

# DrayTek

## Vigor2925 Series

Dual-WAN Security Router



Your reliable networking solutions partner

## User's Guide

V1.3



# **Vigor2925 Series Dual-WAN Security Router User's Guide**

**Version: 1.3**

**Firmware Version: V3.7.3**

**(For future update, please visit DrayTek web site)**

**Date: 29/10/2013**

## Copyright Information

### Copyright Declarations

Copyright 2013 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

### Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

## Safety Instructions and Approval

### Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

### Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore 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.dayTek.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 303  
Product: Vigor2925 Series Router

DrayTek Corp. declares that Vigor2925 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 2.4GHz WLAN network throughout the EC region.



# Table of Contents

## 1

<b>Introduction.....</b>	<b>1</b>
1.1 Web Configuration Buttons Explanation .....	2
1.2 LED Indicators and Connectors .....	3
1.2.1 For Vigor2925 .....	3
1.2.2 For Vigor2925n .....	5
1.3 Hardware Installation .....	7
1.4 Printer Installation .....	8

## 2

<b>Basic Settings.....</b>	<b>13</b>
2.1 Accessing Web Page .....	13
2.2 Changing Password .....	15
2.3 Quick Start Wizard .....	16
2.3.1 For WAN1/WAN2 (Ethernet) .....	17
2.3.2 For WAN3 (USB) .....	25
2.4 Service Activation Wizard.....	27
2.5 Wireless Wizard .....	31
2.6 Introducing Dashboard.....	34
2.6.1 Virtual Panel .....	35
2.6.2 Name with a Link .....	35
2.6.3 Quick Access for Common Used Menu.....	36
2.6.4 GUI Map .....	37
2.6.5 Web Console .....	38
2.6.6 Config Backup .....	39
2.7 Online Status.....	40
2.7.1 Physical Connection .....	40
2.7.2 Virtual WAN .....	42
2.8 Saving Configuration.....	42
2.9 Registering Vigor Router.....	43

## 3

<b>Tutorials and Applications.....</b>	<b>47</b>
3.1 How to configure settings for IPv6 Service in Vigor2925.....	47
3.2 How to establish OpenVPN - host to LAN tunnels(authenticated without CA) via SmartVPN Client? .....	57
3.3 How can I get the files from USB storage device connecting to Vigor router? .....	61
3.4 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPSec Tunnel (Main Mode) .....	64

3.5 How to Optimize the Bandwidth through QoS Technology .....	68
3.6 QoS Setting Example.....	72
3.7 How to use Landing Page Feature .....	76
3.8 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection.....	80
3.9 How to Create an Account for MyVigor.....	84
3.9.1 Create an Account via Vigor Router .....	84
3.9.2 Create an Account via MyVigor Web Site .....	88
3.10 How to Configure Certain Computers Accessing to Internet .....	92
3.11 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter.....	96
3.12 How to Setup Address Mapping.....	102
3.13 How to Setup Load Balance for Packets? .....	106
3.14 How to Authenticate Clients via User Management.....	108
3.15 How to use DNS Filter.....	118
3.16 How to use AP Management function (in Vigor2925) to check AP status and deploy WLAN profile.....	121

# 4

## **Advanced Configuration..... 125**

4.1 WAN .....	125
4.1.1 Basics of Internet Protocol (IP) Network.....	125
4.1.2 General Setup.....	127
4.1.3 Internet Access .....	131
4.1.4 Multi-VLAN.....	150
4.1.5 WAN Budget .....	154
4.2 LAN .....	155
4.2.1 Basics of LAN .....	155
4.2.2 General Setup.....	157
4.2.3 Static Route .....	167
4.2.4 VLAN.....	172
4.2.5 Bind IP to MAC .....	176
4.2.6 LAN Port Mirror.....	178
4.2.7 Web Portal Setup.....	179
4.3 Load-Balance /Route Policy.....	180
4.4 NAT .....	183
4.4.1 Port Redirection .....	184
4.4.2 DMZ Host.....	187
4.4.3 Open Ports.....	191
4.4.4 Port Triggering .....	193
4.5 Hardware Acceleration .....	196
4.5.1 Setup.....	196
4.6 Firewall.....	198
4.6.1 Basics for Firewall.....	198
4.6.2 General Setup.....	200
4.6.3 Filter Setup .....	205



4.6.4 DoS Defense .....	213
4.7 User Management.....	217
4.7.1 General Setup.....	218
4.7.2 User Profile .....	219
4.7.3 User Group .....	223
4.7.4 User Online Status.....	224
4.8 Objects Settings .....	225
4.8.1 IP Object .....	225
4.8.2 IP Group .....	228
4.8.3 IPv6 Object .....	229
4.8.4 IPv6 Group.....	231
4.8.5 Service Type Object .....	232
4.8.6 Service Type Group.....	234
4.8.7 Keyword Object .....	235
4.8.8 Keyword Group.....	237
4.8.9 File Extension Object.....	238
4.8.10 SMS/Mail Service Object.....	240
4.8.11 Notification Object.....	245
4.9 CSM Profile .....	247
4.9.1 APP Enforcement Profile .....	248
4.9.2 URL Content Filter Profile.....	252
4.9.3 Web Content Filter Profile.....	256
4.9.4 DNS Filter .....	260
4.9.5 APPE Support List.....	261
4.10 Bandwidth Management .....	262
4.10.1 Sessions Limit.....	262
4.10.2 Bandwidth Limit .....	264
4.10.3 Quality of Service.....	265
4.11 Applications .....	274
4.11.1 Dynamic DNS .....	274
4.11.2 LAN DNS .....	277
4.11.3 Schedule.....	279
4.11.4 RADIUS .....	282
4.11.5 Active Directory/ LDAP .....	282
4.11.6 UPnP.....	285
4.11.7 IGMP.....	287
4.11.8 Wake on LAN.....	288
4.11.9 SMS / Mail Alert Service.....	289
4.11.10 Bonjour .....	291
4.12 VPN and Remote Access.....	294
4.12.1 VPN Client Wizard .....	294
4.12.2 VPN Server Wizard.....	301
4.12.3 Remote Access Control.....	306
4.12.4 PPP General Setup .....	306
4.12.5 IPSec General Setup.....	308
4.12.6 IPSec Peer Identity .....	310
4.12.7 OpenVPN General Setup .....	312
4.12.8 Remote Dial-in User .....	313
4.12.9 LAN to LAN.....	316
4.12.10 VPN TRUNK Management.....	327
4.12.11 Connection Management .....	336
4.13 Certificate Management.....	337
4.13.1 Local Certificate.....	337

4.13.2 Trusted CA Certificate .....	341
4.13.3 Certificate Backup.....	342
4.14 Wireless LAN .....	342
4.14.1 Basic Concepts.....	342
4.13.2 General Setup.....	345
4.14.3 Security .....	347
4.14.4 Access Control.....	349
4.14.5 WPS.....	351
4.14.6 WDS.....	354
4.14.7 Advanced Setting.....	357
4.14.8 WMM Configuration.....	359
4.14.9 AP Discovery .....	361
4.14.10 Station List.....	362
4.15 SSL VPN .....	363
4.15.1 General Setup.....	363
4.15.2 SSL Web Proxy .....	364
4.15.3 SSL Application .....	365
4.15.4 User Account .....	368
4.15.5 User Group .....	372
4.15.6 Online User Status.....	374
4.16 USB Application .....	375
4.16.1 USB General Settings.....	375
4.16.2 USB User Management.....	376
4.16.3 File Explorer.....	379
4.16.4 USB Disk Status .....	379
4.16.5 Temperature Sensor.....	381
4.16.6 Modem Support List.....	382
4.17 System Maintenance.....	383
4.17.1 System Status.....	383
4.17.2 TR-069.....	385
4.17.3 Administrator Password.....	386
4.17.4 User Password .....	387
4.17.5 Login Page Greeting.....	390
4.17.6 Configuration Backup .....	392
4.17.7 Syslog/Mail Alert.....	394
4.17.8 Time and Date .....	397
4.17.9 SNMP.....	398
4.17.10 Management.....	400
4.17.11 Reboot System .....	402
4.17.12 Firmware Upgrade .....	403
4.17.13 Activation .....	404
4.18 Diagnostics.....	405
4.18.1 Dial-out Triggering .....	406
4.18.2 Routing Table .....	407
4.18.3 ARP Cache Table.....	408
4.18.4 IPv6 Neighbour Table.....	408
4.18.5 DHCP Table.....	409
4.18.6 NAT Sessions Table.....	410
4.18.7 Ping Diagnosis.....	411
4.18.8 Data Flow Monitor.....	412
4.18.9 Traffic Graph.....	414
4.18.10 Trace Route .....	415
4.18.11 Syslog Explorer.....	416
4.18.12 IPv6 TSPC Status.....	417

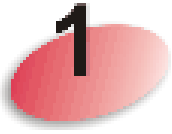
4.19 External Devices .....	418
4.19.1 All Devices .....	418
4.19.2 Access Point Devices .....	419

# 5

## **Trouble Shooting.....426**

5.1 Checking If the Hardware Status Is OK or Not.....	426
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not .....	427
5.3 Pinging the Router from Your Computer .....	429
5.4 Checking If the ISP Settings are OK or Not.....	430
5.5 Problems for 3G Network Connection .....	430
5.6 Backing to Factory Default Setting If Necessary .....	431
5.7 Contacting Your Dealer .....	432





# Introduction

Vigor2925 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.

User Management implemented on your router firmware can allow you to prevent any computer from accessing your Internet connection without a username or password. You can also allocate time budgets to your employees within office network.

With the 6-port Gigabit switch on the LAN side provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. The tagged VLANs (IEEE802.1Q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation. The said functionality is tag-based Multi-subnet (Multiple-Private LAN Subnets).


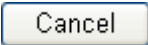
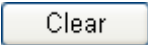
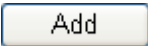

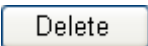
On the Wireless-equipped models each of the wireless SSIDs can also be grouped within one of the VLANs.

In addition, Vigor2925 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2925 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:

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

**Note:** For the other buttons shown on the web pages, please refer to Chapter 3, 4 for detailed explanation.

## 1.2 LED Indicators and Connectors

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

### 1.2.1 For Vigor2925



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
USB1~USB2	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
WAN1~WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
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> ).
DMZ	On	The DMZ function is enabled.
	Off	The DMZ function is disabled.
	Blinking	The data is transmitting.

#### LED on Connector

WAN1~ WAN2	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
		Blinking	The data is transmitting.
LAN1~ LAN5	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		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.
USB1~USB2	Connector for a USB device (for 3G USB Modem or printer).
WAN1~WAN2	Connector for local network devices or modem for accessing Internet.
LAN1~LAN5	Connectors for local network devices.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.



## 1.2.2 For Vigor2925n



LED	Status	Explanation
ACT (Activity)	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.)
WAN1~WAN2	On	Internet connection is ready.
	Off	Internet connection is not ready.
	Blinking	The data is transmitting.
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> ).
DMZ	On	The DMZ function is enabled.
	Off	The DMZ function is disabled.
	Blinking	The data is transmitting.

### LED on Connector

WAN1~ WAN2	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps
		Blinking	The data is transmitting.
LAN1~ LAN5	Left LED	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps



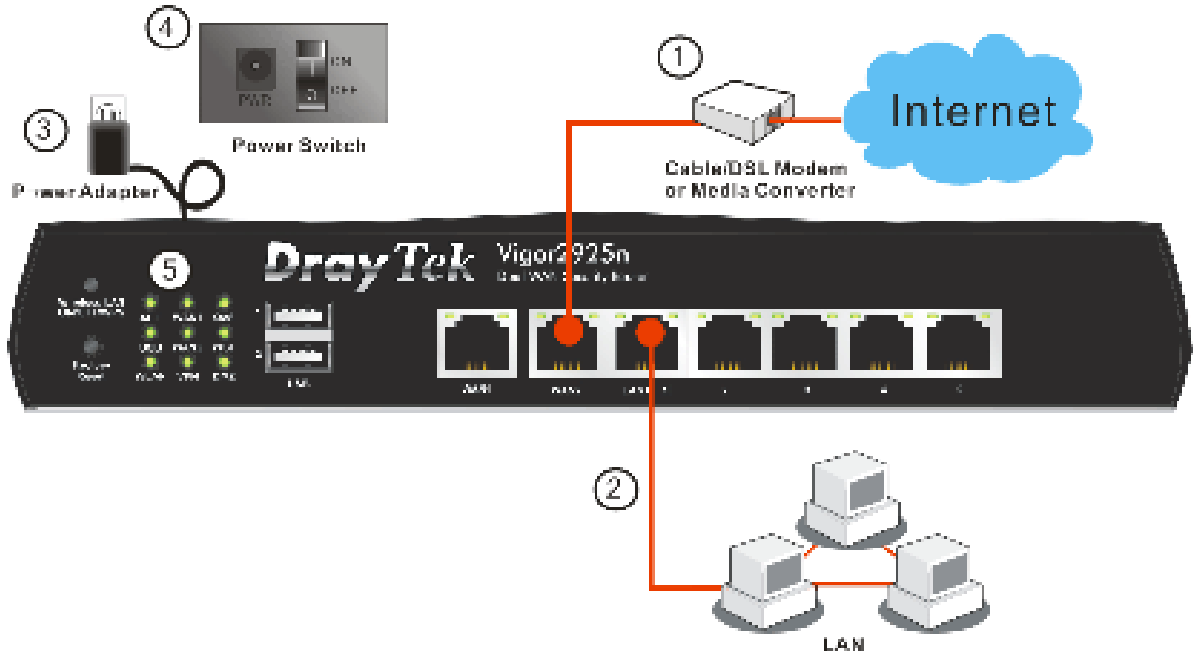
Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default 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.
USB1~USB2	Connector for a USB device (for 3G USB Modem or printer).
WAN1~WAN2	Connector for local network devices or modem for accessing Internet.
LAN1~LAN5	Connectors for local network devices.
PWR	Connector 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.

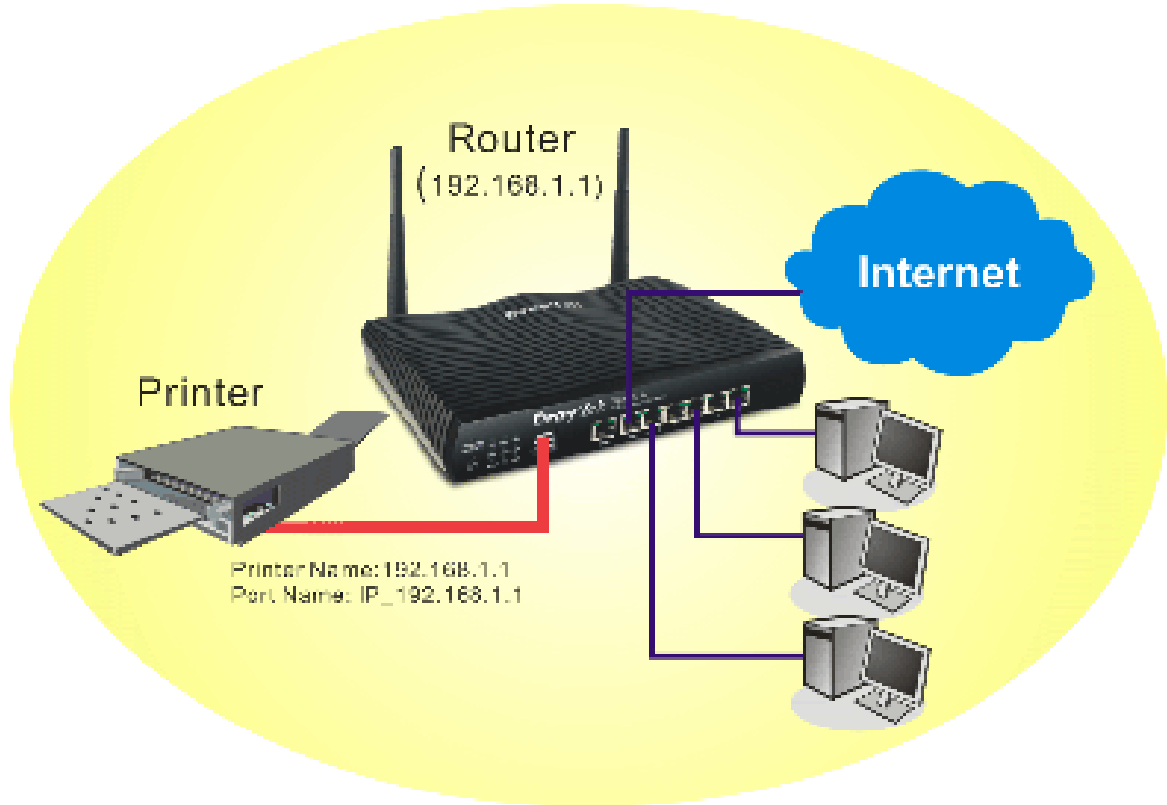
1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
4. Power on the device by pressing down the power switch on the rear panel.
5. 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.)



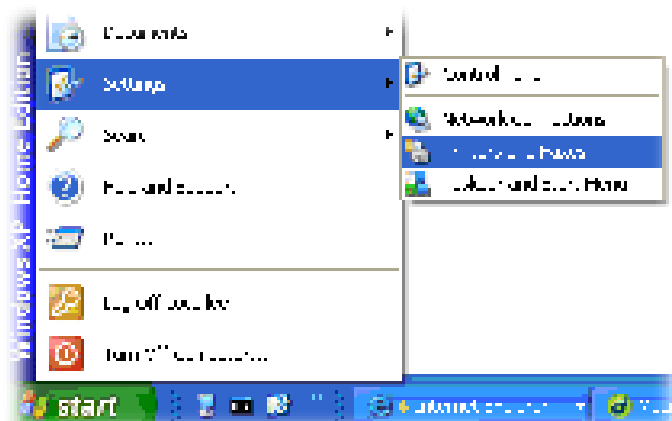
## 1.4 Printer Installation

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](http://www.DrayTek.com).

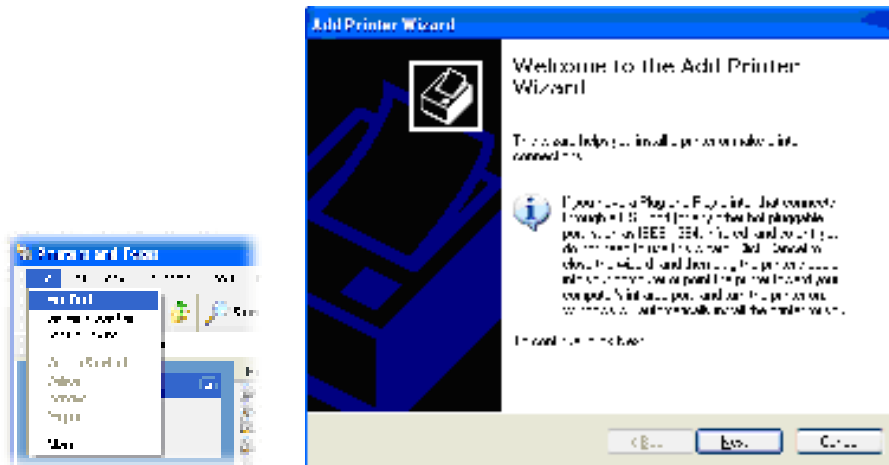


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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



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



- Click **Local printer attached to this computer** and click **Next**.



- 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**.



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**.



7. Click **Standard** and choose **Generic Network Card**.



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



- 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**.



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

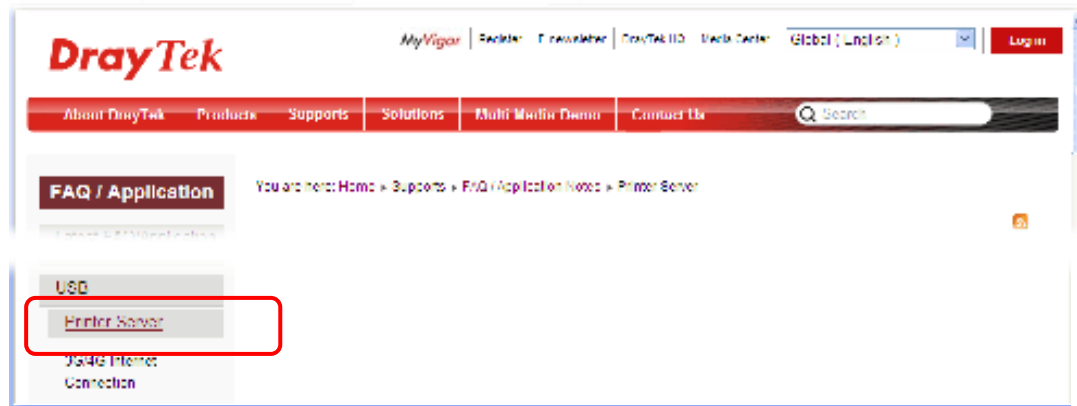


- Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.

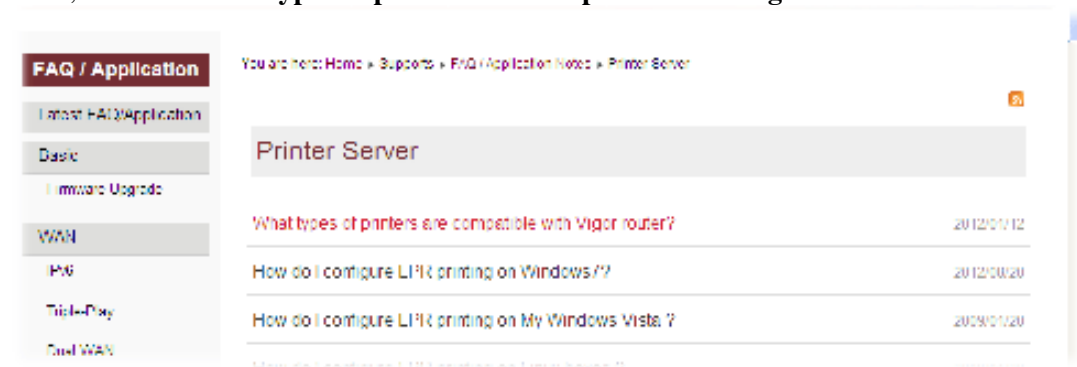


The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

**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](http://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.



Then, click the **What types of printers are compatible with Vigor router?** link.



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



# 2

## Basic Settings

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.

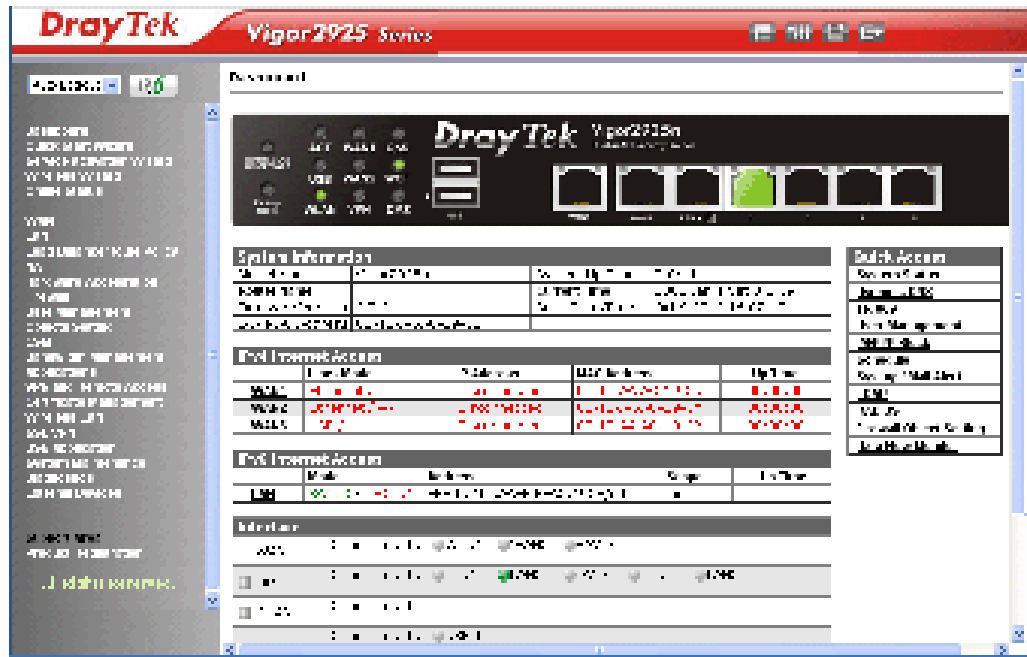
2. Open a web browser on your PC and type **http://192.168.1.1**. The following window will be open to ask for username and password.



3. Please type “admin/admin” as the Username/Password and click **Login**.

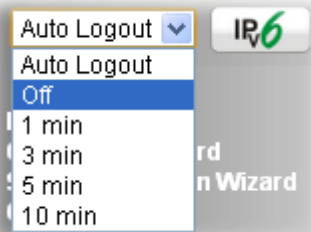
**Notice:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

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



**Note:** The home page will be different slightly in accordance with the type of the router you have.

- 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.



## 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**.

System Maintenance => Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Note: Password can contain only a-z A-Z 0-9 , . : \* ' " = - \ | ? @ # ^ & ! ( )

OK

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.



**Note:** Even the password has been 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-numeric string as your Password (Max 20 characters).

Old Password	*****
New Password	*****
Confirm Password	*****

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

### Quick Start Wizard

#### WAN Interface

WAN Interface	WAN-1
Display Name	
Physical Mode	Ethernet
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/WAN2 (Ethernet)

WAN1/WAN2 is dedicated to physical mode in Ethernet. If you choose WAN1/WAN2, please specify physical type. Then, click **Next**.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN2
Interface Name:	
Physical Mode:	Ethernet
Physical Type:	10/100/1000

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

Connect to Internet

WAN 2

Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPP
- L2TP
- Static IP
- DHCP

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

**Quick Start Wizard**

**PPPoE Client Mode**

**WAN 2**  
Enter the user name and password provided by your ISP.

User Name

Password

Confirm Password

Available settings are explained as follows:

Item	Description
<b>User Name</b>	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.
<b>Password</b>	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.
<b>Back</b>	Click it to return to previous setting page.
<b>Next</b>	Click it to get into the next setting page.
<b>Cancel</b>	Click it to give up the quick start wizard.

- Please manually enter the Username/Password provided by your ISP. 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:	PPPoE

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

### 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

Connect to Internet

WAN 2  
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

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

**Quick Start Wizard**

**PPTP Client Mode**

**WAN 2**  
Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.

User Name:

Password:

Confirm Password:

**WAN IP Configuration**

Obtain an IP address automatically

Specify an IP address

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

Second DNS:

PPTP Server:

Available settings are explained as follows:

Item	Description
<b>User Name</b>	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.
<b>Password</b>	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.
<b>WAN IP Configuration</b>	<b>Obtain an IP address automatically</b> – the router will get an IP address automatically from DHCP server. <b>Specify an IP address</b> – you have to type relational settings manually. <b>IP Address</b> - Type the IP address. <b>Subnet Mask</b> –Type the subnet mask. <b>Gateway</b> – Type the IP address of the gateway. <b>Primary DNS</b> –Type in the primary IP address for the router. <b>Second DNS</b> –Type in secondary IP address for necessity in the future.
<b>PPTP Server / L2TP Server</b>	Type the IP address of the server.
<b>Back</b>	Click it to return to previous setting page.
<b>Next</b>	Click it to get into the next setting page.
<b>Cancel</b>	Click it to give up the quick start wizard.



3. 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:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE

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

### Static IP

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

##### Connect to Internet

WAN 2  
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPPoE
- L2TP
- Static IP
- DHCP

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

**Quick Start Wizard**

**Static IP Client Mode**

WAN 2  
Enter the Static IP configuration provided by your ISP.

WAN IP	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
Primary DNS	
Secondary DNS	(optional)

Available settings are explained as follows:

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

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

**Quick Start Wizard**

**Please confirm your settings:**

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP

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

- 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!

- Now, you can enjoy surfing on the Internet.

## DHCP

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

Quick Start Wizard

Connect to Internet

WAN 2

Select one of the following Internet Access types provided by your ISP.

PPPoE  
 PPP  
 L2TP  
 Static IP  
 DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 2

If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name \_\_\_\_\_ (optional)

MAC  -  -  -  -  -  (optional)

Available settings are explained as follows:

Item	Description
Host Name	Type the name of the host. <b>Note:</b> The maximum length of the host name you can set is

	39 characters.
<b>MAC</b>	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
<b>Back</b>	Click it to return to previous setting page.
<b>Next</b>	Click it to get into the next setting page.
<b>Cancel</b>	Click it to give up the quick start wizard.

- 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 Address:	192.168.1.1

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

- 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!

- Now, you can enjoy surfing on the Internet.

### 2.3.2 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

WAN Interface: WAN3

Display Name:

Physical Mode: USB

< Back Next Finish Cancel

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

Quick Start Wizard

#### Connect to Internet

Connect to Internet

WAN 3

Internet Access : 3G/4G USB Modem(PPP mode)

3G/4G USB Modem(PPP mode)

SIM Pin code

Modem Initial String

APN Name

Apply

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
<b>Internet Access</b>	Choose a protocol for accessing the Internet.
<b>3G/4G USB Modem (PPP mode)</b>	<p><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.</p> <p><b>Modem Initial String</b> – 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.</p>

---

	<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> .
--	---

---

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

**Quick Start Wizard**

Please confirm your settings:

WAN Interface:	WAN3
Physical Mode:	USB
Internet Access:	PPPoE

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

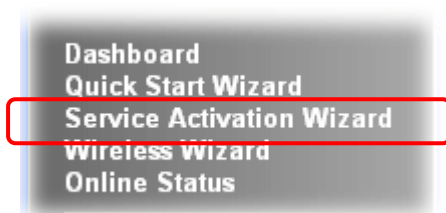
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type “admin/admin” on Username/Password while Logging into the web user interface.**

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 <http://myvigor.draytek.com>. 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.

**Note:** Such function is available only for **Admin Mode**.

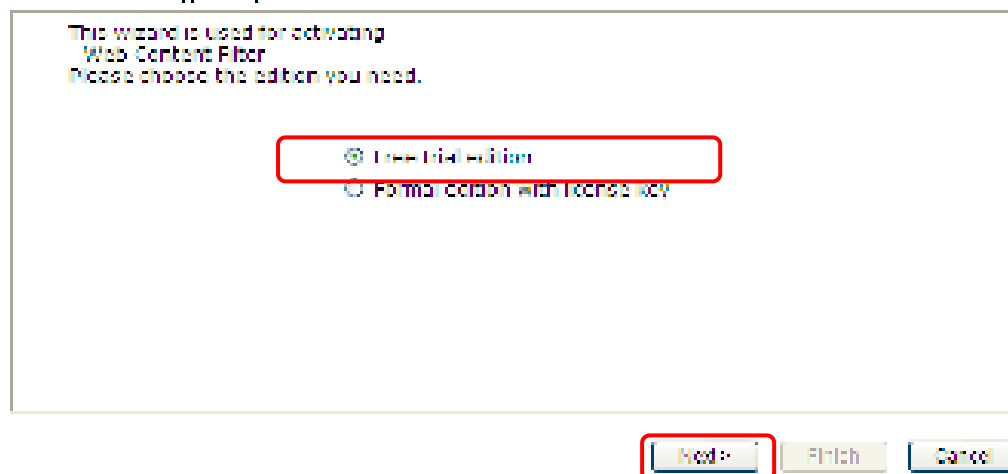
1. Open **Service Activation Wizard**.



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 trial edition.

Service Activation Wizard

Select the service type that you want to activate

A screenshot of the Service Activation Wizard selection screen. The text reads: "This wizard is used for activating Web Content Filter. Please choose the edition you need." Below this text are two radio button options: "Free trial edition" (selected and highlighted with a red rectangle) and "Formal edition with license key". At the bottom right, there are three buttons: "Next" (highlighted with a red rectangle), "Finish", and "Cancel".

**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.

- 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**.

Service Activation Wizard

---

Select the service type that you want to activate

This product provides 30 days of free trial, please choose the license you want to use.

WCF service:

Web Content Filter (BPjM) **License Agreement**  
 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.  
 Activation Date: 2013-02-18

---

Web Content Filter (fragFINN) **License Agreement** **Activation Date: 2013-02-18**

I have read and accept the above Agreement. (Please check this box).

Note: The activation date is brought out by the server automatically and cannot be changed.

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.

BPjM is WCF for German Speaking users. The fragFINN is whitelist for German Speaking users. The BPjM is ideal for your family to provide more Internet security for youngsters.

The fragFINN is designed for protecting kids from inadequate web sites. More info is available at <http://www.draytek.de/jugendschutz>.

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

Service Activation Wizard

---

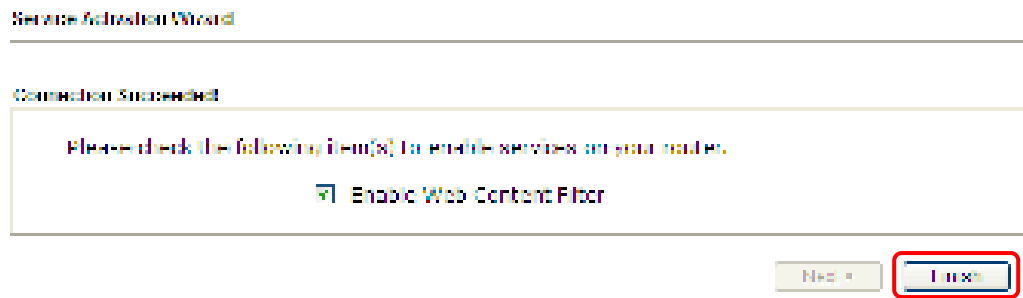
Please confirm your settings

Service Type : trial version  
 Service Activated : Web Content Filter (Commtouch)

Please click Back to re-select service type you to activate.



- Wait for a moment till the following page appears.



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**.

- 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.



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

Select the service type that you want to activate

This wizard is used for activating  
- Web Content Filter

Please choose the edition you need.

Free trial edition

Licensed edition with license key

### Service Activation Wizard

Select the service type that you want to activate

Please choose the item you want to use.

WCF service:

Web Content Filter (Commodity) License Agreement  
Commodity is the activation. This license is Domain independent on the available.  
Enter your license key:  Activation Date: 2013-03-22

Web Content Filter (TrapFDN) License Agreement  
Enter your license key:  Activation Date: 2013-03-22

I have read and accept the above agreement. (Please check this box).

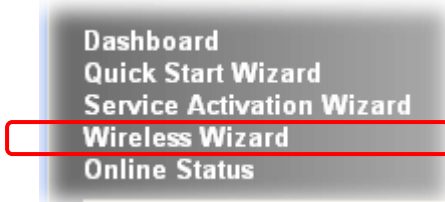
Note: The activation date is brought out by the server automatically and cannot be changed.

## 2.5 Wireless Wizard

The wireless wizard allows you to configure settings specified for a host AP (for home use or internal use for a company) and specified for a guest AP (for any wireless clients accessing into Internet).

Follow the steps listed below:

1. Open **Wireless Wizard**.



2. The screen of wireless wizard will be shown as follows. This page will be used for internal users in a company or your home.

### Wireless Wizard

#### Host AP Configuration

**Name:**

**Mode:**

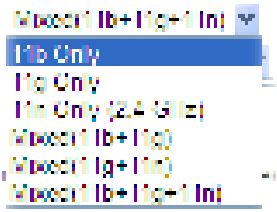
**Channel:**

**Pass-words:**

**Note:** The host AP configured here will be used for home or internal company use.

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type the SSID name of this router. (SSID1) The default name is defined with DratTek.
<b>Mode</b>	At present, the router can connect to 11n Only, 11g Only, Mixed (11b+11g), Mixed (11a+11n), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

	
<b>Channel</b>	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.
<b>Password</b>	The wireless mode offered by this wizard is WPA2/PSK. 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>Next</b>	Click it to get into the next setting page.
<b>Cancel</b>	Exit the wireless wizard without saving any changes.

- After typing the required information, click **Next**. The settings in the page limit the wireless station (guest) accessing into Internet but not being allowed to share the LAN network and VPN connection.

#### Wireless Wizard

#### Guest AP Configuration

Enable     Disable

Name:

Password:

Rate Control:  Enable    Upload  kbps    Download  kbps

Note: the configured guest AP will not be able to access the LAN network, VPN connections, or communicate with wireless devices connecting to the router's other APs. This AP interface should be used for Internet access only.

Available settings are explained as follows:

Item	Description
<b>Enable/Disable</b>	Click it to enable or disable settings in this page.
<b>Name</b>	Type the SSID name of this router. (SSID2)

<b>Password</b>	The wireless mode offered by this wizard is WPA2/PSK. 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>Rate Control</b>	It controls the data transmission rate through wireless connection. <b>Upload</b> – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. <b>Download</b> – Type the transmitting rate for data download. Default value is 30,000 kbps.
<b>Next</b>	Click it to get into the next setting page.
<b>Cancel</b>	Exit the wireless wizard without saving any changes.

- After typing the required information, click **Next**.
- The following page will display the configuration summary for wireless setting.

Wireless Wizard

Configuration Summary

**Basic Wireless Settings**

Mode: WPA2/PSK (TKIP+AES)  
Channel: Channel 6, 2437MHz

**Host AP Configurations**

Vendor: DrayTek  
Access: 1:111111111111

**Guest AP Configurations**

Mode: Disabled  
Vendor: DrayTek\_Guest  
Access: 1:111111111111  
Pass Control: Disabled

- Click **Finish** to complete the wireless settings configuration.

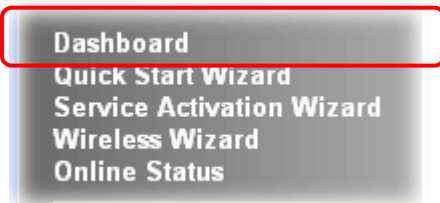
Wireless Wizard

Wireless Wizard Setup OK!

## 2.6 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:

The screenshot shows the DrayTek Vigor2925n Dashboard. At the top, there is a status bar with various indicators (Wireless LAN, ACT, WAN1, DoS, USB, WAN2, WCF, Factory Reset, WLAN, VPN, DNS) and a physical connection diagram. Below this are several data tables and a quick access menu.

**System Information**

Model Name	Vigor2925n	System Up Time	1: 18:1
Router Name		Current Time	2013-10-1 14:1:18:1
Firmware Version	E7.3	Boot Date/Time	Oct 3 2013 15:08:3
LAN MAC Address	00:1D:AA:8C:1D:08		

**IPv4 Internet Access**

WAN	Line Mode	IP Address	MAC Address	Up Time
WAN1	Dynamic	Disconnected	11-11-2000-11-11	11:11:11
WAN2	Ethernet	Disconnected	00-1D-AA-8C-1D-0A	00:00:00
WAN3	Static	Disconnected	11-11-2000-11-11	11:11:11

**IPv6 Internet Access**

LAN	Mode	Address	Scope	Up Time
LAN	Static	111-11-11-11	Link-Local	1:1

**Interface**

Interface	Status	Connections
WAN1	Connected	WAN1, WAN2, WAN3
LAN	Connected	LAN1, LAN2, LAN3, LAN4, LAN5
WLAN	Connected	
USB1	Connected	USB1

**Quick Access**

- System Status
- Dynamic DNS
- VPN
- User Management
- DMZ/PIBock
- Schedule
- System Mail Alert
- LOG
- LOGOUT
- Firewall Object Setting
- Data Flow Monitor

## 2.6.1 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



Port	Color Displayed	Explanation
Ethernet Port (WAN/LAN)	Black	It means such port is disconnected.
	Green	It means such port is connected (with Giga transmission rate) physically.
	Orange	It means such port is connected physically.
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**.

## 2.6.2 Name with a Link

A name with a link (e.g., [Router Name](#), [Current Time](#), [WAN1/2/3](#) and etc.) below means you can click it to open the configuration page for modification.

System Information				
Model Name	Vigor2925n	System Time	11:11	
Router Name		Current Time	2011-10-11 14:11:11	
Firmware Version	V.7.2	Boot Date/Time	2011-09-13 10:08:13	
LAN MAC Address	00:10:5A:AC:10:0A			

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
<a href="#">WAN1</a>	Line 1 / --	Disconnected	11-10-2011-14:11:11	11:11:11
<a href="#">WAN2</a>	Ethernet /	Disconnected	00:10:5A:AC:10:0A	00:00:00
<a href="#">WAN3</a>	ADSL / --	Disconnected	11-10-2011-14:11:11	11:11:11

IPv6 Internet Access				
----------------------	--	--	--	--

## 2.6.3 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
<a href="#">System Status</a>
<a href="#">Dynamic DNS</a>
<a href="#">TR-069</a>
<a href="#">User Management</a>
<a href="#">IM/P2P Block</a>
<a href="#">Schedule</a>
<a href="#">SysLog / Mail Alert</a>
<a href="#">LDAP</a>
<a href="#">RADIUS</a>
<a href="#">Firewall Object Setting</a>
<a href="#">Data Flow Monitor</a>

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	
WAN	WAN-eth 1, WAN-eth 2, WAN-eth 3
LAN	Connected 0, LAN-eth 1, LAN-eth 2, LAN-eth 3, LAN-eth 4, LAN-eth 5
USB	USB-eth 1, USB-eth 2

Security	
VPN	Connected : 1 Remote Dial-In User / LAN to LAN

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 Remote Dial-In User / LAN to LAN		
Current Page: 1 Page No: 1 Go			
Name / User	Type / Security	Host IP	Up Time
V2020	IPsec/3DES	172.16.2.145	0:0:20

How Many: 0 / 1 rows.



WAN	Connected : 1, <input type="radio"/> WAN1 <input checked="" type="radio"/> WAN2 <input type="radio"/> WAN3						
LAN	Connected : 1, <input type="radio"/> LAN1 <input checked="" type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4 <input type="radio"/> LAN5						
	<table border="1"> <thead> <tr> <th>Host ID</th> <th>IP Address</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>CARRIE-0C7CB251</td> <td>192.168.1.10</td> <td>E0-CB-4E-DA-48-79</td> </tr> </tbody> </table>	Host ID	IP Address	MAC	CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79
Host ID	IP Address	MAC					
CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79					
USB	Connected : 0, <input type="radio"/> USB 1						

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).

## 2.6.4 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

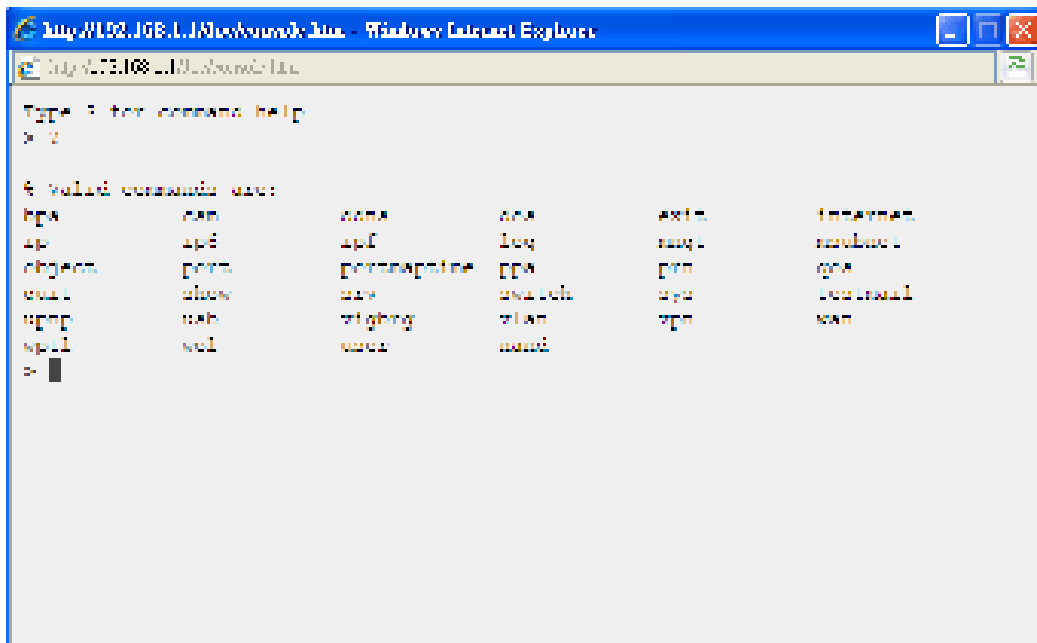
<b>Dashboard</b> <b>Wizard</b>	<b>Quick Start Wizard</b> General Configuration <b>Initial</b> Wireless-Management <b>SSH</b> Wireless-Management <b>SSH</b>	<b>VPN and Remote Access</b>	<b>VPN Configuration</b> VPN Management <b>Remote Access Control</b> VPN General Setup <b>Export General Setup</b> Export General Setup <b>Local-VPN General Setup</b> General Setup Local-VPN <b>Local-VPN</b> VPN General Management
<b>Online Status</b>	<b>Connected Connection</b> General-WAN	<b>Certificate Management</b>	<b>Local Certificate</b> Initial & General <b>Local Certificate Backup</b>
<b>WAN</b>	General Setup <b>WAN Management</b> WAN Setup <b>WAN Budget</b>	<b>Wireless LAN (WLAN)</b>	<b>General Setup</b> General <b>Access Control</b> WLAN <b>SSID</b>
<b>LAN</b>	<b>General Setup</b> General LAN <b>SSH</b> LAN General <b>LAN Port Mode</b> LAN General Setup		
<b>Load-Balance/Route</b>			

## 2.6.5 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.



## 2.6.6 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.



Click **Save** to store the setting.

## 2.6.7 Logout



Click the **Logout** icon to exit the web user interface.

## 2.7 Online Status

Online Status  
Physical Connection  
Virtual WAN

### 2.7.1 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 Connection		System Uptime: 0day 0:29:52			
IPv4		IPv6			
<b>LAN Status</b>		Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets			
192.168.1.1	108816	2022			
<b>WAN 1 Status</b>					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet			00:00:00	
IP	GW IP	TX Bytes	TX Rate(Bps)	RX Bytes	RX Rate(Bps)
		0 (0)	0	0 (0)	0
<b>WAN 2 Status</b>					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet			00:00:00	
IP	GW IP	TX Bytes	TX Rate(Bps)	RX Bytes	RX Rate(Bps)
		0 (0)	0	0 (0)	0
<b>WAN 3 Status</b>					
Enable	Line	Name	Mode	Up Time	Signal
Yes	PPPOE			00:00:00	
IP	GW IP	TX Bytes	TX Rate(Bps)	RX Bytes	RX Rate(Bps)
		0 (0)	0	0 (0)	0

#### Physical Connection for IPv6 Protocol

Online Status

Physical Connection		System Uptime: 0t:18	
IPv4		IPv6	
<b>LAN Status</b>			
IP Address			
2001:4D00:FF00:83E4:21D:A AFF:FEA6:2568/64 (Global)			
FE80::21D:A AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
147	187	34205	19176
<b>WAN2 IPv6 Status</b>			
Enable	Mode	Up Time	
Yes	AICCU	0:00:48	
IP	Gateway IP		
2001:4D00:FF00:3E4::2/64 (Global)			
FE80::4CD0:FF00:3E4::2/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
185	137	16438	33093

Detailed explanation (for IPv4) is shown below:

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

Detailed explanation (for IPv6) is shown below:

Item	Description
<b>LAN Status</b>	<p><b>IP Address</b>- Displays the IPv6 address of the LAN interface..</p> <p><b>TX Packets</b>-Displays the total transmitted packets at the LAN interface.</p> <p><b>RX Packets</b>-Displays the total received packets at the LAN interface.</p> <p><b>TX Bytes</b> - Displays the speed of transmitted octets at the LAN interface.</p> <p><b>RX Bytes</b> - Displays the speed of received octets at the LAN interface.</p>
<b>WAN IPv6 Status</b>	<p><b>Enable – No</b> in red means such interface is available but not enabled. <b>Yes</b> in green means such interface is enabled. <b>No</b> in red means such interface is not available.</p>

Item	Description
	<p><b>Mode</b> - Displays the type of WAN connection (e.g., TSPC).</p> <p><b>Up Time</b> - Displays the total uptime of the interface.</p> <p><b>IP</b> - Displays the IP address of the WAN interface.</p> <p><b>Gateway IP</b> - Displays the IP address of the default gateway.</p>

**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.

## 2.7.2 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						System Uptime: 3:15:25
<b>WAN 5 Status</b>						
Enable	Line	Name	Mode	Up Time	Application	
Yes	Ethernet			00:00:00	Management	
IP	GW IP	Tx Packets	Tx Rate(Rps)	Rx Packets	Rx Rate(Rps)	
		0	0	0	0	
<b>WAN 6 Status</b>						
Enable	Line	Name	Mode	Up Time	Application	
Yes	Ethernet			00:00:00	Management	
IP	GW IP	Tx Packets	Tx Rate(Rps)	Rx Packets	Rx Rate(Rps)	
		0	0	0	0	
<b>WAN 7 Status</b>						
Enable	Line	Name	Mode	Up Time	Application	
Yes	Ethernet			00:00:00	Management	
IP	GW IP	Tx Packets	Tx Rate(Rps)	Rx Packets	Rx Rate(Rps)	
		0	0	0	0	

## 2.8 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.

## 2.9 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.



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



Support Area  
Product Registration

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

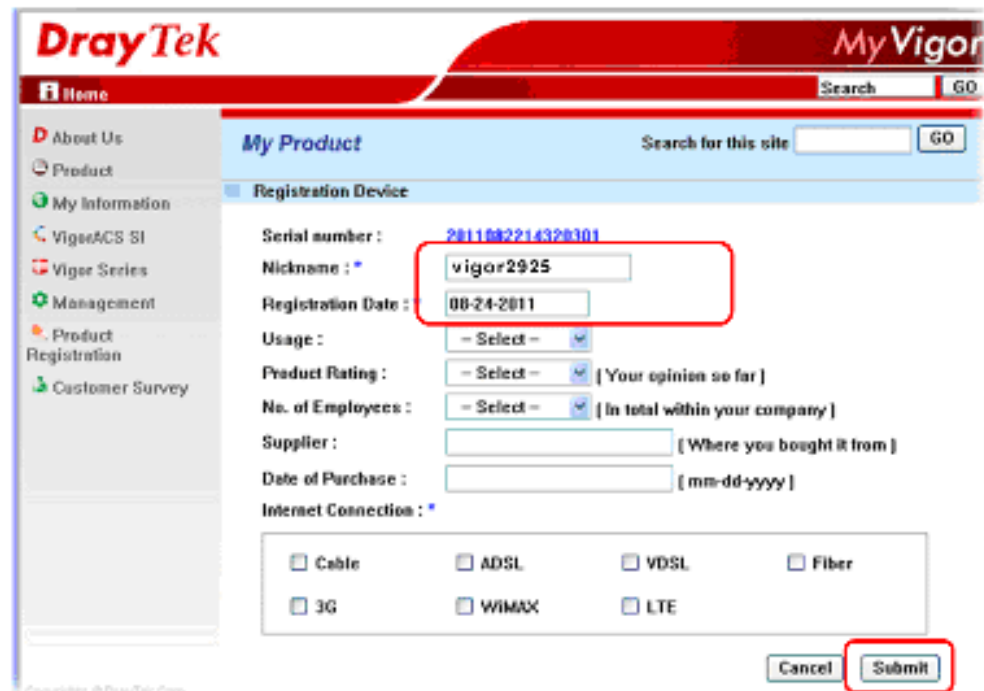
Create an account now'." data-bbox="242 619 870 865"/>

Please send any comments or suggestions to our customer service team.  
© 2012 DrayTek Corp. All Rights Reserved.

- 4 The following page will be displayed after you logging in MyVigor. From this page, please click **Add** or **Product Registration**.



- 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**.





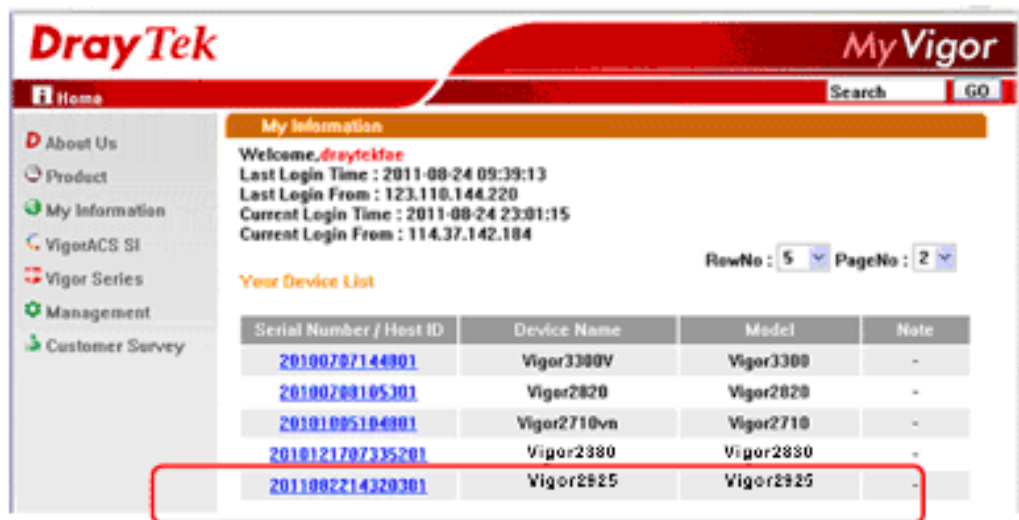
- When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.

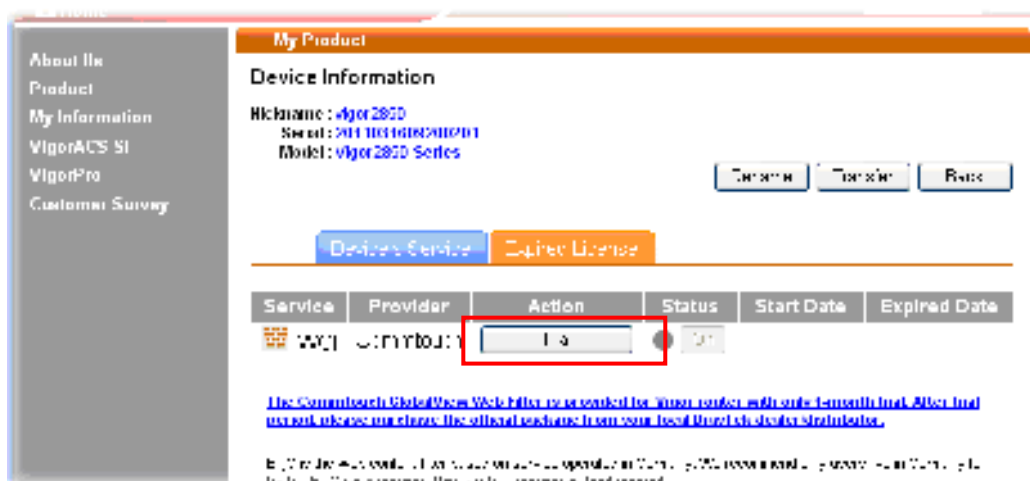


- Now, you have finished the product registration.
- After clicking **OK**, you will see the following page. Your router has been registered to *myvigor* website successfully.

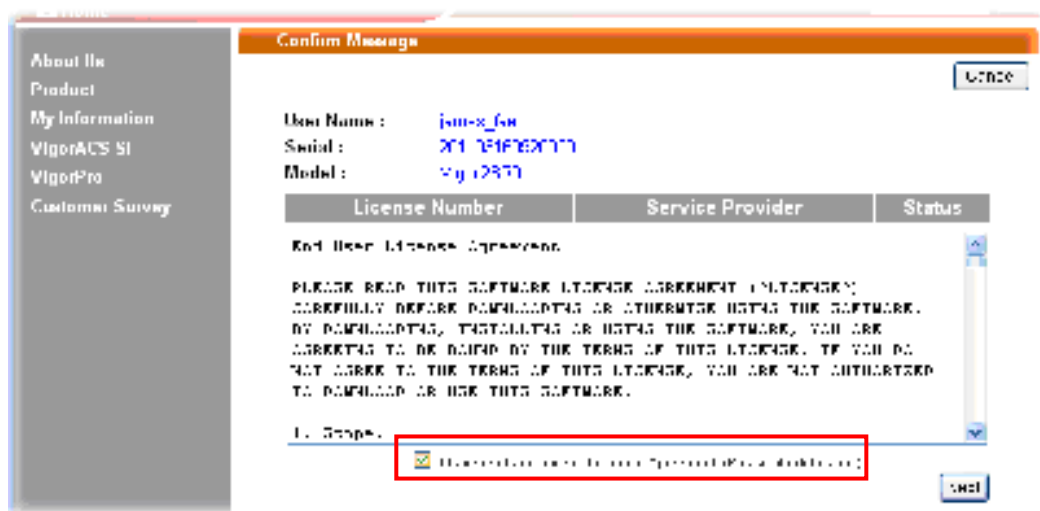
If you have not activated web content filter service by using **Service Activation Wizard**, you can activate the service from this step. Please click the serial number link.



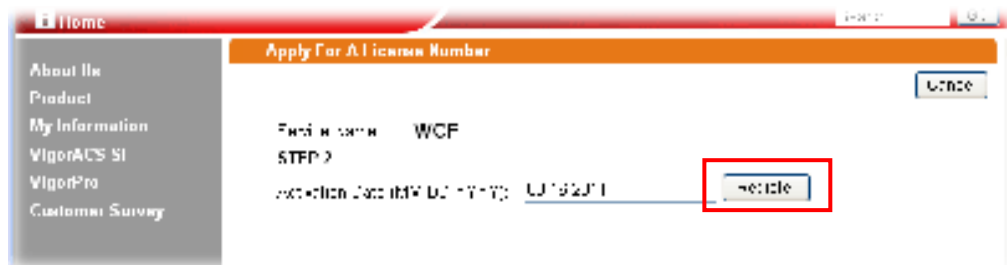
- From the **Device's Service** section, click the **Trial**.



- 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**.



12 Wait for a moment until the following page appears.

**DrayTek Service Activation**

Service Name	Start Date	Extra Date	Level
Warranted Time	2011-10-21	2011-10-22	Commercial

Please check if the license ID is the service provider of your Vigor user. To ensure normal use for Vigor user, update your Vigor user login information.

Copyright © DrayTek Corp. All Rights Reserved.

[Close]

13 Click **Close**.

# 3

## Tutorials and Applications

### 3.1 How to configure settings for IPv6 Service in Vigor2925

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 Vigor2925, 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 Vigor2925, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

1. Access into the web user interface of Vigor2925. 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

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	None	<a href="#">Details Page</a> <a href="#">IPv6</a>
WAN2		Ethernet	PPPoE	<a href="#">Details Page</a> <a href="#">IPv6</a>
WAN3		USB	None	<a href="#">Details Page</a> <a href="#">IPv6</a>

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.

- 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	PPTPL2TP	IPv6
Internet Access Mode			
Connection Type		<input type="radio"/> Online <input type="radio"/> Online <input checked="" type="radio"/> PPP <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> PPTPL2TP <input type="radio"/> Static IPv6	

OK

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	PPTPL2TP	IPv6
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<b>ISP Access Setup</b> Username: <input type="text" value="admin@home.net"/> Password: <input type="password" value="*****"/> Endless (S) in Schedule Setup: <input type="checkbox"/>		<b>PPPoE Setup</b> PPP Authentication: <input type="text" value="PAP or CHAP v2"/> Idle Timeout: <input type="text" value="1"/> second(s) IP Address Assignment Method (PCP): <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address: <input type="text"/>	
<b>WAN Connection Selection</b> Mode: <input type="text" value="All Default"/> Ping IP: <input type="text"/> TTL: <input type="text"/>		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00   10   5A   58   87   0A"/>	
MTU	1442	(Max: 1490)	

OK Cancel

Access into the setting page for IPv6 service, it is not necessary for you to configure anything.

WAN => Internet Access

WAN 2

PPPoE	Static or Dynamic IP	PPTPL2TP	IPv6
Internet Access Mode			
Connection Type		<input type="radio"/> Online <input type="radio"/> Online <input checked="" type="radio"/> PPP <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> PPTPL2TP <input type="radio"/> Static IPv6	
Note: IPv4 WAN setting should be PPPoE client.			

OK Cancel

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

---

Physical Connection System Uptime: 0:1:17

IPv4		IPv6			
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1	
IP Address		TX Packets	RX Packets		
192.168.1.1		0	3085		
WAN 1 Status <span style="float: right;">&gt;&gt; <a href="#">Dial PPPoE</a></span>					
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Eps)	RX Packets	RX Rate(Eps)
—	—	0	0	0	0
WAN 2 Status <span style="float: right;">&gt;&gt; <a href="#">Drop PPPoE</a></span>					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:54	
IP	GW IP	TX Packets	TX Rate(Eps)	RX Packets	RX Rate(Eps)
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(Eps)	RX Packets	RX Rate(Eps)
—	—	0	0	0	0
ADSL Information (ADSL Firmware Version: 05-04-04-04-00-01)					
ATM Statistics	TX Cells	RX Cells	TX CRC errs		RX CRC errs
	0	0	0		0
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin
		READY	0	0	0

Online Status

---

Physical Connection System Uptime: 02:12

IPv4		IPv6	
LAN Status			
IP Address			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	4	690	328
WAN2 IPv6 Status <span style="float: right;">&gt;&gt; <a href="#">Drop PPP</a></span>			
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP	Gateway IP		
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)	FE80::9G:1A00:242:AD52		
FE8D::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:B000:168::1			
2001:B000:168::2			
TX Packets	RX 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 <http://gogo6.com/> after applied for the service.)

WAN2 -> Internet Access

WAN2

PPPoE	Static or Dynamic IP	PPPoL2TP	IPv6
<b>Internet Access Mode</b>			
Connection Type		TSPC	
<b>TSPC Configuration</b>			
Username		gogogogo	
Password		*****	
Confirm Password		*****	
Tunnel Broker		gogogogo	
OK		Cancel	

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status

Physical Connection System Uptime: 0:2:3

IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
2001:5C0:1502:000:210:AFF:FEA6:2568/64 (Global)			
FE80::210:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
88	121	15596	10249
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	TSPC	0:01:40	
<b>IP</b>		<b>Gateway IP</b>	
2001:5C0:1400:8::1089/128 (Global)		—	
FE80::722C:3009/128 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
127	89	9219	15866

- **AICCU – Tunnel application**

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 <https://www.sixxs.net/main/> after applied for the service.)

WAN2 > Internet Access

---

WAN2

PPPoE	Static or Dynamic IP	PPPoE/2IP	IPv6
			Internet Access Mode
			Connection Type: AICCU
			AICCU Configuration <input type="checkbox"/> Always On Username: JCR33IXXS Password: ***** Confirm Password: ***** Tunnel Broker: https://www.sixxs.net Subnet Prefix: 2001:4DD0:FF00:3E4:2 / 64

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

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status

---

Physical Connection System Uptime: 0:1:18

IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address:</b>			
2001:4DD0:FF00:3E4:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
147	187	34205	19176
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	AICCU	0:00:48	
<b>IP</b>	2001:4DD0:FF00:3E4:2/64 (Global)		<b>Gateway IP</b>
FE80::4CD0:FF00:3E4:2/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
186	137	16438	33093

- **DHCPv6 Client**

Choose DHCPv6 Client. Click one of the identity associations and type the IAID number.

**WAN 2 Internet Access**

**WAN 2**

PPPoE	Status: (Dynamic) IP	PPPoE 2/1P	IPv6
<b>Internet Access Mode</b>			
Connection Type		<b>DHCPv6 Client</b>	
<b>DHCPv6 Client Configuration</b>			
Identity Association		<input type="radio"/> Prefix Delegation   <input checked="" type="radio"/> Non-temporary Address	
IAID (Identity Association ID)		<b>974273090</b>	
<b>OK</b>		<b>Cancel</b>	

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shown as follows:

**Online Status**

Physical Connection		System Uptime: 00:50	
IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
<b>FE80::21D:A AFF:FEA6:256B/64 (Link)</b>			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
6	2	588	156
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	<b>DHCPv6 Client</b>	0:00:40	
<b>IP</b>		<b>Gateway IP</b>	
<b>2001:8010:7300:201:21D:A AFF:FEA6:256A/64 (Global)</b>		---	
2001:1111:2222:5555:21D:A AFF:FEA6:256A/64 (Global)			
2001:1111:2222:3333::1111/128 (Global)			
FE80::21D:A AFF:FEA6:256A/64 (Link)			
<b>DNS IP</b>			
2001:4860:4860::8888			
2001:4850:4850::8844			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
14	5	1174	694



- **Static IPv6**

Choose Static IPv6. Type IPv6 address, Prefix Length and Gateway Address.

WAN >> Internet Access

---

WAN 2

PPPoE      Static or Dynamic IP      PPTP/L2TP      IPv6

Internet Access Mode

Connection Type: Static IPv6

Static IPv6 Address configuration

IPv6 Address: 2001:B010:7300:201:21D:AFF:FEA6:256A / Prefix Length: 64

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	2001:B010:7300:201:21D:AFF:FEA6:256A/64	Global
2	2001:1111:2222:5555:21D:AFF:FEA6:256A/64	Global
3	FE80::21D:AFF:FEA6:256A/64	Link

Static IPv6 Gateway configuration

IPv6 Gateway Address: —

OK      Cancel

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shown as follows:

Online Status

---

Physical Connection      System Uptime: 0:4:2

IPv4      IPv6

LAN Status

IP Address: FE80::21D:AFF:FEA6:2568/64 (Link)

TX Packets	RX Packets	TX Bytes	RX Bytes
4	0	312	0

WAN2 IPv6 Status

Enable	Mode	Up Time	Gateway IP
Yes	Static IPv6	0:03:56	—

IP: 2001:B010:7300:201:21D:AFF:FEA6:256A/64 (Global)

TX Packets	RX 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 Viogr2925. Open **LAN>> General Setup**. Click the **IPv6** button.

**Note:** Only the subnet of **LAN1** supports IPv6 feature.

LAN >> General Setup

LAN 1 Ethernet TCP/IP and DHCP Setup      LAN 1 IPv6 Setup

**RADVD Configuration**

Enable     Disable  
Advertisement Lifetime: 1800    Seconds (Range: 600 - 9000)

**DHCPv6 Server Configuration**

Enable Server     Disable Server

Start IPv6 Address: 2001:1111:2222:3333:1111  
End IPv6 Address: 2001:1111:2222:3333:2222

**DNS Server IPv6 Address**

Primary DNS Server: 2001:4860:4860:8988  
Secondary DNS Server: 2001:4860:4860:8844

**Static IPv6 Address configuration**

IPv6 Address: / Prefix Length: /    Add    Delete

**Current IPv6 Address Table**

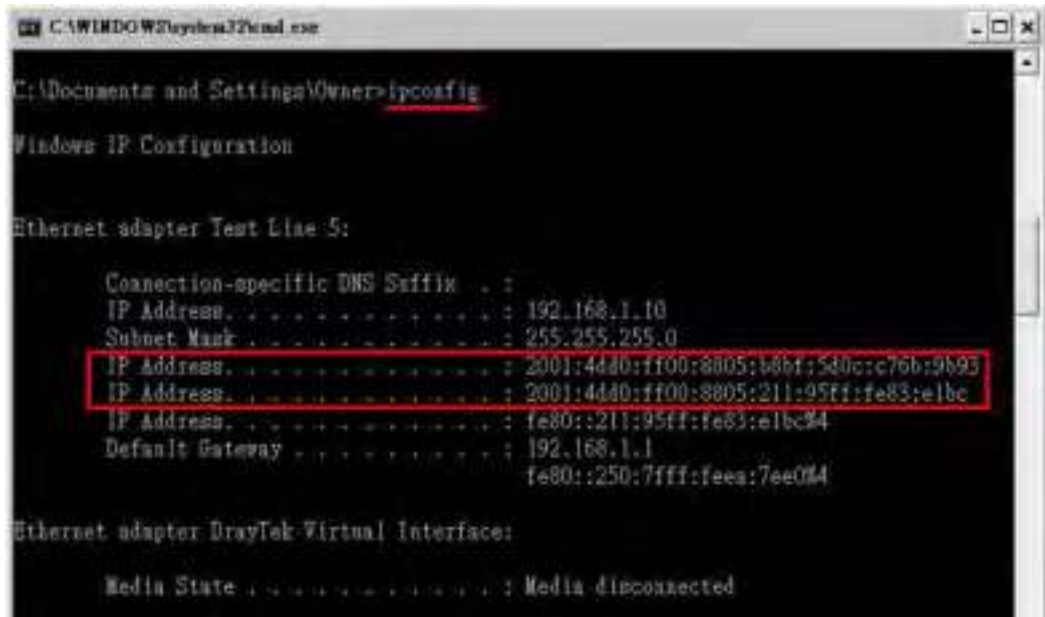
Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FEA6:2568/64	Link

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.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Owner>ipconfig

Windows IP Configuration

Ethernet adapter Test Line 5:

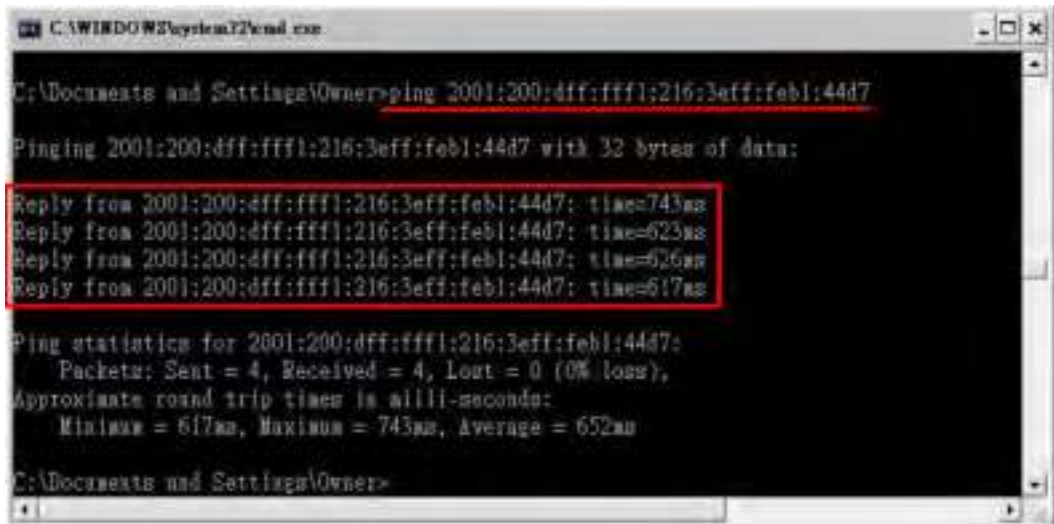
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 192.168.1.10
    Subnet Mask . . . . .              : 255.255.255.0
    IP Address. . . . .                : 2001:4440:ff00:8005:211:95ff:fe83:e1bc
    IP Address. . . . .                : 2001:4440:ff00:8005:211:95ff:fe83:e1bc
    Default Gateway . . . . .          : 192.168.1.1
                                         Fe80::250:7fff:feea:7ee0%4

Ethernet adapter DrayTek Virtual Interface:

    Media State . . . . .              : Media disconnected
```

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, [www.kame.net](http://www.kame.net) 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
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>
```

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., [www.kame.net](http://www.kame.net). 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.

### 3.2 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:** 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 => OpenVPN General Setup

OpenVPN General Setup

Port	1194
Cipher Algorithm	AES128
HMAC Algorithm	SHA1
Certificate authentication	<input type="checkbox"/>

Note: OpenVPN on vigor only 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

Enable this account

Idle Timeout 300 second(s)

Allowed Dial In Type

- PPP
- IPsec Tunnel
- L2TP with IPsec Policy None
- NAT Tunnel
- OpenVPN Tunnel

Specify Remote Node

Remote Client IP

Username jos

Password \*\*\*

Enable Mobile One-Time Password(MOTP)

MIN Code

Secret

IKL Authentication Method

Pre-Shared Key

Pre-Shared Key

Digital Signature(X.509)

None

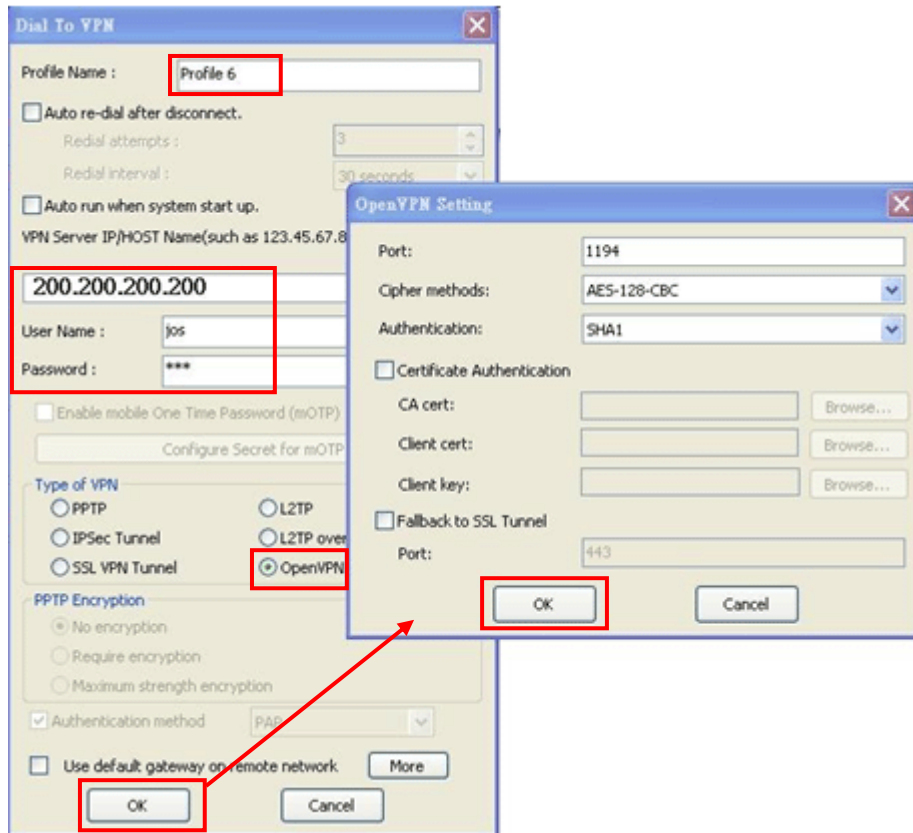
IKL Security Method

## Settings for PC (Remote User)

1. Execute **SmartVPN Client**. Click **Insert** to create a new dial-in VPN profile (e.g., Profile 6).



2. 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.



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

The screenshot displays the 'VPN and Remote Access => Connection Management' page. At the top, there is a 'Dial-out Tool' section with three rows: 'General Mode:', 'Backup Mode:', and 'Load Balance Mode:', each with a dropdown menu and a 'Dial' button. To the right, there is a 'Refresh Seconds' dropdown set to '10' and a 'Refresh' button. Below this is the 'VPN Connection Status' section, which includes 'Current Page: 1' and 'Page No.' with 'Go' and '>>' buttons. A table lists the VPN connections:

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Ups)	Rx Pkts	Rx Rate (Ups)	UpTime
1	OpenVPN	192.168.1.1	192.168.1.1	14	50	21	50	0:00

The screenshot shows a Windows command prompt window titled 'C:\WINDOWS\system32\cmd.exe - ping 192.168.1.1'. The text in the window reads: 'Pinging 192.168.1.1 with 32 bytes of data:' followed by eight lines of 'Reply from 192.168.1.1: bytes=32 time<1ms TTL=255'.



### 3.3 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 device, 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 Application >> USB Disk Status

The screenshot shows the 'USB Mass Storage Device Status' section. The 'Connection Status' is 'Disk Connected', which is highlighted with a red box. There is a 'Disconnect USB Disk' button. Below this, it shows 'Write Protect Status: No' and 'Disk Capacity: 5000 MB'. A 'Refresh' button is also present. At the bottom, there is a table with columns: Index, Service, IP Address(Port), and 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.

2. Then, please open **USB Application >> USB General Settings** to enable Samba service.

USB Application >> USB General Settings

The screenshot shows the 'USB General Settings' page. The 'Samba Service Settings(Network Neighborhood)' section is highlighted with a red box. It contains radio buttons for 'Enable' (selected) and 'Disable'. Below it are 'Access Mode' options: 'LAN only' and 'LAN and WAN'. There are also fields for 'Workgroup Name' and 'Host Name' (set to 'Vigor200').

Note: 1. If Charset is set to 'English', only English lang file name is supported.  
2. Multi-session ftp download will be banned by router if server. If your ftp client has 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 16 characters and a host name can have as many as 24 characters, but both cannot contain any of the following: \, /, <, >, |, =, /, \, /, \.

OK

- 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.

USB Application >> USB User Management

Profile Index: 1

FTP/Samba User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="password"/> (Maximum 11 Characters)
Confirm Password	<input type="password"/>
Home Folder	<input type="text"/> 📁
Access Rule	
File	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input checked="" type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z and 0-9 & % ! - \_ @ ~ \* ' ! ! ! / and space.

OK Clear Cancel

- Click **OK** to save the configuration.
- Make sure the FTP service is running properly. Please open a browser and type <ftp://192.168.1.1>. Use the account "**user1**" to login.

Log On

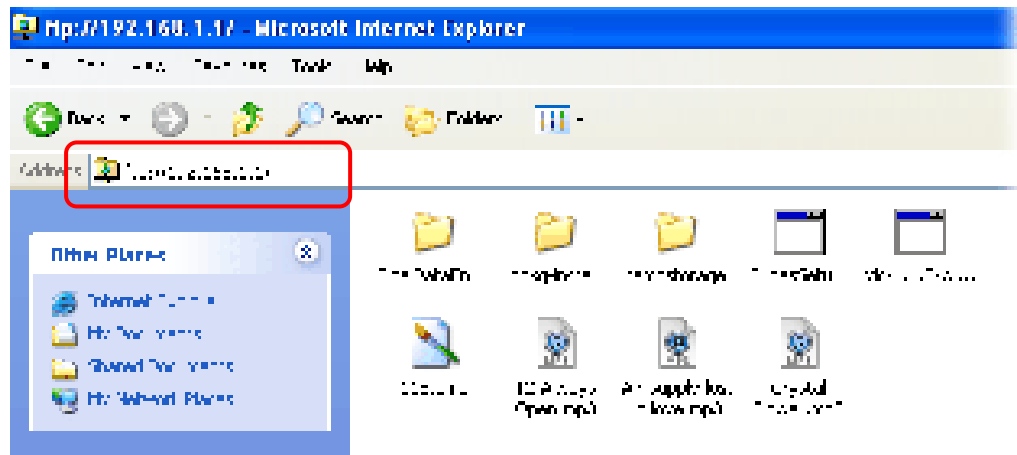
FTP Address: 192.168.1.1

Username:

Password:

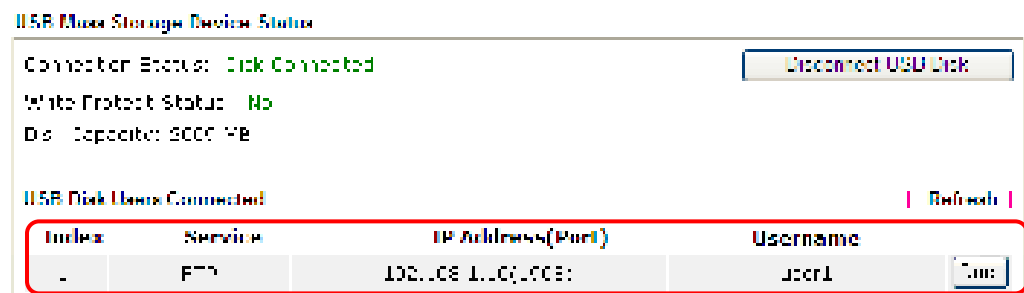
Log On Cancel

6. When the following screen appears, it means the FTP service is running properly.



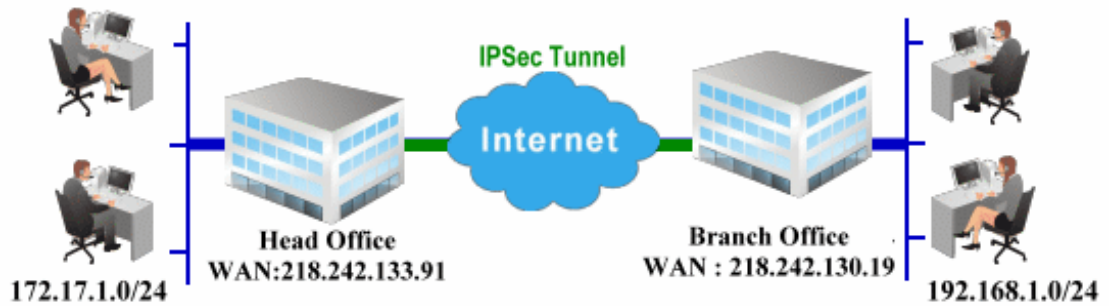
7. Return to **USB Application >> USB Disk Status**. The information for FTP server will be shown as below.

USB Application >> USB Disk Status



Now, users in LAN of Vigor2925 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**.

### 3.4 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.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: [Set to Factory Default](#)

View:  All  Online  Offline  Trunk  Search

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>		17.	???	<input type="checkbox"/>	
2.	???	<input type="checkbox"/>		18.	???	<input type="checkbox"/>	
3.	???	<input type="checkbox"/>		19.	???	<input type="checkbox"/>	
4.	???	<input type="checkbox"/>		20.	???	<input type="checkbox"/>	
5.	???	<input type="checkbox"/>		21.	???	<input type="checkbox"/>	
6.	???	<input type="checkbox"/>		22.	???	<input type="checkbox"/>	
7.	???	<input type="checkbox"/>		23.	???	<input type="checkbox"/>	

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**.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name:

Enable this profile

Call Direction:  Both  Dial Out  Dial In

always on

Idle Timeout:  second(s)

Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

VPN Dial Out Through WAN1 Port:

Netbios Naming Method:  Pass  Block

Multicast via VPN:  Pass  Block  
(for some ICMP, IP-Camera, DHCP Relay, etc.)

- 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

- PPTP
- IPSec Tunnel
- L2TP with IKEv2 Policy: None

Specify Remote VPN Gateway

Peer VPN Server IP: 218.242.130.19

or Peer ID: [ ]

Username: 999

Password: [ ]

IKE Compression:  On  Off

IKE Authentication Method

- Pre-Shared Key
- Digital Signature(X.509)

None [v]

Local ID

- Alternative Subject Name List
- Subject Name List

IPSec Security Method

Medium(AH)

High(ESP):  DES/3DES  AES

4. Go over IPsec Settings

- Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for remote side.

High(ESP)  IPsec Security Method: DES/3DES/AES

4. Go over IPsec Settings

Enable IPsec Dial-Out function (401 over IPsec)

Logical Traffic: My GRE ID: [ ] Peer GRE ID: [ ]

5. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.0

Remote Network Mask: 255.255.255.0

Local Network IP: 192.168.1.0

Local Network Mask: 255.255.255.0

More

ESP Direction: Disable [v]

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

Route [v]

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

OK Clear Cancel

- Click **OK** to save the settings.

- Open **VPN and Remote Access**>>**Connection Management** to check the dial-in connection status (from branch office).

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh: 5 seconds

(V2920) 172.16.2.145

VPN Connection Status

Current Page: 1 Page No:

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Pps)	Rx Pkts	Rx Rate (Pps)	UpTime
1	...	...	...	...	...	...	...	...

(Detailed) : Data is not type  
 x x x x : Data is not type

### Configuration on Vigor Router for Branch Office

- Log into the web user interface of Vigor router.
- 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-LAN Profiles:

View:  All  Online  Offline  Trunk

Index	Name	Action	Status	Index	Name	Action	Status
1.	???	?		17.	???	??	
2.	???	??		18.	???	??	
3.	???	??		19.	???	??	
4.	???	??		20.	???	??	
5.	???	??		21.	???	??	
6.	???	??		22.	???	??	
7.	???	??		23.	???	??	

- 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.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name:

Enable this profile

Call direction:  both  Dial out  Dial in

Always on

Idle Timeout:  second(s)

Enable ping to keep alive

PING to the IP:

2. Dial-Out Settings

- 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.

3. Dial Out Settings

Type of Server Tunneling

- PPP
- IPSec Tunnel
- L2TP with IPSec Policy (None)

Server IP/Host Name for VPN  
(Search as draytek.com or 1.2.1.4, etc.)

218.242.133.91

Username: [text field]

Password: [text field]

VPN Authentication: [PAP/MS/PEAP]

VPN Compression:  On  Off

IKE Authentication Method

- IKE Pre-Shared Key
- Digital Signature(X.509)

IKE Pre-Shared Key: [button] [masked text]

Peer ID: [text field]

Local ID:

- Alternative Subject Name List
- Subject Name List

IPSec Security Method

- Medium(AH)
- High(ESP) - TLS with Authentication

[Advanced]

Insect(1-16) in Schedule Setup:

- Continue to navigate to the **TCP/IP Network Settings** for setting the LAN IP for the remote side.

4. GRE over IPsec Settings

Enable IPsec Dial-Out function GRE over IPsec

Logical Traffic My WAN IP: [text field] Peer WAN IP: [text field]

5. TCP/IP Network Settings

My WAN IP	[0.0.0.0]	VPN Direction	[Bidirectional]
Remote Gateway IP	[0.0.0.0]	From first subnet to remote network, you have to do	
Remote Network IP	[192.168.1.0]	[Route]	
Remote Network Mask	[255.255.255.0]		
Local Network IP	[192.168.1.3]	<input type="checkbox"/> Change default route to this VPN tunnel ( Only Single WAN supports this )	
Local Network Mask	[255.255.255.0]		

[Main]

[OK] [Cancel] [Cancel]

- Click **OK** to save the settings.

- Open **VPN and Remote Access>>Connection Management** to check the dial-in connection status (from head office).

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Connection: [S] [W] [Refresh]

( V2820 ) 172.18.2.145 [Dial]

VPN Connection Status

Current Page: 1 Page No: [ ] [Go] [OK]

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Rps)	Rx Pkts	Rx Rate (Rps)	UpTime
1	IPSec Tunnel	200.0.0.100/31	172.17.1.0/24	0	0	100	0	00:00:00

[Drop]

x x x x : 1944-10-10 10:10:10  
x x x x : 1944-10-10 10:10:10

### 3.5 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:

- Open **Bandwidth Management>> Quality of Service**.

CSM

**Bandwidth Management**

Sessions Limit

Bandwidth Limit

Quality of Service

Applications

- You will get the following page. Click the **Edit** link for **Class 1**.

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	WIP Bandwidth Control	Online Statistics
WAN1	Disable	100000000kps/90000000kps		25%	25%	25%	25%	Inactive	Status Setup
WAN2	Disable	100000000kps/100000000kps		25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000000kps/100000000kps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		<b>Fill</b>	
Class 2		Fill	Fill
Class 3		Fill	

- In the following page, type a name (e.g., VoIP) for such class and click **Add**.



Bandwidth Management >> Quality of Service

Class Index 21

Name:  Log packets as:

ID	Status	Local Address	Remote Address	Diffserv CodePoint	Service Type
1	Empty				

4. Check the box of **ACT**. Click **Edit** to specify the local address.

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Internet Type:  IPv4  IPv6

Local Address:

Remote Address:

Diffserv CodePoint:

Service Type:

Note: Please choose/setup the Service Type 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.

Internet Type: IPv4

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

6. Click **OK** again to save the settings.

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Internet Type:  IPv4  IPv6

Local Address:

Remote Address:

Diffserv CodePoint:

Service Type:

Note: Please choose/setup the Service Type first.

- The class rule for VoIP has been set. Click **OK** to return to previous page.

Bandwidth Management >> Quality of Service

Class Index 41

Name: VoIP  Tag packets as: Default

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
10	active	172.16.1.240 ~ 172.16.1.241	Any	any	any

- Do the same steps to add class rules for IPTV and Data/Email with IP addresses as shown below.

Bandwidth Management >> Quality of Service

Class Index 42

Name: IPTV  Tag packets as: Default

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
10	active	172.16.1.242 ~ 172.16.1.243	Any	any	any

and

Bandwidth Management >> Quality of Service

Class Index 43

Name: DataEmail  Tag packets as: Default

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
10	active	Any	Any	IP precedence 2	any

- 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.

Bandwidth Management >> Quality of Service

General Setup Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	Setup
WAN1	Disable	101000000bps/50100000bps		20%	20%	20%	20%	Inactive	10-0-0	Setup
WAN2	Disable	10000000bps/10000000bps		20%	20%	20%	20%	Inactive	10-0-0	Setup
WAN3	Disable	10000000bps/10000000bps		20%	20%	20%	20%	Inactive	10-0-0	Setup

Class Rule

Index	Name	Rule	Service type
Class 1	VoIP	Fili	Fili
Class 2	IPTV	Fili	
Class 3	Data/Email	Fili	

- 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**.

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control QoS

Index	Class Name	Reserved Bandwidth Ratio
Class 1	VoIP	30 %
Class 2	IPTV	50 %
Class 3	Data/Email	15 %
	Others	0 %

Enable UDP Bandwidth Control Limited Bandwidth Ratio 25 %

Outbound TCP ACK Priorize

- Click **OK** to save the settings. The class rules for WAN1 are defined as shown below.

Bandwidth Management >> Quality of Service

General Setup Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Enable	101000000bps/50100000bps	Outbound	30%	50%	15%	0%	Inactive	Status Setup
WAN2	Disable	10000000bps/10000000bps		20%	20%	20%	20%	Inactive	10-0-0 Setup
WAN3	Disable	10000000bps/10000000bps		20%	20%	20%	20%	Inactive	10-0-0 Setup

Class Rule

Index	Name	Rule	Service type
Class 1	VoIP	Fili	Fili
Class 2	IPTV	Fili	Fili
Class 3	Data/Email	Fili	Fili

### 3.6 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

---

General Setup | Set to Factory Default

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	QoS Bandwidth Control	Online Statistics	Setup
WAN1	Disable	101080.000Kbps/90100.000Kbps		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
Class 1		Fifo	
Class 2		Fifo	Fifo
Class 3		Fifo	

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

Enable the QoS Control BOTH ▾

WAN Inbound Bandwidth

WAN Outbound Bandwidth

3. Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

---

WAN2 General Setup

Enable the QoS Control BOTH ▾

WAN Inbound Bandwidth 100000 Kbps

WAN Outbound Bandwidth 100000 Kbps

Index	Class Name	Reserved bandwidth Ratio
Class 1	VoIP	20 %

**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.

- 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.

Bandwidth Management >> Quality of Service

Class Index #1

Name: E-mail Tag packets as: Default

NO	Status	Local Address	Remote Address	DHIServ CodePoint	Service Type
1	Active	Any	Any	ANY	ANY

- 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.

Bandwidth Management >> Quality of Service

WAN2 General Setup

Enable the QoS Control QoS

WAN Inbound Bandwidth: 10000 Kbps

WAN Outbound Bandwidth: 10000 Kbps

Index	Class Name	Reserved Bandwidth Ratio
Class 1	E-mail	<u>25</u> %
Class 2		25 %
Class 3		25 %
	Others	25 %

Enable UDP Bandwidth Control Limited bandwidth ratio: 25 %

Outbound TCP ACK Priorize

- 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**.

Bandwidth Management >> Quality of Service

Class Index #2

Name: HTTPS Tag packets as: Default

NO	Status	Local Address	Remote Address	DHIServ CodePoint	Service Type
1	Active	172.16.1.242 - 172.16.1.249	Any	ANY	ANY

- Click **Setup** link for WAN2.

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	Setup
WAN1	Enable	10000000kbits/4000000kbits	Outbound	0%	10%	15%	5%	Inactive	Status	Setup
WAN2	Enable	1000000kbits/1000000kbits	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	1000000kbits/1000000kbits		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	Default	Fall	Fall
Class 2	00:19:	Fall	
Class 3		Fall	

- Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic influent other application. Click **OK**.

Bandwidth Management >> Quality of Service

WAN2 General Setup

Enable the QoS Control UDP

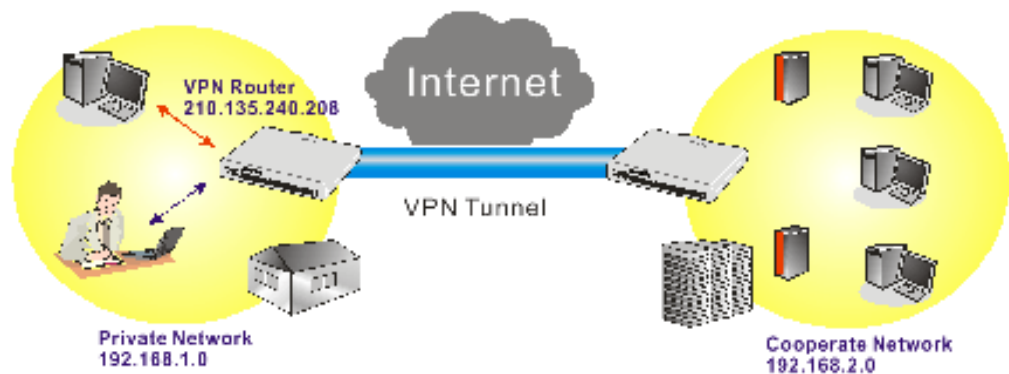
WAN Inbound Bandwidth	100000	kbits
WAN Outbound Bandwidth	100000	kbits

Index	Class Name	Reserved Bandwidth Ratio
Class 1	Default	25 %
Class 2	00:19:	25 %
Class 3		25 %
	Others	25 %

Enable UDP Bandwidth Control Unified Bandwidth Ratio: 25 %

Outbound TCP ACK Priorize

- 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.



- Click **Edit** for Class 3 to open a new window. In this index, the user will set reserved bandwidth for **VPN**.

Bandwidth Management => Quality of Service

Class Index #1

Name:  Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

- Click **Add** to open the following window. Check the **ACT** box, first.

Bandwidth Management => Quality of Service

Rule Edit

ACT

Ethernet Type:  IPv4  IPv6

Local Address:

Remote Address:

DiffServ CodePoint:

Service Type:

Note: Please choose/setup the Service Type first.

- 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**.

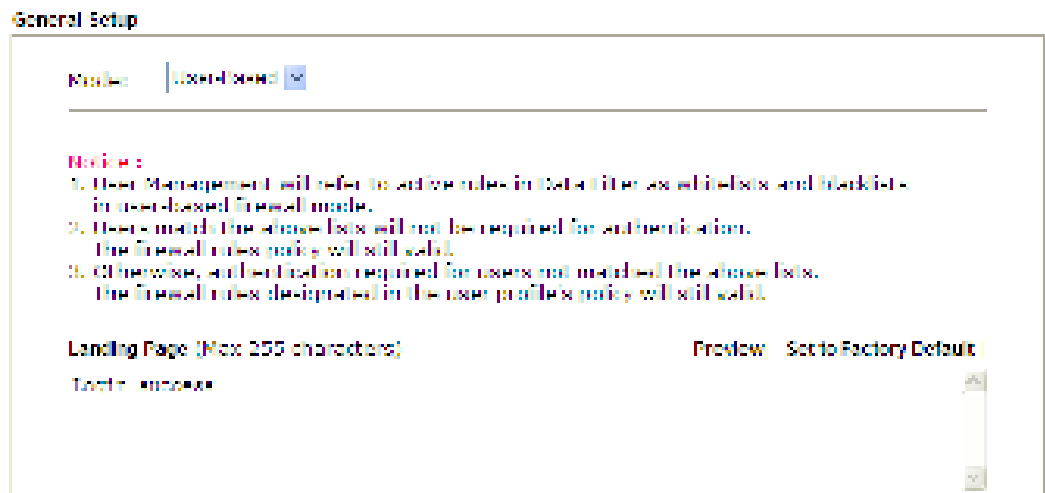
### 3.7 How to use Landing Page Feature

**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 Vigor2925 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 Vigor2925.
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.

User Management >> General Setup



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
<a href="#">1.</a>	admin
<a href="#">2.</a>	Dial-In User
<a href="#">3.</a>	
<a href="#">4.</a>	



- In the following page, check the box of **Landing page** and click **OK** to save the settings.

User Management => User Profile

Profile Index 3

<input checked="" type="checkbox"/> Enable this account	
User Name	CaCa
Password	****
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	11 0:Unlimited
External Server Authentication	None
Log	None
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Web Tool <input checked="" type="checkbox"/> Telnet
<b>Landing Page</b>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Enable Time Quota	0 min(s) Refresh Add min(s) min(s)
Index(1-15) in Schedule Section	

OK Clear Cancel

- 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.

- 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 <http://www.draytek.com> 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'>window.location='http://www.draytek.com'</script></body>”**

User Management >> General Setup

General Setup

Mode:

---

**Notice :**

1. User Management will refer to active rules in state filter, whitelist and blacklist in user-based firewall mode.
2. Users match the choice box will not be required for authentication, the firewall rules policy will still valid.
3. Otherwise, authentication required for users not matched the choice box, the firewall rules designated in the user profile policy will still valid.

**Landing Page (Max 255 characters)** Preview    Set to Factory Default

`<body stats=1><script language='javascript'>window.location='http://www.draytek.com'</script></body>`

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
<b><u>3.</u></b>	
<u>4.</u>	
<u>5.</u>	

3. In the following page, check the box of **Landing page** and click **OK** to save the settings.

User Management > User Profile

Profile Index >

<input checked="" type="checkbox"/> Enable this account	
User Name	CaCa
Password	****
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimtd
Max User Login	11 0:Unlimtd
External Server Authentication	None
Flow	None
Pop Browser Tracking Window	<input checked="" type="checkbox"/>
Authentication	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Web Tool <input checked="" type="checkbox"/> Other
Logging Page	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Enable Time Quota	0 min(s) Refresh Add more min(s)
Index(1-15) in Schedule(1-15)	

OK Clear Cancel

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

Copyright © DrayTek Corp. All Rights Reserved. DrayTek

5. Click **Login**. If the logging is successful, you will be directed into the website of [www.draytek.com](http://www.draytek.com).



### 3.8 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection

Follow the steps listed below:

1. Log into the web user interface of Vigor router.
2. Configure relational objects first. Open **Object Settings>>SMS/Mail Server Object** to get the following page.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index	Profile Name	SMS Provider	
1.		kat-sms.com.tw (TW)	
2.		kat-sms.com.tw (TW)	
3.		kat-sms.com.tw (TW)	
4.		kat-sms.com.tw (TW)	
5.		kat-sms.com.tw (TW)	
6.		kat-sms.com.tw (TW)	
7.		kat-sms.com.tw (TW)	
8.		kat-sms.com.tw (TW)	
9.	Custom 1		
10.	Custom 2		

Index 1 to Index 8 allows you to choose the built-in SMS service provider. If the SMS service provider is not on the list, you can configure Index 9 and Index 10 to add the new service provider to Vigor router.

3. Choose any index number (e.g., Index 1 in this case) to configure the SMS Provider setting. In the following page, type the username and password and set the quota that the router can send the message out.

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Local number
Service Provider	kat-sms.com.tw (TW)
Username	ab09020
Password	***
Quota	0
Sending Interval	0 (seconds)

- After finished the settings, click **OK** to return to previous page. Now you have finished the configuration of the SMS Provider profile setting.

Object Settings >> SMS / Mail Service Object

Index	Profile Name	SMS Provider
1	Local number	kctsms.com.tw (TW)
2		kctsms.com.tw (TW)
3		kctsms.com.tw (TW)
4		kctsms.com.tw (TW)
5		kctsms.com.tw (TW)
6		kctsms.com.tw (TW)
7		kctsms.com.tw (TW)
8		kctsms.com.tw (TW)
9	Custom 1	
10	Custom 2	

- Open **Object Settings>>Notification Object** to configure the event conditions of the notification.

Object Settings >> Notification Object

Index	Profile Name	Settings
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

- Choose any index number (e.g., Index 1 in this case) to configure conditions for sending the SMS. In the following page, type the name of the profile and check the Disconnected and Reconnected boxes for WAN to work in concert with the topic of this paper.

Object Settings >> Notification Object

Profile Index: 1

Profile Name	WAN_Notify	
Category	Status	
WAN	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected
VPN Tunnel	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected
Temperature Alert	<input type="checkbox"/> Out of Range	

OK Clear Cancel

- After finished the settings, click **OK** to return to previous page. You have finished the configuration of the notification object profile setting.

Object Settings >> Notification Object

| Set to Factory Default |

Index	Profile Name	Settings
1.	WAN Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

- Now, open **Application >> SMS / Mail Alert Service**. Use the drop down list to choose SMS Provider and the Notify Profile (specify the time of sending SMS). Then, type the phone number in the field of Recipient (the one who will receive the SMS).

Application >> SMS / Mail Alert Service

| Set to Factory Default |

SMS Provider		Mail Server		Schedule	
Index	SMS Provider	Recipient	Notify Profile	Start	End
1 <input checked="" type="checkbox"/>	1 Local number	0512345678	1 WAN Notify		
2 <input type="checkbox"/>	1 Local number		1 WAN Notify		
3 <input type="checkbox"/>	1 Local number		1 WAN Notify		
4 <input type="checkbox"/>	1 Local number		1 WAN Notify		
5 <input type="checkbox"/>	1 Local number		1 WAN Notify		
6 <input type="checkbox"/>	1 Local number		1 WAN Notify		
7 <input type="checkbox"/>	1 Local number		1 WAN Notify		
8 <input type="checkbox"/>	1 Local number		1 WAN Notify		
9 <input type="checkbox"/>	1 Local number		1 WAN Notify		
10 <input type="checkbox"/>	1 Local number		1 WAN Notify		

- Click **OK** to save the settings. Later, if one of the WAN connections fails in your router, the system will send out SMS to the phone number specified. If the router has only one WAN interface, the system will send out SMS to the phone number while reconnecting the WAN interface successfully.

## Remark: How the customize the SMS Provider

Choose one of the Index numbers (9 or 10) allowing you to customize the SMS Provider. In the web page, type the URL string of the SMS provider and type the username and password. After clicking OK, the new added SMS provider will be added and will be available for you to specify for sending SMS out.

Object Settings => SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text" value="clicktel"/>
<hr/>	
Please contact with your EMS provide to get the exact URL String eg:bulksms.vsms.net:8867/cep/submiton/send_sms/2/2.0?username=#####&password=#####&sidn=#####&message=#####	
Username	<input type="text" value="jan123"/>
Password	<input type="password" value="*****"/>
Quota	<input type="text" value="0"/>
Sending Interval	<input type="text" value="0"/> (seconds)

### 3.9 How to Create an Account for MyVigor

The website of MyVigor (a server located on <http://myvigor.draytek.com>) 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.

#### 3.9.1 Create an Account via Vigor Router

1. Click CSM>> **Web Content Filter Profile**. The following page will appear.

Or

Click **System Maintenance>>Activation** to open the following page.





5. Type your personal information in this page and then click **Continue**.

The screenshot shows a registration form titled "Register" with the subtitle "Create an account - Please enter personal profile (fields marked with \* are required)". The form is divided into four steps: 1. Agreement, 2. Personal Information (highlighted), 3. Preferences, and 4. Completion. Under "Account Information", there are fields for Username (filled with "Mary"), Password (masked with "\*\*\*\*"), and Confirm Password (masked with "\*\*\*\*"). A "Check Account" button is next to the Username field. Under "Personal Information", there are fields for First Name (filled with "Mary"), Last Name (filled with "Tech"), Company Name (filled with "Tech Ltd"), and Email Address (filled with "mary\_tech@tech.com"). Below these are fields for Tel (with a country code dropdown), Country (filled with "SWITZERLAND"), and Career (filled with "Supervisor"). At the bottom right, there are "Back" and "Continue" buttons.

6. Choose proper selection for your computer and click **Continue**.

The screenshot shows the same registration form, but now at step 3, "Preferences". The subtitle is "Create an account - Please enter personal profile.". The form asks for preferences: "How did you find out about this website?" (dropdown menu), "What kind of antivirus do you use?" (dropdown menu), "I would like to subscribe to the MyVigor e-Jetter." (checkbox checked), "I would like to receive DrayTek product news." (checkbox checked), and "Please select the mail server for receiving the verification mail." (dropdown menu). At the bottom right, there are "Back" and "Continue" buttons.

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 myvigor.draytek.com**.

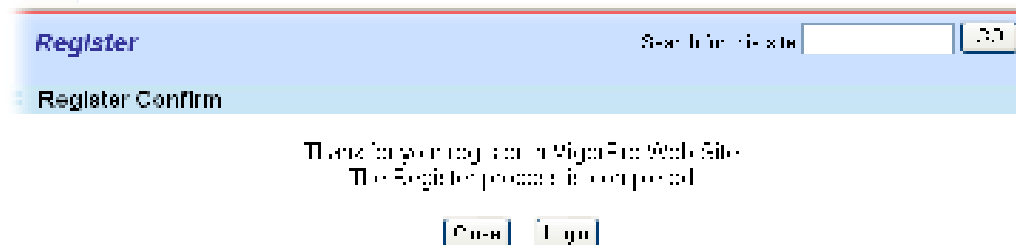
\*\*\*\*\* This is an automated message from myvigor.draytek.com. \*\*\*\*\*

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**.



- When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

If you are having difficulty logging in, contact our customer service.  
Customer Service : (888) 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.

### 3.9.2 Create an Account via MyVigor Web Site

- Access into <http://myvigor.draytek.com>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



- Now you have created an account successfully. Click **START**.



- Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

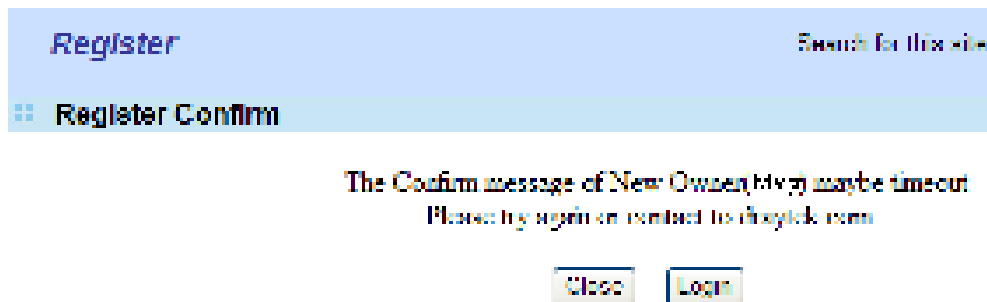
\*\*\*\*\* This is an automated message from myvigor.draytek.com. \*\*\*\*\*

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

- 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**.



- 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 :

Password :

Auth Code :  **T4he1C**

If you cannot read the word, [click here](#)

[Forgot password?](#)

---

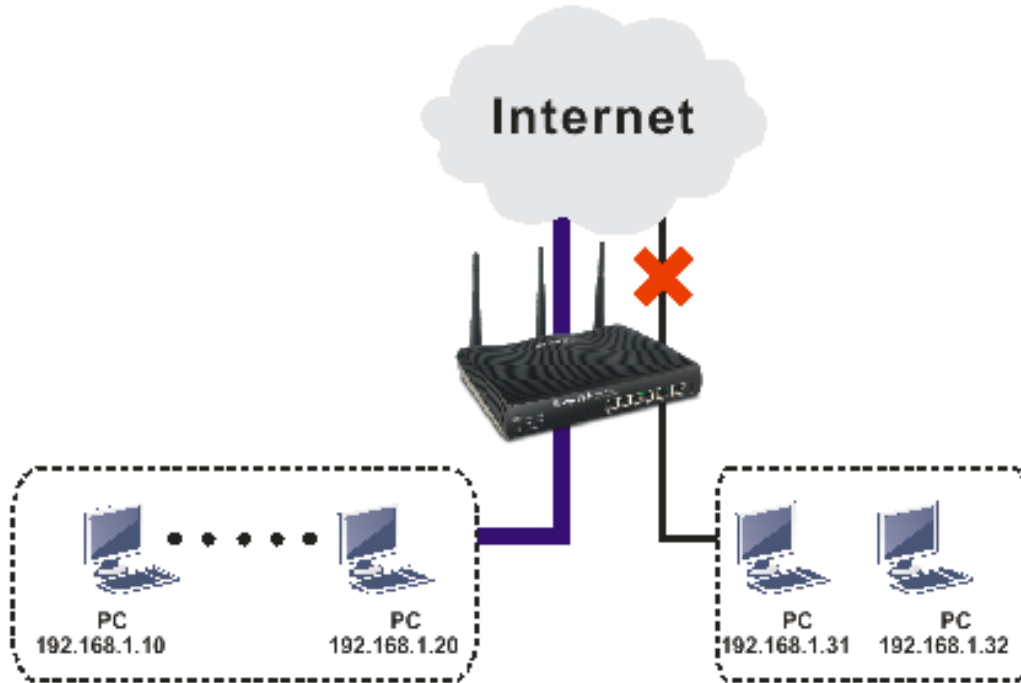
Don't have a MyVigor Account? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.  
Customer Service : (888) 3 587 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.

### 3.10 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.

Firewall >> Filter Setup

Set	Comments	Set	Comments
1	Default Set Filter	7	
<b>2</b>	Default Data Filter	<b>8</b>	
3		9	
4		10	
5		11	
6		12	

Firewall >> Filter Setup >> Edit Filter Set

Filter Rule 2

Comments: Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
<b>1</b>	<input checked="" type="checkbox"/>	Default Data Filter	UP	Down
<b>2</b>	<input type="checkbox"/>		UP	Down
3	<input type="checkbox"/>		UP	Down



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**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments:

Invert:  In Schedule Setup:  Clear sessions when schedule ON:

Direction:

Source IP:

Destination IP:

Service Type:

Protocols:

Application:

Filter:

Back to Filter Set Edit Filter Set

**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**.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments:

Invert:  In Schedule Setup:  Clear sessions when schedule ON:

Direction:

Source IP:

Destination IP:

Service Type:

Protocols:

Application:

Filter:

Back to Filter Set Edit Filter Set

- 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.

**IP Address Edit**

<b>Address Type</b>	Range Address
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	<input type="checkbox"/>
<b>IP Group</b>	None
or <b>IP Object</b>	None
or IP Object	None
or IP Object	None
<b>IPv6 Group</b>	None
or <b>IPv6 Object</b>	None
or IPv6 Object	None
or IPv6 Object	None

OK Close

- 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 Filter Set 2 Rule 0

Check to enable this Filter Rule

Comments: [open]

Enable ( ) in **Schedule** Setup

Time Zone: [GMT+08:00] [Full]

Start Date: [2018-10-10] [Full]

End Date: [2018-10-10] [Full]

Start Time: [00:00] [Full]

End Time: [00:00] [Full]

Parameters: [In Case] [Full]

Application: [ActionProfile] [Full]

Filter: [Pass Immediately] [Full]

System Log: [ ]

- Both filter rules have been created. Click **OK**.

Home > Filter Setup > Edit Filter Set

**Filter Set 2**

Comments: Default Data Filter

Filter Rule	Action	Comments	Block Up	Block Down
1	<input checked="" type="checkbox"/>	Net Filter - 10.1		Down
2	<input checked="" type="checkbox"/>	Block_01	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	Block_1	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

Next Filter Set

- 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.



- Open CSM >> **Web Content Filter Profile** to create a WCF profile. Check **Social Networking** with Action, **Block**.

The screenshot shows the 'Web Content Filter Profile' configuration page. The 'Social Networking' checkbox is checked and highlighted with a red box. The page is organized into several sections with 'Select All' and 'Clear All' buttons for each.

Category	Options
Leisure	<input type="checkbox"/> Entertainment <input type="checkbox"/> Games <input type="checkbox"/> Sports <input type="checkbox"/> Travel <input type="checkbox"/> Leisure & Recreation <input type="checkbox"/> Fashion & Beauty
Business	<input type="checkbox"/> Business <input type="checkbox"/> Job Search <input type="checkbox"/> Web-based Mail
Chatting	<input type="checkbox"/> Chat <input type="checkbox"/> Instant Messaging
Computer/Internet	<input type="checkbox"/> Anonymous <input type="checkbox"/> Forums & Newsgroups <input type="checkbox"/> Computers <input type="checkbox"/> Download Sites <input type="checkbox"/> Streaming, Downloads <input type="checkbox"/> Phishing & Fraud <input checked="" type="checkbox"/> Search Engine/Portals <input checked="" type="checkbox"/> Social Networking <input type="checkbox"/> Spam Sites <input type="checkbox"/> Malware <input type="checkbox"/> Botnets <input type="checkbox"/> Hacking <input type="checkbox"/> Illegal Software <input type="checkbox"/> Information Security <input type="checkbox"/> Peer-to-Peer
Other	<input type="checkbox"/> Adv & Pop-Ups <input type="checkbox"/> Arts <input type="checkbox"/> Transportation <input type="checkbox"/> Compromised <input type="checkbox"/> Dating & Romance <input type="checkbox"/> Education

- Enable this profile in **Firewall>>General Setup>>Default Rule**.

Firewall >> General Setup

The screenshot shows the 'General Setup' page with the 'Default Rule' tab selected. The 'Web Content Filter' dropdown menu is open, and '1-Default' is selected and highlighted with a red box.

Setting	Action/Profile	Syslog
Application	Block	<input type="checkbox"/>
Filter	CE / SUCDD	<input type="checkbox"/>
Sessions Control	Name	<input type="checkbox"/>
Quality of Service	App-Sets	<input type="checkbox"/>
Load Balance policy	Name	<input type="checkbox"/>
User Management	Name	<input type="checkbox"/>
APP Enforcement	Name	<input type="checkbox"/>
URI Content Filter	Name	<input type="checkbox"/>
Web Content Filter	1-Default	<input type="checkbox"/>
Advanced Filtering	1-Default	<input type="checkbox"/>

- 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]

## II. Via URL Content Filter

### A. Block the web page containing the word of “Facebook”

- Open **Object Settings>>Keyword Object**. Click an index number to open the setting page.
- In the field of **Contents**, please type *facebook*. Configure the settings as the following figure.

Object Setting >> Keyword Object Setup

Profile Index : 1

Name	facebook
Contents	facebook

Limit of Contents: Max 3 Words and 80 Characters.  
Each word should be separated by a single space.

You can replace a character with %HEX.  
Example:  
Contents: backdoor%7E virus keep%20out

Result:  
1. backdoor  
2. virus  
3. keep out

OK Cancel Cancel

- Open **CSM>>URL Content Filter Profile**. Click an index number to open the setting page.
- Configure the settings as the following figure.

Profile Index: 1

Profile Name:

Priority:  Log:

**1. URL Access Control**

Enable URL Access Control  Prevent web access from IP address

Action:

**2. Web Feature**

Enable Restrict Web Feature

Action:   Cookie  Proxy  Upload File Extension Profile:

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.

Firewall >> General Setup

General Setup

General Setup    Default Rule

Actions for default rule:	Action/Profile	Syslog
Application	<input type="text" value="Pass"/>	<input type="checkbox"/>
Filter	<input type="text" value="0 / 50000"/>	<input type="checkbox"/>
Sessions Control	<input type="text" value="None"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="None"/>	<input type="checkbox"/>
User Management	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement	<input type="text" value="None"/>	<input type="checkbox"/>
<b>URL Content Filter</b>	<input type="text" value="1-Facebook"/>	<input type="checkbox"/>
Web Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

### 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: app=facebook

Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.

You can replace ' ' character with %20.

Example:  
Contents: facebook /? v=vs=keep%20out

Result:  
1. facebook  
2. v=vs  
3. keep out

OK Clear Cancel

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 Index : 2

Profile Name: fbcc.apps

Priority: Filter HTTP Access Control First Tag: None

1.URL Access Control

Enable URL Access Control  Prevent web access from IP address

Action: Block Group/Object Selection: facebook. Edit

2.Web Feature

Enable Restrict Web Feature

Action: Deny  Cookie  Proxy  Upload File Extension Profile: None

OK Clear Cancel

5. When you finished the above steps, please open **Firewall>>General Setup**.



- 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.

Firewall >> General Setup

#### General Setup

The screenshot shows the 'General Setup' page for a firewall rule, with the 'Default Rule' tab selected. The page is divided into two sections: 'General Setup' and 'Default Rule'. The 'Default Rule' section contains a table of configuration options for the default rule. The 'URL Content Filter' option is highlighted with a red box and is set to '2 face.spss'. Below the table is an 'Advanced Setting' section with a 'Fill' button.

Application	Action/Profile	System
Filter	Pass	<input type="checkbox"/>
Sessions Control	1 / 6000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
Load-Balance policy	Auto Select	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
<b>URL Content Filter</b>	<b>2 face.spss</b>	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>

Advanced Setting

### 3.12 How to Setup 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 Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

NAT Address Mapping function lets you specify the outgoing IP address(es) for one internal IP address or a block of internal IP addresses.

We will take an example to introduce how to make use of this feature.

1. Log into the web user interface of Vigor2925.
2. Open **WAN>>Internet Access**. For WAN1, choose **MPoA/Static or Dynamic IP** as the **Access Mode**.

WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static	[-] [x] [OK]	[+]
WAN2		Ethernet	Static	[-] [x] [OK]	[+]
WAN3		WiFi	Static	[-] [x] [OK]	[+]

Note: Only WAN1, WAN2, WAN3 are supported.



- After finished configuration for WAN1, open **Load-Balance/Route Policy**.

**Load Balance/Route Policy**

Policy Route | [Set to Factory Default](#)

Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input type="checkbox"/>	any	WAN1	---								Down
2	<input checked="" type="checkbox"/>	any	WAN1								UP	Down
3	<input type="checkbox"/>	any	WAN1	---							UP	Down
4	<input checked="" type="checkbox"/>	any	WAN1								UP	Down
5	<input type="checkbox"/>	any	WAN1	---							UP	Down
6	<input checked="" type="checkbox"/>	any	WAN1								UP	Down
7	<input type="checkbox"/>	any	WAN1								UP	Down
8	<input checked="" type="checkbox"/>	any	WAN1	---							UP	Down
9	<input type="checkbox"/>	any	WAN1								UP	Down
10	<input checked="" type="checkbox"/>	any	WAN1	---							UP	Down

← 1 10 | 11 20 | 21 30 | 31 40 | 41 50 → [Next](#) →

- Click Index number 1 and 2 to configure the details. After finished the settings, click **OK** to save the settings respectively.

**Load Balance/Route Policy**

Index: 1

Enable criteria

Protocol: any

Source IP:
 

- any
- Src IP Start: 100.108.1.10 Src IP End: 100.108.1.31

Destination IP:
 

- any
- Dest IP Start: | Dest IP End: |

Destination Port:
 

- any
- Dest Port Start: | Dest Port End: |

send to if criteria matched

Interface: WAN1

Interface Address: ---

Gateway IP:
 

- default gateway
- specific gateway: \_\_\_\_\_

more options

Auto Failover To The Other WAN

Packet Forwarding to WAN via:
 

- force NAT
- force Routing

And

Load-Balance/Route Policy

Index: 2

Enable

criteria

---

Protocol: any

Source IP:
 

- any
- Src IP Start: 192.168.1.100 Src IP End: 192.168.1.101

Destination IP:
 

- any
- Dest IP Start: Dest IP End: \*
- any
- Dest Port Start: Dest Port End: \*

extend to all criteria matched

---

Interface: WAN1

Interface Address: 202.211.100.11

Gateway IP:
 

- default gateway
- specific gateway:

more options

Auto Failover To The Other WAN

Packet Forwarding to WAN via:
 

- force NAT
- force Routing

OK Cancel Done

- Upon completing the above configuration, you have specified the outgoing IP address(es) for some specific computers.

Load-Balance/Route Policy

Policy Route [Set to Factory Default](#)

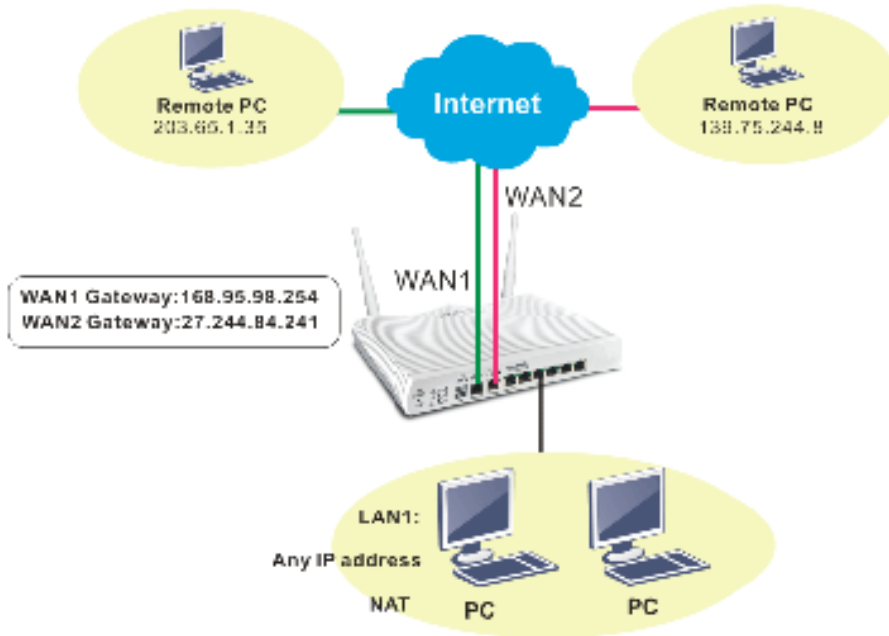
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	More Up	More Down
1	<input checked="" type="checkbox"/>	any	WAN1		192.168.1.10	192.168.1.31	Any	Any	Any	Any		Down
2	<input checked="" type="checkbox"/>	any	WAN1	202.211.100.11	192.168.1.100	192.168.1.101	Any	Any	Any	Any	UP	Down
3	<input type="checkbox"/>	any	WAN1	---							UP	Down
4	<input type="checkbox"/>	any	WAN1	---							UP	Down
5	<input type="checkbox"/>	any	WAN1	---							UP	Down
6	<input type="checkbox"/>	any	WAN1	---							UP	Down
7	<input type="checkbox"/>	any	WAN1	---							UP	Down
8	<input type="checkbox"/>	any	WAN1	---							UP	Down
9	<input type="checkbox"/>	any	WAN1	---							UP	Down
10	<input type="checkbox"/>	any	WAN1	---							UP	Down

« 1 10 | 11 20 | 21 30 | 31 40 | 41 50 » Next >>

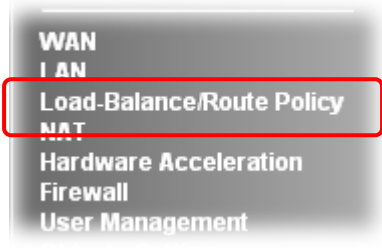
- Now, you bind some specific computers to some WAN IP alias for outgoing traffic.

### 3.13 How to Setup Load Balance for Packets?

The following figure shows a simple application of load balance. WAN1 and WAN2 can be used to access into Internet. The PC in LAN1 can send the data to the remote PC through the specified WAN1.



1. Access into web user interface of Vigor2925series. Open **Load-Balance/Route Policy**.



2. From the following web page, simply click index number #1.

Load Balance/Route Policy

Policy Route Set to Factory Default

Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input type="checkbox"/>	any	WAN1	---								Down
2	<input checked="" type="checkbox"/>	IP	WAN1	---							UP	Down
3	<input type="checkbox"/>	any	WAN1	---							UP	Down
4	<input checked="" type="checkbox"/>	IP	WAN1	---							UP	Down
5	<input type="checkbox"/>	any	WAN1	---							UP	Down
6	<input checked="" type="checkbox"/>	IP	WAN1	---							UP	Down
7	<input type="checkbox"/>	any	WAN1	---							UP	Down
8	<input checked="" type="checkbox"/>	IP	any	---							UP	Down
9	<input type="checkbox"/>	any	WAN1	---							UP	Down
10	<input checked="" type="checkbox"/>	IP	any	---							UP	Down

[1:10](#) | [11:20](#) | [21:30](#) | [31:40](#) | [41:50](#) >>
 [Next](#) >>

- In the following page, check **Enable**; set Dest IP Start and Dest IP End with 203.65.1.35 and 203.65.1.35; choose WAN1 as the **Interface**; click **default gateway**; do not check **Auto Failover To The Other WAN**.

Load Balance/Route Policy

---

Index: 1

**Enable**

---

Protocol:  any  ip

Interface:  WAN1  WAN2

Dest IP Start:  ..

Dest IP End:  default gateway  specific gateway

Dest IP Start: 203.65.1.35 .. 203.65.1.35

Dest IP End:  any  default gateway

---

send to all criteria matched

Interface:  WAN1  WAN2

Interface Address:

Gateway IP:  default gateway  specific gateway

---

more options

Auto Failover To The Other WAN

Fixed NAT  Fixed Routing

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

Load Balance/Route Policy

PolicyRoute [Set to Factory Default](#)

Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Mode Up	Mode Down
1	<input checked="" type="checkbox"/>	any	WAN1	203.65.1.35	Any	Any	203.65.1.35	203.65.1.35	Any	Any	UP	DOWN
2	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
3	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
4	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
5	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
6	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
7	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
8	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
9	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN
10	<input type="checkbox"/>	any	WAN1	--	--	--	--	--	--	--	UP	DOWN

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >>

Reset >>

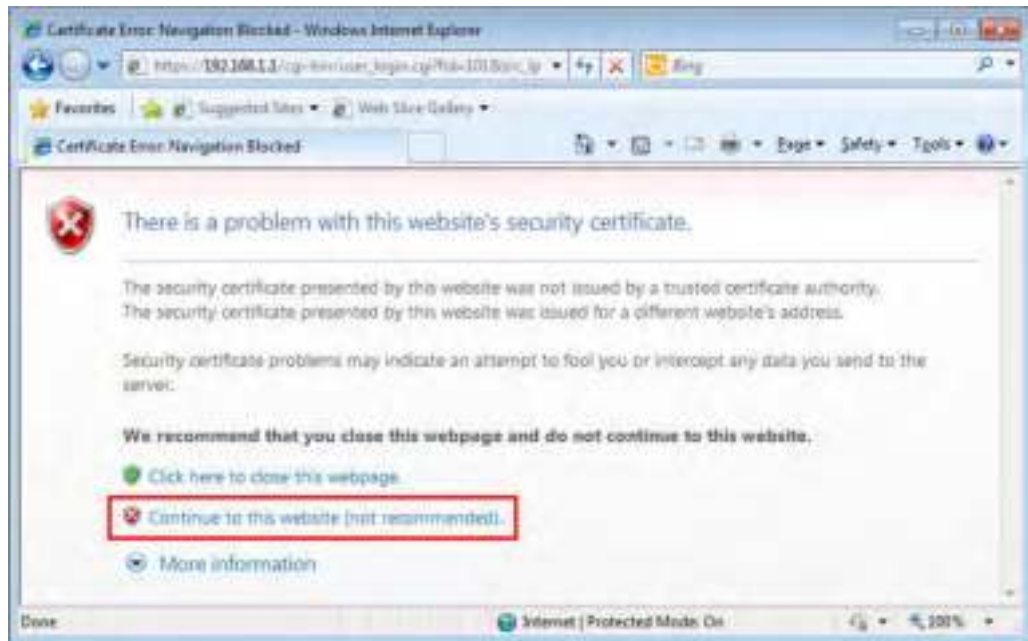
Now, the packets sent to the remote PC (IP address: 203.65.1.35) will be forcefully to pass through WAN1.



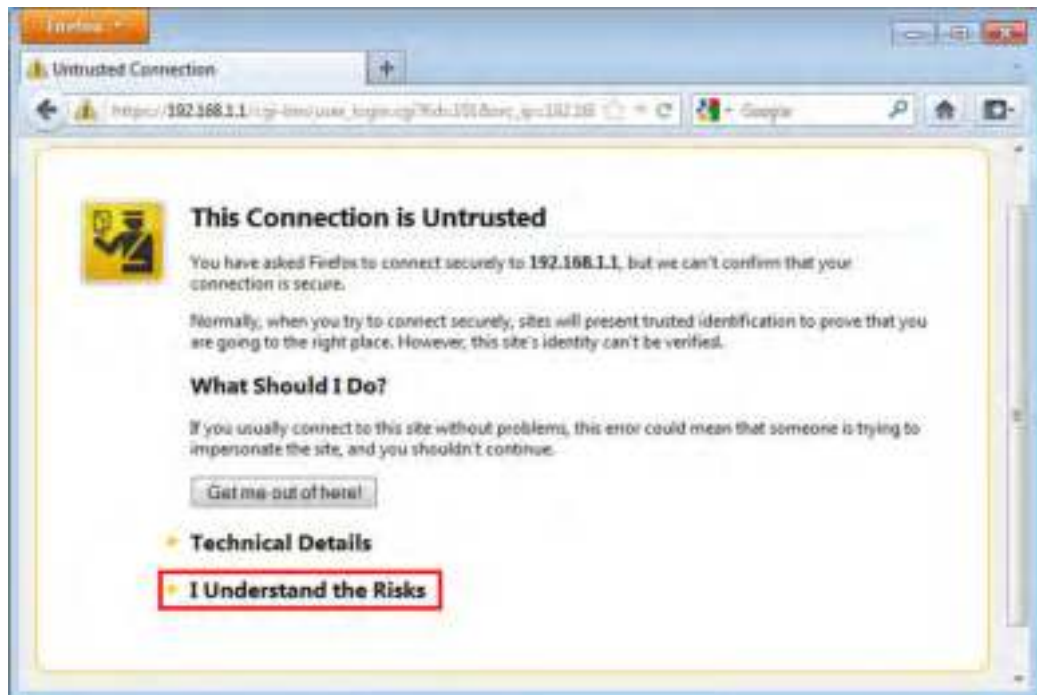


## Authentication via Web

- If a LAN client who hasn't passed the authentication opens an external web site in his browser, he will be redirected to the router's Web authentication interface first. Then, the client is trying to access <http://www.draytek.com> and but brought to the Vigor router. Since this is an SSL connection, some web browsers will display warning messages.
  - With Microsoft Internet Explorer, you may get the following warning message. Please press **Continue to this website (not recommended)**.



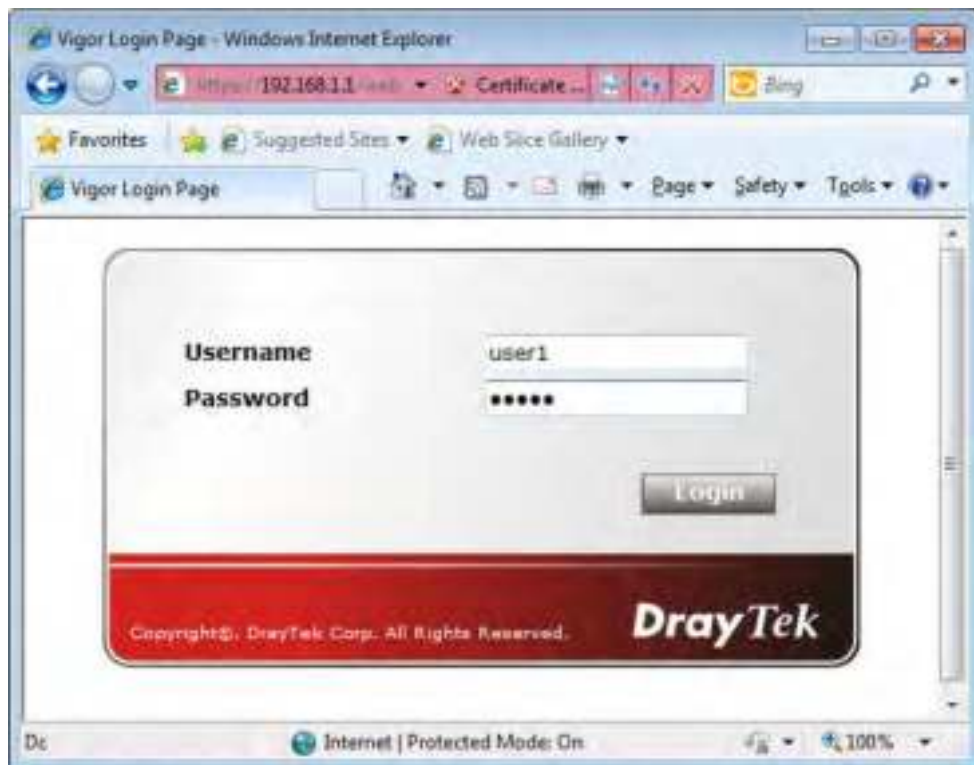
- With Mozilla Firefox, you may get the following warning message. Select **I Understand the Risks**.



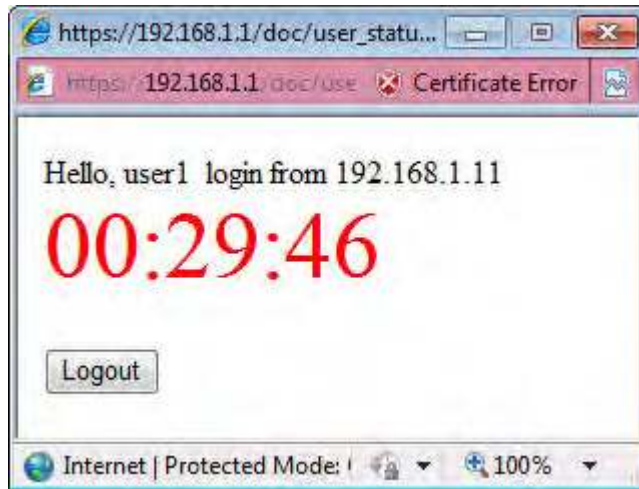
- With Chrome browser, you may get the following warning. Click **Proceed anyway**.



After that, the web authentication window will appear. Input the user name and the password for your account (defined in **User Management**) and click **Login**.



If the authentication is successful, the client will be redirected to the original web site that he tried to access. In this example, it is <http://www.draytek.com> . Furthermore, you will get a popped up window as the following. Then you can access the Internet.



Note, if you block the web browser to pop up any window, you will not see such window.

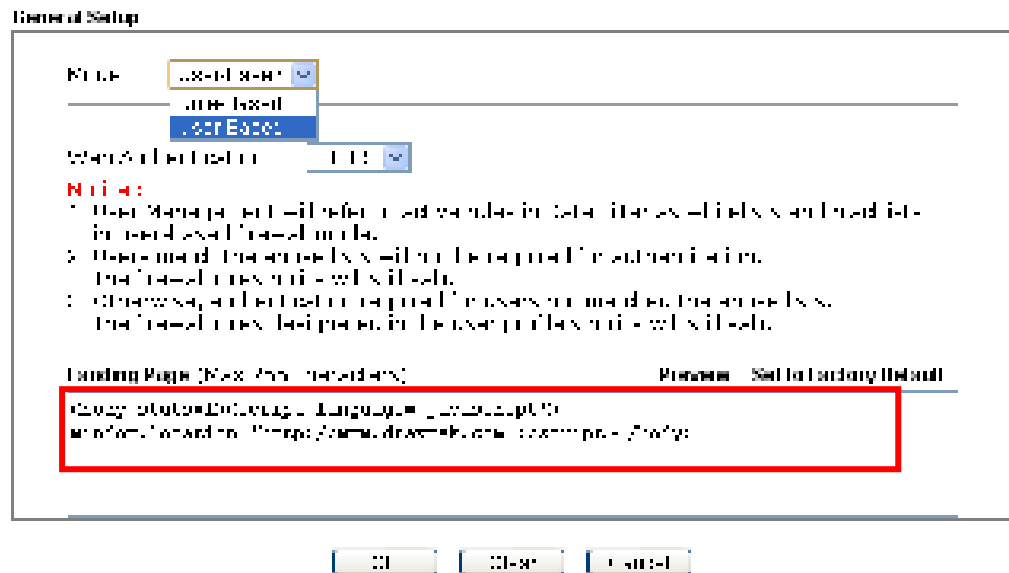
If the authentication is failed, you will get the error message, **The username or password you entered is incorrect.** Please login again.



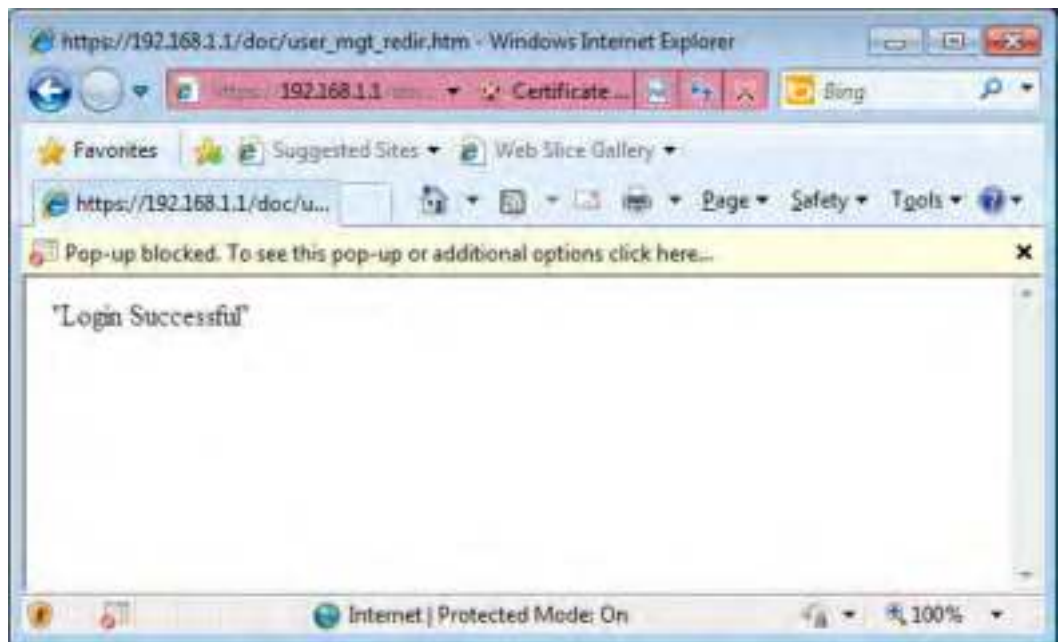
- In above description, you access an external web site to trigger the authentication. You may also directly access the router's Web UI for authentication. Both HTTP and HTTPS are supported, for example <http://192.168.1.1> or <https://192.168.1.1>. Replace 192.168.1.1 with your router's real IP address, and add the port number if the default management port has been modified.

If the authentication is successful, you will get the **Welcome Message** that is set in the **User Management >> General Setup** page.

User Management >> General Setup



With the default setup `<body status=1><script language='javascript'>window.location='http://www.draytek.com'</script></body>`, you will be redirected to <http://www.draytek.com>. You may change it if you want. For example, you will get the following welcome message if you enter **Login Successful** in the **Welcome Message** table.



Also you will get a **Tracking Window** if you don't block the pop-up window.

- Don't setup a user profile in **User Management** and a VPN Remote Dial-in user profile with the same Username. Otherwise, you may get unexpected result. It is because the VPN Remote Dial-in User profiles can be extended to the User profiles in User Management for authentication.

There are two different behaviors when a User Management account and a VPN profile share the same Username:

- If **SSL Tunnel** or **SSL Web Proxy** is enabled in the VPN profile, the user profile in User Management will always be invalid for Web authentication. For example, if you create a user profile in User Management with **chaochen/test** as username/password, while a VPN Remote Dial-in user profile with the same username "chaochen" but a different password "1234", you will always get error message **The username or password you entered is incorrect** when you use **chaochen/test** via Web to do authentication.

VPN and Remote Access >> Remote DialIn User

The screenshot shows the configuration page for a Remote Dial-In User. The 'Allowed Dial-In Type' section contains several options: 'SSL Tunnel' is checked and highlighted with a red rectangular box. Other options include 'SSL Web Proxy' and 'IPsec Tunnel'. The 'User account and Authentication' section shows 'chaochen' as the username and 'test' as the password. The 'IKE Authentication Method' section has 'Pre-Shared Key' selected. The 'Peer Security Method' section has 'IPsec' selected. At the bottom of the form, there are 'OK', 'Gett', and 'Cancel' buttons.

- If **SSL Tunnel** or **SSL Web Proxy** is disabled in the VPN profile, a User Management account and a remote dial-in VPN profile can use the same Username, even with different passwords. However, we recommend you to use different usernames for different user profiles in User Management and VPN profiles.

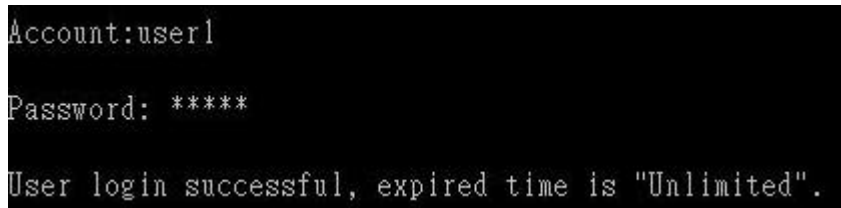
## Authentication via Telnet

The LAN clients can also authenticate their accounts via telnet.

1. Telnet to the router's LAN IP address and input the account name for the authentication:

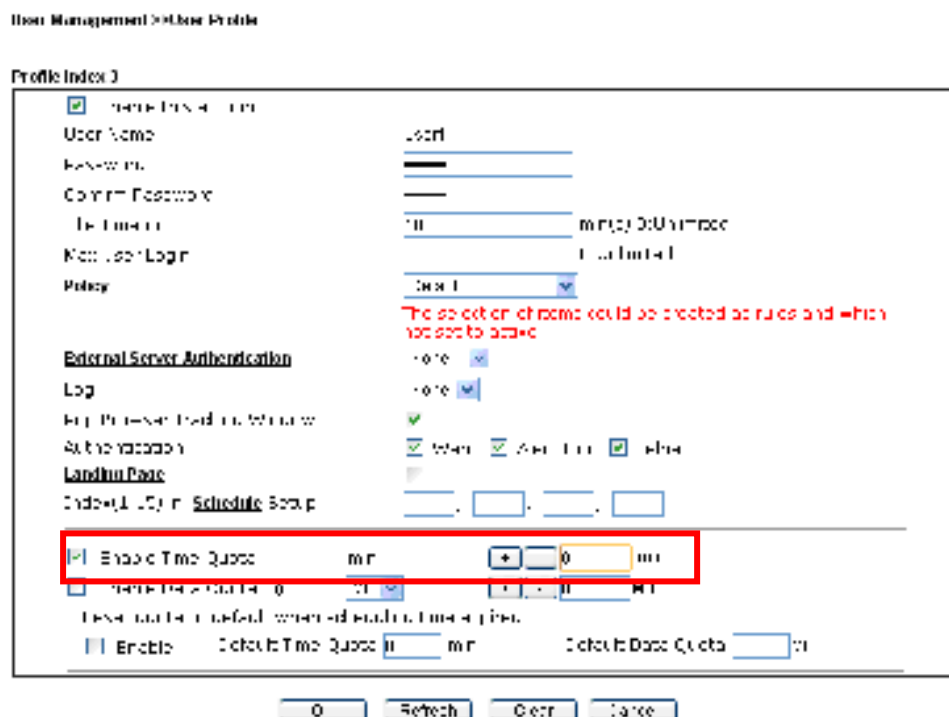


2. Type the password for authentication and press **Enter**. The message **User login successful** will be displayed with the expired time (if configured).



**Note:** Here **expired time** is “Unlimited” means the **Time Quota** function is not enabled for this account. After login, this account will not be expired until it is logout.

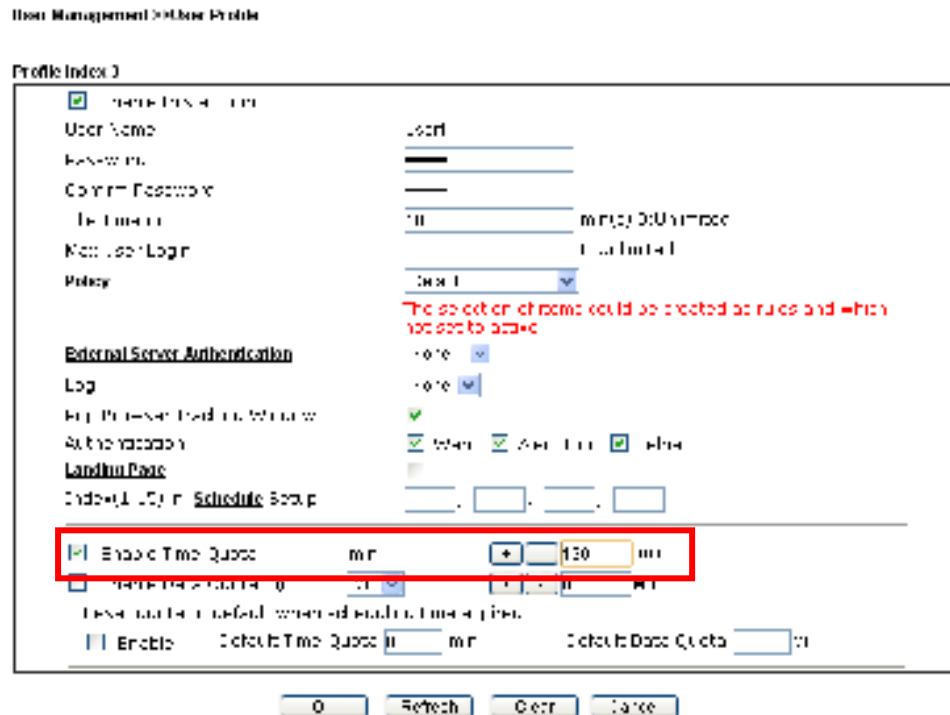
3. In the Web interface of router, the configuration page of **Time Quota** is shown as below.



- If the Time Quota is set with "0" minute, you will get the following message which means this account has no time quota.

```
Account:user1
Password: *****
User's time is up, or it has not enough time quota.
```

If the **Time Quota** is enabled and time is not 0 minute,



You will get the following message. The expired time is shown after you login.

```
Account:user1
Password: *****
User login successful, expired time is "12-23 10:21:33".
```

After you run out the available time, you can't use this account any more until the administrator manually adds additional time for you.



## Authentication via VigorPro Alert Notice Tool

Authentication via Web or Telnet is convenient for users; however, it has some limitations. The most advantage with VigorPro Alert Notice Tool to operate the authentication is the ability to do **auto login**. If the timeout value set on the router for the user account has been reached, the router will stop the client computer from accessing the Internet until it does an authentication again. Authentication via VigorPro Alert Notice Tool allows user to setup the re-authentication interval so that the utility will send authentication requests periodically. This will keep the client hosts from having to manually authenticate again and again.

The configuration of the VigorPro Alert Notice Tool is as follows:

1. Click **Authenticate Now!!** to start the authentication immediately.



2. You may get the **VigorPro Alert Notice Tool** from the following link:  
<http://www.draytek.com/user/SupportDLUtility.php>

### Note:

- Any modification to the Firewall policy will break down the connections of all current users. They all have to authenticate again for Internet access.
- The administrator may check the current users from **User Online Status** page.





### 3.15 How to use DNS Filter

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF (web content filter) to help with categorizing HTTPS URL's.

**Note:** For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.

In the following example, we will block search engine (e.g., www.google.com) and social networking website (e.g., https://facebook.com).

1. Open **CSM>>Web Content Filter Profile** to set the categories. Make sure **WCF License** has already been activated.

CSM >> Web Content Filter Profile i

Web-Filter License [Activate](#)  
 , Status: **COMMITTED** , Start Date: **2013-10-28** , End Date: **2013-11-28**

Setup Query Server  [Find more](#)

Setup Test Server  [Find more](#)

[Check URL Category or report incorrect classification](#)

Web Content Filter Profile Table: [Set to Factory Default](#)

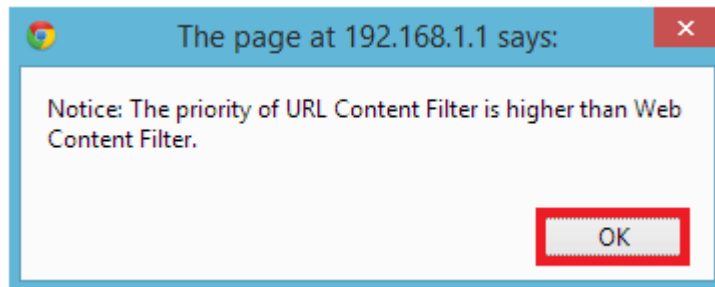
Profile	Name	Profile	Name
1	Default	1	
2		2	
3		3	

2. Click Index 1 link to open the following page. Disable all of the categories first. Then, enable **Search Engine, Portals**, and **Social Networking**.

Action: **Lock** ▼

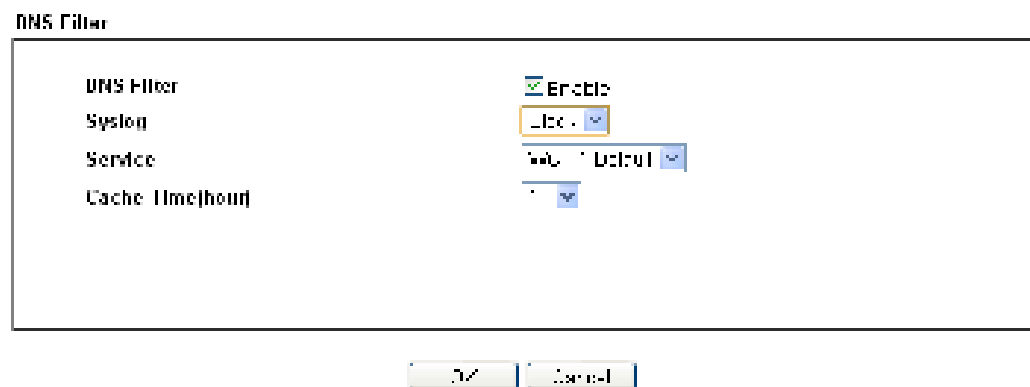
Groups	Categories		
<p><b>Child Protection</b></p> <p><input type="button" value="Select All"/></p> <p><input type="button" value="Clear All"/></p>	<p><input type="checkbox"/> Adult &amp; Mature</p> <p><input type="checkbox"/> Hate &amp; Intolerance</p> <p><input type="checkbox"/> Porn &amp; Sexuality</p> <p><input type="checkbox"/> School Cheating</p> <p><input type="checkbox"/> Child Labor &amp; Images</p>	<p><input type="checkbox"/> Criminal Activity</p> <p><input type="checkbox"/> Illegal Drug</p> <p><input type="checkbox"/> Violence</p> <p><input type="checkbox"/> Bio Education</p>	<p><input type="checkbox"/> Gambling</p> <p><input type="checkbox"/> Nudity</p> <p><input type="checkbox"/> Weapons</p> <p><input type="checkbox"/> Tobacco</p>
<p><b>Media</b></p> <p><input type="button" value="Selected"/></p> <p><input type="button" value="Clear All"/></p>	<p><input type="checkbox"/> Entertainment</p> <p><input type="checkbox"/> Travel</p>	<p><input type="checkbox"/> Games</p> <p><input type="checkbox"/> Leisure &amp; Recreation</p>	<p><input type="checkbox"/> Sports</p> <p><input type="checkbox"/> Fashion &amp; Beauty</p>
<p><b>Business</b></p> <p><input type="button" value="Selected"/></p> <p><input type="button" value="Clear All"/></p>	<p><input type="checkbox"/> Business</p>	<p><input type="checkbox"/> Job Search</p>	<p><input type="checkbox"/> Web-Based Mail</p>
<p><b>Chatting</b></p> <p><input type="button" value="Selected"/></p> <p><input type="button" value="Clear All"/></p>	<p><input type="checkbox"/> Chat</p>	<p><input type="checkbox"/> Instant Message</p>	
<p><b>Computer Related</b></p> <p><input type="button" value="Selected"/></p> <p><input type="button" value="Clear All"/></p>	<p><input type="checkbox"/> Applications</p> <p><input type="checkbox"/> Download Files</p> <p style="border: 2px solid red;"><input checked="" type="checkbox"/> Search Engine, Portals</p> <p><input type="checkbox"/> Malware</p> <p><input type="checkbox"/> Spam Software</p>	<p><input type="checkbox"/> Forums &amp; Newsboards</p> <p><input type="checkbox"/> Learning Resources</p> <p style="border: 2px solid red;"><input checked="" type="checkbox"/> Social Networking</p> <p><input type="checkbox"/> Virtual</p> <p><input type="checkbox"/> Download Software</p>	<p><input type="checkbox"/> Computers</p> <p><input type="checkbox"/> Hidden IP Address</p> <p><input type="checkbox"/> Spam Sites</p> <p><input type="checkbox"/> Hacking</p> <p><input type="checkbox"/> Programs/Tools</p>

- Click **OK** to save the configuration.
- A message box will appear. It's a message which reminds that the priority of URL Content Filter is higher than Web Content Filter. Just press **OK** button to continue.



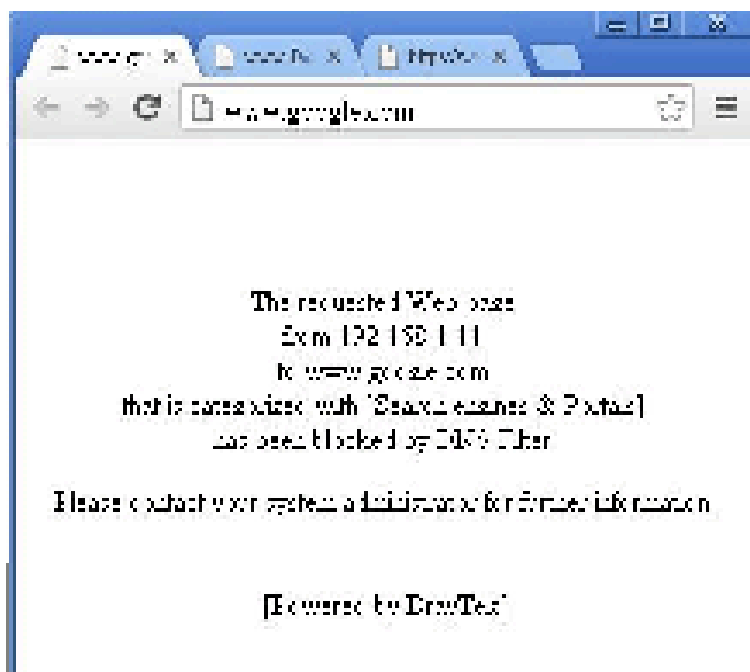
- Open **CSM>>DNS Filter**. Enable the DNS filter; choose **Block** as the Syslog; choose **WCF-1 Default**.

CSM >> DNS Filter

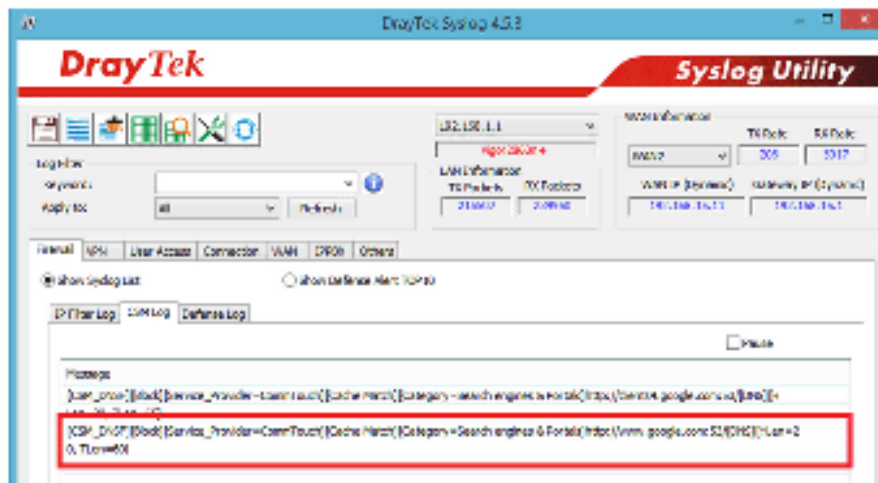


- Click **OK** to save the DNS filter configuration.

Now, all settings about blocking search engine and social website are complete. Please try to access into [www.google.com](http://www.google.com) (the search engine) to see the result.



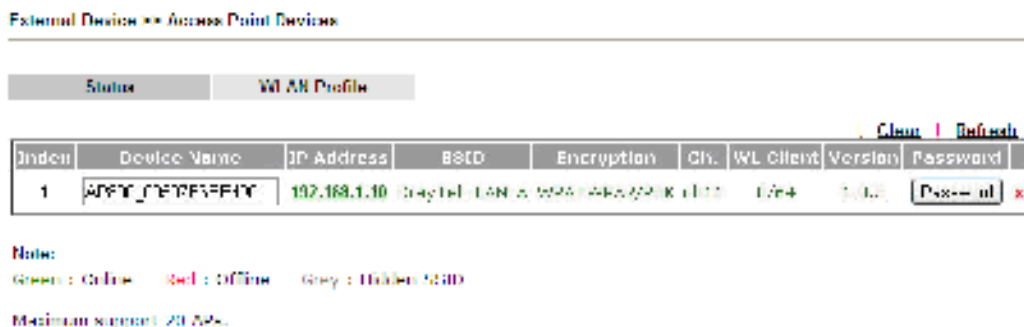
From the Syslog, we can find out “google” is blocked.



### 3.16 How to use AP Management function (in Vigor2925) to check AP status and deploy WLAN profile

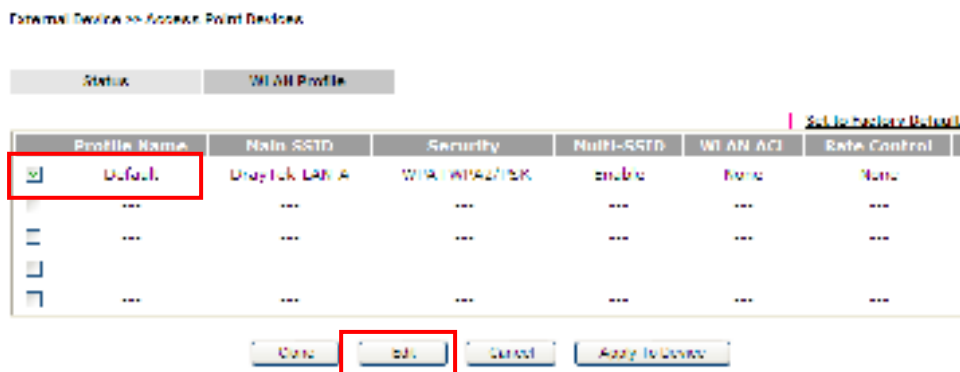
The administrator can manage the access points linked to Vigor2925.

1. Open **External Devices>>Access Point Devices**. Vigor2925 will detect the AP connecting to the router automatically and display as below:

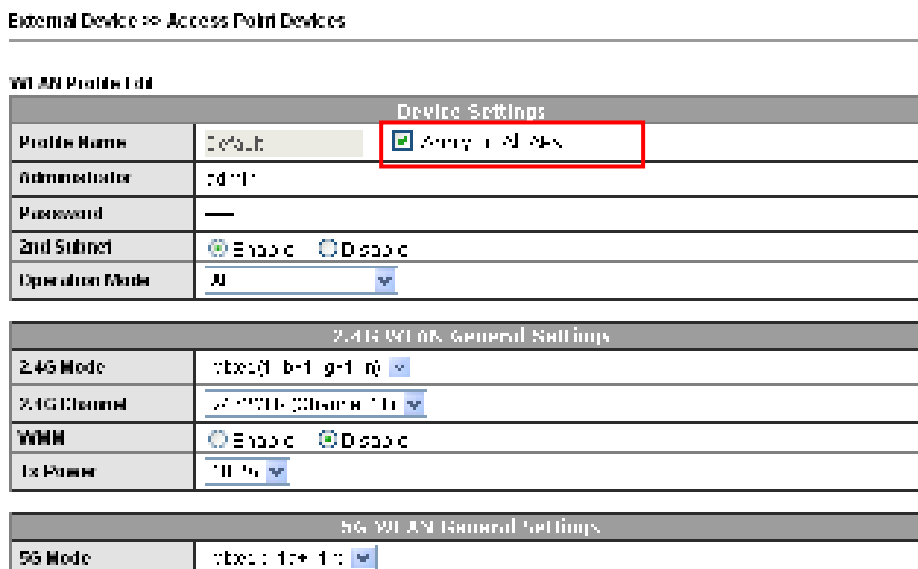


In this case, a device named with AP800\_00507F6EE4980 has been detected by Vigor router.

2. Click the **WLAN Profile** tab to get the following page. Check the box of the default profile to make the **Edit** button being available. Then, click the **Edit** button.



3. When the following configuration page appears, make the changes you want and check **Apply to All APs**. Then, click **Next** to access into the next page.



**Note: Apply to All APs** can automatically apply the settings on **Default** profile to all of the access points registered to Vigor2925 later. Hence, it is not necessary for you to manually apply wireless profiles for APs respectively. Such feature will be convenient for people who want to *quickly deploy* multiple Vigor APs in a large exhibition to reach the goal of “plug and play” and “zero-configuration”.

- The following page allows you to modify related settings for 2.4G SSID of managed AP. Make the changes you want for 2.4G SSID. Click **Next** for next page.

External Network > Access Point Network

SSID1	SSID2	SSID3	SSID4
2.4G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek LAN 2 <input type="text" value="LAN2"/> <input type="checkbox"/> Filter SSID		
WLAN	2 <input type="text" value="2.4G LAN2"/>		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	WPA-PSK (TKIP)		
	Set up RADIUS Server (RADIUS is enabled).		
	WPA Authentication	<input type="radio"/> KIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP	
	Pass Phrase	<input type="text" value=""/>	
	Key Renewal Interval	3600	Minutes
	PMK Cache Period	0	Minutes
Pre-Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
WEP	Set up WEP Key if WPA is not selected.		
	WEP Key 1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None <input type="checkbox"/>		
List	Clients MAC Address: <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>		
	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
	Bandwidth Limit		
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		Auto Adjustment <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	<input type="text" value=""/> Mbps		Download <input type="text" value=""/> Mbps
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Next"/>			

- The following page is offered for you to modify related settings for 5G SSID of managed AP. Continue to make any changes you want. After finished all of the changes, simply click **Finish**.

External Network > Access Point Network

5G SSID			
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SSID	DrayTek 5G	LANA	<input type="checkbox"/> Hide SSID
WLAN	2		
Isolate	<input type="checkbox"/> From Member		
Security Settings			
Encryption	Security: <input type="text" value="WPA2-PSK"/>		
	Set up <b>RADIUS Server</b> if RADIUS is enabled.		
	WPA2 Authentication	<input type="radio"/> KIP <input type="radio"/> TKIP <input checked="" type="radio"/> AES-CCMP	
	Pass Phrase	<input type="text" value=""/>	
	Key Renewal Interval	3600	seconds
	PMK Cache Period	0	minutes
Pre Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
WEP	Set up WEP Key if WEP is enabled.		
	Key 1 to WEP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Access Control			
Mode	None		
List	<input type="text" value=""/>		
	<input type="text" value=""/>		
	Client's MAC Address : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>		
	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>		
Bandwidth Limit			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Auto Adjustment	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload	<input type="text" value=""/> Mbps	Download	<input type="text" value=""/> Mbps
<input type="button" value="Back"/> <input type="button" value="Cancel"/> <input type="button" value="Finish"/>			

Now, the AP (represented with *AP800\_00507F6EE4980*) detected by Vigor router will be applied with the settings modified by Vigor router.

This page is left blank.



# 4

## Advanced Configuration

This chapter will guide users to execute advanced (full) configuration through admin mode operation.

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. Be aware that “Admin mode” will be displayed on the bottom left side.

The screenshot displays the DrayTek Vigor2925 Series web management interface. The top navigation bar includes the DrayTek logo and the product name 'Vigor2925 Series'. A left-hand navigation menu lists various configuration options such as Dashboard, Quick Start Wizard, Service Activation Wizard, Wireless Wizard, Online Status, WAN, LAN, Load-Balance/Route Policy, NAT, Hardware Acceleration, Firewall, User Management, Object Setting, CSN, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, Wireless LAN, SSL VPN, LAN Application, System Maintenance, Diagnostics, and External Devices. The main content area is titled 'Dashboard' and features a central status bar with 'DrayTek Vigor2925n' and 'Dual WAN Broad Router'. Below this, there are several data tables:

System Information			
Model Name	Vigor2925n	System Up Time	0:0:41
Router Name		Current Time	2011-01-14 10:14
Firmware Version	3.7.3	Build Date/Time	2010-09-03 10:00:43
LAN MAC Address	DD-DD-AA-AA-DD-DD		

IPv4 Internet Access				
Line/Mode	IP Address	MAC Address	Up Time	
WAN1/Ethernet/7	192.168.1.1	11-11-11-11-11-11	11:11:11	
WAN2/Ethernet/7	192.168.1.1	CC-DD-AA-AA-DD-DD	00:00:00	
WAN3/Ethernet/7	192.168.1.1	11-11-11-11-11-11	11:11:11	

IPv6 Internet Access				
Line	Mode	Address	Scope	Up Time
LAN	Ethernet/7	FE80::1	Link	

Interface	
WAN	Connector C, LAN1, WAN2, WAN3
LAN	Connector C, LAN1, LAN2, LAN3, LAN4, LAN5
WLAN	Connector C
USB	Connector C, USB

On the right side of the dashboard, there is a 'Quick Access' menu with links to System Status, Dynamic DNS, User Management, WAP/WiFi, Schedule, System Log/Event, LDAP, Profiles, Firewall Object Setting, and Help/How Member.

### 4.1 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.

#### 4.1.1 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, Vigor2925 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2925, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2925n 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 Vigor2925n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2925n 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](http://www.draytek.com) for more detailed information.

Below shows the menu items for WAN.



### 4.1.2 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:

Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Online Mode
WAN1	<input checked="" type="checkbox"/>	Line Speed/DSL	1/1	Always On
WAN2	<input checked="" type="checkbox"/>	Line Speed/DSL	1/1	Always On
WAN3	<input checked="" type="checkbox"/>	DSL	1/1	Always On

Note: The line speed setting of WAN interface is available only when you click the link that is selected as the Load Balance Mode.



Available settings are explained as follows:

Item	Description
<b>Load Balance Mode</b>	<p>This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of <b>According to Line Speed</b>. Otherwise, please choose <b>Auto Weigh</b> to let the router reach the best load balance.</p> <p>Load Balance Mode: <input type="text" value="Auto Weight"/></p>
<b>Index</b>	Click the WAN interface link under Index to access into the WAN configuration page.

<b>Enable</b>	V means such WAN interface is enabled and ready to be used.
<b>Physical Mode / Type</b>	Display the physical mode and physical type of such WAN interface.
<b>Line Speed</b>	Display the downstream and upstream rate of such WAN interface.
<b>Active Mode</b>	Display whether such WAN interface is Active device or backup device.

**Note:** In default, each WAN port is enabled.

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

## WAN1/WAN2 with Ethernet

WAN1/WAN2 is fixed with physical mode of Ethernet.

WAN >>> General Setup

WAN 1


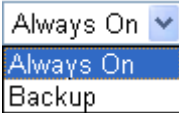
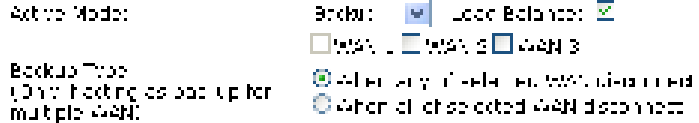
Enable:	Yes
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Line Speed(Kbps):	
Downlink	0
Uplink	0
VLAN Tag Insertion :	Disable (Please configure Internet Access setting first)
Tag value:	0 (0-4095)
Priority:	0 (0-7)
Active Mode:	Backup Load Balance: <input type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> WAN 3
Backup Type (only if setting as backup for multiple WAN):	<input checked="" type="radio"/> When any of selected WAN disconnect <input type="radio"/> When all of selected WAN disconnect

Note : 1.The Line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
<b>Display Name</b>	Type the description for such WAN interface.
<b>Physical Mode</b>	Display the physical mode of such WAN interface.
<b>Physical Type</b>	You can change the physical type for WAN2 or choose <b>Auto negotiation</b> for determined by the system.

	
<b>Line Speed</b>	<p>If you choose <b>According to Line Speed</b> as the <b>Load Balance Mode</b>, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.</p>
<b>VLAN Tag insertion</b>	<p><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.</p> <p><b>Disable</b> – Disable the function of VLAN with tag.</p> <p><b>Tag value</b> – Type the value as the VLAN ID number. The range is from 0 to 4095.</p> <p><b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
<b>Active Mode</b>	<p>Choose <b>Always On</b> to make the WAN2 connection being activated always.</p> 
<b>Backup Type</b>	<p>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.</p>  <p><b>When any of selected WAN disconnect</b> – Such backup WAN will be activated when any master WAN interface disconnects.</p> <p><b>When all of selected WAN disconnect</b> – Such backup WAN will be activated only when all master WAN interfaces disconnect.</p> <p><b>Load Balance:</b> Check this box to enable <b>auto</b> load balance function for such WAN interface.</p> <p>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.</p>

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

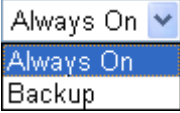
### WAN3

Enable:	Yes
Display Name:	
Physical Mode:	USB
Line Speed(Kbps):	
DownLink:	0
UpLink:	0
Active Mode:	Backup <input checked="" type="checkbox"/> Load Balance: <input checked="" type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3
Backup Type (Only if acting as backup for multiple WAN):	<input type="radio"/> When any of selected WAN disconnect <input checked="" type="radio"/> When all of selected WAN disconnect

Note: 1. The line speed setting of WAN interface is available only when According to Line Speed is selected as the Load Balance Mode.

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
<b>Display Name</b>	Type the description for such WAN interface.
<b>Physical Mode</b>	Display the physical mode of such WAN interface.
<b>Line Speed</b>	If you choose <b>According to Line Speed</b> as the <b>Load Balance Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
<b>Active Mode</b>	Choose <b>Always On</b> to make the WAN3 connection being activated always. 
<b>Backup Type</b>	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: <input checked="" type="checkbox"/> Backup <input checked="" type="checkbox"/> Load Balance: <input checked="" type="checkbox"/> <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 Backup Type (Only if acting as backup for multiple WAN): <input checked="" type="radio"/> When any of selected WAN disconnect <input type="radio"/> When all of selected WAN disconnect <b>When any of selected WAN disconnect</b> – Such backup WAN will be activated when any master WAN interface disconnects. <b>When all of selected WAN disconnect</b> – Such backup WAN will be activated only when all master WAN interfaces disconnect.

	<p><b>Load Balance:</b> Check this box to enable <b>auto</b> load balance function for such WAN interface.</p> <p>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.</p>
--	--

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

### 4.1.3 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

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static/Dynamic IP	Details Page IPv6
WAN2		Ethernet	None PPTP	Details Page IPv6
WAN3		USB	Static/Dynamic IP PPTP/STP	Details Page IPv6

Note : Only one WAN can support IPv6.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static/Dynamic IP	Details Page IPv6
WAN2		Ethernet	None	Details Page IPv6
WAN3		USB	None	Details Page IPv6

Note : Only one WAN can support IPv6.

Available settings are explained as follows:

Item	Description
<b>Index</b>	Display the WAN interface.
<b>Display Name</b>	It shows the name of the WAN1/WAN2/WAN3 that entered in general setup.
<b>Physical Mode</b>	It shows the physical connection for WAN1/WAN2 (Ethernet) /WAN3 (USB) according to the real network connection.
<b>Access Mode</b>	Use the drop down list to choose a proper access mode. Then, click <b>Details Page</b> for accessing the settings page to configure the settings.

<b>Details Page</b>	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/VDSL physical mode specified on <b>WAN&gt;&gt;General Setup</b> .
<b>IPv6</b>	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/WAN2

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

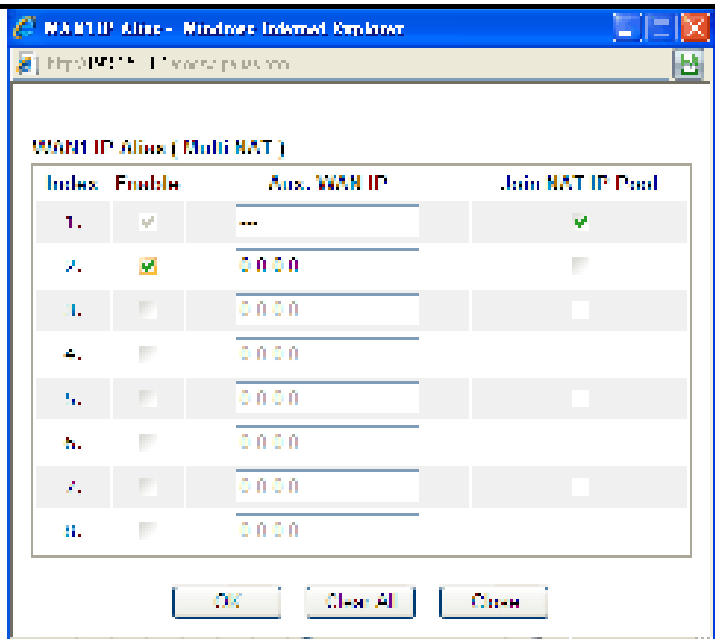
WAN >> Internet Access

Available settings are explained as follows:

Item	Description
<b>Enable/Disable</b>	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.
<b>ISP Access Setup</b>	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.



	<p><b>Password</b> – Type in the password provided by ISP in this field.</p> <p>The maximum length of the password you can set is 62 characters.</p> <p><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 &gt;&gt; Schedule</b> web page and you can use the number that you have set in that web page.</p>
<b>WAN Connection Detection</b>	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p><b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.</p> <p><b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p><b>TTL (Time to Live)</b> – Displays value for your reference. TTL value is set by telnet command.</p>
<b>MTU</b>	<p>It means Max Transmit Unit for packet. The default setting is 1442.</p>
<b>PPP/MP Setup</b>	<p><b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.</p> <p><b>Idle Timeout</b> – Set the timeout for breaking down the Internet after passing through the time without any action.</p>
<b>IP Address Assignment Method (IPCP)</b>	<p>Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.</p> <p><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. Type the additional WAN IP address and check the Enable box. Then click <b>OK</b> to exit the dialog.</p>



**Fixed IP** – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.

**Default MAC Address** – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.

**Specify a MAC Address** – Type the MAC address for the router manually.

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

### Details Page for Static or Dynamic IP in WAN1/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.

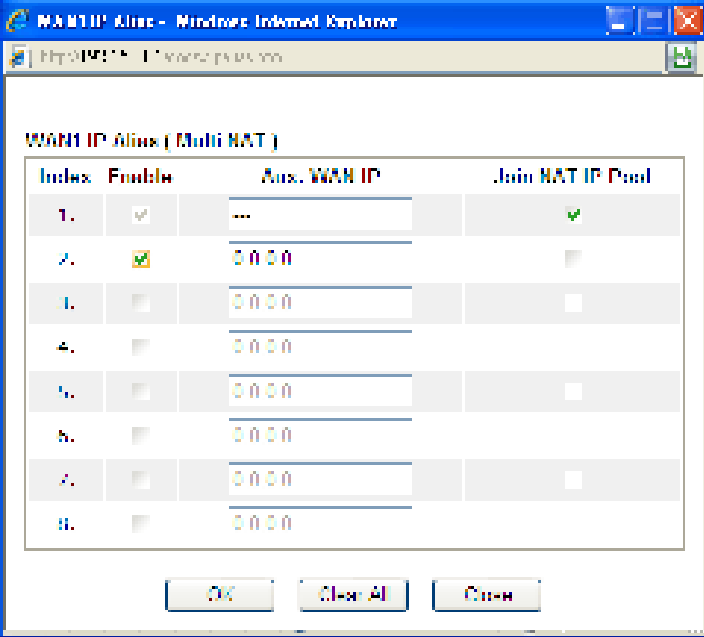
WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Disable <input checked="" type="radio"/> Enable	<p>Keep WAN Connection</p> <input type="checkbox"/> Enable PING to keep alive PING to the IP: _____ PING Interval: 0 (Min:10, Max:60)	<p>WAN IP Networks Settings: [Static / Dynamic]</p> <input type="radio"/> Obtain an IP address automatically Client Name: _____ Server Name: _____ <small>: Required for some ISPs</small> DHCP Client Identifier for some ISP: _____	
	<p>WAN Connection Detection</p> Mode: [ARP Detect]	<input type="checkbox"/> Enable Username: _____ Password: _____	
	Ping IP: _____ TTL: _____	<input checked="" type="radio"/> Specify an IP address IP Address: _____ Subnet Mask: _____ Gateway IP Address: _____	
<p>MTU</p> 1492 (Max:1500)		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: [00] [10] [80] [00] [00] [00]	
<p>PPP Protocol</p> <input type="checkbox"/> Enable PPP		DNS Server IP Address: _____ Primary DNS Address: _____ Secondary IP Address: 1.1	

Available settings are explained as follows:

Item	Description
<b>Enable / Disable</b>	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.
<b>Keep WAN Connection</b>	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. <b>PING Interval</b> - Enter the interval for the system to execute the PING operation.
<b>WAN Connection Detection</b>	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.
<b>MTU</b>	It means Max Transmit Unit for packet. The default setting

	is 1492.
<b>RIP Protocol</b>	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.
<b>WAN IP Network Settings</b>	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p><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.</p>  <p><b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically if you want to use <b>Dynamic IP</b> mode.</p> <ul style="list-style-type: none"> <li>● <b>Router Name:</b> Type in the router name provided by ISP.</li> <li>● <b>Domain Name:</b> Type in the domain name that you have assigned.</li> </ul> <p><b>DHCP Client Identifier for some ISP</b></p> <ul style="list-style-type: none"> <li>● <b>Enable:</b> Check the box to specify username and password as the DHCP client identifier for some ISP.</li> <li>● <b>Username:</b> Type a name as username. The maximum length of the user name you can set is 63 characters.</li> <li>● <b>Password:</b> Type a password. The maximum length of the password you can set is 62 characters.</li> </ul> <p><b>Specify an IP address</b> – Click this radio button to specify some data if you want to use <b>Static IP</b> mode.</p> <ul style="list-style-type: none"> <li>● <b>IP Address:</b> Type the IP address.</li> </ul>

	<ul style="list-style-type: none"> <li>● <b>Subnet Mask:</b> Type the subnet mask.</li> <li>● <b>Gateway IP Address:</b> Type the gateway IP address.</li> </ul> <p><b>Default MAC Address:</b> Click this radio button to use default MAC address for the router.</p> <p><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.</p>
<b>DNS Server IP Address</b>	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 WAN1/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.

WAN1 >> Internet Access

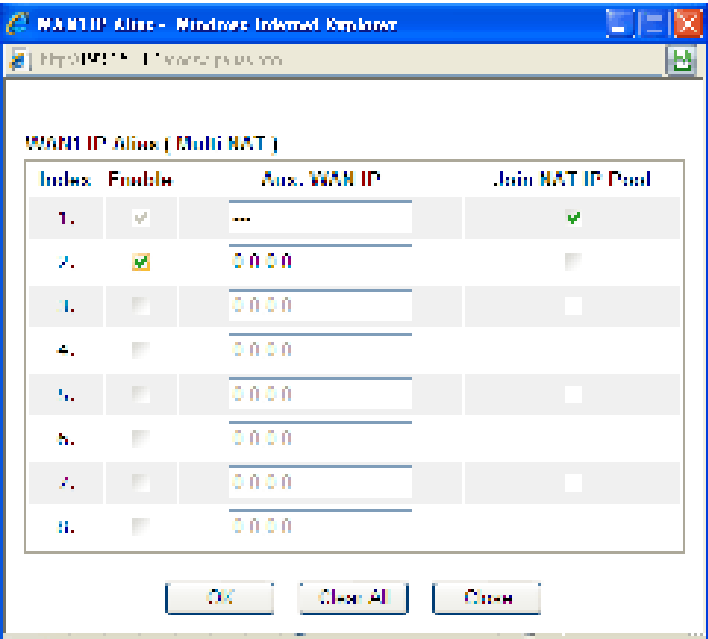
WAN1

PPTP	Static or Dynamic IP	PPTP/L2TP	IPv6
<input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable		<b>PPTP Setup</b> PPTP Authentication: [PPTP CHAP]	
Server Address: [ ] Specify Gateway IP Address: [ ]		PPTP Timeout: [ ] [ ]	
<b>PPP Access Setup</b> Username: [ ] Password: [ ]		<b>IP Address Assignment Method (PPTP)</b> <input checked="" type="radio"/> WAN1 Access	
<b>Advanced L2TP or Scheduling Setup</b> [ ] [ ] [ ] [ ]		Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Specify IP)	
<b>MTU</b> [ ] (Max: 1500)		<b>Fixed IP Address</b> <b>WAN IP Network Settings</b> <input checked="" type="radio"/> Obtain IP Address automatically <input type="radio"/> Specify IP address	
		IP Address: [ ] Subnet Mask: [ ]	

Available settings are explained as follows:

Item	Description
<b>PPTP/L2TP</b>	<p><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.</p> <p><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.</p> <p><b>Disable</b> – Click this radio button to close the connection through PPTP or L2TP.</p> <p><b>Server Address</b> - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.</p> <p><b>Specify Gateway IP Address</b> – Specify the gateway IP</p>

	address for DHCP server.
<b>ISP Access Setup</b>	<p><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.</p> <p><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.</p> <p><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 &gt;&gt; Schedule</b> web page and you can use the number that you have set in that web page.</p>
<b>MTU</b>	It means Max Transmit Unit for packet. The default setting is 1492.
<b>PPP Setup</b>	<p><b>PPP Authentication</b> - Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.</p> <p><b>Idle Timeout</b> - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
<b>IP Address Assignment Method(IPCP)</b>	<p><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.</p>  <p><b>Fixed IP</b> - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click <b>Yes</b> to use this function and type in a fixed IP address in the box.</p> <p><b>Fixed IP Address</b> -Type a fixed IP address.</p>
<b>WAN IP Network Settings</b>	<b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically.

	<p><b>Specify an IP address</b> – Click this radio button to specify some data.</p> <ul style="list-style-type: none"> <li>● <b>IP Address</b> – Type the IP address.</li> <li>● <b>Subnet Mask</b> – Type the subnet mask.</li> </ul>
--	--

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 > Internet Access](#)

**WAN 3**

**3G/4G USB Modem(PPP mode)**       Enable    Disable

**SIM PIN code**     

**Modem Initial String**       (Default: AT&FECVIX1&0280190=0)

**APN Name**     

**Modem Initial String2**     

**Modem Dial String**       (Default: ATDT\*999, CDMA: ATDT\*777, TD-SCDMA: ATDT\*98\*1#)

**PPP Username**       (Optional)

**PPP Password**       (Optional)

**PPP Authentication**     

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

→

---

**WAN Connection Detection**

**Mode**     

**Ring IP**     

**MTU**

Available settings are explained as follows:

Item	Description
<b>3G /4G USB Modem (PPP mode)</b>	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.
<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.

<b>Modem Initial String</b>	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> . The maximum length of the name you can set is 43 characters.
<b>Modem Initial String2</b>	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.
<b>Modem Dial String</b>	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.
<b>PPP Username</b>	Type the PPP username (optional). The maximum length of the name you can set is 63 characters.
<b>PPP Password</b>	Type the PPP password (optional). The maximum length of the password you can set is 62 characters.
<b>PPP Authentication</b>	Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.
<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 &gt;&gt; Schedule</b> web page and you can use the number that you have set in that web page
<b>WAN Connection Detection</b>	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.

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 Access

WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type: <input type="text" value="Offline"/>			

## 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

WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type: <input type="text" value="PPP"/>			
Note : IPv6 WAN setting should be PPPoE client.			

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

## Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:BD10:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
7	4	690	328
<b>WAN2 IPv6 Status</b> >> <a href="#">Drop PPP</a>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	PPP	0:02:08	
<b>IP</b>		<b>Gateway IP</b>	
2001:BD10:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::98:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
<b>DNS IP</b>			
2001:8000:168::1			
2001:8000:168::2			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
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 (<http://gogonet.gogo6.com/page/freenet6-account>) 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.

[WAN](#) >> [Internet Access](#)

**WAN 1**

PPPoE	Static or Dynamic IP	PPTP	IPv6
<b>Internet Access Mode</b>			
<b>Connection Type</b>		TSPC	
<b>TSPC Configuration</b>			
<b>Username</b>	<input type="text"/>		
<b>Password</b>	<input type="text"/>		
<b>Confirm Password</b>	<input type="text"/>		
<b>Tunnel Broker</b>	<input type="text"/>		

Available settings are explained as follows:

Item	Description
<b>Username</b>	Type the name obtained from the broker. It is suggested for you to apply another username and password for <a href="http://gogonet.gogo6.com/page/freenet6-account">http://gogonet.gogo6.com/page/freenet6-account</a> . The maximum length of the name you can set is 63 characters.
<b>Password</b>	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.
<b>Tunnel Broker</b>	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
<b>Internet Access Mode</b>			
Connection Type		AICCU	
<b>AICCU Configuration</b>			
<input type="checkbox"/> Always On			
Username	_____		
Password	_____		
Confirm Password	_____		
Tunnel Broker	sixxs.net		
Subnet Prefix	_____ / _____		

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

Available settings are explained as follows:

Item	Description
<b>Always On</b>	Check this box to keep the network connection always.
<b>Username</b>	Type the name obtained from the broker. Please apply new account at <a href="http://www.sixxs.net/">http://www.sixxs.net/</a> . It is suggested for you to apply another username and password. The maximum length of the name you can set is 19 characters.
<b>Password</b>	Type the password assigned with the user name. The maximum length of the password you can set is 19 characters.

<b>Confirm Password</b>	Type the password again to make the confirmation.
<b>Tunnel Broker</b>	Type the address for the tunnel broker IP, FQDN or an optional port number.
<b>Subnet Prefix</b>	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

WAN 1

PPPv6	Static or Dynamic IP	PPPoE	IPv6
Internet Access Mode			
Connection Type		DHCPv6 Client	
DHCPv6 Client Configuration			
Identify Association	<input checked="" type="radio"/> Prefix Delegation	<input type="radio"/> Non-temporary Address	
IAID (Identity Association ID)	4230642002		

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.

WAN => Internet Access

WAN 1

PPPoE	Static or Dynamic IP	PPoP	IPv6						
Internet Access Mode									
Connection Type		Static IPv6							
Static IPv6 Address configuration									
IPv6 Address		/ Prefix Length							
<input type="text"/>		/ <input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>						
Current IPv6 Address Table									
Index	IPv6 Address/Prefix Length	Scope							
<table border="1"> <thead> <tr> <th>Index</th> <th>IPv6 Address/Prefix Length</th> <th>Scope</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				Index	IPv6 Address/Prefix Length	Scope			
Index	IPv6 Address/Prefix Length	Scope							
Static IPv6 Gateway configuration									
IPv6 Gateway Address		<input type="text" value="::"/>							

Available settings are explained as follows:

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

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

## Details Page for IPv6 – 6in4 Static Tunnel in WAN1/WAN2

This type allows you to setup 6in4 Static Tunnel for WAN interface.

Such mode allows the router to access IPv6 network through IPv4 network.

However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.

WAN > Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/2TP	IPv6
Internet Access Mode			
Connection Type		6in4 Static Tunnel	
6in4 Static Tunnel			
Remote Endpoint IPv4 Address		<input type="text"/>	
6in4 IPv6 Address		<input type="text"/> / 64	(default: 64)
LAN Routed Prefix		<input type="text"/> / 64	(default: 64)
Tunnel TTL		<input type="text"/> 255 (default: 255)	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Available settings are explained as follows:

Item	Description
<b>Remote Endpoint IPv4 Address</b>	Type the static IPv4 address for the remote server.
<b>6in4 IPv6 Address</b>	Type the static IPv6 address for IPv4 tunnel with the value for prefix length.
<b>LAN Routed Prefix</b>	Type the static IPv6 address for LAN routing with the value for prefix length.
<b>Tunnel TTL</b>	Type the number for the data lifetime in tunnel.

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

Below shows an example for successful IPv6 connection based on 6in4 Static Tunnel mode.

Online Status

Physical Connection		System Uptime: 0day 0:4:16	
IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:41000:ff00:8314::211:AAFF:1183:1114/64 (Global)			
FE80::211:AAFF:1183:1114/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
14	80	1244	6815
<b>WAN1 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	6in4 Static Tunnel	0:04:07	
<b>IP</b>		<b>Gateway IP</b>	
2001:41000:ff00:8314::2111/64 (Global)		::	
FE80::30A8:651D:128 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
3	26	211	2302

### Details Page for IPv6 – 6rd in WAN1/WAN2

This type allows you to setup 6rd for WAN interface.

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<b>Internet Access Mode</b>			
<b>Connection Type</b>		6rd	<input type="checkbox"/>
<b>6rd Settings</b>			
<b>6rd Mode</b>		<input checked="" type="radio"/> Auto 6rd <input type="radio"/> Static 6rd	
<b>Static 6rd Settings</b>			
<b>IPv4 Border Relay:</b>	192.168.101.111		
<b>IPv4 Mask Length:</b>	0		
<b>6rd Prefix:</b>	2001::11..		
<b>6rd Prefix Length:</b>	32		
		<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Available settings are explained as follows:

Item	Description
<b>6rd Mode</b>	<b>Auto 6rd</b> – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". <b>Static 6rd</b> - Set 6rd options manually.
<b>IPv4 Border Relay</b>	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
<b>IPv4 Mask Length</b>	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.



<b>6rd Prefix</b>	Type the 6rd IPv6 address.
<b>6rd Prefix Length</b>	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.

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

Below shows an example for successful IPv6 connection based on 6rd mode.

**Online Status**

Physical Connection		System Uptime: 0day 0:9:16	
IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:E11:A065:1D00:21D:AAFF:FE03:11B4/64 (Global)			
FE60::21D:AAFF:FE03:11B4/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
15	113	1351	10040
<b>WAN1 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	6rd	0:09:06	
<b>IP</b>		<b>Gateway IP</b>	
2001:E11:A065:1D01:21D:AAFF:FE03:11B5/120 (Global)		---	
FE60::C0A0:651D/120 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
13	29	967	2620

## 4.1.4 Multi-VLAN

Multi-VLAN allows users to create profiles for specific WAN interface and bridge connections for user applications that require very high network throughput. Simply go to WAN and select **Multi-VLAN**.

### General

This page shows the basic configurations used by every channel.

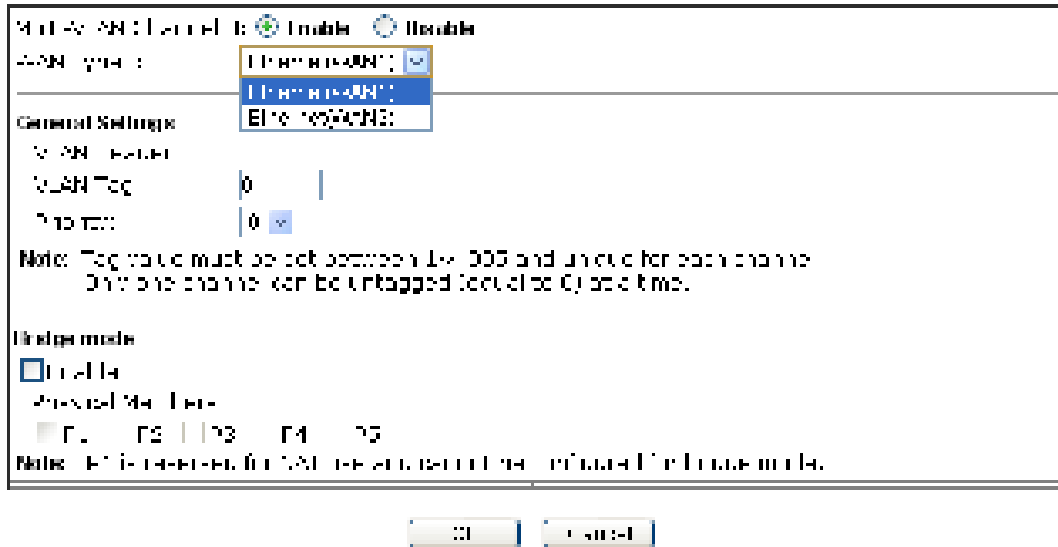
Multi-VLAN															
General															
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge											
1	Yes	Ethernet(WAN)	None												
2	Yes	Ethernet(WAN)	None												
3	No	Ethernet(WAN)	None												
4	No	Ethernet(WAN)	None												
5	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5
6	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5
7	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5
8	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5
9	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5
10	No	Ethernet(WAN)	None	<input type="checkbox"/>	Enable	<input type="checkbox"/>	P1	<input type="checkbox"/>	P2	<input type="checkbox"/>	P3	<input type="checkbox"/>	P4	<input type="checkbox"/>	P5

Available settings are explained as follows:

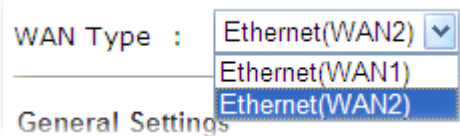
Item	Description
<b>Channel</b>	<p>Display the number of each channel.</p> <p>Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here.</p> <p>Channels 3 ~ 8 are configurable.</p>
<b>Enable</b>	<p>Display whether the settings in this channel are enabled (Yes) or not (No).</p>
<b>WAN Type</b>	<p>Displays the physical medium that the channel will use.</p>
<b>VLAN Tag</b>	<p>Displays the VLAN tag value that will be used for the packets traveling on this channel.</p>
<b>Port-based Bridge</b>	<p>The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p><b>Enable</b> - Check this box to enable the port-based bridge function on this channel.</p> <p><b>P1 ~ P5</b> – Check the box(es) to build bridge connection on LAN.</p>

Click any index (8, 9 and 10) to get the following web page:

WAN >> Multi-VLAN >> Channel 8



Available settings are explained as follows:

Item	Description
<b>Multi-VLAN Channel 8/9/10</b>	<p><b>Enable</b> – Click it to enable the configuration of this channel.</p> <p><b>Disable</b> –Click it to disable the configuration of this channel.</p>
<b>WAN Type</b>	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.</p> 
<b>General Settings</b>	<p><b>VLAN Tag</b> – Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p><b>Priority</b> – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
<b>Bridge mode</b>	<p><b>Enable</b> – Click it to enable Bridge mode for such channel.</p> <p><b>Physical Members</b> – Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.</p>

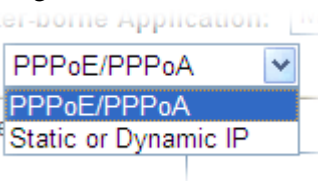
Moreover, WAN link for Channel 5, 6 and 7 are provided for router-borne application such as **TR-069**. The settings must be applied and obtained from your ISP. For your special request,

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

Available settings are explained as follows:

Item	Description
<b>Multi-VLAN Channel 5/6/7</b>	<p><b>Enable</b> – Click it to enable the configuration of this channel.</p> <p><b>Disable</b> –Click it to disable the configuration of this channel.</p>
<b>WAN Type</b>	<p>The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.</p>

<p><b>General Settings</b></p>	<p><b>VLAN Tag</b> – Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network traffic flowing on each channel will be identified by the system via their VLAN Tags. Channels using the same WAN type may not configure the same VLAN tag value.</p> <p><b>Priority</b> – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
<p><b>Open Port-based Bridge Connection for this Channel</b></p>	<p>The settings here will create a bridge between the LAN ports selected and the WAN. The WAN interface of the bridge connection will be built upon the WAN type selected using the VLAN tag configured.</p> <p><b>Physical Members</b> – Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p>
<p><b>Open WAN Interface for this Channel</b></p>	<p>Check the box to enable relating function.</p> <p><b>WAN Application - Management</b> 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.</p> <p><b>IPTV</b> - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.</p> <p><b>WAN Setup</b> – Choose <b>PPPoE/PPPoA</b> or <b>Static or Dynamic IP</b> to determine what WAN settings must be configured.</p> 
<p><b>ISP Access Setup, IP Address From ISP, WAN IP Network Settings, DNS Server IP Address</b></p>	<p>For other settings, refer to <b>Details Page for PPPoE in WAN1</b>.</p>

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

## 4.1.5 WAN Budget

This function is used to determine the data traffic volume for each WAN interface respectively to prevent from overcharges for data transmission by the ISP. Please note that the Time and Date settings will need to be configured correctly first in order for some period calculations to be performed correctly.

WAN >> WAN Budget

Index	Enable	Budget Status	Budgeting Period	Budget Action
WAN1	<input type="checkbox"/>	OK:0MB		
WAN2	<input type="checkbox"/>	OK:0MB		
WAN3	<input type="checkbox"/>	OK:0MB		

Note: The WAN Budget application provided here will allow users to define the limit of network traffic amount and setting each WAN interface separately. To edit the WAN budget, click on the WAN interface link, the screenshot is provided as follows:

Click WAN1/WAN2/WAN3 link to open the following web page.

The WAN Budget application will be set in the user interface. The WAN budget has exceeded the budget limit. Please configure the WAN Budget status of the WAN interface and click OK in the user interface.

Please make sure the **Time and Date** settings of the router is configured so that this application uses the correct time information in calculation.

Click WAN1/WAN2/WAN3 link to open the following web page.

WAN >> WAN Budget

WAN1

Enable:	<input checked="" type="checkbox"/>
Budget Limit:	0 MB
Budget Refreshing:	<input type="radio"/> Do not refresh <input type="radio"/> Periodically <input checked="" type="radio"/> Monthly <input type="radio"/> Do not refresh
Budget Apply:	<input type="checkbox"/> All WAN Interfaces <input type="checkbox"/> Some WAN Interfaces

Note: Please note that the WAN interface's counts is used in this application will be reset every time the configuration has been modified.

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Yes – Choose it to enable such function.
<b>Budget Limit</b>	Please insert the maximum network traffic limit here (in megabytes).
<b>Budget Refreshing</b>	This setting is used to restart the network connection traffic calculations. <b>Monthly</b> – The connection charges will be reset monthly. <b>Periodically</b> – The connection charges will be reset periodically. <b>Do not refresh</b> – The connection charges will not be reset.

<b>Budget Action</b>	<p>The system can choose one of the following actions to perform when the traffic has exceeded the budget limit.</p> <p><b>Shutdown WAN interface</b> – All the outgoing traffic through such WAN interface will be terminated.</p> <p><b>Send Mail Alert to Administrator</b> – The system will send out a warning message to the administrator. However, the connection charges will be calculated continuously.</p>
----------------------	--

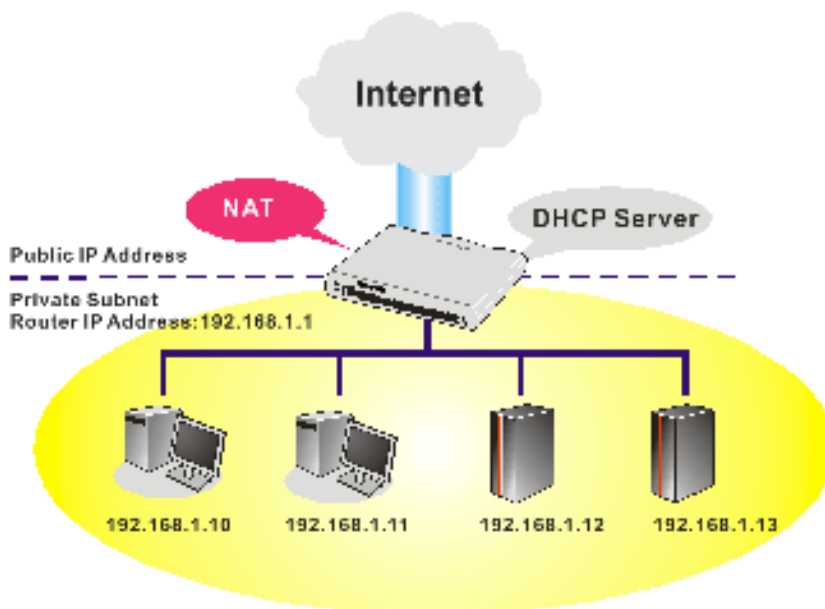
## 4.2 LAN

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



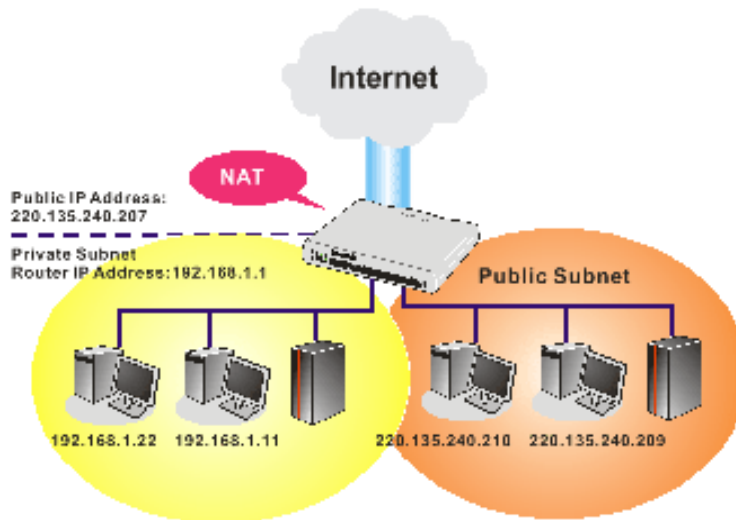
### 4.2.1 Basics of LAN

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)

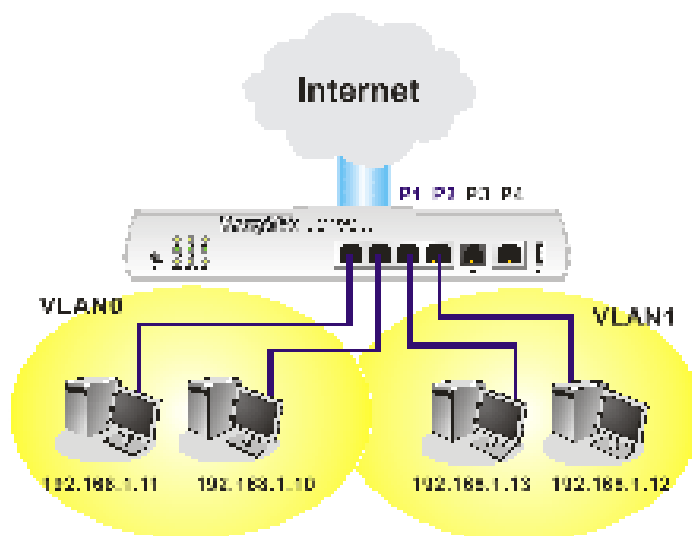
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### 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.





## 4.2.2 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 – LAN5). 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 – LAN5 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	Details Page	IPv6
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.1.1	Details Page	<input checked="" type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	<input type="checkbox"/>
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	<input type="checkbox"/>

**Advanced** - You can configure DHCP options here.

Force router to use DNS server IP address settings specified in

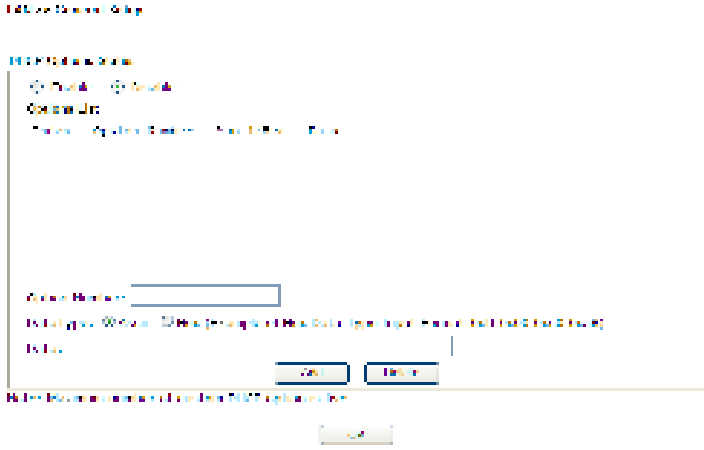
### Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: LAN 2/3/4/5 are available when VLAN is enabled.  
DMZ subnet is default bound to P1, and will overwrite the settings of P1 at LAN > VLAN page.

Available settings are explained as follows:

Item	Description
<b>General Setup</b>	<p>Allow to configure settings for each subnet respectively.</p> <p><b>Index</b> - Display all of the LAN items.</p> <p><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>.</p> <p><b>DHCP</b>- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.</p> <p><b>IP Address</b> - Display the IP address for each LAN item. Such information is set in default and you can not modify it.</p> <p><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></p> <p><b>IPv6</b> – Click it to access into the settings page of IPv6.</p>

<p><b>Advanced</b></p>	<p>DHCP packets can be processed by adding option number and data information when such function is enabled.</p>  <p><b>Enable/Disable</b> – 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</p> <p>When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.</p> <p><b>Option Number</b> – Type a number for such function.</p> <p><b>Data Type</b> – Choose the type (ASCII or Hex) for the data to be stored.</p> <p><b>Data</b> – Type the content of the data to be processed by the function of DHCP option.</p>
<p><b>Force router to use DNS server IP address .....</b></p>	<p>Force Vigor router to use DNS servers configured in LAN1/LAN2/LAN3/LAN4/LAN5 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).</p>
<p><b>Inter-LAN Routing</b></p>	<p>Check the box to link two or more different subnets (LAN and LAN).</p>

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

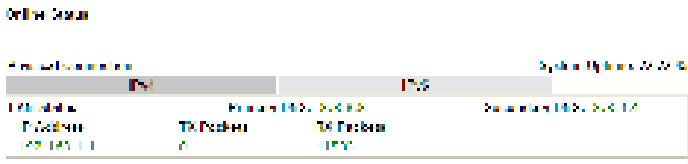
## Details Page for LAN1 – Ethernet TCP/IP and DHCP Setup

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.

LAN1 >> General Setup

Available settings are explained as follows:

Item	Description
<b>Network Configuration</b>	<p><b>For NAT Usage,</b></p> <p><b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p><b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p><b>RIP Protocol Control,</b></p> <p><b>Disable</b> - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)</p> <p><b>Enable</b> – activate the RIP protocol.</p>
<b>DHCP Server Configuration</b>	<p>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.</p> <p>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.</p> <p><b>Enable Server</b> - Let the router assign IP address to every host in the LAN.</p> <p><b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.</p> <p><b>Enable Relay Agent</b> –Specify which subnet that DHCP server is located the relay agent should redirect the DHCP</p>

	<p>request to.</p> <p><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.</p> <p><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.</p> <p><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.</p> <p><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.</p> <p><b>Lease Time</b> - Enter the time to determine how long the IP address assigned by DHCP server can be used.</p>
<p><b>DNS Server IP Address</b></p>	<p>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.</p> <p><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.</p> <p><b>Secondary IP Address</b> - 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.</p> <p>The default DNS Server IP address can be found via Online Status:</p>  <p>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.</p> <p>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.</p>

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.

LAN => General Setup

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

Available settings are explained as follows:

Item	Description
<b>RADVD Configuration</b>	<p><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.</p> <p><b>Disable</b> – Click it to disable RADVD server.</p> <p><b>Advertisement Lifetime</b> - 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</p>

	list.
<b>DHCPv6 Server Configuration</b>	<p><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.</p> <p><b>Disable Server</b> –Click it to disable DHCPv6 server.</p> <p><b>Start IPv6 Address / End IPv6 Address</b> –Type the start and end address for IPv6 server.</p>
<b>DNS Server IPv6 Address</b>	<p><b>Primary DNS Sever</b> – Type the IPv6 address for Primary DNS server.</p> <p><b>Secondary DNS Server</b> –Type another IPv6 address for DNS server if required.</p>
<b>Static IPv6 Address configuration</b>	<p><b>IPv6 Address</b> –Type static IPv6 address for LAN.</p> <p><b>Prefix Length</b> – Type the fixed value for prefix length.</p> <p><b>Add</b> – Click it to add a new entry.</p> <p><b>Delete</b> – Click it to remove an existed entry.</p>
<b>Current IPv6 Address Table</b>	Display current used IPv6 addresses.

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

## Details Page for LAN2 ~ LAN5 and DMZ

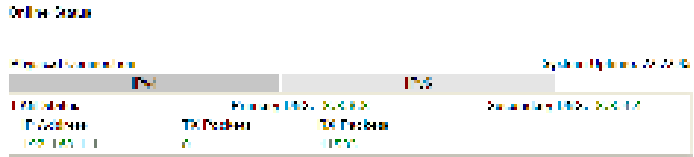
LAN >> General Setup

### DHCP (Dynamic TCP/IP and DHCP) Setup

<b>Network Configuration</b> <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>		<b>DHCP Server Configuration</b> <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server <input type="checkbox"/> Enable Relay Agent Start IP Address: <input type="text" value="01.08.0.0"/> DHCP Count: <input type="text" value="01"/> Gateway IP Address: <input type="text" value="01.08.0.1"/> Lease Time: <input type="text" value="1"/> (h) <input type="text" value="0"/> (m)	
		<b>DHCP Server IP Address</b> Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/> Tertiary IP Address: <input type="text"/>	

Available settings are explained as follows:

Item	Description
<b>Network Configuration</b>	<p><b>Enable/Disable</b> - Click <b>Enable</b> to enable such configuration; click <b>Disable</b> to disable such configuration.</p> <p><b>For NAT Usage</b> - Click this radio button to invoke NAT function.</p> <p><b>For Routing Usage</b> - Click this radio button to invoke this function.</p> <p><b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p><b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p>
<b>DHCP Server Configuration</b>	<p>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.</p> <p><b>Enable Server</b> - Let the router assign IP address to every host in the LAN.</p> <p><b>Disable Server</b> - Let you manually assign IP address to every host in the LAN.</p> <p><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.</p> <p><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.</p> <p><b>Start IP Address</b> - Enter a value of the IP address pool for</p>

	<p>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.</p> <p><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.</p> <p><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.</p> <p><b>Lease Time</b> - Enter the time to determine how long the IP address assigned by DHCP server can be used.</p>
<p><b>DNS Server IP Address</b></p>	<p>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.</p> <p><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.</p> <p><b>Secondary IP Address</b> - 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.</p> <p>The default DNS Server IP address can be found via Online Status:</p>  <p>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.</p> <p>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.</p>

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



## Details Page for IP Routed Subnet

1.6.1.1 General Setup

DHCP and DHCP Setup for IP Routed Subnet

<p><b>Network Configuration</b></p> <p><input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>For Routing Usage</p> <p>IP Address: 192.168.0.1</p> <p>Subnet Mask: 255.255.255.0</p> <hr/> <p>RIP Protocol Control: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p>	<p><b>DHCP Server Configuration</b></p> <p>Start IP Address: _____</p> <p>End IP Address: _____ (Max: 32)</p> <p>Lease Time: 300 (0-180)</p> <p><input type="checkbox"/> Use DHCP <input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2</p> <p><input checked="" type="checkbox"/> Use MAC Address</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Matched MAC Address</th> <th>Given IP Address</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p>MAC Address:     : : :  </p> <p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/></p> <p><input type="button" value="OK"/></p>	Index	Matched MAC Address	Given IP Address			
Index	Matched MAC Address	Given IP Address					

Available settings are explained as follows:

Item	Description
<b>Network Configuration</b>	<p><b>Enable/Disable</b> - Click <b>Enable</b> to enable such configuration; click <b>Disable</b> to disable such configuration.</p> <p><b>For Routing Usage,</b></p> <p><b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p><b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p><b>RIP Protocol Control,</b></p> <p><b>Disable</b> - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)</p> <p><b>Enable</b> – activate the RIP protocol.</p>
<b>DHCP Server Configuration</b>	<p>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.</p> <p>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.</p> <p><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</p>

---

192.168.1.254.

**IP Pool Counts** - 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.

**Lease Time** - Enter the time to determine how long the IP address assigned by DHCP server can be used.

**Use LAN Port** – 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.

**MAC Address:** Enter the MAC Address of the host one by one and click **Add** 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.

**Delete** – Click it to delete the selected MAC address.

**Edit** – Click it to edit the selected MAC address.

**Cancel** – 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.

### 4.2.3 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 Table
Index	Destination Address	Status	Index	Destination Address	Status		
1.	???	?	6.	???	?		
2.	???	?	7.	???	?		
3.	???	?	8.	???	?		
4.	???	?	9.	???	?		
5.	???	?	10.	???	?		

1 10 | 11 20 | 21 30 >>> Next >>>

Status:  Active,  Inactive,  Empty

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all of the settings and return to factory default settings.
<b>Viewing Routing Table</b>	Displays the routing table for your reference. <a href="#">Click here to view the routing table</a>
<b>Index</b>	The number (1 to 30) 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.
<b>Status</b>	Displays the status of the static route.

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

[LAN >> Static Route Setup](#)

**Index No. 1**

**Enable**

Destination IP Address:

Subnet Mask:

Gateway IP Address:

Network Interface: LAN1 ▾

Available settings are explained as follows:

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

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

## 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			<a href="#">Set to Factory Default</a>	<a href="#">View IPv6 Routing Table</a>
Index	Destination Address	Status	Index	Destination Address	Status		
<a href="#">1.</a>	::/0	x	<a href="#">11.</a>	::/0	x		
<a href="#">2.</a>	::/0	x	<a href="#">12.</a>	::/0	x		
<a href="#">3.</a>	::/0	x	<a href="#">13.</a>	::/0	x		
<a href="#">4.</a>	::/0	x	<a href="#">14.</a>	::/0	x		
<a href="#">5.</a>	::/0	=	<a href="#">15.</a>	::/0	=		
<a href="#">6.</a>	::/0	=	<a href="#">16.</a>	::/0	=		
<a href="#">7.</a>	::/0	=	<a href="#">17.</a>	::/0	=		
<a href="#">8.</a>	::/0	=	<a href="#">18.</a>	::/0	=		
<a href="#">9.</a>	::/0	=	<a href="#">19.</a>	::/0	=		
<a href="#">10.</a>	::/0	=	<a href="#">20.</a>	::/0	=		

[<< 1-20](#) | [21-40 >>](#)

[Next >>](#)

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

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all of the settings and return to factory default settings.
<b>Viewing IPv6 Routing Table</b>	Displays the routing table for your reference.
<b>Index</b>	The number (1 to 40) 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.
<b>Status</b>	Displays the status of the static route.

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

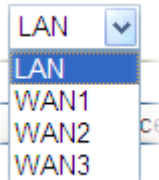
[LAN >> Static Route Setup](#)

Index No. 1

<input type="checkbox"/> Enable	
Destination IPv6 Address / Prefix Len	:: / 0
Gateway IPv6 Address	
Network Interface	LAN

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check it to enable this profile.

<b>Destination IPv6 Address / Prefix Len</b>	Type the IP address with the prefix length for this entry.
<b>Gateway IPv6 Address</b>	Type the gateway address for this entry.
<b>Network Interface</b>	Use the drop down list to specify an interface for this static route. 

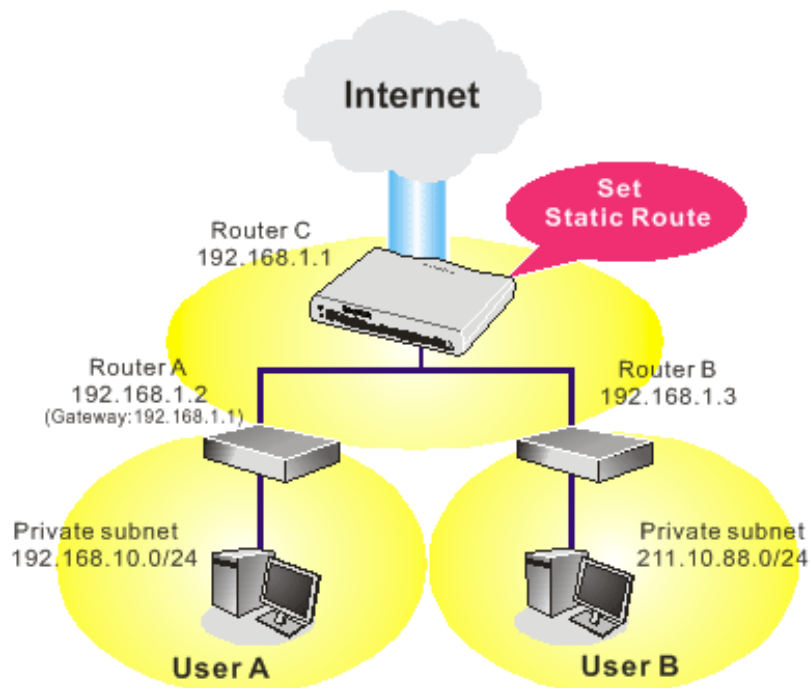
After finishing all the settings here, please click **OK** to save the configuration.

### Add Static Routes to Private and Public Networks (based on IPv4)

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.

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**.

LAN >> Static Route Setup

---

Index No. 1

Enable

Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN1

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**.

LAN >> Static Route Setup

---

Index No. 2

Enable

Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN1

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

Diagnostics >> View Routing Table

Current Running Routing Table		IPv6 Routing Table		Refresh
Key:	C connected, S static, R RIPv1, * redistributed, - private			
S*	192.168.10.0/24	255.255.255.0	via 192.168.1.2	LAN1
C*	192.168.1.0/24	255.255.255.0	directly connected	LAN1
S*	222.200.88.0/24	255.255.255.0	via 192.168.1.2	LAN1

## 4.2.4 VLAN

With the 5-port Gigabit switch on the LAN side, Vigor router provides extremely high speed connectivity for the highest speed local data transfer of any server or local PCs. On the wireless-equipped model, each of the wireless SSIDs can also be grouped within one of the VLANs.

### Tagged VLAN

The tagged VLANs (802.1q) can mark data with a VLAN identifier. This identifier can be carried through an onward Ethernet switch to specific ports. The specific VLAN clients can also pick up this identifier as it is just passed to the LAN. You can set the priorities for LAN-side QoS. You can assign each of VLANs to each of the different IP subnets that the router may also be operating, to provide even more isolation. The said functionality is **tag-based multi-subnet**.

### Port-Based VLAN

Relative to tag-based VLAN which groups clients with an identifier, port-based VLAN uses physical ports (P1 ~ P5) to separate the clients into different VLAN group.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.



LAN => VLAN Configuration

VLAN Configuration

	LAN					Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	P5	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1	<input type="checkbox"/>	1	1

Click the Enable checkbox to enable VLAN configuration.

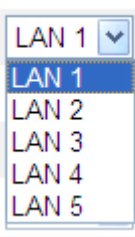
1. Tag-based VLAN only applied for LAN ports.

2. The selected Wireless LAN SSID filter use VLAN tagging function and generate a joining SSID.

3. The selected LAN port(s) must be made active first.

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

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Click it to enable VLAN configuration.
<b>LAN</b>	<b>P1 – P5</b> – Check the LAN port(s) to be grouped under the selected VLAN.
<b>Wireless LAN</b>	<b>SSID1 – SSID4</b> – Check the SSID boxes to group them under the selected VLAN.
<b>Subnet</b>	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.  <div style="text-align: center;"> <p><b>Subnet</b></p>  </div>
<b>VLAN Tag</b>	<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.

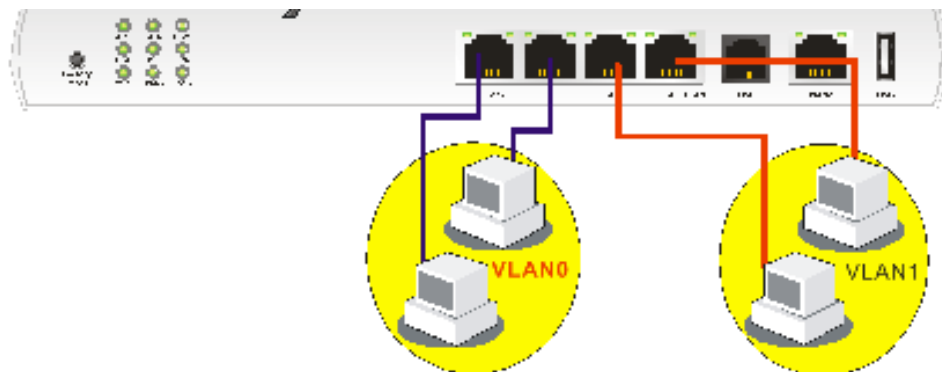
	<p>Please type the tag value and specify the priority for the packets sending by LAN.</p> <p><b>VID</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p><b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
<p><b>Permit untagged device in P1 to access router</b></p>	<p>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.</p>

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

Vigor2925 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

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.



- 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.

LAN >> VLAN Configuration

VLAN Configuration

	LAN					Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	P5	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	1	1
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	10	1
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input checked="" type="checkbox"/>	11	1
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 4	<input checked="" type="checkbox"/>	12	1
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 5	<input checked="" type="checkbox"/>	13	1
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	1	1
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	1	1
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	1	1

Permit untrusted device in VLAN to access router:

- The basic VLAN can't apply for LAN Ports.
- The basic or Wireless LAN SSID will not have VLAN tagging function but required as joining VLAN GROUP.
- The basic VLAN ID (VID) must be unique and not duplicate.

The Vigor router also supports up to six private IP subnets on the LAN. Each can be independent (isolated) or common (able to communicate with each other). This is ideal for departmental or multi-occupancy applications.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address	Details Page	[IPv6]
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	<input type="checkbox"/>
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	Details Page	<input type="checkbox"/>
IP Pooled Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	<input type="checkbox"/>

You can configure DHCP options here.

Force router to use "DNS server IP address" settings specified in

Inter LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



<b>Refresh</b>	Refresh the ARP table listed below to obtain the newest ARP table information.
<b>Add or Update</b>	<p><b>IP Address</b> – Type the IP address that will be used for the specified MAC address.</p> <p><b>Mac Address</b> – Type the MAC address that is used to bind with the assigned IP address.</p> <p><b>Comment</b> – Type a brief description for the entry.</p> <p><b>Show Comment</b> – Check this box to display the comment on IP Bind List box.</p>
<b>IP Bind List</b>	It displays a list for the IP bind to MAC information.
<b>Add</b>	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> .
<b>Update</b>	It allows you to edit and modify the selected IP address and MAC address that you create before.
<b>Delete</b>	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> .

**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.

## 4.2.6 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 Mirror

Port Mirror:  
 Enable  Disable

Mirror port:  
 e7  e1  e4  e11

Mirrored port:  
 p1  p2  p3  p4  p5

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.

## 4.2.7 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 Table:

Profile	Status	Interface	
1	Disable	None	Preview
2	Disable	None	Preview
3	Disable	None	Preview
4	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 4

Disable

URL Redirect

Message

URL

eg. http://www.router.com

Note: If the User Management application is enabled, it will override the Web Portal settings seen here.

HTML/JavaScript content (HTML/JavaScript/Flash/ActiveX/Java) - (Optional)

Content: (HTML/JavaScript/Flash/ActiveX/Java)

Preview: (HTML/JavaScript/Flash/ActiveX/Java)

Note: All characters!

Applied Interfaces

	LAN1	LAN2	LAN3	LAN4	LAN5
WLAN1 :	SSID1	SSID2	SSID3	SSID4	
WLAN2 :	SSID1	SSID2	SSID3	SSID4	


Available settings are explained as follows:

Item	Description
<b>Disable</b>	Click this button to close this function.
<b>URL Redirect</b>	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.
<b>Message</b>	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.
<b>Applied Interfaces</b>	Check the box(es) representing different interfaces to be applied by such profile.  The advantage is that each LAN (1/2/3/4) interface <b>and/or</b> each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.

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


### 4.3 Load-Balance /Route Policy

**Load-Balance / Route Policy** (Cisco called it "policy-based routing") is a feature where a set of rules or "policies" are defined first. Then, if there comes a packet that matches any one of the "policies", it will be directed to the specified interface.

Load Balance/Route Policy 

Policy Route | **Serial Factory Default** |

Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Next IP End	Dest Port Start	Dest Port End	Match Up	Match Down
1	<input checked="" type="checkbox"/>	Any	WAN1	--									Down
2	<input type="checkbox"/>	Any	WAN2									UP	Down
3	<input checked="" type="checkbox"/>	Any	WAN1	--								UP	Down
4	<input type="checkbox"/>	Any	WAN2									UP	Down
5	<input checked="" type="checkbox"/>	Any	WAN1	--								UP	Down
6	<input type="checkbox"/>	Any	WAN2									UP	Down
7	<input checked="" type="checkbox"/>	Any	WAN1	--								UP	Down
8	<input type="checkbox"/>	Any	WAN2									UP	Down
9	<input checked="" type="checkbox"/>	Any	WAN1	--								UP	Down
10	<input type="checkbox"/>	Any	WAN2									UP	Down

1-10 | 11-20 | 21-30 | 31-40 | 41-50 

Available settings are explained as follows:

Item	Description
<b>Index</b>	Click the number of index to access into the configuration web page.



<b>Enable</b>	Check this box to enable this policy.
<b>Protocol</b>	Display the protocol used for this policy.
<b>Interface</b>	Display the interface to send packets to once the policy is matched.
<b>Interface Address</b>	Display the WAN IP or WAN IP alias address which is used as source IP of the outgoing packets.
<b>Src IP Start</b>	Displays the IP address for the start of the source IP.
<b>Src IP End</b>	Displays the IP address for the end of the source IP.
<b>Dest IP Start</b>	Displays the IP address for the start of the destination IP.
<b>Dest IP End</b>	Displays the IP address for the end of the destination IP.
<b>Dest Port Start</b>	Displays the IP address for the start of the destination port.
<b>Dest Port End</b>	Displays the IP address for the end of the destination port.
<b>Move UP/Move Down</b>	Use <b>Up</b> or <b>Down</b> link to move the order of the policy.

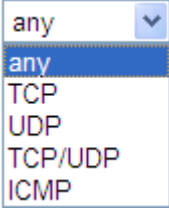
Click **Index 1** to access into the following page for configuring load-balance policy.

#### Load-Balance/Fault Policy

Index: 1

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check this box to enable this policy.

<b>Protocol</b>	<p>Use the drop-down menu to choose a proper protocol for the WAN interface.</p> 
<b>Source IP</b>	<p><b>Any</b> – Any IP can be treated as the source IP.</p> <p><b>Src IP Start</b> - Type the source IP start for the specified WAN interface.</p> <p><b>Src IP End</b> - 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.</p>
<b>Destination IP</b>	<p><b>Any</b> – Any IP can be treated as the destination IP.</p> <p><b>Dest IP Start</b>- Type the destination IP start for the specified WAN interface.</p> <p><b>Dest IP End</b> - 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.</p>
<b>Destination Port</b>	<p><b>Any</b> – Any port number can be treated as the destination port.</p> <p><b>Dest Port Start</b> - Type the destination port start for the destination IP.</p> <p><b>Dest Port End</b> - 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.</p>
<b>Send to if criteria matched</b>	<p><b>Interface</b> – Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.</p> <p><b>Gateway IP</b> – <b>Specific gateway</b> is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.</p>
<b>More options</b>	<p><b>Auto Failover To The Other WAN</b> – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is down.</p> <p><b>Packet Forwarding to WAN via</b> – Choose <b>Force NAT</b> or <b>Force Routing</b>.</p>

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

Local Network/Route Policy

Policy Route											Set to Factory Default	
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Source IP	Source Mask
1	<input checked="" type="checkbox"/>	IP	LAN1	--	Any	Any	Any	Any	Any	Any		Down
2	<input type="checkbox"/>	IP	LAN1	--							IP	Down
3	<input type="checkbox"/>	IP	LAN1	--							UP	Down
4	<input type="checkbox"/>	IP	LAN1	--							UP	Down
5	<input type="checkbox"/>	IP	LAN1	--							UP	Down
6	<input type="checkbox"/>	IP	LAN1	--							UP	Down
7	<input type="checkbox"/>	IP	LAN1	--							UP	Down
8	<input type="checkbox"/>	IP	LAN1	--							UP	Down
9	<input type="checkbox"/>	IP	LAN1	--							UP	Down
10	<input type="checkbox"/>	IP	LAN1	--							UP	Down

1-10 |  11-20 |  21-30 |  31-40 |  41-50  Next

## 4.4 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.

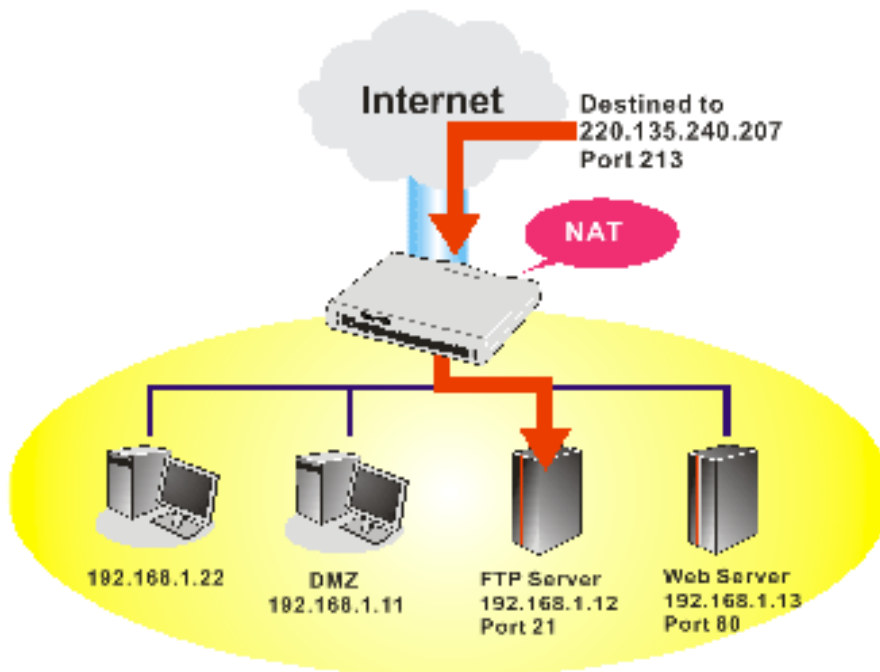
**Note:** On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be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

Below shows the menu items for NAT.



#### 4.4.1 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.

NAI >> Port Redirection

Port Redirection | [Set to Factory Default](#)

Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
1.		All				x
2.		All				x
3.		All				x
4.		All				x
5.		All				x
6.		All				x
7.		All				x
8.		All				x
9.		All				x
10.		All				x

<< 1-10 | 11-20 >> [Next >>](#)

Each item is explained as follows:

Item	Description
<b>Index</b>	Display the number of the profile.
<b>Service Name</b>	Display the description of the specific network service.
<b>WAN Interface</b>	Display the WAN IP address used by the profile.
<b>Protocol</b>	Display the transport layer protocol (TCP or UDP).
<b>Public Port</b>	Display the port number which will be redirected to the specified <b>Private IP and Port</b> of the internal host.
<b>Private IP</b>	Display the IP address of the internal host providing the service.
<b>Status</b>	Display if the profile is enabled (v) or not (x).

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

NAI >> Port Redirection

Index No. 1

Enable

Mode: Range   
 Service Name:   
 Protocol:   
 WAN IP: All   
 Public Port:   
 Private IP:   
 Private Port:

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

Available settings are explained as follows:

<b>Item</b>	<b>Description</b>
<b>Enable</b>	Check this box to enable such port redirection setting.
<b>Mode</b>	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.
<b>Service Name</b>	Enter the description of the specific network service.
<b>Protocol</b>	Select the transport layer protocol (TCP or UDP).
<b>WAN IP</b>	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.
<b>Public Port</b>	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.
<b>Private IP</b>	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).
<b>Private Port</b>	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.

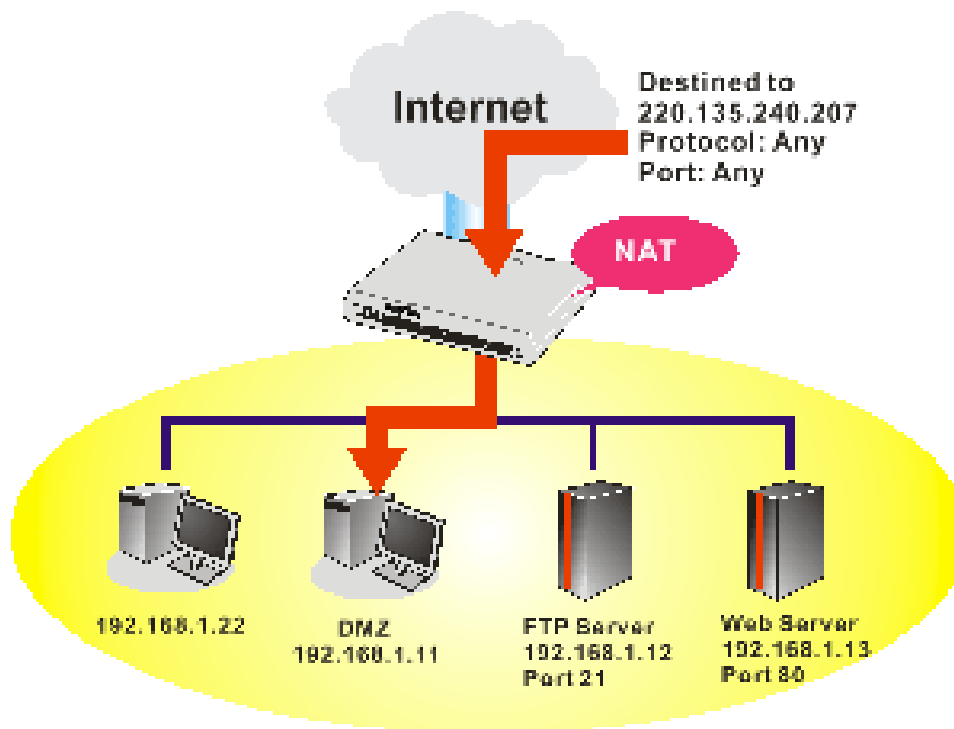
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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.

IPv4 Management Setup		IPv6 Management Setup													
<b>Hoster Name</b> <input type="text"/>		<b>Management Port Setup</b> <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports													
<b>Management Access Control</b> <input type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet		Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) SSH Port <input type="text" value="22"/> (Default: 22)													
<b>Access List</b>															
<table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>			
List	IP	Subnet Mask													
1	<input type="text"/>	<input type="text"/>													
2	<input type="text"/>	<input type="text"/>													
3	<input type="text"/>	<input type="text"/>													
<input type="button" value="OK"/>															

#### 4.4.2 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.

NAT or DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3
<p>WAN 1</p> <p>None <input type="button" value="Choose PC"/></p> <p>Private IP <input type="text"/></p> <p>MAC Address of the True IP DMZ Host <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/></p> <p>Note: When a true IP DMZ host is turned on, it will force the router's WAN connection to be always on.</p> <p><input type="button" value="OK"/></p>		

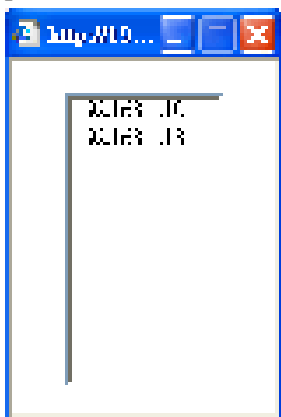
Available settings are explained as follows:

Item	Description
<p>WAN 1</p> <p>None <input type="button" value="Choose PC"/></p> <p>Private IP <input type="text"/></p> <p>MAC Address of the True IP DMZ Host <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/></p>	<p>Choose <b>Private IP</b> or <b>Active True IP</b> first.</p> <p><b>Active True IP</b> selection is available for WAN1 only.</p>
<b>Private IP</b>	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.



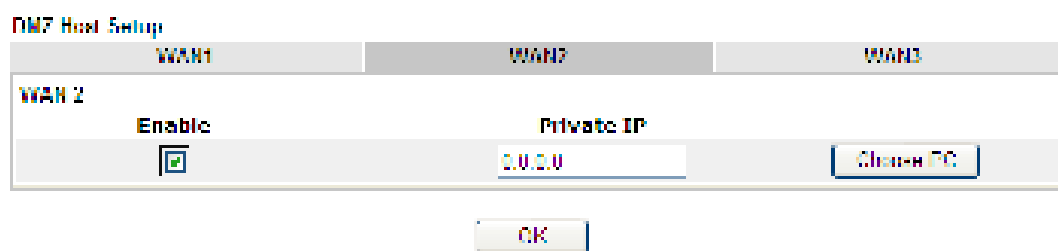
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.



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



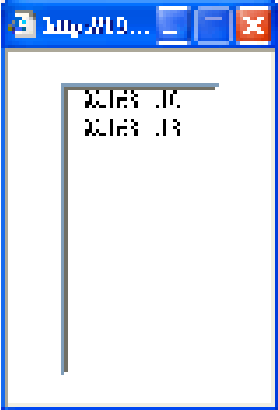
If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2 interface, you will find them in **Aux. WAN IP** for your selection.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1		WAN2		WAN3
<b>WAN 2</b>				
Index	Enable	Aux. WAN IP	Private IP	
1.	<input type="checkbox"/>	---	0.0.0.0	<input type="button" value="Choose PC"/>
2.	<input checked="" type="checkbox"/>	192.168.1.43	0.0.0.0	<input type="button" value="Choose PC"/>

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable the DMZ Host function.
<b>Private IP</b>	Enter the private IP address of the DMZ host, or click Choose PC to select one.
<b>Choose PC</b>	<p>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.</p>  <p>When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click <b>OK</b> to save the setting.</p>

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

### 4.4.3 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:

[NAI >> Open Ports](#)

Open Ports Setup [Set to Factory Defaults](#)

Index	Comment	WAN Interface	Local IP Address	Status
1				X
2				X
3				X
4				X
5				X
6				X
7				X
8				X
9				X
10				X

«: 1 10 | 11 20 »: Next »:

Available settings are explained as follows:

Item	Description
<b>Index</b>	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.
<b>Comment</b>	Specify the name for the defined network service.
<b>WAN Interface</b>	Display the WAN interface used by such index.
<b>Local IP Address</b>	Display the private IP address of the local host offering the service.
<b>Status</b>	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.

Index No. 1

Enable Open Ports

Comment:

WAN Interface:

Local Computer:

	Protocol	Start Port	End Port		Protocol	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

Available settings are explained as follows:

Item	Description
<b>Enable Open Ports</b>	Check to enable this entry.
<b>Comment</b>	Make a name for the defined network application/service.
<b>WAN Interface</b>	Specify the WAN interface that will be used for this entry.
<b>WAN IP</b>	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.
<b>Local Computer</b>	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.
<b>Protocol</b>	Specify the transport layer protocol. It could be <b>TCP</b> , <b>UDP</b> , or <b>-----</b> (none) for selection.
<b>Start Port</b>	Specify the starting port number of the service offered by the local host.
<b>End Port</b>	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](#)

**Open Ports Setup** [Set to Factory Default](#)

Index	Comment	WAN Interface	Local IP Address	Status
1.	WWW	WAN1	192.168.1.49	✓
2.				=
3.				=
4.				=
5.				=
6.				=
7.				=

#### 4.4.4 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 Triggering** [Set to Factory Default](#)

Index	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Status
1.						×
2.						×
3.						×
4.						×
5.						×
6.						×
7.						×
8.						×
9.						×
10.						×

◀ [1-10](#) | [11-20](#) ▶ [Next](#) ▶▶

Available settings are explained as follows:

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

<b>Comment</b>	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.
<b>Incoming Protocol</b>	Display the protocol for the incoming data of such triggering profile.
<b>Incoming Port</b>	Display the port for the incoming data of such triggering profile.
<b>Status</b>	Display if the rule is active or de-active.

Click the index number link to open the configuration page.

**NAT** >> **Port Triggering**

No. 1

**Enable**

**Service** User Defined ▾

**Comment** [ ]

**Triggering Protocol** TCP ▾

**Triggering Port** 80


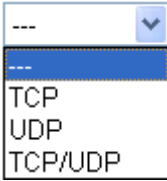
**Incoming Protocol** UDP ▾

**Incoming Port** 1024

**Note:** The Triggering Port and Incoming Port should be input like this : 120.456.777.289 (leg4), 121.456.789 (leg4), but 121.456.789 (ileg4).

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable this entry.
<b>Service</b>	Choose the <b>predefined</b> service to apply for such trigger profile. <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> User Defined ▾  User Defined  Real Player  QuickTime  WMP  IRC  AIM Talk  ICQ  PaITalk  BitTorrent </div>
<b>Comment</b>	Type the text to memorize the application of this rule.
<b>Triggering Protocol</b>	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.

	
<b>Triggering Port</b>	Type the port or port range for such triggering profile.
<b>Incoming Protocol</b>	<p>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.</p> 
<b>Incoming Port</b>	Type the port or port range for the incoming packets.

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

## 4.5 Hardware Acceleration

Hardware Acceleration is also called **PPA** in DrayTek for it is based on **Protocol Processing Engine (PPE)** of Infinion. It can only support 128 sessions for network traffic (IN & OUT) with implementing three kinds of modes - Disable, Auto and Manual.

### 4.5.1 Setup

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself. Open **Hardware Acceleration>>Setup** to access into the following page:

Hardware Acceleration >> Setup

Mode:  ▼

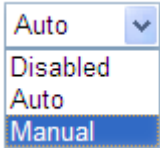
Protocol:  TCP  UDP

Options:  Accelerate most heavy traffic sessions  
 Apply the Class Rule in Quality of Service  
 Specific Hosts:

Index	Enable	Start port	End port	Private IP	
1.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
3.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
4.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>
5.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="button" value="Choose PC"/>

Note: Bandwidth Management will not work if Hardware Acceleration was enabled.

Available settings are explained as follows:

Item	Description
Mode	<p><b>Auto Mode</b> - When the hardware acceleration is configured with the <b>Auto</b> mode, the sessions with the most heavy loading sessions and the lower latency traffic will be added into PPA. However, the Auto mode does not support UDP protocol by designed.</p> <p><b>Manual Mode</b> - The Manual mode implements three sub-items-- <i>Accelerate most heavy traffic sessions</i>, <i>Apply the Class Rule in Quality of Service</i>, and <i>Specific Hosts</i>. Each of these sub-items can support TCP and UDP protocol.</p> 
Protocol	There are two types supported by this function, TCP and UDP.
Option	<b>Accelerate most heavy traffic sessions</b> – Such option is

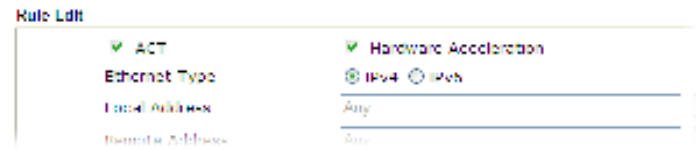


available in Auto Mode, too. But the UDP protocol is only supported in this sub-item.

**Apply the Class Rule in Quality of Service** – Users can apply the information provided by QoS in this sub-item.

**Note:** Please visit our website for referring the detailed configuration of QoS.

[Bandwidth Management >> Quality of Service](#)



**Specific Hosts** – This sub-item provides 5 hosts for adding NAT sessions into the PPA. For the PPA only support s128 sessions, these hosts will share these sessions. Therefore, the performance will be lower than only one host.

Choose this option to specify certain PCs on LAN to apply the hardware acceleration.

- **Enable** – Check the box to make PC(s) specified in the selected index entry to be applied.
- **Start port** – Type the starting port for the PC(s) in LAN.
- **End port** – Type the ending port for the PC(s) in LAN.
- **Private IP/Choose PC** – Type the IP address as the selected host. Or click the Choose PC button to specify one IP address from the pop-up window.

## Checking the PPA status

For checking whether the rule of PPA is working or not, a user can login to Vigor2925 series by using telnet. User can view how many sessions is transferring in each direction of PPA table after entering “**ppa -v**”.

```

> ppa -v
* PPA mode is Auto
* PPA mode is Manual (<traffic>)
* PPA time is 10
* PPA range is 255
-----
WAN Acceleration session
Session - Src ip:Src port ----- Dest ip:Dest port --- Nat ip:Nat port
-----
-----
LAN Acceleration session
Session - Src ip:Src port ----- Dest ip:Dest port --- Nat ip:Nat port
-----
0 - 192.168. 1. 10: 2930 - 119.236.154.122: 5590 - 192.168. 3. 10:52524
Src mac:00:22:15:06:05:59 ---- Dest mac:00:50:76:37:c8:4c
1 - 192.168. 1. 10: 2952 - 193. 88. 6. 13:33033 - 192.168. 3. 10:52530
Src mac:00:22:15:06:05:59 ---- Dest mac:00:50:76:37:c8:4c

```

## 4.6 Firewall

### 4.6.1 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:

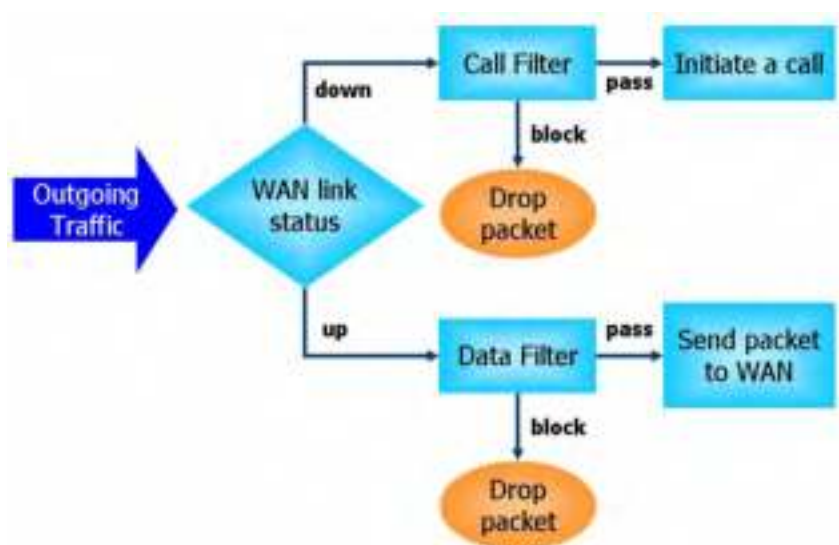
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

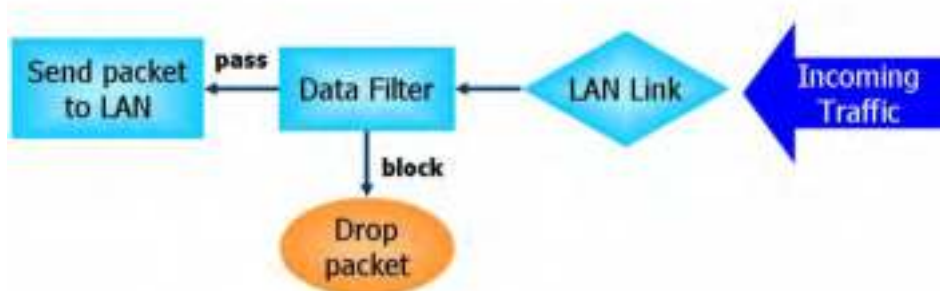
#### IP Filters

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.





## 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  | 9. SYN fragment          |
| 2. UDP flood attack  | 10. Fraggle attack       |
| 3. ICMP flood attack | 11. TCP flag scan        |
| 4. Port Scan attack  | 12. Tear drop attack     |
| 5. IP options        | 13. Ping of Death attack |
| 6. Land attack       | 14. ICMP fragment        |
| 7. Smurf attack      | 15. Unknown protocol     |
| 8. Trace route       |                          |

Below shows the menu items for Firewall.

```

NAT
Firewall
  General Setup
  Filter Setup
  DoS Defense
  User Management
  
```

## 4.6.2 General Setup

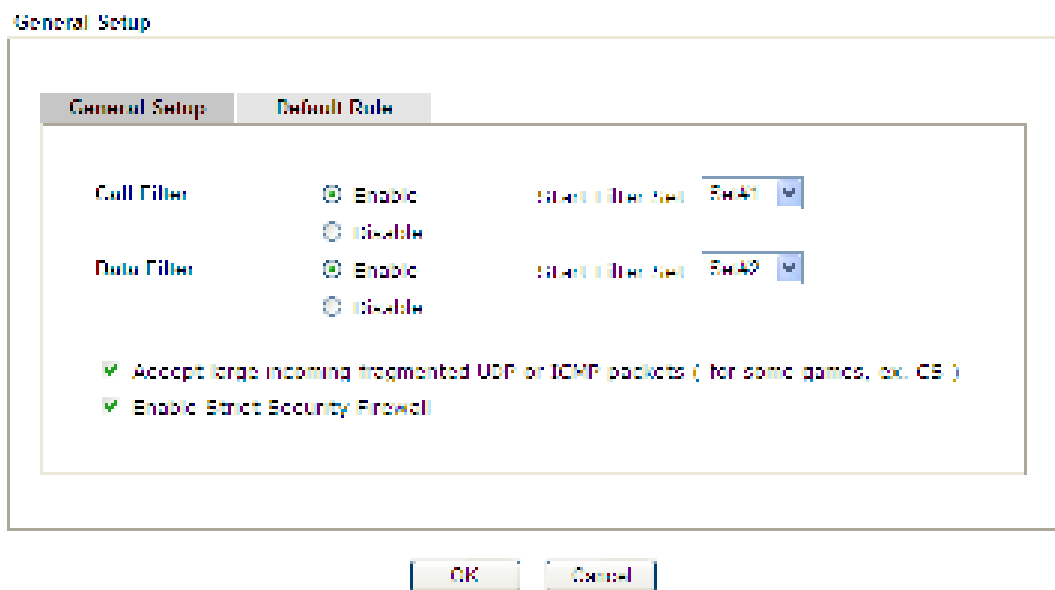
General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure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



Available settings are explained as follows:

Item	Description
<b>Call Filter</b>	Check <b>Enable</b> to activate the Call Filter function. Assign a start filter set for the Call Filter.
<b>Data Filter</b>	Check <b>Enable</b> to activate the Data Filter function. Assign a start filter set for the Data Filter.
<b>Accept large incoming...</b>	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 " <b>Accept large incoming fragmented UDP or ICMP Packets</b> ". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable " <b>Accept large incoming fragmented UDP or ICMP Packets</b> ".

## 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, Policy Route, WCF, APP Enforcement, URL Content Filter for data transmission via Vigor router.


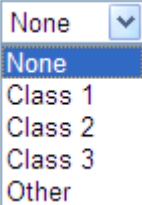
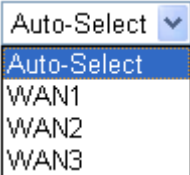
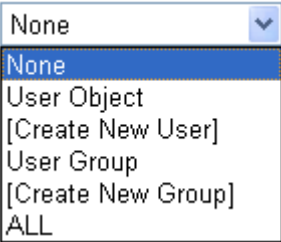
Firewall >> General Setup

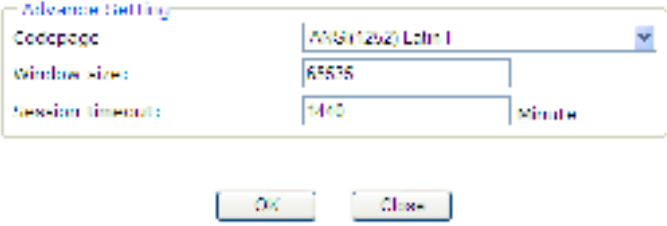
General Setup

Actions for default rule:	Action Profile	System
Application		
Filter	Pass	<input type="checkbox"/>
Security Control	2 / PRIORITY	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
Load Balance policy	Auto-Selected	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>

Advanced Settings

Available settings are explained as follows:

Item	Description
<b>Filter</b>	<p>Select <b>Pass</b> or <b>Block</b> for the packets that do not match with the filter rules.</p> <p>Filter </p>
<b>Sessions Control</b>	<p>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.</p>
<b>Quality of Service</b>	<p>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.</p> 
<b>Policy Route</b>	<p>Choose the WAN interface for applying Policy Route.</p> 
<b>User Management</b>	<p>Such item is available only when <b>Rule-Based</b> is selected in User <b>Management</b>&gt;&gt;<b>General Setup</b>. The general firewall rule will be applied to the user/user group/all users specified here.</p>  <p><b>Note:</b> 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.</p>
<b>APP Enforcement</b>	<p>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</p>

	Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
<b>URL Content Filter</b>	Select one of the <b>URL Content Filter</b> profile settings (created in <b>CSM&gt;&gt; URL Content Filter</b> ) for applying with this router. Please set at least one profile for choosing in <b>CSM&gt;&gt; URL 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>URL 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.
<b>Web Content Filter</b>	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.
<b>Advance Setting</b>	<p>Click <b>Edit</b> to open the following window. However, it is <b>strongly recommended</b> to use the default settings here.</p> <p><b>Firewall =&gt; General Setup</b></p>  <p><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.</p> <p>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.</p>



**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.

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



### 4.6.3 Filter Setup

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

Firewall => Filter Setup

Filter Setup | [Set to Factory Default](#)

Set	Comments	Set	Comments
<a href="#">1</a>	Default Call Filter	<a href="#">1</a>	
<a href="#">2</a>	Default Data Filter	<a href="#">1</a>	
<a href="#">3</a>		<a href="#">2</a>	
<a href="#">4</a>		<a href="#">10</a>	
<a href="#">5</a>		<a href="#">11</a>	
<a href="#">6</a>		<a href="#">12</a>	

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 :

Filter Rule	Active	Comments	Move Up	Move Down
<a href="#">1</a>	<input checked="" type="checkbox"/>	Block NetExec		<a href="#">Down</a>
<a href="#">2</a>	<input type="checkbox"/>		<a href="#">Up</a>	<a href="#">Down</a>
<a href="#">3</a>	<input type="checkbox"/>		<a href="#">Up</a>	<a href="#">Down</a>
<a href="#">4</a>	<input type="checkbox"/>		<a href="#">Up</a>	<a href="#">Down</a>
<a href="#">5</a>	<input type="checkbox"/>		<a href="#">Up</a>	<a href="#">Down</a>
<a href="#">6</a>	<input type="checkbox"/>		<a href="#">Up</a>	<a href="#">Down</a>
<a href="#">7</a>	<input type="checkbox"/>		<a href="#">Up</a>	

Next Filter Set

Available settings are explained as follows:

Item	Description
<b>Filter Rule</b>	Click a button numbered (1 ~ 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.
<b>Active</b>	Enable or disable the filter rule.
<b>Comment</b>	Enter filter set comments/description. Maximum length is 23-character long.
<b>Move Up/Down</b>	Use <b>Up</b> or <b>Down</b> link to move the order of the filter rules.
<b>Next Filter Set</b>	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.

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments: Block H-File

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

Clear sessions when schedule ON:  Enable

Direction: LAN/WAN/RTN/VPN or WAN

Source IP: Any

Destination IP: Any

Service Types: TCP/UDP, Port Area 137-139 to any

Protocols: Don't Care

Application: Action Profile

Filter: Pass if No Further Match   Spelling

Overwrite to Other Filter Sets: None

Escalation Control: 0 / 60000

Max. Inlet IP: Any-Same

Quality of Service: None

Load-Balance policy: Auto Select

User Management: None

APP Enforcement: None

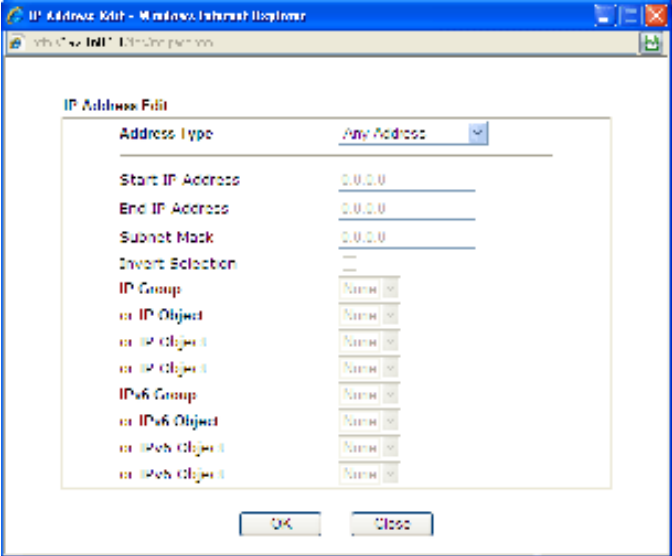
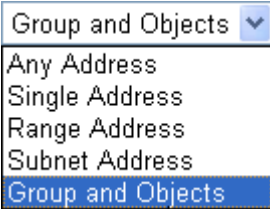
URL Content Filter: None

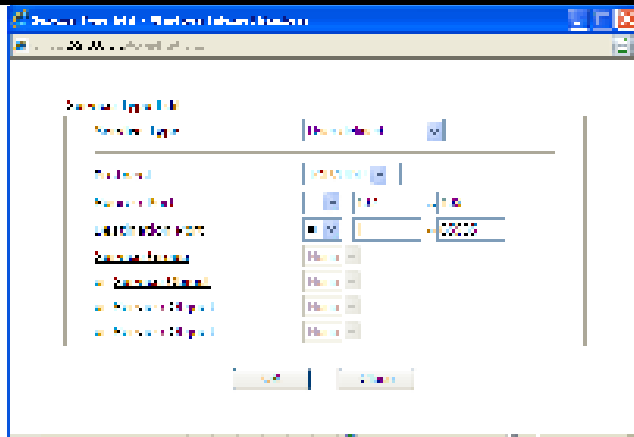
Web Content Filter: None

Advanced Setting

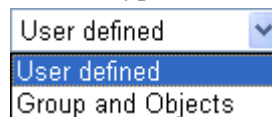
Available settings are explained as follows:

Item	Description
<b>Check to enable the Filter Rule</b>	Check this box to enable the filter rule.
<b>Comments</b>	Enter filter set comments/description. Maximum length is 14- character long.
<b>Index(1-15)</b>	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 &gt;&gt; Schedule</b> setup. The default setting of this field is blank and the function will always work.
<b>Clear sessions when schedule ON</b>	Check this box to clear the sessions when the above schedule profiles are applied.
<b>Direction</b>	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.

	<p>LAN/DMZ/RT/VPN -&gt; WAN  LAN/DMZ/RT/VPN -&gt; WAN  WAN -&gt; LAN/DMZ/RT/VPN  LAN/DMZ/RT/VPN -&gt; LAN/DMZ/RT/VPN</p> <p><b>Note:</b> RT means routing domain for 2nd subnet or other LAN.</p>
<p><b>Source/Destination IP</b></p>	<p>Click <b>Edit</b> to access into the following dialog to choose the source/destination IP or IP ranges.</p>  <p>To set the IP address manually, please choose <b>Any 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.</p>  <p>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.</p>
<p><b>Service Type</b></p>	<p>Click <b>Edit</b> to access into the following dialog to choose a suitable service type.</p>



To set the service type manually, please choose **User defined** 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.



**Protocol** - 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.

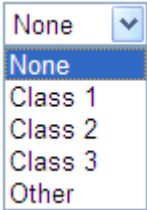
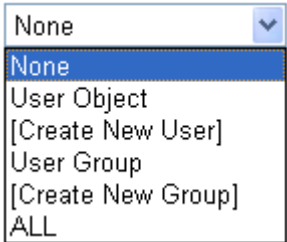
(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

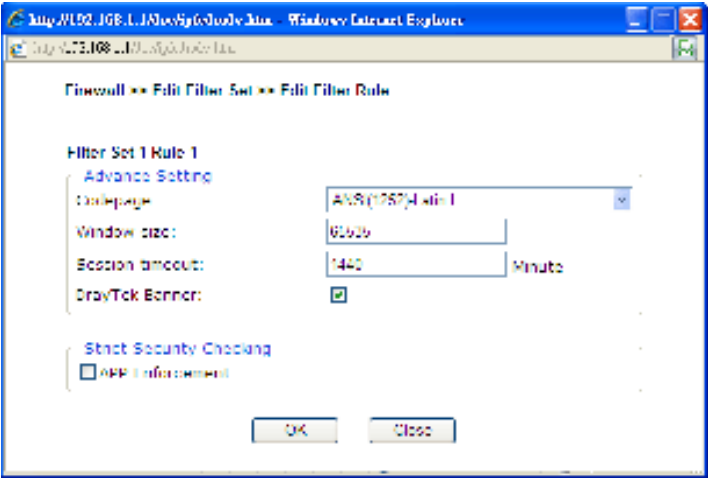
(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

**Service Group/Object** - Use the drop down list to choose the one that you want.

<p><b>Fragments</b></p>	<p>Specify the action for fragmented packets. And it is used for <b>Data Filter</b> only.</p> <p><b>Don't care</b> -No action will be taken towards fragmented packets.</p> <p><b>Unfragmented</b> -Apply the rule to unfragmented packets.</p> <p><b>Fragmented</b> - Apply the rule to fragmented packets.</p> <p><b>Too Short</b> - Apply the rule only to packets that are too short to contain a complete header.</p>
<p><b>Filter</b></p>	<p>Specifies the action to be taken when packets match the rule.</p> <p><b>Block Immediately</b> - Packets matching the rule will be dropped immediately.</p> <p><b>Pass Immediately</b> - Packets matching the rule will be</p>

	<p>passed immediately.</p> <p><b>Block If No Further Match</b> - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p><b>Pass If No Further Match</b> - A packet matching the rule, and that does not match further rules, will be passed through.</p>
<b>Branch to other Filter Set</b>	<p>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.</p>
<b>Sessions Control</b>	<p>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.</p>
<b>MAC Bind IP</b>	<p><b>Strict</b> - Make the MAC address and IP address settings configured in <b>IP Object</b> for <b>Source IP</b> and <b>Destination IP</b> be bound for applying such filter rule.</p> <p><b>No-Strict</b> - no limitation.</p>
<b>Quality of Service</b>	<p>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.</p> 
<b>Load-Balance policy</b>	<p>Choose the WAN interface for applying Policy Route.</p>
<b>User Management</b>	<p>Such item is available only when <b>Rule-Based</b> is selected in User <b>Management</b>&gt;&gt;<b>General Setup</b>. The general firewall rule will be applied to the user/user group/all users specified here.</p>  <p><b>Note:</b> 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.</p>
<b>APP Enforcement</b>	<p>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</p>

	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.
<b>URL Content Filter</b>	Select one of the <b>URL Content Filter</b> profile settings (created in <b>CSM&gt;&gt; URL Content Filter</b> ) for applying with this router. Please set at least one profile for choosing in <b>CSM&gt;&gt; URL 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>URL 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.
<b>URL Content Filter</b>	Select one of the <b>URL Content Filter</b> profile settings (created in <b>CSM&gt;&gt; URL Content Filter</b> ) for applying with this router. Please set at least one profile for choosing in <b>CSM&gt;&gt; URL 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>URL 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.
<b>Web Content Filter</b>	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.
<b>Advance Setting</b>	<p>Click <b>Edit</b> to open the following window. However, it is <b>strongly recommended</b> to use the default settings here.</p>  <p><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</p>

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.

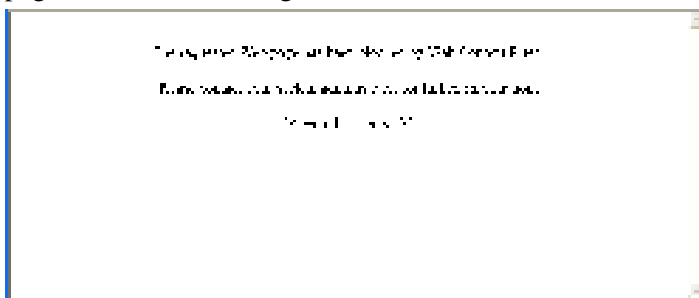
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



**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.

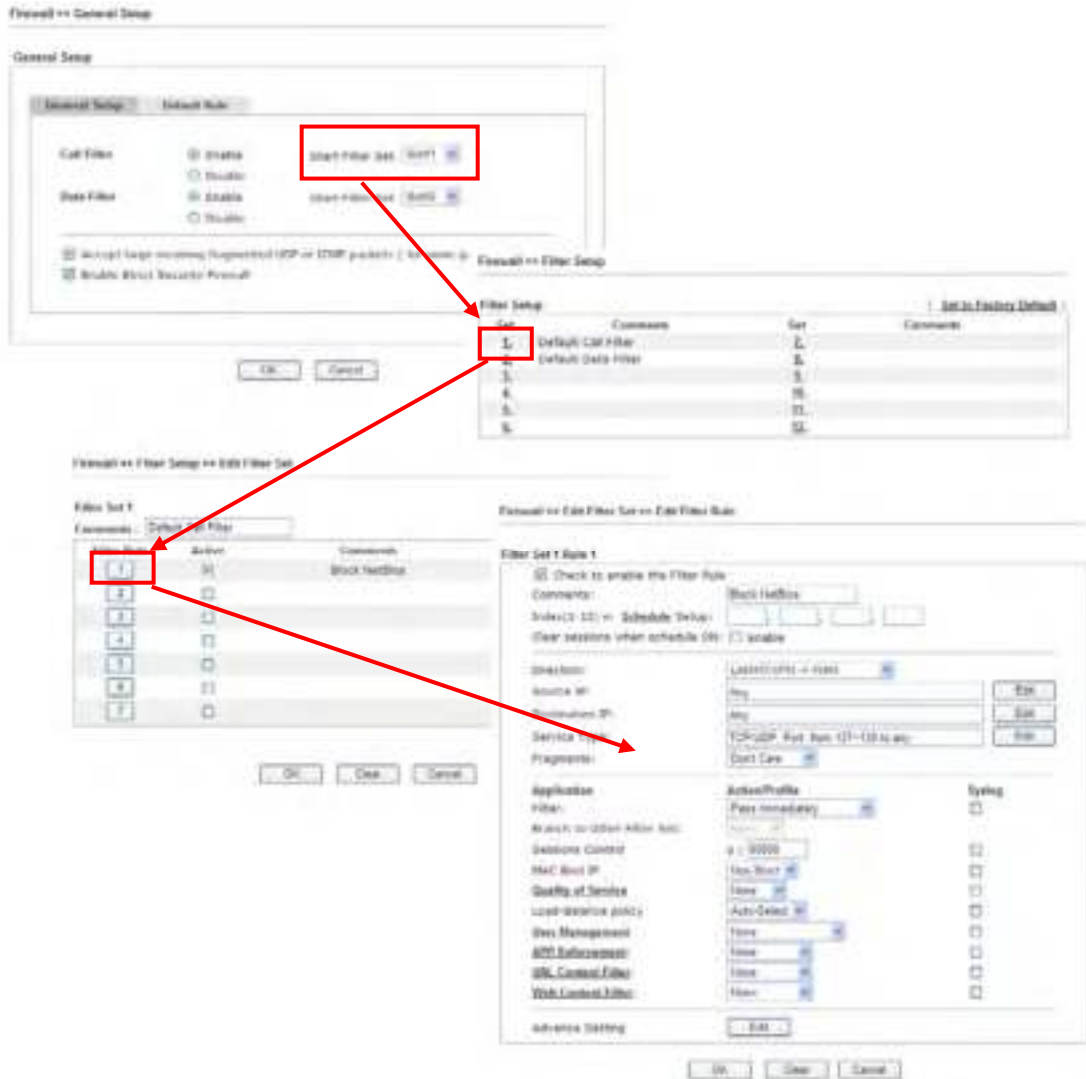


**Strict Security Checking** - For the sake of security, you might want the router executing strict security checking for data transmission. The router performance will be affected if you invoke strict security checking.

**APP Enforcement** – Check this box to execute the critical checking for all the files transferred via IM/P2P.

## Example

As stated before, all the traffic will be separated and arbitrated using one 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.





## 4.6.4 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

DoS defense Setup

Enable DoS Defense

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="150"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="150"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP Reset		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unassigned Numbers		
<input type="checkbox"/> Block Fraggle Attack			

Enable DoS defense function to prevent the attacks from hacker or crackers.

Available settings are explained as follows:

Item	Description
<b>Enable Dos Defense</b>	Check the box to activate the DoS Defense Functionality.
<b>Select All</b>	Click this button to select all the items listed below.
<b>Enable SYN flood defense</b>	<p>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.</p> <p>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.</p>
<b>Enable UDP flood defense</b>	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

	<p>will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>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.</p>
<b>Enable ICMP flood defense</b>	<p>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.</p> <p>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.</p>
<b>Enable PortScan detection</b>	<p>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.</p> <p>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”.</p>
<b>Block IP options</b>	<p>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 messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
<b>Block Land</b>	<p>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.</p>
<b>Block Smurf</b>	<p>Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.</p>
<b>Block trace router</b>	<p>Check the box to enforce the Vigor router not to forward any trace route packets.</p>
<b>Block SYN fragment</b>	<p>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.</p>
<b>Block Fraggle Attack</b>	<p>Check the box to activate the Block fraggle Attack function.</p>

	<p>Any broadcast UDP packets received from the Internet is blocked.</p> <p>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.</p>
<b>Block TCP flag scan</b>	<p>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 scan</i>, <i>SYN FINscan</i>, <i>Xmas scan</i> and <i>full Xmas scan</i>.</p>
<b>Block Tear Drop</b>	<p>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.</p>
<b>Block Ping of Death</b>	<p>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.</p>
<b>Block ICMP Fragment</b>	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>
<b>Block Unassigned Numbers</b>	<p>Check the box to activate the 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.</p>
<b>Warning Messages</b>	<p>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.</p> <p>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.</p>



## 4.7 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.

Firewall  
**User Management**  
 General Setup  
 User Profile  
 User Group  
 User Online Status  
 Objects Setting

## 4.7.1 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

**General Setup**

Mode: **Rule Based**

---

Web Authentication: **HTTPS**

**Notes :**

1. User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode.
2. Users match the above lists will not be required for authentication. The firewall rules policy will still valid.
3. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.

Landing Page (Max 255 characters) [Preview](#) [Set to Factory Default](#)

```
<body language="javascript" language="javascript">
<index location="http://www.draytek.com/~/scripted/index">
```

**OK** **Clear** **Cancel**

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.</p> <p><b>User-Based</b> - If you choose such mode, the router will apply the filter rules configured in <b>User Management&gt;&gt;User Profile</b> to the users.</p> <p><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.</p>
<b>Web Authentication</b>	Choose the protocol for web authentication.
<b>Landing Page</b>	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.

## 4.7.2 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**.

[User Management >> User Profile](#)

User Profile Table [Set to Factory Defaults](#)

Profile	Name	Profile	Name
<a href="#">1</a>	admin	<a href="#">17</a>	
<a href="#">2</a>	Dial-In User	<a href="#">18</a>	
<a href="#">3</a>	LAN_User_Group_1	<a href="#">19</a>	
<a href="#">4</a>	WLAN_User_Group_1A	<a href="#">20</a>	
<a href="#">5</a>	WLAN_User_Group_3	<a href="#">21</a>	
<a href="#">6</a>		<a href="#">22</a>	
<a href="#">7</a>		<a href="#">23</a>	
<a href="#">8</a>		<a href="#">24</a>	
<a href="#">9</a>		<a href="#">25</a>	
<a href="#">10</a>		<a href="#">26</a>	
<a href="#">11</a>		<a href="#">27</a>	
<a href="#">12</a>		<a href="#">28</a>	
<a href="#">13</a>		<a href="#">29</a>	
<a href="#">14</a>		<a href="#">30</a>	
<a href="#">15</a>		<a href="#">31</a>	
<a href="#">16</a>		<a href="#">32</a>	

[1 37](#) | [33 64](#) | [65 96](#) | [97 128](#) | [129 160](#) | [161 192](#) | [193 200](#)
[Next >>](#)

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](#)

Profile Index 3

Enable this account

User Name:

Password:

Confirm Password:

Idle Timeout:  | Inactive Unlimited

Max User Limit:  | 0: Unlimited

Log:

Admin when making profile:

Authentication:  Local  External  Portal

[Linking Page](#)

Incompat. with [Schedule Setup](#):  .  .  .

---


Enable Time Quota:  min.  sec.

Enable Data Quota:  MB  KB

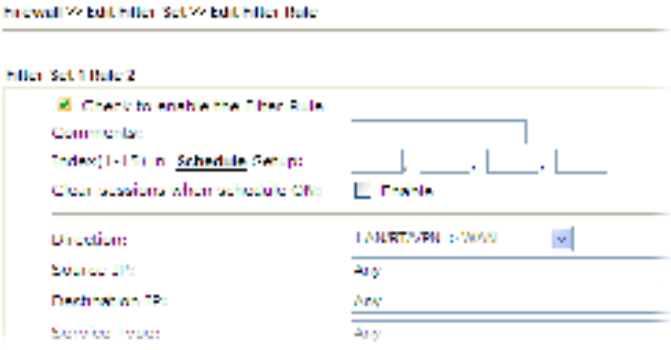
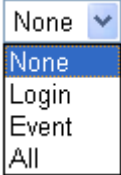
Use number 0 default when set each of time quota.

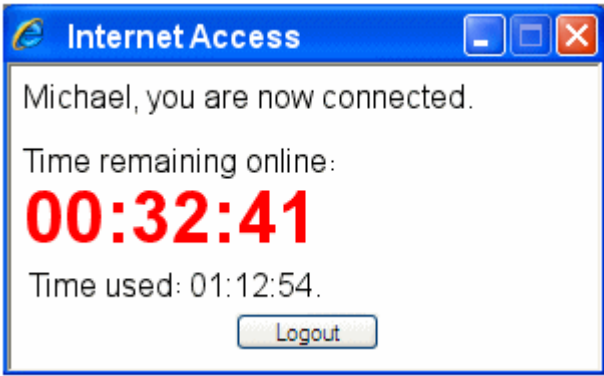
Enable Default Time Quota:  min. Default Data Quota:  KB

Available settings are explained as follows:

Item	Description
<b>Enable this account</b>	Check this box to enable such user profile.
<b>User Name</b>	Type a name for such user profile (e.g., <i>LAN_User_Group_1</i> , <i>WLAN_User_Group_A</i> , <i>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. The maximum length of the name you can set is 24 characters.
<b>Password</b>	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. The maximum length of the password you can set is 24 characters.
<b>Confirm Password</b>	Type the password again for confirmation.
<b>Idle Timeout</b>	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.
<b>Max User Login</b>	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.
<b>Policy</b>	<p>It is available only when <b>User-Based</b> mode selected in <b>User Management&gt;&gt;General Setup</b>.</p>  <p><b>Default</b> – If you choose such item, the filter rules pre-configured in <b>Firewall</b> can be adopted for such user profile.</p> <p><b>Create New Policy</b> – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.</p>



	 <p>For the detailed configuration, simply refer to <b>Firewall&gt;&gt;Filter Rule</b>. The firewall filter rules that are not selected in <b>Firewall&gt;&gt;General&gt;&gt;Default rule</b> can be available for use in <b>User Management&gt;&gt;User Profile</b>.</p>
<p><b>Log</b></p>	<p>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).</p> 
<p><b>Pop Browser Tracking Window</b></p>	<p>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.</p>
<p><b>Authentication</b></p>	<p>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.</p> <p><b>Web</b> – 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 <b>Welcome Message</b> (configured in <b>User Management &gt;&gt; General Setup</b>) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.</p> <p><b>Alert Tool</b> – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A 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.</p> <p><b>Telnet</b> – If it is selected, the user can use Telnet command to perform the authentication job.</p>
<p><b>Landing Page</b></p>	<p>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</p>

	Landing Page field in <b>User Management&gt;&gt;General Setup</b> . Check this box to enable such function.
<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 &gt;&gt; Schedule</b> web page and you can use the number that you have set in that web page.
<b>Enable Time Quota</b>	<p>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.</p> <p><input type="button" value="+"/> – Click this box to set and increase the time quota for such profile.</p> <p><input type="button" value="-"/> – Click this box to decrease the time quota for such profile.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>Note:</b> A dialog will be popped up to notify how many time remained when a user accesses into Internet through Vigor router successfully.</p>  <p>When the time is up, all the connection jobs including network, IM, social media, facebook, and etc. will be terminated.</p> </div>
<b>Enable Data Quota</b>	<p>Data Quota means the total amount for data transmission allowed for the user. The unit is MB.</p> <p><input type="button" value="+"/> – Click this box to set and increase the data quota for such profile.</p> <p><input type="button" value="-"/> – Click this box to decrease the data quota for such profile.</p>
<b>Reset quota to default when scheduling time expired</b>	<p>Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically.</p> <p><b>Enable</b> – Check it to use the default setting for time quota and data quota.</p> <p><b>Default Time Quota</b> – Type the value for the time manually.</p> <p><b>Default Data Quota</b> – Type the value for the data manually.</p>

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

### 4.7.3 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.

User Management >> User Group

User Group Table: [Set to Factory Default](#)

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

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

User Management >> User Group

Profile Index : 1

Name:

Available User Objects

- 1 Admin
- 2 Dial-In User
- 3 LAN User Group 1
- 4 LAN User Group 2
- 5 LAN User Group 3

Selected User Objects(Max 32 Objects)

Available settings are explained as follows:

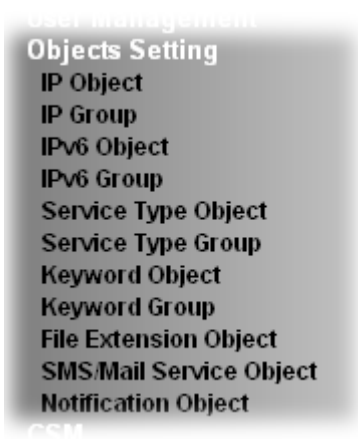
Item	Description
<b>Name</b>	Type a name for this user group.
<b>Available User Objects</b>	You can gather user profiles (objects) from <b>User Profile</b> page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined profiles will be numbered with 3, 4, 5 and so



<b>Data Quota</b>	Display the quota for data transmission.
<b>Idle Time</b>	Display the idle timeout setting for such profile.
<b>Action</b>	<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.

## 4.8 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).



### 4.8.1 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
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

⏪ 1-32 | 17-34 | 65-96 | 97-128 | 129-160 | 161-192 ⏩ [Next](#) ⏪

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:

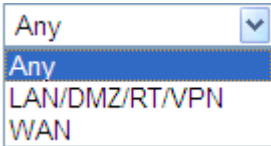
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index: 1

Name:	153 Department
Interface:	Any
Address Type:	Range Address
Start IP Address:	00.00.000.000.000.00
Start IP Address:	192.168.1.50
End IP Address:	192.168.1.60
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

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

	<p>for IP address.</p> <p>Select <b>Any Address</b> if this object contains any IP address.</p> <p>Select <b>Mac Address</b> if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px;"> <p>Range Address ▾</p> <p>Any Address</p> <p>Single Address</p> <p style="background-color: #e0e0e0;">Range Address</p> <p>Subnet Address</p> <p>Mac Address</p> </div>
<b>MAC Address</b>	Type the MAC address of the network card which will be controlled.
<b>Start IP Address</b>	Type the start IP address for Single Address type.
<b>End IP Address</b>	Type the end IP address if the Range Address type is selected.
<b>Subnet Mask</b>	Type the subnet mask if the Subnet Address type is selected.
<b>Invert Selection</b>	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

- 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
1.	RD Department	12.
2.	Financial Dept	13.
3.	HR Department	14.
4.		20.
5.		21.
6.		22.

## 4.8.2 IP Group

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

[Objects Setting](#) >> [IP Group](#)

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

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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:	<input type="text" value="Administration"/>
Interface:	<input type="text" value="Any"/>
Available IP Objects	Selected IP Objects
<ul style="list-style-type: none"> <li>143 Department</li> <li>2 Financial Dept</li> <li>24 HR Department</li> </ul>	<div style="border-left: 1px solid black; border-right: 1px solid black; height: 100px; margin: 5px 0;"></div> <div style="display: flex; justify-content: center; gap: 10px;"> <div style="border: 1px solid gray; padding: 2px 5px;">&gt;&gt;</div> <div style="border: 1px solid gray; padding: 2px 5px;">&gt;&gt;</div> </div>



Available settings are explained as follows:

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

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

### 4.8.3 IPv6 Object

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

Network Settings >> IPv6 Object

IPv6 Object Profiles		Set to Factory Default	
Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

1-32 | 33-64

Next

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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:

Network Settings > IPv6 Control

---

Profile Index: 1

Name:	<input type="text"/>
Address Type:	Subnet Address ▾
Mac Address:	<input type="text" value="00:00:00:00:00:00"/>
Start IP Address:	<input type="text"/>
End IP Address:	<input type="text"/>
Prefix Len:	<input type="text"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type a name for this profile. Maximum 15 characters are allowed.
<b>Address Type</b>	<p>Determine the address type for the IPv6 address.</p> <p>Select <b>Single Address</b> if this object contains one IPv6 address only.</p> <p>Select <b>Range Address</b> if this object contains several IPv6s within a range.</p> <p>Select <b>Subnet Address</b> if this object contains one subnet for IPv6 address.</p> <p>Select <b>Any Address</b> if this object contains any IPv6 address.</p> <p>Select <b>Mac Address</b> if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px;"> Range Address ▾  Any Address  Single Address  Range Address  Subnet Address  Mac Address </div>
<b>Mac Address</b>	Type the MAC address of the network card which will be controlled.
<b>Start IP Address</b>	Type the start IP address for Single Address type.
<b>End IP Address</b>	Type the end IP address if the Range Address type is selected.
<b>Prefix Len</b>	Type the number (e.g., 64) for the prefix length of IPv6 address.
<b>Invert Selection</b>	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

#### 4.8.4 IPv6 Group

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

Objects Setting >> IPv6 Group

IPv6 Group Table: | [Set to Factory Default](#) |

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

Available settings are explained as follows:

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

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

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

Objects Setting >> IPv6 Group

Profile Index: 1

Name: \_\_\_\_\_

Available IPv6 Objects	Selected IPv6 Objects

Available settings are explained as follows:

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

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

## 4.8.5 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	
1		17		
2		18		
3		19		
4		20		
5		21		
6		22		
7		23		
8		24		
9		25		
10		26		
11		27		
12		28		
13		29		
14		30		
15		31		
16		32		

1 32 | 33 64 | 65 96 :: **Next** >>

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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.

- The configuration page will be shown as follows:

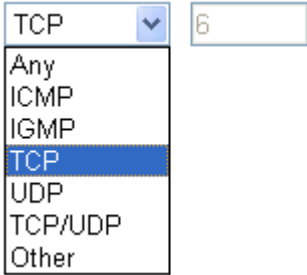
Objects Setting > Service Type Object Setup

Profile Index: 1

Name	www	
Protocol	TCP	6
Source Port	- 1	- 65535
Destination Port	- 1	- 65535

OK    Close    Cancel

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type a name for this profile.
<b>Protocol</b>	Specify the protocol(s) which this profile will apply to. 
<b>Source/Destination Port</b>	<b>Source Port</b> and the <b>Destination Port</b> column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) – 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. (!=) – 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.

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

Objects Setting > Service Type Object

Service Type Object Profiles:

Index	Name	Index
1	www	12
2	udp	13
3		14
4		27



Item	Description
<b>Name</b>	Type a name for this profile.
<b>Available Service Type Objects</b>	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.
<b>Selected Service Type Objects</b>	Click >> button to add the selected IP objects in this box.

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

### 4.8.7 Keyword Object

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

Objects Setting >> Keyword Object

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

1 32 | 33 64 | 65 96 | 97 128 | 129 160 | 161 192 | 193 200
First

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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:

Object Settings >> Keyword Object Setup

---

Profile Index: 1

Name	<input type="text"/>
Contents	<input type="text"/>

Limit of Contents: Max 8 Words and 80 Characters.  
Each word should be separated by a single space.

You can replace a character with %HEX.  
Example:  
Contents: backdoor%72 virus keep%20out

Result:  
1. backdoor  
2. virus  
3. keep out

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type a name for this profile, e.g., game. Type a name for this profile, e.g., game.
<b>Contents</b>	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.



## 4.8.8 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**.

[Objects Setting](#) => [Keyword Group](#)

Keyword Group Table: [Set to Factory Default](#)

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

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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](#)

Profile Index : 1

Name: \_\_\_\_\_

<p>Available Keyword Objects</p> <ul style="list-style-type: none"> <li>1-Key-1</li> <li>2-Key-2</li> </ul>	<p>Selected Keyword Objects(Max 16 Objects)</p> <div style="border: 1px solid black; height: 100px; margin-top: 10px;"></div>
---	---

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type a name for this group. Maximum 15 characters are allowed.
<b>Available Keyword Objects</b>	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.
<b>Selected Keyword Objects</b>	Click <input type="button" value="&gt;&gt;"/> button to add the selected Keyword objects in this box.

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

### 4.8.9 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 Object Profiles:](#) [Set to Factory Default](#)

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Index</b>	Display the profile number that you can configure.
<b>Name</b>	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 Profile column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> File Extension Object Setup

Profile Index: 1      Profile Name: |      |

Categories	File Extensions
<b>Image</b> <input type="button" value="Default"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .dib <input type="checkbox"/> .ico <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pct <input type="checkbox"/> .png <input type="checkbox"/> .tiff <input type="checkbox"/> .tiff <input type="checkbox"/> .tiff
<b>Video</b> <input type="button" value="Default"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .avi <input type="checkbox"/> .asf <input type="checkbox"/> .rm <input type="checkbox"/> .rm <input type="checkbox"/> .rm <input type="checkbox"/> .3gp <input type="checkbox"/> .3gp <input type="checkbox"/> .3gp <input type="checkbox"/> .3gp
<b>Audio</b> <input type="button" value="Default"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .aiff <input type="checkbox"/> .ac3 <input type="checkbox"/> .ram <input type="checkbox"/> .wav <input type="checkbox"/> .wav <input type="checkbox"/> .wma
<b>Text</b> <input type="button" value="Default"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .doc <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe <input type="checkbox"/> .jpe
<b>Archive</b> <input type="button" value="Default"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .zip <input type="checkbox"/> .rar <input type="checkbox"/> .rar

Completion      [Back](#)      [Cancel](#)      [OK](#)

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	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.

## 4.8.10 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**.

[Object Settings >> SMS / Mail Service Object](#)

SMS Provider		Mail Server	<a href="#">Set to Factory Default</a>
Index	Profile Name	SMS Provider	
<a href="#">1.</a>		<a href="#">kctams.com.tw (TW)</a>	
<a href="#">2.</a>		<a href="#">kct-eme.com.tw (TW)</a>	
<a href="#">3.</a>		<a href="#">kct-eme.com.tw (TW)</a>	
<a href="#">4.</a>		<a href="#">kctams.com.tw (TW)</a>	
<a href="#">5.</a>		<a href="#">kct-eme.com.tw (TW)</a>	
<a href="#">6.</a>		<a href="#">kct-eme.com.tw (TW)</a>	
<a href="#">7.</a>		<a href="#">kctams.com.tw (TW)</a>	
<a href="#">8.</a>		<a href="#">kct-eme.com.tw (TW)</a>	
<a href="#">9.</a>	Custom 1		
<a href="#">10.</a>	Custom 2		

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all of the settings and return to factory default settings.
<b>Index</b>	Display the profile number that you can configure.
<b>Profile</b>	Display the name for such SMS profile.
<b>SMS Provider</b>	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	
<a href="#">1.</a>		
<a href="#">2.</a>		
<a href="#">3.</a>		
<a href="#">4.</a>		

- The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	Time down
Service Provider	ktctsmc.com.tw (TW)
Username	lncf
Max-words	****
Quota	10
Sending Interval	3 (seconds)

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for such SMS profile. The maximum length of the name you can set is 31 characters.
<b>Service Provider</b>	Use the drop down list to specify the service provider which offers SMS service.
<b>Username</b>	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.
<b>Password</b>	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.
<b>Quota</b>	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.
<b>Sending Interval</b>	To avoid quota being exhausted soon, type time interval for sending the SMS.

- 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
1.	Time down	ktctsmc.com.tw (TW)
2.		ktctsmc.com.tw (TW)
3.		ktctsmc.com.tw (TW)
4.		ktctsmc.com.tw (TW)



<b>Username</b>	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.
<b>Password</b>	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.
<b>Quota</b>	Type the total number of the messages that the router will send out.
<b>Sending Interval</b>	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**.

[Object Settings >> SMS > Mail Service Object](#)

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

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all of the settings and return to factory default settings.
<b>Index</b>	Display the profile number that you can configure.
<b>Profile</b>	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.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
<b>Index</b>	
<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 Index: 1

Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	465
Sender Address	camer1@draytek.com
<input checked="" type="checkbox"/> Use SSL	
IP Authentication	
Username	john
Password	****
Sending Interval	0 (seconds)

OK Clear Cancel

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
<b>SMTP Server</b>	Type the IP address of the mail server. The maximum length of the name you can set is 63 characters.
<b>SMTP Port</b>	Type the port number for SMTP server.
<b>Sender Address</b>	Type the e-mail address of the sender.
<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.



<b>Authentication</b>	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.
<b>Sending Interval</b>	Define the interval for the system to send the SMS out.

- 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
<b>Index</b>	<b>Profile Name</b>	
1	Mail_Notify	
2		
3		

#### 4.8.11 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

Index	Profile Name	Settings	Set to Factory Default
1			
2			
3			
4			
5			
6			
7			
8			

Each item is explained as follows:

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

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
<a href="#">1.</a>	
<a href="#">2.</a>	
<a href="#">3.</a>	
<a href="#">4.</a>	
<a href="#">5.</a>	

2. The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Index: 1

Profile Name	Notify_atack	
Category	Status	
WAN	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected
VPN Tunnel	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected
Temperature Alert	<input type="checkbox"/> Out of Range	

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for such notification profile. The maximum length of the name you can set is 15 characters.
<b>Category</b>	Display the types that will be monitored.
<b>Status</b>	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

Index	Profile Name	Settings
<a href="#">1.</a>	Notify_atack	WAN VPN
<a href="#">2.</a>		
<a href="#">3.</a>		
<a href="#">4.</a>		

## 4.9 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 misuse 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.

<b>Note:</b> The priority of URL Content Filter is higher than Web Content Filter.
--

Objects Setting  
**CSM**  
 APP Enforcement Profile  
 URL Content Filter Profile  
 Web Content Filter Profile  
 DNS Filter  
 APPE Support List  
 Bandwidth Management

### 4.9.1 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

APP Enforcement Profile Table: | [Set to Factory Default](#) |

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

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Profile</b>	Display the number of the profile which allows you to click to set different policy.
<b>Name</b>	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**.

CSM >> APP Enforcement Profile

Profile Index: 1 Profile Name:

IM	P2P	Protocol	Others
<input type="checkbox"/> Select All <input type="checkbox"/> Clear All	<input type="checkbox"/> Support List	<input type="checkbox"/> Action	<input type="checkbox"/> Block <input type="checkbox"/> Pass
<input type="checkbox"/> DNS <input type="checkbox"/> DHCP <input type="checkbox"/> SSH <input type="checkbox"/> Oracle	<input type="checkbox"/> FTP <input type="checkbox"/> P2P <input type="checkbox"/> SSL/TLS <input type="checkbox"/> P2P Protocol	<input type="checkbox"/> HTTP <input type="checkbox"/> POP <input type="checkbox"/> TELNET <input type="checkbox"/> SSH	<input type="checkbox"/> IMAP <input type="checkbox"/> POP3 <input type="checkbox"/> MySQL <input type="checkbox"/> Oracle

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
<b>Select All</b>	Click it to choose all of the items in this page.
<b>Clear All</b>	Uncheck all the selected boxes.
<b>Support List</b>	Display the all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.
<b>Action</b>	<p><b>Block</b> – Block all the packets passing with the settings configured in this page.</p> <p><b>Pass</b> – Pass all the packets with the settings configured in this page.</p>

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**.

SD-WAN QoS Enforcement Profile

Profile Index: 1 Profile Name: |

DO	DDP	Webcam	Music
<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>		

Advanced Management				
Activity / Application	Host	Video/IM	Audio (VoIP)	IM
Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Messaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
File Transfer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Screen	<input type="checkbox"/>		<input type="checkbox"/>	
Conference (Video/Voice)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Other Activities	<input type="checkbox"/>	<input type="checkbox"/>		

IM Application				VoIP
<input type="checkbox"/> WhatsApp	<input type="checkbox"/> iMessage	<input type="checkbox"/> iChat	<input type="checkbox"/> WhatsApp (Voice)	<input type="checkbox"/> Skype
<input type="checkbox"/> Google Chat	<input type="checkbox"/> Xfire	<input type="checkbox"/> Gadu Gadu	<input type="checkbox"/> Paltalk	<input type="checkbox"/> Kubeo
<input type="checkbox"/> Jitsi	<input type="checkbox"/> QQ (IM/MSN)	<input type="checkbox"/> Tencent	<input type="checkbox"/> Mikrow	<input type="checkbox"/> Skype (V)
<input type="checkbox"/> Lave Lave	<input type="checkbox"/> QQ (V)	<input type="checkbox"/> QQ (V)	<input type="checkbox"/> UC	<input type="checkbox"/> TeamSpeak
<input type="checkbox"/> WeChat (IM)	<input type="checkbox"/> KakaoIM	<input type="checkbox"/> Line		

Webcam / Video (more than one address)				
<input type="checkbox"/> Webcam URL	<u>Webcam:</u> 002.000000 000.000000 <u>WebcamURL</u>	<u>Webcam:</u> 000.000000 0000.00 <u>WebcamURL</u>	<u>Webcam:</u> 00000000 00000000 <u>WebcamURL</u>	<u>Webcam:</u> 00000000 00000000 <u>WebcamURL</u>

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

CSM == APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	Misc																
<input type="button" value="Select All"/> <input type="button" value="Clear All"/>																			
<table border="1"> <thead> <tr> <th>Protocol</th> <th>Applications</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> eMule</td> <td>SoaSeek</td> </tr> <tr> <td><input type="checkbox"/> eDonkey</td> <td>eDonkey, eMule, Shareaza</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td>Kazaa, BearShare, Mosh</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td>KCrazy, FileFlot</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td>BearShare, Limewire, Shareaza, Foxy, KCrazy</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td>Lodotter, XNap, WinLop</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td>BitTorrent, BitSprint, BitComet</td> </tr> </tbody> </table>		Protocol	Applications	<input type="checkbox"/> eMule	SoaSeek	<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza	<input type="checkbox"/> eMule	Kazaa, BearShare, Mosh	<input type="checkbox"/> eMule	KCrazy, FileFlot	<input type="checkbox"/> eMule	BearShare, Limewire, Shareaza, Foxy, KCrazy	<input type="checkbox"/> eMule	Lodotter, XNap, WinLop	<input type="checkbox"/> eMule	BitTorrent, BitSprint, BitComet		
Protocol	Applications																		
<input type="checkbox"/> eMule	SoaSeek																		
<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza																		
<input type="checkbox"/> eMule	Kazaa, BearShare, Mosh																		
<input type="checkbox"/> eMule	KCrazy, FileFlot																		
<input type="checkbox"/> eMule	BearShare, Limewire, Shareaza, Foxy, KCrazy																		
<input type="checkbox"/> eMule	Lodotter, XNap, WinLop																		
<input type="checkbox"/> eMule	BitTorrent, BitSprint, BitComet																		
<table border="1"> <thead> <tr> <th colspan="5">Other P2P Applications</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> eXtreme</td> <td><input type="checkbox"/> Vuzaa</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> Cubbox</td> </tr> <tr> <td><input type="checkbox"/> eAres</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> Kuwo</td> </tr> </tbody> </table>				Other P2P Applications					<input type="checkbox"/> eXtreme	<input type="checkbox"/> Vuzaa	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> Cubbox	<input type="checkbox"/> eAres	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> Kuwo	
Other P2P Applications																			
<input type="checkbox"/> eXtreme	<input type="checkbox"/> Vuzaa	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> Cubbox															
<input type="checkbox"/> eAres	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> Kuwo															
<input type="button" value="OK"/> <input type="button" value="Cancel"/>																			

The items categorized under **Misc** -----

CSM == APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	Protocol	Misc																									
<input type="button" value="Select All"/> <input type="button" value="Clear All"/>																												
<table border="1"> <thead> <tr> <th colspan="5">Networking</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Cockatiel</td> <td><input type="checkbox"/> POPNet</td> <td><input type="checkbox"/> HTTP Proxy</td> <td><input type="checkbox"/> Tor</td> <td><input type="checkbox"/> VPN</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> Ring Tunnel</td> <td><input type="checkbox"/> TinyVPN</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> UltraVPN</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Networking					<input type="checkbox"/> Cockatiel	<input type="checkbox"/> POPNet	<input type="checkbox"/> HTTP Proxy	<input type="checkbox"/> Tor	<input type="checkbox"/> VPN	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> Ring Tunnel	<input type="checkbox"/> TinyVPN	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> UltraVPN	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule			
Networking																												
<input type="checkbox"/> Cockatiel	<input type="checkbox"/> POPNet	<input type="checkbox"/> HTTP Proxy	<input type="checkbox"/> Tor	<input type="checkbox"/> VPN																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> Ring Tunnel	<input type="checkbox"/> TinyVPN	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> UltraVPN																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																											
<table border="1"> <thead> <tr> <th colspan="5">Streaming</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> </tbody> </table>				Streaming					<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule
Streaming																												
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<table border="1"> <thead> <tr> <th colspan="5">Remote Control</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> </tbody> </table>				Remote Control					<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule					
Remote Control																												
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<table border="1"> <thead> <tr> <th colspan="5">Webcam</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> <tr> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> <td><input type="checkbox"/> eMule</td> </tr> </tbody> </table>				Webcam					<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule										
Webcam																												
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule	<input type="checkbox"/> eMule																								
<input type="button" value="OK"/> <input type="button" value="Cancel"/>																												

## 4.9.2 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.

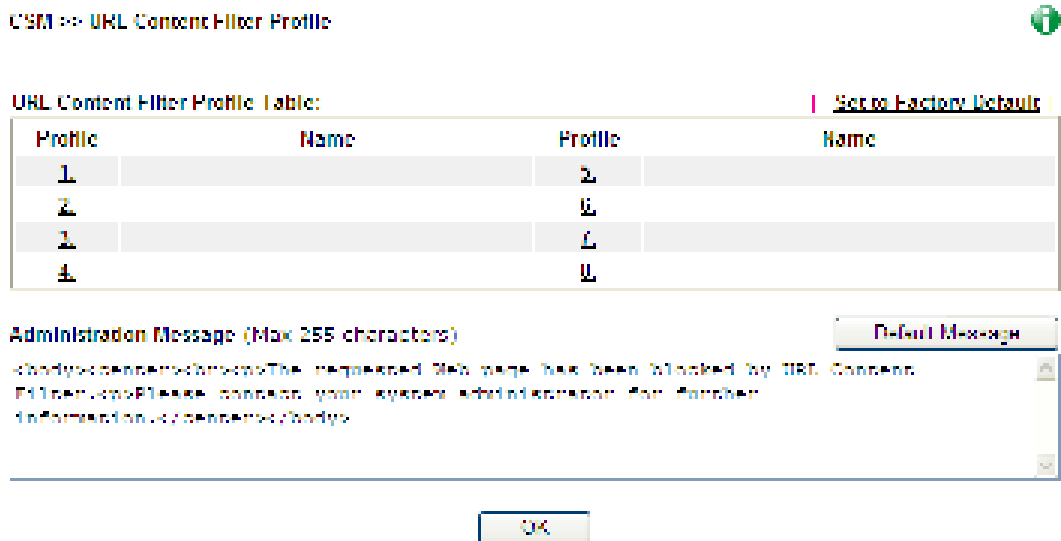
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines 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.



Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles.
<b>Profile</b>	Display the number of the profile which allows you to click to set different policy.
<b>Name</b>	Display the name of the URL Content Filter Profile.



<b>Administration Message</b>	<p>You can type the message manually for your necessity.</p> <p><b>Default Message</b> - You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of <b>Administration Message</b>.</p>
-------------------------------	--

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 Index: 1

Profile Name:

Priority:

**1. URL Access Control**

Enable URL Access Control       Prevent web access from IP address

Action:       Group/Object Selection:

**2. Web Feature**

Enable Restrict Web Feature

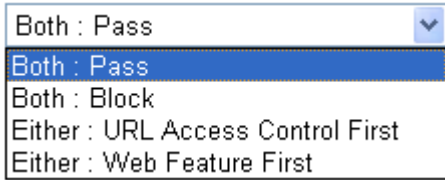
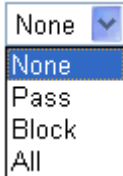

Action:

Cookie    Proxy    Upload File Extension Profile:

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
<b>Priority</b>	<p>It determines the action that this router will apply.</p> <p><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.</p> <p><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.</p> <p><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.</p> <p><b>Either: Web Feature First</b> –When all the packages</p>

	<p>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.</p> 
<p><b>Log</b></p>	<p><b>None</b> – There is no log file will be recorded for this profile.  <b>Pass</b> – Only the log about Pass will be recorded in Syslog.  <b>Block</b> – Only the log about Block will be recorded in Syslog.  <b>All</b> – All the actions (Pass and Block) will be recorded in Syslog.</p> 
<p><b>URL Access Control</b></p>	<p><b>Enable URL Access Control</b> - Check the box to activate URL Access Control. Note that the priority for <b>URL Access Control</b> is higher than <b>Restrict Web Feature</b>. 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.</p> <p><b>Prevent web access from IP address</b> - 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.</p> <p><b>Action</b> – This setting is available only when <b>Either : URL Access Control First</b> or <b>Either : Web Feature First</b> is selected.</p> <p><b>Pass</b> - Allow accessing into the corresponding webpage with the keywords listed on the box below.</p> <p><b>Block</b> - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action.</p> <p>Action:</p>  <p><b>Group/Object Selections</b> – The Vigor router provides several frames for users to define keywords and each frame</p>

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 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.

ObjectGroup Edit

### 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 First** 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.

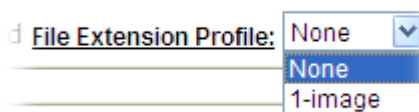
**Cookie** - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

**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.



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

### 4.9.3 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 <http://myvigor.draytek.com>.

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.



<b>Cache</b>	<p><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.</p> <p><b>L1</b> – 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.</p> <p><b>L2</b> – 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.</p> <p><b>L1+L2 Cache</b> – the router will check the URL with fast processing rate combining the feature of L1 and L2.</p>
--------------	---

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.

**CSM => Web Content Filter Profile**

Profile Index: 1  
 Profile Name:  Group Block

**Black/White List**

Enable

Action: Block

Address:  [Edit]

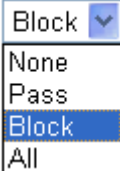
Action: Block

Group	Categories		
Child Protection <input type="button" value="View All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> Alcohol & Tobacco <input checked="" type="checkbox"/> Hate & Intolerance <input checked="" type="checkbox"/> Porn & Sexually <input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Criminal Activity <input checked="" type="checkbox"/> Illegal Drug <input checked="" type="checkbox"/> Violence <input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Gambling <input checked="" type="checkbox"/> Nudity <input checked="" type="checkbox"/> Weapons <input checked="" type="checkbox"/> Tobacco

All Websites	All Categories	All Profiles & Profiles
<input type="checkbox"/> News <input type="checkbox"/> Politics <input type="checkbox"/> Restaurants & Dining <input type="checkbox"/> General <input type="checkbox"/> Image Sharing <input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> Non-profits & NGOs <input type="checkbox"/> Real Estate <input type="checkbox"/> Shopping <input type="checkbox"/> Cults <input type="checkbox"/> Network Errors <input type="checkbox"/> Uncategorized Sites	<input type="checkbox"/> Personal Sites <input type="checkbox"/> Religion <input type="checkbox"/> Translators <input type="checkbox"/> Greeting cards <input type="checkbox"/> Parked Domains

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
<b>Black/White List</b>	<p><b>Enable</b> – Activate white/black list function for such profile.</p> <p><b>Group/Object Selections</b> – Click <b>Edit</b> to choose the group or object profile as the content of white/black list.</p> <p><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.</p> <p><b>Block - 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.</p>
<b>Action</b>	<p><b>Pass</b> - allow accessing into the corresponding webpage with the categories listed on the box below.</p> <p><b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.</p> <p>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</p>
<b>Log</b>	<p><b>None</b> – There is no log file will be recorded for this profile.</p> <p><b>Pass</b> – Only the log about Pass will be recorded in Syslog.</p> <p><b>Block</b> – Only the log about Block will be recorded in Syslog.</p> <p><b>All</b> – All the actions (Pass and Block) will be recorded in Syslog.</p> 

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

## 4.9.4 DNS Filter

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

**Note:** For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.

OSM >> DNS Filter

The screenshot shows a configuration window titled "DNS Filter". It contains the following settings:

- DNS Filter:** A checked checkbox.
- Syslog:** A dropdown menu currently set to "None".
- Service:** A dropdown menu currently set to "None".
- Cache Time(hour):** A dropdown menu currently set to "1".

At the bottom of the window are "OK" and "Cancel" buttons.

Available settings are explained as follows:

Item	Description
<b>DNS Filter</b>	Check Enable to enable such feature.
<b>Syslog</b>	<p>The filtering result can be recorded according to the setting selected for Syslog.</p> <p><b>None</b> – There is no log file will be recorded for this profile.</p> <p><b>Pass</b> – Only the log about Pass will be recorded in Syslog.</p> <p><b>Block</b> – Only the log about Block will be recorded in Syslog.</p> <p><b>All</b> – All the actions (Pass and Block) will be recorded in Syslog.</p>
<b>Service</b>	<p>Set the filtering conditions. Specify one of the WCF profiles as Service.</p> <p>Choose the WCF profiles to apply DNS filter.</p>
<b>Cache Time (hour)</b>	Set the time for DNS query.

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



## 4.9.5 APPE Support List

This page offers the software versions for each applications managed by APP Enforcement Profiles by Vigor router. Click the IM/P2P/PROTOCOL/MISC tab to open the information page for different APP type.

CSM >> APP Support List

This page lists out the APP information supported by Vigor routers (Vigor2925-2925-15).

IM	P2P	PROTOCOL	OTHERS
APP Type	APP Name	Version	Note
	AIM	1.4	
	AIM	2.0	Only model type 1 users have already updated AIM version, not be model 1.
	AIM2	2.0.1	
	AIM3	2.0.5	
	AIM4	2.0.1	
	AIM5	2.0.1	
	AIM6	2.0.1	
	AIM7	2.0.1	
	AIM8	2.0.1	
	AIM9	2.0.1	
	AIM10	2.0.1	
	AIM11	2.0.1	
	AIM12	2.0.1	
	AIM13	2.0.1	
	AIM14	2.0.1	
	AIM15	2.0.1	
	AIM16	2.0.1	
	AIM17	2.0.1	
	AIM18	2.0.1	
	AIM19	2.0.1	
	AIM20	2.0.1	
	AIM21	2.0.1	
	AIM22	2.0.1	
	AIM23	2.0.1	
	AIM24	2.0.1	
	AIM25	2.0.1	
	AIM26	2.0.1	
	AIM27	2.0.1	
	AIM28	2.0.1	
	AIM29	2.0.1	
	AIM30	2.0.1	
	AIM31	2.0.1	
	AIM32	2.0.1	
	AIM33	2.0.1	
	AIM34	2.0.1	
	AIM35	2.0.1	
	AIM36	2.0.1	
	AIM37	2.0.1	
	AIM38	2.0.1	
	AIM39	2.0.1	
	AIM40	2.0.1	
	AIM41	2.0.1	
	AIM42	2.0.1	
	AIM43	2.0.1	
	AIM44	2.0.1	
	AIM45	2.0.1	
	AIM46	2.0.1	
	AIM47	2.0.1	
	AIM48	2.0.1	
	AIM49	2.0.1	
	AIM50	2.0.1	
	AIM51	2.0.1	
	AIM52	2.0.1	
	AIM53	2.0.1	
	AIM54	2.0.1	
	AIM55	2.0.1	
	AIM56	2.0.1	
	AIM57	2.0.1	
	AIM58	2.0.1	
	AIM59	2.0.1	
	AIM60	2.0.1	
	AIM61	2.0.1	
	AIM62	2.0.1	
	AIM63	2.0.1	
	AIM64	2.0.1	
	AIM65	2.0.1	
	AIM66	2.0.1	
	AIM67	2.0.1	
	AIM68	2.0.1	
	AIM69	2.0.1	
	AIM70	2.0.1	
	AIM71	2.0.1	
	AIM72	2.0.1	
	AIM73	2.0.1	
	AIM74	2.0.1	
	AIM75	2.0.1	
	AIM76	2.0.1	
	AIM77	2.0.1	
	AIM78	2.0.1	
	AIM79	2.0.1	
	AIM80	2.0.1	
	AIM81	2.0.1	
	AIM82	2.0.1	
	AIM83	2.0.1	
	AIM84	2.0.1	
	AIM85	2.0.1	
	AIM86	2.0.1	
	AIM87	2.0.1	
	AIM88	2.0.1	
	AIM89	2.0.1	
	AIM90	2.0.1	
	AIM91	2.0.1	
	AIM92	2.0.1	
	AIM93	2.0.1	
	AIM94	2.0.1	
	AIM95	2.0.1	
	AIM96	2.0.1	
	AIM97	2.0.1	
	AIM98	2.0.1	
	AIM99	2.0.1	
	AIM100	2.0.1	

## 4.10 Bandwidth Management

Below shows the menu items for Bandwidth Management.



### 4.10.1 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.

**Bandwidth Management** > **Sessions Limit**

**Sessions Limit**

Enable  Disable

Default Max Sessions:

**Session List**

Index	Start IP	End IP	Max Sessions

Special Condition

Start IP:  End IP:

Maximum Sessions:

Administration Message (Max 255 characters)

**Time Schedule**

Index(1-10) in Schedule Setup:

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit session, simply click **Enable** and set the default session limit.

Available settings are explained as follows:

Item	Description
<b>Session Limit</b>	<p><b>Enable</b> - Click this button to activate the function of limit session.</p> <p><b>Disable</b> - Click this button to close the function of limit session.</p>

	<b>Default session limit</b> - Defines the default session number used for each computer in LAN.
<b>Limitation List</b>	Displays a list of specific limitations that you set on this web page.
<b>Specific Limitation</b>	<p><b>Start IP</b>- Defines the start IP address for limit session.</p> <p><b>End IP</b> - Defines the end IP address for limit session.</p> <p><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.</p> <p><b>Add</b> - Adds the specific session limitation onto the list above.</p> <p><b>Edit</b> - Allows you to edit the settings for the selected limitation.</p> <p><b>Delete</b> - Remove the selected settings existing on the limitation list.</p>
<b>Administration Message</b>	<p>Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p><b>Default Message</b> - Click this button to apply the default message offered by the router.</p>
<b>Time Schedule</b>	<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 &gt;&gt; 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.



	<p>downstream for each computer in LAN.</p> <p><b>Allow auto adjustment</b>...- Check this box to make the best utilization of available bandwidth.</p>
<b>Limitation List</b>	<p>Display a list of specific limitations that you set on this web page.</p>
<b>Specific Limitation</b>	<p><b>Start IP</b> - Define the start IP address for limit bandwidth.</p> <p><b>End IP</b> - Define the end IP address for limit bandwidth.</p> <p><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.</p> <p><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.</p> <p><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.</p> <p><b>Add</b> - Add the specific speed limitation onto the list above.</p> <p><b>Edit</b> - Allow you to edit the settings for the selected limitation.</p> <p><b>Delete</b> - Remove the selected settings existing on the limitation list.</p>
<b>Smart Bandwidth Limit</b>	<p>Check this box to have the bandwidth limit determined by the system automatically.</p> <p><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.</p> <p><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.</p>
<b>Time Schedule</b>	<p><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 &gt;&gt; Schedule</b> web page and you can use the number that you have set in that web page.</p>

### 4.10.3 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?

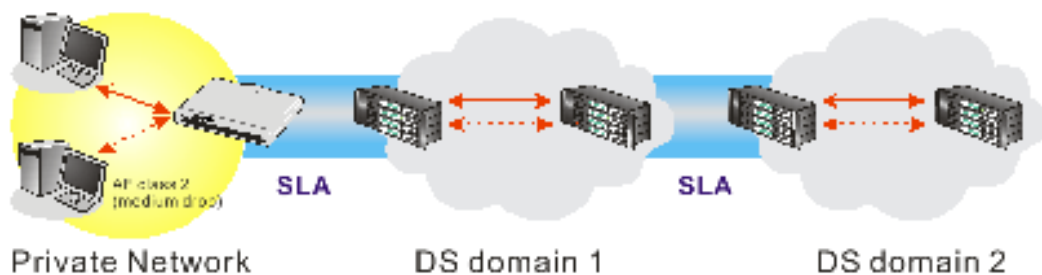
There are two components within Primary configuration of QoS deployment:

- **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 Set to Factory Default

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	1000000Kbps/1000000Kbps	Inbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps	Outbound	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
Class 1		<a href="#">Edit</a>	
Class 2		<a href="#">Edit</a>	<a href="#">Edit</a>
Class 3		<a href="#">Edit</a>	

Enable the First Priority for VoIP SIP/RTP

SIP UDP Port: 2020    |    SIP UDP Port: 5060

Available settings are explained as follows:

Item	Description
<b>General Setup</b>	<p><b>Index</b> - Display the WAN interface number that you can edit.</p> <p><b>Status</b> - Display if the WAN interface is available for such function or not.</p> <p><b>Bandwidth</b> - Display the inbound and outbound bandwidth setting for the WAN interface.</p> <p><b>Direction</b> - Display which direction that such function will influence.</p> <p><b>Class 1/Class2/Class 3/Others</b> - Display the bandwidth percentage for each class.</p> <p><b>UDP Bandwidth Control</b> - Display the UDP bandwidth control is enabled or not.</p> <p><b>Online Statistics</b> - Display an online statistics for quality of service for your reference</p> <p><b>Setup</b> - Allow to configure general QoS setting for WAN interface.</p>
<b>Class Rule</b>	<p><b>Index</b> - Display the class number that you can edit.</p> <p><b>Name</b> - Display the name of the class.</p> <p><b>Rule</b> - Allow to configure detailed settings for the selected Class.</p> <p><b>Service Type</b> - Allow to configure detailed settings for the service type.</p>
<b>Enable the First Priority for VoIP SIP/RTP</b>	<p>When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority.</p> <p><b>SIP UDP Port</b> - Set a port number used for SIP.</p>

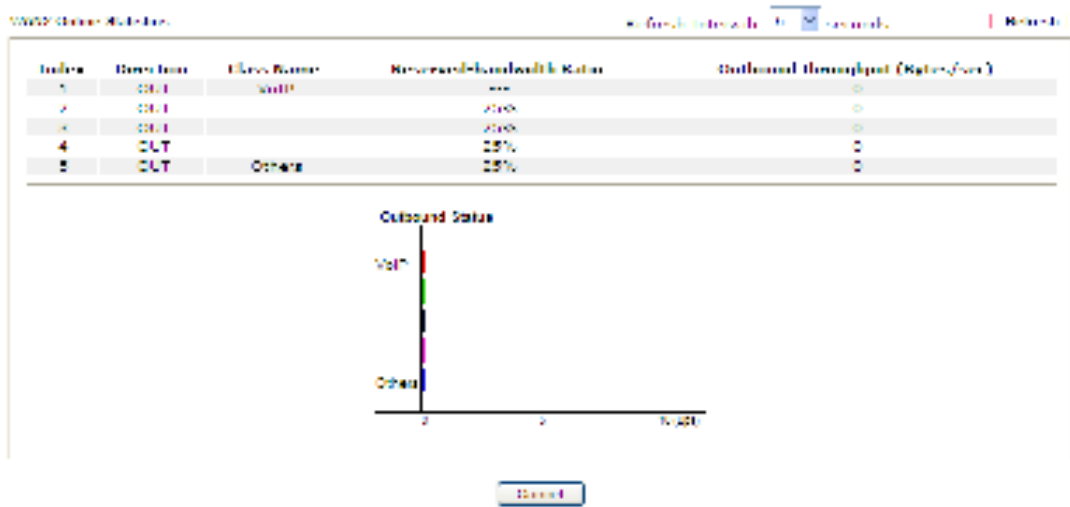
This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

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.

Bandwidth Management >> Quality of Service



## General Setup for WAN Interface

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.

Bandwidth Management >> Quality of Service

WAN2 General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth:  Kbps

WAN Outbound Bandwidth:  Kbps

Index	Class Name	Reserved_Bandwidth Ratio
Class 1		<input type="text" value="25"/> %
Class 2		<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable TCP Bandwidth Control Enabled Bandwidth Ratio: 25 %

Enable TCP ACK Priority



Available settings are explained as follows:

Item	Description
<b>Enable the QoS Control</b>	<p>The factory default for this setting is checked.</p> <p>Please also define which traffic the QoS Control settings will apply to.</p> <p><b>IN</b> - apply to incoming traffic only.</p> <p><b>OUT</b> - apply to outgoing traffic only.</p> <p><b>BOTH</b> - apply to both incoming and outgoing traffic.</p> <p>Check this box and click <b>OK</b>, then click <b>Setup</b> link again. You will see the <b>Online Statistics</b> link appearing on this page.</p>
<b>WAN Inbound Bandwidth</b>	<p>It allows you to set the connecting rate of data input for WAN interface. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.</p>
<b>WAN Outbound Bandwidth</b>	<p>It allows you to set the connecting rate of data output for WAN interface. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.</p>
<b>Reserved Bandwidth Ratio</b>	<p>It is reserved for the group index in the form of ratio of <b>reserved bandwidth to upstream speed</b> and <b>reserved bandwidth to downstream speed</b>.</p>
<b>Enable UDP Bandwidth Control</b>	<p>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.</p>
<b>Outbound TCP ACK Prioritize</b>	<p>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.</p>
<b>Limited_bandwidth Ratio</b>	<p>The ratio typed here is reserved for limited bandwidth of UDP application.</p>

**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

- 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.

Bandwidth Management >> Quality of Service

General Setup Set to Factory Default

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	WRR Bandwidth Control	Online Statistics
WAN1	Disable	1000000Kbps/1000000Kbps	Inbound	25%	25%	25%	25%	Inactive	Status <a href="#">Setup</a>
WAN2	Disable	1000000Kbps/1000000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status <a href="#">Setup</a>
WAN3	Disable	1000000Kbps/1000000Kbps		25%	25%	25%	25%	Inactive	Status <a href="#">Setup</a>

Class Rule

Index	Name	Rule	Service Type
Class 1		<a href="#">Edit</a>	
Class 2		<a href="#">Edit</a>	<a href="#">Edit</a>
Class 3		<a href="#">Edit</a>	

Enable the Test Priority for VoIP SIP/UDP  
 SIP UDP Port: 5060 (ip=6.6.6.6)

- 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.

Bandwidth Management >> Quality of Service

Class Index #1

Name:   Log packets to: Default

ID	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty				

- For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit

IP ACT  Hardware Acceleration

Ethernet Type:  IPv4  IPv6

Local Address:

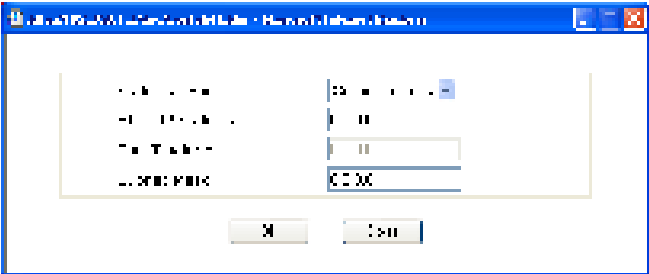
Remote Address:

DiffServ CodePoint:

Service Type:

Note: Please choose/setup the Service Type first.

Available settings are explained as follows:

Item	Description
<b>ACT</b>	Check this box to invoke these settings.
<b>Hardware Acceleration</b>	Check this box to enable the hardware acceleration when such rule is applied.
<b>Ethernet Type</b>	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
<b>Local Address</b>	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.
<b>Remote Address</b>	<p>Click the <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.</p>  <p><b>Address Type</b> – Determine the address type for the source address.</p> <p>For <b>Single Address</b>, you have to fill in Start IP address.</p> <p>For <b>Range Address</b>, you have to fill in Start IP address and End IP address.</p> <p>For <b>Subnet Address</b>, you have to fill in Start IP address and Subnet Mask.</p>
<b>DiffServ CodePoint</b>	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.
<b>Service Type</b>	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.

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.

[Bandwidth Management](#) >> [Quality of Service](#)

Class Index #1  
 Name:   Log packets as:

NO	Status	Local Address	Remote Address	Diffserv CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	ANY
2 <input checked="" type="radio"/>	Active	192.168.1.12	192.168.1.0/24	ANY	ANY

### Edit the Service Type for Class Rule

- 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

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	DSP Bandwidth Control	Online Statistics
WAN1	Disable	100000Kbps/100000Kbps	Inbound	20%	25%	20%	25%	Inactive	Monitor <input type="button" value="Setup"/>
WAN2	Disable	100000Kbps/100000Kbps	Outbound	20%	25%	20%	25%	Inactive	Status <input type="button" value="Setup"/>
WAN3	Disable	100000Kbps/100000Kbps		20%	25%	20%	25%	Inactive	Status <input type="button" value="Setup"/>

Class Rule

Index	Name	Rule	Service Type
Class 1		<a href="#">Edit</a>	<a href="#">Edit</a>
Class 2		<a href="#">Edit</a>	
Class 3		<a href="#">Edit</a>	

Enable the DSCP Priority for VoIP SIP/RTSP

VoIP DSCP Mark:

- 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		

- For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

---

Service Type Edit

Service Name

Service Type

Port Configuration

Type  Single  Range

Port Number  -

Available settings are explained as follows:

Item	Description
<b>Service Name</b>	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
<b>Service Type</b>	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
<b>Port Configuration</b>	<p><b>Type</b> - Click <b>Single</b> or <b>Range</b> as the <b>Type</b>. If you select <b>Range</b>, you have to type in the starting port number and the end porting number on the boxes below.</p> <p><b>Port Number</b> – Type in the starting port number and the end porting number here if you choose <b>Range</b> as the type.</p>

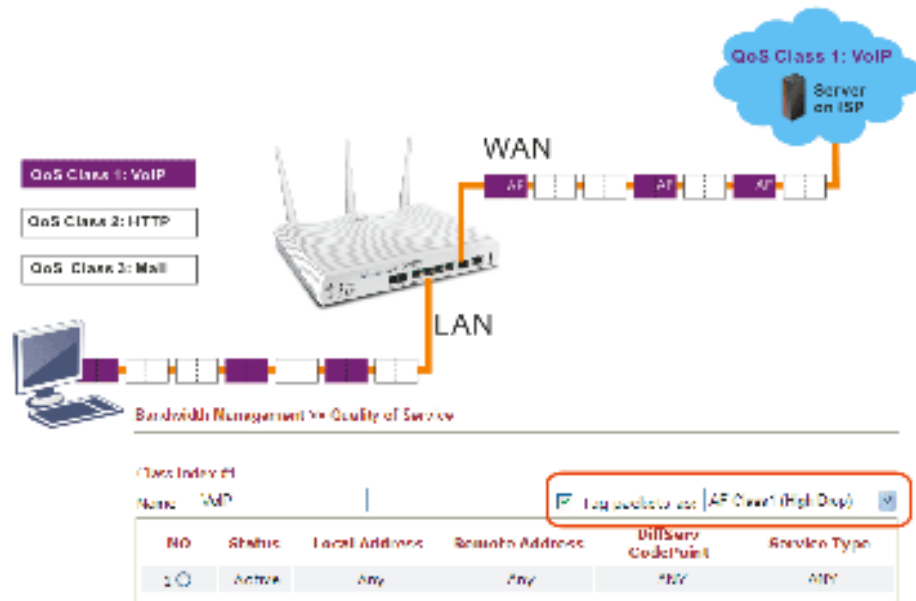
- After finishing all the settings here, please click **OK** to save the configuration.

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/Delete** for modification.

### Retag the Packets for Identification

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



## 4.11 Applications

Below shows the menu items for Applications.



### 4.11.1 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](http://www.dyndns.org), [www.no-ip.com](http://www.no-ip.com), [www.dtdns.com](http://www.dtdns.com), [www.changeip.com](http://www.changeip.com), [www.dynamic-nameserver.com](http://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*.

- In the DDNS setup menu, check **Enable Dynamic DNS Setup**.

Applications » Dynamic DNS Setup

---

Dynamic DNS Setup | Set to Factory Default

Enable Dynamic DNS Setup View Log Force Update

Auto-Update Interval:  Min(s) (1-14400)

Accounts:

Index	WAN Interface	Domain Name	Action
1.	WAN1 (eth1)		x
2.	WAN1 (eth1)		x
3.	WAN1 (eth1)		x

OK Clear All

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles and recover to factory settings.
<b>Enable Dynamic DNS Setup</b>	Check this box to enable DDNS function.
<b>View Log</b>	Display DDNS log status.
<b>Force Update</b>	Force the router updates its information to DDNS server.
<b>Auto-Update interval</b>	Set the time for the router to perform auto update for DDNS service.
<b>Index</b>	Click the number below Index to access into the setting page of DDNS setup to set account(s).
<b>WAN Interface</b>	Display the WAN interface used.
<b>Domain Name</b>	Display the domain name that you set on the setting page of DDNS setup.
<b>Active</b>	Display if this account is active or inactive.

- 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*.

Index: 1

Enable Dynamic DNS Account

WAN Interface: WAN1 First

Service Provider: dynamic.org (new dynamic.org)

Service Type: Dynamic

Domain Name: dynamic.org dynamic.org

Login Name: dynamic008 (max. 64 characters)

Password: \*\*\*\*\* (max. 28 characters)

Wildcards

Backup MX

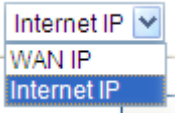
Mail Extender:

Determine Default WAN IP: InternetIP

Available settings are explained as follows:

Item	Description
<b>Enable Dynamic DNS Account</b>	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).
<b>WAN Interface</b>	<p><b>WAN1/WAN2/WAN3 First</b> - 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.</p> <p><b>WAN1/WAN2/WAN3 Only</b> - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account.</p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <p>WAN1 First</p> <p style="background-color: #e0e0e0;">WAN1 First</p> <p>WAN1 Only</p> <p>WAN2 First</p> <p>WAN2 Only</p> <p>WAN3 First</p> <p>WAN3 Only</p> </div>
<b>Service Provider</b>	Select the service provider for the DDNS account.
<b>Service Type</b>	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.
<b>Domain Name</b>	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
<b>Login Name</b>	Type in the login name that you set for applying domain.
<b>Password</b>	Type in the password that you set for applying domain.
<b>Wildcard and Backup MX</b>	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.



<b>Mail Extender</b>	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.
<b>Determine Real WAN IP</b>	<p>If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP.</p> <p>When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.</p> <p>There are two methods offered for you to choose:</p>  <p><b>WAN IP</b> - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.</p> <p><b>Internet IP</b> - If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.</p>

- 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.

### 4.11.2 LAN DNS

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

Applications >> LAN DNS

LAN DNS Description Set to Factory Default

Enable	Index	Profile	Domain Name
<input type="checkbox"/>	1		
<input type="checkbox"/>	2		
<input type="checkbox"/>	3		
<input checked="" type="checkbox"/>	4		
<input type="checkbox"/>	5		
<input type="checkbox"/>	6		
<input checked="" type="checkbox"/>	7		
<input type="checkbox"/>	8		
<input type="checkbox"/>	9		
<input checked="" type="checkbox"/>	10		

<< 1 10 | 11 20 >>

**OK**

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles and recover to factory settings.
<b>Enable</b>	Check the box to enable the selected profile.
<b>Index</b>	Click the number below Index to access into the setting page of schedule.
<b>Profile</b>	Display the name of the LAN DNS profile.
<b>Domain Name</b>	Display the domain name of the LAN DNS profile.

You can set up to 20 LAN DNS profiles.

To create a LAN DNS profile:

1. Click any index, say Index No. 1.
2. The detailed settings of the call schedule with index 1 are shown below.

[Applications >> LAN DNS](#)

**Profile Index : 1**

Enable

Profile: \_\_\_\_\_

Domain Name: \_\_\_\_\_

IP Address List

Index	IP Address	Gate	Forward	Reply

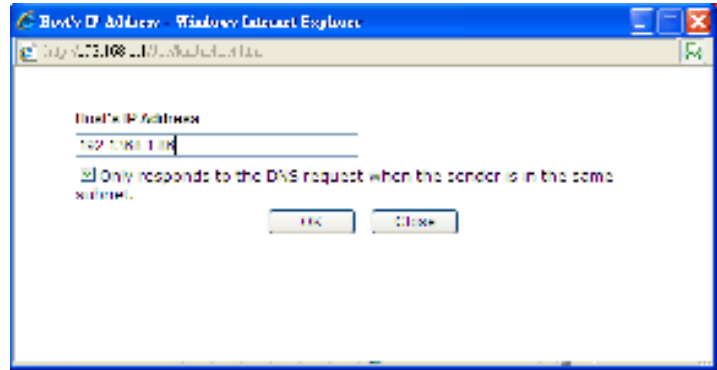
Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check this box to enable such profile.
<b>Profile</b>	Type a name for such profile.
<b>Domain Name</b>	Type the domain name for such profile.

### IP Address List

The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name..

**Add** – Click it to open a dialog to type the host's IP address.



**Only responds to the DNS....** – Different LAN PCs can share the same domain name. However, you have to check this box to make the router identify & respond the IP address for the DNS query coming from different LAN PC.

**Delete** – Click it to remove an existed IP address on the list.

3. Click **OK** button to save the settings.
4. A new LAN DNS profile has been created.

Applications >> LAN DNS

Enable	Index	Profile	Domain Name
<input checked="" type="checkbox"/>	1	192.168.1.10	www.draytek.com
<input type="checkbox"/>	2		
<input type="checkbox"/>	3		
<input type="checkbox"/>	4		
<input type="checkbox"/>	5		
<input type="checkbox"/>	6		
<input type="checkbox"/>	7		
<input type="checkbox"/>	8		
<input type="checkbox"/>	9		
<input type="checkbox"/>	10		

1-10 | 11-20 >>

OK

### 4.11.3 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.

[Applications >> Schedule](#)

Schedule:				<a href="#">Set to Factory Default</a>
Index	Status	Index	Status	
<a href="#">1.</a>	=	<a href="#">9.</a>	x	
<a href="#">2.</a>	=	<a href="#">10.</a>	x	
<a href="#">3.</a>	=	<a href="#">11.</a>	x	
<a href="#">4.</a>	=	<a href="#">12.</a>	x	
<a href="#">5.</a>	x	<a href="#">13.</a>	x	
<a href="#">6.</a>	x	<a href="#">14.</a>	x	
<a href="#">7.</a>	x	<a href="#">15.</a>	x	
<a href="#">8.</a>	x			

Status: = Active, x Inactive

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Clear all profiles and recover to factory settings.
<b>Index</b>	Click the number below Index to access into the setting page of schedule.
<b>Status</b>	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](#)

Index No. 1

Enable Schedule Setup

Start Date (yyyy-mm-dd)    2005   1   1

Start Time (hh:mm)    0 : 0

Duration Time (Hours)    0 : 0

Action    Force On

Idle Timeout    0    minute(x).(max.: 255, 0 for default)

How Often

Once

Weekdays

Sun    Mon    Tue    Wed    Thu    Fri    Sat

OK   Clear   Cancel

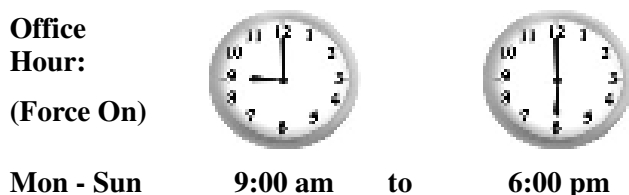
Available settings are explained as follows:

Item	Description
<b>Enable Schedule Setup</b>	Check to enable the schedule.
<b>Start Date (yyyy-mm-dd)</b>	Specify the starting date of the schedule.
<b>Start Time (hh:mm)</b>	Specify the starting time of the schedule.
<b>Duration Time (hh:mm)</b>	Specify the duration (or period) for the schedule.
<b>Action</b>	Specify which action Call Schedule should apply during the period of the schedule. <b>Force On</b> -Force the connection to be always on. <b>Force Down</b> -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.
<b>Idle Timeout</b>	Specify the duration (or period) for the schedule. <b>How often</b> -Specify how often the schedule will be applied <b>Once</b> -The schedule will be applied just once <b>Weekdays</b> -Specify which days in one week should perform the schedule.

- 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).



- Make sure the PPPoE connection and **Time Setup** is working properly.
- Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 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.

## 4.11.4 RADIUS

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

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

Applications >> RADIUS

**RADIUS Setup**

<input checked="" type="checkbox"/> Enable	
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable RADIUS client feature.
<b>Server IP Address</b>	Enter the IP address of RADIUS server
<b>Destination Port</b>	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
<b>Shared Secret</b>	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.
<b>Confirm Shared Secret</b>	Re-type the Shared Secret for confirmation.

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

## 4.11.5 Active Directory/ LDAP

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.

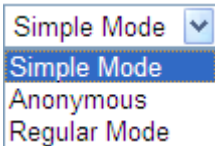
### General Setup

This page allows you to create several profiles, enable the function and specify general settings for LDAP server.

Applications >> Active Directory /LDAP

Note: After finishing the configuration of the LDAP profiles, they will be listed in the page of VPN and Remote Access >> [PPP General Setup](#). If you want to use the profiles for VPN authentication, check the boxes under PPP LDAP Profiles in VPN and Remote Access >> PPP General Setup list.

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check to enable such function.
<b>Bind Type</b>	<p>There are three types of bind type supported.</p>  <p><b>Simple Mode</b> – Just simply do the bind authentication without any search action.</p> <p><b>Anonymous</b> – Perform a search action first with Anonymous account then do the bind authentication.</p> <p><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.</p> <p>For the regular mode, you'll need to type in the <b>Regular DN</b> and <b>Regular Password</b>.</p>
<b>Server IP Address</b>	Enter the IP address of LDAP server.
<b>Destination Port</b>	Type a port number as the destination port for LDAP server.
<b>Use SSL</b>	Check the box to use the port number specified for SSL.

<b>Regular DN</b>	Type this setting if <b>Regular Mode</b> is selected as <b>Bind Type</b> .
<b>Regular Password</b>	Specify a password if <b>Regular Mode</b> is selected as <b>Bind Type</b> .

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 /LDAP [Set to Factory Default](#)

General Setup	Active Directory / LDAP Profiles
---------------	----------------------------------

Index	Name	Distinguished Name
1		
2		
3		
4		
5		
6		
7		
8		

Note: After clicking the configuration item, the link on the left will be issued on the page of VPN and Remote Access >> PPP General Setup. If you want to use the link for PPP authentication, click the link on the left on the page of VPN and Remote Access >> PPP General Setup.

Click any index number link to open the following page.


Applications >> Active Directory /LDAP >> Server Profiles

Index No. 1

Name	RDI
Common Name Identifier	ULI
Base Distinguished Name	
Additional Filter	
Note: Please type in your additional filter for LDAP search request. For example, 1) For OpenLDAP: (gidNumber=100) 2) For AD: (memberOf=CN=100)	
Group Distinguished Name	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Available settings are explained as follows:



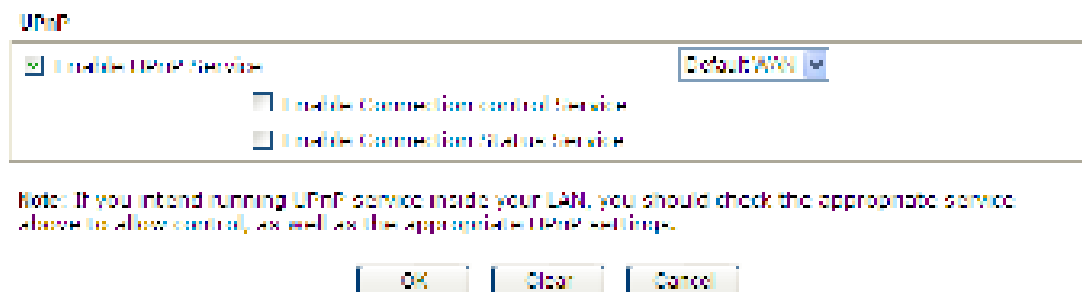
Item	Description
<b>Name</b>	Type a name for such profile.
<b>Common Name Identifier</b>	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is “cn”.
<b>Base Distinguished Name / Group Distinguished Name</b>	Type or edit the distinguished name 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  button to list all the account information on the AD/LDAP Server to assist you finish the setup.

After finished the above settings, click **OK** to save and exit this page. A new profile has been created.

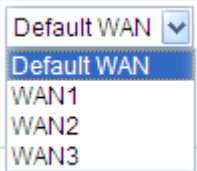
#### 4.11.6 UPnP

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.

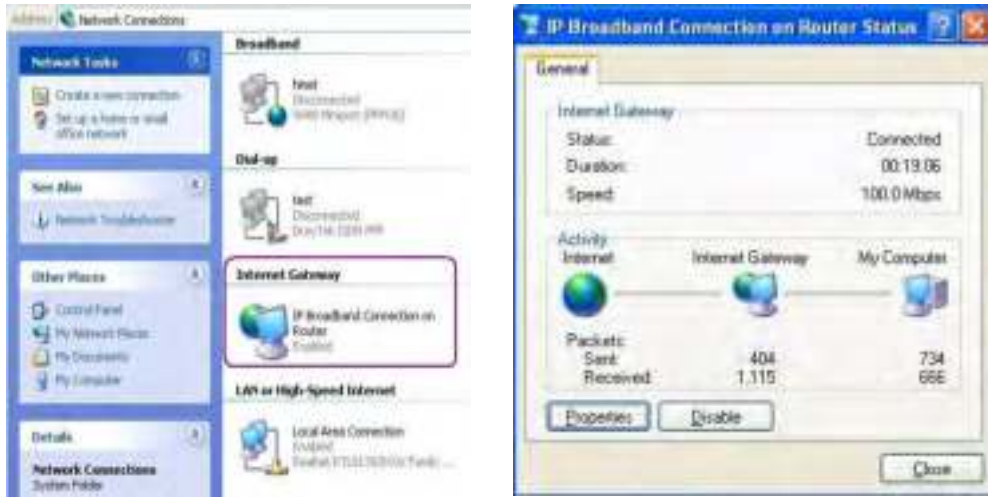
Applications >> UPnP



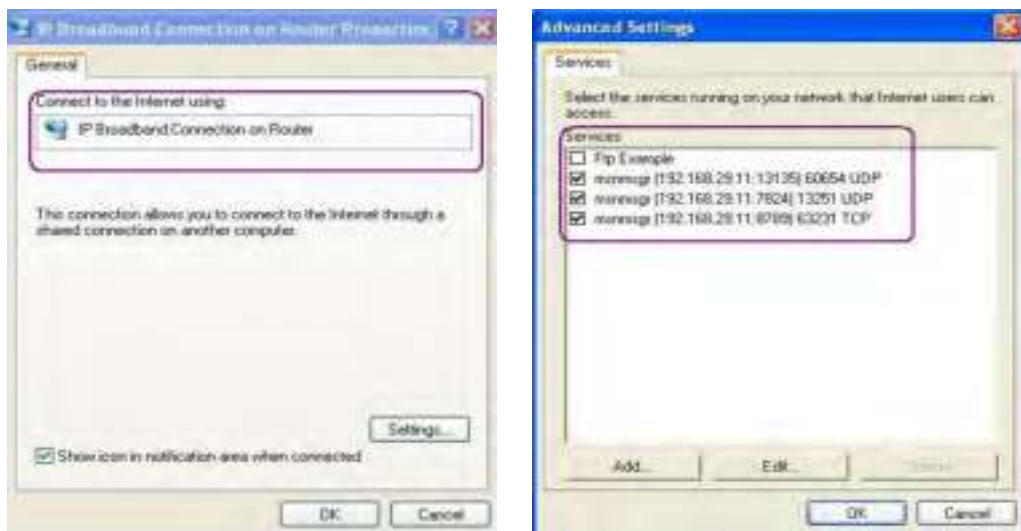
Available settings are explained as follows:

Item	Description
<b>Enable UPNP Service</b>	Accordingly, you can enable either the <b>Connection Control Service</b> or <b>Connection Status Service</b> .
<b>Default WAN</b>	It is used to specify the WAN interface for applying such function.  

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.



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



The reminder as regards concern about Firewall and UPnP

**Can't work with Firewall Software**  
 Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

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

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

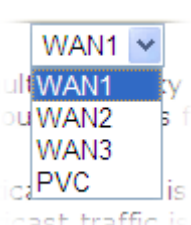
The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

#### 4.11.7 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

Available settings are explained as follows:

Item	Description
<b>Enable IGMP Proxy</b>	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. 
<b>Enable IGMP Snooping</b>	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.
<b>Refresh</b>	Click this link to renew the working multicast group status.
<b>Group ID</b>	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.
<b>P1 to P5</b>	It indicates the LAN port used for the multicast group.

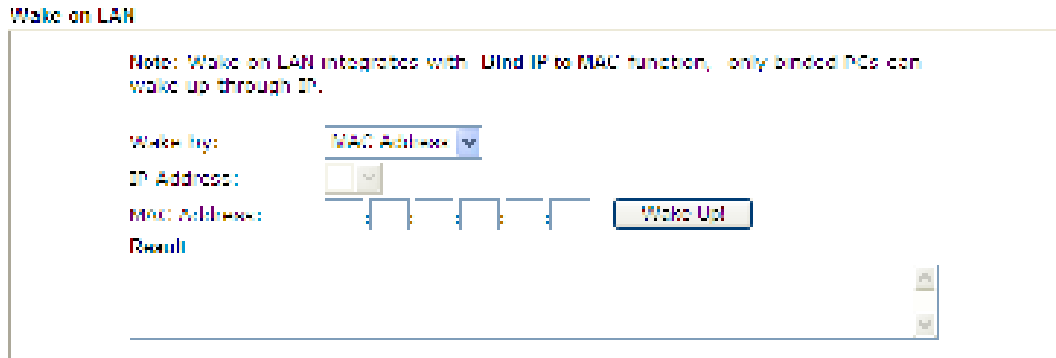
After finishing all the settings here, please click **OK** to save the configuration.

### 4.11.8 Wake on LAN

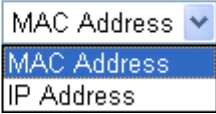
A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** (WOL) of this router.

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



Available settings are explained as follows:

Item	Description
<b>Wake by</b>	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: 
<b>IP Address</b>	The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
<b>MAC Address</b>	Type any one of the MAC address of the bound PCs.
<b>Wake Up</b>	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**

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

Wake by: MAC Address

IP Address: \_\_\_\_\_

MAC Address: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_ Wake Up!

Result: and pressed to change time

### 4.11.9 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.

Application => SMS / Mail Alert Service

**SMS Provider** Mail Server Set to Factory Default

Index	SMS Provider	Recipient	Notify Profile	Schedule (1-24)
1 <input checked="" type="checkbox"/>	1 Line down		1 Notify attack	
2 <input type="checkbox"/>	1 Line down		1 Notify attack	
3 <input type="checkbox"/>	1 Line down		1 Notify attack	
4 <input type="checkbox"/>	1 Line down		1 Notify attack	
5 <input type="checkbox"/>	1 Line down		1 Notify attack	
6 <input type="checkbox"/>	1 Line down		1 Notify attack	
7 <input type="checkbox"/>	1 Line down		1 Notify attack	
8 <input type="checkbox"/>	1 Line down		1 Notify attack	
9 <input type="checkbox"/>	1 Line down		1 Notify attack	
10 <input type="checkbox"/>	1 Line down		1 Notify attack	

OK Cancel

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.

<b>Recipient</b>	Type the name of the one who will receive the SMS.
<b>Notify</b>	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.
<b>Schedule</b>	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.

Application => SMS / Mail Alert Service

Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)
1 <input checked="" type="checkbox"/>	1 Mail_Notify		1 Notify_attack	
2 <input type="checkbox"/>	1 Mail_Notify		1 Notify_attack	
3 <input type="checkbox"/>	1-Mail_Notify		1-Notify_attack	
4 <input type="checkbox"/>	1-Mail_Notify		1-Notify_attack	
5 <input type="checkbox"/>	1 Mail_Notify		1 Notify_attack	
6 <input type="checkbox"/>	1 Mail_Notify		1 Notify_attack	
7 <input type="checkbox"/>	1 Mail_Notify		1 Notify_attack	
8 <input type="checkbox"/>	1-Mail_Notify		1-Notify_attack	
9 <input type="checkbox"/>	1-Mail_Notify		1-Notify_attack	
10 <input type="checkbox"/>	1 Mail_Notify		1 Notify_attack	

Available settings are explained as follows:

Item	Description
<b>Index</b>	Check the box to enable such profile.
<b>Mail Service</b>	Use the drop down list to choose mail service provider. You can click <b>Mail Service</b> link to define the mail server.
<b>Recipient</b>	Type the e-mail address of the one who will receive the notification message.
<b>Notify</b>	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.

<b>Schedule</b>	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.

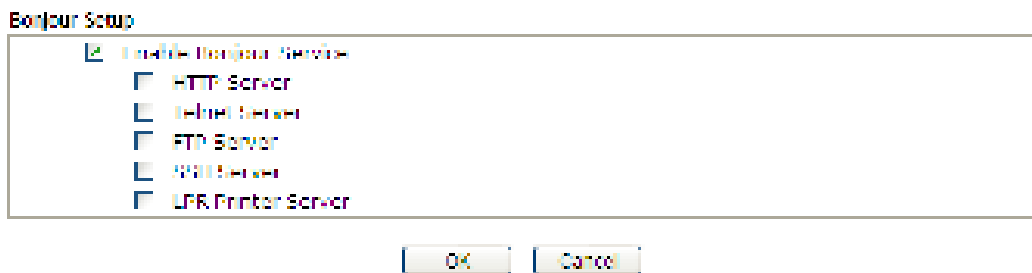
### 4.11.10 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there are correspondent softwares to enable this function for free.

Usually, users have to configure the router or personal computers to use above services. Sometimes, the configuration (e.g., IP settings, port number) is complicated and not easy to complete. The purpose of Bonjour is to decrease the settings configuration (e.g., IP setting). If the host and user's computer have the plug-in Bonjour driver install, they can utilize the service offered by the router by clicking the router name icon. In short, what the Clients/users need to know is the name of the router only.

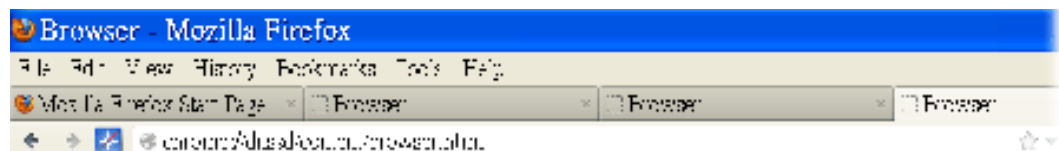
To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

Applications => Bonjour

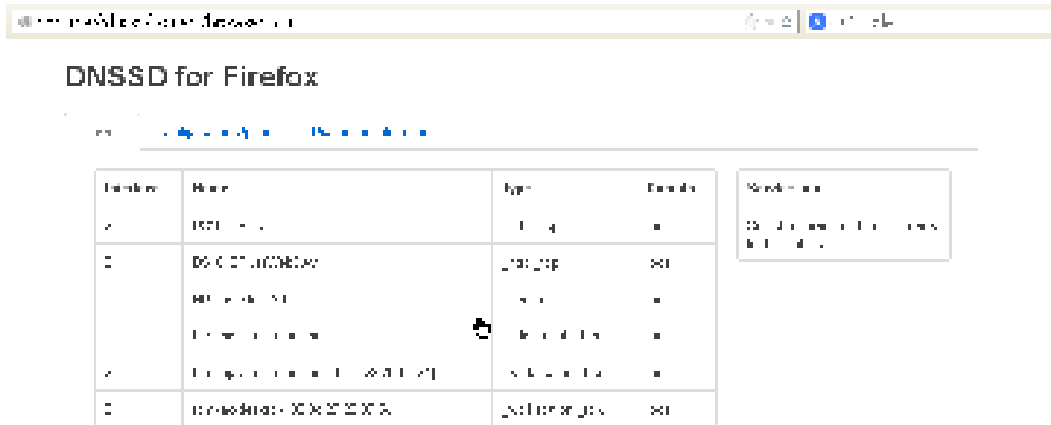


Below shows an example for applying the Bonjour feature that Vigor router can be used as the FTP server.

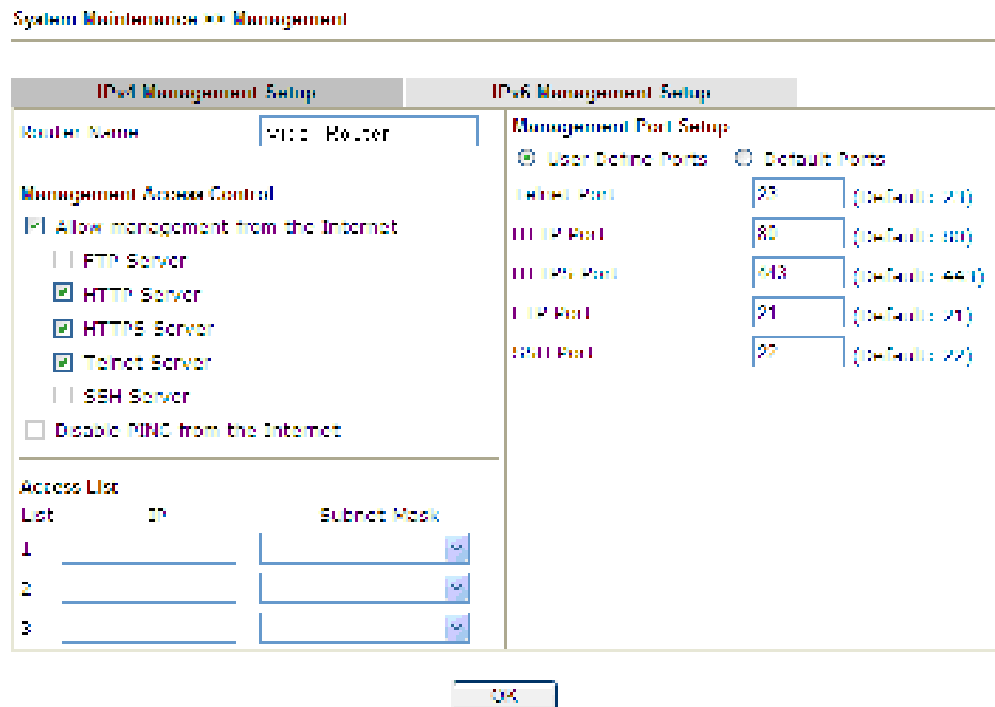
1. Here, we use Firefox and DNSSD to discover the service in such case. Therefore, just ensure the Bonjour client program and DNSSD for Firefox have been installed on the computer.



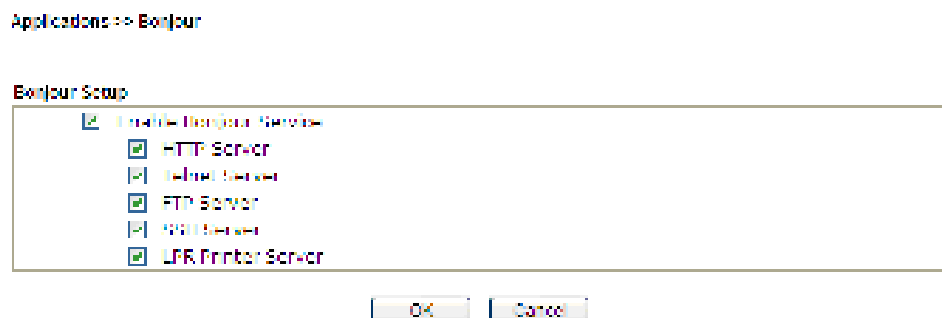
- Open the web browser, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.



- Open **System Maintenance**>>**Management**. Type a name (e.g., Dray\_2925) as the Router Name and click **OK**.

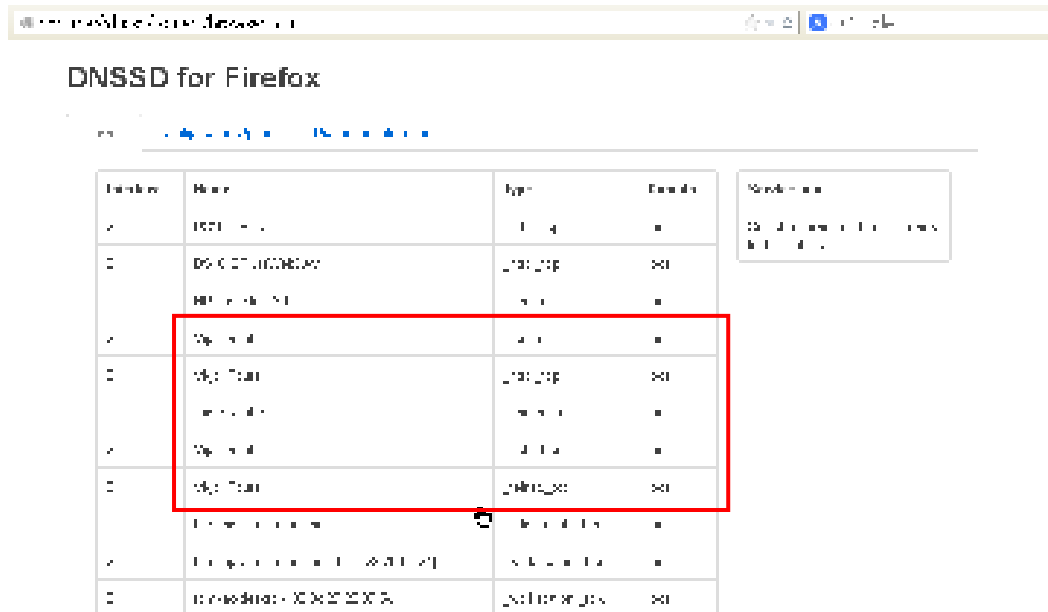


- Next, open **Applications**>>**Bonjour**. Check the service that you want to use via Bonjour.

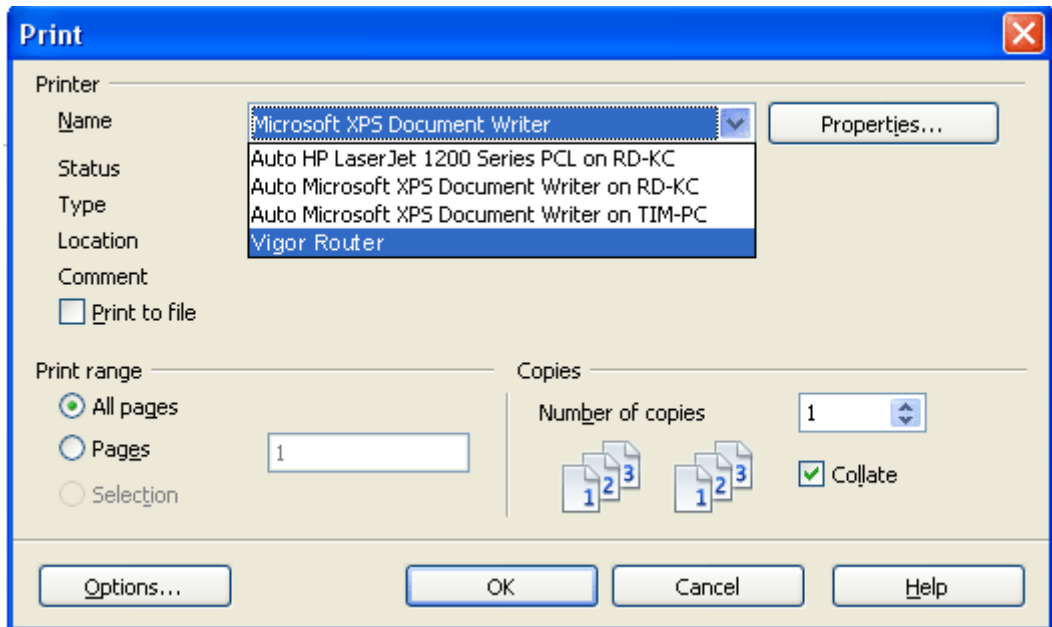




- Open the DNSSD page again. The available items will be changed as the follows. It means the Vigor router (based on Bonjour protocol) is ready to be used as a printer server, FTP server, SSH Server, Telnet Server, and HTTP Server.



- Now, any page or document can be printed out through Vigor router (installed with a printer).



## 4.12 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.



### 4.12.1 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.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environment

LAN to LAN VPN Client Mode Selection:

Please choose a LAN to LAN Profile:

**Note:** In a typical LAN to LAN tunnel, please select **Route Mode**.  
 If the remote network is expecting only a single client IP and is not configured to route the subnet, then select **NAT Mode**.  
 If in doubt, then select **Route Mode**.

< Back   Next >   Finish   Cancel

Available settings are explained as follows:

Item	Description
<b>LAN-to-LAN Client Mode Selection</b>	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

	<p>mode, otherwise please choose Route Mode.</p> <div style="border: 1px solid black; padding: 2px;"> <span>Route Mode</span> ▾  <span style="background-color: #0056b3; color: white;">Route Mode</span>  <span>NAT Mode</span> </div>																																																																																										
<p><b>Please choose a LAN-to-LAN Profile</b></p>	<p>There are 32 VPN profiles for users to set.</p> <table border="1"> <thead> <tr> <th>[Index]</th> <th>[Status]</th> <th>[Name]</th> </tr> </thead> <tbody> <tr><td>1</td><td>x</td><td>???</td></tr> <tr><td>2</td><td>x</td><td>???</td></tr> <tr style="background-color: #0056b3; color: white;"><td>3</td><td>x</td><td>???</td></tr> <tr><td>4</td><td>x</td><td>???</td></tr> <tr><td>5</td><td>x</td><td>???</td></tr> <tr><td>6</td><td>x</td><td>???</td></tr> <tr><td>7</td><td>x</td><td>???</td></tr> <tr><td>8</td><td>x</td><td>???</td></tr> <tr><td>9</td><td>x</td><td>???</td></tr> <tr><td>10</td><td>x</td><td>???</td></tr> <tr><td>11</td><td>x</td><td>???</td></tr> <tr><td>12</td><td>x</td><td>???</td></tr> <tr><td>13</td><td>x</td><td>???</td></tr> <tr><td>14</td><td>x</td><td>???</td></tr> <tr><td>15</td><td>x</td><td>???</td></tr> <tr><td>16</td><td>x</td><td>???</td></tr> <tr><td>17</td><td>x</td><td>???</td></tr> <tr><td>18</td><td>x</td><td>???</td></tr> <tr><td>19</td><td>x</td><td>???</td></tr> <tr><td>20</td><td>x</td><td>???</td></tr> <tr><td>21</td><td>x</td><td>???</td></tr> <tr><td>22</td><td>x</td><td>???</td></tr> <tr><td>23</td><td>x</td><td>???</td></tr> <tr><td>24</td><td>x</td><td>???</td></tr> <tr><td>25</td><td>x</td><td>???</td></tr> <tr><td>26</td><td>x</td><td>???</td></tr> <tr><td>27</td><td>x</td><td>???</td></tr> <tr><td>28</td><td>x</td><td>???</td></tr> <tr><td>29</td><td>x</td><td>???</td></tr> </tbody> </table>	[Index]	[Status]	[Name]	1	x	???	2	x	???	3	x	???	4	x	???	5	x	???	6	x	???	7	x	???	8	x	???	9	x	???	10	x	???	11	x	???	12	x	???	13	x	???	14	x	???	15	x	???	16	x	???	17	x	???	18	x	???	19	x	???	20	x	???	21	x	???	22	x	???	23	x	???	24	x	???	25	x	???	26	x	???	27	x	???	28	x	???	29	x	???
[Index]	[Status]	[Name]																																																																																									
1	x	???																																																																																									
2	x	???																																																																																									
3	x	???																																																																																									
4	x	???																																																																																									
5	x	???																																																																																									
6	x	???																																																																																									
7	x	???																																																																																									
8	x	???																																																																																									
9	x	???																																																																																									
10	x	???																																																																																									
11	x	???																																																																																									
12	x	???																																																																																									
13	x	???																																																																																									
14	x	???																																																																																									
15	x	???																																																																																									
16	x	???																																																																																									
17	x	???																																																																																									
18	x	???																																																																																									
19	x	???																																																																																									
20	x	???																																																																																									
21	x	???																																																																																									
22	x	???																																																																																									
23	x	???																																																																																									
24	x	???																																																																																									
25	x	???																																																																																									
26	x	???																																																																																									
27	x	???																																																																																									
28	x	???																																																																																									
29	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

**VPN Connection Setting**

**Security ranking (1 is the highest, 5 is the lowest)**

1. L2TP over IPsec
2. IPsec
3. PPTP (Encryption)
4. L2TP
5. PPTP (None Encryption)

**Throughput ranking (1 is the highest, 5 is the lowest)**

1. PPTP (None Encryption)
2. L2TP
3. IPsec
4. L2TP over IPsec
5. PPTP (Encryption)

Select VPN type: PPTP (Encryption) ▾

PPTP (Encryption)  
PPTP (None Encryption)  
IPsec  
L2TP  
L2TP over IPsec (None to Host)  
L2TP over IPsec (Host)

Back
Next >
Finish
Cancel

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	PPTP
VPN Dial Out Through	WAN1 Eth0
<input type="checkbox"/> Always on	
Server ID/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

- When you choose **IPSec**, you will see the following graphic:

VPN and Remote Access => VPN Client Wizard

**VPN Client IPSec Settings**

Profile Name	???
VPN Client Through	WAN1 Flex
<input type="checkbox"/> Always on	
Server ID/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPsec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	
Local Security Method	DES without Authentication
Remote Network IP	0.0.0.0
Remote 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 Client Through	WAN1 Flex
<input type="checkbox"/> Always on	
Server ID/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

- When you choose **L2TP over IPSec (Nice to Have)** or **L2TP over IPSec (Must)**, you will see the following graphic:

VPN and Remote Access => VPN Client Wizard

VPN Client L2TP over IPSec (Nice to Have) Settings

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for such profile. The length of the file is limited to 10 characters.
<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. <div data-bbox="730 1444 1129 1765" data-label="Image"> </div> <p><b>WAN1 First/ WAN2 First/ WAN3 First</b> - 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.</p> <p><b>WAN1 Only /WAN2 Only/WAN 3 Only</b>- While</p>

	<p>connecting, the router will use WAN1/WAN2/WAN3 as the only channel for VPN connection.</p> <p><b>WAN1 Only: Backup WAN2</b> - While connecting, the router will use WAN2 for VPN connection. If WAN2 fails, the router will use backup WAN1 interface instead.</p> <p><b>WAN2 Only: Backup WAN1</b> - While connecting, the router will use WAN1 for VPN connection. If WAN1 fails, the router will use backup WAN2 interface instead.</p>
<b>Always On</b>	Check to enable router always keep VPN connection.
<b>Server IP/Host Name for VPN</b>	Type the IP address of the server or type the host name for such VPN profile.
<b>IKE Authentication Method</b>	<p>IKE Authentication Method 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.</p> <p><b>Pre-Shared Key</b>- Specify a key for IKE authentication.</p> <p><b>Confirm Pre-Shared Key</b>-Confirm the pre-shared key.</p>
<b>Digital Signature (X.509)</b>	<p>Click <b>Digital Signature</b> to invoke this function.</p> <p><b>Peer ID</b> – Choose the peer ID selection from the drop down list.</p> <p><b>Local ID</b> – Choose <b>Alternative Subject Name First</b> or <b>Subject Name First</b>.</p> <p><b>Local Certificate</b> – 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 &gt;&gt; Local Certificate</b>. Otherwise, the setting you choose here will not be effective.</p>
<b>IPSec Security Method</b>	<p><b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p><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.</p>
<b>User Name</b>	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.</p> <p>The length of the use name is limited to 11 characters.</p>
<b>Password</b>	<p>This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.</p> <p>The length of the password is limited to 11 characters.</p>
<b>Remote Network IP</b>	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
<b>Remote Network Mask</b>	Please type the network mask (according to the real location of the remote host) for building VPN connection.

- 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 Client Wizard

---

Please confirm your settings

LAN to LAN Index:	20
Profile Name:	VPN 2
VPN Connection Type:	IPsec over IPsec (Site-to-Site)
VPN Dial Out Through:	WAN1 Eth0
Always on:	No
Server IP/Host Name:	172.16.0.10
Auth Authentication Method:	Pre-Shared Key
IPsec Security Method:	011:0101
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Client Wizard setup.
- View more detailed configurations.

Available settings are explained as follows:

Item	Description
<b>Go to the VPN Connection Management</b>	Click this radio button to access <b>VPN and Remote Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.
<b>Do another VPN Server Wizard Setup</b>	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
<b>View more detailed configuration</b>	Click this radio button to access <b>VPN and Remote Access&gt;&gt;LAN to LAN</b> for viewing detailed configuration.



## 4.12.2 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.

VPN and Remote Access >> VPN Server Wizard

**Choose VPN Establishment Environment**

VPN Server Mode Selection: Remote Dial-in User (Teleworker) ▼

Please choose a LAN-to-LAN Profile: 2 x 222 ▼

Please choose a Dial-in User Accounts: 2 x 111 ▼

Allowed Dial-in type:

L2TP

IPsec

L2TP with IPsec Policy None ▼

[- Lock] [Next >] [Back <] [Cancel]

Available settings are explained as follows:

Item	Description
<b>VPN Server Mode Selection</b>	<p>Choose the direction for the VPN server.</p> <p><b>Site to Site VPN</b> – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.</p> <p><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.</p> <p>Site to Site VPN (LAN-to-LAN) ▼</p> <p>Site to Site VPN (LAN-to-LAN)</p> <p>Remote Dial-in User (Teleworker)</p>
<b>Please choose a LAN-to-LAN Profile</b>	<p>This item is available when you choose <b>Site to Site VPN (LAN-to-LAN)</b> as VPN server mode. There are 32 VPN profiles for users to set.</p>

[Index]	[Status]	[Name]
1	x	???
2	x	???
3	x	???
4	x	???
5	x	???
6	x	???
7	x	???
8	x	???
9	x	???
10	x	???
11	x	???
12	x	???
13	x	???
14	x	???
15	x	???
16	x	???
17	x	???
18	x	???
19	x	???
20	x	???
21	x	???
22	x	???
23	x	???
24	x	???
25	x	???
26	x	???
27	x	???
28	x	???
29	x	???

**Please choose a Dial-in User Accounts** This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.

**Allowed Dial-in Type** This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).

PPTP  
 IPsec  
 L2TP with IPsec Policy

None ▼  
 None  
 Nice to Have  
 Must

Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected.

- 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 **Site-to-Site VPN** as the **VPN Server Mode**.

- When you check **PPTP**, you will see the following graphic:

VPN and Remote Access == VPN Server Wizard

VPN Authentication Setting

Profile Name	YYY
PPTP / L2TP / L2TP over IPsec Authentication	
Username	YYY
Password	
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

- 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:

VPN and Remote Access == VPN Server Wizard

VPN Authentication Setting

Profile Name	YYY
PPTP / L2TP / L2TP over IPsec Authentication	
Username	YYY
Password	
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

- When you check **IPSec**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

---

VPN Authentication Settings

Profile Name	007
IPSec/L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Local ID First	
Confirm Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	10000
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input checked="" type="radio"/> Subject Name First	
Peer IP/VPN Client IP	
Peer ID	
Peer ID (Maximum 47)	
Peer ID (Maximum 47)	
Remote Network Mask	255.255.255.0

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type a name for such profile. The length of the file is limited to 10 characters.
<b>User Name</b>	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.
<b>Password</b>	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.
<b>Pre-Shared Key</b>	For IPSec/L2TP IPSec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
<b>Confirm Pre-Shared Key</b>	Type the pre-shared key again for confirmation.
<b>Digital Signature (X.509)</b>	Check the box of Digital Signature to invoke this function. <b>Peer ID</b> – Choose the peer ID selection from the drop down list. <b>Local ID</b> – Choose <b>Alternative Subject Name First</b> or <b>Subject Name First</b> .
<b>Peer IP/VPN Client IP</b>	Type the WAN IP address or VPN client IP address for the remote client.
<b>Peer ID</b>	Type the ID name for the remote client. The length of the name is limited to 47 characters.

<b>Remote Network IP</b>	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
<b>Remote Network Mask</b>	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 ID/VPN Client ID:	192.168.1.100
Peer ID:	David

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Server Wizard setup.
- View more detailed configurations.

Available settings are explained as follows:

Item	Description
<b>Go to the VPN Connection Management</b>	Click this radio button to access <b>VPN and Remote Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.
<b>Do another VPN Server Wizard Setup</b>	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
<b>View more detailed configuration</b>	Click this radio button to access <b>VPN and Remote Access&gt;&gt;LAN to LAN</b> for viewing detailed configuration.

### 4.12.3 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.

VPN and Remote Access >> Remote Access Control Setup

#### Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service
<input checked="" type="checkbox"/>	Enable OpenVPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

OK Clear Cancel

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

### 4.12.4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

VPN and Remote Access >> PPP General Setup

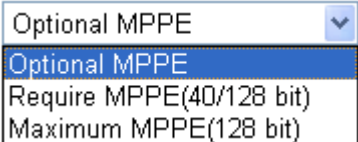
#### PPP General Setup

<b>PPP/MP Protocol</b> Dial-In PPP Authentication: <input type="text" value="PAP or CHAP"/> Dial-In PPP Encryption (MPPE): <input type="text" value="Optional MPPE"/> Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No Username: <input type="text"/> Password: <input type="text"/> <b>IP Address Assignment for Dial-In Users (When DHCP Disabled)</b> 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	<b>LDAP Server Profiles for PPP Authentication</b> PPTP LDAP Profile
---	---

OK

Available settings are explained as follows:

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.

	<p><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.</p>
<p><b>Dial-In PPP Encryption (MPPE)</b></p>	<p><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.</p>  <p><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.</p> <p><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.</p>
<p><b>Mutual Authentication (PAP)</b></p>	<p>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.</p> <p>The length of the name/password is limited to 23/19 characters.</p>
<p><b>Assigned IP Start</b></p>	<p>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.</p> <p>You can configure up to four start IP addresses for LAN1 ~ LAN5.</p>
<p><b>LDAP Server Profiles for PPP Authentication</b></p>	<p>Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.</p> <p>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.</p> <p>For detailed information about LDAP application, refer to section <b>4.7 How to Implement the AD/LDAP Authentication for User Management?</b></p>

## 4.12.5 IPsec General Setup

In **IPsec General Setup**, there are two major parts of configuration.

There are two phases of IPsec.

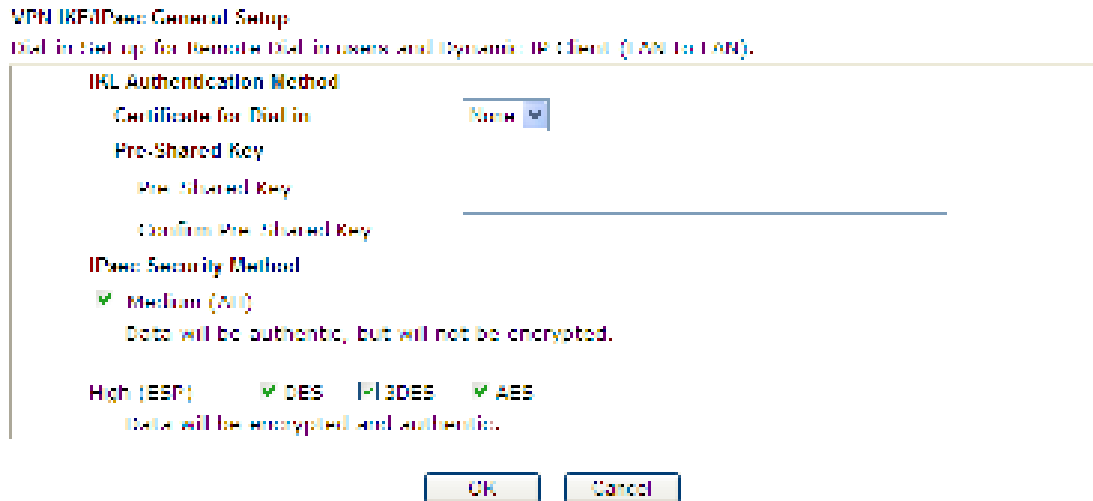
- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies 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 and Remote Access >> IPsec General Setup](#)



Available settings are explained as follows:

Item	Description
<b>IKE Authentication Method</b>	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



	<p>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>.</p> <p><b>Certificate for Dial-in</b> –Choose one of the local certificates from the drop down list.</p> <p><b>Pre-Shared Key</b>- Specify a key for IKE authentication.</p> <p><b>Confirm Pre-Shared Key</b>- Retype the characters to confirm the pre-shared key.</p> <p><b>Note:</b> Any packets from the remote dial-in user which does not match the rule defined in <b>VPN and Remote Access&gt;&gt;Remote Dial-In User</b> will be applied with the method specified here.</p>
<b>IPSec Security Method</b>	<p><b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p><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.</p>

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

## 4.12.6 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 **64** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPsec Peer Identity

VPN Peer ID Accounts: Set to Factory Default

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

« 1-32 | 12-34 » Next »

Available settings are explained as follows:

Item	Description
<b>Set to Factory Default</b>	Click it to clear all indexes.
<b>Index</b>	Click the number below Index to access into the setting page of IPsec Peer Identity.
<b>Name</b>	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.

Profile Index : 4

Profile Name

Enable this account

Accept Any Peer ID

---

Accept Subject Alternative Name

Type

Domain Name

---

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

Available settings are explained as follows:

Item	Description
<b>Profile Name</b>	Type the name of the profile. The maximum length of the name you can set is 32 characters.
<b>Enable this account</b>	Check it to enable such account profile.
<b>Accept Any Peer ID</b>	Click to accept any peer regardless of its identity.
<b>Accept Subject Alternative Name</b>	Click to check one specific field of digital signature to accept the peer with matching value. The field can be <b>IP Address, Domain, or 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.
<b>Accept Subject Name</b>	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), Organization Unit (OU), Common Name (CN), and Email (E)</b> .

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

## 4.12.7 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:** Vigor2925 will support up to 25 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 Mac OS.
- 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

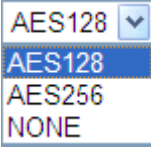
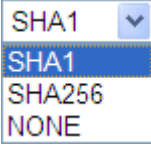
### OpenVPN General Setup

Port	1194
Cipher Algorithm	AES128
HMAC Algorithm	SHA1
Certificate Authentication	<input type="checkbox"/>

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
<b>Port</b>	Usually, the default UDP port number for OpenVPN is 1194.
<b>Cipher Algorithm</b>	Two encryptions are supported, AES128 and AES256. 
<b>HMAC Algorithm</b>	The HMAC algorithm only supports SHA1/SHA256. 
<b>Certificate Authentication</b>	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.

## 4.12.8 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 **64** 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.

VPN and Remote Access >> Remote Dial-in User

Remote Access Over Accounts Set to Factory Default

View:  All  Online  Offline Search

Index	User	Active	Status	Index	User	Active	Status
1	???	<input type="checkbox"/>		17	???	<input type="checkbox"/>	
2	???	<input type="checkbox"/>	---	18	???	<input type="checkbox"/>	---
3	???	<input type="checkbox"/>		19	???	<input type="checkbox"/>	
4	???	<input type="checkbox"/>		20	???	<input type="checkbox"/>	
5	???	<input type="checkbox"/>	---	21	???	<input type="checkbox"/>	---
6	???	<input type="checkbox"/>		22	???	<input type="checkbox"/>	
7	???	<input type="checkbox"/>		23	???	<input type="checkbox"/>	
8	???	<input type="checkbox"/>	---	24	???	<input type="checkbox"/>	---
9	???	<input type="checkbox"/>		25	???	<input type="checkbox"/>	
10	???	<input type="checkbox"/>	---	26	???	<input type="checkbox"/>	---
11	???	<input type="checkbox"/>	---	27	???	<input type="checkbox"/>	---
12	???	<input type="checkbox"/>		28	???	<input type="checkbox"/>	
13	???	<input type="checkbox"/>	---	29	???	<input type="checkbox"/>	---
14	???	<input type="checkbox"/>		30	???	<input type="checkbox"/>	
15	???	<input type="checkbox"/>		31	???	<input type="checkbox"/>	
16	???	<input type="checkbox"/>	---	32	???	<input type="checkbox"/>	---

OK Cancel

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
View	<b>All</b> – Click it to display the all of the user accounts. <b>Online</b> – Click it to display the online user accounts. <b>Offline</b> – Click it to display the offline user accounts.
Index	Click 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.
Active	Check the box to activate such profile.

<b>Status</b>	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 User

Index No. 1

Available settings are explained as follows:

Item	Description
<b>User account and Authentication</b>	<p><b>Enable this account</b> - Check the box to enable this function.</p> <p><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.</p>
<b>Allowed Dial-In Type</b>	<p><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.</p> <p><b>IPSec Tunnel</b> - Allow the remote dial-in user to make an IPSec VPN connection through Internet.</p> <p><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</p>

	<p>below:</p> <ul style="list-style-type: none"> <li>● <b>None</b> - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.</li> <li>● <b>Nice to Have</b> - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.</li> <li>● <b>Must</b> - Specify the IPsec policy to be definitely applied on the L2TP connection.</li> </ul> <p><b>SSL Tunnel</b> – Allow the remote dial-in user to make an SSL VPN connection through Internet.</p> <p><b>OpenVPN Tunnel</b> - Allow the remote dial-in user to make an OpenVPN connection through Internet.</p> <p><b>Specify Remote Node</b> - You can specify the IP address of the remote dial-in user, or peer ID (used in IKE aggressive mode).</p> <p>Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b>.</p> <p><b>Netbios Naming Packet</b> -</p> <ul style="list-style-type: none"> <li>● <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</li> <li>● <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.</li> </ul> <p><b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> <li>● <b>Pass</b> – Click this button to let multicast packets pass through the router.</li> <li>● <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.</li> </ul> <p><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/password is limited to 23 characters.</p> <p><b>Password</b> - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name/password is limited to 19 characters.</p> <p><b>Enable Mobile One-Time Passwords (mOTP)</b> - Check this box to make the authentication with mOTP function.</p> <p><b>PIN Code</b> – Type the code for authentication (e.g., 1234).</p> <p><b>Secret</b> – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
<b>Subnet</b>	<p>Chose one of the subnet selections for such VPN profile.</p> <p><b>Assign Static IP Address</b> – Please type a static IP address</p>

	for the subnet you specified.
<b>IKE Authentication Method</b>	<p>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.</p> <p><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.</p> <p><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 &gt;&gt;IPSec Peer Identity</b>.</p>
<b>IPSec Security Method</b>	<p>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.</p> <p><b>Medium-Authentication Header (AH)</b> means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p><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.</p> <p><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.</p>

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

#### 4.12.9 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 Factory Default](#) |

View:  All  Online  Offline  Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1	Carly	V	OK	17	???	X	
2	Jack	V	OK	18	???	X	
3	Trime	V	OK	19	???	X	
4	John	X		20	???	X	
5	???	X		21	???	X	
6	???	X		22	???	X	
7	???	X		23	???	X	
8	???	X		24	???	X	
9	???	X		25	???	X	
10	???	X		26	???	X	
11	???	X		27	???	X	
12	???	X		28	???	X	
13	???	X		29	???	X	
14	???	X		30	???	X	
15	???	X		31	???	X	
16	???	X		32	???	X	

1 32 33 64 Next

[XXXXXXXXX This Default profile has already joined to VPN Load Balance Mechanism.]  
[XXXXXXXXX This Default profile has already joined to VPN Backup Mechanism.]  
[XXXXXXXXX This Default profile does not join to VPN TRUNK.]

The following shows profiles joined into VPN Load Balance and VPN Backup mechanism.

VPN and Remote Access for LAN to LAN

LAN-to-LAN Profiles:

View:  All  Online  Offline  Trunk

Name	Active	Members	Status
<a href="#">LoadBal</a>	V	Carly Jack	OK OK

[XXXXXXXXX This Default profile has already joined to VPN Load Balance Mechanism.]  
[XXXXXXXXX This Default profile has already joined to VPN Backup Mechanism.]

Available settings are explained as follows:

Item	Description
<b>View</b>	<b>All</b> – Click it to display the LAN to LAN profiles. <b>Online</b> – Click it to display the online profiles. <b>Offline</b> – Click it to display the offline profiles. <b>Trunk</b> – Click it to display the Trunk profiles.
<b>Set to Factory Default</b>	Click to clear all indexes.
<b>Name</b>	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
<b>Active</b>	V – means the profile has been enabled. X – mans the profile has not been enabled.

<b>Status</b>	Online – means such LAN to LAN profile is in use. Offline – means such LAN to LAN profile isn't in use even if the profile has been enabled.
---------------	---

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:

Enable this profile

VPN Dial-Out Through:

Network Naming Packet:  Pass  Block

Multicast via VPN:  Pass  Block  
(for some ICMP, IP-Cameras, DHCP Relay...etc.)

Call Direction:  Both  Dial-Out  Dial-In

Always on

Idle Timeout:  second(s)

Enable PING to keep alive

Ping to the IP:

**2. Dial Out Settings**

Type of Server I am calling

PPTP

IPsec Tunnel

L2IP with IPsec Policy:

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

Username:

Password:

PPP Authentication:

MP Compression:  On  Off

**IPsec Authentication Method**

Pre-Shared Key

IP Pre-Shared Key:

Digital Signature(X.509)

Peer ID:

Local ID:

Alternative Subject Name First

Subject Name First

Local Certificate:

**IPsec Security Method**

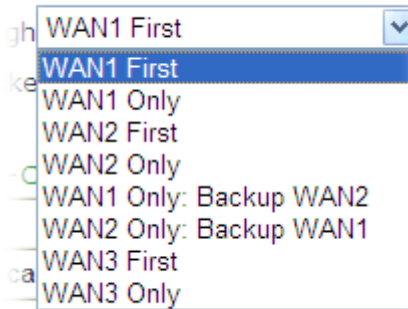
Medium(AH)

High(ESP):

Index(1-15) in Schedule Setup:

Available settings are explained as follows:

Item	Description
<b>Common Settings</b>	<p><b>Profile Name</b> – Specify a name for the profile of the LAN-to-LAN connection.</p> <p><b>Enable this profile</b> - Check here to activate this profile.</p> <p><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.</p>



- **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.
- **WAN1 Only: Backup WAN2** - While connecting, the router will use WAN2 for VPN connection. If WAN2 fails, the router will use backup WAN1 interface instead.
- **WAN2 Only: Backup WAN1** - While connecting, the router will use WAN1 for VPN connection. If WAN1 fails, the router will use backup WAN2 interface instead.

#### Netbios Naming Packet

- **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
- **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

**Multicast via VPN** - Some programs might send multicast packets via VPN connection.

- **Pass** – Click this button to let multicast packets pass through the router.
- **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.

**Call Direction** - Specify the allowed call direction of this LAN-to-LAN profile.

- **Both**:-initiator/responder
- **Dial-Out**- initiator only
- **Dial-In**- responder only.

**Always On**-Check to enable router always keep VPN connection.

**Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.

	<p><b>Enable PING to keep alive</b> - 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.</p> <p><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 of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).</p> <p><b>PING to the IP</b> - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.</p>
<p><b>Dial-Out Settings</b></p>	<p><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.</p> <p><b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.</p> <p><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:</p> <ul style="list-style-type: none"> <li>● <b>None:</b> Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</li> <li>● <b>Nice to Have:</b> Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.</li> <li>● <b>Must:</b> Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul> <p><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.</p> <p><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.</p> <p><b>PPP Authentication</b> - This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.</p> <p><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</p>

---

compression. Normally set to **Yes** to improve bandwidth utilization.

**IKE Authentication Method** - This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.

- **Pre-Shared Key** - 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**.  
**Peer ID** - Select one of the predefined Profiles set in **VPN and Remote Access >>IPSec Peer Identity**.  
**Local ID** - 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**.

**IPSec Security Method** - 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:
- **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.
- **DES with Authentication**-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
- **3DES without Authentication**-Use triple DES encryption algorithm and not apply any authentication scheme.
- **3DES with Authentication**-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
- **AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme.
- **AES with Authentication**-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.

The window of advance setup is shown as below:

---



**3. Dial In Settings**

<b>Allowed Dial In Type</b> <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <i>None</i>	Username <input type="text" value="999"/> Password <input type="password"/> V2 Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	<b>IKF Authentication Method</b> <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	<b>IPsec Security Method</b> <input checked="" type="checkbox"/> Medium(AI) High(ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input type="checkbox"/> AES

**4. GRE over IPsec Settings**

Enable IPsec Dial In Function GRE over IPsec:  
 Logical Traffic: My GRE IP  Peer GRE IP

**5. TCP/IP Network Settings**

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Operation <input type="text" value="Fixed"/> From first subnet to remote network, you have to do <input type="text" value="Route"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel ( Only single WAN supports this )
Remote Network IP	<input type="text" value="0.0.0.0"/>	
Remote Network Mask	<input type="text" value="255.255.255.0"/>	
Local Network IP	<input type="text" value="192.168.1.1"/>	
Local Network Mask	<input type="text" value="255.255.255.0"/>	

Available settings are explained as follows:

Item	Description
<b>Dial-In Settings</b>	<p><b>Allowed Dial-In Type</b> - Determine the dial-in connection with different types.</p> <ul style="list-style-type: none"> <li>● <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.</li> <li>● <b>IPSec Tunnel</b>- Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.</li> <li>● <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:           <ul style="list-style-type: none"> <li>■ <b>None</b> - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</li> <li>■ <b>Nice to Have</b> - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the</li> </ul> </li> </ul>

---

dial-in VPN connection becomes one pure L2TP connection.

- **Must** - Specify the IPSec policy to be definitely applied on the L2TP connection.

**Specify Remote VPN Gateway** - You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side.

If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.

**User Name** - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The length of the named is limited to 11 characters.

**Password** - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The length of the password is limited to 11 characters.

**VJ Compression** - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

**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.

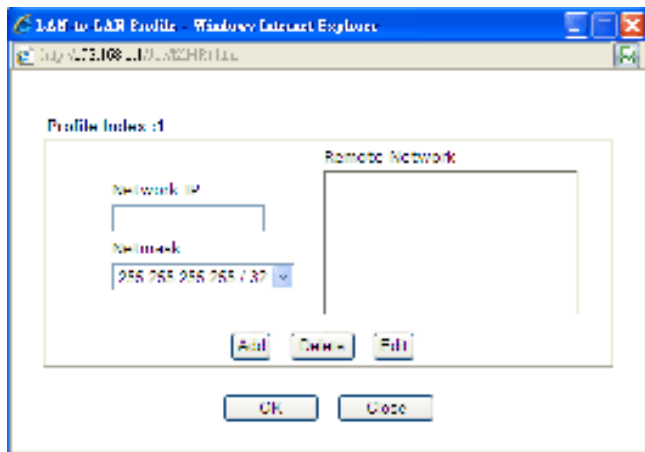
- **Pre-Shared Key** - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
- **Digital Signature (X.509)** –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
  - **Local ID** – Specify which one will be inspected first.
  - **Alternative Subject Name First** – The alternative subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.
  - **Subject Name First** – The subject name (configured in **Certificate Management>>Local Certificate**) will be inspected first.

**IPSec Security Method** - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.

- **Medium**- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
-



	<ul style="list-style-type: none"> <li>● <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.</li> </ul>
<p><b>Gre over IPSec Settings</b></p>	<p><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.</p> <p><b>Logical Traffic:</b> 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.</p> <p><b>My GRE IP:</b> Type the virtual IP for router itself for verified by peer.</p> <p><b>Peer GRE IP:</b> Type the virtual IP of peer host for verified by router.</p>
<p><b>TCP/IP Network Settings</b></p>	<p><b>My WAN IP</b> –This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, 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 L2TP.</p> <p><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 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the 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 L2TP.</p> <p><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.</p> <p><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.</p> <p><b>More</b> - 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.</p>



**RIP Direction** - The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

**From first subnet to remote network, you have to do** - If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

**Change default route to this VPN tunnel** - Check this box to change the default route with this VPN tunnel.

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

## 4.12.10 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
- Fully compliant with VPN Server LAN Site 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

**Backup Profile List** | Set to Factory Default |

Note: [Active:ND] The LAN to LAN Profile is disabled in under Dial-In(Call Direction) at present.

No.	Profile Name	Member1 (Profile) Type	Member2 (Profile) Type

Advanced ▼

**Load Balance Profile List** | Set to Factory Default |

Note: [Active:ND] The LAN to LAN Profile is disabled in under Dial-In(Call Direction) at present.

No.	Profile Name	Member1 (Profile) Type	Member2 (Profile) Type

Advanced ▼

**General Setup**

Status:  Enable  Disable

Profile Name:

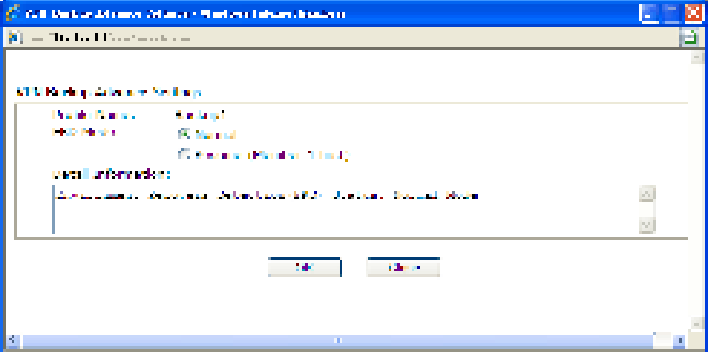
Member1:  ▼

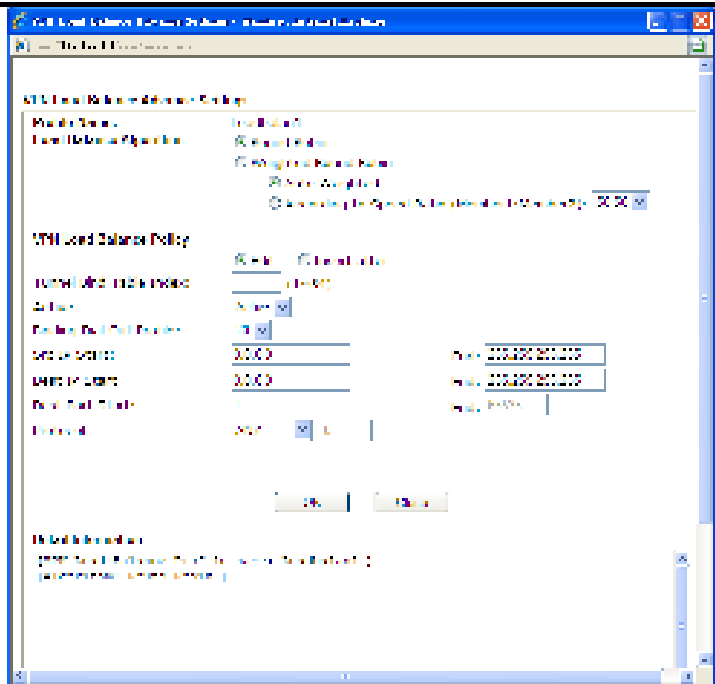
Member2:  ▼

Active Mode:  Backup  Load Balance

Available settings are explained as follows:

Item	Description
<b>Backup Profile List</b>	<p><b>Set to Factory Default</b> - Click to clear all VPN TRUNK-VPN Backup mechanism profile.</p> <p><b>No</b> – The order of VPN TRUNK-VPN Backup mechanism profile.</p> <p><b>Status</b> - “v” means such profile is enabled; “x” means such profile is disabled.</p> <p><b>Name</b> - Display the name of VPN TRUNK-VPN Backup mechanism profile.</p> <p><b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.</p> <p><b>Active</b> - “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.</p> <p><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.</p> <p><b>Member2</b> - Display the dial-out profile selected from the</p>

	<p>Member2 drop down list below.</p> <p><b>Advanced</b> – This button is available only when LAN to LAN profile (or more) is created.</p>  <p>Detailed information for this dialog, see later section - <b>Advanced Load Balance and Backup</b>.</p>
<p><b>Load Balance Profile List</b></p>	<p><b>Set to Factory Default</b> - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.</p> <p><b>No</b> - The order of VPN TRUNK-VPN Load Balance mechanism profile.</p> <p><b>Status</b> - “v” means such profile is enabled; ”x” means such profile is disabled.</p> <p><b>Name</b> - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.</p> <p><b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.</p> <p><b>Active</b> - “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.</p> <p><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.</p> <p><b>Member2</b> - Display the dial-out profile selected from the Member2 drop down list below.</p> <p><b>Advanced</b> – This button is only available when there is one or more profiles created in this page.</p>



Detailed information for this dialog, see later section - **Advanced Load Balance and Backup.**

## General Setup

**Status-** After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.

**Profile Name-** 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.
- **Connection Type** - 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.

**Update-** Click this button to save the changes to the **Status** (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.

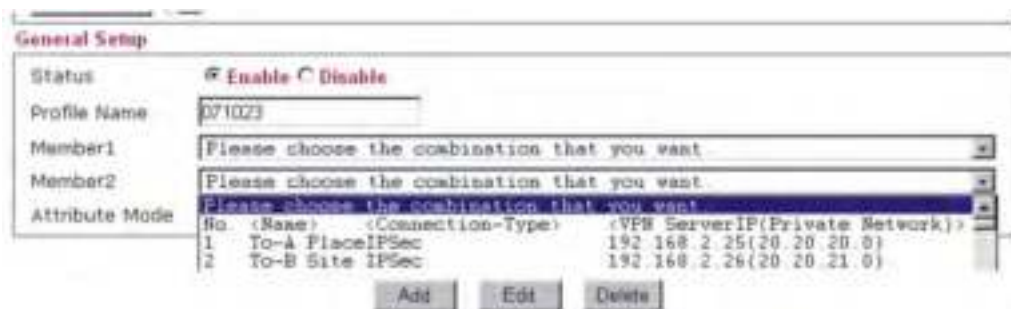
### Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

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?

1. 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**.
3. 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.



- 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.

**LAN-to-LAN Profiles:**

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	---

**How can you set a GRE over IPSec profile?**

- Please go to LAN to LAN to set a profile with IPSec.
- 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.

- 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.



## 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

Available settings are explained as follows:

Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	<p><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.</p> <p><b>Weighted Round Robin</b> –Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio.</p> <p><b>Auto Weighted</b> 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. <b>According to Speed Ratio</b> allows</p>

	<p>user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).</p>
<p><b>VPN Load Balance Policy</b></p>	<p>Below shows the algorithm for Load Balance.</p> <p><b>Edit</b> – Click this radio button for assign a blank table for configuring Binding Tunnel.</p> <p><b>Insert after</b> – Click this radio button to adding a new binding tunnel table.</p> <p><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.</p> <p><b>Active</b> – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.</p> <p><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.</p> <p><b>Src IP Start /End</b>– Specify source IP addresses as starting point and ending point.</p> <p><b>Dest IP Start/End</b> – Specify destination IP addresses as starting point and ending point.</p> <p><b>Dest Port Start /End</b>– Specify destination service port as starting point and ending point.</p> <p><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.</p> <p><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 ICMP 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 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 tunnel table can be established.</p>



Item	Description
<b>Profile Name</b>	List the backup profile name.
<b>ERD Mode</b>	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.
<b>Detail Information</b>	This field will display detailed information for Environment Recovers Detection.

#### 4.12.11 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

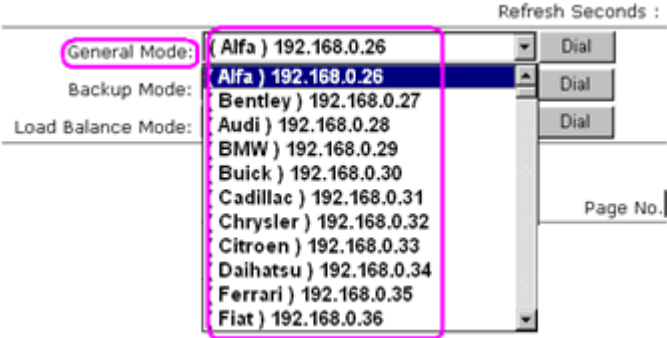
Dial out Tool Refresh Seconds : 10

General Mode:   
 Backup Mode:   
 Load Balance Mode: | Loadbalan1 | 192.168.0.8

VPN Connection Status  
 Current Page: 1 Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Pps)	Rx Pkts	Rx Rate (Pps)	UpTime
xxxxxxx : Data is encrypted. xxxxxxx : Data isn't encrypted.								

Available settings are explained as follows:

Item	Description
<b>Dial-out Tool</b>	<p><b>General Mode</b> - This field 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.</p>  <p><b>Backup Mode</b> - This field displays the profile name saved in VPN TRUNK Management (with Index number and</p>

VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.

General Mode:	(Alfa) 192.168.0.26	192.168.0.26	192.168.0.26
Backup Mode:	(VpnBackup) 192.168.2.103	192.168.2.103	192.168.2.103
Load Balance Mode:	(VpnBackup) 192.168.2.103	192.168.2.103	192.168.2.103
	(VpnBackup) 192.168.2.203	192.168.2.203	192.168.2.203

**Dial** - Click this button to execute dial out function.

**Refresh Seconds** - Choose the time for refresh the dial information among 5, 10, and 30.

**Refresh** - Click this button to refresh the whole connection status.

## 4.13 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.



### 4.13.1 Local Certificate

Certificate Management > Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
---	---	---	<a href="#">View</a> <a href="#">Delete</a>
---	---	---	<a href="#">View</a> <a href="#">Delete</a>
---	---	---	<a href="#">View</a> <a href="#">Delete</a>

[GENERAL](#) [IMPORT](#) [RELOAD](#)

Available settings are explained as follows:

Item	Description
<b>Generate</b>	Click this button to open <b>Generate Certificate Request</b> window. Type in all the information that the window requests. Then

	click <b>Generate</b> again.
<b>Import</b>	Click this button to import a saved file as the certification information.
<b>Refresh</b>	Click this button to refresh the information listed below.
<b>View</b>	Click this button to view the detailed settings for certificate request.
<b>Delete</b>	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 Request

Certificate Name	<input type="text"/>
Subject Alternative Name	
Type	IP Address
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	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:

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
-----	-----	Requesting	<a href="#">View</a>	<a href="#">Delete</a>
---	---	---	<a href="#">View</a>	<a href="#">Delete</a>
---	---	---	<a href="#">View</a>	<a href="#">Delete</a>

[GENERATE](#) [IMPORT](#) [REQUEST](#)

### 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.

Import X509 Local Certificate


**Upload Local Certificate**  
 Select a local certificate file.  
 Certificate file:  [Browse](#)  
 Click **Import** to upload the local certificate.

**Upload PKCS12 Certificate**  
 Select a PKCS12 file.  
 PKCS12 file:  [Browse](#)  
 Password:   
 Click **Import** to upload the PKCS12 file.

**Upload 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.

Available settings are explained as follows:

Item	Description
<b>Upload Local Certificate</b>	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 “OK”.

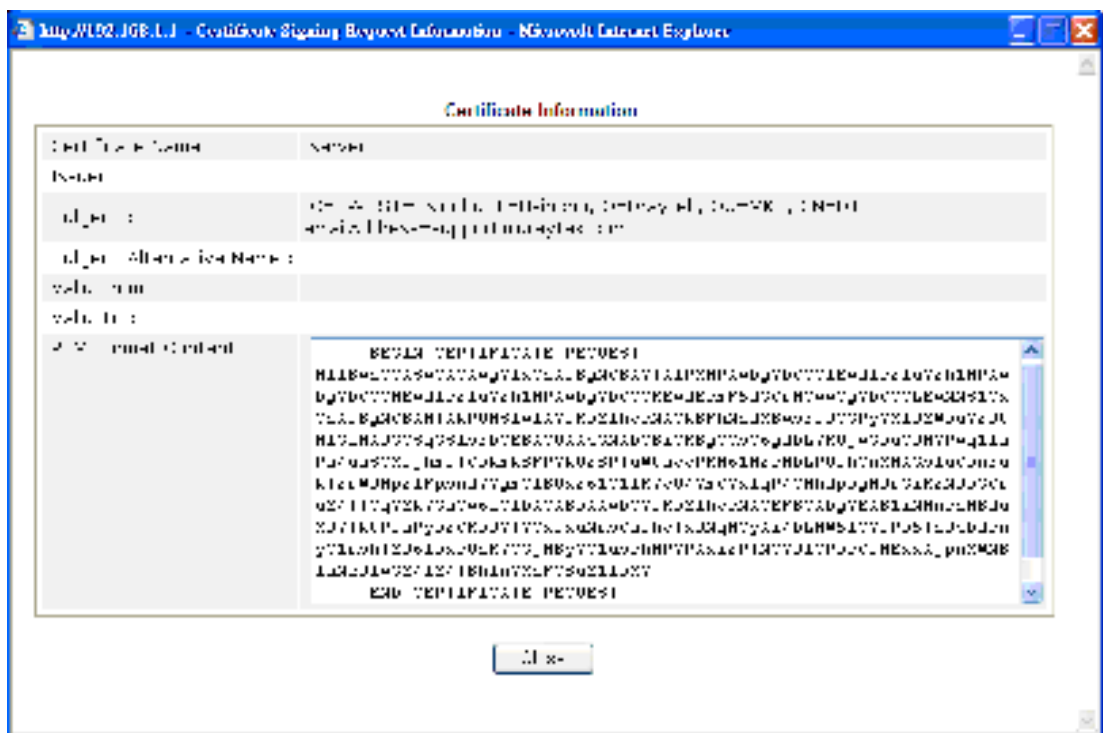
	
<p><b>Upload PKCS12 Certificate</b></p>	<p>It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.</p> <p><b>Note:</b> PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.</p>
<p><b>Upload Certificate and Private Key</b></p>	<p>It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.</p>

**REFRESH**

Click this button to refresh the information listed below.

**View**

Click this button to view the detailed settings for certificate request.



**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.

### 4.13.2 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			<a href="#">View</a>	<a href="#">Delete</a>
Trusted CA-2	---	---	<a href="#">View</a>	<a href="#">Delete</a>
Trusted CA-3	---	---	<a href="#">View</a>	<a href="#">Delete</a>

[IMPORT](#) [RESET](#)

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 CA Certificate

Import X509 Trusted CA Certificate

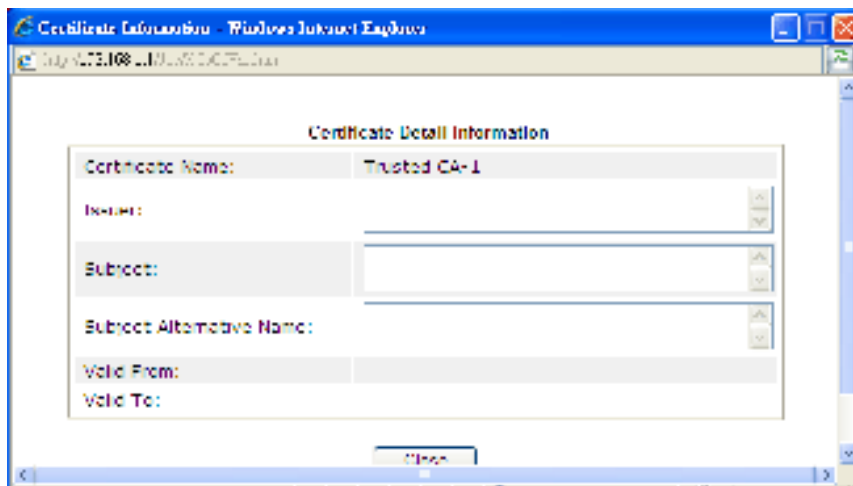
Select a trusted CA certificate file.

[Browse...](#)

Click Import to import the certificate.

[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.



### 4.13.3 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 Backup / 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.

**Choose**

Decrypt password:

Click **Restore** to upload the file.

## 4.14 Wireless LAN

This function is used for “n” models only.

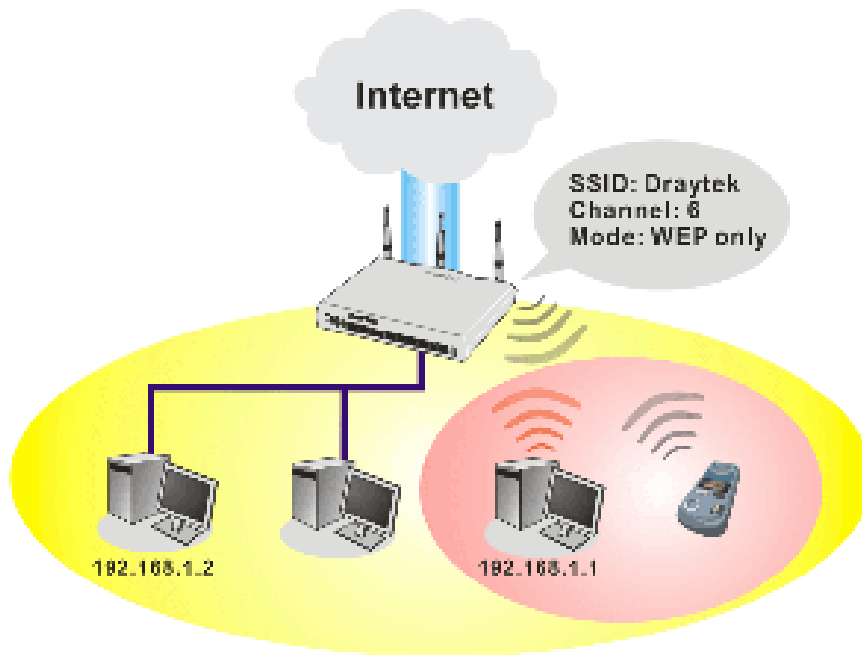
### 4.14.1 Basic Concepts

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.



### 4.13.2 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.

Wireless LAN => General Setup

General Setting (VLL002.11)

Enable Wireless LAN

Mode: Mixed(11b+11g+11n)

Index(1-15) in Schedule Setup: [ ] [ ] [ ] [ ]

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

Index	Enable	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">DrayTek</span>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">DrayTek_Guest</span>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;"> </span>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;"> </span>	<input type="checkbox"/>	<input type="checkbox"/>

Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.  
Isolate VPN: Isolate wireless with remote dial in and LAN to LAN VPN.

Channel: Channel 6, 240MHz Long Preamble:

Long Preamble: necessary for some old 802.11 b devices only (lower performance)

Packet-OVERDRIVE™  
 Tx Burst

Note:  
The same technology must also be supported in clients to boost WLAN performance.

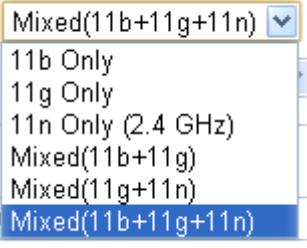
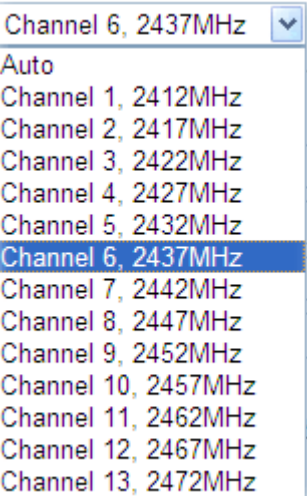
Rate Control	Enable	Upload	Download
SSID 1	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps
SSID 2	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps
SSID 3	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps
SSID 4	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps	<span style="border: 1px solid black; padding: 2px;">20000</span> kbps

Note: range 100-50,000 kbps

OK
Cancel

Available settings are explained as follows:

Item	Description
<b>Enable Wireless LAN</b>	Check the box to enable wireless function.
<b>Mode</b>	At present, the router can connect to 11b Only, 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.

	
<p><b>Channel</b></p>	<p>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.</p> 
<p><b>Hide SSID</b></p>	<p>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.</p>
<p><b>SSID</b></p>	<p>Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.</p>
<p><b>Isolate</b></p>	<p><b>VPN</b> – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.  <b>Member</b> –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
<p><b>Rate Control</b></p>	<p>It controls the data transmission rate through wireless connection.</p> <p><b>Upload</b> – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.</p> <p><b>Download</b> – Type the transmitting rate for data download. Default value is 30,000 kbps.</p>

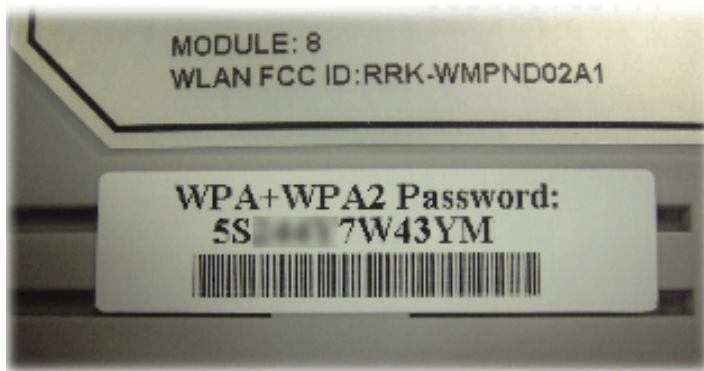
<b>Schedule</b>	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications &gt;&gt; Schedule</b> setup. The default setting of this field is blank and the function will always work.
-----------------	--

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

### 4.14.3 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.

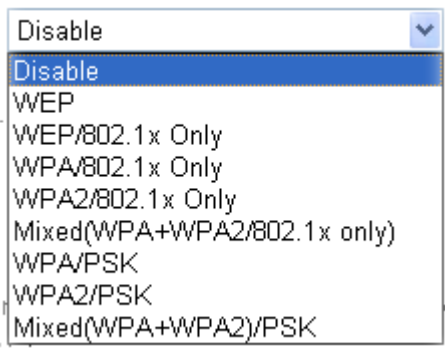


By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

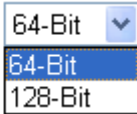
Wireless LAN => Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
<p>Mode: <span style="border: 1px solid black; padding: 2px;">Mixed(WPA+WPA2)/PSK</span></p>			
<p><b>WPA2</b></p>			
<p>Encryption Mode: <span style="border: 1px solid black; padding: 2px;">TKIP for WPA/WEP for WPA2</span></p>		<p>Pre Shared Key (PSK): <span style="border: 1px solid black; padding: 2px;">*****</span></p>	
<p>Note: Type 8-33 ASCII characters or 10 Hexadecimal digits (adding a "0" for example "0123456789" or "00EE3bccc01").</p>			
<p><b>WEP</b></p>			
<p>Encryption Mode: <span style="border: 1px solid black; padding: 2px;">802.1x</span></p>		<p><input checked="" type="radio"/> Key 1: <span style="border: 1px solid black; padding: 2px;">*****</span></p>	
		<p><input type="radio"/> Key 2: <span style="border: 1px solid black; padding: 2px;">*****</span></p>	
		<p><input type="radio"/> Key 3: <span style="border: 1px solid black; padding: 2px;">*****</span></p>	
		<p><input type="radio"/> Key 4: <span style="border: 1px solid black; padding: 2px;">*****</span></p>	
<p>Note:                      Please configure the <b>RADIUS Server</b> if 802.1x is used.                      For 64-bit WEP key configurations, please insert 8 ASCII characters or 10 Hexadecimal digits (adding a "0": Examples are "AS312" or "0: 1233132"                      For 128-bit WEP key configurations, please insert 16 ASCII characters or 20 Hexadecimal digits (adding a "0":</p>			
<span style="border: 1px solid black; padding: 2px;">OK</span>		<span style="border: 1px solid black; padding: 2px;">Cancel</span>	

Available settings are explained as follows:

Item	Description
Mode	<p>There are several modes provided for you to choose.</p>  <p><b>Note:</b> You should also set <b>RADIUS Server</b> simultaneously if 802.1x mode is selected.</p> <p><b>Disable</b> - Turn off the encryption mechanism.</p> <p><b>WEP</b>-Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p><b>WEP/802.1x Only</b> - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p><b>WPA/802.1x Only</b>- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS</p>



	<p>server with 802.1X protocol.</p> <p><b>WPA2/802.1x Only</b>- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p><b>Mixed (WPA+WPA2/802.1x only)</b> - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p><b>WPA/PSK</b>-Accepts only WPA clients and the encryption key should be entered in PSK.</p> <p><b>WPA2/PSK</b>-Accepts only WPA2 clients and the encryption key should be entered in PSK.</p> <p><b>Mixed (WPA+ WPA2)/PSK</b> - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.</p>
<b>WPA</b>	<p>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...").</p> <p><b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only.</p> <p><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...").</p>
<b>WEP</b>	<p><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, such as 0x4142434445.)</p> <p><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).</p> <p>Encryption Mode: </p> <p>All wireless devices must support the same WEP encryption bit size and have the same key. <b>Four keys</b> can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.</p>

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

#### 4.14.4 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.

**Access Control**

Enable Mac Address Filter  SSID 1  White List  SSID 2  White List   
 SSID 3  White List  SSID 4  White List

**MAC Address Filter**

Index	Attribute	MAC Address	Apply SSID
Client's MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> Apply SSID : <input type="checkbox"/> SSID 1 <input type="checkbox"/> SSID 2 <input type="checkbox"/> SSID 3 <input type="checkbox"/> SSID 4 Attribute : <input type="checkbox"/> Isolate the station from LAN <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>			

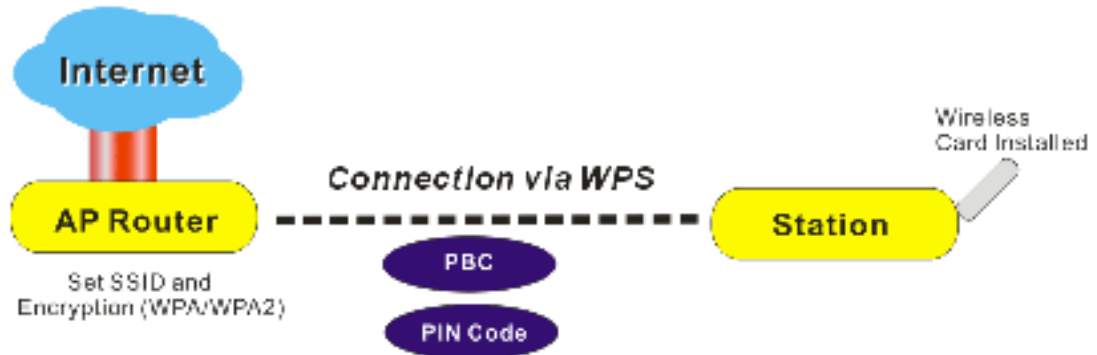
Available settings are explained as follows:

Item	Description
<b>Enable Mac Address Filter</b>	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.
<b>MAC Address Filter</b>	Display all MAC addresses that are edited before.
<b>Client's MAC Address</b>	Manually enter the MAC address of wireless client.
<b>Apply SSID</b>	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
<b>Attribute</b>	<b>s: Isolate the station from LAN</b> - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
<b>Add</b>	Add a new MAC address into the list.
<b>Delete</b>	Delete the selected MAC address in the list.
<b>Edit</b>	Edit the selected MAC address in the list.
<b>Cancel</b>	Give up the access control set up.
<b>OK</b>	Click it to save the access control list.
<b>Clear All</b>	Clean all entries in the MAC address list.

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

#### 4.14.5 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.



**Note:** Such function is available for the wireless station with WPS supported.

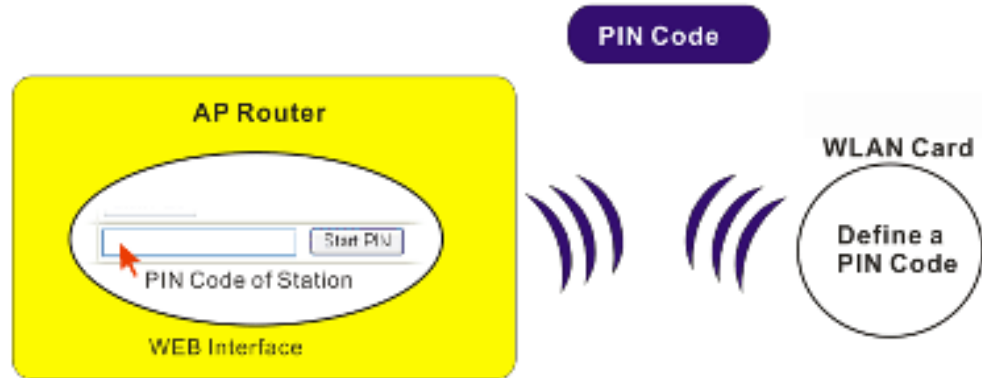
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for 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*.

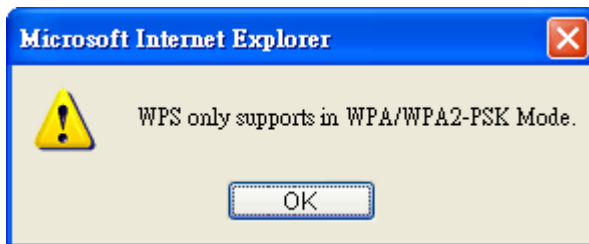
- On the side of Vigor 2850 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- 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	DrayTek
Authentication Mode	WPA2/PSK

**Device Configure**

Configure via Push Button	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/>

Status: Ready

Note: WPS can help your wireless client automatically connect to the Access point.  
: WPS is Disabled.  
: WPS is Enabled.  
: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

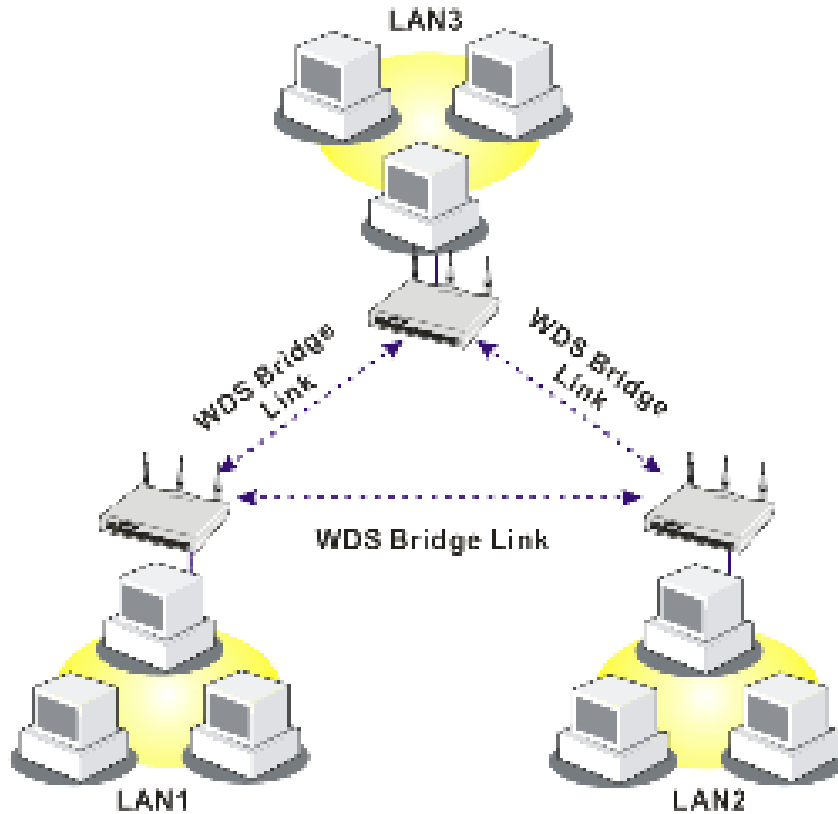
Item	Description
<b>Enable WPS</b>	Check this box to enable WPS setting.
<b>WPS Status</b>	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
<b>SSID</b>	Display the SSID1 of the router. WPS is supported by SSID1 only.
<b>Authentication Mode</b>	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
<b>Configure via Push Button</b>	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)
<b>Configure via Client PinCode</b>	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)

#### 4.14.6 WDS

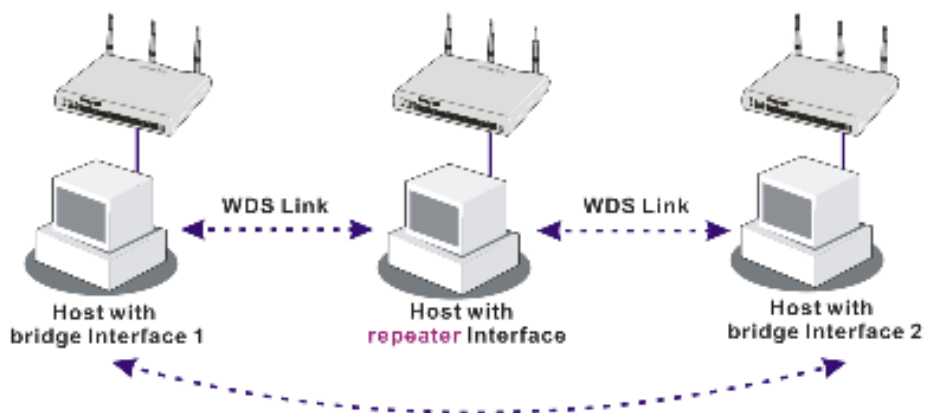
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:



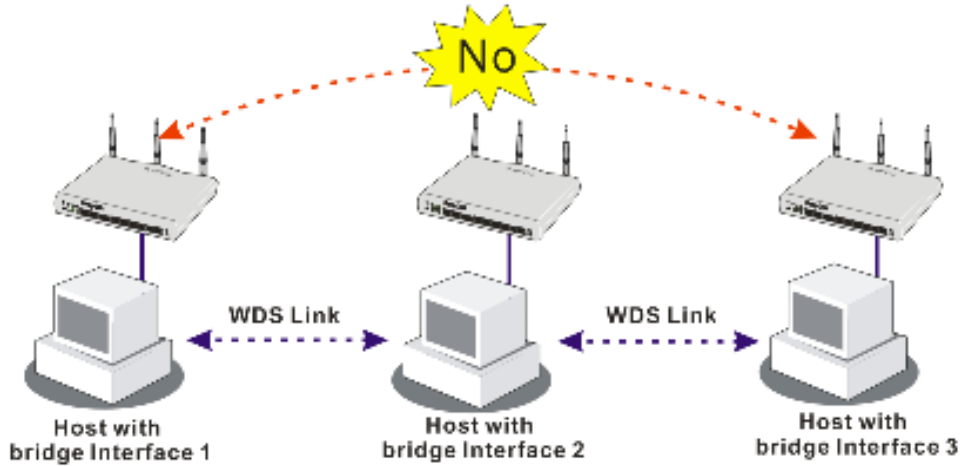
The application for the WDS-Repeater mode is depicted as below:



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.



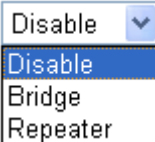
Click **WDS** from **Wireless LAN** menu. The following page will be shown.

Wireless LAN => WDS Settings

WDS Settings [Set to Factory Default](#)

<b>Mode:</b> <span style="border: 1px solid black; padding: 2px;">Bridge</span>	<b>Bridge</b> <b>Enable:</b> <input type="checkbox"/> Peer MAC Address <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <b>Note:</b> Disable unused links to get better performance.
<b>Security:</b> <input checked="" type="radio"/> Disable <input type="radio"/> WEP <input type="radio"/> Pre-shared Key	<b>Repeater</b> <b>Enable:</b> <input type="checkbox"/> Peer MAC Address <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <b>Access Point Function:</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>WEP:</b> Use the same WEP key set in <a href="#">Security Settings</a> .	<b>Status:</b> <input type="checkbox"/> Send "Hello" message to peers. <input type="button" value="Link Status"/>
<b>Pre-shared Key:</b> <b>Type:</b> <input type="radio"/> WPA <input checked="" type="radio"/> WPA2 <b>Key:</b> <input type="text" value=""/> <b>Note:</b> WPA and WPA2 are not compatible with legacy WPA. Type hex(1600) characters or 64 hexadecimal digits leading by "0x", for example "0f980142..." or "0f980142...".	<b>Note:</b> The status is valid only when the peer also supports this function.

Available settings are explained as follows:

Item	Description
<b>Mode</b>	<p>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.</p> 
<b>Security</b>	<p>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.</p>
<b>WEP</b>	<p>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.</p>
<b>Pre-shared Key</b>	<p><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.</p> <p><b>Key</b> - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.</p>
<b>Bridge</b>	<p>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 <b>Enable</b> box in the front of the MAC address after typing.</p>
<b>Repeater</b>	<p>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.</p>
<b>Access Point Function</b>	<p>Click <b>Enable</b> to make this router serving as an access point; click <b>Disable</b> to cancel this function.</p>
<b>Status</b>	<p>It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.</p>

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



## 4.14.7 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(2.4GHz) >> Advanced Setting

### HT Physical Mode

Operation Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Long Preamble	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Packet OVERDRIVE™ TX Burst	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

OK

Wireless LAN(5GHz) >> Advanced Setting

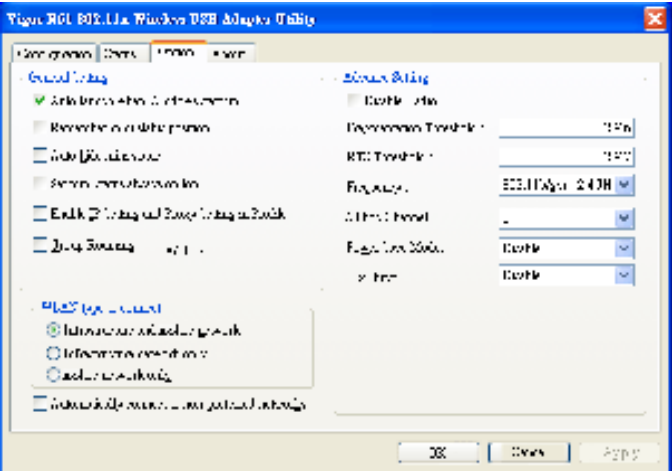
### Physical Mode

Operation Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

OK

Available settings are explained as follows:

Item	Description
<b>Operation Mode</b>	<p><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.</p> <p><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.</p>
<b>Channel Bandwidth</b>	<p><b>20-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p><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.</p>
<b>Guard Interval</b>	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.
<b>Aggregation MSDU</b>	Aggregation MSDU can combine frames with different

	<p>sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable</b>.</p>
<p><b>Long Preamble</b></p>	<p>This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click <b>Enable</b> to use <b>Long Preamble</b> if needed to communicate with this kind of devices.</p>
<p><b>Packet-OVERDRIVE</b></p>	<p>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.</p> <p><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>).</p>  <p>Tx Burst : <span style="border: 1px solid black; padding: 2px;">Disable</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px;">Disable</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px; background-color: #e0e0e0;">Enable</span></p> <p><b>Note:</b> * means the real transmission rate depends on the environment of the network.</p>

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

## 4.14.8 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.

[Wireless LAN >> WMM Configuration](#)

WMM Configuration
[Set to Factory Default](#)

WMM Capable  Enable  Disable

APSD Capable  Enable  Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	ArbPolicy
AC_BE	3	4	6	0	FI	<input type="checkbox"/>
AC_BK	7	4	10	0	FI	<input type="checkbox"/>
AC_VI	1	3	4	94	FI	<input type="checkbox"/>
AC_VO	1	2	3	47	FI	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	4	10	0	FI
AC_BK	7	4	10	0	FI
AC_VI	2	3	4	94	FI
AC_VO	2	2	3	47	FI

Available settings are explained as follows:

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.
<b>Txop</b>	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.
<b>ACM</b>	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> Vigor2925 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
<b>AckPolicy</b>	“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.

## 4.14.9 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.

[Wireless LAN => Access Point Discovery](#)

Access Point List

BSSID	Channel	SSID
<input type="button" value="Scan"/>		

See [Statistics](#).

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the router.

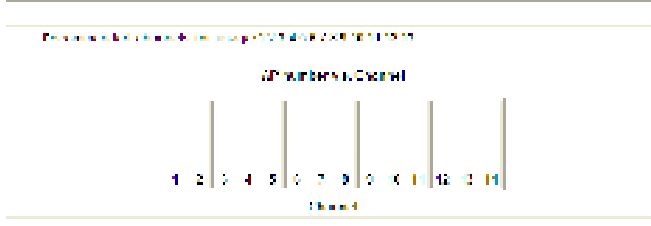
---

Add to [WDS Settings](#) :

AP's MAC address:

Bridge  Repeater

Available settings are explained as follows:

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. 
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.

### 4.14.10 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.

Wireless LAN >> Station List

Station List

Status	MAC Address	Associated with
Refresh		

**Status Codes :**  
 C: Connected, No encryption.  
 E: Connected, WEP.  
 P: Connected, WPA.  
 A: Connected, WPA2.  
 B: Blocked by Access Control.  
 N: Connecting.  
 I: Fail to pass WPA/WPA2 authentication.

**Note:** When a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

**Add to Access Control :**

Client's MAC address     :  :  :  :  :

Add

Available settings are explained as follows:

Item	Description
<b>Refresh</b>	Click this button to refresh the status of station list.
<b>Add</b>	Click this button to add current typed MAC address into <b>Access Control</b> .

## 4.15 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.



### 4.15.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

---

SSL VPN General Setup

Port	443 (Default: 443)
Server Certificate	self-signed
Encryption Key Algorithm	<input type="radio"/> High - AES(128 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) <input type="radio"/> Low - DES

Note: The settings will set on all SSL applications.

Available settings are explained as follows:

Item	Description
<b>Port</b>	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in <b>System Maintenance&gt;&gt;Management</b> . In general, the default setting is 443.
<b>Server Certificate</b>	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 Algorithm</b>	Choose the encryption level for the data connection in SSL VPN server.
---------------------------------	--

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

## 4.15.2 SSL Web Proxy

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

[SSL VPN >> SSL Web Proxy](#)

SSL Web Proxy Servers Profiles: | [Set to Factory Default](#)

Index	Name	URL	Active
<a href="#">1.</a>			=
<a href="#">2.</a>			=
<a href="#">3.</a>			=
<a href="#">4.</a>			x
<a href="#">5.</a>			x
<a href="#">6.</a>			x
<a href="#">7.</a>			x
<a href="#">8.</a>			=
<a href="#">9.</a>			=
<a href="#">10.</a>			=

Each item is explained as follows:

Item	Description
<b>Name</b>	Display the name of the profile that you create.
<b>URL</b>	Display the URL.
<b>Active</b>	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	<input type="text"/>
URL	<input type="text"/>
Host IP Address	<input type="text"/>
Access Method	<input type="text" value="Disable"/> <input type="text" value="Disable"/> <input type="text" value="Required Full Redirection"/>

Note: URL format must be entered as http://  
Domain\_name is a FQDN.  //Domain\_name/directory where  
Domain\_name is a FQDN.

Available settings are explained as follows:

Item	Description
<b>Name</b>	Type name of the profile. The length of the name is limited to 15 characters.



<b>URL</b>	Type the address (function variation or IP address) or path of the proxy server.
<b>Host IP Address</b>	If you type function variation as URL, you have to type corresponding IP address in this field. Such field must match with URL setting.
<b>Access Method</b>	<p>There are three modes for you to choose.</p> <p><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.</p> <p><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.</p> <p><b>SSL</b> – if you choose such selection, web proxy over SSL will be applied for VPN.</p>

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

### 4.15.3 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

SSL Applications Profiles: | [Set to Factory Default](#)

Index	Name	Host Address	Service	Active
1.				<input type="checkbox"/>
2.				<input type="checkbox"/>
3.				<input type="checkbox"/>
4.				<input type="checkbox"/>
5.				<input type="checkbox"/>
6.				<input type="checkbox"/>
7.				<input type="checkbox"/>
8.				<input type="checkbox"/>
9.				<input type="checkbox"/>
10.				<input type="checkbox"/>

Each item is explained as follows:

Item	Description
<b>Name</b>	Display the application name of the profile that you create.
<b>Host Address</b>	Display the IP address for VNC/RDP or SAMBA path.
<b>Service</b>	Display the type of the service selected, e.g., VNC/RDP/SAMBA.
<b>Active</b>	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	Host
<a href="#">1.</a>		
<a href="#">2.</a>		
<a href="#">3.</a>		
<a href="#">4.</a>		

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: \_\_\_\_\_

Port: \_\_\_\_\_

Idle Timeout: \_\_\_\_\_

Bandwidth: 100%

Available settings are explained as follows:

Item	Description
<b>Enable Application Server</b>	Check the box to enable such profile.
<b>Application Name</b>	Type a name for such application. The length of the name is limited to 23 characters.
<b>Application</b>	<p>There are three types offered for you to create an application profile.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>---Please Select---</p> <p>---Please Select---</p> <p>Virtual Network Computing (VNC)</p> <p>Remote Desktop Protocol (RDP)</p> <p>Samba Application</p> </div> <p><b>Virtual Network Computing (VNC)</b> – It allows you to access and control a remote PC through VNC protocol.</p> <p><b>Remote Desktop Protocol (RDP)</b> – It allows you to access and control a remote PC through RDP protocol.</p>

	<b>Samba Application</b> – It allows you to access and control a remote PC through Samba service.
<b>IP Address</b>	If you choose VNC or RDP, you have to type the IP address for this protocol.
<b>Port</b>	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
<b>Idle Timeout</b>	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
<b>Scaling</b>	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
<b>Screen Size</b>	If you choose RDP, you have to choose the screen size for such application.
<b>Samba Path</b>	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: | Restore Factory Default |

Index	Name	Host Address	Service	Active
1	VNC_1	192.168.1.51:5900	VNC	<input checked="" type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>

## 4.15.4 User Account

With SSL VPN, Vigor2925 series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, Vigor2925series allows up to 16 simultaneous incoming users.

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**.

SSL VPN >> Remote Dial in User

Remote Access User Accounts Set to Factory Default

Views:  All  Online  Offline Search

Index	User	Active	Status	Index	User	Active	Status
1	???	<input type="checkbox"/>	---	16	???	<input type="checkbox"/>	---
2	???	<input type="checkbox"/>	---	17	???	<input type="checkbox"/>	---
3	???	<input type="checkbox"/>	---	18	???	<input type="checkbox"/>	---
4	???	<input type="checkbox"/>	---	19	???	<input type="checkbox"/>	---
5	???	<input type="checkbox"/>	---	20	???	<input type="checkbox"/>	---
6	???	<input type="checkbox"/>	---	21	???	<input type="checkbox"/>	---
7	???	<input type="checkbox"/>	---	22	???	<input type="checkbox"/>	---
8	???	<input type="checkbox"/>	---	23	???	<input type="checkbox"/>	---
9	???	<input type="checkbox"/>	---	24	???	<input type="checkbox"/>	---
10	???	<input type="checkbox"/>	---	25	???	<input type="checkbox"/>	---
11	???	<input type="checkbox"/>	---	26	???	<input type="checkbox"/>	---
12	???	<input type="checkbox"/>	---	27	???	<input type="checkbox"/>	---
13	???	<input type="checkbox"/>	---	28	???	<input type="checkbox"/>	---
14	???	<input type="checkbox"/>	---	29	???	<input type="checkbox"/>	---
15	???	<input type="checkbox"/>	---	30	???	<input type="checkbox"/>	---
16	???	<input type="checkbox"/>	---	31	???	<input type="checkbox"/>	---

1/37 | 18/64 Next

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

**Note:** There are 64 profiles for configuration but the number of concurrent sessions is up to 25 sessions.

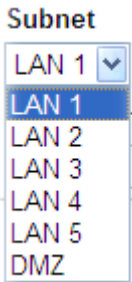
Click each index to edit one remote user profile.

Index No. 1

<p><b>User account and Authentication</b></p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout: <input type="text" value="300"/> seconds</p> <p><b>Allowed Dial-In Type</b></p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy: <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> L2TP Tunnel</p> <p><input checked="" type="checkbox"/> OpenVPN Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP</p> <p>or Peer ID: <input type="text"/></p> <p>Network Naming Method: <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block (For some ISMP, IP Camera, DSCP Delay, etc.)</p> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username: <input type="text" value="999"/></p> <p>Password (Max 19 char): <input type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords (MOTP)</p> <p>PIN Code: <input type="text"/></p> <p>Secret: <input type="text"/></p> <p><b>IKL Authentication Method</b></p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKL Pre-Shared Key: <input type="text"/></p> <p><input type="checkbox"/> Digital Signature (X.509)</p> <p>Name: <input type="text"/></p> <p><b>IPsec Security Method</b></p> <p><input checked="" type="checkbox"/> Medium (AH)</p> <p>High (ESP): <input type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input type="checkbox"/> AES</p> <p>Local ID (optional): <input type="text"/></p>
--	---

Available settings are explained as follows:

Item	Description
<b>User account and Authentication</b>	<p><b>Enable this account</b> - Check the box to enable this function.</p> <p><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.</p>
<b>Allowed Dial-In Type</b>	<p><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.</p> <p><b>IPsec Tunnel</b> - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p><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:</p> <ul style="list-style-type: none"> <li>● <b>None</b> - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.</li> <li>● <b>Nice to Have</b> - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.</li> </ul>

Item	Description
	<ul style="list-style-type: none"> <li>● <b>Must</b> -Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul> <p><b>SSL Tunnel</b> - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p><b>OpenVPN Tunnel</b> - Allow the remote dial-in user to make an OpenVPN connection through Internet.</p> <p><b>Specify Remote Node</b> - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b>.</p> <p><b>Netbios Naming Packet</b></p> <ul style="list-style-type: none"> <li>● <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</li> <li>● <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.</li> </ul> <p><b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> <li>● <b>Pass</b> – Click this button to let multicast packets pass through the router.</li> <li>● <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.</li> </ul>
<b>Subnet</b>	<p>Chose one of the subnet selections for such VPN profile.</p>  <p><b>Assign Static IP Address</b> – Please type a static IP address for the subnet you specified.</p>
<b>User Name</b>	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
<b>Password</b>	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
<b>Enable Mobile One-Time Passwords</b>	Check this box to make the authentication with mOTP function.

Item	Description
<b>(mOTP)</b>	<p><b>PIN Code</b> – Type the code for authentication (e.g, 1234).</p> <p><b>Secret</b> – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
<b>IKE Authentication Method</b>	<p>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.</p> <p><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.</p> <p><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 &gt;&gt;IPSec Peer Identity</b>.</p>
<b>IPSec Security Method</b>	<p>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.</p> <p><b>Medium-Authentication Header (AH)</b> means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p><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.</p> <p><b>Local ID</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.</p>

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

## 4.15.5 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 VPN >> User Group](#)

[SSL User Group Profiles](#) [Set to Factory Default](#)

Index	Name	Status
1.		=
2.		=
3.		=
4.		=
5.		=
6.		=
7.		=
8.		=
9.		=
10.		=

Each item is explained as follows:

Item	Description
<b>Set to Factory Default</b>	Click to clear all indexes.
<b>Index</b>	Display the number of the client which connecting to FTP server.
<b>Name</b>	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**  
 **Enable**

**Group Name**

**Access Authority**

**SSL Web Proxy**       **SSL Application**

**Authentication Methods**


**Local User Database**

Available User Accounts	Selected User Accounts

**RADIUS**  
 **LDAP / Active Directory**



Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check this box to enable such profile.
<b>Group Name</b>	Type a name for such profile. The length of the name is limited to 23 characters.
<b>Access Authority</b>	<p>Specify the authority for such profile.</p> <p>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.</p> 
<b>Authentication Methods</b>	<p>It can determine the authentication method used for such profile.</p> <p><b>Local User DataBase</b> – The system will do the authentication by using the user defined account profiles (in <b>VPN and Remote Access&gt;&gt;Remote Dial-In User</b>). The enabled profiles will be listed in the <b>Available User Account</b> on the left box. To add a profile into a group, simply choose the one from the left box and click the &gt;&gt; button. It will be displayed in the <b>Selected User Account</b> on the right box. For detailed information about configuring the profile setting, refer to <b>Objects Setting&gt;&gt;IP Group</b>.</p> <p><b>RADIUS</b> – The RADIUS server will do the authentication by using the username and password</p> <p><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.</p> <p>If the above three options are enabled, the system will do the authentication based on them in sequence.</p>

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

## 4.15.6 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.



Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.

SSL VPN >> Online User Status

Refresh Seconds:

Active User	Host IP	Time out(seconds)	Action
mike	172.17.1.2	255	<input type="button" value="Drop"/>

Available settings are explained as follows:

Item	Description
<b>Active User</b>	Display current user who visit SSL VPN server.
<b>Host IP</b>	Display the IP address for the host.
<b>Time out</b>	Display the time remaining for logging out.
<b>Action</b>	You can click <b>Drop</b> to drop certain login user from the router's SSL Portal UI.

## 4.16 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.



### 4.16.1 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](#)

**USB General Settings**

**General Settings**

Simultaneous FTP Connectors:  (Maximum 6)

Default Charset:

**Samba Service Settings(Network Neighborhood)**

Enable  Disable

**Access Mode**

LAN Only  LAN And WAN

**NetBios Name Service**

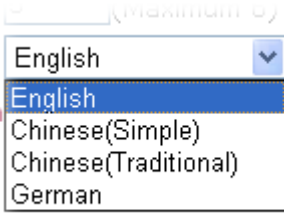
Workgroup Name:

Host Name:

Note: 1. If charset is set to "English", only English long file name is supported.  
 2. Multi sessions ftp download will be banned by Router FTP server. If your ftp client have multi connection mechanisms, such as FileZilla, you may limit a 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 16 characters and a host name can have as many as 21 characters, but both cannot contain any of the following: \ : \* ' / | ?

Available settings are explained as follows:

Item	Description
General Settings	<b>Simultaneous FTP Connections</b> - This field is used to specify the quantity of the FTP sessions. The router allows

	<p>up to 6 FTP sessions connecting to USB storage disk at one time.</p> <p><b>Default Charset</b> - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.</p> 
<b>Samba Service Settings</b>	Click <b>Enable</b> to invoke samba service via the router.
<b>Access Mode</b>	<p><b>LAN Only</b> – Users coming from internet cannot connect to the samba server of the router.</p> <p><b>LAN And WAN</b> - Both LAN and WAN users can access samba server of the router.</p>
<b>NetBios Name Service</b>	<p>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--- ; : " &lt; &gt; * + = \   ?.</p> <p><b>Workgroup Name</b> – Type a name for the workgroup.</p> <p><b>Host Name</b> – Type the host name for the router.</p>

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

## 4.16.2 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](#)

USB User Management			<a href="#">Set to Factory Default</a>		
Index	Username	Home Folder	Index	Username	Home Folder
<a href="#">1.</a>			<a href="#">9.</a>		
<a href="#">2.</a>			<a href="#">10.</a>		
<a href="#">3.</a>			<a href="#">11.</a>		
<a href="#">4.</a>			<a href="#">12.</a>		
<a href="#">5.</a>			<a href="#">13.</a>		
<a href="#">6.</a>			<a href="#">14.</a>		
<a href="#">7.</a>			<a href="#">15.</a>		
<a href="#">8.</a>			<a href="#">16.</a>		

Click index number to access into configuration page.



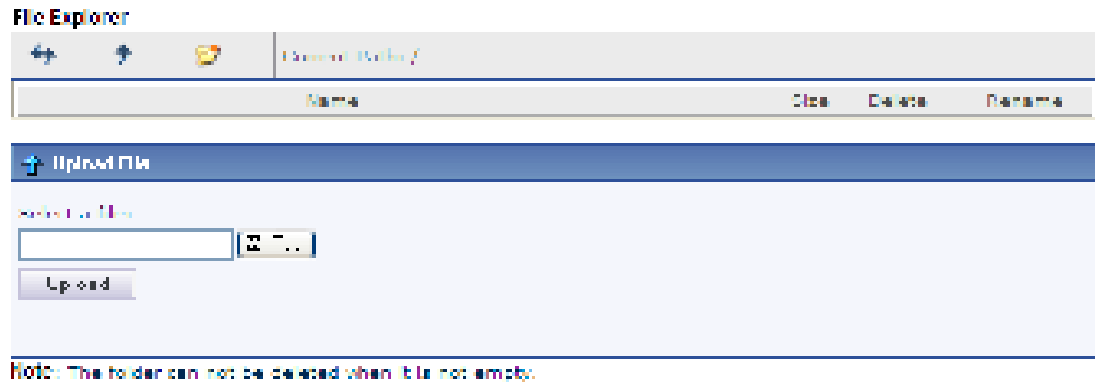
	<p>Only “/” can be used in such case.</p> <p>You can click  to open the following dialog to add any new folder which can be specified as the Home Folder.</p> 
<p><b>Access Rule</b></p>	<p>It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.</p> <p><b>File</b> – Check the items (Read, Write and Delete) for such profile.</p> <p><b>Directory</b> –Check the items (List, Create and Remove) for such profile.</p>

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.




### 4.16.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Application >> File Explorer



Available settings are explained as follows:

Item	Description
 <b>Refresh</b>	Click this icon to refresh files list.
 <b>Back</b>	Click this icon to return to the upper directory.
 <b>Create</b>	Click this icon to add a new folder.
<b>Current Path</b>	Display current folder.
<b>Upload</b>	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.

### 4.16.4 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. In addition, the status of the USB modem or USB printer connecting to Vigor router can be checked from such page. 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

### USB Mass Storage Device Status

Connection Status: No Disk Connected		Disconnected USB Disk	
Disk Capacity: 0 MB			
Free Capacity: 0 MB <a href="#">Refresh</a>			
USB Disk Users Connected		<a href="#">Refresh</a>	
Index	Service	IP Address(Host)	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.

Available settings are explained as follows:

Item	Description
<b>Connection Status</b>	If there is no USB storage disk connected to Vigor router, “ <b>No Disk Connected</b> ” will be shown here.
<b>Disk Capacity</b>	It displays the total capacity of the USB storage disk.
<b>Free Capacity</b>	It displays the free space of the USB storage disk. Click <b>Refresh</b> at any time to get new status for free capacity.
<b>Index</b>	It displays the number of the client which connecting to FTP server.
<b>IP Address</b>	It displays the IP address of the user’s host which connecting to the FTP server.
<b>Username</b>	It displays the username that user uses to login to the FTP server.

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.



## 4.16.5 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 >> Temperature Sensor Setting

Temperature Sensor Settings      Temperature Chart

Display Settings

Temperature Calibration: 0.00

Temperature Unit:  Celsius  Fahrenheit

Alarm Settings

Enable Syslog Alarm

Upper temperature limit: 35.00

Lower temperature limit: 15.00

OK

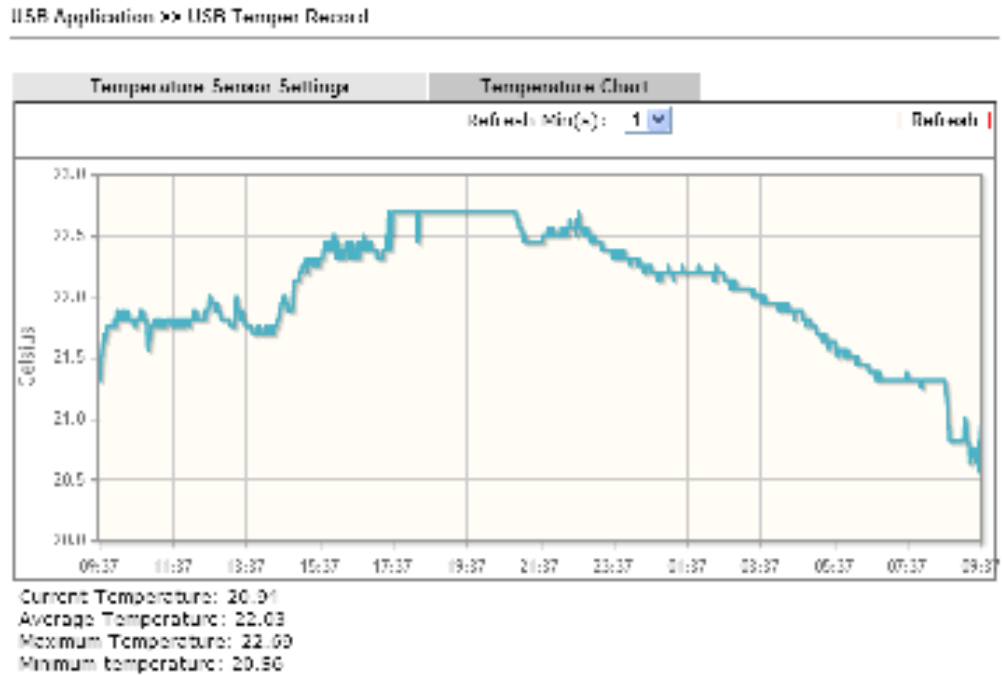
Available settings are explained as follows:

Item	Description
Display Settings	<b>Temperature Calibration</b> - Type a value used for correcting the temperature error. <b>Temperature Unit</b> - Choose the display unit of the temperature. There are two types for you to choose.
Alarm Settings	<b>Enable Syslog Alarm</b> – Check this box to enable the function. <b>Upper temperature limit/Lower temperature limit</b> - Type the upper limit and lower limit for the system to send out temperature alert.

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

## Temperature Chart

Below shows an example of temperature graph:



### 4.16.6 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.

USB Application >> Modem Support List

---

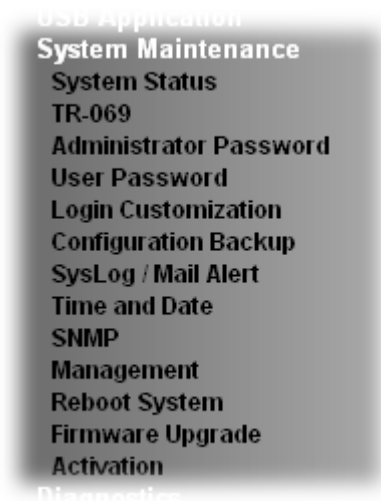
The following compatibility tests listed above vigor router models with USB modems / mobiles. If it is confirmed as the latest and still does not work, please contact support@draytek.com

3.5G		
Brand	Model	Status
Aiko	Aiko 810	✓
Benliao	Benliao C170	✓
Benliao	Benliao C270	✓
Benliao	Benliao C121	✓
Benliao	Benliao C111	✓
Benliao	Benliao C102	✓
Huawei	Huawei E1550	✓
Huawei	Huawei E171	✓
Huawei	Huawei E220	✓
Sony Ericsson	Sony Ericsson M1000	✓
Vodafone	Vodafone K1060 /	✓
Vodafone	Vodafone K4600	✓
ZTE	ZTE M 525	✓
ZTE	ZTE M 527 plus	✓
ZTE	ZTE M 511	✓
ZTE	ZTE M 515	✓

## 4.17 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 Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.



### 4.17.1 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 : Vigor2925n  
 Firmware Version : 3.7.3  
 Build Date/Time : Oct 9 2013 16:07:43

LAN									
	MAC Address	IP	Subnet	Mask	Static	Wan	Bridge	SN	
LAN1	11-10-5A-1111	1	192.168.1	255.255.255	0			01	01
LAN2	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01
LAN3	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01
LAN4	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01
LAN5	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01
DMZ/PC	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01
2nd PC/Server	11-10-5A-1111	1	192.168.1	255.255.255	Yes			01	01

Wireless LAN			
MAC Address	Frequency	Channel	Transmit Power
11-10-5A-1111	5.180	11	200mW

WAN				
Interface	MAC Address	Connection	IP Address	Default Gateway
WAN1	11-10-5A-1111	PPPoE		
WAN2	11-10-5A-1111	PPPoE		
WAN3	11-10-5A-1111	PPPoE		

IPv6		
Address	Prefix	Interface
LAN	FE80::5A11:1111::1	eth0

User Mode : 3.0.1.11

Available settings are explained as follows:

<b>Item</b>	<b>Description</b>
<b>Model Name</b>	Display the model name of the router.
<b>Firmware Version</b>	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
<b>LAN</b>	<p><b>MAC Address</b> - Display the MAC address of the LAN Interface.</p> <p><b>IP Address</b> - Display the IP address of the LAN interface.</p> <p><b>Subnet Mask</b> - Display the subnet mask address of the LAN interface.</p> <p><b>DHCP Server</b> - Display the current status of DHCP server of the LAN interface</p> <p><b>DNS</b> - Display the assigned IP address of the primary DNS.</p>
<b>WAN</b>	<p><b>Link Status</b> - Display current connection status.</p> <p><b>MAC Address</b> - Display the MAC address of the WAN Interface.</p> <p><b>Connection</b> - Display the connection type.</p> <p><b>IP Address</b> - Display the IP address of the WAN interface.</p> <p><b>Default Gateway</b> - Display the assigned IP address of the default gateway.</p>
<b>IPv6</b>	<p><b>Address</b> - Display the IPv6 address for LAN.</p> <p><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.</p> <p><b>Internet Access Mode</b> – Display the connection mode chosen for accessing into Internet.</p>

## 4.17.2 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.

System Maintenance >> TR-069 Setting

### ACS and CPE Settings

ACS Server On	<input checked="" type="checkbox"/> Enable
ACS Server	
URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
CPE Client	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
URL	<input type="text"/>
Port	<input type="text" value="4444"/>
Username	<input type="text" value="Mpor"/>
Password	<input type="password"/>

### Periodic Inform Settings

<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	
Interval Time	<input type="text" value="300"/> second(s)

### STUN Settings

<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
Server Address	<input type="text"/>
Server Port	<input type="text" value="3443"/>
Minimum Keep Alive Period	<input type="text" value="60"/> second(s)
Maximum Keep Alive Period	<input type="text" value="1"/> second(s)

Available settings are explained as follows:

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.
<b>STUN Settings</b>	<p>The default is <b>Disable</b>. If you click <b>Enable</b>, please type the relational settings listed below:</p> <p><b>Server IP</b> – Type the IP address of the STUN server.</p> <p><b>Server Port</b> – Type the port number of the STUN server.</p> <p><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”.</p> <p><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.</p>

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

### 4.17.3 Administrator Password

This page allows you to set new password.

[System Maintenance > Administrator Password Setup](#)

Administrator Password

Old Password	.....
New Password	.....
Confirm Password	.....

Note: Password can contain only a-z A-Z 0-9 . : ; ' " ! ~ ! ? \* ^ & | { }

**OK**

Available settings are explained as follows:

Item	Description
<b>Old Password</b>	Type in the old password. The factory default setting for password is “ <b>admin</b> ”.
<b>New Password</b>	Type in new password in this field. The length of the password is limited to 23 characters.
<b>Confirm Password</b>	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.

## 4.17.4 User Password

This page allows you to set new password for user operation.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password Set to Factory Default

Password	<input type="password"/>
Confirm Password	<input type="password"/>

Note: Password can contain only a-z, A-Z, 0-9, \_ and - ( ), / and @ is illegal, but "!" and "!" is illegal, but "!" and "!" is OK.

Available settings are explained as follows:

Item	Description
<b>Enable User Mode for simple web configuration</b>	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 use interface accessed by using the administrator password.
<b>Password</b>	Type in new password in this field. The length of the password is limited to 31 characters.
<b>Confirm Password</b>	Type in the new password again.
<b>Set to Factory Default</b>	Click to return to the factory default setting.

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**.
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**.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password

Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password

---

Global 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 field of **Password** and click **Login**.

**DrayTek****Vigor2925 Series**

**Login**

**Username**

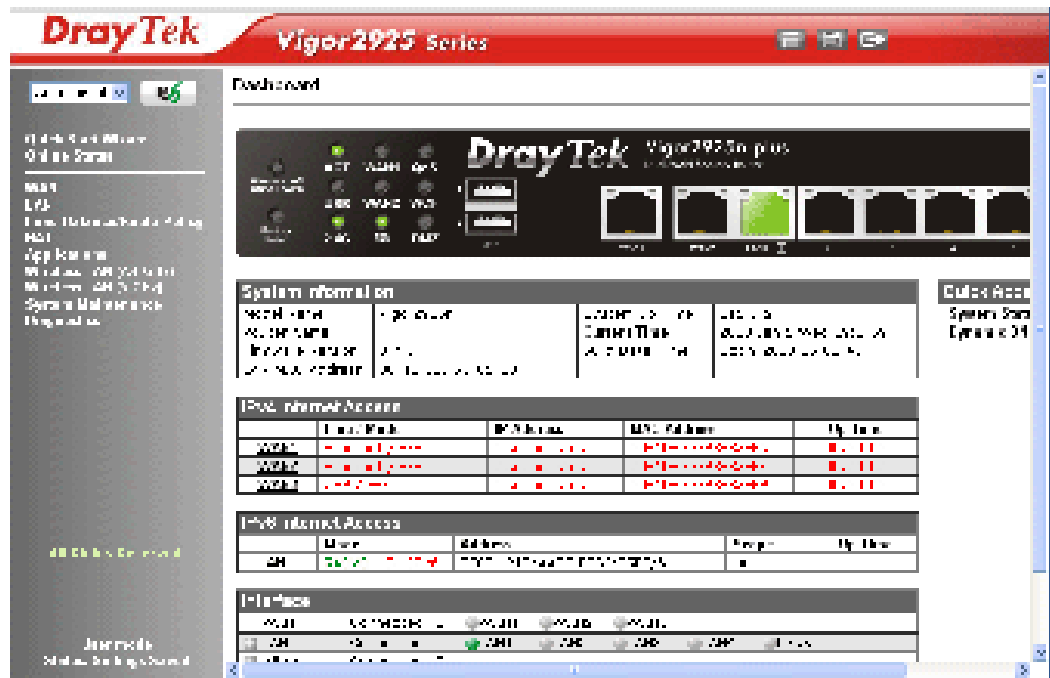
**Password**

**Group**  ▼

Copyright © 2012 DrayTek Corp. All Rights Reserved.



- The main screen with User Mode will be shown as follows.



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.

## 4.17.5 Login Page Greeting

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 Page Greeting](#)

### Login Page Greeting

Enable

Login Page Title:  (31 char max.)

Welcome Message and Bulletin (Max 511 characters): [Preview](#) [Set to Factory Default](#)

```
<div style=font-size:12px;color:red>Welcome Message</div><div style=font-size:10px>This welcome message is displayed in the login page of the router. Replace this text with your own message. </div></div>
```

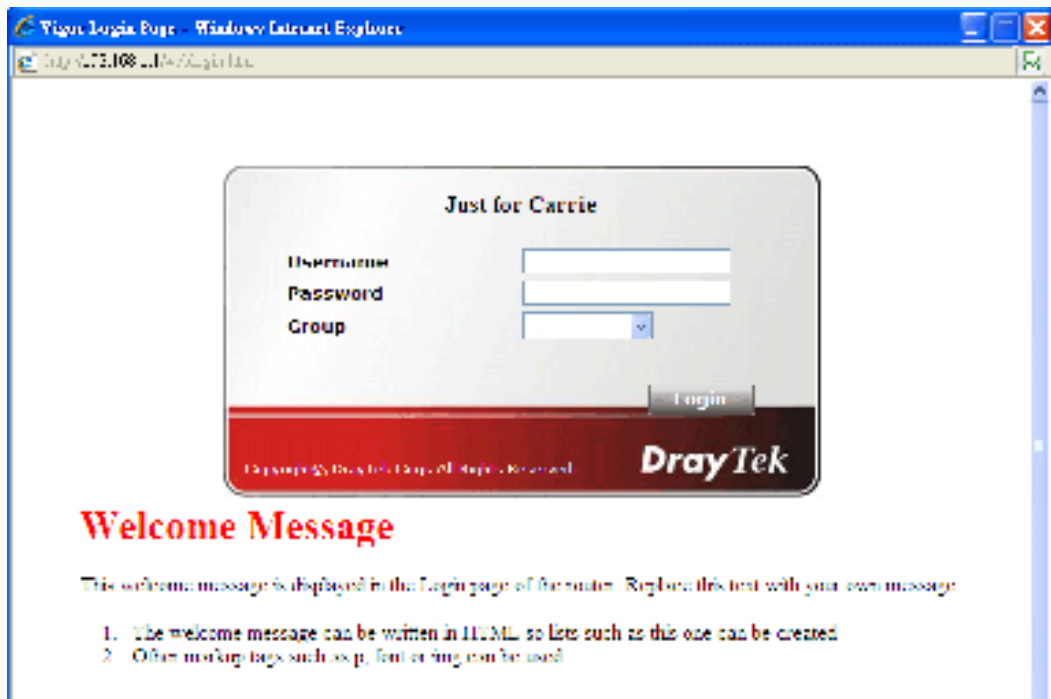
Examples of Welcome Message and Bulletin:  

```
<div style=font-size:12px;color:red>Welcome Message</div><div style=font-size:10px>This welcome message is displayed in the login page of the router. Replace this text with your own message. </div></div>
```

Available settings are explained as follows:

Item	Description
<b>Enable</b>	Check this box to enable the login customization function.
<b>Login Page Title</b>	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
<b>Welcome Message and Bulletin</b>	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
<b>Preview</b>	Click it to display the preview of the login window based on the settings on this web page.
<b>Set to Factory Default</b>	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.



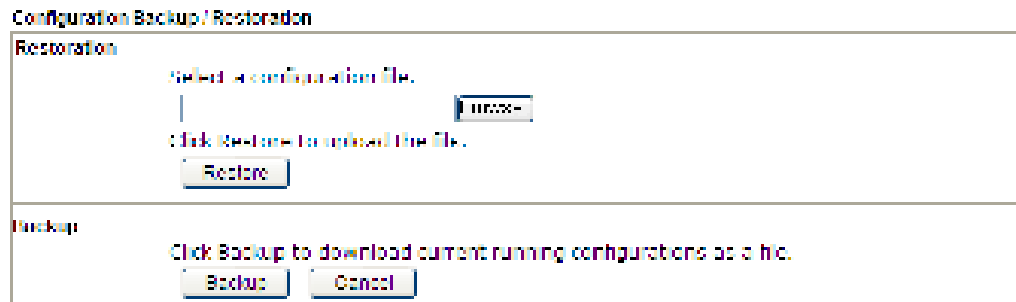
## 4.17.6 Configuration Backup

### Backup the Configuration

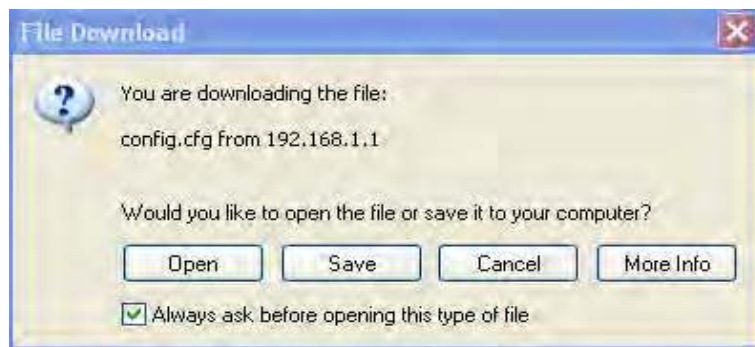
Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

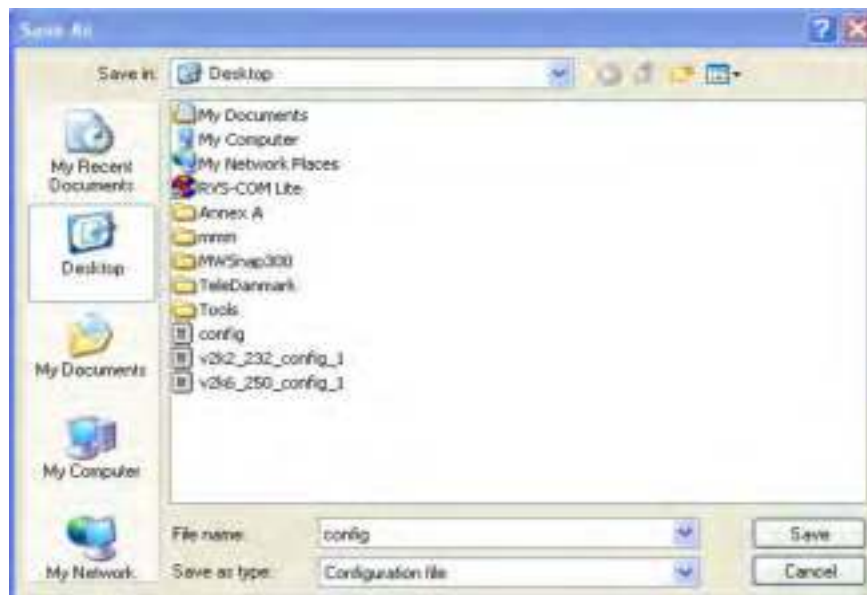
System Maintenance >> Configuration Backup



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

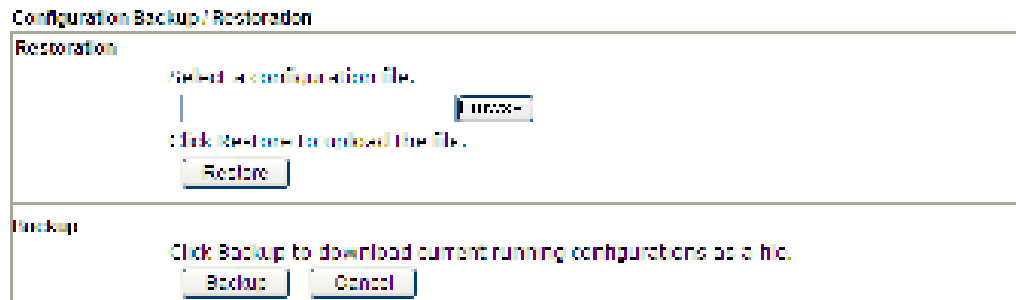
The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

## Restore Configuration

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup



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.

## 4.17.7 Syslog/Mail Alert

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

[System Maintenance](#) >> [Syslog / Mail Alert Setup](#)

**Syslog / Mail Alert Setup**

<p><b>Syslog Access Setup</b></p> <p><input checked="" type="checkbox"/> <b>Enable</b></p> <p><b>Syslog Save to:</b></p> <p><input checked="" type="checkbox"/> <b>Syslog Server</b></p> <p><input type="checkbox"/> <b>USB Disk</b></p> <p><b>Router Name:</b> _____</p> <p><b>Server IP Address:</b> _____</p> <p><b>Destination Port:</b> <input type="text" value="514"/></p> <p><b>Mail Syslog:</b> <input type="checkbox"/> <b>Enable</b></p> <p><b>Enable syslog messages:</b></p> <p><input checked="" type="checkbox"/> <b>Firewall Log</b></p> <p><input checked="" type="checkbox"/> <b>VPN Log</b></p> <p><input checked="" type="checkbox"/> <b>User Access Log</b></p> <p><input checked="" type="checkbox"/> <b>WAN Log</b></p> <p><input checked="" type="checkbox"/> <b>Router/DSL Information</b></p> <p><b>Mail log Setup</b></p> <p><input type="checkbox"/> <b>Enable</b></p> <p><b>Mail log Port:</b> <input type="text" value="514"/></p>	<p><b>Mail Alert Setup</b></p> <p><input type="checkbox"/> <b>Enable</b> <span style="float: right;"><input type="button" value="Send a test e-mail"/></span></p> <p><b>SMTP Server:</b> _____</p> <p><b>SMTP Port:</b> <input type="text" value="25"/></p> <p><b>Mail To:</b> _____</p> <p><b>Return-Path:</b> _____</p> <p><input type="checkbox"/> <b>Use SSL</b></p> <p><input type="checkbox"/> <b>Authentication</b></p> <p><b>User Name:</b> _____</p> <p><b>Password:</b> _____</p> <p><b>Enable E-Mail Alert:</b></p> <p><input checked="" type="checkbox"/> <b>Mail Attack</b></p> <p><input checked="" type="checkbox"/> <b>IM POP</b></p> <p><input checked="" type="checkbox"/> <b>VPN Log</b></p>
--	---

**Note:** 1. Mail Syslog cannot be activated unless USB Disk is listed 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.

Available settings are explained as follows:

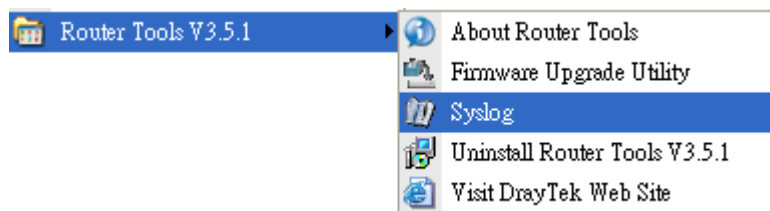
Item	Description
<b>SysLog Access Setup</b>	<p><b>Enable</b> - Check <b>Enable</b> to activate function of syslog.</p> <p><b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.</p> <p><b>USB Disk</b> - Check <b>USB Disk</b> to save the log to the attached USB storage disk.</p> <p><b>Router Name</b> - Display the name for such router configured in <b>System Maintenance</b>&gt;&gt;<b>Management</b>.</p> <p>If there is no name here, simply lick the link to access into <b>System Maintenance</b>&gt;&gt;<b>Management</b> to set the router name.</p> <p><b>Server IP Address</b> -The IP address of the Syslog server.</p> <p><b>Destination Port</b> - Assign a port for the Syslog protocol.</p> <p><b>Mail Syslog</b> – Check the box to recode the mail event on Syslog.</p> <p><b>Enable syslog message</b> - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, WAN, Router/DSL information to Syslog.</p>

<b>AlertLog Setup</b>	<p>Check <b>Enable</b> to activate function of alert log.</p> <p><b>AlertLog Port</b> - Type the port number for alert log. The default setting is 514.</p>
<b>Mail Alert Setup</b>	<p>Check <b>Enable</b> to activate function of mail alert.</p> <p><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.</p> <p><b>SMTP Server/SMTP Port</b> - The IP address/Port number of the SMTP server.</p> <p><b>Mail To</b> - Assign a mail address for sending mails out.</p> <p><b>Return-Path</b> - Assign a path for receiving the mail from outside.</p> <p><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.</p> <p><b>Authentication</b> - Check this box to activate this function while using e-mail application.</p> <ul style="list-style-type: none"> <li>● <b>User Name</b> - Type the user name for authentication.</li> <li>● <b>Password</b> - Type the password for authentication.</li> </ul> <p><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.</p>

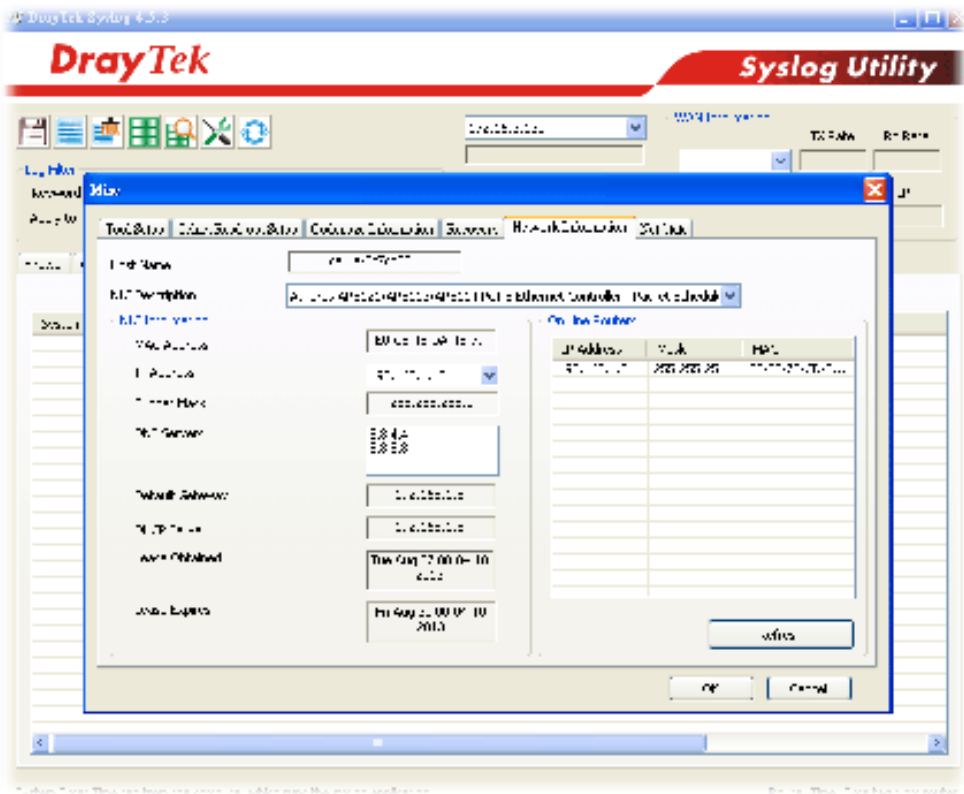
Click **OK** to save these settings.

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.





## 4.17.8 Time and Date

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

System Maintenance >> Time and Date

### Time Information

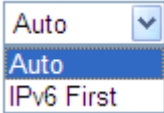
Current System Time	2008 Jan 2 Sat 19:12:4	Inquire Time
---------------------	------------------------	--------------

### Time Setup

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> Use Internet Time	
Time Server	pool.ntp.org
Priority	Auto
Time Zone	(GMT) Greenwich Mean Time Dublin
Enable Daylight Saving	<input type="checkbox"/>
Automatically Update Interval	30 min

OK Cancel

Available settings are explained as follows:

Item	Description
<b>Current System Time</b>	Click <b>Inquire Time</b> to get the current time.
<b>Use Browser Time</b>	Select this option to use the browser time from the remote administrator PC host as router's system time.
<b>Use Internet Time</b>	Select to inquire time information from Time Server on the Internet using assigned protocol.
<b>Time Server</b>	Type the IP address of the time server.
<b>Priority</b>	Choose Auto or IPv6 First as the priority. 
<b>Time Zone</b>	Select the time zone where the router is located.
<b>Enable Daylight Saving</b>	Check the box to enable the daylight saving. Such feature is available for certain area.
<b>Automatically Update Interval</b>	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

## 4.17.9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

Applications >> SNMP

### SNMP Setup

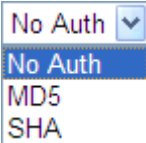
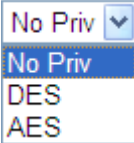
<input checked="" type="checkbox"/> Enable SNMP Agent	
Get Community	public
Set Community	private
Manager Host IP(IPv4)	
Manager Host IP(IPv6)	
Trap Community	public
Notification Host IP(IPv4)	
Notification Host IP(IPv6)	
Trap Timeout	10
<input type="checkbox"/> Enable SNMPv3 Agent	
USEM User	
Auth Algorithm	No Auth
Auth Password	
Privacy Algorithm	No Priv
Privacy Password	

OK

Cancel

Available settings are explained as follows:

Item	Description
<b>Enable SNMP Agent</b>	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> . The maximum length of the text is limited to 23 characters.
<b>Set Community</b>	Set community by typing a proper name. The default setting is <b>private</b> . The maximum length of the text is limited to 23 characters.
<b>Manager Host IP (IPv4)</b>	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
<b>Manager Host IP (IPv6)</b>	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.
<b>Trap Community</b>	Set trap community by typing a proper name. The default setting is <b>public</b> . The maximum length of the text is limited to 23 characters.
<b>Notification Host IP (IPv4)</b>	Set the IPv4 address of the host that will receive the trap community.

<b>Notification Host IP (IPv6)</b>	Set the IPv6 address of the host that will receive the trap community.
<b>Trap Timeout</b>	The default setting is 10 seconds.
<b>Enable SNMPV3 Agent</b>	Check it to enable this function.
<b>USM User</b>	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
<b>Auth Algorithm</b>	Choose one of the encryption methods listed below as the authentication algorithm. 
<b>Auth Password</b>	Type a password for authentication. The maximum length of the text is limited to 23 characters.
<b>Privacy Algorithm</b>	Choose one of the methods listed below as the privacy algorithm. 
<b>Privacy Password</b>	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

## 4.17.10 Management

This page allows you to manage the settings for access control, access list and port 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 Management Setup	IPv6 Management Setup												
<p>Router Name <input type="text"/></p> <p><b>Management Access Control</b></p> <p><input type="checkbox"/> Allow management from the Internet</p> <p>    <input type="checkbox"/> FTP Server</p> <p>    <input type="checkbox"/> HTTP Server</p> <p>    <input type="checkbox"/> HTTPS Server</p> <p>    <input type="checkbox"/> Telnet Server</p> <p>    <input type="checkbox"/> SSH Server</p> <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p><b>Access List</b></p> <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	<p><b>Management Port Setup</b></p> <p><input checked="" type="radio"/> User Define Ports    <input type="radio"/> Default Ports</p> <p>Telnet Port <input type="text" value="23"/> (Default: 23)</p> <p>HTTP Port <input type="text" value="80"/> (Default: 80)</p> <p>HTTPS Port <input type="text" value="443"/> (Default: 443)</p> <p>SSH Port <input type="text" value="21"/> (Default: 21)</p> <p>SNMP Port <input type="text" value="22"/> (Default: 22)</p>
List	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											
<input type="button" value="OK"/>													

Available settings are explained as follows:

Item	Description
<b>Router Name</b>	Type in the router name provided by ISP.
<b>Management Access Control</b>	<p><b>Allow management from the Internet</b> - 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.</p> <p><b>Disable PING from the Internet</b> - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
<b>Access List</b>	<p>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.</p> <p><b>List IP</b> - Indicate an IP address allowed to login to the router.</p> <p><b>Subnet Mask</b> - Represent a subnet mask allowed to login to the router.</p>
<b>Management Port Setup</b>	<b>User Define Ports</b> - Check to specify user-defined port

numbers for the Telnet, HTTP and FTP servers.

**Default Ports** - Check to use standard port numbers for the Telnet and HTTP servers.

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

## For IPv6

System Maintenance >> Management

IPv4 Management Setup | IPv6 Management Setup

**Management Access Control**

Allow management from the Internet

Telnet Server (Port: 23)

HTTP Server (Port: 80)

Enable PING from the Internet

---

**Access List**

List IPv6 Address / Prefix Length

1.		/ 128
2.		/ 128
3.		/ 128

Note: Telnet / HTTP server port is the same as IPv4.

OK

Available settings are explained as follows:

Item	Description
<b>Management Access Control</b>	<p><b>Allow management from the Internet</b> - 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.</p> <p><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.</p>
<b>Access List</b>	<p>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.</p> <p><b>IPv6 Address /Prefix Length</b>- Indicate the IP address(es) allowed to login to the router.</p>

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

## 4.17.11 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System

### Reboot System

**Do you want to reboot your router ?**

Using current configuration  
 Using factory default configuration

### 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.

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.

## 4.17.12 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](http://www.DrayTek.com) (or local DrayTek's web site) and FTP site is [ftp.DrayTek.com](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

Click Upgrade to upgrade the file.

### TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.3

Firmware Upgrade Procedures:


1. Click "OK" in the TFTP server.
2. Open the Firmware Upgrade Utility on the router by the TFTP server.
3. Check that the firmware filename is correct.
4. Click "Upgrade" in the Firmware Upgrade Utility on the router.
5. After the upgrade is completed, the TFTP server will automatically stop running.

Do you want to upgrade firmware?

Choose the right firmware by clicking **Browse**. Then, click **Upgrade**. The system will upgrade the firmware of the router automatically.

Or, click **OK**. The following screen will appear. Then, execute the firmware upgrade utility.

System Maintenance >> Firmware Upgrade

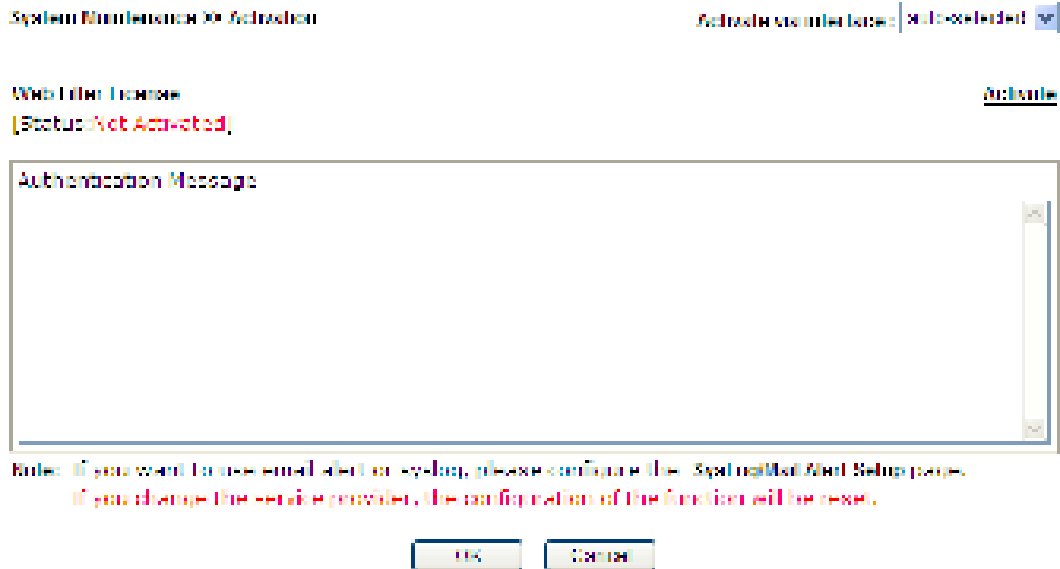
 TFTP server is running. Please execute the Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

### 4.17.13 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>.

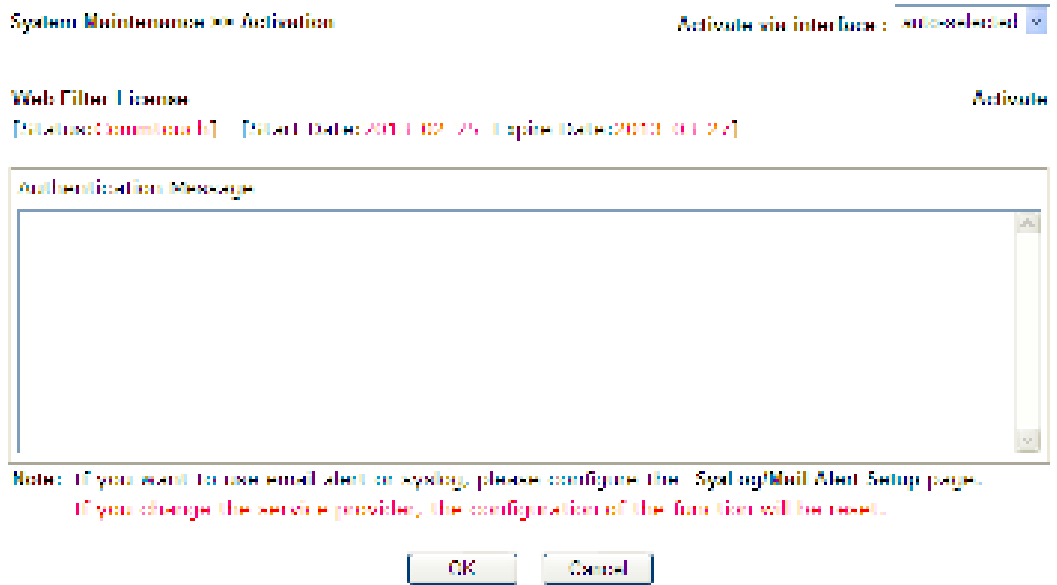


Available settings are explained as follows:

Item	Description
<b>Activate via Interface</b>	Choose WAN interface used by such device for activating Web Content Filter.  <div style="text-align: right;">                     Activate via interface : <span style="border: 1px solid black; padding: 2px;">auto-selected ▼</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px;">auto-selected</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px;">WAN 1</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px;">WAN 2</span>  <span style="border: 1px solid black; padding: 2px; display: inline-block; width: 100px;">WAN 3</span> </div>
<b>Activate</b>	The <b>Activate</b> link brings you accessing into <a href="http://www.vigorpro.com">www.vigorpro.com</a> to finish the activation of the account and the router.
<b>Authentication Message</b>	As for authentication information of <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.



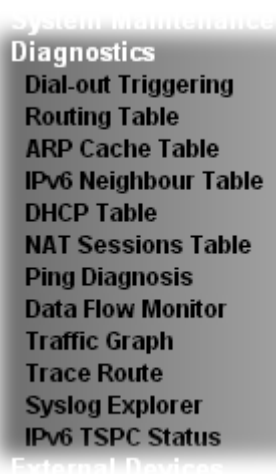
Below shows the successful activation of Web Content Filter:



## 4.18 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



## 4.18.1 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](#)

**Dial-out Triggered Packet Header** [Refresh](#)

```

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 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 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

Decoded Format:
19.19.19.19 -> 19.19.19.19
Protocol Length (0)
    
```

Available settings are explained as follows:

Item	Description
<b>Decoded Format</b>	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
<b>Refresh</b>	Click it to reload the page.

## 4.18.2 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
<pre> Legend: C = connected, S = static, R = RIP, A = default, U = unreach C=      192.168.1.0/24 255.255.255.0   directly connected   LAN1           </pre>		

[Diagnostics >> View Routing Table](#)

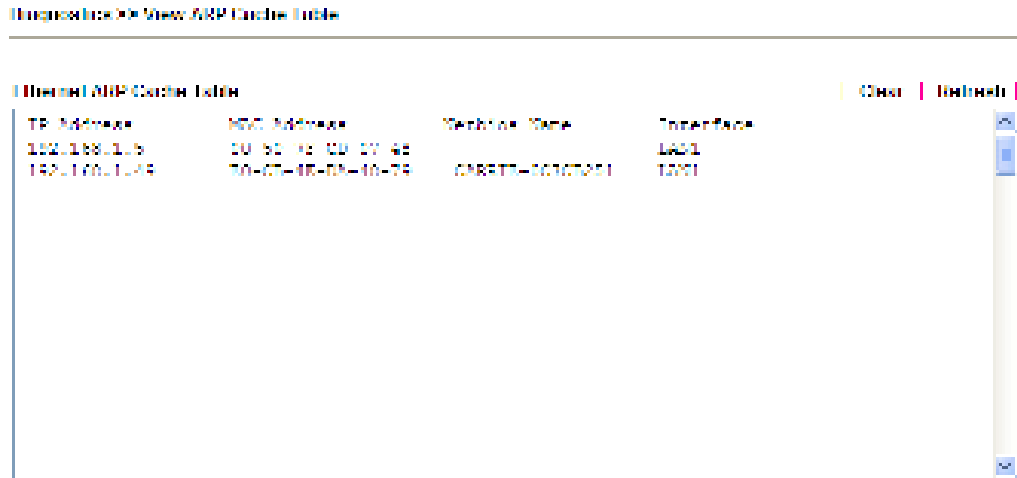
Current Running Routing Table	IPv6 Routing Table	Refresh	
Destination	Interface	Flags	Next Hop
FE70::/64	LAN	D	255
FE00::/48	LAN	U	255

Available settings are explained as follows:

Item	Description
<b>Refresh</b>	Click it to reload the page.

### 4.18.3 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.



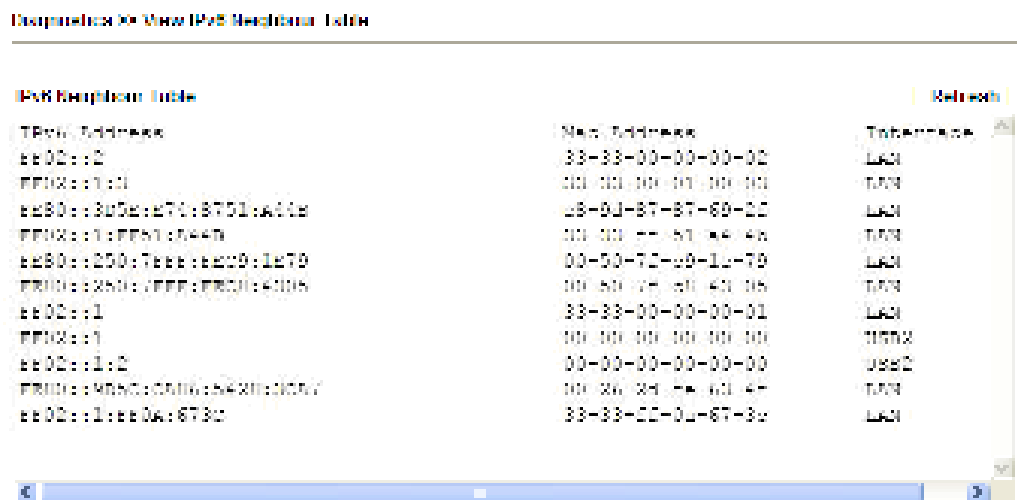
Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

### 4.18.4 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.



Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

### 4.18.5 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](#)

DHCP IP Assignment Table		DHCPv6 IP Assignment Table			Refresh
VLAN : 192.168.1.1/255.255.255.0, DHCP server: On					
Index	IP Address	MAC Address	Leased Time	HOST ID	
1	192.168.1.10	80-C0-4E-00-40-08	10:20:20	carrie-0a70a301	
2	192.168.1.1	00-10-00-00-00-00			

[Diagnostics => View DHCP Assigned IP Addresses](#)

DHCP IP Assignment Table		DHCPv6 IP Assignment Table			Refresh
DHCPv6 server running status:					
Index	IP Address	MAC Address	Leased Time		

Available settings are explained as follows:

Item	Description
<b>Index</b>	It displays the connection item number.
<b>IP Address</b>	It displays the IP address assigned by this router for specified PC.
<b>MAC Address</b>	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
<b>Leased Time</b>	It displays the leased time of the specified PC.
<b>HOST ID</b>	It displays the host ID name of the specified PC.
<b>Refresh</b>	Click it to reload the page.

## 4.18.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

[Diagnostics >> NAT Sessions Table](#)

Private IP:Port	#Pseudo Port	Peer IP:Port	Interface
192.168.1.11:443	51000	142.251.113.44	MS91
192.168.1.11:443	51000	172.16.16.1:70	MS91
192.168.1.11:443	51000	172.16.16.1:70	MS91

Available settings are explained as follows:

Item	Description
<b>Private IP:Port</b>	It indicates the source IP address and port of local PC.
<b>#Pseudo Port</b>	It indicates the temporary port of the router used for NAT.
<b>Peer IP:Port</b>	It indicates the destination IP address and port of remote host.
<b>Interface</b>	It displays the representing number for different interface.
<b>Refresh</b>	Click it to reload the page.

## 4.18.7 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

**Diagnostics** => **Ping Diagnosis**

**Ping Diagnosis**

**Diagnostics** => **Ping Diagnosis**

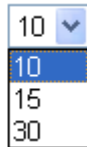
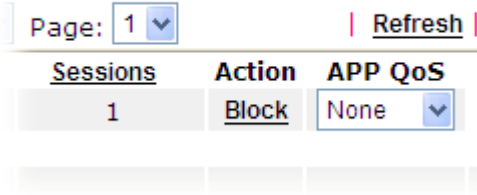
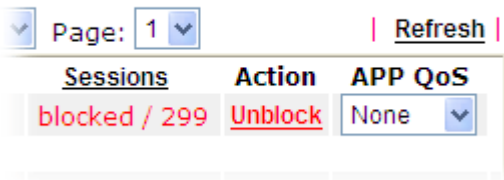
**Ping Diagnosis**

Available settings are explained as follows:

Item	Description
<b>IPV4 /IPV6</b>	Choose the interface for such function.
<b>Ping through</b>	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.
<b>Ping to</b>	Use the drop down list to choose the destination that you want to ping.
<b>IP Address</b>	Type the IP address of the Host/IP that you want to ping.
<b>Ping IPv6 Address</b>	Type the IPv6 address that you want to ping.

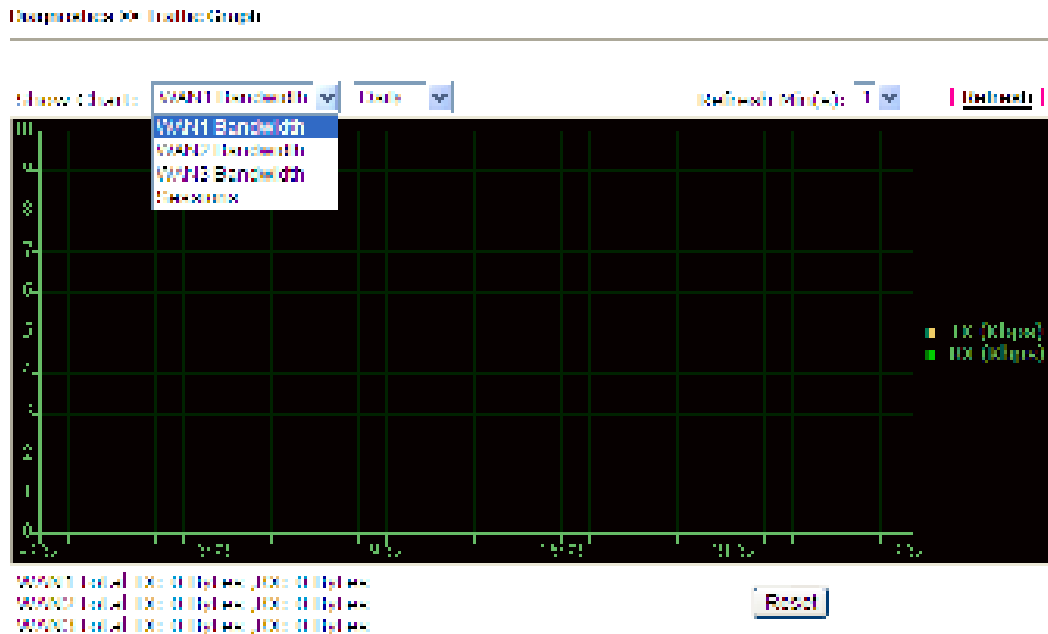




<b>Enable Data Flow Monitor</b>	Check this box to enable this function.
<b>Refresh Seconds</b>	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.  Refresh Seconds: 
<b>Refresh</b>	Click this link to refresh this page manually.
<b>Index</b>	Display the number of the data flow.
<b>IP Address</b>	Display the IP address of the monitored device.
<b>TX rate (kbps)</b>	Display the transmission speed of the monitored device.
<b>RX rate (kbps)</b>	Display the receiving speed of the monitored device.
<b>Sessions</b>	Display the session number that you specified in Limit Session web page.
<b>Action</b>	<p><b>Block</b> - can prevent specified PC accessing into Internet within 5 minutes.</p>  <p><b>Unblock</b> – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.</p> 
<b>Current /Peak/Speed</b>	<p><b>Current</b> means current transmission rate and receiving rate for WAN interface.</p> <p><b>Peak</b> means the highest peak value detected by the router in data transmission.</p> <p><b>Speed</b> means line speed specified in <b>WAN&gt;&gt;General Setup</b>. If you do not specify any rate at that page, here will display <b>Auto</b> for instead.</p>

## 4.18.9 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/WAN3 Bandwidth 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.

## 4.18.10 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    IPv6  
 Trace Through:   
 Protocol:   
 Host / IP Address:

Result

or

[Diagnostics >> Trace Route](#)

Trace Route

IPv4    IPv6  
 Trace Host / IP Address:

Result

Available settings are explained as follows:

Item	Description
<b>IPv4 / IPv6</b>	Click one of them to display corresponding information for it.
<b>Trace through</b>	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 that you want to ping through.
<b>Host/IP Address</b>	It indicates the IP address of the host.
<b>Trace Host/IP Address</b>	It indicates the IPv6 address of the host.
<b>Run</b>	Click this button to start route tracing work.
<b>Clear</b>	Click this link to remove the result on the window.

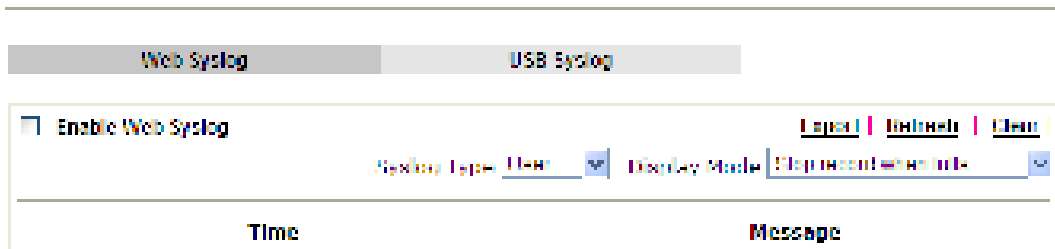
### 4.18.11 Syslog Explorer

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.

URL Application >> Syslog Explorer



Available settings are explained as follows:

Item	Description
<b>Enable Web Syslog</b>	Check this box to enable the function of Web Syslog.
<b>Syslog Type</b>	Use the drop down list to specify a type of Syslog to be displayed. 
<b>Export</b>	Click this link to save the data as a file.
<b>Refresh</b>	Click this link to refresh this page manually.
<b>Clear</b>	Click this link to clear information on this page.
<b>Display Mode</b>	There are two modes for you to choose.

	<div style="border: 1px solid black; padding: 2px;">         Stop record when fulls <span style="float: right;">▼</span>          Stop record when fulls          Always record the new event       </div> <p><b>Stop record when fulls</b> – when the capacity of syslog is full, the system will stop recording.</p> <p><b>Always record the new event</b> – only the newest events will be recorded by the system.</p>
<b>Time</b>	Display the time of the event occurred.
<b>Message</b>	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 while the saved syslog file size is over 1MB.

Time	Log Type	Message
------	----------	---------

Available settings are explained as follows:

Item	Description
<b>Time</b>	Display the time of the event occurred.
<b>Log Type</b>	Display the type of the record.
<b>Message</b>	Display the information for each event.

### 4.18.12 IPv6 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.

[Diagnoses >> IPv6 TSPC Status](#)

WAN1	WAN2	WAN3	<a href="#">Refresh</a>
<b>TSPC Enabled</b> <b>TSPC Connection Status</b> Local Endpoint v4 Address: 114.44.4.221 Local Endpoint v6 Address: 2001:0:0:1401::100:100:100:100 Remote DNS name: 100.100.100.100:53 Remote Endpoint v4 Address: 11.11.11.11 Remote Endpoint v6 Address: 2001:0:0:1401::100:100:100:100 Type Prefix: 2001:0:0:1401::100:100:100:100 Type Prefixlen: 64 Tunnel Broker: 100.100.100.100:53 Tunnel Status: <span style="color: green;">connected</span>			

Available settings are explained as follows:

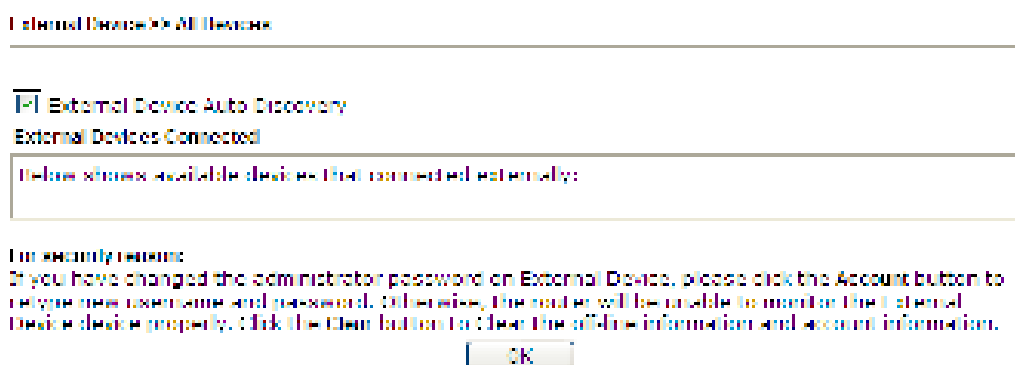
Item	Description
Refresh	Click this link to refresh this page manually.

## 4.19 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.



### 4.19.1 All Devices



Available settings are explained as follows:

Item	Description
<b>External Device Auto Discovery</b>	Check this box to detect the external device automatically 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.

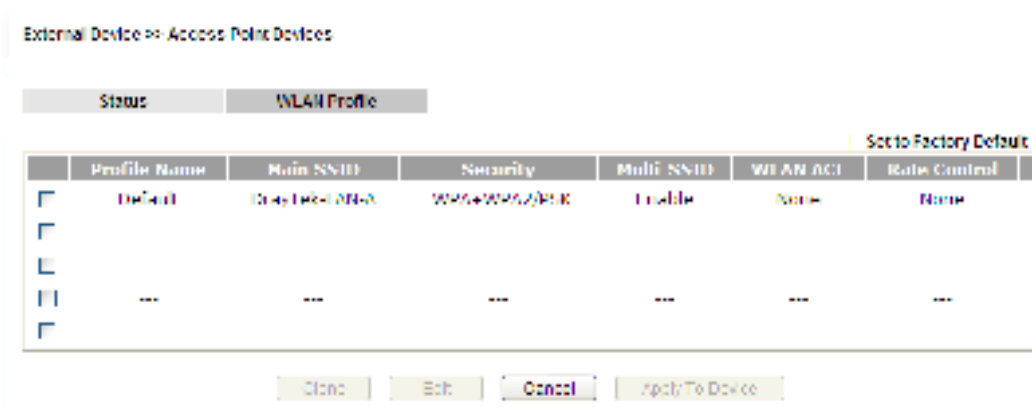


<b>Clear</b>	Click it to remove all the settings modified in this page.
<b>Refresh</b>	Click it to refresh current page.
<b>Index</b>	Click the number index to open the settings page of the device.
<b>Device Name</b>	Display the name of the device.
<b>IP Address</b>	Display the IP address of the device.
<b>SSID</b>	Display the SSID configure by the device.
<b>Encryption</b>	Display the encryption method used by the device.
<b>Ch. (Channel)</b>	Display the channel used by the device.
<b>WL Client</b>	Display the number of the host (wireless client) connecting to such AP device.
<b>Version</b>	Display firmware version used by the device.
<b>Password</b>	Click the button to review /edit the username and password of the device.



## WLAN Profile

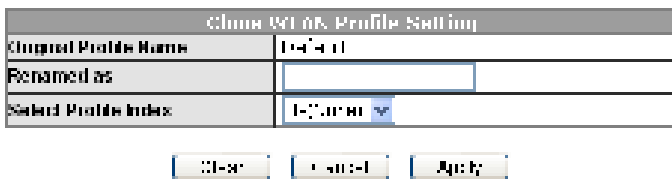
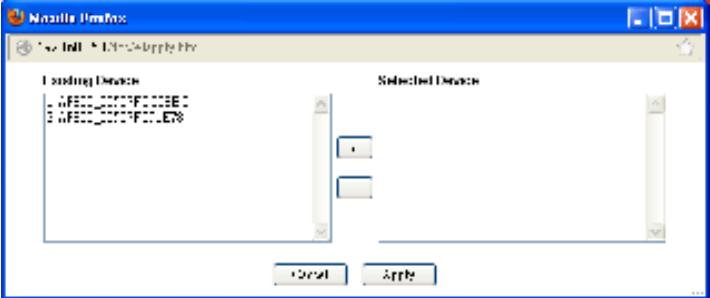
This page can be used to configure **five** different WLAN profiles which can be applied to the connected AP devices. The WLAN profile can be used for connected Vigor Access Point only.




Available settings are explained as follows:

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



<b>Set to Factory Default</b>	Clear all of the settings and return to factory default settings.
<b>Profile Name</b>	Display the name of the profile scanned by Vigor router.
<b>Main SSID</b>	Display the SSID used by the Vigor router.
<b>Security</b>	Display the mode used by the Vigor router.
<b>Multi-SSID</b>	Display if the multi-SSID function is enabled or not.
<b>WLAN ACL</b>	Display the access control (None, White List, or Black List) configured for such profile.
<b>Rate Control</b>	Display if the function of rate control is enabled or not.
<b>Clone</b>	<p>It will pop up a window for you to copy the parameter settings from a profile to another profile.</p>  <p><b>Original Profile Name</b> – Display the original profile name of the selected index.</p> <p><b>Select Profile Index</b> – Choose the index number of the profile that you want to clone from.</p> <p><b>Renamed as</b> – 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.</p>
<b>Edit</b>	It allows you to modify the detailed settings for each WLAN profile.
<b>Cancel</b>	It can cancel the settings you just made on this page.
<b>Apply To Device</b>	<p>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.</p>  <p><b>Existing Device</b> – This field will display the access point connected to Vigor2925 and worked well.</p> <p><b>Selected Device</b> – This field will display the access point which will be applied with the WLAN profile.</p> <p>Choose one of the devices from the Existing Device and</p>

click  to move it to the right field of Selected Device. Then click Apply. The selected device now will be applied with the selected WLAN profile.

To edit a WLAN 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
<input type="checkbox"/>	Default	DrayTek-LAN-A	WPA+WPA2/PSK
<input checked="" type="checkbox"/>	---	---	---
<input type="checkbox"/>	---	---	---
<input type="checkbox"/>	---	---	---
<input type="checkbox"/>	---	---	---

2. The following page will appear. All the wireless connection related to Vigor Access Point (e.g., AP800) will be shown as follows.

1 Selected Device of Access Point Devices

#### WLAN Profile Edit

Device Setting	
Profile Name	
Administrator	
Password	
2nd Subnet	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

WLAN General Setting	
Mode	<input type="radio"/> 802.11n <input checked="" type="radio"/> 802.11ac
Channel	36 (2.4GHz) Channel 36
WMM	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Tx Power	100%

Available settings are explained as follows:

Item	Description
<b>Device Setting</b>	<p><b>Profile Name</b> – Type a name for such profile.</p> <p><b>Administrator</b> – Type the username for such profile. It will be used for the clients trying to connect to the access point.</p> <p><b>Password</b> – Type a password for such profile. It will be used for the clients trying to connect to the access point.</p> <p><b>2<sup>nd</sup> Subnet</b> – Click <b>Enable</b> to enable the second subnet.</p>
<b>WLAN General Setting</b>	<p><b>Mode</b> – Specify a connection mode for wireless network.</p> <p><b>Channel</b> – Specify a channel for the wireless connection.</p> <p><b>WMM</b> – To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.</p> <p><b>Tx Power</b> - The default setting is the maximum (100%).</p>

	Lower down the value may degrade range and throughput of wireless.
<b>Cancel</b>	Cancel the setting configured on this page.
<b>Next</b>	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.

External Device >> Access Point Devices

---

SSID1    SSID2    SSID3    SSID4

**SSID**

Address:  Local LAN     Global LAN

SSID:     LAN-A     Hide SSID

VLAN:     (0-4095)

Isolate:  From LAN     From SSID

**Security Setting**

Mode:  Disable     Enable

WPA

WPA Algorithm:  TKIP     AES     WPA2

Pass Phrase:

Key Renewal Interval:     (Default)

TKIP Disable Force:     (Minimize)

WPA Authentication:  Enable     Disable

WEP

WEP Key (WPA 2 is enabled):

WPA2 Key:  Local LAN     Global LAN

**Access Control**

Mode:

User:

Client's MAC Address:    

**Bandwidth Limit**

Status:  Enable     Disable    Auto Adjustment:  Enable     Disable

Upload:     (Kbps)    Download:     (Kbps)

Available settings are explained as follows:

Item	Description
<b>SSID</b>	<p><b>Active</b> – Click <b>Enable</b> to activate such SSID setting.</p> <p><b>SSID</b> – The default name will be displayed. Change the SSID if it is required. Next, choose LAN-A or LAN-B as the subnet. If required, you can check the box of <b>Hide SSID</b>. Then it will not be recognized by wireless station when the user tries to search the Access Point for connection.</p> <p><b>VLAN</b> – Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number.</p> <p><b>Isolate – From LAN</b> - Check this box to make the wireless clients (stations) with the same SSID not accessing for</p>

	<p>wired PC in LAN.</p> <p><b>Isolate – From Member</b> - Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
<p><b>Security Setting</b></p>	<p><b>Disable</b> – There are several modes provided for you to choose.</p> <p><b>WPA Algorithm</b> –Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for <b>WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.</b></p> <p><b>Pass Phrase</b> –Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.</b></p> <p><b>Key Renewal Interval</b> – Either <b>8~63</b> ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for <b>WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK mode.</b></p> <p><b>PMK Cache Period</b> –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 <b>WPA2/802.1 mode.</b></p> <p><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.</p> <p><b>WEP Key</b> – 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 <b>WEP mode.</b></p> <p><b>802.1X WEP - Enable</b> - Enable the WEP Encryption.</p>
<p><b>Access Control</b></p>	<p><b>Mode (Black List/White List)</b> – Select to enable black list or white list filter policy.</p> <p><b>List</b> –Display all MAC addresses that are edited before.</p> <p><b>Client’s MAC Address</b> –Manually enter the MAC address of wireless client.</p> <p><b>Add</b> –Add a new MAC address into the list.</p> <p><b>Delete</b> –Delete the selected MAC address in the list.</p> <p><b>Edit</b> –Edit the selected MAC address in the list.</p> <p><b>Cancel</b> - Give up the access control set up.</p>

<b>Bandwidth Limit</b>	<p><b>Status</b> – Click <b>Enable</b> to enable the function of bandwidth limit.</p> <p><b>Upload</b> – Type the value as the uploading rate of data transmission.</p> <p><b>Auto Adjustment</b> – Click <b>Enable</b> to make the router manage the bandwidth limit automatically.</p> <p><b>Download</b> - Type the value as the downloading rate of data transmission.</p>
<b>Back</b>	Return to the previous setting page.
<b>Cancel</b>	Cancel the setting configured on this page.
<b>Finish</b>	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.

External Device >> Access Point Devices

Status		WLAN Profile					Set to Factory Default
		Profile Name	Main SSID	Security	Multi-SSID	WLAN ACL	Rate Control
<input type="checkbox"/>		Default	Default-SSID	WPA+WPA2+WPA3	Enable	None	None
<input type="checkbox"/>		WLAN_5 Floor	DrayTek	Disable	Disable	None	None
<input type="checkbox"/>		--	--	--	--	--	--
<input type="checkbox"/>		--	--	--	--	--	--

# 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 still 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](http://www.DrayTek.com).

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



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



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

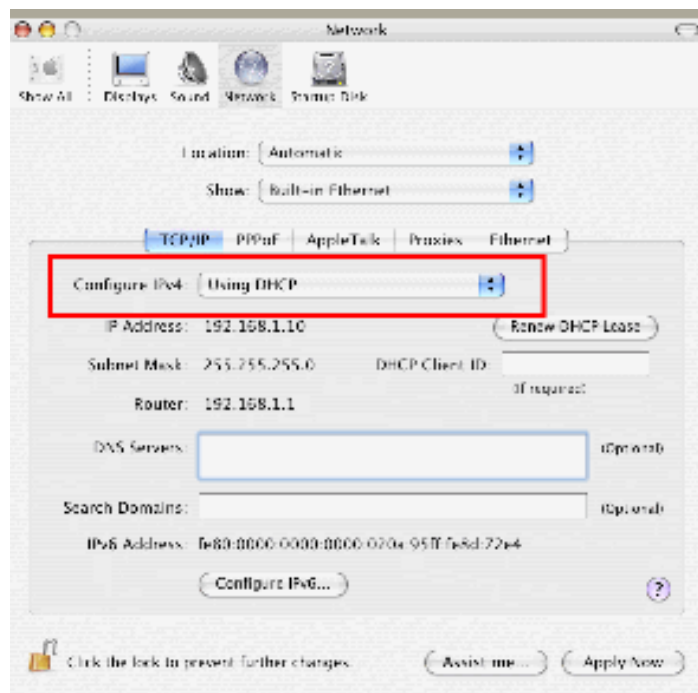


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



### For Mac OS

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





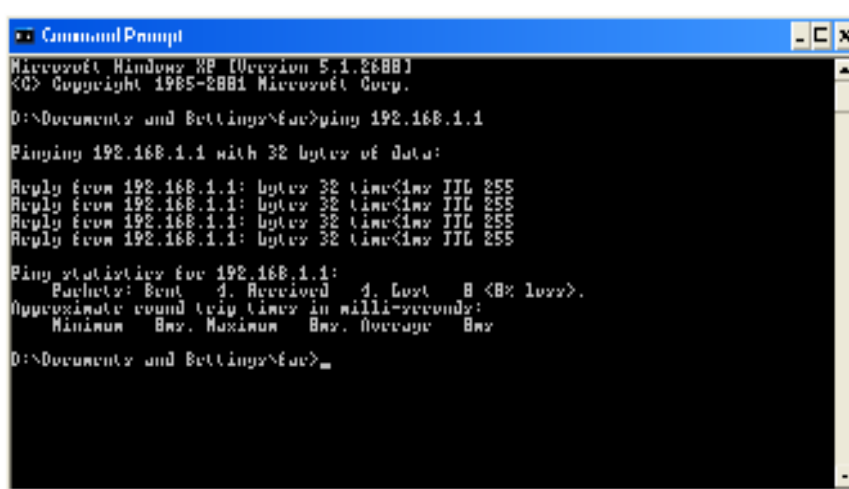
## 5.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

### For Windows

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



```
Microsoft Windows [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fac>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fac>
```

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

### For Mac OS (Terminal)

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

```

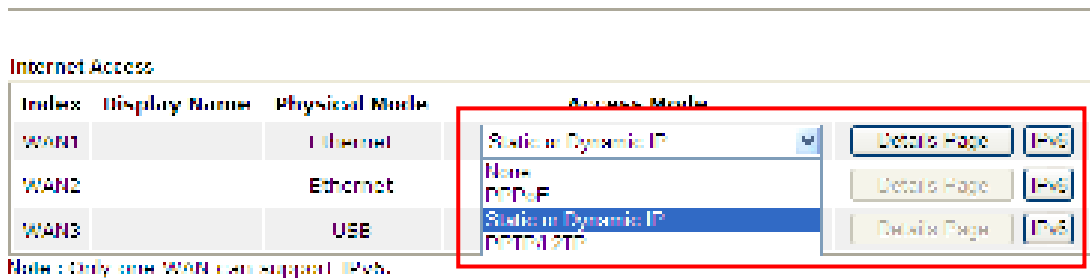
Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

```

## 5.4 Checking If the ISP Settings are OK or Not

Open 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



## 5.5 Problems for 3G Network Connection

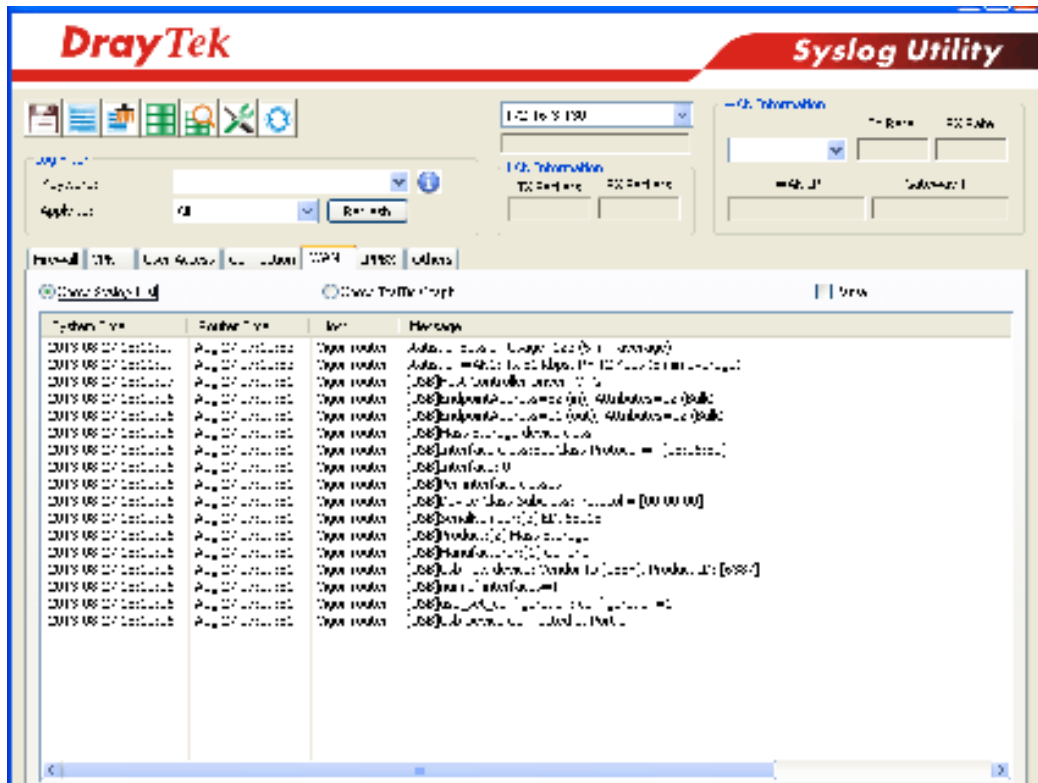
When you have trouble in using 3G network transmission, please check the following:

### Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2925. 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 Vigor2925.

### 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.



### 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 Vigor2925. 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 lose all settings you did before. Make sure you have recorded all useful settings before you pressing.

### 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.

### Reboot System

Do you want to reboot your router ?

Using current configuration

Using factory default configuration

Reboot Now

### Auto Reboot Time Schedule

Index(1-10) in Schedule Setup: \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_

Note: Action 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](mailto:support@DrayTek.com).