Enable This Prof I	Description VLAN ID

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.

Global PP	TP Static	DHCP	PPPoE	StaticV6	DHCPV6	
Side 1	Charles and the second s	2				
Profile :	wan1_1					
Enable This Pro	ofile					
Description :		(Optio	nal)			
VLAN ID :	111					
VLAN Tag :	Disable	~				
Port :	WAN1	~				
Default MAC Addre	ss : 💿 Enable 🔿 Disa	able				
MAC Address :	00 : 50 :	7f : e7	: do : 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.

Dray Tek	damp ( ) )				HH - H
Auto Logout 3 min 💌					
VigorSwitch P2260 System Port			Tag-l	based Gro	oup
PoE Loop Detection		No	VLAN N	AME	VID
SNMP		_			
DHCP Boot		1	defa	uit	1
IGMP Snooping					
VLAN					
VLAN Mode					
Tag-based Group					
PVID					
Port based Group					
Management Vlan					
MAC Table					
GVRP					
STP					
Trunk					
802.1X					
Alarm					
Configuration					
Security					
Bandwidth					
QoS					
Diagnostics					
TFTP Server				-	and and
Log			Add	Edit	Delete
Firmware Upgrade					
Reboot					
Logout					

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

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

Tag-based	VLAN
-----------	------

•	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 <b>wan1_1</b> to <b>wan1_24</b> ). Therefore VigorSwitch
	Port 26 must be the member of VLAN Group ID 111 to 134.

Apply

- 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.

	-	•	
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	Ξ
8	117	117	
9	118	118	
10	119	119	
11	120	120	
12	121	121	
13	122	122	
14	123	123	
15	124	124	
16	125	125	
17	126	126	~
	Add Edit	Delete	

#### **Tag-based Group**

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

### PVID

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

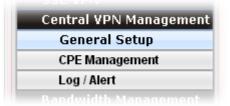
- 1. Access into the web user interface of Vigor3900.
- 2. Open **System Maintenance>>Access Control**. Check **Enable** for **Web Allow** and type the value for **Web Port**. Then click **Apply** to save the settings.

n Maintenance >> Acce	ess Control	
Web Allow :	💿 Enable i 🔿 Disable	
Web Port :	80	
Teinet Allow :	💿 Enable  🔿 Disable	
Teinet Port :	23	
SSH Allow :	Enable Oisable	
SSH Port :	22	
HTTPS Allow :	💿 Enable  🔿 Disable	
HTTPS Port :	443	
Server Certificate :	Default	
User Define :	🔿 Enable 💿 Disable	
Allowed IP1		~

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

13:53:06	Login: Admin	6
	Fotal number of devices:	:0
		13:53:06 Login: Admin Total number of devices:

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.

eneral Setup VP	N General Setup
🗷 Enable	
WAN Profile :	wan1
Port :	9000
Username :	acs
Password	
Polling Status :	Enable Obisable
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 >>	<ul> <li>TR-069 Setting</li> </ul>
-----------------------	------------------------------------

ACS	and	CPE	Settings	;
-----	-----	-----	----------	---

ACS Server On	Internet <b>v</b>
ACS Server	
URL	http://172.17.1.182:9000
Username	acs
Password	
<b>CPE Client</b>	ile
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.

System Maintenance >> Management

- 2. Open System Maintenance>>Management Setup.
- 3. Check Allow management from the Internet to set management access control.

IPv6 Management Setup	
Management Port Setup	)
<ul> <li>User Define Ports</li> </ul>	O 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)
—	
	<ul> <li>User Define Ports</li> <li>Telnet Port</li> <li>HTTP Port</li> <li>HTTPS Port</li> <li>FTP Port</li> </ul>

### 3.7.4 Enable WAN Connection on CPE

1. Login the web user interface of the CPE.

WAN >> Internet Access

- 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**.

ΡΡΡοΕ / ΡΡΡοΑ	MPoA (RI	FC1483/2684)	IP∨6
💿 Enable 🛛 Disable		WAN IP Network Settings	WAN IP Alias
DSL Modem Settings		¯ │ ○ Obtain an IP address a	utomatically
Multi-PVC channel	Channel 2 🛛	Router Name	Vigor
Encapsulation			*
1483	Bridged IP LLC 🛛 😽	Domain Name	*
VPI	0	* : Required for some IS	SPs
VCI	88	Specify an IP address	
Modulation	Multimode 🛛 😪	IP Address	172.16.3.229
		– Subnet Mask	255.255.0.0
WAN Connection Detection	n	Gateway IP Address	172.16.3.4
Mode	ARP Detect 💙		
Ping IP		O Default MAC Address	
TTL:		🔘 O Specify a MAC Addre	55
RIP Protocol		MAC Address: 00 ⋅50	·7F:00 ·00 ·01
Enable RIP		DNS Server IP Address	
Bridge Mode		Primary IP Address	
Enable Bridge Mode		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**.

Vigor 3900 Series			13:53:06	Login: Admin
Central VPN Management >> CPE Ma	nagement >>	CPE Maintenance		
CPE Maintenance VPN Manageme	ent Map			
iiiManaged Devices Status				
🔀 Edit 📰 Detail 🝈 Delete	🛸 Refresh	📠 Recycle Bin		Fotal number of devices: : 0
2830 172.17.1.208				

# **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.

Maintenance	VPN Manage	ement Map				
👺 PPTP 🏼	🐮 IPsec 🛛 🔀	Advanced 🛛 📢 I	Refresh	Keep VPN Se	ettings	
				🚯 Add	🔟 Delete 🛛 🗲	5 Refresh
		)		Profile	Device	Name
SH_Data 8.242.130.18	Eric Te 220,128,22					
۲	۷					
Connected D	evices					🔊 Re
۲	۷	Remote IP	Virtual Networ Up Time	RX(Packets)	TX(Packets)	C Re Disconnect

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

PPTP PPTP	🐮 IPsec	🔀 Advance	ed 🛛 🗳 Ref	resh	
		time:0			
SH_Data 218.242.130.18		_Test 8.228.219			

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

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 IPse DrayTek_00507F_Vigor2920Vn_	
	OKCa	ncel

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

÷	🖇 PPTP 🐮 IPsec 🔀 Advanced 🗳 Refresh					Keep VPN Settings		
						🕼 Add 📺 I	Delete 🛛 🗳 Refresh	
						Profile	Device	Name
2	SH_Data 18.242.130.18	Eric_Test 220.128.228.219						
С	connected Devices							🖈 Rei
	VPN	Туре	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect
	CVM CC19F0			192.168.20.0/24	00.00.45	1	0	X

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

LAN-to-LAI View: 💿 /								
Index	Name	Active	Status	Index	Name	Active	Status	
<u>1.</u> C'	VM_CC19F0	<ul><li>✓</li></ul>	online	<u>17.</u>	???			
Profile Inde 1. Commo				L				
Profile Name cvm_CC19F0     Image: Constraint of the second se				🗖 Alwa	Call Direction O Both O Dial-Out O Dial-in Always on Idle Timeout O second(s)			
VPN Dial-Out Through WAN1 First				1	Enable PING to keep alive			
Netbios Naming Packet   Pass   Block					PING to the IP			
Multicast (for som	via VPN 1e IGMP,IP-Car	○Pass ( mera,DHCP	210011	Find to				
3. Dial-In S	ettings							
Allowed Dial-In Type				Usernam	ie	7D9D00		
🗹 РРТЕ	)			Passwor	d(Max 11 ch	ar) ••••	•	
🗖 IPse	c Tunnel			VJ Comp	ression	💿 On (	Off	
L2TP with IPsec Policy None			IKE Authe	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.

VPN and Remote Access >> LAN to LAN

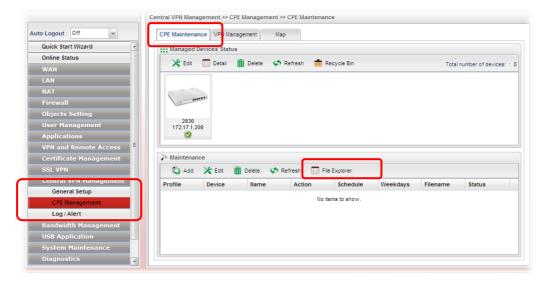
# 3.9 CVM Application - How to upgrade CPE firmware through Vigor3900?

#### 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.

cess Control	
Web Allow :	
Web Port :	80
Teinet Allow :	⊙ Enable 🔿 Disable
Teinet Port :	23
SSH Allow :	● Enable              ○ Disable
SSH Port :	22
HTTPS Allow :	
HTTPS Port :	443
Server Certificate :	Default
User Define :	🔿 Enable 💿 Disable
Allowed ID1	

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



- File Explorer  $-\times$ 💓 Upload 🏢 Delete 🔍 Download 🚯 Create folder < Refresh Property Filename Size LastModify Directory Directory 224 2013/05/07/ 09:4 ./cvm/files/00507F Directory 1248 2013/05/07/ 09:4 ./cvm/files 2013/05/07/ 09:4 ./cvm/files/00507F test file 5620 📄 Select 🛛 🐼 Cancel
- 5. In the File Explorer dialog, click **Upload**.

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

ile Explorer	<u> n</u> Delete	📮 Download	🚯 Create folder	🗐 💭
Filename	Property	Size	LastModify	Directory
Upload	Directory	360	2013/05/09/ 16:3	./cvm/files/00507
Select F	ile: 選擇檔案	2830_0508	👩 Uplo:	ad 🐼 Cancel

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/0050            Directory         1248         2013/05/07/ 09:4 ./cvm/files/0050           test         file         160         2013/05/09/ 16:3 ./cvm/files/0050	📄 前 Delete	<table-of-contents> Download</table-of-contents>	🚯 Create folder	🗳 Refresh
Directory 1248 2013/05/07/ 09:4 ./cvm/files	Property	Size	LastModify	Directory
	Directory	432	2013/05/09/ 16:4	./cvm/files/00507
test file 160 2013/05/09/16:3./cvm/files/0050	Directory	1248	2013/05/07/ 09:4	./cvm/files
	file	160	2013/05/09/ 16:3	./cvm/files/00507
2830_0508 file 666061 2013/05/09/16:3./cvm/files/0050	file	666061	2013/05/09/ 16:3	./cvm/files/00507
2830_0508		Property Directory Directory file	PropertySizeDirectory432Directory1248file160	Property         Size         LastModify           Directory         432         2013/05/09/16:4           Directory         1248         2013/05/07/09:4           file         160         2013/05/09/16:3

## 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.

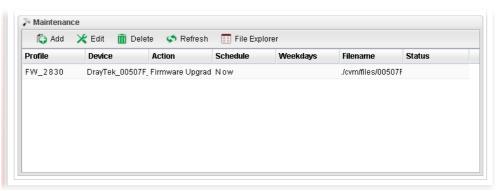
Online Status         WAN         LAN         NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         General Setup         CPR Management         Log / Alert         Paraduktit Management         Log / Alert			Managed Devices Status	
WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management General Setup CER Management Log / Alert Benefativitik Management Log / Alert Benefativitik Management	Online Status	-		
NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         General Setup         Central VPN Management         General Setup         CPE Management         Log / Alert         Prome         Device         No items to show.	WAN			
Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         General Setup         CPE Management         Log / Alert         Promie         Verice         No tems to show.	LAN			
Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         General Setup         CPE Management         Log / Alert         Provide Management         Log / Alert    No items to show.	NAT			
User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management General Setup CPK Management Log / Alert Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile Profile P	Firewall		(and the second s	
User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management General Setup CPE Management Log / Alert	Objects Setting			
Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management General Setup CPE Management Log / Alert Profile Device Name Action Schedule Weekdays Filename Status No items to show.	User Management			
Certificate Management SSL VPN Central VPN Management General Setup CPE Management Log / Alert Profile Maintenance File Explorer No items to show.	Applications		٢	
Certral VPN         Central VPN Management         General Setup         CPE Management         Log / Alert	VPN and Remote Access	=		
Central VPN Hanagement         Profile         Device         Name         Action         Schedule         Weekdays         Filename         Status           CPE Management         Log / Alert         No items to show.	Certificate Management		Maintenance	
General Setup CPE Management Log / Alert Provide Management Log / Alert	SSL VPN		🕼 Add 🗙 Edit 🏢 Delete 🗳 Refresh 🔲 File Explorer	
CPE Management No items to show.			Profile Device Name Action Schedule Weekdays Filename Status	
CPE Management Log / Alert Perden/th Management	-		Na itama ta abaur	
Pauduidth Managamant	CPE Management		no tena te anone.	
	-			
USB Application	-			
	-	-		

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

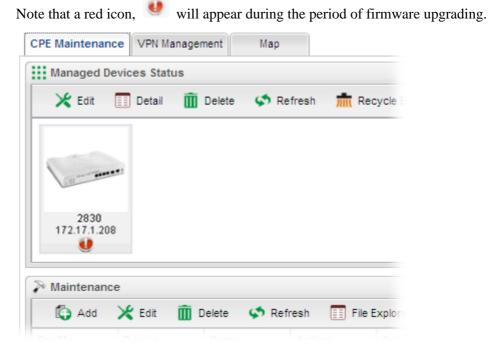
type the string of the firmware filename or click to choose a correct one.

Ĩ	Maintenance				-×	
/i						
1	Profile :	FW_2830				
Î	Device :	DrayTek_00507F	_Vigo 👻			1
l	Action :	Firmware Upgrad	e v			
1	Schedule :	Now	~			
1	Filename :	./cvm/files/00507F	000			
ł						
				E A	pply 🔇 Cancel	
	into foracc					
			<b>7</b>	1		
		File Explorer		998 I INININ 77.3	REILERU	- ×
		💓 Upload	🔟 Delete	<table-of-contents> Download</table-of-contents>	🕼 Create folder	< Refresh
		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.



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



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.

LU	og Alert			
\$	Refresh	Auto Refresh : 10	Seconds 🗸	
D	Time	Device Name	Туре	Description
	2013-05-17 14:58:20	UTC DrayTek_00507F_Vigo	r_( Firmware Upgrade	[Processing][1] Request CPE to download firm
2	2013-05-17 14:58:21	UTC DrayTek_00507F_Vigo	r_( Firmware Upgrade	[Processing][1] CPE start to download firmwar
3	2013-05-17 15:01:42	UTC DrayTek_00507F_Vigo	r_( Firmware Upgrade	[Finished] Profile: V2830_Test, CPE firmware

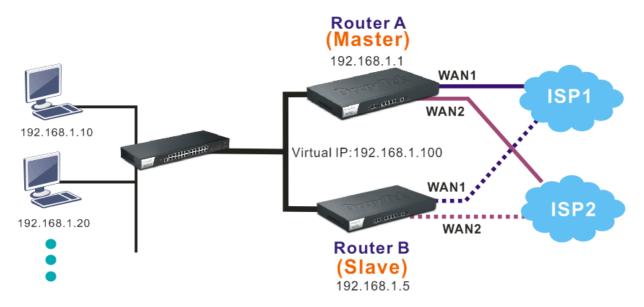
# 3.9.3 Check the Device Information

- 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 :	
Lating :	
IP :	172.17.1.208
Port :	8069
URI :	/cwm/CRN.html
Description :	DrayTek Vigor Router
Hardware Version :	101
Software Version :	3.3.6.1db
Modem Firmware Version :	211011_A Annex_A

# 3.10 How to use High Availability for Vigor routers?

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



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

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

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

### For router A

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

Арр	lications
(	ynamic DNS
0	SVRP
	GMP Proxy
ι	IPnP
H	ligh Availability
١	Vake on LAN
5	MS / Mail Alert Service

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.

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		

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

A	pplications >> I	High A∨ailability >> High A∨	ailability Profile Setup			3
	High Availabil	ity Global Setup High Ava	ilability Profile Setup			
	🕼 Add	🤾 Edit   🏛 Delete 🛭 🛠	Refresh		Profile	εN
Ľ	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.

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.

A	pplications
-	Dynamic DNS
	GVRP
	IGMP Proxy
	UPnP
	High Availability
	Wake on LAN
	SMS / Mail Alert Service

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.

Redundant Method :       Hot-Standby       Image: Config Synchronization Role(Hot-Standby) :       Secondary       Image: Config Synchronization IP(Hot-Standby) :       Secondary       Image: Config Synchronization IP(Hot-Standby) :       192       168       1       1       Image: Config Synchronization IP(Hot-Standby) :       100       Image: Config Synchronization IP(Hot-Standby) :       100       100       Image: Config Synchronization IP(Hot-Standby) :       100       100       Image: Config Synchronization IP(Hot-Standby) :       100       Image: Config Synchronization IP(Hot-Standby)	High Availability Global Setup High Availability	/ Profile Setup	
Config Synchronization Role(Hot-Standby) :       Secondary       IP address configured is configured in Router A         Config Synchronization IP(Hot-Standby) :       192       168       1       1         Priority ID(Hot-Standby) :       1       (1-30)       Router A         Authentication Key :       draytek       Automatic	Redundant Method :	Hot-Standby	Type the lan
Config Synchronization IP(Hot-Standby):       192       168       1       1       Router A         Priority ID(Hot-Standby):       1       (1-30)       4uthentication Key:       draytek         Advance Preemption Mode :       Automatic       •			
Priority ID(Hot-Standby) :     1     (1-30)       Authentication Key :     draytek       Advance Preemption Mode :     Automatic			
Authentication Key:     draytek       Advance Preemption Mode :     Automatic			Router A
Advance Preemption Mode : Automatic		· · · · · · · · · · · · · · · · · · ·	
LAN Port Detection Mode : At_Least_One_Up	Advance Preemption Mode :		
	LAN Port Detection Mode :	At_Least_One_Up	
Enable High Availability	🔤 Enable High Availability		



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



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

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.

gh 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	~

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.



# 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.

WAN	
General Setup	
Default Route	
Load Balance	
Switch	E

## 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.

Ger	neral Setup	USB WAN	1						
	🔀 Edit 🕠	娕 Refresh	Mode :	Basic		*		Profile Nun	nber Limit : 50
	Profile (m	Enable	Descriptio	VLAN Tag	VLAN ID	Priority	Port	IPv4 Proto	IPv6 Proto
1	wan1	false		Disable	10	0	WAN1	None	Link-Local
2	wan2	true		Disable	11	0	WAN2	Static	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 Basic Mode

Web Page in Advance Mode

	🚯 Add	🔀 Edit	🔟 Delete	🗳 Refr	resh Moo	de :	Advance	~	Profile
	Profile (m	Enable	Descriptio	VLAN Tag	VLAN ID	Pri	Basic Advance		Pv6 Pro
1	wan1	false		Disable	10	0	WAN1	None	Link-Loca
2	wan2	true		Disable	11	0	WAN2	Static	Link-Loca
3	wan3	false		Disable	12	0	WAN3	None	Link-Loca
4	wan4	false		Disable	13	0	WAN4	None	Link-Loca
5	wan5	false		Disable	14	0	WAN5	None	Link-Loca

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 <b>Edit</b> 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	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, <b>Enable</b> will be displayed in this field. Otherwise, <b>Disable</b> will be shown instead.
VLAN ID	Display the VLAN ID of the profile.
Priority	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.

🔀 Edit	< Refresh	Mode :	Basic	~	
Profile	Enable This P	Descript	Basic		Unt

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

Confirm		3
•	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.

ieral Setup								
Global	PPTP	Static	DHCP	PPPoE	StaticV6	DHCPV6	DMZ	
Profile (ma	x length:7) :							
Enable								
Description	d.			(Optional)				
VLAN Tag :		Disable		*				
VLAN ID :		0						
Priority :		0		~				
Port :		WAN1		*				
Default MA	C Address :	💽 Enabl	e 🔿 Disable					
MAC Addre	SS :	00 :	50 : 7f	: 7f : fc	: e9			
IPv4 Protoc	ol :	None		*				
IPv4 Mode :		NAT		~				
IPv6 Protoc	ol :	Link-Loca	al	*				
Enable Sch	edule Reconne	ect: OEnabl	e 💿 Disable					
								💾 Apply 🛛 🔞 Can

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 <b>Enable</b> to tag the packets passing through the port specified below.
VLAN ID	Type the VLAN ID number for such profile.
Priority	Type the packet priority number for such VLAN. The range is from 0 to 7.
Port	Choose the physical WAN interface for such profile. WAN1 WAN1 WAN2 WAN3 WAN4 WAN5
Default MAC Address	<ul> <li>Enable – Click it to enable the default MAC address for such profile.</li> <li>Disable – Click it to type the MAC address manually for such profile.</li> </ul>
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. None Static DHCP PPPoE PPTP DMZ The DMZ protocol is available for WAN4 profile only.
IPv4 Mode	Determine such profile will be used for. ROUTING NAT ROUTING

IPv6 Protocol	There are four connection modes for you to specify for IPv6 protocol type. Each mode will bring up different web page.
Enable Schedule Reconnect	<ul> <li>Enable – Click it to enable the function of reconnecting the network automatically within the time schedule.</li> <li>Disable – Click it to disable the schedule reconnect function.</li> </ul>
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:

eral Setup						
Global PPTP	Static DHCP	PPPoE	StaticV6	DHCPV6	DMZ	
IP Address :						
Subnet Mask :	255.255.255.0/24	~				
Gateway IP Address :		. n	(Optional)			
	🚯 Add  🗎 Save					Profile Number Lin
	DNS Server IP Add	ress				
DNS Server IP Address :			No ite	ms to show.		
	🕼 Add  Save					Profile Number Lir
	IP					
IP Alias :			No ite	ms to show.		
						💾 Apply 🛛 🚱 Ca

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 (Doma Server). To add a new IP address, simply place the m cursor on this filed. The following dialog will appear						
		🚯 Add 💾 Save					
		DNS Server IP Address					
		168.95.1.1	m				
	DNS Server IP Address :						
	Add – click this b address.	utton to have a field	d for adding a new IP				
	Save – click this b	utton to save the se	etting.				
	$\mathbf{\hat{m}}$ – click the ico	n to remove the sel	ected entry.				
IP Alias	setting is optional. see and choose it i	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).					
	box near to the Ad	To add a new IP address, simply type the IP address on the box near to the <b>Add</b> button. Next, click <b>Add</b> . The new one will be added and displayed on the field under the box.					
		🚯 Add 🔚 Save					
		IP	Subnet Mask				
		192.168.1.85	255.255.255.0				
	IP Alias :						
	<b>Add</b> – click this button to have a field for adding a new IP address.						
	<b>Save</b> – Click this button to save the setting.						
	i – click the ico	n to remove the sel	ected entry.				
MTU/MRU	Type the value of	MTU/MRU. The d	lefault value is 1500.				
Connection Detection Mode	three ways ARP,		N interface. There are supported in Vigor request out.				
	HTTP						
Connection Detection Host	detected whether router) or not. If r	the host is active (s	ne as a destination to be sending reply to the of WAN interface will function is available				



	when <b>Connection HTTP</b> .	<b>Detection Mode</b> is set with <b>PING</b> or		
	Connection Detection Mode :	PING		
		🕼 Add  🛗 Save		
	Connection Detection Host :	Connection Detection Host 192.168.1.28		
	Connection Detection Interva	- 40		
	Add – click this bu address.	atton to have a field for adding a new IP		
	<b>Save</b> – click this button to save the setting.			
	$\mathbf{\hat{m}}$ – click the icon	n 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:

eneral Setup	onoral Cotun 55 Conoral Cotun	(
Global PPTP S	tatic DHCP PPPoE StaticV6 DHCPV6 DI	MZ
Host Name :	(Optional)	
	🕼 Add  🗎 Save	Profile Number Lim
	IP	
IP Alias :	No items to show.	
MTU/MRU:	1500	
Connection Detection Mode :	ARP	
Connection Detection Interval	10	
Connection Detection Retry :	3	
Vendor Class ID (option 60) :	(Optional)	
	(Optional)	
DHCP Client ID (option 61)		
DHCP Client ID (option 61) : Specify DNS :	○ Enable    Oisable	
	C Enable ③ Disable	

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 <b>Add.</b> Type the IP address and use the drop down list to specify the subnet mask. Next, click <b>Save</b> . The new one will be added and displayed on the field under the box.					
	🕼 Add 💾 Save					
	IP Subnet Mask					
	192.168.1.86 255.255.255.0					
	<ul> <li>Add – click this button to have a field for adding a new IP address.</li> <li>Save – click this button to save the setting.</li> </ul>					
	$\mathbf{I}$ – 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 <b>ARP</b> , <b>PING</b> and <b>HTTP</b> supported in Vigor router for you to choose to send the request out. PING 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 <b>Connection Detection Mode</b> is set with <b>PING</b> or <b>HTTP</b> .					
	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.	
	<b>Save</b> – click this button to save the setting.	
	$\mathbf{I}$ – 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	<b>Enable</b> – 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.	
	<b>Disable</b> – Click it to disable the function of DNS specified.	
DNS	<b>Add</b> – click this button to have a field for adding a new IP address.	
	<b>Save</b> – click this button to save the setting.	
	$\mathbf{I}$ – 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:

eral Setup	- Conoral Satur 55 Conoral	Satur				
Global PPTP	Static DHCP	PPPoE	StaticV6	DHCPV6	DMZ	
		-				
Username :						
Password						
MTU/MRU:	1492					
Service Name :		(Optional)				
Debug :	🔵 Enable 💿 Disable					
Always On :	💿 Enable i 🔘 Disable					
Fixed IP :	🔵 Enable 💿 Disable					
Connection Detection Mode	None 🗸					
	🚯 Add  💾 Save					Profile Number Limit
	IP					
IP Alias :			No iten	ns to show.		
Specify DNS	← Fnable 💿 Disable					
		111				

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 <b>Enable</b> to display the PPPoE debug message in Syslog. The default setting is <b>Disable</b> .
Always On	<ul> <li>Enable – Click it to enable the function of Always On. The router will keep network connection all the time.</li> <li>Disable – Click it to disable the function of Always On.</li> </ul>
Fixed IP	<b>Enable</b> – Click it to enable the function of fixed IP. <b>Disable</b> – 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 <b>PING</b> and <b>HTTP</b> 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 <b>host address</b> in this field. Use the default setting.



Specify DNS       Add - click this button to have a field for adding a new IP address.         Save - click this button to save the setting.       Image: 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. After passing the times you set in this field and no reply received by the router, the connection of WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN 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 Alias       Add - click this button to have a field for adding a new IP address.         Save -click this button to save the setting.       Image: Save - Click this button to have a field for adding a new IP address.         Save -click this button to save the setting.       Image: Save - Click this button to save the setting.         Image: Save - click this button to save the setting.       Image: Save - Click this button to save the setting.         Image: Save - click this button to save the setting.       Image: Save - Click this button to save the setting.         Image: Save - Click this button to save the setting.       Image: Save - Click this button to save the setting.         Image: Save - Click this button to save the setting.       Image: Click this button to save the set		Connection Detection Mode :	PING 👻			
Connection Detection Hest       Image: Detection Hest         Image: Detection Detection Hest       Image: Detection Hest         Add - click this button to have a field for adding a new IP address.         Save - click this button to save the setting.         Image: Detection Interval         Assign an interval period of time for each detecting.         Detection Interval         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.         Image: I						
Add - click this button to have a field for adding a new IP address.         Save - click this button to save the setting.         Image: click this button to save the setting.         Image: click this button to remove the selected entry.         Connection Detection Interval         Assign an interval period of time for each detecting.         Connection Detection Interval         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.         Image: Image: Image: Image: Image: Image set image:						
address.         Save - click this button to save the setting.         Image: - click the icon to remove the selected entry.         Connection Detection Interval         Connection Detection Retry         Image: - click the icon to remove the selected entry.         Assign an interval period of time for each detecting.         Detection Retry         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.         Image:		Connection Detection Host :	192.168.1.28			
address.         Save - click this button to save the setting.         Image: - click the icon to remove the selected entry.         Connection Detection Interval         Connection Detection Retry         Image: - click the icon to remove the selected entry.         Assign an interval period of time for each detecting.         Detection Retry         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.         Image:						
address.         Save - click this button to save the setting.         Image: - click the icon to remove the selected entry.         Connection Detection Interval         Connection Detection Retry         Image: - click the icon to remove the selected entry.         Assign an interval period of time for each detecting.         Detection Retry         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.         Image:						
Image: Connection Detection Interval- click the icon to remove the selected entry.Connection Detection IntervalAssign an interval period of time for each detecting.Connection Detection RetryAssign 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 AliasType 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.Image: Add I image: Add I image		ç				
Connection Detection IntervalAssign an interval period of time for each detecting.Connection Detection RetryAssign 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 AliasType 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 AliasAdd = click this button to have a field for adding a new IP address. Save -click this button to save the setting.IP address.Save IP		Save – click this but	tton to save the setting.			
Detection IntervalAssign 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 AliasType 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.Image: Add Image: Subnet MaskImage: Subnet Mask192.168.1.86255.255.255.0255.255.255.0Image: Subnet Mask192.168.1.86255.255.255.0Image: Subnet MaskImage: Subnet MaskImage: Click this button to have a field for adding a new IP address.Save - click this button to save the setting.Image: Click the icon to remove the selected entry.Specify DNSEnable - 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.		<b>*</b>				
Detection Retry       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.         Image: Add Image: Save Image: Submet Mask Image: Submet Mask Image: Submet Mask Image: Save Image: Submet Mask Image: Save Image						
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.         Image: Add Image:		interface. After passing the times you set in this field and no reply received by the router, the connection of WAN				
Add       Save         P       Subnet Mask         192.168.1.86       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.         Image: Click this button 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.	IP Ahas	<ul> <li>setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., NAT&gt;&gt;Port Redirection/DMZ Host).</li> <li>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</li> </ul>				
P       Subnet Mask         192.168.1.86       255.255.255.0         192.168.1.86       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.         Image: - 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.						
192.168.1.86       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.         Image: - 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.		🏠 Add 💾 Save				
Add – click this button to have a field for adding a new IP address.         Save –click this button to save the setting.         Image: 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.		IP	Subnet Mask			
address.         Save –click this button to save the setting.         im       – 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.		192.168.1.86	255.255.255.0 💼			
Save –click this button to save the setting.         Image: provide the setting of the setting of the set of						
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.			ton to have a field for adding a new IP			
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.		address.				
Specify DNSEnable – 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.		address. <b>Save</b> –click this but				
<b>DNS</b> Add – click this button to have a field for adding a new IP		address. Save –click this but	ton to save the setting.			
	Specify DNS	address. <b>Save</b> –click this butt — click the icon Enable – Click it to It is used for local se used for forwarding	ton to save the setting. to remove the selected entry. enable the function of DNS specified. ervice (e.g., NTP, ping diagnostic) or packets to PC on LAN/VPN.			

	address.
	<b>Save</b> – click this button to save the setting.
	$\mathbf{I}$ – 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:

neral Setup			atun >> Gana					
Global	PPTP	Static	DHCP	PPPOE	StaticV6	DHCPV6	DMZ	
PPTP Over		Static		~				
Server Add	lress :	0.0.0.0						
Username	:							
Password	:							
MTU/MRU :		1452						
Debug :		⊖ Ena	ble 💿 Disab	le				
Always On	:	💿 Ena	ble 🔿 Disab	le				
Connection	n Detection Mode	: HTTP		*				
		🚯 Ad	d 💾 Save					Profile Number Lir
		Conne	ction Detectio	on Host				
Connection	n Detection Host :				No ite	ms to show.		
	n Detection Interv							
Composition								

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. <b>Please contact your ISP</b> <b>before you want to use this function.</b> Choose a proper protocol, <b>Static</b> or <b>DHCP</b> .
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 <b>Enable</b> to display the PPTP debug message in syslog. The default setting is <b>Disable</b> .
Always On	<ul> <li>Enable – Click it to enable the function of Always On. The router will keep network connection all the time.</li> <li>Disable – Click it to disable the function of Always On.</li> </ul>
Connection	Select a detecting mode for this WAN interface. There are



Detection Mode	two ways <b>PING</b> and <b>HTTP</b> 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 <b>host address</b> 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. Detection 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 <b>Static</b> or <b>DHCP</b> (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:

neral Setup							_×
Global	PPTP	Static	DHCP	PPPoE	StaticV6	DHCPV6	DMZ
IPv6 Addre							
IPv6 Prefix							
	ay Address :			(Optional	I)		
		🚯 Add 📘	Save				Profile
		IPv6 DNS Set	rver Address				
IPv6 DNS S	erver Address :				No items to s	show.	
							2

Item Description **IPv6 Address** Type the IP address for such protocol. **IPv6 Prefix Length** Type your IPv6 address prefix length. **IPv6** Gateway Type your IPv6 gateway address. Address **IPv6 DNS Server** Type your IPv6 primary DNS Server address. Address IPv6 Gateway Address : (Optional) 🚯 Add 💾 Save IPv6 DNS Server Address 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. Ш – 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:

eral Setup									-
Global	PPTP	Stati	ic	DHCP	PPPoE	StaticV6	DHCPV6	DMZ	
		г				<b>-</b>			
DHCPv6(IA	_NA) Gateway A	ddress :				(Optional)			
			🚯 Add	📑 Save					
			DHCPv6	(IA_NA) DNS	Address				
DHCPv6(IA	_NA) DNS Addre	SS :				No it	ems to show.		
		L							
				111					
							Ap	oply 🙆 Ca	

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. <b>Add</b> – click this button to have a field for adding a new IP address.
	<ul> <li>Save – click this button to save the setting.</li> <li>— click the icon to remove the selected entry.</li> </ul>
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.

Ge	eneral Setup	USB WA	N						
	🚯 Add	🗶 Edit	<u> I</u> Delete	🦃 Refree	sh Mode :	Advance		*	Profile Number Lir
	Profile (m	Enable	Descriptio	VLAN Tag	VLAN ID	Priority	Port	IPv4 Proto	IPv6 Protoc
1	wan1	false		Disable	10	0	WAN1	None	Link-Local
2	wan2	true		Disable	11	0	WAN2	Static	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
6	market	true	marketing	Enable	250	0	WAN1	Static	Link-Local

# 4.1.1.2 USB WAN Profiles

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

🔀 Edit 🗳	5 Refresh				
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 <b>Edit</b> 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.

General Setup	USB WAN	
🔀 Edit	🗳 Refresh	
Profile	Enable	Description
usb1	false	
usb2	false	

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

USB WAN					- ×
Global	USB 3G				
Profile :	usb1				
Description		(Optional)			
Port :	USB1				
Protocol :	3G 🗸				
1					
1					
1					
		\$	🕻 Default  🗎	Apply 🧯	Cancel

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					_ ×
Global USB 3G					
1					
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)			
			Doferit	Annte:	Opport
				Apply	🔇 Cancel

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).
<b>PPP Password</b>	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.

General Setup	USB WAN			
🔀 Edit	📢 Refresh			
Profile	Enable	Description	Port	Protocol
Profile usb1	Enable true	Description for test	USB1	Protocol 3G

#### 4.1.2 Default Route

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

<b>Dray</b> Tek	Vigor 3900 Series	16:20:24	Login: Admin	E
	WAN >> Default Route			
Auto Logout : 5Min 🗸	Default Route			
Quick Start Wizard				
Online Status	WAN Profile/Loadbalance Pool Name	; wan1 🗸		
WAN				
General Setup	Auto Failover to Active WANs :	Enable Oisable		
Default Route				
Load Balance				
Switch				
LAN				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				
USB Application			Apply	🐼 Cancel
System Maintenance 📃 💽				

Item	Description
WAN Profile /Load Balance Pool	Display the WAN profiles for user to choose as a default route.
Name	In which, wan1 to wan5 are factory default settings.
Auto Failover to Active WANs	<b>Enable</b> – Check it to let the network connection being established through any active WAN interface.
	<b>Disable</b> – 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 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:

Dray Tek	Vigor 3900 Series	16:27:57	Login: Admin 🕞
	WAN >> Load Balance >> Rule		
Logout Shim Y	Pool Rule intound Load Balance		
Duick Start Wizard			Profile Number
Online Status	🕼 Add 💥 Eldt 🏢 Delete 🖙 Refresh 🧣 Move Up 🦉 Move Down 🔓 Rename		
NAIL	Profile Enable Protoci Addres Source Source Destina Destina Source IP Address	Destination IP Address	Destina Destina Load B. Auto Fai
General Setup	fin items to show		
Default Route			
Load Balance			
Switch			
AR			
TAT			
In Contail			
objects Seming			
user Management			
Applications			
VPH and Remote Access			
Certificate Management			
SSL VPN			
Central VPN Management			
Jandwidth Management			
ISB Application			
System Maintenance			
Diagnostics			
External Devices			
Product Registration			
	(e) m		

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 <b>Edit</b> 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 <b>Delete</b> 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 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.
<b>Destination IP Group</b>	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.
<b>Destination Port Start</b>	Display the starting port value for the destination.
<b>Destination Port End</b>	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.

W	AN >> Load Ba	lance >> Ru	lle				
	Pool	Rule	Int	bound Loa	d Balance		
	🚯 Add	🔀 Edit	🔟 De	elete 🗳	5 Refresh	<u></u>	M
	Profile	Enable	Protoco	Address	Source IF	o Obje	So

3. The following dialog will appear.

	-
	=
Test111	
ALL	*
Subnet	*
	. (Option:
255.255.255.0/24	🗸 (Optional)
	. (Option:
255.255.255.0/24	<ul> <li>(Optional)</li> </ul>
:	🗸 (Must have value)
💿 Enable 🔵 Disa	ble
🔵 Enable 💿 Disa	ble
	📑 Apply 🛛 🚳 Cancel
	ALL Subnet 255.255.255.0/24 255.255.255.0/24 255.255.255.0/24

Item	Description	
Profile	Type the name of the rule.	
Enable	Check this box to enable st	uch profile.
Protocol	· · · ·	TCP, UDP, ICMP, FTP, TFTP, P/UDP) for such rule applied to Fault setting.
Address Type		Subnet or Object) for such rule. ent settings for configuration.
	source IP address for such — click the icon to cl Source Mask - Use the dro a suitable mask for the sou	lear the IP setting. op down list on the right to choose
	Source Mask :	255.255.255.0 <b>v</b> (C
	Destination IP Address :	255.255.255.0 255.255.254.0 255.255.00 255.254.0.0 0.0.0.0
	Destination Mask :	128.0.0.0 😑 (0
	the destination IP address f	Type a WAN IP address here as for such rule. lear the IP setting.
		ieur the fr setting.



	choose a suitable mask for the dest	tination.
Object	<b>Source IP Object</b> – Use the drop the source IP objects for such rule	
	<b>Source IP Group</b> –Use the drop d	-
	the source IP group for such rule p	
	<b>Destination IP Object</b> – Use the of one of the destination IP objects for	*
	<b>Destination IP Group -</b> Use the d one of the destination IP group for	-
	Address Type : Object	~
	Source IP Object :	🗸 🗙 (Optional)
	Source IP Group :	🗸 🗙 (Optional)
	Destination IP Object :	🗸 🗙 (Optional)
	Destination IP Group :	👻 🗙 (Optional)
	<ul><li>page also will be displayed here.</li><li>To have user-defined WAN profile</li></ul>	e, please refer to
		ed information.
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>wan1</th></general>	wan1
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>ed information.</th></general>	ed information.
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>wan1</th></general>	wan1
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>ed information. wan1 wan2 wan3</th></general>	ed information. wan1 wan2 wan3
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>ed information.</th></general>	ed information.
	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>ed information. wan1 wan2 wan3 wan4 wan5</th></general>	ed information. wan1 wan2 wan3 wan4 wan5
Failover to the Default Route	To have user-defined WAN profile WAN< <general detaile<="" for="" setup="" th=""><th>ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason,</th></general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason,
	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, e to perform data
	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, to perform data unction.
	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, e to perform data unction. function. function. onnects, the traffic via other diately. The router will use
Default Route	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile When the specified interface disco the router can use the default route transmission. Enable – Click it to enable such fu Disable – Click it to disable such fu</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, e to perform data unction. function. function. onnects, the traffic via other diately. The router will use nsmission again.
Default Route	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile When the specified interface disco the router can use the default route transmission. Enable – Click it to enable such for Disable – Click it to disable such for When the specified interface re-co interface will be interrupted immed the specified interface for data transit</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, e to perform data unction. function. function. function. onnects, the traffic via other diately. The router will use assmission again. unction.
Default Route	To have user-defined WAN profile WAN< <general details<br="" for="" setup="">Load Balance Pool/WAN Profile When the specified interface disco the router can use the default route transmission. Enable – Click it to enable such fu Disable – Click it to disable such fu When the specified interface re-co interface will be interrupted immed the specified interface for data tran Enable – Click it to enable such fu</general>	ed information. wan1 wan2 wan3 wan4 wan5 usb3g1 usb3g2 onnects due to some reason, e to perform data unction. function. function. function. onnects, the traffic via other diately. The router will use assmission again. unction.

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



# 4.1.3.2 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.

<b>Dray</b> Tek	Vigor 3900 Series	16:24:37	Login: Admin	•
	WAN >> Load Balance >> Pool			
Auto Logout : 5Min 👻	Pool Rule Inbound Loa	d Balance		
Quick Start Wizard * Online Status	🏠 Add 💥 Edit 🏢 Delete 🗳	Refresh		Profile
WAN	Profile Mode	Interface Pr	imary Profile Backup Profile	
General Setup		No items to show.		
Default Route				
Load Balance				
Switch				
LAN				
NAI				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				
USB Application				1.1
System Maintenance		m		100

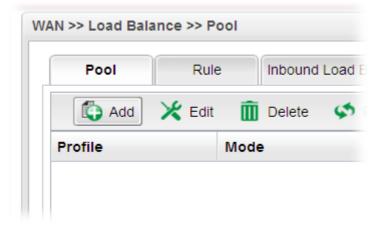
Each item will be explained as follows:

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 <b>Edit</b> 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 <b>Delete</b> 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.



2. Simply click the **Add** button to open the following dialog. Type a name (e.g., LB\_1) for such profile.

Profile :	LB_1	
Mode :	Load_Balance 👻	
	🕼 Add   Save	Profile Number Limit :
	Interface	Weight
Interface :	wan1 🗸	80

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

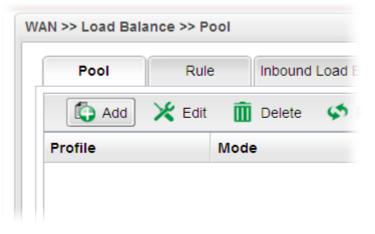
3. Click **Apply**. A new profile will be added on the page.

Pool F	Rule Inbound Load Balar	nce		
🖏 Add 🛛 🗶	Edit 👖 Delete 🛭 娕 Refre	esh		Profile Number Limit : 1
Profile	Mode	Interface	Primary Profile	Backup Profile
LB_1	Load_Balance	wan1 80		

#### 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.



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.

ol			
Profile :			
Mode :	Failover 👻		
Primary Profile :	Load_Balance		
Primary Profile : Backup Profile :	Failover		
			-
		💾 Apply	🥝 Canc

Item	Description
Profile	Type the name of the profile.
Mode	Choose <b>Failover</b> as the <b>Mode</b> 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.

<b>Backup Profile</b>	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.

Pool F	Rule Inbound Load Bala	nce		
🕼 Add 🔀 Edit 🏢 Delete 🤝 Refresh Profile Number Limit				
Profile	Mode	Interface	Primary Profile	Backup Profile
LB_1	Load_Balance	wan1 80		
FL_1	Failover		wan1	wan2

## 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.

Status         Domain Name         Mode         IP Mapping         Weight         Alias Interface         IP           Image: true         www.draytek.co         Failover         wan3,wan2         3,1         (none)         192.168.3	Alias Weight
true www.draytek.co Failover wan3,wan2 3,1 (none) 192.168.3	3.12 1

Item	Description
Status	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 <b>Edit</b> 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.
Status	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**.

Pool	Rule	Inbound Loa	ad Balance	
1 001	T Caro			
V Status		Add 🔀 Ed	dit 🛅 Delete	e 🗳 Refres
Status	Domain	Name Mode	IP Mapp	ing Weight
			No it	ems to show

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

Basic Detail				
<b></b>				
Domain Name :	www.draytek.com			
Mode :	💿 Load Balance 🔘	Failover		
	🕼 Add  🛗 Save		Profile N	lumber Limit : 16
	IP Mapping	Weight		
Interface Mapping/Weight :	· · · -	1		ŵ
	🕼 Add  🛗 Save 🗛			
	Alias Interface (none)	Alias 192.168.1.133	Weight 2	Ŵ
Alias Setting :	Alias Interface	Alias	Weight	Ŵ

Item	Description				
Status	Check this box to enal	ble such profile.			
Domain Name	Type an available don balance.	nain name to serve the inbound load			
Mode	Specify the type (Load profile for inbound load	l Balance or Failover) of the WAN ad balance			
Priority Setting	It is available only when Failover is selected as the Mode. There are five levels (Top, 2, 3, 4 and 5) which can be specified for WAN profiles (including default WAN profiles and user-defined WAN profiles).				
	Interface Priority				
	wan1	3			
	wan2	3			
	wan3	Тор			
	wan4	2 3 =			
	wan5	4			
	usb1	3 			
	usb2	3			
	extern	3			
	🕼 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 Mapping will be processed according to the weight value.				
	Add – Click it to choo	se a WAN interface and weight.			
	Save – Click it to save	the settings.			
		e drop down list to choose a WAN a will be used by the domain.			
	Weight – Use the drop	o down list to choose the one you want.			



	$\mathbf{I}$ – 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.
	<b>Save</b> – 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.
	$\mathbf{I}$ – 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.

Basic	Detail						
		– DNS Parameters –					
		TTL:	1800				
		Refresh:	900				
DNS Para	meter	Retry :	450				
billo i dit		Expire :	604800				
		Nagative Cache TTL :	1800				
		Email :					
		🕼 Add  Save				Profile Number Limit : 16	ì
		HOST	Name	e Server	IP Address		
NS Recor	rd :			No items to st	10W.		
		🕼 Add 📙 Save				Profile Number Limit : 16	- ì
		Host Ma	il Server	IP Address		Preference	
		1					🖞 Apply 🔞 Ca

Item	Description
<b>DNS Parameter</b>	To configure Vigor router as a DNS server, type the related information for applying the function of DNS.
	<b>TTL</b> – It means Time to live of a DNS response. Available setting range is from 0 to 2147483647.
	<b>Refresh</b> – 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

Expire – PC stops responding to the query from Vigor route 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 RecordThis 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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.MX RecordThis is used to specify the mail server with IP address. Add – Click it to add a new server with specified name and I address.MX RecordThis is used to specify the mail server. IP Address – Type the name (URL) of the mail server. IP Address.Add – Click it to save the settings. Host – Type the name (URL) of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address. Add –Click it to add a new host with specified IP address. Save – 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. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail serv		
when such time setting has expired.Nagative Cache TTL – Set the negative caching time (namerror).Email – Type the e-mail address of the administrator.NS RecordThis 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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.III – click the icon to remove the selected entry.MX RecordMX RecordAdd –Click it to save the settings.Host – Type the name (URL) of the mail server.III – click the icon to remove the selected entry.MA address – Type the IP address of the mail server.III – click the icon to remove the selected entry.Mail Server – Type the name (URL) of the mail server.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to remove the selected entry.IIII – click the icon to r		Vigor router before the refreshing expired.
error).Email – Type the e-mail address of the administrator.NS RecordThis 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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.III – click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address.Add –Click it to save the settings.Host –Type the name (URL) of the mail server.III – click the icon to remove the selected entry.MX RecordAdditional A RecordRecordAddress – Type the IP address of the mail server.II is used to record the DNS query by IPv4 address.Save – Click it to save the settings.Host –Type the it on the mail server.III = click the icon to remove the selected entry.Additional A RecordRecordAddress – Type the IP address of the mail server.III = click the icon to remove the selected entry.Add –Click it to save the settings.Host –Stet a domain name.IP Address – Type the IP address of the mail server.III = click the icon to remove the selected entry.Add –Click it to save the settings.Host –Set a domain name.		
NS RecordThis 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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.Image: - click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address.Add - Click it to save the settings.Host - Type the name (URL) of the mail server.Im - click the icon to remove the selected entry.Mail Server - Type the name (URL) of the mail server.Im Address - Type the name (URL) of the mail server.Im Address - Type the name (URL) of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im Address - Type the IP address of the mail server.Im 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.Im - Click the icon to remove the selected entry.Im Address - Type the IP address of the mail server. <th></th> <th><b>Nagative Cache TTL</b> – Set the negative caching time (name error).</th>		<b>Nagative Cache TTL</b> – Set the negative caching time (name error).
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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.Im - click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address. Add -Click it to save the settings.Host -Type the name (URL) of the mail server. IP Address - Type the IP address of the mail server.Mail Server - Type the IP address of the mail server.Mail Server - Type the IP address of the mail server.IP Address - Type the IP address of the mail server.Im - click the icon to remove the selected entry.Add -Click it to save the settings.Host -Type the name (URL) of the mail server.Im - click the icon to remove the selected entry.Additional A RecordIt is used to record the DNS query by IPv4 address.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.Im - Click the icon to remove the selected entry.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.Im - Click the icon to remove the selected entry.Im - Click the icon to remove the selected entry. <th></th> <th><b>Email</b> – Type the e-mail address of the administrator.</th>		<b>Email</b> – Type the e-mail address of the administrator.
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 th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.III – click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address. Add –Click it to add a new server with specified name and 1 address.Save – Click it to save the settings. Host –Type the name (URL) of the mail server. III – click the icon to remove the selected entry.Additional A RecordAdditional A RecordIt is used to record the DNS query by IPv4 address. Add –Click it to save the settings. Host –Type the IP address of the mail server. III – click the icon to remove the selected entry.Additional A RecordIt is used to record the DNS query by IPv4 address. Save – Click it to save the settings. Host –Set a domain name. IP Address – Type the IP address of the mail server. III – Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.	NS Record	This page is used to specify name server which will be used as DNS server.
HOST – Type the domain name of the server. This is optional. If no information added here, the router will use th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.MX RecordThis is used to specify the mail server with IP address. Add –Click it to add a new server with specified name and I 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. IP Address – Type the IP address of the mail server.Additional A RecordIt is used to record the DNS query by IPv4 address. Save – Click it to save the settings. Host –Set a domain name. IP Address – Type the IP address of the mail server. IP -Click the icon to remove the selected entry.Addational A RecordIt is used to record the DNS query by IPv4 address. Save – Click it to save the settings. Host –Set a domain name. IP Address – Type the IP address of the mail server. III – Click the icon to remove the selected entry.		-
optional. If no information added here, the router will use th DNS server configured in Domain Name under the Basic tal 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 I address of the NS record server.MX RecordThis is used to specify the mail server with IP address. Add –Click it to add a new server with specified name and I address.Save – Click it to save the settings. Host –Type the name (URL) of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server. IP Address – Type the IP address of the mail server.AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>Save</b> – Click it to save the settings.
will be used to receive the DNS query forwarded by HOST.IP Address – This is optional. If required, simply type the I address of the NS record server.III – click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address.Add –Click it to add a new server with specified name and I 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.III – click the icon to remove the selected entry.Additional A RecordRecordIt is used to record the DNS query by IPv4 address.Save – Click it to save the settings.Host –Set a domain name.IP Address – Type the IP address of the mail server.III – click the icon to remove the selected entry.Add –Click it to save the settings.Host –Set a domain name.IP Address – Type the IP address of the mail server.III – Click the icon to remove the selected entry.III is used to record the DNS query by IPv6 address.		<b>HOST</b> – 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.
address of the NS record server.Im- click the icon to remove the selected entry.MX RecordThis is used to specify the mail server with IP address.Add -Click it to add a new server with specified name and 1 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.IP Address - Type the IP address of the mail server.Im- click the icon to remove the selected entry.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.Im- Click the icon to remove the selected entry.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.Im- Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>Name Server</b> – Type the URL for the name server which will be used to receive the DNS query forwarded by HOST.
MX RecordThis is used to specify the mail server with IP address.Add -Click it to add a new server with specified name and 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.im - click the icon to remove the selected entry.Add -Click it to save the settings.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.im - Click the icon to remove the selected entry.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.im - Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>IP</b> Address – This is optional. If required, simply type the IP address of the NS record server.
MX RecordThis is used to specify the mail server with IP address.Add -Click it to add a new server with specified name and 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.im - click the icon to remove the selected entry.Add -Click it to save the settings.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.im - Click the icon to remove the selected entry.Add -Click it to save the settings.Host -Set a domain name.IP Address - Type the IP address of the mail server.im - Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		$\square$ – click the icon to remove the selected entry.
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.II - click the icon to remove the selected entry.Additional A RecordRecordIt is used to record the DNS query by IPv4 address.Save - 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.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Click the icon to remove the selected entry.II - Sel - S	MX Record	
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.ID – click the icon to remove the selected entry.Additional A RecordRecordIt 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.ID – Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		Add –Click it to add a new server with specified name and IP address.
Mail Server – Type the name (URL) of the mail server.IP Address – Type the IP address of the mail server.IP Address – Type the IP address of the mail server.II - click the icon to remove the selected entry.Additional A RecordIt 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.IIP Address – Type the IP address of the mail server.III – Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>Save</b> – Click it to save the settings.
IP Address – Type the IP address of the mail server.Image: click the icon to remove the selected entry.Additional A RecordIt 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.Image: click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		Host –Type the name (URL) of the mail server.
Additional A RecordIt 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.Image: Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		Mail Server – Type the name (URL) of the mail server.
Additional A RecordIt 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.IIIP Address – Type the IP address of the mail server.IIII– Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>IP</b> Address – Type the IP address of the mail server.
RecordAdd -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.Image: Add -Click it to save the settings. Host -Set a domain name. IP Address - Type the IP address of the mail server. Image: -Click the icon to remove the selected entry.AAAA RecordIt is used to record the DNS query by IPv6 address.		$\square$ – click the icon to remove the selected entry.
Add -Click it to add a new nost with specified if address.         Save - Click it to save the settings.         Host -Set a domain name.         IP Address - Type the IP address of the mail server.         Image: - Click the icon to remove the selected entry.         AAAA Record         It is used to record the DNS query by IPv6 address.	Additional A	It is used to record the DNS query by IPv4 address.
Host –Set a domain name.         IP Address – Type the IP address of the mail server.         Image: - Click the icon to remove the selected entry.         AAAA Record         It is used to record the DNS query by IPv6 address.	Record	Add –Click it to add a new host with specified IP address.
IP Address – Type the IP address of the mail server.         Image: - Click the icon to remove the selected entry.         AAAA Record       It is used to record the DNS query by IPv6 address.		<b>Save</b> – Click it to save the settings.
Image: Click the icon to remove the selected entry.         AAAA Record       It is used to record the DNS query by IPv6 address.		Host –Set a domain name.
AAAA RecordIt is used to record the DNS query by IPv6 address.		<b>IP</b> Address – Type the IP address of the mail server.
		Image: Description of the selected entry.
Add –Click it to add a new host with specified IPv6 address	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.
<b>Save</b> – Click it to save the settings.		<b>Save</b> – Click it to save the settings.
Host – Set a domain name.		Host – Set a domain name.
<b>IPv6 Address</b> – Type the IPv6 address of the host.		IPv6 Address – Type the IPv6 address of the host.
Any query concerning of Host will be forwarded to the serv selected in Reference for advanced process.		Any query concerning of Host will be forwarded to the server selected in Reference for advanced process.
$\mathbf{I}$ – Click the icon to remove the selected entry.		— Click the icon to remove the selected entry.
<b>CNAME Record</b> It is used to record the DNS query for CNAME.	CNAME Record	It is used to record the DNS query for CNAME.
Add – Click it to add a new host with specified reference.		



<b>Save</b> – Click it to save the settings.
Host – Set a domain name.
<b>Reference</b> – 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.
$\mathbf{I}$ – Click the icon to remove the selected entry.

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

	Status	🚯 Add	🔀 Edit	前 Delete 🕻	🔊 Refresh		Profile	e Number Limit : 1
	Status	Domain Name	Mode	IP Mapping	Weight	Alias Interfac	IP	Alias Weight
₽	true	www.draytek.com	Failover	wan3,wan2	3,1	(none)	192.168.3.12	1

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

Status	🚺 Add	🔀 Edit		🔟 Delete	- 9	nefres 🔊	h	
Status	Domain Name	Mode		IP Mappi	ng	Weight		AI
true	www.draytek.com	Failover		wan3,wan2	2	3,1		(no
🚯 Add	🔀 Edit 🧃	Delete	ø	Refresh				
Status	Sub Domain	Node	IP I	Mapping	Wei	ght	Alias	In
				No iten	ns 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.

<b>Dray</b> Tek	Vigor 390	0 Series 15:32:52	Login: Admin	Ð
	WAN >> Switch >> 802.1Q	VLAN		
Auto Logout : Off 🛛 🗸	802.1Q VLAN Mi	rror Interface Status		
Quick Start Wizard				
Online Status	C Refresh			
WAN	VLAN ID	Member	Untag	
General Setup	10	WAN1		
Default Route	11	WAN2	WAN2	
Load Balance	12	WAN3	WAN3	
Switch	13	WAN4	WAN4	
LAN	14	WAN5	WAN5	
NAT	22	WAN1	WAN1	
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
System Maintenance				
Disenseties				

## 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.

02.1Q VLAN Min	ror Interface Status		
< Refresh			
/LAN ID	Member	Untag	
0	CPU,WAN1	WAN1	
1	CPU,WAN2	WAN2	
2	CPU,WAN3	VVAN3	
3	CPU,WAN4	VVAN4	
4	CPU,WAN5	VVAN5	



Item	Description
Refresh	Click it to reload this page.
VLAN ID	Display the VLAN ID number.
Member	Display <b>number</b> of the WAN interface for the packets tagged with such VLAN ID number to pass through.
Untag	Display <b>number</b> 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.

<b>Dray</b> Tek	Vigor 3900 Series	15:34:49	Login: Admin	Ð
	WAN >> Switch >> Mirror			
uto Logout : Off 🛛 👻	802.1Q VLAN Mirror Interface	Status		
Quick Start Wizard				
Online Status	Enable This Profile			
WAN				
General Setup		~		
Default Route	Mirrored Port : WAN2	*		
Load Balance				
second Switch second second second				
LAN				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management			Apply	🐼 Cancel
System Maintenance			Apply	Cancel
Disquestics				

Item	Description	Description				
Enable This Profile	Check the box	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	ort Select a port to make the packets passing through it monitored by the administrator.  Mirroring Port : WAN1 Mirrored Port : WAN2 WAN1 WAN2 WAN3 WAN4					
		WAN5 CPU				

ApplyClick 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.

	WAN >> Switch >>	Interface					
Auto Logout : Off 🛛 👻	802.1Q VLAN	Mirror Interface	Status				
Quick Start Wizard							
Online Status	🔀 Edit 🥰	5 Refresh					
WAN	Interface	Enable	Duplex	Speed	flow_control	Note	
General Setup	WAN1	true	Full	Auto			
Default Route	WAN2	true	Full	Auto			
Load Balance	WAN3	true	Full	Auto			
Switch	WAN4	true	Full	Auto			
LAN	WAN5	true	Full	Auto			
NAT							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Central VPN Management							
Bandwidth Management							
USB Application							
System Maintenance							
Diagnostics							
External Devices							
Product Registration							

Item	Description
Edit	Choose the interface listed below and click the <b>Edit</b> button to modify the settings. A pop up window will appear for you to change the settings.
	Interface - X
	Interface: WAN2
	<b>Interface</b> – Display the name of WAN interface.
	Enable This Profile – Check it to enable such interface.
	<b>Speed</b> – Use the drop down list to specify the transmission rate ( <b>Auto, 10M, 100M</b> or <b>1000M</b> ) for such interface.
	<b>flow_control</b> – Click <b>Enable</b> 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.



	Annly Click it to save and wit the dialog
	<b>Apply</b> – Click it to save and exit the dialog.
	<b>Cancel</b> – 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.

### Status of the Switch

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

<b>Dray</b> Tek		Vigor 3900	Series	10:32:59	Login: Admin	Ð
		WAN >> Switch >> Status				
Auto Logout : Off 🛛 🗸		802.1Q VLAN Mirr	or Interface S	tatus		
Quick Start Wizard	~			h 10 Seconds		
Online Status		S Refresh	Auto Refres	h : 10 Seconds 🗸		
WAN		Interface	Status	Speed	Duplex	
General Setup		WAN1	Down			
Default Route	_	WAN2	Up	100M	Full	
Load Balance		WAN3	Down			
Switch		WAN4	Down			
LAN		WAN5	Down(SFP module disc	onnect		
NAT	Ξ	CPU	Up	1000M	Full	
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						
SSL VPN						
Central VPN Management						
Bandwidth Management						
USB Application						
System Maintenance	-					

Available parameters are listed as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Interface	Display the physical port of the WAN interface.
Status	Display if the port connection for WAN interface is linked or not. <b>Up</b> means the network is connected; <b>Down</b> means the network is not connected.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto)

	of the date for such WAN interface.
Duplex	Display the duplex used (full or half) by such WAN interface.

# 4.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from private IP address to public IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host.

LAN	
General Setup	
PPPoE Server	
IP Routing	
Static Route	
Switch	
Bind IP to MAC	
<b>RIP</b> Configuration	
OSPF Configuration	

#### 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 Setu	ip						
uto Logout : Off 🛛 🗸	Ge	eneral Setu	IDHCP	Relay RA	ADVD	DHCPv6	1				
Quick Start Wizard	l í –	🕼 Add	🔀 Edit	前 Delete	( Dof	roch				Profile Nu	mber Limit : 5
Online Status											
WAN			(n Enable	Descripti		-		telP Address	Subnet Mask		er IPv6 Proto
LAN	1	lantest	true	Just for te		4	static	0.0.0.0	255.255.255.0	Disable	Link-Local
General Setup	2	lan1	true		10	0	static	192.168.1.3	255.255.255.0	Enable	Link-Local
PPPoE Server											
IP Routing											
Static Route											
Switch											
Bind IP to MAC											
RIP Configuration											
OSPF Configuration											
NAT											
Firewall											
Objects Setting											
User Management											
Applications											
VPN and Remote Acces:											
Certificate Management											
SSL VPN											
Central VPN Manageme											
Bandwidth Management											
USB Application											
System Maintenance 📃											



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 <b>Edit</b> 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 <b>Delete</b> 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.
Priority	Display the level of the priority for such profile.
IPv4 Protocol	Display the IPv4 protocol type for the LAN profile.
IP Address	Display the IP address for such LAN profile.
Subnet Mask	Display the subnet mask for such LAN profile.
DHCP Server	Display the status (Enable/Disable) of the DHCP server.
IPv6 Protocol	Display the IPv6 protocol type for the LAN profile.

## How to add a new LAN profile

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



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

eneral Setup		-
Profile (max length:7) : I Enable	lantes1	
Description :	For test only (Optional)	
VLAN ID :		
Priority :	0	
Default MAC Address :	💿 Enable 🔿 Disable	
MAC Address :	00 : 50 : 7f : 7f : fc : e8	
IPv4 Protocol :	static	
Mode :	NAT	
IP Address :		
Subnet Mask :	255.255.255.0/24 👻	
DHCP Server :	⊙ Enable ◯ Disable	
DHCP Start IP :	192 168 1 1	
DHCP End IP :		
	🕼 Add 🗎 Save Profile Number Lim	nit : 16
	DNS	
DNS :	No items to show.	
DHCP Routers :	(Optional)	
	· · · · · · · · · · · · · · · · · · ·	b.
	📑 Apply 🔇	) Cancel

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	Type the packet priority number for such profile. The range is from 0 to 7.			
Default MAC Address	<ul> <li>Enable – Click it to enable the default MAC address for such profile.</li> <li>Disable – Click it to type the MAC address manually for such profile.</li> </ul>			
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 <b>NAT</b> or <b>ROUTING</b> 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.				
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 DHCO server.				
DNS	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.   Image: Add Image: Save				
DHCP Routers	<ul> <li>In general, this box will be blank. It means Vigor3900 will be regarded as the gateway for the user.</li> <li>However, if you want to use other gateway, please assign the IP address in this field.</li> <li> — click the icon to clear the IP setting.</li></ul>				
DHCP Options	<ul> <li>DHCP packets can be processed by adding option number and data information when such function is enabled.</li> <li>Each DHCP option is composed by an option number with data. For example,</li> <li>Option number:100</li> <li>Data: abcd</li> <li>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</li> </ul>				

	🕼 Add   Save	Profile Number Limit : 1
	DHCP Option	Value
	option 56 (Message) 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 serve option 46 (NetBIOS over TCP/IP Node Type) option 47 (NetBIOS over TCP/IP Scope) option 50 (Requested IP Address) option 54 (Server Identifier)	
	Add – Click it to add a new I	OHCP option profile.
	Save – Click it to save the set	tting.
	<b>DHCP Option</b> – Use the dro you want.	p down list to choose the one
	function of DHCP option.	the data to be processed by the
	— Click the icon to remov	ve the selected entry.
Lease Time	Set a lease time for the DHCI	P server. The time unit is minute
Specify Remote Dial-in IP	<b>Enable</b> – Check the box to en clients within the range speci Vigor3900 WUI.	
Gateway IP Address (optional)	Such IP address is ready for r Virtual System. — click the icon to clear	natching with the function of r the IP setting.
	Add Save IP Subne 192.168.1.83 255.25 255.25 Add – Click it to add a new s specified mode.	at Mask Mode to NAT TO MAT Stubnet mask with IP address and
	<b>Save</b> – Click it to save the set <b>IP</b> – Type the IP address if ye entry.	ttings. ou click Add for adding a new
	want.	down list to choose the one you
	<b>Mode</b> – Specify NAT or Rou $\boxed{10}$ – click the icon to remove	C C
IPv6 Protocol	It defines the IPv6 connection	n types for LAN interface. Local, Static and DHCP-SLA.
	<b>Link-Local</b> - Link-Local addr with neighbouring nodes on t	ress is used for communicating he same link. It is defined by the 1 don't need to setup Link-Local

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

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

Ge	neral Setup DHCP F	Relay RA	ADVD DHO	Pv6			
	🚯 Add 🛛 🔀 Edit	🔟 Delete	🔇 Refresh				F
	Profile (max length	:7) <sup>4</sup> Enable	Descripti VLA	NID Priority	IPv4 Protocol	IP Address	DHCF IPv6 Prot
1	lan1	true	10	0	static	192.168.1.3	Ena Link-Local
2	lantest	true	Just for t 2	4	static	0.0.0	Disa Link-Local

## 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.

<b>Dray</b> Tek		Vigor 390	<b>Series</b>	17:06:37	Login: Admin	Ð
		LAN >> General Setup >	>> DHCP Relay			
uto Logout : Off 🛛 👻		General Setup DI	HCP Relay RADVD	DHCPv6		
Quick Start Wizard			- 1			
Online Status		🔀 Edit 🛭 🛠 F	Refresh			
WAN		Profile	Enable	DHCP Server Location	DHCP Server IP	
LAN		lan1	false			
General Setup		lantest	false			
PPPoE Server	-					
IP Routing	-					
Static Route	- 1					
Switch						
Bind IP to MAC	E					
RIP Configuration						
OSPF Configuration						
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						
SSL VPN						
Central VPN Management						
Bandwidth Management	-					

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 <b>Edit</b> 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.
<b>DHCP Server Location</b>	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.

General Setup DH	ICP Relay RADVD
🔀 Edit 🛛 🗳 R	efresh
Profile	Enable
lan1	false
lantest	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 :	lantest	
DHCP Server Location	wan5	~
DHCP Server IP :	192 . 168 . 1	. 90
		📑 Apply 🛛 🐼 Cancel

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.	
<b>DHCP Server IP</b>	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.



#### 4.2.1.3 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.

<b>Dray</b> Tek	Vigor 3900	Series 17:09	:49 Login: Admin	E.
	LAN >> General Setup >> R	ADVD		
Auto Logout Off 🛛 👻	General Setup DHCP	Relay RADVD DHCPv6		
Quick Start Wizard				
Online Status	🗶 Edit 🦃 Refro	ish		
WAN	Profile	Enable	Advertisement Lifetime	
LAN	tan 1	true	30	
General Setup	lantest	true	30	
PPPoE Server				
IP Routing				
Static Route				
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				

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 <b>Edit</b> 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 $10 \sim 150$ . 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.

	HCP Relay RADVD DHCPv6
Profile	Enable
an1	true
antest	true

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

ADVD		
Profile : V Enable	lantest	
Advertisement Lifetime	: 30	Minutes
		📑 Apply 🛛 😵 Cancel

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 **Appl**y to save the configuration and exit the dialog.
- 4. The LAN profile has been edited.

General Setup DHCP Rela	ay RADVD DHCPv6	
🔀 Edit 🛛 🗳 Refresh		
Profile	Enable	Advertisement Lifetime
an1	true	30
antest	true	40

## 4.2.1.4 DHCP6

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

Auto Logout: Off   Quick Start Wizard   Online Status   WAN   LAN   Ceneral Setup   PPO6 Server   IP Routing   Static Route   Switch   Bind IP to MAC   RIP Configuration   OSPF Configuration   NAT   Firewall   Objects Setting   User Management   Applications   VPN and Remote Access   Central VPN Management   Bandwidth Management	<b>Dray</b> Tek		Vigo	r 390	0 Seri	ies	17:12:32		Login: Admin	(	E>
Quick Start Wizard   Online Status   WAN   LAN   Ceneral Setup   PPF0E Server   IP Routing   Static Route   Switch   Bind IP to MAC   E   RIP Configuration   OSPF Configuration   Objects Setting   Objects Setting   User Management   Applications   VPN and Remote Access   Central VPN Management   SSL VPN   Central VPN Management			LAN >> Gene	ral Setup >	> DHCPv6						
Online Status   WAN   LAN   General Setup   PPOE Server   IP Routing   Static Route   Switch   Bind IP to MAC   RIP Configuration   OSpEr Configuration   Objects Setting   User Management   Applications   VPN and Remote Access   Central VPN Management   Bandwidth Management	Auto Logout : Off 🛛 🗸		General S	Setup DH	ICP Relay	RADVD	HCPv6				
WAN   LAN   General Setup   PPPOE Server   IP Routing   Static Route   Switch   Bind IP to MAC   RIP Configuration   OSPF Configuration   OSPF Configuration   OSPF Configuration   OSPF Configuration   NAT   Firewall   Objects Setting   User Management   Applications   VPN and Remote Access   Certral VPN Management   Badwidth Management	Quick Start Wizard	^	¥ -	ant (* 17	ofreeh						
LAN   General Setup   PPPoE Server   IP Routing   Static Route   Switch   Bind IP to MAC   RiP Configuration   OSPF Configuration   OSPF Configuration   Objects Setting   User Management   Applications   VPN and Remote Access   Central VPN Management   Bandwidth Management	Online Status	_		-							
General Setup   PPPDE Server   IP Routing   Static Route   Switch   Bind IP to MAC   RIP Configuration   OSPF Configuration   OSPF Configuration   NAT   Firewall   Objects Setting   User Management   Applications   VPN and Remote Access   Central VPN Management   Bandwidth Management	WAN				Mode	Start IP		End IP		DNS	
PPPOE Server  PPPOE Server  PPOE Server  PRouting  Static Route  Switch  Bind IP to MAC  RIP Configuration  OSPF Configuration  OSPF Configuration  NAT  Firewall  Objects Setting  User Management  Applications  VPN and Remote Access  Certificate Management  SSL VPN  Central VPN Management	LAN										
IP Routing Static Route Switch Bind IP to MAC RIP Configuration OSPF Configuration NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management	General Setup		lantest	false	Automatic.						
Static Route         Switch         Bind IP to MAC         RIP Configuration         OSPF Configuration         NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management	PPPoE Server	_									
Switch     F       Bind IP to MAC     F       RIP Configuration     F       OSPF Configuration     F       NAT     F       Firewall     F       Objects Setting     F       User Management     F       Applications     F       VPN and Remote Access     F       Certificate Management     F       SSL VPN     Central VPN Management	IP Routing										
Bind IP to MAC       F         RIP Configuration       OSPF Configuration         OSPF Configuration       NAT         Firewall       Objects Setting         User Management       Applications         VPN and Remote Access       Certificate Management         SSL VPN       Central VPN Management         Bandwidth Management       F	Static Route	- 11									
RIP Configuration       OSPF Configuration       NAT       Firewall       Objects Setting       User Management       Applications       VPN and Remote Access       Certificate Management       SSL VPN       Central VPN Management       Bandwidth Management											
OSPF Configuration         NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management	Bind IP to MAC	=									
NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management	RIP Configuration	_									
Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management	OSPF Configuration										
Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management											
User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management	Firewall										
Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management	Objects Setting										
VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management	User Management										
Certificate Management SSL VPN Central VPN Management Bandwidth Management	Applications										
SSL VPN Central VPN Management Bandwidth Management	VPN and Remote Access										
Central VPN Management Bandwidth Management	Certificate Management										
Bandwidth Management	SSL VPN										
Bandwidth Management	Central VPN Management										
	Bandwidth Management	-									

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 <b>Edit</b> 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.

General	Setup DH	CP Relay RAI	DVD DHCPv6	
K	Edit 🗳 R	efresh		
Profile	Enable	Mode	Start IP	End IF
lan1	false			
lantest	false	Automatic Setting		

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

ICPv6	Bus (its			24-14 15	 2112	_
Profile :	lantest					
🗸 Enable						
Mode	Automatic Setting	~				
Auto Start IP :	Automatic Setting		]			
Auto End IP :	Manual Setting					
	DNS (auto)					
DNS (auto) :				No items to show.		
					📑 Apply 🔇	Cance

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
	<ul> <li>Automatic Setting – It is not necessary to configure Start IP, End IP and DNS setting. The system will assign suitable address automatically.</li> <li>Manual Setting – You should type the Start IP address and End IP address manually.</li> </ul>
	DHCPv6 Profile : lantest Difference Enable Mode : Manual Setting Start IP : End IP : 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: 2000:0000:0000:0000:0000:0000:10 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: 2000:0000:0000:0000:0000:0000:10 or 2000::10.
DNS	Set the private IP address for DNS server. If this field is blank, users on LAN will treat Vigor3900 as the DNS server.
	<ul> <li>Add – Click it to add a new IP address for DNS server.</li> <li>Save – Click it to save the setting.</li> <li> <ul> <li> <li> <li> – click the icon to remove the selected entry.</li> </li></li></ul> </li> </ul>
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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



4. The LAN profile has been edited.



#### 4.2.2 PPPoE Server

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

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

#### 4.2.2.1 General Setting

Dray Tek	Vigor 3900 Series		16:31:46	Login: Admin	Ð
	LAN >> PPPoE Server >> General Setting				0
Auto Logout : Off	General Setting Status				
Quick Start Wizard       Online Status       WAN       LAN       General Setup       PPPoE Server       IP Routing       Static Route       Switch       Bind IP to MAC       RIP Configuration       OSF Configuration       NAT       Firewall       Objects Setting       User Management       Applications       VPN and Remote Acces:       Certificate Management       SSL VPN       Central VPN Management       Bandwidth Management	PPPoE Server : PPPoE User Isolation : Deny Internet Access Except PPPoE User : PPPoE Server Name : Primary DNS : PPPoE Server Authentication Type : User Authentication Type : LAN Profile :	Disable      Enable     Disable      Di			
USB Application System Maintenance Diagnostics				🗎 Apply 🌘	3 Cancel
External Devices	1				

Item	Description
<b>PPPoE Server</b>	<b>Disable</b> – Click it to disable this function. <b>Enable</b> – Click it to enable the function of PPPoE server.
<b>PPPoE User Isolation</b>	<ul> <li>Disable – Click it to disable this function.</li> <li>Enable – Click it to isolate the PPPoE users who access into Internet via Vigor router</li> </ul>
Deny Internet Access Except PPPoE User	<b>Disable</b> –Click it to disable this function. <b>Enable</b> – If you click <b>Enable</b> , only the PPPoE user can access into Internet.



<b>PPPoE Server Name</b>	The default name is "v3900". You can modify it if required.					
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.					
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 UserAuthentication Type.If you choose LDAP as the authentication type, use the drop down list to specify the LDAP profile.					
LAN Profile	It is available when <b>RADIUS</b> or <b>LDAP</b> is selected as User Authentication Type. Use the drop down list to specify LAN profile for authentication.					
Apply	Click it to save and exit the dialog.					
Cancel	Click it to discard current page modification.					

## 4.2.2.2 Status

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

<b>Dray</b> Tek	Vigor 3	900 Series		16:3	7:51	Login: Admin	Ð
	LAN >> PPPoE	Server >> Status					(
Auto Logout : Off 🛛 🚽	General Set	ting Status					
Quick Start Wizard	🔹 Refre	sh 💥 Disconnect	Burder D	after all a dia Generale			
Online Status				efresh : 10 Seconds			
WAN	MAC Addres	ss User Name	IP Address	Up Time	RX Bytes	TX Bytes	
LAN			N	o items to show.			
General Setup							
PPPoE Server							
IP Routing							
Static Route							
Switch							
Bind IP to MAC							
RIP Configuration							
OSPF Configuration							
NAT							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Acces:							
Certificate Management							
SSL VPN							
Central VPN Manageme							
Bandwidth Managemen							
USB Application							
System Maintenance							
Diagnostics							
External Devices							

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.
Disconnect	Click it to disconnect the profile connection.
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.

### 4.2.3 IP Routing

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

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

<b>Dray</b> Tek		Vigor 3900	Series	10:23:50	Login: Admin	•
		LAN >> IP Routing				
uto Logout Off 🗸 🗸		IP Routing				
Quick Start Wizard		a	-			
Online Status		Add 💥 Edit	m Delete 🌩 Refre	sh GB Rename		
WAN		Profile Ena	ble WAN Profile	LAN Profile IP	Mask	
LAN				tio items to show.		
General Setup						
PPPoE Server						
IP Routing						
Static Route						
Switch						
Bind IP to MAC	E					
RIP Configuration						
OSPF Configuration						
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						
SSL VPN						
Central VPN Management						
Bandwidth Management		4	11			5

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



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

## How to add a new IP Routing profile

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

IP	Routing		
	🚯 Add 📏	Edit 🛛 <u> </u>	ete 🛛 🗭 Refres
	Profile	Enable	WAN Profile

3. The following dialog will appear.

Profile :	Routingtest1	
📝 Enable		
WAN Profile	wan1	
LAN Profile :	lan1 🗸	
IP :	192 . 168 . 1 . 54	
Mask	255.255.255.0/24	

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

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

IP	Routing					
🚯 Add 🔀 Edit 🏛 Delete 🔝 Refresh 🛛 😘 Rename						
	Profile	Enable	WAN Profile	LAN Profile	IP	Mask
1	Routingtest1	true	wan1	lan1	192.168.1.54	255.255.255.0

#### 4.2.4 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.

<b>Dray</b> Tek		Vigor 3900 Series	10:32:12	Login: Admin	Ð
		AN >> Static Route >> Static Route			
uto Logout : Off 🛛 🗸		Static Route IPv6 Static Route Inter-LAN Route			
Quick Start Wizard			. 9		
Online Status		🚯 Add 🔀 Edit 🛅 Delete 🔇 Refresi	a 🕻 Rename		
WAN		Profile Enable Destination IP Address	Subnet Gateway	WAN/L/ Met	tric
LAN			No items to show.		
General Setup					
PPPoE Server					
IP Routing					
Static Route					
Switch					
Bind IP to MAC	E				
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Management					
Bandwidth Management		4. III.			

#### 4.2.4.1 Static Route

Each item will be explained as follows:

Item	Description
Add	Add a new static route setting.
Edit	Modify the selected static route setting.
	To edit static route setting, simply select the one you want to modify and click the <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.

Rename	Allow to modify the selected profile name.
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 LAN>>Static Routing and click the Static Route tab.
- 2. Click the **Add** button.

Stat	ic Route	IPv6 S	tatic Route	Inter-LAN Rou	te
ĺ	🕒 Add	🔀 Ed	it <u> m</u> Del	lete 🛛 娕 Refr	es
	Profile	Enable	Destinatio	n IP Address	T

3. The following dialog will appear.

Profile :	vincent	
📝 Enable		
Destination IP Address	: 192 . 168 . 1 . 130	
Subnet Mask :	255.255.255.0/24 V (Option	onal)
Gateway :	172 . 16 . 3 . 1	
WAN/LAN Profile :	wan1	
Metric	(Opti	onal)

Item	Description
Profile	Type the name of the static route profile.

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

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

AN	N >> Static Route >> Static Route							
	Static Route IPv6 Static Route Inter-LAN Route							
	🕼 Add 🔀 Edit 🏢 Delete 🔝 Refresh 🖓 Rename							
	Profile	Enable	Destination IP Address	S	Subnet	Gateway	WAN/L	Metric
1	vincent	false	192.168.1.130	2	55.2	172.16.3.1	lantest	

## 4.2.4.2 IPv6 Static Route

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

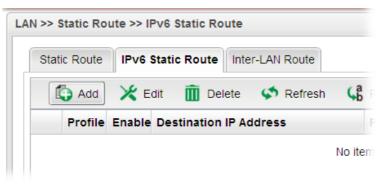
<b>Dray</b> Tek	Vigor 3900 Series	11:09:53	Login: Admin 🕞
	LAN >> Static Route >> IPv6 Static Route		
to Logout : Off 🛛 🗸	Static Route IPv6 Static Route Inter-LAN Route	te	
Quick Start Wizard	🚯 Add 🔀 Edit 🛅 Delete 🗳 Refr	resh 🕻 Rename	
Online Status		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
WAN	Profile Enable Destination IP Address	Prefix   Nexthop	WAN/L/ Metric
LAN		No items to show.	
General Setup			
PPPoE Server			
IP Routing			
Static Route			
Switch			
Bind IP to MAC			
RIP Configuration			
OSPF Configuration			
NAT			
Firewall			
Objects Setting			
User Management			
Applications			
VPN and Remote Access			
Certificate Management			
SSL VPN			
Central VPN Management			
Bandwidth Management			>

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 <b>Edit</b> 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 <b>Delete</b> button.	
Refresh	Renew current web page.	
Rename	Allow to modify the selected profile name.	
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 LAN>>Static Route and click the IPv6 Static Route tab.
- 2. Click the **Add** button.



3. The following dialog will appear.

Profile :	internal	
📝 Enable		
Destination IP Address	; fc20::1	
Prefix Length :	64	
Nexthop :		
WAN/LAN Profile :	wan2 🗸	
Metric	(0	Optional)

Available parameters are listed as follows:

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

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



### 4.2.4.3 Inter-LAN Route

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

<b>Dray</b> Tek		Vigor 3900 Series 11:14:55	Login: Admin 🕞	
		LAN >> Static Route >> Inter-LAN Route		
auto Logout : Off 🛛 👻		Static Route IPv6 Static Route Inter-LAN Route		
Quick Start Wizard	-			
Online Status		Enable		
WAN		Enable		
LAN				
General Setup				
PPPoE Server				
IP Routing	-			
Static Route				
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access			📑 Apply 🛛 😣 Cancel	
Certificate Management				1



#### 4.2.5 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.

<b>Dray</b> Tek	Vigor 3900 Series	16:07:18	Login: Admin	₽
	LAN >> Switch >> 802.1Q VLAN			
Auto Logout : Off 🛛 🗠	802.1Q VLAN Mirror Int	terface Status		
Quick Start Wizard	🕼 Add 🔀 Edit 🛅 Dela	ete 🔇 Refresh	Profil	le Number Li
Online Status				
WAN	VLAN ID	Member	Untag	
LAN	1 10	LAN_Port_1,LAN_Port_2,LAN_SFP	LAN_Port_1,LAN_Port_2,LAN_	_SFP
General Setup				
PPPoE Server				
IP Routing				
Static Route				
Switch				
Bind IP to MAC =				
RIP Configuration				
OSPF Configuration				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
System Maintenance 🖃	4			>

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
VLAN ID	Display the VLAN ID number.
Member	Display the LAN interface that is used to access into Internet for such LAN profile with the VLAN ID number.
Untag	Display the LAN interface that packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or untagged.

# How to add a new 802.1Q VLAN profile

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

80	2.1Q VLAN	Mirror	Interface	Status
(	🕼 Add 🔀	🕻 Edit 🛛 🔟	Delete 🛛 🖈	Refresh
	VLAN ID			Member
1	10			LAN_Port_1

3. The following dialog will appear.

VLAN ID :	12		
Member :	LAN_Port_2		
Untag :	LAN_Port_2		

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 <sup>(1)</sup> 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 Ξ 🔲 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 <sup>40</sup> 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. Click it to save and exit the dialog. Apply 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.

802.1Q VLAN	Mirror	Interface	Status	
🚯 Add 💙	🗲 Edit 🛛 🛅	Delete 🧳	Refresh	
VLAN ID		Men	nber	Untag
10		LAN1	LAN2,LAN3	LAN1,LAN2,LAN3
100		LAN1	LAN2	
1		LAN1	LAN2,LAN3	
15		LAN3		

#### 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.

<b>Dray</b> Tek	Vigor 3900 Series	16:18:15	Login: Admin	Ð
	LAN >> Switch >> Mirror			
uto Logout : Off 🛛 👻	802.1Q VLAN Mirror Interface Status			
Quick Start Wizard				
Online Status	Enable This Profile			
WAN	Mirroring Port : LAN_Port_2			
LAN	Mirrored Port : LAN_Port_1			
General Setup				
PPPoE Server				
IP Routing				
Static Route				
Switch Bind IP to MAC =				
RIP Configuration				
OSPF Configuration				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management			💾 Apply	🔇 Cancel
System Maintenance 🖃				

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.  Prome LAN_Port_2 LAN_Port_1 LAN_Port_2 LAN_SFP CPU
Mirrored Port	Select which port is necessary to be mirrored.
Refresh	Renew current web page.
Apply	Click it to save the settings.

### Interface

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

	LAN >> Switch >> I	nterface					(
to Logout : Off 🛛 🖌	802.1Q VLAN	Mirror Interface	Status				
Quick Start Wizard							
Online Status	🔀 Edit 🐓	Refresh					
WAN	Interface	Enable	Duplex	Speed	flow_control	Note	
LAN	LAN_Port_1	true	Full	Auto			
General Setup	LAN_Port_2	true	Full	Auto			
PPPoE Server	LAN_SFP	true	Full	Auto			
IP Routing							
Static Route							
Switch							
Bind IP to MAC							
RIP Configuration							
OSPF Configuration							
NAT							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Central VPN Manageme							
Bandwidth Management							
USB Application							
System Maintenance 📃							

Each item will be explained as follows:

Item	Description
Edit	Choose the interface listed below and click the <b>Edit</b> 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.
Note	Display additional information.

## 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.

802.1Q VLAN	Mirror Inte	erface	Status
🔀 Edit 🔍	S Refresh		
Interface	Enable		Dupl
LAN_Port_1	true		Full
LAN Port 2	true		Full

3. The following dialog will appear.

Interface : V Enable	LAN_SFP	
Duplex :	Full	~
Speed :	Auto	
flow_contro	l : 🔵 Enable 💿	Disable
Note :		ode connection may result in duplex mismatch and become ve connect auto to auto and fixed to fixed mode.

Available parameters are listed as follows:

Item	Description
Interface	Display the name of LAN interface profile.
Enable	Check the box to enable the Mirror function for the switch.
Speed	Use the drop down list to specify the transmission rate for such profile.
flow_control	Click <b>Enable</b> 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.



### Status

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

	LAN >> Switch >> Status	3			
nto Logout : Off 🛛 🚽	802.1Q VLAN Mir	ror Interface State	us		
Quick Start Wizard					
Online Status	🗢 Refresh		: 10 Seconds -		
WAN	Interface	Status	Speed	Duplex	
LAN	LAN_Port_1	Up	1000M	Full	
General Setup	LAN_Port_2	Down			
PPPoE Server	LAN_SFP	Down(SFP module	disconnec		
IP Routing	CPU	Up	1000M	Full	
Static Route					
Switch					
Bind IP to MAC =					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
Applications VPN and Remote Acces:					
VPN and Remote Access					

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 statu The information will update immediately when the Refresh button is clicked.	
Interface	Display the profile name of the interface.	
Status	Display the status (up or down) for the interface.	
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.	
Duplex	Display the duplex used (full or half) by such profile.	

## 4.2.6 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.

<b>Dray</b> Tek	Vigor 3900 s	ieries	16:57:25	5 Login: Adm	in 🕞
	LAN >> Bind IP to MAC				2
Auto Logout : Off 🛛 🗸	Bind IP to MAC				
Quick Start Wizard			5 A.L. V		
Online Status	Mode : Disable	🚽 💣 Select All 🛸 Move 🗳 R		🕻 Edit   🏛 Delete 📑 Select	All 😘 Rename 🕝
WAN	ARP Table		Bind Table		
LAN	IP	Mac Address	Profile	IP Address	MAC
General Setup	192.168.1.10	e0:cb:4e:da:48:79		No items to show	<i>с</i>
PPPoE Server					
IP Routing					
Static Route					
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Acces:					
Certificate Management					
SSL VPN					
Central VPN Manageme					
Bandwidth Management					
USB Application					
System Maintenance 🚽					
Diagnostics	4				>
External Devices		(3) Microsoft Office Mard			

Each item will be explained as follows:

Item	Description	
Mode	<b>Enable -</b> Choose it to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.	
	<b>Disable -</b> Choose it to disable this function. All the settings on this page will be invalid.	
	<b>Strict Bind</b> – 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 <b>Move</b> on IP Bind List.	
	<b>IP</b> 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 <b>IP Bind List</b> .
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 <b>IP Bind List</b> . Simply click and select the one, and click <b>Delete</b> . The selected item will be removed from the <b>IP Bind List</b> .
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.
	<b>Profile -</b> Display the name of the profile.
	<b>IP</b> Address - Display the IP address specified for the profile.
	<b>MAC</b> - Display the MAC address specified for the profile.

## How to configure Bind IP to MAC

#### 1. Open LAN>>Bind IP to MAC.

2. Use the drop down menu to specify a suitable mode.

Bind IP t	to MAC		
Mode :	Enable	~	<b></b>
ADD T-1	Disable		
ARP Ta	Enable		
IP	Strict_Bind		Idress
192 168	139.10	00-14-60	-59-0d-1b

There are three modes offered for you to choose.

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

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

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

3. Click Add.



4. The following dialog appears.

nd IP to MAC	-
Profile :	Bind_IP1
IP Address	: 192 . 168 . 1 . 99
MAC :	00 : 50 : 7F : CA : 8E : 9D
	📑 Apply 🔞 Cancel

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

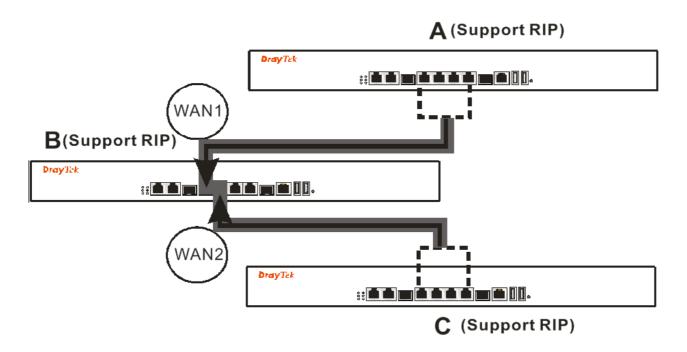
- 5. Enter all the settings and click **Apply**.
- 6. A new profile has been added onto **Bind Table**.

C				
	🏠 Add	🔀 Edit 🛛 🔟 Dele	te 📑 Select All	
	Bind Table			
ddress	Profile	IP Address	MAC	
e:da:48:79	Bind_IP1	192.168.1.99	00:50:7F:CA:8E:9D	

### 4.2.7 RIP Configuration

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

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



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

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

In another direction, C will do the same thing.

<b>Dray</b> Tek	Vigor 390	O Series	11:55:33	Login: Admin	Ð
Auto Logout : Off  Quick Start Wizard Online Status WAN LAN General Setup PPPoE Server IP Routing Static Route Switch E Bind IP to MAC RIP Configuration OSPF Configuration NAT Firewall Objects Setting User Management Applications VPN and Remote Access	LAN >> RIP Configuration				
Certificate Management SSL VPN				Apply	🐼 Cancel

Available parameters are listed as follows:

Item	Description
Enable This Profile     Check the box to enable such function.	
<b>Profile</b> Choose the LAN/WAN profile(s).	
Apply	Click it to save the settings.
<b>Cancel</b> Click it to discard the settings configured in this page.	

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

# 4.2.8 OSPF Configuration

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

<b>Dray</b> Tek	Vigor 390	00 Series	17:00:47	Login: Admin	Ð
	LAN >> OSPF Config				
to Logout : Off	OSPF Configura	tion			
Quick Start Wizard					
Online Status	Enable				
WAN	Lindore	<b>6</b>		Profile Number Limit : 64	
LAN		C Add		Frome Number Linnt . 04	
General Setup		LAN Profile	Area		
PPPoE Server	Profile :		No items to show.		
IP Routing					
Static Route					
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Acces:					
Certificate Management					
SSL VPN					
Central VPN Manageme					
Bandwidth Managemen					
USB Application					
System Maintenance 📃				💾 Apply	O O O P
Diagnostics				Apply	🔇 Cance

Available parameters are listed as follows:

Item	Description	n				
Enable This Profile	Check the b	box to enable such	h function.			
Profile	Choose a L such config		the drop down	list to apply for		
		C Add				
		LAN Profile				
	Profile :	lan1 lantest	<b>v</b>			
		K Add				
		C Add	Area			
	Profile :	_	Area 35			
Apply		LAN Profile				

# 4.3 NAT

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

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

NAT
Port Redirection
DMZ Host
Address Mapping
ALG

### 4.3.1 Port Redirection

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



		<b>gor 3</b> > Port Ref										
to Logout : Off 🔹 🗸		rt Redired										
Quick Start Wizard												
Online Status		🖏 Add	🔀 Edit	🛄 Del	ete 🗳	Refresh	襘 Move Up 🚽	🐣 Move Down	🔩 Rename			
WAN		Profile	Enable	WAN Pr	Use IP /	A Alias	Private IP		Protocol Port Ree	Public F	Public P	Private Po
LAN	1	PR_1	false	wan3	All		192.168.1.23		TCP/UDF Range-t	c100	110	20
NAT												
Port Redirection												
DMZ Host												
Address Mapping												
ALG												
Firewall												
Objects Setting												
User Management												
Applications												
VPN and Remote Access												
Certificate Management												
SSL VPN												
Central VPN Management												
Bandwidth Management												
USB Application												
System Maintenance												
Diagnostics												
External Devices												
Product Registration												

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 <b>Edit</b> 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 <b>Delete</b> 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 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.

Port	Redired	ction				
				_		
	🖏 Add	X	Edit	Del	ete	🗢 Re
	<b>v</b>					-

3. The following dialog will appear.

ort Redirection			-
Profile :	PR_1		
🔽 Enable			
WAN Profile :	wan3	~	
Use IP Alias :	Single_Alias	~	
Alias		✓ Mus	st have value
Private IP :		].	
Protocol	TCP/UDP	~	
Port Redirection Mode :	Range-to-One	~	
Public Port Start :	100		
Public Port End :	110	Mus	st be greater than start port
Private Port :	20		
			📄 Apply 🛛 🔞 Cancel



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.
Use IP Alias	<ul> <li>When All is selected as WAN Profile, such feature is unavailable.</li> <li>Use the drop down list to select the type you want.</li> <li>Single_Alias</li> <li>All</li> <li>Single_Alias – You have to type one IP address used for IP Alias.</li> <li>All – All the IP address can be treated as IP Alias.</li> </ul>
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 Range-to-One Range-to-Range
Public Port Start/	It is available when <b>Range-to-One</b> or <b>Range-to-Range</b> is

Public Port End	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.

#### 4.3.2 DMZ Host

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

<b>Dray</b> Tek	Vigor 39				Login: Admin 🕞
	NAT >> DMZ Host				
Logout : Off	DMZ Host				
Quick Start Wizard	Add \	🕻 Edit 🛛 前 Deleti	e 🗳 Refresh 🛛 🔩 Rename		Profile Nu
Online Status					
WAN	Profile	Enable	Outgoing WAN Pro IP Alias	DMZ Host IP	Allow DMZ Host to /
LAN	DMZ_1_RD	true	wan1	192.168.1.111	Enable
NAT					
Port Redirection					
DMZ Host					
Address Mapping					
ALG					
Firewall					
Objects Setting					
Jser Management					
Applications					
PN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Management					
Bandwidth Management					
JSB Application					
System Maintenance					
Diagnostics					
External Devices					
Product Registration					

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 <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected
Delete	rule. Remove the selected profile. To delete a profile, simply select the one you want to delete and click the <b>Delete</b> button.
Refresh	Renew current web page.
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.
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.

DMZ Host				
🕼 Add	🔀 Edit	<u> m</u> Delete	< Refresh	🕻 Renam
Profile	Enable		Outgoing WAN Pro IP A	

3. The following dialog will appear.

Profile :	DMZ_1_RD	
📝 Enable		
Outgoing WAN Profile :	wan1	~
Use IP Alias :	📀 Enable i 🔘 🛛	)isable
IP Alias :		
DMZ Host IP :	192 . 168 .	1 . 111
Allow DMZ Host to Access Net	work : 💿 Enable 🔿 🛙	)isable
Allowed IP Object :	IP_object_1	👻 🗙 (Optiona
Allowed IP Group :		👻 🗙 (Optiona
Allowed Service Type :	BGP,L2TP	🗸 🗙 (Optional

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 <b>WAN&gt;&gt;General Setup</b> and enable the <b>wan1</b> profile. Add several IP addresses under <b>Static</b> 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.

🕼 Add 刘	🕻 Edit 🛛 🛅 Dele	ite 🗳 Refresh 📢 Rename		Profile N
Profile	Enable	Outgoing WAN Pro IP Alias	DMZ Host IP	Allow DMZ Host to Access Netwo
DMZ_1_RD	true	wan2	192.168.1.111	Enable

## 4.3.3 Address Mapping

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

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

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

<b>Dray</b> Tek	Vigor 3900 Series	13:33:29	Login: Admin	8
	NAT >> Address Mapping			
to Logout Off	Address Mapping			
Quick Start Wizard	🔂 Ada 🗶 Edit. 🏢 Delete 🔊 Refresh 💣 Move Up 🥊 Move Down 📢			Profile Number I
Online Status				
WAN	Profile Enable WAN Profile Source IP Ot Source IP Group Private IP	Private IP Subnet Mask Protocol	IP Alias Failover Status	Failback
LAN	No items a	o show		
Port Redirection				
DMZ Host				
Address Mapping				
ALG				
Ficewali				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
handwidth Management				
USB Application				
System Maintenance				
Diagnostics				
External Devices				
Product Registration	(a)			

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 <b>Edit</b> 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 <b>Delete</b> 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.

Α	ddress Map	oping		
	🚯 Add	🔀 Edit	<u> </u> Delete	娕 Ref
	Profile	Ena	ble WAN	I Profile

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	
		Apply 🔇 Cancel

Item	Description	
Profile	Type the name of the profile	2.
Enable	Check the box to enable the	Address Mapping profile.
WAN Profile	Choose the active WAN inte	erface for such entry.
Address Type	Choose <b>Subnet</b> or <b>Object</b> as setting options will be displa	• •
	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 <b>Object</b> Use the drop down list to sp profile. If there is nothing to <b>Object Settings</b> to create th	be specified, simply open
Source IP Group	It is available when Object i Use the drop down list to sp profile. If there is nothing to <b>Object Settings</b> to create th	ecify one IP group for such be specified, simply open
Protocol	Choose the protocol used fo	r the entry.



	All V TCP UDP TCP/UDP All	
Use IP Alias	Click <b>Enable</b> to invoke IP Alias function.	
IP Alias	Select the Alias IP for this Address Mapping profile.	
Failover to the Default Route	<ul><li>Enable - When the specified WAN profile is down, the data traffic will be transmitted by suing default route.</li><li>Disable - When the specified WAN profile is down, the data</li></ul>	
	traffic will be blocked.	
Failback	<ul> <li>Enable – The connection session made by default route will be redirected with the specified route configured in Address Mapping.</li> <li>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.</li> </ul>	
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.

Ac	dress Mapp	ing										
	Add	×	Edit		Delete	C Refresh	T Move Up	🐣 Move Down	<b>G</b> <sup>a</sup> Rename			
	Profile		Enable	0	WAN	Profile Sourc	e IP Ot Source I	IP Gr Private IP		Private IP Su Protocol	IP Alias	Failover S
1	Add_M_1		true		wan2			192 168 1 125		255 255 255 0 All		Enable

### 4.3.4 ALG

### 4.3.4.1 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.

<b>Dray</b> Tek	Vigor 3900 Series	13:48:49	Login: Admin	Ð
	NAT >> ALG >> SIP ALG			
Auto Logout : Off	SIP ALG H.323 ALG			
Quick Start Wizard				
Online Status	Enable SIP ALG			
WAN		*		
LAN				
NAT	WAN Interface : wan1	*		
Port Redirection				
DMZ Host				
Address Mapping				
ALG				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				
USB Application				
System Maintenance			Apply	🔇 Cancel
Diagnostics				

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.

## 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.

G		
-		
	i	

# 4.4 Firewall

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

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

Firewall	
Filter Setup	
DoS Defense	
MAC Block	

#### 4.4.1 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.

### 4.4.1.1 IP Filter

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

Auto Logout: Off   Quick Start Wizard   Online Status   Online Status   WAN   LAN   LAN   NAT   Firewall   Firewall   Firewall   Britler Setup   DoS Defense   MAC Block   Objects Setting   User Management   Applications   YPN and Remote Access   Central VPN Management   Bandwidth Management   Bandwidth Management   Disgnostics   External Devices   Product Registration	<b>Dray</b> Tek	Vigor 3900 Seri	es	15:01:42	Login: Admin	Ð
Ouick Start Wizad         Onine Status         WAN         LAN         NAT         Firewall         Firewall         Filter Setup         DoS Defense         MAC Block         Objects Setting         User Management         Applications         YPN and Remote Access         Certrificate Management         Bandwidth Management         <		Firewall >> Filter Setup >> IP Fil	ter			2
Online Status       Add		IP Filter Application Filte	er URLWeb Category Filter QQ Filter			
WAN       Group       Enable       Comment         LAN       NAT       IPF_Market       true       used for MKT Dept         Filter Setup       DoS Defense       MAC Block       Volume and Remote Access       Vent and Remote Access         Objects Setting       User Management       Applications       VPN and Remote Access       Vent and Remote Access         Central VPN Management       Bandwidth Management       USB Application       Vent and Remote Access         System Maintenance       Diagnostics       External Devices       Vent and the manual set of the manual set o		🕼 Add 🔀 Edit 🟢	Delete 🛭 🔄 Refresh 🏻 💡 Move Up 🛛 🤻	Move Down	Profile Numb	er Limit : 12
LAN       IPF_Market       true       used for MKT Dept         NAT       Firewall       Filter Setup       Do Do Bofense         MAC Block       Objects Setting       User Management         Applications       VPN and Remote Access       Certificate Management         SSL VPN       Central VPN Management       Bandwidth Management         USB Application       System Maintenance       Diagnostics         External Devices       Image: Central Devices       Image: Central Devices		Group	Enable	Comm	ent	
NAT Firewall Filter Setup DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices		-				
Filter Setup         DoS Defense         MAC Block         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management         USB Application         System Maintenance         Diagnostics         External Devices						
Filter Setup         DoS Defense         MAC Block         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management         USB Application         System Maintenance         Diagnostics         External Devices						
DoS Defense         MAC Block         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management         USB Application         System Maintenance         Diagnostics						
Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management         USB Application         System Maintenance         Diagnostics         External Devices						
User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices	MAC Block					
Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices	Objects Setting					
VPN and Remote Access Certificate Management SSL VPN Central VPN Management USB Application System Maintenance Diagnostics External Devices	User Management					
Certificate Management SSL VPN Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices	Applications					
SSL VPN Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices	VPN and Remote Access					
Central VPN Management Bandwidth Management USB Application System Maintenance Diagnostics External Devices	Certificate Management					
Bandwidth Management USB Application System Maintenance Diagnostics External Devices	SSL VPN					
USB Application System Maintenance Diagnostics External Devices	Central VPN Management					
System Maintenance Diagnostics External Devices	Bandwidth Management					
Diagnostics External Devices	USB Application					
External Devices	System Maintenance					
	Diagnostics					
Product Registration	External Devices					
	Product Registration					

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 <b>Edit</b> 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 <b>Delete</b> 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.
Group	Display the name of the <b>IP filter group</b> 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.

P Filter			_
Group :	IPF_Market		
🔽 Enable	•		
Comment	used for MKT Dept	(Optional)	

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.

IP	Filter Application Filter URLA	Neb Category Filter QQ Filter	
ſ	🕽 Add 🛛 💥 Edit 👖 Delete 📢	🔊 Refresh 🛛 👚 Move Up 🛛 🐣 Mo	Profile Number Limit :
	Group	Enable	Comment

6. You can create filter rule by clicking **b** 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	Application F	ilter URL/Web Category	Filter QQ Filte	r		
🚯 Add	🔀 Edit 🧵	🛚 Delete 🛛 🗭 Refresh	襘 Move Up ,	통 Move Down	Profile Number Li	mit :
Group	)	Enable		Comment		
📣 IPF_Ma	arket	true		used for MK	(T Dept	
	Add 🔀 Edit	前 Delete 🛛 🐼 Refr	esh 🕻 🥵 Rename	e 👉 Move Up	🐣 Move Down	Rro
Rule	Enable	Block Actior Next Gro	up Syslog G	eneral Fire Source	Fire Destination I	
		No	tems to show.			

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

Group		-	Enable
IPF_Market		t	rue
🚯 Add	🔀 Edit	🔟 Delete	🖈 Re
Rule	Enable	Block Action	Next Gr
			No

8. The following page for configuration will appear.

tule			
Profile :	For_outgoing		
	V Enable		
Block Action :	Pass	*	
Next Group :		~	
SysLog :	💿 Enable (	Disable	
Input Interface :	wan2	*	
Output Interface :	wan2	*	
While no target has	s been specifi	ed, firewall rules	are applied to Any object
Firewall Obje			
general targe			
Fime Object			
Time Group			
Service Type	Object		
Service Type	Group		
source target			
Source IP Ob	ject		
Source IP Gro	pup		
Source User	Profile		
Source User	Group		
destination ta	arget		
Destination If			
Destination IF			
Destination U			
Destination U	Iser Group		

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. <b>Block</b> - Packets matching the rule will be dropped
	<pre>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 Block Block</pre>
	Pass Block_If_No_Further_Match Pass_If_No_Further_Match wan2
Next Group	When you choose <b>Block_If_No_Further_Match</b> or <b>Pass_If_No_Further_Match</b> as <b>Block Action</b> , you have to specify next IP filter group for further matching.
Syslog	Click <b>Enable</b> to make the history of firewall actions appearing on the <b>System Maintenance</b> >> <b>Syslog/Mail</b> <b>Alert</b> >> <b>Syslog File</b> .



	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.
general target	<b>Time Object</b> - Click the triangle icon b to display the profile selection box. Choose a schedule object profile to be applied on such rule. You can click to create another
	<ul> <li>new time object profile.</li> <li><b>Time Group</b> - Click the triangle icon b 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.</li> </ul>
	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
	<ul> <li>another new service type object profile.</li> <li>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.</li> </ul>
source target	<b>Source IP Object -</b> Click the triangle icon b 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 I 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 I
	group profile. <b>Source User Profile</b> –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.
	<b>Source User Group</b> –Click the triangle icon $\triangleright$ 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 anothe new user group profile.

destination target	<b>Destination IP -</b> Click the triangle icon <b>&gt;</b> 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 <b>&gt;</b> to create another new IP object profile.
	<b>Destination IP</b> - Click the triangle icon b 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.
	<b>Destination User Profile</b> –Click the triangle icon <b>b</b> 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.
	<b>Destination User Group</b> –Click the triangle icon b 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.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

- Enter all the settings and click **Apply**. 9.
- 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		ti	rue			used for MK	T Dej	ot	
🚯 Add	🔀 Edit	<u> </u> Delete	< Refresh	n 🕻 🥵 Rena	ime 👉	Move Up	-	Move Down	Profile
Rule	Enable	Block Actior	Next Group	Syslog	General	Fire 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.

## 4.4.1.2 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.

	Vigor 3900 Series			
	Firewall >> Filter Setup >> Application Filter			
uto Logout Off 🛛 👻	IP Filter Application Filter URL/Web Category	Filter QQ Filter		
Quick Start Wizard	A 16 A			
Online Status	🕼 Add 💥 Edit 🔟 Delete 🔊 Refresh	😭 Move Up 🛛 🐣 Move Down	GB Rename	
WAN	Profile Enable Time Ot Time Gr IP Objec IP 0	Brouj User Pri User Gr. Protoco Pi	rotoco IM Pass IM Bloci P2P Pas P2P	Block
LAN		No items to show		
NAL				
Firewall				
Filter Setup				
DoS Defense				
MAC Block				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				
USB Application				
System Maintenance				
Diagnostics				
External Devices				
Product Registration	Eel m			1.8.

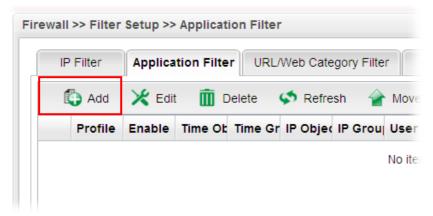
Each item will be explained as follows:

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 <b>Edit</b> 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 <b>Delete</b> 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, <b>None</b> will be shown in this field.
Time Group	Display the Time group profile selected for such application

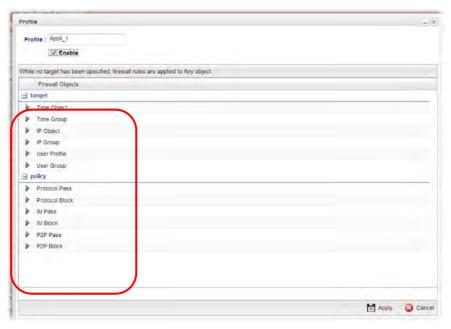
Item	Description
	profile.
IP Object	Display the IP object profile selected for such application profile.
IP Group	Display the IP group profile selected for such application profile.
User Profile	Display the user object profile selected for such application profile.
User Group	Display the user group profile selected for such application profile.
Protocol Pass	Display the protocol object profile selected for such application profile.
Protocol Block	Display the protocol object profile selected for such application profile.
IM Pass	Display the IM object profile selected for such application profile.
IM Block	Display the IM object profile selected for such application profile.
P2P Pass	Display the P2P object profile selected for such application profile.
P2P Block	Display the P2P 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).



Item	Description
Profile	Type the name of the application filter profile.
Enable	Check the box to enable this profile.
target	<ul> <li>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</li> <li>to create another new time object profile, or you can click the edit icon  to modify the existed object profile.</li> </ul>
	<b>Time Group</b> - Click the triangle icon by 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.
	<b>IP Object -</b> Click the triangle icon ▶ to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected IP will be filtered by the router when such application filter profile is applied. You can click to create another new IP object profile.
	<b>IP Group -</b> 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.

	_
	<b>User Profile -</b> Click the triangle icon <b>b</b> 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 <b>c</b> to create another new
	user profile, or you can click the edit icon $\bowtie$ to modify the existed user profile.
	<b>User Group -</b> Click the triangle icon $\triangleright$ 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 the edit icon $\bowtie$ to modify the existed group profile.
policy	<ul> <li>Protocol Pass / Protocol Block - Click the triangle icon ▶ to display the profile selection box. Choose one or more Protocol 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 protocol object profile, or you can click the edit icon  to modify the existed object profile.</li> <li>IM Pass / IM Block - Click the triangle icon ▶ to display the profile selection box. Choose e one or more IM object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the edit icon  to modify the existed object profile selection box. Choose e one or more IM object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the edit icon  to modify the existed object profile.</li> <li>P2P Pass / P2P Block - Click the triangle icon ▶ to display the profile selection box. Choose one or more P2P object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the edit icon  to display the profile selection box. Choose one or more P2P object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the edit icon  to display the profile selection box. Choose one or more P2P object profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the edit icon the drop down list which will be allowed / not be allowed to pass through the router. You can click to create profiles from the drop down list which will be allowed / not be allowed to pass through the router. You can click the triangle icon the drop down list which will be allowed / not be allowed to pass through the router. You can click the triangle to pass through the router. You can click the triangle to pass through the router. You can click the triangle to pass through the router. You can click the trouter t</li></ul>
	create another new P2P object profile, or you can click the edit icon it 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.

Fire	wa	all >> Filte	r Setup >:	> Applica	tion Filter											3
	IF	P Filter	Applicati	ion Filter	URLWe	eb Categor	y Filter	QQ Fil	ter							
		🚯 Add	🔀 Edit	<u> m</u> Del	lete 🗳	Refresh	💣 M	ove Up	🐣 М	ove Down	🔓 Ren	ame				
		Profile	Enable	Time Ob	Time Gr	IP Objec l	P Group	User Pr	User	ir: Protoc	o Protoco	IM Pass	IM Block	P2P Pa	P2P Bloc	
	1	no_im	true					Aron								
	2	Appl_1	true			IP_objec										

# 4.4.1.3 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.

IP Filter	Application Filter URL/We	in Category F		Q Filter				
🕼 Add	🔀 Edit 🛛 🕅 Delete 🛭 🛠	Refresh	🛉 Move U	Jp 栆	Move Dowr	n 🕻 🥵 Rena	ame	
Profile	Enable T Filter Httj Time F	Pro IP Object	P Group l	User Pro	o User Gro H	(eyword Key	yword File Ext	ei Web Cate
		I	lo items to	o show.				
Use Defau	lt Message :		⊙ Enable	e ODis	able			
Use Defau	It Message :		 html>≺he	ead> <titl< td=""><td>e&gt;URL Cont</td><td></td><td>tle&gt;<b< td=""><td>C</td></b<></td></titl<>	e>URL Cont		tle> <b< td=""><td>C</td></b<>	C
		ł		ad> <title ghtblue&gt;</title 	e>URL Cont <center><h< td=""><td>3&gt;URL Cont</td><td>tent Filter≺br&gt;b</td><td>)y ≺a</td></h<></center>	3>URL Cont	tent Filter≺br>b	)y ≺a
	It Message : eb Category Administration	1 Message : H	html> <he gcolor=lig ref=http://</he 	ead> <titli ghtblue&gt; www.dra</titli 	e>URL Coni <center><h: aytek.com/ ta</h: </center>	3>URL Cont arget=draytel		oy Ka decoration:n
		1 Message :	html> <he gcolor=lig ref=http:// font color= age &lt;</he 	ead> <title ghtblue&gt; www.dra ≃red&gt;<i: from</i: </title 	e>URL Cont <center><h aytek.com/ ta &gt;DrayTeki <font color:<="" td=""><td>3&gt;URL Cont arget=draytel &gt;</td></font> =blue&gt; %SIF</h </center>	3>URL Cont arget=draytel >	tent Filter k k STYLE=text-o The i %	oy Ka decoration:n requested W rto Kfont
		1 Message :	html> <he gcolor=lig ref=http:// font color= age &lt;</he 	ead> <title ghtblue&gt; www.dra ≃red&gt;<i: from</i: </title 	e>URL Cont <center><h aytek.com/ ta &gt;DrayTeki <font color:<="" td=""><td>3&gt;URL Cont arget=draytel &gt;</td></font> =blue&gt; %SIF</h </center>	3>URL Cont arget=draytel >	tent Filter k k STYLE=text-o The i	oy Ka decoration:n requested W rto Kfont
Default W		1 Message :	html> <he gcolor=lig ref=http:/// font color: age &lt; olor=blue</he 	ead> <title ghtblue&gt; www.dra ≃red&gt;<i: from</i: </title 	e>URL Cont <center><h aytek.com/ ta &gt;DrayTeki <font color:<="" td=""><td>3&gt;URL Cont arget=draytel &gt;</td></font> =blue&gt; %SIF</h </center>	3>URL Cont arget=draytel >	tent Filter k k STYLE=text-o The i %	oy Ka decoration:n requested W rto Kfont
		1 Message :	html> <he gcolor=lig ref=http:// font color= age &lt;</he 	ead> <title ghtblue&gt; www.dra ≃red&gt;<i: from</i: </title 	e>URL Cont <center><h aytek.com/ ta &gt;DrayTeki <font color:<="" td=""><td>3&gt;URL Cont arget=draytel &gt;</td></font> =blue&gt; %SIF</h </center>	3>URL Cont arget=draytel >	tent Filter k k STYLE=text-o The i %	oy <a decoration:n requested W to <font I <font< td=""></font<></font </a 

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 <b>Edit</b> 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 <b>Delete</b> 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.
Filter Https	Display if the HTTPs filter is enabled or not.
Time Object	If no time schedule is set, <b>None</b> will be shown in this field.



Item	Description
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.
Use Default Message	<ul> <li>Enable – Use the default message to display on the page that the user tries to access into the blocked web page.</li> <li>Disable – Type the message manually to display on the page that the user tries to access into the blocked web page.</li> </ul>
Default Web Category Administration Message	Such field is available when you disable the function of Use <b>Default Message</b> .
	The message will display on the user's browser when he/she tries to access the blocked web page.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

#### How to create a URL Filter profile

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



3. The following dialog will appear.

		👽 Ena							
Filt	er	Https: 💿 En	able 🔘 Disable (For Keywor	rd and Web Cate	gory)				
Vhil	le n	o target has I	peen specified, firewall rules a	are applied to An	y object				
	Fi	rewall Object	ts						
3 t	arg	jet							
₽	Tir	me Object							
₽	Tir	me Group							
₽	IP	Object							
₽	IP	Group							
₽	Us	ser Profile							
₽	Us	ser Group							
3 p	ooli	cy							
₽		e Extension I							
₽		e Extension I	Block						
₽		eyword Pass							
₽		eyword Block							
4	W	eb Category I		During	01-01-0	0	04	F .04	-
		Profile	Child Protecti Leisure	Business	Chatting	Computer	Other	Edit	4
		WCO_1	Alcohol-And-T Entertainme	ent Web-Based-E	= Chat	Social-Netwo	r Government,F	X	

Item	Description
Profile	Type the name of the URL filter profile.
Enable	Check the box to enable this profile.
Filter https	<ul> <li>Enable – Click it to enable the HTTPS filtering job.</li> <li>Disable – When only keyword and web category are selected for such rule, choose Disable.</li> </ul>
target	<b>Time Object</b> - Click the triangle icon <b>b</b> to display the profile selection box. Choose a schedule profile to be applied on such application filter profile. The router will perform the

Item	Description
	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.
	<b>Time Group</b> - 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.
	<b>IP Object -</b> 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.
	<b>IP Group -</b> 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 $\bowtie$ 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 URL filter profile is
	applied. You can click 💿 to create another new user
	profile, or you can click the edit icon $\checkmark$ to modify the existed user profile.
	<b>User Group -</b> Click the triangle icon <b>&gt;</b> 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 URI
	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.
policy	<b>File Extension Pass / File Extension Block -</b> Click the triangle icon ▶ to display the profile selection box. Choose one or more File Extension object profiles from the drop down list which will be allowed / not be allowed to pass
	through the router. You can click to create another new File Extension object profile, or you can click the edit icon
	to modify the existed object profile.
	Keyword Pass / 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,



Item	Description
	or you can click the edit icon it to modify the existed object profile.
	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.

IF	P Filter	Applicatio	n Filter 🛛 U	RL/Web Ca	ntegory Fi	ilter G	Q Filter					
	🕼 Add	🔀 Edit	🔟 Delet	e 🛭 🗳 Re	fresh 🛉	鹶 Move	Up 🌷	Move Dow	m <mark>⊊a</mark> lf	Rename		
	Profile	Enable T	Filter Http	Time Pro II	P Object I	IP Group	User Pre	User Gro	Keyword	Keyword	File Exter	Web Cate
1	Keyword	true	enable				Tom			gambling		

## 4.4.1.4 QQ Filter

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

	Vigor 3900						
uto Logout Off			and the second				
Quick Start Wizard	IP Filter Applicat	ion Filter URL/Web Categ	ory Filter QQ Filter				
Online Status	🖾 Add 💥 Edit	Delete 🕼 Refrest	Move Up 🐣 Nove I	Coun 🔓 Rename		1	Profile Number U
WAR	Profile	Enable	Time Profile	Source IP	QQ Account Pass	QQ Account Block	
LAN				tas items to show			
NAT				And reality of action			
Firewal							
Filter Setup							
DoS Defense							
MAC Block							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Central VPN Mästagement							
Gandwidth Management							
USB Application							
System Maintenance							
Diagnostics							
External Devices							
Product Registration							
	at.						

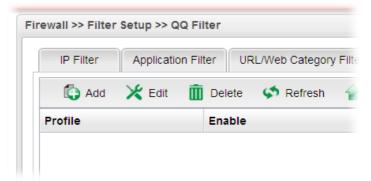
Item	Description
Add	Add a new group profile for QQ filter.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify



Item	Description
	and click the <b>Edit</b> 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 <b>Delete</b> 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 Profile	If no time schedule is set, <b>None</b> will be shown in this field.
Source IP	Display the IP object profile selected for each rule.
QQ Account Pass	Display the account name which is allowed to pass if the selected QQ profile is enabled.
QQ Account Block	Display the account name which will be blocked if the selected QQ profile is enabled.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

## How to create a QQ Filter profile

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



3. The following dialog will appear.

Profile :	Draytek			
	Diayton			
👽 Enable				
Time Profile :	None	× 🛟		
	Any	1		
	Aron			
			_	
Source IP :			Ē.	
QQ Account Pass	Shan_T	× 🛟		
QQ Account Block	None	× 🛟		

Item	Description
Profile	Type the name of the QQ filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Use the drop down list to specify a time profile for such profile. You can click to create another new time object profile.
Source IP	Use the drop down list to specify a user profile for such profile. The select user 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.
Add	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 **Add**.
- 5. A new QQ filter profile has been added.



IP Filter	Application Filter UP	RL/Web Category Filter	QQ Filter		
🚯 Add	🔀 Edit 🛛 🛅 Delete	🔇 Refresh 🛛 😭 M	love Up 🛛 🐣 Move D	own 🕻 Rename	
Profile	Enable	Time Profile	Source IP	QQ Account Pass	QQ Account Block
Draytek	true	None	Any	Shan T	None

#### 4.4.2 DoS Defense

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

4.4.2.1 Switch
----------------

<b>Dray</b> Tek	Vigor 3900 Series	11:15:56	Login: Admin	Ê
Auto Logout : Off	Firewall >> DoS Defense >> Switch Switch System Broadcast Storm Defense : Multicast Storm Defense : Unknown Unicast Storm Defense : Unknown Multicast Storm Defense : Storm Filtering Rate :	<ul> <li>Enable (a) Disable</li> <li>Enable (b) Disable</li> <li>Enable (c) Disable</li> <li>Enable (c) Disable</li> <li>1</li> </ul>	Apply	Cancel
External Devises				

Item	Description
Broadcast Storm Defense	Click <b>Enable</b> to block the packets attacks coming from broadcast storm.
Multicast Storm Defense	Click <b>Enable</b> to block the packets attacks coming from multicast storm.
Unknown Unicast Storm Defense	Click <b>Enable</b> to block the packets attacks coming from unknown unicast storm.
Unknown Multicast Storm Defense	Click <b>Enable</b> 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.

## 4.4.2.2 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.

<b>Dray</b> Tek	Vigor 3900 Se	ries		10:38:57	Login: Admin	Ð
	Firewall >> DoS Defense >> Sys	tem				0
Auto Logout : 5Min 💌	Switch System					
Quick Start Wizard	oman oyuan					
Online Status	Enable					
WAN	Block SYN Flood	( ) Enable ( ) Disable				
LAN	SYN Flood Threshold :		Packets/Second			
NAT		500	Packets/Second			
Firewall	SYN Flood Timeout :	10				
Filter Setup	Block ICMP Flood :	🔵 Enable 💿 Disable				
DoS Defense MAC Block	ICMP Flood Threshold :	500	Packets/Second			
Objects Setting	ICMP Flood Timeout :	10				
User Management	Block UDP Flood	🔵 Enable   💿 Disable				
Applications	UDP Flood Threshold :	1500	Packets/Second			
VPN and Remote Access	UDP Flood Timeout :	10				
Certificate Management	Block Port Scan :	Enable     O     Disable				E
SSL VPN						
Central VPN Management	Port Scan Threshold :	500	Packets/Second			
Bandwidth Management	Block IP Options	🔵 Enable 💿 Disable				
USB Application	Block Land :	🔵 Enable   💿 Disable				
System Maintenance	Block SMURF :	🔵 Enable   💿 Disable				
Diagnostics	Block Trace Route :	( Enable ) Disable				
External Devices Product Registration	Block SYN Fragment :	C Enable ( Disable				
Product Registration	_	0 0				
	Block Fraggle :	💮 Enable   💿 Disable				
	Block Tear Drop :	🔵 Enable   💿 Disable				
	Block Ping of Death :	🔵 Enable   💿 Disable				
	Block ICMP Fragment :	🔵 Enable 💿 Disable				
	Diaak Unknown Drataaal					-
					💾 Apply	🔇 Cancel

Available parameters are	listed as follows:
--------------------------	--------------------

Item	Description
Enable	Check the box to enable this profile.
Block SYN Flood	Click <b>Enable</b> 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 <b>300</b> packets per second.
SYN Flood Timeout	The default setting for timeout is <b>10</b> seconds.
Block ICMP Flood	Click <b>Enable</b> 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 <b>300</b> packets per second.
ICMP Flood Timeout	The default setting for timeout is <b>10</b> seconds.
Block UDP Flood	Click <b>Enable</b> 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

Item	Description
	randomly discard the subsequent UDP packets within the user-defined timeout period.
UDP Flood Threshold	The default setting for threshold is <b>300</b> packets per second.
UDP Flood Timeout	The default setting for timeout is <b>10</b> seconds.
Block Port Scan	Click <b>Enable</b> 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 <b>300</b> pps (packets per second).
Block IP Options	Click <b>Enable</b> 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 <b>Enable</b> 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 <b>Enable</b> to activate the Block Smurf function. The router will reject any ICMP echo request destined for the broadcast address.
Block Trace Route	Click <b>Enable</b> to activate the Block Trace Route function.
Block SYN Fragment	Click <b>Enable</b> to activate the Block SYN fragment function. Any packets having the SYN flag and fragmented bit sets will be dropped.
Block Fraggle	Click <b>Enable</b> to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet are blocked.
Block Tear Drop	Click <b>Enable</b> 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 <b>Enable</b> 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 <b>Enable</b> to activate the Block ICMP fragment function. Any ICMP packets with fragmented bit sets are dropped.
Block Unknown Protocol	Click <b>Enable</b> 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.



#### 4.4.3 MAC Block

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

<b>Dray</b> Tek	Vigor3								₽
	Firewall >> MAC	Block							
uto Logout : 5Min 🗸	MAC Block								
Quick Start Wizard	hhA 🗿	tiha 🛠	m Delete	🔹 Refresh	🕻 Rename			Profile Number	Limit: 10
Online Status	Profile	~			Enable		MAC Address		
WAN	Profile				Ellable		MAC Address		
LAN						No items to show.			
NAT Firewall									
Filter Setup									
DoS Defense									
MAC Block									
Objects Setting									
User Management									
Applications									
VPN and Remote Access									
Certificate Management									
SSL VPN									
Central VPN Management									
Bandwidth Management									
USB Application									
System Maintenance									
Diagnostics									
External Devices									
Product Registration									

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
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.
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.

MAC Block				
🚯 Add	🔀 Edit	前 Delete	< Refresh	🔓 Renam
Profile				Enable

3. The following dialog will appear.

MAC Block						-×
Profile :	MB_1					
🔽 Enable						
MAC Address :	00 : 50	: 7F	: CA	: BE	: 9D	
					Apply 🔞 C	ancel

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.

Fir	ewall >> MAC	Block			
	MAC Block				
	🚯 Add	🔀 Edit	🔟 Delete	< Refresh	🔩 Rename
	Profile				Enable
	MB_1				true

# 4.5 Objects Setting

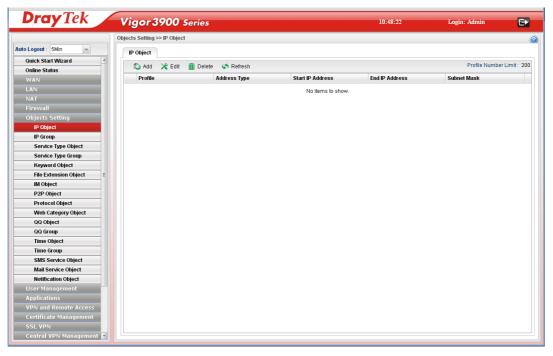
Vigor3900 allows users to set different filter profiles based on IP, service type, keyword, file extension, instant message application, P2P application, protocol application, web category, QQ application, time setting, SMS service, mail service and notification. These objects setting profiles can be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

Objects S	Setting
IP Obje	ct
IP Grou	ıp.
Service	e Type Object
Service	e Type Group
Keywo	rd Object
File Ext	ension Object
IM Obje	ect
P2P Ob	ject
Protoc	ol Object
Web Ca	ategory Object
QQ Obj	ect
QQ Gro	up
Time O	bject
Time G	roup
SMS Se	ervice Object
Mail Se	ervice Object
Notifica	ation Object

#### 4.5.1 IP Object

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

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



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 <b>Edit</b> 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 <b>Delete</b> 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 <b>Start IP Address</b> only when you choose <b>Range</b> as the <b>Address Type</b> .
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.

P (	Object			
ľ	👌 Add	🔀 Edit	面 Delete	娕 Refresh
	Profile			Address Type

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.  Range Single Range Subnet
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 <b>Subnet</b> as <b>Address Type</b> .
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.

🕼 Add 🛛 🗶 Edit 🛛 👖	Delete 🗳 Refresh			Profile Number Li
Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
IP_object_1	Subnet	192.168.1.78		255.255.255.0

## 4.5.2 IP Group

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

Dray Tek	Vigor 3900 Se	ries	1	0:54:07	Login: Admin	Ð
	Objects Setting >> IP Group					
o Logout : 5Min 👻	IP Group					
Quick Start Wizard						
Online Status	🕼 Add 🔀 Edit 👖	Delete 🗳 Refresh			Profile Number L	urriit. a
WAN	Group Name	D	Description	Objects		
N			No items to show.			
AT						
irewall						
bjects Setting						
IP Object						
IP Group						
Service Type Object						
Service Type Group						
Keyword Object						
File Extension Object 🛛 🗉						
IM Object						
P2P Object						
Protocol Object						
Web Category Object						
QQ Object						
QQ Group						
Time Object						
Time Group						
SMS Service Object						
Mail Service Object						
Notification Object						
ser Management						
pplications						
'PN and Remote Access						
Certificate Management						
SSL VPN						
Central VPN Management 🖃						

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 <b>Edit</b> 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 <b>Delete</b> 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.

IP Group			
🚯 Add	🔀 Edit	前 Delete	< Refresh
Group Name	1		

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 <b>Objects</b> <b>Setting&gt;&gt;IP Object</b> will be seen here. To clear the selected one, click to remove current object selections.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

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

5. A new IP Group profile has been created.



## 4.5.3 Service Type Object

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

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

<b>Dray</b> Tek	Vigor 3900	Series		1	0:58:27 L	ogin: Admin	₽
	Objects Setting >> Service	e Type Object					
nto Logout : 5Min 👻	Service Type Object						
Quick Start Wizard						Profile Number Lin	
Online Status	🕼 Add 🔀 Edit	🛄 Delete 🛭 娕 Refre:	sh			Frome Number Lin	int. 9
WAN	Profile	Protocol	Source Port Start	Source Port End	Destination Port Start	Destination Port End	
LAN	1 AUTH	TCP	1	65535	113	113	-
NAT	2 BGP	TCP	1	65535	179	179	
Firewall	3 BOOTPCLIENT	UDP	1	65535	68	68	
Objects Setting	4 BOOTPSERVER	UDP	1	65535	67	67	
IP Object	5 CU_SEEME_HI	TCP/UDP	1	65535	24032	24032	
IP Group	6 CU_SEEME_LO	TCP/UDP	1	65535	7648	7648	
Service Type Object	7 DNS	TCP/UDP	1	65535	53	53	
Service Type Group	8 FINGER	TCP	1	65535	79	79	
Keyword Object	9 FTP	TCP	1	65535	20	21	
File Extension Object 🛛 🗉	10 H_323	TCP	1	65535	1720	1720	
IM Object	11 HTTP	TCP	1	65535	80	80	
P2P Object	12 HTTPS	TCP	1	65535	443	443	
Protocol Object	13 IKE	UDP	1	65535	500	500	
Web Category Object	14 IRC	TCP/UDP	1	65535	6667	6667	
QQ Object	15 L2TP	UDP	1	65535	1701	1701	
QQ Group	16 NEWS	TCP	1	65535	144	144	
Time Object	17 NFS	UDP	1	65535	2049	2049	
Time Group	18 NNTP	TCP	1	65535	119	119	
SMS Service Object	19 PING	ICMP	1	65535	1	65535	
Mail Service Object	20 POP3	TCP	1	65535	110	110	
Notification Object	21 PPTP	TCP	1	65535	1723	1723	
User Management	22 RCMD	TCP	1	65535	512	512	
Applications	23 REAL_AUDIO	TCP	1	65535	7070	7070	
VPN and Remote Access	24 RTSP	TCP/UDP	1	65535	554	554	
Certificate Management	25 SFTP	TCP	1	65535	115	115	
SSL VPN	26 SMTP	TCP	1	65535	25	25	

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (96) of the object profiles to be created.



Item	Description
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.
<b>Destination Port Start</b>	Display the starting destination port for such profile.
<b>Destination Port End</b>	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.

Service Type	Object		
🚺 Add	🔀 Edit	🔟 Delete	📢 Refresh
Profile	Proto	ocol	Source Port 9

3. The following dialog will appear.

Profile :	Others		
Protocol :	тср	~	
Source Port Start :	1		
Source Port End :	65535		
Destination Port Start	1		
Destination Port End:	65535		

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.





Item	Description
	Type a port number $(0 - 65535)$ as the starting source port.
Source Port End	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number $(0 - 65535)$ as the ending source port.
Destination Port Start	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number (0 – 65535) as the starting destination port.
Destination Port End	It is available for TCP/UDP protocol. It can be ignored for ICMP. Type a port number $(0 - 65535)$ as the ending destination port.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving anything.

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

	TCP/UDP			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			111			

## 4.5.4 Service Type Group

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

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

<b>Dray</b> Tek		Vigor 3900 Series	12:00:44	Login: Admin	E
		Objects Setting >> Service Type Group			
ito Logout : Off 🛛 👻		Service Type Group			
Firewall		Add 🔀 Edit 🛅 Delete	K Refresh		Profile N
Objects Setting		Group Name	Description	Objects	
IP Object				,	
IP Group					
Service Type Object					
Service Type Group					
Keyword Object					
File Extension Object					
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
QQ Object					
QQ Group					
Time Object					
Time Group					
SMS Service Object					
Mail Service Object					
Notification Object					
User Management					
Applications	-	4			•

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 <b>Edit</b> 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 <b>Delete</b> 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.

C	Cross Dept		
Group Name :	cross_bept	_	
Description :	Used for departments	(Optional)	
Objects :	AUTH V	٢	

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 <b>Objects Setting&gt;&gt;Service Type Object</b> 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.

Service Type Group				
💱 Add 🛛 🔀 Edit	🔟 Delete	📢 Refresh		Profile
Group Name		Description	Objects	
Cross Dept		Used for departments	AUTH	

#### 4.5.5 Keyword Object

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

<b>Dray</b> Tek	Vigor 3900	Series			11:04:08	Login: Admin	Ð
Ì	Objects Setting >> Keyw	ord Object					
Logout : 5Min 🛩	Keyword Object						
Quick Start Wizard	🚯 Add 🔀 Edi	t 💼 Doloto	🗢 Refresh			Profile Numbe	r Limit : 10
Online Status		it III Delete	<ul> <li>Reliesh</li> </ul>			1101101101100	
WAN	Profile				Member		
.AN				No items	to show.		
TAL							
irewall							
bjects Setting							
IP Object							
IP Group							
Service Type Object							
Service Type Group Keyword Object							
File Extension Object =							
IM Object							
P2P Object							
Protocol Object							
Web Category Object							
QQ Object							
QQ Group							
Time Object							
Time Group							
SMS Service Object							
Mail Service Object							
Notification Object							
ser Management							
pplications							
PN and Remote Access							
ertificate Management							
SL VPN							
Central VPN Management 🖃							

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (100) of the object profiles to be created.



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

## How to create a new keyword object profile

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

Keywor	d Obje	ect		
	Add	🔀 Edit	前 Delete	📢 Refrest
Profile				

3. The following dialog will appear.

yword Obje	ct	-8
Profile :	K0_1	
	🏠 Add  🗎 Save	Profile Number Limit: 64
	Member	
Member :	game	Ē
		🛗 Apply 🛛 🐼 Cancel

Available parameters are listed as follows:

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

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



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



## 4.5.6 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.

<b>Dray</b> Tek		Vigor	3900	Series		16:50:57		Login: Admin		Ð
		Objects Setting >	▹ File Extens	sion Object						
uto Logout : Off 🛛 🗸		File Extensio	n Object							
Firewall	<u> </u>	🐴 Add	🔀 Edit	m Delete	5 Refresh					Profile N
Objects Setting		Profile	Image	Video	Audio	Java	ActiveX	Compression	Execution	
IP Object		Profile	image	Video	Audio	Java	ActiveA	Compression	Execution	
IP Group					No	o items to show.				
Service Type Object										
Service Type Group										
Keyword Object										
File Extension Object										
IM Object										
P2P Object										
Protocol Object										
Web Category Object										
QQ Object										
QQ Group										
Time Object										
Time Group										
SMS Service Object										
Mail Service Object										
Notification Object										
User Management										
Applications		4								•

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 <b>Edit</b> 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 <b>Delete</b> 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
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.

File Extens	ion Object		
🚯 Ado	l 🔀 Edit	前 Delete	<b>\$</b> R
Profile	Image	Video	A

3. The following dialog will appear.

Profile :	File_Ext_1		
Image :	.bmp, .dib	~	
Video :	.mov, .mpe, .mpeg,	mr 🗸	
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

Item	Description
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.

File Extension	n Object						
🚯 Add 🔀 Edit 🏢 Delete 🗳 Refresh							
Profile	lmage	Video	Audio	Java	ActiveX	Compression	Execution
File_Ext_1	.bmpdib	.movmpemp	.au,.mp3,.m4a	.classjad	.alxapbaxs	.ace	.exeinfpif

#### 4.5.7 IM Object

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

Auto Logout : Off	ects Setting >> IM Object			
Firewall Objects Setting	IM Object	elete 🐼 Refresh Member No items to show.	WebIM	Prof
Notification Object		m		•

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Profile	Display the name of the IM object profile.
Member	Display the IM application specified in such profile.
WebIM	Display the status of IM object whether including the specified set of web IM or not.

## How to create a new IM object profile

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

IM Object			
🚯 Add	🔀 Edit	前 Delete	🖈 Re
Profile			Member

3. The following dialog will appear.

Profile :	IM_1
Member :	MSN, QQ, iCQ, iCHAT 👻
📝 WebiM	
eMessenger	
WebMSN	
Meebo*	
MessengerAdictos	
WebYahoolM	

Item	Description	
Profile	Type the name of the IM object group. The number of the characters allowed to be typed here is 10.	
Member		eations offered for you to choose. Check the o add for such profile.



Item	Description	
WebIM	It lists a package of IM application based on web page. You may check the box to include all of them.	
Apply	Click it to save the configuration.	
Cancel	Click it to exit the dialog without saving the configuration.	

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

IM Object		
🚯 Add 🛛 🔀 Edit	🏢 Delete 🛛 📢 Refresh	
Profile	Member	WebIM
v1_1	MSN,QQ,ICQ,ICHAT	enable

#### 4.5.8 P2P Object

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

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

<b>Dray</b> Tek		Vigor 3900 Serie	<b>s</b> 16:57:17	Login: Admin	Ð
		Objects Setting >> P2P Object			
uto Logout : Off 🛛 👻		P2P Object			
Firewall	~	🕼 Add 🔀 Edit 🛅 Delet	e 🔇 Refresh		Prof
Objects Setting			-		
IP Object		Profile	Member		
IP Group			No items to show.		
Service Type Object					
Service Type Group					
Keyword Object					
File Extension Object					
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
QQ Object					
QQ Group					
Time Object					
Time Group					
SMS Service Object					
Mail Service Object					
Notification Object	-	4	111		•

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 <b>Edit</b> 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 <b>Delete</b> 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 P2P object profile.
Member	Display the P2P application specified in such profile.



## How to create a new P2P object profile

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

P2P Object		-	
C Add	🔀 Edit	🏢 Delete	< Refresh
Profile			

3. The following dialog will appear.

Profile :	P2P_Obj_1	
Member	: SoulSeek, eDonkey, Fa 🗸	
	·	

Available parameters are listed as follows:

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

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



5. A new P2P Object profile has been created.

P2P Object	
🚯 Add 🛛 🔀 Edit 🛚 🛅 Delete	🗇 Refresh
Profile	Member
2P_Obj_1	SoulSeek,eDonkey,FastTrack

#### 4.5.9 Protocol Object

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

<b>Dray</b> Tek		Vigor 3900 s	ieries	17:00:19	Login: Admin	e
	Ot	jects Setting >> Protocol Obj	iect			
o Logout : Off 🛛 👻		Protocol Object				
Firewall		🚯 Add 🔀 Edit	前 Delete 🛛 🔇 Re	fresh		Prof
Objects Setting		Profile	-	Member		
IP Group				No items to show.		
Service Type Object						
Service Type Group						
Keyword Object						
File Extension Object =						
IM Object						
P2P Object						
Protocol Object						
Web Category Object						
QQ Object						
QQ Group						
Time Object						
Time Group						
SMS Service Object						
Mail Service Object		4				>
Notification Object -		41				,

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be



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

## How to create a new protocol object profile

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

Protocol Object		
🚯 Add 🛛 🔀 Edit	前 Delete	🗳 Refres
Profile		

3. The following dialog will appear.

Profile :	Proto_Obj_1	
Member	: PostgreSQL, Sybase, [ 🐱	
		🛗 Apply 🛛 😡 Cance

Item	Description
Profile	Type the name of the protocol object profile. The number of the characters allowed to be typed here is 10.
Member	Several protocols offered for you to choose. Check the one (s) you want to add for such profile. MSSQL MYSQL Oracle Protocol Objec Profile : Member : PostgreSQL, Sybase, L

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

- 4. Enter all the settings and click **Apply**.
- 5. A new P2P Object profile has been created.

Protocol Object	
🕼 Add 🛛 💥 Edit 🛚 🏢 Delet	e 🗳 Refresh
Profile	Member
Proto_Obj_1	PostgreSQL,Sybase,DB2

#### 4.5.10 Web Category Object

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

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

**Note:** Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **Commtouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.

# 4.5.10.1 Web Category Object

<b>Dray</b> Tek		Vigor	3900 Series	17:04:5	0	Login: Adr	nin	E
		Objects Setting >	>> Web Category Object >> Web C	ategory Object				
ito Logout : Off 🛛 🗸		Web Categor	y Object Content Filter License					
Firewall	~	Add	🔀 Edit 🏢 Delete 🗳 R	efresh				Prof
Objects Setting		Profile	Child Protection Leisure	Business	Chatting	Computer	Other	
IP Object		Tronic	child i fotocilor Ecistic	business	chutting	compater	ounci	
IP Group				No items to s	how.			
Service Type Object								
Service Type Group								
Keyword Object								
File Extension Object	=							
IM Object								
P2P Object								
Protocol Object								
Web Category Object								
QQ Object								
QQ Group								
Time Object								
Time Group								
SMS Service Object								
Mail Service Object								
Notification Object	-	4						•

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 <b>Edit</b> 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 <b>Delete</b> button.				
Refresh	Renew current web page.				
Profile Number Limit	Display the total number (16) of the object profiles to be created.				
Profile	Display the name of the object profile.				
Child Protection	Display the items under certain category that you choose to block for protecting the children.				
Leisure	Display the items under certain category that you choose to block.				
Business	Display the items under certain category that you choose to block.				
Chatting	Display the items under certain category that you choose to block.				
Computer	Display the items under certain category that you choose to block.				

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

#### How to create a new web category object profile

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



3. The following dialog will appear.

Profile :	WCO_1		
Child Protection	Alcohol-And-Tobacco,	~	
Leisure :	Sports, Travel	~	
Business :	Web-Based-Email	~	
Chatting :	Chat	~	
Computer :	Botnets, Hacking	~	
Other :	News, Translators	~	

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 :       Image: Alcohol-And-Tobacco         Image: Criminal-And-Activity       Image: Criminal-And-Activity         Business :       Image: Gambling         Chatting :       Image: Hate-And-Intolerance         Image: Nonline       Image: Chatting					
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.

Web Catego	ry Object Content	Filter License				
🚯 Add	🔀 Edit 🛛 🕅 De	elete – 娕 Ref	resh			
Profile	Child Protection	Leisure	Business	Chatting	Computer	Other
		Sports,Travel	Web-Based-Er		Botnets,Hacki	

## 4.5.10.2 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.

<b>Dray</b> Tek	Vigor 3900	Series	17:07:08	Login: Admin	Ð
Auto Logout : Off	Objects Setting >> Web Cat		Filter License		
Objects Setting         IP Object         IP Group         Service Type Object         Service Type Group         Keyword Object         File Extension Object         IM Object         P2P Object         P2P Object         Protocol Object	Enable This Profile : Info : Serial Number : Start Date :	Activate URL disable Commouch 00033556 2012-08-07 2012-08-14			
Web Category Object           QQ Object           QQ Group           Time Object           Time Group           SMS Service Object           Mail Service Object           Notification Object				Apply	Cancel

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



# 4.5.11 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.

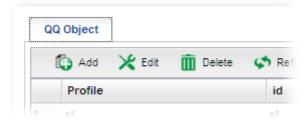
<b>Dray</b> Tek		Vi	gor 3900	Series	17:08:01	Login: Admin	Ð
		Object	s Setting >> QQ Object				
to Logout : Off 🛛 🗸		G	Q Object				
Firewall	~		🚯 Add 🔀 Edit	前 Delete 🛛 📢 Ref	resh		Prof
Objects Setting			Profile	id		Description	
IP Object						Description	
IP Group		1	all	all			
Service Type Object							
Service Type Group							
Keyword Object							
File Extension Object	-						
IM Object							
P2P Object							
Protocol Object							
Web Category Object							
QQ Object							
QQ Group							
Time Object							
Time Group							
SMS Service Object	- 11						
Mail Service Object							
Notification Object	-	4					>

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 <b>Edit</b> 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 <b>Delete</b> button.				
Refresh	Renew current web page.				
Profile Number Limit	Display the total number (16) of the object profiles to be created.				
Profile	Display the name of the QQ object profile.				
id	Display the account name of the QQ object profile.				
Description	Display a brief explanation of the QQ object profile.				

## How to create a new QQ object profile

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



3. The following dialog will appear.

Profile :	Shan_T	
	🚯 Add 🛗 Save	Profile Number Limit : 6
	id	
id :	12345678	â
Description	Office (Optio	al)

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.

G	Q Object			
	🚯 Add 🔀 Edit 🛅	Delete 🔇 📢 Refresh		
	Profile	id	Description	
1	all	all		
2	Shan_T	12345678	Office	

#### 4.5.12 QQ Group

This page allows you to group several QQ object profiles.

<b>Dray</b> Tek	Vigor 3900 Ser	ries 17:11:04	Login: Admin	E
	Objects Setting >> QQ Group			
Auto Logout : Off 🗸 🗸	QQ Group			
Firewall	🕼 Add 🔀 Edit 面 D	elete 🔇 Refresh		F
Objects Setting	Group Name	Description	Objects	
IP Object		beschption	00,000	
IP Group		No items to show.		
Service Type Object				
Service Type Group				
Keyword Object				
File Extension Object				
IM Object				
P2P Object				
Protocol Object				
Web Category Object				
QQ Object				
QQ Group				
Time Object				
Time Group				
SMS Service Object				
Mail Service Object				
Notification Object	4			•

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 <b>Edit</b> 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 <b>Delete</b> 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.

QQ Group	
🕼 Add 🔀 Edit 🝈 Delete	📢 Refresh
Group Name	Description

3. The following dialog will appear.

QQ Group		->
	QQaccount_grp_1 For Marketing Only (Optional) Shan_T ¥ X	
		🗎 Apply 🚫 Cancel

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 <b>Objects</b> <b>Setting&gt;&gt;QQ Object</b> 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.

QQ Group			
🚯 Add 🔀 Edit 👖	Delete 🔇 📢 Refresh		
Group Name 🎽	Description	Objects	
Qaccount_grp_1	For Marketing Only	Shan T	

# 4.5.13 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.

<b>Dray</b> Tek		Vigor 3	900 Se	ries	17:12:27		Login: Adm	in	Ð	
Auto Logout : Off	Obj	jects Setting >>	Time Object							
		Time Object								
Firewall		🚯 Add	🗶 Edit 🖷	Delete 🗳 Re	fresh				F	
Objects Setting		Profile	Frequency	Start Date	Start Time	End Date	End Time	Weekdays		
IP Object		FIONE	rrequency	start bate			Life fille	Weekuays		
IP Group					No items to sh	ow.				
Service Type Object										
Service Type Group										
Keyword Object										
File Extension Object =										
IM Object										
P2P Object										
Protocol Object										
Web Category Object										
QQ Object										
QQ Group										
Time Object										
Time Group										
SMS Service Object										
Mail Service Object										
Notification Object		4							121	

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 <b>Edit</b> 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 <b>Delete</b> 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.

Time Object				
🚯 Add	🔀 Edit	🇰 Dele	ete 🛛 娕 R	efre
Profile	Frequency	s	tart Date	5

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
	VVed
	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.

Time Object					
🖏 Add 🔀 Edit 📺 Delete 🛭 😒 Refresh					
Profile	Frequency	Start Date	Start Time	End Date	End Time
TimeO_1	Weekdays	2010-01-01	00:00:00	2010-01-01	00:00:00

# 4.5.14 Time Group

This page allows you to group several time object profiles.

<b>Dray</b> Tek	Vi	gor 3900 Ser	ies 10:30:41	Login: Admin	Ð
	3.6	ts Setting >> Time Group			
uto Logout : 5Min 👻	Т	me Group			
NAT		🕼 Add 🔀 Edit 🏛 D	elete 🔇 Refresh		F
Firewall		🚯 Add 🔀 Edit 🏛 D	siete 💭 Refresh		
Objects Setting	Gr	oup Name	Description	Objects	
IP Object			No items to sho	IW.	
IP Group					
Service Type Object					
Service Type Group					
Keyword Object					
File Extension Object					
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
QQ Object					
QQ Group					
Time Object					
Time Group					
SMS Service Object					
Mail Service 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 <b>Edit</b> 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 <b>Delete</b> 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.

Time Group		
🚯 Add 🔀 Kait	前 Delete	🖈 Refresh
Group Name		Description
		No iter

3. The following dialog will appear.

Group Name :	TimeGrp_1		
Description :	For Market only	(Optional)	
Objects :	Night 🗸 🗸	C	

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 <b>Objects Setting&gt;&gt;Time Object</b> 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.

Time Group			
🚯 Add 🔀 Edit 🛅 De	elete 🔇 🧐 Refresh		F
Group Name	Description	Objects	
TimeGrp_1	For Market only	Night	

# 4.5.15 SMS Service Object

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

<b>Dray</b> Tek	Vigor3	900 Serie:	<b>s</b> 10:35:36	Login:	Admin	Ð
	Objects Setting >>	SMS Service Object				
uto Logout : 5Min v	SMS Service O	bject				
Keyword Object	🕼 Add	🔀 Edit 🛛 🔟 Delete	e 📢 Refresh			F
File Extension Object	Profile	Enable	SMS Service Provi Username	Quota	Interval(s)	
IM Object			No items to show.			
P2P Object			NO ILEMS TO SHOW.			
Protocol Object						
Web Category Object						
QQ Object						
QQ Group						
Time Object						
Time Group						
SMS Service Object						
Mail Service Object						
Notification Object						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						
SSL VPN	4					•
Central VPN Management						

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 <b>Edit</b> 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 <b>Delete</b> 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.

SMS Service Object	<b>:t</b>	
🚯 Add 🛛 🔀	Edit 前 Delete	📢 Re
Profile	Enable	SMS Ser

3. The following dialog will appear.

Profile :	Line_down	
Enable		
SMS Service Provider :	kotsms.com.tw	
Username :	line1	
Password :	•••••	
Quota :	10	
Interval(s):	3	

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.

SMS Service O	bject				
🚯 Add	🗶 Edit 🛛 🔟 De	lete 🗳 Refresh			
Profile	Enable	SMS Service Provi	Username	Quota	Interval(s)
Line_down	true	kotsms.com.tw	line1	10	3

# 4.5.16 Mail Service Object

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

<b>Dray</b> Tek	Vigor	3900 s	eries	11:32:19		Login: Admin		Ð
	Objects Setting >	» Mail Service (	Object					
Auto Logout : 5Min 🗸	Mail Service	Object						
IP Object	- Ch							
IP Group	<table-cell> Add</table-cell>	🔀 Edit 🔟	🖞 Delete 🛛 🗳 Re	tresh				_
Service Type Object	Profile	Enable	Mail From	SMTP Port	SMTP Server	Authentication	User Name	
Service Type Group				No items to sho	ow.			
Keyword Object								
File Extension Object								
IM Object								
P2P Object								
Protocol Object								
Web Category Object								
QQ Object								
QQ Group								
Time Object								
Time Group								
SMS Service Object								
Mail Service Object								
Notification Object								
User Management							1	
	4			111				

Each item will be explained as follows:

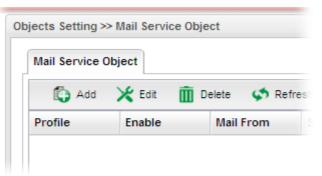
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the <b>Delete</b> 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	
V Enable		
Mail From :	carrie@draytek.com	
SMTP Port :	25	
SMTP Server:	192.168.1.98	
Authentication :	💽 Enable 🔘 Disable	
User Name :	john	
User Password		
		📄 Apply 🛛 😵 Cancel

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.
	<ul> <li>User Name – Type a name for authentication. The maximum length of the name you can set is 31 characters.</li> <li>User Password – Type a password for authentication. The maximum length of the password you can set is 31</li> </ul>
	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.

Mail Service	Object					
🟠 Add	🔀 Edit 🧃	👖 Delete 🛛 📢 Refr	resh			
Profile	Enable	Mail From	SMTP Port	SMTP Server	Authentication	User Name

# 4.5.17 Notification Object

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

<b>Dray</b> Tek	Vigor 3900	Series 12:00:37	Login: Admin	•
	Objects Setting >> Notification	on Object		
Auto Logout : Off	Notification Object			
File Extension Object	🕼 Add 🛛 💥 Edit	前 Delete 🛭 📢 Refresh		F
IM Object	Profile WAN	Disconnectio WAN Reconnection VPN Disco	nnectior VPN Reconnection Temperature	
P2P Object		No items to show.		
Protocol Object		No tena to anow.		
Web Category Object				
QQ Object				
QQ Group				
Time Object				
Time Group				
SMS Service Object				
Mail Service Object				
www.www.Notification Object				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management 🥃	4	m		•
<u> </u>				

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 <b>Edit</b> 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 <b>Delete</b> 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.

## How to create a new notification profile

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

		_				
Ι.	Notification Obje	ect				
	🚯 Add	🗶 E	dit 🛅	Delete	ø	R
	Profile	W	AN Disco	nnectio	WAN	R

3. The following dialog will appear.

Profile :	Notify_attack	
WAN Disconnection :	💿 Enable 🔘 Disable	
WAN Reconnection :	🔵 Enable 💿 Disable	
VPN Disconnection :	💿 Enable 🔘 Disable	
VPN Reconnection :	🔿 Enable 💿 Disable	
Temperature :	🔵 Enable 💿 Disable	

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	<b>Enable</b> – When disconnection happened to WAN interface, the router system will send the alert message to the recipient.
WAN Reconnection	<b>Enable</b> - When reconnection happened to WAN interface, the router system will send the alert message to the recipient.
VPN Disconnection	<b>Enable</b> – When disconnection happened to a VPN tunnel, the router system will send the alert message to the recipient.
VPN Reconnection	<b>Enable</b> - When reconnection happened to a VPN tunnel, the router system will send the alert message to the recipient.



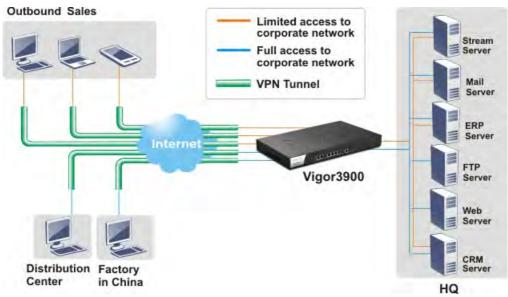
Temperature	<b>Enable -</b> When the temperature is out of range, the router system will send the alert message to the recipient.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

🖏 Add	🔀 Edit 🛛 前 Del	ete 🗳 Refresh			
Profile	WAN Disconne	ectio WAN Reconnection	VPN Disconnection	VPN Reconnection	Temperature
Notify attack	Enable	Disable	Enable	Disable	Disable

# 4.6 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:

User Management
General Setup
User Profile
User Group
RADIUS
LDAP / Active Directory
Applications

#### 4.6.1 General Setup

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

#### 4.6.1.1 General Setup

There are two modes, Rule-Based and User-Based which are necessary to be configured to meet different requirements for users. Rule-Based is configured in default.

<b>Dray</b> Tek	Vigor 3900 s	Series 11:53:	31 Logi	in: Admin	E>
	User Management >> General S	Setup >> General Setup			
to Logout : Off 🛛 👻	General Setup User-Based	d Firewall Status			
NAT					
Firewall	Mode : Rule	e-Based 🗸			
Objects Setting					
User Management					
General Setup					
User Profile					
User Group					
RADIUS					
LDAP / Active Directory					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Bandwidth Management					
System Maintenance					
Diagnostics					
External Devices				💾 Apply 🛛 🙆 Ca	ancel
Product Registration					
					Ì
<b>Drav</b> Tek	Vigor 3900		-24 Log	in: Admin	
<b>Dray</b> Tek	Vigor 3900 s		:34 Log	in: Admin	C>
	Vigor 3900 S		:34 Log	in: Admin	
to Logout : Off	User Management >> General		:34 Log	in: Admin	
io Logout : Off	User Management >> General	Setup >> General Setup	:34 Log	in: Admin	
to Logout : Off	User Management >> General	Setup >> General Setup	:34 Log	in: Admin	E*
o Logout : Off v LAN A NAT Firewall	User Management >> General	Setup >> General Setup d Firewall Status User-Based	:34 Log	in: Admin	E*
to Logout : Off  LAN AT Firewall Objects Setting	User Management >> General General Setup User-Base Mode :	Setup >> General Setup Id Firewall Status User-Based Local V	:34 Log	in: Admin	E*
to Logout : Off	User Management >> General General Setup User-Base Mode :	Setup >> General Setup  d Firewall Status  User-Based v  Local v  Firewall Objects	:34 Log	in: Admin	E*
o Logout: Off v LAN AT Firewall Objects Setting User Management General Setup	User Management >> General General Setup User-Base Mode :	Setup >> General Setup  d Frewall Status  User-Based  User-Based  Frewall Objects  P Object			C)
o Logout: Off v LAN AT NAT Firewall Objects Setting User Management General Setup User Profile	User Management >> General General Setup User-Base Mode :	Setup >> General Setup d Frewall Status User-Based v Local v Frewall Objects P Object P Object P Object	34 Log Address Type Subnet	In: Admin Start IP Address 192.168.1.78	
o Logout: Off v LAN AT NAT Firewall Objects Setting User Management General Setup User Profile User Group	User Management >> General General Setup User-Base Mode :	Setup >> General Setup  d Frewall Status  User-Based  User-Based  Frewall Objects  P Object	Address Type	Start IP Address	
o Logout : Off v LAN AT Firewall Objects Setting User Management General Setup User Profile User Group RADIUS LDAP / Active Directory	User Management >> General General Setup User-Base Mode :	Setup >> General Setup d Frewall Status User-Based v Local v Frewall Objects P Object P Object P Object	Address Type	Start IP Address	
o Logout : Off v LAN AT NAT Firewall Objects Setting User Management General Setup User Profile User Group RADIUS LDAP / Active Directory	User Management >> General General Setup User-Base Mode :	Setup >> General Setup d Frewall Status User-Based v Local v Frewall Objects P Object P Object P Object	Address Type	Start IP Address	
to Logout : Off  LAN NAT Firewall Objects Setting User Management General Setup User Profile User Group RADIUS LDAP / Active Directory Applications	User Management >> General General Setup User-Base Mode :	Setup >> General Setup d Frewall Status User-Based v Local v Frewall Objects P Object P Object P Object	Address Type	Start IP Address	
to Logout : Off	User Management >> General General Setup User-Base Mode : L Authentication Type : L	Setup >> General Setup d Frewall Status User-Based v Local v Frewall Objects Pobject Profile P_object_1	Address Type	Start IP Address	
to Logout : Off  LAN NAT Firewall Objects Setting User Management General Setup User Profile User Group RADIUS LDAP / Active Directory Applications VPN and Remote Access	User Management >> General General Setup User-Base Mode :	Setup >> General Setup d Frewall Status User-Based User-Based Frewall Object Frewall Object Pobject Pobject_1 Pobjec	Address Type Subnet	Start IP Address 192.168.1.78	
to Logout : Off  LAN NAT Firewall Objects Setting User Management General Setup User Profile User Group RADIUS LDAP / Active Directory Applications VPN and Remote Access Certificate Management	User Management >> General General Setup User-Base Mode : L Authentication Type : L	Setup >> General Setup  d Frewall Status  User-Based  User-Based  Frewall Objects  P Object  P Object  P Cobject_1  P Group  P Group Group Name	Address Type Subnet	Start IP Address 192.168.1.78	
to Logout : Off  LAN LAN NAT Firewall Objects Setting User Management General Setup User Group RADUS LDAP / Active Directory Applications VPN and Remote Access Certificate Management SSL VPN	User Management >> General General Setup User-Base Mode : L Authentication Type : L	Setup >> General Setup d Frewall Status User-Based User-Based Frewall Object Frewall Object Pobject Pobject_1 Pobjec	Address Type Subnet	Start IP Address 192.168.1.78	
LAN AT NAT Firewall Objects Setting User Management General Setup User Group RADIUS LDAP / Active Directory Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management	User Management >> General General Setup User-Base Mode : L Authentication Type : L	Setup >> General Setup  d Frewall Status  User-Based  User-Based  Frewall Objects  P Object  P Object  P Cobject_1  P Group  P Group Group Name	Address Type Subnet	Start IP Address 192.168.1.78 scription up for sales	
to Logout : Off	User Management >> General General Setup User-Base Mode : Authentication Type : White IP List :	Setup >> General Setup d Firewall Status User-Based v Local v Firewall Objects P Object Profile P_object_1 P_object_1 P_object_1 P_object_1 P_object_1 P_object_1	Address Type Subnet	Start IP Address 192.168.1.78 scription up for sales	

Available parameters will be explained as follows:

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



Item	Description
	User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.
	<b>Rule-Based</b> –If you choose such mode, the router will apply the filter rules configured in <b>Firewall&gt;&gt;Filter Setup</b> to the users.
Authentication Type	Under User-Based mode, please specify the authentication type.
LDAP Profiles	It is available when <b>LDAP</b> is selected as <b>Authentication</b> <b>Type</b> . You have to specify one profile from the drop down list for authentication.
White IP List	Under User_Based mode, check the IP object and/or IP group profiles you want.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

#### 4.6.1.2 User-Based Firewall Status

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

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

		8900 s	eries	11:28:38		Login: Adm		E>
	User Managemen	it >> General Se	etup >> User-Based	Firewall Status				
o Logout : 5Min 👻	General Setup	User-Based	d Firewall Status					
Quick Start Wizard								
Online Status	S Refres	h	Auto Ref	resh: 10 Second	ds 🗸			
WAN	User Name	IP	Allow Time	Start Time	End Time	Rest Time	Disconnect	
LAN				No items to sh	now.			
NAT								
Firewall								
Objects Setting								
User Management								
General Setup								
User Profile								
User Group								
RADIUS								
LDAP / Active Directory								
Applications								
VPN and Remote Access								
Certificate Management								
SSL VPN								
Bandwidth Management 📃								
System Maintenance								

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 <b>Refresh</b> button is clicked.
User Name	Display the name of the client (wireless station) who accesses into Internet through the wireless connection.
IP	Display the IP address of the wireless station.
Allow Time	Display the total connection time allowed for the wireless station.
Start Time	Display the starting time of the wireless station.
End Time	Display the ending time of the wireless station.
Rest Time	Display the rest time for the wireless station to browse the Internet.
Disconnect	It is available for the administrator to turn off a specific user's connection immediately.

Available parameters will be explained as follows:

#### 4.6.2 User Profile

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

<b>Dray</b> Tek	Vi	gor 3	900	Serie	s					16:28:33		login: Adm	in	B
) [	User	Managem	ent >> U:	ser Profi	le									
uto Logout : Off 🛛 🖌	Us	ser Profile												
Quick Start Wizard				-								Durich		
Online Status		🕼 Add	🔀 Edi	t 🔟 C	elete	🤝 Refre	esh					Profile	Number Li	mit : 50
WAN		Userna	Enable	System	Group	PPTP	L2TP	SSL Tu	DHCP from	Use Static IP	A PPPoE	Qu Tim	e Traffic Q	uota(N
LAN	1	Aron	true	false	User	Enable	Disable	Enable	lan1	Dis:	Disable	No 0/-1	0/-1	
NAT														
Firewall														
Objects Setting														
User Management														
General Setup														
User Profile														
User Group														
RADIUS														
LDAP / Active Directory														
Applications														
VPN and Remote Access														
Certificate Management														
SSL VPN														
Central VPN Management														
Bandwidth Management														
USB Application														
System Maintenance														
Diagnostics														
External Devices														
Product Registration														
	4													

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 <b>Edit</b> 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 <b>Delete</b> 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.
Group	Display the group name that the user profile belongs to.
РРТР	Display the status of PPTP/L2TP connection for such user profile.

Item	Description
L2TP	Display the LAN profile that such profile belongs to.
DHCP from	Display the LAN profile that DHCP server used for assigning IP address(es).
Static IP Address	Display the IP address for such user profile which accesses Internet with PPTP/L2TP connection.
Use mOTP	Display if mOTP is activated (enable or disable) or not.
PPPoE	Display the status of PPPoE connection for such user profile. (enable or disable)
Quota Reset	Display the frequency for the quota reset.
Time Quota(min)	Display the time quota allowed for such user profile.
Traffic Quota(MB)	Display the traffic quota allowed for such user profile.

#### How to create a new User Profile

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

Us	er Profil	е						
	🏠 Add		🗶 E	dit	Ô	Delete	<b>\$</b> F	lefresh
	User	Ena	Syste	Gro	РРТІ	L2TP	SSL Tu	PPPoE

3. The following dialog will appear.

er Profile		
Username :	Allen	
🕼 Enable		
Password :		
Idle Timeout (sec) :	300	
Usage Time (min) :	480 (for User-based Firewall)	
Account Login Quota :	-1 (for User-based Firewall)	
System User :	false 👻	
PPTP :	🔵 Enable 💿 Disable	
L2TP :	🔵 Enable 💿 Disable	
		-
DHCP from :	lan1 👻	
Static IP Address :		
Use mOTP :	○ Enable    Disable	
SSL Proxy :	× ×	
SSL Application(VNC)		
SSL Application(RDP) :		
<ul> <li>for PPPoE Server sett</li> </ul>		
PPPoE :	CENABLE  CENABLE	
Quota Reset :	None	
Time Quota(min) :	-1 for unlimited	
Current Time Used(min)	0 Reset	F

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., <i>lug123</i> , <i>wug123</i> , <i>wug456</i> , etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.
Idle Timeout (sec)	If the user is idle over the limitation of the timer, the <b>network connection will be stopped for such user.</b> By default, the Idle Timeout is set to 300 seconds.
Usage Time (min)	It means the maximum usage duration for the user. By default, the Usage Time is 480 minutes.
Account Login Quota	It means the maximum persons allowed logging into Internet via Vigor router. The range is from 1 to 2551 means not limit; 0 means No access.
System User	Choose <b>True</b> to allow the user accessing into WUI of Vigor3900 via the username and password above. If you choose <b>False</b> , you can set SSL for such profile.
PPTP/L2TP	Click <b>Enable</b> to make network connection through PPTP/L2TP protocol for users who access into Internet via such profile.
DHCP from	Choose a LAN profile for DHCP server.
Static IP Address	Type an IP address for such user profile which accesses Internet with PPTP/L2TP connection.
Use mOTP	Click <b>Enable</b> to make the authentication with mOTP function. <b>mOTP PIN Code -</b> Type the code for authentication (e.g, 1234). <b>mOTP secret -</b> Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
SSL Proxy	It is available when <b>System User</b> is set with <b>false</b> . The web proxy over SSL will be applied for VPN. To clear the selected one, click to remove current object
SSL Application (VNC)	selections.         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 is to remove current object selections.
SSL Application (RDP)	It is available when <b>System User</b> is set with <b>false</b> . Choose one of the SSL Application profiles (RDP) for applying into this profile. To clear the selected one, click to remove current object selections.



For PPPoE Server se	ttings
PPPoE	Click <b>Enable</b> to activate related PPPoE configuration.
Quota Reset	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).
	<b>Everyday</b> – The quota for PPPoE will be reset every day.
	<b>Everymonth</b> – 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. <b>Reset -</b> 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.
	<b>Reset -</b> 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.
	<b>Enable</b> – Click it to enable the function.
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.

	🕼 Add	🖌 Edi	t 前 D	oloto	🔹 Refre	ch					Profile N	Jumber Limit : 500
	-		System		-	_	SSL Tur	DHCP from	Use Static IP A	<b>PPPoE</b>	Qu Time	Traffic Quota(N
1	Aron	true	false	User	Enable	Disable	Enable	lan1	Dis:	Disable	No 0/-1	0/-1
2	Allen	true	false	User	Disable	Enable	Disable	lan1	Ena	Enable	Ev: 0/-1	0/-1

# 4.6.3 User Group

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

][1	ser Management >> User Group				
to Logout : Off	User Group				
Quick Start Wizard					
Online Status	🕼 Add 🛛 🗶 Edit  🔟 Deleti	e 🗳 Refresh		Profile Number Limit : 5	.01
WAN	Usergroup	Enable	Member		
LAN	1 Grp_marketing	true	Aron,Allen		
NAT					
Firewall					
Objects Setting					
User Management					
General Setup					
User Profile					
User Group					
RADIUS					
LDAP / Active Directory					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Management					
Bandwidth Management					
USB Application					
System Maintenance					
Diagnostics					
External Devices					
Product Registration					

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (200) of the object profiles to be created.
Usergroup	Display the name of the user group.
Enable	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.

e B	م ما ما		💼 Delete	( Defreek
	Add	🔀 Edit	III Delete	🔇 Refresh
1	Usergro	oup		Enable
				Ν

3. The following dialog will appear.

User Group	Enable	- Member
Usergroup :	Grp_marketing	
V Enable Member :	Aron,Allen 🗸 🗙	
		💾 Apply 🔞 Cancel

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.



🚯 Add 🛛 🔀 Edit	🔟 Delete 🛛 📢 Refresh		
Usergroup	Enable	Member	
Grp_marketing	true	Aron, Allen	

#### **4.6.4 RADIUS**

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

<b>Dray</b> Tek	Vigor 3900 Series	16:41:30	Login: Admin	Ð
	User Management >> RADIUS			2
Auto Logout : Off 🛛 🗸	RADIUS			
Quick Start Wizard	NADIO3			
Online Status	Enable			
WAN				
LAN	Server IP Address :			
NAT	Destination Port : 1812	_		
Firewall	Shared Secret :			
Objects Setting				
User Management				
General Setup				
User Profile				
User Group				
RADIUS				
LDAP / Active Directory				
Applications				
VPN and Remote Acces:				
Certificate Management				
SSL VPN				
Central VPN Manageme				
Bandwidth Management				
USB Application				
System Maintenance				
Diagnostics			🗎 Apply (	🔰 Cancel
External Devices 🚽				

Item	Description
Enable	Check this box to enable such profile.
Server IP Address	Enter the IP address of RADIUS server.
<b>Destination Port</b>	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.



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

#### 4.6.5 LDAP/Active Directory

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

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

<b>Dray</b> Tek	Vigo	r 39(	00 Series	16:43:4	6 Login: Admin	Ð
	User Mana	gement :	>> LDAP / Active Directory			(3)
Auto Logout : Off		Active Di	rectory			
Quick Start Wizard			-			
Online Status	😱 P	kdd 🗙	Edit 🏢 Delete 🛭 娕 Refresh			Profile Nui
WAN	Profile	Enable	Bind Typ: Server IP Address	Port	Commo Base DN Group D Regular	Regular F
LAN	profile	false		389		
NAT						
Firewall						
Objects Setting						
User Management						
General Setup						
User Profile						
User Group						
RADIUS						
LDAP / Active Directory						
Applications						
VPN and Remote Acces:						
Certificate Management						
SSL VPN						
Central VPN Manageme						
Bandwidth Management						
USB Application						
System Maintenance						
Diagnostics						
External Devices	4		III			>

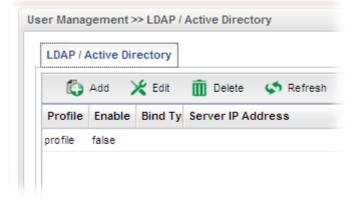
Available parameters are listed as follows:

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.

Item	Description
Profile	Display the name of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
Bind Type	Display the type setting selected for such profile.
Server IP Address	Display the IP address of the LDAP server.
Port	Display the port number set for such profile.
Common Name Identifier	Display the name for identification.
Base DN	Display the configured Base DN if Bind Type is set with Simple Mode.
Group DN	Display the configured Group DN if Bind Type is set with Simple Mode.
Regular DN	Display the configured regular DN if Bind Type is set with Regular Mode.
Regular Password	Display the configured regular password if Bind Type is set with Regular Mode.

## How to create a new LDAP/Active Directory Profile

- 1. Open User Management>>LDAP/Active Directory.
- 2. Simply click the **Add** button.



3. The following dialog will appear.

LDAP / Active Directory		-×
Profile :	rd_1	
Tenable		
Bind Type :	Simple Mode 🗸	
Server IP Address :	192 . 168 . 1 .	220
Port :	389	
Common Name Identifier :	cn	(Optional)
Base DN:		
Group DN :		(Optional)
Regular DN :		(Optional)
Regular Password :		(Optional)
Usage Time (min) :	480	(for User Management)
		📑 Apply 🐼 Cancel

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 " <b>Base Distinguished Name</b> ". 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 <b>Regular Mode</b> is selected as <b>Bind Type.</b>
<b>Regular Password</b>	Specify a password if <b>Regular Mode</b> is selected as <b>Bind Type.</b>
Usage Time	It means the maximum usage duration for LDAP authentication. By default, the Usage Time is 480 minutes.
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.

Active Dir	ectory							Profile Nu
			Port	Commo	Base DN	Group D	Regular	Regular f
false			389					
true	Simple 192.168.1	.220	389	cn	ou=simp	cn=rd1		
	Active Dir dd X Enable false	Active Directory dd 💥 Edit ៣ Delete Enable Bind Tyr Server IP false	Active Directory dd 🔆 Edit 🔟 Delete 🗢 Refresh Enable Bind Tyr Server IP Address false	dd X     Edit     Im Delete     Refresh       Enable     Bind Tyr     Server IP Address     Port       false     389	Active Directory dd 🔀 Edit 🍈 Delete 🗢 Refresh Enable Bind Tyr Server IP Address Port Common false 389	Active Directory       dd X Edit     Im Delete     Refresh       Enable     Bind Tyr     Server IP Address     Port     Commo Base Div       false     389	Active Directory dd 🔀 Edit 🍈 Delete 🗇 Refresh Enable Bind Tyr Server IP Address Port Commo Base DN Group D false 389	Active Directory dd 🔀 Edit 🕅 Delete 🗢 Refresh Enable Bind Tyr Server IP Address Port Commo Base DN Group D Regular false 389

## 4.7 Application

Below shows the menu items for Applications.

Applications	
Dynamic DNS	
GVRP	
IGMP Proxy	
UPnP	
High Availability	
Wake on LAN	
SMS / Mail Alert Service	

#### 4.7.1 Dynamic DNS

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

<b>Dray</b> Tek	Vigor 3900 Se	1103	3 Login: Admin	Ð
	Applications >> Dynamic DN	S >> Status		
luto Logout : Off 🛛 👻	Status Setting	DDNS log		
Quick Start Wizard				
Online Status	S Refresh	Auto Refresh : 10 Seconds 🛩		
WAN	Profile	Status	Domain Name	
LAN	ddns1	Not Connected		
NAT	ddns2	Not Connected		
Firewall	ddns3	Not Connected		
Objects Setting	ddns4	Not Connected		
User Management	ddns5	Not Connected		
Applications	ddns6	Not Connected		
Dynamic DNS	ddns7	Not Connected		
GVRP	ddns8	Not Connected		
IGMP Proxy	ddns9	Not Connected		
UPnP	ddns10	Not Connected		
High Availability				
Wake on LAN				
SMS / Mail Alert Service				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Manageme				
Bandwidth Management				
USB Application				

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.



### 4.7.1.1 Status

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

Status S	etting DDNS log	1		
< Refresh	A	uto Refresh : 10 Seconds 👻		
Profile		Status	Domain Name	
idns1		Not Connected		
idns2		Not Connected		
idns3		Not Connected		
idns4		Not Connected		
idns5		Not Connected		
dns6		Not Connected		
idns7		Not Connected		
dns8		Not Connected		
dns9		Not Connected		
idns10		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 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.

### 4.7.1.2 Setting

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

Status	Setting	DDNS log						
🔀 Edit	💾 Force	Update						
Profile	Enable	WAN Profile	Routing Pol	Service Pro	Service Typ	Domain Nar	IP Source	Force update
ddns1	true	wan1	selected_wa	dyndns	Dynamic	draytek	My WAN IP	
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			
ddns9	false	wan1		dyndns	Dynamic			
ddns10	false	wan1		dyndns	Dynamic			

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 <b>Edit</b> 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.

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 💿 Disab	le
Backup MX :	🔵 Enable 💿 Disab	le
Mail Extender :		(Optional)
Force update interval :	14400	Minutes (1~43200)

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. <pre>selected_wan_first selected_wan_first selected_wan_only Dynamic</pre> 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.

Status	Setting	DDNS log					
🔀 🔀	it 🔡 Force	e Update					
Profile	Enable	WAN Profile	Routing Poli	Service Pro	Service Typ	Domain Nar	Force update interval
ddns1	true	wan1	selected_wa	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		

### 4.7.1.3 DDNS Log

This page displays the information related to all DDNS.

Status Setting DDNS log	
🗇 Refresh	
Gearch	Ø0
Log	
2011/01/02 12:51:32 gethostbyname() failed: members.dyndns.org	*
2011/01/02 12:51:22 Connecting to DDNS server	E
2011/01/02 12:51:21 gethostbyname() failed: members.dyndns.org	
2011/01/02 12:51:11 Connecting to DDNS server	
2011/01/02 12:51:10 gethostbyname() failed: members.dyndns.org	
2011/01/02 12:51:00 Connecting to DDNS server	
011/01/02 12:51:00 User-Agent: Vigor3900 series, Host: members.dyndns.org	
2011/01/02 12:51:00 >>>>> DDNS1 is updateing.<<<<<	
2011/01/02 12:40:59 gethostbyname() failed: members.dyndns.org	
2011/01/02 12:40:49 Connecting to DDNS server	
2011/01/02 12:40:48 gethostbyname() failed: members.dyndns.org	
011/01/02 12:40:38 Connecting to DDNS server	
011/01/02 12:40:37 gethostbyname() failed: members.dyndns.org	
011/01/02 12:40:27 Connecting to DDNS server	
011/01/02 12:40:27 User-Agent: Vigor3900 series, Host: members.dyndns.org	
:011/01/02 12:40:27 >>>> DDNS1 is updateing.<<<<<	
:011/01/02 12:30:25 gethostbyname() failed: members.dyndns.org	
011/01/02 12:30:15 Connecting to DDNS server	_

#### 4.7.2 GVRP

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

<b>Dray</b> Tek	Vigor 3900 Series	15:19:13	Login: Admin	E î
Auto Logout : Off   LAN  LAN  NAT  Firewall  Objects Setting  User Management  Applications  Dynamic DNS  GVRP  KGNP Proxy  UPnP  High Availability  Wake on LAN  SMS / Mail Alert Service  VPN and Remote Access  Certificate Management  SSL VPN  Central VPN Management  Bandwidth Management  USB Application	Applications >> GVRP GVRP Enable Interface : Join Time : 20	Seconds	Apply	Cancel
<				>



Item	Description
Enable	Check this box to enable GVRP function.
Interface	Choose LAN and/or WAN profiles. To clear the selected one, click is 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.

#### 4.7.3 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.

<b>Dray</b> Tek	Vigor 3900 Series	15:59:33	Login: Admin	Ð
Auto Logout : Off  LAN LAN NAT Firewall Objects Setting User Management Applications Dynamic DNS GVRP USMP Proxy UPnP High Availability Wake on LAN SMS / Mail Alert Service VPN and Remote Access Certificate Management SSL VPN Central VPN Management Bandwidth Management USB Application	Applications >> IGMP Proxy IGMP Proxy IGMP Proxy IGMP Proxy Channel: wan1 Downstream: lan1		Apply	Cancel
(				>

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.

#### 4.7.4 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.



<b>Dray</b> Tek	Vigor 3900	) Series	16:09:19	Login: Admin	E	^
Auto Logout : Off   LAN LAN NAT Firewall Objects Setting User Management Applications Dynamic DIS GVRP IGMP Proxy UPnP High Availability Wake on LAN SMS / Mail Alert Service VPN and Remote Access Certificate Management SSL VPN Central VPN Management	Applications >> UPnP UPnP Download : Upload : External Interface : Internal Interface : Max Session :	1024 512 wan1	<ul> <li>Kbps Mbps</li> <li>Kbps Mbps</li> <li>Kbps Mbps</li> </ul>			
Bandwidth Management USB Application				Apply	🔇 Cancel	
<					)>	~

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.

	Broadband	📜 IP Broadband Connection o	
Network Tasks (Received a new connection Create a new connection Set up a home or small office network	hinet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status:	Connected
iee Also	and test	Duration: Speed:	00:19:06 100.0 Mbps
Network Troubleshooter Other Places	Disconnected DrayTek ISDN PPP	Activity Internet Internet Gate	eway My Computer
Control Panel My Network Places My Documents My Computer	IP Broadband Connection on Router Enabled	Packets: Sent: 404 Received: 1.115	734
3 Hy compares	LAN or High-Speed Internet		
Details	Local Area Connection	Properties Disable	
Network Connections System Folder	Enabled Realtek RTL8139/810x Family		

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.

eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
Section on Router	Services
This connection allows you to connect to the Internet through a shared connection on another computer.	<ul> <li>Ftp Example</li> <li>msnmsgr (192:168.29.11:13135) 60654 UDP</li> <li>msnmsgr (192:168.29.11:7824) 13251 UDP</li> <li>msnmsgr (192:168.29.11:8789) 63231 TCP</li> </ul>

The reminder as regards concern about Firewall and UPnP

#### Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

#### Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.



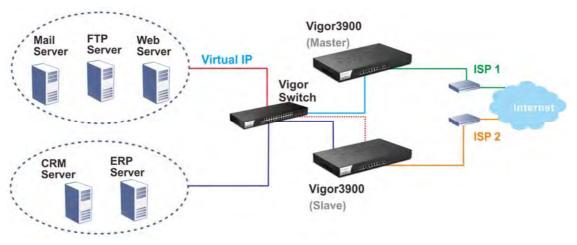
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

#### 4.7.5 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.



## 4.7.5.1 High Availability Global Setup

<b>Dray</b> Tek	Vigor 3900 Series	13:50:53	Login: Admin 🕞
	Applications >> High Availability >> High Availability	ty Global Setup	(
Auto Logout : Off 🛛 🗸	High Availability Global Setup High Availability	Profile Setup	
Quick Start Wizard			
Online Status			
WAN			
LAN	Redundant Method :	Hot-Standby	
NAT	Config Synchronization Role(Hot-Standby)	Secondary 👻	
Firewall	Config Synchronization IP(Hot-Standby) :	0 0 0 0	
Objects Setting	Priority ID(Hot-Standby) :	1 (1-30)	
User Management	Authentication Key :	dravtek	
Applications	Advance Preemption Mode :	Automatic	
Dynamic DNS			
GVRP	LAN Port Detection Mode :	At_Least_One_Up v	
IGMP Proxy	Enable High Availability		
UPnP			
High Availability			
Wake on LAN	General Note:		
SMS / Mail Alert Service	1. The VHID is the unique identifier for each High		
VPN and Remote Acces	same VHID. If the HA device is configured for mu 2. Each LAN profile can only be assigned to one		ve a different VHID.
Certificate Management	<ol> <li>Each LAN profile can only be assigned to one</li> <li>Changes to HA Profiles while HA is running w</li> </ol>		ulv" in [High Availability Global Setup] again.
SSL VPN	4. If you are going to setup a [Multi-HA LAN] scer		
Central VPN Manageme	Hot-Standby Method Note:		
Bandwidth Managemen	<ol> <li>Always complete the settings of the "primary"</li> <li>Do not enable High Availability before the prof</li> </ol>		essential to prevent config synchronizations
USB Application	before the configuration is finished.		
System Maintenance	3. Setup LAN profiles and the LAN VLAN ID confi		
Diagnostics	The LAN profile name on the secondary must be	same to the LAN profile name on the	primary as well as the LAN VLAN ID
External Devices			El obbit. 🖉 cancer

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 Hot-Standby 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 Primary Secondary 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.
	<b>Advance Preemption Mode</b> – Specify a mode for changing the Config Synchronization Role.
	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.
	<ul> <li>Manual – Restoring must be done according to the setting of Manual Preemption Status.</li> </ul>
	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 no 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 <b>Apply</b> 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.
	<b>Secondary</b> – 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 a primary.
	<b>Authentication Key</b> – 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.				
	<b>Delayed Interval:</b> Specify the time for waiting.				
	• Manual – Restoring must be done according to the setting of Manual Preemption Status.				
	<ul> <li>Manual Preemption Status – Click Active or Inactive.</li> <li>Manual Mode Threshold – Set a period of time for the system to determine the master router when there is no master router detected.</li> <li>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</li> </ul>				
	<ul><li>To solve the problem, two methods can be executed:</li><li>1. Simply reset Manual Preemption Status from Inactive to Active and then click Apply to save the settings.</li></ul>				
	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:				
	All_Must_Be_Up At_Least_One_Up All_Must_Be_Up				
	• 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.				
	<b>Enable High Availability</b> – Check the box to enable HA function.				
Settings under Active-Standby	<b>Config Synchronization IP</b> ( <b>Hot-Standby</b> ) – Type the IP address of the router plays the role of Master.				
·	<b>Priority ID</b> (Hot-Standby) – Type a value (1~30). The secondary router with the highest priority will take charge of				



Item	Description
	the service when the primary (master) router fails.
	<b>Authentication Key</b> – Type a string as the authentication key. It is used for encrypting the HA session communication to prevent malicious attack.
	<b>Enable High Availability</b> – Check the box to enable HA function.

## 4.7.5.2 High Availability Profile Setup

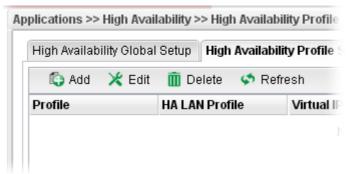
Dray Tek	Vigor 390	0 Series	14	:04:32	Login: Admin	Ξ
	Applications >> High	Availability >> High Avail	ability Profile Setup			
o Logout : Off 🛛 🗸	High Availability G	lobal Setup High Availa	bility Profile Setup			
Quick Start Wizard					5 a N	
Online Status	🖏 Add 🔀	Edit <u> </u>	lefresh		Profile Nun	iber Lim
WAN	Profile	HA LAN Profile	Virtual IP for Gateway	VHID	HA Status	
LAN			No items to show.			
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
Dynamic DNS						
GVRP						
IGMP Proxy						
UPnP						
High Availability						
Wake on LAN						
SMS / Mail Alert Service						
VPN and Remote Acces:						
Certificate Management						
SSL VPN						
Central VPN Manageme						
Bandwidth Management						
USB Application						
System Maintenance						
Diagnostics 🚽						
External Devices 🚽	4					

Available parameters are listed as follows:

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
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 User Profile

- 1. Open **Applications>>High Availability** and click the **High Availability Profile Setup** tab.
- 2. Simply click the **Add** button.



3. The following dialog will appear.

Profile :	HA_1	
HA LAN Profile :	lan1	~
Virtual IP for Gateway	192 168 1	. 55
VHID :	1	
Role(Hot-Standby) :	Primary	*

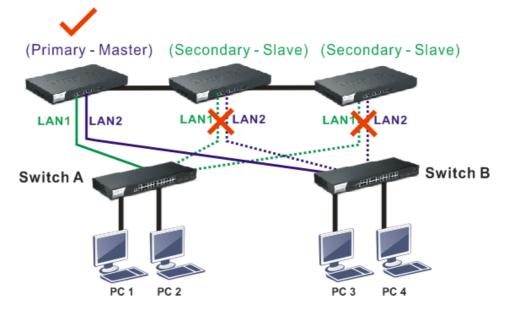
Item	Description			
Profile	Type a name for such profile.			
HA LAN Profile	Choose one of the LAN profiles that such function will be applied to.			
Virtual IP for Gateway	Assign an IP address as a virtual IP.			
VHID	It means Virtual Host ID. Type a number as VHID for such function. VHID is used for Backup router to identify which Master will be backed up.			
Role (Hot-Standby)	Select a role for this device as <b>Primary</b> or <b>Secondary</b> . Role(Hot-Standby) : Secondary Primary Secondary			
Apply	Click it to save the configuration.			
Cancel	Click it to discard the settings configured in this page.			



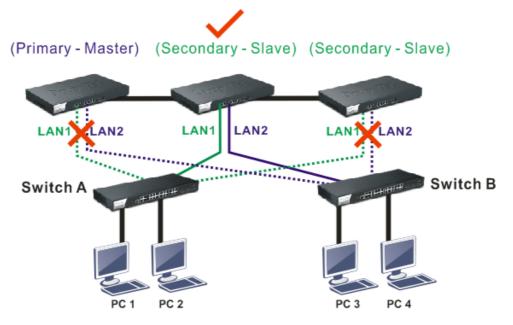
4. Enter all the settings and click **Apply**. The profile has been edited.

#### **Hot-Standby Mechanism**

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.

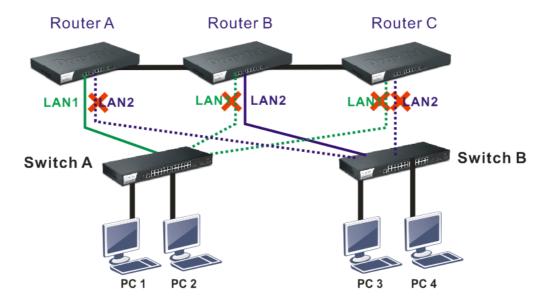


When the Master device fails, one of the slave devices will be chosen as the Master device to offer the network service for the connected PCs.

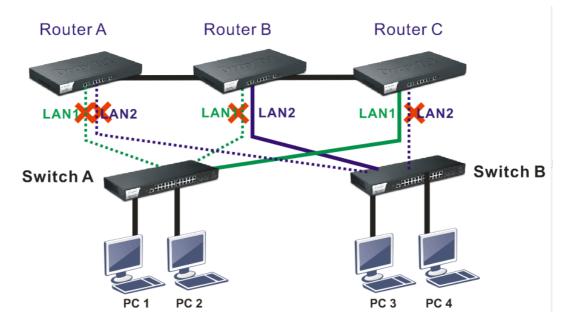


#### **Active-Standby Mechanism**

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.





#### 4.7.6 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.

<b>Dray</b> Tek	Vigor 3900 Series	16:14:46	Login: Admin	E
	Applications >> Wake on LAN			
Auto Logout : Off	Wake on LAN			
LAN	Configure Bind IP to MAC			
NAT	Note: Wake on LAN integrates w	ith Bird TD to MDG	function only binded DOs	
Firewall	wake up through IP	WITH BING IF to MAC	runction, only binded PCs	can
Objects Setting				
User Management				
Applications				
Dynamic DNS				
GVRP				
IGMP Proxy				
UPnP				
High Availability				
www.www.Wake on LAN www.www.www.				
SMS / Mail Alert Service				
VPN and Remote Access				
Certificate Management				
SSL VPN	() IP Address	v .		
Central VPN Management	Wake By: Mac Address :	LAN Profile :	lan1 👻 🕟 Wake	Up 🛄 [
Bandwidth Management				
USB Application	4	111		•
				>
• )				

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.
	<b>IP Address -</b> The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
	<b>MAC Address -</b> Type any one of the MAC address of the bind PCs.
	<b>LAN Profile</b> – 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.

#### 4.7.7 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.

#### **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.

<b>Dray</b> Tek		900 Series				Đ
	Applications >> S	MS / Mail Alert Service >> SI	Alert Service			
o Logout : Off 🛛 🗸	SMS Alert Ser	vice Mail Alert Service				
LAN	, X Edit	🔇 Refresh				
NAT		-				
Firewall	Index	Enable	SMS Provider	Recipient	Notify Profile	
Objects Setting	1	false				
User Management	2	false				
Applications	3	false				
Dynamic DNS	4	false				
GVRP	5	false				
IGMP Proxy	6	false				
UPnP E	7	false				
High Availability	8	false				
Wake on LAN	9	false				
SMS / Mail Alert Service	10	false				
VPN and Remote Access						
Certificate Management						
SSL VPN						
Central VPN Management						
Bandwidth Management						
USB Application						

Each item will be explained as follows:

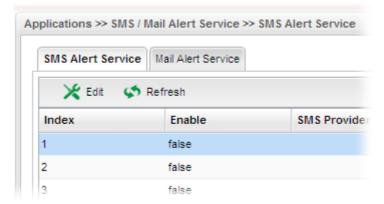
Item	Description
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable	Display the status of the profile. False means disabled; True means enabled.
SMS Provider	Display the name of the SMS provider.
Recipient	Display the one who will receive the SMS.
Notify Profile	Display the name of the notify profile.

#### How to edit the SMS alert service profile

1. Open Applications>> SMS/Mail Alert Service and click the SMS Alert Service tab.



2. Choose one of the index numbers and click the **Edit** button.



3. The following dialog will appear.

Index:	1		
Enable			
SMS Provider :	Line_down	*	
Recipient :			
Notify Profile :	Notify_attack	*	

Available parameters are listed as follows:

Item	Description
Enable	Check this box to enable such profile.
SMS Provider	Choose the SMS provider object profile from the drop down list.
	Such profiles can be created from <b>Object Setting&gt;&gt;SMS</b> 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 <b>Object</b> 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.

SMS Alert Serv	ice Mail Alert Service			
🔀 Edit	🔇 Refresh			
Index	Enable	SMS Provider	Recipient	Notify Profile
1	true	Line_down	carrie@yahoo.com	Notify_attack
2	false			
3	false			
4	false			

#### **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.

<b>Dray</b> Tek	Vigor	900 Series	16:35:21	Lo	gin: Admin	Ð
	2.6	MS / Mail Alert Service >> Mail	Alert Service			
Auto Logout : Off	SMS Alert Ser	vice Mail Alert Service				
User Management	🔀 Edit	🖨 Refresh				
Applications Dynamic DNS	Index	Enable This Profile	Mail Profile	Recipient	Notify Profile	
GVRP	1	false				
IGMP Proxy	2	false				
UPnP	3	false				
High Availability	4	false				
Wake on LAN	5	false				
SMS / Mail Alert Service	6	false				
VPN and Remote Access	7	false				
Certificate Management	8	false				
SSL VPN	9	false				
Central VPN Management	10	false				
Bandwidth Management						
USB Application						
System Maintenance						
Diagnostics						
External Devices						
Product Registration						

Each item will be explained as follows:

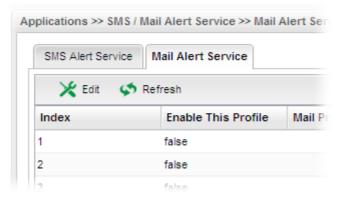
Item	Description
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Refresh	Renew current web page.
Index	Display the index number (from 1 to 10) of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Mail Profile	Display the name of the mail profile.
Recipient	Display the one who will receive the mail alert.



Notify Profile	Display the name of the notify profile.
----------------	-----------------------------------------

#### How to edit the mail alert service profile

- 1. Open **Applications>> SMS/Mail Alert Service** and click the **Mail Alert Service** tab.
- 2. Choose one of the index numbers and click the **Edit** button.



3. The following dialog will appear.

Index :	1	
🗸 Enable Thi	s 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 <b>Object Setting&gt;&gt;Mail</b> <b>Service Object</b> .
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 <b>Object</b> <b>Setting&gt;&gt;Notification Object</b> .
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.

plications >> SM	IS / Mail Alert Service >> Mail	Alert Service		
SMS Alert Servi	ce Mail Alert Service			
🔀 Edit	🐝 Refresh			
Index	Enable This Profile	Mail Profile	Recipient	Notify Profile
1	true	Mail_Notify	carrie@yahoo.com	Notify_attack
2	false			
3	false			
4	false			

### **4.8 VPN and Remote Access**

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

Below shows the menu items for VPN and Remote Access.

VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
IPSec General Setup
VPN Profiles
VPN TRUNK Management
Connection Management

#### 4.8.1 VPN Client Wizard

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

<b>Dray</b> Tek	Vigor 3900 Series	14:17:50	Login: Admin	E>
	VPN and Remote Access Step 1 Step 2			
Auto Logout : Off	Step 1 Step 2			
Firewall				
Objects Setting	Туре: 💿 РРТР 🔘	) IPSec		
User Management	VPN Settings Via : <ul> <li>Select From Curr</li> </ul>	ent Settings 🔘 Create New	VPN Profile	
Applications				
VPN and Remote Access	Profile - Status			
VPN Client Wizard	to2920 enable			
VPN Server Wizard				
Remote Access Control				
PPP General Setup				
IPSec General Setup				
VPN Profiles				
VPN TRUNK Management				
Connection Management				
Certificate Management				
SSL VPN				
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices			Vext Finish	Cancel

#### 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.

and Remot	e Access				
Step 1	Step 2				
Туре:	💿 РРТР	OIPSec			
VPN Settin	gs Via 🗧 💿 Select Fr	om Current Setting	s 🔵 Create New VP	'N Profile	
Profile	Status				
	No items to sh	ow.			

Item	Description
Туре	Specify which protocol ( <b>PPTP</b> or <b>IPSec</b> ) will be used for such VPN profile.
VPN Settings Via	<b>Select From Current Settings</b> – Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need.
	<b>Create New VPN Profile</b> – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of <b>Profile Name</b> . 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**.

and Remote Acces	s					
Step 1 Step	2					
Туре :		○IPSec				
VPN Settings Via	🔵 Select From	Current Settings	💿 Create New '	VPN Profile		
Profile Name :	VPN_CLI_1					
				Previous 🛋	Next Finis	sh 🔇 Cance

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

VPN and Remote Access				
Step 1 Step 2				
				-
Profile :	VPN_CLI_1			
V Enable				
Always On :	🔵 Enable 💿 Disable			
Idle Timeout (sec) :	300	(Optiona	0	
Server IP/Host Name :	192.168.1.10			
PPTP User Name :	pptp_user	(Optiona	D	Ε
PPTP Password :	••••			
Local IP / Subnet Mask :	192 . 168 . 3 .	65	255.255.255.0/24 🗸	
	🏠 Add 🗮 Save		F	
	IP		Subnet Mask	
Remote IP / Subnet Mask :	192.168.3.98		255.255.255.0	
				_
4				+
			An Arrow Service Serv	_

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.		
<b>PPTP User Name</b>	Type a user name for authentication in PPTP connection.		
<b>PPTP Password</b>	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		
Step 1 Step 2		
Profile :		-
Frome :	VPN_CLL_1	
	wan1	
WAN Profile :	wan1 v	
Local IP / Subnet Mask :	192 . 168 . 1 . 0 255.255.0/24 🗸	
Local Next Hop :		E
Remote Host :	0.0.0.0	
Remote IP / Subnet Mask :	0.0.255.255.255.255/32	
	🕼 Add 🛗 Save	
	IP Subnet Mask	
More Remote Subnet :	No items to show.	
Auth Tuno -	DSK w Othile Demote Neet on 0.0.0. DSK will be defined in IDage Concert Sk	•
	y Previous ា Next 📑 Finish 🙆 Cancel	

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).
<b>Remote Host</b>	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 <b>PSK</b> or <b>RSA</b> 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 <b>ESP</b> to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose <b>AH</b> 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.

Step 1	Step 2					 
Type : VPN Settings	● PPT Via : ● Sele		) IPsec rent Settings	🔿 Create New	VPN Profile	
Profile		Status				
VPN_CLI_1		enable				

#### 4.8.2 VPN Server Wizard

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

<b>Dray</b> Tek		Vigor 3900 Series	14:23:28	Login: Admin	Ð
	1	VPN and Remote Access			
Auto Logout : Off 🛛 👻		Step 1 Step 2 Step 3			
Firewall					
Objects Setting		Type: OPPTP OIPS	ес		
User Management		VPN Settings Via : ( Select From Current S	ettings 🦳 Create New	VPN Profile	
Applications					
VPN and Remote Access		Profile Status			
VPN Client Wizard		No items to show.			
VPN Server Wizard					
Remote Access Control	-				
PPP General Setup					
VPN Profiles					
VPN TRUNK Management	=				
Connection Management	-				
Certificate Management					
SSL VPN					
Bandwidth Management					
System Maintenance					
Diagnostics				🕼 Previous 🛋 Next 📑 Finish	Cancel
External Devices					Calicer
:					>

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.

Step 1 Ste	ep 2			
Туре :	PPTP     IPsec			
VPN Settings Via :	O Select From Current Settin	gs 💿 Create New VPN	Profile	
Profile Name :	VPN_Ser_1			
			Previous 🔊 Next	

Item	Description



Туре	Specify which protocol ( <b>PPTP</b> or <b>IPSec</b> ) will be used for such VPN profile.	
VPN Settings Via	<b>Select From Current Settings</b> - Current VPN LAN to LAN profiles will be listed below such setting. Choose the one you need.	
	<b>Create New VPN Profile</b> – It allows you to create a new VPN LAN to LAN profile. Simply type the name in the field of <b>Profile Name</b> . 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:

VPN and Remote	Access		
Step 1	Step 2		
Profile :		/PN_Ser_1	
PPTP User N	ame :	Aron 🗸	
Local IP / Su	bnet Mask :	192 . 168 . 1 . 45 255.255.2	255.0/24
Remote IP /	Subnet Mask :	192 168 2 5 255.255.2	255.0/24 🗸
			📡 Previous 🛋 Next 📑 Finish 🔇 Cancel

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 <b>User Management&gt;&gt;User</b> <b>Profile</b> 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	Type the LAN IP address and LAN subnet mask for the
Mask	remote host.

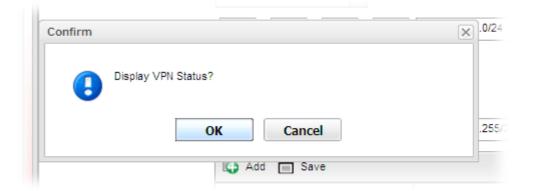
If you choose **IPSec** as the **Type** in Step 1, you will get the following page:

VPN and Remote Access		
Step 1 Step 2		
		*
Profile :	VPN_Ser_1	
V Enable		
WAN Profile :	wan1 🗸	
Local IP / Subnet Mask :	192 . 168 . 1 . 0 255.255.0/24 🗸	
Local Next Hop :		E
Remote Host :	172.16.1.88	
Remote IP / Subnet Mask :	192 . 168 . 2 . 45 255.255.255/32 💌	
	🏠 Add 🛗 Save	
	IP Subnet Mask	_
More Remote Subnet :	No items to show.	
Auth Tuno	DSK (Mihis Dometo Host op 0.0.0. DSK will be defined in Done Conoral Sc	Ŧ
	🔨 Previous 🔹 Next 📑 Finish 🔇 Cancel	

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 <b>PSK</b> or <b>RSA</b> 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 <b>ESP</b> to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose <b>AH</b> 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.



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.

Step 1 S	Step 2		
Type : VPN Settings Via	PPTP     IPsec     Select From Current Sett	ings 🔘 Create New VPN Profile	
Profile	Status		
VPN_Ser_1	enable		

#### 4.8.3 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.



Item	Description
Enable PPTP VPN Service / L2TP VPN Service/DHCP over IPSec Service/L2TP over IPSec Service	Check the box(es) to enable the service.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

### 4.8.4 PPP General Setup

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

### 4.8.4.1 PPTP

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

<b>Dray</b> Tek	Vigor 3900 Serie	5	14:22:02	Login: Admin	Ð
	VPN and Remote Access >> PPP	General Setup >> PPTP			0
Auto Logout : Off	PPTP L2TP				
Quick Start Wizard					
Online Status	Authenticate Protocol :	MS-CHAP-v2			
WAN	MPPE Encryption :	128-bit 🗸			
LAN					
NAT	User Authentication Type :	Local			
Firewall	LAN Profile :	lan1 🗸			
Objects Setting	NetBIOS Naming Packet :	🔘 Pass 💿 Block			
User Management					
Applications					
VPN and Remote Acces:					
VPN Client Wizard					
VPN Server Wizard =					
Remote Access Control					
PPP General Setup					
IPsec General Setup					
VPN Profiles					
VPN TRUNK Managemen					
Connection Managemen					
Certificate Management					
SSL VPN					
Central VPN Manageme					
Bandwidth Management					
USB Application					
System Maintenance				💾 Apply	🔇 Cancel
Diagnostics 🖃					

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				
	<b>PAP</b> - It means the router will attempt to authenticate dial-in users with the PAP protocol.				
	<b>CHAP</b> - 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 V Local RADIUS LDAP		
LDAP profiles	<ul> <li>Choose a LDAP profile for PPTP Server if LDAP is selected as user authentication type.</li> <li>To clear the selected one, click to remove current object selections.</li> </ul>		
LAN Profile	Choose a LAN profile for PPTP Server if <b>RADIUS</b> or <b>LDAP</b> is selected as user authentication type.		
NetBIOS Naming Packet	<b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.		
	<b>Block</b> – 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.		
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**.

# 4.8.4.2 L2TP

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

<b>Dray</b> Tek	Vigor 3900 Series	14:39:51	Login: Admin	Ð
	VPN and Remote Access >> PPP General Setup >> L2T	p		(
Auto Logout : Off 🛛 🖌	PPTP L2TP			
Quick Start Wizard				
Online Status	Authoritizate Destavate			
WAN		~		
LAN	User Authentication Type : Local	~		
NAT	LAN Profile : lan1	v		
Firewall	Force L2TP with IPsec policy			
Objects Setting				
User Management				
Applications				
VPN and Remote Acces				
VPN Client Wizard				
VPN Server Wizard =				
Remote Access Control				
PPP General Setup				
IPsec General Setup				
VPN Profiles				
VPN TRUNK Managemen				
Connection Managemen				
Certificate Management				
SSL VPN				
Central VPN Manageme				
Bandwidth Management				
USB Application				
System Maintenance			💾 Apply (	🔕 Cancel
Diagnostics 🖃			0	

Item	Description
Authenticate Protocol	The router will authenticate the dial-in user with the protocol selected here. MS-CHAP-v2 PAP CHAP MS-CHAP-v2 MS-CHAP-v2
	<ul> <li>PAP - It means the router will attempt to authenticate dial-in users with the PAP protocol.</li> <li>CHAP - It means the router will attempt to authenticate</li> </ul>
	dial-in users with the CHAP protocol.
User Authentication Type	Set user authentication to <b>Local</b> server or <b>RADIUS</b> server.
LDAP profiles	Choose a LDAP profile for PPTP Server if <b>LDAP</b> is selected as user authentication type. To clear the selected one, click to remove current object selections.
LAN Profile	Choose a LAN profile for L2TP Server if <b>RADIUS/LDAP</b> is selected as user authentication type.



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**.

### 4.8.5 IPSec General Setup

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

<b>Dray</b> Tek	Vigor 3900	Series	14:42:53	Login: Admin	E>
	VPN and Remote Access	>> IPsec General Setup			0
Auto Logout : Off	IPsec General Setup				
Outer start wizard Online Status WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Acces: VPN Client Wizard VPN Server Wizard Remote Access Control PPP General Setup VPN Profiles VPN Profiles VPN TRUNK Management SSL VPN Central VPN Management	Preshared Key : WAN Profile : DHCP LAN Profile : IKE Port : NAT-T Port : IPsec MSS :	wan1,usb2 v × lan1 v 500 4500 1360			
USB Application System Maintenance Diagnostics				🗎 Apply (	🕉 Cancel

Item	Description
Preshared Key	Specify a key for IKE authentication <b>Confirm Pre-Shared Key-</b> 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 it 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**.

## 4.8.6 VPN Profiles

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

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

<b>Dray</b> Tek	V	igor 3900	Series		14:43:51	Login: Admin	Ð
	VPN	and Remote Acce	ss >> VPN Profi	iles			
luto Logout : Off 🛛 🗸		PN Profiles					
Quick Start Wizard							
Online Status		🕼 Add 🛛 💥 E	lit <u> î</u> Delete	🗭 Refresh	● IPsec ○ PPTP Dial-Out ○ PPT	P Dial-In Profile Number Lin	
WAN		Profile	Enable	WAN Profile	Local IP / Subnet Remote Host	Remote IP / Subi More Remo	te Sul
LAN	1	VPN_CLI_1	false	wan1	192.168.1.0/24 192.168.2.3	192.168.2.99/32	
NAT	2	VPN_Ser_1	false	wan1	192.168.1.0/24 172.16.1.88	192.168.2.45/32	
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Acces:							
VPN Client Wizard							
VPN Server Wizard							
Remote Access Control							
PPP General Setup	8						
IPsec General Setup							
VPN Profiles							
VPN TRUNK Managemen							
Connection Managemen							
Certificate Management							
SSL VPN							
Central VPN Manageme							
Bandwidth Managemen							
USB Application							
System Maintenance							
Diagnostics 🕞							

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 <b>Edit</b> 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 <b>Delete</b> 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.
<b>PPTP Dial-in</b>	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.
WAN Profile	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.

VF	N Profiles		
[	🚯 Add 🔀	Edit 🔟	Delete 🧳 Refre
	Profile	Enable	WAN Profile
1 2	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.

IPsec	
Profile : L2L_1 Type :	ec 🔘 PPTP Dial-Out 🔘 PPTP Dial-In
Basic Advanced	GRE Proposal PPTP
Always On : For Remote Dial-In User : WAN Profile :	<ul> <li>○ Enable <ul> <li>○ Disable</li> <li>○ Enable <ul> <li>○ Disable</li> </ul> </li> <li>wan1 <ul> <li>✓ O Default WAN IP</li> <li>○ WAN Alias IP</li> </ul> </li> </ul></li></ul>
Local IP / Subnet :	
Local Next Hop :	
Remote Host :	0.0.0.0
	💾 Apply 🔇 Cancel

Item	Description			
Profile	Type the name of the profile.			
Enable	Check this box to enable this profile.			
Туре	There are three types offered here for you to choose. Please choose <b>IPSec</b> 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.			
	<b>WAN Profile-</b> Choose a wan profile to be used by such profile.			
	<b>Local IP/Subnet -</b> Type the IP address and subnet mask of local host.			
	<b>Local Next Hop -</b> Specify the gateway for WAN interface. Usually, use the default setting (leave it in blank).			
	<b>Remote Host -</b> Type the WAN IP address for the remote host.			
	<b>Remote IP / Subnet Mask -</b> Type the LAN IP address and LAN subnet mask for the remote host.			
	<b>More Remote Subnet</b> – Add more remote subnet in this field if required.			
	Auth Type - The authentication to be used by Pre-Shared Key or RSA Signature. Choose <b>PSK</b> or <b>RSA</b> for such			



profile.
<b>Certificate -</b> Choose a local certificate from the drop down list if RSA is selected as Auth Type.
<b>Preshared Key</b> – Specify a key for IKE authentication if PSK is selected as Auth Type.
<b>Security Protocol</b> – Choose <b>ESP</b> to specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated. Choose <b>AH</b> to specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.

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

Profile :	L2L_1				
V Enable					
Type :	💿 IPsec	🔿 PPTP Dia	al-Out 🔘 PPTP	Dial-In	
Basic	Advanced	GRE	Proposal	PPTP	
Phase1 Ke	y Life Time :	28800			
Phase2 Ke	y Life Time :	3600			
Perfect For	ward Secrecy St	atus : 🔵 En	able 💿 Disable	;	
Dead Peer	Detection Status	: 💿 En:	able 🔿 Disable	,	
DPD Delay :		30			
DPD Timeout :		120			
Source IP :		auto_d	etect_srcip	~	

Item	DescriptionEnable – Click it to enable Aggressive Mode.Disable – Click it to disable Aggressive Mode.			
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	<ul> <li>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.</li> <li>Disable – Click it to disable DPD.</li> </ul>
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.
Source IP	Choose one of the LAN profiles as a source IP.

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

					-
Profile :	L2L_1				
🗸 Enable					
Туре:	💽 IPs	ec 🔘 PPTP Dia	I-Out 🔘 PPTP [	)ial-In	
Basic	Advanced	GRE	Proposal	PPTP	
Enable GRE	Function :	💿 Enable 🔘 I	Disable		
Local GRE II	Ρ:	192 . 168	. 1 . 66		
Remote GR	E IP :	192 . 168	. 1 . 84		
Auto Gener	ate GRE Key :	🔵 Enable 💿 I	Disable		
GRE In Key	:		(Op	tional)	
GRE Out Ke	<b>y</b> :		(Op	tional)	

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 <b>Enable</b> to generate the GRE key by the system automatically. If you click <b>Disable</b> , 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.

1	IPsec						-×
A	Profile :	L2L_1	ec 🔿 PPTP	P Dial-Out O PPTP	Dial-In		
	Basic	Advanced	GRE	Proposal	PPTP		
	IKE Phase1 IKE Phase2 IKE Phase2	Proposal [Dial- Authentication Proposal [Dial- Authentication Proposal [Dial-In	[Dial-Out] : Out] : [Dial-Out] :	3DES_with_auth	> > > >		
						Apply	🔇 Cancel

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	Propose the local available algorithms to the VPN peers, and get its feedback to find a match.

(Dial-Out)				
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.			
	<b>Only accept proposal listed above (acceptabove)</b> - 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.			

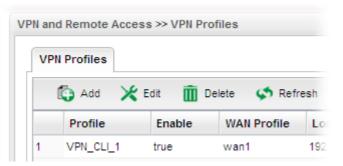
- 7. Enter all the settings and click **Apply**.
- 8. A new IPSec LAN-to-LAN profile has been created.

VPN Profiles							
	🏠 Add 🔀	Edit 👖 Delete	📢 Refresh	⊙ IPSec 🔿	PPTP Dial-Out (	O PPTP Dia	
	Profile	Enable	WAN Profile	Local IP / Subn	Remote Host	Remote II	
1	VPN_CLI_1	false	wan1	192.168.1.0/24	0.0.0.0	0.0.0/32	
2	VPN_Serv_1	false	wan1	192.168.1.0/24	0.0.0.0	0.0.0/32	
3	L2L 1	true	wan1	192,168,1,0/24	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.



3. The following dialog will appear.

			_
_	_out_1		
Enable			
Туре: 🔘	IPsec 💿 PPTP Dial-Out 🤇	) PPTP Dial-In	
Basic Advance	ed GRE Pro	posal	
Always On :	🔵 Enable 💿 Disable	9	
Idle Timeout (sec) :	300	(Optional)	
Server IP/Host Name :	172.16.3.250		
PPTP User Name :	pptptest	pptptest (Optional)	
PPTP Password :	•••••		
Local IP / Subnet Mas	k: 192 . 168 . 1	. 54 255.255.255.0/24	*
			•
A			

Item	Description
Profile	Type the name of the profile.
Enable	Check this box to enable this profile.
Туре	There are three types offered here for you to choose. Please choose <b>PPTP Dial-Out</b> for this case.
РРТР	<ul> <li>Always On - Click Enable to make the profile being always on.</li> <li>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.</li> <li>Server IP/Host Name - Type the IP address or the host name of PPTP server.</li> <li>PPTP User Name - Type a user name for authentication in</li> </ul>
	<ul> <li>PPTP connection.</li> <li>PPTP Password - Type a password for authentication in PPTP connection.</li> <li>Local IP/Subnet Mask - Type the IP address and subnet mask of local host.</li> <li>Remote IP / Subnet Mask - Type the LAN IP address and LAN subnet mask for the remote host.</li> <li>Route / NAT Mode - Specify the purpose for such profile.</li> </ul>

	NAT 🗸	
	Route	
_	NAT	
Apply	Click it to save the configuration.	
Cancel	Click it to exit the page without saving the configuration.	

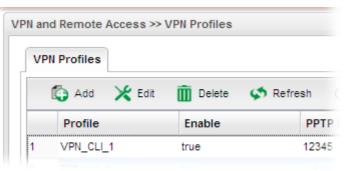
- 4. Enter all the settings and click **Apply**.
- 5. A new PPTP Dial-Out profile has been created.

	🚯 Add 🛛 🔀 Edit	前 Delete 🗳	Refresh 🔿 IPsec 💿 F	PPTP Dial-Out O PPTP Dial-In Profile Number
	Profile	Enable	PPTP User Name	Local IP / Subnet Mas Remote IP / Subnet M
1	VPN_CLI_1	true	12345	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.



3. The following dialog will appear.

rofile :		PTP_ir	L1			
🔽 Enable						
ype :		⊖ IP	sec 🔿 P	PTP Dial-(	Out 💿 PPTP Dial-In	
Set PPTP Dial-In For Use	er Prof	ie				
			_			
Basic Advanced	0	GRE	Propos	al	РРТР	
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	~
		•	· ·	•		

Item	Description
Profile	Display the name of the profile.
Enable	Check this box to enable this profile.
Туре	There are three types offered here for you to choose. Please choose <b>PPTP Dial-In</b> for this case.
Set PPTP Dial-In For User Profile	Click it to create a new user profile or to modify an existing profile.
	User Profile
	🕼 Add 🔀 Edit 🏢 Delete 🔊 Refresh Profile Nur
	Username Enable Thi System Us Group PPTP L2TP DHCP from Static IP A; Use mOTP No items to show.
	See the explanation later.
PPTP User Name	Choose a PPTP user profile for authentication in PPTP connection.
	Such profile shall be created in User Management>>User

	<b>Profile</b> 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.

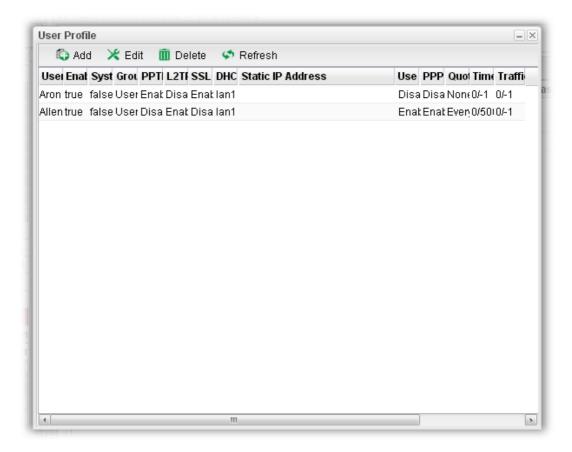
- 4. Enter all the settings and click **Apply**.
- 5. A new PPTP Dial-In profile has been created.

🕼 Add 🔀 Edit 🏢 Delete 🐼 Refresh 🔿 IPsec 🔿 PPTP Dial-Out 💿 PPTP Dial-In Profile Number Lin							
C	Profile	Enable	PPTP User Name	Local IP / Subnet M	as 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	0.0.0/24	0.0.0/24		

### Set PPTP Dial-In For User Profile

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

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



### 4.8.7 VPN Trunk Management

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

<b>Dray</b> Tek	Vigor 3900 Series	14:53:58	Login: Admin 🕞
	VPN and Remote Access >> VPN TRUNK Management :	>> Load Balance Rule	
Auto Logout : Off 🛛 🗸	Load Balance Rule Load Balance Pool		
Quick Start Wizard			Des Glach Longham Ling V
Online Status	🕼 Add 🔀 Edit 🛅 Delete 🕏 Refresh		Profile Number Limit
WAN	Profile Enable Protoc Source IP Address	Sourc Destination IP Address	Destin Destin Destin Load E
LAN			
NAT			
Firewall			
Objects Setting			
User Management			
Applications			
VPN and Remote Access			
VPN Client Wizard			
VPN Server Wizard =			
Remote Access Control			
PPP General Setup			
IPsec General Setup			
VPN Profiles			
VPN TRUNK Managemen			
Connection Managemen			
Certificate Management			
SSL VPN			
Central VPN Manageme			
Bandwidth Management			
USB Application			
System Maintenance			
Diagnostics 🥃	4		



# 4.8.7.1 Load Balance Rule

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

🖏 Add	🔀 Edit 🛛 👖 Delet	e 🗳 Refresh		Profile Number Lim
Profile	Enable Protoe Source	IP Address	Sourc Destination IP Address	Destin Destin Destin Load E

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 <b>Edit</b> 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 <b>Delete</b> 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.
<b>Destination Port Start</b>	Display the start point specified in the <b>Dest Port Range</b> for this entry.
<b>Destination Port End</b>	Display the end point specified in the <b>Dest Port Range</b> 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.

_	Load	Balance	Rule Lo	ad Balance Po	lool
	ĺ.	👌 Add	🔀 Edit	<u>î</u> Delet	e 🥩
		Profile	Enable	Protocol	Source

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 :		*
		📄 Apply 🔞 Cancel

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.			
	TCP/UDP   ALL   TCP   UDP   TCP/UDP   ICMP   FTP   TFTP   TFTP   MTTP   SMTP   POP3			
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.

Loa	ad Balance	Rule Lo	ad Balance F	Pool						
	🚯 Add	🔀 Edit	🔟 Dele	ete 🗳 Refresh						
	Profile	Enable	Protocol	Source IP Address	Source Mask	Destination IP Add	Del	De De	Lo	
1	LB rule	true	ALL	192,168,1,46	255,255,255.0	192,168,2,89	2			

# 4.8.7.2 Load Balance Pool

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

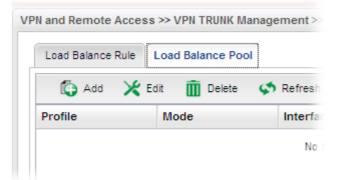
🕼 Add 🛛 💥 E	dit   🔟 Delete 🛭 🗳 Re	esh Profile Number L		
Profile	✓ Mode	Interface	Primary Interface	Backup Interface

### 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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
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.

oad Balance	Pool	-×
Profile :	LB_Pool_1	
Mode :	Load_Balance 🗸	
Interface :	L2L_1 × ×	
	VPN_CLI_1	
	☑ L2L_1	🛗 Apply 🔕 Cancel

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. 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.



🚯 Add 🔀 Edit 🏛 Delete 🔊 Refresh 🤄 Profile Number L				
rofile	<ul> <li>Mode</li> </ul>	Interface	Primary Interface	Backup Interface
3_Pool_1	Failover		L2L_1	VPN_CLI_1

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

# 4.8.8 Connection Management

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

<b>Dray</b> Tek	Vigor39	<b>OU</b> Series		15:49	-10	Login: Admi	in 🖸
	VPN and Remote A	ccess >> Conne	ction Managem	ent			
Auto Logout : 5Min 💌	Connection Ma	nagement					
Quick Start Wizard							
Online Status	Dial-Out tool						
WAN	() IPsec (	PPTP Profile	is:	👻 🚭 Connect	< Refresh		
LAN							
NAT	VPN Connectio						
Firewall	VPN	Туре	Remote IP	Virtual Netwo Up Time	RX(Packets)	TX(Packets)	Disconnect
Objects Setting				No items to show.			
User Management							
Applications							
VPN and Remote Access							
VPN Client Wizard							
VPN Server Wizard 💡							
Remote Access Control							
PPP General Setup							
IPsec General Setup							
VPN Profiles							
VPN TRUNK Managemen							
Connection Managemen							
Certificate Management							
SSL VPN							
Central VPN Manageme							
Bandwidth Management							
USB Application 🔤							
System Maintenance							

Each item will be explained as follows:

Item	Description			
IPSec	Click it to perform IPSec VPN connection.			
РРТР	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.			
Туре	Display the connection type (PPTP or IPSec) for such VPN profile.			
Remote IP	Display the remote IP configure by VPN profile.			
Virtual Network	Display the virtual network established by such VPN profile.			
Up Time	Display the connection time of this VPN tunnel.			
RX (Packets)	Display the total received packets through this VPN.			
TX (Packets)	Display the total transmitted packets through this VPN.			
Disconnect	Terminate the VPN connection.			



# 4.9 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.

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

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

# 4.9.1 Local Certificate

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

<b>Dray</b> Tek	Vigor 39	00 Series		15:51:	:20 Lo	ogin: Admin	Ð
	Certificate Manag	gement >> Local Cert	ificate				(
Auto Logout : 5Min 💌	Local Certifica	ate					
Quick Start Wizard							
Online Status	🚺 🚺 Upload	🔟 Delete 🛛 🐺 D	ownload  🧔 Gen	erate			
WAN							
LAN	Select File	: 選擇檔案 未選	擇檔案				
NAT		0.1	•	21-1			
Firewall	Name	Subject	Issuer	Status	Valid from	Valid to	
Objects Setting				No items to show.			
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
Local Certificate							
Trusted CA Certificate							
Remote Certificate							
SSL VPN							
Central VPN Management							
Bandwidth Management							
USB Application							
System Maintenance							
Diagnostics							
External Devices							
Product Registration							

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 <b>Browse</b> 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.

Local Certificate				
💽 Upload	🛅 Delete 🛛 🐺 Do	ownload 🛛 🧔 Gene	erate	
Select File :	選擇檔案 未選擇	澤檔案		
Name	Subject	Issuer	Status	Valid fr

3. The following dialog will appear.

Local Certificate		->
Certificate Name :	Local CA	
ID Type :	IP V	ā.
ID Value :		_
Organization Unit :	DT	
Organization :	DrayTek	
Locality(City) :	HS	
State/Province :	Taiwan	
Common Name :	DT_License	
Email Address :	service@draytek.com	
Key Size :	1024 🗸	
Country :	TW	
Self Sign :	🔵 Enable 💿 Disable	
Passphrase :		
		📑 Apply 🛛 😡 Cancel

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

	<b>Domain Name</b> : Certificated by domain name.
	<b>IP</b> : Certificated by IP address.
	<b>Email</b> : Certificated by email address.
	None None Domain_Name IP Email Drayree
ID Value	The ID value is determined by the <b>ID Type</b> selected for such certificate.
	For example, if you choose <b>Domain_Name</b> as the ID Type, please type the domain name in this field.
<b>Organization Unit</b>	Type a description for the organization unit.
Organization	Type the name of the organization.
Locality (City)	Type the name of the city for such certificate.
State/Province	Type the name of the state /province for such certificate.
Common Name	Type the common name for such certificate.
Email Address	Type the e-mail address for such certificate.
Key Size	Choose one of the key sizes for such certificate.
Country	Type the name of the country that such certificate located.
Self Sign	Click <b>Enable</b> 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 <b>Disable</b> to disable the self sign function. A certificate without self sign can be approved or signed by a Root CA server, e.g., Vigor3900.
Passphase	Such string will be used for confirmation while signing remote CA. It is similar to a password but generally it is longer for security.
Apply	Click it to create a new local certificate based on the configuration here.
Cancel	Click it to exit the web page without saving the configuration.

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

5. A new generated Local Certificate has been created.

Local Certifica	te					
🗊 Upload	<u> iii</u> Delete 🛛 🐺 D	ownload 🛛 🧔 Gene	rate			
Select File :		擇檔案	21-1	11-12-16	V-544-	
Select File : Name	選擇檔案〕未選 Subject	擇檔案 Issuer	Status	Valid from	Valid to	

# 4.9.2 Trusted Certificate

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

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

<b>Dray</b> Tek	Vigor 39	00 Series		15:58:4	16 L	ogin: Admin	Ð
	Certificate Manag	ement >> Trusted C/	A				(
Auto Logout : Off 🛛 🗸	Trusted CA						
Quick Start Wizard			~				
Online Status	🔯 Upload	🔟 Delete 🛛 🐺 D	iownload 🛛 🎤 Build	I RootCA			
WAN							
LAN	Select File :	[選擇檔案] 未選	擇檔案				
NAT							
Firewall	Name	Subject	Issuer	Status	Valid from	Valid to	
Objects Setting			1	No items to show.			
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
Local Certificate							
Trusted CA Certificate							
Remote Certificate							
SSL VPN							
Central VPN Management							
Bandwidth Management							
USB Application							
System Maintenance							
Diagnostics							
External Devices							
Product Registration							

Each item will be explained as follows:

Item	Description
Upload	Allow you to upload current configuration to the host as a CA certificate.
Delete	Remove the selected item of trusted CA listed below.
Download	Allow you to download an existing trusted CA certificate to the router.
Build RootCA	Allow to create a new CA certificate as Root CA.
Select File	Use the <b>Browse</b> 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.

🗊 Upload	前 Delete 🛛 🔍 D	ownload 🛛 🎤 Build	I RootCA
Ma Obioad	🎹 Delete 👒 D	ownioad 🎢 Built	TRUDICA
Select File :	選擇檔案 未選掛	睪檔案	
		-	
ame	Subject	Issuer	Status

3. The following dialog will appear.

Certificate Name :	RootCA		
Organization Unit :	DT		
Organization :	DrayTek		
Locality(City) :	HS		
State/Province :	Taiwan		
Common Name :	CA_license		
Email Address :	service@drayte	ccom	
Key Size :	1024	~	
Country :	TW		
Passphrase :			

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.

Trusted CA					
🚺 Upload	<u> iii</u> Delete 🛛 🐺 Do	wnload 🛛 🔊 Build R	RootCA		
Select File :	選擇檔案]未選擇	檔案			
Select File : Name	[選擇檔案] 未選擇 Subject	檔案 Issuer	Status	Valid from	Valid to

### 4.9.3 Remote Certificate

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

<b>Dray</b> Tek	Vigor 3900 Ser	ies	16:03:00	Login: Admin	Ð
[]	Certificate Management >> Re	mote Certificate			2
Auto Logout : Off 🛛 🗸	Remote Certificate				
Quick Start Wizard		-			
Online Status	💓 Upload 🛚 🍈 Delete	<table-of-contents> Download 🔌 Sign</table-of-contents>			
WAN		-			
LAN	Select File: 選擇檔:	<b>案</b> 】未選擇檔案			
NAT		0	<b>21</b> - 1		
Firewall	Name	Subject	Status		
Objects Setting		No iter	ms to show.		
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
Local Certificate					
Trusted CA Certificate					
Remote Certificate					
SSL VPN					
Central VPN Management					
Bandwidth Management					
USB Application					
System Maintenance					
Diagnostics					
External Devices					
Product Registration					

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 <b>Browse</b> button to specify a file to be used as trusted CA certificate.
Name	Display the name of remote certificate built.
Subject	Display the subject of remote certificate built.
Status	Display the status of remote certificate built.

# 4.10 SSL VPN

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

There are two benefits that SSL VPN provides:

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

SSL VPN	V
SSL W	/eb Proxy
SSL A	pplication
Online	User Status
Contral	VPN Managemer

### 4.10.1 SSL Web Proxy

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

<b>Dray</b> Tek	Vigor 3900 Se	eries 14:07:0	6 Login: Admin	Ð
Auto Logout : Off v	SSL VPN >> SSL Web Proxy SSL Web Proxy			
Online Status	🕼 Add 🔀 Edit 👖	Delete 🧳 Refresh		Profile Num
WAN	Profile	URL	Host IP Address	
LAN	swm	http://swm.draytek.com	172.18.2.19	
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
SSL Web Proxy				
SSL Application				
Online User Status				
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices				
Product Registration	4			•

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 <b>Edit</b> 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 <b>Delete</b> 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.

SSL Web Proxy		
🚺 Add 🔀 Kedit	<u> iii</u> Delete	< Refresh
Profile	URL	

3. The following dialog will appear.

Profile :	SSL_WP_1	
URL:	www.draytek.com	
Host IP Address	: 172 16 3	89

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.

SSL Web Proxy		
🕼 Add 🛛 🔀 Edit	🏢 Delete 🛛 📢 Refresh	
Profile	URL	Host IP Addre

# 4.10.2 SSL Application

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

### 4.10.2.1 VNC

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

<b>Dray</b> Tek	Vigor 3900 s	eries	14:08:35	Login: Admin	Đ
	SSL VPN >> SSL Application >>	VNC			
Auto Logout : Off	VNC RDP				
Quick Start Wizard					Profile Num
Online Status	🚺 Add 🔀 Edit	🔟 Delete 🛭 🛠 Refresh			Frome Nom
WAN	Profile	IP Address	Port	Scaling	
LAN	vnc	192.168.139.10	5900	100%	
NAT	vnc_pc	192.168.139.12	5900	100%	
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
SSL Web Proxy					
SSL Application					
Online User Status					
Online User Status Bandwidth Management					
Bandwidth Management					
Bandwidth Management System Maintenance					

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 <b>Edit</b> 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 <b>Delete</b> 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.

VNC	RDP		
🚯 Add	🔀 Edit	🔟 Delete	🥩 Refr
Profile		IP Address	

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.

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



5. A new SSL Application profile has been created.



### 4.10.2.2 RDP

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

<b>Dray</b> Tek	Vigor 390	O Series	14:15:58	Login: Admin	Ð
	SSL VPN >> SSL Applica	tion >> RDP			
Auto Logout : Off 🛛 🗸	VNC	2DP			
Quick Start Wizard	🕼 Add 💥 E	dit <u> Delete</u> 🐼 Refresh			Profile Num
Online Status					
WAN	Profile	IP Address	Port	Screen Size	
LAN	rdp	192.168.139.10	3389	Fullscreen	
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
SSL Web Proxy					
SSL Application					
Online User Status					
Bandwidth Management					
System Maintenance					
Diagnostics					
External Devices					
Product Registration	4		111		•

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 <b>Edit</b> 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 <b>Delete</b> 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.

VNC RDP		
🕼 Add 🛛 🗶 Edit	前 Delete	< Refresh
Profile	IP Address	P

3. The following dialog will appear.

P		-
Profile :	RDP_1	
IP Address :	192 . 168 . 1 . 57	
Port :	3389	
Screen Size :	Fullscreen 🗸	
		_
	📑 Apply 🄇	3 Cancel

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	
1440×900	
1280x1024	
1280x768	
1152x864	
1024x768	
1024x600	
800×600	
640x480	

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

VNC	RDP		
🚯 Add	🔀 Edit	🏢 Delete 🛛 🗳 Refresh	
ofile		IP Address	Port

## 4.10.3 Online User Status

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

<b>Dray</b> Tek	Vigor 3900 s	ieries 14:17:	9 Login: Admin	Ð
	SSL VPN >> SSL VPN Status			
Auto Logout : Off	SSL VPN Status			
Quick Start Wizard				
Online Status	S Refresh	Auto Refresh : 10 Seconds 👻		
WAN	User Name	Remote IP	Time out	
LAN	vivian	192.168.139.10	0	
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
SSL Web Proxy				
SSL Application				
Online User Status				
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				

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

# **4.11 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.

Central VPN Management
General Setup
CPE Management
Log / Alert

Note: 1. Such menu can manage the CPE connected through WAN only.

2. Up to 16 devices can be managed.

#### 4.11.1 General Setup

#### 4.11.1.1 General Setup

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

<b>Dray</b> Tek	Vigor 3900 Series	13:48:35	Login: Admin	Ð
	Central VPN Management >> General Setup >> General Setup			
uto Logout : Off 🛛 👻	General Setup VPN General Setup			
Quick Start Wizard				
Online Status	Enable			
WAN	WAN Profile : wan1			
LAN				
NAT	Port:			
Firewall	Username :			
Objects Setting	Password :			
User Management	Polling Status :      Enable      Disable			
Applications	Polling Interval : 900			
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
General Setup				
CPE Management				
Log / Alert				
Bandwidth Management				
USB Application				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				
			<b>D</b>	<b>•</b> •
			💾 Apply (	🔇 Cance

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	<b>Enable</b> – Click it to enable the polling function. <b>Disable</b> – Click it to disable the polling function.
Polling Interval	Type the time value (unit is second). The range is from $60 \sim 86400$ .
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

## 4.11.1.2 VPN General Setup

This page allows you to configure the basic settings for the VPN tunnel of Vigor3900.

<b>Dray</b> Tek	Vigor 3900 Series	13:51:20	Login: Admin	Ð
	Central VPN Management >> General Setup >> VPN	l General Setup		
to Logout : Off 🛛 🖌	General Setup VPN General Setup			
Quick Start Wizard				
Online Status				
WAN	WAN Profile : wan1	~		
LAN	Local IP / Subnet : 192 168 1	0 255.255.255.0/24 ~		
NAT	IPsec Security Method : AH	~		
Firewall	IKE Phase1 Mode : Aggressive	~		
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
General Setup				
CPE Management				
Log / Alert				
Bandwidth Management				
USB Application				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				
			💾 Apply	🙆 Cance

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 <b>AH</b> 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.

## 4.11.2 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

<b>Dray</b> Tek	Vigor 3	<b>,</b>						min 🕒
	Central VPN Ma	nagement >:	> CPE Manage	ment >> CPE I	Vaintenance			
to Logout : Off 🛛 👻	CPE Mainten	ance VPN	Management	Map				
Quick Start Wizard	Managed		-					
Online Status		Devices sta		< Refresh	蒇 Recycle Bin		Total nu	mber of devices: : (
WAN	- Edit	🔝 Detall	III Delete	So Reiresti	M Recycle Bin		Totarna	mber of devices
LAN								
NAT								
Firewall								
Objects Setting								
User Management								
Applications								
VPN and Remote Access								
Certificate Management								
SSL VPN								
SSL VPN Central VPN Management	➢ Maintenai	nce						
SSL VPN Central VPN Management General Setup	Maintenai		m Delete (	A Refresh	File Explorer			
SSL VPN Central VPN Management General Setup CPE Management	🚯 Add	🔀 Edit	m Delete		File Explorer		<b>F</b> H	<b>0</b> -1-1-2
SSL VPN Central VPN Management General Setup CPE Management Log / Alert			Delete •	Refresh		Weekdays	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management	🚯 Add	🔀 Edit				_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application	🚯 Add	🔀 Edit			Schedule	_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application System Maintenance	🚯 Add	🔀 Edit			Schedule	_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application System Maintenance Diagnostics	🚯 Add	🔀 Edit			Schedule	_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application System Maintenance Diagnostics External Devices	🚯 Add	🔀 Edit			Schedule	_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application System Maintenance Diagnostics	🚯 Add	🔀 Edit			Schedule	_	Filename	Status
SSL VPN Central VPN Management General Setup CPE Management Log / Alert Bandwidth Management USB Application System Maintenance Diagnostics External Devices	🚯 Add	🔀 Edit			Schedule	_	Filename	Status

Page with CPE connected

	Central VPN Ma	nagement >:	> CPE Manage	ement >> CPE I	Jaintenance			
uto Logout : Off 🛛 👻	CPE Mainter	ance VPN	Management	Мар				
Quick Start Wizard		Devices Sta	-					
Online Status							Total r	number of devices:
WAN	🗶 Edit	🛄 Detail	III Delete	🖈 Refresh	👬 Recycle Bin		rutarr	iumper of devices.
LAN								
NAT			-					a sector
Firewall			1					10000
Objects Setting			- HI		4.111	A 111		a iii
User Management								
Applications	bbb		chongq		2830	pbx		3200
VPN and Remote Access	172.17.1	.246	172.17.1	.215	172.17.1.208	172.17.1	.247	172.17.1.116
Certificate Management	S		$\leq$		<b>S</b>	2		
SSL VPN								
Central VPN Management	P Maintena							
General Setup			m Delete	🍊 Defeerb	File Explorer			
CPE Management	🕼 Add			-				
Log / Alert	Profile	Device	Name	Action	Schedule	Weekdays	Filename	Status
	test	DrayTek <u></u>	_00507F_ Con	figuration Bac	Once		test	[Finished]
Bandwidth Management		DravTek	_00507F_ Firm	ware Upgrad	Weekdays		./cvm/files/00	50
Bandwidth Management USB Application	2830							
Bandwidth Management	2830	Diajion						
Bandwidth Management USB Application System Maintenance Diagnostics	2830	Drayron						
Bandwidth Management USB Application System Maintenance	2830	Draftor						
				-	Once	Weekdays		•

Item	Description

Managed Devices Status	This area displays icons for the CPE managed by Vigor3900. <b>Edit</b> – To modify the name and location of specific CPE, click the one you want and click the <b>Edit</b> 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         Lating :       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					
	<b>Detail</b> – It displays the same content as the Edit button. However, it cannot be used to modify name or location. <b>Delete</b> – To disconnect the management of any CPE, click the CPE icon you want and click the Delete button.					
	<ul> <li>Refresh – Click it to refresh current page.</li> <li>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.</li> </ul>					
	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 <b>Managed Devices Status</b> area again.					
Maintenance	This area displays all the profiles which are created for applying to the managed device. <b>Add</b> – To add a new profile, simply click it to open a pop up window.					

**Dray** Tek

Profile :	2830	
Device :	DrayTek_00507F_Vigo 🗸	
Action :	~	
Schedule :	Firmware Upgrade	
oonouno i	Configuration Backup	
Start Date :	Configuration Restore	
Start Time :	00:00:00	
End Date :	2010-01-01	
End Time :	00:00:00	
Weekdays :	~	
Filename :	<b>(</b>	

**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.

🔯 Upload	🔟 Delete	<table-of-contents> Download</table-of-contents>	🕼 Create folder	< Refresh	
Filename	Property	Size	LastModify	Directory	
	Directory	1248	2013/05/07/ 09:4	./cvm/files	1
	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	L
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.

1. Click Add from the Maintenance area

		 e 🗳 Refresh
ofile	Device	Action

3. The Maintenance dialog appears.

Profile :		
Device :	*	
Name :		
Action :	~	
Schedule :	Once 👻	
Start Date :	2010-01-01	
Start Time :	00:00:00	
End Date :	2010-01-01	
End Time :	00:00:00	
Weekdays :	~	
Filename :	(b)	

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.

**Dray** Tek

	DrayTek_00507F_Vigo 🗸				
	DrayTek_00507F_Vigor_00507FEC2130 DrayTek_00507F_Vigor2110V_00507F987B80 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				
	<ul> <li>Firmware Upgrade – It means such profile will be used for firmware upgrade.</li> <li>Configuration Backup – It means such profile will be used for configuration backup of the selected CPE.</li> <li>Configuration Restore – It means such profile will be used for restoring the configuration of the selected CPE.</li> </ul>				
Schedule	The new created profile can be applied to the selected CPE based on the schedule configured here.				
	<ul> <li>Now – The action will be performed for the selected CPE immediately.</li> <li>Once – The action will be performed for the selected CPE at the specified time, and will be done for once.</li> <li>Weekdays – The action will be performed for the selected CPE at the time and date specified below every week.</li> </ul>				
Start Date / End Date	It is available only when <b>Once</b> is selected as <b>Schedule</b> . Specify the starting date /ending time with the format YYYY-MM-DD.				
Start Time / End Time	It is available only when <b>Once</b> is selected as <b>Schedule</b> . Specify the starting date /ending date with the format YYYY-MM-DD.				
Weekdays	It is available only when <b>Weekdays</b> is selected as <b>Schedule</b> . Simply check the day you want.				



	Mon Tue Wed Thu Fri Sat Sun		
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.		

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

## 4.11.2.2 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).

<b>Dray</b> Tek	Vigor 390	O Series			14:34:00	Login: Adn	nin	₽
	Central VPN Manage	ement >> CPE Manag	jement >> \	VPN Management				
Auto Logout : Off 🛛 🗸	CPE Maintenanc	e VPN Managemer	nt Map					
Quick Start Wizard	NTR DOTO			Defend	Keep VPN Se	ttinge		
Online Status	T PPTP	🖇 IPsec 🛛 🔀 Advar	icea 🔊 i	Refresh		-	Defeat	
WAN							Refresh	
LAN					Profile	Device	Name	
NAT						No items to sh	10W.	
Firewall								
Objects Setting								
User Management								
Applications								
VPN and Remote Access								
Certificate Management								
SSL VPN								
Central VPN Management	Connected De						(* 5)	· · · ·
General Setup	VPN			Made al Made a Un Tit	DV(Deslate)	TV(Declarks)	🖈 Re	
CPE Management	VPN	Type R	emote IP	Virtual Netwoi Up Tir	ne RX(Packets)	TX(Packets)	Disconnect	
Log / Alert				No items to sho	Ν.			
Bandwidth Management								
USB Application								
System Maintenance								
Diagnostics								
External Devices								
Product Registration								

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 <b>"3.7 How to manage the CPE (router) through</b> <b>Vigor3900?"</b> for more detailed information. If the VPN isn't established successfully, a red line will

	appear instead.
	CPE Maintenance VPN Management Map
	The sec X Advanced S Refresh
РРТР	To build a quick VPN connection with <b>PPTP</b> , 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 <b>IPsec</b> , simply click the remote CPE (waiting for the icon to be bigger) first and then click it. If the connection is built successfully, a blue line will appear.
Advanced	To build a VPN connection with detailed configuration (such as PPP authentication and VJ compression), click Advanced tool.
	Specify the CPE from the Device drop down list; choose the name of the CPE; select PPTP or IPsec as the Dial Type; choose PAP_only or PAP_or_CHAP as PPP authentication; enable or disable VJ Compression; then click <b>Connect</b> to build the VPN connection. <b>Note:</b> If the VPN connection has been established successfully, a new <i>LAN to LAN profile</i> will be created for the CPE automatically. See the following example.
	Vigor2830 Series         ADSL2 + Security Firewall         Off         Outlok Start Wizard         Service Activation Wizard         Online Status         VNAN         LAN         LAN         Differsation         Provide Activation Wizard         Online Status         VNAN         LAN         LAN </th



Keep VPN Settings	<ul> <li>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.</li> <li>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.</li> </ul>
	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_Vigor3200_00507FCD0440         DrayTek_00507F_Vigor0507FCF673C
	<ul> <li>Delete – Click it to delete the profile. The VPN between the router and the client might not be guaranteed.</li> <li>Refresh – Click it to refresh current page.</li> <li>Profile – Display of the profile used now.</li> <li>Device – Display the name of the CPE connected to Vigor router via VPN.</li> <li>Name – Display the name (can be modified by the administrator) of the device. Refer to 4.11.2.1 CPE</li> </ul>
Connected Devices	<ul> <li>Maintenance for detailed information.</li> <li>Once the VPN is established successfully, the basic information such as the connection type, IP address, RX/RX will be displayed on this field.</li> <li>Refresh – Click it to refresh current page.</li> <li>VPN – Display the name of the VPN.</li> <li>Type – Display the type of the connection mode.</li> <li>Remote IP – Display the IP address of the remote end.</li> <li>Virtual Network – Display the IP address of Vigor3900.</li> <li>Up Time –Display the connection time of such VPN.</li> </ul>
	<ul> <li>RX(Packets) /TX(Packets) –Display the number of the packets exchanged in such VPN.</li> <li>Disconnect – Click it to disconnect the VPN.</li> </ul>

## 4.11.2.3 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**.



# **Dray** Tek

#### 4.11.3 Log/Alert

The Log page offers brief information to identify the CPE connected to Vigor3900.



The Alert page offers brief information to identify the CPE connected to Vigor3900.

<b>Dray</b> Tek	Vigor 390	<b>V</b> Series		06:05	Login: Fae	Ð
	Central VPN Managem	ent >> Log / Alert >> Ale	ert			
to Logout : 5Min 🗸 🗸	Log	lert				
Quick Start Wizard						
Online Status	🗢 Refresh	Auto	Refresh : 10 Seconds 👻			
WAN	ID *	Time	Device Name	Туре	Description	
LAN	1	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	1
NAT	2	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	=
Firewall	3	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	
Objects Setting	4	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor2' CPE Connection	CPE is offline!	
User Management	5	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor2{ CPE Connection	CPE is offline!	
Applications	6	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor2{ CPE Connection	CPE is offline!	
VPN and Remote Access	7	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	
Certificate Management	8	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	
SSL VPN	9	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is offline!	
Central VPN Management	10	2011-01-01 08:00	:48 UTC DrayTek_00507F_Vi	gor3: CPE Connection	CPE is offline!	
General Setup	11	2011-01-01 08:00	:53 UTC DrayTek_00507F_Vi	gor2' CPE Connection	CPE is Online!	
Topology Management	12	2013-05-08 11:52	:41 UTC DrayTek_00507F_Vi	gor2' CPE Connection	CPE is offline!	
Log / Alert	13	2013-05-08 11:52	:57 UTC CVM_EC2130	PPTP	CVM_EC2130 connel	cted!
Bandwidth Management	14	2013-05-08 11:52	:58 UTC pptp	PPTP	pptp connected!	
USB Application	15	2013-05-08 11:52	:59 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is Online!	
System Maintenance	16	2013-05-08 11:53	:01 UTC DrayTek_00507F_Vi	gor_( CPE Connection	CPE is Online!	
Diagnostics	17	2013-05-08 11:53	:03 UTC DrayTek_00507F_Vi	gor2' CPE Connection	CPE is Online!	
External Devices	18	2013-05-08 11:53	:13 UTC CVM_6AFAF8	IPSec	CVM_6AFAF8 connec	ted!
Product Registration	19	2013-05-08 11:53	:15 UTC DrayTek_00507F_Vi	gor3: CPE Connection	CPE is Online!	-

# 4.12 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management
Quality of Service
QoS Rule
Sessions Limit
Bandwidth Limit

The QoS (Quality of Service) guaranteed technology in the Vigor router allows the network administrator to monitor, analyze, and allocate bandwidth for various types of network traffic in real-time and/or for business-critical traffic. Thus, timing-sensitive applications will not be impacted by web surfing traffic or other non-critical applications, such as file transfer. Without QoS-guaranteed control, there would be virtually no way to prioritize users/services or guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications.

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



### 4.12.1 Quality of Service

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

## 4.12.1.1 General Setup

This page allows you to set WAN interface for QoS. Choose one of the WAN interfaces and click **Apply** to save the settings.

<b>Dray</b> Tek	Vigor 3900 Series	14:47:41	Login: Admin	Ð
	Bandwidth Management >> Quality of Service >> General	Setup		0
Auto Logout : Off 🛛 🗸	General Setup Outgoing Queue Incoming Queue			
Quick Start Wizard				
Online Status	QoS WAN : Disable 🗸			
WAN	Disable			
LAN	wan1			
NAT	wan2			
Firewall	wan3 wan4			
Objects Setting	wan4 wan5			
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management				
Quality of Service				
QoS Rule				
Sessions Limit				
Bandwidth Limit				
USB Application				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				
			💾 Apply	🔉 Cancel
				-

## 4.12.1.2 Outgoing Queue

This page allows you to configure bandwidth percentage of data and voice signals transmission for outgoing data.

	Bandwidth Manageme	ent >> Quality of Ser	vice >> Outgoing Queue		(
Auto Logout : Off 🛛 👻	General Seturi O	Itgoing Queue Inco	mina Queue		
Quick Start Wizard	- Outgoing Queue		adddo		
Online Status	- Outgoing Queue	1~5			
WAN	Status :	🔵 Enable 💿 Disa	ible		
LAN	Bandwidth	0	💿 Kbps  🔿 Mbps		
NAT	Queue 5 Weight :	5	(Local Service)		
Firewall	Queue 4 Weight :	4			
Objects Setting	Queue 3 Weight :	3			
User Management	Queue 2 Weight :	2			
Applications	Queue 1 Weight :	1	(Default Queue)		
VPN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Management					
Bandwidth Management					
Quality of Service					
QoS Rule					
Sessions Limit					
Bandwidth Limit					
USB Application					
System Maintenance					
Diagnostics					
External Devices					
Product Registration					



Item	Description
Status	Click <b>Enable</b> to enable such function.
Bandwidth	Type the number as the total transmission rate for the outgoing data. The range can be set from 64000 to 10000000.
	Click the unit for such rate.
Queue 5 Weight ~ Queue 1 Weight	There are several available outgoing queues, four shapers at varying levels, and five data queues with weights. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0. 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.

## 4.12.1.3 Incoming Queue

This page allows you to configure bandwidth percentage of data and voice signals transmission for incoming data.

<b>Dray</b> Tek	Vigor 3900	Series	14:49:09	Login: Admin	E
	Bandwidth Management	>> Quality of Service >> Incomi	ng Queue		(
Auto Logout : Off	General Setup Outg	ina Queue Incomina Queue			
Quick Start Wizard	- Incoming Queue 1~				
Online Status					
WAN	Status: (	) Enable 💿 Disable			
LAN	Bandwidth : 0	Kbps	○ Mbps		
NAT	Queue 5 Weight : 5				
Firewall	Queue 4 Weight : 4				
Objects Setting	Queue 3 Weight : 3				
User Management	Queue 2 Weight : 2				
Applications	Queue 1 Weight : 1	(Default Q	ueue)		
VPN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Management					
Bandwidth Management					
Quality of Service					
QoS Rule					
Sessions Limit					
Bandwidth Limit					
USB Application					
System Maintenance					
Diagnostics					
External Devices					
Product Registration					_
				💾 Apply	- 🙆 Cance

Item	Description
Status	Click <b>Enable</b> to enable such function.
Bandwidth	Type the number as the total transmission rate for the incoming data. The range can be set from 64000 to 10000000. Click the unit for such rate.
Queue 5 Weight ~	There are several available incoming queues, four shapers at



Queue 1 Weight	<ul><li>varying levels, and five data queues with weights. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0.</li><li>Type the weight of queues in bytes, range from 0 to 1000000.</li></ul>
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

## 4.12.2 QoS Rule

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

<b>Dray</b> Tek	Vigor	500 5	eries	14:49		Login: Adm	in 🖯
	Bandwidth Ma	nagement >	> QoS Rule				
uto Logout : Off 🛛 👻	QoS Rule						
Quick Start Wizard			-				_
Online Status	C Add	🔀 Edit	🔟 Delete 🛭 📢	🕨 Refresh 🛛 🕻 Rename			Prot
WAN	Profile	Enable	Source IP	Destination IF Service Type Match	Type DSCP	TOS	Queue Numb
LAN				No items to show.			
NAT							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Central VPN Management							
Bandwidth Management							
Quality of Service							
QoS Rule							
Sessions Limit							
Bandwidth Limit							
USB Application							
System Maintenance							
Diagnostics							
External Devices							
Product Registration							

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 <b>Edit</b> 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 <b>Delete</b> button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile for the filter.
Enable	Display the status of the profile. False means disabled; True

# **Dray** Tek

	means enabled.
Source IP	Display the source IP address for the filter.
Destination IP	Display the destination IP address for the filter.
Service Type	Display the service type (e.g., IKE, HTTP, AUTH and etc) for the filter.
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.
Queue Number	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.

QoS F	Rule		
6	Add 🔀	Edit <u> m</u> Del	ete 🥩
Profile	Enable	Source	IP Desti

3. The following dialog will appear.

Profile					- 0
Profile :					
	Enable				
Match Type :	None	~			
DSCP :	Default	~			
TOS :	Normal-Service	~			
Queue Number :	1 [Weighted Queue]	~			
source target Source IP C					
source targe	et				
Source IP G destination					
Destination	_				
Destination					
<ul> <li>general targ</li> </ul>					
Service Typ	e				

Item	Description					
Profile	Type the name of the filter profile.					
Enable	Check this box to enable such profile.					
Match Type	Use the drop down list to specify a suitable match type.					
	DSCP					
	None					
	DSCP					
	TOS					
DSCP	It is available when DSCP is selected as the Match type.					
	AF Class1 [High Drop]					
	AF Class2 [Low Drop]					
	AF Class2 [Medium Drop]					
	AF Class2 [High Drop]					
	AF Class3 [Low Drop]					
	AF Class3 [Medium Drop]					
	AF Class3 [High Drop]					
	AF Class4 [Low Drop]					
	AF Class4 [Medium Droo]					
	DSCP : IP precedence 7					
TOS	It is available when TOS is selected as the Match type.					
	Normal-Service					
	Normal-Service					
Queue Number	Choose a queue number to category the packets matching					
	with the condition configured as above. Queue 5 is the highest; 1 is the lowest.					
	1 [Weighted Queue] 🐱					
	1 [Weighted Queue]					
	as 2 [Weighted Queue]					
	oje 3 [Weighted Queue] 4 [Weighted Queue]					
	et 5 [Weighted Queue]					
	Object					
source target	Click on the left side of the <b>Source IP Object/Source</b>					
	Group profile. Check the object profile(s) as the source					
	target.					
	source target					
	Source P Object Profile Address Type Start IP Address End IP Address Subnet Mask Edit					
	P_styrc_1 Subret 192.165.178 255.255.5 X					
	0					
	<b>Source IP Object</b> – Use the drop down list to choose one of					
	the source IP objects for such rule profile.					
	<b>Source IP Group</b> – Use the drop down list to choose one of					
	the source IP group for such rule profile.					

	If you want to create a new IP object, simply click to open the following dialog.
	Source IP Object
	Profile :
	Address Type : Single
	Start IP Address :
	Apply 🐼 Cancel
	<b>Profile</b> – 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.
	<b>Start IP Address</b> - Type the IP address of the starting point for such profile.
	<b>End IP Address</b> - Type the IP address of the ending point for such profile if you choose <b>Range</b> as <b>Address Type</b> .
	Subnet Mask – Choose the subnet mask from the drop down list if you choose Subnet as Address Type.
destination target	Click on the left side of the <b>Destination IP Object</b> / <b>Destination IP Group</b> profile. Check the object profile(s) as the destination target.
	<b>Destination IP Object</b> – Use the drop down list to choose
	one of the destination IP objects for such rule profile.
	<b>Destination IP Group</b> – 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.
	Destination IP Object
	Profile :
	Address Type : Single v
	Start IP Address :
	Apply 🔇 Cancel
	<b>Profile</b> – 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.
	<b>Start IP Address</b> - Type the IP address of the starting point for such profile.
	<b>End IP Address</b> - Type the IP address of the ending point for such profile if you choose <b>Range</b> as <b>Address Type</b> .
	<b>Subnet Mask</b> – Choose the subnet mask from the drop down list if you choose <b>Subnet</b> as <b>Address Type</b> .



general target	Service Type - Choose one of the service types from the drop down list.
	Profile         Protocol         Source Port Start         Source Port End         Destination Port St         Destination Port St <thdest< th="">         Dest         <thdestinatin p<="" th=""></thdestinatin></thdest<>
	If you want to create a new service type, simply click to open the following dialog.
	Profile :     for_out_filter       Protocol :     TCP       Source Port Start :     1
	Source Port End :     65535       Destination Port Start :     1       Destination Port End :     65535
	<b>Profile</b> – type a new name for such service type.
	<b>Protocol</b> –There are two options: <b>TCP</b> , <b>UDP</b> and <b>TCP/UDP</b> . Select the protocol that you want to use.
	<b>Source Port Start /End -</b> Type the start /end number for the port range of the source port for such filter.
	<b>Destination Port Start / End -</b> Type the start /end number for the port range of the destination port for such filter.
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

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

🕼 Add	🔀 Edit	🔟 Delete 🛛 🖈	Refresh 🕻	Rename				Prof
Profile	Enable	Source IP	Destination I	Service Type	Match Type	DSCP	TOS	Queue Numb
QoS_11	true	IP_object_1	IP_object_1	AUTH	TOS	Default	Normal-Servi	1 [Weighted Q

#### 4.12.3 Sessions Limit

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

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

<b>Dray</b> Tek	Vigor 3900 Series	15:05:00	Login: Admin	Ð
	Bandwidth Management >> Sessions Limit			(
Auto Logout : Off 🛛 💌	Sessions Limit			
Quick Start Wizard		A	- <b>9</b>	
Online Status	🕼 Add 🔀 Edit 🝈 Delete 🗳 Refresh	🚡 Move Up 🛛 🐣 Move Dow	n 🕻 Rename	
WAN	Profile Enable Source IP	Object Source IP Group	Time Object Time Group	
LAN		No items to show.		
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				-
Bandwidth Management	Default Session Limit	🔵 Enable 💿 Disable		
Quality of Service	Default Max Sessions :			
QoS Rule	Use Default Message :	💿 Enable 🔵 Disable		
Sessions Limit		<html><head><title>Acces&lt;/td&gt;&lt;td&gt;s Denied</title></head><body< td=""><td>Ξ</td></body<></html>	Ξ	
Bandwidth Limit			> <h3> &gt;<font color="blue&lt;/td" face="arial"><td></td></font></h3>	
USB Application	Default Connection Limit Administration Message		nt> > > > > <b< td=""><td></td></b<>	
System Maintenance			tions to allow furthur Internet access.	ase
Diagnostics			administrator for further information br	> <hr< td=""></hr<>
External Devices	4	ш		
Product Registration			🗎 Apply 🛛 😣 C	ancel
	1			>

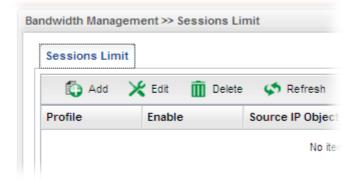
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile.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



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, <b>None</b> 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	<ul> <li>Enable – Use the default message to display on the page that the user tries to access into the blocked web page</li> <li>Disable – Type the message manually to display on the page that the user tries to access into the blocked web page.</li> </ul>
Default Connection Limit Administration Message	Such field is available when you disable the function of <b>Use</b> <b>Default Message</b> . 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.

rofile	-
Profile :	
Enable	
Max Sessions : 1000	
/hile no target has been specified, firewall rules	are applied to Any object
Firewall Objects	
🗉 general target	
Time Object	
Time Group	
source target	
Source IP Object	
Source IP Group	

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         Image: Profile interval object         Image: P
source target	<b>Source IP Object -</b> Click the triangle icon by to display the profile selection box. Choose one or more IP object profiles from the drop down list. The selected profile will be treated



	<ul> <li>as source target. You can click to create another new IP object profile.</li> <li>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.</li> </ul>
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.

Sessions Limit					
🕼 Add 🛛 🗙	Edit 前 Delete	🔹 Refresh 🛛 😭 Move	Up 🛛 🐣 Move Dowr	n 🕻 🥵 Rename	
Profile	Enable	Source IP Object	Source IP Group	Time Object	Time Group

#### 4.12.4 Bandwidth Limit

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

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

<b>Dray</b> Tek	Vigor 3900 Series	15:12:19	Login: Admin	Ð
	Bandwidth Management >> Bandwidth Limit			2
Auto Logout : Off	Bandwidth Limit			
Quick Start Wizard			4 3 -	
Online Status	🕼 Add 💥 Edit 🛅 Delete 🗳 Refresh 🔮	Move Up 🛛 🐣 Move Down	🔓 Rename	
WAN	Profile Enable Source IP O	ject Source IP Group	Time Object Time Group	
LAN	Band_1 enable			
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Central VPN Management				
Bandwidth Management	Enable Smart Bandwidth Limit (Will apply to the L	AN IP not in Limitation List,v	/hose session number exceeds the t	threshold)
Quality of Service	Sessions Threshold : 1000			
QoS Rule	TX Limit : 5000	ops () Mbps		
Sessions Limit	· · · · · · · · · · · · · · · · · · ·	ops () Mbps		
Bandwidth Limit		· · ·	also not bounded by smart bandwidt	linoit
USB Application		ops () Mbps	also not boanded by smart bandwidt	ar min.
System Maintenance				
Diagnostics	Default RX Limit : 0	ops 🔘 Mbps		
External Devices	1			
Product Registration			🗎 Apply 🛛 🚳	Cancel
				•
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			

Item	Description
Add	Add a new profile.

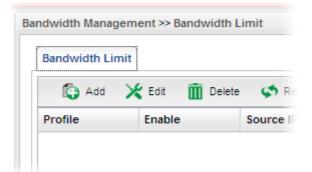


<b>T</b> 1''	
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the <b>Edit</b> button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile.
	To delete a profile, simply select the one you want to delete and click the <b>Delete</b> 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.
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, <b>None</b> 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	<ul> <li>The default limit will apply to LAN IP(s) not in the above configuration profiles</li> <li>Default TX Limit – Define the limitation for the speed of the upstream.</li> <li>Default RX Limit –Define the limitation for the speed of the upstream.</li> </ul>
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.



#### How to add a bandwidth limit profile

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



3. The following dialog will appear.

Profile			
Profile :			
	Enable		
TX Limit :	1024	💿 Kbps 🔘 Mbps	
RX Limit :	1024	💿 Kbps 🔘 Mbps	
Mode :	📀 Each 🔘 Share		
		·····	
		ified, firewall rules are applied to Any object	
	wall Objects		
genera			
	Object		
source	Group		
	ce IP Object		
	ce IP Group		
	oo n oroop		
			🗎 Apply 🛛 🛞 Cano
			Apply 🐼 card

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. Select <b>Each</b> 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 <b>Shared</b> to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.				
Mode					
general target	<b>Time Object</b> - Click the triangle icon $\triangleright$ 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				
	<b>Time Group</b> - Click the triangle icon $\blacktriangleright$ 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	<b>Source IP Object -</b> Click the triangle icon <b>b</b> 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.				
	<b>Source IP Group -</b> Click the triangle icon be 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 Li	imit				
🚺 Add	🔀 Edit 👖 De	lete 🗳 Refresh	👉 Move Up 🛛 🜷	Move Down	<b>G</b> Rename
Profile	Enable		Source IP Group		Time Group
Band 1	enable				

# 4.13 USB Application

## 4.13.1 Temperature Sensor

A USB Thermometer can be attached to Vigor router to monitor the environmental temperature. If the temperature is higher the upper limit or lower than the lower limit, an alert would be sent out for notification.

### 4.13.1.1 General Setup

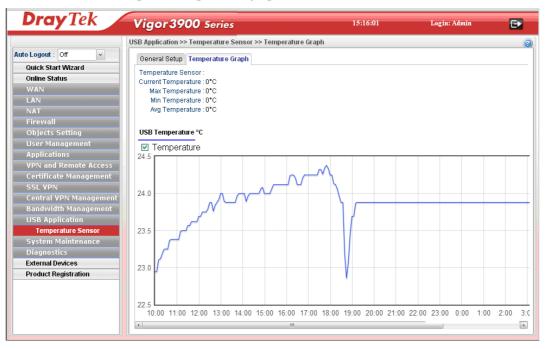
Auto Logout: Off       Image: Off Outick Start Wizard         Outick Start Wizard       General Setup         Outick Start Wizard       Image: Off Outick Start Wizard         Ouline Status       Image: Off Outick Start Wizard         WAN       Image: Off Outick Start Wizard         Usb Applications       Image: Off Outick Start Wizard         WAN       Image: Off Outick Start Wizard         Ush And       Image: Off Outick Start Wizard         VAN       Image: Off Outick Start Wizard         Objects Setting       Image: Off Outick Start Upper limit: 50         Objects Setting       Image: Off Outick Outice Start Outice Sta	<b>Dray</b> Tek	Vigor 3900 Series		15:15:05	Login: Admin	Ð
Ouick Start Wizard   Online Status   WAN   LAN   NAT   Firewall   Objects Setting   User Management   Applications   VPN   Central VPN Management   Bandwidth Management   USB Application   Temperature Sensor   System Maintenace   Diagnostics   External Devices   Product Registration		USB Application >> Temperature Sens	sor >> General Setup			2
Online Status   WAN   LAN   NAT   NAT   Firewall   Objects Setting   User Management   Applications   VPN and Remote Access   Certral VPN Management   Bandwidth Management   USB Application   Temperature Sensor   System Maintenance   Diagnostics   External Devices   Product Registration		General Setup Temperature Grap	h			
	Online Status         WAN         LAN         NAT         Firewall         Objects Setting         User Management         Applications         VPN and Remote Access         Certificate Management         SSL VPN         Central VPN Management         Bandwidth Management         USB Application         Temperature Sensor         System Maintenance         Diagnostics         External Devices	Enable Temperature Sensor Display Unit : Temperature Alert Lower limit : Temperature Alert Upper limit :	Celsius 0 50			
					🗎 Apply	🔇 Cancel

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.

## 4.13.1.2 Temperature Graph

Below shows an example of temperature graph:



# **Dray** Tek

# 4.14 System Maintenance

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

Below shows the menu items for System Maintenance.

S	System Maintenance
	TR-069
	Administrator Password
	Configuration Backup
	Syslog / Mail Alert
	Time and Date
	Access Control
	SNMP Setup
	Reboot System
	Firmware Upgrade

#### 4.14.1 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.

<b>Dray</b> Tek	Vigor 3900 Ser	ies		15:19:54	Login: Admin	
	System Maintenance >> TR-00					(2)
Auto Logout : Off 🛛 👻	TR-069					
LAN						
NAT	Enable					
Firewall	ACS Server URL :					
Objects Setting	ACS Server Username :	are				
User Management	ACS Server Osername :					
Applications	WAN Profile :	wan1 🗸	1			
VPN and Remote Acces:						
Certificate Management	Port : CPE URL :	8069 http://:8069/cwmp/creg				
SSL VPN	Periodic Status	Disable      Enable				
Central VPN Manageme	Periodic Time :	900	sec (60-86400)			
Bandwidth Management	CPE Username :		Sec (60-86400)			
USB Application	CPE Disername : CPE Password :	vigor				
System Maintenance	CPE Password .					
TR-069						
Administrator Password						
Configuration Backup						
Syslog / Mail Alert Time and Date						
Access Control						
SNMP Setup						
Reboot System						
Firmware Upgrade						
Diagnostics						
External Devices					💾 Apply	🔉 Cancel
Product Registration -					E Abbiy	Gancer
Froduct registration						

Item	Description
Enable	Check this box to enable such profile.
ACS Server	Such data must be typed according to the ACS (Auto



URL/Username	Configuration Server) you want to link. Please refer to Auto
/Password	Configuration Server user's manual for detailed information.
WAN Profile	Choose one of the WAN profiles which will be recognized by VigorACS.
Port	Type the port number for Vigor3900 which will be recognized by VigorACS.
CPE URL	Display the URL of such CPE.
Periodic Status	The default setting is <b>Enable</b> . Please set periodic time for VigorACS to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.
Periodic Time	Set the time for VigorACS to send notification to CPE.
CPE Username	Type the user name for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
CPE Password	Type the password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

## 4.14.2 Administrator Password

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

<b>Dray</b> Tek	Vigor 3900 Series	15:20:40	Login: Admin	Ð
	System Maintenance >> Administrator Password			(2)
Auto Logout : Off   LAN  LAN  NAT  Firewall  Objects Setting  User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Manageme Bandwidth Management USB Application System Maintenance TR-069  Administrator Password Configuration Backup Sysiog / Mail Alert Time and Date Access Control SNMP Setup Reboot System Firmware Upgrade Diagnostics	Administrator Password         Original Password :         New Password :         Confirm Password :			
External Devices Product Registration			l	Apply

Item	Description
User Name	Display the name of the administrator.

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

## 4.14.3 Configuration Backup

Most of the settings can be saved locally as a configuration file, and can be applied to another router. The router supports functions of **restore and backup** for the configuration file.

4.14.3.1 Backup

<b>Dray</b> Tek	Vigor 3900 Sei	ies	15:21:29	Login: Admin	Ð
	System Maintenance >> Conf	iguration Backup >> Backup			0
Auto Logout : Off  LAN LAN LAN LAN LAN KAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Managemen Bandwidth Managemen USB Application System Maintenance TR-069 Administrator Password Configuration Backup Systog / Mail Alert Time and Date Access Control SNMP Setup Reboot System Firmware Upgrade	Backup Restore Password : Confirm Password : Backup Type :	Backup to Local File Backup to Local File Backup to Remote TFTP Server Backup Selected Config 900_2013-09-03.tgz			
Diagnostics External Devices				🗣 E	Эаскир
Product Registration -	4	T	11		•

Item	Description
Encrypt Config	Check this box to encrypt the configuration file.
	<b>Password</b> – Type a password for encrypting the file.
	<b>Confirm Password</b> – Retype the password for confirmation.
Backup Type	Choose one of the types to determine where the file will be stored.
	<b>Backup to Local File</b> – The configuration file will be stored in local host.
	<b>Backup to Remote TFTP Server</b> – The configuration file will be stored in the remote TFTP server specified.
	<b>Backup Selected Config</b> – 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.

## 4.14.3.2 Restore

<b>Dray</b> Tek	Vigor 3900 Series	15:22:29	Login: Admin	E
	System Maintenance >> Configuration Backup >> Resto	re		(
uto Logout : Off 🛛 👻	Backup Restore			
LAN 🕑				
NAT	Decrypt Config			
Firewall	Password :			
Objects Setting 📃	Confirm Password :			
User Management		10.5.51		
Applications	Restore Type:     Restore Settings via Loca	-		
VPN and Remote Acces:	Restore Settings via TFTF	Server		
Certificate Management	Select File: 選擇檔案 未選擇檔案			
SSL VPN				
Central VPN Manageme				
Bandwidth Managemen				
USB Application				
System Maintenance				
TR-069				
Administrator Password				
Configuration Backup				
Syslog / Mail Alert				
Time and Date				
Access Control				
SNMP Setup				
Reboot System				
Firmware Upgrade				
Diagnostics			1	🕈 Restore
External Devices				Residre
Product Registration -	4			>

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.
	<b>Password</b> – Type a password for encrypting the file.
	<b>Confirm Password</b> – Retype the password for confirmation.
<b>Restore Type</b>	Choose one of the types to determine where the file will be downloaded from.
	<b>Restore Settings via Local Config File</b> – Click it to restore the configuration settings through a configuration file stored locally.
	<b>Restore Settings via TFTP Server</b> – Click it to restore the configuration settings through TFTP server.
Select File	Use the <b>Browse</b> button to locate the file for uploading to the router.
Restore	Click it to upload the selected file to the router. After finishing the restoration, the system will ask you to reboot the router.

Confirm	×
Restore success, reboot now?	

#### 4.14.4 Syslog / Mail Alert

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

### 4.14.4.1 Syslog Access Setup

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

<b>Dray</b> Tek	Vigor 3900 Series	15:24:14	Login: Admin	Ð
	System Maintenance >> Syslog / Mail Alert >> Syslog	Access Setup		(
uto Logout : Off 🛛 👻	Syslog Access Setup Syslog File Mail Alert			
LAN	cyclog needed comp cyclog no mannen			
NAT	Chattan I want			
Firewall	Status Local -			
Objects Setting		ional)		
User Management	Firewall Log : 💿 Enable 🔘 Disable			
Applications	VPN Log : 💿 Enable 🔘 Disable			
VPN and Remote Acces	User Access Log : 🔘 Enable 💿 Disable			
Certificate Management	WAN Log : 💿 Enable 🔘 Disable			
SSL VPN	Others Log: <ul> <li>Enable</li> <li>Disable</li> </ul>			
Central VPN Manageme				
Bandwidth Management				
USB Application				
System Maintenance				
TR-069 =				
Administrator Password				
Configuration Backup				
Syslog / Mail Alert				
Time and Date				
Access Control				
SNMP Setup				
Reboot System				
Firmware Upgrade				
Diagnostics				
External Devices			💾 Apply	🔇 Cancel
Product Registration				

Item	Description		
Status	Choose one of the selections to determine current status for Syslog access. If you choose <b>Local</b> 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 <b>Remote</b> or <b>Both</b> is selected as <b>Status</b> .		
Server Port	Type the port number for the Syslog server.It is available when <b>Remote</b> or <b>Both</b> is selected as <b>Status</b> .		
Router Name	Type the name of the router. The default name is <i>Vigor</i> .		
Firewall Log	Click <b>Enable</b> to make the firewall log recorded in the Syslog.		



VPN Log	Click <b>Enable</b> to make the VPN log recorded in the Syslog.
User Access Log	Click <b>Enable</b> to make the user access log recorded in the Syslog.
WAN Log	Click <b>Enable</b> to make the WAN log recorded in the Syslog.
Others Log	Click <b>Enable</b> 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.

## 4.14.4.2 SysLog File

<b>Dray</b> Tek	Vigor 3900 Series	15:26:37	Login: Admin	•
	System Maintenance >> Syslog / Mail Alert >> Syslog File			
Auto Logout : Off 🛛 💌	Syslog Access Setup Syslog File Mail Alert			
LAN 🛃				
NAT	🗢 Refresh 🔍 Download Log 📠 Clear Syslog			
Firewall	Search			5
Objects Setting 📃	Log			
User Management	<13>Jan 6 11:00:02 Vigor: Hourly firewall iptables snapshot don	e		*
Applications	<13>Jan 6 10:00:01 Vigor: Hourly firewall iptables snapshot don	e		=
VPN and Remote Access	<13>Jan 6 09:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Certificate Management	<13>Jan 6 08:00:01 Vigor: Hourly firewall iptables snapshot don	e		
SSL VPN	<13>Jan 6 07:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Central VPN Manageme	<13>Jan 6 06:00:01 Vigor: Hourly firewall iptables snapshot don	e		
Bandwidth Management	<13>Jan 6 05:00:02 Vigor: Hourly firewall iptables snapshot don	e		
USB Application	<13>Jan 6 04:00:01 Vigor: Hourly firewall iptables snapshot don	e		
System Maintenance	<13>Jan 6 03:00:02 Vigor: Hourly firewall iptables snapshot don	e		
TR-069	<13>Jan 6 02:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Administrator Password	<13>Jan 6 01:00:01 Vigor: Hourly firewall iptables snapshot don	e		
Configuration Backup	<13>Jan 6 00:00:02 Vigor: Daily firewall iptables snapshot done			
Syslog / Mail Alert	<13>Jan 6 00:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Time and Date	<13>Jan 5 23:00:01 Vigor: Hourly firewall iptables snapshot don	e		
Access Control	<13>Jan 5 22:00:01 Vigor: Hourly firewall iptables snapshot don	e		
SNMP Setup	<13>Jan 5 21:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Reboot System	<13>Jan 5 20:00:01 Vigor: Hourly firewall iptables snapshot don	e		
Firmware Upgrade	<13>Jan 5 19:00:02 Vigor: Hourly firewall iptables snapshot don	e		
Diagnostics	<13>Jan 5 18:00:01 Vigor: Hourly firewall iptables snapshot don	e		
External Devices	<13>Jan 5 17:00:02 Vigor: Hourly firewall iptables snapshot don	e		

Item	Description	
Refresh	Renew the web page.	
Download Log	Save or open the Syslog file.	
Clear Syslog	Remove all of the records.	

## 4.14.4.3 Mail Alert

<b>Dray</b> Tek	Vigor 3900	Series	15:27:30	Login: Admin	Ð
	System Maintenance >	> Syslog / Mail Alert >> Mail Alert	1		(
Auto Logout : Off 🛛 🗸	Syslog Access Setu	p Syslog File Mail Alert			
LAN NAT Firewall Objects Setting User Management	Enable Mail From :	Add 🖬 Save		Profile Number Limit : 16	
Applications VPN and Remote Acces: Certificate Management SSL VPN	Mail To :	Mail To	No items to show.		
Central VPN Manageme Bandwidth Managemen USB Application System Maintenance TR-069	SMTP Port : SMTP Server : Authentication : User Name :	25 • Enable Disable			
Administrator Password Configuration Backup Syslog / Mail Alert Time and Date	User Password :				
Access Control SNMP Setup Reboot System					
Firmware Upgrade Diagnostics					
External Devices Product Registration				😂 Send A Test Mail 🔡 Apply 🛛 😵	Cancel

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.
	<b>Save</b> – 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.
Authentication	Click <b>Enable</b> to make any user logging into the mail server. If you click <b>Enable</b> , 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.



#### 4.14.5 Time and Date

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

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

<b>Dray</b> Tek	Vigor 3900 Series	15:34:50	Login: Admin	Ð
	System Maintenance >> Time and Date			6
Into Logout : Off  Interval In	Time and Date         Time Type :       NTP         Server :       pool.ntp.org         Port :       123         Interval :       600         Time Zone :       Taipei         Daylight Saving :       © Enable       Disable			
Firmware Upgrade Diagnostics External Devices			<b>D</b>	
			🗎 Apply 🧯	3 Cancel

Item	Description	
Time Type	<b>NTP</b> – Select to inquire time information from Time Server on the Internet using assigned protocol.	
	<b>Browser</b> - 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 <b>Enable</b> to enable the daylight saving. Such feature is available for certain area.	
Apply	Click this button to save the configuration and exit the web page.	
Cancel	Click it to discard the settings configured in this page.	



## 4.14.6 Access Control

This page allows you to open or close the Web User Interface of Vigor 3900 by using Telnet, SSH, HTTP, HTTPS... and etc...

<b>Dray</b> Tek	Vigor 3900 Serie	25	15:36:30	Login: Admin	•
	System Maintenance >> Access	Control			
uto Logout : Off 🛛 💌	Access Control				
LAN					
NAT	Web Allow :	🔿 Enable 💿 Disable			
Firewall	Web Port :	80			
Objects Setting	Telnet Allow :	C Enable () Disable			
User Management	Telnet Port :	23			
Applications	SSH Allow :	C Enable   Disable			
VPN and Remote Acces:	SSH Port :	22			
Certificate Management	HTTPS Allow :	C Enable ( Disable			
SSL VPN		443			
Central VPN Manageme Bandwidth Management	HTTPS Port :				
USB Application	Server Certificate :	Default 🗸			
System Maintenance	User Define :	🔘 Enable 💿 Disable			
TD 0C0	Allowed IP1 :		0.0.0/0 🗸		
Administrator Password	Allowed IP2 :		0.0.0/0		
Configuration Backup	Allowed IP3 :				
Syslog / Mail Alert			0.0.070		
Time and Date	Allow Ping from the WAN :				
Access Control	Block LAN Profile :	~ ×			
SNMP Setup	Allow Ping from the LAN :	💿 Enable 🔘 Disable			
Reboot System					
Firmware Upgrade					
Diagnostics					
External Devices				💾 Apply 🛛 😡 Cano	сe
Product Registration					

Item	Description
Web Allow	Click <b>Enable</b> 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 <b>Enable</b> 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 <b>Enable</b> 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 <b>Enable</b> 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.

User Define	Click <b>Enable</b> 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.
	<b>Allowed IP1 - Allowed IP3 -</b> Type the first IP address for the system administrator to login.
	The former box indicates an IP address allowed to login to the router, and the later box indicates a subnet mask allowed to login to the router.
Allow Ping from WAN	Click <b>Enable</b> 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.
Allow Ping form LAN	Click <b>Enable</b> to allow system administrator to ping the router from LAN interface.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

## 4.14.7 SNMP Setup

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

	Vigor 3900 Series	15:39:21	Login: Admin 🕞
	System Maintenance >> SNMP Agent		
Auto Logout : Off   LAN  LAN  NAT  Firewall  Objects Setting  User Management  Applications  VPN and Remote Access  Certificate Management  SSL VPN  Central VPN Management  USB Application  System Maintenance  TR-069  Administrator Password  Configuration Backup  Syslog / Mail Alert  Time and Date  Access Control  SNMP Setup  Reboot System  Firmware Upgrade	System Maintenance >> SNMP Agent SNMP Agent Enable Get Community: public Set Community: private Default Host IP/Mask :  Enable Disable		
Diagnostics			
External Devices Product Registration			💾 Apply 🛛 😵 Cancel

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 <b>public.</b>
Set Community	Set community by typing a proper name. The default setting

	is <b>private.</b>	
Default Host IP/Mask	Click <b>Enable</b> to use the default IP and mask of the host as the SNMP agent.	
	If you click <b>Disable</b> , you need to type the IP address and choose the mask manually in related fields.	
Manager Host IP/Mask	Type the IP address for the <b>manager host.</b>	
Apply	Click this button to save the configuration and exit the web page.	
Cancel	Click it to discard the settings configured in this page.	

#### 4.14.8 Reboot System

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

If you want to reboot the router using the current configuration, choose **Reboot with Current Configurations** and click **Reboot**. To reset the router settings to default values, click **Reboot with Factory Default Configurations** and click **Reboot**. The router will take a period of time to reboot the system.

Open System Maintenance>> Reboot System.

<b>Dray</b> Tek	Vigor 3900 Series	15:47:46	Login: Admin	Ð
	System Maintenance >> Reboot System >> Reboot System			2
Auto Logout : Off v LAN v NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Central VPN Management USB Application System Maintenance TR-069 E Administrator Password Configuration Backup Syslog / Mail Alert Time and Date Access Control SNMP Setup	System Maintenance >> Reboot System >> Reboot System Reboot System Schedule Reboot Reboot Option Reboot with Current Configuration Reboot Option Reboot with Factory Default Configuration Reboot with Customized Configuration Select Config File Reboot With Customized Configuration Select Config File Reboot With Customized Configuration Reboot With Customized Configuration Reboot With Customized Configuration Select Config File Reboot With Reboot With Customized Configuration Reboot With Customized Configuration	figurations		
Reboot System Firmware Upgrade				
Diagnostics				
External Devices			Č	Reboot
Product Registration -				

Item	Description
Reboot with Current Configurations	Click it to reboot the router using the current configuration. Then, click <b>Reboot</b>
Reboot with Factory Default Configurations	Click it to reset the router settings to default values. Then, click <b>Reboot</b> .
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, <b>Select Config File</b> 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 <b>Reboot</b> .
Reboot	Click this button to execute the rebooting job.

#### 4.14.9 Firmware Upgrade

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

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

Click System Maintenance>> Firmware Upgrade.

<b>Dray</b> Tek	Vigor 3900 Series	15:49:11	Login: Admin	Ð
	System Maintenance >> Upgrade Firmware			0
Auto Logout : Off 🛛 👻	Upgrade Firmware			
LAN 🕑				
NAT	Current Firmware Version : 1.0.7_RC12			
Firewall	Select File: 選擇檔案]未選擇檔案			
Objects Setting				
User Management				
Applications				
VPN and Remote Acces:				
Certificate Management				
SSL VPN				
Central VPN Manageme				
Bandwidth Management				
USB Application				
System Maintenance				
TR-069 =				
Administrator Password				
Configuration Backup				
Syslog / Mail Alert				
Time and Date				
Access Control				
SNMP Setup				
Reboot System				
Firmware Upgrade				
Diagnostics				
External Devices			2	Upgrade
Product Registration -				

Available parameters are listed as follows:

Item	Description
Current Firmware Version	Display current version of the firmware.
Select File	Use the <b>Browse</b> button to locate and select the new firmware.
Upgrade	Click it to perform the firmware upgrade.

## 4.15 Diagnostics

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

Diagno	stics	
Rou	ting Table	
AR	P Cache Tab	le
DHO	P Table	
NAT	Session Ta	ble
Trat	fic Graph	
We	Console	
Pin	g/Trace Rou	te
Dat	a Flow Moni	itor

#### 4.15.1 Routing Table

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

#### 4.15.1.2 Routing Table

Display the information for each route.

<b>Dray</b> Tek	Vigor 39	00 Series		15:5	0:54	Login: Admin	Ð
	Diagnostics >> Ro	uting Table >> Rout	ting Table				
uto Logout : Off 🛛 👻	Routing Table	IPv6 Routing Table	3				
WAN 🗾	🗢 Refresh				L e	gend : U=Up;G=Gatev	/ov/U=Uoe
LAN							
NAT	Search	🦘 Search	🐟 Search	🐟 Search	🦘 Search	\infty Search	60
Firewall	Destination	Gateway	Genmask	Flags	Metric	lface	
Objects Setting	192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1	
User Management	192.168.123.0	0.0.0.0	255.255.255.0	U	0	tun0	
Applications							
VPN and Remote Acces							
Certificate Management							
SSL VPN							
Central VPN Manageme							
Bandwidth Managemen							
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							

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



	Routing Tab	le IPv6 Routing	Table		
	📢 Refr	esh			
	Search	<b>1</b>	\infty Search	1	
	Destination	Gateway	Genmask	_	
	192.168.1.0	0.0.0.0	255.255.25	5.0	
	192.168.123.0	0.0.0.0	255.255.25	5.0	
Destination	Display the des	tination IP add	lress for various ro	outings.	
Gateway	Display the default gateway.				
Genmask	Display the subnet mask for various routings.				
Flags	Display the flag	g of the routing	g entry. Possible fl	ags inc	
	U (route is up)				
	H (target is a h	ost)			
	G (use gateway	·)			
	R (reinstate rou	te for dynamic	c routing)		
	D (dynamically	v installed by d	aemon or redirect)	)	
	M (modified fr	om routing dae	emon or redirect)		
	A (installed by	addrconf)			
	C (cache entry)				
	! (reject route)				
Metric	Display the dis It may be needed		get (usually count laemons.	ed in ho	
Iface		ofile (starting f	route represented v rom LAN/WAN p		

## 4.15.1.2 IPv6 Routing Table

Display the information for each route with IPv6 protocol.

<b>Dray</b> Tek	Vigor 390	O Series		15:52:00	Login: Admin	Ð
	Diagnostics >> Rout	ing Table >> IPv6 Routir	ng Table			
Auto Logout : Off 🛛 🗸	Routing Table	Pv6 Routing Table				
WAN 💽	S Refresh	-				
LAN						
NAT	Search	🦘 Search	🦘 Search	🖘 Search	\infty Search	5
Firewall	Destination	Next Hop	Flags	Metric	lface	
Objects Setting	fe80::/64		U	256	eth0	
User Management	fe80::/64		U	256	eth2	
Applications	fe80::/64		U	256	lan-lan1	
VPN and Remote Access	fe80::/64		U	256	lan-lantest	
Certificate Management	::1/128		U	0	lo	
SSL VPN	fe80::/128		U	0	lo	
Central VPN Manageme	fe80::/128		U	0	lo	
Bandwidth Management	fe80::/128		U	0	lo	
USB Application	fe80::/128		U	0	lo	
System Maintenance 🗧	fe80::250:7fff:fe7f:	:fce8/12 ::	U	0	lo	
Diagnostics	fe80::250:7fff:fe7f:	:fce8/12 ::	U	0	lo	
Routing Table	fe80::250:7fff:fe7f:	fce8/12 ::	U	0	lo	
ARP Cache Table	fe80::250:7fff:fe7f:	fce9/12 ::	U	0	lo	
DHCP Table	ff00::/8		U	256	eth0	
NAT Session Table	ff00::/8		U	256	eth2	
Traffic Graph	ff00::/8		U	256	lan-lan1	
Web Console	ff00::/8		U	256	lan-lantest	
Ping/Trace Route						
Data Flow Monitor						
External Devices						
Product Registration						

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							
	C Refresh							
	Search 🗞 Search 🗞 Sear							
	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 <i>addrconf</i> )							



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

#### 4.15.2 ARP Cache Table

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

#### 4.15.2.1 ARP Cache Table

<b>Dray</b> Tek	Vigor 3	900 Serie	5		15:53:19	Log	gin: Admin	Ξ
	Diagnostics >> /	ARP Cache Table	>> ARP Cache Tab	le				
nto Logout : Off 🛛 🗸	ARP Cache T	able IPv6 Neigh	bor Table					
WAN 💽	🗢 Refres	:h 🔞 Clear All			Log	and : C=Complete	;M=Permanent;P=F	ublicho
LAN								
NAT	Search	\infty Search	🖘 Search	🖘 Search	🐟 Search	🖘 Search	🐟 Search	5
Firewall	IP Address	HW Type	MAC Address	Flags	Profile	User	Clear	
Objects Setting	192.168.1.10	ether	e0:cb:4e:da:48	8:79 C	lan-lan1	NA	ли	
User Management								
Applications								
VPN and Remote Access								
Certificate Management								
SSL VPN								
Central VPN Manageme								
Bandwidth Management								
USB Application								
System Maintenance 🗧								
Diagnostics								
Routing Table								
ARP Cache Table								
DHCP Table								
NAT Session Table								
Traffic Graph								
Traffic Graph Web Console								
· · · · · · · · · · · · · · · · · · ·								
Web Console								
Web Console Ping/Trace Route								

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 \infty Search \infty 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.					

# 4.15.2.2 IPv6 Neighbor Table

<b>Dray</b> Tek	Vigor 3900	Series	15:54:14	Login: Admin	Ð
	Diagnostics >> ARP Ca	che Table >> IP∨6 Neighbor T	able		(
Auto Logout : Off 🛛 👻	ARP Cache Table	P√6 Neighbor Table			
WAN					
LAN	S Refresh				
NAT	Search	\infty Search	🦘 Search	🖘 Search	<b>S</b>
Firewall	IP Address	Profile	MAC Address	Status	
Objects Setting			No items to show.		
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Central VPN Manageme					
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 -					

Item	Description

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 show							
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	<ul> <li>Display the status for such neighbor.</li> <li>INCOMPLETE - Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.</li> <li>REACHABLE - The neighbor is reachable recently (within tens of seconds ago).</li> <li>STALE-The neighbor is no longer to be reachable. Yet, until traffic is sent to the neighbor, no attempt should be made to</li> </ul>							
	verify its reachability. <b>DELAY</b> - 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.							
	<b>PROBE</b> - The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.							

#### 4.15.3 DHCP Table

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

#### 4.15.3.1 DHCP Table

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

<b>Dray</b> Tek			900 Sei	-								Đ
	Diagnostics	>> DHCF	P Table >> DHCP	Tab	е							_
Logout : Off v	DHCP T	able (	DHCPv6 Table									
User Management	\$	Refresh										
Applications	Search	2	Search	1	Search	1	Search	-	Search	1	Search	88
VPN and Remote Access	IP Addres	s	Start Date		Start Time	-	End Date	-	End Time		Mac Address	
Certificate Management	192,168,1	.17	2011/01/05		11:24:15		2011/01/06		11:24:15		30:39:26:a2	:8c:4a
SSL VPN	192,168,1		2011/01/05		11:11:17		2011/01/06		11:11:17		e8:99:c4:6e	
Central VPN Management	192,168,1	.13	2011/01/05		11:34:03		2011/01/06		11:34:03		34:f6:2d:0c	0b:c9
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												

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 🗞 Search							
	IP Address Start Date Start Time End							
	No items to si							
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.

## 4.15.3.2 DHCPv6 Table

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

<b>Dray</b> Tek		Vigor 39	0	0 Series	;	13:43:03		Log	in: A	dmin	Đ
		Diagnostics >> DHCP	Tabl	e >> DHCPv6 Ta	ble						3
Auto Logout : Off		DHCP Table D	HCP	/6 Table							
User Management	•	🗘 Refresh									
Applications		Search	685	Search	60	Search	68	Search	68	Search	1 1 1 1
VPN and Remote Access		Interface		IPv6 Address	0.0	Start Time	~	End Time		DUID	0.4
Certificate Management		internace		IFV0 Address		Start Time		Ling time		000	
SSL VPN						No items to	show.				
Central VPN Management											
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	-										

Each item will be explained as follows:

Item	Desc	Description						
Refresh	Rene	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.							
	Diag	nostics >> DH	ICP 1	Table >> DHCP	Tabl	е		
	DHCP Table DHCPv6 Table							
	1	92	1	Search	1	Search	1	Searc
	1	P Address	Start Date		Start Time End			
	No iter							ns to st
Interface	Displ	lay the inte	erfa	ce used by	the	DHCP set	rver.	
IPv6 Address	Display the IPv6 address of the static DHCP server.							
Start Time	Displ	lay the star	tin	g time that	DH	CP server	is ac	tivated.
End Time	Displ	lay the end	l tir	ne that DH	CP	server is c	losec	1.

Item	Description
DUID	Display the detailed information for DUID.

## 4.15.4 NAT Session Table

This table can display about 30000 sessions with 20 pages.

<b>Dray</b> Tek	Vigor 390	Series		16:0	1:21 10	gin: Admin	Đ
	Diagnostics >> NAT S	ession Table					
nto Logout : Off 🛛 💌	NAT Session Table	e					
WAN		-					
LAN	🗢 Refresh						
NAT	Search	🕸 Search	🖘 Search	🖘 Search	🦘 Search	🦘 Search	5
Firewall	Source	Destination	WAN	Protocol	State	TTL	
Objects Setting	172.16.3.130:514	255.255.255.25	5:51+255.255.255.25	5 udp		0:00:29	-
User Management	192.168.1.3	192.168.1.98	192.168.1.98	icmp	8/0	(12602) 0:00:00	
Applications	192.168.1.10:6163	192.168.1.3:80	192.168.1.3	top	TIME_WAIT	0:01:28	
VPN and Remote Access	192.168.1.10:6154	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:02	
Certificate Management	192.168.1.10:6143	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:00:19	
SSL VPN	192.168.1.10:6176	192.168.1.3:80	192.168.1.3	tcp	ESTABLISHED	0:04:59	
Central VPN Manageme	192.168.1.10:6144	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:00:29	
Bandwidth Management	192.168.1.10:6171	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:58	Ξ
USB Application	192.168.1.10:6156	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:09	
System Maintenance 🗧	192.168.1.10:6175	192.168.1.3:80	192.168.1.3	tcp	ESTABLISHED	0:04:59	
Diagnostics	192.168.1.10:6165	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:41	
Routing Table	192.168.1.10:6162	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:28	
ARP Cache Table	192.168.1.10:6161	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:29	
DHCP Table	192.168.1.10:6157	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:19	
NAT Session Table	192.168.1.10:6151	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:02	
Traffic Graph	192.168.1.10:6159	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:27	
Web Console	192.168.1.10:6152	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:01	
Ping/Trace Route	192.168.1.10:6160	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:01:27	
Data Flow Monitor	192.168.1.10:6174	192.168.1.3:80	192.168.1.3	tcp	ESTABLISHED	0:04:59	
External Devices	192.168.1.10:6145	192.168.1.3:80	192.168.1.3	tcp	TIME_WAIT	0:00:40	4

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 \infty 168 🗞 Search 🗞 Sea							
	Source Destination WAN Pro							
	192.168.1.10:4655 192.168.1.3:80 192.168.1.3 tcp							
	192 168 1 10:4658 192 168 1 3:80 192 168 1 3 ten							
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.							



Item	Description
State	Display the actual state of the TCP connection.
TTL	Display how long the conntrack entry has to live.

## 4.15.5 Traffic Graph

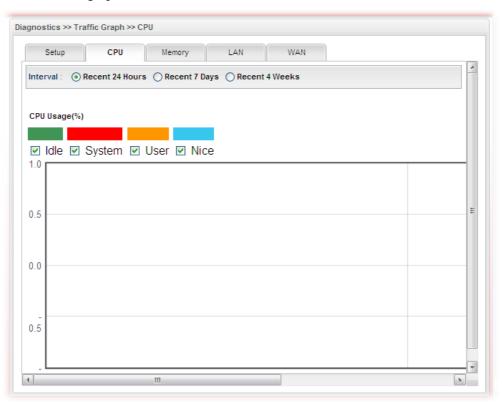
Click **Diagnostics** and click **Traffic Graph** to pen the web page. Specify LAN and WAN profiles to display corresponding graphs for CPU, Memory, LAN and WAN configurations. Click **Refresh** to renew the graph at any time.

<b>Dray</b> Tek	Vigor 3900 Series	16:02:22	Login: Admin	E
	Diagnostics >> Traffic Graph >> Setup			(2)
Auto Logout :       Off         WAN       ✓         LAN       ✓         NAT       Firewall         Objects Setting       User Management         Applications       VPN and Remote Access         Certificate Management       SSL VPN         Central VPN Management       USB Application         System Maintenance       Diagnostics         Routing Table       ARP Cache Table         DHCP Table       NAT Session Table         Traffic Graph       Web Console         Ping/Trace Route       Ping/Trace Route	Diagnostics >> Traffic Graph >> Setup       Setup     CPU     Memory     LAN     WAN       Enable     LAN :     Image: Setup     Image: Setup     Image: Setup       WAN :     Image: Setup     Image: Setup     Image: Setup     Image: Setup			
External Devices Product Registration				H Apply

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.					
	<b>Enable</b> – Check this box to enable such profile.					
	LAN – Use the drop down menu to choose a LAN profil					
	<b>WAN</b> –Use the drop down menu to choose a WAN profi					
	<b>Apply</b> - 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.					
	<b>Recent 24 Hours</b> – Display the information of CPU operation about recent 24 hours.					
	<b>Recent 7 Days</b> – Display the information of CPU operation about recent 7 days.					
	<b>Recent 4 Weeks</b> – Display the information of CPU operation about recent 4 weeks.					

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

Below show a graphic for CPU:



#### 4.15.6 Web Console

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



## 4.15.7 Ping/Trace Route

i.

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.

<b>Dray</b> Tek	Vigor 3900 Series	16:03:26	Login: Admin	Ð
	Diagnostics >> Ping/Trace Route			
uto Logout : Off 🛛 👻	Ping/Trace Route			
WAN				
LAN				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Acces:				
Certificate Management				
SSL VPN				
Central VPN Manageme				
Bandwidth Managemen				
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	● Ping     ○ ID-4 Uset:		0.011	
External Devices	⊙ IPv4 Host: ○ TraceRoute	Interface : lan1	1 💽 Start	🗿 Sto
Product Registration				

Item	Description
Ping / TraceRoute	Click <b>Ping</b> to perform ping function. Click <b>TraceRoute</b> to invoke trace router function.
IPv4	<ul><li>Host - Type the IP address of the host.</li><li>Interface - Choose one of the LAN or WAN profile to be applied by such function.</li></ul>
Start	Click it to start the action of Ping or TraceRoute.
Stop	Click it to terminate the action of Ping or TraceRoute.

## 4.15.8 Data Flow Monitor

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

<b>Dray</b> Tek	Vigor 39						
	Diagnostics >> Dat	ta Flow Monitor					
luto Logout : Off 🛛 👻	Data Flow Moni	itor					
WAN 💽							
LAN	🗑 Enable Data	aflow Monitor 🛛 🐼 F	Refresh 🛛 💘 Charl	t 🔠 Block 📰 🕻	JnBlock 💿 Rec	ent 1 Hour 🔿 Recent 2	24 Hours
NAT	IP Address	TX rate(Kbp	s) RX rat	e(Kbps) S	essions	Block Time	
Firewall			N	o items to show.			
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
SSL VPN							
SSL VPN Central VPN Manageme							
SSL VPN Central VPN Manageme Bandwidth Managemen	Profile	IP	RX Rate	TX Rate	RX byte	TX byte	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application	Profile wan2	IP 172.16.3.130	0	TX Rate 0	RX byte 0	0	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application System Maintenance					2	-	
SSL VPN Central VPN Managemen Bandwidth Managemen USB Application System Maintenance Diagnostics	wan2		0	0	0	0	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table	wan2		0	0	0	0	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table ARP Cache Table	wan2		0	0	0	0	
SSL VPN Central VPN Managemen Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table ARP Cache Table DHCP Table	wan2		0	0	0	0	
SSL VPN Central VPN Managemen Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table ARP Cache Table DHCP Table NAT Session Table	wan2		0	0	0	0	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table ARP Cache Table DHCP Table NAT Session Table Traffic Graph	wan2		0	0	0	0	
SSL VPN Central VPN Manageme Bandwidth Managemen USB Application System Maintenance Diagnostics Routing Table ARP Cache Table DHCP Table NAT Session Table Traffic Graph Web Console	wan2		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
Block	Prevent the specified PC accessing into Internet within 5 minutes.
UnBlock	Allow the specified PC accessing into Internet within 5 minutes.
Recent 1 Hour/ Recent 24 Hours / Recent 7 Days	Display the records with 1 hour/24 hours/7 days recently.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh

	button is clicked.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Block Time	Display the time for the duration of the block.
Profile	Display the WAN interface.
IP	Display the IP address of the WAN interface.
RX Rate	Display the rate of data received.
TX Rate	Display the rate of data transmitted.
RX byte	Display the file size of data received.
TX byte	Display the file size of data transmitted.

## **4.16 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.

<b>Dray</b> Tek	Vigor 39	00 Series		16:17:03	Login: Admin	E
	External Devices >					
Logout : Off 🛛 👻	External Device	s				
wan 🔄		Deriver of the state				
LAN	Enable Exte	ernal Devices 🔄 Refresh				
AT 🗖	Status	Model Name	IP Address	Connection Time	Clear	
rewall			No items to :	show.		
bjects Setting						
er Management						
plications						
N and Remote Acces						
rtificate Management						
L VPN						
ntral VPN Manageme						
ndwidth Management						
B Application						
tem Maintenance 🛛 🗉						
nostics						
uting Table						
Cache Table						
P Table						
Session Table						
ffic Graph						
eb Console						
Ping/Trace Route						
Data Flow Monitor						
ternal Devices						
roduct Registration 🚽						

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.

## **4.17 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.

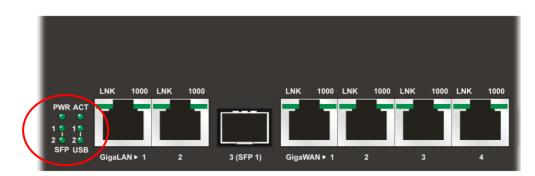
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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.

ieneral	Authentication	Advanced	
Connec	st using:		
<b>##</b> /	SUSTeK/Broad	lcom 440x 10/100 Ir	Configure
This cg	nnection uses th	ne following items:	
	Client for Micro File and Printer QoS Packet Si Internet Protoc	r Sharing for Microsoft cheduler sol (TCP/IP)	Networks
	nstall	Umnetall	Properties
Tran wide	area network pr	Protocol/Internet Prot otocol that provides co onnected networks.	
dero			

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

Internet	Protocol (TCP/IP) Properties
General	Alternate Configuration
this cap	an get IP settings assigned automatically if your network supports pability. Otherwise, you need to ask your network administrator for propriate IP settings.
<u>o o</u> t	btain an IP address automatically
OU	se the following IP address:
(P ad	dress
Subr	nel mask
<u>D</u> ela	aul/ gateway:
00	tain DNS server address automatically
OU:	se the following DNS server addresses:
Erek	ened DNS server
Alten	mate DNS server
	Advanced
	DK Cancel

#### For Mac OS

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

				Netw	ork				(
Show All	Displays Se	ound Net	work S	Startup Dis	k				
		Location Show	_	omatic It-in Ethe	rnet		:		
	ТС		PPoE	AppleT		roxies	Ethern	et J	
Co	nfigure IPv4	: Using	DHCF	>			•		
	IP Address	5: 192.1	.68.1.1	.0			Ren	ew DHC	P Lease
S	ubnet Mask Router		55.25 68.1.1		DHCP	Client II		equired)	
	DNS Servers	s:							(Optional)
Sear	ch Domains	s: [							(Optional)
IF	v6 Address	s: fe80:0	000:00	000:000	:020a:9	5ff:fe8d	:72e4		
		Con	figure l	Pv6)					?
Click	k the lock to	prevent f	urther	changes.		Assis	t me		pply Now

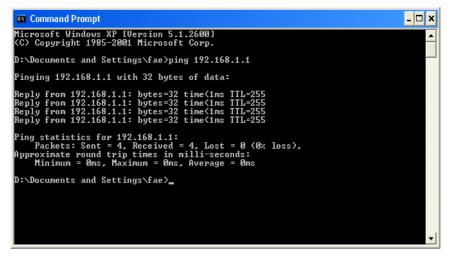
## **5.3 Pinging the Router from Your Computer**

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

Please follow the steps below to ping the router correctly.

#### **For Windows**

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



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

#### For Mac OS (Terminal)

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

Terminal - bash - 80x24	
02:24:18 on ttyp1 192.168.1.1 58.1.1): 56 data bytes .1: icmp_seq=0 tt1=255 time=0.755 ms .1: icmp_seq=1 tt1=255 time=0.697 ms .1: icmp_seq=2 tt1=255 time=0.716 ms .1: icmp_seq=3 tt1=255 time=0.731 ms .1: icmp_seq=4 tt1=255 time=0.72 ms	2
58.1.1): 56 data bytes .1: icmp_seq=0 ttl=255 time=0.755 ms .1: icmp_seq=1 ttl=255 time=0.697 ms .1: icmp_seq=2 ttl=255 time=0.716 ms .1: icmp_seq=3 ttl=255 time=0.731 ms .1: icmp_seq=4 ttl=255 time=0.72 ms	
	22:24:18 on ttyp1 192.168.1.1 58.1.1): 56 data bytes 1: icmp_seq=0 ttl=255 time=0.755 ms 1: icmp_seq=1 ttl=255 time=0.697 ms 1: icmp_seq=2 ttl=255 time=0.716 ms 1: icmp_seq=3 ttl=255 time=0.731 ms 1: icmp_seq=4 ttl=255 time=0.72 ms

# 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.

<b>Dray</b> Tek	Vigo	or 3	900 Se	ries				16:18:38		Lo	gin: Adm	ш	E
	🗳 Refre	sh											
uto Logout : Off  Quick Start Wizard Online Status WAN LAN NAT Firewall	Device Model : Hardwa Firmwar Build Da Revision	re : re : ate :	nation Vigor3900 1.0 1.0.7_RC12 2013-08-27 2733		)	*****	CP Me Co Sys		36% Memory U CPU Usag 5 days 4:3	je:0% :0:19	Mei	ory Cache mory Usa	12
Objects Setting	IPv4		IPv6										
User Management	Profile	Conne	ect Descript	Uptime	Mac	Protocol IP		Gateway DNS	RX Rate	TX Rate	RX byte	TX byte	Operatio
Applications	lan1	up		5 days 4:	00:50:7f:	Static(N#19	2.16	8.	20997	5674	42.50 (M	27.00 (M	
/PN and Remote Acces:	lantest	up	Just for t	5 days 4:	00:50:7f:	Static(N# 0.0	0.0.0		0	0	0	0	
Certificate Management	wan2	down		0 days 0:	00:50:7f	Static(N#17	2.16	.3 172.16.3 8.8.8.8	0	0	0	0	
SL VPN													
entral VPN Manageme													
andwidth Managemen													
JSB Application													
System Maintenance													
Diagnostics													
Routing Table													
ARP Cache Table													
DHCP Table													
NAT Session Table													
Traffic Graph													
Web Console													
Ping/Trace Route													
Data Flow Monitor 📃 🚽													

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

<b>Dray</b> Tek	VI.	gors	900 Serie	-5			16:19:20		Login: Admin	Ð
	WAN >	>> Genera	al Setup >> Gene	ral Setup						
Auto Logout : Off 🛛 🖌	Ge	neral Set	USB WAN							
Quick Start Wizard	II (		•			_				
Online Status		🕼 Add	🔀 Edit  🕅 🛙	)elete 🛛 🗳 Re	fresh Mod	e : Advance		·	Profile I	Number Limit : 50
WAN		Profile	(max Enable	Description	VLAN Tag	VLAN ID	Priority	Port	IPv4 Protoc	IPv6 Protocol
General Setup	1	wan1	false		Disable	10	0	WAN1	None	Link-Local
Default Route	2	wan2	true		Disable	11	0	WAN2	Static	Link-Local
Load Balance	3	wan3	false		Disable	12	0	WAN3	None	Link-Local
Switch	4	wan4	false		Disable	13	0	WAN4	None	Link-Local
LAN	5	wan5	false		Disable	14	0	WAN5	None	Link-Local
NAT										
Firewall										
Objects Setting										
User Management										
Applications										
VPN and Remote Access										
Certificate Management										
SSL VPN										
Central VPN Management										
Bandwidth Management										
USB Application										
System Maintenance										
Diagnostics										
External Devices										
Product Registration										

## 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

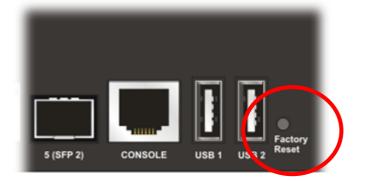
You can reset router to factory default via Web page.

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.

stem Maintenance	>> Reboot System >> Reboot System	
Reboot System	Schedule Reboot	
	Reboot with Current Configurations	
Reboot Option	Reboot with Factory Default Configurations	
	Reboot with Customized Configurations	
	🟅 Reboo	

#### **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 **<u>support@draytek.com</u>**.

