

# Vigor2860 Series

**VDSL2** Security Firewall



Your reliable networking solutions partner

# User's Guide

# Vigor2860 Series VDSL2 Security Firewall User's Guide

Version: 1.0 Firmware Version: V3.7.1\_RC5a (For future update, please visit DrayTek web site) Date: 22/02/2013



# **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	<ul> <li>The following trademarks are used in this document:</li> <li>Microsoft is a registered trademark of Microsoft Corp.</li> <li>Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.</li> <li>Apple and Mac OS are registered trademarks of Apple Inc.</li> <li>Other products may be trademarks or registered trademarks of their respective manufacturers.</li> </ul>

# Safety Instructions and Approval

Safety Instructions	<ul> <li>Read the installation guide thoroughly before you set up the router.</li> <li>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.</li> <li>Do not place the router in a damp or humid place, e.g. a bathroom.</li> <li>The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.</li> <li>Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.</li> <li>Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.</li> <li>Keep the package out of reach of children.</li> <li>When you want to dispose of the router, please follow local regulations on conservation of the environment.</li> </ul>
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, Hsinchu County, Taiwan 303Product:Vigor2860 Series Router

DrayTek Corp. declares that Vigor2860 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE 1999/5/EC, ErP 2009/125/EC and RoHS 2011/65/EU.

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 B and EN55024/Class B.

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 B 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



This product is designed for the DSL and 2.4GHz WLAN network throughout the EC region. Please see the user manual for the applicable networks on your product.



# Table of Contents



Introduction	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor2860 1.2.2 For Vigor2860n	. 2
1.3 Hardware Installation	6
1.4 Printer Installation	7



Basic Settings	13
2.1 Accessing Web Page	13
2.2 Changing Password	15
2.3 Quick Start Wizard	16
2.3.1 For WAN1 (ADSL/VDSL) 2.3.2 For WAN2 (Ethernet) 2.3.3 For WAN3 (USB)	
2.4 Service Activation Wizard	33
2.5 Introducing Dashboard	
<ul> <li>2.5.1 Virtual Panel</li> <li>2.5.2 Name with a Link</li> <li>2.5.3 Quick Access for Common Used Menu</li> <li>2.5.4 GUI Map</li> <li>2.5.5 Web Console</li> <li>2.5.6 Config Backup</li> </ul>	
2.6 Online Status	42
2.6.1 Physical Connection 2.6.2 Virtual WAN	
2.7 Saving Configuration	45
2.8 Registering Vigor Router	



Web Configuration	51
3.1 WAN	51
3.1.1 Basics of Internet Protocol (IP) Network	
3.1.2 General Setup	
3.1.3 Internet Access	
3.1.4 Multi-PVCs	
3.1.5 Multi-VLAN	
3.1.6 Load-Balance Policy	



3.2 LAN	99
3.2.1 Basics of LAN	99
3.2.2 General Setup	
3.2.3 Static Route	
3.2.4 VLAN	
3.2.5 Bind IP to MAC	
3.2.6 LAN Port Mirror	
3.2.7 Web Portal Setup	121
3.3 NAT	123
3.3.1 Port Redirection	124
3.3.2 DMZ Host	
3.3.3 Open Ports	
3.3.4 Address Mapping	
3.3.5 Port Triggering	
3.4 Firewall	
3.4.1 Basics for Firewall	
3.4.2 General Setup	
3.4.3 Filter Setup	
3.4.4 DoS Defense	152
3.5 User Management	156
3.5.1 General Setup	157
3.5.2 User Profile	
3.5.3 User Group	
3.5.4 User Online Status	
3.6 Objects Settings	
3.6.1 IP Object	
3.6.2 IP Group	
3.6.3 IPv6 Object	
3.6.4 IPv6 Group	
3.6.5 Service Type Object	
3.6.6 Service Type Group 3.6.7 Keyword Object	
3.6.8 Keyword Group	
3.6.9 File Extension Object	
3.6.10 SMS/Mail Service Object	
3.6.11 Notification Object	
3.7 CSM Profile	
	-
3.7.1 APP Enforcement Profile	
3.7.2 URL Content Filter Profile	
3.7.3 Web Content Filter Profile	195
3.8 Bandwidth Management	199
с. С	
3.8.1 Sessions Limit 3.8.2 Bandwidth Limit	
3.8.3 Quality of Service	
3.9 Applications	210
3.9.1 Dynamic DNS	210
3.9.2 Schedule	213
3.9.3 RADIUS	
3.9.4 LDAP /Active Directory Setup	
3.9.5 UPnP	
3.9.6 IGMP	
3.9.7 Wake on LAN	223



3.9.8 SMS /	/ Mail Alert Service	224
3.10 VPN and	Remote Access	226
3.10.2 VPN 3.10.3 Rem 3.10.4 PPP 3.10.5 IPSe 3.10.6 IPSe 3.10.7 Oper 3.10.8 Rem 3.10.9 LAN 3.10.10 VPI	Client Wizard Server Wizard ote Access Control General Setup c General Setup c Peer Identity nVPN General Setup ote Dial-in User to LAN N TRUNK Management nnection Management	233 238 240 242 244 245 245 248 259
	e Management	
3.11.2 Trust	I Certificate ted CA Certificate ficate Backup	273
	LAN	
	c Concepts	
	urity	
3.12.5 WPS	S	283
3.12.7 Adva	anced Setting	289
3.12.9 AP D	M Configuration	292
	tion List	
	eral Setup Web Proxy	
	Application	
	Group	
3.13.6 Onlir	ne User Status	301
	plication	
	General Settings User Management	
	Explorer	
	Disk Status	
	og Explorer perature Sensor	
3.15 System N	Maintenance	310
	em Status	
	69 inistrator Password	
3.15.4 User	Password	314
	n Customization	
	iguration Backup og/Mail Alert	
3.15.8 Time	and Date	322
	agement	
	nware Upgrade	



15.12 Activation	327
6 Diagnostics	328
16.1 Dial-out Triggering	
16.2 Routing Table	330
.16.3 ARP Cache Table	331
16.4 IPv6 Neighbour Table	331
.16.5 DHCP Table	332
16.6 NAT Sessions Table	333
16.7 Ping Diagnosis	334
16.8 Data Flow Monitor	335
16.9 Traffic Graph	
16.10 Trace Route	
16.11 Web Firewall Syslog	
16.12 TSPC Status	
7 External Devices	
17.1 All Devices	
17.2 Access Point Devices	



Tutorials and Applications3	849
4.1 How to configure settings for IPv6 Service in Vigor2860	349
4.2 How to establish OpenVPN - host to LAN tunnels(authenticated without CA) via SmartVPI Client?	
4.3 How can I get the files from USB storage device connecting to Vigor router?	363
4.4 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPSec Tun (Main Mode)	
4.5 How to Optimize the Bandwidth through QoS Technology	370
4.6 QoS Setting Example	374
4.7 How to Implement the LDAP/AD Authentication for User Management?	378
4.8 How to use Landing Page Feature	381
4.9 How to Send out SMS via Vigor Router	385
4.10 How to Create an Account for MyVigor	388
4.10.1 Create an Account via Vigor Router	
4.11 How to Setup Address Mapping	396
4.12 How to Configure Certain Computers Accessing to Internet 4	400
4.13 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter	404



Trouble Shooting	.409
5.1 Checking If the Hardware Status Is OK or Not	409
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	410
5.3 Pinging the Router from Your Computer	412



5.4 Checking If the ISP Settings are OK or Not	413
5.5 Problems for 3G Network Connection	413
5.6 Backing to Factory Default Setting If Necessary	414
5.7 Contacting Your Dealer	415



Vigor2860 series is a VDSL2 router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DES, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to **32** VPN tunnels.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside. Object-based firewall is flexible and allows your network be safe.

In addition, Vigor2860 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2860 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

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

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

Note: For the other buttons shown on the web pages, please refer to Chapter 3, 4 for detailed	
Delete	Delete the selected item with the corresponding settings.
Edit	Edit the settings for the selected item.
Add	Add new settings for specified item.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Cancel	Cancel current settings and recover to the previous saved settings.
OK	Save and apply current settings.

explanation.

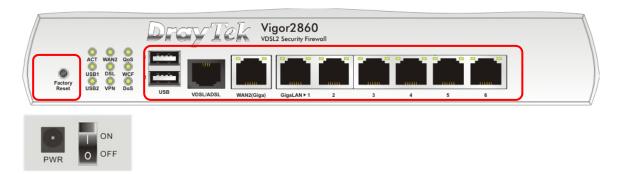
#### **1.2 LED Indicators and Connectors**

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

### 1.2.1 For Vigor2860

$\int$		$\square$		ר	Dre	γT	ek vi	gor2860	) wali					
		0	0	QoS			8					÷		
1	Factory Reset	۲	0	WCF O DoS	2	<b>L</b>								
/	Reset	0352	P N	003	USB	VDSL/ADSL	WAN2(Giga)	GigaLAN ► 1	2	3	4	5	6	

LED		Status	Explanation			
ACT (Activ	vity)	Blinking	The router is powered on and running normally.			
		Off	The router is powered off.			
USB1~2		On	USB device is connected and ready for use.			
		Blinking	The data is transmitting.			
WAN2		On	Internet connection is ready.			
		Off	Internet connection is not ready.			
		Blinking	The data is transmitting.			
DSL		On	The router is ready to access Internet through DSL link.			
		Blinking	Slowly: The DSL connection is ready.			
			Quickly: The connection is training.			
VPN		On	The VPN tunnel is active.			
QoS		On	The QoS function is active.			
WCF	WCF		The Web Content Filter is active. (It is enabled from			
			Firewall >> General Setup).			
DoS		On	The DoS/DDoS function is active.			
		Blinking	It will blink while detecting an attack.			
LED on Co	nnector					
	Left	On	The port is connected.			
WAN2	LED	Off	The port is disconnected.			
(Giga)		Blinking	The data is transmitting.			
	Right	On	The port is connected with 1000Mbps.			
	LED	Off	The port is connected with 10/100Mbps			
	Left	On	The port is connected.			
GigaLAN	LED	Off	The port is disconnected.			
1~6		Blinking	The data is transmitting.			
	Right	On	The port is connected with 1000Mbps.			
	LED	Off	The port is connected with 10/100Mbps			



Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
USB	Connecter for a USB device (for 3G USB Modem or printer).
VDSL/ADSL	Connecter for accessing the Internet.
WAN2	Connecter for local network devices or modem for accessing Internet.
GigaLAN (1-6)	Connecters for local network devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

# 1.2.2 For Vigor2860n

		Dre	$\mathbf{y}T$		gor2860						_	
Wireless LAN ON/OFF/WPS	00				•		<b>a s</b> ë		ì			
Factory ORES	0 0		<u> </u>									
		USB	VDSL/ADSL	WAN2(Giga)	GigaLAN ► 1	2	3	4	5	6		

LED		Status	Explanation				
ACT (Activ	vity)	Blinking	The router is powered on and running normally.				
		Off	The router is powered off.				
USB		On	USB device is connected and ready for use.				
		Blinking	The data is transmitting.				
WLAN	On		Wireless access point is ready.				
		Blinking	It will blink slowly while wireless traffic goes through.				
			ACT and WLAN LEDs blink quickly and				
			simultaneously when WPS is working, and will return				
			to normal condition after two minutes. (You need to				
			setup WPS within 2 minutes.)				
WAN2		On	Internet connection is ready.				
		Off	Internet connection is not ready.				
		Blinking	The data is transmitting.				
DSL		On	The router is ready to access Internet through DSL link.				
		Blinking	Slowly: The DSL connection is ready.				
			Quickly: The connection is training.				
VPN		On	The VPN tunnel is active.				
QoS		On	The QoS function is active.				
WCF		On	The Web Content Filter is active. (It is enabled from <b>Firewall &gt;&gt; General Setup</b> ).				
DoS		On	The DoS/DDoS function is active.				
		Blinking	It will blink while detecting an attack.				
LED on Co	nnector	· • • •	· · · · · · · · · · · · · · · · · · ·				
	Left	On	The port is connected.				
WAN2	LED	Off	The port is disconnected.				
(Giga)		Blinking	The data is transmitting.				
	Right	On	The port is connected with 1000Mbps.				
	LED	Off	The port is connected with 10/100Mbps				
	Left	On	The port is connected.				
GigaLAN	LED	Off	The port is disconnected.				
1~6		Blinking	The data is transmitting.				
	Right	On	The port is connected with 1000Mbps.				
	LED	Off	The port is connected with 10/100Mbps				





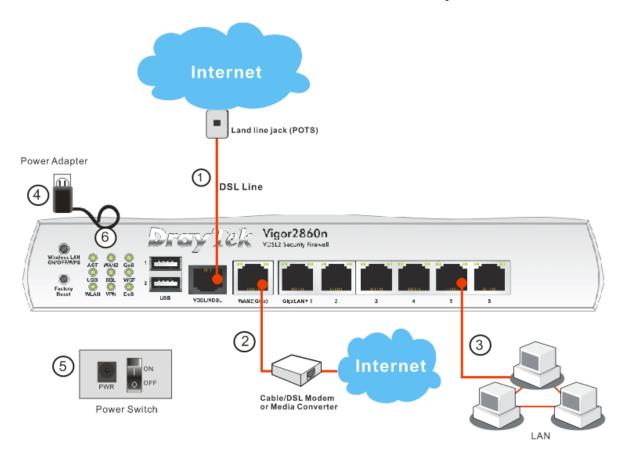
Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client
ON/OFF/WPS	device making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN
	LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is
	blinking). Press the hole and keep for more than 5 seconds. When you
	see the ACT LED begins to blink rapidly than usual, release the button.
	Then the router will restart with the factory default configuration.
USB	Connecter for a USB device (for 3G USB Modem or printer).
VDSL/ADSL	Connecter for accessing the Internet.
WAN2 (Giga)	Connecter for local network devices or modem for accessing Internet.
GigaLAN (1-6)	Connecters for local network devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

#### 1.3 Hardware Installation

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

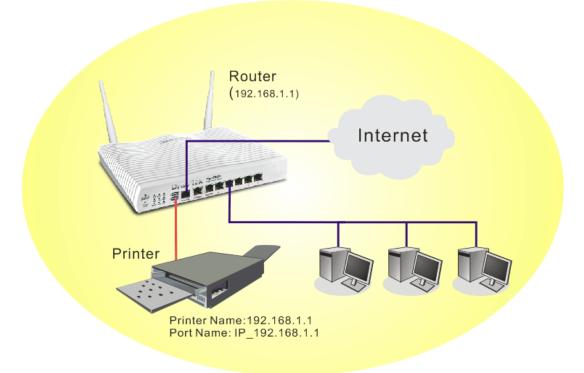
- 1. Connect the DSL interface to the land line jack with a DSL line cable.
- 2. Connect the cable Modem/DSL Modem/Media Converter to the WAN port of router with Ethernet cable (RJ-45).
- 3. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 4. Connect one end of the power adapter to the router'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.
- 6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

(For the hardware connection, we take "*n*" model as an example.)



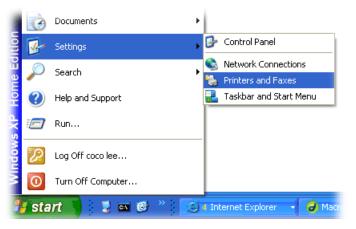
#### **1.4 Printer Installation**

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE/Vista, please visit **www.DrayTek.com**.



Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

- 1. Connect the printer with the router through USB/parallel port.
- 2. Open Start->Settings-> Printer and Faxes.



3. Open File->Add Printer. A welcome dialog will appear. Please click Next.



4. Click Local printer attached to this computer and click Next.



5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.

Computers communicate v	vith printers through ports.	(
Select the port you want yo new port.	our printer to use. If the port is not listed, you (	can create a
OUse the following port:	LPT1: (Recommended Printer Port)	~
© Create a new port:		_

6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name** or **IP Address** and type **IP\_192.168.1.1** as the port name. Then, click **Next**.

<b>udd Port</b> For which device do you want	t to add a port?
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Port Name:	IP_192.168.1.1
	<pre>&lt; Back Next &gt; Cancel</pre>

7. Click Standard and choose Generic Network Card.

۱	dd Standard TCP/IP Printer Port Wizard 🛛 🛛 🔀
	Additional Port Information Required The device could not be identified.
	The detected device is of unknown type. Be sure that: 1. The device is property configured. 2. The address on the previous page is correct. Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.
	Device Type           O Standard         Genetic Network Card           O Eustom         Sgttings
	( <u>B</u> ack <u>N</u> ext ) Cancel

8. Then, in the following dialog, click **Finish**.



9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.

Add Printer Wizard	
Install Printer Softwar The manufacturer an	e d model determine which printer software to use.
	sturer and model of your printer. If your printer came with an installation sk. If your printer is not listed, consult your printer documentation for oftware.
Manufacturer AST AT&T	Printers
Brother Bull Canon	Brother HL-1070 BR-Script2     Brother HL-1070     Brother HL-1070     Stronger HL-1070     Stronger HL-107570 PS
This driver is digitally signed at the second secon	
	< <u>₿</u> ack <u>N</u> ext > Cancel

10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.

General Sha	ring Ports Advance	d Device Settings	_
Br	other HL-1070		
		nts will print to the first free	
checked por			
Port	Description	Printer	1
3.250	Standard TCP/IP Port	Epson Stylus COLOR 1160	
□ IP_1	Standard TCP/IP Port		
D IP_1	Standard TCP/IP Port	HP LaserJet 1300	
[] IP_1	Standard TCP/IP Port		
[] IP_1	Standard TCP/IP Port		
✓ IP_1	Standard TCP/IP Port	Brother HL-1070	
D PDF	Local Port	PDF995	1
Add P	or <u>t</u> <u>D</u> eleti	e Port Configure Port.	
177 2000 - 117 - 117 - 117 - 117	an an an an		-
	directional support		
Enable pri	nter pooling		

11. Select "LPR" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.

Port Name:	IP_192.168.1.1
Printer Name or IP <u>A</u> ddress	: 192.168.1.1
Protocol O <u>R</u> aw	<u>⊚ </u> LPR
Raw Settings	
Port Number:	9100
LPR Settings	_
Queue Name:	p1
LPR Byte Counting Er	nabled
SNMP Status Enabled	1
Community Name:	public
SNMP Device Index	1

The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

**Note 1:** Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ/Application Notes**; find out the link of **USB>>Printer Server** and click it.

DrayTek About DrayTek Products Suppo	orts Solutions Multi-Media Demo Contact Us	rch
FAQ / Application You are here	e: Home + Supports + FAQ / Application Notes + Printer Server	6
USB Printer Server 3G/4G Internet Connection		
n, click the What types	s of printers are compatible with Vigor ro	uter? link.
AQ / Application	Home > Supports > FAQ / Application Notes > Printer Server	

<b>Dray</b> Tek
-----------------

Latest FAQ/Application

Basic Firmware Upgrade

WAN IPv6

Triple-Play

Dual WAN

port.

Printer Server

What types of printers are compatible with Vigor router?

How do I configure LPR printing on My Windows Vista ?

Note 2: Vigor router supports printing request from computers via LAN ports but not WAN

How do I configure LPR printing on Windows7?

2012/01/12

2012/08/20

2009/01/20

This page is left blank.

#### Vigor2860 Series User's Guide



For using 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 accessing into the web user interface of Vigor router and how to adjust settings for accessing Internet successfully.

#### 2.1 Accessing Web Page

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

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 the guide.

2. Open a web browser on your PC and type http://192.168.1.1. The following window will be open to ask for username and password.

<b>Dray</b> Tek	Vigor2860 Series
Login	
Username	admin
Password	• • • • •
Group	💙
	Login
Сор	yright © 2012 DrayTek Corp. All Rights Reserved.

3. Please type "admin/admin" as the Username/Password and click Login.

**Notice:** If you fail to access to the web configuration, please go to "Trouble Shooting" for detecting and solving your problem.

4. Now, the **Main Screen** will appear.

kuto Logout 💌 🛛 IRO	Dashboar	d						
Ishboard Lick Start Wizard Inne Status AN N N	Wireless LAN ONIOFFWPS Factory Reset	ACT WAN2 USB DSL WLAN VPN	() I	USB VDSL/ADSL		GigaLAN > 1 2	3 4	5 6
wall er Management jects Setting M ndwidth Management plications	Model Na Router Na	me Version 3.7.	or2860n 1_RC5a 04-04-04-0		System Up Tir <u>Current Time</u> Build Date/Tin LAN MAC Addi	2013 Feb	18 Mon 8:0:42 3 12:24:58 A8-86-A8	Quick Access System Status Dynamic DNS <u>TR-069</u> User Management
I and Remote Access tificate Management eless LAN . VPN 3 Application	IPv4 Inte WAN1 WAN2	ernet Access Line / Mode ADSL / PPP Ethernet / 3	oE	IP Address Disconnecte		dress AA-A8-B6-A9 AA-A8-B6-AA	<b>Up Time</b> 00:00:00 0:00:40	IMP2P Block Schedule SysLog / Mail Alert LDAP RADIUS
tem Maintenance gnostics ernal Devices port Area	WAN3	USB / ernet Access Mode RADVD / DF	Add	Disconnecte		AA-A8-B6-AB Scope	00:00:00 Up Time	Firewall Object Setting Data Flow Monitor
Juct Registration	Interface DSL WAN + LAN + WLAN	)	: Down Str : 1, WA : 0, LAN	eam : OKbps / N1 @WAN2	/ Up Stream :	1	N5 OLAN6	

5. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.

Auto Logout 💌	
Auto Logout	
Off	
1 min	
3 min	
5 min	
10 min	

#### 2.2 Changing Password

Please change the password for the original security of the router.

- 1. 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.
- 2. Please type "admin/admin" as Username/Password for accessing into the web user interface with admin mode.
- 3. Go to System Maintenance page and choose Administrator Password/.

dministrato	r Password	
	Old Password	
	New Password	
	Confirm Password	
lote:Passw	ord can contain only a-z A-Z 0-9	9,;:"<>*+=-\ ?@#^!()

4. Enter the login password (the default is "admin") on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.

Note: The maximum length of the password you can set is 23 characters.

5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.

<b>Dray</b> Tek	Vigor2860 Series
Login	
Username Password Group	
Group	Login
Сор	yright © 2012 DrayTek Corp. All Rights Reserved.

**Note:** Even the password is changed, the Username for logging to the web user interface is still "admin".

#### 2.3 Quick Start Wizard

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click Next.

Quick Start Wizard			
Enter login password			
Please enter an alpha-nume	ric string as your Passw	word (Max 23 characters).	
Old Password	••••		
New Password	••••		
Confirm Password	••••		
	< Bac	ck Next > Finish	Cancel

On the next page as shown below, please select the WAN interface that you use. If DSL interface is used, please choose WAN1; if Ethernet interface is used, please choose WAN2; if 3G USB modem is used, please choose WAN3. Then click **Next** for next step.

Interface	
WAN Interface:	WAN1 🗸
Display Name:	
Physical Mode:	ADSL / VDSL
Physical Type:	Auto negotiation

WAN1, WAN2 and WAN3 will bring up different configuration page. Refer to the following for detailed information.



#### 2.3.1 For WAN1 (ADSL/VDSL)

WAN1 is specified for ADSL or VDSL connection.

Quick Start Wizard

WAN Interface: Display Name:	WAN1 💌
Physical Mode:	ADSL / VDSL2
Physical Type:	Auto negotiation 🛛 🔽

You have to select the appropriate Internet access type **according to the information from your ISP**. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. In addition, the field of **For ADSL Only** will be available only when ADSL is detected. Then click **Next** for next step.

#### PPPoE/PPPoA

Quick Start Wizard

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page.

WAN 1	
Protocol	PPPoE / PPPoA
For ADSL Only:	
Encapsulation	PPPoe LLC/SNAP 🔽
VPI	0 Auto detect
VCI	33
Fixed IP	🔿 Yes 💿 No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	8.8.8.8
Second DNS	8.8.4.4

Available settings are explained as follows:

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface.

	PPPoE / PPPoA PPPoE / PPPoA MPoA / Static or Dynamic IP Choose <b>PPPoE or PPPoA</b> as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click <b>Auto detect</b> to find out the best values.
Fixed IP	Click <b>Yes</b> to enable Fixed IP feature.
IP Address	Type the IP address if <b>Fixed IP</b> is enabled.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

2. After finished the above settings, simply click **Next.** Manually enter the Username/Password provided by your ISP

Quick Start Wizard

WAN 1	
User Name	84005755@hinet.net
Password	•••••
Confirm Password	•••••

Available settings are explained as follows:

Item	Description
User Name	Assign a specific valid user name provided by the ISP.

Item	Description
	<b>Note:</b> The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP.
	<b>Note:</b> The maximum length of the password you can set is 62 characters.
<b>Confirm Password</b>	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. After finished the above settings, click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:	
WAN Interface: Physical Mode: VPI: VCI: Protocol / Encapsulation: Fixed IP: Primary DNS: Secondary DNS:	WAN1 ADSL / VDSL2 0 33 PPPoE / LLC No 8.8.8.8 8.8.4.4
	<pre>&lt; Back Next &gt; Finish Cancel</pre>

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

#### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

#### MPoA / Static or Dynamic IP

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page.

ct to Internet	
WAN 1	
Protocol	MPoA / Static or Dynamic IP 💌
For ADSL Only:	
Encapsulation	1483 Bridged IP LLC
VPI	0 Auto detect
VCI	88
Fixed IP	Yes ○ No(Dynamic IP)
IP Address	⊙Yes ○No(Dynamic IP)
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

Available settings are explained as follows:

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. MPoA / Static or Dynamic IP PPPoE / PPPoA MPoA / Static or Dynamic IP Choose MPoA / Static or Dynamic IP as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click <b>Auto detect</b> to find out the best values. 1483 Bridged IP LLC 1483 Bridged IP LLC 1483 Routed IP LLC 1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE) Ves No(Dynamic IP)
Fixed IP	Click <b>Yes</b> to enable Fixed IP feature.
IP Address	Type the IP address if <b>Fixed IP</b> is enabled.
Subnet Mask	Type the subnet mask.



Primary DNS	Type in the primary IP address for the router.	
Secondary DNS	Type in secondary IP address for necessity in the future.	
Back	Click it to return to previous setting page.	
Next	Click it to get into the next setting page.	
Cancel	Click it to give up the quick start wizard.	

2. Please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:	
WAN Interface: Physical Mode: VPI: VCI: Protocol / Encapsulation: Fixed IP: Primary DNS: Secondary DNS:	WAN1 ADSL / VDSL2 0 33 1483 Route LLC No 8.8.8.8 8.8.4.4
	< Back Next > Finish Cancel

3. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

#### Quick Start Wizard Setup OK!

4. Now, you can enjoy surfing on the Internet.

#### 2.3.2 For WAN2 (Ethernet)

WAN2 is dedicated to physical mode in Ethernet. If you choose WAN2, please specify physical type. Then, click **Next**.

Quick Start Wizard

WAN Interface:	WAN2 V
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 💌

On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

#### **PPPoE**

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

WAN 2		
Select one of the	following Internet Access types provided	d by your ISP.
	PPPoE	
	O PPTP	
	C L2TP	
	O Static IP	
	O DHCP	
	O DHCP	

2. Click **PPPoE** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

WAN 2	
Enter the user name and pa	ssword provided by your ISP.
User Name	84005657@hinet.net
Password	•••••
Confirm Password	•••••

Available settings are explained as follows:

Item	Description	
User Name	Assign a specific valid user name provided by the ISP.	
	<b>Note:</b> The maximum length of the user name you can set is 63 characters.	
Password	Assign a valid password provided by the ISP.	
	<b>Note:</b> The maximum length of the password you can set is 62 characters.	
<b>Confirm Password</b>	Retype the password.	
Back	Click it to return to previous setting page.	
Next	Click it to get into the next setting page.	
Cancel	Click it to give up the quick start wizard.	

3. Please manually enter the Username/Password provided by your ISP. Click **Next** for viewing summary of such connection.

Quick Start Wizard	Qu	uick	Start	Wizard
--------------------	----	------	-------	--------

WAN2
Ethernet
Auto negotiation
PPPoE

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

#### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

#### PPTP/L2TP

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

WAN 2					
Select one of the	following Internet Acce	ess types provid	led by your ISP	·	
	O PPPoE				
	PPTP				
	O L2TP				
	O Static IP				
	O Brief				

2. Click **PPTP/L2TP** as the Internet Access Type. Then click **Next** to continue.

#### Quick Start Wizard

WAN 2	and WAN ID configuration an	d PPTP, conver IP, provided by
your ISP.	ord, WAN IP configuration an	d PPTP server IP provided by
User Name	5477aec	
Password	••••	
Confirm Password	••••	
WAN IP Configuration		
🔘 Obtain an IP address a	utomatically	
Specify an IP address		
IP Address	192.168.3.100	
Subnet Mask	255.255.255.0	
Gateway	192.168.3.1	
Primary DNS		
Second DNS		
PPTP Server		

Item	Description	
User Name	Assign a specific valid user name provided by the ISP. <b>Note:</b> The maximum length of the user name you can set is 63 characters.	
Password	Assign a valid password provided by the ISP. <b>Note:</b> The maximum length of the password you can set is 62 characters.	
<b>Confirm Password</b>	Retype the password.	
WAN IP Configuration	<ul> <li>Obtain an IP address automatically – the router will get an IP address automatically from DHCP server.</li> <li>Specify an IP address – you have to type relational settings manually.</li> <li>IP Address - Type the IP address.</li> <li>Subnet Mask –Type the subnet mask.</li> <li>Gateway – Type the IP address of the gateway.</li> <li>Primary DNS –Type in the primary IP address for the router.</li> <li>Second DNS –Type in secondary IP address for necessity in the future.</li> </ul>	
PPTP Server / L2TP Server	Type the IP address of the server.	
Back	Click it to return to previous setting page.	
Next	Click it to get into the next setting page.	
Cancel	Click it to give up the quick start wizard.	

Available settings are explained as follows:

3. Please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for viewing summary of such connection.

 Please confirm your settings:

 WAN Interface:
 WAN2

 Physical Mode:
 Ethernet

 Physical Type:
 Auto negotiation

 Internet Access:
 PPTP

 Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.

 Back

Quick Start Wizard

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

### Static IP

Quick Start Wizard

1. Choose **WAN2** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

WAN 2	
Select one of the	ollowing Internet Access types provided by your ISP.
	O PPPoE
	○ РРТР
	O L2TP
	<ul> <li>Static IP</li> </ul>
	O DHCP

2. Click Static IP as the Internet Access type. Simply click Next to continue.

Quick Start Wizard

WAN 2		
Enter the Static IP config	uration provided by your ISP.	
WAN IP	192.168.3.100	
Subnet Mask	255.255.255.0	
Gateway	192.168.3.1	
Primary DNS		
Secondary DNS		(optional)

**Dray** Tek

Available settings are explained as follows:

Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. Please type in the IP address information originally provided by your ISP. Then click **Next** for next step.

Quick Start Wizard

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
Click <b>Back</b> to modify chan settings and restart the Vi	iges if necessary. Otherwise, click <b>Finish</b> to save the current igor router.

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

### DHCP

1. Choose **WAN2** as WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

WAN 2		
Select one of the	following Internet Access types provided by your ISP.	
	O PPPoE	
	O PPTP	
	C L2TP	
	Static IP	
	DHCP	

2. Click **DHCP** as the Internet Access type. Simply click **Next** to continue.

Quick Start Wizard

Quick Start Wizard

DHCP Client Mode WAN 2 If your ISP requenter it in.	uires you to enter a specific host name or specific MAC address, please
Host Name MAC	(optional) 00 - 1D - AA - A8 - B7 - 6A (optional)
	< Back Next > Finish Cancel

Item	Description
Host Name	Type the name of the host. Note: The maximum length of the host name you can set is 39 characters.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous setting page.

Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. After finished the settings above, click **Next** for viewing summary of such connection.

Quick Start Wizard Please confirm your settings: WAN Interface: WAN2 Physical Mode: Ethernet Physical Type: Auto negotiation Internet Access: DHCP  $\mathsf{Click}\;\mathsf{Back}\;$  to modify changes if necessary. Otherwise,  $\mathsf{click}\;\mathsf{Finish}\;$  to save the current settings and restart the Vigor router. < Back Next > Finish Cancel

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

### 2.3.3 For WAN3 (USB)

WAN3 is dedicated to physical mode in USB. If WAN3 is selected, it is not necessary for you to type any information for such connection.

1. Choose **WAN3** as WAN Interface.

Quick Start Wizard	
WAN Interface	
WAN Interface: Display Name: Physical Mode:	WAN3
	< Back Next > Finish Cancel

2. Then, click **Next** for getting the following page.

#### Quick Start Wizard

WAN 3	
Internet Access :	3G/4G USB Modem(PPP mode) 🔽
	3G/4G USB Modem(PPP mode)
3G/4G USB Modem(PPP mode)	4G USB Modem(DHCP mode)
SIM PIN code	
Modem Initial String	AT&FE0V1X1&D2&C1S0=0
	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	Apply

Item	Description
Internet Access	Choose one of the selections as the protocol of accessing the internet.
3G/4G USB Modem (PPP mode)	<b>SIM Pin code</b> –Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.
	Modem Initial String – Such value is used to initialize

	USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters. <b>APN Name</b> – APN means Access Point Name which is provided and required by some ISPs. Type the name and click <b>Apply</b> .
4G USB Modem (DHCP mode)	<b>SIM Pin code</b> –Type PIN code of the SIM card that will be used to access Internet.
	Network Mode – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically. APN Name – APN means Access Point Name which is provided and required by some ISPs.

3. Then, click **Next** for viewing summary of such connection.

e confirm your settings:	
WAN Interface:	WAN3
Physical Mode:	USB
Internet Access:	DHCP
settings and restart the \	iges if necessary. Otherwise, click <b>Finish</b> to save the curr /igor router.

4. Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

### Quick Start Wizard Setup OK!

5. Now, you can enjoy surfing on the Internet.

# 2.4 Service Activation Wizard

Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.

Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (*MyVigor*) located on <u>http://myvigor.draytek.com</u>. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for detailed information.

Now, follow the steps listed below to activate WCF feature for your router.

|--|

1. Open Service Activation Wizard.

Service Activation Wizard



2. The screen of **Service Activation Wizard** will be shown as follows. Choose the one you need and click **Next**. In this case, we choose to activate free trail edition.

- Web Content	sed for activating Filter .he edition you need.	
	<ul> <li>Free trial edition</li> <li>Formal edition with license key</li> </ul>	

**Free trial edition**: it offers a period of trial for you to get acquainted with WCF function. **Formal edition with license key**: you can extend the license valid time manually.

**Note:** If you activate **Formal edition with license key** first, the free trial edition will be invalid.

3. In the following page, you can activate the Web content filter services at the same time or individually. When you finish the selection, please click **Next**.

This	s product provides 30 days of free trial, please choose the item(s) you want to use.	
wci	F service:	
0	Web Content Filter (BPjM)	
	BPjM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPjM WCF service. This is a free service without guarantee.	
	Activation Date : 2013-02-18	
	Web Content Filter (Commtouch) License	
	Agreement Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.	
	Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from	
	Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets. Activation Date : 2013-02-18 Web Content Filter (fragFINN) License	Activation Date : [2013-02-18

Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.

4. Setting confirmation page will be displayed as follows, please click Next.

Service Activation Wizard

Please confirm your sett	ings			
Sevice Type Sevice Activ		Trial version Web Content Filter ( Commtouch )		
Please click	( <b>Back</b> to re-select serv	vice type you to activate.		
		< Back Next >	Finish	Cancel

# **Dray** Tek

5. Wait for a moment till the following page appears.

Service Activation Wizard

Service Activation Wizard

Please check the	following item(s)	to enable services on y	your router.	
	🗹 Enat	ole Web Content Filter		

When such page appears, you can enable or disable these services for your necessity. Then, click **Finish.** 

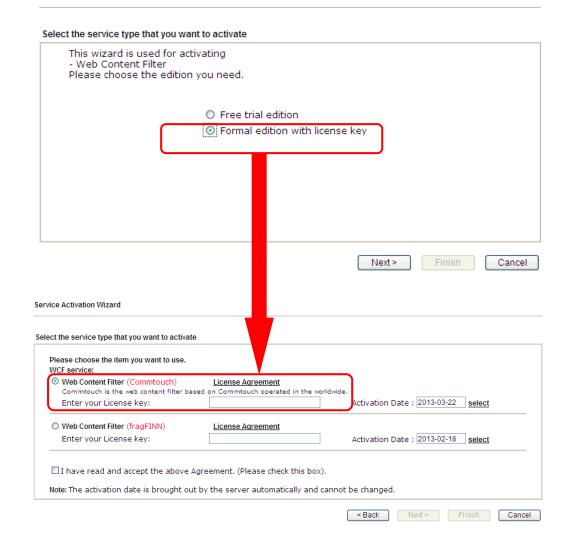
**Note:** The service will be activated and applied as the default rule configured in **Firewall>>General Setup**.

6. Now, the web page will display the service that you have activated according to your selection(s). The valid time for the free trial of these services is one month.

	DrayTek Servic	e Activation	
Service Name	Start Date	Expire Date	Status
Web Content filter	2013-02-18	2013-03-21	Commtouch
ormal operation for you	ir router, update you	r signature again is	recommended.
ormal operation for you	Ir router, update you Copyright@DrayTek Corp.		recommended.

Later, if you need to extend the license valid time for the **same service**, you can also use the **Service Activation Wizard** again to reach your goal by clicking the radio button of **Formal edition with license key** and clicking **Next**.

#### Service Activation Wizard



## 2.5 Introducing Dashboard

Dashboard shows the connection status including System Information, IPv4 Internet Access, IPv6 Internet Access, Interface (physical connection), Security and Quick Access.

Click **Dashboard** from the main menu on the left side of the main page.



A web page with default selections will be displayed on the screen. Refer to the following figure:

#### Dashboard

		) //	Deerv	Tol	Vigor28	860n		
۲	ACT WAN2 Qos	s 🗎	e wy i	E Ch	VDSL2 Security	Firewall		
Wireless LAN ON/OFF/WPS		) · E				910 - N		P 92 9
۲	USB DSL WC	F						
Factory Reset	WLAN VPN Dos							
	WLAN VPN DO	5	USB VDSL/ADS	SL W	AN2(Giga) GigaLA	N⊁1 2	3 4	5 6
	nformation							Quick Access
lodel Nar		60n		- /	em Up Time	0:47:55	0 Mar 0: 46-7	System Status
touter Nan	<u>ne</u> Version 3.7.1 R	CEN			<u>nt Time</u> Data Tima	2013 Feb 3 Feb 5 2013	18 Mon 8:46:7	Dynamic DNS
OSL Versio			0_01		Date/Time MAC Address			TR-069
	5/1 [05-04-0		0-01		-inc Addiess	00-10-44-	-0-00-A0	User Management
Pv4 Inte	rnet Access							Schedule
	Line / Mode		IP Address		MAC Addres	s	Up Time	SysLog / Mail Alert
WAN1	ADSL / PPPoE		Disconnect	ed	00-1D-AA-A	8-86-A9	00:00:00	LDAP
WAN2	Ethernet / Stat	ic IP	172.16.3.13	30	00-1D-AA-A	.8-B6-AA	0:47:43	RADIUS
WAN3	USB /		Disconnect	ed	00-1D-AA-A	8-86-AB	00:00:00	Firewall Object Setting
				_				Data Flow Monitor
Pv6 Inte	rnet Access							4
	Mode		ress			Scope	Up Time	-
LAN	RADVD / DHCPV	/ <b>D</b>   FE8	0::21D:AAFF	(FEA8)	8048/04	Link		
nterface								
DSL	Connected : Do	wn Str	eam : OKbos	/Un 9	Stream : OKhi	25		1
WAN	Connected : 1,	WA			WAN3			1
LAN	Connected : 0,	<b>LAN</b>	J1 @LAN2	<u></u>	LANG 🥥LA	N4 🔍 LAN	15 @LAN6	]
WLAN	Connected : O							1
USB	Connected : 0,							
	0,	056	02					1
Security								
VPN	Connected : 0				Remo	te Dial-in Use	er / LAN to LAN	1
								J

User Mode is OFF now.

### 2.5.1 Virtual Panel

On the top of the Dashboard, a virtual panel (simulating the physical panel of the router) displays the physical interface connection. It will be refreshed every five seconds.

Dashboard

	ACT	(O) WAN2	QoS	Dre	$\mathbf{Y}T$		por2860 2 Security Firev	vall				
Factory Reset	USB1	DSL	WCF									
Reset	USB2	VPN	DoS	USB	VDSL/ADSL	WAN2(Giga)	GigaLAN ▶ 1	2	3	4	5	6

Port	Color Displayed	Explanation		
Ethernet Port	Black	It means such port is disconnected.		
(WAN/LAN)	Green	It means such port is connected (with Giga transmission rate) physically.		
	Orange	It means such port is connected physically.		
VDSL/ADSL	Black	It means such port is disconnected.		
	Green	It means such port is connected with VDSL.		
	Orange	It means such port is connected with ADSL.		
USB	Black	It means no USB device is connected.		
	Green	It means a USB device is connected.		
LED (left side)	Black	It means the router or the function is not working.		
	Green	It means the router or the function is working.		

For detailed information about the LED display, refer to **1.2 LED Indicators and Connectors**.

### 2.5.2 Name with a Link

A name with a link (e.g., <u>Router Name</u>, <u>Current Time</u>, <u>WAN1</u> and etc.) below means you can click it to open the configuration page for modification.

System Information					
Model Name	Vigor2860	System Up Time			
Router Name	Vigor2860-Alpha	Current Time			
Firmware Versio	n beta_0414	Build Date/Time			
DSL Version	05-03-02-08-01-	06			

IPv4 Internet Access						
	Line / Mode	IP Address	MAC Address			
WAN1	VDSL / Static IP	172.16.2.132	00-1D-AA-A6			
WAN2	Ethernet / PPPoE	1.169.137.242	00-1D-AA-A6			
WAN3	USB /	Disconnected	00-1D-AA-A6			

### 2.5.3 Quick Access for Common Used Menu

All the menu items can be accessed and arranged orderly on the left side of the main page for your request. However, some **important** and **common** used menu items which can be accessed in a quick way just for convenience.

Look at the right side of the Dashboard. You will find a group of common used functions grouped under **Quick Access**.

Quick Access
System Status
Dynamic DNS
<u>TR-069</u>
User Management
IM/P2P Block
Schedule
SysLog / Mail Alert
LDAP
RADIUS
Firewall Object Setting
Data Flow Monitor

The function links of System Status, Dynamic DDNS, TR-069, User Management, IM/P2P Block, Schedule, Syslog/Mail Alert, LDAP, RADIUS, Firewall Object Setting and Data Flow Monitor are displayed here. Move your mouse cursor on any one of the links and click on it. The corresponding setting page will be open immediately.

In addition, quick access for VPN security settings such as **Remote Dial-in User** and **LAN to LAN** are located on the bottom of this page. Scroll down the page to find them and use them if required.

Interface							
DSL	Connected : Dov	vn Stream :	101060Kbps	s / Up Strea	im: 96772K	bps	
WAN	Connected : 2,	WAN1	WAN2	@WAN3			
🖬 LAN	Connected : 2,	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
USB	Connected : 0,	OUSB 1					
030	0,	OUSB 2					
Cecurity							
🔛 VPN	Connected : 1				Remote Di	ial-in User /	LAN to LAN

User Mode is OFF now.

Note that there is a plus ( ) icon located on the left side of VPN/LAN. Click it to review the VPN connection(s) used presently.

Security				
VPN	Connected : 1		<u>Remote Dial-in L</u>	lser / LAN to LAN
	Current Page: 1		Pa	ge No. 1 🌱 Go To
	Name / User	Type / Security	Host IP	Up Time
	V2920	IPsec/3DES	172.16.2.145	0:0:20

User Mode is OFF now.



WAN	Connected : 2,	VVAN1	VVAN2	- UVP	W3				
🔲 LAN	Connected : 3,	LAN1	LAN2	LAN	V3	LAN4	LAN5	LAN6	
	Host ID	IP Add	ress		MAC				
	ALPHA-NB	10.28	.60.13		1C-4	4B-D6-D2-I	D7-DB		
		10.28	.60.14		00-1	L5-AF-09-7	7E-FA		
		10.28	.60.11		00-5	50-7F-C9-7	76-45		
	Connected + 0	Such 4							

Host connected physically to the router via LAN port(s) will be displayed with green circles in the field of Connected.

All of the hosts (including wireless clients) displayed with Host ID, IP Address and MAC address indicates that the traffic would be transmitted through LAN port(s) and then the WAN port. The purpose is to perform the traffic monitor of the host(s).

### 2.5.4 GUI Map



All the functions the router supports are listed with table clearly in this page. Users can click the function link to access into the setting page of the function for detailed configuration. Click the icon on the top of the main screen to display all the functions.

#### GUI Map

Dashboard		Applications	
Wizard			Dynamic DNS
	Quick Start Wizard		Schedule
	Service Activation Wizard		RADIUS
Online Status			Active Directory /LDAP
	Physical Connection		UPnP
	Virtual WAN		IGMP
WAN			Wake on LAN
	General Setup		Short Message Service
	Internet Access	VPN and Remote Access	
	Multi-PVCs		VPN Client Wizard
	Multi-VLAN		VPN Server Wizard
	Load-Balance Policy		Remote Access Control
LAN			PPP General Setup
	General Setup		IPsec General Setup
	Keyword Group		Activation
	File Extension Object	Diagnostics	
CSM			Dial-out Triggering
	APP Enforcement Profile		Routing Table
	URL Content Filter Profile		ARP Cache Table
<b>D</b>	Web Content Filter Profile		IPv6 Neighbour Table
Bandwidth Management			DHCP Table
	Sessions Limit		NAT Sessions Table
	Bandwidth Limit Quality of Service		Ping Diagnosis Data Flow Monitor
	quality of Service		Traffic Graph
			Trace Route
			Web Firewall Syslog
			TSPC Status
		External Devices	

# **Dray** Tek

### 2.5.5 Web Console



It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

Click the **Web Console** icon on the top of the main screen to open the following screen.

<i>(</i> http://172.16	.2.132:8080/doc/	console.htm - Wi	ndows Internet Explor	er		
🔊 http://172.16.2	. <b>132</b> :8080/doc/consc	le.htm				
Type ? for > ?	command help	)				
% Valid com	mands are:					
adsl internet	bpa ip	csm ip6	ddns ipf	dos log	exit mngt	
	object show	port srv	portmaptime switch	-	qos testmail	
upnp user ≻∎	vigbrg nand	vlan	vpn	wan	wol	
, 完成				🚷 網際網路		🔍 105% 🔻 🛒

**Dray** Tek

### 2.5.6 Config Backup



There is one way to store current used settings quickly by clicking the **Config Backup** icon. It allows you to backup current settings as a file. Such configuration file can be restored by using **System Maintenance>>Configuration Backup**.

Simply click the icon on the top of the main screen and a pop up dialog will appear.

檔案下載	
是否要	開啓或儲存這個檔案?
<b>0</b> 8 00	名稱: V2860_20120917.cfg 類型: Microsoft Office Outlook 設定檔,5.21KB 従: <b>172.16.2.132</b>
	開啓舊檔(①) 儲存(②) 取消
2	雖然來自網際網路的檔案可能是有用的,但是 <u>某些</u> 檔案有可 能會傷害您的電腦。如果您不信任其來源,諸不要開啓或儲 存這個檔案。 <u>有什麼樣的風險?</u>

Click **Save** to store the setting.

### 2.6 Online Status



### **2.6.1 Physical Connection**

Such page displays the physical connection status such as LAN connection status, WAN connection status, ADSL information, and so on.

# Physical Connection for IPv4 Protocol

**Online Status** 

Physical Connectio	n			Sy	stem Uptime: 0:1:1)
	IPv4		IPv6		
LAN Status	Prima	ry DNS: 168.95	5.192.1	Secondary D	NS: 168.95.1.1
IP Address	TX Packets	RX Pac	kets		
192.168.1.1	0	3085			
WAN 1 Status					>> Dial PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
200		0	0	0	0
WAN 2 Status					>> Drop PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:54	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
114.44.49.54	168.95.98.254	800	4761	821	6617
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB		222	00:00:00	1411
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
	0.000	0	0	0	0

## **Physical Connection for IPv6 Protocol**

**Online Status** 

Physical Connect	ion			System Uptime: 0:1:14
IPv4			IPv6	114 7427
LAN Status				
IP Address				
	00:83E4:21D:AAFF FF:FEA6:2568/64 (L		obal)	
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
147	187	34205	19176	
WAN2 IPv6 Statu	5			
Enable	Mode	Up Time		
Yes	AICCU	0:00:48		
IP			Gateway IP	
	00:3E4::2/64 (Glob F00:3E4:2/64 (Link)			
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
186	137	16438	33093	

Detailed explanation (for IPv4) is shown below:

Item	Description		
LAN Status	<b>Primary DNS-</b> Displays the primary DNS server addres for WAN interface.		
	<b>Secondary DNS -</b> Displays the secondary DNS server address for WAN interface.		
	<b>IP</b> Address-Displays the IP address of the LAN interface.		
	TX Packets-Displays the total transmitted packets at the		

Item	Description
	LAN interface.
	<b>RX Packets</b> -Displays the total received packets at the LAN interface.
WAN1/WAN2/WAN3 Status	<b>Enable</b> – <b>Yes</b> in red means such interface is available but not enabled. <b>Yes</b> in green means such interface is enabled.
	<b>Line</b> – Displays the physical connection (VDSL, ADSL, Ethernet, or USB) of this interface.
	<b>Name</b> – Display the name of the router.
	<b>Mode</b> - Displays the type of WAN connection (e.g., PPPoE).
	<b>Up Time</b> - Displays the total uptime of the interface.
	<b>IP</b> - Displays the IP address of the WAN interface.
	<b>GW IP</b> - Displays the IP address of the default gateway.
	<b>TX Packets</b> - Displays the total transmitted packets at the WAN interface.
	<b>TX Rate</b> - Displays the speed of transmitted octets at the WAN interface.
	<b>RX Packets</b> - Displays the total number of received packets at the WAN interface.
	<b>RX Rate</b> - Displays the speed of received octets at the WAN interface.

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	<b>IP Address</b> - Displays the IPv6 address of the LAN interface
	<b>TX Packets</b> -Displays the total transmitted packets at the LAN interface.
	<b>RX Packets</b> -Displays the total received packets at the LAN interface.
	<b>TX Bytes</b> - Displays the speed of transmitted octets at the LAN interface.
	<b>RX Bytes</b> - Displays the speed of received octets at the LAN interface.
WAN IPv6 Status	<b>Enable</b> – <b>No</b> in red means such interface is available but not enabled. <b>Yes</b> in green means such interface is enabled. No in red means such interface is not available.
	<b>Mode</b> - Displays the type of WAN connection (e.g., TSPC).
	<b>Up Time</b> - Displays the total uptime of the interface.
	<b>IP</b> - Displays the IP address of the WAN interface.
	<b>Gateway IP</b> - Displays the IP address of the default gateway.



**Note:** The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface is not ready for accessing Internet.

### 2.6.2 Virtual WAN

Such page displays the virtual WAN connection information.

Virtual WAN are used by TR-069 management, VoIP service and so on.

The field of Application will list the purpose of such WAN connection.

Online Status

Virtual WAN				Sys	tem Uptime: 3:1
WAN 5 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	Ethernet			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 6 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	Ethernet			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
		0	0	0	0
WAN 7 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	Ethernet			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
		0	0	0	0

# 2.7 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Admin mode Status: Settings Saved

**Ready** indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click Finish or OK button.

# 2.8 Registering Vigor Router

You have finished the configuration of Quick Start Wizard and you can surf the Internet at any time. Now it is the time to register your Vigor router to MyVigor website for getting more service. Please follow the steps below to finish the router registration.

1 Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.

<b>Dray</b> Tek	Vigor2860 Series
Login	
Username	admin
Password	••••
Group	💌
	Login
Cop	yright © 2012 DrayTek Corp. All Rights Reserved.

2 Click **Support Area>>Production Registration** from the home page.



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

		stration entitles you d product and recei	to upgrade firmware ve news about
LOGIN			
UserName :	james_fae		
Password :	•••••		
Auth Code :	txxhdd	t <b>x x h d</b> d	
	If you cannot read the word	, <u>click here</u>	
	Forgotten password?	Login	
Don't have a	MyVigor Account ?	Create an account	now
L			

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or 4 The following page will be displayed after you logging in MyVigor. From this page, please click **Add** or **Product Registration**.

<b>Dray</b> Tek	My	Login
E Home	Search	You
	My Information	
About Us Product My Information VigorACS SI VigorPro Product Registration Customer Survey	Welcome,james_fae Last Login Time : 2011-03-16 01:45:09 Last Login From : 172.16.2.180 Current Login Time : 2011-03-16 18:20:31 Current Login From : 172.16.3.148 RowNo : 5 V PageNo : Add Your Device List Serial Number / Device Name Model Note	<b>Regist</b> e

5 When the following page appears, please type in Nickname (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**.

About Us Product	My Product		Search for thi	s site	GO
My Information	📖 Registration Device	e			
VigorACS SI VigorPro Product Registration	Serial number : Nickname : *	20110316092002 vigor2850	201		
Customer Survey	Registration Date : *	03-16-2011			
	Usage :	Select	*		
	Product Rating :	Select	📝 ( Your opinion so far	)	
	No. of Employees :	Select	📝 ( In total within your d	company )	
	Supplier :		( Where y	rou bought it from )	
	Date of Purchase :		( mm-dd-	/УУУ )	
	Internet Connection :	*			
	Cable	🗹 ADSL	VDSL	📃 Fiber	
	🗖 3G	WIMAX	🗌 LTE		
Please use IE 5.0 or above (resolution 1024 * 768 ) for best display. © DrayTek Corp.				Cancel Sub	mit

6 When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.

OK	ΟK	
----	----	--

7 Now, you have finished the product registration.



8 After clicking **OK**, you will see the following page. Your router has been registered to *myvigor* website successfully.

If you have not activated web content filter service by using **Service Activation Wizard**, you can activate the service from this step. Please click the serial number link.

Home -			Sea	rch GO	
	My Information				~
About Us Product My Information VigorACS SI VigorPro Customer Survey	Welcome,james_fae Last Login Time : 2011-03-16 0 Last Login From : 172.16.2.180 Current Login Time : 2011-03-1 Current Login From : 172.16.3. Your Device List	6 18:20:31	RowNo : 5 💌 Pa	ageNo : 🚺 💌	
	Serial Number / Host ID	Device Name	Model	Note	
	<u>2011031609200201</u>	vigor 2850	Vigor2850	-	

9 From the **Device's Service** section, click the **Trial**.

	My Product
About Us Product	Device Information
My Information	Nickname : vigor2850 Serial : 2011031609200201
VigorACS SI	Model : Vigor2850 Series
VigorPro	Rename Transfer Back
Customer Survey	
	Device's Service Expired License
	Service Provider Action Status Start Date Expired Date
	📅 WCF Commtouch 🛛 Trial 🛛 🌗 On 🛛 - 🔹 -
	The Commtouch GlobalView Web Filter is provided for Vigor router with only 1-month trial. After trial
	period, please purchase the official package from your local DrayTek dealer/distributor.
	BPJM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPJM WCF service. This is a free service without guarantee.

10 In the following page, check the box of "I have read and accept the above Agreement". The system will find out the date for you to activate this version of service. Then, click Next.



11 When this page appears, click **Register**.

About Us Product	GO
My Information     Service Name:     WCF       VigorACS SI     STEP 2       VigorPro     Activation Date (MM-DD-YYYY):       Customer Survey     Register	Cancel

12 Wait for a moment until the following page appears.

#### **DrayTek Service Activation**

Service Name	Start Date	Expire Date	Status
Web Content filter	2011-03-28	2011-04-27	Commtouch

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

Close

13 Click Close.

This page is left blank.

# **Dray** Tek



This chapter will guide users to execute web configuration.

- 1. Open a web browser on your PC and type http://192.168.1.1. The window will ask for typing username and password.
- 2. Please type "admin/admin" on Username/Password for administration operation.

Now, the Main Screen will appear. Note that different model will have different web pages.

<b>Dray</b> Tek	Vigo	r 2860 Series				E 111	
Auto Logout 💌 🛛 🛛 🛛 🛛 🛛 🖓	Dashboar	d					
Dashboard Quick Start Wizard Service Activation Wizard Online Status WAN LAN NAT	Wireless LAN ON/OFF/WPS	ACT WAN2 QoS USB DSL WCF WLAN VPN DoS	USB VDSI/ADSL	Vigor28 VDSL2 Security WAN2(Giga) GigaLAB	Firewall	3 4	5 6
Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access	Model Na Router Na	Me Version 3.7.1_RC5a	Cu Bu	rent Time	Feb 5 2013		Quick Access <u>System Status</u> <u>Dynamic DNS</u> <u>TR-069</u> <u>User Management</u> <u>IMP2P Block</u>
Certificate Management Wireless LAN SSL VPN USB Application System Maintenance	WAN1 WAN2	Ernet Access Line / Mode ADSL / PPPoE Ethernet / Static IP	IP Address Disconnected 172.16.3.130	MAC Address 00-1D-AA-A 00-1D-AA-A	<mark>8-B6-A9</mark> 8-B6-AA	Up Time 00:00:00 0:00:40	Schedule SysLog / Mail Alert LDAP RADIUS
Diagnostics External Devices Support Area	WAN3		Disconnected	00-1D-AA-A	8-B6-AB Scope	00:00:00	Firewall Object Setting Data Flow Monitor
Support Area Product Registration All Rights Reserved.	LAN Interface DSL WAN						
		Connected : 1, W4 Connected : 0, LA Connected : 0		OLAN3 OLAI	N4 @LAN	5 @LAN6	·

### 3.1 WAN

**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.

### 3.1.1 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.

### **Network Connection by 3G USB Modem**

For 3G mobile communication through Access Point is popular more and more, Vigor2860 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2860, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2860n with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2860n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2860n series.



After connecting into the router, 3G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN3 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.



WAN
General Setup
Internet Access
Multi-PVCs
Multi-VLAN
Load-Balance Policy
LAN

### 3.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1, WAN2 and WAN3 in details.

This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs 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. Please configure WAN1, WAN2 and WAN3 settings.

This webpage allows you to set general setup for WAN1, WAN2 and WAN3 respectively. In default, WAN2 is disabled. If you want to enable it, simply click the WAN2 link and select **Yes** in the field of **Enable**.

WAN >> General Setup

Load Balance Mode:		Auto Weight 💌		
Setup				
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	V	ADSL/-	0/0	Always On
WAN2	V	Ethernet/Auto negotiation	0/0	Always On
WAN3	V	USB/-	0/0	Always On

Note: The line speed setting of WAN interface is avaialbe only when According to Line Speed is selected as the Load Balance Mode.

OK

Item	Description		
Load Balance ModeThis option is available for multiple-WAN for g enough bandwidth for each WAN port. If you k practical bandwidth for your WAN interface, pl the setting of According to Line Speed. Other choose Auto Weigh to let the router reach the b balance.Load Balance Mode:Auto Weight According to Line Speed		Ach WAN port. If you know the your WAN interface, please choose to Line Speed. Otherwise, please et the router reach the best load	
Index	Click the WAN interface link under Index to access into the WAN configuration page.		
Enable	V means such WAN interface is enabled and ready to be used.		

Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
Line Speed	Display the downstream and upstream rate of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Backup WAN	Display the Backup WAN interface for such WAN when it is disabled.

Note: In default, each WAN port is enabled.

After finished the above settings, click **OK** to save the settings.

### WAN1 with ADSL/VDSL

Vigor router will **detect** the physical line is connected by ADSL or VDSL2 **automatically**. Therefore, this page allows you to configure settings for ADSL and VDSL2 at one time. That is, it is not necessary for you to configure different profile settings for ADSL and VDSL2 respectively.

WAN >> General Setup

WAN 1	
Enable:	Yes 💌
Display Name:	
Physical Mode:	ADSL
DSL Mode:	Auto 🔽
Physical Type:	Auto negotiation 😽
DSL Modem Code:	Default 💌
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion (ADSL):	Disable 💙 (for channel 1)
Tag value:	0 (0~4095)
Priority:	0 (0~7)
VLAN Tag insertion (VDSL2):	Disable 👻
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On 💙 Load Balance: 🗹

Note : In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.

	Canaal
UK	Cancel

Item	Description
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
Display Name	Type the description for such interface.



Physical Mode	Display the physical mode of such interface. If VDSL2 is detected, this field will display " <b>VDSL2</b> "; if ADSL is detected, it will display " <b>ADSL</b> ".	
DSL Mode	Specify the physical mode (VDSL or ADSL) for such router manually.	
Physical Type	For such interface, no type can be selected.	
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection.  Default  Default  annexA_531a16_533011  annexA_532816_533b11  annexA_541316_540411  annexA_542016_533b11  annexA_547916_544411  annexA_548006_544401  If you have no idea about the selection, simply choose Default or contact the dealer for assistance.	
Line Speed (Kpbs)	If your choose <b>According to Line Speed</b> as the <b>Load</b> <b>Balance Mode</b> in previous page, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.	
VLAN Tag insertion (ADSL)	<ul> <li>The settings configured in this field are available for ADSL.</li> <li>Enable – Enable the function of VLAN with tag.</li> <li>The router will add specific VLAN number to all packets on the WAN while sending them out.</li> <li>Please type the tag value and specify the priority for the packets sending by WAN1.</li> <li>Disable – Disable the function of VLAN with tag.</li> <li>Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.</li> <li>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</li> </ul>	
VLAN Tag insertion (VDSL2)The settings configured in this field are available for VDSL2.Enable – Enable the function of VLAN with tag. The router will add specific VLAN number to all pact on the WAN while sending them out. Please type the tag value and specify the priority for packets sending by WAN1.Disable – Disable the function of VLAN with tag. Tag value – Type the value as the VLAN ID number range is form 0 to 4095. Priority – Type the packet priority number for such The range is from 0 to 7.		

Active Mode	Choose <b>Always On</b> to make the WAN1 connection being activated always; Always On Always On Backup		
	<b>Load Balance</b> : Check this box to enable <b>auto</b> load balance function for such WAN interface.		
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.		
Backup Type	If you choose <b>Backup</b> as the <b>Active Mode</b> , <b>Backup Type</b> will appear. Please specify which WAN will be the Backup interface.		
	Active Mode:	Backup 💌	
	Backup Type (Only if acting as backup for multiple WAN):		
	-	<b>connect</b> – Such backup WAN will naster WAN interface disconnects.	
	When all of selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.		

After finished the above settings, click **OK** to save the settings.

### WAN2 with Ethernet

WAN2 is fixed with physical mode of Ethernet.

WAN >> General Setup

NAN 2		
Enable:	Yes 💌	
Display Name:		
Physical Mode:	Ethernet	
Physical Type:	Auto negotiation 💌	
Line Speed(Kbps):		
DownLink	0	
UpLink	0	
VLAN Tag insertion :	Disable 💌	
Tag value:	0 (0~4095)	
Priority:	0 (0~7)	
Active Mode:	Always On 🖌 Load Balance: 🗹	

Note : In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.



Item	Description	
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.	
Display Name	Type the description for such WAN interface.	
Physical Mode	Display the physical mode of such WAN interface.	
Physical Type	You can change the physical type for WAN2 or choose <b>Auto negotiation</b> for determined by the system.	
	Physical Type: Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex	
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load</b> <b>Balance Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.	
VLAN Tag insertion	<b>Enable</b> – Enable the function of VLAN with tag.	
	The router will add specific VLAN number to all packets on the WAN while sending them out.	
	Please type the tag value and specify the priority for the packets sending by WAN1.	
	<b>Disable</b> – Disable the function of VLAN with tag.	
	<b>Tag value</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.	
	<b>Priority</b> – Type the packet priority number for such VLAN The range is from 0 to 7.	
Active Mode	Choose <b>Always On</b> to make the WAN2 connection being activated always.	
	Always On <mark>❤</mark> Always On Backup	
	<b>Load Balance</b> : Check this box to enable <b>auto</b> load balance function for such WAN interface.	
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.	

Backup Type		the <b>Active Mode</b> , <b>Backup Type</b> by which WAN will be treated as
	Active Mode: Backup Type (Only if acting as backup for	Backup WAN 1 WAN 2 WAN 3 When any of selected WAN disconnect When all of selected WAN disconnect
	e e	AN disconnect – Such backup hen any master WAN interface
		AN disconnect – Such backup nly when all master WAN

After finished the above settings, click **OK** to save the settings.

### WAN3 with USB

To use 3G network connection through 3G USB Modem, please configure WAN3 interface.

#### WAN >> General Setup

WAN 3	
Enable:	Yes 💌
Display Name:	
Physical Mode:	USB
Physical Type:	Auto negotiation 😽
Line Speed(Kbps):	
DownLink	0
UpLink	0
Active Mode:	Always On 💌 Load Balance: 🔽
Note : In DSL bute mode, the r	outer will repeat outematically while switching between VDSL2 and ADSL

Note : In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.



Available settings are explained as follows:

Item	Description
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical type	In such WAN interface, no type can be selected.
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load</b> <b>Balance Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.

# **Dray** Tek

Active Mode	Choose Always On to make the WAN3 connection being activated always. Always On Always On
	Backup           Load Balance: Check this box to enable auto load balance function for such WAN interface.
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.
Backup Type	If you choose <b>Backup</b> as the <b>Active Mode</b> , <b>Backup Type</b> will appear. Please specify which WAN will be treated as the Backup WAN.
	Active Mode: Backup V WAN 1 WAN 2 WAN 3 Backup Type Wikes any of calented WAN discovery
	(Only if acting as backup for multiple WAN):
	When any of selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.
	When all of selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.

After finished the above settings, click **OK** to save the settings.

\_

### 3.1.3 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3) for Internet Access. Due to different Physical Mode for WAN interface, the Access Mode for these connections also varies. Refer to the following figures.

WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	PPPoE / PPPoA	*	Details Page IPv6
WAN2		Ethernet	None PPPoE / PPPoA		Details Page IPv6
WAN3		USB	MPoA / Static or Dynamic IP		Details Page IPv6

Note : Only one WAN can support IPv6.

WAN >> Internet Access

-		-	
Inte	rnet	Acc	229

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	PPPoE / PPPoA	*	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	~	Details Page IPv6
WAN3		USB	None PPPoE		Details Page IPv6
Note : Or	nly one WAN can	support IPv6.	Static or Dynamic IP		
	ing one trait can	support if you	PPTP/L2TP		

#### WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	PPPoE / PPPoA	*	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page IPv6
WAN3		USB	None	*	Details Page IPv6
lote : Or	nly one WAN can	support IPv6.	None 3G/4G USB Modem(PPP mode) 4G USB Modem(DHCP mode)		

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1(ADSL/VDSL2) /WAN2 (Ethernet) /WAN3 (3G USB Modem) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.



Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface.
	Note that <b>Details Page</b> will be changed slightly based on ADSL/VDSL2 physical mode specified on <b>WAN&gt;&gt;General Setup</b> .
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface.
	If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.

### Details Page for PPPoE in WAN1 (Physical Mode: VDSL2)

To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN1** page. The following web page will be shown.

#### WAN >> Internet Access

WAN 1					
PPPoE	Static or Dynamic IP		PPTP/L2TP		IPv6
Enable	O Disable	PPP/N	IP Setup		
		PPP A	uthentication	PAP or C	HAP 🔽
ISP Access Set	ир	Idle T	imeout	-1	second(s)
Username		IP Add	Iress Assignment Met	hod (IPCF	2)
Password			N IP Alias		
Index(1-15) in	Schedule Setup:	Fixed	IP: 🔘 Yes 💿 No (	(Dynamic	IP)
=>,	, , , ,	Fixed	IP Address		
WAN Connectio	on Detection	⊙ D€	afault MAC Address		
Mode	ARP Detect 💙	O Sp	ecify a MAC Addres	s	
Ping IP		MAC	Address: 00 1D	. AA • A8	B7 .69
TTL:					
мти	1442 (Max:1492)				
,	ОК	Ca	ncel		

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	<b>Username</b> – Type in the username provided by ISP in this field.
	Password – Type in the password provided by ISP in this

	of time s set previ	chedule ously in	for your request. Al <b>Application &gt;&gt; Sch</b>	bu can type in four sets I the schedules can be <b>nedule</b> web page and e set in that web page.		
WAN Connection Detection		Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.				
			ARP Detect or Ping AN detection.	<b>g Detect</b> for the system		
			choose Ping Detect ddress in this field fo	as detection mode, you or pinging.		
	TTL (Ti	me to L		e for your reference.		
MTU	It means is 1442.	It means Max Transmit Unit for packet. The default setting is 1442.				
PPP/MP Setup	for PPP. Idle Tim	<ul> <li>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</li> <li>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</li> </ul>				
IP Address Assignment		•	amically assigns IP a	-		
Method (IPCP)	provides wheneve address i you wan	service or you rean the Fix t to use t	to always assign you quest. In this case, y ked IP field. Please c his function.	a some case, your ISP a the same IP address ou can fill in this IP contact your ISP before		
	and wou use WA	ld like to N IP Alia	o utilize them on the as. You can set up to	e public IP addresses WAN interface, please 8 public IP addresses		
	and wou use WA1 other tha	ld like to N IP Alia In the cu	o utilize them on the as. You can set up to rrent one you are usi	WAN interface, please 8 public IP addresses ing.		
	and would use WAN other that	ld like to N IP Alia In the cu	o utilize them on the as. You can set up to rrent one you are usi ndows Internet Explorer	WAN interface, please 8 public IP addresses		
	and would use WAN other that	ld like to N IP Alia In the cu Alias - Wi	o utilize them on the as. You can set up to rrent one you are usi ndows Internet Explorer	WAN interface, please 8 public IP addresses ing.		
	and would use WAN other tha	ld like to N IP Alia In the cu Alias - Wi 2.168.1.1/doc/	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm	WAN interface, please 9 8 public IP addresses ing.		
	and would use WAN other tha	ld like to N IP Alia n the cu: 2 Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipsliss.htm	WAN interface, please o 8 public IP addresses ing.		
	and would use WAN other that WAN111 WAN1 IF Index 1.	Id like to N IP Alia In the cur Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm Iti-NAT ) Aux. WAN IP	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that WAN111 WAN1 IF Index 1. 2.	Id like to N IP Alia In the cu: Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm Itti-NAT ) Aux. WAN IP  0.0.0.0	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that WAN111 WAN1 IF Index 1.	Id like to N IP Alia In the cur Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm Iti-NAT ) Aux. WAN IP	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that would be wanted by the wanted	Id like to N IP Alia In the cu: Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm Itti-NAT ) Aux. WAN IP  0.0.0.0 0.0.0	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that WANTIN WANTIN WANTIN WANTIN THE Index 1. 2. 3. 4.	Id like to N IP Alia In the cur Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelies.htm Itti-NAT ) Aux. WAN IP  0.0.0.0 0.0.00	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that WAN1 IF WAN1 IF Index 1. 2. 3. 4. 5.	Id like to N IP Alia In the cu: Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipelias.htm Itti-NAT ) Aux. WAN IP  0.0.0.0 0.0.0 0.0.0	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool		
	and would use WAN other that WANTIN WANTIN WANTIN WANTIN WANTIN UNDER STATE 1. 2. 3. 4. 5. 6.	Id like to N IP Alia In the cur Alias - Wi Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipdies.htm Iti-NAT ) Aux. WAN IP  0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool U		
	and would use WAN other that WAN1IF WAN1IF WAN1IF Index 1. 2. 3. 4. 5. 6. 7.	Id like to N IP Alia In the cur Alias - Wi 2.168.1.1/doc/ P Alias ( Mu Enable	o utilize them on the as. You can set up to rrent one you are usindows Internet Explorer wipalias.htm Itti-NAT ) Aux. WAN IP  0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	WAN interface, please 8 public IP addresses ing. Join NAT IP Pool U		



fixed IP address in the box of <b>Fixed IP Address</b> .
<b>Default MAC Address</b> – You can use <b>Default MAC</b> <b>Address</b> or specify another MAC address by typing on the
boxes of MAC Address for the router. <b>Specify a MAC Address</b> – Type the MAC address for the
router manually.

#### Details Page for Static or Dynamic IP in WAN1 (Physical Mode: VDSL2)

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

To use **Static or Dynamic IP** as the accessing protocol of the Internet, select **Static or Dynamic IP** from the **WAN>>Internet Access >>WAN1** page. The following web page will appear.

PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
O Enable	<ul> <li>Disable</li> </ul>	WAN	IP Network Settings	WAN IP Alias
		- O O	btain an IP address a	utomatically
Keep WAN Conr		Rout	ter Name	Vigor
		Dom	ain Name	
PING to the IP		* :	Required for some IS	SPs .
PING Interval	0 minute(s)		pecify an IP address	
	Detection.	-1 .	ddress	
WAN Connection Mode	ARP Detect V	Sub	net Mask	
Ping IP		Gate	eway IP Address	
TTL:				
		- 💿 De	efault MAC Address	
MTU	1442 (Max:1500)	O SI	pecify a MAC Addres	s
RIP Protocol		MAC	Address: 00 .1D	.AA A8 .B7 .69
Enable RIP		DNS S	Server IP Address	
		Prima	ry IP Address	8.8.8.8
		Secor	ndary IP Address	8.8.4.4

WAN >> Internet Access

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode – Choose ARP Detect or Ping Detect for the system

	to execute	for WAN detection.	
		f you choose Ping Detect	as detection mode, you
	have to type IP address in this field for pinging.		
		e to Live) – Displays valu is set by telnet command	-
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.		
Bridge Mode	this box to	If you choose <b>Bridged IP</b> as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.	
WAN IP Network Settings	<ul> <li>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</li> <li>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK</li> </ul>		
	to exit the o	-	
		ias - Windows Internet Explorer 8.1.1/doc/wipalias.htm	
		ias ( Multi-NAT )	
	Index En	able Aux. WAN IP	Join NAT IP Pool
	2. [	0.0.0.0	
	2. [ 3.		
	2. [ 3. 4.	0.0.0.0	
	2. [ 3. 4.	0.0.0.0	
	2. [ 3. 4. 5. 6.	0.0.0.0       0.0.0.0       0.0.0.0	
	2. ( 3. 4. 5. 6. 7.	0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0	
	2. ( 3. 4. 5. 6. 7.	0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0	Close



	• Gateway IP Address – Type in gateway IP address.
	<b>Default MAC Address</b> – Type in MAC address for the router. You can use <b>Default MAC Address</b> or specify another MAC address for your necessity.
	<b>Specify a MAC Address</b> – Type in the MAC address for the router manually.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to activate them.

#### Details Page for PPTP/L2TP in WAN1 (Physical Mode: VDSL2)

To use **PPTP/L2TP** as the accessing protocol of the internet, please click the **PPTP/L2TP** tab. The following web page will be shown.

WAN 1				
PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
O Enable F	PPTP 🔘 Enable L2TP 💿 Disable	PPP S	etup	
Server Address	5	PPP A	uthentication	PAP or CHAP 🔽
Specify Gatew	ay IP Address	Idle Ti	meout	1 second(s)
			Iress Assignment Meth	ood (IPCP)
ISP Access Setu	цр	Fixed	IP: 🔘 Yes 💽 No	(Dynamic IP)
Username		Fixed	IP Address	
Password		WAN I	P Network Settings	
Index(1-15) in	Schedule Setup:	O Ob	tain an IP address a	utomatically
=>,	, , , ,	⊙ Sp	ecify an IP address	
		IP A	ddress	
МТО	1442 (Max:1460)	Subr	net Mask	
	ОК	Car	ncel	

WAN >> Internet Access

Item	Description
PPTP/L2TP	<b>Enable PPTP-</b> Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
	<b>Enable L2TP</b> - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.
	<b>Disable</b> – Click this radio button to close the connection through PPTP or L2TP.
	<b>Server Address</b> - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
	<b>Specify Gateway IP Address</b> – Specify the gateway IP

	address for DHCP server.		
ISP Access Setup	Username -Type in the username provided by ISP in this field. Password -Type in the password provided by ISP in this		
	<ul> <li>field.</li> <li>Index (1-15) in Schedule Setup - You can type in four se of time schedule for your request. All the schedules can be set previously in Application &gt;&gt; Schedule web page and you can use the number that you have set in that web page</li> </ul>	e	
MTU	It means Max Transmit Unit for packet. The default setting is 1442.	g	
PPP Setup	<b>PPP Authentication</b> - Select <b>PAP only</b> or <b>PAP or CHAI</b> for PPP.	Р	
	Idle Timeout - Set the timeout for breaking down theInternet after passing through the time without any action.		
IP Address Assignment Method(IPCP)	<b>WAN IP Alias</b> - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.		
	🖉 WAN1IP Alias - Windows Internet Explorer	×	
	http://192.168,1.1/doc/wipalias.htm	3	
	WAN1 IP Alias ( Multi-NAT ) Index Enable Aux, WAN IP Join NAT IP Pool	1	
	2, 🔽 0.0.0.0		
	3. 0.0.0.0		
	4. 0.0.0.0		
	5. 0.0.0.0		
	6. 0.0.0.0		
	7. 0.0.0.0		
	8. 0.0.0.0		
	OK Clear All Close		
	<ul> <li>Fixed IP - 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 I address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your IS before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.</li> <li>Fixed IP Address -Type a fixed IP address.</li> </ul>	, P SP	
WAN IP Network Settings	<b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically.	to	
~~~~ <u>~</u> ~~	<ul> <li>Specify an IP address – Click this radio button to specify some data.</li> </ul>	7	



•	<b>IP</b> Address – Type the IP address.
•	Subnet Mask – Type the subnet mask.

After finishing all the settings here, please click **OK** to activate them.

## Details Page for PPPoE/PPPoA in WAN1 (Physical Mode: ADSL)

WAN >> Internet Access

WAN 1			
PPPoE / PPPoA	MPoA / Static or	Dynamic IP	IPv6
💿 Enable 🔘 Disa	ble	ISP Access Setup	
Modem Settings (for ADSL Multi-PVC channel VPI VCI Encapsulating Type Protocol Modulation	only) Channel 1 0 33 LLC/SNAP PPPoE Multimode	Username Password Separate Account f PPP Authentication Idle Timeout IP Address From ISP Fixed IP O Yes  Fixed IP Address	PAP or CHAP  -1 second(s) WAN IP Alias
PPPoE Pass-through For Wired LAN For Wireless LAN		<ul> <li>Default MAC Addres</li> <li>Specify a MAC Add</li> <li>MAC Address: 00</li> </ul>	
WAN Connection Detection Mode Ping IP TTL: MTU	ARP Detect	Index(1-15) in <u>Schedu</u>	Ile Setup:
	ОК	Cancel	

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	<b>VPI</b> - Type in the value provided by ISP.
	<b>VCI</b> - Type in the value provided by ISP.
	<b>Encapsulating Type</b> - Drop down the list to choose the type provided by ISP.

	<b>Protocol</b> - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP.		
	If you have already used <b>Quick Start Wizard</b> to set the protocol, then it is not necessary for you to change any settings in this group.		
	<b>Modulation</b> –Default setting is Multimode. Choose the one that fits the requirement of your router.		
	Modulation T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode		
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.		
	<b>For Wired LAN</b> – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.		
	<b>For Wireless LAN</b> – It is available for $n$ model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.		
	<b>Note:</b> To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.		
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.		
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.		
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.		
	<b>TTL (Time to Live)</b> – Displays value for your reference. TTL value is set by telnet command.		
MTU	It means Max Transmit Unit for packet. The default setting is 1442.		
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.		
	<b>Username</b> – Type in the username provided by ISP in this		



	field.		
		e in the password pro	ovided by ISP in this
	Separate Accourt VDSL2/ADSL ar password for cont another account a checking this box to type another gr	nd uses the same PP nection. If required, nd password for AE . If it is checked, the roup of account and	you can configure
		et the timeout for bi	reaking down the e without any action.
IP Address From ISP	<ul> <li>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 befor you want to use this function.</li> <li>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, pleasuse WAN IP Alias. You can set up to 8 public IP addresses</li> </ul>		
	other than the cur	rent one you are usi	ng.
	🏉 WAN1IP Alias - Win	dows Internet Explorer	
	WAN1 IP Alias ( Mu		
	Index Enable	Aux. WAN IP	Join NAT IP Pool
	2.	0.0.0.0	
	3.	0.0.0.0	
	4.	0.0.0.0	
	5.	0.0.0.0	
	6.	0.0.0.0	
	7.	0.0.0.0	
	8.	0.0.0.0	
		OK Clear All	Close
	<b>Fixed IP</b> – Click <b>Yes</b> to use this function and type in a fixed IP address in the box of <b>Fixed IP Address</b> .		
	Address or specia	<b>ldress</b> – You can us fy another MAC add ddress for the router	dress by typing on the
	<b>Specify a MAC</b> A router manually.	Address – Type the	MAC address for the
	Index (1-15) in S	for your request. All	ou can type in four sets I the schedules can be

you can use the number that you have set in that web page.

After finishing all the settings here, please click **OK** to activate them.

# Details Page for MPoA/Static or Dynamic IP in WAN1 (Physical Mode: ADSL)

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

To use **MPoA/Static or Dynamic IP** as the accessing protocol of the Internet, select **MPoA** /**Static or Dynamic IP** from the **WAN>>Internet Access >>WAN1** page. The following web page will appear.

WAN >> Internet Access

WAN 1			
PPPoE / PPPoA	MPoA / Static or	Dynamic IP	IPv6
🔘 Enable 🛛 💿 Disat	ble	WAN IP Network Settings	WAN IP Alias
		Obtain an IP address a	automatically
Modem Settings (for ADSL		Router Name	Vigor *
Multi-PVC channel	Channel 2	Domain Name	
Encapsulation			
1483 8	Bridged IP LLC 🛛 👻	* : Required for some 1	ISPs
VPI	0	Specify an IP address	
VCI	88	IP Address	
		Subnet Mask	
Modulation	Multimode 💌	Cohoway ID Address	
		Gateway IP Address	
WAN Connection Detection			
Mode	ARP Detect 💙	Oefault MAC Address	5
Ping IP		Specify a MAC Addre	ess
TTL:		MAC Address: 00 .1	D .AA A8 .B7 .69
MTU	1442 (Max:1500)	DNS Server IP Address	
	(110/12000)	Primary IP Address	8.8.8.8
RIP Protocol			8.8.4.4
Enable RIP		Secondary IP Address	0.0.4.4
Bridge Mode			
Enable Bridge Mode			
		1	
	ОК	Cancel	

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >>Multi PVCs.



	Select M-PVCs Channel m chosen.	neans no selection will be
	<b>Encapsulating</b> - Drop down provided by ISP.	n the list to choose the type
	<b>VPI</b> - Type in the value pro	vided by ISP.
	<b>VCI</b> - Type in the value pro	•
	<b>Modulation</b> –Default settin that fits the requirement of y	g is Multimode. Choose the one your router.
	Modulation	Multimode T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.	
	• •	lays value for your reference.
MTU	It means Max Transmit Uni is 1442.	t for packet. The default setting
RIP Protocol		ol is abbreviated as RIP ow routers exchange routing nable RIP for activating this
Bridge Mode	If you choose <b>Bridged IP</b> as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.	
WAN IP Network Settings	and allows you type in IP ac WAN IP Alias - If you have and would like to utilize the use WAN IP Alias. You can other than the current one you setting is available for WAN	e multiple public IP addresses m on the WAN interface, please n set up to 8 public IP addresses pu are using. Notice that this

C WAN11	r Anas - mi	ndows Internet Explorer	
🔊 http://19	2.168.1.1/doc/	Wipalias.htm	
	PAlias (Mu		
	Enable	Aux. WAN IP	Join NAT IP Pool
1.			
2.		0.0.0.0	
3.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
	ne IP add <b>Route</b> provic	OK Clear All Idress automatically. Irress automatically. Idress automatically. Idress automatically. Idress automatically. Idress automatically. Idress automatically. Idress automatically. Idress automatically. Idress automatically.	he router name
obtain th	ne IP add Route provic Doma you ha	Idress automatically. Iress au	y – Click this butto he router name the domain name t
obtain th	ne IP add Route provic Doma you ha an IP ad	Idress automatically. Iress automatically. Irer Name – Type in t Ited by ISP. Inn Name – Type in	y – Click this butto he router name the domain name t
obtain th • Specify	ne IP add Route provic Doma you ha an IP ad ta.	Idress automatically. Iress automatically. Iress automatically. Iress automatically. Irest and a transformatically. Irest and the set of the se	y – Click this button the router name the domain name t adio button to spec
obtain th • Specify	ne IP add Route provic Doma you ha an IP ad ta. IP Ad	Idress automatically. Iress automatically. Iress automatically. Iress automatically. Iress – Type in t Idress – Type in ave assigned. Idress – Click this r	y – Click this butto he router name the domain name t adio button to spec private IP address.
obtain th • Specify	ne IP add Route provic Doma you ha an IP ad ta. IP Ad Subne	Idress automatically. Iress automatically. Iress automatically. Iress automatically. Iress – Type in the Idress – Click this ra- Idress – Type in the Idresk – Type in the Idress – Type in th	y – Click this butto he router name the domain name t adio button to spec private IP address. he subnet mask.
obtain the	ne IP add Route provid Doma you ha an IP ad ta. IP Ad Subne Gatev addres MAC A You can u	Idress automatically. Iress automatically. Iress automatically. Iress automatically. Iress – Type in the Idress – Click this ra- Idress – Type in the Idresk – Type in the Idress – Type in th	y – Click this butto he router name the domain name tl adio button to speci private IP address. he subnet mask. ype in gateway IP AC address for the address or specify
obtain the solution of the sol	ne IP add Route provid Doma you ha an IP ad ta. IP Ad Subne Gatev addres MAC A	Idress automatically. Iress automatically. Iress automatically. Iress automatically. Iress automatically. Irest Name – Type in the ave assigned. Idress – Click this ra- Idress – Type in the Idress – Type in the Idress – Type in Mase Default MAC A Idress for your necess Address – Type in the Idress – Type - T	y – Click this butto he router name the domain name th adio button to speci private IP address. he subnet mask. ype in gateway IP AC address for the address or specify sity.

After finishing all the settings here, please click  $\mathbf{OK}$  to activate them.

### Details Page for PPPoE in WAN2

To choose PPPoE as the accessing protocol of the Internet, please select **PPPoE** from the **WAN>>Internet Access >>WAN2** page. The following web page will be shown.

PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
🔿 Enable 🧕 🧕	) Disable	PPP/MP	Setup	
ISP Access Setup Username Password Index(1-15) in <u>Sch</u> =>,	nedule Setup:	Idle Tim IP Addre WAN Fixed IP		od (IPCP)
WAN Connection De Mode Ping IP TTL:	ARP Detect	O Spe	ault MAC Address cify a MAC Address ddress: 00 .1D	.AA:A8 .B7 .6A
мти	1442 (Max:1492)			

WAN >> Internet Access

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	<b>Username</b> – Type in the username provided by ISP in this field.
	The maximum length of the user name you can set is 63 characters.
	<b>Password</b> – Type in the password provided by ISP in this field.
	The maximum length of the password you can set is 62 characters.
	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system

	to execu	ite for W	AN detection.	
	Ping IP have to TTL (T	– If you type IP a <b>ime to L</b>		
MTU		s Max Tr	-	et. The default setting
PPP/MP Setup		<b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.		nly or PAP or CHAP
			Set the timeout for br using through the time	-
IP Address Assignment Method (IPCP)	<ul> <li>It Usually ISP dynamically assigns IP additime you connect to it and request. In supprovides service to always assign you to whenever you request. In this case, you address in the Fixed IP field. Please conyou want to use this function.</li> <li>WAN IP Alias - If you have multiple prand would like to utilize them on the Wuse WAN IP Alias. You can set up to 8 other than the current one you are using additional WAN IP address and check click OK to exit the dialog.</li> </ul>		some case, your ISP the same IP address ou can fill in this IP ontact your ISP before public IP addresses WAN interface, please 8 public IP addresses ng. Type the	
	🏉 WANII	🤌 WAN1IP Alias - Windows Internet Explorer		
		92.168.1.1/doc. P Alias ( Mi		
		Enable	Aux. WAN IP	Join NAT IP Pool
				_
	1.			✓
	1. 2.		0.0.0.0	
		,	0.0.0.0	
	2.	,		
	2. 3.	,	0.0.0.0	
	2. 3. 4.		0.0.0.0	
	2. 3. 4. 5.		0.0.0.0	
	2. 3. 4. 5. 6.		0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	

After finishing all the settings here, please click **OK** to activate them.



#### Details Page for Static or Dynamic IP in WAN2

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.

WAN 2			
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<ul> <li>Enable</li> </ul>	O Disable	WAN IP Network Settings	WAN IP Alias
Keep WAN Con	nection G to keep alive 0	<ul> <li>WAN IP Network Settings</li> <li>Obtain an IP address a Router Name</li> <li>Domain Name</li> <li>* : Required for some IS</li> <li>DHCP Client Identifier for some Enable</li> <li>Username</li> <li>Password</li> <li>Specify an IP address</li> <li>Subnet Mask</li> <li>Gateway IP Address</li> </ul>	automatically
Enable RIP	OK	<ul> <li>Default MAC Address</li> <li>Specify a MAC Address</li> <li>MAC Address: 00 .1D</li> <li>DNS Server IP Address</li> <li>Primary IP Address</li> <li>Secondary IP Address</li> <li>Cancel</li> </ul>	

WAN >> Internet Access

Item	Description
Enable / Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check <b>Enable PING to keep alive</b> box to activate this function. <b>PING to the IP</b> - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.

			Enter the interval for G operation.	or the system to	
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.				
		<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.			
				as detection mode, you	
	TTL (Ti	<ul> <li>have to type IP address in this field for pinging.</li> <li>TTL (Time to Live) – Displays value for your reference.</li> <li>TTL value is set by telnet command.</li> </ul>			
MTU	It means is 1480.	It means Max Transmit Unit for packet. The default setting is 1480.			
RIP Protocol	(RFC1 tables in	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.			
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, pleas use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.				
	WANIIP Alias - Windows Internet Explorer     Image: http://192.168.1.1/doc/wipalias.htm				
		P Alias ( M Enable	ulti-NAT ) Aux. WAN IP	Join NAT IP Pool	
		P Alias ( M Enable 		Join NAT IP Pool	
	Index	Enable		_	
	Index 1.	Enable	Aux. WAN IP	_	
	Index 1. 2.	Enable	Aux. WAN IP	_	
	Index 1. 2. 3.	Enable	Aux. WAN IP 0.0.0.0 0.0.0.0	_	
	Index 1. 2. 3. 4.	Enable	Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0		
	Index           1.           2.           3.           4.           5.	Enable	Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0 0.0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.		
	Index 1. 2. 3. 4. 5. 6.	Enable	Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0		
	Index           1.           2.           3.           4.           5.           6.           7.	Enable	Aux. WAN IP            0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0		
	Index 1. 2. 3. 4. 5. 6. 7. 8. Obtain :	Enable	Aux. WAN IP         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0.0.0.0         0K         Clear All         Idress automatically if         de.         er Name: Type in th	✓ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	



	• Enable: Check the box to specify username and
	password as the DHCP client identifier for some ISP.
	• Username: Type a name as username. The maximum length of the user name you can set is 63 characters.
	• <b>Password:</b> Type a password. The maximum length of the password you can set is 62 characters.
	<b>Specify an IP address</b> – Click this radio button to specify some data if you want to use <b>Static IP</b> mode.
	• <b>IP Address</b> : Type the IP address.
	• <b>Subnet Mask</b> : Type the subnet mask.
	• Gateway IP Address: Type the gateway IP address.
	<b>Default MAC Address</b> : Click this radio button to use default MAC address for the router.
	<b>Specify a MAC Address</b> : Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the <b>Specify a MAC Address</b> and enter the MAC address in the MAC Address field.
DNS Server IP Address	Type in the primary IP address for the router if you want to use <b>Static IP</b> mode. If necessary, type in secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to activate them.

#### Details Page for PPTP/L2TP in WAN2

To use **PPTP/L2TP** as the accessing protocol of the internet, please click the **PPTP/L2TP** tab. The following web page will be shown.

WAN >> Internet Access

PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
O Enable P	PTP 🔿 Enable L2TP 💿 Disable	PPP Set	up	
Server Address		PPP Aut	hentication F	PAP or CHAP 🔽
Specify Gatewa	ay IP Address	Idle Tim	eout -	1 second(s)
			ess Assignment Meth	od (IPCP)
ISP Access Setu	р	Fixed IP	: 🔘 Yes 💿 No (	Dynamic IP)
Username		Fixed IP	Address	
Password		WAN IP	Network Settings	
Index(1-15) in	Schedule Setup:	O Obta	ain an IP address au	utomatically
=> ,		Specific	cify an IP address	
		- IP Add	ress	
МТО	1442 (Max:1460)	Subne	t Mask	

Item	Description		
PPTP/L2TP	<b>Enable PPTP-</b> Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.		
	<b>Enable L2TP</b> - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.		
	<b>Disable</b> – Click this radio button to close the connection through PPTP or L2TP.		
	<b>Server Address</b> - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.		
	<b>Specify Gateway IP Address</b> – Specify the gateway IP address for DHCP server.		
ISP Access Setup	<b>Username</b> -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.		
	<b>Password</b> -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.		
	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.		
MTU	It means Max Transmit Unit for packet. The default setting is 1480.		
PPP Setup	<b>PPP Authentication</b> - Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.		
	<b>Idle Timeout</b> - Set the timeout for breaking down the Internet after passing through the time without any action.		
IP Address Assignment Method(IPCP)	<b>WAN IP Alias</b> - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.		

		ATTRACTOR	Alias - W	indows Internet Explorer			
	<b>e</b> 1	http://192	2.168.1.1/doc	Avipalias.htm	8		
WAN1 IP Alias ( Multi-NAT )							
		ndex	Enable	Aux. WAN IP	Join NAT IP Pool		
		1.	<b>V</b>				
		2.		0.0.0.0			
		з.		0.0.0.0			
		4.		0.0.0.0			
		5.		0.0.0.0			
		6.		0.0.0.0			
		7.		0.0.0.0			
		8.		0.0.0.0			
				OK Clear All	Close		
	you you add this befo fund <b>Fix</b> o	each r ISP ress v IP ac ore yc ction ed IP	time yo provide wheneve ddress in ou want and typ Addre	lly ISP dynamically a ou connect to it and re es service to always as er you request. In this n the Fixed IP field. P to use this function. C e in a fixed IP address ss -Type a fixed IP ad	quest. In some case, ssign you the same IF case, you can fill in lease contact your IS Click <b>Yes</b> to use this s in the box. ldress.		
WAN IP Network Settings	you you add this befo fund <b>Fix</b> <b>Obt</b> obta	each r ISP ress v IP ac ore yc ction ed IP tain a	time yo provide wheneve ddress in ou want and typ <b>Addre</b> an IP ac e IP add	bu connect to it and re es service to always as er you request. In this in the Fixed IP field. P to use this function. C e in a fixed IP address	quest. In some case, ssign you the same IF case, you can fill in lease contact your IS Click <b>Yes</b> to use this in the box. Idress. – Click this button to		
	you you add: this befo fund <b>Fixo</b> <b>Obt</b> obta <b>Spe</b>	each r ISP ress v IP ac ore yc ction ed IP tain a	time yo provide wheneve ddress in ou want and typ <b>Addre</b> <b>Addre</b> IP ado an IP ado	bu connect to it and re es service to always as er you request. In this in the Fixed IP field. P to use this function. C e in a fixed IP address ss -Type a fixed IP ad dress automatically dress automatically.	quest. In some case, ssign you the same IF case, you can fill in lease contact your IS Click <b>Yes</b> to use this in the box. Idress. - Click this button to		
	you you add: this befo fund <b>Fixo</b> <b>Obt</b> obta <b>Spe</b>	each r ISP ress v IP ac ore yc ction ed IP tain a ain th ccify a	time yo provide wheneve ddress in ou want and typ <b>Addre</b> <b>an IP ac</b> <b>an IP ac</b> <b>an IP ac</b> <b>an IP ac</b> <b>a.</b>	bu connect to it and re es service to always as er you request. In this in the Fixed IP field. P to use this function. C e in a fixed IP address ss -Type a fixed IP ad dress automatically dress automatically.	quest. In some case, ssign you the same II case, you can fill in lease contact your IS Click <b>Yes</b> to use this s in the box. Idress. – Click this button to dio button to specify		

After finishing all the settings here, please click **OK** to activate them.

#### Details Page for 3G/4G USB Modem (PPP mode) in WAN3

To use **3G/4G USB Modem (PPP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **3G/4G USB Modem (PPP mode)** for WAN3. The following web page will be shown.

#### WAN 3

3G/4G USB Modem(PPP mode)	4G USB Modem(DHCP mode)	IPv6
3G/4G USB Modem(PPP mode)	🔿 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	
	(Default:AT&FE0V1X1&D2&C1	S0=0)
APN Name		Apply
Modem Initial String2	AT	
Modem Dial String	ATDT*99#	
	(Default:ATDT*99#, CDMA:AT SCDMA:ATDT*98*1#)	ГDT#777, TD-
PPP Username		(Optional)
PPP Password		(Optional)
PPP Authentication	PAP or CHAP	
Index(1-15) in <u>Schedule</u> Setup:		
=>,,,		
WAN Connection Detection		
Mode	ARP Detect 💌	
Ping IP		
TTL:		
	OK Cancel Default	

Available settings are explained as follows:

Item	Description
3G /4G USB Modem (PPP mode)	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 47 characters.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click <b>Apply</b> . The maximum length of the name you can set is 43 characters.

Modem Initial String2	The initial string 1 is shared with APN.
	In some cases, user may need another initial AT command to restrict 3G band or do any special settings.
	The maximum length of the string you can set is 47 characters.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
	The maximum length of the string you can set is 31 characters.
PPP Username	Type the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Type the PPP password (optional). The maximum length of the password you can set is 62 characters.
<b>PPP</b> Authentication	Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	<b>TTL</b> ( <b>Time to Live</b> ) – Displays value for your reference. TTL value is set by telnet command.

After finishing all the settings here, please click  $\mathbf{O}\mathbf{K}$  to activate them.

#### Details Page for 4G USB Modem (DHCP mode) in WAN3

To use **4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **4G USB Modem (DHCP mode)** for WAN3. The following web page will be shown.

WAN 3				
3G/4G USB Modem(PPP	mode)	4G USB Modem(DHCP mode)	IPv6	
4G USB Modem(DHCP mode)	OEnable	e 💿 Disable		
SIM PIN code				
Network Mode	4G/3G/20	) 🕐 (Default:4G/3G/2G)		
APN Name				
мти	1380	(Default: 1380)		
LTE software version				
LTE hardware version				
Supported dongle list:				
Samsung swc-u200				
LG VL600				
Yota-One LU150 / ZTE MP	821D			
		OK Cancel		

Available settings are explained as follows:

WAN >> Internet Access

Item	Description
4G USB Modem (DHCP mode)	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 19 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click <b>Apply</b> . The maximum length of the name you can set is 47 characters.
MTU	It means Max Transmit Unit for packet. The default setting is 1380.

After finishing all the settings here, please click **OK** to activate them.

#### Details Page for IPv6 – Offline in WAN1/WAN2/WAN3

When Offline is selected, the IPv6 connection will be disabled.



WAN >> Internet Acces	S		
WAN 1			
PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access	Mode		
Connection Typ	offline Offline	*	
	OK Cancel		

#### Details Page for IPv6 – PPP in WAN1/WAN2

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor router through IPv6CP. Later, use DHCPv6 or Accept RA to acquire the IPv6 prefix address (such as: 2001:B010:7300:200::/64) offered by the ISP. In addition, PCs under LAN also can have the public IPv6 address for Internet access by means of the generated prefix.

No need to type any other information for PPP mode.

WAN	>>	Internet	Access
		meernoe	100000

PPPoE	Static or Dynamic IP		PPTP	IPv6
Internet Access	Node			
Connection Ty	e	PPP	~	
Note : IPv4 WA	I setting should be PPP	oE client.		

Below shows an example for successful IPv6 connection based on PPP mode.

#### **Online Status**

Physical Connect	ion		System Uptim	em Uptime: 0:2:32	
IPv4			IPv6		
LAN Status					
IP Address					
	00:201:21D:AAFF:F FF:FEA6:2568/64 (L	EA6:2568/64 (Global) .ink)			
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes		
7	4	690	328		
WAN2 IPv6 Status	3		>> <u>Dr</u>	op PPP	
Enable	Mode	Up Time			
Yes	PPP	0:02:08			
IP			Gateway IP		
	00:201:21D:AAFF:F F:FEA6:256A/128 (L		) FE80::90:1A00:242:AD52		
DNS IP					
2001:B000:16 2001:B000:16					
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes		
7	9	544	1126		



**Note**: At present, the **IPv6 prefix** can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

#### Details Page for IPv6 – TSPC in WAN1/WAN2/WAN3

Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (<u>http://gogonet.gogo6.com/page/freenet6-account</u>) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type	TSPC	*	
TCDC Configuration			
TSPC Configuration			
Username			
Password			
Confirm Password			
commin r assword			
Tunnel Broker			

Available settings are explained as follows:

WAN >> Internet Access

Item	Description		
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for <u>http://gogonet.gogo6.com/page/freenet6-account</u> . The maximum length of the name you can set is 63 characters.		
Password	Type the password assigned with the user name. The maximum length of the name you can set is 19 characters.		
<b>Confirm Password</b> Type the password again to make the confirmation			
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.		

After finished the above settings, click **OK** to save the settings.

#### Details Page for IPv6 – AICCU in WAN1/WAN2/WAN3

WAN >> Internet Access

WAN 1			
PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode	)		
Connection Type	AICCU	*	
AICCU Configuration			
Always On			
Username			
Password			
Confirm Password			
Tunnel Broker	tic.sixxs.net		
Subnet Prefix		/	]

Note : If "Always On" is not enabled, AICCU connection would only retry three times.

OK Cancel

Available settings are explained as follows:

Item Description		
Always On	Check this box to keep the network connection always.	
Username	Type the name obtained from the broker. Please apply new account at <u>http://www.sixxs.net/</u> . It is suggested for you to apply another username and password. The maximum length of the name you can set is 19 characters.	
Password	Type the password assigned with the user name. The maximum length of the password you can set is 19 characters.	
Confirm Password	Type the password again to make the confirmation.	
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.	
Subnet Prefix	Type the subnet prefix address getting from service provider. The maximum length of the prefix you can set is 128 characters.	

After finished the above settings, click **OK** to save the settings.

#### Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

DHCPv6 client mode would use DHCPv6 protocol to obtain IPv6 address from server.

#### WAN >> Internet Access

AN 1				
PPPoE	Stati	c or Dynamic IP	PPTP	IPv6
Internet Acce	ss Mode			
Connection	Гуре	DHCPv6 Client 🗸	·	
DHCPv6 Clie	nt Configuration			
Identity As		Prefix Delegation 🔘 Non-tem	porary Address	
IAID (Ident	tity Association ID)	4230640032	. ,	
		OK Cancel		

Available settings are explained as follows:

Item	Description	
Identify Association	Choose <b>Prefix Delegation</b> or <b>Non-temporary Address</b> as the identify association.	
IAID	Type a number as IAID.	

After finished the above settings, click **OK** to save the settings.

#### Details Page for IPv6 – Static IPv6 in WAN1/WAN2

This type allows you to setup static IPv6 address for WAN interface.

PPOE	Static or Dynamic	IP	PPTP	IPv6
Internet Acc	ess Mode			
Connection	Туре	Static IPv6	*	
Static IPv6 A	ddress configuration			
IPv6 Addre		/ Prefix	Length	
		/	Add	Delete
Current IP	/6 Address Table			
Static IPv6 G	ateway configuration			
	<b>ateway</b> configuration way Address	_		
		]		

Available settings are explained as follows:

Item	Description
Static IPv6 Address	<b>IPv6 Address</b> – Type the IPv6 Static IP Address.
configuration	<b>Prefix Length</b> – Type the fixed value for prefix length.
	Add – Click it to add a new entry.
	<b>Delete</b> – Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.
Static IPv6 Gateway Configuration	<b>IPv6 Gateway Address -</b> Type your IPv6 gateway address here.

After finished the above settings, click **OK** to save the settings.

#### 3.1.4 Multi-PVCs

This router allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVCs** page.

#### General

The system allows you to set up to eight channels which are ready for choosing as the first PVC line that will be used as multi-PVCs.

WAN >> Multi-PVCs

🗹 Enal	ble Mul	ti-PVCs S	etup					
Gene	eral	ATN	l Qo S	Port-b	ased Bridge	PVC Redirect/Add Tag		
Channe	el 👘	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation	
1.			0	33	UBR 💌	PPPoE 💌	LLC/SNAP 💌	
2.		✓	0	88	UBR 💌	MPoA 💌	1483 Bridged IP LLC 🖌	
з.			1	43	UBR 🖌	PPPoA 🗸	VC MUX 🗸	
4.			1	44	UBR 🗸	PPPoA 🗸	VC MUX 🗸	
5.	WAN		1	45	UBR 🖌	PPPoA 🗸	VC MUX 🗸	
6.	WAN		1	46	UBR 🗸	PPPoA 🗸	VC MUX 🗸	
7.	WAN		1	47	UBR 🖌	PPPoA 🗸	VC MUX 🗸	
8.			1	48	UBR 🛩	PPPoA 👻	VC MUX 🗸	

Note:VPI/VCI must be unique for each channel!

OK	Clear	Cancel

Item	Description			
Enable Multi-PVCs Setup	Check the box to enable such function.			
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the <b>Multi-PVC channel</b> drop down list on the web page of <b>Internet Access</b> . Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of <b>Internet Access</b> .			
VPI	Type in the value provided by your ISP.			
VCI	Type in the value provided by your ISP.			
QoS Type	Select a proper QoS type for the channel. QoS Type UBR V UBR CBR ABR nrtVBR rtVBR			

Protocol	Select a proper pro Protocol PPPoE PPPoA PPPoE MPoA	rotocol for this channel.		
Encapsulation	Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.			
		1483 Route IP LLC 🛛 👻		
		1483 Bridged IP LLC		
		1483 Route IP LLC		
	VC MUX LLC/SNAP	1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux(IPoA) 1483 Bridged IP(IPoE)		

After finished the above settings, click **OK** to save the settings.

WAN links for Channel 5, 6 and 7 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 5, 6 or 7 to configure your router.

WAN >> Multi-PVCs >> PVC Channel 5

WAN for Router-bo	orne Applicatio	n: Management 🗸				
⊙ Enable ○ D	)isable					
DSL Modem Setti	ngs					
VPI	1	QoS Type	UBR 🖌	PVC Redirect	Disable 👻	
VCI	45	Protocol	PPPoA 🛩	Add Tag 🔲	0	
L		Encapsulation	VC MUX 🗸			
WAN Connection	Detection					
Mode	е	ARP Dete	ect 💌			
Ping	IP					
TTL:						
PPPoE/PPPoA Cli	ient		MPoA (RFC	1483/2684)		
ISP Access Setup			⊖ Obtain a	n IP address au	itomatically	
ISP Name			Router Na	ime	Vigor	*
Username			Domain Na	ame		*
Password			*: Require	ed for some ISI	P <sub>S</sub>	
PPP Authenticati	on PAP	or CHAP 🔽	Specify a	an IP address		
🗹 Always On			IP Addres	s		
Idle Timeout	-1	second(s)	Subnet M	ask		
IP Address From	ISP		Gateway	IP Address		
Fixed IP 🛛 🔿 Y	ies 💿 No (Dyr	namic IP)	DNS Server	IP Address		
Fixed IP Address			Primary IP	Address	8.8.8.8	
			Secondary	IP Address	8.8.4.4	
		OK	Cancel	1		

Item	Description			
WAN for Router-borne	Choose the router service for channel 5, 6 or 7.			
Application	Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be			
	effective for Web configuration/telnet/TR069.			
	<b>VoIP</b> - It can be specified for VoIP only. If you choose VoIP, the configuration for this PVC will be effective for VoIP data transmitting and receiving.			
DSL Modem Settings	<b>VPI</b> - Type in the value provided by ISP.			
	<b>VCI</b> - Type in the value provided by ISP.			
	<b>QoS Type -</b> Select a proper QoS type for the channel according to the information that your ISP provides.			
	<b>Protocol</b> - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP.			
	<b>Encapsulation</b> - Drop down the list to choose the type provided by ISP.			
	<b>PVC Redirect</b> – Choose on PVC to be bound with such WAN interface.			
	Add Tag – It is used to identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).			
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.			
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.			
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, yo have to type IP address in this field for pinging.			
	<b>TTL (Time to Live)</b> – Displays value for your reference. TTL value is set by telnet command.			
PPPoE/PPPoA Client	Enter your allocated username, password and authenticatio parameters according to the information provided by your ISP.			
	<b>ISP Name</b> – Type in the name of your ISP.			
	<b>Username</b> – Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters.			
	<b>Password</b> – Type in the password provided by ISP in this field. The maximum length of the password you can set is 48 characters.			
	<b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.			
	<b>Always On</b> – Check it to keep the network connection always.			
	Idle Timeout – Set the timeout for breaking down the			



	Internet after passing through the time without any action.
	<b>Fixed IP</b> – Click <b>Yes</b> to use this function and type in a fixed IP address in the box of <b>Fixed IP Address</b> .
MPoA (RFC1483/2684)	<b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically.
	• <b>Router Name</b> – Type in the router name provided by ISP.
	• <b>Domain Name</b> – Type in the domain name that you have assigned.
	<b>Specify an IP address</b> – Click this radio button to specify some data.
	• <b>IP Address</b> – Type in the private IP address.
	• Subnet Mask – Type in the subnet mask.
	• Gateway IP Address – Type in gateway IP address.
	DNS Server IP Address - Type in the primary IP address
	for the router if you want to use <b>Static IP</b> mode. If necessary, type in secondary IP address for necessity in the future.

After finished the above settings, click **OK** to save the settings and return to previous page.

### ATM QoS

WAN >> Multi-PVCs

Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.

eneral	ATM QoS	Port-based Bridge PCR	SCR	Redirect/Add Tag MBS
annel 1.	QoS Type	0	0	0
2.	UBR 🗸	0	0	0
3.	UBR 🖌	0	0	0
4.	UBR 🗸	0	0	0
5.	UBR 🖌	0	0	0
6.	UBR 🛩	0	0	0
7.	UBR 🗸	0	0	0
8.	UBR 🗸	0	0	0

Available settings are explained as follows:

Item	Description

QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides.
PCR	It represents Peak Cell Rate. The default setting is "0".
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.

After finished the above settings, click **OK** to save the settings

#### **Port-based Bridge**

General page lets you set the first PVC. As to set the second PVC line, please click the **Port-based Bridge** tab to open Bridge configuration page.

WAN >> Multi-PVCs

ieneral	neral ATM QoS		Port-based Bridge				PVC Redirect/Add Tag		
Channel	Enable	P1	P2	<b>P</b> 3	P4	P5	P6	Service Type	
1.								Normal 🛩	
2.								Normal 😪	
з.								Normal 🛩	
4.								Normal 💌	
5.								Normal 🛩	
6.								Normal 🛩	
7.								Normal 🛩	
8.								Normal 🛩	

Available settings are explained as follows:

OK

Item	Description		
Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT using.		
P1 to P6	It means the LAN port 1 to 6. Check the box to designate the LAN port for channel 3 to 8.		

Clear

Cancel



Service Type	Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. Such feature is used for specific application. Please choose <b>Normal</b> as the <b>Service Type</b> .
	Normal – It means that the PVC can accept all packets.
	<b>IGMP</b> –It means that such PVC can accept IGMP packets only. Such type just meets a specific environment on some ISPs. Data and IGMP packets will be transmitted and received with different PVC.

Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click **Cancel** to abort the configuration and exit this page.

#### **PVC Redirect/Add Tag**

This page allows you to make a channel sharing the same network connection (VPI/VCI) with specified channel. For example, Channel 3 is set with *PVC Redirect=1*. It means that such channel will use the physical connection of Channel 1 to have data transmission. In other word, two WAN interfaces share the same physical WAN connection.

WAN >> Multi-PVCs

General	ATM QoS	Port-based Br	0	Redirect/Add Tag
Channel	PVC	Redirect	Add Tag	Priority
1.	Disa	able 💙	0	0
2.	Dis	able 😪	0	0
з.	Dis	able 💙	0	0
4.		able 💌	0	0
5.	Disa 1	able	0	0
6.	2		0	0
7.	4		0	0
8.	5		0	0
: Multiple ch	annels may us 8	channel li	nk through the PVC Redired	ct configuratiion.

Clear

Cancel

OK

Available settings are explained as follows:

Item	Description
PVC Redirect	Specify one PVC channel for redirection.  Disable  Disable  1  2  3  4  5  6  7  8
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

Click Clear to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click OK to save and exit this page. Or click Cancel to abort the configuration and exit this page.

#### 3.1.5 Multi-VLAN

This router allows you to create multi-VLAN for different data transferring for using. Simply go to WAN and select Multi-VLAN.

#### General

The system allows you to set up to eight channels for multi-VLAN.

WAN >> Multi-VLAN

Gener	al	Bridge		
Channel	Enable		Add Tag	Priority
1.			0	0 ~
2.			0	0 ~
з.			0	0 ~
4.			0	0 🗸
5.		WAN	0	0 🗸
6.		WAN	0	0 🗸
7.		WAN	0	0 🛩
8.			0	0 🗸

Note: 1. Tag value must be set between 1 ~ 4095 and unique for each channel.

2. Only one channel can be untagged (equal to 0) at a time.

3. Channel 1 and channel 2 are reserved for NAT/Route application.

4. Channel 5 to channel 7 can be used for Router-borne application.

OK Clear

Item	Description
Enable	Check it to enable such function.
Channel	Display the number of each channel.
Enable	Check this box to enable that channel. The channels that you enabled here will be shown in the <b>Multi-VLAN</b> channel drop down list on the web page of <b>Internet Access</b> . Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of <b>Internet</b> <b>Access</b> .
Add Tag	To identify the usage of VLAN, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

WAN link for Channel 5, 6 and 7 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 5, 6 or 7 to configure your router.

WAN >> Multi-VLAN >> Channel 5

PPPoE/PPPoA Client O Enable O Disable	Static or Dynamic IP O Enable  O Disable
ISP Access Setup	WAN IP Network Settings
ISP Name	Obtain an IP address automatically
Username	Router Name Vigor *
Password	Domain Name
PPP Authentication PAP or CHAP	*: Required for some ISPs
Always On	Specify an IP address
Idle Timeout -1 second(s)	IP Address
IP Address From ISP	Subnet Mask
Fixed IP 🛛 Yes 💿 No (Dynamic IP)	Gateway IP Address
Fixed IP Address	
	DNS Server IP Address
	Primary IP Address 8.8.8.8
	Secondary IP Address 8.8.4.4

Item	Description
WAN for Router-borne Application	<ul> <li>Choose the router service for channel 5, 6 or 7.</li> <li>Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069.</li> <li>VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this VLAN will be effective for</li> </ul>

	a transmitting and receiving.
IPTV, the	t can be specified for IPTV only. If you choose e configuration for this VLAN will be effective for a transmitting and receiving.

For other settings, refer to Details Page for PPPoE in WAN1.

#### Bridge

General page lets you set the first channel. As to set the third channel, please click the **Bridge** tab to open **Bridge** configuration page.

WAN >> Multi-VLAN

Gener	al	Bridge					
Channel	Enable	P1	P2	P3	P4	P5	P6
1.							
2.							
з.							
4.							
5.							
6.							
7.							
8.							

Note: P1 is reserved for Nat/Route use.

OK Clear

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT/Route using.
P1 to P6	It means the LAN port 1 to 6. Check the box to designate the LAN port for channel 3 to 8.

Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click **Cancel** to abort the configuration and exit this page.

### 3.1.6 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN1, WAN2, and WAN3 interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

**Note:** Load-Balance Policy is running only when WAN1, WAN2 and WAN3 are activated.

WAN >> Load-Balance Policy

Load-Balance Policy	

Index	Enable	Protoco	I	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Move Up	Move Down
1		any	¥	WAN1 🛩							<u>Down</u>
2		any	¥	WAN1 👻						<u>UP</u>	<u>Down</u>
<u>3</u>		any	×	WAN1 🛩						<u>UP</u>	<u>Down</u>
4		any	¥	WAN1 🛩						<u>UP</u>	<u>Down</u>
<u>5</u>		any	*	WAN1 🛩						<u>UP</u>	<u>Down</u>
<u>6</u>		any	¥	WAN1 👻						<u>UP</u>	<u>Down</u>
7		any	¥	WAN1 🗸						<u>UP</u>	<u>Down</u>
<u>8</u>		any	¥	WAN1 👻						<u>UP</u>	<u>Down</u>
<u>9</u>		any	*	WAN1 🛩						<u>UP</u>	<u>Down</u>
<u>10</u>		any	¥	WAN1 🛩						<u>UP</u>	<u>Down</u>
<< <u>1-10</u>	<u>11-20</u>	<u>21-30   31</u>	-32	>>						1	<u>Vext</u> >>

OK

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the load-balance policy configuration web page.
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to change the protocol for the WAN interface.
WAN	Use the drop-down menu to change the WAN interface.
Src IP Start	Displays the IP address for the start of the source IP.
Src IP End	Displays the IP address for the end of the source IP.
Dest IP Start	Displays the IP address for the start of the destination IP.
Dest IP End	Displays the IP address for the end of the destination IP.
Dest Port Start	Displays the IP address for the start of the destination port.
Dest Port End	Displays the IP address for the end of the destination port.
Move UP/Move Down	Use <b>Up</b> or <b>Down</b> link to move the order of the policy.

Click Index 1 to access into the following page for configuring load-balance policy.

```
WAN >> Load-Balance Policy
```

Enable	
Protocol	any 🗸
Binding WAN Interface	WAN1 👻 🗹 Auto failover to the other WAN
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

Item	Description
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
	Protocol any any TCP UDP TCP/UDP ICMP IGMP
Binding WAN interface	Choose the WAN interface (WAN1/WAN2/WAN3) for binding. <b>Auto failover to other WAN</b> – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is failover.
Src IP Start	Type the source IP start for the specified WAN interface.
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Dest IP Start	Type the destination IP start for the specified WAN interface.
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Dest Port Start	Type the destination port start for the destination IP.



Dest Port End	Type the destination port end for the destination IP. If this
	field is blank, it means that all the destination ports will be
	passed through the WAN interface.

When you finish the configuration, please click **OK** to save and exit this page.

WAN >> Load-Balance Policy										
Load-Ba	alance Po	olicy								
Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Move Up	Mov Dow
1	<b>V</b>	any 🗸	WAN1 💌	192.168.1.56	192.168.1.60	172.16.3.88	172.16.3.92			Dow
<u>2</u>		any 🗸	WAN1 🔽						<u>UP</u>	Dow
			INCONTA							

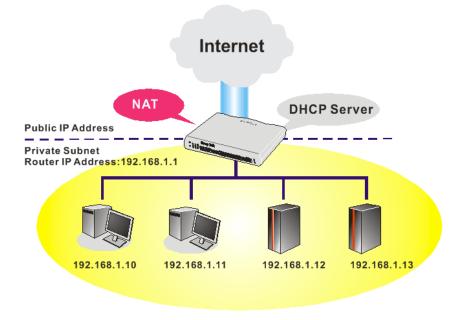
### 3.2 LAN

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.

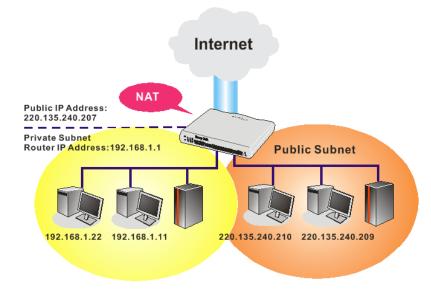
W M/HUN
LAN
General Setup
Static Route
VLAN
Bind IP to MAC
LAN Port Mirror
Web Portal Setup
NAT

### 3.2.1 Basics of LAN

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 public IP address to private 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. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



### What is Routing Information Protocol (RIP)

Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### What is Static Route

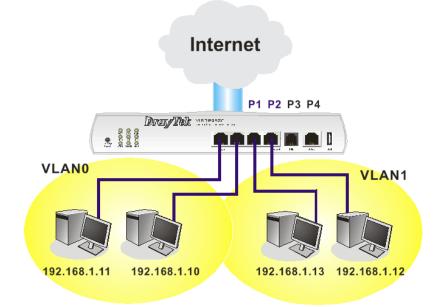
When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to



forward data from one specified subnet to another specified subnet without the presence of RIP.

### What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



# 3.2.2 General Setup

This page provides you the general settings for LAN. Click **LAN** to open the LAN settings page and choose **General Setup**.

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN6). In addition, different subnets can link for each other by configuring **Inter-LAN Routing**. At present, LAN1 setting is fixed with NAT mode only. LAN2 – LAN6 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup				
Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page IPv6
LAN 2		<b>V</b>	192.168.2.1	Details Page
LAN 3		<b>V</b>	192.168.3.1	Details Page
LAN 4		$\checkmark$	192.168.4.1	Details Page
LAN 5		<b>V</b>	192.168.5.1	Details Page
LAN 6		$\checkmark$	192.168.6.1	Details Page
IP Routed Subnet			192.168.0.1	Details Page

Advanced You can configure DHCP options here.

Inter-LAN Routing						
Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6
LAN 1	<b>V</b>					
LAN 2		$\checkmark$				
LAN 3			<b>V</b>			
LAN 4				<b>V</b>		
LAN 5					<b>V</b>	
LAN 6						$\checkmark$

Note: LAN 2/3/4/5/6 are available when VLAN is enabled.



Item	Description
General Setup	Allow to configure settings for each subnet respectively.
	Index - Display all of the LAN items.
	<b>Status-</b> Basically, LAN1 status is enabled in default. LAN2 –LAN6 and IP Routed Subnet can be observed by checking the box of <b>Status</b> .
	<b>DHCP-</b> LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.
	<b>IP Address -</b> Display the IP address for each LAN item. Such information is set in default and you can not modify it.
	<b>Details Page -</b> Click it to access into the setting page. Each LAN will have different LAN configuration page. <b>Each LAN must be configured in different subnet.</b>



	<b>IPv6</b> – Click it to access into the settings page of IPv6.
Advanced	DHCP packets can be processed by adding option number and data information when such function is enabled.
	DHCP Options Status
	C Enable O Disable
	Options List Index Option Number Ascii/Hex Data
	Option Number: DataType: <sup>(</sup> ) Ascii <sup>(</sup> ) Hex (Example of Hex Data Type Input Format:0xff 0x00 0xc0 0xa8) Data: Add Delete Note: Maximum number of custom DHCP option is five.
	Enable/Disable – Enable/Disable the function of DHCP
	Option. Each DHCP option is composed by an option number with data. For example,
	Option number: 100
	Data: abcd
	When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.
	<b>Option Number</b> – Type a number for such function.
	<b>DataType</b> – Choose the type (ASCII or Hex) for the data to be stored.
	<b>Data</b> – Type the content of the data to be processed by the function of DHCP option.
Inter-LAN Routing	Check the box to link two or more different subnets (LAN and LAN).

When you finish the configuration, please click  $\mathbf{OK}$  to save and exit this page.

# Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information.

LAN 1 Ethernet TCP / IP	and DHCP Setup	LAN 1 IPv6 Setup	
Network Configuration		DHCP Server Configuration	on
For NAT Usage		Senable Server ○ Disa	able Server
IP Address	192.168.1.1	Enable Relay Agent	
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
		IP Pool Counts	150
RIP Protocol Control	Disable 🚩	Gateway IP Address	192.168.1.1
		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	
		Force router to use	address for DNS

#### LAN >> General Setup

Item	Description
Network Configuration	For NAT Usage,
	<b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask -</b> Type in an address code that determines the size of the network. (Default: 255.255.255.0/24)
	RIP Protocol Control,
	<b>Disable -</b> deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	<b>Enable</b> – activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.
	<b>Enable Relay Agent</b> –Specify which subnet that DHCP server is located the relay agent should redirect the DHCP



	request to.
	<b>DHCP Server IP Address</b> – It is available when <b>Enable</b> <b>Relay Agent</b> is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	<b>Primary IP Address -</b> You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
	Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
	The default DNS Server IP address can be found via Online Status: Online Status
	Physical Connection         System Uptime: 22:22:45           IPv4         IPv6           LAN Status         Primary DNS: 8.8.8.8         Secondary DNS: 8.8.4.4           IP Address         TX Packets         RX Packets           192.168.1.1         0         41533
	If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
	If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.
	<b>Force router to use address for DNS-</b> Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP of DHCP server).

When you finish the configuration, please click **OK** to save and exit this page.

### Details Page for LAN1 – IPv6 Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
RADVD Configuration	
Enable     O Disable	
Advertisement Lifetime 1800 Seconds (	(Range : 600 - 9000)
DHCPv6 Server Configuration	
Enable Server     O Disable Server	
Start IPv6 Address	
End IPv6 Address	
DNS Server IPv6 Address	
Primary DNS Server	
Secondary DNS Server	
Static IPv6 Address configuration IPv6 Address Current IPv6 Address Table	/ Prefix Length / Add Delete
Index IPv6 Address/Prefix Length	Scope
1 FEBO::21D:AAFF:FEA8:B768/64	Link

It provides 2 daemons for LAN side IPv6 address configuration. One is **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

Item	Description
RADVD Configuration	<b>Enable</b> – Click it to enable RADVD server. The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.
	<b>Disable</b> – Click it to disable RADVD server.
	Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to



	18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
DHCPv6 Server Configuration	<b>Enable Server</b> –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.
	<b>Disable Server</b> – Click it to disable DHCPv6 server.
	<b>Start IPv6 Address</b> / <b>End IPv6 Address</b> – Type the start and end address for IPv6 server.
DNS Server IPv6 Address	<b>Primary DNS Sever</b> – Type the IPv6 address for Primary DNS server.
	<b>Secondary DNS Server</b> –Type another IPv6 address for DNS server if required.
Static IPv6 Address	<b>IPv6 Address</b> – Type static IPv6 address for LAN.
configuration	<b>Prefix Length</b> – Type the fixed value for prefix length.
	Add – Click it to add a new entry.
	<b>Delete</b> – Click it to remove an existed entry.
Current IPv6 Address Table	Display current used IPv6 addresses.

When you finish the configuration, please click **OK** to save and exit this page.

# Details Page for LAN2 ~ LAN6

LAN >> General Setup

Network Configuration		DHCP Server Configurat	ion
O Enable O Disable		● Enable Server ○ Dis	able Server
● For NAT Usage	○ For Routing Usage	Enable Relay Agent	
IP Address	192.168.2.1	Start IP Address	192.168.2.10
Subnet Mask	255.255.255.0	IP Pool Counts	100
		Gateway IP Address	192.168.2.1

Item	Description
Network Configuration	<b>Enable/Disable -</b> Click <b>Enable</b> to enable such configuration; click <b>Disable</b> to disable such configuration.
	<b>For NAT Usage -</b> Click this radio button to invoke NAT function.
	<b>For Routing Usage -</b> Click this radio button to invoke this function.
	<b>IP</b> Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask -</b> Type in an address code that determines the size of the network. (Default: 255.255.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.
	<b>Enable Relay Agent</b> - If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>DHCP Server IP Address</b> – It is available when <b>Enable Relay Agent</b> is checked. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.



<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

When you finish the configuration, please click **OK** to save and exit this page.

# **Details Page for IP Routed Subnet**

LAN >> General Setup

TCP/IP and DHCP Setup f	or IP Routed Subnet	
Network Configuration		DHCP Server Configuration
© Enable	192.168.0.1	Start IP Address     IP Pool Counts     0     Use LAN Port   P1  P2
Subnet Mask	255.255.255.0	Use MAC Address
RIP Protocol Control	Disable 💌	Index Matched MAC Address given IP Address
		MAC Address : : : : : : : : : : : : : : : : : :
		ок

Item	Description
Network Configuration	<b>Enable/Disable -</b> Click <b>Enable</b> to enable such configuration; click <b>Disable</b> to disable such configuration.
	For Routing Usage,
	<b>IP Address -</b> Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask -</b> Type in an address code that determines the size of the network. (Default: 255.255.25.0/24)
	RIP Protocol Control,
	<b>Disable -</b> deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	<b>Enable</b> – activate the RIP protocol.

DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network. If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Use LAN Port</b> – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.
	Use MAC Address - Check such box to specify MAC address.
	<b>MAC Address:</b> Enter the MAC Address of the host one by one and click <b>Add</b> to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2 <sup>nd</sup> DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2 <sup>nd</sup> subnet won't get an IP address belonging to 1 <sup>st</sup> subnet.
	Add – Type the MAC address in the boxes and click this button to add.
	<b>Delete</b> – Click it to delete the selected MAC address.
	Edit – Click it to edit the selected MAC address.
	<b>Cancel</b> – Click it to cancel the job of adding, deleting and editing.

When you finish the configuration, please click **OK** to save and exit this page.

### 3.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

### Static Route for IPv4

LAN >> Static Route Setup

IPv4		IPv6		Set	to Factory Default	View Routing Tal	ble
Index	Destina	ation Address	Status	Index	Destination Ad	dress Stat	us
<u>1.</u>		???	?	<u>6.</u>	???	?	
<u>2.</u>		???	?	<u>7.</u>	???	?	
<u>3.</u>		???	?	<u>8.</u>	???	?	
<u>4.</u>		???	?	<u>9.</u>	???	?	
<u>5.</u>		???	?	<u>10.</u>	???	?	

Status: v --- Active, x --- Inactive, ? --- Empty

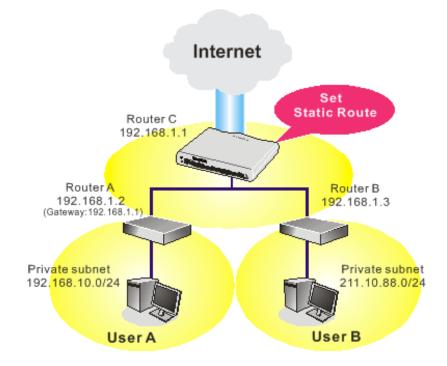
Item	Description	
Index	The number (1 to 10) under Index allows you to open next page to set up static route.	
<b>Destination Address</b>	Displays the destination address of the static route.	
Status	Displays the status of the static route.	
Set to Factory Default	Clear all of the settings and return to factory default settings.	
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table          Current Running Routing Table       IPv6 Routing Table       Refresh         Rey: C - connected, S - static, R - RIP, * - default, ~ - private       C~         C- 192.168.1.0/ 255.255.255.0       directly connected       LRN1	

### Add Static Routes to Private and Public Networks

Here is an example (based on IPv4) of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



1. Go to LAN page and click General Setup, select 1st Subnet as the RIP Protocol Control. Then click the OK button.

**Note:** There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

# **Dray** Tek

2. Click the LAN >> Static Route and click on the Index Number 1. Check the Enable box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click OK.

Enable		
	Destination IP Address	192.168.1.10
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN1 😽

LAN >> Static Route Setup

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.
Destination IP Address	Type an IP address as the destination of such static route.
Subnet Mask	Type the subnet mask for such static route.
Network Interface	Use the drop down list to specify an interface for such static route.

3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3. Click **OK**.

<ul> <li>Enable</li> </ul>		
	Destination IP Address	211.100.88.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.3
	Network Interface	LAN1 🔽

LAN >> Static Route Setup

4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
C~ 192.168.1.0/ 255.255.255.	- RIP, * - default, ~ - private 0 via 192.168.1.2 LAN1 0 directly connected LAN1 0 via 192.168.1.3 LAN1	

### Static Route for IPv6

You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:

LAN >> Static Route Setup

IPv4	IPv6		Set to Fa	ctory Default   View IPv6 Ro	uting Table
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	::/0	х	<u>11.</u>	::/0	х
<u>2.</u>	::/0	х	<u>12.</u>	::/0	x
<u>3.</u>	::/0	х	<u>13.</u>	::/0	х
<u>4.</u>	::/0	х	<u>14.</u>	::/0	x
<u>5.</u>	::/0	х	<u>15.</u>	::/0	х
<u>6.</u>	::/0	х	<u>16.</u>	::/0	x
<u>7.</u>	::/0	х	<u>17.</u>	::/0	x
<u>8.</u>	::/0	х	<u>18.</u>	::/0	x
<u>9.</u>	::/0	х	<u>19.</u>	::/0	х
<u>10.</u>	::/0	х	<u>20.</u>	::/0	х
<< 1 - 20   21	<u>- 40</u> >>				<u>Next</u> >>

<< <u>1 - 20</u> | <u>21 - 40</u> >>

Status: v --- Active, x --- Inactive, ? --- Empty

Available settings are explained as follows:

Item	Description
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.

Click any underline of index number to get the following page.

#### LAN >> Static Route Setup

Enable	
Destination IPv6 Address / Prefix Len	:: / 0
Gateway IPv6 Address	
Network Interface	LAN 🗸

Available settings are explained as follows:

Item	Description			
Enable	Click it to enable this profile.			
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.			
Gateway IPv6 Address	Type the gateway address for this entry.			
Network Interface	Use the drop down list to specify an interface for this static route. LAN V VAN1 WAN2 WAN3			

When you finish the configuration, please click **OK** to save and exit this page.

**Dray** Tek

### 3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to LAN page and select VLAN. The following page will appear. Click **Enable** to invoke VLAN function.

VLAN Configur	ation									
🗹 Enable										
		VLAN Tag				LA	AN .			
	Enable	VID	Priority	P1	P2	P3	P4	P5	P6	Subnet
VLAN0		0	0 🕶							LAN 1 💌
VLAN1	<b>~</b>	10	0 🛰		<b>~</b>					LAN 2 💌
VLAN2	<b>V</b>	20	0 🛰			<b>V</b>				LAN 3 💌
VLAN3	<b>~</b>	30	0 🛰				<b>~</b>			LAN 4 💌
VLAN4	<b>V</b>	40	0 🛰					<b>V</b>		LAN 5 💌
VLAN5		0	0 🛰						<b>~</b>	LAN 6 💌
VLAN6		0	0 🛰							LAN 1 💌
VLAN7		0	0 🛰							LAN 1 💌

#### LAN >> VLAN Configuration

Enable management port for P1

1. Tag based VLAN only applied for LAN Ports;

2. The set VLAN ID (VID) must be unique and not duplicate.

OK Clear Cancel

Note: Settings in this page only applied to LAN port but not WAN port.

Available settings are explained as follows:	
----------------------------------------------	--

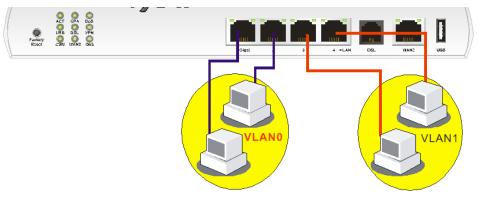
Item	Description				
Enable	Click it to enable VLAN configuration.				
VLAN Tag	<b>Enable</b> – Check the box to enable the function of VLAN with tag.				
	The router will add specific VLAN number to all packets on the LAN while sending them out.				
	Please type the tag value and specify the priority for the packets sending by LAN.				
	<b>VID</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.				
	<b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.				
LAN	P1 - P6 – Check the LAN port(s) to be grouped under the selected VLAN.				

Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet. Subnet LAN 1 V LAN 1 LAN 2 LAN 3 LAN 4 LAN 5 LAN 6 LAN 5 V
Enable management port for P1	It can help users to communicate with the router still even though configuring wrong VLAN tag setting. For Vigor router has one LAN physical port only, it is recommended to enable the management port (LAN 1) to ensure the data transmission is unimpeded.

**Note:** Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error.

To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4. VLAN0 and VLAN1 are configured with different subnets.



2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below. Click **OK** to save the settings.

**Dray** Tek

#### LAN >> VLAN Configuration

Enable										
		VLAN Tag				L	AN			
	Enable	VID	Priority	P1	P2	P3	P4	P5	P6	Subnet
VLAN0		0	0 🛩	✓						LAN 1 🛩
VLAN1	<b>~</b>	10	0 🗸		<b>~</b>					LAN 2 🔽
VLAN2	<ul><li>✓</li></ul>	20	0 🗸			<b>~</b>				LAN 3 🔽
VLAN3	<b>~</b>	30	0 🗸				<b>~</b>			LAN 4 🔽
VLAN4	<ul><li>✓</li></ul>	40	0 🗸					<b>~</b>		LAN 5 🔽
VLAN5		0	0 🗸						<b>~</b>	LAN 6 💌
VLAN6		0	0 🛩							LAN 1 💌
VLAN7		0	0 🗸							LAN 1 💌

To remove VLAN, uncheck the needed box and click **OK** to save the results.

# 3.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening 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.

Click LAN and click Bind IP to MAC to open the setup page.

LAN >> Bind IP to MAC

Bind IP to MAC		
○ Enable		
ARP Table   <u>Select All</u>   <u>Sort</u>   <u>Refresh</u>	IP Bind List	Select All   Sort
IF Address Mac Address 192.168.1.49 E0-CB-4E-DA-48-79	Index IP Address	Mac Address
Add and Edit		
IP Address		
Mac Address		
Comment		Show Comment
Add	Edit Delete	

#### Note: IP-MAC binding presets DHCP Allocations.

If you select Strict Bind, unspecified LAN clients cannot access the Internet.

OK



Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in 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 <b>Add</b> below.
Select All	Click this link to select all the items in the ARP table.
Sort	Reorder the table based on the IP address.
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add and Edit	<ul> <li>IP Address - Type the IP address that will be used for the specified MAC address.</li> <li>Mac Address - Type the MAC address that is used to bind with the assigned IP address.</li> <li>Comment - Type a brief description for the entry.</li> </ul>
	<b>Show Comment</b> – Check this box to display the comment on IP Bind List box.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Delete</b> . The selected item will be removed from the <b>IP Bind List</b> .

Available settings are explained as follows:

**Note:** Before you select **Strict Bind**, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web user interface of the router might not be accessed.

When you finish the configuration, click **OK** to save the settings.

### 3.2.6 LAN Port Mirror

LAN port mirror can be applied for the users in LAN. Generally speaking, this function copies traffic from one or more specific ports to a target port. 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. First, it is more economical without other detecting equipments to be set up. Second, it may be able to view traffic on one or more ports within a VLAN at the same time. Third, 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.

LAN >> LAN Port Mirror

LAN Port Mir	ror				
Port Mirror:					
O Enable (	Disable				
Mirror port:					
OP2	O P3	○ P4	O P5	O P6	
Mirrored po	rt:				
□P1	<b>P2</b>	<b>P</b> 3	<b>P</b> 4	<b>P5</b>	P6
1					
			OK		

Available settings are explained as follows:

Item	Description
Port Mirror	Check <b>Enable</b> to activate this function. Or, check <b>Disable</b> to close this function.
Mirror Port	Select a port to view traffic sent from mirrored ports.
Mirrored port	Select which ports are necessary to be mirrored.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.2.7 Web Portal Setup

This page allows you to configure a profile with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router. No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal.

#### LAN >> Web Portal Setup

Web Portal Ta	ble:		
Profile	Status	Interface	
<u>1.</u>	Disable	None	Preview
<u>2.</u>	Disable	None	Preview
<u>3.</u>	Disable	None	Preview
<u>4.</u>	Disable	None	Preview

Each item is explained as follows:

Item	Description
Profile	Display the number link which allows you to configure the profile.
Status	Display the content (Disable, URL Redirect or Message) of the profile.
Interface	Display the applied interfaced of the profile.
Preview	Open a preview window according to the configured settings.

To configure the profile, click any index number link to open the following page.

```
LAN >> Web Portal Setup
```

#### Profile Index: 1

URL Redirect	http://	
	e.g. http://www.draytek.com Note : If the User Management application is enabled, it will override the Web Portal settings seen here.	
○ Message	<h1><font color="red">Vigor</font></h1> <h2> - Reliable connectivity</h2> <h2> - Robust firewall protection</h2> <h2> - Multi-site secure communication</h2>	~
		~
	(Max 255 characters)	
Applied Interfaces	SSID1 SSID2 SSID3 SSID4	



Available settings	are explained	l as follows:

Item	Description
Disable	Click this button to close this function.
URL Redirect	Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit.
Message	Type words or sentences here. The message will be displayed on the screen for several seconds when the wireless users access into the web page through the router.
Applied Interfaces	<ul><li>Check the box(es) representing different interfaces to be applied by such profile.</li><li>The advantage is that each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.</li></ul>

After finishing all the settings here, please click **OK** to save the configuration.

# 3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

**Note:** On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

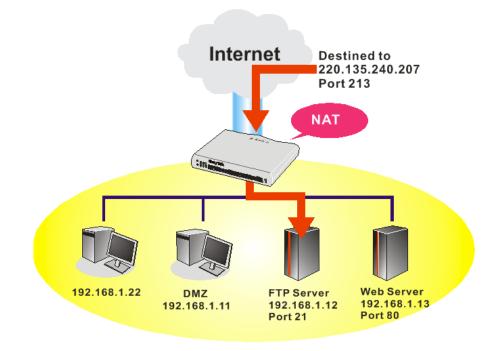
Below shows the menu items for NAT.



**Dray** Tek

### 3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.

NAT >> Port Redirection

	-			actory Default
Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				х
<u>2.</u>				x
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				х
<u>10.</u>				x

Press any number under Index to access into next page for configuring port redirection.



Index No. 1	
Enable	
Mode	Range 💌
Service Name	Single Range
Protocol	💙
WAN IP	1.All 💌
Public Port	0 -
Private IP	-
Private Port	0

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

OK	Clear	Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select <b>Range</b> . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is <b>All</b> which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified <b>Private IP and Port</b> of the internal host. If you choose <b>Range</b> as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
Private IP	Specify the private IP address of the internal host providing the service. If you choose <b>Range</b> as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.

After finishing all the settings here, please click **OK** to save the configuration.



Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web user interface in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance** >>**Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

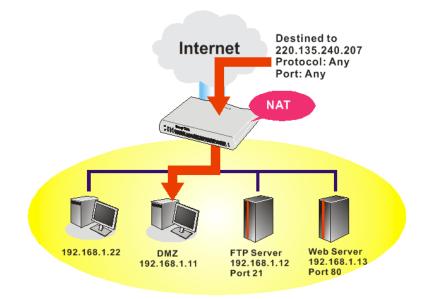
anagement Port Setup ) User Define Ports O Default Ports elnet Port 23 (Default: 23)		
Inet Port 23 (Default: 22)		
(Default, 25)		
TP Port 80 (Default: 80)		
TPS Port 443 (Default: 443)		
P Port 21 (Default: 21)		
SH Port 22 (Default: 22)		
SNMP Setup		
Enable SNMP Agent		
Get Community public		
Set Community private		
Manager Host IP		
Frap Community public		
Notification Host IP		
Trap Timeout 10 seconds		

System Maintenance >> Management

### 3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.





The security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.

WAN1	WAN2	WAN3
AN 1		
None 💌		
Private IP		Choose PC
MAC Address of the True IP [	DMZ Host 00 . 00 . 00 . 00	0.00.00
Note: When a True-IP DMZ always on.	host is turned on, it will force the ro	outer's WAN connection to be

Available settings are explained as follows:

NAT >> DMZ Host Setup

Item	Description	
WAN 1 None Private IP Active True IP h∈	Choose <b>Private IP</b> or <b>Active True IP</b> first. <b>Active True IP</b> selection is available for WAN1 only.	
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.	
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.	

the IP address will be <b>OK</b> to save the setting	shown on the fol	
DMZ Host Setup WAN1	WAN2	WAN3
	192.168.1.49 00 0 00 00 00 00 00 00 00 00 00 00 00 0	Choose PC 00 . 00
	Image: 192.168.1.10         192.168.1.10         192.168.1.18         Image: 192.168.1.18         Image: 192.168.1.18         When you have select         the IP address will be         OK to save the setting         NAT >> DMZ Host Setup         DMZ Host Setup         Image: 10 mm         WAN1         Private IP         MAC Address of the True IP DMZ Host Set         Note: When a True-IP DMZ host i	Image: 192.168.1.10         192.168.1.18         Image: 192.168.1.18

DMZ Host for WAN2 and WAN3 is slightly different with WAN1. Active True IP selection is available for WAN1 only.

See the following figure.

NAT >> DMZ Host Setup

DMZ Host Setup							
WAN1	WAN2	WAN3					
WAN 2							
Enable	Private IP						
	0.0.0	Choose PC					
	ОК						

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2 interface, you will find them in **Aux. WAN IP** for your selection.

NAT >> DMZ Host Setup

	WAN1		WAN2	WAN3
WAN 2 Index	Enable	Aux. WAN IP	Private IP	
1.			0.0.0.0	Choose PC
2.	<b>~</b>	192.168.1.45	0.0.0.0	Choose PC

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. Image: http://19Image: http://19.Image: http://10.Image: http:/

After finishing all the settings here, please click **OK** to save the configuration.



# 3.3.3 Open Ports

**Open Ports** allows you to open a range of ports for the traffic of special applications.

Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:

NAT >> Open Ports

Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>				х
<u>2.</u>				х
<u>3.</u>				x
<u>4.</u>				x
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				х
<u>10.</u>				х

Available settings are explained as follows:

Item	Description	
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.	
Comment	Specify the name for the defined network service.	
WAN Interface	Display the WAN interface used by such index.	
Local IP Address	Display the private IP address of the local host offering the service.	
Status	Display the state for the corresponding entry. X or V is to represent the <b>Inactive</b> or <b>Active</b> state.	

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



### NAT >> Open Ports >> Edit Open Ports

#### Index No. 1

Enable Open Ports								
	Co	omment	P2261					
	W	AN Interface	WAN	· · ·				
	Lo	cal Computer	192.16	8.1.49	Choose	PC		
	Protocol	Start Port	End Port	Pro	tocol	Start Port	End Port	
1.	TCP	80	80	2	*	0	0	
3.	`	0	0	4	*	0	0	
5.	•	0	0	6	*	0	0	
7.	``	0	0	8	*	0	0	
9.		0	0	10	*	0	0	

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
Local Computer	Enter the private IP address of the local host or click <b>Choose PC</b> to select one.
	<b>Choose PC -</b> Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be <b>TCP</b> , <b>UDP</b> , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

After finishing all the settings here, please click **OK** to save the configuration.

NAT >> Open Ports

en Ports Setup Set to				
Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>	P2261	WAN1	192.168.1.49	v
<u>2.</u>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
7.				x

# 3.3.4 Address Mapping

Address Mapping is used to map a specified private IP or a range of private IPs of NAT subnet into a specified WAN IP (or WAN IP alias IP). Refer to the following figure.



Suppose the WAN settings for a router are configured as follows:

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11 WAN2: 203.98.200.10

Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host1 to always map to 202.211.100.10 (WAN1); Host2 to always map to 202.211.100.11 (WAN1 alias); Host3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

Address Map	ping Setup	Set to Facto	ory Default		
Index	Protocol	Public IP	Private IP	Mask	Status
<u>1.</u>	ALL			/32	х
<u>2.</u>	ALL			/32	х
<u>3.</u>	ALL			/32	х
<u>4.</u>	ALL			/32	х
<u>5.</u>	ALL			/32	х
<u>6.</u>	ALL			/32	х
<u>7.</u>	ALL			/32	х
<u>8.</u>	ALL			/32	х
<u>9.</u>	ALL			/32	х
<u>10.</u>	ALL			/32	x

Available settings are explained as follows:

Item	Description
Protocol	Display the protocol used for this address mapping.
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10.
Mask	Display the subnet mask selected for this address mapping.
Status	Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1	
🗹 Enable	
Protocol:	ALL 💌
WAN Interface	WAN1 🗸
WAN IP	▼
Private IP:	
Subnet Mask:	/32 💌
	OK Clear Cancel

Item	Description
Enable	Check to enable this entry.
Protocol	Specify the transport layer protocol. It could be <b>TCP</b> , <b>UDP</b> , or <b>ALL</b> for selection.

	ALL V ALL TCP UDP
WAN Interface	Choose the WAN interface for such address mapping profile.
WAN IP	Select an IP address (the selections provided here are set in <b>IP Alias List</b> of <b>Network &gt;&gt;WAN</b> interface). Local host can use this IP to connect to Internet.
	If you want to choose any one of the Public IP settings, you must specify some IP addresses in the IP Alias List of the Static/DHCP Configuration page first. If you did not type in any IP address in the IP Alias List, the Public IP setting will be empty in this field. When you click <b>Apply</b> , a message will appear to inform you.
Private IP	Assign an IP address (e.g., 192.168.1.10) or a subnet to be compared with the Public IP address for incoming packets.
Subnet Mask	Select a value of subnet mask for private IP address.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.3.5 Port Triggering

Port Triggering is a variation of open ports function.

The key difference between "open port" and "port triggering" is:

- Once the OK button is clicked and the configuration has taken effect, "open port" keeps the ports opened forever.
- Once the OK button is clicked and the configuration has taken effect, "port triggering" will only attempt to open the ports once the triggering conditions are met.
- The duration that these ports are opened depends on the type of protocol used. The "default" durations are shown below and these duration values can be modified via telnet commands.

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

#### NAT >> Port Triggering

Port Trig	gering				Set to Factory	Default
Index	Comment	<b>Triggering Protocol</b>	<b>Triggering Port</b>	<b>Incoming Protocol</b>	Incoming Port	Status
<u>1.</u>						х
<u>2.</u>						х
<u>3.</u>						х
<u>4.</u>						х
<u>5.</u>						х
<u>6.</u>						х
<u>7.</u>						х
<u>8.</u>						х
<u>9.</u>						x
<u>10.</u>						x
<< <u>1-10</u>	<u>11-20</u> >>					Next >>

Available settings are explained as follows:

Item	Description	
Comment	Display the text which memorizes the application of this rule.	
<b>Triggering Protocol</b>	Display the protocol of the triggering packets.	
<b>Triggering Port</b>	Display the port of the triggering packets.	
Incoming Protocol	Display the protocol for the incoming data of such triggering profile.	
Incoming Port	Display the port for the incoming data of such triggering profile.	
Status	Display if the rule is active or de-active.	

Click the index number link to open the configuration page.

NAT	>>	Port	Triggerin	g
-----	----	------	-----------	---

No. 1	
🗹 Enable	
Service	User Defined 💌
Comment	
Triggering Protocol	TCP 🗸
Triggering Port	80
Incoming Protocol	UDP 🗸
Incoming Port	1024
Note: The Triggering Port and Incoming Port 123-456,777-789 (legal),123-456,789 (legal)	
OK Cle	ar Cancel

**Dray** Tek

Item	Description	
Enable	Check to enable this entry.	
Service	Choose the <b>predefined</b> service to apply for such trigger profile. User Defined Wer Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent	
Comment	Type the text to memorize the application of this rule.	
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.	
Triggering Port	Type the port or port range for such triggering profile.	
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.	
Incoming Port	Type the port or port range for the incoming packets.	

Available settings are explained as follows:

After finishing all the settings here, please click **OK** to save the configuration.

# 3.4 Firewall

## 3.4.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

#### **Firewall Facilities**

The users on the LAN are provided with secured protection by the following firewall facilities:

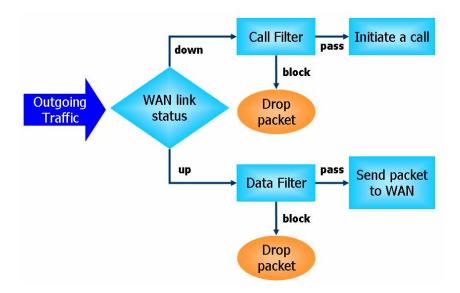
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

#### **IP Filters**

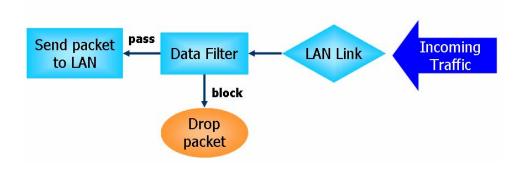
Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.



**Dray** Tek



#### **Stateful Packet Inspection (SPI)**

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

#### **Denial of Service (DoS) Defense**

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

- 1. SYN flood attack
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. Port Scan attack
- 5. IP options
- 6. Land attack
- 7. Smurf attack
- 8. Trace route

- 9. SYN fragment
- 10. Fraggle attack
- 11. TCP flag scan
- 12. Tear drop attack
- 13. Ping of Death attack
- 14. ICMP fragment
- 15. Unknown protocol

Below shows the menu items for Firewall.

Firewall General Setup Filter Setup DoS Defense

#### 3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.

#### **General Setup Page**

Such page allows you to enable / disable Call Filter and Data Filter, determine general rule for filtering the incoming and outgoing data.

Firewall	>>	General	Setup
		00110101	ootap

ieneral Setup	Default Rule	
Call Filter	Enable	Start Filter Set Set#1 💌
	🔘 Disable	
Data Filter	<ul> <li>Enable</li> </ul>	Start Filter Set Set#2 💌
	🔘 Disable	
	ge incoming fragmented ct Security Firewall	UDP or ICMP packets ( for some games, ex. CS )

Item	Description
Call Filter	Check <b>Enable</b> to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check <b>Enable</b> to activate the Data Filter function. Assign a start filter set for the Data Filter.
Accept large incoming	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".

Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission.
	Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.

# **Default Rule Page**

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

Firewall >> General Setup

General Setup		-		
Actions for defa	ault rule:			
Application		Action/Profile	Syslog	
Filter		Pass 💌		
Sessions Contr	ol	0 / 60000		
Quality of Serv	ice	None 💌		
Load-Balance	policy	Auto-Select 🐱		
<u>User Management</u>		None 💌		
APP Enforceme	ent	None 💌		
URL Content Fi	lter	None 💌		
Web Content F	ilter	None 💌		
Advance Setti	ng	Edit		

Item	Description
Filter	Select <b>Pass</b> or <b>Block</b> for the packets that do not match with the filter rules.
	Filter Pass V Pass Block
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default
Load-Balance Policy	Choose the WAN interface for applying Load-Balance Policy. Auto-Select WAN1 WAN2 WAN3
User Management	Such item is available only when <b>Rule-Based</b> is selected in User <b>Management&gt;&gt;General Setup</b> . The general firewall rule will be applied to the user/user group/all users specified here. None User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile existed, <b>Create New User</b> or <b>Create New Group</b> item will appear for you to click to create a new one.

APP Enforcement	Select an <b>APP Enforcement</b> profile for global IM/P2P application blocking. If there is no profile for you to select, please choose <b>[Create New]</b> from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the <b>APP Enforcement</b> profile selected here. For detailed information, refer to the section of <b>APP Enforcement</b> profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
URL Content Filter	<ul> <li>Select one of the URL Content Filter profile settings</li> <li>(created in CSM&gt;&gt; URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM&gt;&gt; URL Content Filter web page first. Or choose</li> <li>[Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</li> </ul>
Web Content Filter	Select one of the <b>Web Content Filter</b> profile settings (created in <b>CSM&gt;&gt; Web Content Filter</b> ) for applying with this router. Please set at least one profile for anti-virus in <b>CSM&gt;&gt; Web Content Filter</b> web page first. Or choose [ <b>Create New</b> ] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for <b>Web Content Filter</b> by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.

Advance Setting	Click <b>Edit</b> to open the following window. However, it is <b>strongly recommended</b> to use the default settings here. Firewall >> General Setup		
	Advance Setting		
	Codepage	ANSI(1252)-Latin	<b>~</b>
	Window size:	65535	
	Session timeout:	1440	Minute
	<b>Codepage</b> - This fun among different lang help the system obtai	uages. Choose con ining correct ASCI	rect codepage can I after decoding d
	from URL and enhan Filter. The default va I. If you do not choos URL will be processe choose a codepage.	lue for this setting se any codepage, n	is ANSI 1252 Lation decoding job of
	If you do not have an please open Syslog. I dialog, you will see t the dialog box.	From Codepage In	formation of Setur
	💓 DrayTek Syslog 3.9.1		
	Controls	192.168.1.1 Vigor series RX Packets	WAN Information WAN1 IP (Fix 172.16.2.21 WAN2 IP (Fix
	28489	15285	
	Setup		
	Tool Setup   Telnet Read-or	ut Setup Codepage Informatio	on
	Codepage To Select		•
	Windows Version: 5.0 RECOMMENDED CC 950 (ANSI/OEM - Tr 00a1:21 00a6:7c 00a9		052:32 0053:33 0059:31 0054
	Window size – It det (0~65535). The more performance will be.	e the value is, the b However, if the ne	etter the
	small value will be p	-	
	<b>Session timeout</b> $-$ Set the best utilization of	0	

After finishing all the settings here, please click  $\mathbf{O}\mathbf{K}$  to save the configuration.

## 3.4.3 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.

Firewall >> Filter Setup

Filter Setup Set to Factor				
Set	Comments	Set	Comments	
<u>1.</u>	Default Call Filter	<u>7.</u>		
<u>2.</u>	Default Data Filter	<u>8.</u>		
<u>3.</u>		<u>9.</u>		
<u>4.</u>		<u>10.</u>		
<u>5.</u>		<u>11.</u>		
<u>6.</u>		<u>12.</u>		

To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1					
Comments : De	afault Call Filter				
Filter Rule	Active	Comments		Move Up	Move Down
1		Block NetBios			<u>Down</u>
2				UP	<u>Down</u>
3				<u>UP</u>	<u>Down</u>
4				UP	<u>Down</u>
5				UP	<u>Down</u>
6				UP	<u>Down</u>
7				<u>UP</u>	
-				Next Filter	Set None 🛩
		OK Clear	Cancel		

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered $(1 \sim 7)$ to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Move Up/Down	Use <b>Up</b> or <b>Down</b> link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

To edit Filter Rule, click the Filter Rule index button to enter the Filter Rule setup page.



Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule OI	N: 🗌 Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to any	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter:	Pass Immediately	
Branch to Other Filter Set:	None 😪	
Sessions Control	0 / 60000	
MAC Bind IP	Non-Strict 💌	
Quality of Service	None 💌	
Load-Balance policy	Auto-Select 💌	
<u>User Management</u>	None 🗸	
APP Enforcement:	None 🖌	
URL Content Filter:	None 🗸	
Web Content Filter:	None 🔽	
Advance Setting	Edit	

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for <b>Data Filter</b> only. For the <b>Call Filter</b> , this setting is not available since <b>Call Filter</b> is only applied to outgoing traffic.

Source/Destination IP	LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN Note: RT means routing domain for 2nd subnet or other LAN. Click Edit to access into the following dialog to choose the
	source/destination IP or IP ranges.
	Address Edit Address Type Any Address
	Start IP Address       0.0.0         End IP Address       0.0.0         Subnet Mask       0.0.0         Invert Selection       Invert Selection         IP Group       None V         or IP Object       None V         or IP Sobject       None V
	OK Close
	To set the IP address manually, please choose <b>Any</b> <b>Address/Single Address/Range Address/Subnet Address</b> as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose <b>Group and Objects</b> as the Address Type. Group and Objects
	Any Address Single Address Range Address Subnet Address Group and Objects From the <b>IP Group</b> drop down list, choose the one that you
	want to apply. Or use the <b>IP Object</b> drop down list to choose the object that you want.
Service Type	Click <b>Edit</b> to access into the following dialog to choose a suitable service type.

	C Service Type Edit - Windows Internet Explorer
	http://192.168.1.1/doc/ipfstedt.htm
	Service Type Edit
	Service Type User defined 💌
	Protocol TCP/UDP V Source Port = V 137 ~139
	Destination Port = V 1 ~65535
	or <u>Service Object</u> None
	or Service Object None
	or Service Object None
	OK Close
	To get the service type menually, places above Ugan
	To set the service type manually, please choose <b>User</b> <b>defined</b> as the Service Type and type them in this dialog. In
	addition, if you want to use the service type from defined
	groups or objects, please choose Group and Objects as the
	Service Type.
	User defined 🗸
	User defined
	Group and Objects
	<b>Protocol -</b> Specify the protocol(s) which this filter rule will
	apply to.
	Source/Destination Port –
	(=) – when the first and last value are the same, it indicates
	one port; when the first and last values are different, it
	indicates a range for the port and available for this service type.
	(!=) – when the first and last value are the same, it
	indicates all the ports except the port defined here;
	when the first and last values are different, it indicates that
	all the ports except the range defined here are available for this service type.
	(>) – the port number greater than this value is available.
	(<) – the port number less than this value is available for
	this profile.
	<b>Service Group/Object</b> - Use the drop down list to choose the and that you must
	the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for <b>Data Filter</b> only.
	Don't care - No action will be taken towards fragmented
	packets.
	<b>Unfragmented</b> - Apply the rule to unfragmented packets.
	<i>Fragmented</i> - Apply the rule to fragmented packets.
	<i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule.
	Block Immediately - Packets matching the rule will be
	dropped immediately.
	<b>Pass Immediately -</b> Packets matching the rule will be

	nessed immediately
	<ul> <li>passed immediately.</li> <li>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</li> <li>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</li> </ul>
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.
MAC Bind IP	<ul> <li>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP be bound for applying such filter rule.</li> <li>No-Strict - no limitation.</li> </ul>
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default
Load-Balance policy	Choose the WAN interface for applying Load-Balance Policy.
User Management	Such item is available only when <b>Rule-Based</b> is selected in User <b>Management&gt;&gt;General Setup</b> . The general firewall rule will be applied to the user/user group/all users specified here. None User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile existed,
	<b>Create New User</b> or <b>Create New Group</b> item will appear for you to click to create a new one.
APP Enforcement	Select an <b>APP Enforcement</b> profile for global IM/P2P application blocking. If there is no profile for you to select, please choose <b>[Create New]</b> from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the <b>APP Enforcement</b> profile selected here. For detailed information, refer to the



	section of <b>APP Enforcement</b> profile setup. For troubleshooting needs, you can specify to record informatio for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
URL Content Filter	<ul> <li>Select one of the URL Content Filter profile settings (created in CSM&gt;&gt; URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM&gt;&gt; URL Content Filter web page first. Or choose</li> <li>[Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</li> </ul>
URL Content Filter	<ul> <li>Select one of the URL Content Filter profile settings (created in CSM&gt;&gt; URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM&gt;&gt; URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</li> </ul>
Web Content Filter	<ul> <li>Select one of the Web Content Filter profile settings         (created in CSM&gt;&gt; Web Content Filter) for applying with         this router. Please set at least one profile for anti-virus in         CSM&gt;&gt; Web Content Filter web page first. Or choose         [Create New] from the drop down list in this page to create         a new profile. For troubleshooting needs, you can specify to         record information for Web Content Filter by checking the         Log box. It will be sent to Syslog server. Please refer to         section Syslog/Mail Alert for more detailed information.</li> </ul>
Advance Setting	Click <b>Edit</b> to open the following window. However, it is <b>strongly recommended</b> to use the default settings here.
	♦ http://192.168.1.1/doc/ipfedrady.htm • Windows Internet Explorer          Intp://192.168.1.1/doc/ipfedrady.htm         Firewall >> Edit Filter Set >> Edit Filter Rule         Filter Set 1 Rule 1         Advance Setting         Codepage         AlVSI(1252)-Latin I         Vindow size:         65535         Session timeout:         I440         Minute         DrayTek Banner:         V         OK
	<b>Codepage</b> - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content

Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

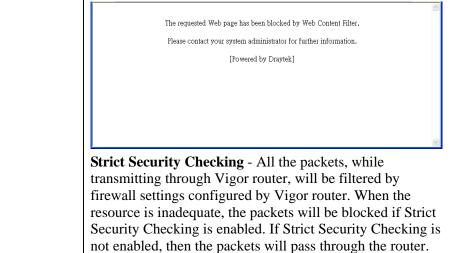
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

Dray Tek Syslog 3.9.1      Controls      Dray Controls      Dray Controls      Dray Controls      Dray Tek Syslog 3.9.1	192.168.1.1	WAN Information WAN1 IP (Fixed)
LAN Status TX Packets 28489	RX Packets	WAN2 IP (Fixed)
Setup Tool Setup   Telnet Read-out Setup Codepage To Select	Codepage Information	
Windows Version: 5.01.2600 RECOMMENDED CODEPA 950 (ANSI/OEM - Tradition 00a1:21.00a6:7c.00a9:63.00a		063:33 0069:31 006a:6f

**Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

**Session timeout**–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

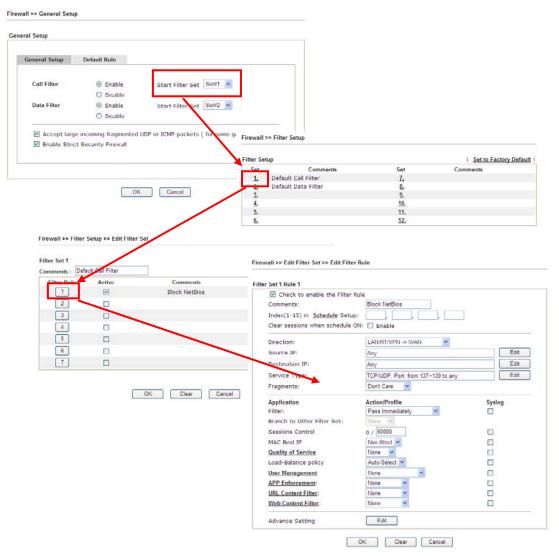
**DrayTek Banner** – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.





#### Example

As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



**Dray** Tek

#### 3.4.4 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click Firewall and click DoS Defense to open the setup page.

Firewall >> DoS defense Setup	Firewall	>>	DoS	defense	Setup
-------------------------------	----------	----	-----	---------	-------

DoS defense Setup			
Enable DoS Defense Select All			
Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable Port Scan detection	Threshold	150	packets / sec
Block IP options	Block TCP flag	scan	
Block Land	🔲 Block Tear Drop	)	
Block Smurf	Block Ping of De	eath	
Block trace route	🔲 Block ICMP frag	ment	
Block SYN fragment	🔲 Block Unassigne	ed Numbers	
Block Fraggle Attack			
Enable DoS defense function to preve crackers.	nt the attacks fr	om hacker	or 🔼
GLUGATID.			$\sim$

Clear All

Cancel

Available settings are explained as follows:

ΟK

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router.
	By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router



	will start to randomly discard the subsequent UDP packets for a period defined in Timeout.
	The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively. That means, when 150 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.
	The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.
	By default, the Vigor router sets the threshold as 150 packets per second. That means, when 150 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function.

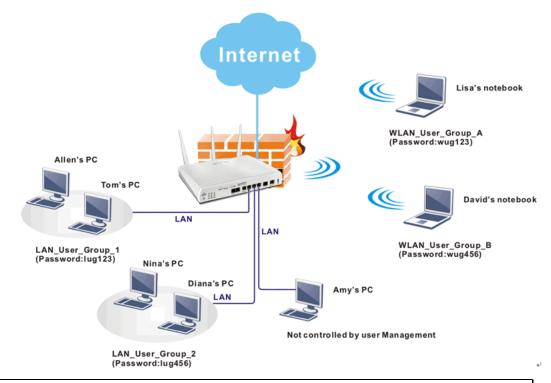


	Any broadcast UDP packets received from the Internet is
	blocked.
	Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK</i> <i>scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unassigned Numbers	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.
	All the warning messages related to <b>DoS Defense</b> will be sent to user and user can review it through Syslog daemon. Look for the keyword <b>DoS</b> in the message, followed by a name to indicate what kind of attacks is detected.

SysLog Access Set	up	Mail Alert Setup	
Enable	-ap	Enable	Send a test e-m
Syslog Save to:		SMTP Server	
Syslog Ser	ver		25
USB Disk		SMTP Port	20
Router Name		Mail To	
Server IP Addres	s	Return-Path	
Destination Port	514	Authentica	ation
Mail Syslog	Enable	User Name	
Enable syslog me		Password	
Firewall Lo		Enable E-Mail	
User Acce	ss Log	DoS Att	ack
✓ WAN Log ✓ Router/DS	Linformation	VPN LOG	
AlertLog Setup	Lintormation	E VPN LOG	2
Enable			
AlertLog Port	514		
Controls	1 192.168.1.1 Vigor Series	WAN Status Gateway IP (Fixed) 172:16:3.4	TX Packets TX Rote
Controls	0	WAN Stotus Gateway IP (Fixed)	
Controls	Vigor Sortes RX Packets 3660 Uter Access Log Call Log WAN	WAN Status Gateway IP (Fixed) 172.16.3.4 WAN ID (Fixed)	343         3           RX Packets         RX Rate           2558         126
Controls LAN Status TX Packets Furwell Log VPN Log Time Ina 1000042	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gaterway IP (Fixed) 172.16.3.4 WAN IP (Fixed) 172.16.3.29	343 3 RX Packets RX Rate 2558 126 et State Tradiic Oraph 108 1 1,23 PR Ofean Jan 20 40 -5 394375
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5
Controls	In the second se	WAN Status Gatemay IP (Frond) 172.16.3.4 WAN IP (Frond) 172.16.3.229	343 3 RX Packets RX Rate 2558 126 et State Tradiic Graph 108 1 1,23 PR (flup) Im 20 40 -2 59417/5

## 3.5 User Management

User Management is a security feature which disallows any IP traffic (except DHCP-related packets) from a particular host until that host has correctly supplied a valid username and password. Instead of managing with IP address/MAC address, User Management function manages hosts with user account. Network administrator can give different firewall policies or rules for different hosts with different User Management accounts. This is more flexible and convenient for network management. Not only offering the basic checking for Internet access, User Management also provides additional firewall rules, e.g. CSM checking for protecting hosts.



**Note**: Filter rules configured under Firewall usually are applied to the host (the one that the router installed) only. With user management, the rules can be applied to every user connected to the router with customized profiles.

**Note**: If **Transparency Mode** is selected in **Firewall>>General Setup**, User Management cannot be used any more. Please uncheck Transparency Mode first if you want to utilize user management to handle users in LAN, WAN or WLAN.

User Management General Setup User Profile User Group User Online Status



## 3.5.1 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.

User Management >> General Setup

Mode: Rule-Based 🚩		
Notice :		
1. User Management will refer to a	ctive rules in Data Filter as whiteli	sts and blacklists
in user-based firewall mode. 2. Users match the above lists will	not be required for authentication	۱.
The firewall rules policy will still		
3. Otherwise, authentication requir	red for users not matched the abo	
3. Otherwise, authentication requir		
3. Otherwise, authentication requir	red for users not matched the abo the user profile's policy will still va	
3. Otherwise, authentication requir The firewall rules designated in Landing Page (Max 255 characters <body stats="1"><script languag<="" td=""><td>red for users not matched the abo the user profile's policy will still va ;) <u>Preview</u> ge='javascript'></td><td>lid.</td></tr><tr><td><ol>     <li>Otherwise, authentication requir The firewall rules designated in Landing Page (Max 255 characters</li> </ol></td><td>red for users not matched the abo the user profile's policy will still va ;) <u>Preview</u> ge='javascript'></td><td>lid.</td></tr><tr><td>3. Otherwise, authentication requir The firewall rules designated in Landing Page (Max 255 characters <body stats=1><script languag</td><td>red for users not matched the abo the user profile's policy will still va ;) <u>Preview</u> ge='javascript'></td><td>lid.</td></tr></tbody></table></script></body>		

Available settings are explained as follows:

Item	Description
Mode	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.
	User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.
	<b>Rule-Based</b> –If you choose such mode, the router will apply the filter rules configured in <b>Firewall&gt;&gt;General Setup</b> and <b>Filter Rule</b> to the users.
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

After finishing all the settings here, please click **OK** to save the configuration.

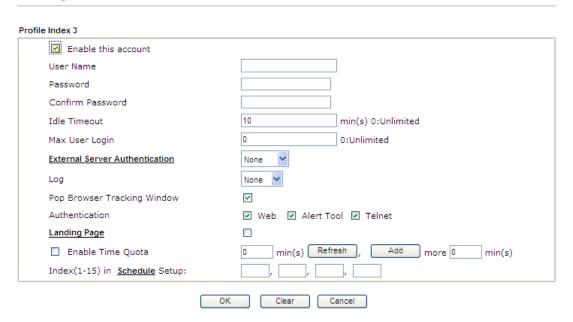
#### 3.5.2 User Profile

This page allows you to set customized profiles (up to 200) which will be applied for users controlled under **User Management**. Simply open **User Management>>User Profile**.

Profile	Name	Profile	Name
<u>1.</u>	admin	<u>17.</u>	
<u>2.</u>	Dial-In User	<u>18.</u>	
<u>3.</u>	LAN_User_Group_1	<u>19.</u>	
<u>4.</u>	WLAN_User_Group_A	<u>20.</u>	
<u>5.</u>	WLAN_User_Group_B	<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

User Management >> User Profile

To set the user profile, please click any index number link to open the following page. Notice that profile 1 (**admin**) and profile 2 (**Dial-In User**) are factory default settings. Profile 2 is reserved for future use.



User Management >>User Profile

Item	Description
Enable this account	Check this box to enable such user profile.
User Name	<ul> <li>Type a name for such user profile (e.g., <i>LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B</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 User Name 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.</li> <li>The maximum length of the name you can set is 24 characters.</li> </ul>
Password	<ul> <li>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.</li> <li>The maximum length of the password you can set is 24 characters.</li> </ul>
Confirm Password	Type the password again for confirmation.
Idle Timeout	If the user is idle over the limitation of the timer, the <b>network connection will be stopped for such user.</b> By default, the Idle Timeout is set to 10 minutes.
Max User Login	Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
Policy	It is available only when <b>User-Based</b> mode selected in <b>User Management&gt;&gt;General Setup</b> .
	<ul> <li>Default</li> <li>Default</li> <li>[Create New Policy]</li> <li>Default – If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile.</li> <li>Create New Policy – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.</li> </ul>

	Firewall >> Edit Filter Set >> Edit Filter Rule		
	Filter Set 1 Rule 2         Check to enable the Filter Rule         Comments:         Index(1-15) in <u>Schedule</u> Setup:         Clear sessions when schedule ON:         Enable         Direction:         Source IP:         Any         Destination IP:         Service Type:         Any         For the detailed configuration, simply refer to         Firewall>>Filter Rule. The firewall filter rules that are not		
External Service Authentication	selected in Firewall>>General>>Default rule can be available for use in User Management>>User Profile.The router will authenticate the dial-in user by itself or by external service such as LDAP server or Radius server. If LDAP or Radius is selected here, it is not necessary to 		
	None V None LDAP Radius		
Log	Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the log items to take down relational records for the user(s). None Login Event All		
Pop Browser Tracking Window	If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.		
Authentication	<ul> <li>Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.</li> <li>Web – If it is selected, the use can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in User Management &gt;&gt; General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.</li> <li>Alert Tool – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A</li> </ul>		



	window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site.	
	<b>Telnet</b> – If it is selected, the user can use Telnet command to perform the authentication job.	
Landing Page	When a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in User Management>>General Setup.	
	Check this box to enable such function.	
Enable Time Quota	Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet. <b>Refresh</b> – Click this button to recalculate the time quota. <b>Add</b> – Click this box to set the time quota for such profile.	
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.	

After finishing all the settings here, please click **OK** to save the configuration.

## 3.5.3 User Group

This page allows you to bind several user profiles into one group. These groups will be used in **Firewall>>General Setup** as part of filter rules.

Iser Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		27.	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

User Management >> User Group

**Dray** Tek

Please click any index number link to open the following page.

User Management >> User Group

Name:	
Available User Objects	Selected User Objects(Max 32 Objects)
1-admin 2-Dial-In User 3-LAN_User_Group_1 4-WLAN_User_Group_A 5-WLAN_User_Group_B	>> ((

Available settings are explained as follows:

Item	Description	
Name	Type a name for this user group.	
Available User Objects	You can gather user profiles (objects) from User Profile page within one user group. All the available user object that you have created will be shown in this box. Notice t user object, Admin and Dial-In User are factory settings User defined profiles will be numbered with 3, 4, 5 and on.	
Selected Keyword Objects	Click button to add the selected user objects in this box.	

After finishing all the settings here, please click **OK** to save the configuration.

## 3.5.4 User Online Status

This page displays the user(s) connected to the router and refreshes the connection status in an interval of several seconds.

User Management >> User Online Status

Index	Profile V	IP Address	User	Last Login Time	econds: 10 V F		
1				-			
1	admin	192.168.1.49	admin	01-03 10:40:59	Unlimited	Unlimited	BIOCK LOGOU

Item	Description		
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.		
	Refresh Seconds: 10 V 10 15 30		
Refresh	Click this link to refresh this page manually.		
Index	Display the number of the data flow.		
Active User	Display the users which connect to Vigor router currently. You can click the link under the username to open the user profile setting page for that user.		
IP Address	Display the IP address of the device.		
Last Login Time	Display the login time that such user connects to the router last time.		
Expired Time	Display the expired time of the network connection for the user.		
Idle Time	Display the idle timeout setting for such profile.		
Action	<b>Block</b> - can prevent specified user accessing into Internet. <b>Unblock</b> – the user will be blocked.		
	<b>Logout</b> – the user will be logged out forcefully.		

# 3.6 Objects Settings

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore 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).

Objects Setting
IP Object
IP Group
IP∨6 Object
IP∨6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
SMS/Mail Service Object
Notification Object

### 3.6.1 IP Object

You can set up to 192 sets of IP Objects with different conditions.

Objects Setting >> IP Object

IP Object Profiles:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

<< 1.32 | 33.64 | 65.96 | 97.128 | 129.160 | 161.192 >>

<u>Next</u> >>

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.



To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Name:	RD Department
Interface:	Any 💌
Address Type:	Range Address 🐱
Mac Address:	00 00 00 00 00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	0.0.0.0
Invert Selection:	

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Interface	Choose a proper interface.          Any         Any         LAN/RT/VPN         WAN         For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page.	
Address Type	<ul> <li>Determine the address type for the IP address.</li> <li>Select Single Address if this object contains one IP address only.</li> <li>Select Range Address if this object contains several IPs within a range.</li> <li>Select Subnet Address if this object contains one subnet for IP address.</li> <li>Select Any Address if this object contains any IP address.</li> <li>Select Mac Address if this object contains Mac address.</li> <li>Range Address</li> <li>Single Address</li> <li>Subnet Address</li> <li>Subnet Address</li> <li>Mac Address</li> </ul>	

MAC Address	Type the MAC address of the network card which will be controlled.	
Start IP Address	Type the start IP address for Single Address type.	
End IP Address	Type the end IP address if the Range Address type is selected.	
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.	
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.	

3. After finishing all the settings here, please click **OK** to save the configuration. Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:	
---------------------	--

Index	Name	Index
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>	Financial Dept	<u>18.</u>
<u>3.</u>	HR Department	<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>
6.		22.

# 3.6.2 IP Group

This page allows you to bind several IP objects into one IP group.

Objects Setting >> IP Group

IP Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Objects Setting >> IP Group

Profile Index : 1		
Name:	Administration	
Interface:	Any 💌	
Available IP Object	Selected IP Objects	
1-RD Department 2-Financial Dept 3-HR Department	~	
	OK Clear Cancel	

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

3. After finishing all the settings here, please click **OK** to save the configuration.

#### 3.6.3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

Objects Setting >> IPv6 Object

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1	
Name:	
Address Type:	Subnet Address 💌
Mac Address:	00 00 00 00 00
Start IP Address:	
End IP Address:	
Prefix Len:	
Invert Selection:	
ОК	Clear Cancel

Vigor2860 Series User's Guide

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Address Type	<ul> <li>Determine the address type for the IPv6 address.</li> <li>Select Single Address if this object contains one IPv6 address only.</li> <li>Select Range Address if this object contains several IPv6s</li> </ul>	
	within a range. Select <b>Subnet Address</b> if this object contains one subnet for IPv6 address.	
	Select <b>Any Address</b> if this object contains any IPv6 address.	
	Select Mac Address if this object contains Mac address.	
	Range Address         Any Address         Single Address         Range Address         Subnet Address         Mac Address	
Mac Address	Type the MAC address of the network card which will be controlled.	
Start IP Address	Type the start IP address for Single Address type.	
End IP Address	Type the end IP address if the Range Address type is selected.	
Prefix Len	Type the number (e.g., 64) for the prefix length of IPv6 address.	
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.	

3. After finishing all the settings, please click **OK** to save the configuration.

## 3.6.4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

Pv6 Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1	
Name:	
Available IPv6 Objects	Selected IPv6 Objects
	>>
	~~ · · · · · · · · · · · · · · · · · ·
1	
	OK Clear Cancel



Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

3. After finishing all the settings, please click **OK** to save the configuration.

# 3.6.5 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

```
Objects Setting >> Service Type Object
```

Service Type Object	Profiles:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	
<< 1-32   33-64   65	5-96 >>		<u>Next</u> >>

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

```
Objects Setting >> Service Type Object Setup
```

Name	WWW
Protocol	TCP 6
Source Port	= 💙 1 ~ 65535
Destination Port	= 🖌 1 ~ 65535

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         ICMP       IGMP         IGMP       TCP         UDP       TCP/UDP         Other       0	
Source/Destination Port	<ul> <li>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</li> <li>(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.</li> <li>(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</li> <li>(&gt;) – the port number greater than this value is available.</li> <li>(&lt;) – the port number less than this value is available for</li> </ul>	



3. After finishing all the settings, please click **OK** to save the configuration.

Objects Setting >> Service Type Object

Service Type Object	Profiles:	
Index	Name	Inde
<u>1.</u>	www	<u>17</u> .
<u>2.</u>	SIP	<u>18</u> .
<u>3.</u>		<u>1</u> 9.
4.		20.

# 3.6.6 Service Type Group

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

Objects Setting >> Service Type Group

ervice Type Group 1	Table:		Set to Factory Default
Group	Name	Group	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Group column for configuration in details.
- 2. The configuration page will be shown as follows:

Name:	VoIP		
Available Service T	ype Objects	Selected Service Typ	e Objects
1-www			
2-SIP			
		>>	

Objects Setting >> Service Type Group Setup

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available Service Type Objects	All the available service objects that you have added on <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

3. After finishing all the settings, please click **OK** to save the configuration.

# 3.6.7 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in CSM >>URL Web Content Filter Profile.

eyword Object Prof	files:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	
< <u>1-32   33-64   65</u>	5-96   <u>97-128   129-160   161</u> -	<u>192   193-200 &gt;&gt;</u>	<u>Next</u> >

Objects Setting >> Keyword Object

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.
You can replace a character with %HEX. Example: Contents: backdoo%72 virus keep%20out
Result: 1. backdoor 2. virus

Available settings are explained as follows:

Item	Description	
Name	Type a name for this profile, e.g., game. Maximum 15 characters are allowed.	
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.	

3. After finishing all the settings, please click **OK** to save the configuration.

# 3.6.8 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM** >>**URL** /**Web** Content Filter Profile.

Keyword Group Ta	ible:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Objects Setting >> Keyword Group

Available settings are explained as follows:

Item	Description		
Set to Factory Default	Clear all profiles.		
Index	Display the profile number that you can configure.		
Name	Display the name of the group profile.		

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Index column for configuration in details.
- 2. The configuration page will be shown as follows:

Objects Setting >> Keyword Group Setup

rofile Index : 1	
Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Key-1 2-Key-2	
2-Ney-2	
	»
	~
	OK Clear Cancel



Item	Description	
Name	Type a name for this group. Maximum 15 characters are allowed.	
Available Keyword Objects	You can gather keyword objects from <b>Keyword Object</b> page within one keyword group. All the available Keyword objects that you have created will be shown in this box.	
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.	

3. After finishing all the settings, please click **OK** to save the configuration.

## 3.6.9 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Objects Setting >> File Extension Object

File Extension Obje	ect Profiles:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

Item	Description		
Set to Factory Default	Clear all profiles.		
Index	Display the profile number that you can configure.		
Name	Display the name of the object profile.		

# **Dray** Tek

To set a new profile, please do the steps listed below:

- 1. Click the number (e.g., #1) under Profile column for configuration in details.
- 2. The configuration page will be shown as follows:

Profile Index: 1	P	rofile Name	:				
Categories	File Extensions						
Image Select All Clear All	□.bmp □.pct	.dib .pcx	.gif .pic	□.jpeg □.pict	.jpg .png	□.jpg2 □.tif	jp2 tiff
Video Select All Clear All	🗌 .asf 🔲 .qt	🗌 .avi 🗋 .rm	□.mov □.wmv	.mpe	.mpeg .3gpp	.mpg .3gpp2	.mp4
Audio Select All Clear All	🗌 .aac 🗌 .ra	□.aiff □.ram	🗌 .au 🗌 .vox	.mp3 .wav	□.m4a □.wma	.m4p	ogg. 🗌
Java Select All Clear All	□ .class □ .jse	□.jad □.jsp	□.jar □.jtk	🗌 .jav	🗌 .java	🗌 .jcm	🗌 .js
ActiveX Select All Clear All	□ .alx □ .viv	.apb .vrm	.axs	.ocx	olb. 🗌	ole .	.tlb
Compression							

Objects Setting >> File Extension Object Setup

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile. The maximum length of the name you can set is 7 characters.

3. Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

# 3.6.10 SMS/Mail Service Object

## **SMS Service Object**

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

SMS Provider	Mail Server		Set to Factory Default
Index	Profile	e Name	SMS Provider
<u>1.</u>			kotsms.com.tw (TW)
<u>2.</u>			kotsms.com.tw (TW)
<u>3.</u>			kotsms.com.tw (TW)
<u>4.</u>			kotsms.com.tw (TW)
<u>5.</u>			kotsms.com.tw (TW)
<u>6.</u>			kotsms.com.tw (TW)
<u>7.</u>			kotsms.com.tw (TW)
<u>8.</u>			kotsms.com.tw (TW)
<u>9.</u>	Cust	tom 1	
<u>10.</u>	Cust	tom 2	

Object Settings >> SMS / Mail Service Object

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

To set a new profile, please do the steps listed below:

1. Click the **SMS Provider** tab, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
Index	Profile Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Name	Line_down
Service Provider	kotsms.com.tw (TW)
Username	line1
Password	••••
Quota	10
Sending Interval	3 (seconds)

Available settings are explained as follows:

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

3. After finishing all the settings here, please click **OK** to save the configuration.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index	Profile	Name	SMS Provider
<u>1.</u>	Line_	down	kotsms.com.tw (TW)
<u>2.</u>			kotsms.com.tw (TW)
<u>3.</u>			kotsms.com.tw (TW)
4.			kotsms.com.tw (TW)

## **Customized SMS Service**

Vigor router offers several SMS service provider to offer the SMS service. However, if your service provider cannot be found from the service provider list, simply use Index 9 and Index 10 to make customized SMS service. The profile name for Index 9 and Index 10 are fixed.

SMS Provider	Mail Server		Set to Factory Default
Index	Profile	e Name	SMS Provider
<u>1.</u>			kotsms.com.tw (TW)
<u>2.</u>			kotsms.com.tw (TW)
<u>3.</u>			kotsms.com.tw (TW)
<u>4.</u>			kotsms.com.tw (TW)
<u>5.</u>			kotsms.com.tw (TW)
<u>6.</u>			kotsms.com.tw (TW)
<u>7.</u>			kotsms.com.tw (TW)
<u>8.</u>			kotsms.com.tw (TW)
<u>9.</u>	Cust	tom 1	
<u>10.</u>	Cust	tom 2	

Object Settings >> SMS / Mail Service Object

You can click the number (e.g., #9) under Index column for configuration in details.

```
Object Settings >> SMS / Mail Service Object
```

Profile Name	Custom 1	
Service Provider		
		1
Plance contact with your SN	45 provide to get the exact LIRL String	
	1S provide to get the exact URL String	
eg:bulksms.vsms.net:5567/	/eapi/submission/send_sms/2/2.0?usern	
eg:bulksms.vsms.net:5567/		
eg:bulksms.vsms.net:5567/	/eapi/submission/send_sms/2/2.0?usern	
eg:bulksms.vsms.net:5567/ &password=###txtPwd##	/eapi/submission/send_sms/2/2.0?usern	
eg:bulksms.vsms.net:5567/ &password=###txtPwd## Username	/eapi/submission/send_sms/2/2.0?usern	

Item	Description	
Profile Name	Display the name of this profile. It cannot be modified.	
Service Provider	Type the website of the service provider. Type the URL string in the box under the filed of Service Provider. You have to contact your SMS provider to obtain the exact URL string.	



Username	Type a user name that the sender can use to register to selected SMS provider. The maximum length of the name you can set is 31 characters.
Password	Type a password that the sender can use to register to selected SMS provider. The maximum length of the password you can set is 31 characters.
Quota	Type the total number of the messages that the router will send out.
Sending Interval	Type the shortest time interval for the system to send SMS.

After finishing all the settings here, please click **OK** to save the configuration.

## **Mail Service Object**

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

SMS Pro	ovider	Mail Server		Set to Factory Default
Index			Profile Name	
<u>1.</u>				
<u>2.</u>				
<u>3.</u>				
<u>4.</u>				
<u>5.</u>				
<u>6.</u>				
<u>7.</u>				
<u>8.</u>				
<u>9.</u>				
<u>10.</u>				

Object Settings >> SMS / Mail Service Object

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.

To set a new profile, please do the steps listed below:

1. Click the Mail Server tab, and click the number (e.g., #1) under Index column for configuration in details.

SMS Pro	ovider	Mail Server
Index		
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

Object Settings >> SMS / Mail Service Object

2. The configuration page will be shown as follows:

Profile Name	Mail_Notify	
SMTP Server	192.168.1.98	
SMTP Port	80	
Sender Address	carrieni@draytek.com	
Authentication		
Username	john	
Password	1234	
Sending Interval	0 (seconds)	

Object Settings >> SMS / Mail Service Object

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Type the IP address of the mail server. The maximum length of the name you can set is 63 characters.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function.
	<b>Username</b> – Type a name for authentication. The maximum length of the name you can set is 31 characters.
	<b>Password</b> – Type a password for authentication. The maximum length of the password you can set is 31 characters.
Sending Interval	Define the interval for the system to send the SMS out.

3. After finishing all the settings here, please click **OK** to save the configuration.

 Object Settings >> SMS / Mail Service Object

 SMS Provider
 Mail Server
 Set to Factory Default

 Index
 Profile Name

 1.
 Mail\_Notify

 2.
 3

## 3.6.11 Notification Object

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

You can set an object with different monitoring situation.

Object Settings >> Notification Object

		Set to Factory Default
Index	Profile Name	Settings
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		

To set a new profile, please do the steps listed below:

1. Open **Object Setting>>Notification Object**, and click the number (e.g., #1) under Index column for configuration in details.

Object Settings >> Notification Object

Index	Profile Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	
5.	

2. The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Name	Notify_attack	
Category		Status
WAN	Disconnected	Reconnected
VPN Tunnel	Disconnected	Reconnected
Temperature Alert	Out of Range	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box you want to be monitored.

3. After finishing all the settings here, please click **OK** to save the configuration.

Object Settings >> Notification Object

		Set to Factory Default
Index	Profile Name	Settings
<u>1.</u>	Notify_attack	WAN VPN
<u>2.</u>		
<u>3.</u>		

# 3.7 CSM Profile

## **Content Security Management (CSM)**

**CSM** is an abbreviation of **Content Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

## **APP Enforcement Filter**

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

## **URL Content Filter**

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

### Web Content Filter

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 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.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Note: The priority of URL Content Filter is higher than Web Content Filter.





## 3.7.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

CSM >> APP Enforcement Profile

PP Enforcement Pr	ofile Table:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.

There are four tabs IM, P2P, Protocol and Misc displayed on this page. Each tab will bring out different items that you can choose to disallow people using.



Below shows the items which are categorized under Protocol.

rofile Index : 1	Profile Name:				
IM	P2P	Protocol	Misc		
Select All	Clear All				
			Protocol		
DNS	□ FT P	I	Энттр	IMAP	□ IRC
<b>NNTP</b>	POP3	I	SMB	SMTP	SNMP
SSH	SSL/TLS	I	TELNET	MSSQL	MySQL
Oracle	PostgreSQL	[	Sybase	DB2	Informix

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

Below shows the items which are categorized under IM.

CSM >> APP Enforcement Profile

IM	P2P	Protocol	Misc		
Select All CI	ear All				
		Advanced	l Management		
Activity /	Application	MSN	YahooIM	AIM(<= v5.9)	ICQ
Lo	gin				
Mes	sage				
File T	ransfer				
Ga	ime				
Conference(Video/Voice)					
Other /	Activities				
		IM Application			VoIP
AIM6/7	□ QQ/ТМ	iChat	🗌 Jabber/0	BoogleTalk	
GoogleChat	XFire	GaduGadu	🗌 Paltalk		Skype Kubao
Qnext	POCO/PP365	AresChat	Aliww		Gizmo SIP/RTP
Lava-Lava	ICU2	□iSpQ			■TelTel ■TeamSpeak
MobileMSN	🗌 BaiduHi	Fetion			
		Web IM ( * = mo	ore than one address)		
	eMessenger	WebMSN meeb	o* <u>eBuddy</u>	ILovelM*	
WebIM URLs	ICQ Java*	ICQ Flash* goow		getMessenger	
	IMUnitive* MessengerFX*	Wablet* mabb MessengerAdictos WebY		KooliM	
	wessengerra.	wessengerAdiolos Webt	anoond		

#### The items categorized under **P2P** -----

ile Index : 1 Profi	le Name:				
IM	P2P	Protocol	Misc		
Select All C	lear All				
Proto	col			Applications	
SoulSeek		SoulSeek			
eDonkey e		eDonkey, eMule, Sharea	za		
FastTrack	FastTrack KazaA, BearShare, iMesh				
OpenFT	KCeasy, FilePipe				
Gnutella	utella BearShare, Limewire, Shareaza, Foxy, KCeasy		Ceasy		
OpenNap Lopster, XNap, WinLop					
BitTorrent	BitTorrent BitTorrent, BitSpirit, BitComet				
		Other P2P	Applications		
Xunlei Vagaa		PP365		POCO	Clubbox
Ares	ezPeer	🗌 Pando		Huntmine	Kuwo

#### The items categorized under Misc -----

ile Index : 1 Profile	Name:			
IM		otocol Misc		
Select All Cle	ar All			
		Tunneling		
Socks4/5	PGPNet	HTTP Proxy	Tor	VNN VNN
SoftEther	MS TEREDO	Uujie/UltraSurf	Hamachi	HTTP Tunnel
Ping Tunnel	TinyVPN	RealTunnel	DynaPass	UltraVPN
FreeU	Skyfire			
		Streaming		
]ммs	RTSP	TVAnts	PPStream	PPTV
FeiDian	UUSee	NSPlayer	PCAST	Πτνκοο
SopCast	UDLiveX	TVUPlayer	MySee	Joost
]FlashVideo	SilverLight	Slingbox	QVOD	
		Remote Control		
VNC	Radmin	SpyAnywhere	ShowMyPC	LogMeIn
TeamViewer	Gogrok	RemoteControlPro	CrossLoop	WindowsRDP
]pcAnywhere	Timbuktu	WindowsLiveSync	SharedView	
		Web HD		
HTTP Upload	HiNet SafeBox	MS SkyDrive	GDoc Uploader	ADrive
MyOtherDrive	Mozy	BoxNet	OfficeLive	

## 3.7.2 URL Content Filter Profile

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.



On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p\_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click CSM and click URL Content Filter Profile to open the profile setting page.

URL Content Filter Pr	ofile Table:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

CSM >> URL Content Filter Profile

Administration Message (Max 255 characters)

<body><center><br>The requested Web page has been blocked by URL Content
Filter.Please contact your system administrator for further information.</center></body>

#### OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.
Administration Message	You can type the message manually for your necessity.

You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.

#### CSM >> URL Content Filter Profile

Profile Name:		
Priority:	Both : Pass	✓ Log: None ✓
1.URL Access	Control	
Enat	le URL Access Control	Prevent web access from IP address
Actio	n:	Group/Object Selections
Pass	*	Edit
I		
2.Web Feature		
🗌 Enat	le Restrict Web Feature	
Actio	n:	
Pass	🗠 🗌 Cookie 🔲 Proxy	🗌 Upload <u>File Extension Profile:</u> None 💌

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	It determines the action that this router will apply.
	<b>Both: Pass</b> – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
	<b>Both:Block</b> –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
	<b>Either: URL Access Control First</b> – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.
	<b>Either: Web Feature First</b> –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

# **Dray** Tek

	Both : Pass Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First
Log	<ul> <li>None – There is no log file will be recorded for this profile.</li> <li>Pass – Only the log about Pass will be recorded in Syslog.</li> <li>Block – Only the log about Block will be recorded in Syslog.</li> <li>All – All the actions (Pass and Block) will be recorded in Syslog.</li> <li>None</li> <li>Pass</li> <li>Block</li> <li>All</li> </ul>
URL Access Control	<ul> <li>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</li> <li>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</li> <li>Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. Pass - Allow accessing into the corresponding</li> </ul>
	<ul> <li>webpage with the keywords listed on the box below.</li> <li>Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.</li> <li>If the web pages do not match with the keyword set here, it will be processed with reverse action.</li> <li>Action:</li> <li>Block</li> <li>Block</li> <li>Group/Object Selections – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or</li> </ul>
	semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It

should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs. **Object/Group Edit** Keyword Object None or Keyword Object None or Keyword Object None or Keyword Object None or Keyword Object None None or Keyword Object None or Keyword Object or Keyword Object None None or Keyword Group or Keyword Group None 🗸 None 🗸 or Keyword Group None 🗸 or Keyword Group or Keyword Group None 🗸 or Keyword Group None 🗸 or Keyword Group None V or Keyword Group None V 0K Close Web Feature Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed. Action - This setting is available only when Either: URL Access Control First or Either: Web Feature Firs is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below. **Pass** - Allow accessing into the corresponding webpage with the keywords listed on the box below. Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. **Proxy** - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. **Upload** – Check the box to block the file upload by way of web page. File Extension Profile – Choose one of the profiles that you configured in **Object Setting>> File Extension** Objects previously for passing or blocking the file downloading.



d File Extension Profile: None 💌
None
1-image

After finishing all the settings, please click **OK** to save the configuration.

# 3.7.3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (*MyVigor*) located on <u>http://myvigor.draytek.com</u>.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (*MyVigor*) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

**Note:** If you have used **Service Activation Wizard** to activate WCF service, you can skip this section.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware 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 the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

#### CSM >> Web Content Filter Profile

Setup Query Server	auto-selecte	ed	Find more
Setup Test Server	auto-selecte	ed	Find more
Veb Content Filter Pro	file Table:		Set to Factory Det
Profile	Name	Profile	Name
<u>1.</u>	Default	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
<pre> conter&gt; body&gt;<center> is categorized wit</center></pre>	h %CL% has been		-
,	%DIP% - Destina %RNAME% - Route	ation IP,%URL% - UF r Name	ιL

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.

# **Dray** Tek

Cache	<b>None</b> – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.
	L1 – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.
	L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.
	<b>L1+L2 Cache</b> – the router will check the URL with fast processing rate combining the feature of L1 and L2.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.

Profile Index: 1			
Profile Name: Default			Log: Block
Black/White List			
Enable			
Action:	G	roup/Object Selections	
Block 🗸			Edit
Action: Block 🗸			
Groups	Categories		
Child Protection	Alcohol & Tobacco	Criminal Activity	🗹 Gambling
Select All	Hate & Intolerance	🗹 Illegal Drug	✓ Nudity
Clear All	Porn & Sexually	✓ Violence	✓ Weapons
	School Cheating	Sex Education	🗹 Tasteless
	Linnance	L overnment.	Li nealtri a NeGiane
	News	Non-profits & NGOs	Personal Sites
	Politics	Real Estate	Religion
	Restaurants & Dining	Shopping	Translators
	General	Cults	Greeting cards
	Image Sharing	Network Errors	Parked Domains
	Private IP Addresses	Uncategorised Sites	

**Dray** Tek

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	<b>Enable</b> – Activate white/black list function for such profile. <b>Group/Object Selections</b> – Click <b>Edit</b> to choose the group or object profile as the content of white/black list.
	<b>Pass - allow</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
	<b>Block</b> - <b>restrict</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
Action	<b>Pass</b> - allow accessing into the corresponding webpage with the categories listed on the box below.
	<b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.
	If the web pages do not match with the specified feature set here, it will be processed with reverse action.
Log	None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog. All – All the actions (Pass and Block) will be recorded in Syslog. Block Mone Pass Block All

After finishing all the settings, please click **OK** to save the configuration.

# 3.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management Sessions Limit Bandwidth Limit Quality of Service

### 3.8.1 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.

Sessions Limit	
C Enable ③ Disable	
Default Max Sessions: 100	
Limitation List	
Index Start IP End IP Max Sessions	
Specific Limitation	
Start IP: End IP:	
Maximum Sessions:	
Add Edit Delete	
dministration Message (Max 256 characters)	Default Message
	~
ime Schedule	
Index(1-15) in <u>Schedule</u> Setup:,,,	
Note: Action and Idle Timeout settings will be ignored.	
ОК	

Bandwidth Management >> Sessions Limit

To activate the function of limit session, simply click **Enable** and set the default session limit. Available settings are explained as follows:

Item	Description
Session Limit	<b>Enable -</b> Click this button to activate the function of limit session.
	<b>Disable</b> - Click this button to close the function of limit session.

# **Dray** Tek

	<b>Default session limit -</b> Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Specific Limitation	Start IP- Defines the start IP address for limit session.
	End IP - Defines the end IP address for limit session.
	<b>Maximum Sessions -</b> 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.
	<b>Add -</b> Adds the specific session limitation onto the list above.
	<b>Edit -</b> Allows you to edit the settings for the selected limitation.
	<b>Delete -</b> Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
	<b>Default Message -</b> Click this button to apply the default message offered by the router.
Time Schedule	<b>Index (1-15) in Schedule Setup</b> - You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.

After finishing all the settings, please click **OK** to save the configuration.

## 3.8.2 Bandwidth Limit

Bandwidth Management >> 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.

🔘 Enable 🗌 IP Rou	ted Subnet (	Disable		
Default TX Limit: 2000	Kbps 🗸	Default RX Lin	nit: 8000	Kbps 🐱
Allow auto adjust	ment to make	the best utilizati	on of <u>availat</u>	ole bandwidth.
Limitation List				
Index Start IP	End IP	TX limit	RX limit	Shared
Specific Limitation				
Start IP:	En	d IP:		
⊙ Each ○ Shared T	X Limit:	Kbps 🔽 RX I	.imit:	Kbps 🗸
	Add	Edit Delete	)	
🗌 Smart Bandwidth Lin	nit			
For any LAN IP Not ir	Limitation Lis	st, when session	number exc	eeds 1000
TX Limit : 200	Kbps 🔽 RX Li	imit : 800 🛛 🖡	(bps 🔽	
: For TX/RX, a setting of "0"	means unlimit	ed bandwidth.		
e Schedule				
	up:			
Index(1-15) in <u>Schedule</u> Set				

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Item	Description
Bandwidth Limit	<b>Enable</b> - Click this button to activate the function of limit bandwidth.
	<b>IP Routed Subnet</b> – Check this box to apply the
	bandwidth limit to the second subnet specified in
	LAN>>General Setup.
	<b>Disable -</b> Click this button to close the function of limit bandwidth.
	<b>Default TX limit -</b> Define the default speed of the upstream for each computer in LAN.
	Default RX limit - Define the default speed of the

	downstream for each computer in LAN.
	Allow auto adjustment Check this box to make the
	best utilization of available bandwidth.
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	<b>Start IP -</b> Define the start IP address for limit bandwidth.
	End IP - Define the end IP address for limit bandwidth.
	<b>Each /Shared -</b> Select <b>Each</b> to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select <b>Shared</b> to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.
	<b>TX limit -</b> 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.
	<b>RX limit -</b> 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.
	Add - Add the specific speed limitation onto the list above.
	<b>Edit -</b> Allow you to edit the settings for the selected limitation.
	<b>Delete -</b> Remove the selected settings existing on the limitation list.
Smart Bandwidth Limit	Check this box to have the bandwidth limit determined by the system automatically.
	<b>TX limit -</b> 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.
	<b>RX limit -</b> 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.
Time Schedule	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.

## 3.8.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

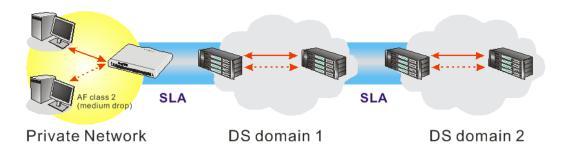
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.





However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

General	Setup								to Factory D	
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

Bandwidth Management >> Quality of Service

$\sim$		Deal	-
	ass	RU	е

clubb Nule			
Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Item	Description
General Setup	<b>Index</b> – Display the WAN interface number that you can edit.
	<b>Status</b> – Display if the WAN interface is available for such function or not.
	<b>Bandwidth</b> – Display the inbound and outbound bandwidth setting for the WAN interface.
	<b>Direction</b> – Display which direction that such function will influence.
	<b>Class 1/Class2/Class 3/Others</b> – Display the bandwidth percentage for each class.
	<b>UDP Bandwidth Control</b> – Display the UDP bandwidth control is enabled or not.
	<b>Online Statistics</b> – Display an online statistics for quality of service for your reference
	<b>Setup</b> – Allow to configure general QoS setting for WAN interface.
Class Rule	<b>Index</b> – Display the class number that you can edit.
	<b>Name</b> – Display the name of the class.
	<b>Rule</b> – Allow to configure detailed settings for the selected Class.
	<b>Service Type</b> - Allow to configure detailed settings for the service type.
Enable the First Priority for VoIP SIP/RTP	When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority.
	<b>SIP UDP Port</b> - Set a port number used for SIP.



This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

## **Online Statistics**

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.

Randwidth Management >> Quality of Service						
WAN2 Online	Statistics		Refresh Interval: 5 💙 seconds			
Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)		
1	OUT	VoIP		0		
2	OUT		25%	0		
3	OUT		25%	0		
4	OUT		25%	0		
5	OUT	Others	25%	0		
			ValP Others 0 5	10 (Bps)		
			Cancel			

### **General Setup for WAN Interface**

Bandwidth Management >> Quality of Service

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

VAN2 General Setup		
Enable the QoS Cor	ntrol OUT 💌	
WAN	Inbound Bandwidth	100000 Kbps
WAN	Outbound Bandwidth	100000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Band	width Control	Limited_bandwidth Ratio 25 %
Outbound TCP AC	X Prioritize	



Item	Description	
Enable the QoS Control	<ul> <li>The factory default for this setting is checked.</li> <li>Please also define which traffic the QoS Control settings will apply to.</li> <li>IN- apply to incoming traffic only.</li> <li>OUT-apply to outgoing traffic only.</li> <li>BOTH- apply to both incoming and outgoing traffic.</li> <li>Check this box and click OK, then click Setup link again.</li> <li>You will see the Online Statistics link appearing on this page.</li> </ul>	
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN2/WAN3. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.	
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN2/WAN3. For example, if your ADSL supports 1M o downstream and 256K upstream, please set 256kbps for thi box. The default value is 10000kbps.	
Reserved Bandwidth Ratio		
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.	
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.	
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.	

**Note:** The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

### Edit the Class Rule for QoS

1. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

General	Setup							Set	to Factory D	efault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Class Rule Index Name Rule Service Type							уре			
Clas	s 1							Edit		
Clas	s 2							Edit	Edit	
Clas	s 3							Edit		

Bandwidth Management >> Quality of Service

2. After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.

Class Ind	lex #1							
Name	Test			Tag packets as:	Default	*		
NO	Status	Local Address	Remote Address	DiffServ CodeP	oint Service Type			
1	Empty	-	-	-	-			
Add Edit Delete								
	OK Cancel							

Bandwidth Management >> Quality of Service

3. For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit				
	ACT			
	Ethernet Type	⊙ IPv4 ○ IPv6		
	Local Address	Any		Edit
	Remote Address	Any		Edit
	DiffServ CodePoint	ANY	*	
	Service Type	Predefined	*	
	Note: Please choose/setup the	e <u>Service Type</u> first.		
-		OK Cancel	]	

**Dray** Tek

Item	Description		
АСТ	Check this box to invoke these settings.		
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.		
Local Address	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.		
<b>Remote Address</b>	Click the <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.		
	🗿 http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer		
	Address Type     Subnet Address       Start IP Address     0.0.00       End IP Address     0.0.00       Subnet Mask     0.0.00		
	OK Close		
	Address Type – Determine the address type for the source address.		
	<ul><li>For Single Address, you have to fill in Start IP address.</li><li>For Range Address, you have to fill in Start IP address and End IP address.</li></ul>		
	For <b>Subnet Address</b> , you have to fill in Start IP address and Subnet Mask.		
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.		
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.		

Available settings are explained as follows:

4. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

ass Index	c #1					
ime Te	est			Tag packets as: Defau	lt	
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
10	Active	Any	Any	ANY	ANY	
2 🔿	Active	192.168.1.12	192.168.1.56	ANY	ANY	
Add Edit Delete						

## Edit the Service Type for Class Rule

1. To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

Bandwidth Management >> Quality of Service

General Setup Set to Factory Defi										
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN2	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

Class Rule			
Index	Name	Rule	Service Type
Class 1	Test	Edit	
Class 2		Edit	Edit
Class 3		<u>Edit</u>	

2. After you click the **Edit** link, you will see the following page.

Bandwidth Management >> Quality of Service

User Defined Service Type							
NO	Name	Protocol	Port				
1	Empty	-	-				
	Add Edit Delete						
		Cancel					

3. For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Name	
Service Type	TCP 🖌 6
Port Configuration	
Туре	💿 Single 🔿 Range
Port Number	0 - 0

Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	<ul> <li>Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.</li> <li>Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.</li> </ul>

5. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

## 3.9 Applications

Below shows the menu items for Applications.

Applications
Dynamic DNS
Schedule
RADIUS
Active Directory /LDAP
UPnP
IGMP
Wake on LAN
SMS/Mail Alert Service
VDN and Domoto Access

### 3.9.1 Dynamic DNS

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



Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three 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.

### Enable the Function and Add a Dynamic DNS Account

- 1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
- 2. In the DDNS setup menu, check Enable Dynamic DNS Setup.

Applications >> Dynamic DNS Setup

Dynamic DNS Se	tup	Set t	o Factory Default
🗹 Enable Dyna	amic DNS Setup	View Log	Force Update
Auto-Update ir	nterval 14400 Min(s) (1~14400)		
Accounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		х
<u>3.</u>	WAN1 First		х



Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display the WAN interface used.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



Applications >> D	vnamic DNS	Setup >> D	vnamic DNS	Account Setup
reppindent on the set of	1	ootap · · · D	J	noovune ootup

Enable Dynamic DNS	Account	
WAN Interface	WAN1 First 🐱	
Service Provider	dyndns.org (www.dyndns.org)	*
Service Type	Dynamic 💌	
Domain Name	chronic6653 dyndns.org	dyndns.org 💙
Login Name	chronic6653	(max. 64 characters)
Password	•••••	(max. 23 characters)
Wildcards		
Backup MX		
Mail Extender		
Force WAN IP	Update	

Item	Description	
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).	
WAN Interface	WAN1/WAN2/WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account. WAN1 First WAN1 First WAN1 Only WAN2 First WAN2 Only WAN3 First WAN3 Only	
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.	
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 (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.	



Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.	
Force WAN IP Update	When the IP address of the WAN interface in Vigor router is private IP, the system will detect the Public IP used by the router in front of Vigor router and use that Public IP to update DDNS server forcefully.	

4. Click **OK** button to activate the settings. You will see your setting has been saved.

### Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

### **Delete a Dynamic DNS Account**

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

### 3.9.2 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also 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.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Schedule:			Set to Factory Default
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	х
<u>2.</u>	х	<u>10.</u>	х
<u>3.</u>	х	<u>11.</u>	x
<u>4.</u>	х	<u>12.</u>	x
<u>5.</u>	х	<u>13.</u>	x
<u>6.</u>	х	<u>14.</u>	x
<u>7.</u>	х	<u>15.</u>	x
<u>8.</u>	х		

Applications >> Schedule

Status: v --- Active, x --- Inactive

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN** and **Remote Access** >> **LAN-to-LAN** settings.

To add a schedule:

- 1. Click any index, say Index No. 1.
- 2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

🗹 Enable	Schedule Setup	
	Start Date (yyyy-mm-dd)	2000 🗸 - 1 🔽 - 1 👻
	Start Time (hh:mm)	0 🕶 : 0 🕶
	Duration Time (hh:mm)	0 🕶 : 0 🕶
	Action	Force On
	Idle Timeout	0 minute(s).(max. 255, 0 for default)
	How Often	
	O Once	
	Weekdays	
	🗌 Sun 🗹 Mon 🗹	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🗌 Sat

Item	Description	
Enable Schedule Setup	Check to enable the schedule.	
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.	
Start Time (hh:mm)	Specify the starting time of the schedule.	
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.	
Action Specify which action Call Schedule should apply dependent of the schedule.		
	<b>Force On</b> -Force the connection to be always on.	
	Force Down -Force the connection to be always down.	
	<b>Enable Dial-On-Demand -</b> Specify the connection to be dial-on-demand and the value of idle timeout should be specified in <b>Idle Timeout</b> field.	
	<b>Disable Dial-On-Demand -</b> Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.	
Idle Timeout	Specify the duration (or period) for the schedule.	
	How often -Specify how often the schedule will be applied Once -The schedule will be applied just once	
	<b>Weekdays</b> -Specify which days in one week should perform the schedule.	



3. Click **OK** button to save the settings.

### Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).



- 1. Make sure the PPPoE connection and **Time Setup** is working properly.
- 2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- 3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

### **3.9.3 RADIUS**

Applications >> RADIUS

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

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

Enable	
Server IP Address	
Destination Port 1812	
Shared Secret	
Confirm Shared Secret	

Item	Description
Enable	Check to enable RADIUS client feature.
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. The maximum length of the shared secret you can set is 36 characters.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

After finished the above settings, click **OK** button to save the settings.

## 3.9.4 LDAP /Active Directory Setup

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.

### **General Setup**

This page allows you to enable the function and specify general settings for LDAP server.

General Setup	Active Directory / LDAP Profiles	
Enable		
Bind Type		Simple Mode
Server Addre	ess	
Destination (	Port	389
Use SSL		
Regular DN		
Regular Pass	word	
		OK Cancel

Applications >> Active Directory /LDAP



Item	Description	
Enable	Check to enable such function.	
Bind Type	There are three types of bind type supported.          Simple Mode         Simple Mode         Anonymous         Regular Mode	
	<b>Simple Mode</b> – Just simply do the bind authentication without any search action.	
	<b>Anonymous</b> – Perform a search action first with Anonymous account then do the bind authentication.	
	<b>Regular Mode</b> – Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.	
	For the regular mode, you'll need to type in the <b>Regular DN</b> and <b>Regular Password</b> .	
Server IP Address	Enter the IP address of LDAP server.	
Destination Port	Type a port number as the destination port for LDAP server.	
Use SSL	Check the box to use the port number specified for SSL.	
Regular DN	Type this setting if <b>Regular Mode</b> is selected as <b>Bind Type.</b>	
Regular Password	Specify a password if <b>Regular Mode</b> is selected as <b>Bind</b> <b>Type.</b>	

Available settings are explained as follows:

After finished the above settings, click **OK** button to save the settings.

## Profiles

You can configure eight AD/LDAP profiles. These profiles would be used with User Management for different purposes in management.

Applications >> Active Directory /LDAP

Active Directory /LDA	2	Set to Factory Default
General Setup	Active Directory / LDAP Profiles	
Index	Name	Distinguished Name
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		
		LDAP for VPN authentication, you'll have to check the Remote Access PPP General Setup"

Click any index number link to open the following page.

Applications >>	∆ctive.	Directory	/LDAP>>Server	Profiles
Applications	Active	Directory	EDAI ** SCIVCI	1 1011103

Imp	
Vpn	
uid	
ou=People,dc=ms,dc=draytek,dc=com	9
gidNumber=500	
filter for BaseDN search request.	
cn=vpn,ou=Group,dc=ms,dc=draytek,dc=com	<u>S</u>
OK Cancel	
	ou=People,dc=ms,dc=draytek,dc=com gidNumber=500 filter for BaseDN search request. cn=vpn,ou=Group,dc=ms,dc=draytek,dc=com

Item	DescriptionType a name for such profile. The length of the use name is limited to 19 characters.	
Name		
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".	



Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the substant button to list all the account information on the AD/LDAP Server to assist you finish the setup.	
Additional Filter	This is an optional setting.	

After finished the above settings, click **OK** to save and exit this page. A new profile has been created.

For detailed information about LDAP application, refer to section 4.7 How to Implement the AD/LDAP Authentication for User Management?

## 3.9.5 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.

Applications >> UPnP

JPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK	Clear	Cancel
----	-------	--------

Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the <b>Connection Control</b> <b>Service</b> or <b>Connection Status Service</b> .

After setting **Enable 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.

iress 🔕 Network Connections	Broadband	🐮 IP Broadband Connection o	n Router Status
Network Tasks (8) Create a new connection Set up a home or small office network	hinet Disconnected WAIN Miniport (PPPOE) Dial-up	General Internet Gateway Status:	Connected
ee Also 🔅	test Disconnected DrayTek.ISDN PPP	Duration: Speed: Activity	00:19:06 100.0 Mbps
Other Places <ul> <li>Control Panel</li> <li>My Network Places</li> </ul> <ul> <li>Angel</li> <li>My Network Places</li> </ul> <ul> <li>Angel</li> </ul> <li>Angel</li>	Internet Gateway IP Broadband Connection on Router Enabled	Internet Internet Gate	🔊
My Documents Wy Computer	LAN or High-Speed Internet	Sent: 404 Received: 1,115 Properties Disable	734 666
Details (*) Network Connections System Folder	Local Area Connection Enabled Realtek RTL8139/810x Family	Properties Disable	Close

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 chared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>☑ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>☑ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>☑ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>
Settings	

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.

## 3.9.6 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications	>> IGMP						
IGMP							
Enable IG	MP Proxy W	/AN1 👻					
	(y is to act as a multic is any multicast group.						
Enable IG	MP Snooping MP Snooping, multicast MP snooping, multicast						group.
		04	< C;	ancel			
							Refresh
Working Mul	ticast Groups						
Index	Group ID	P1	P2	P3	P4	P5	P6

Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P6	It indicates the LAN port used for the multicast group.

After finishing all the settings here, please click **OK** to save the configuration.

## 3.9.7 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** (WOL) 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.

Application >> Wake on LAN

wake up throug	LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs can h IP.
Wake by:	MAC Address 🗸
IP Address:	🐦
MAC Address:	: : : : : Wake Up!
Result	

Item	Description
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.         Wake by:       MAC Address >         MAC Address       IP Address         IP Address       IP Address
IP Address	The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the bound PCs.
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

#### Application >> Wake on LAN

#### Wake on LAN

Wake by:	MAC Address 🗸
IP Address:	💙
MAC Address:	Wake Up!
Result	

## 3.9.8 SMS / Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

### **SMS** Provider

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

SMS Provider	Mail Server		<u> </u>	Set to Factory Default
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 🔽	1 - Line_down 💌		1 - Notify_attack 💌	
2	1 - Line_down 🗸		1 - Notify_attack 🗸	
3	1 - Line_down 💌		1 - Notify_attack 💌	
4	1 - Line_down 💙		1 - Notify_attack 💙	
5 🗌	1 - Line_down 💌		1 - Notify_attack 💌	
6	1 - Line_down 💙		1 - Notify_attack 🗸	
7 🗌	1 - Line_down 🗸		1 - Notify_attack 🗸	
8	1 - Line_down 💙		1 - Notify_attack 💙	
9 🔲	1 - Line_down 💌		1 - Notify_attack 💌	
10 🔲	1 - Line_down		1 - Notify_attack 💙	
1				

Application >> SMS / Mail Alert Service

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click <b>SMS Provider</b> link to define the SMS server.

Cancel



OK

Recipient	Type the name of the one who will receive the SMS.
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the SMS.
Schedule	Type the schedule number that the SMS will be sent out. You can click the <b>Schedule(1-15)</b> link to define the schedule.

After finishing all the settings here, please click **OK** to save the configuration.

### **Mail Server**

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

SMS Provider	Mail Server	<u> </u>	<u> </u>	Set to Factory Defa
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - Mail_Notify 💙		1 - Notify_attack 💌	
2 🗆	1 - Mail_Notify 🗸		1 - Notify_attack 🗸	
3 🗌	1 - Mail_Notify 💙		1 - Notify_attack	
4	1 - Mail_Notify 💙		1 - Notify_attack 💙	
5 🗌	1 - Mail_Notify 💙		1 - Notify_attack 💙	
6	1 - Mail_Notify 💙		1 - Notify_attack 💙	
7 🗌	1 - Mail_Notify 🗸		1 - Notify_attack 🗸	
8	1 - Mail_Notify 💙		1 - Notify_attack 👻	
9 🗌	1 - Mail_Notify 💌		1 - Notify_attack 👻	
10 🗆	1 - Mail_Notify 🗸		1 - Notify_attack 💌	

Cancel

OK

Application >> SMS / Mail Alert Service

Item	Description
Index	Check the box to enable such profile.
Mail Service	Use the drop down list to choose mail service provider. You can click <b>Mail Service</b> link to define the mail server.
Recipient	Type the e-mail address of the one who will receive the notification message.
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the mail message.

Schedule	Type the schedule number that the notification will be sent out.
	You can click the <b>Schedule(1-15)</b> link to define the schedule.

After finishing all the settings here, please click **OK** to save the configuration.

## 3.10 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

### 3.10.1 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 (from server to client) step by step.

1. Open VPN and Remote Access>>VPN Client Wizard. The following page will appear.

Route Mode 💌
[Index] [Status] [Name]
elect Route Mode. single client or ip and is not configured to route the

# **Dray** Tek

Available settings	are	explained	as	follows:	
--------------------	-----	-----------	----	----------	--

Item	Description		
LAN-to-LAN Client Mode Selection	Choose the client mode. <b>Route Mode/NAT Mode</b> – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode. Route Mode <u>Route Mode</u> NAT Mode		
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set. $\begin{bmatrix} Index \end{bmatrix} \begin{bmatrix} Status \end{bmatrix} \begin{bmatrix} Name \end{bmatrix} \land \\ 1 & x & ??? \\ 2 & x & ??? \\ 3 & x & ??? \\ 3 & x & ??? \\ 4 & x & ??? \\ 5 & x & ??? \\ 6 & x & ??? \\ 6 & x & ??? \\ 7 & x & ??? \\ 8 & x & ??? \\ 9 & x & ??? \\ 10 & x & ??? \\ 10 & x & ??? \\ 11 & x & ??? \\ 12 & x & ??? \\ 12 & x & ??? \\ 13 & x & ??? \\ 14 & x & ??? \\ 15 & x & ??? \\ 15 & x & ??? \\ 16 & x & ??? \\ 16 & x & ??? \\ 17 & x & ??? \\ 18 & x & ??? \\ 19 & x & ??? \\ 19 & x & ??? \\ 20 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 25 & x & ??? \\ 26 & x & ??? \\ 28 & x & ??? \\ 29 & x & ??? \\ 27 & x & ??? \\ 29 & x & ??? \\ 29 & x & ??? \\ 27 & x & ??? \\ 29 & x & ??? \\ 29 & x & ??? \\ 20 & x & ??? \\ 20 & x & ??? \\ 20 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 27 & x & ??? \\ 28 & x & ??? \\ 29 & x & ??? \\ 29 & x & ??? \\ 21 & x & ??? \\ 21 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 27 & x & ??? \\ 28 & x & ??? \\ 29 & x & ??? \\ 20 & x & ??? \\ 21 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 25 & x & ??? \\ 27 & x & ??? \\ 28 & x & ??? \\ 29 & x & ??? \\ 20 & x & ??? \\ 20 & x & ??? \\ 20 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 25 & x & ??? \\ 25 & x & ??? \\ 26 & x & ??? \\ 27 & x & ??? \\ 27 & x & ??? \\ 28 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 25 & x & ??? \\ 25 & x & ??? \\ 26 & x & ??? \\ 27 & x & ??? \\ 27 & x & ??? \\ 21 & x & ??? \\ 22 & x & ??? \\ 23 & x & ??? \\ 24 & x & ??? \\ 25 & x & ??? \\ 27 & x & ??? \\ 21 & x & ??$		

2. When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

security ranking (1 is the highest; 5 is the lowe	est) Throughput ranking (1 is the highest; 5 is the lowest)
1. L2TP over IPsec	1. PPTP (None Encryption)
2. IPsec	2. L2TP
<ol><li>PPTP (Encryption)</li></ol>	3. IPsec
4. L2TP	<ol><li>L2TP over IPsec</li></ol>
<ol><li>PPTP (None Encryption)</li></ol>	<ol><li>PPTP (Encryption)</li></ol>
	PPTP (Encryption) IPsec L2TP L2TP over IPsec (Nice to Have) L2TP over IPsec (Must)

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

**Note:** The following descriptions for VPN Type are based on the **Route Mode** specified in **LAN-to-LAN Client Mode Selection.** 

• When you choose **PPTP** (**None Encryption**) or **PPTP** (**Encryption**), you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP Encryption Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0
]	
	< Back Next > Finish Cancel

## • When you choose **IPSec**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

rofile Name	???
/PN Dial-Out Through	WAN1 First
Always on	
erver IP/Host Name for VPN e.g. draytek.com or 123.45.67.89) KE Authentication Method	
Pre-Shared Key	
Confirm Pre-Shared Key	
<ul> <li>Digital Signature (X.509)</li> </ul>	
Peer ID	None 🗸
Local ID	
Iternative Subject Name First	
🔿 Subject Name First	
Local Certificate	None 🗸
Psec Security Method Medium (AH)	
O High (ESP)	DES without Authentication
Remote Network IP	0.0.0.0
emote Network Mask	255.255.255.0

### • When you choose **L2TP**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP Settings		
Profile Name	???	
VPN Dial-Out Through	WAN1 First	
Always on		
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)		
Username	???	
Password		
Remote Network IP	0.0.0.0	
Remote Network Mask	255.255.255.0	
	< Back Next > Finish Cance	

**Dray** Tek

• When you choose L2TP over IPSec (Nice to Have) or L2TP over IPSec (Must), you will see the following graphic:

ofile Name	VPN-2
PN Dial-Out Through	WAN1 First 🗸
Always on	
erver IP/Host Name for VPN .g. draytek.com or 123.45.67.89)	
E Authentication Method	
Interstate Pre-Shared Key	••••
Confirm Pre-Shared Key	•••••
<ul> <li>Digital Signature (X.509)</li> </ul>	
Peer ID	None 🗸
Local ID	
Iternative Subject Name First	
🔘 Subject Name First	
Local Certificate	None
sec Security Method Medium (AH)	
O High (ESP)	DES without Authentication
sername	???
assword	
emote Network IP	0.0.0.0
emote Network Mask	255.255.255.0

VPN and Remote Access >> VPN Client Wizard

Item	Description		
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.		
VPN Dial-Out Through	Inimed to To characters.         Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.         WAN1 First         WAN1 First         WAN1 Only         WAN2 First         WAN2 Only         WAN1 Only: Backup WAN2         WAN2 Only: Backup WAN1         WAN3 First         WAN3 Only         WAN1 First/ WAN2 First / WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for VPN connection. If		
	WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.		
	WAN1 Only /WAN2 Only/WAN 3 Only- While connecting, the router will use WAN1/WAN2/WAN3 as		



	the only channel for VPN connection. <b>WAN1 Only: Backup WAN2/WAN2 Only: Backup</b> <b>WAN1</b> - While connecting, the router will use WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 fails, the router will use backup WAN2/backup WAN1 interface instead.
Always On	Check to enable router always keep VPN connection.
Pre-Shared Key	<ul> <li><b>IKE Authentication Method</b> usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.</li> <li><b>Pre-Shared Key-</b> Specify a key for IKE authentication.</li> </ul>
	Confirm Pre-Shared Key-Confirm the pre-shared key.
Digital Signature (X.509)	Click <b>Digital Signature</b> to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local Certificate.</b> Otherwise, the setting you choose here will not be effective.
	<b>Peer ID</b> – Choose the peer ID selection from the drop down list.
	Local ID – Choose Alternative Subject Name First or Subject Name First.
IPSec Security Method	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above. The length of the use name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above. The length of the password is limited to 11 characters.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

Please confirm your settings	
LAN-to-LAN Index:	20
Profile Name:	VPN-2
VPN Connection Type:	L2TP over IPsec (Nice to Have)
VPN Dial-Out Through:	WAN1 First
Always on:	No
Server IP/Host Name:	172.16.3.8
IKE Authentication Method:	Pre-Shared Key
IPsec Security Method:	AH-SHA1
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0
	ecessary. Otherwise, click Finish to save the current settings and
proceed to the following action:	
	O to the VPN Connection Management.
	O Do another VPN Client Wizard setup.
	View more detailed configurations.
	-
	< Back Next > Finish Cancel

VPN and Remote Access >> VPN Client Wizard

Item	Description
Go to the VPN Connection Management	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;LAN to LAN</b> for viewing detailed configuration.

## 3.10.2 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 (from client to server) step by step.

1. Open VPN and Remote Access>>VPN Server Wizard. The following page will appear.

PN and Remote Access >> VPN Server Wizard		
hoose VPN Establishment Environment		
VPN Server Mode Selection:	Remote Dial-in User (Teleworker)	
Please choose a LAN-to-LAN Profile:	2 x ??? v	
Please choose a Dial-in User Accounts:	2 x ??? 🗸	
Allowed Dial-in Type:	_	
	■ PPTP ✓ IPsec	
	L2TP with IPsec Policy None	
	< Back Next > Finish	Cance

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. <b>Site to Site VPN</b> – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. <b>Remote Dial-in User</b> –You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. Site to Site VPN (LAN-to-LAN) Site to Site VPN (LAN-to-LAN) Remote Dial-in User (Teleworker)
Please choose a LAN-to-LAN Profile	This item is available when you choose <b>Site to Site VPN</b> (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.

	[Index]	[Status]	[Name]	~	
	1	х	???	ī	
	2 3	X	???		
	4	x	???		
	4 5 6	x	???		
	7	x x	777 777		
	8	x	???		
	9	x	???		
	10	x x	777 777		
	12	x	???		
	13	х	???		
	14	x x	??? ???		
	16	x	???		
	17	х	???		
	18	x	??? ???		
	20	x x	222		
	21	x	???		
	22	x	???		
	23	x x	777 777		
	25	x	???		
	26	х	???	_	
	27 28	x x	777 777		
	29	x	???	¥	
Please choose a	This item i	is available v	when you	cho	oose Remote Dial-in
Dial-in User					node. There are 32 VPN
Accounts		users to set.		1 11	iode. There are 52 virit
Allowed Dial-in Type			-		ose any one of dial-in
		-			e to select suitable
	. –		_		ile. There are several
	types prov	ided here (si	milar to V	PN	Client Wizard).
	V PPT	D			
	🗹 IPSe	9C			
	🗹 L2TF	P with IPSe	c Policy	N	one 🚩
					one
					ce to Have
				Μ	ust
	Different I	Dial-in Type	will lead	to c	lifferent configuration
		• •			for each dial-in type will
					erver Mode (Site to Site
		Remote Dial			
			i in Oser)	SCI	

2. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made.

Here we take the examples of choosing **Remote-Dial-in User** as the **VPN Server Mode**.



• When you check **PPTP**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

PPTP / L2TP / L2TP over IPsec Authentica	ation
Jsername	???
Password	
Authentication Type	Local User Database 💌
Peer IP/VPN Client IP	

• When you check **PPTP & IPSec & L2TP** (three types) or **PPTP&IPSec** (two types) or **L2TP with Policy** (**Nice to Have/Must**), you will see the following graphic:

??? Local User Database	
Local User Database	
Local User Database	
	~
None	~
	None

VPN and Remote Access >> VPN Server Wizard

## • When you check **IPSec**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

IPsec / L2TP over IPsec Authentication			
Pre-Shared Key			
Confirm Pre-Shared Key			
Digital Signature (X.509)			
Peer ID	None	~	
Peer IP/VPN Client IP			
Peer ID			

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPSec/L2TP IPSec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local</b> <b>Certificate.</b> Otherwise, the setting you choose here will not be effective.
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client. The length of the name is limited to 47 characters.



Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

3. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

VPN and Remote Access >> VPN Server Wizard

Please Confirm Your Settings	
VPN Environment:	Remote Access VPN (Host-to-LAN)
Index:	2
Username:	???
Authentication Type:	Local User Database
Allowed Service:	IPsec
Peer IP/VPN Client IP:	192.168.1.100
Peer ID:	David
	Go to the VPN Connection Management.
	<ul> <li>Do another VPN Server Wizard setup.</li> </ul>
	View more detailed configurations.
	< Back Next > Finish Cancel

Item	Description
Go to the VPN Connection Management	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access <b>VPN and Remote</b> Access>>LAN to LAN for viewing detailed configuration.

## 3.10.3 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 of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

emote Access	Control Setup	
	<b>~</b>	Enable PPTP VPN Service
	✓	Enable IPSec VPN Service
	$\checkmark$	Enable L2TP VPN Service
	$\checkmark$	Enable SSL VPN Service
		Enable OpenVPN Service

ОК	Clear	Cancel
----	-------	--------

After finishing all the settings here, please click **OK** to save the configuration.

## 3.10.4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

PPP General Setup				
PPP/MP Protocol		LDAP Server Profiles for PPP Authentication		
Dial-In PPP Authentication	PAP or CHAP			PPTP LDAP Profile
Dial-In PPP Encryption (MPPE)	Optional MPPE		*	
Mutual Authentication (P	AP)	🔘 Yes 💿 No		
Username				
Password	Password			
IP Address Assignment for Dial-In Users (When DHCP Disable set)				
Assigned IP start	LAN 1	192.168.1.200		
	LAN 2	192.168.2.200		
	LAN 3	192.168.3.200		
	LAN 4	192.168.4.200		
	LAN 5	192.168.5.200		
	LAN 6	192.168.6.200		

VPN and Remote Access >> PPP General Setup

OK

Item	Description	
Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.	



	<b>PAP or CHAP</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.		
<b>Dial-In PPP Encryption</b> (MPPE)	<b>Optional MPPE</b> - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.		
	Optional MPPE Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit)		
	<b>Require MPPE (40/128bits) -</b> Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.		
	<b>Maximum MPPE -</b> This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.		
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.		
Assigned IP Start	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.		
	You can configure up to four start IP addresses for LAN1 ~ LAN6.		
LDAP Server Profiles for PPP Authentication	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.		
	However, if there is no profile listed, simply click the link of <b>PPTP LDAP Profile</b> to create/add some new LDAP profiles you want.		
	For detailed information about LDAP application, refer to section <b>4.7 How to Implement the AD/LDAP</b> Authentication for User Management?		

## 3.10.5 IPSec General Setup

In IPSec General Setup, there are two major parts of configuration.

There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN IKE/IPsec General Setup	
Dial-in Set up for Remote Dial-in users and $D_{Y}$	namic IP Client (LAN to LAN).
IKE Authentication Method	
Certificate for Dial-in	None 💌
Pre-Shared Key	
Pre-Shared Key	
Confirm Pre-Shared Key	
IPsec Security Method	
Medium (AH)	
Data will be authentic, but will no	t be encrypted.
High (ESP) ☑ DES ☑ 3DES Data will be encrypted and auther	☑ AES
	OK Cancel

Available settings are explained as follows:

VPN and Remote Access >> IPsec General Setup

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec



	and IPSec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, <b>Certificate (X.509)</b> and <b>Pre-Shared Key</b> .
	<b>Certificate for Dial-in</b> –Choose one of the local certificates from the drop down list.
	Pre-Shared Key- Specify a key for IKE authentication.
	<b>Confirm Pre-Shared Key-</b> Retype the characters to confirm the pre-shared key.
	Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.
<b>IPSec Security Method</b>	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High (ESP)</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

After finishing all the settings here, please click **OK** to save the configuration.

## 3.10.6 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

509 Peer ID Accounts:			Set to Factory Default		
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	Х	<u>17.</u>	???	Х
<u>2.</u>	???	Х	<u>18.</u>	???	х
<u>3.</u>	???	Х	<u>19.</u>	???	Х
<u>4.</u>	???	Х	<u>20.</u>	???	х
<u>5.</u>	???	Х	<u>21.</u>	???	Х
<u>6.</u>	???	Х	<u>22.</u>	???	х
<u>7.</u>	???	Х	<u>23.</u>	???	Х
<u>8.</u>	???	Х	<u>24.</u>	???	х
<u>9.</u>	???	Х	<u>25.</u>	???	Х
<u>10.</u>	???	Х	26.	???	х
<u>11.</u>	???	Х	<u>27.</u>	???	Х
<u>12.</u>	???	Х	<u>28.</u>	???	х
<u>13.</u>	???	Х	<u>29.</u>	???	Х
<u>14.</u>	???	Х	<u>30.</u>	???	х
<u>15.</u>	???	Х	<u>31.</u>	???	Х
<u>16.</u>	???	Х	<u>32.</u>	???	Х

VPN and Remote Access >> IPsec Peer Identity

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPSec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

#### VPN and Remote Access >> IPsec Peer Identity

Profile Index : 1		
Profile Name	???	
Enable this a	account	
O Accept Any P	leer ID	
O Accept Subje	ct Alternative Name	
Туре		IP Address
IP		
Domain Name		
E-Mail		
O Accept Subje	ct Name	
Country (C)		
State (ST)		
Location (L)		
Orginization (C	))	
Orginization Ur	nit (OU)	
Common Name	e (CN)	
Email (E)		
	ОК	Clear Cancel

Available settings are explained as follows:

Item	Description	
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.	
Enable this account	Check it to enable such account profile.	
Accept Any Peer ID	Click to accept any peer regardless of its identity.	
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be <b>IP</b> <b>Address, Domain,</b> or <b>E-mail Address</b> . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.	
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes <b>Country (C), State (ST), Location (L), Organization (O),</b> <b>Organization Unit (OU), Common Name (CN),</b> and <b>Email (E)</b> .	

After finishing all the settings here, please click **OK** to save the configuration.

## 3.10.7 OpenVPN General Setup

OpenVPN is a comprehensive SSL VPN software that combines OpenVPN server functions, enterprise management mechanism, simplified OpenVPN Connect User Interface and OpenVPN Client software package. It can work on Windows, Linux OS, and Macintosh operating system.

OpenVPN Access Server offers a wide range of configurations for remote access to private cloud network resources and/or internal network.

Note: Vigor2860 will support up to 10 simultaneous dial-in OpenVPN tunnels.

In general, there are two advantages of OpenVPN:

- OpenVPN can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-clients to connect to a single OpenVPN Server process over a single TCP or UDP port.

VPN and Remote Access >> OpenVPN General Setup

OpenVPN General Setup

Port	1194
Cipher Algorithm	AES128 ¥
HMAC Algorithm	SHA1 ¥
Certificate Authentication	

Note: OpenVPN on vigor only support UDP protocol and TUN device interface currently. So please setup corresponding configurations on the client side.

#### OK

Available settings are explained as follows:

Item	Description		
Port	Usually, the default UDP port number for OpenVPN is 1194.		
Cipher Algorithm	Two encryptions are supported, AES128 and AES256. AES128 AES256 NONE		
HMAC Algorithm	The HMAC algorithm only supports SHA1/SHA256. SHA1 SHA256 NONE		
Certificate Authentication	If certificate authentication is required for OpenVPN, simply check the box to apply the trusted CA certificate and local certificate for OpenVPN tunnel. Certificate authentication can offer more secure VPN tunnel between the client and the router.		

After finishing all the settings here, please click **OK** to save the configuration.



## 3.10.8 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	X		<u>17.</u>	???	×	
<u>2.</u>	???	×		<u>18.</u>	???	x	
<u>3.</u>	???	х		<u>19.</u>	???	Х	
<u>4.</u>	???	×		<u>20.</u>	???	х	
<u>5.</u>	???	х		<u>21.</u>	???	Х	
<u>6.</u>	???	х		<u>22.</u>	???	х	
<u>7.</u>	???	х		<u>23.</u>	???	х	
<u>8.</u>	???	х		<u>24.</u>	???	х	
<u>9.</u>	???	х		<u>25.</u>	???	х	
<u>10.</u>	???	×		<u>26.</u>	???	х	
<u>11.</u>	???	х		<u>27.</u>	???	х	
<u>12.</u>	???	х		<u>28.</u>	???	х	
<u>13.</u>	???	х		<u>29.</u>	???	х	
<u>14.</u>	???	×		<u>30.</u>	???	х	
<u>15.</u>	???	х		<u>31.</u>	???	х	
16.	???	×		32.	???	×	

VPN and Remote Access >> Remote Dial-in User

Available settings are explained as follows:

Item	Description		
Set to Factory Default	Click to clear all indexes.		
IndexClick the number below Index to access into the setting page of Remote Dial-in User.			
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.		
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.		

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> Remote Dial-in Use
---------------------------------------------

Index No. 1	
User account and Authentication Enable this account Idle Timeout 300 second(s)	Username ??? Password Enable Mobile One-Time Passwords(mOTP) PIN Code
Allowed Dial-In Type          Image: PPTP         IPsec Tunnel         SSL Tunnel         OpenVPN Tunnel         Specify Remote Node         Remote Client IP	Secret IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None
or Peer ID Netbios Naming Packet ③ Pass ③ Block Multicast via VPN ③ Pass ③ Block (for some IGMP,IP-Camera,DHCP Relayetc.) Subnet LAN 1 ♥ Assign Static IP Address 0.0.0	✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES Local ID (optional)
ОК	Clear Cancel

Item	Description		
User account and Authentication	<b>Enable this account</b> - Check the box to enable this function.		
	<b>Idle Timeout-</b> If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.		
Allowed Dial-In Type	<b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.		
	<b>IPSec Tunnel</b> - Allow the remote dial-in user to make an IPSec VPN connection through Internet.		
	<b>L2TP with IPSec Policy</b> - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:		
	• None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.		
	• Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in		



	VPN connection becomes one pure L2TP connection.
	• <b>Must</b> -Specify the IPSec policy to be definitely applied on the L2TP connection.
	<b>SSL Tunnel</b> – Allow the remote dial-in user to make an SSL VPN connection through Internet.
	<b>OpenVPN Tunnel -</b> Allow the remote dial-in user to make an OpenVPN connection through Internet.
	<b>Specify Remote Node -</b> You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).
	Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .
	Netbios Naming Packet -
	• <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
	<b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.
	<b>User Name</b> - This field is applicable when you select PPTF or L2TP with or without IPSec policy above. The length of the name is limited to 23 characters.
	<b>Password</b> - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The length of the password is limited to 19 characters.
	<b>Enable Mobile One-Time Passwords (mOTP) -</b> Check this box to make the authentication with mOTP function.
	<b>PIN Code</b> – Type the code for authentication (e.g, 1234).
	Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
Subnet	Chose one of the subnet selections for such VPN profile. Assign Static IP Address – Please type a static IP address for the subnet you specified.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.

	invoke this function and type in the required characters (1-63) as the pre-shared key.
	<b>Digital Signature (X.509)</b> – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer</b> <b>Identity.</b>
<b>IPSec Security Method</b>	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium-Authentication Header (AH) means data will be
	authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.
	<b>High-Encapsulating Security Payload (ESP)</b> means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
	<b>Local ID (Optional)-</b> Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

After finishing all the settings here, please click **OK** to save the configuration.

## 3.10.9 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router supports up to 32 VPN tunnels simultaneously. The following figure shows the summary table.

The following figure shows the summary table according to the item (All/Trunk) selected for **View**.

LAN-to-LAN	Profiles:					Set to	o Factory Default
View: 💿 A	ll 🔿 Trun	ık					
Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	???	х		<u>17.</u>	???	×	
<u>2.</u>	???	×		<u>18.</u>	???	Х	
<u>3.</u>	???	х		<u>19.</u>	???	×	
<u>4.</u>	???	Х		<u>20.</u>	VPN-2	V	offline
<u>5.</u>	???	х		<u>21.</u>	???	Х	
<u>6.</u>	???	×		<u>22.</u>	???	V	offline
<u>7.</u>	???	×		<u>23.</u>	???	Х	
<u>8.</u>	???	х		<u>24.</u>	???	х	
<u>9.</u>	???	х		<u>25.</u>	???	Х	
<u>10.</u>	???	×		<u>26.</u>	???	х	
<u>11.</u>	???	х		<u>27.</u>	???	х	
12.	???	×		<u>28.</u>	???	Х	
<u>13.</u>	???	Х		<u>29.</u>	???	Х	
<u>14.</u>	???	х		<u>30.</u>	???	х	
<u>15.</u>	???	Х		<u>31.</u>	???	Х	
<u>16.</u>	???	Х		<u>32.</u>	???	Х	

[XXXXXX:This Dial-out profile has already joined for VPN Load Balance Mechanism] [XXXXX:This Dial-out profile has already joined for VPN Backup Mechanism] [XXXXXX:This Dial-out profile does not join for VPN TRUNK]

The following shows profiles joined into VPN Load Balance and VPN Backup mechanism.

VPN	and	Remote	Access	>>	LAN	to	LAN

LAN-to-LAN Profiles:					
View: 🔘 All	Trunk				
Nam	ne	Activate	Members	Status	
Loadba	alan1	v	VPN-2	Offline	
			Connection	Offline	

[XXXXXX:This Dial-out profile has already joined for VPN Load Balance Mechanism] [XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism]

If there is no profile joined yet, this page will be shown as follows:

VPN and Remote Access >> LAN to LAN

#### LAN-to-LAN Profiles:

View: 🔘 All	Trunk			
Name	9	Activate	Members	Status

[XXXXXX:This Dial-out profile has already joined for VPN Load Balance Mechanism] [XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism]

Item	Description	
View	All – Click it to display the LAN to LAN profiles.	
	<b>Trunk</b> – Click it to display the Trunk profiles.	

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.
Active	<ul><li>V – means the profile has been enabled.</li><li>X – mans the profile has not been enabled.</li></ul>
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

VPN and Remote Access >> LAN to LAN

Profile Index : 1 1. Common Settings	
Profile Name     School       ✓     Enable this profile       VPN Dial-Out Through WAN1 First     ▼       Netbios Naming Packet        ● Pass        ● Block       Multicast via VPN        ● Pass        ● Block	Call Direction O Both O Dial-Out Dial-in Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP
(for some IGMP,IP-Camera,DHCP Relayetc.) 2. Dial-Out Settings	
Type of Server I am calling           Image: PPTP           IPsec Tunnel           L2TP with IPsec Policy	Username ??? Password PPP Authentication PAP/CHAP V VJ Compression © On © Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) Peer ID Local ID Alternative Subject Name First Subject Name First Local Certificate None IPsec Security Method Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in Schedule Setup: , , , , ,



Item	Description
Common Settings	<b>Profile Name</b> – Specify a name for the profile of the LAN-to-LAN connection.
	<b>Enable this profile -</b> Check here to activate this profile.
	<b>VPN Dial-Out Through -</b> Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.
	<ul> <li>WAN1 First</li> <li>WAN1 First</li> <li>WAN1 Only</li> <li>WAN2 First</li> <li>WAN2 Only</li> <li>WAN1 Only: Backup WAN2</li> <li>WAN2 Only: Backup WAN1</li> <li>WAN3 First</li> <li>WAN3 Only</li> </ul>
	<ul> <li>WAN1 First/ WAN2 First/ WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for VPN connection. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.</li> <li>WAN1 Only /WAN2 Only/WAN 3 Only- While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for VPN connection.</li> <li>WAN1 Only: Backup WAN2/WAN2 Only: Backup WAN1 - While connecting, the router will use WAN1/WAN2 only: Backup WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 fails, the router will use backup WAN2/backup WAN1 interface instead.</li> </ul>
	Netbios Naming Packet
	<ul> <li>Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</li> </ul>
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
	<b>Multicast via VPN -</b> Some programs might send multicast packets via VPN connection.
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.
	<b>Call Direction -</b> Specify the allowed call direction of this LAN-to-LAN profile.
	• <b>Both</b> :-initiator/responder
	• <b>Dial-Out</b> - initiator only

	• <b>Dial-In-</b> responder only.
	<b>Always On-</b> Check to enable router always keep VPN connection.
	<b>Idle Timeout:</b> The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
	<ul> <li>Enable PING to keep alive - This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.</li> </ul>
	<b>Enable PING to keep alive</b> is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router
	will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence o this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
	<b>PING to the IP -</b> Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
Dial-Out Settings	<b>Type of Server I am calling - PPTP</b> - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
	<b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.
	<b>L2TP with IPSec Policy -</b> Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
	• None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
	• Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.
	<b>Must:</b> Specify the IPSec policy to be definitely applied on the L2TP connection.
	<b>User Name -</b> This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. The length of the name is limited to 49 characters.
	<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The length of the password is limited to 15 characters
	the password is limited to 15 characters.



select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
<b>VJ compression -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to <b>Yes</b> to improve bandwidth utilization.
<b>IKE Authentication Method -</b> This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.
• <b>Pre-Shared Key</b> - Input 1-63 characters as pre-shared key.
• Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.
<b>Peer ID</b> - Select one of the predefined Profiles set in <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity.</b>
<b>Local ID</b> – Specify a local ID (Alternative Subject Name First or Subject Name First) to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
• Local Certificate – Select one of the profiles set in Certificate Management>>Local Certificate.
<b>IPSec Security Method -</b> This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
• Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.
• High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:
• <b>DES without Authentication</b> -Use DES encryption algorithm and not apply any authentication scheme.
• <b>DES with Authentication-</b> Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
• <b>3DES without Authentication</b> -Use triple DES encryption algorithm and not apply any authentication scheme.
• <b>3DES with Authentication-</b> Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
• <b>AES without Authentication</b> -Use AES encryption algorithm and not apply any authentication scheme.
• <b>AES with Authentication-</b> Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.

KE advanced settings			
KE phase 1 mode	Main mod	le	O Aggressive mode
KE phase 1 proposal	Auto		
KE phase 2 proposal	HMAC_SHAT/HMAC_MD5		
KE phase 1 key lifetime	28800	(900 ~ \$6400)	
KE phase 2 key lifetime	3600	(600 ~ 86400)	
erfect Forward Secret	Disable		O Enable
ocal ID			

OK Close

**IKE phase 1 mode -**Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

- **IKE phase 1 proposal-**To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
- **IKE phase 2 proposal-**To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
- **IKE phase 1 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
- **IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.
- **Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

**Local ID-**In **Aggressive** mode, Local 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.

**Index(1-15)** - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this field is blank and the function will always work.



_			
3.	Dia	I-In	Settings

3. Dial-In Settings		
Allowed Dial-In Type		Username ???
✓ РРТР		Password
IPsec Tunnel		VJ Compression  On Off
L2TP with IPsec Poli	cy None 🖌	
_		IKE Authentication Method
Specify Remote VPN	Gateway	Pre-Shared Key
Peer VPN Server IP		IKE Pre-Shared Key
		Digital Signature(X.509)
or Peer ID		None 🗸
		Local ID
		Alternative Subject Name First
		🔘 Subject Name First
		IPsec Security Method
		Medium(AH)
		High(ESP) 🗹 DES 🗹 3DES 🗹 AES
4. Gre over IPsec Settings		
Enable IPsec Dial-Out	t function GRE over IPs	ec
Logical Traffic	My GRE IP	Peer GRE IP
5. TCP/IP Network Settings	;	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, youhave to do
Remote Network IP	0.0.0.0	Route 💌
Remote Network Mask	255.255.255.0	Change default route to this VPN tunrel ( Only
Local Network IP	192.168.1.1	single WAN supports this )
Local Network Mask	255.255.255.0	
	More	
	ОК	Clear Cancel

Item	Description
Dial-In Settings	Allowed Dial-In Type - Determine the dial-in connection with different types.
	• <b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
	• <b>IPSec Tunnel-</b> Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
	• L2TP with IPSec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
	None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
	■ Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the

	dial-in VPN connection becomes one pure L2TP connection.
	Must - Specify the IPSec policy to be definitely applied on the L2TP connection.
addr same box.	<b>cify Remote VPN Gateway -</b> You can specify the IP ess of the remote dial-in user or peer ID (should be the e with the ID setting in dial-in type) by checking the Also, you should further specify the corresponding rity methods on the right side.
selec	bu uncheck the checkbox, the connection type you of above will apply the authentication methods and rity methods in the general settings.
or L2	<b>Name -</b> This field is applicable when you select PPTP 2TP with or without IPSec policy above. The length of name is limited to 11 characters.
or L2	<b>word -</b> This field is applicable when you select PPTP 2TP with or without IPSec policy above. The length of password is limited to 11 characters.
proto	Compression - VJ Compression is used for TCP/IP bool header compression. This field is applicable when select PPTP or L2TP with or without IPSec policy ve.
appli when only you	Authentication Method - This group of fields is icable for IPSec Tunnels and L2TP with IPSec Policy n you specify the IP address of the remote node. The exception is Digital Signature (X.509) can be set when select IPSec tunnel either with or without specify the IP ess of the remote node.
•	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
•	<b>Digital Signature (X.509)</b> –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the <b>VPN and Remote</b> <b>Access &gt;&gt;IPSec Peer Identity</b> .
	Local ID – Specify which one will be inspected first.
	<ul> <li>Alternative Subject Name First – The alternative subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
	<ul> <li>Subject Name First – The subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
IPSe	<b>ec Security Method -</b> This group of fields is a must for the compared to the
•	<b>Medium-</b> Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active



this option is active.

	• <b>High-</b> Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Gre over IPSec Settings	<b>Enable IPSec Dial-Out function GRE over IPSec</b> : Check this box to verify data and transmit data in encryption with GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.
	Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.
	<b>My GRE IP</b> : Type the virtual IP for router itself for verified by peer.
	<b>Peer GRE IP</b> : Type the virtual IP of peer host for verified by router.
TCP/IP Network Settings	My WAN IP –This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TF <b>Remote Gateway IP -</b> This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPI IP address is fixed by remote side, specify the fixed IP
	address here. Do not change the default value if you do not select PPTP or L2TP.
	<b>Remote Network IP/ Remote Network Mask -</b> Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
	<b>Local Network IP / Local Network Mask -</b> Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.
	More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

-	LAN-to-LAN Profile - Windows Internet Explorer  http://192.168.1.1/doc//2LMRt.htm
	Profile Index :1
	Remote Network
	Network IP
	Netmask
	255.255.255.255 / 32 💌
	Add Delete Edit
	OK Close
	<b>IP Direction -</b> The option specifies the direction of RI
	Routing Information Protocol) packets. You can
	hable/disable one of direction here. Herein, we provide
	our options: TX/RX Both, TX Only, RX Only, and
)	isable.
F	rom first subnet to remote network, you have t
	<b>o</b> - If the remote network only allows you to dial in wi
	ngle IP, please choose NAT, otherwise choose Route.
	hange default route to this VPN tunnel - Check this
J	change the default route with this VPN tunnel.

2. After finishing all the settings here, please click **OK** to save the configuration.

## 3.10.10 VPN TRUNK Management

VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPSec, and Binding tunnel policy.

## Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- > The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network
- Mail Alert support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Syslog support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

## Features of VPN TRUNK – VPN Load Balance Mechanism

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.

- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and GRE over IPSec
- > The web page is simple to understand and easy to configure
- The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably



ackup Profile List		Set to Factory De	efaul
Note: [Active:NO] 1	he LAN-to-LAN Profile is disabled or u	nder Dial-In(Call Direction) at present.	
No. Status Name	Memberl (Active) Type	Member2(Active)Type	
Advanced v	ict	Set to Factory De	ofaul
	The LAN-to-LAN Profile is disabled or u		eraur
No. Status Name	Memberl (Active) Type	Member2(Active)Type	
Advanced			
eneral Setup			
Status	Inable ○ Disable		
Profile Name			
Member1	Please select a LAN-to-LAN Dia	1-Out profile.	~

Member1	Please select a LAN-to-LAN Dial-Out profile.	۷
Member2	Please select a LAN-to-LAN Dial-Out profile.	۷
Active Mode	● Backup ○ Load Balance	

Add Edit Delete

Item	Description
Backup Profile List	<b>Set to Factory Default -</b> Click to clear all VPN TRUNK-VPN Backup mechanism profile.
	<b>No</b> – The order of VPN TRUNK-VPN Backup mechanism profile.
	<b>Status</b> - "v" means such profile is enabled; "x" means such profile is disabled.
	<b>Name -</b> Display the name of VPN TRUNK-VPN Backup mechanism profile.
	<b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
	<b>Type -</b> Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.

	Member2 - Display the dial-out profile selected from the
	Member2 drop down list below.
	Advanced – This button is available only when LAN to LAN profile (or more) is created.
	VPN Backup Advance Settings - Windows Internet Explorer  Nttp //192.168.1.1/doc/vpntbak.htm  VPN Backup Advance Settings
	Profile Name: Backup1 ERD Mode: O Normal Resume (Member 1 first) Detail Information: Environment Recovers Detection (ERD) Status: Normal Mode
	OK Close
	Detailed information for this dialog, see later section - Advanced Load Balance and Backup.
Load Balance Profile List	<b>Set to Factory Default -</b> Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.
	<b>No</b> - The order of VPN TRUNK-VPN Load Balance mechanism profile.
	<b>Status</b> - "v" means such profile is enabled; "x" means such profile is disabled.
	<b>Name -</b> Display the name of VPN TRUNK-VPN Load Balance mechanism profile.
	<b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
	<b>Type -</b> Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.
	<b>Member2 -</b> Display the dial-out profile selected from the Member2 drop down list below.
	Advanced – This button is only available when there is one or more profiles created in this page.

🖉 VPN Load Balance Advance Settings - Windows Internet Explorer
VPN Load Balance Advance Settings Profile Name: Loadbalan1 Load Balance Algorithm: © Round Robin © Weighted Round Robin
VPN Load Balance Policy © Edit © Insert after Tunnel Bind Table Index: (1~64)
Tunnel Bind Table Index: (1~64) Active: Active Binding Dial Out Profile: 20 v
Src IP Start:         0.0.0         End:         255 255 255           Dest IP Start:         0.0.0         End:         255 255 255
Dest Port Start: 1 End: 65535
Protocol:
OK Close
Detail Information [VFN Load Balance Profile name: Loadbalan1 ]
[Algorithm: Round Robin ]
Detailed information for this dialog, see later section -
Advanced Load Balance and Backup.
<b>Profile Name</b> - Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields. The length of the name is limited to 11 characters.
Member 1/Member2 - Display the selection for
LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >> LAN-to-LAN) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.
• No - Index number of LAN-to-LAN dial-out profile.
• Name - Profile name of LAN-to-LAN dial-out profile
• <b>Connection Type</b> - Connection type of LAN-to-LAN dial-out profile.
• VPN ServerIP (Private Network) - VPN Server IP of LAN-to-LAN dial-out profiles.
Active Mode - Display available mode for you to choose. Choose Backup or Load Balance for your router.
Add - Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in red. VPN TRUNK –
VPN Load Balance mechanism profile will be locked. The



profiles in LAN-to-LAN will be displayed in blue.	
<b>Edit -</b> Click this button to save the changes to the <b>Status</b> (Enable or Disable), profile name, member1 or member2.	
Delete - Click this button to delete the selected VPN	
TRUNK profile. The corresponding members	
(LAN-to-LAN profiles) grouped in the deleted VPN	
TRUNK profile will be released and that profiles in	
LAN-to-LAN will be displayed in black.	

## Time for activating VPN TRUNK – VPN Backup mechanism profile

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

## Time for activating VPN TRUNK – VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

# Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

# How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

- First of all, go to VPN and Remote Access>>LAN-to-LAN. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup /Load Balance mechanism profile management well.
- 2. Access into VPN and Remote Access>>VPN TRUNK Management.
- Set one group of VPN TRUNK VPN Backup/Load Balance mechanism backup profile by choosing Enable radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click Add at last.

ieneral Setup	
Status	© Enable C Disable
Profile Name	071023
Member1	Please choose the combination that you want.
Member2	Please choose the combination that you want.
Attribute Mode	Please choose the combination that you want.       No. <name> <connection-type>        1 To-A PlaceIPSec       2 To-B Site IPSec       192.168.2.25(20.20.20.0)</connection-type></name>
	Add Edit Delete

4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup/Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

View: 🧕	All 🛛 🔿 Trunk		
Index	Name	Active	Status
<u>1.</u>	To-A Place	V	offline
<u>2.</u>	To-B Site	V	offline
<u>3.</u>	To-C Place	V	offline
<u>4.</u>	To-D Site	V	offline
5.	???	X	

#### LAN-to-LAN Profiles:

#### How can you set a GRE over IPSec profile?

- 1. Please go to LAN to LAN to set a profile with IPSec.
- 2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

			High(ES	P)	🗹 DES 🗹	3DES 🗹	AES
4. Gre over IPsec Settings							
Enable IPsec Dial-O	t function GRE over IP		0				
🗖 Logical Traffic	My GRE IP 192.168.50.20	)0		Pee	er GRE IP 19	2.168.50.100	)
5. TCP/IP Network Settings							
My WAN IP	0.0.0.0		RIP Dire	ection	I	Disable	*
Remote Gateway IP	192.168.1.1		From fir	st su	bnet to rem	ote netwo	ork, you have
Remote Network IP	192.168.1.0					Route 💌	
Remote Network Mask	255.255.255.0						
Local Network IP	192.168.25.1				default rout		'PN tunnel (
Local Network Mask	255.255.255.0		Uniy sir	igie V	VAN support	ts this )	
	More						

3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.

			High(E	5P)	🗹 DES 🛙	🛛 3DES 🗹 i	AES
4. Gre over IPsec Settings							
🗹 Enable IPsec Dial-O	ut function GRE over IF	)sei	C				
💷 Logical Traffic	My GRE IP 192.168.50.1	00 Peer GRE IP 192.168.50.200					
5. TCP/IP Network Settings	5. TCP/IP Network Settings						
My WAN IP	0.0.0.0		RIP Din	ection	1	Disable	~
Remote Gateway IP	192.168.25.1		From fii to do	rst su	bnet to rer	note netwo	irk, you have
Remote Network IP	192.168.25.0	)				Route 🔽	
Remote Network Mask	255.255.255.0	L					
Local Network IP	192.168.1.1					te to this VPN tunnel (	
Local Network Mask	255.255.255.0	J	Only si	ngle v	VAN suppo	orts this )	
	More						

## Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

### Advanced Load Balance

C	<b>VPN</b> Load Balance Advance Settings	s - Windows Internet Explorer		×
e	) http://192.168.1.1/doc/vpntrlb.htm		E	3
				^
1	/PN Load Balance Advance Setti	nas		
Γ	Profile Name:	Loadbalan1		
	Load Balance Algorithm:	Round Robin		
		O Weighted Round Robin		
		Auto Weighted	ล	
		🔿 According to Speed Ratio (Member1:Member2): 50:50 💌		
	VPN Load Balance Policy			
		● Edit ○ Insert after		
	Tunnel Bind Table Index:	(1~64)		
	Active:	Active 🗸		
	Binding Dial Out Profile:	20 💌		
	Src IP Start:	0.0.0.0 End: 255.255.255		
	Dest IP Start:	0.0.0.0 End: 255.255.255		
	Dest Port Start:	1 End: 65535		
	Protocol:	ANY 🕑 0		
		OK Close		
	Detail Information			
	[VPN Load Balance Profile	•	^	
	[Algorithm: Round Robin ]			
			=	
				~
<				

Item	Description			
Profile Name	List the load balance profile name.			
Load Balance Algorithm	<b>Round Robin</b> – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.			
	Weighted Round Robin –Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. Auto Weighted can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. According to Speed Ratio allows			

	user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).				
VPN Load Balance Policy	Below shows the algorithm for Load Balance.				
	<b>Edit</b> – Click this radio button for assign a blank table for configuring Binding Tunnel.				
	<b>Insert after</b> – Click this radio button to adding a new binding tunnel table.				
	<b>Tunnel Bind Table Index</b> - 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.				
	Active – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.				
	<b>Binding Dial Out Index</b> – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.				
	<b>Scr IP Start /End</b> – Specify source IP addresses as starting point and ending point.				
	<b>Dest IP Start/End</b> – Specify destination IP addresses as starting point and ending point.				
	<b>Dest Port Start /End</b> – Specify destination service port as starting point and ending point.				
	<b>Protocol</b> – <b>Any</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.				
	<b>TCP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. <b>UDP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. <b>TCP/UPD</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. <b>ICMP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMF Service Port also fits the number here, such binding tunnel table can be established. <b>IGMP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMF Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. <b>Other</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding				



Detail Information		splay detailed information for Binding elow shows a successful binding tunnel					
	policy for load ba						
	VPN Load Balance Advance						
	3 192.168.1.1/doc/vpntrlb.htm						
	VPN Load Balance Advance Se	ettinas					
	Profile Name:	1					
	Load Balance Algorithm:	<ul> <li>Round Robin</li> <li>Weighted Round Robin</li> <li>Auto Weighted</li> <li>According to Speed Ratio (Member1:Member2): 50:50 ▼</li> </ul>					
	VPN Load Balance Policy						
	Tunnel Bind Table Index: Active: Binding Dial Out Profile:	Edit Insert after     (1~64)     Active      I					
	Src IP Start:	0.0.0.0 End: 255.255.255 0.0.0.0 End: 255.255.255					
	Dest IP Start: Dest Port Start:	1 End: 65535					
	Protocol:	ANY 💽 🛛					
		Set OK!! OK Close					
	Detail Information						
	[ <u>XPN</u> Load Balance Profi [Algorithm: Round Robin						
	%No.l> Tunnel Bind						
	Binding Dial Out Index Binding protocol	:= 1					
		= 192.168.10.24 ~ 255.255.255 = 192.168.1.20 ~ 255.255.255.255					
	Binding Dat Port	= 1 ~ 65535					
		• ii.					
	<						
	Note : To configure a successful binding tunnel, you						
	have to:						
	Type Binding Sro	r IP range (Start and End) and Binding Des					
	IP range (Start an	d End). Choose TCP/UDP, IGMP/ICMP					
	or Other as Bindi	ng Protocol.					

Detailed Settings for Advanced Backup

🖉 YPN Backup Advance Settings - Windows Internet Explorer	
2 http://192.168.1.1/doc/vpntrbak.htm	
	<u>~</u>
VPN Backup Advance Settings	
Profile Name: Backup1	
ERD Mode: 💿 Normal	
Resume (Member 1 first)	
Detail Information:	
Environment Recovers Detection(ERD) Status: Normal Mode	<u>~</u>
	<u> </u>
OK Close	
	~
<	>



Item Description			
Profile Name List the backup profile name.			
ERD Mode	ERD means "Environment Recovers Detection".		
	<b>Normal</b> – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.		
	<b>Resume</b> – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.		
Detail Information	This field will display detailed information for Environment Recovers Detection.		

## 3.10.11 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management

Dial-out Too	bl					Refre	sh Seco	onds : 10	✓ Refresh
		General Mode:				~	Dial		
	I	Backup Mode:				¥ [	Dial		
	Load B	alance Mode:	( Loadbalan1	) 172.1	6.3.8	*	Dial		
VPN Connec	ction Status								
Current Pag	je: 1						Pa	ge No.	Go >>
VPN	Туре	Remote II	P Virtual Ne	etwork	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
						xxxxx : Da xxxxx : Da		crypted. encrypted	l.

Item	Description					
Dial-out Tool	<b>General Mode -</b> 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.					
	Refresh Seconds :					
	General Mode: (Alfa ) 192.168.0.26 Dial					
	Backup Mode: (Alfa ) 192.168.0.26 Dial					
	Load Balance Mode: Audi ) 192.168.0.28 Dial					
	BMW ) 192.168.0.29 Buick ) 192.168.0.30					
	Cadillac ) 192.168.0.31					
	Chrysler ) 192.168.0.32 Citroen ) 192.168.0.33					
	(Daihatsu ) 192.168.0.34					
	(Ferrari) 192.168.0.35					
	(Fiat) 192.168.0.36					
	Backup Mode - This filed displays the profile name saved					
	in VPN TRUNK Management (with Index number and					



VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.
General Mode: (Alfa ) 192.168.0.26 🔽 Dial
Backup Mode:         (VpnBackup)         192.168.2.103         Dial           Load Balance Mode:         (VpnBackup)         192.168.2.103         Dial
<b>Dial -</b> Click this button to execute dial out function.
<b>Refresh Seconds -</b> Choose the time for refresh the dial information among 5, 10, and 30.
<b>Refresh -</b> Click this button to refresh the whole connection status.

## 3.11 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 manage 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.

Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup

## 3.11.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

	v		
Name	Subject	Status	Modify
			View Delete
			View Delete
			View Delete
	GENERATE IMPORT	REFRESH	

Item	Description
Generate	Click this button to open Generate Certificate Request window.



	Type in all the information that the window requests. Then click <b>Generate</b> again.	
Import	Click this button to import a saved file as the certification information.	
Refresh	Click this button to refresh the information listed below.	
View	Click this button to view the detailed settings for certificate request.	
Delete	Click this button to delete selected name with certification information.	

#### GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Certificate Management >> Local Certificate

Generate Certificate Signing Reque Certificate Name	
Subject Alternative Name	
Туре	IP Address
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA 🔽
Key Size	1024 Bit 🔽

Generate

**Note:** Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O	Requesting	View Delete	
			View Delete	
			View Delete	
GENERATE IMPORT REFRESH				

#### IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Certificate Management >> Local Certificate

nport X509 Local Certificate			
pload Local Certificate			
Select a local certificate file.			
Certificate file: Browse.			
Click Import to upload the local certificate.			
Import Cancel			
Ipload PKCS12 Certificate			
Select a PKCS12 file.			
PKCS12 file: Browse.			
Password:			
Click Import to upload the PKCS12 file.			
Import Cancel			
Ipload Certificate and Private Key			
Select a certificate file and a matchable Private Key.			
Certificate file: Browse.			
Key file: Browse.			
Password:			
Click Import to upload the local certificate and private key.			
Import Cancel			

Item	Description
Upload Local Certificate	It allows users to import the certificate which is generated by vigor router and signed by CA server.
	If you have done well in certificate generation, the Status of the certificate will be shown as " <b>OK</b> ".

	Import X509 Local Certificate			
	Congratulation! Local Certificate has been imported successfully. Please click Back to view the certificate.			
	Name	Subject	Status	Modify
	draytekdemo	/O=Draytek/OU=Draytek Sales/	OK	View Delete
				View Delete
	···· View Delete			
		GENERATE	REFRESH	
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.			
	Note: PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.			
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.			

#### REFRESH

Click this button to refresh the information listed below.

#### View

Click this button to view the detailed settings for certificate request.

0	🔰 http://192.168.1.1 - Certificate Signing Request Information - Microsoft Internet Explorer						
				-			
	Certificate Information						
	Certificate Name : server						
	Issuer :						
	Subject :	C=TW, ST=Hsinchu, L=Hsinchu, O=Draytek, OU=MKT, CN=DT, emailAddress=support@draytek.com					
	Subject Alternative Name :						
	Valid From :						
	Valid To :						
	PEM Format Content :	BEGIN CERTIFICATE REQUEST MIIBwzCCASwCAQAwgYIxCzAJBgNVBAYTAIRXMRAwDgYDVQQIEwdIc2luY2h1MRAw DgYDVQQHEwdIc2luY2h1MRAwDgYDVQQKEwdEcmF5dGVrMQwwCgYDVQQLEwNNS1Qx CzAJBgNVBAMTAKRUMSIwIAYJKoZIhvcNAQkBFhNZdXBwb3J0QGRyYX10ZWsuY29t MIGFMAOGCSqGSIb3DQEBAQUA4GNADCBiQKBgQcb06gdDl7KUjwGouC9HYPwq1Ia Ra/uaSCXJjhmJ+Vokmk8FRYkU28PTuWtavvPKH61M2cHDLRUJhQnXMAGbIuVsn3u k+2zW0Mp2IFpbnd7YgmQIBUx261QIIK7vU/YmVYXIQ4/CMhdpsgM0rGiK2N9sGVr uZ/T+QqYZk7GaQw6fQIDAQABoAAmDQYJKoZIhvcNAQEFBQAbgYEAB1iNMnczHBdu X07+ktPJaRyo2VKo9YTYQxJxuNrbVaJhvTx9NqHCyAi/DLMW5IQYJPs5Tz94Ddcr yC1rbh+206IsxcUzK70GjMByY01ubchHRYRAxi2RTNQY0ICRscVJMExxAjpnXWNF IaNe0IwGZ/1Z/+BhlnYXzFQ8u2IIsXY= END CERTIFICATE REQUEST	( ; 1 ≣ 1				
		Close		~			

**Note:** You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into



it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

#### Delete

Click this button to remove the selected certificate.

## 3.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Management >> Trusted CA Certificate						
X509 Trusted CA Certificate Configuration						
Name	Subject	Status	Modify			
Trusted CA-1			View Delete			
Trusted CA-2			View Delete			
Trusted CA-3			View Delete			
1	IMPORT F	REFRESH				

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

	Certificate	Management >	>>	Trusted	СА	Certificate	
--	-------------	--------------	----	---------	----	-------------	--

mport X509 Trusted CA Certificate				
Select a trusted CA certificate file.				
Browse.,				
Click Import to upload the certification.				
Import Cancel				

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

**Dray** Tek

ertificate Information - Windows Internet Explorer				
http:// <b>192.168.1.1</b> /doc/XCaCfVi1.htm				
Cer	tificate Detail Information			
Certificate Name:	Trusted CA-1			
Issuer:				
Subject:				
Subject Alternative Name:				
Valid From:	<u>×</u>			
Valid To:				
<u> </u>				
	Close	1.4		
		>		

## 3.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backu	p / Restoration
Backup	
	Encrypt password:
	Confirm password:
	Click Backup to download certificates to your local PC as a file.
Restoration	
	Select a backup file to restore.
	Browse.,
	Decrypt password:
	Click Restore to upload the file.

# **3.12 Wireless LAN**

This function is used for "n" models only.

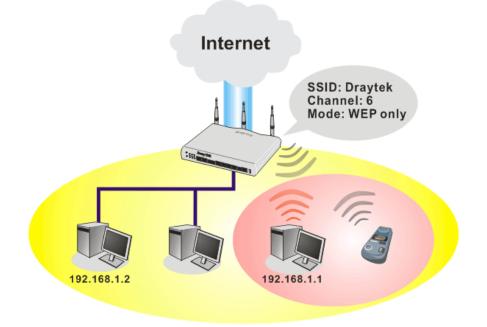
## 3.12.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note**: \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



## **Multiple SSIDs**

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.



## Security Overview

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

Wireless LAN General Setup Security Access Control WPS WDS Advanced Setting WMM Configuration AP Discovery Station List



**Dray** Tek

## 3.12.2 General Setup

Wireless LAN >> General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

ble Wireles	5 LAN				
Mode :			Mixed(11b+1	1g+11n) 🔽	
Index(1-15)	in <u>Sched</u>	ule Setup:	, [		
Only schedu other action	ule profiles ns are ignor	that have the ac red.	ction "Force Down	n" are applied to the	WLAN, all
Enable I	Hide SSID	S	SSID	Isolate Member	Isolate VPN
1		DrayTek			
2		DrayTek_Guest			
3					
4					
Channel:	hannel 6, 24	37MHz 💌	e dial-in and LAN Long Preaml I 802.11 b device		ance)
Channel: C	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup>	37MHz 💌	Long Preaml	ble:	ance)
Isolate VPN Channel: C Long Pream Packet-OVE Tx Burs Note:	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t	37MHz 🔽	Long Preaml 802.11 b device	ble:	
Isolate VPN Channel: C Long Pream Packet-OVE TX Burs Note: The same t	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t echnology	37MHz 💌 sary for some old must also be sup	Long Pream 1 802.11 b device ported in clients	ble:  ble:	ormance.
Isolate VPN Channel: C ong Pream Packet-OVE Tx Burs Note: The same t Rate Contro	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t echnology	37MHz 💌 sary for some old must also be sup	Long Pream 802.11 b device ported in clients	ble:  ble:	ormance.
Isolate VPN Channel: C Long Pream Packet-OVE Tx Burs Note:	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t echnology	37MHz 💌 sary for some old must also be sup	Long Pream 1 802.11 b device ported in clients bload	ble:  ble:	ormance.
Channel: C Channel: C Long Pream Packet-OVE TX Burs Note: The same t Rate Contro SSID 1	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t echnology	37MHz  sary for some old must also be sup	Long Pream 1 802.11 b device ported in clients load 00 kbps 00 kbps	ble:  ble:	ormance.
Isolate VPN Channel: C ong Pream Packet-OVE Tx Burs Note: The same t SSID 1 SSID 2	hannel 6, 24 ble: neces: RDRIVE <sup>TM</sup> t echnology	37MHz 💌 sary for some old must also be sup le Up 3000	Long Pream 1 802.11 b device ported in clients bload 00 kbps 00 kbps	ble: s only(lower perform to boost WLAN perfo Download 30000 30000	ormance.

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, the router can connect to 11g Only, 11n Only(2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	Mixed(11b+11g+11n) 11g Only 11n Only (2.4 GHz) Mixed(11b+11g) Mixed(11g+11n) Mixed(11a+11n 5 GHz) Mixed(11b+11g+11n) In which, 802.11b/g operates on 2.4G band, 802.11a operates on 5G band, and 802.11n operates on either 2.4G or 5G band.		
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.		
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.		
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.		
Isolate	<ul> <li>VPN – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</li> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> </ul>		
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.         Channel:       Channel 6, 2437MHz         Auto       Channel 1, 2412MHz         Channel 2, 2417MHz       Channel 3, 2422MHz         Channel 4, 2427MHz       Channel 5, 2432MHz         Channel 5, 2432MHz       Channel 6, 2437MHz         Channel 9, 2422MHz       Channel 6, 2437MHz         Channel 1, 2412MHz       Channel 7, 2422MHz         Channel 9, 2422MHz       Channel 6, 2437MHz         Channel 1, 2412MHz       Channel 7, 2442MHz         Channel 9, 2452MHz       Channel 7, 2442MHz         Channel 9, 2452MHz       Channel 9, 2452MHz         Channel 10, 2457MHz       Channel 10, 2457MHz         Channel 11, 2462MHz       Channel 11, 2462MHz         Channel 12, 2467MHz       Channel 11, 2462MHz         Channel 13, 2472MHz       Channel 13, 2472MHz		

Long Preamble	This option is to define the 802.11 packet. Most mode preamble with 56 bit sync with 128 bit sync field. Ho wireless network devices of Check it to use <b>Long Prea</b> with this kind of devices.	rn wireless netw field instead of wever, some or only support lor	work uses short long preamble riginal 11b ng preamble.
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burst</b> ). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.		
	<b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b> ).		
	Vigor N61 802.11n Wireless USB Adapter Utility	-	
	Configuration Status Option About		
	General Setting Auto launch when Windows start up	Advance Setting Disable <u>R</u> adio	
	Remember mini status position	Fragmentation Threshold :	2346
	Auto <u>h</u> ide mini status	RTS Threshold :	2347
	Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH 💙
	Enable IP Setting and Proxy Setting in Profile	Ad-hoc <u>C</u> hannel:	1
	Group Roaming Ad-hoc	Po <u>w</u> er Save Mode:	Disable
		Tx Burst :	Disable 🔽
	WLAN type to connect         ③ Infrastructure and Ad-hoc network         ○ Infrastructure network only         ○ Ad-hoc network only		
	Automatically connect to non-preferred networks		
		ОК	Cancel Apply
Tx <u>B</u> urst : Disable □ Disable Enable		×	
	<b>Note:</b> * means the real tran environment of the networ		lepends on the
Rate Control	It controls the data transmi connection.	ssion rate throu	igh wireless
	<b>Upload</b> – Check Enable an data upload. Default value		
	<b>Download</b> – Type the transmitting rate for data download. Default value is 30,000 kbps.		

After finishing all the settings here, please click  $\mathbf{O}\mathbf{K}$  to save the configuration.

## 3.12.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

The password (PSK) of default security mode is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

Wireless LAN >> Security Settings

	Mode:	[	Disable 💌	
WPA:	Set up <u>RADIUS S</u>	<u>erver</u> if 802.1)	is enabled.	
••••	ption Mode:		TKIP for WPA/AES for WPA2	
	Pre-Shared Key(I	PSK):	*****	
	Type 8~63 ASCI "cfgs01a2" or '		64 Hexadecimal digits leading by ".	"0x", for example
WEP:				
	Encryption Mode	: [	64-Bit 🗸	
	⑧Key 1 :	[	*******	
	○Key 2 :	[	*******	
	○Key 3 :	[	******	
	○Key 4 :	[	*******	
For 64 bit WEP key Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132". For 128 bit WEP key Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".				

Available settings are explained as follows:

Item	Description

**Dray** Tek

Mode	There are several modes provided for you to choose.
	Disable 💙
	1 WEP WEP/802.1x Only WPA/802.1x Only WPA2/802.1x Only Mixed(WPA+WPA2/802.1x only) WPA/PSK WPA2/PSK
	Mixed(WPA+WPA2)/PSK Note: You should also set RADIUS Server simultaneously
	if 802.1x mode is selected.
	<b>Disable</b> - Turn off the encryption mechanism. <b>WEP</b> -Accepts only WEP clients and the encryption key
	should be entered in WEP Key.
	<b>WEP/802.1x Only -</b> Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>WPA/802.1x Only-</b> Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>WPA2/802.1x Only-</b> Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. WPA/PSK-Accepts only WPA clients and the encryption
	key should be entered in PSK.
	<b>WPA2/PSK-</b> Accepts only WPA2 clients and the encryption key should be entered in PSK.
	<b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
	<b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only. <b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
WEP	<b>64-Bit</b> - For 64 bits WEP key, either <b>5</b> ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x,

**Dray** Tek

such as 0x4142434445.)	
<b>128-Bit</b> - For 128 bits WEP key, either <b>13</b> ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).	
Encryption Mode:	64-Bit 64-Bit 128-Bit
All wireless devices must support th	
bit size and have the same key. Four	
here, but only one key can be selected at a time. The keys	
 can be entered in ASCII or Hexadec you wish to use.	imal. Check the key

After finishing all the settings here, please click **OK** to save the configuration.

## 3.12.4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Enable Mac Address Filter	SSID 1 White List 🗸	SSID 2 White List V
	SSID 3 White List 🗸	SSID 4 White List 🕶
	MAC Address Filter	
Index Attribute	MAC Address	Apply SSID
Client's M	1AC Address : : : : : : : : : : : : : : : : : :	:::
	1AC Address : : : : : : : : : : : : : : : : : :	
Apply SSID :		SSID 3 SSID 4

Wireless LAN >> Access Control

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be

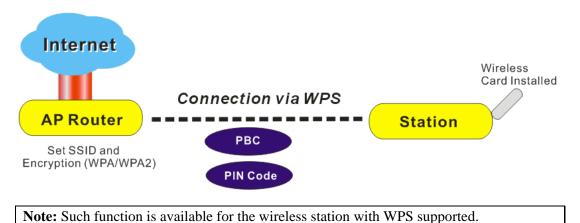


	grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.	
MAC Address Filter	Display all MAC addresses that are edited before.	
Client's MAC Address	Manually enter the MAC address of wireless client.	
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.	
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.	
Add	Add a new MAC address into the list.	
Delete	Delete the selected MAC address in the list.	
Edit	Edit the selected MAC address in the list.	
Cancel	Give up the access control set up.	
OK	Click it to save the access control list.	
Clear All	Clean all entries in the MAC address list.	

After finishing all the settings here, please click **OK** to save the configuration.

## 3.12.5 WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



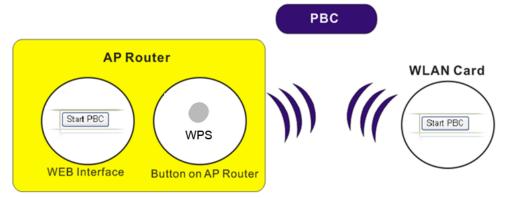
It is the simplest way to build connection between wireless network clients and vigor router.

Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

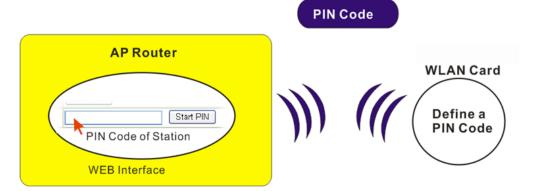
There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.



• On the side of Vigor 2850 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



• If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

#### Below shows Wireless LAN>>WPS web page:

#### Wireless LAN >> WPS (Wi-Fi Protected Setup)

Enable WPS

#### Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	V2860
Authentication Mode	Disable

#### **Device Configure**

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status:

Note: WPS can help your wireless client automatically connect to the Access point.

♀: WPS is Disabled.

♀: WPS is Enabled.

 $\mathcal{C}$ : Waiting for WPS requests from wireless clients.

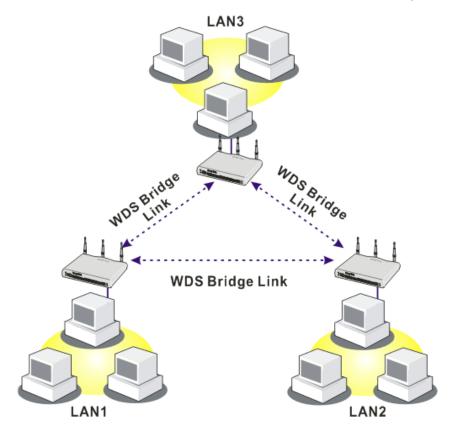
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

## 3.12.6 WDS

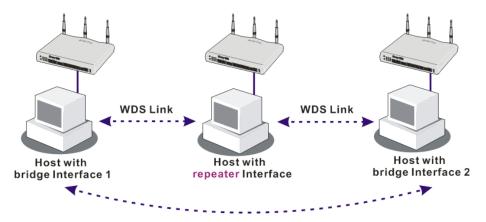
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:



The application for the WDS-Repeater mode is depicted as below:

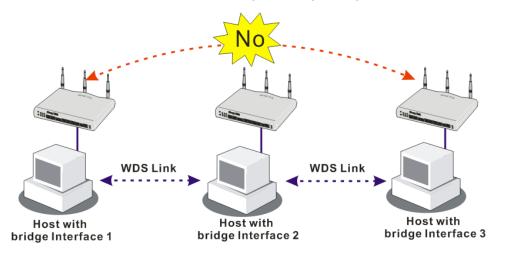


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in



**Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

Wireless LAN >> WDS Settings

WDS Settings	Set to Factory Default
Mode: Bridge 💌	Bridge Enable Peer MAC Address
Security:	
● Disable ○ WEP ○ Pre-shared Key	
WEP:	
Use the same WEP key set in <u>Security Settings</u> .	Note: Disable unused links to get better
Pre-shared Key:	performance.
Туре:	Repeater
○ WPA	Enable Peer MAC Addess
Кеу : милики ники	
Note: WPA and WPA2 are not compatible with DrayTek WPA.	
Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2" or	
"0x655abcd".	Access Point Function:
	€ Enable
	Status:
	Send "Hello" message to peers.
	Link Status
	Note: The status is valid only when the peer also supports this function.
ОК	Cancel

**Dray** Tek

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. <b>Disable</b> mode will not invoke any WDS setting. <b>Bridge</b> mode is designed to fulfill the first type of application. <b>Repeater</b> mode is for the second one.
	Disable Disable Bridge Repeater
Security	There are three types for security, <b>Disable</b> , <b>WEP</b> and <b>Pre-shared key</b> . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in <b>Security Settings</b> page. If you did not set any key in <b>Security Settings</b> page, this check box will be dimmed.
Pre-shared Key	<b>Type</b> – There are some types for you to choose. <b>WPA</b> and <b>WPA2</b> are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. <b>Key</b> - Type 8 ~ 63 ASCII characters or 64 hexadecimal
Bridge	<ul> <li>digits leading by "0x".</li> <li>If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.</li> </ul>
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check <b>Enable</b> box in the front of the MAC address after typing.
Access Point Function	Click <b>Enable</b> to make this router serving as an access point; click <b>Disable</b> to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.12.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN >> Advanced Setting

Operation Mode	💿 Mixed Mode 🔘 Green Field	
Channel Bandwidth	○ 20 ④ 20/40	
Guard Interval	🔘 long 💿 auto	
Aggregation MSDU(A-MSDU)	🔘 Disable 💿 Enable	

Available settings are explained as follows:

Item	Description
Operation Mode	<b>Mixed Mode</b> – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
	<b>Green Field</b> – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	<b>20-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.
	<b>20/40</b> – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose <b>auto</b> as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable.</b>

After finishing all the settings here, please click **OK** to save the configuration.

**Dray** Tek

# 3.12.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC\_BE, AC\_BK, AC\_VI and AC\_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.

WMM Configura	tion				Set to	Factory Default	
WMM Capable		💿 Enable 🔘	) Disable				
APSD Capable		🔘 Enable 🧿	) Disable				
WMM Paramete	ers of Access P	oint					
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy	
AC_BE	3	4	6	0			
AC_BK	7	4	10	0			
AC_VI	1	3	4	94			
AC_VO	1	2	3	47			
WMM Paramete	ers of Station						
	Aifsn	CWMin		CWMax	Тхор	ACM	
AC_BE	3	4	[	10	0		
AC_BK	7	4	-	10	0		
AC_VI	2	3	4	4	94		
AC_VO	2	2		3	47		

Wireless LAN >> WMM Configuration

ОК

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
APSD Capable	The default setting is <b>Disable</b> .
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO



	categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	<ul> <li>It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.</li> <li>Note: Vigor2920 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.</li> </ul>
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.12.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List				
	BSSID	Channel	SSID	
	1	Scan		
See <u>St</u>	atistics.			
	uring the scanning p e router.	rocess (~5 secor	nds), no station is allowed to connect	
Add to	WDS Settings :			
AP's MA	C address	: :::::::::::::::::::::::::::::::::::::	::::	
Add	to	💿 Bridge	○ Repeater	

Wireless LAN >> Access Point Discovery

Item	Description	
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.	
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics Recommended channels for usage:1 2 3 4 5 6 7 8 9 10 11 12 13 AP number v.s. Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Channel Cancel	
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click <b>Add to</b> . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.	



# 3.12.10 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

	Status	MAC Address	Associated with	
		Refre	sb	
Sta	atus Codes :			
	Connected, N Connected, W			
P:	Connected, W	VPA.		
	Connected, W Blocked by Ac			
N:	Connecting.			
F:	Fail to pass W	/PA/PSK authentication		
No	te: After a sta	tion connects to the ro	uter successfully, it may be turned	
	without notic nnection expir		till be on the list until the	
0	nnection expli	Co.		
	d to <u>Access Co</u>	ontrol :		
Ad				

Wireless LAN >> Station List

Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into Access Control.

Add

# 3.13 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 less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.

SSL VPN
General Setup
SSL Web Proxy
SSL Application
User Account
User Group
Online User Status

### 3.13.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

```
SSL VPN >> General Setup
```

Port	443 (Default: 443)	
Server Certificate	self-signed 💌	
Encryption Key Algorit	ım	
◯High - AES(128	bits) and 3DES	
💿 Default - RC4(1	8 bits)	
O Low - DES		

Note: The settings will act on all SSL applications.

OK ] [	Cancel
--------	--------

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in <b>System</b> <b>Maintenance&gt;&gt;Management</b> . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose <b>Self-signed</b> to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.



<b>Encryption Key</b>	Choose the encryption level for the data connection in SSL
Algorithm	VPN server.

After finishing all the settings here, please click  $\mathbf{OK}$  to save the configuration.

# 3.13.2 SSL Web Proxy

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

SSL	VPN >	>> \$\$	SL We	b Proxy	

SSL Web Prox	y Servers Profiles:	I	Set to Factory Default
Index	Name	URL	Active
<u>1.</u>			х
<u>2.</u>			х
<u>3.</u>			х
<u>4.</u>			х
<u>5.</u>			х
<u>6.</u>			х
<u>7.</u>			х
<u>8.</u>			х
<u>9.</u>			х
<u>10.</u>			х

Each item is explained as follows:

Item	Description
Name	Display the name of the profile that you create.
URL	Display the URL.
Active	Display current status (active or inactive) of such profile.

Click number link under Index filed to set detailed configuration.

```
SSL VPN >> SSL Web Proxy
```

Profile Index : 1		
Name		
URL		]
Host IP Address		
Access Method	Disable 💌	
Note: URL format must be entered as http:/ Domain_name is a FQDN.	Disable Secured Port Redirection SSL //Domain_name	directory where
ОК	Clear Cancel	

Item	Description
Name	Type name of the profile. The length of the name is limited to 15 characters.

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.
Access Method	There are three modes for you to choose.
	<b>Disable</b> – the profile will be inactive. If you choose <b>Disable</b> , all the web proxy profile appeared under VPN remote dial-in web page will disappear.
	<b>Secured Port Redirection</b> – such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute "Connect" manually in SSL Client Portal page.
	<b>SSL</b> – if you choose such selection, web proxy over SSL will be applied for VPN.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.13.3 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.

SSL	VPN	>>	SSL	Application	
000			000	Applied to the	

index	Name	Host Address	Service	Active
muex	Name	HOST Address	Service	Active
<u>1.</u>				х
<u>2.</u>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				х
<u>10.</u>				x

Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP or SAMBA path.
Service	Display the type of the service selected, e.g., VNC/RDP/SAMBA.
Active	Display current status (active or inactive) of the selected profile.



To create a new SSL application profile:

1. Click number link under Index filed to set detailed configuration.

#### SSL VPN >> SSL Application

#### SSL Applications Profiles:

Index	Name	Hos
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

2. The following page will appear.

SSL VPN >> SSL Application

Profile Index : 1	
Enable Application Service	
Application Name	
Application	Virtual Network Computing (VNC)
IP Address	Please Select Virtual Network Computing (VNC)
Port	Remote Desktop Protocol (RDP)
Idle Timeout	Samba Application
Scaling	100%

Clear

Cancel

0K

Item	Description		
Enable Application Server	Check the box to enable such profile.		
Application Name	Type a name for such application. The length of the name is limited to 23 characters.		
Application	There are three types offered for you to create an application profile. Please Select Virtual Network Computing (VNC) Remote Desktop Protocol (RDP) Samba Application  Virtual Network Computing (VNC) – It allows you to access and control a remote PC through VNC protocol.  Remote Desktop Protocol (RDP) – It allows you to access and control a remote PC through RDP protocol.		

	<b>Samba Application</b> – It allows you to access and control a remote PC through Samba service.		
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.		
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.		
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.		
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.		
Screen Size	If you choose RDP, you have to choose the screen size for such application.		
Samba Path	If you choose Samba, you have to specify the path of the Samba service.		

- 3. Enter the required information.
- 4. After finished the above settings, click **OK** to save the configuration.

#### SSL VPN >> SSL Application

SSL Applications Profiles:			1	Set to Factory Default
Index	Name	Host Address	Service	Active
<u>1.</u>	VNC_1	192.168.1.51:5900	VNC	v
<u>2.</u>				х
<u>3.</u>				x

## 3.13.4 User Account

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into **VPN and Remote Access>>Remote Dial-in user**.

Remote Access User Accounts: Set to							Factory Default
Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	carrie	V	LAN1-DHCP	<u>17.</u>	???	×	
<u>2.</u>	???	Х		<u>18.</u>	???	х	
<u>3.</u>	???	Х		<u>19.</u>	???	Х	
<u>4.</u>	???	х		<u>20.</u>	???	х	
<u>5.</u>	???	Х		<u>21.</u>	???	Х	
<u>6.</u>	???	х		<u>22.</u>	???	х	
<u>7.</u>	???	Х		<u>23.</u>	???	Х	
<u>8.</u>	???	х		<u>24.</u>	???	х	
<u>9.</u>	???	Х		<u>25.</u>	???	х	
<u>10.</u>	???	х		<u>26.</u>	???	×	
<u>11.</u>	???	Х		<u>27.</u>	???	Х	
<u>12.</u>	???	х		<u>28.</u>	???	Х	
<u>13.</u>	???	Х		<u>29.</u>	???	Х	
<u>14.</u>	???	х		<u>30.</u>	???	Х	
<u>15.</u>	???	Х		<u>31.</u>	???	Х	
<u>16.</u>	???	х		<u>32.</u>	???	Х	

SSL VPN >> Remote Dial-in User

### 3.13.5 User Group

There are 10 user group profiles which can be created for authentication by LDAP server. Such profiles will be used by applications such as User Management, VPN and etc.

SSL User Group Profiles:		Set to Factory Default
Index	Name	Status
<u>1.</u>		x
<u>2.</u>		x
<u>3.</u>		x
<u>4.</u>		x
<u>5.</u>		x
<u>6.</u>		x
<u>7.</u>		x
<u>8.</u>		x
<u>9.</u>		x
<u>10.</u>		х

SSL VPN >> User Group

Each item is explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Display the number of the client which connecting to FTP server.

#### Name

Display the name of the group profile.

Click any index number link to open the following page for detailed configuration.

SSL VPN >> User Group		
Index No. 1 Finable Group Name SSL_group1 Access Authority		
SSL Web Proxy	SSL Application	
Authentication Methods		
Local User DataBase Available User Accounts	Selected User Accounts	
RADIUS     LDAP / Active Directory		
	OK Clear Cancel	

Item	Description		
Enable	Check this box to enable such profile.		
Group Name	Type a name for such profile. The length of the name is limited to 23 characters.		
Access Authority	Specify the authority for such profile.		
	At present, Vigor router allows you to create SSL Web Proxy and SSL Application profiles used for SSL VPN. The available profiles will be displayed here for you to select.		
	Access Authority		
	SSL Web Proxy SSL Application		
	SSL_WP_1 Game_APP		
Authentication Methods	It can determine the authentication method used for such profile.		
	Local User DataBase – The system will do the authentication by using the user defined account profiles (in VPN and Remote Access>>Remote Dial-In User). The enabled profiles will be listed in the Available User Account on the left box. To add a profile into a group, simply choose the one from the left box and click the >> button. It will be displayed in the Selected User Account on the right box. For detailed information about configuring the profile setting, refer to Objects Setting>>IP Group.		



<b>RADIUS</b> – The RADIUS server will do the authentication by using the username and password
<b>LDAP / Active Directory -</b> If it is checked, the LDAP / AD server will do the authentication by using the username, password, information stated on the selected profiles.
If the above three options are enabled, the system will do the authentication based on them in sequence.

After finishing all the settings here, please click **OK** to save the configuration.

# 3.13.6 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.

Provide SSL VPN	Home	SSL Web Proxy	SSL Tunnel	[ logout
INFO	Main Page:			
mike , (172.17.1.42) Welcome to DrayTek SSL VPN!		You have successfu You are given the f SSL Web F SSL Tunne	ollowing privileges: Iroxy	
Timeout after5 minutes. [ <u>Reset</u> ]				

Next, users can open SSL VPN>> Online Status to view logging status of SSL VPN.

SSL VPN >> Online User Status

			Refresh Seconds : 5 💌 refresh
Active User	Host IP	Time out(seconds)	Action
Kate	192.168.30.14	299	Drop

Available settings are explained as follows:

Item	Description
Active User	Display current user who visit SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click <b>Drop</b> to drop certain login user from the router's SSL Portal UI.

**Dray** Tek

# 3.14 USB Application

USB storage disk connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the Samba service through Vigor router.



## 3.14.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

eneral Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English 🗸
amba Service Settings(Network Neigh	nborhood)
🔿 Enable 💿 Disable	
Access Mode	
● LAN Only ○ LAN And WAN	
etBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor

2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: .; : " <> \* + = / \ | ?.

OK
U.N.

Item	Description
General Settings	<b>Simultaneous FTP Connections -</b> This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one



	time.	
	Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name. English English Chinese(Simple) Chinese(Traditional) German	
Samba Service Settings	Click <b>Enable</b> to invoke samba service via the router.	
Access Mode	<ul> <li>LAN Only – Users coming from internet cannot connect to the samba server of the router.</li> <li>LAN And WAN - Both LAN and WAN users can access samba server of the router.</li> </ul>	
NetBios Name Service	For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following; : " $<>$ * + = $\setminus$   ?.	
	<b>Workgroup Name</b> – Type a name for the workgroup.	
	<b>Host Name</b> – Type the host name for the router.	

After finishing all the settings here, please click **OK** to save the configuration.

## 3.14.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

USB Application >> USB User Management

SB User Mar	nagement			I	Set to Factory Defaul
Index	Username	Home Folder	Index	Username	Home Folder
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

Click index number to access into configuration page.



Profile Index: 1	
FTP/Samba User	🛇 Enable 💿 Disable
Username	
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	2 Contraction (1997)
Access Rule	
File	🗌 Read 🔲 Write 🔛 Delete
Directory	List Create Remove
Note: The folder name can only cont space.	tain the following characters: A-Z a-z 0-9 $ \  \  \  \  \  \  \  \  \  \  \  \  \$

ОК	Clear	Cancel
	0.00	

Available settings are explained as follows:	
----------------------------------------------	--

Item	Description
FTP/Samba User	<b>Enable</b> – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.
	<b>Disable</b> – Click this button to disable such profile.
Username	Type the username for FTP/Samba users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters.
	<b>Note:</b> "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
	<b>Note:</b> FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.
	<b>Note:</b> When write protect status for the USB storage disk is <b>ON</b> , you cannot type any new folder name in this field.



	Only "/" can be used in such case.	
	You can click $\overleftrightarrow$ to open the following dialog to add any new folder which can be specified as the Home Folder.	
	Mitp://1921.168.1.5/Hoe/Hpsenfolder.htm - Microsoft Taleraset Explorer USB User Management	
	Choose Folder Folder Name	
	Create Hew Home Folder Folder Name: Test Create Note: The folder name can only contain the following characters: A-2 a-2 0-9 \$ % ' @ ~ ' ! ( ) and space. Only 11 characters are allowed.	
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.	
	<b>File</b> – Check the items (Read, Write and Delete) for such profile.	
	<b>Directory</b> –Check the items (List, Create and Remove) for such profile.	

Before you click **OK**, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

# 3.14.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

File Expl	File Explorer							
<del>49</del>	•	9	Current Path: /					
			Name		Size	Delete	Rename	
1								
🔶 Uplo	ad File							
Select a	ad		<b>刘覽</b>					

USB Application >> File Explorer

Note: The folder can not be deleted when it is not empty.

Available	settings	are ex	plained	as	follows:

Item	Description	
** Refresh	Click this icon to refresh files list.	
✤ Back	Click this icon to return to the upper directory.	

Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

## 3.14.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

```
USB Application >> USB Disk Status
```

Connection 9	Status: No Disk Conr	nected	Disconnect USB Disk
Disk Capacit	y: 0 MB		
Free Capacit	y: 0 MB Refresh		
USB Disk Use	rs Connected		Refresh
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

Item	Description
<b>Connection Status</b>	If there is no USB storage disk connected to Vigor router, "No Disk Connected" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click <b>Refresh</b> at any time to get new status for free capacity.
Index	It displays the number of the client which connecting to FTP server.
IP Address	It displays the IP address of the user's host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

Available settings are explained as follows:

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

# 3.14.5 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

## For Web Syslog

USB Application >> Syslog Explorer

Time		Message
	Syslog Type User 🔽 Display Mo	ode Stop record when fulls
Enable Web Syslog		Export Refresh Clear
Web Syslog	USB Syslog	

Item	Description	
Enable Web Syslog	Check this box to enable the function of Web Syslog.	
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. User User Firewall Call WAN VPN All	
Display Mode	There are two modes for you to choose. Stop record when fulls Stop record when fulls Always record the new event Stop record when fulls – when the capacity of syslog is full, the system will stop recording. Always record the new event – only the newest events will be recorded by the system.	
Time	Display the time of the event occurred.	
Message	Display the information for each event.	

# For USB Syslog

This page displays the syslog recorded on the USB storage disk.

USB Application >> Syslog Explorer

Web Syslog		USB Syslog		
Note:The syslog will show y	while the saved sy	slog file size is over 1MB.		
Folder: n/a	File: n/a	Page: n/a	Log Type: n/a	
Time	Log Type		Message	

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

### 3.14.6 Temperature Sensor

A USB Thermometer can be attached to Vigor router to monitor the environmental temperature. If the temperature is higher the upper limit or lower than the lower limit, an alert would be sent out for notification.

### **Temperature Sensor Settings**

USB Application >> USB Temper Setting

Temperature Sensor Settings	Temperature Chart
Display Settings	
Temperature Calibration 0	0.00
Temperature Unit (	🖲 Celsius 🛛 🔿 Fahrenheit
Alarm Settings	
Alarm Method [	Disable 🚩
Upper temperature limit	30.00
Lower temperature limit	18.00
	OK

Item	Description
Display Settings	<ul> <li>Temperature Calibration - Type a value used for correcting the temperature error.</li> <li>Temperature Unit - Choose the display unit of the temperature. There are two types for you to choose.</li> </ul>
Alarm Settings	Alarm Method – Choose one of the options as the alarm method.

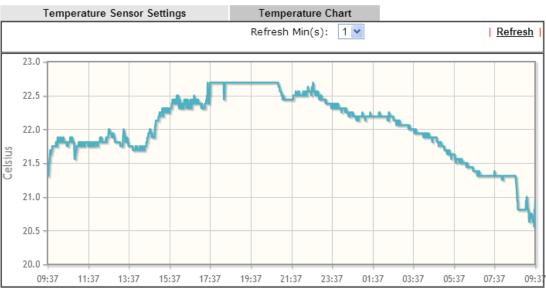


	SMS V Disable Syslog SMS EMAIL Disable – The function is disabled.
	<ul> <li>Syslog –The temperature log will be recorded on Syslog.</li> <li>SMS – The alert will be sent via SMS app.</li> <li>EMAIL - The alert will be sent to the e-mail address that you offer on the page of System Maintenance&gt;&gt;Syslog / Mail Alert Setup.</li> </ul>
	<b>Upper temperature limit/Lower temperature limit</b> - Type the upper limit and lower limit for the system to send out temperature alert.
ОК	Save the settings.

## **Temperature Chart**

Below shows an example of temperature graph:

USB Application >> USB Temper Record



Current Temperature: 20.94 Average Temperature: 22.03 Maximum Temperature: 22.69 Minimum temperature: 20.56

**Dray** Tek

# 3.15 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Customization, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
TR-069
Administrator Password
User Password
Login Customization
Configuration Backup
SysLog / Mail Alert
Time and Date
Management
Reboot System
Firmware Upgrade
Activation

## 3.15.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System Status						
Model Name Firmware Version Build Date/Time	: Vigor2860n : 3.7.1_RC5a : Feb 5 2013 12:24	1:58				
		LAN				
	MAC Address	IP Address	Subnet Mask	DHCP	Server	DNS
LAN1	00-1D-AA-A8-B6-A8	192.168.1.1	255.255.255.	0 Yes		168.95.1.1
LAN2	00-1D-AA-A8-B6-A8	192.168.2.1	255.255.255.	0 Yes		168.95.1.1
LAN3	00-1D-AA-A8-B6-A8	192.168.3.1	255.255.255.	0 Yes		168.95.1.1
LAN4	00-1D-AA-A8-B6-A8	192.168.4.1	255.255.255.	0 Yes		168.95.1.1
LAN5	00-1D-AA-A8-B6-A8	192.168.5.1	255.255.255.	0 Yes		168.95.1.1
LAN6	00-1D-AA-A8-B6-A8	192.168.6.1	255.255.255.	0 Yes		168.95.1.1
IP Routed Subnet	00-1D-AA-A8-B6-A8	192.168.0.1	255.255.255.	0 Yes		168.95.1.1
		Wireless LAN				
MAC Address	Erequer		Eirmware \	/orgion	SS	ID
00-1D-AA-A8-I		ricequerce, bornani		rension		avTek
00 10 /01/10			21010111			.,
		WAN				
Link Status	MAC Address	Connec	ction IP Add	ress	Default	Gateway
WAN1 Disconnecte	ed 00-1D-AA-A8-B6-	-A9 PPPoE				
WAN2 Connected	00-1D-AA-A8-B6-	-AA Static	IP 172.16	.3.130	172.16.	1.1
WAN3 Disconnecte	ed 00-1D-AA-A8-B6-	-AB				
		IPv6				
Address			Scope Inter	net Acce	ess Mode	3
	AFF:FEA8:B6A8/64		Link			-

User Mode is OFF now.



Item	Description		
Model Name	Display the model name of the router.		
Firmware Version	Display the firmware version of the router.		
Build Date/Time	Display the date and time of the current firmware build.		
LAN	MAC Address		
	- Display the MAC address of the LAN Interface.		
	IP Address		
	- Display the IP address of the LAN interface.		
	Subnet Mask		
	- Display the subnet mask address of the LAN interface.		
	DHCP Server		
	- Display the current status of DHCP server of the LAN interface		
	DNS		
	- Display the assigned IP address of the primary DNS.		
WAN	Link Status		
	- Display current connection status.		
	MAC Address		
	- Display the MAC address of the WAN Interface.		
	Connection		
	- Display the connection type.		
	IP Address		
	- Display the IP address of the WAN interface.		
	Default Gateway		
	- Display the assigned IP address of the default gateway.		
IPv6	Address - Display the IPv6 address for LAN.		
	<b>Scope -</b> Display the scope of IPv6 address. For example, IPv6 <b>Link Local</b> could only be used for direct IPv6 link. It can't be used for IPv6 internet.		
	<b>Internet Access Mode</b> – Display the connection mode chosen for accessing into Internet.		

# 3.15.2 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.

S and CPE Settings		
ACS Server On	Internet 💌	
ACS Server		
URL		
Username		
Password		
CPE Client		
O Enable O Disat	le	
URL		
Port	8069	
Username	vigor	
Password	••••••	
riodic Inform Settings		
O Disable		
Enable		
Interval Time	900 second(s)	
run settings		
<ul> <li>Disable</li> </ul>		
O Enable		
Server Address		
Server Port	3478	
Minimum Keep Aliv	Period 60 second(s)	
Maximum Keep Aliv	e Period -1 second(s)	

System Maintenance >> TR-069 Setting

Item	Description		
ACS Server On	Choose the interface for the router connecting to ACS server.		
ACS Server	<b>URL/Username/Password</b> – 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.		
CPE Client	Such information is useful for Auto Configuration Server <b>Enable/Disable</b> – Allow/Deny the CPE Client to connect with Auto Configuration Server.		
	<b>Port</b> – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.		
Periodic Inform Settings	The default setting is <b>Enable</b> . Please set interval time or schedule time for the router to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.		



The default is <b>Disable</b> . If you click <b>Enable</b> , please type the relational settings listed below:
Server IP – Type the IP address of the STUN server.
<b>Server Port</b> – Type the port number of the STUN server.
<b>Minimum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
<b>Maximum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

## 3.15.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Old Password	•••••	
New Password	•••••	
Confirm Password	•••••	

ОК

Available settings are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is <b>"admin"</b> .
New Password	Type in new password in this field. The length of the password is limited to 23 characters.
Confirm Password	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

## 3.15.4 User Password

This page allows you to set new password for user operation.

User Passwo	lser Mode for simple web configu ord	ration	
	Password	••••	
	Confirm Password	••••	
Note:Passw	vord can contain only a-z A-Z 0-9	$,;:."<>^*+=\setminus  ?$	@#^!()
		ОК	

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration.
	The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

Below shows an example for accessing into User Operation with User Password.

1. Open System Maintenance>>User Password.

System Maintenance >> User Password

2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

	Password Confirm Password	••••
		••••

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password			
Active Configuration			
Password	, ***** '		

4. Log out Vigor router web user interface by clicking the Logout button.



5. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.

<b>Dray</b> Tek	Vigor2860 Series
Login	
Username Password	
Group	💌
	Login
Сор	yright © 2012 DrayTek Corp. All Rights Reserved.

6. The main screen with User Mode will be shown as follows.

<b>Dray</b> Tek	Vig	<b>jor 2860 S</b> e	eries			88	<b>€</b>
Auto Logout 👻 🛛 📭 🖌	Dashboard	1					
Quick Start Wizard Online Status WAN LAN NAT Applications System Maintenance Diagnostics	Factory Reset	ACT WAN2 QoS USB1 DSL WCF USB2 VPN DoS	USB VOSLAC	CCC Vigor28 VDSL2 Securit WAX2(Gips) GipsLA	y Firewall	<b>2</b> 4	
	System In Model Nan Router Nam Firmware N DSL Versio	version 3.7.1_RC3	3	System Up Time Current Time Build Date/Time LAN MAC Address	0:42:35 2000 Jan 1 Jan 8 2013 00-1D-AA-A		Quick Access System Status Dynamic DNS TR-069 User Management
	IPv4 Inter WAN1	Line / Mode	IP Address Disconnecte	MAC Addres		Up Time 00:00:00	IM/P2P Block Schedule SysLog / Mail Alert LDAP
	WAN2 WAN3	Ethernet / USB /	Disconnect Disconnect			00:00:00 00:00:00	RADIUS Firewall Object Setting Data Flow Monitor
All Rights Reserved.	LAN	Mode RADVD / DHCPv6	Address FE80::21D:AAFF	FEA8:B768/64	Scope Link	Up Time	
User mode Status: Settings Saved	Interface DSL	1	n Stream : OKbps /	Up Stream : OKbps			×

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

Note: Setting in User Mode can be configured as same as in Admin Mode.

### 3.15.5 Login Customization

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify login URL and the heading on the Login window if you have such requirement.

System Maintenance >> Login Customiza	ation
---------------------------------------	-------

Login Customization		
Login Background URL	(63 char max.)	
Login Description	(31 char max.)	

OK Cancel

Item	Description	
Login Background URL	Type the URL for the web page which will be shown as the background.	
Login Description	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.	

## 3.15.6 Configuration Backup

### **Backup the Configuration**

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup				
Configuration B	ackup / Restoration			
Restoration				
	Select a configuration file.			
	Browse			
	Click Restore to upload the file.			
	Restore			
Backup				
	Click Backup to download current running configurations as a file.       Backup    Cancel			

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Dov	vnload 🔀
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer?           Open         Save         Cancel         More Info           Image: Ways ask before opening this type of file         Image: Ways ask before opening the type of file         Image: Ways ask before opening the type of file

3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

Save As						? 🗙
Save in:	🞯 Desktop		*	0 Ø	• 🖽 🍤	
My Recent Documents Desktop My Documents	My Documen My Computer My Network I RVS-COM Lit: Annex A mmm MWSnap300 TeleDanmark Tools Config Ny2k2_232_cc V2k6_250_cc	Places ∋ nfig_1				
My Computer						
	File name:	config			~	Save
My Network	Save as type:	Configuration file			~	Cancel

4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

### **Restore Configuration**

System Maintenance >> Configuration Backup

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

Configuration E Restoration	Backup / Restoration
	Select a configuration file. Browse Click Restore to upload the file. Restore
Backup	Click Backup to download current running configurations as a file. Backup Cancel

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

# 3.15.7 Syslog/Mail Alert

Destination Port

Enable syslog message: Firewall Log

> ✓ User Access Log WAN Log

Router/DSL information

Mail Syslog

AlertLog Setup

AlertLog Port

Enable

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

Authentication

DoS Attack ✓ IM-P2P

VPN LOG

User Name

Password Enable E-Mail Alert:

SysLog Access Setup	Mail Alert Setup	
Enable	Enable	Send a test e-mail
Syslog Save to:	SMTP Server	
Syslog Server	SMTP Port	25
Router Name	Mail To	
Server IP Address	Return-Path	
Destination Dant [144	Use SSL	

System Maintenance >> SysLog / Mail Alert Setup

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".

2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.

3. We only support secured smtp connection on port 465.

514

514

Enable



Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog.
	<b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.
	Check <b>USB Disk</b> to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in <b>System</b> <b>Maintenance&gt;&gt;Management.</b>
	If there is no name here, simply lick the link to access into <b>System Maintenance&gt;&gt;Management</b> to set the router name.
	Server IP Address - The IP address of the Syslog server.
	<b>Destination Port -</b> Assign a port for the Syslog protocol.
	<b>Mail Syslog</b> – Check the box to recode the mail event on Syslog.
	<b>Enable syslog message -</b> Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to

	Syslog.
AlertLog Setup	Check <b>Enable</b> to activate function of alert log.
	<b>AlertLog Port</b> - Type the port number for alert log. The default setting is 514.
Mail Alert Setup	Check <b>Enable</b> to activate function of mail alert.
	<b>Send a test e-mail -</b> Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
	<b>SMTP Server/SMTP Port -</b> The IP address/Port number of the SMTP server.
	Mail To - Assign a mail address for sending mails out.
	<b>Return-Path -</b> Assign a path for receiving the mail from outside.
	<b>Use SSL</b> - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
	Authentication - Check this box to activate this function while using e-mail application.
	User Name - Type the user name for authentication.
	<b>Password -</b> Type the password for authentication.
	<b>Enable E-mail Alert -</b> Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

		Vigor series	G	ateway IP (Fixed)	TX Packets	TX Rate
Status TX Pa		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
all Log VPI		ess Log Call Log	WAN Log Others Host Name:	Network Information Ne	t State	
IP Address	Mask 255.255.2	MAC 00-50-7F-54-6	NIC Description:		°CI Fast Ethernet Adapt	er - Packet St 💙
192.100.1.1	200.200.2	00-30-71 -34-0	MAC Address:	00-11-D8-E4-58-CE	Default Geteway;	192.168.1.1
			IP Address:	192.168.1.10	DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Mon Jan 22 01:28:23 2007
*,	Refresh	>	DNS Servers:	168.95.1.1	Lease Expires:	Thu Jan 25 01:28:23 2007

# 3.15.8 Time and Date

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

System Maintenance >> Time and Date

Current System Time	2000 Jan	1 Sat 0 : 48 : 30 Inquire Time
Time Setup		
🔘 Use Browser Time		
💿 Use Internet Time (	Client	
Server IP Address		pool.ntp.org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🗸 🗸
Enable Daylight Sav	ing	
Automatically Updat	e Interval	30 min 🔽

Available settings are explained as follows:

Item	Description			
Current System Time	Click <b>Inquire Time</b> to get the current time.			
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.			
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.			
Time Protocol	Select a time protocol.			
Server IP Address	Type the IP address of the time server.			
Time Zone	Select the time zone where the router is located.			
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.			
Automatically Update Interval	Select a time interval for updating from the NTP server.			

Click **OK** to save these settings.

### 3.15.9 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

The management pages for IPv4 and IPv6 protocols are different.

### For IPv4

System Maintenance >> Management

IPv4 Managemen	t Setup	IPv6 Management Setup			
Router Name		Management Port Setup			
		💿 User Define Ports	🔘 Default	Ports	
Management Access Contr	ol	Telnet Port	23	(Default: 23)	
Allow management fr	rom the Internet	HTTP Port	80	(Default: 80)	
FTP Server		HTTPS Port	443	(Default: 443)	
HTTP Server		FTP Port	21	(Default: 21)	
<ul> <li>✓ HTTPS Server</li> <li>✓ Telnet Server</li> </ul>		SSH Port	22	(Default: 22)	
SSH Server		SNMP Setup			
Disable PING from th	e Internet	Enable SNMP Agen	t		
Access List		Get Community	public		
List IP	Subnet Mask	Set Community	private		
1	*	Manager Host IP			
2	¥	Trap Community	public		
3	~	Notification Host IP			
		Trap Timeout	10	seconds	

OK

Item	Description		
Router Name	Type in the router name provided by ISP.		
Management Access Control	<ul> <li>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</li> <li>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</li> </ul>		
Access List	<ul> <li>You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.</li> <li>List IP - Indicate an IP address allowed to login to the router.</li> <li>Subnet Mask - Represent a subnet mask allowed to login to the router.</li> </ul>		

Management Port Setup	<b>User Define Ports -</b> Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
	<b>Default Ports -</b> Check to use standard port numbers for the Telnet and HTTP servers.
	Enable SNMP Agent - Check it to enable this function.
	<b>Get Community -</b> Set the name for getting community by typing a proper character. The default setting is <b>public.</b>
	<b>Set Community -</b> Set community by typing a proper name. The default setting is <b>private.</b>
	<b>Manager Host IP -</b> Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
	<b>Trap Community -</b> Set trap community by typing a proper name. The default setting is <b>public.</b>
	<b>Notification Host IP -</b> Set the IP address of the host that will receive the trap community.
	<b>Trap Timeout -</b> The default setting is 10 seconds.

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

## For IPv6

System Maintenance >> Management

	v4 Management Setup	IPv6 Management Setup	
Manag	gement Access Control		
Allov	v management from the Interr	net	
	🔲 Telnet Server ( Port : 23)		
	HTTP Server ( Port : 80)		
<b>E</b>	Enable PING from the Internet		
List	IPv6 Address / Prefix Length	/ 128	
		/ 120	
1.			
1. 2.		/ 128	
		/ 128	
2. 3.	Telnet / Http server port is the	/ 128	

Item	Description
Management Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	<b>Enable PING from the Internet</b> - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.



Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
_	<b>IPv6 Address /Prefix Length-</b> Indicate the IP address(es) allowed to login to the router.

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

### 3.15.10 Reboot System

System Maintenance >> Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System** Maintenance to open the following page.

Pohoot Sustam
Reboot System
Do you want to reboot your router ?
<ul> <li>Using current configuration</li> </ul>
<ul> <li>Using factory default configuration</li> </ul>
Reboot Now
Repool Now
Auto Reboot Time Schedule
Index(1-15) in Schedule Setup: , , , ,
Note: Action and Idle Timeout settings will be ignored.

**Index (1-15) in Schedule Setup -** You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications** >> **Schedule** web page and you can use the number that you have set in that web page.

Cancel

OK

If you want to reboot the router using the current configuration, check **Using current configuration** and click **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.

**Note:** When the system pops up Reboot System web page after you configure web settings, please click **Reboot Now** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

### 3.15.11 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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 to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

#### Web Firmware Upgrade

Select a firmware file.			
		Browse.	
Click Upgrade to upload the file.	Upgrade		

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.1_R	C5a
Firmware Upgrade Procedures:	
<ol> <li>Check that the firmware filer</li> <li>Click "Upgrade" on the Firmw</li> </ol>	Utility or other 3-party TFTP client software.
Do you want to upgrade firmware ?	OK

Click OK. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade



For the detailed information about firmware update, please go to Chapter 5.



### 3.15.12 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

System Maintenance >> Activation	Activate via interface : auto-selected 💌
Web-Filter License [Status:Not Activated]	Activate
Authentication Message	
	×
Note: If you want to use email alert or syslog, please config If you change the service provider, the configuration of	
OK Can	cel

Item	Description		
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.		
	Activate via interface : auto-selected auto-selected WAN 1 WAN 2 WAN 3		
Activate	The <b>Activate</b> link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.		
Authentication Message	As for authentication information of <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.		

Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation	Activate via interface : auto-selected 💌
Web-Filter License [Status:Commtouch] [Start Date:2011-03-28 Expire Dat	<u>Activate</u> te:2011-04-27]
Authentication Message	
WebFilter, Activation authenticate fail, contact 01 00:00:24	t with support@draytek.com, 2C 🦰
Note: If you want to use email alert or syslog, please configur If you change the service provider, the configuration of	
OK Cance	

# 3.16 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.



# 3.16.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

```
Diagnostics >> Dial-out Triggering
```

HEX Format:	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00-00 00 00 00 00 0	
00 00 00 00 00 00 00 00-00 00 00 00 00 0	
Decoded Format:	
0.0.0.0 -> 0.0.0.0	
Pr 0 len 0 (0)	

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

# 3.16.2 Routing Table

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh
	R - RIP, * - default, ~ - private 5.0 directly connected LAN1	
		~

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 R	outing Table		<u> </u>	Refres	<u>h</u>
Destination	Interface	-		Next Hop		^
FE80::/64	LAN		256			
FF00::/8	LAN	U	256			
						~
<					>	

Item	Description
Refresh	Click it to reload the page.

### 3.16.3 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.

```
Diagnostics >> View ARP Cache Table
```

Ethernet ARP Cache	Table			Clear Refresh
IP Address 192.168.1.5	MAC Address 00-50-7F-CD-07-48	Netbios Name	Interface LAN1	^
192.168.1.49	E0-CB-4E-DA-48-79	CARRIE-0C7CB251	LAN1	
				~

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

### 3.16.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Diagnostics >> View IPv6 Neighbour Table

IPv6 Address	Mac Address	Interface
FF02::2	33-33-00-00-00-02	LAN
FF02::1:3	33-33-00-01-00-03	LAN
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN
FF02::1	33-33-00-00-00-01	LAN
FF02::1	00-00-00-00-00	USB2
FF02::1:2	00-00-00-00-00	USB2
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN
<		>

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



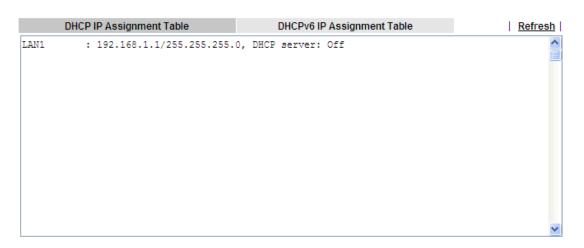
Refresh	Click it to reload the page.
---------	------------------------------

### 3.16.5 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.

Diagnostics >> View DHCP Assigned IP Addresses



#### Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table	DHCPv6 IP Assignment Table	Refresh
DHCPv6 server binding client: Index IPv6 Address	MAC Address Leased Time	<
<u>s</u>		>

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.



HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

## 3.16.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

Diagnostics >> NAT Sessions Table

```
NAT Active Sessions Table

        Private IP :Port #Pseudo Port
        Peer IP :Port Interface

        192.168.1.11
        2491
        52078
        24.9.93.189
        443
        WAN1

        192.168.1.11
        2493
        52080
        207.46.25.2
        80
        WAN1

        192.168.1.10
        3079
        52665
        207.46.5.10
        80
        WAN1
```

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

# 3.16.7 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis			
⊙ IPV4 01	IPV6		
		a LAN PC or you don't want to speci ct "Unspecified".	fy which WAN to
Ping thro	ough: Unspecifi	ied 🔽	
	Host / IP V Host / IP DNS	IP Address:	
Result	Gateway 1 Gateway 2 Gateway 3		Clear
			*

#### Diagnostics >> Ping Diagnosis

Ping Diagnosis	
○ IPV4 ③ IPV6	
Ping IPv6 Address:	
Run	
Result	Clear
	<u>~</u>
	~

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose <b>Unspecified</b> to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.



Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

### 3.16.8 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Bandwidth	Management >>	Sessions Limit
-----------	---------------	----------------

Enab	le 🔘 Disable	
Default	Max Sessions:	100
imitatio.	n List	
	Start IP	End IP

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

Diagnostics >> Data Flow Monitor

Refresh Seconds: 10 💌 Page: 1 💌 🛛 🛔						Refresh
Index	IP Address	TX rate(Kbps)	RX rate(Kbps) 😪	Sessions	Action	APP QoS
1	192.168.1.10_CARRIE- 0C7CB251	34	1	138	Block	None 💌
		0 (ID 11	0 (ID 1)	<b>6</b>		
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak		
WAN1	172.16.3.130	40 / 2476 / Auto	9 / 4022 / Auto	138		
WAN2		0 / 0 / Auto	0 / 0 / Auto	0		
WAN3			0 / 0 / Auto			
Total		4ባ / 2476 / Auto	9 / 4022 / Auto	UR,/ RAF		

Enable Data Flow Monitor

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

3. (Kbps): shared bandwidth

+ : residual bandwidth used Current/Peak are average.

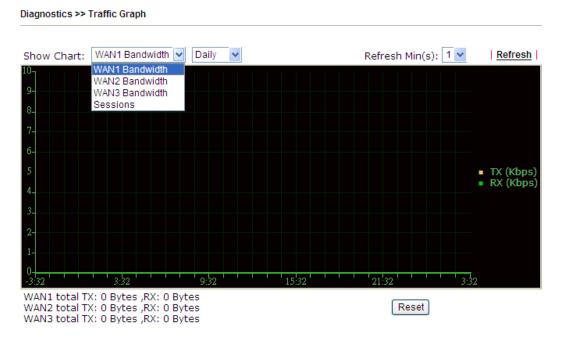


Item Description			
Enable Data Flow Monitor	Check this box to enable this function.		
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 10  10 15 30		
Refresh	Click this link to refresh this page manually.		
Index	Display the number of the data flow.		
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.		
	within 5 minutes. Page: 1 V Refresh Sessions Action APP QoS 1 Block None V Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column. Page: 1 V Refresh Sessions Action APP QoS blocked / 299 Unblock None V		
Current /Peak/Speed	<ul> <li>Current means current transmission rate and receiving rate for WAN interface.</li> <li>Peak means the highest peak value detected by the router in data transmission.</li> <li>Speed means line speed specified in WAN&gt;&gt;General Setup. If you do not specify any rate at that page, here will display Auto for instead.</li> </ul>		



# 3.16.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

### 3.16.10 Trace Route

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

Diagnostics >> Trace Route		
Trace Route		
⊙ IPV4 O IPV6		
Trace through:	Unspecified 🗸	
Protocol:	ICMP 🗸	
Host / IP Address:		
	Run	
Result		Clear
		<u></u>

#### or

Diagnostics >> Trace Route

○ IPV4		
Trace Host / IP Address:		
	Run	
Result		Clear
		~

Item	Description	
IPv4 / IPv6	Click one of them to display corresponding information for it.	
Trace through	Use the drop down list to choose the interface that you want to ping through.	



<b>Protocol</b> Use the drop down list to choose the protocol th to ping through.		
Host/IP Address	It indicates the IP address of the host.	
Trace Host/IP Address	It indicates the IPv6 address of the host.	
Run	Click this button to start route tracing work.	
Clear	Click this link to remove the result on the window.	

# 3.16.11 Web Firewall Syslog

Such page provides real-time syslog and displays the information on the screen.

### For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

USB Application >> Syslog Explorer		
Web Syslog	USB Syslog	
web sysiog	USD Syslog	
Enable Web Syslog		Export Refresh Clear
	Syslog Type User 🔽 Display Mo	de Stop record when fulls
Time		Message

Available settings are explained as follows:

Item	Description	
Enable Web Syslog	Check this box to enable the function of Web Syslog.	
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. User V User Firewall Call WAN VPN All	
Export	Click this link to save the data as a file.	
Refresh	Click this link to refresh this page manually.	
Clear	Click this link to clear information on this page.	
Display Mode	There are two modes for you to choose.	

	Stop record when fulls Stop record when fulls Always record the new event
	<b>Stop record when fulls</b> – when the capacity of syslog is full, the system will stop recording.
	Always record the new event – only the newest events will be recorded by the system.
TimeDisplay the time of the event occurred.	
Message	Display the information for each event.

## For USB Syslog

This page displays the syslog recorded on the USB storage disk.

USB Application >> Syslog Explorer

Web Syslog

USB Syslog

Time	Log Type		Message			
Folder: n/a	File: n/a	Page: n/a	Log Type: n/a			
Note:The syslog will show while the saved syslog file size is over 1MB.						

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

## 3.16.12 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

Diagnostics >>	IPv6	TSPC	Status
----------------	------	------	--------

WAN1	WAN2	WAN3		<u>Refres</u> h
TSPC Enabled				
TSPC Connectio	n Status			
Local Endpoint	tv4 Address :	114.44.54.220		
Local Endpoint v6 Address :		2001:05c0:1400:000b:0000:0000:0000:10b9		
Router DNS name :		88886666.broker.freenet6.net		
Remote Endpoint v4 Address :		81.171.72.11		
Remote Endpo	intv6Address:	2001:05c0:1400:00	)0b:0000:0000:0000:10b8	
Tspc Prefix :		2001:05c0:1502:0d	100:0000:0000:0000:0000	
Tspc Prefixlen	:	56		
Tunnel Broker	:	amsterdam.freenet	6.net	
Tunnel Status :		Connected		



Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

# 3.17 External Devices

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

External Devices All Devices Access Point Devices

## 3.17.1 All Devices

External Device >> All Devices

External Device Auto Discovery

Below shows available devices that connected externally:

For security reason:

If you have changed the administrator password on External Device, please click the Account button to retype new username and password. Otherwise, the router will be unable to monitor the External Device device properly. Click the Clear button to Clear the off-line information and account information.

Available settings are explained as follows:

Item	Description
External Device Auto	Check this box to detect the external device automatically
Discovery	and display on this page.

From this web page, check the box of **External Device Auto Discovery**. 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.

<b>~</b>	External	Device Auto Discovery
Ext	ornal Dovi	cos Connected

External D	evices connected	
Below sh	ows available devices that connected externally:	
<u>On Line</u>	Vigor3900, Connection Uptime:00:00:16	
	IP Address:196.17.5.140	Account Clear
<u>On Line</u>	Vigor2960, Connection Uptime:00:00:16	
	IP Address:196.17.5.184	Account Clear
<u>On Line</u>	VigorIPPBX 3510, Connection Uptime:00:00:16	
	IP Address:196.17.3.1	Account Clear
<u>On Line</u>	Vigor2820 Series, Connection Uptime:00:00:16	
	IP Address:196.17.3.193	Account Clear
<u>On Line</u>	VigorIPPBX 3510, Connection Uptime:00:00:16	
	IP Address:196.17.3.160	Account Clear
On Line	Vigor2850 Series, Connection Uptime:00:00:16	

When you finished the configuration, click **OK** to save it.

Note: Only DrayTek products can be detected by this function.
---------------------------------------------------------------

### 3.17.2 Access Point Devices

Vigor2860 can be treated as a server, named APM server, which manages access point devices. Basically, Vigor2860 can manage up to 5 devices (Access Point, treated as a client) at one time.

The access point shall be registered to Vigor2860 first. Then the Status page will display the registered access point automatically when this page is open. This page is very convenient for the network administrator to control or modify the managed access point at any time.

### Status

The status page can display related information of the registered client such as device name, IP address, SSID, encryption, channel, the number of the wireless clients, firmware version of the access point, the accessing password about the managed access point.

	Status	WLAN	l Profile						
								<u>Clear</u>	<u>Refresh</u>
Index	Device N	Jame	IP Address	SSID	Encryption	Ch.	WL Client	Version Pa	issword
<u>1</u>	AP800_00507F	CC08BC	192,168,86,12					E	assword 🛛 🗙
2	AP800_00507F	C91E78	192,168,86,13					F	assword 🛛 🗴
Note:									

Green : Online Red : Offline Grey : Hidden SSID

Item	Description
Index	Click the index number link to open the detailed configuration page for the selected entry.
Clear	Click it to remove all the settings modified in this page.



Refresh	Click it to refresh current page.		
Index	Click the number index to open the settings page of the device.		
Device Name	Display the name of the device.		
IP Address	Display the IP address of the device.		
SSID	Display the SSID configure by the device.		
Encryption	Display the encryption method used by the device.		
Ch. (Channel)	Display the channel used by the device.		
WL Client	Display the number of the host (wireless client) connecting to such AP device.		
Version	Display firmware version used by the device.		
Password	Click the button to review /edit the username and password of the device. 192.168.1.1/doc/spdeviceauth.htm - Google Chr		

### **WLAN Profile**

This page can be used to configure **five** different WLAN profiles which can be applied to the connected AP devices. The WLAN profile can be used for connected Vigor Access Point only.

Status	WLAN Profile				
					Set to Factory Defau
Profile Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Control
Default	DrayTek-LAN-A	WPA+WPA2/PSK	Enable	None	None

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default

	settings.				
Profile Name	Display the name of the profile scanned by Vigor router.				
Main SSID	Display the SSID used by the Vigor router.				
Security	Display the mode used by the Vigor router.				
Multi-SSID	Display if the multi-SSID function is enabled or not.				
WLAN ACL	Display the access control (None, White List, or Black List) configured for such profile.				
Rate Control	Display if the function of rate control is enabled or not.				
Clone	It will pop up a window for you to copy the parameter settings from a profile to another profile.				
	Clone WLAN Profile Setting         Original Profile Name       Default         Renamed as				
	<ul> <li>Original Profile Name – Display the original profile name of the selected index.</li> <li>Select Profile Index – Choose the index number of the profile that you want to clone from.</li> <li>Renamed as – When a profile index is selected, the original name will be displayed in the box first. You can change it by typing a new name.</li> </ul>				
Edit	It allows you to modify the detailed settings for each WLAN profile.				
Cancel	It can cancel the settings you just made on this page.				
Apply To Device	The WLAN profile can be applied to specified Device (AP device) if it is required. Simply check the box on the left side of the WLAN profile you want, and then click the <b>Apply To Device</b> button. The following dialog box will appear.				
	<ul> <li>Existing Device – This field will display the access point connected to Vigor2860 and worked well.</li> <li>Selected Device – This field will display the access point which will be applied with the WLAN profile.</li> <li>Choose one of the devices from the Existing Device and click with the worked to the right field of Selected Device.</li> </ul>				



Then click Apply. The selected device now will be applied
with the selected WLAN profile.

To edit a WALN profile, follow the step listed below:

1. Check the box of the entry that you want to edit. Then, click the **Edit** button.

Profile Name	Main SSID	Security
Default	DrayTek-LAN-A	WPA+WPA2/F
	Clone	Edit

2. The following page will appear. All the wireless connection related to Vigor Access Point (e.g., AP800) will be shown as follows.

External Device >> Access Point Devices

Device Setting	
Profile Name	
Administrator	
Password	
2nd Subnet	OEnable ODisable

	WLAN General Setting
Mode	Mixed(11g+11n)
Channel	2417MHz (Channel 2) 💌
WMM	⊙Enable ⊙Disable
Tx Power	100% 🗸

Cancel Next

Item	Description		
Device Setting	<b>Profile Name</b> – Type a name for such profile.		
	<b>Administrator</b> – Type the username for such profile. It will be used for the clients trying to connect to the access point.		
	<ul> <li>Password – Type a password for such profile. It will be used for the clients trying to connect to the access point.</li> <li>2<sup>nd</sup> Subnet – Click Enable to enable the second subnet.</li> </ul>		
WLAN General Setting	<ul> <li>Mode – Specify a connection mode for wireless network.</li> <li>Channel – Specify a channel for the wireless connection.</li> <li>WMM – To apply WMM parameters for wireless data transmission, please click the Enable radio button.</li> </ul>		
	<b>Tx Power -</b> The default setting is the maximum (100%). Lower down the value may degrade range and throughput of wireless.		

Cancel	Cancel the setting configured on this page.
Next	Access into the next setting page.

3. Type the required information and click **Next** to open next page. You can configure the settings for SSID1, SSID2, SSID3 and SSID4 respectively.

SSID1	SSID2	SSID3	SSID4				
			SSID				
Active	💿 Enable 🔇	Disable					
SSID	DrayTek	LAN-	A 🔽 📃 Hide	SSID			
VLAN	0 (0:u	ntag)					
Isolate	From LAN	E From mem	ber				
		s	ecurity Setting				
	Disable	~					
	Set up <u>RADIU</u> WPA	<u>S Server</u> if 802.	.1X is enabled.				
	WPA Algori			AES 💿	TKIP/AES		
	Pass Phras						
Encryption	Key Renew	al Interval	-	onds			
	PMK Cache	Period	0 Mini	utes			
	Pre-Auther	itication	○Enable (	Disable	е		
	WEP	Key if WEP is e	nabled				
	802.1X WE			Disable			
		-	Access Control		<u> </u>		
Mode	None 💌						
							~
List							~
		Client's MAC	Address :	: : : :	: :	:	
		Add	Delete	Edit	Cance	el	
		В	andwidth Limit				
Status	🔵 Enable (	) Disable	Auto Adjus	stment	🔘 Enable	💿 Disab	le
Upload	0	Kbps	Download		0		Kbps
		Back	Cancel	Finish			

External Device >> Access Point Devices

Item	Description
SSID	Active – Click Enable to activate such SSID setting.
SSID if it is required. Next, choose LAN-A or LAN-B a the subnet. If required, you can check the box of <b>Hide</b>	<b>SSID</b> . Then it will not be recognized by wireless station when the user tries to search the Access Point for
	<b>VLAN</b> – Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.
	<b>Isolate – From LAN -</b> Check this box to make the wireless clients (stations) with the same SSID not accessing for wired PC in LAN.
	Isolate – From Member - Check this box to make the



	wireless clients (stations) with the same SSID not accessing for each other.
Security Setting	<b>Disable</b> – There are several modes provided for you to choose.
	WPA Algorithm –Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
	<ul> <li>Pass Phrase –Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.</li> </ul>
	Key Renewal Interval – Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Such feature is available for WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.
	<ul> <li>PMK Cache Period –Set the expired time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for WPA2/802.1 mode.</li> </ul>
	<b>Pre-Authentication</b> – Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure (Only valid in WPA2). <b>Enable</b> - Enable IEEE 802.1X Pre-Authentication.
	WEP Key – Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for WEP mode.
	<b>802.1X WEP - Enable</b> - Enable the WEP Encryption.
Access Control	<b>Mode (Black List/White List)</b> – Select to enable black list or white list filter policy.
	<ul> <li>List –Display all MAC addresses that are edited before.</li> <li>Client's MAC Address –Manually enter the MAC address of wireless client.</li> </ul>
	<ul> <li>Add –Add a new MAC address into the list.</li> <li>Delete –Delete the selected MAC address in the list.</li> <li>Edit –Edit the selected MAC address in the list.</li> </ul>
	<b>Cancel -</b> Give up the access control set up.
Bandwidth Limit	<b>Status</b> – Click <b>Enable</b> to enable the function of bandwidth limit.

	<b>Upload</b> – Type the value as the uploading rate of data transmission.
	<b>Auto Adjustment</b> – Click <b>Enable</b> to make the router manage the bandwidth limit automatically.
	<b>Download -</b> Type the value as the downloading rate of data transmission.
Back	Return to the previous setting page.
Cancel	Cancel the setting configured on this page.
Finish	Complete the configuration of this page.

4. Continue to type the required information on this page. When you finished the configuration, click **Finish**. A new WLAN profile has been created as follows.

Status	WLAN Profile					
				5	iet to Factory Defa	<u>ult</u>
Profile Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Control	
Default	DravTek-LAN-A	WPA+WPA2/PSK	Enable	None	None	
WLAN_2 Floor	DrayTek	Disable	Disable	None	None	x
						C
						ĥ

External Device >> Access Point Devices

#### Vigor2860 Series User's Guide



# 4.1 How to configure settings for IPv6 Service in Vigor2860

Due to the shortage of IPv4 address, more and more countries use IPv6 to solve the problem. However, to continually use the original rich resources of IPv4, both IPv6 and IPv4 networks shall communicate for each other via intercommunication mechanism to complete the shifting job from IPv4 to IPv6 gradually. At present, there are three common types of intercommunication mechanisms:

#### Dual Stack

The user can use both IPv4 and IPv6 techniques at the same time. That means adding an IPv6 stack on the origin network layer to let the host own the communication capability of IPv4 and IPv6.

#### Tunnel

Both IPv6 hosts can communication for each other via existing IPv4 network environment. The IPv6 packets will be encapsulated with the header of IPv4 first. Later, the packets will be transformed and judged by IPv4 router. Once the packets arrive the border between IPv4 and IPv6, the header of IPv4 on the packets will be removed. Then, the packets with IPv6 address will be forwarded to the destination of IPv6 network.

#### • Translation

Such feature is active only for the user who uses IPv4 to communicate with other user using IPv4 service.

Before configuring the settings on Vigor2860, you need to know which connection type that your IPv6 service used.

**Note**: For the IPv6 service, you have to configure WAN/LAN settings before using the service.

### I. Configuring the WAN Settings

For the IPv6 WAN settings for Vigor2860, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

1. Access into the web user interface of Viogr2860. Open **WAN>> Internet Access**. Choose one of the WAN interfaces as the one supporting IPv6 service. Then, click the IPv6 button of the selected WAN.

WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL	Static or Dynamic IP	*	Details Page IPv6
WAN2		Ethernet	PPPoE	*	Details Page
WAN3		USB	None	*	Details Page IPv6

Note : Only one WAN can support IPv6.



**Note:** Only one WAN interface support IPv6 service at one time. In this example, WAN2 is chosen as the one supporting IPv6 service.

2. In the following figure, use the drop down list to choose a proper connection type.

WAN >> Internet Access

WAN 2								
PPPoE		Static or Dynamic IP		F	PPTP/L2	тр	1	Pv6
Internet Ac	cess Mode							
Connectio	on Type		Offline		~			
			Offline					
			PPP					
		ОК	TSPC AICCU DHCPv Static IF	6 Client V6				

Different connection types will bring out different configuration page. Refer to the following:

• PPP – Dual Stack application, IPv4 and IPv6 services can be utilized at the same time

Choose PPP and type the information for PPPoE of IPv4.

WAN >> Internet Access

WAN 2	_					
PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6		
Enable	🔿 Disable	PPP/MP Setup				
ISP Access Setup Username Password Index(1-15) in <u>S</u> =>,	73768635@hinet.net	Idle Ti IP Add WA Fixed	uthentication meout N IP Alias IP: O Yes O No (D IP Address			
WAN Connection I Mode Ping IP TTL:	ARP Detect	O Sp	efault MAC Address Decify a MAC Address Address: 00 (10 (	AA A8 B7 6A		
МТО	1442 (Max:1492)					
	ОК	Car	ncel			

Access into the setting page for IPv6 service, it is not necessary for you to configure anything. WAN >> Internet Access

PPPoE	Static or Dynamic	IP	PPTP/L2TP	IPv6
Internet Acces	s Mode			
Connection T	/pe	PPP	✓	
Note: IPv4 W/	N setting should be PPPo	E client.		
Note: IPv4 WA	N setting should be PPPo	E client.		

Click **OK** and open **Online Status**. If the connection is successful, you will get the IP address for IPv4 and IPv6 at the same time.

#### **Online Status**

	IPv4		IPv6		
LAN Status	Prim	ary DNS: 168.9	5,192,1	Secondary DN	IS: 168.95.1.1
IP Address	TX Packets	RX Pac			
192.168.1.1	0	3085			
WAN 1 Status					>> Dial PPPo
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
	07770	0	0	0	0
WAN 2 Status					>> Drop PPPc
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:54	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
114.44.49.54	168.95.98.254	800	4761	821	6617
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	-
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
		0	0	0	0
ADSL Information	( ADSL Firmware	Version: 05-0	4-04-04-00-01)		
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RX C	RC errs
	0	0	0	0	
ADSL Status M	ode State	Up Speed	Down Speed	SNR Margin	Loop Att.
	READY	0	0	0	0

#### **Online Status**

Physical Connect	ion			System Uptime: 0:2:32
	IPv4		IPv6	
AN Status				
IP Address				
2001:B010:73	00:201:21D:AAFF:F	EA6:2568/64 (Glol	pal)	
FE80::21D:AA	FF:FEA6:2568/64 (L	.ink)		
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
7	4	690	328	
NAN2 IPv6 Statu	6			>> Drop PPP
Enable	Mode	Up Time		
Yes	PPP	0:02:08		
IP			Gateway IP	
2001:B010:73	00:201:21D:AAFF:F	EA6:256A/128 (Gl	obal) FE80::90:1A00:242	:AD52
FE80::1D:AAF	-:FEA6:256A/128 (L	.ink)		
DNS IP				
2001:B000:16 2001:B000:16				
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
7	9	544	1126	

#### • TSPC – Tunnel application, both IPv6 hosts communicate through IPv4 network

Choose **TSPC** and type the information for TSPC service.

**Note:** While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the TSPC information is obtained from <u>http://gogo6.com/</u> after applied for the service.)

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type	Т	SPC 💌	
TSPC Configuration			
Username	cacahsu		
Password	•••••		
Confirm Password	•••••		
Tunnel Broker	broker.freenet6.ne	t	

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

#### **Online Status**

WAN >> Internet Access

Physical Connect	tion			System Uptime: 0:2:3
	IPv4		IPv6	
LAN Status				
IP Address				
2001:5C0:15	02:D00:21D:AAFF:FE	EA6:2568/64 (Glob	al	
FE80::21D:A4	NFF:FEA6:2568/64 (L	.ink)	Statements in	
TX Packets	RX Packets	TX Bytes	RX Bytes	
88	121	15596	10249	
WAN2 IP∨6 Statu	S			
Enable	Mode	Up Time		
Yes	TSPC	0:01:40		
IP			Gateway IP	
2001:5C0:14	00:B::10B9/128 (Gld	obal)	1242	
FE80::722C:3	(559/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes	
127	89	9219	15866	

#### • AICCU – Tunnel application

WAN >> Internet Access

Choose AICCU and type the information for AICCU of IPv6.

**Note:** While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the AICCU information is obtained from <u>https://www.sixxs.net/main/</u> after applied for the service.)

PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
Internet Access Mode				
Connection Type		AICCU	×	
AICCU Configuration				
🗌 Always On				
Username	JCR3-SIXXS			
Password	••••			
Confirm Password	••••			
Tunnel Broker	tic.sixxs.net			
Subnet Prefix	2001:4DD0:FF00:88	305::2	/ 64	
	enabled,AICCU connecti			

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status				
Physical Connect	ion			System Uptime: 0:1:18
	IPv4		IPv6	1199 PRPA
LAN Status				
IP Address				
	00:83E4:21D:AAFF		obal)	
TX Packets	RX Packets	TX Bytes	RX Bytes	
147	187	34205	19176	
WAN2 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	AICCU	0:00:48		
IP			Gateway IP	
2001:4DD0:FF	00:3E4::2/64 (Glob	al)		
FE80::4CD0:F	F00:3E4:2/64 (Link)	)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
186	137	16438	33093	

#### • DHCPv6 Client

Online Status

Choose DHCPv6 Client. Click one of the identity associations and type the IAID number.

2			
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet A	ccess Mode		
Connecti	on Type Di	HCPv6 Client 💌	
DHCPv6 C	lient Configuration		
Identity	Association O Prefix Delegation	Non-temporary Address	
IAID (Id	entity Association ID) 972573680		

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Physical Connect	ion			System Uptime: 0:0:50
	IPv4		IPv6	
LAN Status				
IP Address				
FE80::21D:AA	FF:FEA6:2568/64 (L	ink)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
6	2	588	156	
WAN2 IPv6 Statu	s			
Enable	Mode	Up Time		
Yes	DHCPv6 Client	0:00:40		
IP			Gateway IP	
2001:B010:73	300:201:21D:AAFF:F	EA6:256A/64 (Glob	pal)	
2001:1111:22	22:5555:21D:AAFF: 22:3333::1111/128 FF:FEA6:256A/64 (L	3 (Global)	obal)	
DNS IP				
2001:4860:48 2001:4860:48				
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
14	5	1174	694	

Vigor2860 Series User's Guide

#### • Static IPv6

Choose Static IPv6. Type IPv6 address, Prefix Length and Gateway Address.

WAN >>	Internet	Access
	million not	100000

PPOE	Static or Dynamic IP	PPTP/L2TP	IP∨6
Internet Acces	s Mode		
Connection T	ype Stat	ic IPv6 🛛 👻	
Static IPv6 Add	Iress configuration		
IPv6 Addres	55	/ Prefix Length	
2001:B010:730	00:201:21D:AAFF:FEA6:256A	/ 64 Add I	Delete
Current IPv6	Address Table		
Index IPv6	Address/Prefix Length	Scope	-
	:B010:7300:201:21D:AAFF:FEA6:25	5A/64 Global	
	:1111:2222:5555:21D:AAFF:FEA6:2	56A/64 Global	
3 FE80	::21D:AAFF:FEA6:256A/64	Link	
			~
Static IDe Cat	eway configuration		Contraction of the local division of the loc
IPv6 Gatew	av Address		
::			
has a			
Lay			

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

#### **Online Status**

Physical Connect	ion			System Uptime: 0:4:2
	IPv4		IPv6	
LAN Status				
IP Address				
FE80::21D:AA	FF:FEA6:2568/64 (L	ink)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
4	0	312	0	
WAN2 IPv6 Status	3			
Enable	Mode	Up Time		
Yes	Static IPv6	0:03:56		
IP			Gateway IP	
2001:B010:73	00:201:21D:AAFF:F	EA6:256A/64 (Glob	pal)	
	22:5555:21D:AAFF FF:FEA6:256A/64 (L		obal)	
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
8	2	608	364	

#### **II. Configuring the LAN Settings**

After finished the WAN settings for IPv6, please configure the LAN settings to make the router's client getting the IPv6 address.

1. Access into the web user interface of Viogr2860. Open LAN>> General Setup. Click the IPv6 button.

**Note**: Only the subnet of **LAN1** supports IPv6 feature.

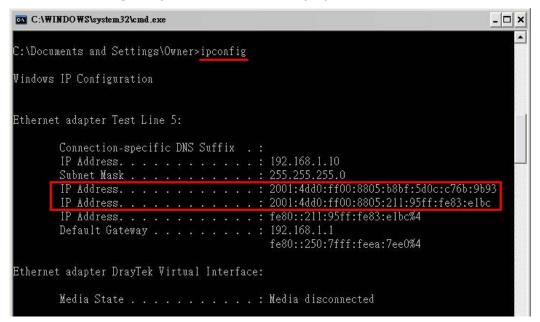
Ethernet TCP / IP and DHCP Set	up LAN	1 IPv6 Setup	
● Enable       ○ Disable         Advertisement Lifetime       18	00 Seconds (Rang	e : 600 - 9000)	
DHCPv6 Server Configuration			
💿 Enable Server 🛛 🔿 Dis	able Server		
Start IPv6 Address	2001:1111:2222:3333:::	1111	
End IPv6 Address	2001:1111:2222:3333:::	2222	
DNS Server IPv6 Address			
Primary DNS Server	2001:4860:4860::8888		
Secondary DNS Server	2001:4860:4860::8844		
Static IPv6 Address configurat IPv6 Address Current IPv6 Address Table	ion	/ Prefix Length / AddDe	elete
Index IPv6 Address/Pref l FE80::21D:AAFF:FE		Scope	

- 2. In the field of **RADVD Configuration**, the default setting is **Enable**. The client's PC will ask RADVD service for the Prefix of IPv6 address automatically, and generate an Interface ID by itself to compose a full and unique IPv6 address.
- 3. In the field of **HCPv6 Server Configuration**, when DHCPv6 service is enabled, you can assign available IPv6 address for the client manually.

**Note:** When both mechanisms are enabled, the client can determine which mechanism to be used (e.g., the default mechanism for Windows7 is RADVD).

#### III. Confirming IPv6 Service Run Successfully

1. Make sure you have get the correct IPv6 IP address. Get into MS-DOS interface and type the command of "ipconfig". Refer to the following figure.



From the above figure we can see IPv6 IP address has been captured by the system.

2. Use the Ping command to ping any IPv6 address indicating an IPv6 website. For example, <u>www.kame.net</u> is a website supporting IPv4 IP and IPv6 IP services. Its IPv6 address is seen with a format of 2001:200:dff:fff1:216:3eff:feb1:44d7.

C:\WINDOWS\system32\cmd.exe	<u>- 🗆 ×</u>
C:\Documents and Settings\Owner>ping 2001:200:dff:fff1:216:3eff:feb1:44d7	
Pinging 2001:200:dff:fff1:216:3eff:feb1:44d7 with 32 bytes of data:	
Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=743ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=623ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=626ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=617ms	
Ping statistics for 2001:200:dff:fff1:216:3eff:feb1:44d7: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 617ms, Maximum = 743ms, Average = 652ms	
C:\Documents and Settings\Owner>	<b>→</b>

After getting the above message, it means the IPv6 service has been activated successfully.

3. Connect to the website for IPv6. Open a web browser and type an URL of IPv6, e.g., <u>www.kame.net</u>. If your computer accesses into the website by using IPv6 address, you may see a turtle dancing on the screen. If not, only a steady turtle will be seen.



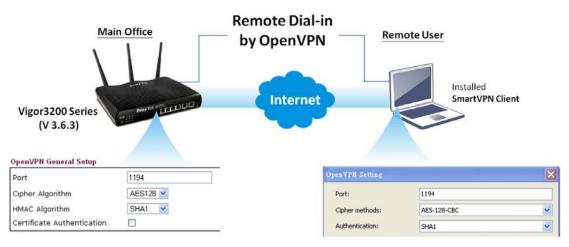
If you can see a turtle dancing on the screen, that means IPv6 service is ready for you to access and utilize.

# 4.2 How to establish OpenVPN - host to LAN tunnels(authenticated without CA) via SmartVPN Client?

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. OpenVPN uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows remote users to authenticate for each other using a pre-shared secret key, certificate, or username/password. When OpenVPN is used in a multi-client server configuration, it allows the server to release an authentication certificate for every client via signature and Certificate authority.

Below shows an illustration for successful OpenVPN tunnel established between Vigor router (Main Office) and notebook (Remote User). The OpenVPN settings for both ends shall be the same. Otherwise, the VPN connection is unable to establish successfully.



Note:

The OpenVPN choice supported by Vigor3200 Series can work with Windows, Linux and Mac OS. For the Windows-based PC, users can use SmartVPN client to simplify settings in the client devices.

**Note:** Before configuring settings for OpenVPN, you should install **SmartVPN Client 4.1.0.1** on your PC and latest firmware version on your Vigor router.

#### Settings for Router (Main Office)

- 1. Access into the web user interface of Vigor router.
- 2. Open VPN and Remote Access >> OpenVPN General Setup to configure the OpenVPN setting with disabled Certificate Authentication. Click OK to save the settings.

VPN and Remote Access >> Op	enVPN General Setup
OpenVPN General Setup	
Port	1194
Cipher Algorithm	AES128 V
HMAC Algorithm	SHA1 💌
Certificate Authentication	
Note: OpenVPN on vigor only s	support UDP protocol and TUN device interface currently. So please setup

corresponding configurations on the client side.

- OK
- 3. Open VPN and Remote Access >> Remote Dial-in User to create a profiles for Dial-in User. Set the Username (e.g., jos) and Password (e.g., jos) for OpenVPN. Click OK to save the settings.

VPN and Remote Access >> Remote Dial-in User

Index No. 1		
User account and Authentication	Username	jos
Enable this account	Password	•••
Idle Timeout 300 second(s)	Enable Mobile One-Tim	
Allowed Dial-In Type	PIN Code	
РРТР	Secret	
IPsec Tunnel	IKE Authentication Method	
L2TP with IPsec Policy None		
SSL Tunnel	Pre-Shared Key	
✓ OpenVPN Tunnel	IKE Pre-Shared Key	
	Digital Signature(X.509	)
Specify Remote Node	None 🗸	
Remote Client IP		
	IPsec Security Method	

#### Settings for PC (Remote User)

1. Execute **SmartVPN Client.** Click **Insert** to create a new dial-in VPN profile (e.g., Profile 6).

<b>Dray</b> Te	Smart VPN Client
Shee O. Enable/Alley	v IPSec NAT-Traversal and L2TP
This step will add the AssumeUDPEncapsul computer. For more i	Prohibit/Dserversion of the and the lationContextOnSendRule registry value to infomation, please read the article Q240262 Microsoft Knowledgement Base.
Step 1. Dial to ISP	
	gotten a public IP, you can skip this step.
	gotten a public IP, you can skip this step.
If you have already	gotten a public IP, you can skip this step.

Type a name (e.g., Profile 6) as the Profile Name and an IP address (e.g., 200.200.200.200) as VPN Server IP. Set jos/jos as the User Name/Password. Click OpenVPN as the type of VPN and click OK to display the OpenVPN Setting dialog.

Dial To VPN Profile Name : Profile 6			
Auto re-dial after disconnect. Redial attempts :	3		
Redial interval :	30 seconds		Contra
Auto run when system start up.			×
VPN Server IP/HOST Name(such as	123.45.67.8 Port:	1194	
200.200.200.200	Cipher methods:	AES-128-CBC	*
User Name : jos	Authentication:	SHA1	~
Password : ***	Certificate Authenticati	ion	
Enable mobile One Time Passv	rord (mOTP) CA cert:	Browse.	
Configure Sec	ret for mOTP Client cert:	Browse.	
Type of VPN	Client key:	Browse.	
	CL2TP Fallback to SSL Tunnel		
	OpenVPN     Port:	443	
PPTP Encryption	OK	Cancel	
No encryption			
Require encryption			
Maximum strength encrypti	xn		
Authentication method	PAD 🖌		
Use default gateway on rem	ote network More		
OK	Cancel		

3. Configure the Port number, Cipher methods and Authentication as the settings defined above. Then click **OK**.



#### **Checking the VPN Connection Status**

Now both ends (router and remote PC) are configured well.

- 1. Access into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>Connection Management** to check the VPN connection status. From the following figure, we can know that the remote user can access the Vigor router's LAN successfully by using the username/password (jos/jos).

VPN and Remote Access >> Connection Management

al-out Tool	Refresh Seconds : 10 🔽 Refre
General Mode:	✓ Dial
Backup Mode:	Dial
Load Balance Mode:	✓ Dial

Current Page: 1							ge No.	Go >>
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	<sup>e</sup> UpTime
( jo Local User	1 os ) r Database <sup>AES</sup>	OpenVPN <b>188.188</b> -SHA1 Auth via V	.188.188 VAN1 192.168.1.1	1/32 1	4 52	20	52 (	0:0:31 Drop

'inging 192.168.1.1 with 32 bytes of data:	-
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	

## 4.3 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening USB Application>>File Explorer. If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SAMBA server or FTP server.

Samba service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure Disk Connected appears on the **Connection Status** as the figure shown below:

USB Applicatio	n >> USB Disk Status		
USB Mass Stor	age Device Status		
Connection S	itatus Disk Connec	ted	Disconnect USB Disk
Write Protect	t Status: No		
Disk Capacity	/: 2009 MB		
USB Disk User	rs Connected		Refresh
Index	Service	IP Address(Port)	Username
Note: If the w	rite protect switch o	of USB disk is turned on, the USB	disk is in READ-ONLY mode. No data

can be written to it.

2. Then, please open **USB Application** >> **USB General Settings** to enable Samba service.

General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English
Samba Service Settings(Network Neig	hborhood)
Enable     Disable	
Access Mode	
CLAN Only CLAN And WAN	
NetBios Name Service	
Workgroup Name	
Host Name	Vigor2860
Note: 1. If Charset is set to "English", 2. Multi-session ftp download v connection mechanism, such as better performance.	Vigor2860 , only English long file name is supported. vill be banned by Router FTP server. If your ftp client have mult s FileZilla, you may limit client connections setting to 1 to get be the same as the host name. The workgroup name and the h

USB Application >> USB General Settings

name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; : " <> \* + = / \ | ?.

OK	

3. Setup a user account for the FTP service by using **USB Application** >>**USB User Management.** Click **Enable** to enable FTP/Samba User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

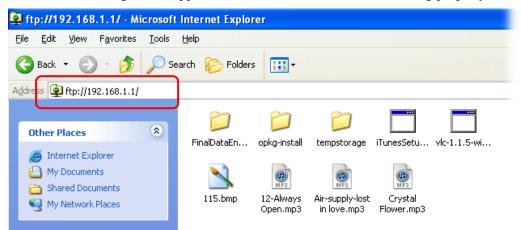
FTP/Samba User	Inable O Disable
Username	user1
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	<b>1</b>
Access Rule	
File	🗹 Read 🛛 Write 🗌 Delete
Directory	☑ List □ Create □ Remove
The folder name can onl	$\gamma$ contain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( )

USB Application >> USB User Management

- 4. Click **OK** to save the configuration.
- 5. Make sure the FTP service is running properly. Please open a browser and type <u>ftp://192.168.1.1</u>. Use the account "**user1**" to login.

Log On a	As 🛛 🔀
<b>?</b> >	Either the server does not allow anonymous logins or the e-mail address was not accepted.
	FTP server: 192.168.1.1
	User name:
	Password:
	After you log on, you can add this server to your Favorites and return to it easily.
⚠	FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.
	Learn more about using Web Folders.
	Log on anonymously

6. When the following screen appears, it means the FTP service is running properly.



7. Return to **USB Application** >> **USB Disk Status**. The information for FTP server will be shown as below.

USB Application >> USB Disk Status

USB Mass Sto	rage Device Stat	us		
Connection	Status: Disk Co	onnected	Disconnect U	SB Disk
Write Protec	ct Status: No			
Disk Capacit	:y: 2009 MB			
USB Disk Use	ers Connected			<u>Refresh</u>
Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.10(1963)	user1	Drop

Now, users in LAN of Vigor2710 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application** >>**USB User Management.** 

# 4.4 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPSec Tunnel (Main Mode)



#### **Configuration on Vigor Router for Head Office**

- 1. Log into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

LAN-to-LA View: 💿	N Profiles: All O Tru	nk				Set to	Factory Default
Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>		х		<u>17.</u>		х	
<u>2.</u>		x		<u>18.</u>		х	
<u>3.</u>		х		<u>19.</u>		Х	
<u>4.</u>		x		<u>20.</u>		х	
<u>5.</u>		х		<u>21.</u>		х	
<u>6.</u>		×		<u>22.</u>		X	
7		×		23		×	

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*), and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.

Profile Index : 1					
1. Common Settings					
Profile Name VF	PN Server		Call Direction	O Both O Dial	Out 💽 Dial-in
VPN Dial-Out Through WAN1 Netbios Naming Packet I Multicast via VPN I (for some IGMP,IP-Camera,	Pass OBlock Pass OBlock	~	Enable PING PING to the IP	to keep alive	

Vigor2860 Series User's Guide

4. Now navigate to the next section, **Dial-In Settings** to check PPTP, IPSec Tunnel and L2TP boxes. Check the box of **Specify Remote...** and type the **Peer VPN Server IP** (e.g., 218.242.130.19 in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

3. Dial-In Settings	
Allowed Dial-In Type	Username ???
✓ РРТР	Password
✓ IPsec Tunnel	VJ Compression On Off
L2TP with IPsec Policy None	
	IKE Authentication Method
Specify Remote VPN Gateway	▼ Pre-Shared Key
Peer VPN Server IP	IKE Pre-Shared Key
218.242.130.19	✓ Digital Signature(X.509)
or Peer ID	None 🛩
	Local ID
	<ul> <li>Alternative Subject Name First</li> </ul>
	🔿 Subject Name First
	IPsec Security Method
	Medium(AH)
	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
4. Gre over IPsec Settings	

5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for remote side.

			High(ESP	)	💌 DES 💌	3DES 🗹 AES
4. Gre over IPsec Settings						
Enable IPsec Dial-Out	t function GRE over IPsec					
Logical Traffic	My GRE IP			Pee	r GRE IP	
5. TCP/IP Network Settings	3					
My WAN IP	0.0.0.0		RIP Direc	tion		Disable 🖌
Remote Gateway IP	0.0.0.0		From firs do	t sub	net to remo	te network, you have to
Remote Network IP	192.168.1.0		40			Route 🛩
Remote Network Mask	255.255.255.0					
Local Network IP	192.168.1.9	ر ا		-	efault route	to this VPN tunnel ( Only
Local Network Mask	255.255.255.0		Single W			)
	More					
	ОК	Cle	ear	Can	cel	

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

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from branch office).

Dial-out Tool						R	efres	h Seco	nds: 5	<ul> <li>Refresh</li> </ul>
		( V2920 ) <sup>·</sup>	172.16.2	.145		✓ D	ial			
/PN Connecti	on Status									
Current Page	: 1							Pag	je No.	Go >
VPN	Туре	Remote IP	Virtua	l Network	Tx Pkts	Tx R (Bp		Rx Pkts	Rx Rate (Bps)	UpTime
1 (VPN Server)	IPSec Tunnel DES-SHA1 Auth	218.242.1	30.19	192,168,1.0	0/24	353	з	291	3 0	:13:58 Drop
							· · Da	ta ic o	ncrypted	
						mmmnoon		nta 15 C	погурсой	

VPN and Remote Access >> Connection Management

#### Configuration on Vigor Router for Branch Office

- 1. Log into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

VPN and R	emote Acces	s >> LAN to LA	N				
LAN-to-LAI View: ⓒ A	N Profiles:	nk				Set to	Factory Default
Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>		х		<u>17.</u>		х	
<u>2.</u>		х		<u>18.</u>		х	
<u>3.</u>		Х		<u>19.</u>		Х	
<u>4.</u>		×		<u>20.</u>		×	
<u>5.</u>		Х		<u>21.</u>		Х	
<u>6.</u>		×		<u>22.</u>		×	
7.		×		23		X	

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Client*), and check the box of **Enable This Profile**. For such Vigor router will be set as a **client**, the call direction shall be set as **Dial-out**. Check the box of **Always on** for a permanent VPN connection.

Profile Index : 1 1. Common Settings			
Profile Name	VPN Client		Call Direction O Both ③ Dial-Out O Dial-in
VPN Dial-Out Through Netbios Naming Packe	t 💿 Pass 🔘 Block	~	Idle Timeout     -1     second(s)       Image: Display the second secon
Multicast via VPN (for some IGMP,IP-C	● Pass ○ Block amera,DHCP Relayetc.)		

2. Dial-Out Settings

VPN and Remote Access >> LAN to LAN

4. Now navigate to the next section, **Dial-Out Settings** to select the **IPSec Tunnel** service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

2. Dial-Out Settings	
Type of Server I am calling	Username ???
О РРТР	Password
IPsec Tunnel	PPP Authentication PAP/CHAP
C L2TP with IPsec Policy None	VJ Compression On
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 218.242.133.91	IKE Authentication Method <ul> <li>Pre-Shared Key</li> <li>IKE Pre-Shared Key</li> </ul>
	O Digital Signature(X.509)
	Peer ID None 😒
	Local ID
	Iternative Subject Name First
	🔘 Subject Name First
	IPsec Security Method
	O Medium(AH)
	O High(ESP) 3DES with Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:

5. Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for the remote side.

		•
4. Gre over IPsec Settings	5	
🔲 Enable IPsec Dial-Ou	It function GRE over IPsec	2
Logical Traffic	My GRE IP	Peer GRE IP
5. TCP/IP Network Setting	js	
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 do
Remote Network IP	172.17.1.0	Route 🗸
Remote Network Mask	255.255.255.0	
Local Network IP	192.168.1.9	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	
	More	
	ОК	Clear Cancel

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

7. Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from head office).

)ial-out Tool						Re	fresh	Seco	nds : 🗄	× L	Refresh
		( V2920 ) 17	72.16.2.	145		<ul> <li>Dia</li> </ul>	al				
/PN Connecti	on Status										
	on otatao										
Current Page	: 1							Pad	e No.		Go 🖂
Current Page	: 1 Туре	Remote IP	Virtual	Network	Tx Pkts	Tx Ra (Bps		Pag Rx Pkts	e No. Rx Ra (Bps)	te IIn	Go >: Time

VPN and Remote Access >> Connection Management

### 4.5 How to Optimize the Bandwidth through QoS Technology

Have you ever gotten any problems in uploading/downloading files (Voice, video or email/data only) with the narrow/districted bandwidth you may share from the common Internet connection line? The advanced bandwidth management technology-QoS (Quality of Service) helps you to well allocate the bandwidth upon your demand of Voice, Video, or Data transferring. Let's see how to get the optimum bandwidth per your request by using DrayTek Vigor router as below.

Scenario: The Internet connection you got from ISP line is 2MB/512Kb. There are VoIP telephony network, IPTV set top box and data server at your home. Assume you want to allocate 30% of the bandwidth you got to VoIP demand, 50% for IPTV, 15% for mail/data, 5% for others. Let's see how easily it is to do the setting as below:

1. Open Bandwidth Management>> Quality of Service.



2. You will get the following page. Click the **Edit** link for **Class 1**.

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	101060.00Kbps/98180.00Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Class Ru Ind		Nam	ie				R	ule	Service Ty	pe
Clas	s 1							<u>Edit</u>		
Clas	s 2							Edit	Edit	

3. In the following page, type a name (e.g., VoIP) for such class and click **Add**. Bandwidth Management >> Quality of Service

DiffServ	
CodePoint	Service Type
-	-
	-

 Check the box of ACT. Click Edit to specify the local address. Bandwidth Management >> Quality of Service

ACT		
Ethernet Type	● IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	
Service Type	Predefined	
Note: Please choose/set	up the <u>Service Type</u> first.	

5. In the pop-up window, choose **Range Address** as the **Address Type** and type the start IP address and end IP address in relational fields. Click **OK** to save the settings and exit the window.

Address Type	Range Address 🐱
Start IP Address	172.16.1.240
End IP Address	172.16.1.241
Subnet Mask	0.0.0.0

6. Click **OK** again to save the settings.

Bandwidth Management >> Quality of Service

Rule Edit		
	ACT	
	Ethernet Type	⑧ IPv4 ◎ IPv6
	Local Address	172.16.1.240~172.16.1.241
	Remote Address	Any Edit
	DiffServ CodePoint	ANY 🗸
	Service Type	Predefined
	Note: Please choose/setup th	ne <u>Service Type</u> first.
		OK



7. The class rule for VoIP has been set. Click **OK** to return to previous page.

Bandwidth Management >> Quality of Service

lass Index	<b>x #1</b> 'oIP		🔲 та	ag packets as: Defau	lt 🗸
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY
		A	dd Edit Delet	te	
			OK Cancel		

8. Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

Class In	dex #2				
Name	IPTV		🔲 Та	ag packets as: Defau	ılt 💌
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Active 172.16.1.242 ~ 172.16.1.249		Any	ANY	ANY
		A	Add Edit Delet	te	
			OK Cancel		
			and		

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

Class Inc	lex #3				
Name	Data/Email		П Та	ag packets as: Defau	lt 💌
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Active	Any	Any	IP precedence 2	ANY
		A	Add Edit Dele	te	
			OK Cancel		

9. Assuming you get 2MB/512Kb Internet line. You can click the **Setup** link of WAN1 to set up the bandwidth for different groups among VoIP, IPTV and Data/Email.

Jenera	I Setup							Set t	to Factory D	etault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	101060.00Kbps/98180.00Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
Class R Ind		Nam	ie				R	ule	Service Ty	vpe
Clas	ss 1	V	oIP					Edit	,	
		T	νTV					Edit	Edit	
Clas	5S Z	16	r i v					Lun	Luit	

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

10. In the Setup page, check the box of **Enable the QoS Control**. Type 30, 50 and 15 in the boxes for VoIP, IPTV and Data/Email respectively. Check the box of **Enable UDP Bandwidth Control**.

Enable the QoS Co	ntrol OUT 💌	
Index	Class Name	Reserved_handwidth Ratio
Class 1	VoIP	30 %
Class 2	IPTV	50 %
Class 3	Data/Email	15 %
	Others	5 %
Enable UDP Bandw	idth Control	Limited_bandwidth Ratio 25
Outbound TCP ACK	( Prioritize	

11. Click **OK** to save the settings. The class rules for WAN1 are defined as shown below.

General	l Setup							Set t	o Factory D	<u>efault</u>
Index	Status	Bandwidth	Directio	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	101060.00Kbps/98180.00Kbps	Outbound	30%	50%	15%	5%	Inactive	<u>Status</u>	Setu
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>

## 4.6 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or V PN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

#### 1. Go to Bandwidth Management>>Quality of Service.

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	101060.00Kbps/98180.00Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setur
Class Ru Inde		Nam	ie				R	ule	Service Ty	pe
Clas	s 1							<u>Edit</u>		
Clas	s 2							Edit	<u>Edit</u>	
Clas	s 3							Edit		

2. Click **Setup** link of WAN(1/2/3). Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.

Bandwidth	Management >>	Quality of	Service
-----------	---------------	------------	---------

#### WAN2 General Setup

<b>~</b>	Enable the QoS Control	BOTH 🔽	
	WAN Inboun	IN OUT	lth
	WAN Outbou	BOTH	vidth

3. Set Inbound/Outbound bandwidth.

12 General Setup		
Enable the QoS Co	ntrol BOTH 🔽	
WAN I	nbound Bandwidth	100000 Kbps
WAN (	Outbound Bandwidth	100000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	VoIP	25 %

**Note:** The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

4. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1. Click **OK** to save the settings.

lass In	dex #1				
ame	E-mail		🔲 Tag	g packets as: Defa	ult
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Active	Any	Any	ANY	ANY
		4	Add Edit Delete	•	

5. Click the **Setup** link for WAN2. The user can set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP. Click **OK** to save the settings.

WAN2 General Setu Enable the QoS		
WA	N Inbound Bandwidth	100000 Kbps
WA	N Outbound Bandwidth	100000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Bar	ndwidth Control	Limited_bandwidth Ratio 25 %
Outbound TCP	ACK Prioritize	
1	OK Clear	Cancel

Bandwidth Management >> Quality of Service

6. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth for **HTTPS**. And click **OK**.

Class Ind	dex #2 HTTPS			ag packets as: Defau	ilt 🗸				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type				
1	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY				
	Add Edit Delete								
			OK Cancel						

Bandwidth Management >> Quality of Service

#### 7. Click **Setup** link for WAN2.

Class 3

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

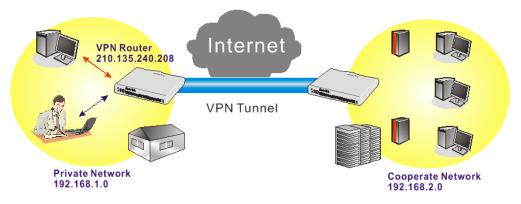
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	101060.00Kbps/98180.00Kbps	Outbound	30%	50%	15%	5%	Inactive	Status	Setup
WAN2	Enable	100000Kbps/100000Kbps	Both	25%	25%	25%	25%	Inactive	<u>Status</u>	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Class R	ule			25%	25%	25%				
Index Nam		e				R	lule	Service Ty	ре	
Clas	s 1	E-	mail					<u>Edit</u>		

<u>Edit</u>

8. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic influent other application. Click **OK**.

Enable the QoS C	ontrol BOTH 🛩	
WAN	Inbound Bandwidth	100000 Kbps
WAN	Outbound Bandwidth	100000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
Enable UDP Bandy		Limited_bandwidth Ratio 25

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.





10. Click **Edit** for Class 3 to open a new window. In this index, the user will set reserved bandwidth for **VPN**.

me	VPN		🗌 Та	g packets as: Defa	ult
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
			Add Edit Delete	•	

Bandwidth Management >> Quality of Service

11. Click Add to open the following window. Check the ACT box, first.

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	
Service Type	Predefined	
Note: Please choose/	setup the <u>Service Type</u> first.	

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

12. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

ACT	
Ethernet Type	● IPv4 ○ IPv6
Local Address	192.168.1.0 Ed
Remote Address	192.168.2.0 Ed
DiffServ CodePoint	ANY
Service Type	Predefined
Note: Please choose/set	up the <u>Service Type</u> first.

## 4.7 How to Implement the LDAP/AD Authentication for User Management?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 3200 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

- 1. Access into the web user interface of the Vigor router.
- 2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings.

Applications >> Active Directory /LDAP	

Active Directory /LDAP		Set to Factory Default
General Setup	Active Directory / LDAP Profiles	
Enable		
Bind Type		Regular Mode 💌
Server IP Ad	ldress	172.16.2.8
Destination (	Port	389
Regular DN		uid=vpntest,ou=vpnuser,dc=ms,dc=draytel
Regular Pass	word	1234
		OK Cancel

There are three types of bind type supported:

- **Simple Mode** Just simply do the bind authentication without any search action.
- Anonymous Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode** Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
- 3. Create LDAP server profiles. Click the **Active Directory /LDAP** tab to open the profile web page and click any one of the index number link.

If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.



#### Applications >> Active Directory /LDAP>> Server Profiles

Name	rd1
Common Name Identifier	uid
ase Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com
Group Distinguished Name	cn=rd1,ou=group,dc=ms,dc=draytek,dc=c

#### and

Applications >> Active Directory /LDAP>> Server Profiles

Name	shrd
Common Name Identifier	uid
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com
Group Distinguished Name	cn=shrd,ou=group,dc=ms,dc=draytek,dc=

- 4. Click **OK** to save the settings above.
- 5. Open User Management>>General Setup. Select User-Based as the Mode option.

User Management >> General Setup

Notice :	
<ol> <li>User Management will refer to active rules in user-based firewall mode.</li> </ol>	s in Data Filter as whitelists and blacklists
<ol> <li>Users match the above lists will not be re-</li> </ol>	quired for authentication.
The firewall rules policy will still valid	-
The firewall rules policy will still valid.	a state of the sta
3. Otherwise, authentication required for use	
· · · · · · · · · · · · · · · · · · ·	
3. Otherwise, authentication required for use	
<ol> <li>Otherwise, authentication required for use The firewall rules designated in the user p</li> </ol>	orofile's policy will still valid. <u>Preview</u> <u>Set to Factory Default</u>
<ol> <li>Otherwise, authentication required for use The firewall rules designated in the user p</li> <li>Landing Page (Max 255 characters)</li> </ol>	profile's policy will still valid. <u>Preview</u> <u>Set to Factory Default</u>   script'>
<ol> <li>Otherwise, authentication required for use The firewall rules designated in the user p</li> <li>Landing Page (Max 255 characters)</li> <li><body stats="1"><script <u="" language="javas&lt;/li&gt; &lt;/ol&gt;&lt;/td&gt;&lt;td&gt;profile" policy="" s="" still="" valid.="" will="">Preview</u> <u>Set to Factory Default</u>  script'></td></tr></tbody></table></script></body></li></ol>	

6. Then open **VPN and Remote Access>>PPP General Setup** to **check** the profile(s) that will be authenticated with LDAP server.

PPP/MP Protocol			LDAP Server Pro	iles for PPP Authentication
Dial-In PPP Authentication	PAP or (	CHAP 🔽		rd1 shrd
Dial-In PPP Encryptio (MPPE)	n Optiona	I MPPE 💌		sind
Mutual Authentication	n (PAP)	🛇 Yes 💿 No		
Username				
Password				
P Address Assignment (When DHCP Disable se		sers		
Assigned IP start	LAN 1	192.168.1.200	]	
	LAN 2	192.168.2.200	]	
	LAN 3	192.168.3.200	]	
	LAN 4	192.168.4.200	]	
			1	

VPN and Remote Access >> PPP General Setup

7. After above configurations, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.

## 4.8 How to use Landing Page Feature

**Landing Page** is a special feature configured under **User Management**. It can specify the message, content to be seen or specify which website to be accessed into when users try to access into the Internet by passing the authentication. Here, we take Vigor2860 series router as an example.

## Example 1: Users can see the message for landing page after logging into Internet successfully

- 1. Open the web user interface of Vigor2860.
- 2. Open User Management -> General Setup to get the following page. In the field of Landing Page, please type the words of "Login Success". Please note that the maximum number of characters to be typed here is 255.

al Setup				
Mode:	User-Based 👻			
in use 2. Users	Management will refer to active rules er-based firewall mode. match the above lists will not be rec			nd blacklists
3. Other	rewall rules policy will still valid. wise, authentication required for use rewall rules designated in the user p			sts.
3. Other The fi	wise, authentication required for use	rofile's policy will still	valid.	sts. Set to Factory Default

3. Now you can enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.

User Management	>> User Profile	
User Profile Table		
Profile	Name	
<u>1.</u>	admin	
<u>2.</u>	Dial-In User	
<u>3.</u>		
<u>4.</u>		
5		

4. In the following page, check the box of **Landing page** and click **OK** to save the settings.

User Management >>User Profile

Enable this account	
User Name	Caca
Password	••••
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None 💌
Log	None 💌
Pop Browser Tracking Window	
Authentication	☑ Web ☑ Alert Tool ☑ Telnet
Landing Page	
Enable Time Quota	0 min(s) Refresh , Add more 0 min(s)
Index(1-15) in <u>Schedule</u> Setup:	

5. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please type the correct username and password.

Username	CaCa
Password	••••
	Login
	Login

6. Click **Login**. If the logging is successful, you will see the message of Login Success from the browser you use.



#### Example 2 : The system will connect to <u>http://www.draytek.com</u> automatically after logging into Internet successfully

1. In the field of **Landing Page**, please type the words as below:

" <body stats="1"><script language="javascript"></th></tr><tr><td>window.location='http://www.draytek.com'</script></body> "
------------------------------------------------------------------------------------------------------------------------------

Mode: User-Based 💌	
Notice : 1. User Management will refer to active rules in in user-based firewall mode.	
<ol> <li>Users match the above lists will not be required for equivalent to the firewall rules policy will still valid.</li> <li>Otherwise, authentication required for users the firewall rules designated in the user process.</li> </ol>	s not matched the above lists. file's policy will still valid.
The firewall rules policy will still valid. 3. Otherwise, authentication required for user. The firewall rules designated in the user pro Landing Page (Max 255 characters)	s not matched the above lists. file's policy will still valid. <u>Preview</u>   <u>Set to Factory Default</u>
The firewall rules policy will still valid. 3. Otherwise, authentication required for user. The firewall rules designated in the user pro	not matched the above lists. file's policy will still valid. <u>Preview</u> <u>Set to Factory Default</u>

2. Next, enable the **Landing Page** function. Open **User Management -> User Profile** and click one of the index number (e.g., index number 3) links.

User Management >> User Profile			
User Profile Table			
Profile	Name		
<u>1.</u>	admin		
<u>2.</u>	Dial-In User		
<u>3.</u>			
<u>4.</u>			
5			

3. In the following page, check the box of Landing page and click OK to save the settings.

User Management >>User Profile

Enable this account	
User Name	Саса
Password	••••
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None 💌
Log	None 🗸
Pop Browser Tracking Window	
Authentication	🗹 Web 🗹 Alert Tool 🗹 Telnet
Landing Page	V
Enable Time Quota	0 min(s) Refresh , Add more 0 min(s)
Index(1-15) in <u>Schedule</u> Setup:	

4. Open any browser (e.g., FireFox, Internet Explorer). The logging page will appear and asks for username and password. Please type the correct username and password.

Username	CaCa
Password	••••
	Login

5. Click **Login**. If the logging is successful, you will be directed into the website of <u>www.draytek.com</u>.

🕽 Dray Tek Corp - Headquarters 🤤		
🔿 C 🏦 🔇 www.draytek.com/us	er/index.php?Lang=en-US	公 4 3
DrayTek Group 🧰 翻譯字典 🧰 電腦科技		🗀 其他書籤
DrawTak	New Homepage MyVigor Login Global (En	glish ) 💌 Search Go
<b>Dray</b> Tek	About DrayTek Products Support Solution	ns Contact Us
		💽 📷
What's New  DrayTek Milestone Development for Reliable IP-based Network >> more		or2830Vn plus
Awards/Reviews > DrayTek Vigor/PPBX 2820 got the positive review by MREZA magazine in Croatia	Card and a state of the Card a	Multis Mathematic ADSL2+
>> more		1 2 3 4 5
Events 🗟 TEXP2 DrayTek Unveils Latest	Solutions	HANNOVER - GERMANY
Solutions for Next Generation Networks at ITEXPO East	DrayTek 2012 Product Catalogue	<b>CeBIT</b> 8-10 March 2012 Hall 13, C56
Jan 31 to Feb 3 2012 Miami FL, USA	SMB Productivity Enhancement solution	Product Quick Finder
>> more	NrauTek IP PRY solutions	Please Select V

### 4.9 How to Send out SMS via Vigor Router

Such vigor router supports the feature of SMS.

- 1. Go to Application >>Short Message Service to create a new SMS profile.
  - Applications Dynamic DNS Schedule RADIUS Active Directory /LDAP UPnP IGMP Wake on LAN Short Message Service
- 2. Click any index number link to access into the following web page.

Application >> Short Message Service

Short Message Service Porfile:   Set to Factory Defa				tory Default
Index	Profile Name	Service Provider	<b>Destination Number</b>	Status
<u>1.</u>				х
<u>2.</u>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				Х

3. In the configuration page, please type profile name, username, password, destination name, quota, sending interval and choose a correct Service Provider. Click **OK** to save the settings and exit this page.

Application >> Short Message Service

Profile Index: 1		
Enable SMS Setup	⊙Enable ○Disable	
Profile Name	For Warning	
Service Provider	kotsms.com.tw (TW)	~
Username	11111	
Password	••••	
Destination Number	123456789	
Quota	10	
Sending Interval	60þ	(seconds)
Send a test Message		
ОК	Clear Cano	el

Click **Enable** to enable SMS setup; type a name for identification as **Profile Name**; use the drop down list to choose the **Service Provider** that you apply for SMS; type the **Username** and **Password** that you apply for SMS; type the telephone number that you want to receive the SMS in the field of **Destination Number**; type the total number of the messages that the router will send out in the field of **Quota**; type the shortest time



interval for the system to send SMS in the field of **Sending Interval**. For example, it is set with 60 (seconds). If WAN1 disconnects for three times within 60 seconds, the system will send the SMS notification just for once. The **Send a test Message** button allows you to send one SMS to the user just for test.

4. Now, a new SMS proifle has been created.

Index	Profile Name	Service Provider	Destination Number	Status
<u>1.</u>	For Warning	KotSMS	123456789	V
<u>2.</u>				Х
<u>3.</u>				Х
<u>4.</u>				х
<u>5.</u>				Х
<u>6.</u>				х
<u>7.</u>				Х
8.				х

Application >> Short Message Service

5. Go to WAN>>General Setup. In this case, choose the WAN2 link as an example.

WAN >> General Setup

Load Balaı	nce Mode:	Auto Weight		
Setup				
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	V	VDSL/-	0 / 0	Always On
WAN2	v	Ethernet/Auto negotiation	0 / 0	Always On
WAN3	V	USB/-	0 / 0	Always On

Note: Line Speed only used for load balance mode: according to Line Speed

OK

Configure the settings as the following figure. Choose one of the SMS profiles. In this example, the profile "For warning" is selected. Then, click OK to save the settings.
 WAN >> General Setup

Enable:	Yes 💌
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
DSL Modem Code:	Default 💌
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion :	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Send <u>SMS</u> if line drops out	1-For Warning
Send Mail Alert if line drops	s out
Active Mode:	Always On 💙

Note : In DSL auto mode, the router will reboot automatically while switching between VDSL and ADSL lines.



When such WAN (e.g., WAN2 in this example) disconnects due to some reason, the system will use other WAN for connection instead and send SMS to notify the user (destination number #123456789). However, if there is no available WAN for connection, the system will send SMS to inform the user after reconnecting WAN2 successfully.

# 4.10 How to Create an Account for MyVigor

The website of MyVigor (a server located on <u>http://myvigor.draytek.com</u>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

## 4.10.1 Create an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

Web-Filter License [Status:Not Activated]				<u>Activa</u>
Setup Query Server	auto-selected		Find more	
Setup Test Server	auto-selected		Find more	
Neb Content Filter Profi	le Table:		Set to Factory	Defaul
Profile	Name	Profile	Name	
<u>1.</u>	Default	<u>5.</u>		
<u>2.</u>		<u>6.</u>		
<u>3.</u>		<u>7.</u>		
<u>4.</u>		<u>8.</u>		
- <body><center> &lt; that is categorFilter.Please co</center></body>	br> The required with %CL% <br ntact your system</br 	ested Web page >has been blocked by administrator for fu	Cache : L1 + L2 C from %SIP% to %URL% %RNAME% Web Content rther	
<pre>kbr&gt;that is categor Filter.Please co information.</pre>	br> The required with %CL% our system r>	ested Web page >has been blocked by administrator for fu OK tion to open the fol	from %SIP% to %URL% %RNAME% Web Content rther owing page.	5
<pre><body><center> <browdy><center> &gt;that is categor</center></browdy></center></body></pre> Filter.Please co information.	br> The required with %CL% our system r>	ested Web page >has been blocked by administrator for fu OK tion to open the fol	from %SIP% to %URL% %RNAME% Web Content rther	5
ck System Maint	br> The required with %CL% our system r>	ested Web page >has been blocked by administrator for fu OK tion to open the fol	from %SIP% to %URL% %RNAME% Web Content rther owing page.	5
<pre>cbody&gt;<center> <center> that is categor Filter.Please co information.ck System Mainten ystem Maintenance &gt;&gt; / /eb-Filter License</center></center></pre>	br> The required with %CL% our system r>	ested Web page >has been blocked by administrator for fu OK tion to open the fol	from %SIP% to %URL% %RNAME% Web Content rther owing page.	lected



2. Click the Activate link. A login page for MyVigor web site will pop up automatically.

	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 : Password :	
Auth Code :	t xxhdd
	If you cannot read the word, <u>click here</u>
	Forgotten password? Login
Don't have a M	yVigor Account ? Create an account now
L	

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

- 3. Click the link of **Create an account now**.
- 4. Check to confirm that you accept the Agreement and click Accept.



**Dray** Tek

5. Type your personal information in this page and then click **Continue**.

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
		(3 ~ 20 characters)
Deserved	Password:*	••••
Personal		(4~20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	tion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND

6. Choose proper selection for your computer and click **Continue**.

Register		
Create an account - F	Please enter personal profile.	
Agreement	How did you find out about this website?	Internet 💌
<b>U</b> system	What kind of anti-virus do you use?	AntiVir
2 Personal	l would like to subscribe to the MyVigor e-letter.	
Information	I would like to receive DrayTek product news.	V
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

\*\*\*\*\* This is an automated message from myvigor draytek.com.\*\*\*\*\*

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site GO
Register Confirm	
	Thank for your register in VigorPro Web Site The Register process is completed
	Close Login

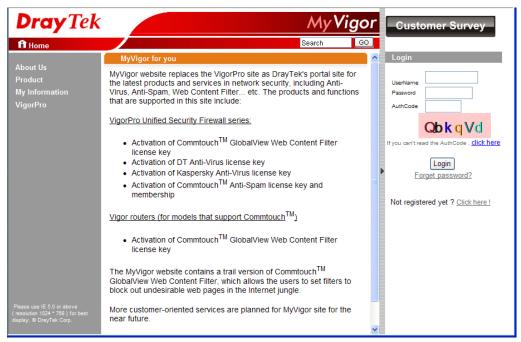
10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

		for your purchas	ment to register. jistration entitles you ed product and recei cts and services!	
LOGIN				
	UserName :	Mary		
	Password :	••••		
	Auth Code :	T4he1C	T4he1C	
		If you cannot read the wo	ord, <u>click here</u>	
		Forgotten passwor	d? Login	
	Don't have a	a MyVigor Account ?	Create an account	now
	lf you	u are having difficulty logging in.	contact our customer service.	

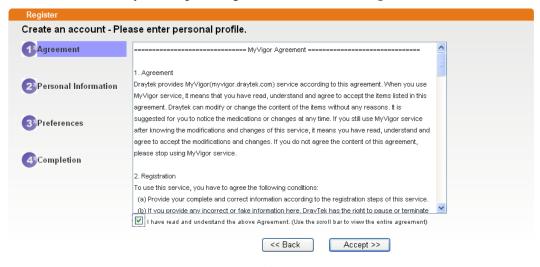
- Customer Service : (886) 3 597 2727 or
- 11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

## 4.10.2 Create an Account via MyVigor Web Site

1. Access into <u>http://myvigor.draytek.com</u>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



2. Check to confirm that you accept the Agreement and click Accept.



3. Type your personal information in this page and then click Continue.

	Account Informati	on
Agreement	UserName:*	Mary Check Account
Descend	Password:*	••••
Personal Information	Confirm Password:*	( 4 ~ 20 characters : Do not set the same as the username.)
	Personal Informat	ion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND
	Career.*	Supervisor

4. Choose proper selection for your computer and click **Continue**.

Register		
Create an account -	Please enter personal profile.	
Agreement	How did you find out about this website?	Internet
<b>U</b> . groomont	What kind of anti-virus do you use?	AntiVir
2 Personal	I would like to subscribe to the MyVigor e-letter.	V
Information	l would like to receive DrayTek product news.	V
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>

**Dray** Tek

5. Now you have created an account successfully. Click START.



6. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

\*\*\*\*\* This is an automated message from myvigor draytek.com.\*\*\*\*\*

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



The Confirm message of New Owner(Mary) maybe timeout Please try again or contact to draytek.com

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

	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 :	Mary
Password :	••••
Auth Code :	T4he1C T4he1C
	If you cannot read the word, <u>click here</u>
	Forgotten password? Login
Don't have a N	MyVigor Account ? Create an account now
(	

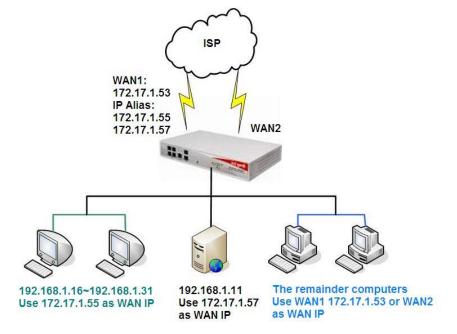
If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

# 4.11 How to Setup Address Mapping

NAT Address Mapping function lets you specify the outgoing IP address(es) for one internal IP address or a block of internal IP addresses.

Now, Vigor2860 and VigorPro 5510 Series support this feature. We will take an example to introduce how to make use of this feature. The scenario is shown below, with a Vigor2860 involved. Both WAN connections are active and the WAN1 connection has 3 IP addresses.



- 1. Log into the web user interface of Vigor2860.
- 2. Open WAN>>Internet Access. For WAN1, choose Static or Dynamic IP as the Access Mode.

WAN >> Internet Access

Internet	Access				
Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL	Static or Dynamic IP	*	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page IPv6
WAN3		USB	None	*	Details Page IPv6

Note : Only one WAN can support IPv6.

3. Click the **Details Page** of WAN 1 to open the following page. From the above figure, set main WAN IP address as *172.17.1.53*.

PPPoE Static or Dynamic IP		PPTP/L2TP			
💿 Enable (	) Disable	WANI	P Network Settings	WAN IP Alias	
Keep WAN Connectio	ann WAN Connection		otain an IP address a	nutomatically	
Enable PING to		Rout	ter Name	Vigor2860	
PING to the IP		Dom	iain Name	Router.Net	
PING Interval	0 minute(s)	*: F	Required for some	ISPs	
	o minuce(s)	_ 🔍 Sp	ecify an IP address		
WAN Connection Det	tection	IP A	ddress	172.167.1.53	
Mode	ARP Detect 🔽	Subr	net Mask	255.255.253.0	
Ping IP		Gate	eway IP Address	172.16.1.1	
TTL:			•		
		— 💿 De	efault MAC Addres	s	
мто	J 1500 (Max:1500)		Specify a MAC Address		
		MAC Address: 00 1D AA A6 26 19			
RIP Protocol					
Enable RIP			erver IP Address		
		Prima	ry IP Address	8.8.8.8	
		Secor	ndary IP Address	168.95.192.1	

Click the WAN IP Alias button to configure the other two IP addresses which are *172.17.1.55* and *172.17.1.57*. Make sure **Join IP NAT Pool** is not checked.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.		172.17.1.53	
2.	<b>~</b>	172.17.1.55	
З.		172.17.1.57	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	

The outgoing traffic is routed to WAN1 port or WAN2 port according to the Load-balance policy. When the traffic is routed to WAN1 port, by default WAN1 main IP address (*172.17.1.53* in this example) is used to replace the source private IP address. Therefore, all the client IP addresses will be transmitted to *172.17.1.53* by default.

Since you have additional IP addresses on WAN1 connection, you may want some of the internal PCs be presented to the Internet with different IP addresses. In this example, the server with IP address *192.168.1.11* is to be presented to the Internet as *172.17.1.57* and the computers with a block of IP addresses from *192.168.1.16* through *192.168.1.31* are to be presented as *172.17.1.55*.

4. Click **OK** to save the settings.

WAN >> Internet Access



5. Open **NAT** >> **Address Mapping**. Pay special attention to the Mask setup.

NAT >> Address Mapping	
------------------------	--

NAT >> Address Mapping

Address Map	ping Setup			Set to Facto	ory Default
Index	Protocol	Public IP	Private IP	Mask	Status
<u>1.</u>	ALL	172.16.2.132		/32	Х
<u>2.</u>	ALL	172.16.2.132		/32	х
<u>3.</u>	ALL	172.16.2.132		/32	х
<u>4.</u>	ALL	172.16.2.132		/32	х
<u>5.</u>	ALL	172.16.2.132		/32	х
<u>6.</u>	ALL	172.16.2.132		/32	×
<u>7.</u>	ALL	172.16.2.132		/32	х
<u>8.</u>	ALL	172.16.2.132		/32	×
<u>9.</u>	ALL	172.16.2.132		/32	×
<u>10.</u>	ALL	172.16.2.132		/32	х

6. Click Index number 1 and 2 to configure the details.

Index No. 2	
🗖 Enable	
Protocol:	ALL 💌
WAN Interface	WAN1 💌
WAN IP	2-172.16.1.55 💌
Private IP:	192.168.1.16
Subnet Mask:	/28 🗸
	OK Clear Cancel

Here the Private IP can be any IP address within the range of 192.168.1.16 through 192.168.1.31. The Subnet Mask defines the size of the IP range, and the Private IP is an indicator of the IP range. Therefore, the combination of Private IP and Subnet Mask determine the IP range.

7. Upon completing the above configuration, you have specified the outgoing IP address(es) for some specific computers. But you still have to specify the outgoing interface for them. Otherwise, the traffic may be routed out with IP address 172.17.1.55 or 172.17.1.57 through WAN2 port. The load-balance policies are below.

Index	Enable	Prot	ocol	WAN	Src IP Start	IP	Dest IP Start	Dest IP End	Dest Port Start	Move Up	Move Down
1		any	*	WAN1 💌			211.78.90.66	211.78.90.66			<u>Down</u>
2		any	*	WAN1 🔽			172.16.0.1	172.17.5.254		<u>UP</u>	Down
<u>3</u>		any	*	WAN1 💌						<u>UP</u>	Down
<u>4</u>		any	*	WAN1 🔽						<u>UP</u>	Down
<u>5</u>		any	~	WAN1 💌						<u>UP</u>	Down
<u>6</u>		any	*	WAN1 💌						<u>UP</u>	Down
Z		any	*	WAN1 💌						<u>UP</u>	Down
<u>8</u>		any	*	WAN1 💌						<u>UP</u>	Down
<u>9</u>		any	*	WAN1 💌						<u>UP</u>	Down
<u>10</u>		any	~	WAN1 💌						<u>UP</u>	Down
< <u>1-1</u>	0 11-20	21-3	<u>0   31-3</u>	<u>2</u> >>						N	lext >>

WAN >> Load-Balance Policy

8. Click Index number 1 and 2 to configure the details. Make sure **Auto failover to the other WAN** is unchecked.

Index: 1 🗹 Enable Protocol any ¥ Auto failover to the other WAN Binding WAN Interface WAN1 🔽 Src IP Start 192.168.1.11 Src IP End 192.168.1.11 Dest IP Start 211.78.90.66 Dest IP End 211.78.90.66 Dest Port Start Dest Port End OK Cancel

## WAN >> Load-Balance Policy

#### And

WAN >> Load-Balance Policy

ndex: 2		
	🗹 Enable	
	Protocol	any 💌
	Binding WAN Interface	WAN1 💌 📃 Auto failover to the other WAN
	Src IP Start	192.168.1.16
	Src IP End	192.168.1.31
	Dest IP Start	172.16.0.1
	Dest IP End	172.17.5.254
	Dest Port Start	
	Dest Port End	
		OK Cancel

9. Click **OK** to save the settings. The load-balance policy has been configured properly.

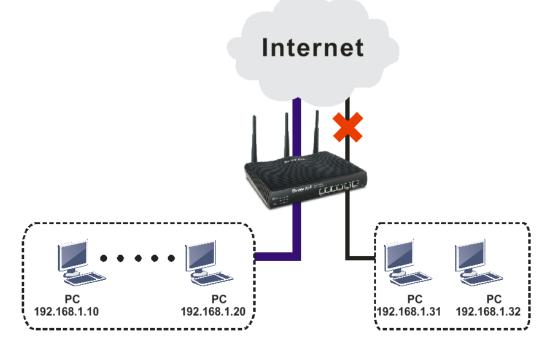
Index	Enable	Protoc	ol	WAN	Src IP Start	Src IP End	Dest IP Start		Dest Port Start	Move Up	Move Dowr
1	<ul><li>✓</li></ul>	any	*	WAN1 💌	192.168.1.11	192.168.1.11	211.78.90.66	211.78.90.66			Down
2	<b>~</b>	any	¥	WAN1 🔽	192.168.1.16	192.168.1.31	172.16.0.1	172.17.5.254		<u>UP</u>	Down
<u>3</u>		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>4</u>		any	*	WAN1 🔽						<u>UP</u>	Down
<u>5</u>		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>6</u>		any	*	WAN1 💌						<u>UP</u>	Down
Z		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
8		any	*	WAN1 💌						<u>UP</u>	Down
<u>9</u>		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>10</u>		any	~	WAN1 🔽						<u>UP</u>	Down
:< <u>1-1</u> (	<u>0   11-20</u>	<u>21-30</u>	<u>31-3</u>	<u>2</u> >>						Ν	lext >:

 Now, you bind some specific computers to some WAN IP alias for outgoing traffic. For incoming traffic, you still have to open the relevant ports by using **Port Redirection**, **DMZ** or **Open Ports** functions.



## 4.12 How to Configure Certain Computers Accessing to Internet

We can specify certain computers (e.g., 192.168.1.10 ~ 192.168.1.20) accessing to Internet through Vigor router. Others (e.g., 192.168.1.31 and 192.168.1.32) outside the range can get the source from LAN only.



The way we can use is to set two rules under **Firewall**. For **Rule 1** of **Set 2** under **Firewall>>Filter Setup** is used as the default setting, we has to create a new rule starting from Filter Rule 2 of Set 2.

- 1. Access into the web user interface of Vigor router.
- 2. Open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 2** button.

р
р

ilter Setup			Set to	Factory Default
Set	Comments	Set	Comments	
_ <b>1</b> [	Default Call Filter	<u>7.</u>		
<u>2.</u> [	Default Data Filter	<u>8.</u>		
1		<u>9.</u>		
4		<u>10.</u>		
<u>4</u> 5 6.		<u>11.</u>		
<u>6.</u>		<u>12.</u>		
irewa >> I	Filter Setup >> Edit Filter Set			
	Filter Setup >> Edit Filter Set			
ilter St 2	Filter Setup >> Edit Filter Set : Default Data Filter			
ilter St 2	: Default Data Filter	Comments	Move Up	Move Down
Filter Set 2 Comments	: Default Data Filter	Comments xNetBios -> DNS	Move Up	Move Down <u>Down</u>
Filter Set 2 Comments	: Default Data Filter Ile Active		Move Up <u>UP</u>	
ilter Sit 2 Comments Filte Ru	: Default Data Filter			<u>Down</u>

3. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., **block\_all**). Choose **Block If No Further Match** for the **Filter** setting. Then, click **OK**.

wall >> Edit Filter Set >> Edit Filter Rule		
r Set 2 Rule 2	_	
🗹 Check to enable the Filter Rul	e	
Comments:	block_all	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule ON:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care 🛛 🐱	
Application	Action/Profile	Syslog
Filter:	Block If No Further Match 💌	
Branch to Other Filter Set:	None 🔽	
Sessions Control	0 / 60000	

**Note:** In default, the router will check the packets starting with Set 2, Filter Rule 2 to Filter Rule 7. If **Block If No Further Match** for is selected for **Filter**, the firewall of the router would check the packets with the rules starting from Rule 3 to Rule 7. The packets not matching with the rules will be processed according to Rule 2.

- 4. Next, set another rule. Just open **Firewall>>Filter Setup**. Click the **Set 2** link and choose the **Filter Rule 3** button.
- 5. Check the box of **Check to enable the Filter Rule**. Type the comments (e.g., **open\_ip**). Click the **Edit** button for **Source IP**.

Sot 2 Pule 3		
🗹 Check to enable the Filter R	ule	
Comments:	open_ip	
Index(1-15) in Schedule Setup:		
Clear sessions when schedule ON:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care 🛛 🐱	
Application	Action/Profile	Syslog
Filter:	Block Immediately 🔽	
Branch to Other Filter Set:	None 🔽	

Firewall >> Edit Filter Set >> Edit Filter Rule

6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.

Address Type	Range Address 🛛 🔽
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	
IP Group	None 🔽
or <u>IP Object</u>	None 🔽
or IP Object	None 🔽
or IP Object	None 🔽
IP∨6 Group	None 🔽
or <u>IPv6 Object</u>	None 🔽
or IPv6 Object	None 🗸
or IPv6 Object	None 🔽

7. Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately.** Then, click **OK** to save the settings.

Firewall >	> Edit	Filter	Set >>	Edit	Filter	Rule
		THUCK I	300	L'une	i neoi	1 Marc

er Set 2 Rule 3		
🗹 Check to enable the Filter Ru	le	
Comments:	open_ip	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule ON: 	Enable	
Direction:	LAN/RT/VPN -> WAN	_
Source IP:	192.168.1.10~192.168.1.20	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter:	Pass Immediately 🔽	
Branch to Other Filter Set:	None 💉	

8. Both filter rules have been created. Click **OK**.

	ault Data Filter			
Filter Rule	Active	Comments	Move Up	Move Down
1		xNetBios -> DNS		Down
2		block_all	UP	Down
3		open_ip	UP	Down
4			UP	Down
5			<u>UP</u>	Down
6			UP	Down
7			UP	
			Next Filter \$	Set None 🐚

9. Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

# 4.13 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

#### Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

#### **URL Content Filter,**

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

## I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.

<b>Dray</b> Tek	Vigor 2860	Series	<b>.</b>					
Off 💌 166	CSM >> Web Content Filt	er Profile			_			
Dashboard Quick Start Wizard Service Activation Wizard Online Status	Web-Filter License [Status: Commtouch] [S	tart Date:2012-12-31 Expire	e Date:2013-01-08]	Activate	ł			
WAN	Setup Query Server	auto-selected	Find more					
LAN NAT	Setup Test Server	Find more						
Firewall User Management _	Web Content Filter Profile Table: Set to Factory Default							
Objects Setting CSM	Profile	Name	Profile	Name				
APP Enforcement Profile	rofile <u>1.</u> Default	Default	<u>5.</u>					
URL Content Filter Profile	<u>2.</u>		<u>6.</u>					
Web Content Filter Profile Bandwidth Management	<u>3.</u>		<u>7.</u>					
Applications	<u>4.</u>		<u>8.</u>					
VPN and Remote Access Certificate Management SSL VPN	Administration Message (Max 255 characters) Cache : L1 + L2 Cache 💌							
USB Application System Maintenance Diagnostics External Devices	<pre>        &lt;</br></br></br></br></br></br></br></br></br></br></br></br></br></pre>							
Admin mode Status: Ready	Legend: %SIP% - Source IP,	%DIP% - Destinatio	on IP, %URL%	- URL	a			

How to register/activate Web Content Filter (WCF) license? Please visit for getting more information:

\*How to Register AI/AV/AS/WCF Service (Service Activation Wizard) (http://www.draytek.com/user/SupportFAQDetail.php?ID=1955)

\***How to Activate Anti-Virus/Anti-Intrusion/Anti-Spam Service** (http://www.draytek.com/user/SupportFAQDetail.php?ID=286)

How to use the Web Content Filter (WCF) (http://www.draytek.com/user/SupportFAQDetail.php?ID=1953)

\* What the Web Content Filter (WCF) license benefits are, (<u>http://www.draytek.com/user/PdInfoDetail.php?Id=110</u>)



2. Open **CSM** >> **Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action, **Block**.

<b>Dray</b> Tek	Vigor 2860	) Series	<b>11</b>	₩ 🕞
Off 🔽 🮼	Clear All	Travel	Leisure & Recreation	Fashion & Beauty
Dashboard Quick Start Wizard Service Activation Wizard Online Status	Business Select All Clear All	Business	Job Search	Web-based Mail
WAN LAN NAT Firewall	Chating Select All Clear All	Chat	Instant Messaging	
User Management Objects Setting CSM APP Enforcement Profile URL Content Filter Profile Web Content Filter Profile Bandwidth Management	Computer-Internet Select All Clear All	Anonymizers  Download Sites Search Engine,Portals Malware Illegal Software	Forums & Newsgroups Streaming, Downloads Social Networking Botnets Information Security	Computers Phishing & Fraud Spam Sites Hacking Peer-to-Peer
Applications VPN and Remote Access Certificate Management SSL VPN USB Application System Maintenance Diagnostics External Devices	Other Select All Clear All	Adv & Pop-Ups Compromised Finance News Politics Restaurants & Dining General	Arts Dating & Personals Government Non-profits & NGOs Real Estate Shopping Cults	Transportation Education Health & Medicine Personal Sites Religion Translators Greeting cards

3. Enable this profile in **Firewall>>General Setup>>Default Rule**.

<b>Dray</b> Tek	Vigor 2860	Series			
Off ▼ 1₽6	Firewall >> General Setu	р			
Dashboard Quick Start Wizard Service Activation Wizard Online Status	General Setup				
	General Setup	Default Rule			
WAN LAN NAT	Actions for defa	ult rule:			
Firewall General Setup	Application		Action/Profile	Syslog	
Filter Setup	Filter		Pass 💙		
DoS Defense User Management	Sessions Contro	d	0 / 60000		
Objects Setting CSM	Quality of Servi	<u>ce</u>	None 🔽		
Bandwidth Management	Load-Balance p	olicy	Auto-Select 🔽		
Applications VPN and Remote Access	User Manageme	ent	None		
Certificate Management SSL VPN	APP Enforceme	nt	None 💌		
USB Application	URL Content Fil	<u>ter</u>	None 💙		
System Maintenance Diagnostics External Devices	Web Content Fi	lter	1-Default 💙		_
	Advance Settir	ng	Edit		
Admin mode Status: Ready					
					¥

4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

The requested Web page from 192.168.2.114 to www.facebook.com/ that is categorized with [Social Networking] has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by DrayTek]

# **Dray** Tek

# **II. Via URL Content Filter**

Objects Setting >> Keyword Object Setup

## A. Block the web page containing the word of "Facebook"

- 1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- 2. In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.

lame	Facebook
Contents	facebook
	Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space. You can replace a character with %HEX. Example:
	Contents: backdoo%72 virus keep%20out Result:
	1. backdoor 2. virus
	3. keep out

- 3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
- 4. Configure the settings as the following figure.

CSM >> URL Content Filter Profile

Profile Name:	Facebook	
Priority:	Either : URL Access Control	First 🕶 Log: None 💌
1.URL Access	Control	
🗹 Enab	le URL Access Control	Prevent web access from IP address
Actio	on:	Group/Object Selections
Block	Y Facebook	Edit
2.Web Featur	e	
🗌 Enat	le Restrict Web Feature	
Actio	in:	
Pass	🖌 🗌 Cookie 🔲 Proxy	🗌 Upload <u>File Extension Profile:</u> None 🛛 👻

5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.

al Setup			
eneral Setup	Default Rule		
Actions for def	ault rule:		
Application		Action/Profile	Syslog
Filter		Pass 💌	
Sessions Contr	ol	0 / 60000	
Quality of Serv	ice	None 💌	
Load-Balance	policy	Auto-Select 💌	
User Managem	ent	None	
APP Enforcem	ent	None 🗸	
URL Content F	ilter	1-Facebook 💌	
Web Content F	ilter	None 💙	
Advance Sett	ing	Edit	

#### B. Disallow users to play games on Facebook

- 1. Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- 2. In the field of **Contents**, please type *apps.facebook*. Configure the settings as the following figure.

Objects	Setting	>>	Keyword	Object	Setup
---------	---------	----	---------	--------	-------

Profile Index : 2					
Name	facebook-apps				
Contents	apps.facebook				
	Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.				
	You can replace a character with %HEX. Example: Contents: backdoo%72 virus keep%20out				
	Result: 1. backdoor 2. virus 3. keep out				
	OK Clear Cancel				

**Dray** Tek

- 3. Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
- 4. Configure the settings as the following figure.

Firewall >> General Setup

- 5. When you finished the above steps, please open **Firewall>>General Setup**.
- 6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

	D.C. K.D.L			
General Setup	Default Rule			
Actions for defa Application	ult rule:	Action/Profile	Syslog	
Filter		Pass V	Systog	
Sessions Contro	4	0 / 60000		
Quality of Servi	<u>ce</u>	None 💌		
Load-Balance p	olicy	Auto-Select 💌		
<u>User Manageme</u>	ent	None 💌		
APP Enforceme	nt	None 🗸		
URL Content Fil	ter	2-face.apps 💙		
Web Content Fi	lter	None 💙		
Advance Settir		Edit		

# 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 the power line and WLAN/LAN cable connections. Refer to "**1.3 Hardware Installation**" for details.
- 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

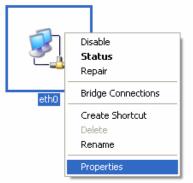


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

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     Elient for Microsoft Networks     Gos Packet Scheduler     Thernet Protocol (TCP/IP)			
Install Uninstall Properties			
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.			
<ul> <li>✓ Show icon in notification area when connected</li> <li>✓ Notify me when this connection has limited or no connectivity</li> </ul>			
OK Cancel			

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

Internet Protocol (TCP/IP) Prope	erties 🛛 🛛 🔀				
General Alternate Configuration					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
Obtain an IP address automatica	lly				
Use the following IP address: —					
IP address:					
S <u>u</u> bnet mask:					
Default gateway:	· · · ·				
Obtain DNS server address auto	matically				
OUse the following DNS server ad	dresses:				
Preferred DNS server:					
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.

			Netwo	ork			
how All	Displays Sou	nd Network Sta	rtup Disk				
	L	ocation: Autor	natic			•	
		Show: Built-	in Ether	net		•	
	TCP/	IP PPPoE	AppleTa	lk Proxie	s Eth	ernet	
Cor	nfigure IPv4:	Using DHCP			;		
	IP Address:	192.168.1.10			C	tenew DHC	P Lease
S	ubnet Mask:	255.255.255.0	D	DHCP Clien			
	Router:	192.168.1.1			(	If required)	
ſ	DNS Servers:						(Optional)
Sear	ch Domains:						(Optional)
IP	v6 Address:	fe80:0000:000	0:0000:	020a:95ff:fe	8d:72e	1	
		Configure IPv	6)				(?)

**Dray** Tek

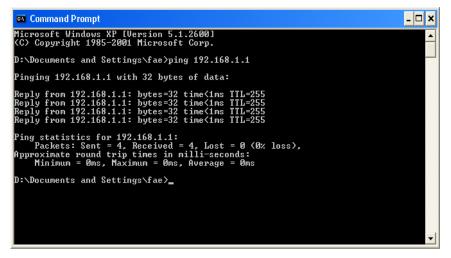
# 5.3 Pinging the Router from Your Computer

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 MacOs 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 Darw	Jan 3 02:24:18 on ttyp1 in! ek\$ ping 192.168.1.1	S
The second s	1 (192.168.1.1): 56 data bytes	
	92.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 19	92.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 19	92.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 19	92.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 19 AC	92.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
192.168.1.1	ping statistics	
5 packets trans	nitted, 5 packets received, 0% packet loss avg/max = 0.697/0.723/0.755 ms	

## 5.4 Checking If the ISP Settings are OK or Not

Open **WAN** >> **Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1-WAN3 to review the settings that you configured previously.

WAN >> Internet Access							
Internet	Access						
Index	Display Name	Physical Mode	Access Mode				
WAN1		ADSL / VDSL	PPPoE	Details Page IPv6			
WAN2		Ethernet	Static or Dynamic IP	✓ Details Page IPv6			
WAN3		USB	None	Details Page IPv6			

Note : Only one WAN can support IPv6.

# 5.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

## Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2860. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2860.

## USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



AN Status		DrayTek Vigor			RX Rate
				0	0
TX Packets	5	RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442		3807		0	0
W.B.I	The second	when Collins WAN	Log Network Infomation	Mart Charles	
Wall Log VPN Lo	g   User Acce	SS LOg   Call Log   WAR	Network Infomation	Net State	
Time	Host	Message			~
pr 12 09:17:49	Vigor		ocol:LCP(c021) ConfReg Ide	ntifier:0x03 ACCM: 0	0x0 Authe:
pr 12 09:17:49	Vigor		0 00 00 00 00 02 00 03 00		
pr 12 09:17:49	Vigor		locol:LCP(c021) ConfReq Ide	ntifier:0x00 MRU: 15	MODACCM
pr 12 09:17:49	Vigor	WAN2 PPPoE <== V:1			
pr 12 09:17:49	Vigor	[3G]Modem response: (			
pr 12 09:17:49	Vigor		0 00 00 00 00 02 00 02 00		
pr 12 09:17:49	Vigor		0 00 00 00 00 02 00 02 00		
pr 12 09:17:49	Vigor	[3G]Modem dial ATDT			
pr 12 09:17:49	Vigor	WAN2 PPPoE -> V:1			-
pr 12 09:17:49	Vigor	WAN2 PPPoE <== V:1			
	Vigor	[3G]Modem response: (			
pr 12 09:17:49		[3GIModem initialize A	T&FE0V1X1&D2&C1S0=0		
pr 12 09:17:49	Vigor				
	Vigor Vigor	WAN2 PPPoE => V:1			<u></u>
pr 12 09:17:49					2

## Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2860. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

# 5.6 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. Such function is available in **Admin Mode** only.



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

## Software Reset

You can reset the router to factory default via Web page. Such function is available in Admin Mode only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

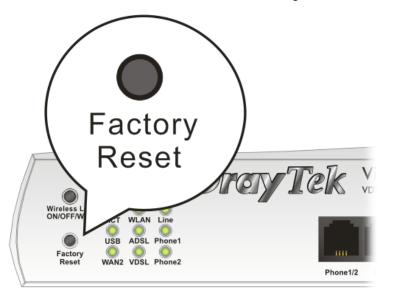


System Maintenance >> Reboot System

Reboot System	
	Do you want to reboot your router ?
	<ul> <li>Using current configuration</li> </ul>
	O Using factory default configuration
	Reboot Now
Auto Reboot Time Sched	ule
Index(1	-15) in <u>Schedule</u> Setup:,,,,
Note: A	ction and Idle Timeout settings will be ignored.
	OK Cancel

## **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.

## **5.7 Contacting Your Dealer**

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

