

Vigor3900

Oray Tek

Multi-WAN Security Appliance

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: 1.5 Firmware Version: V1.0.5 (For future update, contact DrayTek) Date: 30/08/2012

Copyright Information

Copyright Declarations	Copyright 2012 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety	• 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.
	 Do not place the router in a damp or humid place, e.g. a bathroom. The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
	 Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
	 Keep the package out of reach of children. When you want to dispose of the router, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via http://www.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.
	http://www.draytek.com



European Community Declarations

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

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

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

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



Table of Contents

1.1 Web Configuration Buttons Explanation 1 1.2 LED Indicators and Connectors 1 1.3 Hardware Installation 4 1.3.1 Network Connection 4 1.3.2 Rack-Mounted Installation 5 Chapter 2: Initialing Settings 7 2.1 Changing Password 7 2.1 Changing Password 7 2.1 Chapter 2: Initialing Settings 7 2.1 Chapter 3: Application get the WAN Profile 9 2.2.1 Sitep 1 - Specifying the WAN Profile 9 9 2.2.2 Sitep 2 - Configuring the Selected Protocol 11 2.1 Register Vigor Router 18 Chapter 3: Application and Tutorial 21 31 A How to Configure Load Balance with Multi-WAN on Vigor3900 and Other Router (Main Mode) 33 34 How to Configure Load Balance between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How t	Chapter 1: Preface	1
1.2 LED Indicators and Connectors 1 1.3 Hardware Installation 4 1.3.1 Network Connection 4 1.3.2 Rack-Mounted Installation 5 Chapter 2: Initialing Settings 7 2.1 Changing Password 7 2.2 Quick Start Wizard 9 2.2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial 2.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor39007 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor39007 21 3.2 How to Configure USPF? 27 3.3 How to Configure VPN Load Balance between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to setup 50 WANs on Vigor3900. 50 Chapter 4: Advanced Web Configuration 4.1 General Setup 55 4.1 General Setup 56 4.1 General Setup 66	1.1 Web Configuration Buttons Explanation	1
1.3 Hardware Installation 4 1.3.1 Network Connection 4 1.3.2 Rack-Mounted Installation 5 Chapter 2: Initialing Settings 7 2.1 Changing Password 7 2.2 Quick Start Wizard 9 2.2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial 2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial 2.1 Step 1 - Specifying the WAN Profile 9 3.1 How to Configure Load Balance with Multi-WAN on Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 4.1 General Setup 4.1 J General Setup 56 4.1.1 General Setup <t< th=""><th></th><th></th></t<>		
1.3.2 Rack-Mounted Installation 5 Chapter 2: Initialing Settings 7 2.1 Changing Password 7 2.2 Quick Start Wizard 9 2.2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial. 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.11 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2.1 General Setup 56 4.2.1 General Setup 63 4.2.1 General Setup 63		
2.1 Changing Password 7 2.2 Quick Start Wizard 9 2.2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial. 2.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor3900 and Other Router (Main Mode) 33 3.4 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 WAN Setup 55 4.1 Qeneral Setup 55 4.1 General Setup 83 4.2 LAN 83 4.2 LAN 83 4.2 LAN 83 4.2 LAN 99 4.2 Satic Route 99 4.2 Suit Route 99 4.2 Suit Route <t< th=""><th></th><th></th></t<>		
2.2 Quick Start Wizard	Chapter 2: Initialing Settings	7
2.2.1 Step 1 - Specifying the WAN Profile 9 2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial. 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.1 General Setup 83 4.2.1 General Setup 83 4.2.1 General Setup 11 4.2.2 AN 83 4.2.3 Static Route 9	2.1 Changing Password	7
2.2.2 Step 2 - Configuring the Selected Protocol 11 2.3 Register Vigor Router 18 Chapter 3: Application and Tutorial. 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 </th <th>2.2 Quick Start Wizard</th> <th>9</th>	2.2 Quick Start Wizard	9
Chapter 3: Application and Tutorial. 21 3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure OSPF? 27 3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 PR outing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122		
3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor300B or Vigor3900? 21 3.2 How to Configure OSPF? 27 3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 General Setup 4.1 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 122	2.3 Register Vigor Router	18
3.2 How to Configure OSPF? 27 3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 General Setup. 4.1 2 Default Route. 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup. 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3 Address Mapping 125	Chapter 3: Application and Tutorial	21
3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and Other Router (Main Mode) 33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router. 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.1 P Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 111 4.3.1 Port Redirection 118 4.3.1 Port Redirection 118 4.3.2 DWZ Host 125	3.1 How to Configure Load Balance with Multi-WAN on Vigor2960, Vigor30	00B or Vigor3900? 21
33 3.4 How to run RDP service in the browser via logging in 3900's HTTPS Server? 36 3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router 41 3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 55 4.1 WAN Setup 55 4.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.1 General Setup 83 4.2.1 P Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 111 4.2.6 RIP Configuration 111 4.2.7 OSPF Configuration 111 4.3.1 Port Redirection 1122 4.3.1 Ad	3.2 How to Configure OSPF?	
3.5 How to Configure VPN Load Balance between Vigor3900 and Other Router	3.3 How to Configure LAN to LAN IPSec Tunnel between Vigor3900 and C	other Router (Main Mode)
3.6 How to Setup 50 WANs on Vigor3900 50 Chapter 4: Advanced Web Configuration 4.1 WAN Setup 55 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 125	3.4 How to run RDP service in the browser via logging in 3900's HTTPS Se	erver?
Chapter 4: Advanced Web Configuration 55 4.1 WAN Setup 55 4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 118 4.3.1 Port Redirection 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125	3.5 How to Configure VPN Load Balance between Vigor3900 and Other Ro	outer 41
4.1 WAN Setup	3.6 How to Setup 50 WANs on Vigor3900	50
4.1.1 General Setup 56 4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125	Chapter 4: Advanced Web Configuration	
4.1.2 Default Route 70 4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125	4.1 WAN Setup	
4.1.3 Load Balance Policy 71 4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125	4.1.1 General Setup	56
4.1.4 Switch 78 4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125		
4.2 LAN 83 4.2.1 General Setup 83 4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125		
4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3 Address Mapping 125		-
4.2.2 IP Routing 97 4.2.3 Static Route 99 4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3 Address Mapping 125	4.2.1 General Setup	
4.2.4 Switch 105 4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125	4.2.2 IP Routing	
4.2.5 Bind IP to MAC 111 4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125		
4.2.6 RIP Configuration 114 4.2.7 OSPF Configuration 115 4.3 NAT 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host 122 4.3.3 Address Mapping 125		
4.2.7 OSPF Configuration. 115 4.3 NAT. 118 4.3.1 Port Redirection 118 4.3.2 DMZ Host. 122 4.3.3 Address Mapping. 125		
4.3.1 Port Redirection		
4.3.2 DMZ Host	4.3 NAT	118
4.3.3 Address Mapping125		



4.4 Firewall	129
4.4.1 Filter Setup	129
4.4.2 DoS Defense	
4.4.3 MAC Block	146
4.5 Objects Setting	148
4.5.1 IP Object	
4.5.1 IP Object	
4.5.3 Service Type Object	
4.5.4 Service Type Group	
4.5.5 Keyword Object	
4.5.6 Keyword Group	
4.5.7 File Extension Object	
4.5.8 IM Object	
4.5.9 P2P Object	
4.5.10 Protocol Object	
4.5.11 Web Category Object 4.5.12 Time Object	
4.5.12 Time Object	
4.6 User Management	183
4.6.1 General Setup	183
4.6.2 User Profile	
4.6.3 User Group	190
4.6.4 RADIUS	
4.6.5 LDAP/Active Directory	193
4.7 Application	194
4.7.1 Dynamic DNS	
4.7.1 Dynamic DNS	
4.7.3 UPnP	
4.7.4 High Availability	
4.7.5 Wake on LAN	
4.8 VPN and Remote Access	205
4.8.1 VPN Client Wizard 4.8.2 VPN Server Wizard	
4.8.3 Remote Access Control	
4.8.4 PPP General Setup	
4.8.5 IPSec General Setup	
4.8.6 VPN Profiles	
4.8.7 VPN Trunk Management	
4.8.8 Connection Management	
4.9 Certificate Management	237
4.9.1 Local Certificate	
4.9.2 Trusted Certificate	
4.9.3 Remote Certificate	
4.10 SSL VPN	
4.10.1 SSL Web Proxy	
4.10.2 SSL Application	
4.10.3 Online User Status	
4.11 Bandwidth Management	252
4.11.1 Incoming Class	253
4.11.2 Incoming Filter	
4.11.3 Outgoing Class	259
4.11.4 Outgoing Filter	264



4.11.5 Sessions Limit 4.11.6 Bandwidth Limit	
4.12 System Maintenance	272
 4.12.1 TR-069 4.12.2 Administrator Password. 4.12.3 Configuration Backup 4.12.4 Syslog / Mail Alert. 4.12.5 Time and Date 4.12.6 Access Control. 4.12.7 SNMP Setup 4.12.8 Reboot System 	273 274 276 279 280 281
4.12.9 Firmware Upgrade	
 4.13 Diagnostics	
 4.13.1 Routing Table	

Chapter 5: Trouble Shooting	297
5.1 Checking If the Hardware Status Is OK or Not	297
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	298
5.3 Pinging the Router from Your Computer	300
5.4 Checking If the ISP Settings are OK or Not	301
5.5 Backing to Factory Default Setting If Necessary	302
5.6 Contacting Your Dealer	

Chapter 1: Preface

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

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

1.1 Web Configuration Buttons Explanation

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

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

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

1.2 LED Indicators and Connectors

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

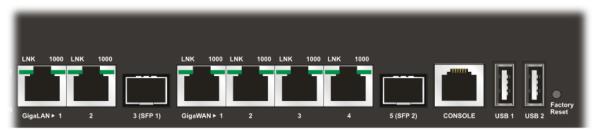


Description for LED

	LNK	1000	LNK	1000		LNK	1000	LNK	1000	LNK	1000	LNK	1000
PWR ACT			-					-					
• • 1• 1•													
													- 1
SFP USB	Gigal A		2		2 (SED 4)	CinaN		:	,		3		
	GigaLA	N 🕨 1			3 (SFP 1)	GigaW/			2		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.				
() I II (I/ <u>2</u> / <u>3</u> / I		Off	No Ethernet link is established.				
	1000	On	It means that a normal 1000Mbps connection is through its corresponding port.				
		Off	It means that a normal 10/100Mbps connection is through its corresponding port.				

Connectors



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

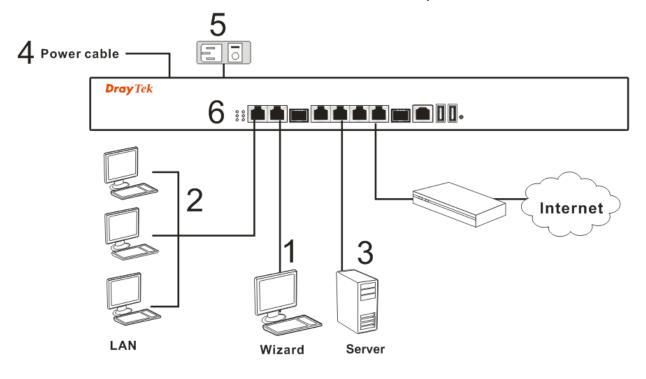
1.3 Hardware Installation

1.3.1 Network Connection

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

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

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

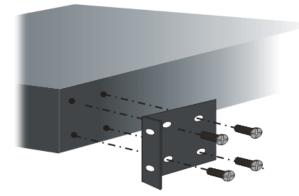


1.3.2 Rack-Mounted Installation

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



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



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



Desktop Type Installation

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



This page is left blank.

Chapter 2: Initialing Settings

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

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

2.1 Changing Password

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

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



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

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

Dray Tel	k 🧖	Vigor3900	
Login			
User : Password :	admin		
	English	✓ Login	

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

	S Refres	h	DrayTek								
to Logout : 5Min 🗸	Device	Informati	on			System	n Informa	tion			
Quick Start Wizard	Model :	Vig	or3900			CPU Usag	je :	21%			
Online Status	Hardware					Memory U	Isage :	24 %			m
WAN	Firmware Build Date		.5RC9			Coproces	-	CPU Usage:	0%	Memory Us	
LAN	Revision :			5:04:09		System U		5 days 5:57			
NAT	iterialen.							-	16:53:28 UTC	2012	
Firewall											
Objects Setting	IPv4	IPv	6								
User Management	Profile	Connectio	Uptime	MAC	Protocol	IP	Gateway	DNS	RX Packet	TX Packet	Operation
Applications	lan1	up	5 days 5:.	00:50:7F:	static(NAT)	192.168.1			517140	1142118	
VPN and Remote Access	lan100	up	0 days 0:.	00:50:7F:	static(NAT)	192.168.1			0	276	
Certificate Management	wan2	up	0 days 0:.	00:50:7F:	pppoe(NAT)	111.243.1	168.95.98	168.95.19	913	710	X
SSL VPN	wan4	up	0 days 0:.	00:50:7F:	static(NAT)	172.16.2	172.16.1.1	8.8.8.8	37190	1582	
Bandwidth Management											
System Maintenance											
Diagnostics											
External Devices											
Product Registration											

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

stem Maintenance >> Ac	Iministrator Password		
Administrator Passwor	rd		
		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 Configurator for this router.

2.2 Quick Start Wizard

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

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

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

2.2.1 Step 1 - Specifying the WAN Profile

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

Quick Start Wizard		
Step 1 St	ep 2	
Profile :	wan1 🗸	
IPv4 Protocol :	Static 🗸	
		_
	🦄 Previous 🔊 Next 📑 Finish 🔇 Cance	el

Available settings are explained as follows:

Item	Description						
Profile	Use the drop down list to choose one WAN profile.						
	wan1	~					
	wan1 wan2 wan3 wan4 wan5						
IPv4 Protocol Type	Use the drop dow WAN profile.	wn list to choose a connection mode for such					
	IPv4 Protocol :	Static 🗸					
		Static					
		DHCP					
		РРРоЕ РРТР					



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

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

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

2.2.2 Step 2 - Configuring the Selected Protocol

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

Quick Start Wiza	rd	
Step 1	Step 2	
IP Address	:	0.0.0
Subnet Mas	k:	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	1
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.			



		is hereiten der dien leis die ID is blanen	C . 1 1 C				
DNS Server IP Address	Add – Click this button to display the IP address field for adding a new IP address. Type the IP address on the tiny boxes one by one.						
		🕼 Add 🛗 Save					
		DNS Server IP Address					
	DNS Server IP Address :	168 . 95 . 1 . 1	Î				
		nished the IP address configuration ing onto the router.	on, click Save				
	DNS Server IP Ad	ldress					
	168.95.1.1		â				
	🔟 – Click the	e icon to remove the selected entry	/.				
Previous	Click it to retur	rn to previous setting page.					
Finish	Click it to finis	sh the configuration.					
Cancel	Click it to disc	ard the settings configured in this	page.				

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

If DHCP is selected

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

Quick Start Wizard	1			
Step 1	Step 2			
Host Name :		(Optional)		
			🐚 Previous 🛋 Next 💾 Finish 🔇 Cance	-1
				21

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	ď					
Step 1	Step 2					
Username :						
Password :						
			Y Previous	Most 1	Eisish	Canaal
			mevious	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 Wiza	ard	L		
Step 1	Step 2			
PPTP Over	:	Static 👻		
Server Add	Iress:	0.0.0.0		
Username	:			
Password	:			
IP Address	1	0.0.0.0		
Subnet Ma	sk:	255.255.255.0		
Gateway IP	Address :			
		🕼 Add 🛗 Save		
		DNS Server IP Address		
DNS Server	IP Address :	No items to show.		
		🕥 Previous 🛋	Next 🔡 Finish	🐼 Cancel
		·		-

Available parameters are listed as follows:

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

	Quick Start Wizard
	Step 1 Step 2
	PPTP Over : DHCP 💌
	Server Address: 0.0.0.0
	Username :
	Password :
Server Address	Type a remote IP address of PPTP server.
Username	Type in the username provided by ISP in this field.
Password	Type in the password provided by ISP in this field.
Previous	Click it to return to previous setting page.
IP Address	Type a public IP address for such WAN profile.
Subnet Mask	Choose the static mask from the drop down list.
Gateway IP Address	Type a public gateway address for such WAN profile.
	- click it to remove the IP address if you are not satisfied
	with it.
DNS Server IP Address	To add a new IP address, simply place the mouse cursor on this filed. The following dialog will appear.
	🕼 Add 🔚 Save
	DNS Server IP Address
	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.

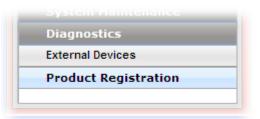
Note	٩	×
•	Wizard Setting Complete	
	ОК	



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 configurator of Vigor3900 and click **Product Registration**.



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

	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 x x hd d
lfy	you cannot read the word, <mark>click here</mark>
	Forgotten password? Login
Don't have a	MyVigor Account ? Create an account now
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**.

Image: Mome My Information D About Us My Information O Product Last Login Time : 2011-08-24 09:39:13 Last Login Time : 2011-08-24 09:39:13 Last Login Time : 2011-08-24 23:01:15 O My Information Current Login Time : 2011-08-24 23:01:15 VigorACS SI Current Login From : 114.37.142.184 PowNo : 5 V PageNo : 1 V Add Your Device List Management Serial Number / Device Name Model Note Product Serial Number / Device Name Model Note 104001703857 VigorPro5300 Customer Survey 200807100001	Dray Tek				N
▶ About Us Welcome,james_fae ▶ Product Last Login Time : 2011-08-24 09:39:13 ■ My Information Current Login Time : 2011-08-24 23:01:15 ♥ VigorACS SI Current Login From : 114.37.142.184 ■ Vigor Series Your Device List ♥ Management Serial Number / Device Name Model Note 104001703857 Vigor2710 Vigor2710	i Home				Sear
Serial Number / Host IDDevice NameModelNoteRegistration104001703857Vigor2710Vigor2710-	Product My Information VigorACS SI Vigor Series	Welcome,james Last Login Time : Last Login From : Current Login Tim Current Login Fro	_ <mark>fae</mark> 2011-08-24 09:3 123.110.144.22 ie : 2011-08-24 2 m : 114.37.142.1	0 3:01:15 84	Add
200911030001 ryan VigorPro5300 -	Product Registration	Host ID 104001703857 200807100001	Vigor2710 VigorPro5300	Vigor2710 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**.

netbilling and a second s	iytek, com/nomerage/main.prip				
Dray Tek	< C			My	/igo
1 Home				Search	G
D About Us	My Product		Search for t	his site	GO
My Information	Registration Device				
G VigorACS SI	Serial number :	20110822143	20301		
🗘 Vigor Series	Nickname : *	vigor3900			
🌣 Management	Registration Date : *	08-24-2011		J	
Product Registration	Usage :	– Select –	*		
Customer Survey	Product Rating :	– Select –	🎽 (Your opinion so	far)	
,	No. of Employees :	– Select –	🎽 (In total within yo	ur company)	
	Supplier :		(When	e you bought it from)	
	Date of Purchase :		(mm-d	d-уууу)	
	Internet Connection : *				
	Cable	ADSL	VDSL	🗌 Fiber	
	🗖 3G	WIMAX	🗌 LTE		
Copyrights © DravTek Corp.				Cancel	omit



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.

٢	Гок	
L		

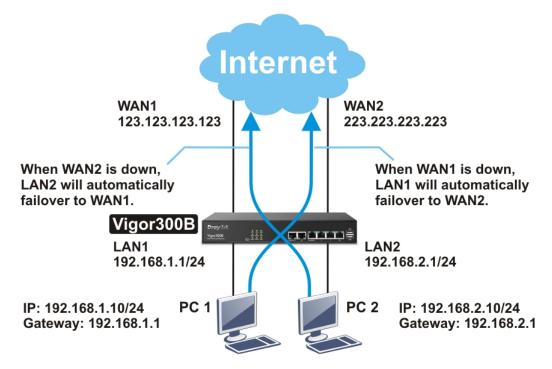
6 Take a look at the page of My Information, the new added Vigor3900 is listed under **Your Device List**.

Dray Tek			/	My Vigo
E Home			Se	arch G(
	My Information			
 About Us Product My Information VigorACS SI Vigor Series 	Welcome,draytekfae Last Login Time : 2011-08-24 Last Login From : 123.110.14 Current Login Time : 2011-08- Current Login From : 114.37.1 Your Device List	4.220 24 23:01:15	RowNo : 5 🔽 Pa	geNo : 2 💌
🌣 Management	Serial Number / Host ID	Device Name	Model	Note
🍐 Customer Survey	20100707144801	Vigor3300V	Vigor3300	-
	<u>20100708105301</u>	Vigor2820	Vigor2820	-
	<u>20101005104801</u>	Vigor2710vn	Vigor2710	-
	2010121707335201	Vigor2920	Vigor2920	
	2011082214320301	vigor3900	Vigor3900	

Chapter 3: Application and Tutorial

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

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



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



		LAN >> General Se	etup >> General Se	tup				
uto Logout : Off 🛛 👻		General Setup	DHCP	DHCP Relay	RADVD	DHCPv6		
Quick Start Wizard	-	🚺 Add	🗶 Edit 🕅 D	elete 🛭 🔇 Re	fraah			Prof
Online Status								
WAN		Profile	Enable This Pro	Description	VLAN ID	IPv4 Protocol	IPv6 Protocol	
LAN		lan1	true		10	static	Link-Local	_
General Setup								
IP Routing								
Static Route								
Switch								
Bind IP to MAC	E							
RIP Configuration								
NAT								
Firewall								
Objects Setting								
User Management								
Applications								
Bandwidth Management								
System Maintenance								
Diagnostics	-	4		111				•

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

2nd Subnet :				
	IP	Subnet Mask	Mode	
	🕼 Add 💾 Save			
Gateway IP Address :		m		(Optional)
Subnet Mask :	255.255.255.0			
IP Address :	192 . 168 . 1 . 1			
Mode :	NAT			
IPv4 Protocol :	static	and a second second second second		
MAC Address :	00 : 50 : 7f : ed	:e1 :59		
Default MAC Address	: 💿 Enable 🔿 Disable			
VLAN ID :	10			
Description :	(Optic	inal)		
Frome .				
Profile :	lan1			

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).

neral Setup				
Profile : V Enable This Profile	lan2			
Description :	(Optiona	D.		
VLAN ID :	11			
Default MAC Address :				
MAC Address :	00 : 50 : 7f : ed :	e1 : 59		
IPv4 Protocol :	static			
Mode :	NAT			
IP Address :	192 . 168 . 2 . 1			
Subnet Mask :	255.255.255.0 🗸			
Gateway IP Address :		MIK	(Optional)	
	🕼 Add 💾 Save			
	IP	Subnet Mask	Mode	
		No items to show.		
2nd Subnet :				
	m			
			💾 Apply 🛛 🔇	Canci

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.

Dray Tek	Vigor 30	OB 14:22:12	Login: Ad	lmin 🕞
uto Logout : Off Quick Start Wizard Online Status WAN	WAN >> Load Balance Pool Control Add Profile	Rule	Refresh Jace Primary Profile	Prof Backup Profile
General Setup		No	items to show.	
Default Route Load Balance				
Switch				
LAN				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices				
Product Registration	4			•

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.

1			-
Mode	Load_Balance Fai	ilover	
Profile :	WAN1WAN2		
	Load_Balance	~	
	Load_Balance		
	Failover		
			💾 Apply 🔞 Can

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

I		
Mode	Load_Balance Failover	
	🕼 Add 🗎 Save	
	Interface Weight	
	wan1 1 💼	
	wan2 1 💼	
Interface		
		💾 Apply 🔞 Ca
		- (PP-) 🖉

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

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

	WAN >> Load Balance >	> Pool							
Auto Logout : Off 🛛 🗸	Pool	ile							
Quick Start Wizard	🕼 Add 💥 Ed	🕼 Add 🔀 Edit 📺 Delete 🛷 Refresh Profile Number Limit							
Online Status WAN	Profile	Mode	Interface	Primary Profile	Backup Profile				
General Setup	WAN1WAN2	Load_Balance	wan1 1,wan2 1						
Default Route									
Load Balance									
Switch									



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

	W	AN >> Loa	ad Balance >	>> Rule								
ito Logout : Off 🛛 👻		Poo	ol	Rule								
Quick Start Wizard	1				-		~					
Online Status			Add 🗙	Edit	Delete	📢 Refn	esh 👕	Move Up	🐣 Move	Down		
WAN		Profile	Enable T	Protoco	Source I	Source N	Destinati	Destinati	Destinati De	stinati L	oad Balar	
General Setup						No iten	ns to show					
Default Route												
Load Balance												
Switch												
LAN												
NAT												
Firewall												
Objects Setting												
User Management												
Applications												
Bandwidth Management												
System Maintenance												
Diagnostics												
External Devices												

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

Profile :	Rule1	
Enable This Profile		
Protocol :	ALL	
Source IP Address :	192 . 168 . 1	0 (Optional
Source Mask :	255.255.255.0	· (Optional)
Destination IP Address :		. Optional
Destination Mask :	255.255.255.0	(Optional)
Load Balance Pool/WAN Profile :	wan1 v	



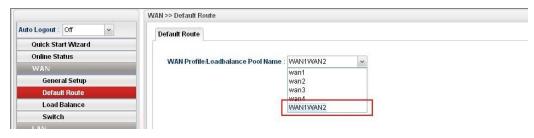
11. Click **Add** again to create a profile for Rule2 accepting 192.168.2.0/24 which always goes Internet via WAN2 when WAN2 is up.

Rule	- ×
Destilation	Rule2
Profile :	Ruiez
Enable This Profile	
Protocol :	ALL v
Source IP Address :	192 . 168 . 2 . 0 (Optional)
Source Mask :	255.255.255.0 V (Optional)
Destination IP Address :	(Optional)
Destination Mask :	255.255.255.0 V (Optional)
Load Balance Pool/WAN Profile :	wan2 🗸
-	🗎 Apply 🛛 🐼 Cancel

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

	WAN >> Load	Balance >> F	tule					
Auto Logout : Off 🛛 🗸	Pool	Rule						
Quick Start Wizard	Ado	i 💥 Edit	m Delete	e 🗳 Refresh	💣 Move Up	🐣 Move Dowi	ì	
Online Status					-			
WAN	Profile	Enable This	Protocol	Source IP A Source	ce Mas Destinatio	n Destination	Destination Destination	Load Balanc
General Setup	Rule1	true	ALL	192.168.1.0 255.25	55.25!	255.255.256		wan1
Default Route	Rule2	true	ALL	192.168.2.0 255.25	55.25!	255.255.25		wan2
Load Balance								

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



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

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

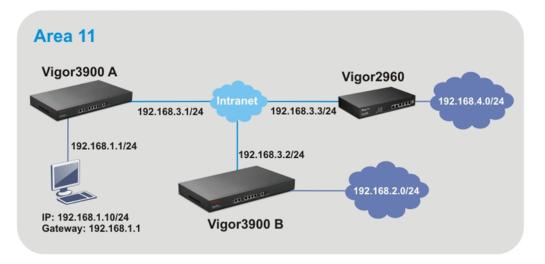
3.2 How to Configure OSPF?

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

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

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

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



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

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



Configuration for Vigor3900 A,

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

Dray Tel		or 3900 Series		14:41:38	Login:		E
	General Setup				-	×	
Auto Logout : Off		lan1					
Quick Start Wizard	Enable This Profile						Profile Numb
Online Status	Description :	(Option	nal)				
WAN	VLAN ID:	10				IPv6 Prot	ocol
LAN	Default MAC Address :	Enable Obisable				Jink-Loca	
General Setup	MAC Address :	00 : 50 : 7f : 7b :	83 : 08			Jink-Loca	d
IP Routing	IPv4 Protocol :	static					
Static Route	Mode :	NAT				1	
Switch							
Bind IP to MAC	IP Address :	192 168 1 1					
RIP Configuration	Subnet Mask :	255.255.255.0 ~					
OSPF Configurati	Gateway IP Address :				(Optional)		
Firewall		🖏 Add 🛗 Save					
Objects Setting		IP	Subnet Mask	Mode			
User Management							
Applications			No items to show.				
VPN and Remote a	2nd Subnet :						
Virtual System	Zing Subnet .						
Certificate Manag						•	
	4						
Bandwidth Manag				8	Apply 🙆 Cancel		
System Maintenane			-	_	M2		

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

Dray Te		or 3900 Series	14:42:03 Log	in: Ad	min 🕞
Auto Logout : Off Ouick Start Wizard		lan2		-	
Online Status WAN	Description : VLAN ID :	(Optional)			Profile Numb
LAN General Setup IP Routing	Default MAC Address : MAC Address :	00 : 50 : 7f : 7b : 83 : 08			Jink-Local Jink-Local
Static Route Switch Bind IP to MAC	IPv4 Protocol : Mode : IP Address :	NAT ~ 192 166 3 1		Е	
RIP Configuration OSPF Configuration	Subnet Mask : Gateway IP Address :	255.255.255.0	(Optional)		
NAT Firewall Objects Setting		C Add Save	Mode		
User Management Applications VPN and Remote 4		No items to show.			
Virtual System Certificate Manag	2nd Subnet :				
SSL VPN Bandwidth Manag System Maintenar			🖿 Apply 😮 Can	cel	

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 Configurati	on		
Quick Start Wizard				
Online Status	🐨 Enable Thi	s Profile		
WAN				
LAN		C Add		
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,

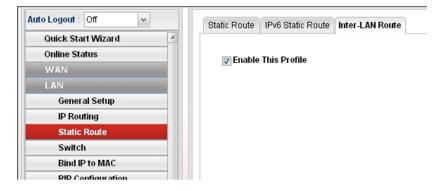
1. Open **LAN** >> **General Setup** to create a LAN (192.168.2.1/24) profile named lan1 with the settings shown below.

General Setup × Inter Logont (M) Profile : lan1 Ordine Status Profile : lan1 WAN Image: constraints VAN Image: constraints Static Route Static Static Route Static Static Route Image: constraints Static Route Static Image: constraints Static Route Static Route Image: constraints Static Route Image: constraints Static Route Image: constraints Object: Setting Gateway IP Address : 192 168 2 1 Object: Setting Gateway IP Address : 192 168 2 1 VPN and Remote Image: constraints VPN and Remote Image: constraints VPN and Remote Image: constraints VPN and Remote Image: conset VPN and	Dray Tel		or 3900 Series	14:58:55	Login: Ad	lmin 🕞
Mo Logonit: Ordine Status Ordine Status Profile: Maximum Image: Status VAN Image: Status LAN Defauit MAC Address: Defauit MAC Address: Image: Status Static Roare MAC Address: Static Roare MAC Address: Static Roare Mode: Static Roare Subnet Mask: Static Roare Mode: Static Roare Subnet Mask: Static Roare Mode: Static Roare Mode: Static Roare Mode: Static Roare Mode: Objects Setting Gateway IP Address: Objects Setting Znd Subnet: Certificts Management No items to show. VPN and Remote Znd Subnet Certificts Management Mode Static Nongo		General Setup				
Ouclex Statu Ward Description: (Optional) Protein WAN VLAN D: 10 Protein						
General Status VLAN ID :: 10 LAN Default MAC Address: © Enable Default MAC Address: © Enable Default MAC Address: B P Exating BAC Address: © Enable Static Roote MAC Address: D : 00 : 77 : 79 : 64 : 80 Bind P to MAC P Address: D : 00 : 77 : 79 : 64 : 80 Bind P to MAC PA Address: D : 00 : 77 : 79 : 64 : 80 Bind P to MAC P Address: D : 10 : 10 : 10 : 10 : 10 : 10 : 10 : 1		65				Profile N
NAT Default MAC Address: © Enable © Disable Increat Setup Proving Static Ronen Switch Bind Pte MAC Image: Size Size Size Size Size Size Size Size		-				Du6 Protocol
Certorial Setup Default and coverss. Consume IP Routing Static Route Static Route Swatch Bind To MAC Bind To MAC Bind To MAC Static Route Swatch Bind To MAC Cateway IP Address : OSPF Configuration Virtual System Certificate Manage SSL VPN Certificate Manage Statice Market : Certificate Market : Certificate Market : Certificate Market : Certificate Market :						and the second se
MAC Address: 00::50::77 ?9:04 :00 MAC Address: 00::50::77 ?9:04 :00 Mode: 04 Switch Bind P to MAC BP Certigurative OSPF						CONTRACTOR OF TAXABLE PARTY OF TAXABLE P
Static Roate BV-4 Protocol: static Switch Hode: NAT Bind Pro MAC IP Address: 192 188 Bind Pro MAC IP Address: 192 188 Skitch Subset Mask: 255.255.0 w Gateway IP Address: (Optional) Firewall Gateway IP Address: Image: Control of the state of	and the second	MAC Address :	00 : 50 : 71 : 79 : 84 : 80			
Switch Mode: NAT Bind P to MAC P Address : 192_168_2_1 BP Configuration Subnet Mask : 255255250 w OSPF Configuration Gateway IP Address : 102_168_2_1 NAT Freevall Image: Configuration of the state of the stat		IPv4 Protocol :	static			
Bind P to MAC P Address : 192 168 2 1 Bind P to MAC Subret Mask : 255:255:0 Image: Configuration of the state of the st		Mode :	NAT v			
OSPE Contigurat NAT Firewall Objects Setting USer Management Applications VPN and Remoto VPN and Remoto VPN and Remoto SSL VPN Randwidth Manag SSL VPN Randwidth Manag		IP Address :	192 168 2 1			
NAT Gateway IP Address : (Optional) Firewall Objects Setting Add Save Objects Setting IP Subnet Mask VDV and Remote No items to show. VPN and Remote Cardificate Manag SSL VPN cl Satt VPN cl Satt VPN cl	RIP Configuration	Subnet Mask :	255.255.255.0 ~			
Firewall Objects Setting User Nanagemen IP Applications Subnet Mask VPN and Remote No items to show. Virtual System Cancel Sst. VPN Image: Concel Sate Monitories Image: Concel	-	Gateway IP Address :	_	(Option	a()	
User Managemen Applications VPN and Remoto VPN and Remoto Virtual System Certificate Manag SSL VPN Bandwidth Manag			🕼 Add 🛗 Save			
User Managemen Applications VPN and Remote Virtual System Certificate Manag SSL VPN Bandwidth Manag	Objects Setting		IP Subnet Mask	Mode		
Applications VPN and Remote VPN and Remote Virtual System Certificate Manag SSL VPN I Bandwidth Manag Certificate Manag	User Management					
Virtual System Certificate Manag SSL VPN Randwidth Manag System Molden a	Applications		No items to show.			
Virtual System Certificate Manag SSL VPN Bandwidth Manag System Moleceare	VPN and Remote a					
SSL VPN Bandwidth Manag System Molden a	Virtual System	2nd Subnet :				
Bandwidth Manag	Certificate Manag				-	
System Maintenauer	SSL VPN	4				
System Maintenante	Bandwidth Manag			Apply	3 Cancel	
	System Maintenand		-	ht		

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

	iaor 3900 Series	14:59:11	Login: Admin	EX.
General Setup				
Auto Logout : Off Profile :	lan2		×	
Quick Start Wizard	(Optional)			Profile No.
Online Status	11		Pv6 Protoc	
TYPE C				-01
LAN Default MAC Add	ress: 💿 Enable 🔿 Disable		Jink-Local	
General Setup MAC Address :	00 : 50 : 7f : 79 : 84 : 80		Jink-Local	
IP Routing IPv4 Protocol :	static			
Static Route Mode :	NAT		-	
Switch Bind IP to MAC IP Address :	192 168 3 2			
RIP Configuration Subnet Mask :	255.255.255.0 ×			
OSPF Configuration Gateway IP Addr	oss : , , , , ,		(Optional)	
Firewall	🖏 Add 🔚 Save			
Objects Setting	IP Subnet Mask	Mode		
User Management	No items to sho			
Applications	NO INFITS ID SHO	Ψ.		
VPN and Remote a 2nd Subnet :				
Virtual System				
Certificate Manag				
SSL VPN				
Bandwidth Manag		H /	rgly 🥝 Cancel	
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.)

	LAN >> OSPF Config	uration		
Auto Logout : Off 🛛 👻	OSPF Configurati	on		
Quick Start Wizard				
Online Status	🐨 Enable Thi	s Profile		
WAN				
LAN		C Add		
General Setup		LAN Profile	Area	
IP Routing		lan2	11	Û
Static Route	Profile :	lan1	11	Ū
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	meral Setup	or 2960 Series	15:04:49	Logins -	
n Logout : Off		lant			
Quick Start Wizard	Enable This Profile				ofile Number Limit : 16
Online Status	Description	(Optional)			
WAN	VLAN ID :	10			Pv6 Protocol
LAN	Default MAC Address :	Enable Olisable Disable			Jink-Local
General Setup	MAC Address :	00 1 60 2 77 1 ent 1 et 2 51			link-Local
IP Routing	IPv4 Protocol :	static			
Static Route	Mode :	NAT			E
Switch Bind IP to MAC	IP Address :	192 168 4 1			
RIP Configuration					
OSPF Configurati	Subnet Mask :	255,255,255.0 ~			
NAT.	Gateway IP Address :			(Optional)	
Firewall		ち Add 🗎 Save			
Objects Setting		IP Subnet Mask	Mode		
User Management		No items to show			-
Applications		110 110 110 110 110 110			
VPN and Remute (2nd Subnet :				
Certificate Manag					
SSL VPN					3
Bandwidth Manag					
System Maintenar Diagnostics				Apply 🥥 Cancel	

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

Dray Tek	or 2960 Series	15:05:32	Login:	Admin
Logout : Off Profile :	lan2			×
Duick Start Wizard Description	(Optional)			ofile Number Limit : 10
nine Status				
VAN VLANID:	11			IPv6 Protocol
	Enable Obisable			_ink-Local
General Setup MAC Address :	00 : 50 : 7f : ed : e1 : 51			Link-Local
IP Routing IPv4 Protocol :	static			-
Static Route Mode :	NAT			
Bind IP to MAC IP Address :	192 168 3 3			
Dirici in to mixe				
OSPF Configuration Subnet Mask :	255.255.255.0			
Gateway IP Address :	·	1	(Optional)	
irewall	🕼 Add 🔚 Save			
Objects Setting	IP Subnet Mask	Mode		
Jser Managemen	No items to show			
Applications	No terns to show.			
/PN and Remote . 2nd Subnet :				
Certificate Manag				
SSL VPN				3
Sandwidth Manag 🚺	m			
System Maintenar Diagnostics		⊟ (oply 🔕 Cancel	

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	C Enable 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.)

	LAN >> OSPF Config	uration		
Auto Logout : Off 🛛 👻	OSPF Configurati	on		
Quick Start Wizard		-		
Online Status	🔽 Enable Thi	s Profile		
WAN	V Endine mi			
LAN		🚯 Add		
General Setup		LAN Profile	Area	
IP Routing		lan2	11	Ô
Static Route	Profile :	lan1	11	â
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration	E			

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				
🦈 Refrest	n				
Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0	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	Ŭ	0	lan-lan1

Routing information for Vigor3900 B

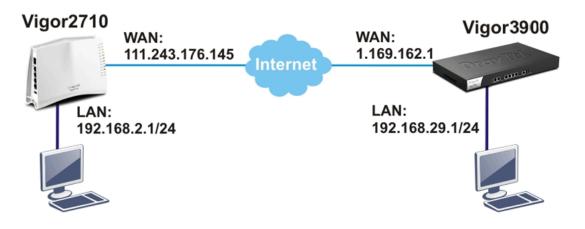
Routing Table	IPv6 Routing Table				
S Refrest	1				
Destination	Gateway	Genmask	Flags	Metric	lface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
192,168,1,0	192.168.3.1	255,255,255,0	UG	20	lan-lan2

Routing information for Vigor2960

Routing Table	IPv6 Routing Table				
S Refresh	n				
Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	0.0.0	255.255.255.0	U	0	lan-lan1
192.168.3.0	0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	192.168.3.1	255.255.255.0	UG	20	lan-lan2

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

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



Configuring Vigor3900

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

IPSec		-×
Profile : 📝 Enable This Profile	2710	
Type :	● IPSec ○ Dial- ○ Dial- Out In	
Set PPTP Dial-In For	User Profie	
Basic Advanced	GRE Proposal PPTP	
Auth Type :	PSK 🗸	~
Preshared Key :		
Security Protocol :	ESP 👻	
WAN Profile :	wan1 👻	=
Local IP / Subnet Mas	k: 192 168 29 0 255.255.255.0 🗸	
Local Next Hop :	0.0.0.0.0	
Remote Host :	111 . 243 . 176 . 145	
Remote IP / Subnet Ma		-
4	III 🗄 Apply 🧯	Concol
	💾 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 configurator 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 🔘 Blo	ck PING to the IP
Multicast via VPN OPass 💿 Bloc	sk
(for some IGMP,IP-Camera,DHCP Relay.	.etc.)

- 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.

ype of Server I am calling	Username	???
O PPTP	Password	
IPsec Tunnel		
C L2TP with IPsec Policy None	PPP Authentication	● On ○ Off
Server IP/Host Name for VPN. such as draytek.com or 123.45.67.89) 1.169.162.1	IKE Authentication	
	 IKE Pre-Shared Key Digital Signature() 	
	Peer ID	None V
	Local ID	None
		ubject Name First
	O Subject Name	
	IPsec Security Meth	od
	O Medium(AH)	
		without Authentication 💌
	Advanced	
	Index(1-15) in <u>Schee</u>	lule Setup:

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

4. TCP/IP Network Set	tings	
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 💌
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						
Dee	files :	v 🙃 Conne	ect	PTP 🔄 Re	fue els		
PIC	anes:	💉 🔁 Conne	ect (a) IPSec () I	PIP 🐨 RE	aresn		
VPN	Type	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.

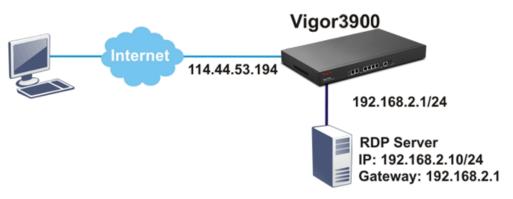
VPN and Remote Access >> Connection Management

Dial-o	ut Tool				R	efrest	n Seconds :	10 💌 🗌	Refresh
		(3900))1.169.162.1		v [)ial 🛛			
	onnection State t Page: 1	15				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
					******		ita is encryp	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 configurator of Vigor3900.
- 2. Enable the HTTPS service from **System Maintenance** >> **Access Control** by clicking **Enable** for **HTTPS Allow** and type **443** as the value of **HTTPS Port.**

Dray Tek	Vigor 3900 s	Series	14:03:42	Login: Admin	Ð
	System Maintenance >> Acc	ess Control			
uto Logout : Off 🛛 👻	Access Control				
Firewall					*
Objects Setting	Web Allow :	💿 Enable 🔿 Disable			
User Management	Web Port :	80			
Applications	Telnet Allow :	Enable Disable			
VPN and Remote Access					
Virtual System	Telnet Port :	23			
Certificate Management	SSH Allow :				
SSL VPN	SSH Port :	22			
Bandwidth Management	HTTPS Allow :	Enable Disable			_
System Maintenance					2 27
TR-069	HTTPS Port :	443	A		
Administrator Password	User Define :	🔘 Enable 💿 Disable			
Configuration Backup	Allowed IP1	0 0 0	0 0.0.0.0	V	
Syslog / Mail Alert					
Time and Date	Allowed IP2 :	0.0.0	0 0.0.0.0	*	
Access Control					
SNMP Setup	Allowed IP3 :	0.0.0	0 0.0.0.0	*	
Reboot System	Allow Ping from the W	/AN : 💿 Enable 🔿 Disable			
Firmware Upgrade	Allow Ping from the L	AN : () Enable () Disable			-
Diagnostics	Allow Ping Hom the Li	an (v/Enable ()Disable	m		
External Devices				🖈 Refresh	💾 Apply
Product Registration -					

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.

Dray Tek	Vigor 3900 Series	17:46:41	Login: Admin	E>
	SSL VPN >> SSL Application >> RDP			
uto Logout : Off 🛛 👻	VNC RDP			
Quick Start Wizard	CARL MEAN PROVIDE 15 D			Profile Nu
Online Status	🕼 Add 💥 Edit 🔟 Delete 🗢 Ro			T TOILE INC
	Profile IP Address	Port	Screen Size	
		No items to show.		
	RDP	- ×		
	Profile : Win7			
	IP Address : 192 168 2	10		
	Port: 3389			
	Screen Size : Fullscreen 🗸			
		💾 Apply 🛛 😡 Cancel		
SSL Web Proxy				
SSL Application				
Online User Status				
External Devices				
Product Registration				
	a l			

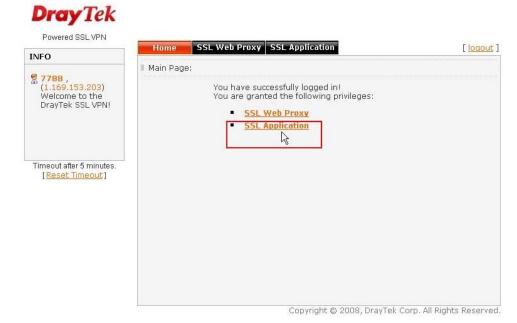
4. Open User Management >> User Profile to create a new profile named "7788". Set the Password as 7788 and choose the profile of Win7 as SSL Application (RDP). Click Apply.

Dray Tek	Vigor 3900	Series	17:48:10		Login: Admin	Ð
	User Management >> Us	er Profile		4		
Logout : Off	User Profile		- ×			
Ouick Start Wizard	Username :	7788	×	_		
Online Status	👿 Enable This Profile				F	Profile N
	Password :	••••		DHCP from	Static IP Addre Use mOTP	
LAN	Idle Timeout (sec) :	300		lan1	Disable	
	Usage Time (min) :	480		lan1	Disable	
	System User :	false		lan1	Disable	
Objects Setting	Group :	User				
		Land Land				
General Setup	PPTP :	🔘 Enable 💿 Disable				
User Profile	L2TP :	🔵 Enable 💿 Disable				
User Group	DHCP from :	lan1 👻	E			
RADIUS	Static IP Address		(Optional			
LDAP / Active Directory			(optorial			
Applications	Use mOTP :	🔘 Enable 💿 Disable				
VPN and Remote Access	mOTP PIN Code :					
Virtual System	mOTP Secret :					
	SSL Proxy :	~				
	SSL Application(VNC)	- Possi				
	SSL Application(RDP)	Win7 🖌				
External Devices	4	111				

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

.ogin				
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.

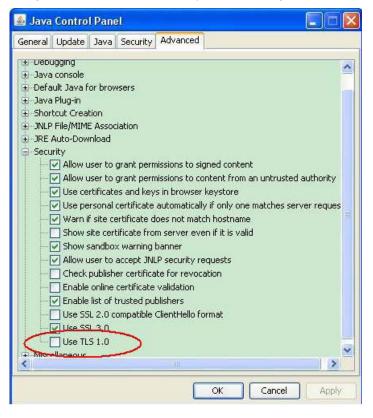


9. After that, you can access into Windows 7 via a browser. Note the message below the window. In which, TLS means Transport Layer Security.

ତ ¥igor SSL ¥PN	- RDP Application	- Google Chrome	R		X
🏂 🍂 🍂 🕅 🍾	194/sslvpn/rdp.htm?app	name=Win7&cookie=2:	IDAEAB8B10.	5B3AB2B0ADC	DBE89
					^
	Java				
Note: If you at	e using Sun TRE 6	0 or newer version	c Diesce or	to the Tarra	
		TLS 1.0 in Advanc			~
EN					
		Ņ			
	Administr	ator 其他使用者			
۲		/indows :7 旗艦版		k	

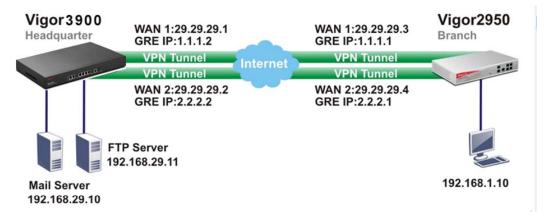
Troubleshooting

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



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

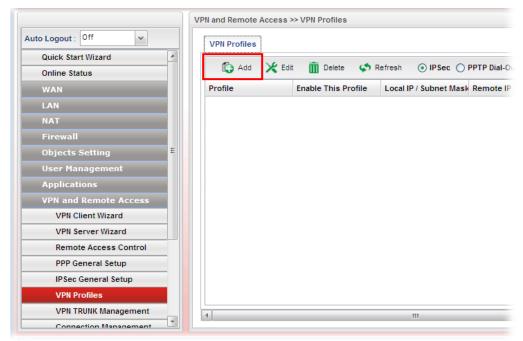
The staff in branch office can access into mail server/FTP server installed in the headquarters via VPN Load Balance tunnels. Refer to the following figure.



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

Configuring Vigor3900

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



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

Profile :	2950WAN1	
Enable This Profile		
Type :	💿 IPSec 🔘 PPTP Dial-Out 🔘 PPTP Dial-In	
Basic Advanced	GRE Proposal PPTP	
Always On :	🔘 Enable 💿 Disable	
For Remote Dial-In :	🔵 Enable 💿 Disable	
Auth Type :	PSK 🗸	
Preshared Key :	•••	
Security Protocol :	ESP 🗸	
WAN Profile :	wan1 👻	

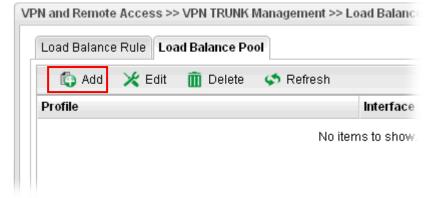
Profile :	2950WAN1
🔽 Enable This Prof	ile
Туре :	💿 IPSec 🔘 PPTP Dial-Out 🔘 PPTP Dial-In
Basic Adva	nced GRE Proposal PPTP
Enable GRE Functio	n: 💿 Enable 🔘 Disable
Local GRE IP :	1 . 1 . 2 (Optional)
Remote GRE IP :	1 . 1 . 1 (Optional)
Auto Generate GRE	Key: 💿 Enable 🔿 Disable

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

IPSec				=×
Profile :	2950WAN2			
Type :	💿 IPSec 🔘 PPTI	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				•
				🗎 Apply 🔞 Cancel

Profile :	2950\	VAN2			
🔽 Enable This P	rofile				
Type :	⊙ IF	Sec 🔘 PPT	P Dial-Out 🔘 PP	TP Dial-In	
Basic Ad	ivanced	GRE	Proposal	PPTP	
		2.12			
Enable GRE Fund	tion : 🧕 🧕) Enable 🔘	Disable		
Local GRE IP :	2	. 2	. 2 . 2	(Optional)	
Remote GRE IP :	2	. 2	. 2 . 1	(Optional)	
Auto Generate G	GRE Key : 🧕	Enable 🔘	Disable		

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



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

jour : joii	-V. Land Delever Dule Land Del	Devi
Load Baland	ce Pool	_ ×
Mode	Load Balance	
Profile	: 2950_LB	
4 		
		📑 Apply 🛛 😵 Cancel
		🔄 Apply 🤯 Calice

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

d Balance I	Pool	
Mode	Load Balance	
Interface	: 2950WAN1,2950WAN2 ~ 39 39_1 2250WAN1 2250WAN1 2250WAN2	
		📑 Apply 🔞 Canc

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	5.255.0		*	(Opti	onal)	
Destination IP Address :	192	168	. 1].	0	mu) (Optiona
Destination Mask :	255.25	5.255.0		~	(Opti	onal)	
Load Balance Pool :	2950_	LB		~			

Configuring Vigor2950

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

Vigor2950 Dual-WAN SSL VPN A		Dray Tek
Off Quick Start Wizard Service Activation Wizard Online Status WAN	VPN and Remote Access >> LAN to LAN Profile Index : 1 1. Common Settings Profile Name 2960WAN1	Call Direction O Both O Dial-Out O Dial-In
LAN NAT Firewall Objects Setting CSM Bandwidth Management Applications VPN and Remote Access > VPN Client Wizard	✓ Enable this profile VPN Dial-Out Through: WAN1 Only ♥ Netbios Naming Packet ● Pass Multicast via VPN ● Pass (for some IGMP,IP-Camera,DHCP Relayetc.)	Always on Idle Timeout Idle Ti
Remote Access Control PPD General Setup IPSec General Setup IPSec General Setup Remote Dial-in User LaN to LAN VPN ITRUNK Management Conscion Management Sci 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) 29.29.29.1	Link Type 64k bps V Username ??? Password PPP Authentication PAP/CHAP V VJ Compression On Off IKE Authentication Method Pre-Shared Key Digital Signature(X.509) Proce ID

- 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**.

ff 💌			🗹 DES 🗹 3DES 🗹 AES	
ick Start Wizard rvice Activation Wizard line Status			Callback Function (CBCP)	
AN			Use the Following Number to Callba	r k
N			Callback Number	
.T ewall				ute(s)
jects Setting M	1 OD5 0 00			
m ndwidth Management	4. GRE over IPSec Setting			
olications	Enable IPSec Dial-Ou			
N and Remote Access	🔲 Logical Traffic	My GRE IP 1.1.1.1	Peer GRE IP 1.1.1.2	
VPN Client Wizard	5. TCP/IP Network Settings	\$		
Remote Access Control		0.000	RIP Direction Disable	
PPP General Setup	My WAN IP	0.0.0.0		
IPSec General Setup IPSec Peer Identity	Remote Gateway IP	0.0.0	From first subnet to remote network, y	ou have to
Remote Dial-in User		100,100,00,0	do	
LAN to LAN	Remote Network IP	192.168.29.0	Route 🛩	
VPN TRUNK Management	Remote Network Mask	255.255.255.0		
Connection Management tificate Management			Change default route to this VPN tur	inel (Only
VPN	Local Network IP	192.168.1.0	single WAN supports this)	
em Maintenance	Local Network Mask	255.255.255.0		
nostics				
		More		

- 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 Dudi-WAN SSL VPN 7		Dray 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 Gleet Wizard > VPN Server Wizard > Remote Access Control	Profile Name 3900WAN2 Profile Name 3900WAN2 VPN Dial-Out Through: WAN2 Only Netbios Naming Packet © Pass © Block Multicast via VPN © Pass © Block (for some IGMP,IP-Camera,DHCP Relayetc.) 2. Dial-Out Settings	Call Direction Both Dial-Out Dial-In Call Always on Idle Timeout -1 second(s) Enable PING to keep alive PING to the IP
Helmote Access Control PPP General Setup IPSec General Setup IPSec Peer Identity Remote Dial in User LAN to LAN VPN TRUKK Management Certificate Management Sst. VPN System Maintenance Diagnostics Support Area Application Note FAQ Status: Ready	Type of Server 1 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) 29.29.2	Link Type 64k bps V Username ??? Password PPP Authentication PAP/CHAP V VJ Compression © On Off IKE Authentication Method © Pre-Shared Key IKE Pre-Shared Key © Digital Signature(X.509) Dest ID

- 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 🗹 3DES 🗄	AES
ick Start Wizard			Callback Function (CBCP)	
line Status			🗌 Enable Callback Function	n
AN			Use the Following Numb	er to Callback
N			Callback Number	
.T ewall			Callback Budget 0	minute(s)
jects Setting		~	Caliback Budget	minuce(s)
M ndwidth Management	4. GRE over IPSec Settings	s		
plications	🗹 Enable IPSec Dial-Ou	t function GRE over IPS	ec	
N and Remote Access	🔲 Logical Traffic	My GRE IP 2.2.2.1	Peer GRE IP 2.2.2.2	
VPN Client Wizard	5. TCP/IP Network Settings			
Remote Access Control				
PPP General Setup	My WAN IP	0.0.0.0		sable 💌
IPSec General Setup IPSec Peer Identity	Remote Gateway IP	0.0.0.0	From first subnet to remote	network, you have to
Remote Dial-in User	Remote Network IP	192 168 29 0		
LAN to LAN	Kelliote Network IP		R	oute 💌
VPN TRUNK Management Connection Management	Remote Network Mask	255.255.255.0		
rtificate Management	Local Network IP	192.168.1.0	Change default route to t single WAN supports this)	his VPN tunnel (Only
		255 255 255 0	single war supports this)	
stem Maintenance	Local Network Mask	255.255.255.0		
rginoanca		More		

- After finished the settings on both VPN connections, please access the web configurator of Vigor2950 and open VPN and Remote Access > VPN Trunk Management to make these two VPN connections into one Load Balance group.
- 4. Type the name (e.g., 3900) of the **Load Balance** in the field of **Profile Name**. Specify the VPN profiles in Member 1 and Member 2 respectively. Then, choose **Load Balance** as the **Active Mode**.

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 M	anagement						
Profiles :		× 9	Connect 🧿 IPS	ec OPPTP	🤝 Refresh		
33328 V0323			10.4.111.4	11. 7	DV/Deelecte)	THERE	Discourse
VPN	Туре	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Disconnect
VPN 2950WAN1	Type IPSec/DES_N		1.1.1.1/32	00:47:13	O RX(Packets)	D D	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:						Pag	e No.	Go	>>
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (3900WAN1)	IPSec Tunnel DES-No Auth	29.29.29.1 via WAN1	192.168.29.0/24		0	0	0	0:0:0	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

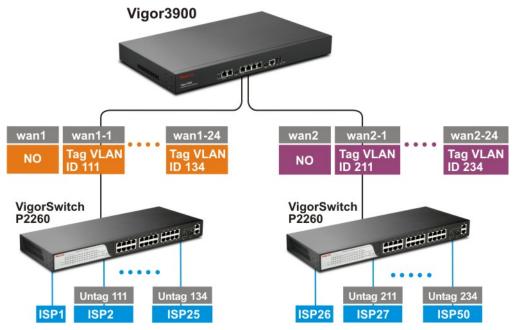
xxxxxxxx : Data is encrypted. xxxxxxxx : Data isn't encrypted.

Vigor3900 Series User's Guide

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:

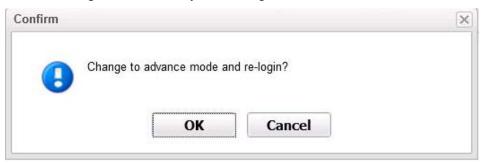


Configuring 50 WAN profiles on Vigor3900

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

	Vigor							
	WAN >> General	Setup						
to Logout : Off	General Setu	P						
Online Status	C Add	🗶 Edit 🕅	Delete 🛛 📢 I	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
NAT	wan5	false		14	Disable	WAN5	None	Link-Local
Firewall	Marketing	true	Marketing Dept	22	Disable	WAN1	DHCP	DHCP-IA_NA
Objects Setting								
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**.

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	🕼 Add	🔀 Edit	🔟 Delete	🐝 Refresh 🛛 Mode :	Advance	¥			Profile Number
wan2 true 11 WAN2 Enable DHCP Link-Local wan3 false 12 WAN3 Enable None Link-Local wan4 false 13 WAN4 Enable None Link-Local wan5 false 14 WAN5 Enable None Link-Local The Selected Config Will be Deleted, Continue?	Profile	Enab	le This Profile	Description	VLAN ID	Port	Untag	IPv4 Protocol	IPv6 Protoco
wan3 false 12 WAN3 Enable None Link-Local wan4 false 13 WAN4 Enable None Link-Local wan5 false Confirm The Selected Config Will be Deleted, Continue?	wan1	true			10	WAN1	Enable	DHCP	Link-Local
wan4 false 13 WAN4 Enable None Link-Local wan5 false Confirm Enable None Link-Local Inter-Local Inter-	wan2	true			11	WAN2	Enable	DHCP	Link-Local
wan5 false Confirm Enable None Link-Local	wan3	false			12	WAN3	Enable	None	Link-Local
Confirm Config Will be Deleted, Continue?	wan4	false			13	WAN4	Enable	None	Link-Local
The Selected Config Will be Deleted, Continue?	wan5	false	(a. c.		1.4	WAANIS	Enable	None	Link-Local
			•			continue?			

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

General Setu	р		
Add	🗶 Edit 🕅	Delete 🛛 📢 Re	efresh Mode
Profile	Enable This Pr	of 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 PPPol	E StaticV6	DHCPV6	
Profile :	wan1_1				
Enable This Pro	ofile				
Description :		(Optional)			
	111	(
VLAN ID :	111				
VLAN Tag :	Disable	*			
Port :	WAN1	~			
Default MAC Addre	ss : 💿 Enable 🔘 Disal	ble			
MAC Address :	00 : 50 : 7	f : e7 : db :	21		
Mode :	NAT	~			
IPv4 Protocol :	None	~			
IPv6 Protocol :	Link-Local	~			
					🗄 Apply 🔞 Can

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			HHH - H
Auto Logout 3 min 🎽			
Marchart Baaca			
VigorSwitch P2260 System	-		
Port		ag-based G	roup
PoE			
Loop Detection	No \	LAN NAME	VID
SNMP		default	1
DHCP Boot	1	derault	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 the second second
Log	Add	d 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. 🗌
Member	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. 🗌
Untra	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 **wan1_1** to **wan1_24**). 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.

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

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

PVID

Port No	PVID	Default Priority	Drop Untag	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 ~	
5	115	0 💙	Disable 🔽	19	129		
6	116	0 🗸	Disable 🗸				
7	117	0 🗸	Disable 💌	20	130		Disable 💌
8	118	0 🗸	Disable 🚩	21	131	0 🗸	Disable 🚩
9	119	0 👻	Disable 💌	22	132	0 🗸	Disable 💌
10	120	0 🗸	Disable 🗸	23	133	0 🗸	Disable 👻
11	121	0 🗸	Disable 🗸	24	134	0 🗸	Disable 🚩
12	122	0 🗸	Disable 🖌	25	1	0 👻	Disable 🔽
13	123	0 👻	Disable 👻	26	1	0 🗸	Disable 🔽

- PVID means VigorSwitch2260 will check and add VLAN tags while receiving packets from Ports.
- ISP modem 1 which connects to Port 1 doesn't support VLAN Tag.
- While the switch receives packets from Port 1, it will add VLAN Tag 111 to the packets Then Vigor3900 wan1_1 will receive the packets.
- 6. After finishing the configuration for one VigorSwitch, please set for another VigorSwitch with the same procedure. The file names shall be wan2_1~ wan2_24 and the VLAN ID shall be set as 211~ 234.

Chapter 4: Advanced Web Configuration

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

4.1 WAN Setup

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

Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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



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

WAN	
General S	etup
Default Ro	ute
Load Bala	nce Policy
Switch	

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.

🔀 Edit	< Refresh	Mode :	Basic	~	
Profile	Enable This P	Descript	Basic		Un
Prome	chable this P	Descript	Advance		UI

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

Profile

Below shows settings in **Basic** mode:

🔀 Edit	< Refresh	Mode : Bas	ic	*		Profile N	Number Limit : 5
Profile	Enable This F	Description	VLAN ID	Port	Untag	IPv4 Protoco	IPv6 Protocol
wan1	false		10	WAN1	Enable	None	Link-Local
wan2	true	carrie	11	WAN2	Enable	Static	Link-Local
wan3	false		12	WAN3	Enable	None	Link-Local
wan4	false		13	WAN4	Enable	None	Link-Local
wan5	false		14	WAN5	Enable	None	Link-Local

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

General Set	General Setup							
🚯 Add 🔀 Edit 🍈 Delete 🧔 Refresh Mode : Advance 🛛 👻 Profile Number Limit								
Profile	Enable This	P Description	VLAN ID	Port	Untag	IPv4 Protoco	IP∨6 Protocol	
wan1	false		10	WAN1	Enable	None	Link-Local	
wan2	true	carrie	11	WAN2	Enable	Static	Link-Local	
wan3	false		12	WAN3	Enable	None	Link-Local	
wan4	false		13	WAN4	Enable	None	Link-Local	
wan5	false		14	WAN5	Enable	None	Link-Local	

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

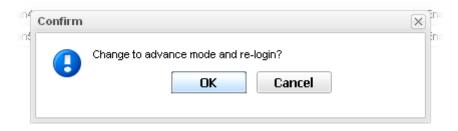
Each item will be explained as follows:

How to add a new WAN profile

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

General Setu	IP				
🔀 Edit	< Refresh	Mode :	Basic	~	
Profile	Enable This D	Descript	Basic		Unt
FIONE	Enable This P	Descript	Advance		Un
				tems to show	

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



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

Global PPTP	Static	DHCP	PPPoE	StaticV6	DHCPV6	
Profile :	Marketing					
📝 Enable This Profile	•					
Description :	Marketing Dept	(Opti	onal)			
VLAN ID :	22					
VLAN Tag :	Disable	*				
Port :	WAN1	*				
Default MAC Address	: 💿 Enable 🔘 Di	sable				
MAC Address :	00 : 50	7f : e7	: cb : 21			
Mode :	NAT	*				
IPv4 Protocol :	None	*				
IPv6 Protocol :	Link-Local	*				

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

VLAN Tag	Choose Enable to tag the packets passing through the port specified below.				
Port	Choose the physical WAN interface for such profile.				
	WAN1				
	WAN1				
	WAN2				
	WAN3				
	WAN4				
	WAN5				
Default MAC	Enable – Click it to enable the default MAC address for				
Address	such profile.				
	Disable – Click it to type the MAC address manually for				
	such profile.				
MAC Address	Specify the MAC address for such profile. In default, the				
	system will determine it automatically.				
Mode	Determine such profile will be used for.				
	ROUTING				
	NAT				
	ROUTING				
IPv4 Protocol Type	There are four connection modes for you to specify for IPv4				
• •	protocol type. Each mode will bring up different web page.				
	None				
	None				
	Static				
	DHCP				
	PPPoE				
	РРТР				
IPv6 Protocol Type	There are four connection modes for you to specify for IPv6				
• 1	protocol type. Each mode will bring up different web page.				
	Link-Local 🗸				
	Link-Local				
	Static				
	otatic				
	DHCP-IA_NA DHCP-IA_PD				

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

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

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

neral Setup		-0
Global PPTP S	Static DHCP PPPoE StaticVI	6 DHCPV6
IP Address :		-
Subnet Mask 🗄	255.255.255.0	
Gateway IP Address 🗄		
	🚯 Add 🛗 Save	
	DNS Server IP Address	
	No items to show.	
DNS Server IP Address :		
		💾 Apply 🛛 🙆 Cancel

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

	NAT>>Port Redirect	tion/DMZ Hos	t).				
	To add a new IP addre box near to the Add b will be added and disp	utton. Next, clie	ck Add. The new one				
		👌 Add 💾 Save					
			Subnet Mask				
	1	92.168.1.85	255.255.255.0				
	IP Alias :						
	Add – click this buttor address.	n to have a field	d for adding a new IP				
	Save – Click this butto	on to save the se	etting.				
	$\mathbf{\hat{m}}$ – click the icon to	remove the sel	ected entry.				
MTU/MRU	Type the value of MT	U/MRU. The d	lefault value is 1500.				
Connection Detection Mode	Select a detecting mo three ways ARP , PIN router for you to choo PING None ARP PING HTTP	G and HTTP s					
Connection Detection Host	detected whether the	nost is active (s he connection ng down. This f	of WAN interface will function is available				
		🏠 Add 🗎 Sa	ve				
		Connection Dete					
		192.168.1.28					
	Connection Detection Host		()				
	Add – click this button to have a field for adding a new IP address.						
	Save – click this button to save the setting.						
	\mathbf{I} – click the icon to remove the selected entry.						
Connection Detection Interval	Assign an interval per						
Connection Detection Retry		ig the times you router, the conr					



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:

eral Setup			C 10				
Global	PPTP	Static	DHCP	PPPoE	StaticV6	DHCPV6	
Host Name	:			(Optional)			
		🚯 Add	Save				
		IP		Subr	et Mask		
IP Alias :			No	items to show.			
MTU/MRU:		1500					
Connection	Detection Mode	None	*				
							🗄 Apply 🙆 Cano

Item	Description	Description						
Host Name (Optional)	Type a name as the	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).							
	use the drop down li	lress, click Add. Type the subnet one will be added and	mask. Next,					
	IP	Subnet Mask						
	192.168.1.86	255.255.255.0	â					
	Add – click this but	ton to have a field for a	dding a new IP					

	address.					
	Save – click this button to save the setting.					
	命					
	— 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 three ways ARP , PING router for you to choose PING ARP PING HTTP	and HTTP supported in				
Connection Detection Host	Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when Connection Detection Mode is set with PING or HTTP .					
	🕼 Add 🗎 Save					
		Connection Detection Host	-			
		192.168.1.28				
	Connection Detection Host :		(0)			
	Add – click this button to have a field for adding a new IP address.					
		o have a field for adding	a new IP			
		-	a new IP			
	address. Save – click this button t	to save the setting.	a new IP			
Connection Detection Interval	address.	to save the setting. move the selected entry.				
	address. Save – click this button to re – click the icon to re	to save the setting. move the selected entry. d of time for each detection of ensure the connection of the times you set in this f tter, the connection of W	ng. of the WAN ield and no			
Detection Interval Connection	address. Save – click this button to — click the icon to re Assign an interval period Assign detecting times to interface. After passing to reply received by the rou	to save the setting. move the selected entry. d of time for each detection o ensure the connection of the times you set in this f tter, the connection of W d as breaking down.	ng. of the WAN ield and no AN			

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

Global	PPTP	Static	DHCP	PPPoE	StaticV6	DHCPV6		
Username:								
Password :								
MTU/MRU:		1492						
Debug :		🔵 Enable 🧕	Disable					
Always On :		💿 Enable 🔘	Disable					
Fixed IP :		💿 Enable 🔘	● Enable ○ Disable					
Fixed IP Add	ress:							
Connection	Detection Mod	e : None	~					
		🚯 Add 🗎	Save					
		IP		Subn	et Mask			
IP Alias :			N	o items to show.				

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

		🚯 Add 🗎 Save
		Connection Detection Host
		192.168.1.28
	Connection Detection Host :	()
	Add – click this button address.	to have a field for adding a new IP
	Save – click this button	to save the setting.
	$\mathbf{\hat{m}}$ – click the icon to r	remove the selected entry.
Connection Detection Interval	Assign an interval perio	od of time for each detecting.
Connection Detection Retry	interface. After passing	to ensure the connection of the WAN g the times you set in this field and no outer, the connection of WAN led as breaking down.
	• •	to be bound to this interface. This what have typed addresses here, you can
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to	r web page settings (e.g.,
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save . The new one	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next,
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save. The new one field under the box.	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next,
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save . The new one field under the box.	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next, e will be added and displayed on the
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save . The new one field under the box. Add Markowski Save P 192.168.1.86 Add – click this button address. Save –click this button to The second sec	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next, e will be added and displayed on the <u>Subnet Mask</u> 255.255.255.0
	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save . The new one field under the box. Add Add Nave P 192.168.1.86 Add – click this button address. Save – click this button to D – click the icon to reduce to the field of the fi	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next, e will be added and displayed on the Subnet Mask 255.255.255.0 To to have a field for adding a new IP to save the setting. emove the selected entry.
Apply Cancel	see and choose it in late NAT>>Port Redirection To add a new IP address use the drop down list to click Save . The new one field under the box. Add Add Add Save P 192.168.1.86 Add – click this button address. Save – click this button to Click it to save the confi	r web page settings (e.g., on/DMZ Host). s, click Add. Type the IP address and o specify the subnet mask. Next, e will be added and displayed on the <u>Subnet Mask</u> 255.255.255.0



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

file			Coturs SS Drofilo				
Global	РРТР	Static	DHCP	PPPoE	StaticV6	DHCPV6	
				_			
PPTP Ove	er :	Static	~				
Server A	ddress :	0.0.0.0					
Usernam	ie :			Optional			
Passwor	d :						
MTU/MRU	J :	1452					
Debug :		⊖ Enabl	e 💿 Disable				
Always O)n :	📀 Enabl	e 🔿 Disable				
Connecti	on Detection Mod	le : None	~				

Item	Description		
PPTP Over	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.		
	Choose a proper protocol, Static or DHCP .		
Server Address	Type the IP address of PPTP server offered by your ISP.		
Username	Type the user name offered by your ISP.		
Password	Type the password offered by your ISP.		
MTU/MRU	Type the value of MTU/MRU. The default value is 1452.		
Debug	Click Enable to display the PPTP debug message in syslog. The default setting is Disable .		
Always On	 Enable – Click it to enable the function of Always On. The router will keep network connection all the time. Disable – Click it to disable the function of Always On. 		
Connection Detection Mode	Select a detecting mode for this WAN interface. There are two ways PING and HTTP supported in Vigor router for you to choose to send the request out. PING None PING HTTP		

Connection Detection Host	If you choose PING/HTTP as Connection Detection Mode, you have to specify the detection host address in this field. Use the default setting.				
		🏠 Add 💾 Save			
		Connection Detection Host 192.168.1.28			
	Connection Detection Host :		(0		
	Add – click this button to have a field for adding a new IP address.				
	Save – click this button to save the setting.				
	\square – click the icon to	remove the selected entr	y.		
Connection Detection Interval	Assign an interval period of time for each detecting.				
Connection Detection Retry	Assign detecting times to ensure the connection of the WAN interface. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.				
Apply	After finished the PPTP configuration, please click Static or DHCP (according to the PPTP Over Protocol setting) to modify the Static/DHCP configuration for such profile.				
	Click it to save the cont	figuration and exit the di	ialog.		
Cancel	Click it to exit the diale	og without saving the co	onfiguration.		

• If you choose Link-Local as IPv6 protocol type

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



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

second line of the local second	CARLES IN A	VAV AND A DATE				
ieral Setup						_
Global PPTP	Static	DHCP	PPPOE	StaticV6	DHCPV6	
ID 4 4 4						
IPv6 Address ∷			(Optional)			
IPv6 Prefix Length:	64					
IPv6 Gateway Address :			(Optional)			
	🚯 Add	💾 Save				
	IPv6 DNS	Server Addres	s			
	N	o items to sho	N.			
IPv6 DNS Server Address	s :					
					💾 Apply 🧯	3 Cance

Available parameters are listed as follows:

Item	Description				
IPv6 Address	Type the IP address for such protocol.				
IPv6 Prefix Length	Type your IPv6 address prefix length.				
IPv6 Gateway Address	Type your IPv6 gateway address.				
IPv6 DNS Server Address	Type your IPv6 primary DNS Server address.				
	🕼 Add 🔚 Save				
	IPv6 DNS Server Address				
	192.168.1.8				
	IPv6 DNS Server Address :				
	Add – click this button to have a field for adding a new IP address.				
	Save – click this button to save the setting.				
	$\mathbf{\hat{m}}$ – 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.				

Dray Tek

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

General Setup		=×
Global PPTP Statio	DHCP PPPoE StaticV6 DH	CPV6
DHCPv6(IA_NA) Gateway Address	: (Optional)	
	DHCPv6(IA_NA) DNS Addre	
	No items to show.	
DHCPv6(IA_NA) DNS Address :		
		Apply 🔞 Cancel

Available parameters are listed as follows:

Item	Description			
DHCP (IA_NA) Gateway Address	Type the gateway IP address for IPv6 DHCP IA_NA mode.			
DHCP (IA_NA) DNS Address	Type your IPv6 primary DNS Server address.			
D110 11001055	🕼 Add 🛗 Save			
	DHCPv6(IA_NA) DNS Addre			
	192.168.1.29			
	DHCPv6(IA_NA) DNS Address :			
	Add – click this button to have a field for adding a new IP address.			
	Save – 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 DHCP-IA_PD as IPv6 protocol type

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

4.1.2 Default Route

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

Dray Tek	Vigor 3900 Series	15:14:34	Login: Admin	Ð
Auto Logout : SMin Quick Start Wizard Online Status WAN General Setup Default Route Load Balance Switch LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN	WAN >> Default Route			
Bandwidth Management System Maintenance			Apply	🐼 Cancel

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

4.1.3 Load Balance Policy

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

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

Rule

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

Dray Tek	Vigor 3900 Series 15:16:22 Login: Admin
	WAN >> Load Balance >> Rule
Auto Logout : Off 🗸	Pool
Quick Start Wizard	
Online Status	🕼 Add 💥 Edit 🝈 Delete 🔊 Refresh 🍲 Move Up 😽 Move Down
WAN	Profile Enable Thi Protocol Source IP / Source Ma Destination Destination Destination Destination Load Balar
General Setup	No items to show.
Default Route	
Load Balance	
Switch	
LAN	
NAT	
Firewall	
Objects Setting	
User Management	
Applications	
VPN and Remote Access	
Certificate Management	
SSL VPN	
Bandwidth Management	
System Maintenance	4 111
Diagnostics	

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



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

How to add a new rule for Load Balance

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



3. The following dialog will appear.

Profile :					
Enabl	e This Profile				
Protocol		ALL		¥ -	
Source IP	Address :].		(Optional)
Source M	ask:	255.255.255.0		(Optional)	
Destinatio	on IP Address :				(Optional)
Destinatio	on Mask :	255.255.255.0		 (Optional) 	
Load Bala	nce Pool/WAN Profile :	wan1		¥	



Item	Description	
Profile	Type the name of the rule.	
Enable This Profile	Check this box to enable su	ch profile.
Protocol	-	CP, UDP, ICMP, FTP, TFTP, /UDP) for such rule applied to load etting.
Source IP Address	Type a WAN IP address he rule.	re as the source IP address for such
Source Mask	Use the drop down list on the for the source.	he right to choose a suitable mask
	Source Mask :	255.255.255.0 V (O 255.255.255.0 V
	Destination IP Address :	255.255.254.0 255.255.0.0 255.254.0.0
	Destination Mask :	0.0.0.0 128.0.0.0 ≡ (C
Destination IP Address	Type a WAN IP address he such rule. — click the icon to cle	re as the destination IP address for ear the IP setting.
Destination Mask	Use the drop down list on the for the destination.	he right to choose a suitable mask
Load Balance Pool /WAN Profile	wan1 to wan5 profiles are c	
	WAN< <general for<="" setup="" th=""><th></th></general>	
	Load Balance Pool/WAN F	Profile : wan1 💌
		wan1
		wan2 wan3
		wan4
		wan5
		usb3g1
		usb3g2
Apply	Click it to save the configur	usb3g2

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



Pool

This page allows the user to integrate **several** WAN profiles as a pool profile specified with the function of load balance or failover. The profiles configured here will be selected in the field of **WAN>>Default Route** page.

Dray Tek	Vigor 39	00 Series	15:15:44	Login	: Admin	Ð
	WAN >> Load Balance	e >> Pool				
Auto Logout : 5Min 💌	Pool	Rule				
Quick Start Wizard		(. .				
Online Status	🚯 Add 💙	🕻 Edit 🔟 Delete 🤇	S Refresh			
WAN	Profile	Mode	Interface	Primary Profile	Backup Profile	
General Setup	two	Load_Balance	wan2 1,wan4 1			
Default Route						
Load Balance						
Switch						
LAN						
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						
SSL VPN						
Bandwidth Management						
System Maintenance	4					>
Disanactice						

Each item will be explained as follows:

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

Dray Tek

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

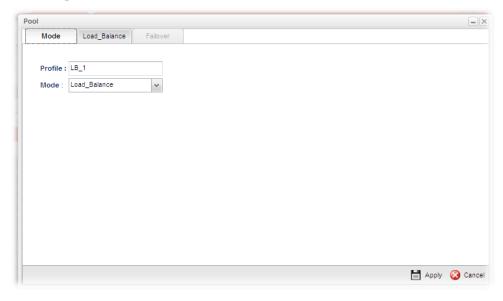
There are two modes, **Load_Balance** and **Failover**, for you to choose as the **Pool** configuration. If you choose **Load_Balance**, the tab of **Load_Balance** will be shown which allows you to configure for different WAN interfaces. If you choose **Failover**, the tab of **Failover** will be displayed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

How to add a Pool profile for Load Balance

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

Pool	Rule	
🚺 Add	🔀 Edit 🛛 🕅 Delete	🔇 Refresh
Profile	Mode	Interface
two	Load_Balance	wan2 1,wan4 1

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





3. Click the **Load_Balance** Tab.

ool		
Mode	Load_Balance Failover	
	🚱 Add 🔚 Save	
	Interface Weight	
	No items to show.	
Interface		
		🛗 Apply 🛛 🥸 Canci

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

Interface	Weight	
wan1	30	m
wan2	60	Ŵ

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

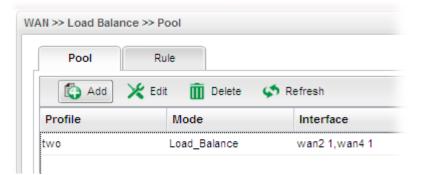
Profile	Mode	Interface
WO	Load_Balance	wan2 1,wan4 1
.B_1	Load_Balance	wan1 30,wan2 60



How to add a Pool profile for Failover

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

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



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

1					-
Mode	Load_Balance	Failover			
Profile :	FL_1				
Mode :	Load_Balance	~			
	Load_Balance				
	Failover				
				EL Appl	y 🐼 Can
				Appl	y 🤯 Ca

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

ol								-
Mode	Load	_Balance	Failove	r				
Primary I	Profile	wan1		~				
Backup P				~				

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

	N		
Mode	Load_Balance	Failover	
			_
Primary Pr	rofile : wan1		~
_	rofile : wan1 ofile : wan3		*

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

Pool	Rule			
🏠 Add 🔰	🗶 Edit 🛛 🔟 Delete	📢 Refresh		
Profile	Mode	Interface	Primary Profile	Backup Pro
two	Load_Balance	wan2 1,wan4 1		
LB_1	Load_Balance	wan1 30		
FL_1	Failover	wan1 30	wan1	wan5

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.

Dray Tek	Vigor 3900	Series 15:32:52	Login: Admin	E
	WAN >> Switch >> 802.1Q V	LAN		
Auto Logout : Off 🛛 👻	802.1Q VLAN Mirr	or Interface Status		
Quick Start Wizard				
Online Status	🔇 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				
Disquastics				

802.1Q VLAN Configuration

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



This page simply displays aurre	nt status of 802 10 VALN satting profiles	
This page simply displays curre	ent status of 802.1Q VALN setting profiles.	

02.1Q VLAN M	irror Interface	Status		
🔇 Refresh				
/LAN ID	Men	nber	Untag	
0	CPU,V	VAN1	WAN1	
1	CPU,V	VAN2	WAN2	
2	CPU,V	VAN3	WAN3	
3	CPU,V	VAN4	WAN4	
4	CPU,V	VAN5	WAN5	

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

Mirror Configuration

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

Dray Tek	Vigor 3900 Series	15:34:49	Login: Admin	Ð
	WAN >> Switch >> Mirror			
Auto Logout : Off 🛛 👻	802.10 VLAN Mirror Interface	Status		
Quick Start Wizard				
Online Status	Enable This Profile			
WAN	Mirroring Port : WAN1	~		
General Setup				
Default Route	Mirrored Port : WAN2	*		
Load Balance				
Switch				
LAN				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management			Apply	🐼 Cancel
System Maintenance			- Abbil	-

Item	Description					
Enable This Profile	Check the box to enable the Mirror function for the switch.					
Mirroring Port	Select a port for the administrator to use for viewing traffic sent from mirrored ports.					
Mirrored Port	Select a port to make the packets passing through it monitored by the administrator.					
	Mirroring Port :	VVAN1	~			
	Mirrored Port :	WAN2	~			
		WAN1				
		WAN2				
		WAN3				
		VVAN4 VVAN5				
		CPU				
Apply	Click it to save the	configuration.				
Cancel	Click it to discard t	he 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.

Dray Tek	vigor 3	900 Series	15:36:22	Login: Admin	Ð
	WAN >> Switch >>	Interface			
Auto Logout : Off 🛛 👻	802.10 VLAN	Mirror Interface	Status		
Quick Start Wizard					
Online Status	🔀 Edit	Kofresh			
WAN	Interface	Enable This Profil	e Duplex	Speed	
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					
Bandwidth Management					
System Maintenance					
Disapactics					

Item	Description				
Edit	Choose the interface listed below and click the Edit button to modify the settings. A pop up window will appear for you to change the settings.				
	Interface : WAN1 Enable This Profile Duplex : Full Speed : Auto				
	 Apply Q Cancel Interface – Display the name of WAN interface. Enable This Profile – Check it to enable such interface. Duplex – Use the drop down list to choose the duplex (Full or Half) for such profile. 				
	Speed – Use the drop down list to specify the transmission rate (Auto, 10M, 100M or 1000M) for such interface.				
	Apply – Click it to save and exit the dialog.				
	Cancel – Click it to exit the dialog without saving anything.				
Refresh	Renew current web page.				
Interface	Display the name of the WAN port on the router.				
Enable This Profile	Display the status of the profile. False means disabled; True				



	means enabled.
Duplex	Display the duplex used (full or half) by such profile.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.

Status of the Switch

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

Dray Tek	Vigor 39				Đ
0#	WAN >> SWITCH >> State	us			
uto Logout : Off	802.1Q VLAN	Mirror Interface	Status		
Quick Start Wizard	C Refresh	Auto Re	fresh: 10 Seconds 🗸		
Online Status	-				
WAN	Interface	Status	Speed	Duplex	
General Setup	WAN4	Up	1000M	Full	
Default Route	WAN5	Down	1000M	Full	
Load Balance	CPU	Up	1000M	Full	
Switch					
LAN					
NAT					
Firewall					
Objects Setting					
User Management					
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 Refresh button is clicked.
Interface	Display the physical port of the WAN interface.
Status	Display if the port connection for WAN interface is linked or not. Up means the network is connected; Down means the network is not connected.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such WAN interface.
Duplex	Display the duplex used (full or half) by such WAN interface.

4.2 LAN

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

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

AN
General Setup
IP Routing
Static Route
Switch
Bind IP to MAC
RIP Configuration
OSPF Configuration

4.2.1 General Setup

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

General Setup

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

Dray Tek		Vigor 3	900 Se	ries 15	:56:51	Login: Ac	lmin	Đ
		LAN >> General Se	tup >> General	Setup				
uto Logout : Off 🛛 👻		General Setup	DHCP	DHCP Relay RAI	DVD DHCP	v6		
Quick Start Wizard	^	Add	Edit 🕅	Delete 🔇 Refresh				
Online Status								_
WAN		Profile	Enable Thi	s Profile Description	VLAN ID	IPv4 Protocol	IPv6 Protocol	
LAN		lan1	true		10	static	Link-Local	
General Setup		lan100	true		100	static	Link-Local	
IP Routing		1	true		1	static	Link-Local	
Static Route								
Switch	=							
Bind IP to MAC								
RIP Configuration								
OSPF Configuration								
NAT								
Firewall								
Objects Setting								
User Management								
Applications								
VPN and Remote Access								
Certificate Management								
	-	4						>

Each item will be explained as follows:

Item	Description
Add	Add a new LAN profile.

Dray Tek

Edit	Modify the selected LAN profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected LAN profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page
Profile	Display the name of the LAN profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Description	Display the brief explanation for the LAN profile.
VLAN ID	Display the VLAN ID configured for the LAN profile.
IPv4 Protocol Type	Display the IPv4 protocol type for the LAN profile.
IPv6 Protocol Type	Display the IPv6 protocol type for the LAN profile.

How to add a new LAN profile

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

General Setup	DHCP	DHCP Relay	RADVD	DHCPv6
🏠 Add 💙	🗶 Edit 🛛 🔟	Delete 🛛 📢 Ref	íresh	
Profile	Enable Th	nis Profile Descrip	otion VI	AN ID

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

Profile :	lantest				
Enable This Profile		_			
Description :	Just for test	(Optional)			
VLAN ID :	0				
Default MAC Address :	💿 Enable 🔘 Disable				
MAC Address :	00 : 50 : 7f :	e7 : cb	: 20		
IPv4 Protocol :	static				
Mode :	NAT				
IP Address :	0.0.0	0			
Subnet Mask :	255.255.255.0				
Gateway IP Address :			(Optional)		
	🏠 Add 🛗 Save				
	IP		Subnet Mask	Mode	
			No items to show.]
	1				

Item	Description
Profile	Type the name of the LAN profile.
Enable This Profile	Check this box to enable such profile.
Description	Type the description for the new LAN profile.
VLAN ID	Type a number as the VLAN ID to make the data be identified while performing data transmission.
Default MAC Address	Enable – Click it to enable the default MAC address for such profile.
	Disable – Click it to type the MAC address manually for such profile.
MAC Address	If Default MAC address is disabled, please specify a MAC address from the drop down list for such profile.
IPv4 Protocol	Display the type for the IPv4 protocol for such profile.
Mode	Choose NAT or ROUTING as the operation mode for such profile.
IP Address	Type the IP address of the router for the LAN profile.
Subnet Mask	Use the drop down list to choose a suitable mask for the LAN profile.
Gateway IP Address	Such IP address is ready for matching with the function of Virtual System. — click the icon to clear the IP setting.
2 nd Subnet	Specify one 2 nd subnet which might be needed in the future.



	<i>c</i> D								
	🚯 Add 🔚 Save								
	IP 192.168.1.83	Subnet Mask Mode 255.255.255.0 NAT	â						
		255.255.255.0 V NAT							
		255.255.255.0	× <u> </u>						
	Add – Click it to add a	new subnet mask with	IP address and						
	specified mode.								
	Save – Click it to save t	he settings.							
	IP – Type the IP addres	s if you click Add for	adding a new						
	entry.		-						
	Subnet Mask – Use the	e drop down list to cho	pose the one						
	you want.								
	Mode – Specify NAT o	r Routing as the mode	2.						
	\mathbf{I} – click the icon to remove the selected entry.								
IPv6 Protocol	It defines the IPv6 connection types for LAN interface. Possible types contain Link-Local, Static and DHCP-SLA. Except Link-Local, each type requires different parameter settings.								
	Link-Local - Link-Local address is used for communicative with neighbouring nodes on the same link. It is defined by the address prefix fe80::/10 . You don't need to setup Link-Local address manually for it is generated automatically according to your MAC Address.								
	Static – This type allows LAN.	s you to setup static II	v6 address for						
	DHCP-SLA - DHCPv6 option of DHCPv6 proto server.		_						
IPv6 Address	If Static is chosen as IPv6 Protocol, please type the IPv6 address in this field.								
IPv6 Prefix Length	Display the IPv6 prefix	length.							
DHCPv6 SLA WAN Interface	If DHCP-SLA is chosen of the WAN profiles in		ease choose one						
DHCPv6 SLA ID	The ID number set here to create its own local ac subnets.	•	•						
	sublicts.								
Apply	Click it to save and exit	the dialog.							

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

General Setup	DHCP DHCP	Relay RADVD	DHCPv6		
🚺 Add	Edit 👖 Delete	< Refresh			
Profile	Enable This Profile	Description	VLAN ID	IPv4 Protocol	IPv6 Protocol
Profile an1	Enable This Profile	Description	VLAN ID	IPv4 Protocol static	IPv6 Protocol Link-Local

DHCP

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

Dray Tek		vigo	r3900) Seri	e <i>s</i>	16:0	2:10		Login: A	dmin	E
		LAN >> Gene	ral Setup >> D	нср							
Logout : Off		General S	Setup D	HCP	DHCP Relay	RADV	D Di	HCPv6			
Quick Start Wizard	*	× E	dit 🔇 Ref	ree h		11	11				
Online Status	_										
WAN		Profile	Enable Thi		End IP	DNS	Routers	Lease Tim			Remote Di
LAN		lan1	true	192.168.1	192.168.1	8.8.8.8		86400	Disable	192.168.1	192.168.1
General Setup		lan100	true	192.168.1	192.168.1			86400	Disable	192.168.1	192.168.1
IP Routing		1	true	192.168.3	192.168.3			86400	Disable	192.168.3	192.168.3
Static Route		lantest	true	0.0.0.10	0.0.0.195			86400	Disable	0.0.0.196	0.0.0.245
Switch	-										
Bind IP to MAC											
RIP Configuration											
OSPF Configuration											
NAT											
Firewall											
Objects Setting											
User Management											
Applications											
VPN and Remote Access											
Certificate Management											
	-										

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

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

How to edit a LAN profile for DHCP

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

- 🗶 E	🔀 Edit 🛛 🗇 Refresh								
Profile	Enable Thi	Start IP	End IP	DNS	Routers	Lease Tim	Specify Re	Remote Di	Remote Di
lan1	true	192.168.1	. 192.168.1	168.95.1.1		86400	Disable	192.168.1	192.168.1
lantest	true	0.0.0.10	0.0.0.195			86400	Disable	0.0.0.196	0.0.0.245

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

P	
Profile :	lantest
Start IP :	0.0.10.
End IP :	0 . 0 . 195
	🕼 Add 🔚 Save
	DNS
DNS :	No items to show.
Routers :	(Optional)
Lease Time :	86400 Seconds
Specify Remote Dial-in	IP : 🔘 Enable 💿 Disable
	🗎 Apply 🙆 Can

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



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

- 4. When you finish the above settings, please click **Appl**y to save the configuration and exit the dialog.
- 5. The LAN profile has been edited.

DHCP Relay

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

Auto Logout: Off Quick Start Wizard Online Status WAN LAN General Setup ILAN General Setup IP Routing Static Route Switch Bind IP to MAC RIP Configuration OSPF Configuration Objects Setting User Management Applications VPN and Remote Access Certificate Management Applications	Dray Tek	Vigor 3900 s	Series 16	:05:42 I	Login: Admin	Ð
VPN and Remote Access Certificate Management	Auto Logout : Off v Quick Start Wizard Online Status WAN LAN General Setup IP Routing Static Route Switch Bind IP to MAC RIP Configuration OSPF Configuration NAT Firewall Objects Setting	LAN >> General Setup >> DHCP General Setup DHCP Edit Setup DHCP Profile lan1 lan100 1	Relay DHCP Relay RAD Enable This Profile false false false	DHCPv6		
	VPN and Remote Access Certificate Management					

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

	rule.	
Refresh	Renew current web page.	
Profile	Display the name of the LAN profile.	
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.	
DHCP Server Location	Display the LAN or WAN profile for the DHCP server.	
DHCP Server IP	Display the IP address of DHCP server.	

How to edit a LAN profile for DHCP Relay

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

General Setup	DHCP	DHCP Relay	RADVD	DHCPv6	
🔀 Edit 🛛 🖨	Refresh				
Profile		Enable This Profi	le	DHCP Server Location	DHCF
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.

ICP Relay		-
Profile :	lantest	
👿 Enable This Pre	file	
DHCP Server Loca	tion: lantest15	
DHCP Server IP :]
	E A	oply 🙆 Cancel

Available parameters are listed as follows:

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
DHCP Server Location	Type the LAN or WAN profile for the DHCP server
DHCP Server IP	Type the IP address of DHCP Server.
Apply	Click it to save and exit the dialog.

Dray Tek

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 DHCP Relay RAD	VD DHCPv6	
🔀 Edit – 🐼 Re	efresh		
Profile	Enable This Profile	DHCP Server Location	DHCP Server IP
lan1	false		
lantest	true	lantest15	192,168,1,90

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.

Dray Tek		Vigor 3900			
		LAN >> General Setup >> RA	DVD		
ito Logout : Off 🛛 👻		General Setup DH	CP DHCP Relay RADV	DHCPv6	
Quick Start Wizard	-	💥 Edit 🗳 Refre	-h		
Online Status	_				
WAN		Profile	Enable This Profi	le Advertiseme	nt Lifetime
LAN		lan1	false	30	
General Setup		lan100	false	30	
IP Routing		1	false	30	
Static Route		lantest	false	30	
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					

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

Profile	Display the name of the LAN profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
Advertisement Lifetime	Display the lifetime value. The lifetime associated with the default router in units of minutes, ranging from $10 \sim 150$. 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.

General Setup	DHCP	DHCP Relay RADV		
🔀 Edit 🛭 🗲	Refresh			
Profile		Enable This Prof	ïle	Advertisement Lifetime
lan1		false		30
lantest		false		30

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

IIIani IDVD	Taise	
Profile :	lantest	
📝 Enable This Pr	ofile	
Advertisement Li	fetime : 30	
		📄 Apply 🛛 🙆 Cancel

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
Advertisement Lifetime	Type a value for advertisement lifetime. The lifetime associated with the default router in units of minutes, ranging from $10 \sim 150$. 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.
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 DHCF	DHCP Relay RADVD D	HCPv6
🔀 Edit 🛛 🖨 Refresi	n	
Profile	Enable This Profile	Advertisement Lifetime
lan1	false	30
lantest	true	30

DHCP6

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

Dray Tek	Vigo	r 3900 Series	16:08:33	Login: Admin	Ð
	LAN >> Gene	ral Setup >> DHCPv6			
Auto Logout : Off 🛛 👻	General S	Setup DHCP DHCP Relay	RADVD DHCPv6		
Quick Start Wizard	× E	dit 🔇 Refresh			
Online Status		-			
WAN	Profile	Enable This Start IP	End IP	D	NS
LAN	lan1	faise			
General Setup	lan100	false			
IP Routing	1	false			
Static Route	lantest	false			
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
					>

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

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

How to edit a LAN profile for DHCPv6

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

General Setup	DHCP DHCP Relay	RADVD	DHCPv6	
🔀 Edit 🛭 🗲	Refresh			
Profile	Enable This Profile	Start IP	End IP	DNS
Profile lan1	Enable This Profile	Start IP	End IP	DNS

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

DHCPv6				-×
Profile :	lan1 • This Profile			
Start IP :	2000::10			
End IP :	2000::ff			
	🏠 Add 🛗 Save			
	DNS			
	2000::2	Ē		
DNS :				
			-	
			💾 Apply 🔞 C	ancel

Item	Description
Profile	Display the name of the LAN profile.
Enable This Profile	Check this box to enable this profile.
Start IP	Set the starting IP address of the IP address pool for DHCP server. The format the IP address shall be similar to the



	following example:
	2000:0000:0000:0000:0000:0000:10 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.
	DNS
	2000::2
	DNS :
	Add – Click it to add a new IP address for DNS server.
	Save – Click it to save the setting.
	\mathbf{I} – click the icon to remove the selected entry.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

- 3. When you finish the above settings, please click **Appl**y to save the configuration and exit the dialog.
- 4. The LAN profile has been edited.

LAN >> General Setup >> DHO	CPv6			
General Setup DHCI	DHCP Relay RADV	DHCPv6		
🔀 Edit 🗳 Refresi	ı			
Profile	Enable This Profile	Start IP	End IP	DNS
lan1	true	2000::10	2000::ff	2000::2

4.2.2 IP Routing

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

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

Dray Tek	Vigor 3900	Series 16	:09:51	Login: Ad	min 🕞
Auto Logout : Off Quick Start Wizard Online Status WAN LAN General Setup IP Routing Static Route Switch Bind IP to MAC RIP Configuration OSPF Configuration NAT Firewall Objects Setting User Management Applications VPN and Remote Access	LAN >> IP Routing IP Routing	🔟 Delete 🗳 Refresh ble This Profile WAll Profile	(β Rename LAN Profile items to show.	IP	Mask
Certificate Management	4	m			
< [Ш))

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



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

How to add a new IP Routing profile

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

IP Routing			
🚯 Add	🔀 Edit	前 Delete	娕 Refres
Profile	Enabl	e This Profik V	VAN Profile

3. The following dialog will appear.

Profile :	Routingtest1		
📝 Enable Ti	nis Profile		
WAN Profile	: wan1	~	
LAN Profile	lan1	*	
IP :	192 . 168 . 1	. 34	
Mask :	255.255.255.0	~	

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

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

IP Routing						
🚯 Add	🔀 Edit 🛛	<u> Î</u> Delete	< Refresh	🔓 Rename		
Profile	Enable	This Profile	WAN Profile	LAN Profile	IP	Mask
Routingtest1	true		wan1	lan1	192.168.1.34	255.255.255.0

4.2.3 Static Route

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

Static Route

Dray Tek	Vigor 3900	Series	16:10:54	Login: A	Admin 🕞
	LAN >> Static Route >> Stat	c Route			
Auto Logout : Off	Static Route IPv6 Sta	ic Route Inter-LAN Route			
Quick Start Wizard	🕼 Add 🔀 Edit	m Delete 🔇 Refre	sh 🕻 Rename		
Online Status					
WAN	Profile Enable	This Pro Destination IP A	Subnet Mask Ga	teway WAN/LAI	V Profile Metric
LAN	vincent true	172.17.3.70	255.255.255.255 172	2.16.2.4 wan4	
General Setup	3 faise	172.17.3.0	255.255.255.0 172	.16.2.4 wan4	
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	4				>
	p. q				

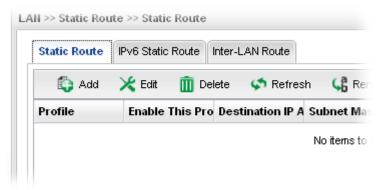
Item	Description	
Add	Add a new static route setting.	
Edit	 Modify the selected static route setting. To edit static route setting, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule. 	
Delete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



Profile	Display the name of such static route.	
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.	
Destination IP Address	Display the IP address for such static route profile.	
Subnet Mask	Display the subnet mask for such static route profile.	
Gateway	Display the gateway address for such static route profile.	
WAN/LAN Profile	Display the subnet / LAN or WAN profile of the gateway.	
Metric	Display the distance to the target.	

How to add a new Static Route profile

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



3. The following dialog will appear.

Static Route			_ ×
Profile : Inable This Profile	vincent		
Destination IP Address :	172 17	3	70
Subnet Mask :	255.255.255.255	*	(Optional)
Gateway:	172 . 16 .	2.	4
WAN/LAN Profile :	wan4	~	
Metric			(Optional)
			💾 Apply 🛛 😡 Cancel

Item	Description	
Profile	Type the name of the static route profile.	
Enable This ProfileCheck 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. LAN >> Static Route >> Static Route

Static Route	IPv6 Stat	ic Route	Inter-LAN Ro	ute			
🕼 Add 🔀 Edit 📺 Delete 🔊 Refresh 🛛 🧯 Rename							
Profile		Enable 1	This Profile	Destination IP Address	Subnet Mask	Gateway	WAN/LAN Profile
vincent		true		172.17.3.70	255.255.255.255	172.16.2.4	wan4
3		true		172.17.3.0	255.255.255.0	172.16.2.5	wan4

IPv6 Static Route

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

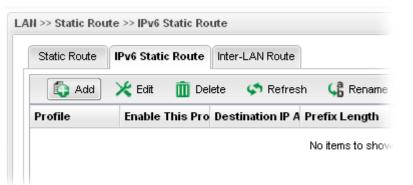
Dray Tek		Vigor 3900 Series	16:12:34	Login: Admin	E
		AN >> Static Route >> IPv6 Static Route			
Auto Logout : Off	1	Static Route IPv6 Static Route Inter-LA	N Route		
Quick Start Wizard					
Online Status		🕼 Add 🔀 Edit 🔟 Delete 🔇	S Refresh 🔓 Rename		
WAN		Profile Enable Destination IP Address	Prefix I Nexthop	WAN/L/ M	letric
LAN			No items to show.		
General Setup					
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		4			•

Each item will be explained as follows:

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

How to add a new IPv6 Static Route profile

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



3. The following dialog will appear.

Enable This Profile		
Destination IP Address : fc2	0::1	
Prefix Length : 64		
Nexthop : fc0	0::2	
WAN/LAN Profile : lar	1 👻	
Metric		(Optional)

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



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

LAN >> Static Route >> IPv6 Static Route

🚺 Add	×	Edit 🛛 前 Del	ete 🛭 🗳 Refresh 🛛 📢 Rename		
Profile		Enable This P	rofile Destination IP Address	Prefix Length	Nexthop
internal		true	fc20::1	64	fc00::2

Inter-LAN Route

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

Dray Tek	Vigor 3900 Series 16:13:48 Login: Admin	E
	LAN >> Static Route >> Inter-LAN Route	
Auto Logout : Off 🛛 👻	Static Route IPv6 Static Route Inter-LAN Route	
Quick Start Wizard		
Online Status	Enable This Profile	
WAN		
LAN		
General Setup		
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	📑 Apply	🐼 Cancel
		_ •
<		>

4.2.4 Switch

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

802.1Q VLAN

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

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

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

Dray Tek		Vigor 3900 Serie	s 16:14:19	Login: Admin	Ð
	L	AN >> Switch >> 802.1Q VLAN			
ito Logout : Off 🛛 👻		802.1Q VLAN Mirror In	terface Status		
Quick Start Wizard	<u>_</u>				
Online Status		🚯 Add 🔀 Edit 🛅 Delet	ie 🔇 Refresh		
WAN		VLAN ID	Member	Untag	
LAN		10	LAN1,LAN2,LAN3	LAN1,LAN2,LAN3	
General Setup		100	LAN1,LAN2		
IP Routing		1	LAN1,LAN2,LAN3		
Static Route					
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management		4			>
SCI VDN	-	21			

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



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

How to add a new 802.1Q VLAN profile

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



3. The following dialog will appear.

	15		
VLAN ID:	15		
Member :	LAN3	~	
Untag :		~	

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

	Internet for such LAN profile with the VLAN ID number.
Untag	Determine if the packets transmitted to Internet through such LAN profile with the VLAN ID number is tagged or not.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

302.1Q VLAN Mirror	Interface Status	
🏠 Add 🔀 Edit 🛅	Delete 🗳 Refresh	
/LAN ID	Member	Untag
0	LAN1,LAN2,LAN3	LAN1,LAN2,LAN3
00	LAN1,LAN2	
	LAN1,LAN2,LAN3	
5	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.

Dray Tek	Vigor 3900 Series	16:17:39	Login: Admin	Ð	^
Auto Logout : Off Quick Start Wizard Quick Start Wizard Online Status WAN LAN General Setup IP Routing Static Route Switch Bind IP to MAC RIP Configuration OSPF Configuration	Vigor 3900 Series	16:17:39	Login: Admin		
OSPF Coniguration NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management cs: vnu			🗎 Apply 🔇	Cancel	~



Available parameters are listed as follows:

Item	Description		
Enable This Profile	Check the box to enable the Mirror function for the switch.		
Mirroring Port	Select a port to view traffic sent from mirrored ports.		
Mirrored Port	CPU 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.

	/igor3900				
Auto Logout : Off 🗸 🗸					
Quick Start Wizard	802.1Q VLAN Mirr	or Interface Sta	tus		
Online Status	🔀 Edit 🛛 🐼 Refr	esh			
WAN	Interface	Enable This Profile	Duplex	Speed	
LAN	LAN_Port_1	true	Full	Auto	
General Setup	LAN_Port_2	true	Full	Auto	
IP Routing	LAN_SFP	true	Full	Auto	
Static Route					
Switch					
Bind IP to MAC					
RIP Configuration					
OSPF Configuration					
NAT					
Firewall					
Objects Setting					
User Management					
Applications					
VPN and Remote Access					

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

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

How to edit an Interface profile

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

802.1Q VLAN M	irror Interface	Status
🔀 Edit 🛛 🐼 R	efresh	
Interface	Enable This F	Profile Duplex
LAN1	true	Full
LAN2	true	Full
LAN3	true	Full
CPU	true	Full

3. The following dialog will appear.

Interface	: LAN3		
📝 Enable	e This Profile		
Duplex :	Full	~	
Speed :	Auto	~	

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



Duplex	Use the drop down list to choose the duplex for such profile.
Speed	Use the drop down list to specify the transmission rate for such profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

Status

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

	LAN >> Sv	vitch >> Status				
Auto Logout : Off 🛛 🗸	802.10	VLAN Mirror	Interface Status			
Quick Start Wizard		Refresh	Auto Refresh : 1	0 Seconds 🗸		
Online Status						
WAN	Interfa	ice	Status	Speed	Duplex	
LAN	LAN1		Up	1000M	Full	
General Setup	LAN2		Up	100M	Full	
IP Routing	LAN3		Down	1000M	Full	
Static Route	CPU		Up	1000M	Full	
Switch						
Bind IP to MAC						
RIP Configuration						
OSPF Configuration						
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access						
Certificate Management						

Each item will be explained as follows:

Item	Description
Refresh	Renew current web page.
Auto Refresh	Specify the interval of refresh time to obtain the latest status. The information will update immediately when the Refresh button is clicked.
Interface	Display the profile name of the interface.
Status	Display the status (up or down) for the interface.
Speed	Display the transmission rate (10M, 100M, 1000M or Auto) of the date for such profile.
Duplex	Display the duplex used (full or half) by such profile.

4.2.5 Bind IP to MAC

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

Dray Tek	Vigor 3900	Series 16:2	2:50	Login	: Admin	Ð
Auto Logout: Off V Quick Start Wizard Image: Constraint of the status Image: Constraint of the status WAN LAN General Setup IP Routing Static Route Static Route Switch E Bind IP to MAC RIP Configuration OSPF Configuration NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management Certificate Management Certificate Management Vertificate Management	LAN >> Bind IP to MAC Bind IP to MAC Mode : Enable ARP Table IP 192.168.139.10 192.168.139.80 1	Select All MAC Address 00:10:60:59:0d:1b 00:50:7f:7a:02:eb	Move	Add X Bind Table Profile 192_166_139_10	Edit Deid IP Address 192.168.139.10	
(>

Item	Description
Mode	Enable - Choose it to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
	Disable - Choose it to disable this function. All the settings on this page will be invalid.
	Strict Bind – Choose it to lock the connection of the IP/MAC which is not listed in IP Bind List.
Select All	Allow you to choose all the items listed in ARP Table.
Move	Move the selected item to IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Move on IP Bind List.
	IP Address - Display the IP address of one device.
	MAC Address - Display the MAC address of the device.
Add	It allows you to add one pair of IP/MAC address and display on the table of IP Bind List .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.



Delete	You can remove any item listed in IP Bind List . Simply click and select the one, and click Delete . The selected item will be removed from the IP Bind List .
Select All	Choose all of the selections at one time.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
Rename	Allow to modify the selected profile name.
Bind Table	It displays a list for the IP bind to MAC information.
	Profile - Display the name of the profile.
	IP Address - Display the IP address specified for the profile.
	MAC - Display the MAC address specified for the profile.

How to configure Bind IP to MAC

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

Bind IP t	o MAC		
Mode :	Enable	~	E
ADD T-1	Disable		
ARP Tal	Enable		
IP	Strict_Bind		Idress
102.169	120.10	00-14-60	-50-0-4-4b

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.

N >> Bind IP to MAC					
Bind IP to MAC					
Mode : Enable		ect All 🔹 🔹 Move	🚺 Add 🔀	🕻 Edit 🛛 前 Dele	ete 📑 Sek
ARP Table			Bind Table		
IP	MAC Address		Profile	IP Address	MAC
IP .	in to ridar out				

4. The following dialog appears.

Profile :	Bind_IP1	
IP Address	: 192 . 168 . 1 . 99	
MAC :	00 : 50 : 7F : CA : 8E : 9D	

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.

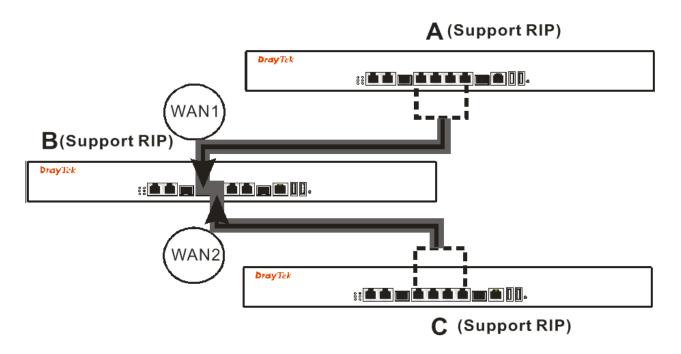
- 5. Enter all the settings and click **Apply**.
- 6. A new profile has been added onto **Bind Table**.

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

4.2.6 RIP Configuration

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

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



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

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

In another direction, C will do the same thing.

Dray Tek	Vigor 3900 Series	16:31:12	Login: Admin	E ^
[LAN >> RIP Configuration			
Auto Logout : Off 🗸 🗸	RIP Configuration			
Quick Start Wizard				
Online Status	Enable This Profile			
WAN	Profile : lan1			
LAN	Profile :	*		
General Setup				
IP Routing				
Static Route				
Switch				
Bind IP to MAC				
RIP Configuration				
OSPF Configuration				
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access			D	
Certificate Management			Apply	🐼 Cancel
				v
<				>

Available parameters are listed as follows:

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

4.2.7 OSPF Configuration

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

Dray Tek	V	igor 390	0 Series	16:33:25	Login: Admin	Ð
	20	>> OSPF Configuratio				
uto Logout : Off 🛛 🗸		SPF Configuration				
Quick Start Wizard		orr conigcitation				
Online Status		Enable This Pro	ofile			
WAN		Enable mistri				
LAN			🚯 Add			
General Setup			LAN Profile	Area		
IP Routing				No items to show.		
Static Route		Profile :				
Switch						
Bind IP to MAC						
RIP Configuration						
OSPF Configuration		l				
NAT						
Firewall						
Objects Setting						
User Management						
Applications						
VPN and Remote Access Certificate Management					Apply	🚫 Cancel
						-



Item	Description	1				
Enable This Profile	Check the b	Check the box to enable the Mirror function for the switch				
Profile	Type a new	name for such pro	file.			
		🚯 Add				
		LAN Profile	Area			
			¥			
	Profile :	lan1 lantest				
		🕼 Add				
		Add LAN Profile	Area 35			
	Profile :	LAN Profile				
Apply		LAN Profile				

Available parameters are listed as follows:

How to add a new profile

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

	🟠 Add			
	LAN Profile		Area	-
		~		
Profile :	lan1 lantest			



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

LAN Profile		Area
lantest	~	30

If you are not satisfied the settings, simply click $\widehat{\mathbf{m}}$ to remove the entry, and then re-type the settings.

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

OSPF Configuration			
🔽 Enable This Pr	ofile		
	🕼 Add		
	LAN Profile	Area	
	lantest	35	m
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 three functions that NAT provides – **Port Redirection**, **DMZ Host** and **Address Mapping**,.

NAT
Port Redirection
DMZ Host
Address Mapping
SIP 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.

Dray Tek	vige	or 390	U Se	ries		0:19:42			ogin: Admin.	e
	NAT >> Por	t Redirection								
to Logout : Off 🛛 👻	Port Re	direction								
Quick Start Wizard			-			. 3				
Online Status		Add 🔀 E	dit 🛄	Delete 🗳	5 Refresh	Ga Rer	name			
WAN	Profile	Enable Th	Interface	Use IP Ali	Alias	Private IP	Protocol	Port Redi	Public Por Public Po	Private Po
LAN	rdp	false	wan2	No		192.168	TCP	One-to-O	3389	3389
NAT	ap800	true	All			192.168	TCP	One-to-O	80	80
Port Redirection	ftp	false	wan4	Single_Al	172.16.2	192.168	TCP/UDP	One-to-O	21	21
DMZ Host	vnc	false	All	No		192.168	TCP/UDP	One-to-O	5900	5900
Address Mapping										
SIP ALG										
Firewall										
Objects Setting										
User Management										
Applications										
VPN and Remote Access										
Certificate Management										
SSL VPN										
Bandwidth Management										
System Maintenance	4									•
Diagnostics										

Item	Description
Add	Add a new port redirect profile.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Interface	Display the WAN interface of this profile.
Source IP	Display the source IP used for this entry.
Private IP	Display the private IP used for this entry.
Protocol	Display the protocol used for the entry
11010001	Display the protocol used for the entry.
Public Port Start	Display the starting number of the public port.
Public Port Start	Display the starting number of the public port.
Public Port Start Public Port End	Display the starting number of the public port. Display the ending number of the public port.

How to add a new Port Redirection profile

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

Port Ree	direct	1					
	Add	×	Edit	Î	Delete	📢 Refr	esh (
Profile	Enab	le T	WAN	Inte	Source I	Private II	Protoc

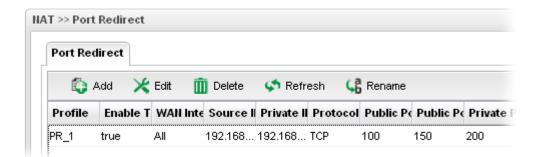
3. The following dialog will appear.

		-
Profile :	PR_1	
📝 Enable This Profile		
Interface :	wan3 🗸	
Use IP Alias :	Single_Alias	
Alias :	~	
Private IP :	192 . 168 . 1 . 66	
Protocol :	TCP/UDP 🗸	
Port Redirection Mode :	Range-to-One	
Public Port Start :		
Public Port End :		
Private Port :		
	Apply	🛛 🚫 Cancel

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

Use IP Alias	Wan1 All Wan1 Wan2 Wan3 Wan4 Wan5 Use the drop down list to select the one you want.
	No Single_Alias All
IP Alias	WAN IP alias that can be selected and used for port redirection. Before using it, please go to WAN>>General Setup and enable the wan1 profile. Add several IP addresses under Static mode for wan1.
Private IP	Specify the private IP address of the internal host providing the service. Simply type the private IP used for this entry.
Protocol	Choose the protocol used for the entry. TCP UDP TCP/UDP
Port Redirection Mode	Specify the direction for the port to be redirected. Range-to-One Range-to-One Range-to-Range
Public Port Start/ Public Port End	Type the starting/ending number of the public port.
Private Port	Specify the private port number of the service offered by the internal host.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

- 4. Enter all the settings and click **Apply**.
- 5. A new profile has been added onto **Port Redirection** table.



4.3.2 DMZ Host

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

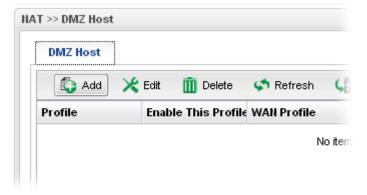
Dray Tek		Vigor 39	00 Series	10:43:42	Login: Ad	dmin	E
	N	IAT >> DMZ Host					
ito Logout : Off 🛛 👻		DMZ Host					
Quick Start Wizard			🖞 Edit 🛛 🕅 Delete 🛛 🔊 Re				
Online Status		🚯 Add 🔀	• • •				
WAN		Profile	Enable This Profile WAN Pro	ofile Private IP	Use IP Alias	IP Alias	
LAN				No items to show.			
NAT							
Port Redirection							
DMZ Host concernences and the							
Address Mapping							
SIP ALG							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Bandwidth Management							
System Maintenance		4	111				•
Disaportice							

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

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

How to add a new DMZ Host profile

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



3. The following dialog will appear.

DMZ Host				-×
Profile :	DMZ_1_RD			
👿 Enable 1	This Profile			
WAN Profile	e : wan1	~		
Private IP :	192 . 168	. 1 . 101		
Use IP Alias	s : 🔿 Enable 💿 🛙	Disable		
IP Alias :		~		
			💾 Apply 🛛 😵	Cancel

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check the box to enable the DMZ Host profile.
WAN Profile	Choose a WAN profile for such entry.
Private IP	Type the private IP used for this entry.
Use IP Alias	Click Enable to invoke IP Alias function.
IP Alias	IP alias that can be selected and used for port redirection. Before using it, please go to WAN>>General Setup and enable the wan1 profile. Add several IP addresses under Static mode for wan1.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

🚯 Add	🔀 Edit	🔟 Delete	< Refresh	ςa	Rename	
Profile	Enab	le This Profile	WAN Profile		Private IP	Use IP Ali
DMZ_1_RD	true		wan1		192.168.1.101	Disable

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.

Dray Tek	Vigor	3900 Series	11:0	1:16	Login: Admin	G	
	NAT >> Address	s Mapping					
o Logout : Off 🛛 👻	Address Ma	apping					
Quick Start Wizard				a _			
Online Status	🚯 Add	🔀 Edit 前 Delete 🔇	Refresh (a Rename			
WAN	Profile	Enable This P WAN Profile	Private IP	Private IP Sub Proto	Use IP Alias	IP Alias	
LAN			No ite	ms to show.			
NAT							
Port Redirection							
DMZ Host							
Address Mapping							
SIP ALG							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Bandwidth Management							
System Maintenance	4						
Disensctice							_

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



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

How to add a new Address Mapping profile

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

Address Ma	pping		
🚯 Add	🔀 Edit 🧵	<u> Î</u> Delete 🔍	🔊 Refresh
Profile	Enable This P	WAN Profile	Private IP

3. The following dialog will appear.

Address Mapping		-×
Profile :	ADO_M_1	
V Enable This Prof	le	
WAN Profile :	wan1 👻	
Private IP :	192 . 168 . 1 . 99	
Private IP Subnet Ma	sk : 255.255.255.255	
Protocol :	All 🗸	
Use IP Alias :	💿 Enable 🔘 Disable	
IP Alias :	87.200.100.15	
	87.200.100.15	

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

Private IP subnet Mask	Type the subnet mask used for this entry.
Protocol	Choose the protocol used for the entry.
	All
	TCP UDP TCP/UDP All
Use IP Alias	Click Enable to invoke IP Alias function.
IP Alias	Select the Alias IP for this Address Mapping profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

- 4. Enter all the settings and click **Apply**.
- 5. A new profile has been added onto **Address Mapping** table.

Address Mapping

🚺 Add	X Edi	t 🔟 Delete 🤇	Refresh 🕻 🔓	Rename		
Profile	1	Enable This Profile	WAN Profile	Private IP	Private IP Subnet Ma	Protoco
ADO_M_1	t	rue	wan1	192.168.1.99	255.255.255.255	All

4.3.4 SIP ALG

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

Dray Tek	Vigor 3900 Series	11:03:55	Login: Admin	Ē
Auto Logout: Off Quick Start Wizard Online Status WAN LAN LAN NAT Port Redirection DMZ Host Address Mapping SIP ALG Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Disagenetice	NAT >> SIP ALG	× ×	Apply	Cancel
<				>

Available parameters are listed as follows:

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

Click **Apply** to save the settings.

4.4 Firewall

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

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

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

Auto Logout : Off Quick Start Wizard Grow DoS Defense MAC Block E Qbjects Setting User Management Applications VPN and Remote Access Certificate Management		URL Filter belete SRefree Enable This false false	10	Comment pass block		
Quick Start Wizard A Online Status WAN LAN NAT Firewall DoS Defense MAC Block E Objects Setting User Management Applications VPN and Remote Access Certificate Management	er Rule Group	elete S Refres Enable This false		pass		
WAN LAN NAT Firewall DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management	· · · · ·	Enable This false		pass		
LAN NAT Firewall DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management	5	false	Profile	pass		
Firewall Filter Setup DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management						
Filter Setup DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management		false		block		
DoS Defense MAC Block Objects Setting User Management Applications VPN and Remote Access Certificate Management						
MAC Block E I I I I I I I I I I I I I I I I I I						
Objects Setting User Management Applications VPN and Remote Access Certificate Management						
User Management Applications VPN and Remote Access Certificate Management		111				•
Applications VPN and Remote Access Certificate Management	er Rules of Selected Group)				
Applications VPN and Remote Access Certificate Management	🕽 Add 🔀 Edit 🕅 D)elete 🗳 Refres	sh 🕻 🧯 Rename	Profile Number Limit: 12		
VPN and Remote Access Certificate Management	Enable This Time F	-	Destination Service	Tur Antina Nor	t Group Syslog	
	Enable This Time P	Profile Source IP	Destination Service	ce typ Action Nex	Group Syslog	
			No items to show.			
SSL VPN						
Bandwidth Management						
System Maintenance						
Diagnostics						
External Dovises						

IP Filter

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

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

IP Filter	Application F		Filter				
IP Filter Rule							
🚺 🖓	🔀 Edit	🔟 Delete	< Refresh	n 🕻 🥵 Rename			
Group			Enable This	Profile	Comment		
			1	No items to show.			
4			111				
	s of Selected	Group	111				
		Group m Delete		n 🕻 Rename Pro	file Number Lim	it : 12	
IP Filter Rule	🔀 Edit		🗳 Refresh	Destination Service 1		it : 12 Next Group	Syslog
	🔀 Edit	m Delete	Source IP				Syslog
IP Filter Rule	🔀 Edit	m Delete	Source IP	Destination Service 1			Syslog
P Filter Rule	🔀 Edit	m Delete	Source IP	Destination Service 1			Syslog
IP Filter Rule	🔀 Edit	m Delete	Source IP	Destination Service 1			Syslog

Each item will be explained as follows:

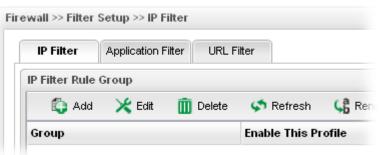
Item	Description
IP Filter Rule Group	
Add	Add a new group profile for IP filter.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete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

Item	Description
Comment	Display the description for such profile.
IP Filter Rule Group of S	elected Group
Add	Add a new IP filter rule profile. Before you create an IP filter rule, you have to create an IP filter group first. Otherwise, you are not allowed to add any IP filter rule here.
Edit	Modify the selected profile. To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Rule	Display the name of the IP filter rule.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
Time Profile	If no time schedule is set, None will be shown in this field.
Source IP	Display the source IP object profile selected for each rule.
Destination IP	Display the destination IP object profile selected for each rule.
Service Type	Display the service type object profile selected for each rule.
Action	Display the action (pass or block) of such rule will use.
Next Group	Display the name for next group selected. If no group is chosen, None will be shown instead.
Syslog	Display the status (enable or disable) of the Syslog function.

How to create an IP Filter group

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

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



3. The following dialog will appear.

Group :	IPF_Marketing	
🔽 Enable	This Profile	
Comment	: used for MKT Dept	

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

- 4. Enter all the settings and click **Apply**.
- 5. A new filter group has been added onto **Address Mapping** table.

IP Filter Application	on Filter URL Filter		
P Filter Rule Group			
🚯 Add 🛛 🔀 Edi	t 🏢 Delete 🗳 Refresh 🛛 🥵 Rena	ame	
Group	Enable This Profile	Comment	
PF_Marketing	true	used for MKT Dept	

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

	plication Filter	URL Filter			
IP Filter Rule Gro	up				
🚯 Add 💙	Edit 🛛 <u> </u>	elete 🛛 🗳 Refresł	n 🕻 🔓 Rena	ame	
Group		Enable This	Profile		Commen
IPF Marketing		true			used for M
4					
IP Filter Rules of	Selected Grou				
IP Filter Rules of			n 🕻 Rens	ame Profile N	umber Lim

7. The following page for configuration will appear.

Rule :	Rule_1			
🔽 Enable This Pr				
Time Profile :	None	~	(
Source IP :	Any	~	(
Destination IP :	Any	~		
Service Type :	Any	~	(
Input Interface :	wan1		~	
Output Interface :	wan3		*	
Fragment :	do_not_care			
Action :	Pass		~	
Next Group :	None		~	
Syslog :	🔵 Enable 🛛 💿 D	isable		

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

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

	System Maintenance >> Syslog / Mail Alert >> Syslog File Syslog Access Setup Syslog File Mail Alert			
Apply	Click it to save and exit the dialog.			
Cancel	Click it to exit the dialog without saving anything.			

- 8. Enter all the settings and click **Apply**.
- 9. A new IP filter rule has been added onto **IP Filter Rules of Selected Group** table.

Group			Enable This Profile			Comment			
PF_Marketin	g		true			used for M	KT Dept		
	s of Selected		111						
🚯 Add	🔀 Edit	🔟 Delete	< Refresh	n 🕻 Rena	me Profile	Number Lir	nit : 12		
Rule	Enable This	Time Profile	Source IP	Destination	Service Type	Action	Next Group	Syslog	
Rule_1	true	None	Any	Any	Any	Pass	None	Disable	

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



Application Filter

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

	Application Filt	er URL	Filter				
🏠 Add	🔀 Edit 🛛 🕅	Delete G	🔊 Refresh 🛛 🔾	Rename			
Profile	Enable This P T	ime Profile	Source IP	Exception IP	IM Block	P2P Block	Protocol Block
			No item	is to show.			

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

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

How to create an Application Filter profile

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

wall >> Filter S	etup >> Applicati	ion Filter		
IP Filter	Application Filter	r URL Filter		
🚺 Add	🔀 Edit 🛛 🔟 D	elete 🛛 🖈 Refr	resh 🛛 🕻 🔓 Rena	me
Profile	Enable This Pre	Time Profile	Source IP	Exception IP
			No item	is to show.
	IP Filter	IP Filter Application Filte	🚯 Add 🔀 Edit ៣ Delete 🗳 Refr	IP Filter Application Filter URL Filter

3. The following dialog will appear.

Profile :	NO_IM	
V Enable This	Profile	
Time Profile :	None 🔽 🏠	
Source IP :	Any 🔽 📢	
Exception IP :	None 🔽 📢	
IM Block :	None 🔽 🏹	
P2P Block :	None 🗸 😜	
Protocol Block	None 🗸 🙀	

Item	Description
Profile	Type the name of the Application filter profile.
Enable This Profile	Check the box to enable this profile.
Time Profile	Choose a schedule profile to be applied on such rule.
	You can click 🔹 to create another new time object profile.
Source IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as source IP.
	You can click 🕼 to create another new IP object profile.
Exception IP	Choose one or more IP object profiles from the drop down list. The selected profile will be treated as exception IP which will not be filtered by the router for such group.
	You can click 🕼 to create another new IP object profile.
IM Block	Choose one or more IM object profiles from the drop down list which will not be allowed to pass through the router.
	You can click 🔹 to create another new IM object profile.
P2P Block	Choose one or more P2P object profiles from the drop down list which will not be allowed to pass through the router.
	You can click 🔹 to create another new P2P object profile.
Protocol Block	Choose one or more Protocol object profiles from the drop down list which will not be allowed to pass through the router.
	You can click 🔹 to create another new protocol object profile.
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

IP Filter	Application Filte	er URL Filter			
🟠 Add	🔀 Edit 🛛 🔟 🕻	Delete 🛛 📢 Ref	iresh 🛛 🕻 Rer	ame	
P. (1)	Enable This Pr	Time Profile	Source IP	Exception IP	IM Bloc
Profile	Linable This Fi				

URL Filter

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

🟠 Ad	d 🔀 Edit	🔟 Delete	🔇 Refresh	⊊a Rename			
Profile	Enable Th	is P Time Prof	file Source I	IP Keyword	Pas Keyword Blo	File Extension	Web Category
face	false	None	Any	None	None	None	face
Use Det	fault Message			• Enable 🔿			
		: y Administratio	n Message :	 	Disable br> br> >Tht %CL% >tantation %CL% >tantation wadministrator fo	en blocked by %	RNAME% Web Co

Each item will be explained as follows:

Item	Description
Add	Add a new group profile for URL filter.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Rename	Allow to modify the selected profile name.
Profile	Display the name of the application filter profile.
Enable The Profile	Display the status of the profile. False means disabled; True means enabled.
Time Profile	If no time schedule is set, None will be shown in this field.
Source IP	Display the source IP object profile selected for each rule.
Keyword Pass	Display the keyword object profile selected for each rule which is allowed to pass through the router.



Item	Description
Keyword Block	Display the keyword object profile selected for each rule which is not allowed to pass through the router.
File Extension Block	Display the file extension object profile selected for each rule which is not allowed to pass through the router.
Web Category Block	Display the web category object profile selected for each rule which is not allowed to pass through the router.
Use Default Message	 Enable – Use the default message to display on the page that the user tries to access into the blocked web page Disable – Type the message manually to display on the page that the user tries to access into the blocked web page.
Default Web Category Administration Message	Such field is available when you disable the function of Use Default Message . The message will display on the user's browser when he/she tries to access the blocked web page.
Apply	Click it to save and exit the dialog.
Cancel	Click it to discard the settings configured in this page.

How to create a URL Filter profile

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

IP Filter	Application Fi	lter URL Filt	ter		
🕼 Add 🔀 Edit 前 Delete 🛭 🛠 Refresh 🛛 📢 Renam					
Profile	Enable This P	Time Profile	Source IP	Keyword	
AP_F_Rule1	true	None	Any	None	

3. The following dialog will appear.

Profile :	Keyword_1		
👿 Enable This Profi	ile		
Time Profile 🗄	None	× 🚯	
Source IP :	Any	× 🚯	
Keyword Pass 🗄	None	× 🔇	
Keyword Block 🗄	None	~ (
File Extension Block	: None	× 🖏	
Web Category Block	: None	× 🚯	

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



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

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

ewall >> Filter	Setup >> URL	Filter					
IP Filter Application Filter URL Filter							
🕼 Add 🔀 Edit 📺 Delete 🔊 Refresh 🛛 🧯 Rename							
Profile	Enable This P	Time Profile	Source IP	Keyword Pas	Keyword Blo	File Extension	Web Category
AP_F_Rule1	true	None	Any	None	None	None	None
Keyword_1	true	None	Any	None	None	None	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.

Switch

Dray Tek	Vigor 3900 Series	11:15:56	Login: Admin	Ð
Auto Logout : Off	Firewall >> DoS Defense >> Switch			
Quick Start Wizard	Broadcast Storm Defense :	🔿 Enable 💿 Disable		
LAN	Multicast Storm Defense : Unknown Unicast Storm Defense :	 Enable Disable Enable Disable 		
Firewall Filter Setup DoS Defense	Unknown Multicast Storm Defense : Storm Filtering Rate :	C Enable ③ Disable		
MAC Block Objects Setting User Management				
Applications VPN and Remote Access				
Certificate Management SSL VPN Bandwidth Management				
System Maintenance Diagnostics			🗎 Apply	🔇 Cancel
External Devises				

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

System

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

Dray Tek	Vigor 3900 s	eries 1	1:17:14	Login: Admin	Ð	^
	Firewall >> DoS Defense >> Syst	em				
Auto Logout : Off 🗸 🗸	Switch System	1				
Quick Start Wizard					A	
Online Status	Enable This Profile					
	Block SYN Flood :	🔵 Enable 💿 Disable				
NAT	SYN Flood Threshold :	300	Packets/Second			
Firewall	SYN Flood Timeout :	10			=	
Filter Setup	Block ICMP Flood :	🔵 Enable 💿 Disable				
DoS Defense and and a second second	ICMP Flood Threshold :	300	Packets/Second			
MAC Block E Objects Setting	ICMP Flood Timeout :	10				
User Management	Block UDP Flood :	🔘 Enable 💿 Disable				
Applications	UDP Flood Threshold :	300	Packets/Second			
VPN and Remote Access	UDP Flood Timeout :	10				
Certificate Management	Block Port Scan :	C Enable (Disable				
SSL VPN						
Bandwidth Management	Port Scan Threshold :	300	Packets/Second			
System Maintenance	Block IR Ontione	🔿 Enshle 🙆 Disshle				
Diagnostics				Apply	🐼 Cancel	
Extornal Doutinon						~
<					>	

Item	Description
Enable This Profile	Check the box to enable this profile.
Block SYN Flood	Click Enable to activate the SYN flood defense function.
	If the amount of TCP SYN packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN packets within the user-defined timeout period.
SYN Flood Threshold	The default setting for threshold is 300 packets per second.
SYN Flood Timeout	The default setting for timeout is 10 seconds.
Block ICMP Flood	Click Enable to activate the ICMP flood defense function.
	If the amount of ICMP echo requests from the Internet exceeds the user-defined threshold value, the router will discard the subsequent echo requests within the user-defined timeout period.
ICMP Flood Threshold	The default setting for threshold is 300 packets per second.
ICMP Flood Timeout	The default setting for timeout is 10 seconds.
Block UDP Flood	Click Enable to activate the UDP flood defense function.
	If the amount of UDP packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent UDP packets within the

Item	Description
	user-defined timeout period.
UDP Flood Threshold	The default setting for threshold is 300 packets per second.
UDP Flood Timeout	The default setting for timeout is 10 seconds.
Block Port Scan	Click Enable to activate the Port Scan detection function. Port scan sends packets with different port numbers to find available services, which respond. The router will identify it and report a warning message if the port scanning rate in packets per second exceeds the user-defined threshold value.
Port Scan Threshold	The default threshold is 300 pps (packets per second).
Block IP Options	Click Enable to activate the Block IP options function. The router will ignore any IP packets with IP option field appearing in the datagram header.
Block Land	Click Enable to activate the Block Land function. A Land attack occurs when an attacker sends spoofed SYN packets with identical source address, destination addresses and port number as those of the victim.
Block SMURF	Click Enable to activate the Block Smurf function. The router will reject any ICMP echo request destined for the broadcast address.
Block Trace Route	Click Enable to activate the Block Trace Route function.
Block SYN Fragment	Click Enable to activate the Block SYN fragment function. Any packets having the SYN flag and fragmented bit sets will be dropped.
Block Fraggle	Click Enable to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet are blocked.
Block Tear Drop	Click Enable to activate the Block Tear Drop function. This attack involves the perpetrator sending overlapping packets to the target hosts so that target host will hang once they re-construct the packets. The routers will block any packets resembling this attacking activity.
Block Ping of Death	Click Enable to activate the Block Ping of Death function. Many machines may crash when receiving an ICMP datagram that exceeds the maximum length. The router will block any fragmented ICMP packets with a length greater than 1024 octets.
Block ICMP Fragment	Click Enable to activate the Block ICMP fragment function. Any ICMP packets with fragmented bit sets are dropped.
Block Unknown Protocol	Click Enable to activate the Block Unknown Protocol function. The router will block any packets with unknown protocol types.
Refresh	Renew current web page.
Apply	Click it to save the configuration.



4.4.3 MAC Block

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



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

How to create a new MAC Block profile

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

MAC Block				
🏠 Add	🔀 Edit	🔟 Delete	📢 Refresh	G b
Profile			Enable This P	rofile

3. The following dialog will appear.

IAC Block		
Profile :	MB_1	
👽 Enable T	is Profile	
MAC Addres	: 00 : 50 : 7F : CA : BE : 9D	

Available parameters are listed as follows:

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

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

5. A new MAC Block profile has been created.

MAC Block				
🚯 Add	🔀 Edit	前 Delete	< Refresh	🔩 Rename
Profile			Enable This Pre	ofile
VIB_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 and time setting. These objects setting profiles can be applied in **Firewall**.

		_
	Objects Setting	
	IP Object	
	IP Group	
_	Service Type Object	_
	Service Type Group	
_	Keyword Object	
	Keyword Group	
	File Extension Object	Ξ
	IM Object	
	P2P Object	
	Protocol Object	
	Web Category Object	
	Time Object	
	Time Group	

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**.

Auto Logout: Off Firewall Objects Setting Objects Setting IP Object Service Type Object Service Type Object Service Type Object Keyword Object Keyword Object Mobject P2 Object P2 Object Time Object Time Object Time Object Time Group User Management Applications	Dray Tek	Vigor 3900	Series 11:	21:59 Login: .	Admin 🕞
Firewall Objects IP Object IP Group Service Type Object Service Type Object Keyword Object Keyword Group File Extension Object IM Object Protocol Object Web Category Object Time Object Time Object Othect Time Object Web Category Object Time Object Web Category Object		C			
Objects Setting IP Object Service Type Object Service Type Group Keyword Object Keyword Object IM Object Protocol Object Web Category Object Time Object User Management Applications VBb and Bemete Access	Auto Logout : Off	IP Object			
Objects Setting IP Object IP Group Service Type Object Service Type Group Keyword Object Iffile Extension Object IM Object Protocol Object Web Category Object Time Object Jose Management Applications	Firewall	🖾 Add 🧏 Edit	🕅 Delete 🗳 Refresh		
IP Object IP Group Service Type Object Service Type Group Keyword Object File Extension Object IM Object P2P Object Protocol Object Time Object Time Object Jime Group User Management Applications	Objects Setting			Start ID Address End ID Addres	e Subnet Maek
Service Type Object Service Type Group Keyword Object Keyword Group File Extension Object IM Object P2P Object Protocol Object Veb Category Object Time Object Time Object Veb Category Object Time Group User Management Applications	needers IP Object neederstaanservaars	Frome	Address Type	Start IF Address	Sa Subiret Maak
Service Type Group Keyword Object Keyword Group File Extension Object File Extension Object P2P Object Protocol Object Web Category Object Time Object Time Group User Management Applications	IP Group				
Keyword Object Keyword Group File Extension Object IM Object P2P Object Protocol Object Web Category Object Time Object Time Group User Management Applications	Service Type Object				
Keyword Group File Extension Object IM Object P2P Object Protocol Object Web Category Object Time Object Time Group User Management Applications	Service Type Group				
File Extension Object File Extension Object IM Object File State St	Keyword Object				
IM Object P2P Object Protocol Object Web Category Object Time Object Time Group User Management Applications VRN and Remate Access	Keyword Group				
P2P Object Protocol Object Web Category Object Time Object Time Group User Management Applications	File Extension Object =				
Protocol Object Web Category Object Time Object Time Group User Management Applications VBN and Remote Access	IM Object				
Web Category Object Time Object Time Group User Management Applications VIDN and Remote Access	P2P Object				
Time Object Time Group User Management Applications VIN and Remote Access	Protocol Object				
Time Group User Management Applications VIN and Remote Access	Web Category Object				
User Management Applications VIN and Remote Accorr	Time Object				
Applications	Time Group				
VDN and Domoto Accore	User Management				
VPN and Remote Access	Applications				
	VPN and Remote Access	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (256) of the object profiles to be created.
Profile	Display the name of the profile.
Interface	Display the category (any, source or destination) of the IP Object.
Address Type	Display the address type (single, range or subnet) for such profile.
Start IP Address	Display the IP address of the starting point for such profile.



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

How to create a new IP Object profile

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

jects Setting >	~ IP Object		
IP Object	🔀 Edit 🛛 前 Delet	e 🗳 Refresh	
Profile	Interface	Address Type	Start IP Addres
		No itr	ems to show.

3. The following dialog will appear.

Profile :	IP_object_1	
Interface :	Source	~
Address Type 🗄	Subnet	~
Start IP Address	192 . 168 . 1	. 78
Subnet Mask 🗄	255.255.255.0	•

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

Item	Description
Address Type	Choose the address type (Single / Range /Subnet) for such profile.
	Range v 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 you choose Range as Address Type .
Subnet Mask	Use the drop down list to choose the subnet mask for such profile if you choose Subnet as Address Type .
Apply	Click it to save and exit the dialog.
Cancel	Click it to exit the dialog without saving anything.

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

IP Object					
🚯 Add	🔀 Edit 🛛 前	Delete 🛛 🗳 R	efresh		
Profile	Interface	Address Type	Start IP Addres	End IP Address	Subnet Mask
IP_object_1	Source	Subnet	192.168.1.78		255.255.255.0
CRM server	Destination	Single	172.16.1.1		

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	Series	11:24:58	Login: Admin	Ð	^
Auto Logout: Off	Dipiects Setting >> IP Group		Refresh Description No items to show.	Objects		
VPN and Remote Access	4		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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Group Name	Display the name of the object group.
Interface	Display the category (any, source or destination) of the IP group.
Description	Display the description for such profile.
Objects	Display the object profiles grouped under such group.

How to create a new IP Group profile

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

IP Group			
C Add	🔀 Edit	<u> (</u> Delete	📢 Refresh
Group Name		Interface	;

3. The following dialog will appear.

Group Name :	IP_Group_1		
Interface :	Source	~	
Description :	Group for Sales	Optional	
Objects :	IP_object_1	~	

Item	Description
Group Name	Type the name of the object group. The number of the characters allowed to be typed here is 10.
Interface	Determine the category (any, source or destination) of this IP group. If the group is set to Source , it will only appear in the field of Source IP on Firewall>>IP Filter Rule . Source Any Source Destination
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the IP object profiles under such group. All the available IP objects that you have added on Objects Setting>>IP Object will be seen here.
Apply	Click it to save the configuration.



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

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

IP Group				
🔯 Add 🛛 🔀 Ed	dit 🔲 Delete 🗳 Refre:	sh		Profile
Group Name	Interface	Description	Objects	
IP_Group_1	Source	Group for Sales	IP_object_1	

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.

Dray Tek	vigor 3	900 Series	11:2		Login: Adm		
	Objects Setting >> S	ervice Type Object					
o Logout : Off 🛛 👻	Service Type Ob	oject					
Firewall	🚯 Add	🗶 Edit 🛛 🕅 Delete	🔇 Refresh				
Objects Setting	Profile	Protocol	Source Port Start	Source Port End	Destination Port S	Destination Port Er	1
IP Object	AUTH	TCP	1	65535	113	113	
IP Group	BGP	TCP	1	65535		179	
Service Type Object	BOOTPCLIENT	UDP	1	65535		68	
Service Type Group	BOOTPSERVER	UDP	1	65535		67	=
Keyword Object	CU SEEME HI	TCP/UDP	1	65535		24032	
Keyword Group		TCP/UDP	1	65535			
File Extension Object	CU_SEEME_LO					7648	
IM Object	DNS	TCP/UDP	1	65535		53	
P2P Object	FINGER	TCP	1	65535		79	
Protocol Object	FTP	TCP	1	65535		21	-
Web Category Object	H_323	TCP	1	65535		1720	
Time Object	HTTP	TCP	1	65535	80	80	
Time Group	HTTPS	TCP	1	65535	443	443	
User Management	IKE	UDP	1	65535	500	500	
Applications	IRC	TCP/UDP	1	65535	6667	6667	-
VPN and Remote Access	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the Delete button.

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

How to create a new Service Type Object profile

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

bjects Setting >>	Service T	ype Object	
Service Type	Object		
🚯 Add	🔀 Edit	前 Delete	📢 Refresh
Profile	Prote	ocol	Source Port St
AUTH	тср		1

3. The following dialog will appear.

Protocol :	TCP	*	
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



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

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

	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	

4.5.4 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.

Dray Tek	Vigor 3900 Series	11:32:27	Login: Admin	Ð
Auto Logout : Off Firewall Objects Setting IP Object IP Group Service Type Object Service Type Group Keyword Object Keyword Group File Extension Object IM Object Protocol Object Veb Category Object Time Object Time Group User Management Applications	Objects Setting >> Service Type Group Service Type Group Add X Edit Delete Group Name	Refresh Description No items to show.	Objects	
VPN and Remote Access		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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Group Name	Display the name of the service type group.
Description	Display the description for such profile.
Objects	Display the service type object profiles grouped under such group.



How to create a new Service Type Group profile

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



3. The following dialog will appear.

Group Name :	Cross_Dept		
Description :	Used for departments	Optional	
Objects :	AUTH	~	

Available parameters are listed as follows:

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

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

Objects Setting >> Service Type Group

Service Type Group					
🏠 Add	🔀 Edit	<u> (</u> Delete	📢 Refresh		Profile
Group Name			Description	Objects	
Cross_Dept			Used for departments	AUTH	

Dray Tek

4.5.5 Keyword Object

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

Each item will be explained as follows	s:
--	----

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



How to create a new Keyword Object profile

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



3. The following dialog will appear.

Keyword Obje	nng >> Keyword Object ct	->
Profile :	K0_1	
	🚯 Add Save	
	Member	
	games 💼	
Member :		
	💾 Ann	ly 🙆 Cancel
		iy 🥁 Cancer

Item	Description
Profile	Type the name of the service type object group. The number of the characters allowed to be typed here is 10.
Member	 Type the content for such profile. For example, type gambling as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings. Add – Type the word in the box of Member and click this button to add the new word as keyword object. Save – Click it to save the setting. Image – click the icon to remove the selected entry.
Apply	Click it to save the configuration.

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

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

Keyword Object		
🖏 Add 🛛 🗶 Edit 🛛 🔟 Delete 🛛 🖍 Refres	h	Profile
Profile	Member	
ко_1	games	

4.5.6 Keyword Group

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

Dray Tek	Vigor 39	00 Series	11:35:55	Login: Admin	E	^
Auto Logout: Off	Objects Setting >> Key	word Group				
Firewall	Keyword Group	Edit <u> </u> Delete	🔇 Refresh			
Objects Setting		Edit III Delete	-	Objects		
IP Object	Group Name		Description	objects		
IP Group			No items to show	v.		
Service Type Object						
Service Type Group						
Keyword Object						
Keyword Group						
File Extension Object						
IM Object						
P2P Object						
Protocol Object						
Web Category Object						
Time Object						
Time Group						
User Management						
Applications						
VPN and Remote Access	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.



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

How to create a new Keyword Group Profile

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

Keyword Group		
🕼 Add 🔀 Edit	前 Delete	🗳 Refresh
Group Name		Description

3. The following dialog will appear.

Group Name :	KG_1		
Description :	first group	Optional	
Objects :	ко_1	~	

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

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

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

Keyword Group		
🖏 Add 🛛 🔀 Edit 🗻 Delete 🛭 🖈 Refresh		Profi
Group Name Description	Objects	
KG_1 first group	KO_1	

4.5.7 File Extension Object

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

Dray Tek	Vigor 39(00 Series	11:37:27	L	ogin: Admin	Ð
	Objects Setting >> File	Extension Object				
Auto Logout : Off	File Extension Obje	ct				
Firewall	🕞 Add 🔀	Edit 前 Delete 🤇	S Refresh			1
Objects Setting	Profile Imag		Audio Java	ActiveX	Compressior Execution	
IP Object			No. 3		•	
IP Group			No items to sho	ow.		
Service Type Object						
Service Type Group						
Keyword Object						
Keyword Group						
File Extension Object 🔤 🗧						
IM Object						
P2P Object						
Protocol Object						
Web Category Object						
Time Object						
Time Group						
User Management						
Applications						
VPN and Remote Access	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile. To delete a rule, simply select the one you want to delete and click the Delete button.

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

How to create a new File Extension Object Profile

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

File Extens	ion Object		
🕼 Ado	l 🔀 Edit	🔟 Delete	\$ 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	~	

Item	Description
Profile	Type the name of the File Extension Object group. The number of the characters allowed to be typed here is 10.
Image	Several file extensions for Image offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Video	Several file extensions for Video offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Audio	Several file extensions for Audio offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Java	Several file extensions for Java offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
ActiveX	Several file extensions for ActiveX offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Compression	Several file extensions for compression offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Execution	Several file extensions for execution offered for you to choose. Use the drop down list to check the box (es) to select the file extension you need.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

n Object						
🔀 Edit	🔟 Delete 🛛 🗲	Refresh				
Image	Video	Audio	Java	ActiveX	Compression	Execution
.bmp,.dib	.mov,.mpe,.mp	.au,.mp3,.m4a	.class,.jad	.alx,.apb,.axs	.ace	.exe,.inf,.pif
	Image	image Video	Kefresh Image Video	X Edit m Delete S Refresh	Kelit Image Video Audio Java ActiveX	Kelit Image Video Audio Java ActiveX Compression

4.5.8 IM Object

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

Dray Tek	Vigor 3900	Series 11:38:40	Login: Admin	Ð
	Objects Setting >> IM Object			
Auto Logout : Off	IM Object			
Firewall	🚯 Add 🔀 Edit	🛄 Delete 🛛 🔇 Refresh		
Objects Setting	Profile	Member	WebIM	
IP Object	Frome	Weinber	WEDIW	
IP Group		No items to a	show.	
Service Type Object				
Service Type Group				
Keyword Object				
Keyword Group				
File Extension Object =				
and an IM Object and a subsequences of the				
P2P Object				
Protocol Object				
Web Category Object				
Time Object				
Time Group				
User Management				
Applications				
VPN and Remote Access	4	111		2
		III		

Each item will be explained as follows:

Item	Description
Add	Add a new profile.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be created.
Profile	Display the name of the IM object profile.
Member	Display the IM application specified in such profile.
WebIM	Display the status of IM object whether including the specified set of web IM or not.

Dray Tek

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
📝 WeblM	
eMessenger	
WebMSN	
Meebo*	
MessengerAdictos	
WebYahoolM	

Item	Description	
Profile		the IM object group. The number of the d 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.

M Object		
🖏 Add 🛛 🔀 Edit 📋	<u>ញ</u> Delete 🛛 📢 Refresh	
Profile	Member	WebIM
vi 1	MSN,QQ,ICQ,ICHAT	enable

4.5.9 P2P Object

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

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

Dray Tek	Vigor 3900	Series 11:39:41	Login: Admin	E)
Auto Logout : Off	Objects Setting >> P2P Object P2P Object	t Îl Delete 🗳 Refresh		
IP Object	Profile	Membe	۲.	
IP Group		No items to show	Γ.	
Service Type Object				
Service Type Group				
Keyword Object				
Keyword Group				
File Extension Object				
IM Object				
P2P Object				
Protocol Object				
Web Category Object				
Time Object				
Time Group				
User Management				
Applications				
VPN and Remote Access 🤤	4	III		•
<				>

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



How to create a new P2P Object Profile

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

P2P Object		-	
🚺 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 Ponkey FastTrack Gnutella BT OpenFT OpenNap Xunlei Varian	
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	e 🧳 Refresh	
Profile			Member
2P_0bj_1			SoulSeek,eDonkey,FastTrack

4.5.10 Protocol Object

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

Dray Tek		Vigor 3900 Seri	ies 11:40:50	Login: Admin	Đ
		Objects Setting >> Protocol Object			
o Logout : Off 🛛 🗸		Protocol Object			
Firewall	-	🕼 Add 🔀 Edit 🏢 De	elete 🛭 📢 Refresh		
Objects Setting		Profile	Member		
IP Object		Tronic	inember		
IP Group			No items to show.		
Service Type Object					
Service Type Group					
Keyword Object					
Keyword Group					
File Extension Object	E				
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
Time Object					
Time Group	-				
User Management					
Applications					
VPN and Remote Access	Ŧ	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (32) of the object profiles to be



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

How to create a new Protocol Object Profile

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

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

3. The following dialog will appear.

otocol Obj	ect	-
Profile :	Proto_Obj_1	
Member	: PostgreSQL, Sybase, [👻	
		📑 Apply 🛛 😣 Cancel

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

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

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

Protocol Object	
🕼 Add 🛛 🗶 Edit 🛛 前 Delete 🛭 娕 Refresh	
Profile	Member
Proto_Obj_1	PostgreSQL,Sybase,DB2

4.5.11 Web Category Object

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

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

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

Web Category Object

Dray Tek		Vigor	3900 Series	11:41:41		Login: Admi	<u> </u>	E
		Objects Setting	>> Web Category Object >> Web	Category Object				
Logout : Off 🗸 🗸		Web Catego	ry Object Content Filter License					
Firewall	~	🚯 Add	🔀 Edit 👖 Delete 🗳 F	Refresh				
Objects Setting		Profile	Child Protection Leisure	Business	Chatting	Computer	Other	
IP Object		face			Chat Instant-M	e Social-Networki	0.0	
IP Group		in the second			onat,instant-in	ooolaritetiionii	''y	
Service Type Object								
Service Type Group								
Keyword Object								
Keyword Group								
File Extension Object	=							
IM Object								
P2P Object								
Protocol Object								
Web Category Object								
Time Object								
Time Group								
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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (16) of the object profiles to be created.
Profile	Display the name of the object profile.
Child Protection	Display the items under certain category that you choose to block for protecting the children.
Leisure	Display the items under certain category that you choose to block.
Business	Display the items under certain category that you choose to block.
Chatting	Display the items under certain category that you choose to block.
Computer	Display the items under certain category that you choose to block.

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

How to create a new Web Category Object Profile

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



3. The following dialog will appear.

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

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

Web Categ	ory Object Content Filte	r License				
🚯 Add	🔀 Edit 🛛 前 Delete	e – 🇳 Ref	resh			
Profile	Child Protectior Lei	sure	Business	Chatting	Computer	Other

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.

		Series		Login: Admin	Ð
	Objects Setting >> Web Catego	ory Object >> Content	Filter License		
uto Logout : Off	Web Category Object Cor	ntent Filter License			
Firewall					
Objects Setting		tivate URL			
IP Object	Enable This Profile : disa				
IP Group		mmtouch 033956			
Service Type Object		12-08-07			
Service Type Group		12-08-14			
Keyword Object					
Keyword Group					
File Extension Object					
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
Time Object					
Time Group					
User Management					
Applications					
				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.



4.5.12 Time Object

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

Dray Tek		Vigor 3	8900 Se	ries	11:45:19		Login: Admi	in	Ð
	0	Objects Setting ≫	> Time Object						
uto Logout : Off 🛛 🗸		Time Object							
Firewall		🚯 Add	🗶 Edit 前	Delete 🛭 📢 Re	fresh				
Objects Setting IP Object		Profile	Frequency	Start Date	Start Time	End Date	End Time	Weekdays	
IP Group					No items to sh	ow.			
Service Type Object									
Service Type Group Keyword Object									
Keyword Object									
File Extension Object									
IM Object									
P2P Object									
Protocol Object									
Web Category Object									
Time Object									
Time Group									
User Management									
Applications									
VPN and Remote Access		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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.					
Delete	Remove the selected profile.					
	To delete a rule, simply select the one you want to delete and click the Delete button.					
Refresh	Renew current web page.					
Profile Number Limit	Display the total number (16) of the object profiles to be created.					
Profile	Display the name of the time object profile.					
Frequency	Display the duration (or period) of the time object profile.					
Start Date	Display the starting date of the time object profile.					
Start Time	Display the starting time of the time object profile.					
End Date	Display the ending date of the time object profile.					
End Time	Display the ending time of the time object profile.					
Weekdays	Display the frequency of such time object profile.					

How to create a new Time Object Profile

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

Time Object	t			
🚯 Add	🛛 🗶 Edit	前 Del	ete 🛛 娕 R	efres
Profile	Frequency	S	Start Date	S

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 🚽	

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
	Ved Ved
	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 🛛 前	Delete 🛛 娕 Re	fresh		
Profile	Frequency	Start Date	Start Time	End Date	End Time
	Weekdays	2010-01-01	00:00:00	2010-01-01	00:00:00

4.5.13 Time Group

This page allows you to group several time object profiles.

Dray Tek		Vigor 3900 s	eries 11:46:15	Login: Admin	E
		Objects Setting >> Time Group			
to Logout : Off 🛛 👻		Time Group			
Firewall	~	🕼 Add 💥 Edit 🧃	Delete 🔇 Refresh		1
Objects Setting			-		
IP Object		Group Name	Description	Objects	
IP Group			No items to s	how.	
Service Type Object					
Service Type Group					
Keyword Object					
Keyword Group					
File Extension Object					
IM Object					
P2P Object					
Protocol Object					
Web Category Object					
Time Object					
Time Group					
User Management					
Applications					
VPN and Remote Access	-	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 Edit 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 rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (8) of the object profiles to be created.
Group Name	Display the name of the group.
Description	Display the brief explanation for such group.
Objects	Display the time objects selected by such group.

How to create a new Time Group Profile

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

Time Group		
ち Add 🔀 Kedit	前 Delete	< Refresh
Group Name		Description
		No iterr

3. The following dialog will appear.

Group Name :	TimeGrp_1]	
Description :	For Market only		Optional	
Objects :	TimeO_1	~]	

Available parameters are listed as follows:

Item	Description
Profile	Type the name of the time group. The number of the characters allowed to be typed here is 10.
Description	Make a brief explanation for such profile if the group name is set not clearly.
Objects	Use the drop down list to check the time object profiles under such group. All the available time objects that you have added on Objects Setting>>Time Object will be seen here. Objects : TimeO_1 TimeO_1
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.

fime Group				
🕼 Add	🔀 Edit	前 Delete	< Refresh	
Group Name			Description	Objects
FimeGrp_1			For Market only	TimeO_1

4.6 User Management

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

User Ma	nagement
Gener	al Setup
User F	Profile
User (Group
RADIU	IS
LDAP	/ Active Directory
Applicat	ions

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.

Dray Tek	Vigor 3	900 Series	11:53:31	Login: Admin	₽
	User Managemen	t >> General Setup >> Gener	ral Setup		Ĩ
Auto Logout : Off	General Setup	User-Based Firewall Status			
NAT					
Firewall	Mode :	Rule-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	🔇 Cancel
Product Registration					
					>

Available parameters will be explained as follows:

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



Item	Description						
	involved.						
	User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.						
	Rule-Based –If you choose such mode, the router will apply the filter rules configured in Firewall>>General Setup and Filter Rule to the users.						
Authentication Type	Under User_Based mode, please specify the authentication type.						
	Mode : User_Based 💌						
	Authentication Type :	Local 🗸					
	White IP List : Local LDAP						
White IP List	Under User_Based mod IP object and/or IP grou	de, use the drop down list to choose p profiles.					
	Mode :	User_Based 🗸					
	Authentication Type :	Local					
	White IP List :	none 🗸					
		None IP_Group_1					

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.

Dray Tek	Vigor 3	900 Se	ries	11:55:10		Login: Admi	in	E>
	User Management	>> General Set	tup >> User-Based	Firewall Status				
Auto Logout : Off	General Setup	User-Based I	Firewall Status					
NAT	🔇 Refresh		Auto Refi	resh : 10 Second	is 👻			
Firewall	User Name	IP	Allow Time	Start Time	End Time	Rest Time	Delete	
Objects Setting								
User Management				No items to sho	ow.			
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								
Product Registration								
								>

Available parameters will be explained as follows:

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



Item	Description	on			
	tus				
	onds Start Time	✓ End Time	Rest Time	Remove	
	2014 40 20 4	6:07:55 2011-10-21 00:0		m	

4.6.2 User Profile

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

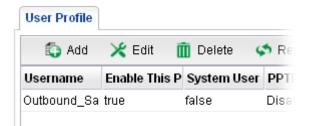
Dray Tek		Vigor		Series		11:57:05		Login	: Admin	E	
		User Manageme	ent >> User P	rofile							
D Logout : Off		User Profile	•								
NAT		👘 🧑 Add	🔀 Edit	🔟 Delete	🧔 Ref	resh					
Firewall		Username	Enable This	System Use	Group	PPTP	L2TP	DHCP from	Static IP Ad	Use mOTP	
Objects Setting		ssi	true	false	User	Disable	Disable	lan1		Disable	-
User Management		vivian	true	true	Admin	Disable	Disable	lan1		Disable	
General Setup		t	true	false	User	Disable	Disable	lan1		Disable	1
User Profile		frankwang	true	false	User	Enable	Enable	lan1		Disable	
User Group		v	true	false	User	Enable	Enable	lan1		Disable	1
RADIUS											-
LDAP / Active Directory											
Applications											
VPN and Remote Access											
Certificate Management											
SSL VPN											
Bandwidth Management											
System Maintenance											
Diagnostics											
External Devices											
Product Registration	-	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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Delete	Remove the selected profile.
	To delete a rule, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile Number Limit	Display the total number (200) of the object profiles to be created.
Username	Display the name of the user.

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

How to create a new User Profile

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



3. The following dialog will appear.

User Profile			-×
Username :	Data_out		
Enable This Profile			
Password :	•••		
Idle Timeout (sec) :	300		
Usage Time (min) :	480		
System User :	false	~	
PPTP :	🔵 Enable 💿 Disable		
L2TP :	🔵 Enable 💿 Disable		
DHCP from :	lan1	~	
Static IP Address :			(Optional)
Use mOTP :	🔵 Enable 💿 Disable		
SSL Proxy :		~	
SSL Application(VNC) :	vnc	~	
SSL Application(RDP) :	rdp	~	
			📑 Apply 😡 Cancel

Item	Description
Username	Type a name for such user profile (e.g., LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B, etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the Username specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Enable This Profile	Check this box to enable such profile.
Password	Type a password for such profile (e.g., <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	If the user is idle over the limitation of the timer, the network connection will be stopped for such user. By default, the Idle Timeout is set to 300 seconds.

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

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

User Profile					
🕼 Add	🔀 Edit 🛛 🚺	👖 Delete 🛛 🥥	🏂 Refresh		
Username	Enable This P	System User	РРТР	L2TP	DHCP from
Outbound_Sa	true	false	Disable	Disable	lan1
Data_out	true	false	Disable	Disable	lan1

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.

Dray Tek	Vigor 3900	Series 13:47:48	Login: Admin	E>
Auto Logout : Off	User Management >> User Gr	roup		
LAN NAT	Add 🔀 Edit	💼 Delete 🗳 Refresh		
Objects Setting User Management	Usergroup	Enable This Profile	Member W.	
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 Product Registration				>
				>

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

How to create a new User Group Profile

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

🕼 Add 🔀 Edit 前 Delete 🔝 Refresh		Jser Group	
😋 Add 🛛 📉 Edit 🔟 Delete 🔊 Reiresh			nta 🦛 Dafrach
Usergroup Enable This Drefile	sergroup Endble mis Prome		

3. The following dialog will appear.

Usergroup	: LAN_UGroup_1	
	This Profile	
Member :	Data_out	
Member	_	

Item	Description
Usergroup	Type the name of such profile.
Enable This Profile	Check this box to enable such profile.
Member	Use the drop down list to check the user profile(s) under such group.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

er Manageme	ent >> User	Group		
User Group				
🚯 Add	🔀 Edit	🔟 Delete	< Refresh	
Usergroup			Enable This Profile	Member
LAN_UGroup	_1		true	Data_out





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.

Auto Logout: Off Auto Logout: Off Auto Logout: Off NAT Image: Composition of the second s	Dray Tek	Vigor 3900 Series	13:49:18	Login: Admin	E
External Devices	LAN 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 Diagnostics	RADIUS Enable This Profile Server IP Address:			
Product Registration				Apply	Cancer

Item	Description
Enable This Profile	Check this box to enable such profile.
Server IP Address	Enter the IP address of RADIUS server.
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Refresh	Renew current web page.
Apply	Click it to save the configuration.

4.6.5 LDAP/Active Directory

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

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

Dray Tek	Vigor 3900	Series 13:51:33	Login: Admin	₽
Auto Logout : Off	User Management >> LDAP / A LDAP / Active Directory Enable This Profile Server IP Address : 17 Port : 38 Base DN : cn	72 . 16 . 2 . 251		
External Devices Product Registration			💾 Apply 🧯	Cancel
<				

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

4.7 Application

Below shows the menu items for Applications.

	Applications
	Dynamic DNS
	GVRP
	UPnP
	High Availability
	Wake on LAN
-	

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.

Dray Tek	Vigor 3900 s	eries 13:54:13	Login: Admin	Ð
	Applications >> Dynamic DNS >>	Status		
o Logout : Off	Status Setting			
NAT	🔇 Refresh	Auto Refresh : 10 Seconds	*	
Firewall	Profile	Status	Domain Name	
Objects Setting	ddns1	Update Success	vkao-3900.no-ip.org	
User Management	ddns2	Not Connected		
Applications	ddns3	Not Connected		
Dynamic DNS	ddns4	Not Connected		
GVRP	ddns5	Not Connected		
UPnP	ddns6	Not Connected		
High Availability	ddns7	Not Connected		
Wake on LAN	ddns8	Not Connected		
VPN and Remote Access	ddns9	Not Connected		
Certificate Management	ddns10	Not Connected		
SSL VPN	dunaro	Not connected		
Bandwidth Management				
System Maintenance				
Diagnostics				
External Devices				
Product Registration				

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

Status

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

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

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.	

Setting

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

🔀 Edit	< Refresh				
Profile	Enable This Prof	WAN Profile	Service Provide	Service Type	Domain Name
dns1	false	wan1	dyndns	Dynamic	
ddns2	false	wan1	dyndns	Dynamic	
dns3	false	wan1	dyndns	Dynamic	
ddns4	false	wan1	dyndns	Dynamic	
idns5	false	wan1	dyndns	Dynamic	
idns6	false	wan1	dyndns	Dynamic	
ddns7	false	wan1	dyndns	Dynamic	
dns8	false	wan1	dyndns	Dynamic	
dns9	false	wan1	dyndns	Dynamic	
dns10	false	wan1	dyndns	Dynamic	

Item	Description
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected rule.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Enable This Profile	Display the status of the profile. False means disabled; True means enabled.
WAN Profile	Display current WAN profile used by such DDNS profile.
Service Provider	Display the name of service provider used by such profile.
Service Type	Display the type for such profile.
Domain Name	Display the domain name of such profile.

How to edit an existing DDNS Profile

There are 10 sets of DDNS server offered for you to modify and configure. Please choose any one of them and click **Edit** to open the following page for modification.

- 1. Open **Applications>>Dynamic DNS** and click the **Setting** tab.
- 2. Simply click the **Edit** button.

Profile :	ddns1			
Enable This Pr				
			1	
WAN Profile :	wan1	*		
Service Provider	: dyndns	~		
Service Type :	Dynamic	~		
Domain Name :]	
User Login Name	:]	
Password :]	
Wild Card 🗄	🔵 Enable 🛛 💿 Dis	sable		
Backup MX 🗄	🔵 Enable 🛛 💿 Dis	sable		
Mail Extender 🗄			Optional	

Item	Description	
Profile	Display the name of the profile.	
Enable This Profile	Check this box to enable such profile.	
WAN Profile	Choose a WAN profile that such profile will apply to.	
Service Provider	Select the service provider for the DDNS account.	
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.	
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.	
User Login Name	Type in the login name that you set for applying domain.	



Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	Type the IP/Domain name of the mail server.
Apply	Click it to save the configuration.
Cancel	Click it to exit the dialog without saving the configuration.

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

Status	Setting				
🔀 Edit	< Refresh				
Profile	Enable This F	Profile WAN Profile	Service Provider	Service Type	Domain Name
ddns1	true	wan1	dyndns	Dynamic	192.168.1.101
ddno2	falce	wan1	dyndins	Dynamic	

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.

Auto Logout: Off LAn NAT Firewall Objects Setting User Management Applications Dynamic Dils GVRP UPnP High Availability VSke on LAli VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices Product Registration	Dray Tek	Vigor 3900 Series	14:04:21	Login: Admin	Ð
LAW GVRP NAT Enable This Profile Objects Setting Interface : User Management Join Time : Applications Join Time : Dynamic DIIS GVRP UPnP High Availability Wake on LAN E VPN and Remote Access E Certificate Management System Maintenance Diagnostics External Devices		Applications >> GVRP			
Firewall Objects Setting User Management Applications Dynamic DNS GVRP UPnP High Availability Wake on LAN VPN and Remote Access Scrtificate Management System Maintenance Diagnostics External Devices	LAIN	GVRP			
User Management Applications Dynamic DNS GVRP UPnP High Availability Wake on LAN VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices		Enable This Profile			
Applications Dynamic DIS GVRP UPnP High Availability Wake on LAN VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices Appy @ Cancel	Objects Setting	Interface :	*		
Dynamic DIIS GVRP UPnP High Availability Wake on LAII VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices	User Management	Join Time : 20	Seconds		
GVRP UPnP High Availability Wake on LAII VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices	Applications				
UPnP High Availability Wake on LAII VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices ▲ Appy & Cancel	Dynamic DNS				
High Availability Wake on LAN VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices	GVRP				
Wake on LAII VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices	UPnP				
VPN and Remote Access E Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices External Devices Appy & Cancel	High Availability				
Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices Apply & Cancel	Wake on LAN				
SSL VPN Bandwidth Management System Maintenance Diagnostics External Devices	VPN and Remote Access				
Bandwidth Management System Maintenance Diagnostics External Devices	Certificate Management				
System Maintenance Diagnostics External Devices	SSL VPN				
Diagnostics Apply Cancel	Bandwidth Management				
External Devices	System Maintenance				
Apply V caller	Diagnostics				
Product Registration	External Devices			Apply	🐼 Cancel
	Product Registration				

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

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

4.7.3 UPnP

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

Dray Tek	Vigor 3900	Series 14	:06:13	Login: Admin	Ð
	Applications >> UPnP				
LAN	UPnP				
NAT Firewall	📝 Enable This Profile				
Objects Setting	Download : 10	024 (🖲 Kbps 🔵 Mbps		
User Management Applications	Upload : 51	12	🖲 Kbps 🔘 Mbps		
Dynamic DNS	External Interface : W	an3 🗸			
GVRP	Internal Interface : lar	n1 🗸			
UPnP	Max Session : 50	10			
High Availability					
Wake on LAN					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Bandwidth Management					
System Maintenance					
Diagnostics					
External Devices				Apply	🙆 Cancel
Product Registration +					

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



Item	Description
Max Session	Determine the maximum session number for UPnP function.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

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

	Broadband	S IF DIVADUNG C	onnection on Rou	iter startis
Network Tasks Image: Constraint of the second	hinet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status:		Connected
	Dial-up	Duration:		00:19:06
See Also 🔹	- test	Speed:		100.0 Mbps
Other Places	Internet Gateway	Activity Internet	Internet Gateway	My Computer
Control Panel W My Network Places	IP Broadband Connection on Router Enabled	Packets: Sent	404	734
🚽 My Computer	LAN or High-Speed Internet	Received:	1,115	666
Details 🔹	Local Area Connection	Properties	<u>D</u> isable	
Network Connections System Folder	Realitek 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.
IP Broadband Connection on Router	(Services
This connection allows you to connect to the Internet through a shared connection on another computer.	 □ Ftp Example ✓ msnmsgr (192.168.29.11:13135) 60654 UDP ✓ msnmsgr (192.168.29.11:7824) 13251 UDP ✓ msnmsgr (192.168.29.11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP Can't work with Firewall Software



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

Security Considerations

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

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

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

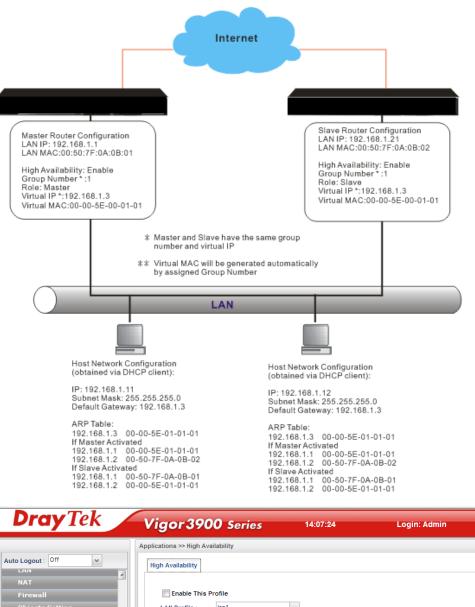
4.7.4 High Availability

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

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

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





-Objects Setting LAN Profile : lan1 ~ User Management 192 139 168 5 Virtual IP : 1 VHID : Dynamic DNS Master v GVRP Role UPnP 🚯 Add 💾 Save High Availabi Peer IP And ID ID Wake on LAN 192,168,139,2 m 1 PN and Remote Acces Certificate Managemen 192.168.139.3 2 m Peer IP And ID Bandwidth Management System Maintena + Diag External Devices 📄 Apply 🛛 🙆 Cancel Product Registration >

Available parameters are listed as follows:

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

Dray Tek

Ð

Item	Description	
LAN Profile	Choose one of applied to.	f the LAN profiles that such function will be
Virtual IP	Assign an IP a	address as a virtual IP.
VHID	It means Virtu function.	al Host ID. Type a number as VHID for such
Role	Select a role f	or this device as Master or Backup.
	Master Backup	~
	If you choose hidden.	Master, the fields of Peer IP and ID will be
	Role :	Master
		🕼 Add 🗎 Save
		Peer IP And ID ID
		No items to show.
	Peer IP And ID :	
	If you choose hidden.	Backup, the field of Peer IP and ID will be
	Role :	Backup
	Peer IP:	
	ID :	
Peer IP	If Master is c the LAN IP ac chosen as the	ddress of the peer side. hosen as the role for Vigor3900, please type ddress of the backup device. If Backup is role of Vigor3900, please type the LAN IP master device.
ID	Type a numbe peer IP.	er value here to represent the privilege of the
Peer IP and ID	• •	several groups of Peer IP and ID for hen it represents the Master device).
Apply	Click it to sav	e the configuration.
Cancel	Click it to disc	card the settings configured in this page.



4.7.5 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.

Dray Tek	Vi	gor 3900	Series	14:09:49	Lo	gin: Admin	EX
	Applica	tions >> Wake on LA	N				
ito Logout : Off 🛛 👻	Wak	e on LAN					
LAN	a	ļ	-				
NAT	Not	e: Wake on LAM	V integrates w	ith Bind IP t	o MAC function,	only binded P	Cs can wak
Firewall							
Objects Setting							
User Management							
Applications							
Dynamic DNS							
GVRP							
UPnP							
High Availability							
Wake on LAN							
VPN and Remote Access							
Certificate Management							
- SSL VPN							
Bandwidth Management							
System Maintenance							
Diagnostics			<u></u>				
External Devices	Wak	e By : () IP Addres	ss 🔘 Mac Address	IP Address :		MAC Address	:
Product Registration	4						•

Item	Description
Configure Bind IP to MAC	Click it to open the setting page of Bind IP to MAC.
Wake by	Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.
IP Address	The IP addresses that have been configured in Firewall>>Bind IP to MAC will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the binded PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.
Delete	Click this button to remove all the settings.

4.8 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

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.

Dray Tek	Vigor 3900 Series 14:17:50 Login: Admi	• 🕞
Auto Logout : Off Firewall Objects Setting	VPN and Remote Access Step 1 Step 2 Type : PPTP IPSec	
User Management Applications	VPN Settings Via : Select From Current Settings Create New VPN Profile	
VPN and Remote Access VPN Client Wizard VPN Server Wizard	Profile Status to2920 enable	
Remote Access Control PPP General Setup IPSec General Setup		
VPN Profiles E VPN TRUNK Management		
Connection Management Certificate Management SSL VPN		
Bandwidth Management System Maintenance		
Diagnostics External Devices	Trevious Next	Einish 🔇 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.

l and Remote A				
Step 1	Step 2			
Туре	PPTP	OIPSec		
		Current Settings	🔿 Create New VPN Profile	
Profile	Status			
	No items to show.			
			🔄 Previous 🛋 Next 📄 Finish 🔇	Car

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

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

and Remote Acces	SS					
Step 1 Step	2					
Туре	PPTP	OIPSec				
VPN Settings Via	🔿 Select From	Current Settings	💿 Create New	VPN Profile		
Profile Name :	VPN_CLI_1					
				Previous	🔖 Next 📃 F	inish 🙆 Cano

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

VPN and Remote Access				
Step 1 Step 2				
Profile : I Enable This Profile	VPN_CLI_1			~
Always On :	💿 Enable 🔿 Disable			
Server IP Address :	172 . 16 . 1	. 10		
PPTP User Name :	pptp_user	(Optional)		
PPTP Password :	••••			
Local IP / Subnet Mask 🗄	192 . 168 . 3	. 55 255.255.255.0	~	E
	🚯 Add 🛗 Save			
	IP	Subnet Mask		
	172 . 6 . 3	. 98 255.255.255.0	▼	
Remote IP / Subnet Mask :				
				-
			🐴 Previous 🛋 Nex	t 📑 Finish 🔞 Cancel

Item	Description	
Profile	Display the name of the VPN profile.	

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

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

Step 1 Step 2				_
Profile :	VPN_CLI_1			
Auth Type :	PSK	~		
Certificate :	None	~		
Preshared Key :				
Security Protocol :	ESP	~		
WAN Profile :	wan1	~		
Local IP / Subnet Mask 🗄	192 . 168 . 1	. 0	255.255.255.0 🗸	
Local Next Hop :	0.0.0	. 0		
Remote Host :	0.0.0	. 0		
Remote IP / Subnet Mask 🗄	0.0.0	. 0	255.255.255	
	🚯 Add 🛗 Save			
	IP		Subnet Mask	
		No items to) show.	
			🖕 🙀 🙀 🙀 🔥 Next 🛛 👹 Finish 🛛 😵 Ca	ar

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

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

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

•	Display VPN	Status?	Cancel	
6			Cancel	

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

Step 1	Step 2				
Type : VPN Settings V	 PPTP ia : Select From 	O IPSec Current Settings	🔿 Create New VPII I	Profile	
Profile	Status		1		
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.

Dray Tek		Vigor 3900 Series	14:23:28	Login: Admin	Ð
	1	/PN and Remote Access			
Auto Logout : Off		Step 1 Step 2 Step 3			
Firewall	~				
Objects Setting		Туре: 💿 РРТР	PSec		
User Management		VPN Settings Via : Select From Curr	ent Settings O 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					
IPSec General Setup					
VPN Profiles	=				
VPN TRUNK Management					
Connection Management					
Certificate Management					
SSL VPN					
Bandwidth Management					
System Maintenance					
Diagnostics	-			🖄 Previous 🛋 Next 📑 Finish	🐼 Cancel
External Devices				······································	

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.

l and Remote Acc				
Step 1 Ste	ep 2 Step 3			
Туре :	O PPTP	OIPSec		
VPN Settings Via	: 🔘 Select From	Current Settings 💿 C	reate New VPN Profile	
Profile Name :	VPN_Ser_1			
			D Brovious -	🔾 Next 🔲 Finish 🙆 Car
			Previous 🗳	Next Finish 🐼 Car

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

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

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

Step 1 Step 2	Step 3		
Enable This Profile			
Authenticate Protocol :	СНАР	*	
User Authentication Type :	Local		
		~	
LAN Profile :	lan1	*	

Item	Description			
Enable This Profile	Check this box to enable such profile.			
Authentication Protocol	The router will authenticate the dial-in user with the protocol selected here.			
	MS-CHAP-v2			
	PAP			
	CHAP MS-CHAP			
	MS-CHAP-v2			
	PAP - It means the router will attempt to authenticate dial-in users with the PAP protocol.			
	CHAP - It means the router will attempt to authenticate			

	dial-in users with th	e CH	AP protocol.
User Authentication	Set user authenticati	on to	Local server or RADIUS server.
Туре	Local	~	
	Local		
	RADIUS		
LAN Profile	Choose a LAN profile for PPTP Server if Local is selected as user authentication type.		

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

VPN and Remote Access	
Step 1 Step 2	Step 3
Profile : Enable This Profile	VPN_Ser_1
PPTP User Name :	~
Local IP / Subnet Mask :	192 168 1 0 255.255.0 v
Remote IP / Subnet Mask :	192 168 10 255.255.255.0 v
	🦘 Previous ា Next 📑 Finish 😵 Cancel

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



and Remote Access				
Step 1 Step	2 Step 3			
Profile :	VPN_Ser_1			
Enable This Prof	ile			
Auth Type :	PSK	~		
Certificate :	None	~		
Preshared Key :				
Security Protocol :	ESP	~		
WAN Profile :	wan1	~		
Local IP / Subnet Ma	sk: 192 . 168 .	1.0	255.255.255.0 🗸	
Local Next Hop :	0.0	0.0		
Remote Host :	0.0.0.0			
Remote IP / Subnet I	Mask: 0 . 0 .	0.0	255.255.255	
	🚯 Add 📑 Sav	/e		
	ID		Subnet Maek	
			🕥 Previous ា Next 📑 Fin	

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

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

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

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

Step 1 Step 2	Step 3
Profile:	VPN_Ser_1
PPTP User Name :	~
Confirm	
Display VPN S	Status?
Display VPN 8	
	OK Cancel

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

	cess	1	
Step 1	Step 2 Step 3		
Type : VPN Settings V	PPTP	OIPSec	s 🔵 Create New VPN Profile
Profile	Status	surrent setting	
VPN_Ser_1	enable		
			🏾 Previous 🔹 Next 📄 Finish 🚫 Car

4.8.3 Remote Access Control

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



4.8.4 PPP General Setup

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

PPTP

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

Auto Logout: Slin Outick Start Wizard Online Status WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access VPN Client Wizard VPN Client Wizard VPN Client Wizard VPN Client Wizard VPN TRUIK Management Connection Management Connection Management Connection Management Connection Management	Dray Tek	Vigor 3900 Series	15:09:56	Login: Admin	E
Ouick Start Wizard Online Status WAN LAN NAT Firewall Objects Setting User Hanagement Applications VPN and Remote Access VPN and Remote Access VPN Server Wizard Remote Access Control PPP General Setup VPN Profiles VPN Profiles VPN TRUIK Management Connection Management Apply		VPN and Remote Access >> PPP General Setup	>> PPTP		
Online Status WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access VPN and Remote Access VPN Server Wizard Remote Access Control PPP General Setup IPSec General Setup IPSec General Setup VPN Profiles	Auto Logout : 5Min 🗸	PPTP L2TP			
WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access VPN Client Wizard VPN and Remote Access VPN Elencry Diard Remote Access Control PPP General Setup IPSec General Setup IPSec General Setup VPN TRUIK Management Connection Management	Quick Start Wizard				
WAN LAN NAT Firewall Objects Setting User Authentication Type: Local Ver Annagement Applications VPN and Remote Access VPN Clent Wizard VPI Clent Wizard VPI Server Wizard Remote Access Control PPP General Setup VPI Profiles VPI TRUIK Management Connection Management	Online Status	Authenticate Protocol : MS-CHAP-v2			
LAN NAT Firewall Objects Setting User Authentication Type: local v LAN Profile : local v local v	WAN				
Firewall Objects Setting User Management Applications VPN and Remote Access VPN Client Wizard VPII Server Wizard Remote Access Control PPSec General Setup VPII Profiles VPII TRUNK Management Connection Management	LAN	MPPE Encryption : 128-bit	*		
Objects Setting User Management Applications VPN and Remote Access VPII Client Wizard VPII Server Wizard Remote Access Control PPP General Setup IPSec General Setup VPII Profiles VPII TRUIK Management Connection Management	NAT	User Authentication Type : Local	*		
User Management Applications VPN and Remote Access VPI Client Wixard VPI Server Wizard Remote Access Control PP9 General Setup IP9Sec General Setup VPI Profiles VPI TRUIK Management Connection Management	Firewall	LAN Profile : lan1	~		
Applications VPN and Remote Access VPII Client Wizard VPII Server Wizard Remote Access Control PPP General Setup IPSec General Setup VPII Profiles VPII TRUIK Management Connection Management	Objects Setting				
VPN and Remote Access VPII Client Wizard VPII Server Wizard Remote Access Control PPP General Setup IPSec General Setup VPII TRUIK Management Connection Management	User Management				
VPN Client Wizard VPN Server Wizard Remote Access Control PPP General Setup IPSec General Setup VPN Profiles VPN TRUNK Management Connection Management	Applications				
VPN Server Wizard Remote Access Control PPP General Setup IPSec General Setup VPN Profiles VPN TRUNK Management Connection Management	VPN and Remote Access				
Remote Access Control PPP General Setup IPSec General Setup VPII Profiles VPII TRUIK Management Connection Management	VPN Client Wizard				
PPP General Setup IPSec General Setup VPII Profiles VPII TRUIK Management Connection Management	VPN Server Wizard				
IPSec General Setup VPII Profiles VPII TRUIK Management Connection Management	Remote Access Control				
VPN Profiles VPN TRUNK Management Connection Management	PPP General Setup				
VPII TRUIK Management	IPSec General Setup				
Connection Management	VPN Profiles				
Connection Management	VPN TRUNK Management				
Castificate Management				Apply	🐼 Cancel
	Contificato Managomont				

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

	selected here.
	MS-CHAP-v2
	PAP
	CHAP
	MS-CHAP MS-CHAP-v2
	PAP - It means the router will attempt to authenticate dial-in users with the PAP protocol.
	CHAP - It means the router will attempt to authenticate dial-in users with the CHAP protocol.
MPPE Encryption	Specify one of the encryptions for such server. It is available only when MS-CHAP or MS-CHAP_v2 is selected.
	128-bit
	40/128-bit
	128-bit
	Disable
User Authentication	Set user authentication to Local server or RADIUS server.
Туре	Local
	Local
	RADIUS
LAN Profile	Choose a LAN profile for PPTP Server if Local is selected
	as user authentication type.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

L2TP

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

Dray Tek	Vigor 3900 Ser	ies 15:11:25	Login: Admin	Ð
	VPN and Remote Access >> PPP Ge	neral Setup >> L2TP		
Auto Logout : 5Min 🗸	PPTP L2TP			
Quick Start Wizard				
Online Status	Authenticate Protocol :	CHAP		
WAN		Local		
LAN				
NAT	LAN Profile :	an1 🗸		
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
VPN Client Wizard				
VPN Server Wizard				
Remote Access Control				
PPP General Setup				
VPN Profiles				
VPN Profiles				
Connection Management			Apply	🔇 Cancel
<				>



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

4.8.5 IPSec General Setup

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

Dray Tek	Vigor 3900	Series	15:12:48	Login: Admin	Ð
	VPN and Remote Access >> I	PSec General Setup			
Auto Logout : 5Min 💌	IPSec General Setup				
Quick Start Wizard					
Online Status	Preshared Key :	•••			
WAN	WAN Profile :	wan2, wan4	~		
LAN		lan1			
NAT	DHCP LAN Profile :		~		
Firewall	IKE Port :	500			
Objects Setting	NAT-T Port :	4500			
User Management	IPSec MSS :	1360			
Applications	GRE over IPSec MSS :	1360			
VPN and Remote Access					
VPN Client Wizard					
Remote Access Control					
PPP General Setup					
IPSec General Setup					
VPN Profiles					
VPN TRUNK Management					
Connection Management				Apply (🔇 Cancel
Contificato Managomont					
<					>

Item	Description



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

4.8.6 VPN Profiles

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

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

Dray Tek		Vigor 390	Series	15:58:19	Login: Admin	e>
		VPN and Remote Access	>> VPN Profiles			
Auto Logout : Off 🛛 👻		VPN Profiles				
Quick Start Wizard	-		- ·			ile Number Lir
Online Status		🚯 Add 🔀 Eo	lit 🔟 Delete 🔇 🐼 I	Refresh 💿 IPSec 🔘 I	PPTP Dial-Out O PPTP Dial-In Profi	le Number Li
WAN		Profile	Enable This Profile	Local IP / Subnet Mask	Remote IP / Subnet Ma More Remote S	ubnet
LAN		128	false	192.168.139.0/24	192.168.128.0/24	
NAT		39	true	192.168.139.0/24	192.168.39.0/24	
Firewall		tim2930	true	192.168.139.0/24	192.168.93.0/24	
Objects Setting		39_1	true	192.168.139.0/24	192.168.39.0/24	
User Management		2850	true	192.168.139.0/24	192.168.128.0/24	
Applications		franksh	true	192.168.139.0/24	0.0.0/32	
VPN and Remote Access		201	true	192.168.139.0/24	192.168.11.0/24	
VPN Client Wizard	- 11	2950WAN1	true	192.168.29.0/24	192.168.1.0/24	
VPN Server Wizard		2950WAN2	true	192.168.29.0/24	192.168.1.0/24	
Remote Access Control						
PPP General Setup						
IPSec General Setup						
VPN Profiles						
VPN TRUNK Management						
Connection Management		4				•
Contificato Managoment						

Each item will be explained as follows:

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

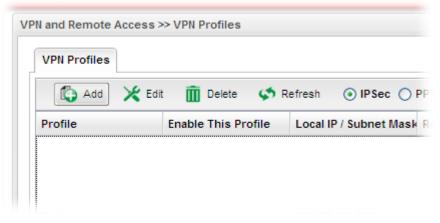


	profile.
Delete	Remove the selected profile.
	To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
IPSec	Display the LAN to LAN profile with IPSec policy.
PPTP Dial-out	Display the LAN to LAN profile with PPTP Dial-out policy.
PPTP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

How to create an IPSec VPN profile

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

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



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

Profile :	L2L-1		
V Enable This Profile			
Туре :	💿 IPSec 🔘 PPT	P Dial-Out 🔘 PPTP Dial-In	
Basic Advance	ed GRE	Proposal PPTP	
Always On :	🔵 Enable	Disable	
For Remote Dial-In :	🔵 Enable	Disable	
Auth Type :	PSK	*	
Preshared Key :			
Security Protocol :	ESP	*	
WAN Profile :	wan1	*	
			•

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



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

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

Sec			-
Profile : L2L-1			
V Enable This Profile			
Type : 💿 IP Sec	OPPTP Dial-Out OPPTP	Dial-In	
Basic Advanced	GRE Proposal	PPTP	
Dasic Auvanceu	GRE Proposal		
Aggressive Mode :	💿 Enable 🔵 Disable		
Local Peer ID :		(Optional)	
Remote Peer ID :		(Optional)	
Phase1 Key Life Time :	28800		
Phase2 Key Life Time :	3600		
Perfect Forward Secrecy Status	: O Enable 💿 Disable		
Dead Peer Detection Status :	💿 Enable 🔿 Disable		
		Appl	v 🙆 Can

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

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

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

Profile :	L2L-1	
V Enable This Profil		
Type :	● IPSec ○ PPTP Dial-Out ○ PPTP Dial-In	
Basic Advan	ed GRE Proposal PPTP	
Busic Autum		
Enable GRE Function	: 💿 Enable 🔵 Disable	
Local GRE IP :	192 . 168 . 1 . 66 m (Option	nal)
Remote GRE IP :	192 . 168 . 1 . 96 m (Option	nal)
Auto Generate GRE	ey: 🔿 Enable 💿 Disable	
GRE In Key :	(Optional)	
GRE Out Key :	(Optional)	

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



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

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

Profile :	L2L_1				
	_				
👿 Enable This					
Туре	(⊙ IP:	Sec 🔘 P	PTP Dial-Out 🔵 PP	TP Dial-In	
Basic A	dvanced	GRE	Proposal	PPTP	
IKE Phase1 Pr	oposal [Dial-O	ut] :	DES_G1	· • •	
IKE Phase1 Au	thentication [[Dial-Out]	: ALL	~	
IKE Phase2 Pr	oposal [Dial-O	ut]:	3DES_with_auth	~	
IKE Phase2 Au	thentication [[Dial-Out]	: ALL	~	
Accepted Proj	osal [Dial-In]	:	acceptall	~	

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

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

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

VPN Profiles			
🚯 Add 🔀	Edit 🔟 Delete 🐝 I	Refresh 💿 IP Sec 🔿	PPTP Dial-Out 🔘 PP
	Fuchic This Dusfile	Local IP / Subnet Masi	Bomoto ID / Subnot
Profile	Enable This Profile	Local IP / Subnet Mass	Kemole IP / Subhet
Profile 128	false	192.168.139.0/24	192.168.128.0/24

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.

🚯 Add	🔀 Edit	🔟 Dele	ete 🗳	Refresh	⊙ IP:	Sec 🔿
Profile		Enable Thi	s Profile	Loca	I IP / Subn	et Mas

3. The following dialog will appear.

Profile :	PTF	_out_1				
🗸 Enable TI	his Profile					
Туре:	0	IPSec 💿 PPT	Dial-Out 🔘	PPTP Dial-In		
Basic	Advanced	GRE	Proposal	РРТР		
Always On :		🔵 Enable 🧕) Disable			
Server IP/Ho	ost Name :	172.16.3.250		1		
PPTP User I	lame :	pptptest		(Optional)		
PPTP Passv	vord :	•••••		1		
Local IP / Su	ibnet Mask :	192 . 168	. 1	54 255	255.255.0	~
		🖾 Add 🗎	Save II			

Item	Description					
Profile	Type the name of the profile.					
Enable This Profile	Check this box to enable this profile.					
Туре	There are three types offered here for you to choose. Please choose PPTP Dial-Out for this case.					
PPTP	Always On - Click Enable to make the profile being always on.					
	Server IP/Host Name - Type the IP address or the host name of PPTP server.					
	PPTP User Name - Type a user name for authentication in PPTP connection.					
	PPTP Password - Type a password for authentication in PPTP connection.					
	Local IP/Subnet Mask - Type the IP address and subnet mask of local host.					
	Remote IP / Subnet Mask - Type the LAN IP address and LAN subnet mask for the remote host.					
	Route / NAT Mode - Specify the purpose for such profile.					
	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 i Delete 🔇	Refresh OIPSec	💿 PPTP Dia
Profile	Enable This Profile	PPTP User Name	Local I
PTP_out_1	true	pptptest	192.168

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.

🚺 Add	🔀 Edit 🛛 前 Delete	娕 Refrest	IPSec 🔿
Profile	Enable This Pr	ofile Loca	al IP / Subnet Mas

3. The following dialog will appear.

Profile :		PTP_	ln_1			
V Enable This Profile		01	PSec 🔿 I	PPTP Dial-	Out 💿 PPTP Dial-In	
Set PPTP Dial-In For Use	er Profi	e				
Basic Advanced	G	RE	Propos	sal	РРТР	
PPTP User Name :	frankw			•		
Local IP / Subnet Mask :	0	. 0	. 0	. 0	255.255.255.0	*
Remote IP / Subnet Mask :	0	. 0	. 0	. 0	255.255.255.0	*

Item	Description
Profile	Display the name of the profile.
Enable This Profile	Check this box to enable this profile.
Туре	There are three types offered here for you to choose. Please choose PPTP Dial-In for this case.
Set PPTP Dial-In For User Profile	Click it to create a new user profile or to modify an existing profile.
	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

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

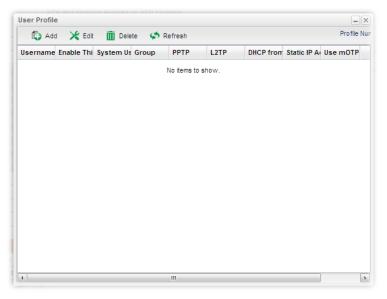
- 4. Enter all the settings and click **Apply**.
- 5. A new PPTP Dial-In profile has been created.

🐴 Add 💙	Edit 🕅 Delete	🔇 Refresh 🔿 IPSec	PPTP Dial-Out
Profile	Enable This Pro	ofile PPTP User Name	Local IP / Subnet
PTP_In_1	true	frankwang	0.0.0/24

Set PPTP Dial-In For User Profile

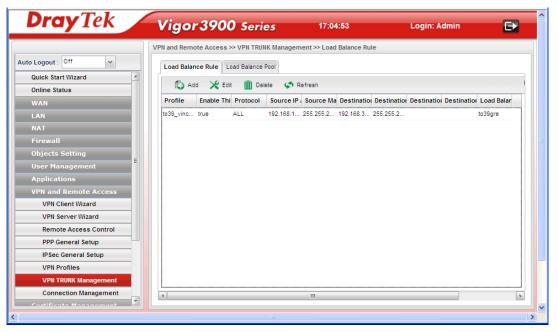
To set PPTP Dial-In connection, you have to create PPTP user profiles previously in **User Management>>User Profile**, or click **Set PPTP Dial-In For User Profile** in this page to configure a new one for choosing for authentication in PPTP connection.

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.**



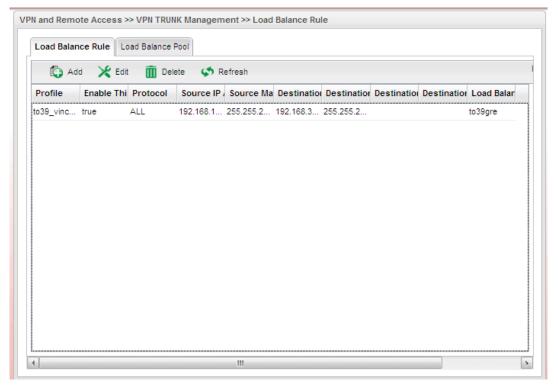
4.8.7 VPN Trunk Management

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.



Load Balance Rule

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



Each item will be explained as follows:



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

How to add a Load Balance Rule profile

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

Lo	ad Bala	nce Rule	Load Bal	ance Pool	
	🚯 Ac	id 🔀 E	Edit 前	Delete	🗳 R
Pr	ofile	Enable Th	Protocol	Source IF	Sour

3. The following dialog will appear.

oad Balance Rule		->
Profile :	LB_rule_1	
📝 Enable This Profile		
Protocol :	ALL 🗸	
Source IP Address :	192 . 168 . 1	46 (Optional)
Source Mask :	255.255.255.0	(Optional)
Destination IP Address :	192 . 168 . 1	89 (Optional)
Destination Mask :	255.255.255.0	(Optional)
Load Balance Pool :	to39gre 🗸 🗸	

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable such profile.
Protocol	Choose the protocol for such profile.
	TCP/UDP ALL TCP UDP TCP/UDP TCP/UDP TCP/UDP TCP/UDP TCP/UDP TCP/UDP O TFTP TFTP TFTP O HTTP 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.

VPN and Rem	iote Access	>> VPN TR	UNK Manage	ement >> Lo	ad Balance	Rule
Load Bala	nce Rule L	.oad Balanc	e Pool			
🚯 Ad	d 🛛 💥 Edi	t <u> î</u> Del	lete – 🗳 R	(efresh		
Profile	Enable Thi	Protocol	Source IP	Source Ma	Destination	Destinati
L8_rule_1	true	TCP/UDP	192.168.1.	255.255.25	192.168.1.)	255.255.2

Load Balance Pool

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

Load Balance	e Rule Loa	nd Balance Po	ol				
🚯 Add	🔀 Edit	前 Delete	娕 Refresh				
Profile				Interfa	ce		
			N	o items to sh	OW.		
			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 Edit button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile.
	To delete a profile, simply select the one you want to delete and click the Delete button.
Refresh	Renew current web page.
Profile	Display the name of the profile.
Interface	Display the name of the Load Balance profile grouped under such pool profile.

How to add a Load Balance Pool Profile

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

Load Balance	Rule Loa	d Balance Poo	1
🚯 Add	🔀 Edit	前 Delete	🗳 Refi
Profile			

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

ut : joii Load Balance	Pool	_>
Mode	Load Balance	
Profile :	LB_Pool_1	
		💾 Apply 🛛 🚫 Cance

Dray Tek

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

l Balance I	lool	
Mode	Load Balance	
Interface	· VPN_CLI_1 v	
	VPN_CLI_1	
		📑 Apply 🛛 😣 C

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

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

		Balance Pool			
🚯 Add 🌖	Edit	前 Delete	< Refresh		
Profile				Interface	

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.

Dray Tek		Vigor	3900	Series		17:18:00	Login: Admin	E
	V	PN and Remote	Access >>	Connection	Management			
Auto Logout : Off 🛛 🗸		Connection	Managemer	nt				
Quick Start Wizard			_					
Online Status		Profiles :			👻 🔁 Co	nnect 💿 IPSec 🔿 P	PTP 🔇 Refresh	
WAN		Index	VPN	Туре	Remote IP	Virtual Netw Up Time	RX(Packets) TX(Packets Disco	nnect
LAN						No items to show.		
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 Management								
Connection Management								
Cortificato Managoment								

Each item will be explained as follows:

Item	Description
Profile	This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.
Connect	Click this button to execute dial out function.
IPSec	Click it to perform IPSec VPN connection.
РРТР	Click it to perform PPTP VPN connection.
Refresh	Renew current web page.
Index	Display the item number of the VPN profile.
VPN	Display the name of VPN profile.
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.

Dray Tek

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.

Certifi	icate Management
Loc	al Certificate
Tru	sted CA Certificate
Ren	note Certificate

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).

Dray Tek	Vigor 390	00 Series		11:18:58	Logi	n: Admin	Ð
Auto Logout: Shin v Quick Start Vizard Online Status WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management Local Certificate Remote Certificate SSL VPN Bandwidth Management System Maintenance	Certificate Managemen	t >> Local Certifica	te Download 🚭 Gene अप्रि Issuer		Logi	N: Admin	
Diagnostics External Devices Product Registration			m				

Each item will be explained as follows:

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

How to build a local certificate

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

Local Certificate			
🚺 Upload	<u> Delete</u> 🛛 🗐	Download 🛛 🧔 Gener	rate
Select File :		Browse	
Name	Subject	Issuer	Status

3. The following dialog will appear.

ocal Certificate			_ ×
Certificate Name:	Local_CA		
ID Type :	None	۷	
ID Value :			Optional
Organization Unit:	DT		
Organization :	Draytek		
Locality(City) :	HS		
State/Province :	Taiwan		
Common Name :	DT_License		
Email Address :	service@draytek.com		
Key Size :	1024	۷	
Country :	TW		
Self Sign :	🔵 Enable 💿 Disable		
Passphrase :			

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



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

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

5. A new generated Local Certificate has been created.

Local Certificate					
🚺 Upload	👖 Delete 🛛 🔍 Do	wnload 🛛 🧔 Genera	te		
Select File :		Browse			
Select File :	Subject	Browse	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**.

Dray Tek	Vigor 3	900 Serie	5	12:00:32	Logir	n: Admin	Đ
Auto Logout : Min v Quick Start Wizard Online Status WAN	Certificate Managen Trusted CA	nent >> Trusted CA	Download 🎤 Bi	uild RootCA			
	Select File :		Browse				
Firewall	Name	Subject	Issuer	Status	Valid from	Valid to	
Objects Setting	RootCA	TW	TW	RootCA	Jul 26 04:04:39	201 Jul 24 04:04:35	202
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
Local Certificate							
Trusted CA Certificate							
Remote Certificate							
SSL VPN							
Bandwidth Management							
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 Browse button to specify a file to be used as trusted CA certificate.
Name	Display the name of trusted certificate built.
Subject	Display the subject of trusted certificate built.
Issuer	Display the issuer of trusted certificate built.
Status	Display the status of trusted certificate built.



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

How to build a trusted CA certificate

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

Trusted CA				
🚺 Upload	<u> Î</u> Delete 🛛 🗐	Download — 🎘 Bu	ild RootCA	
Select File :		Browse		
Name	Subject	Issuer	Status	Va

3. The following dialog will appear.

rusted CA		-×
Certificate Name:	RootCA	
Organization Unit :	DT	
Organization :	DrayTek	
Locality(City) :	HS	
State/Province :	Taiwan	
Common Name :	CA_license	
Email Address :	service@draytek.com	
Key Size 🗄	1024 💌	
Country :	TW	
Passphrase :	123	

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]				
🚺 Uploa	d <u> m</u> Delete 🗔	Download 🏼 🎤 Bu	uild RootCA		
		-			
Select File	H:	Browse			
Select File	s: Subject	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.

Dray Tek	Vigor 3900 s	eries 13:	45:01 Login: Admin	E
Auto Logout : Off Quick Start Wizard Online Status W/AN LAN NAT	Certificate Management >> Remot Remote Certificate			
Firewall	Name	Subject	Status	
Objects Setting	2850	TW	ок	
User Management				
- Applications				
VPN and Remote Access				
Certificate Management				
Local Certificate				
Trusted CA Certificate				
Remote Certificate				
SSL VPN				
Bandwidth Management				
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.
Selected File	Use the Browse button to specify a file to be used as trusted CA certificate.
Name	Display the name of remote certificate built.
Subject	Display the subject of remote certificate built.
Status	Display the status of remote certificate built.

4.10 SSL VPN

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

There are two benefits that SSL VPN provides:

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

SSL VPN
SSL Web Proxy
SSL Application
Online User Status
Bandwidth Management

4.10.1 SSL Web Proxy

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

Dray Tek	Vigor 3900 Se	ries 14:07:06	Login: Admin	₽.
	SSL VPN >> SSL Web Proxy			
o Logout : Off 🛛 👻	SSL Web Proxy			
Quick Start Wizard	🕼 Add 🔀 Edit 🏢	Delete 🔇 Refresh		Profile Num
Online Status				
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			•

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



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

How to create a new SSL Web Proxy

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

SSL Web Proxy		
🚯 Add 🔀 Kedit	前 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
SSL_WP_1	www.draytek.com	172.16.3.89

4.10.2 SSL Application

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

VNC

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

Dray Tek	Vigor 3900) Series	14:08:35	Login: Admin	Ð
Auto Logout : Off v Quick Start Wizard Online Status	SSL VPN >> SSL Applicati	on >> VNC			Profile Num
WAN LAN	Profile	IP Address	Port 5900	Scaling	
NAT Firewall	vnc_pc	192.168.139.12	5900	100%	
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					

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



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

How to create a new SSL Application with VNC protocol

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

VNC	RDP		
🚯 Add	🔀 🔀 Edit	<u>î</u> Delete	🥩 Refr
Profile		IP Address	

3. The following dialog will appear.

Profile :	VNC_1		
IP Address	: 192 . 168 . 1	38	
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.



RDP

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

Dray Tek	Vigor 3900 Series	14:15:58	Login: Admin	Ð
	SSL VPN >> SSL Application >> RDP			
Auto Logout : Off 🛛 👻	VNC RDP			
Quick Start Wizard	🕼 Add 💥 Edit 🛅 Delete 🗳 Refre:			Profile Num
Online Status				
WAN	Profile IP Address	Port	Screen Size	
LAN	rdp 192.188.139.10	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			•

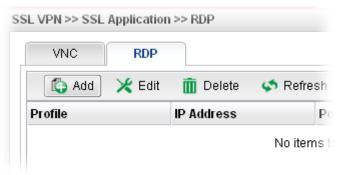
Item	Description
Add	Add a new profile.
Edit	Modify the selected profile.
	To edit a profile, simply select the one you want to modify and click the Edit button. The edit window will appear for you to modify the corresponding settings for the selected profile.
Delete	Remove the selected profile. To delete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



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

How to create a new SSL Application with RDP protocol

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



3. The following dialog will appear.

		J
Profile :	RDP_1	
IP Address :	192 . 168 . 1 . 57	
Port :	3389	
Screen Size :	Fullscreen 🗸	

Available parameters are listed as follows:

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

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

5. A new SSL Application profile has been created.

VNC	RDP		
🚯 Add	🔀 Edit 🛛	<u>前</u> Delete 🛛 📢 Refresh	
Profile		IP Address	Port
RDP_1		192.168.1.57	3389

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.

Dray Tek	Vigor 3900 Ser	ies 14:17:	59 Login: Admin	Ð
Auto Logout : Off v	SSL VPN >> SSL VPN Status			
Online Status	🖍 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 Bandwidth Management

Below shows the menu items for Bandwidth Management.

The QoS (Quality of Service) guaranteed technology in the Vigor router allows the network administrator to monitor, analyze, and allocate bandwidth for various types of network traffic in real-time and/or for business-critical traffic. Thus, timing-sensitive applications will not be impacted by web surfing traffic or other non-critical applications, such as file transfer. Without QoS-guaranteed control, there would be virtually no way to prioritize users/services or guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications.

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

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

4.11.1 Incoming Class

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

Total Rate Control

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

Dray Tek	Vigor 3900 Series	14:20:12	Login: Admin	E
	Bandwidth Management >> Incoming Class >> Tota	al Rate Control		
Auto Logout : Off	Total Rate Control Class Rate Control			
Quick Start Wizard				
Online Status				
WAN	Mode : O Enable O Disable			
LAN	Rate : 0	💽 Kbps 🔘 Mbps		
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
Incoming Class				
Incoming Filter				
Outgoing Class				
Outgoing Filter				
Sessions Limit				
Bandwidth Limit			Apply	🚫 Cancel
System Maintenance				

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

Class Rate Control

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

	Bandwidth Management >> I	ncoming Class >> Class Rate Control		
Logout : Off	Total Rate Control Clas	s Rate Control		
Quick Start Wizard				
Online Status	🔀 Edit 🗳 Refre	sh		
WAN	QoS Policer	Mode	Rate	
LAN	incoming_class0	Disable	0	
NAT	incoming_class1	Disable	0	
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
Incoming Class				
Incoming Filter				
Outgoing Class				
Outgoing Filter				
Sessions Limit				
Bandwidth Limit				

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

How to edit the incoming class rate for the QoS policer

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

Total Rate Control Class	s Rate Control			
🔀 Edit 🛛 🗢 Refresh				
QoS Policer	Mode			
incoming_class0	Disable			
incoming class1	Disable			

3. The following dialog will appear.

QoS Policer	r : incoming_class1		
Mode :	🔵 Enable 💿 Disable		
Rate :	15		

Available parameters are listed as follows:

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

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

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

Total Rate Control Clas	s Rate Control	
🔀 Edit 🛛 🐼 Refre	sh	
QoS Policer	Mode	Rate
QoS Policer ncoming_class0	Mode Disable	Rate 0

4.11.2 Incoming Filter

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

Dray Tek	Vigor 390	0 Series	14:39:51	Login: Admin	Ð
	Bandwidth Management >	>> Filter Rule			
to Logout : Off 🛛 🗸	Filter Rule				
Quick Start Wizard					
Online Status	🔀 Edit 🗳 R	efresh			
WAN	Filter Rule	Policer	Drop	Reserved	
LAN	filter_rule_0	no_rate_control	Disable	Disable	*
NAT	filter_rule_1	no_rate_control	Disable	Disable	
Firewall	filter_rule_2	no_rate_control	Disable	Disable	
Objects Setting	filter_rule_3	no_rate_control	Disable	Disable	
User Management	filter_rule_4	no_rate_control	Disable	Disable	=
Applications	filter_rule_5	no_rate_control	Disable	Disable	
VPN and Remote Access	filter_rule_6	no_rate_control	Disable	Disable	
Certificate Management	filter_rule_7	no_rate_control	Disable	Disable	
SSL VPN	filter_rule_8	no_rate_control	Disable	Disable	
Bandwidth Management	filter_rule_9	no_rate_control	Disable	Disable	
Incoming Class	filter_rule_10	no_rate_control	Disable	Disable	
Incoming Filter	filter_rule_11	no_rate_control	Disable	Disable	
Outgoing Class	filter_rule_12	no_rate_control	Disable	Disable	
Outgoing Filter	filter_rule_13	no_rate_control	Disable	Disable	
Sessions Limit	filter_rule_14	no_rate_control	Disable	Disable	
Bandwidth Limit	filter_rule_15	no_rate_control	Disable	Disable	
System Maintenance	filter rule 18	no rate control	Disable	Disable	*

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

How to edit the incoming filter for the QoS policer

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

ndwidth Management >> Filter Rule				
Filter Rule				
🔀 Edit 🗳	Refresh			
Filter Rule	Policer	Drop		
filter_rule_0	no_rate_control	Disable		
filter_rule_1	no_rate_control	Disable		
filter_rule_2	no_rate_control	Disable		
filter_rule_3	no_rate_control	Disable		
filtor rulo A	no rato control	Dicoblo		

3. The following dialog will appear.

ilter Rule	_	
Filter Rule :	filter_rule_0	
Policer :	no_rate_control v	
Drop :	🔿 Enable 💿 Disable	
Reserved :	🔿 Enable 💿 Disable	
IP Protocol :	None	
Source IP Address :	0.0.0.0	
Source IP Address Mask :	0.0.0.0	
Source Port Enable :	🔘 Enable 💿 Disable	-
Source Port Start :	0	
Source Port End :	0	
Destination IP Address :	0.0.0.0	
Destination IP Address Mask :	0.0.0.0	
Destination port Enable :	🔵 Enable 💿 Disable	
Destination Port Start :	0	
Destination Port End :	0	
	📑 Apply 🔇 Cance	-



Available	parameters	are listed	as follows:
11, 41, 41, 40, 10	parane coro		

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

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

- 4. Enter all the settings and click **Apply**.
- 5. The incoming filter rule for **QoS Policer** has been modified.

Filter Rule				
🔀 Edit 🛛 🗳	Refresh			
Filter Rule	Policer	Drop	Reserved	
filter_rule_0	no_rate_control	Disable	Disable	
filter_rule_1	no_rate_control	Enable	Disable	
filter_rule_2	no_rate_control	Disable	Disable	
filtor rulo 2	no rato control	Dicabla	Disable	

4.11.3 Outgoing Class

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

Total Rate Control

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

Dray Tek	Vigor 3900 Series	14:41:59	Login: Admin	Ð
	Bandwidth Management >> Outgoing Class >> Total	Rate Control		
uto Logout : Off	Total Rate Control Class Rate Control Queue	1-5 Weight		
Quick Start Wizard				
Online Status	Status : O Enable 📀 Disable			
WAN				
LAN	Rate : 0	💽 Kbps 🔘 Mbps		
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
Incoming Class				
Incoming Filter				
Outgoing Class				
Outgoing Filter				
Sessions Limit				
Bandwidth Limit			Apply	🚫 Cancel
System Maintenance 🤤				-

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



Class Rate Control

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

	Vigor 3900	• Outgoing Class >> Class Ra	te Control	
o Logout : Off 🗸 🗸		ss Rate Control Queue 1-5		
Quick Start Wizard	🔀 Edit 🗳 Ref	iresh		
WAN	Profile	Status	Rate	Description
LAN	outgoing_class0	Disable	0	Control queue 7(hightest)
NAT	outgoing_class1	Disable	0	Control queue 6(higher)
Firewall	outgoing_class2	Disable	0	Control queue 1-5(low)
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				
SSL VPN				
Bandwidth Management				
Incoming Class				
Incoming Filter				
Outgoing Class				
Outgoing Filter				
Sessions Limit				
Bandwidth Limit				

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

How to edit the outgoing class rate for the QoS policer

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

Total Rate Control	Class Rate Control)ueue 1-5 Weight
🔀 Edit 🛛 🐼 F	Refresh	
Profile	Status	Rate
outgoing_class0	Disable	0
outgoing_class1	Disable	0
outgoing_class2	Disable	0

3. The following dialog will appear.

nss Rate Con	trol	-
Profile :	outgoing_class1	
Status :	💿 Enable i 🔘 Disable	
Rate :	65	💿 Kbps 🔵 Mbps
Description	: Control queue 6(higher)	
		🛗 Apply 🛛 😡 Cancel

Available parameters are listed as follows:

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

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

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

Total Rate Control	Class Rate Control	ueue 1-5 Weight	
🔀 Edit 🛛 🗳 R	efresh		
Profile	Status	Rate	Description
outgoing_class0	Disable	0	Control queue 7 (hightest)
outgoing_class1	Enable	65	Control queue 6(higher)
outgoing_class2	Disable	0	Control queue 1-5(low)

Outgoing Queue 1-5 Weight

There are several available outgoing queues, four shapers at varying levels, and five data queues with weights. All queues in the data group to be initialized with weights of zero, resulting in a strict service to completion (STC) mechanism across all queues.0.

Dray Tek		Vigor 3900 Series	14:45:57	Login: Admin	E ^
Auto Logout : Off 🛛 🗸		Bandwidth Management >> Outgoing Class >> Qu Total Rate Control Class Rate Control Que	ieue 1-5 Weight ue 1-5 Weight		
Online Status WAN LAN NAT Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Bandwidth Management Incoming Class Incoming Filter Outgoing Class	E	Edit A Refresh CoS Queue Iow_queue_5 Iow_queue_4 Iow_queue_3 Iow_queue_2 Iow_queue_1	Weight 0 0 0 0 0		
Outgoing Filter Sessions Limit Bandwidth Limit System Maintenance					

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

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

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

Total Rate Control	Class Rate Control	Queue 1-5 Weight
🗶 Edit 🗳	Refresh	
QoS Queue		Weight
low_queue_5		0
low_queue_4		0
low_queue_3		0

3. The following dialog will appear.

eue 1-5 Weight	
QoS Queue : low_queue_5	
Weight: 23	
	📑 Apply 🛛 🐼 Cancel

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

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

Total Rate Control Class Rate Control	Queue 1-5 Weight
🔀 Edit 🛛 🐼 Refresh	
QoS Queue	Weight
low_queue_5	25
low_queue_4	0

4.11.4 Outgoing Filter

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

Dray Tek			00 Series		14:47:59	Logini	Admin	Ð
	В	andwidth Managem	ent >> Outgoing Filter					
o Logout : Off 🛛 🗸		Outgoing Filter						
Quick Start Wizard		🚺 Add 💙	🗲 Edit 🛛 🕅 Delete	🔇 Refresh 【	a Rename			
Online Status		E Add		C Retresh	5 Kename			
WAN		Profile	Enable This Profile	Source IP	Destination IP	Service Type	Queue Number	
LAN				No	p items to show.			
NAT								
Firewall								
Objects Setting								
User Management								
Applications								
VPN and Remote Access								
Certificate Management								
SSL VPN								
Bandwidth Management								
Incoming Class								
Incoming Filter								
Outgoing Class								
Outgoing Filter								
Sessions Limit								
Bandwidth Limit								
System Maintenance	3	4		111				>

Each item will be explained as follows:

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

Dray Tek

How to add an outgoing filter for the QoS policer

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

Outgoing Filte				
🚯 Add	🔀 Edit	🔟 Delete	🔇 Refresh	G a Renan
Profile	En	able This Profile	Source IP	De
				No items t

3. The following dialog will appear.

Profile :	Out_filt_1	
🔽 Enable This	Profile	
Source IP :	IP_object_1 🛛 🗸 🏠	
Destination IP :	CRM_server 🔽 🚯	
Service Type :	Any 💉 🕼	
Queue Number	: 0	

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

	Profile
	Profile :for_out_filterProtocol :TCPSource Port Start :1Source Port End :66535Destination Port Start :1Destination Port End :65535
	 Profile – type a new name for such service type. Protocol –There are two options: TCP, UDP and TCP/UDP. Select the protocol that you want to use. Source Port Start /End - Type the start /end number for the port range of the source port for such filter.
	Destination Port Start / End - Type the start /end number for the port range of the destination port for such filter.
Queue Number	Choose a queue number to category the packets matching with the condition configured as above. Queue 7 is the highest; 0 is the lowest.
	Queue Number : 0 • • • • • • • • • • • • • • • • • •
Apply	Click it to save the configuration and exit the page.
Cancel	Click it to exit the page without saving the configuration.

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

ndwidth Managem	ent >> Outgoing Filter			
Outgoing Filter				
🚯 Add 🛛 🔀	Edit <u> </u>	< Refresh 🛛 😘	Rename	
Profile	Enable This Profile	Source IP	Destination IP	Service Type
Out_filt_1	true	192.168.1.8/0	192.168.0.168/1	Any

4.11.5 Sessions Limit

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

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

Dray Tek	Vigor 3900 Series	14:52:59	Login: Admin	E>
	Bandwidth Management >> Sessions Limit			
Auto Logout : Off 🛛 🗸	Sessions Limit			
Quick Start Wizard		(1)		
Online Status	🕼 Add 🔀 Edit ៣ Delete 🗳 Refresh	G Rename		
WAN	Profile Enable This Profile	Source IP	Max Sessions	
LAN		No items to show.		
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
Certificate Management				_
SSL VPN	Use Default Message :	📀 Enable 🔘 Disable		
Bandwidth Management			ed <body><center> You(IP:%SIP%) have reached the r</center></body>	
Incoming Class		permitted Internet sessions.PI	ease close one or more application	
Incoming Filter	Default Connection Limit Administration Message	Internet access.Contact your s information. <td></td> <td></td>		
Outgoing Class		and a starte starter start	-,	
Outgoing Filter				
Sessions Limit		111		>
Bandwidth Limit			Apply	🙆 Cancel

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



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

How to add a session limit profile for the QoS policer

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

Sessions Limit		
🚯 Add 🔀 Kedit	前 Delete 🛛 🗳 Refr	esh
Profile	Enable This Profile	So

3. The following dialog will appear.

Profile :	Session_1		
👿 Enable Thi	s Profile		
Source IP :	192 . 168 . 1 . 35 255.25	5.255.0	
Max Sessions	: 1000		

Item	Description
Profile	Type the name of the profile.
Enable This Profile	Check this box to enable such profile.
Source IP	Type the source IP address with subnet mask for limit session.
Max Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session

	limit for the specific limitation you set for each index. This field cannot be typed with "0", otherwise the profile cannot be saved.
Apply	Click it to save the configuration and exit the dialog.
Cancel	Click it to exit the dialog without saving the configuration.

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

Sessions Limit			
🕼 Add 🛛 🔀 Edit	🏢 Delete 🛛 娕 Refre	sh 🕻 🥵 Rename	
Profile	Enable This Profile	Source IP	Max Sessions

4.11.6 Bandwidth Limit

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

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

Dray Tek	Vigor 3900 Series	14:57:14	Login:	Admin 🕞
	Bandwidth Management >> Bandwidth Limit			
uto Logout : Off	Bandwidth Limit			
Quick Start Wizard				
Online Status	🕼 Add 🔀 Edit 🛅 Delete 🔝	Refresh 🕻 Rename		
WAN	Profile Enable This Profile Sta	rt IP End IP	TX Limit	RX Limit
LAN		No items to show.		
NAT				
Firewall				
Objects Setting				
User Management				
Applications				
VPN and Remote Access				
VPN and Remote Access				
VPN and Remote Access	Enable Smart Bandwidth Limit (Will spp	y to the LAN IP not in Limitation List	whose session number	exceeds the threshold)
VPN and Remote Access Certificate Management	Enable Smart Bandwidth Limit (Will spp Sessions Threshold : 1000	ly to the LAN IP not in Limitation List	whose session number	exceeds the threshold)
VPN and Remote Access Certificate Management SSL VPN		y to the LAN IP not in Limitation List	whose session number	exceeds the threshold)
VPN and Remote Access Certificate Management SSL VPN Bandwidth Management	Sessions Threshold : 1000 TX Limit : 5000		whose session number	exceeds the threshold)
VPN and Remote Access Certificate Management SSL VPN Bandwidth Management Incoming Class	Sessions Threshold : 1000 TX Limit : 8000 RX Limit : 5000	 Kbps Mbps Kbps Mbps 		
VPN and Remote Access Certificate Management SSL VPN Bandwidth Management Incoming Class Incoming Filter	Sessions Threshold : 1000 TX Limit : 8000 RX Limit : 5000			
VPN and Remote Access Certificate Management SSL VPN Bandwidth Management Incoming Class Incoming Filter Outgoing Class	Sessions Threshold : 1000 TX Limit : 8000 RX Limit : 5000	 Kbps Mbps Kbps Mbps 		ardware NAT
VPN and Remote Access Certificate Management SSL VPN Bandwidth Management Incoming Class Incoming Filter Outgoing Class Outgoing Filter	Sessions Threshold : 1000 TX Limit : 8000 RX Limit : 5000	 Kbps Mbps Kbps Mbps 		

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



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

How to add a bandwidth limit profile for the QoS policer

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

Bandwidth Lin	it	
🚯 Add	🔀 Edit 🛛 🛅 🛛	Delete 🛛 🗳 Refre:
Profile	Start IP	End IP

3. The following dialog will appear.



rom start ip	End IP	- EXTIMU - RO	
andwidth Lir	nnt		_
Profile :	Band_limit_1		
👽 Enable	This Profile		
Start IP :	192 . 168 . 1	. 77	
End IP :	192 . 168 . 1	. 82	
TX Limit :	1024	💿 Kbps 🔵 Mbps	
RX Limit :	1024	💿 Kbps i 🔘 Mbps	
		🛗 Apply	/ 🙆 Cancel

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

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

Bandwidth Limit				
🏠 Add 💙	Edit 🛛 前 Delete	🗳 Refresh 🛛 📢	Rename	
Profile	Start IP	End IP	TX Limit	RX Limit
Band_limit_1	192.168.1.77	192.168.1.82	0	0

4.12 System Maintenance

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

Below shows the menu items for System Maintenance.

ystem Maintenanc	
TR-069	
Administrator Pase	sword
Configuration Back	kup
Syslog / Mail Alert	
Time and Date	
Access Control	
SNMP Setup	
Reboot System	
Firmware Upgrade	

4.12.1 TR-069

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

Dray Tek	Vigor 3900 s	eries	15:05:42	Login: Admin	Ð
	System Maintenance >> TR-069				
Auto Logout : Off v Firewall	TR-069				
Objects Setting User Management	Enable This Profile				
Applications	ACS Server URL :				
VPN and Remote Access	ACS Server Username :	acs			
Certificate Management	ACS Server Password				
SSL VPN	WAN Profile	wan1			
Bandwidth Management		8069			
System Maintenance					
		http://:8069/owmp/creq			
Administrator Password	Periodic Status :	📀 Enable 🔘 Disable			
Configuration Backup	Periodic Time :	900			
Syslog / Mail Alert 🗉	CPE Username :	vigor			
Time and Date	CPE Password :				
Access Control					
SNMP Setup					
Reboot System					
Firmware Upgrade					
Diagnostics					
External Devices				Apply	🔇 Cancel
Product Registration					

Item	Description
Enable This Profile	Check this box to enable such profile.
ACS Server URL/Username /Password	Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.



WAN Profile	Choose one of the WAN profiles which will be recognized by VigorACS.
Port	Type the port number for Vigor3900 which will be recognized by VigorACS.
CPE URL	Display the URL of such CPE.
Periodic Status	The default setting is Enable . Please set periodic time for VigorACS to send notification to CPE. Or click Disable to close the mechanism of notification.
Periodic Time	Set the time for VigorACS to send notification to CPE.
CPE Username	Type the user name for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
CPE Password	Type the password for the CPE which will be used by the administrator of VigorACS to log into the WUI of Vigor3900.
Apply	Click it to save the configuration.
Cancel	Click it to discard the settings configured in this page.

4.12.2 Administrator Password

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

Dray Tek	Vigor 3900 Series	15:08:15	Login: Admin	Ð
	System Maintenance >> Administrator Password			
Auto Logout : Off Firewall	Administrator Password			
Objects Setting	Original Password :			
User Management Applications	New Password :			
VPN and Remote Access	Confirm Password :			
Certificate Management	Contirm Password :			
SSL VPN				
Bandwidth Management				
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			l	Apply
Product Registration				

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



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

4.12.3 Configuration Backup

Most of the settings can be saved locally as a configuration file, and can be applied to another router. The router supports functions of **restore and backup** for the configuration file.

Backup

Dray Tek	Vigor 3900 Series	15:10:39	Login: Admin	Ð
Auto Logout: Off	System Maintenance >> Configuration Backup Backup Restore V Encrypt Confi Password : Confirm Password : OBackup to Lo	ig bocal File emote TFTP Server oted Config		
Reboot System Firmware Upgrade Diagnostics			6	Backup
External Devices				

Each item will be explained as follows:

Item	Description	
Encrypt Config	Check this box to encrypt the configuration file.	
	Password – Type a password for encrypting the file.	
	Confirm Password – Retype the password for confirmation.	
Backup Type	Choose one of the types to determine where the file will be stored.	
	Backup to Local File – The configuration file will be stored in local host.	
	Backup to Remote TFTP Server – The configuration file will be stored in the remote TFTP server specified.	
	Backup Selected Config – The configuration file will be stored with an existing file in local host. You must select which file you want to store.	
Config File Name	Display the configuration file name. You can change the name if required.	
Backup	Execute the file downloading job to the computer.	

Dray Tek

Restore

Dray Tek	Vigor 3900 Series	15:11:37	Login: Admin	Ð
	System Maintenance >> Configuration Backup >> Rest	tore		
o Logout : Off 🔍	Backup			
Objects Setting				
User Management	Decrypt Config			
Applications	Password :			
VPN and Remote Access	Confirm Password :			
Certificate Management	• Restore Settings via L	ocal Config File		
SSL VPN	Restore Type : Restore Settings via T	-		
Bandwidth Management		FIP Server		
System Maintenance	Select File : Brow	wse		
TR-069				
Administrator Password				
Configuration Backup				
Syslog / Mail Alert 🗉				
Time and Date				
Access Control				
SNMP Setup				
Reboot System				
Firmware Upgrade				
Diagnostics				💓 Restore
External Devices	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.		
	Password – Type a password for encrypting the file.		
	Confirm Password – Retype the password for confirmation.		
Restore Type	Choose one of the types to determine where the file will be downloaded from.		
	Restore Settings via Local Config File – Click it to restore the configuration settings through a configuration file stored locally.		
	Restore Settings via TFTP Server – Click it to restore the configuration settings through TFTP server.		
Selected File	Use the Browse button to locate the file for uploading to the router.		
Restore	Click it to upload the selected file to the router. After finishing the restoration, the system will ask you to reboot the router.		

4.12.4 Syslog / Mail Alert

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

Syslog Access Setup

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

Auto Logout: Off Freewall System Maintenance >> Syslog / Mail Alert >> Syslog Access Setup Objects Setting Syslog Access Setup User Management Server IP: Applications Server IP: VPN and Remote Access Server Port: Certificate Management Situs: SSL VPN Bandwidth Management System Maintenance Vigor TR-069 User Access Log: Administrator Password E Enable Configuration Backup Sitalia Alert System Enable Time and Date Octors Log: Access Control Sitalia SHMP Setup Reboot System Firmware Upgrade Disable Disgnostics E	Dray Tek	Vigor 3900 Se	eries	15:12:59	Login: Admin	€ ▶
Administrator Password WAN Log: Enable Configuration Backup Enable Disable Systog / Mail Alert E Others Log: © Enable Time and Date Access Control SiNIP Setup Disable Reboot System Firmware Upgrade Diagnostics Diagnostics	Auto Logout : Off Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance	System Maintenance >> Syslog / Syslog Access Setup Syslo Status : Both Server IP : 192 Server Port : 514 Router Name : Vigor Firewall Log : O Er VPN Log : O Er	Mail Alert >> Syslog Access 5 sg File Mail Alert 	Setup	Login: Admin	
Learned version	Configuration Backup Syslog / Mail Alert Time and Date Access Control SIMP Setup Reboot System Firmware Upgrade Diagnostics External Devices	WAN Log : O Er	nable 💿 Disable		🛗 Apply 📢	Cancel

Item	Description	
Status	Choose one of the selections to determine current status for Syslog access. If you choose Local as Status, you don't need to type any server IP and port. Just give a name for the router.	
	Disable Disable Remote Local Both	
Server IP	Type the IP address of the Syslog server.	
Server Port	Type the port number for the Syslog server.	
Router Name	Type the name of the router. The default name is <i>Vigor</i> .	
Firewall Log	Click Enable to make the firewall log recorded in the Syslog.	
VPN Log	Click Enable to make the VPN log recorded in the Syslog.	
User Access Log	Click Enable to make the user access log recorded in the Syslog.	

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

SysLog File

Dray Tek	Vigor 3900 Series	15:14:25	Login: Admin	e
	System Maintenance >> Syslog / Mail Alert >> Syslog F	ile		
Logout : Off	Syslog Access Setup Syslog File Mail Alert			
Objects Setting	🔊 Refresh			
User Management	Log			
Applications	ng nameserver 168.95.192.1#53(via wan-wan3)			*
VPN and Remote Access	<30>Aug 21 15:11:38 Vigor: dnsmasq[8606]: using na	meserver 8.8.8.8#53(via wan-wan4)		
Certificate Management	<30>Aug 21 15:11:38 Vigor: dnsmasq[8606]: using loc	al addresses only for domain lan		-
SSL VPN	<30>Aug 21 15:11:42 Vigor: dnsmasq[8606]: reading	/tmp/resolv.conf.auto		
Bandwidth Management	<30>Aug 21 15:11:42 Vigor: dnsmasq[8606]: using na	meserver 168.95.1.1#53(via wan-war	13)	
System Maintenance	<30>Aug 21 15:11:42 Vigor: dnsmasq[8606]: using na	meserver 168.95.192.1#53(via wan-v	van3)	
TR-069	<30>Aug 21 15:11:42 Vigor: dnsmasq[8606]: using na	meserver 8.8.8.8#53(via wan-wan4)		
Administrator Password	<30>Aug 21 15:11:42 Vigor: dnsmasq[8606]; using loc	al addresses only for domain lan		
Configuration Backup	<28>Aug 21 15:11:52 Vigor: pppd[3824]: Timeout wa	iting for PADO packets		
Syslog / Mail Alert 🗄	<27>Aug 21 15:11:52 Vigor: pppd[3824]: Unable to co	omplete PPPoE Discovery		
Time and Date	<30>Aug 21 15:11:58 Vigor: dnsmasq[8606]: reading	/tmp/resolv.conf.auto		
Access Control	<30>Aug 21 15:11:58 Vigor: dnsmasq[8606]; using na	meserver 168.95.1.1#53(via wan-war	13)	
SNMP Setup	<30>Aug 21 15:11:58 Vigor: dnsmasq[8606]: using na	meserver 168.95.192.1#53(via wan-v	van3)	
Reboot System	<30>Aug 21 15:11:58 Vigor: dnsmasq[8606]: using na	meserver 8.8.8.8#53(via wan-wan4)		
Firmware Upgrade	<30>Aug 21 15:11:58 Vigor: dnsmasq[8606]: using loc	al addresses only for domain lan		
Diagnostics	<28>Aug 21 15:12:07 Vigor: pppd[3824]: Timeout wa	iting for PADO packets		
External Devices	<27>Aug 21 15:12:07 Vigor: pppd[3824]; Unable to co	molete PPPoE Discovery		+

Item	Description
Refresh	Renew the web page.

Mail Alert

Dray Tek	Vigor 390	0 Series	15:16:13	Login: Admin	Ð
	System Maintenance >> S	yslog / Mail Alert >> Mail Alert			
to Logout : Off v	Syslog Access Setup	Syslog File Mail Alert			
Objects Setting User Management	Enable This Pro	ofile			*
Applications	Mail From :				
VPN and Remote Access		🕼 Add 💾 Save			
SSL VPN		Mail To			
Bandwidth Management		No items to show.			
System Maintenance					
TR-069	Mail To :				E
Administrator Password					
Configuration Backup					
Syslog / Mail Alert 🗧 🗧					
Time and Date					
Access Control SNMP Setup	SMTP Port :	25			
Reboot System	SMTP Server :		1		
Firmware Upgrade	lless Lesie :	O Enable 🕢 Disable			
Diagnostics	User Login :	Ulsable			-
External Devices				Apply	🐼 Cancel

Item	Description		
Enable This Profile	Check the box to enable such profile.		
Mail From	Type a mail address for the mail sender.		
Mail To	Assign a mail address for the mail receiver.		
SMTP Port	Type the port number for SMTP server.		
SMTP Server	Type the IP address for SMTP server.		
User Login	Click Enable to make any user logging into the mail server. If you click Enable , you have to type user name and user password on the below fields.		
User Name	Type the user name for authentication.		
User Password	Type the password for authentication.		
Apply	Click this button to save the configuration and exit the web page.		
Cancel	Click it to discard the settings configured in this page.		

4.12.5 Time and Date

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

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

Auto Logout: Off Freewall Ime and Date Objects Setting Ime and Date User Management Server: Applications Port: VPN and Remote Access Certificate Management Skytem Maintenance Skytem Maintenance Time and Date Time and Date Mathemanet System Maintenance Time and Date Time and Date Certificate Management System Maintenance Time Zone: Tapei Daignostics Diagnostics External Devices Product Registration

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



4.12.6 Access Control

This page allows you to open or close the web configurator of Vigor 3900 by using Telnet, SSH, HTTP, HTTPS... and etc...

Dray Tek	Vigor 3900	Series	15:21:15	Login: Admin	Ð
	System Maintenance >> Ac	cess Control			
Auto Logout : Off	Access Control				
Objects Setting					*
User Management	Web Allow :	💿 Enable 🔘 Disable			
Applications	Web Port :	8080]		
VPN and Remote Access	Telnet Allow :	Enable O Disable			
Certificate Management	Telnet Port :	23	7		
SSL VPN	SSH Allow :	C Enable () Disable			
Bandwidth Management		22	7		
System Maintenance	SSH Port :	22			E
TR-069	HTTPS Allow :	📀 Enable 🔘 Disable			
Administrator Password	HTTPS Port :	4433			
Configuration Backup	User Define :	C Enable 💽 Disable			
Syslog / Mail Alert 🗉	User Define :	C Enable O Disable			
Time and Date	Allowed IP1 :	0 0 0	0.0.0.0	~	
Access Control					
SNMP Setup	Allowed IP2 :	0.0	0.0.0.0	*	
Reboot System		0 0 0	0 0.0.0.0		
Firmware Upgrade	Allowed IP3 :	0.0.0	. 0.0.0.0	~	-
Diagnostics	4		111		
External Devices				Apply	🐼 Cancel
Product Registration					

Item	Description	
Web Allow	Click Enable to allow system administrator to login from the Internet and management the web page of the router.	
Web Port	Type the port number for the management through web page.	
Telnet Allow	Click Enable to allow system administrator to login from the telnet and management the web page of the router.	
Telnet Port	Type the port number for the management through telnet page.	
SSH Allow	Click Enable to allow system administrator to login from the SSH server and management the web page of the router.	
SSH Port	Type the port number for the management through SSH server.	
HTTPS Allow	Click Enable to allow system administrator to login from the HTTPS server and management the web page of the router.	
HTTPS Port	Type the port number for the management through HTTPS server.	
User Define	Click Enable to allow system administrator to login from the user defined IP address and management the web page of the router. If you enable such function, the system can be managed by these three IP addresses via WAN.	
Allowed IP1 - Allowed IP3	Type the first IP address for the system administrator to login. The former box indicates an IP address allowed to login to the	

	router, and the later box indicates a subnet mask allowed to login to the router.
Allow Ping from WAN	Click Enable to allow system administrator to ping the router from WAN interface.
Allow Ping form LAN	Click Enable to allow system administrator to ping the router from LAN interface.
Apply	Click this button to save the configuration and exit the web page.
Cancel	Click it to discard the settings configured in this page.

4.12.7 SNMP Setup

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

Dray Tek	Vigor 3900 Series	15:22:05	Login: Admin	Ð
Auto Logout: Off	System Maintenance >> SNMP Agent SHMP Agent C Enable This Profile Get Community : public Set Community : private Manager Host IP : 192.168.139.10/32			
External Devices			Apply	🐼 Cancel

Available parameters are listed as follows:

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



4.12.8 Reboot System

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

If you want to reboot the router using the current configuration, choose **Reboot with Current Configurations** and click **Reboot**. To reset the router settings to default values, click **Reboot with Factory Default Configurations** and click **Reboot**. The router will take a period of time to reboot the system.

Open System Maintenance>> Reboot System.

Auto Logout: Off Firewall Objects Setting User Management Applications Applications Reboot with Current Configurations Certificate Management Reboot with Customized Configurations System Maintenance Reboot with Customized Configurations System Maintenance Reboot office Time and Date Access Control SIMP Setup Firmware Upgrade Diagnostics External Devices	Dray Tek	Vigor 3900 Series	15:25:23	Login: Admin	Ð
Diagnostics C Reboot	Auto Logout: Off Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance TR-069 Administrator Password Configuration Baokup Syslog / Mail Alert Time and Date Access Control SNMP Setup Reboot System	System Maintenance >> Reboot System >> Reboot Reboot System Schedule Reboot Reboot Option : Reboot with Curren Reboot Option : Reboot with Factor Reboot with Custor	t Configurations y Default Configurations nized Configurations		
	Diagnostics	4	11	٢	

Available parameters are listed as follows:

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

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

4.12.9 Firmware Upgrade

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

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

Click System Maintenance>> Firmware Upgrade.

Dray Tek		Vigor 3900 Series	15:37:21	Login: Admin	Đ
		System Maintenance >> Upgrade Firmware			
Auto Logout : Off v		Upgrade Firmware			
Objects Setting					
User Management		Current Firmware Version : 1.0.5RC9			
Applications		Select File :	Browse		
VPN and Remote Access					
Certificate Management					
SSL VPN					
Bandwidth Management					
System Maintenance					
TR-069					
Administrator Password	- 11				
Configuration Backup	- 11				
Syslog / Mail Alert	-				
Time and Date	- 1				
Access Control	- 11				
SNMP Setup	- 11				
Reboot System					
Firmware Upgrade					
Diagnostics				2	🕈 Upgrade
External Devices				(g upgrade
Product Registration	-				

Available parameters are listed as follows:

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

4.13 Diagnostics

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

D	iagnostics	-
	Routing Table	
	ARP Cache Table	
	DHCP Table	
	NAT Session Table	
	Traffic Graph	
	Web Console	
	Ping/Trace Route	
	Data Flow Monitor	

4.13.1 Routing Table

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

Routing Table

Display the information for each route.

Dray Tek	Vigor 39	00 Series		15:39:41	Log	in: Admin	E
	Diagnostics >> Routi	ng Table >> Routing Ta	ble				
D Logout : Off		Pv6 Routing Table					
Firewall	🐼 Refresh						
Objects Setting	Destination	Gateway	Genmask	Flags	Metric	Iface	
User Management	2.2.2.70	168.95.98.254	255.255.255.255	UGH	0	wan-wan3	
Applications	172.17.3.70	172.16.2.4	255,255,255,255	UGH	0	wan-wan4	
VPN and Remote Access	168.95.98.254	0.0.0.0	255 255 255 255	UH	0	wan-wan3	
Certificate Management	192,168,100.0	0.0.0.0	255.255.255.0	0	0	lan-lan100	
SSL VPN	192,168,128,0	168 95 98 254	255,255,255,0	ug	0	wan-wan3	
Bandwidth Management	192.168.33.0	0.0.0.0	255.255.255.0	U	0	lan-1	
System Maintenance	192,168,93,0	168 95 98 254	255 255 255 0	ug	0	wan-wan3	
Diagnostics	192.168.139.0	0.0.0.0	255.255.255.0	U	0	lan-lan1	
Routing Table	192 168 11 0	172 16 1 1	255.255.255.0	ug	0	wan-wan4	
ARP Cache Table		172.16.2.5	255.255.255.0	UG	0	wan-wan4	
DHCP Table	172.16.0.0	0.0.0	255.255.0.0	U	0	wan-wan4	
NAT Session Table	default	172.16.1.1	0.0.0.0	ug	0	wan-wan4	
Traffic Graph	derault	172.10.1.1	0.0.0.0	00	U	wan-wan4	
Web Console							
Ping/Trace Route							
Data Flow Monitor							
External Devices							
Product Registration +							

Item	Description
Refresh	Renew the web page.
Destination	Display the destination IP address for various routings.
Gateway	Display the default gateway.
Genmask	Display the subnet mask for various routings.

Flags	Display the flag of the routing entry. Possible flags include:
	U (route is up)
	H (target is a host)
	G (use gateway)
	R (reinstate route for dynamic routing)
	D (dynamically installed by daemon or redirect)
	M (modified from routing daemon or redirect)
	A (installed by <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).

IPv6 Routing Table

Display the information for each route with IPv6 protocol.

Dray Tek	Vigor 39	00 Series	15	:41:21	Login: Admin	Ð
	Diagnostics >> Routing	g Table >> IPv6 Routing T	able			
Logout : Off	Routing Table IP	v6 Routing Table				
Firewall	🖨 Refresh					
Objects Setting	Destination	Next Hop	Flags	Metric	Iface	
User Management	fe80::/64		U	258	eth0	-
Applications	fe80::/64		U	258	eth2	E
VPN and Remote Access	fe80::/84		U	258	lan-lan1	
Certificate Management	fe80::/64		U	258	eth2.12	
SSL VPN	fe80::/64		U	256	lan-lan100	
Bandwidth Management	fe80::/64		U	256	lan-1	
System Maintenance	fe80::/84		U	258	lan-lantest	
Diagnostics	fe80/84		U	258	wan-wan4	
Routing Table	fe80::/64		U	258	eth2 10	
ARP Cache Table	fe80::/84		U	258	wan-Marketing	
DHCP Table	::1/128		U	0	lo	
NAT Session Table	fe80::/128		U	0	10	
Traffic Graph	fe80::/128		U	0	10	
Web Console				-	-	
Ping/Trace Route	fe80::/128		U	0	lo	
Data Flow Monitor	fe80::/128		U	0	lo	
External Devices	fe80::/128		U	0	lo	
Product Registration +	fe80::/128		U	0	lo	-

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



	R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by addrconf) C (cache entry) ! (reject route)
Metric	Display the distance to the target (usually counted in hops). It may be needed by routing daemons.
Iface	Display the direction of such route represented with LAN/WAN profile (starting from LAN/WAN profile to LAN/WAN profile).

4.13.2 ARP Cache Table

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

ARP Cache Table

Dray Tek	Vi	gor 39	00 Series		15:42:38	Logir	n: Admin	Ð
	Diagno	stics >> ARP Ca	che Table >> ARP Ca	che Table				
uto Logout : Off 🛛 🗸	AR	P Cache Table	IPv6 Neighbor Table					
Firewall		🗳 Refresh	🔞 Clear All					
Objects Setting	IP /	Address	HW Type	MAC Address	Flags	Profile	Clear	
User Management		16.3.103	ether	00:50:7f:00:00:02	c	wan-wan4	蕭	
Applications		18.2.8	ether	00:0c:29:77:4d:b8	c	wan-wan4	m	
VPN and Remote Access		18.1.1	ether	00:1d:aa:a1:31:d8	c	wan-wan4	m	
Certificate Management		16.2.215	ether	00:0c:8e:0e:0c:27	c	wan-wan4	THE	
SSL VPN	2	.168.139.10	ether	00:1d:60:59:0d:1b	c	lan-lan1	, mu	
Bandwidth Management		.16.2.201	ether	00:50:7f:ed:e1:51	c	wan-wan4	THE	
System Maintenance		. 10.2.201	etter	00.00.11.60.61.01	0	Wall-Wall-Y	mu	
Diagnostics								
Routing Table								
ARP Cache Table 🗧								
DHCP Table	555							
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	Description
Refresh	Renew the web page.
Clear All	Remove all of the information from this page.
IP Address	Display the IP address for different ARP cache.
HW type	Display the hardware type of the address from RFC 826.
MAC Address	Display the MAC address for different ARP cache.
Flags	Each complete entry in the ARP cache will be marked with the flag of 0x2. Permanent entries are marked with 0x4 and published entries have the 0x8 flag.
Profile	Display the direction of such route represented with

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

IPv6 Neighbor Table

Dray Tek	Vigor 39	00 Series	15:43:31	Login: Admin	Ð
	Diagnostics >> ARP (Cache Table >> IPv6 Neighbor Table			
Logout : Off 🗸	ARP Cache Table	IPv6 Neighbor Table			
Firewall	🖨 Refresh				
Objects Setting	IP Address	Profile	MAC Address	Status	
User Management	fe80::250:7fff.fe71	:738 wan-wan4	00:50:7f:71:07:38	router STALE	
Applications	fe80::21d:aaff:feat	8:2628 wan-wan4	00:1d:aa:a6:26:28	router STALE	
VPN and Remote Access					
Certificate Management					
SSL VPN					
Bandwidth Management					
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					

Item	Description
Refresh	Renew the web page.
IP Address	Display the IPv6 address of the neighbor.
Profile	Display the interface to which this neighbor is attached.
MAC Address	Display the MAC address of the neighbor.
Status	Display the status for such neighbor.
	INCOMPLETE - Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.
	REACHABLE - The neighbor is reachable recently (within tens of seconds ago).
	STALE -The neighbor is no longer to be reachable. Yet, until traffic is sent to the neighbor, no attempt should be made to verify its reachability.
	DELAY - The neighbor is no longer to be reachable, and the traffic has recently been sent to the neighbor.
	Rather than probe the neighbor immediately, however, delay sending probes for a short while in order to give upper layer protocols a chance to provide reachability confirmation.
	PROBE - The neighbor is no longer to be reachable, and unicast Neighbor Solicitation probes are being sent to verify



Item	Description
	reachability.

4.13.3 DHCP Table

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

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

Dray Tek	vig	or 39	00 Series	•	15:44:14	Logii	n: Admin 🕞
	Diagnosti	cs >> DHCP	Table				
Logout : Off v	DHCF	P Table					
Firewall	ç	Refresh					
Objects Setting	IP Add	dress	Start Date	Start Time	End Date	End Time	Mac Address
User Management	192.16	38,139,10	2012/08/21	14:21:28	2012/08/22	14:21:28	00:1d:60:59:0d:1b
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Bandwidth Management							
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							

Item	Description
Refresh	Renew the web page.
IP Address	Display the IP address of the static DHCP server.
Start Date	Display the starting date that DHCP server is activated.
Start Time	Display the starting time that DHCP server is activated.
End Date	Display the end date that DHCP server is closed.
End Time	Display the end time that DHCP server is closed.
Mac Address	Display the MAC address of the static DHCP server.

4.13.4 NAT Session Table

This table can display about 30000 sessions with 20 pages.

Dray Tek		Vigor 390	00 Series		15:45:02	Login:	Admin	Ð
		Diagnostics >> NAT See	ssion Table					
Logout : Off 🗸 🗸		NAT Session Table						
Firewall		🖨 Refresh						
Objects Setting User Management		Source	Destination	WAN	Protocol	State	TTL	
user management		192.168.139.10:59	74.125.235.222:443	172.18.2.194	top	ESTABLISHED	0:03:16	-
		192.168.139.10:59	172.16.2.17:443	172.18.2.194	top	TIME_WAIT	0:00:13	
VPN and Remote Access		192.168.139.10:59	23.48.2.110:443	172.16.2.194	top	TIME_WAIT	0:00:53	
Certificate Management		192.168.139.10:59	23.48.15.139:443	172.16.2.194	top	ESTABLISHED	23:59:23	
SSL VPN		192.168.139.10:59	69.171.242.70:443	172.16.2.194	top	ESTABLISHED	23:59:57	
Bandwidth Management		192.168.139.10:59	172.16.2.17:443	172.16.2.194	top	TIME_WAIT	0:01:43	
System Maintenance		192.168.139.10:59	172.18.2.17:443	172.18.2.194	tap	TIME_WAIT	0:00:43	
Diagnostics		192.168.139.10:59	173.194.72.101:443	172.18.2.194	tap	ESTABLISHED	23:59:18	
Routing Table		192.168.139.10:59	172.18.2.17:443	172.16.2.194	top	TIME WAIT	0:00:43	-
ARP Cache Table	E	192,168,139,10:59	23.48.2.110:443	172.16.2.194	top	TIME_WAIT	0:00:23	
DHCP Table		192,168,139,10:59	172.18.2.17:443	172.16.2.194	tao	TIME_WAIT	0:00:13	
NAT Session Table		192 168 139 10 59	173.194.72.101:443	172 18 2 194	top	ESTABLISHED	0:02:53	
Traffic Graph		192.168.139.10:59		172.16.2.194	tao	TIME_WAIT	0:00:53	
Web Console		192,168,139,10:59		172.18.2.194	tao	TIME_WAIT	0:00:13	
Ping/Trace Route	- 11		173.194.72.95:443	172.18.2.194	tao	ESTABLISHED	23:59:23	
Data Flow Monitor			173.194.72.190:443		top	ESTABLISHED	23:59:58	
External Devices		192.168.139.10:59		172.16.2.194	top	TIME WAIT	0:00:13	-

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

4.13.5 Traffic Graph

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

Dray Tek		Vigor 3900 Series	15:54:00	Login: Admin	Ð	^
Auto Logout: Off v Firewall Objects Setting User Management Applications VPN and Remote Access Certificate Management SSL VPN Bandwidth Management System Maintenance Diagnostics	2.6	Diagnostics >> Traffic Graph >> Setup Setup CPU Memory P Enable This Profile LAN : Ian1 v WAN : wan2.wan3.wan4 v				and the second se
Routing Table ARP Cache Table DHCP Table NAT Session Table Traffic Graph Web Console Pling/Trace Route Data Flow Monitor External Devices	E				Apply	

Each item will be explained as follows:

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

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

Below show a graphic for CPU:



4.13.6 Web Console

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

: 해외(D)	C http://192.168.1.1/webshell/
login:	

4.13.7 Ping/Trace Route

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

Dray Tek		Vigor 3900 Series	15:58:29	Login: Admin	•
		Diagnostics >> Ping/Trace Route			
Auto Logout : Off		Ping/Trace Route			
Firewall	-				
Objects Setting					
User Management					
Applications					
VPN and Remote Access					
Certificate Management					
SSL VPN					
Bandwidth Management					
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		Ping O TraceRoute Host :	Interface : lan1	💌 🕟 Start 🤇) Stop
Product Registration	-				

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

4.13.8 Data Flow Monitor

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

Dray Tek		Vigor 3	900 Series	15:59:21	L	ogin: Admin	Ð
		Diagnostics >> Dat	a Flow Monitor				
Auto Logout : Off		Data Flow Moni	itor				
Firewall	-	Enable Data	aflow Monitor 🛛 🗳 Refre	sh 👹 Chart 🔛 Block	📰 UnBlock 💽	Recent 1 Hours 🔿 Rec	ent 24 Hours
Objects Setting		IP Address	TX rate(Kbps)	RX rate(Kbps)	Sessions	Block Time	
User Management							
Applications				No items to show.			
VPN and Remote Access	- 11						
Certificate Management	- 11						
SSL VPN							
Bandwidth Management							
System Maintenance							
Diagnostics							
Routing Table	- 11						
ARP Cache Table	Ε						
DHCP Table							
NAT Session Table							
Traffic Graph							
Web Console							
Ping/Trace Route							
Data Flow Monitor							
External Devices							
Product Registration	-	4					>

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



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

4.14 External Devices

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

Dray Tek		Vigor 39	000 Series	16:03	:05 Lo	ogin: Admin	Ð
Auto Logout : Off		External Devices >> External Devices	External Devices				
WAN		Status	ernal Devices 📢 Refresh Model Name	IP Address	Connection Time	Clear	
NAT				No items to she	ow.		
Firewall Objects Setting							
User Management Applications							
VPN and Remote Access	E						
Certificate Management SSL VPN							
Bandwidth Management System Maintenance							
Diagnostics							
Routing Table ARP Cache Table							
DHCP Table NAT Session Table							
Traffic Graph	-]

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

Each item will be explained as follows:

From this web page, check the box of **Enable External Devices**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

Note: Only DrayTek products can be detected by this function.

4.15 Product Registration

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

This page is left blank.

Chapter 5: Trouble Shooting

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

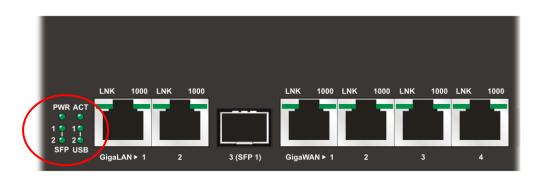
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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



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

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

For Windows



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

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



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



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

🕹 eth0 Properties 🛛 🔹 🔀
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Ir
This connection uses the following items:
 ✓ ■ Client for Microsoft Networks ✓ ■ File and Printer Sharing for Microsoft Networks ✓ ■ QoS Packet Scheduler ✓ Thermet Protocol (TCP/IP)
Install Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 ✓ Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity
OK Cancel

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

Internet Protocol (TCP/IP) Prop	erties 🛛 🛛 🔀
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
Obtain an IP address automatica	ally
Use the following IP address: —	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
⊙ D <u>b</u> tain DNS server address auto	matically
OUse the following DNS server ac	idresses:
Preferred DNS server:	and the second second
Alternate DNS server:	
	Ad <u>v</u> anced
	OK Cancel

For Mac OS

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

⊖ ⊖ ○	Network	0
Show All Displays Sou	Network Startup Disk	
L	ocation: Automatic 🛟 Show: Built-in Ethernet 🛟	
Configure IPv4:		
IP Address:		P Lease
Subnet Mask:	255.255.255.0 DHCP Client ID: (If required)	
Router:		
DNS Servers:		(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	?
Click the lock to p	vrevent further changes.	Apply Now

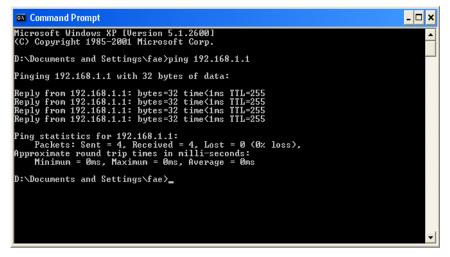
5.3 Pinging the Router from Your Computer

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.

$\Theta \Theta \Theta$	Terminal — bash — 80x24	
Welcome to Darwin! Vigor10:~ draytek\$; PING 192.168.1.1 (19 64 bytes from 192.10 64 bytes from 192.10	3 02:24:18 on ttyp1 ping 192.168.1.1 92.168.1.1): 56 data bytes 68.1.1: icmp_seq=0 ttl=255 time=0.755 ms 68.1.1: icmp_seq=1 ttl=255 time=0.697 ms 68.1.1: icmp_seq=2 ttl=255 time=0.716 ms	8
64 bytes from 192.10	68.1.1: icmp_seq=3 ttl=255 time=0.731 ms 68.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
5 packets transmitte	ed, 5 packets received, 0% packet loss max = 0.697/0.723/0.755 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.

Device Information					System Information						
Model : Vigor3900 Hardware : 1.0 Firmware : 1.0.5RC9 Build Date : 2012-08-07 18:04:09 Revision : 1210			11111	CPU Usage : 23% Memory Usage : 24 % Coprocessor : CPU Usag System Up Time : 5 days 6:8 Current System Time : Tue Aug 1			5				
IPv4		IPv6									
Profile	Connecti	Uptime	MAC	Protocol	IP	Gateway	DNS	RX Packe	TX Packe	Operation	
an1	up	5 days 6:	00:50:7F:	static(NAT)) 192.168			517583	1142956		
an100	up	0 days 0:	00:50:7F:	static(NAT)) 192.168			0	341		
wan2	up	0 days 0:	00:50:7F:	pppoe(N	111.243	168.95.9	168.95.1	1063	851	X	
wan4	up	0 days 0:	00:50:7F:	static(NAT)) 172.16.2	172.16.1.1	8.8.8.8	50850	2754		

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



Dray Tek	Vigo	r 3900 s	eries	17:10:24		Login: Admin	Ð
	WAN >> Gen	eral Setup					
Auto Logout : Off 🔹 👻	General	Setup					
Quick Start Wizard	× E	dit 🔇 Refresh	Mode : Basic	~		Profil	e Number Limit : 50
Online Status		-					
WAN	Profile	Enable This F	Description VLA	N ID VLAN Tag	Port	IPv4 Protoco	I IPv6 Protocol
General Setup	wan1	false	10	Disable	WAN1	None	Link-Local
Default Route	wan2	true	11	Disable	WAN2	PPPoE	Link-Local
Load Balance	wan3	false	12	Disable	WAN3	PPPoE	Link-Local
Switch	wan4	true	13	Disable	WAN4	Static	Link-Local
LAN	wan5	false	14	Disable	WAN5	None	Link-Local
NAT							
Firewall							
Objects Setting							
User Management							
Applications							
VPN and Remote Access							
Certificate Management							
SSL VPN							
Bandwidth Management							
System Maintenance							
Diagnostics							

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	
		と Reboot

Hardware Reset

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



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

5.6 Contacting 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>**.

