

DrayTek

Vigor2120 Series

Broadband Firewall Router



Your reliable networking solutions partner

User's Guide

V1.01

Vigor2120 Series Broadband Firewall Router User's Guide

Version: 1.0

Firmware Version: V3.7.5.1

(For future update, please visit DrayTek web site)

Date: September 10, 2014

Copyright Information

Copyright Declarations

© 2014 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.DrayTek.com>.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

<http://www.DrayTek.com>

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303
Product: Vigor2120 Series Router

DrayTek Corp. declares that Vigor2120 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.

This product is designed for 2.4GHz/5GHz WLAN network throughout the EC region.

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.

The antenna/transmitter should be kept at least 20 cm away from human body.



More update, please visit www.draytek.com.

Table of Contents

1

Introduction.....	1
1.1 Web Configuration Buttons Explanation	2
1.2 LED Indicators and Connectors	3
1.2.1 For Vigor2120	3
1.2.2 For Vigor2120n-plus	5
1.3 Hardware Installation	7
1.4 Printer Installation	8
1.5 Accessing Web Page	16
1.6 Changing Password	17
1.7 Introducing Dashboard.....	18
1.7.1 Virtual Panel	19
1.7.2 Name with a Link	19
1.7.3 Quick Access for Common Used Menu.....	19
1.7.4 GUI Map	21
1.7.5 Web Console	21
1.7.6 Config Backup	22
1.7.7 Logout.....	22
1.8 Online Status.....	23
1.9 Saving Configuration.....	25

2

Quick Setup.....	27
2.1 Quick Start Wizard	27
2.1.1 For WAN1 (Ethernet)	29
2.1.2 For WAN2 (USB)	38
2.2 Service Activation Wizard.....	40
2.3 VPN Client Wizard	44
2.4 VPN Server Wizard.....	50
2.5 Registering Vigor Router.....	55

3

Tutorials and Applications.....	59
3.1 How to configure settings for IPv6 Service in Vigor2120.....	59
3.2 How can I get the files from USB storage device connecting to Vigor router?	69
3.3 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tunnel (Main Mode)	71
3.4 How to Optimize the Bandwidth through QoS Technology	76

3.5 How to Create an Account for MyVigor.....	81
3.5.1 Create an Account via Vigor Router.....	81
3.5.2 Create an Account via MyVigor Web Site.....	85
3.6 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection.....	88
3.7 How to Configure Certain Computers Accessing to Internet.....	92
3.8 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter.....	96

4

Advanced Configuration.....103

4.1 WAN.....	103
4.1.1 Basics of Internet Protocol (IP) Network.....	103
4.1.2 General Setup.....	105
4.1.3 Internet Access.....	107
4.1.4 Multi-VLAN.....	128
4.2 LAN.....	132
4.2.1 Basics of LAN.....	132
4.2.2 General Setup.....	134
4.2.3 Static Route.....	140
4.2.4 VLAN.....	145
4.2.5 Bind IP to MAC.....	148
4.2.6 LAN Port Mirror.....	150
4.2.7 Web Portal Setup.....	151
4.3 NAT.....	152
4.3.1 Port Redirection.....	153
4.3.2 DMZ Host.....	157
4.3.3 Open Ports.....	160
4.3.4 Address Mapping.....	162
4.3.5 Port Triggering.....	164
4.4 Firewall.....	167
4.4.1 Basics for Firewall.....	167
4.4.2 General Setup.....	169
4.4.3 Filter Setup.....	173
4.4.4 DoS Defense.....	181
4.5 Objects Settings.....	185
4.5.1 IP Object.....	185
4.5.2 IP Group.....	188
4.5.3 IPv6 Object.....	189
4.5.4 IPv6 Group.....	191
4.5.5 Service Type Object.....	192
4.5.6 Service Type Group.....	194
4.5.7 Keyword Object.....	195
4.5.8 Keyword Group.....	197
4.5.9 File Extension Object.....	198
4.5.10 SMS/Mail Service Object.....	200
4.5.11 Notification Object.....	205
4.6 CSM Profile.....	207
4.6.1 APP Enforcement Profile.....	208

4.6.2 URL Content Filter Profile.....	210
4.6.3 Web Content Filter Profile.....	214
4.6.4 DNS Filter	218
4.6.5 APPE Support List.....	219
4.7 Bandwidth Management	220
4.7.1 Sessions Limit.....	220
4.7.2 Bandwidth Limit	222
4.7.3 Quality of Service.....	224
4.7.4 APP QoS	232
4.8 Applications	234
4.8.1 Dynamic DNS	234
4.8.2 LAN DNS	237
4.8.3 Schedule.....	239
4.8.4 RADIUS	241
4.8.5 UPnP.....	242
4.8.6 IGMP	244
4.8.7 Wake on LAN.....	245
4.8.8 SMS / Mail Alert Service.....	246
4.8.9 Bonjour.....	248
4.9 VPN and Remote Access.....	251
4.9.1 Remote Access Control.....	251
4.9.2 PPP General Setup	252
4.9.3 IPsec General Setup.....	254
4.9.4 IPsec Peer Identity.....	256
4.9.5 Remote Dial-in User	258
4.9.6 LAN to LAN.....	261
4.9.7 Connection Management.....	271
4.10 Certificate Management.....	271
4.10.1 Local Certificate	272
4.10.2 Trusted CA Certificate	275
4.10.3 Certificate Backup.....	277
4.11 Wireless LAN(2.4GHz/5GHz).....	278
4.11.1 Basic Concepts.....	278
4.11.2 General Setup.....	280
4.11.3 Security.....	282
4.11.4 Access Control.....	284
4.11.5 WPS.....	285
4.11.6 WDS.....	288
4.11.7 Advanced Setting.....	292
4.11.8 WMM Configuration	294
4.11.9 AP Discovery	296
4.11.10 Station List	297
4.11.11 Station Control.....	298
4.12 SSL VPN	299
4.12.1 General Setup.....	299
4.12.2 SSL Application	300
4.12.3 User Account	302
4.12.4 Online User Status.....	306
4.13 USB Application	307
4.13.1 USB General Settings.....	307
4.13.2 USB User Management.....	308
4.13.3 File Explorer.....	310
4.13.4 USB Device Status	311

4.13.5 Modem Support List.....	312
4.14 System Maintenance.....	313
4.14.1 System Status.....	313
4.14.2 TR-069.....	315
4.14.3 Administrator Password.....	316
4.14.4 User Password.....	317
4.14.5 Login Page Greeting.....	320
4.14.6 Configuration Backup.....	322
4.14.7 Syslog/Mail Alert.....	324
4.14.8 Time and Date.....	327
4.14.9 SNMP.....	328
4.14.10 Management.....	330
4.14.11 Reboot System.....	333
4.14.12 Firmware Upgrade.....	334
4.14.13 Activation.....	335
4.15 Diagnostics.....	337
4.15.1 Dial-out Triggering.....	337
4.15.2 Routing Table.....	338
4.15.3 ARP Cache Table.....	339
4.15.4 IPv6 Neighbour Table.....	339
4.15.5 DHCP Table.....	340
4.15.6 NAT Sessions Table.....	341
4.15.7 Ping Diagnosis.....	342
4.15.8 Data Flow Monitor.....	343
4.15.9 Traffic Graph.....	345
4.15.10 Trace Route.....	346
4.15.11 System Explorer.....	347
4.15.12 IPv6 TSPC Status.....	348

5

Trouble Shooting.....349

5.1 Checking If the Hardware Status Is OK or Not.....	349
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not.....	350
5.3 Pinging the Router from Your Computer.....	352
5.4 Checking If the ISP Settings are OK or Not.....	353
5.5 Problems for 3G Network Connection.....	353
5.6 Backing to Factory Default Setting If Necessary.....	354
5.7 Contacting Your Dealer.....	355

1

Introduction

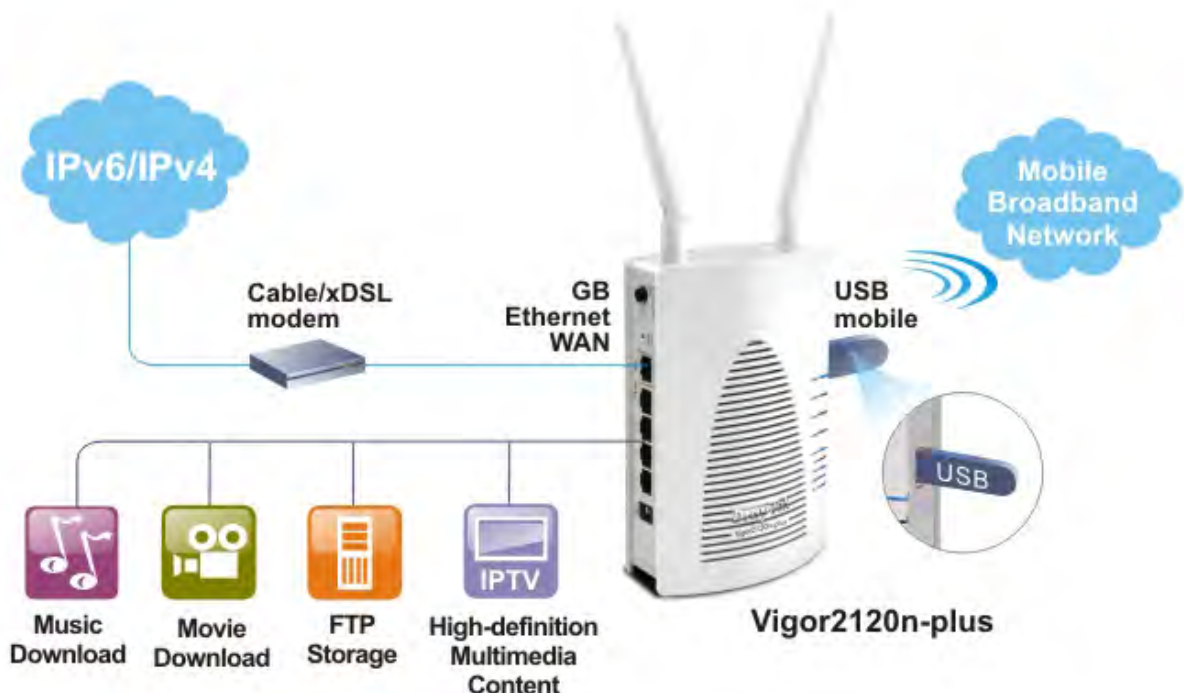
Vigor2120 Series is a broadband router which integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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 2 VPN tunnels.

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


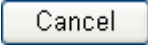
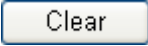


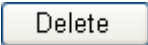
In addition, Vigor2120 Series supports USB interface for connecting USB printer to share printing function or 3G/4G USB modem for network connection.

Vigor2120 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:

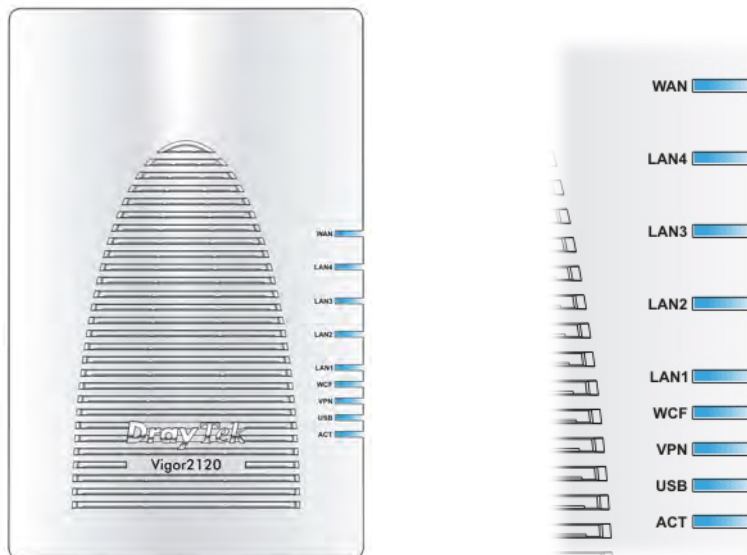
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the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

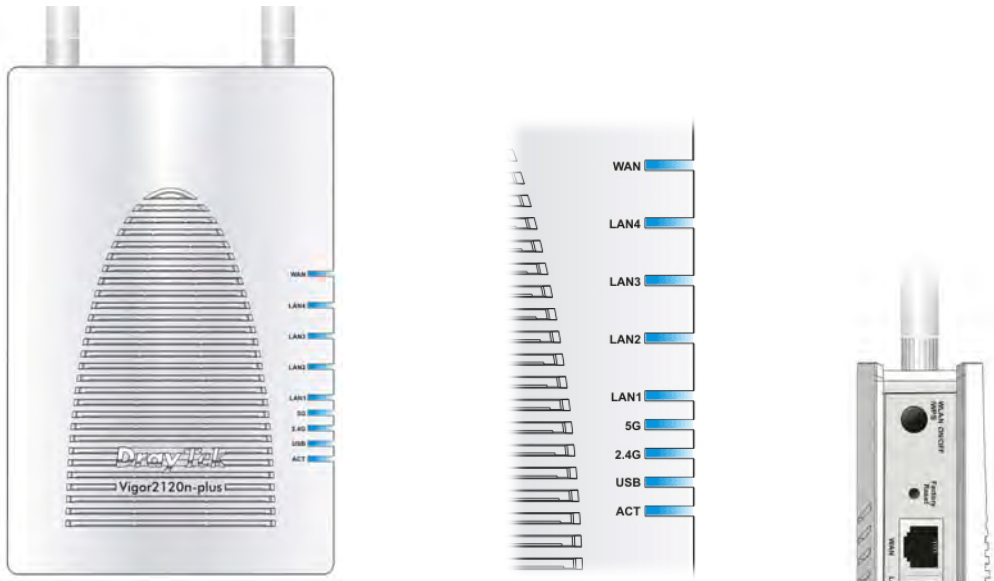
1.2.1 For Vigor2120








LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
WCF	On	The profile(s) of CSM (Content Security Management) for Web Content Filter application can be enabled from Firewall >>General Setup . (Such profile must be established under CSM menu)
LAN 1 - 4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.

	Interface	Description
		Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.
	WAN	Connector for accessing the Internet.
	LAN 1- 4	Connecters for local network devices (LAN).
		PWR: Connector for a power adapter.
		Connector for a USB device (for 3G USB Modem or printer or storage disk).
		ON/OFF: Power switch.

1.2.2 For Vigor2120n-plus



LED	Status	Explanation
ACT	Off	The system is not ready or is failed.
	Blinking	The system is ready and can work normally.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
2.4G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
5G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is transmitting (sending/receiving).
LAN 1 - 4	On	A normal connection is through its corresponding port.
	Off	LAN is disconnected.
WAN	On	The WAN port is connected.
	Blinking	It will blink while transmitting data.

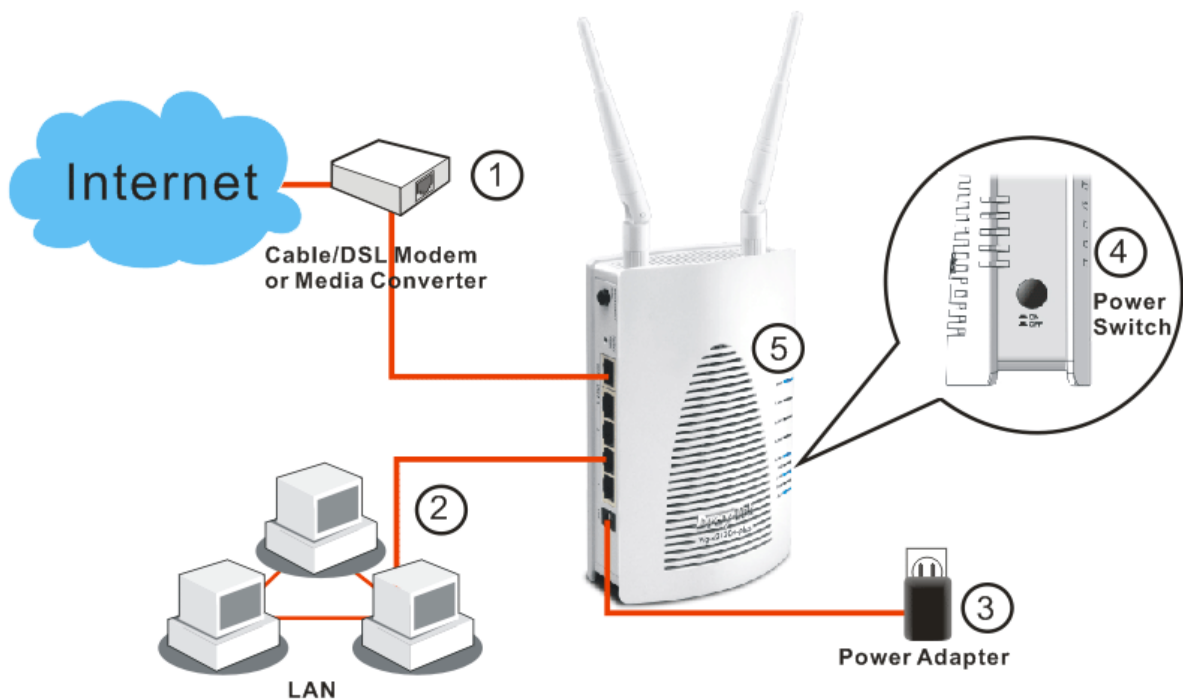
Interface	Description
 <p>WLAN ON/OFF WPS</p>	<p>WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the 2.4G/5G blue LED on front panel will be on.</p> <p>WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, 2.4G/5G blue LED on front panel will be off.</p> <p>WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds. The router will wait for any wireless client connecting to it through WPS.</p>
	<p>Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 6 seconds. Then the router will restart with the factory default configuration.</p>
<p>WAN</p>	<p>Connector for accessing the Internet.</p>
<p>LAN 1- 4</p>	<p>Connectors for local network devices (LAN).</p>
	<p>PWR: Connector for a power adapter.</p>
	<p>Connector for a USB device (for 3G USB Modem or printer or storage disk).</p>
	<p>ON/OFF: Power switch.</p>

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.)

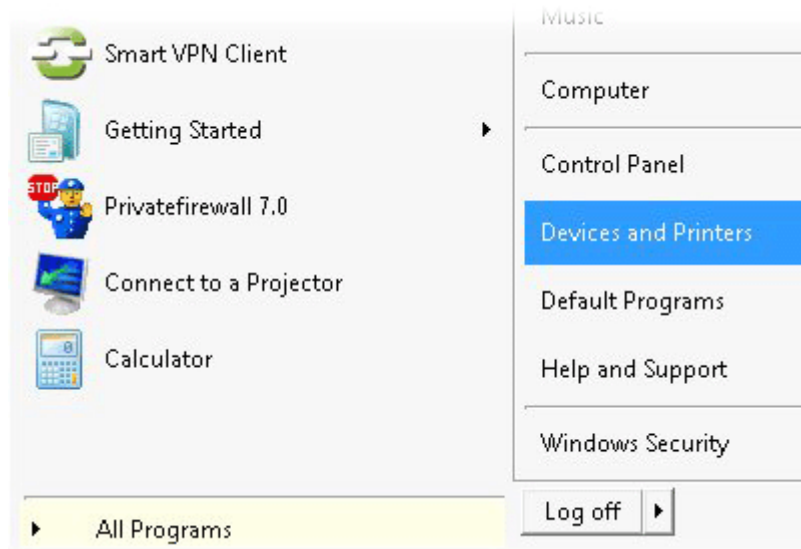


1.4 Printer Installation

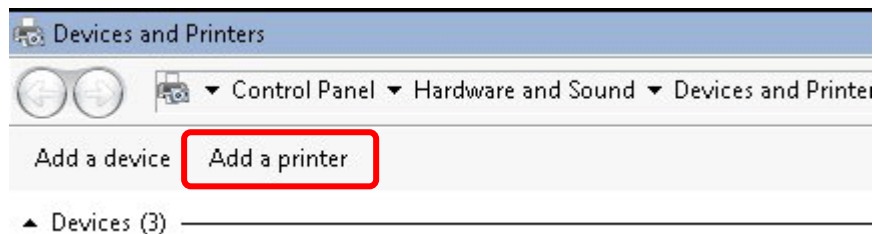
You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE/Vista, please visit www.DrayTek.com.

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

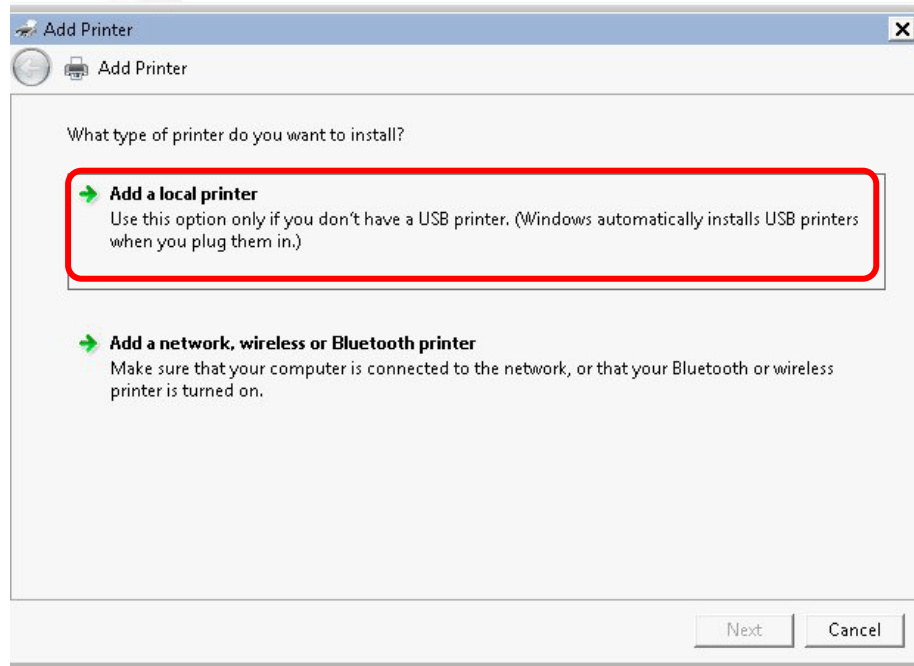
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



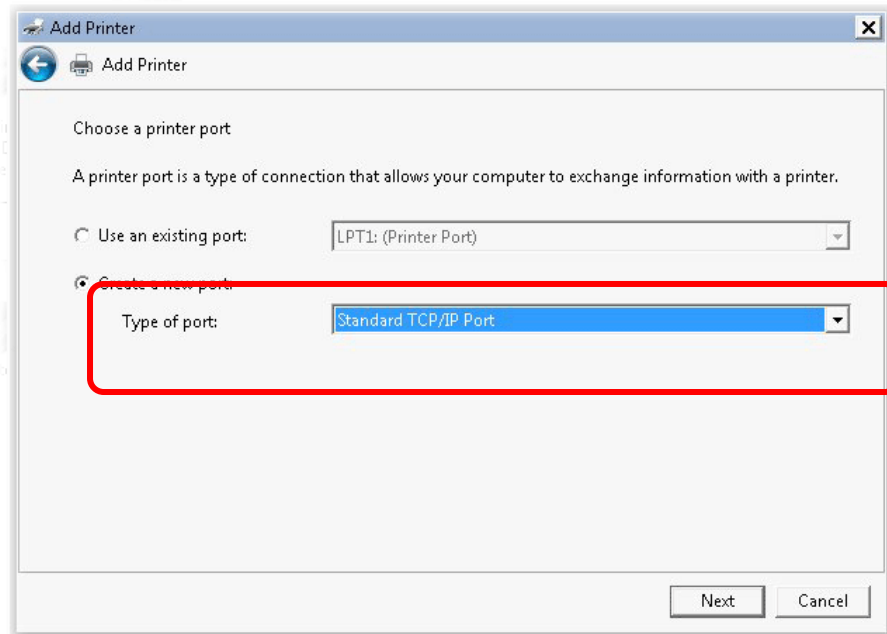
3. Click **Add a printer**.



4. A dialog will appear. Click **Add a local printer** and click **Next**.



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



6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.

The screenshot shows the 'Add Printer' dialog box with the following details:

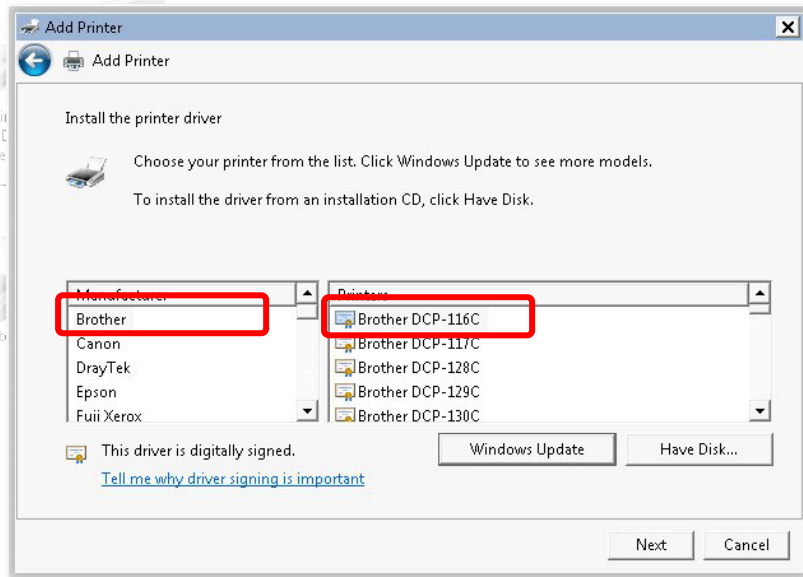
- Device type: TCP/IP Device
- Hostname or IP address: 192.168.1.1
- Port name: 192.168.1.1
- Query the printer and automatically select the driver to use

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

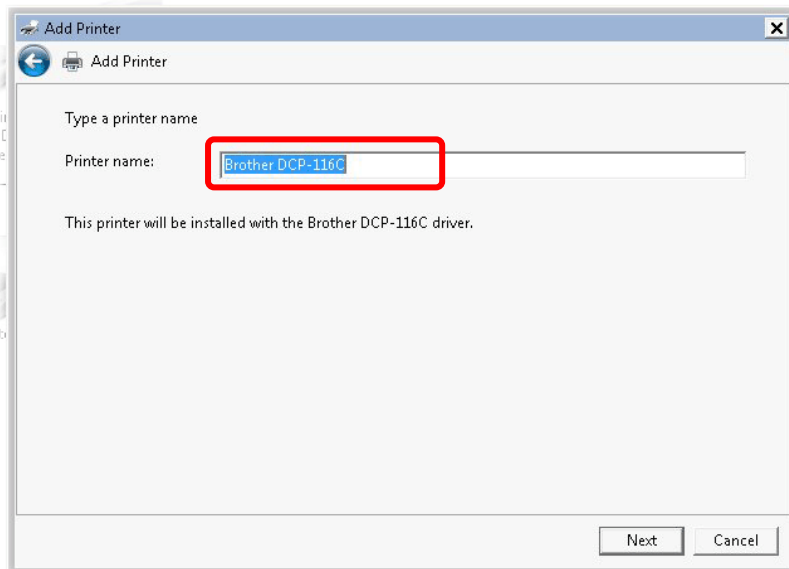
The screenshot shows the 'Add Printer' dialog box with the following details:

- Additional port information required
- The device is not found on the network. Be sure that:
 1. The device is turned on.
 2. The network is connected.
 3. The device is properly configured.
 4. The address on the previous page is correct.
- If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
- Device Type:
 - Standard (Generic Network Card)
 - Custom (Settings...)

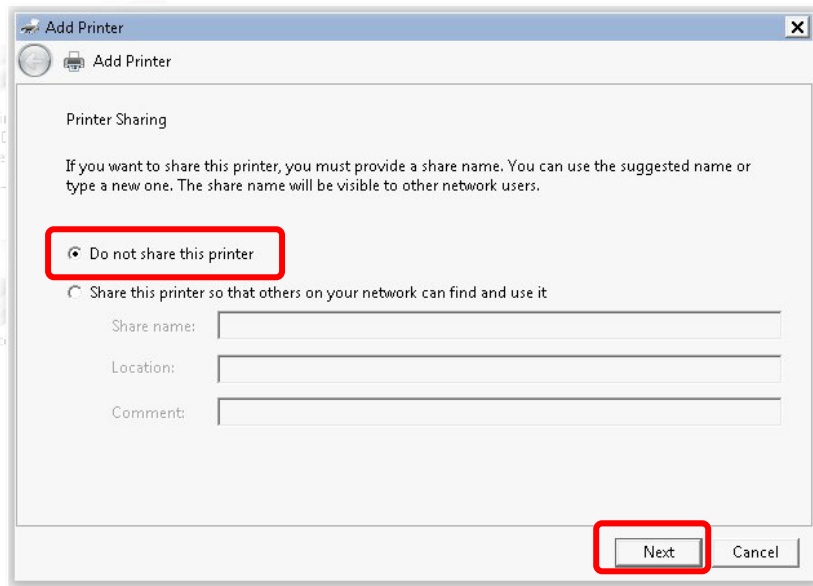
- Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



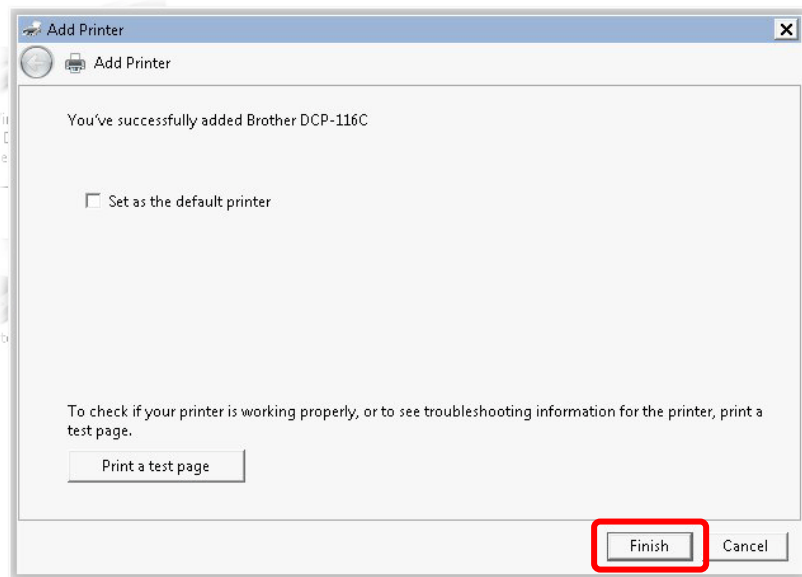
- Type a name for the chosen printer. Click **Next**.



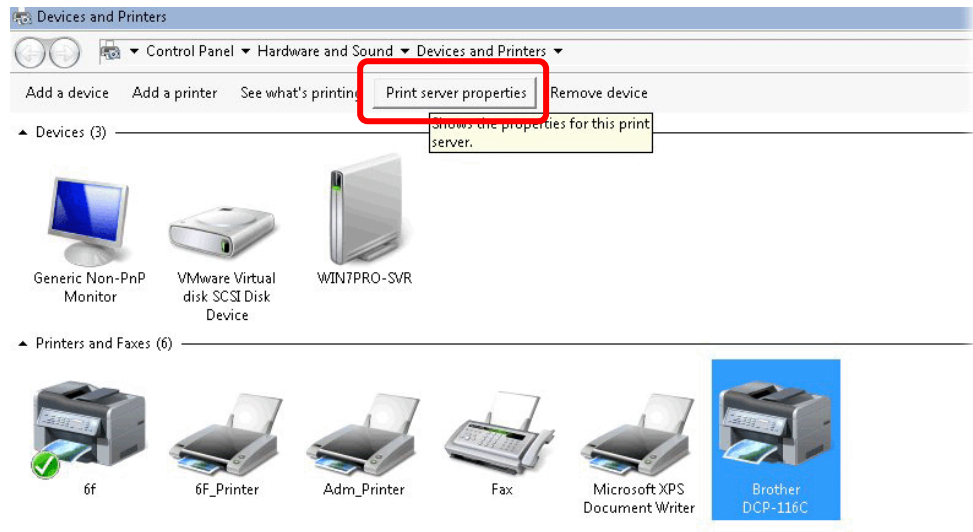
10. Choose **Do not share this printer** and click **Next**.



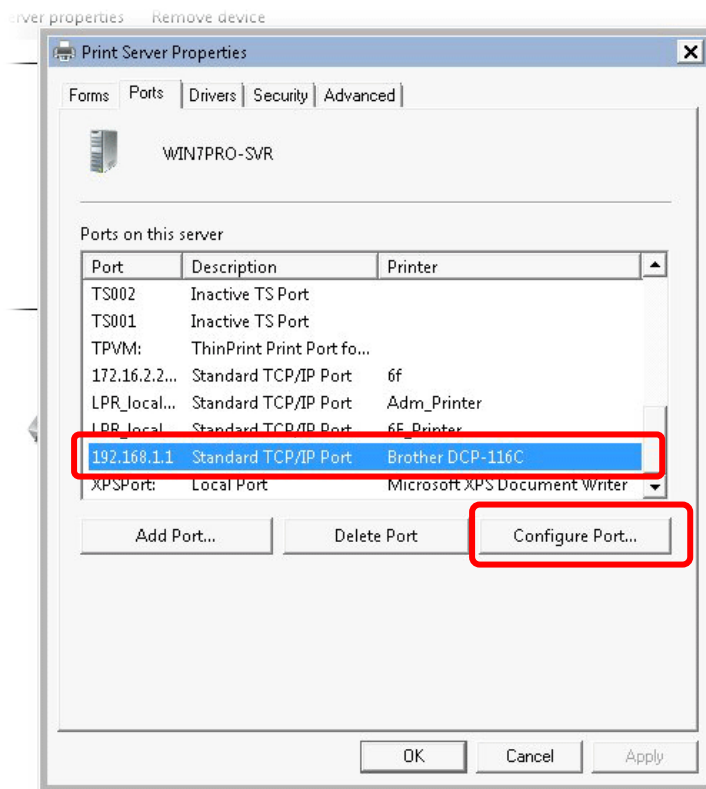
11. Then, in the following dialog, click **Finish**.



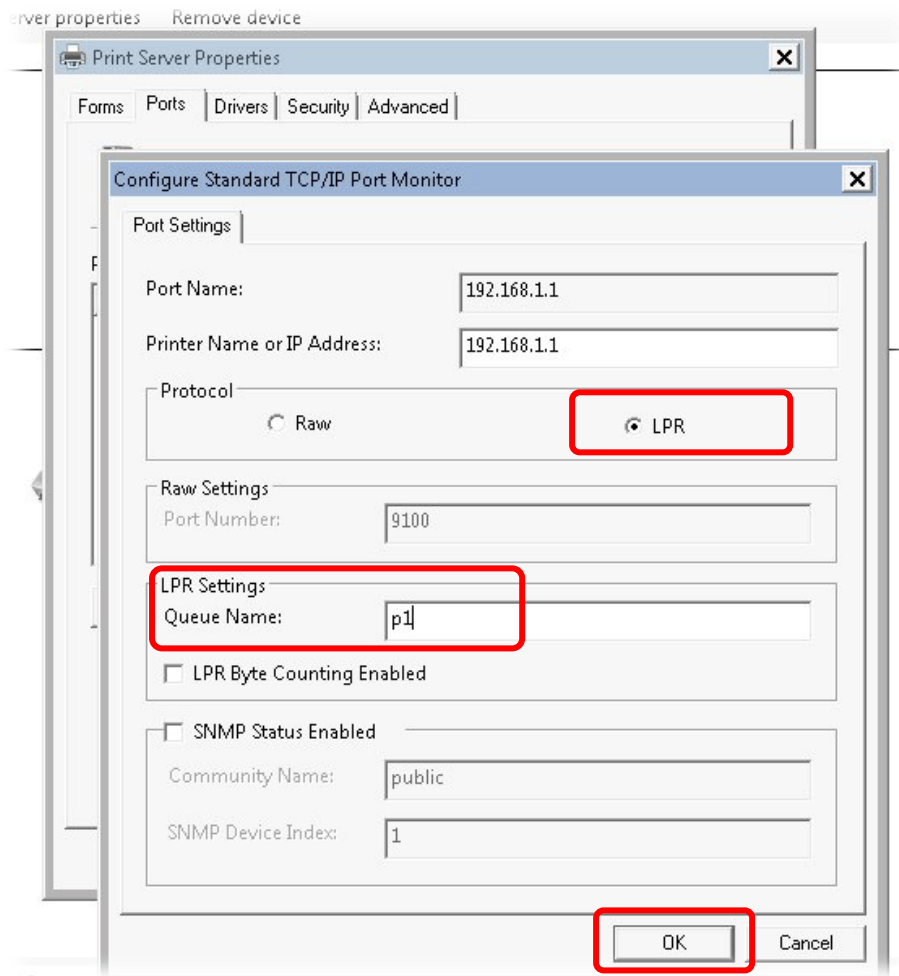
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



13. Edit the property of the new printer you have added by clicking **Configure Port**.

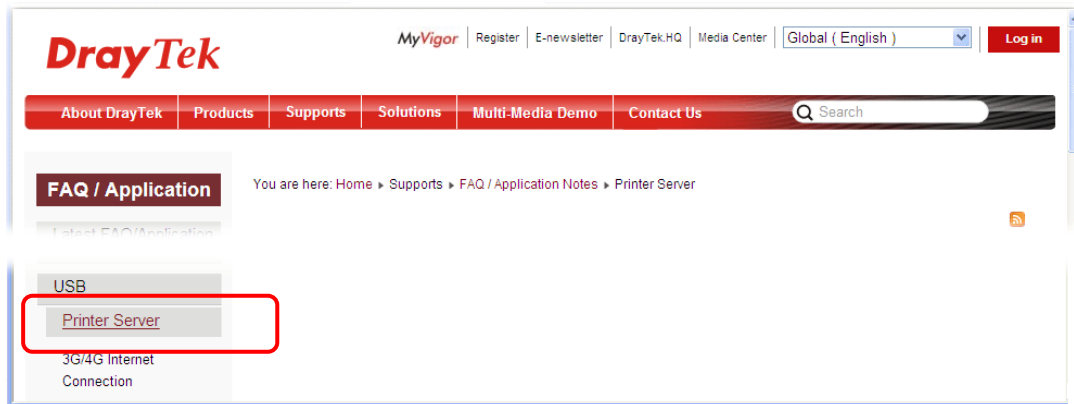


14. Select "**LPR**" on Protocol, type **p1** (number 1) as **Queue Name**. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.

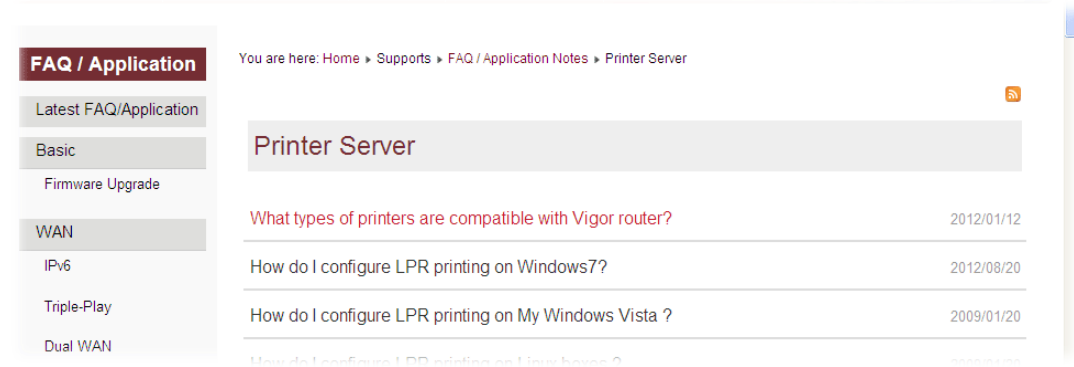


The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

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 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.

1.5 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.

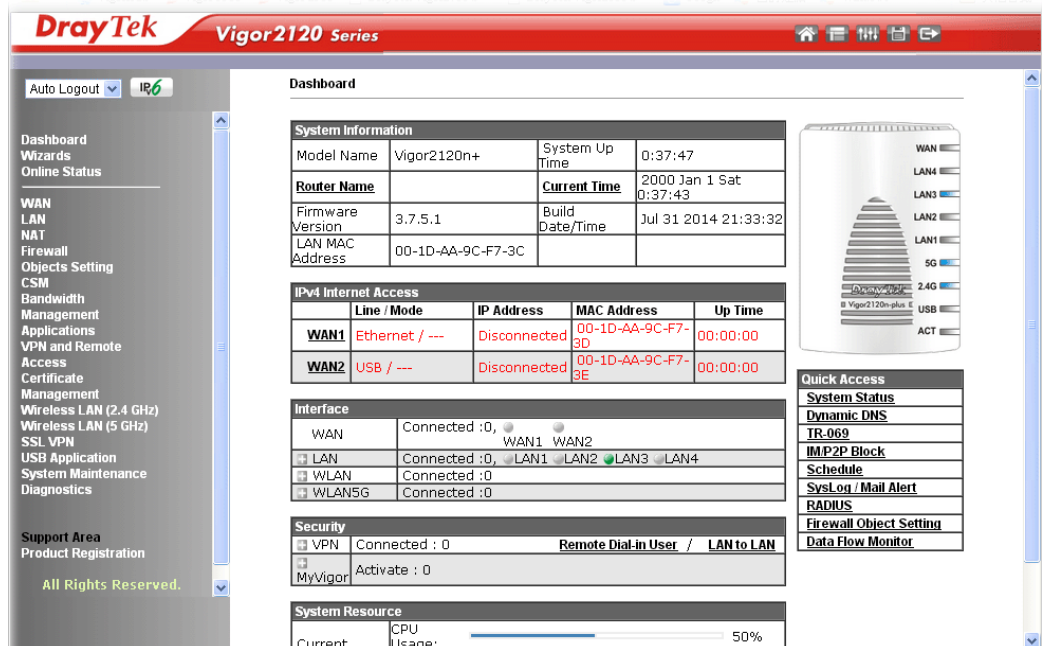


The image shows the login page for the DrayTek Vigor2120 Series router. The page has a red header with the DrayTek logo and "Vigor2120 Series". Below the header is a "Login" section with two input fields: "Username" containing "admin" and "Password" containing "*****". A "Login" button is positioned below the password field. At the bottom of the page, there is a copyright notice: "Copyright © 2013 DrayTek Corp. All Rights Reserved."

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

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

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



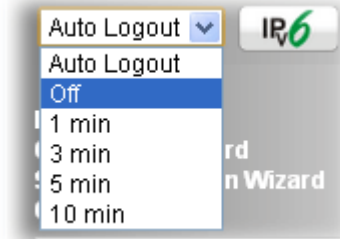
The image shows the main screen of the DrayTek Vigor2120 Series router's web configuration interface. The page has a red header with the DrayTek logo and "Vigor2120 Series". The main content area is divided into several sections:

- System Information:** A table showing Model Name (Vigor2120n+), System Up Time (0:37:47), Router Name, Current Time (2000 Jan 1 Sat 0:37:43), Firmware Version (3.7.5.1), Build Date/Time (Jul 31 2014 21:33:32), and LAN MAC Address (00-1D-AA-9C-F7-3C).
- IPv4 Internet Access:** A table showing WAN1 (Ethernet / ---, Disconnected, 00-1D-AA-9C-F7-3D, 00:00:00) and WAN2 (USB / ---, Disconnected, 00-1D-AA-9C-F7-3E, 00:00:00).
- Interface:** A table showing WAN (Connected :0), LAN (Connected :0), WLAN (Connected :0), and WLAN5G (Connected :0).
- Security:** A table showing VPN (Connected : 0, Remote Dial-in User / LAN to LAN) and MyVigor (Activate : 0).
- System Resource:** A table showing CPU Usage (50%).
- Quick Access:** A list of links including System Status, Dynamic DNS, TR-069, IM/2P Block, Schedule, SysLog / Mail Alert, RADIUS, Firewall Object Setting, and Data Flow Monitor.

The left sidebar contains a navigation menu with options like Dashboard, Wizards, Online Status, WAN, LAN, NAT, Firewall, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, Wireless LAN (2.4 GHz), Wireless LAN (5 GHz), SSL VPN, USB Application, System Maintenance, Diagnostics, Support Area, and Product Registration. The bottom of the sidebar says "All Rights Reserved."

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.



1.6 Changing Password

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

- Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password.
- Please type “admin/admin” as Username/Password for accessing into the web user interface with admin mode.
- 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

- 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.

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

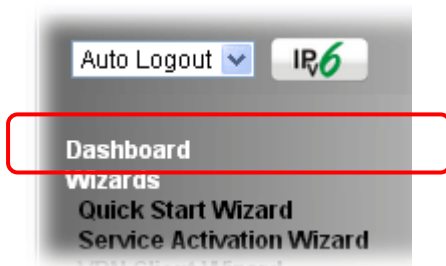


Note: Even the password has been changed, the Username for logging to the web user interface is still “admin”.

1.7 Introducing Dashboard

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

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



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

Dashboard

System Information			
Model Name	Vigor2120n+	System Up Time	0:37:47
Router Name		Current Time	2000 Jan 1 Sat 0:37:43
Firmware Version	3.7.5.1	Build Date/Time	Jul 31 2014 21:33:32
LAN MAC Address	00-1D-AA-9C-F7-3C		

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / ---	Disconnected	00-1D-AA-9C-F7-3D	00:00:00
WAN2	USB / ---	Disconnected	00-1D-AA-9C-F7-3E	00:00:00

Interface	
WAN	Connected :0, WAN1 WAN2
LAN	Connected :0, LAN1 LAN2 LAN3 LAN4
WLAN	Connected :0
WLAN5G	Connected :0

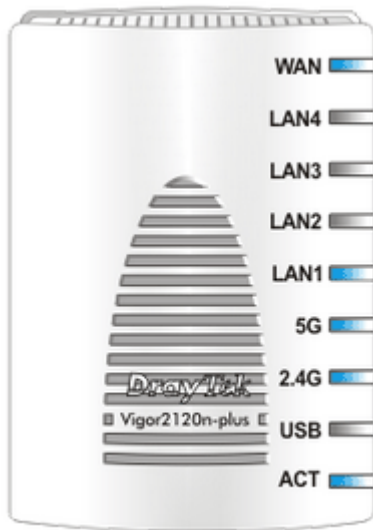
Security	
VPN	Connected : 0 Remote Dial-in User / LAN to LAN
MyVigor	Activate : 0

System Resource	
CPU	50%

Quick Access	
<u>System Status</u>	
<u>Dynamic DNS</u>	
<u>TR-069</u>	
<u>IMP2P Block</u>	
<u>Schedule</u>	
<u>SysLog / Mail Alert</u>	
<u>RADIUS</u>	
<u>Firewall Object Setting</u>	
<u>Data Flow Monitor</u>	

1.7.1 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.



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

1.7.2 Name with a Link

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

Dashboard

System Information			
Model Name	Vigor2120n+	System Up Time	0:3:31
Router Name		Current Time	2000 Jan 1 Sat 0:3:26
Firmware Version	3.7.5.1	Build Date/Time	Feb 27 2014 11:42:56
LAN MAC Address	00-1D-AA-9C-F7-34		

IPv4 Internet Access				
	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / ---	Disconnected	00-1D-AA-9C-F7-35	00:00:00
WAN2	USB / ---	Disconnected	00-1D-AA-9C-F7-36	00:00:00

1.7.3 Quick Access for Common Used Menu

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

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

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

The function links of System Status, Dynamic DDNS, TR-069, IM/P2P Block, Schedule, Syslog/Mail Alert, 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	Connected :0, <input type="radio"/> WAN1 <input type="radio"/> WAN2
LAN	Connected :1, <input checked="" type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4
WLAN	Connected :0
WLAN5G	Connected :0

Security	
VPN	Connected : 0 Remote Dial-in User / LAN to LAN
MyVigor	Activate : 0

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. <input type="text" value="1"/> <input type="button" value="Go To"/>			
Name / User	Type / Security	Host IP	Up Time
V2920	IPsec/3DES	172.16.2.145	0:0:20

User Mode is OFF now.

WAN	Connected : 2, <input checked="" type="radio"/> WAN1 <input checked="" type="radio"/> WAN2 <input type="radio"/> WAN3	
LAN	Connected : 3, <input checked="" type="radio"/> LAN1 <input checked="" type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4	
Host ID	IP Address	MAC
ALPHA-NB	10.28.60.13	1C-4B-D6-D2-D
	10.28.60.14	00-15-AF-09-7E
	10.28.60.11	00-50-7F-C9-76

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).

1.7.4 GUI Map



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

GUI Map

Dashboard Wizard	Quick Start Wizard	Certificate Management	Local Certificate
	Service Activation Wizard		Trusted CA Certificate
	VPN Client Wizard	Wireless LAN (2.4 GHz)	Certificate Backup
	VPN Server Wizard		General Setup
Online Status	Physical Connection		Security
	Virtual WAN		Access Control
WAN	General Setup		WPS
	Internet Access		WDS
	Multi-VLAN		Advanced Setting
LAN	General Setup	Wireless LAN (5 GHz)	WMM Configuration
	Static Route		AP Discovery
	VLAN		Station List
	Bind IP to MAC		Station Control
	LAN Port Mirror		General Setup
	Web Portal Setup		Security
NAT	Port Redirection		Access Control
	DMZ Host		WPS
	Open Ports		WDS
	Address Mapping		Advanced Setting
	Port Triggering		WMM Configuration
Firewall	General Setup	SSL VPN	AP Discovery
			Station List
			Station Control
			General Setup

1.7.5 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.

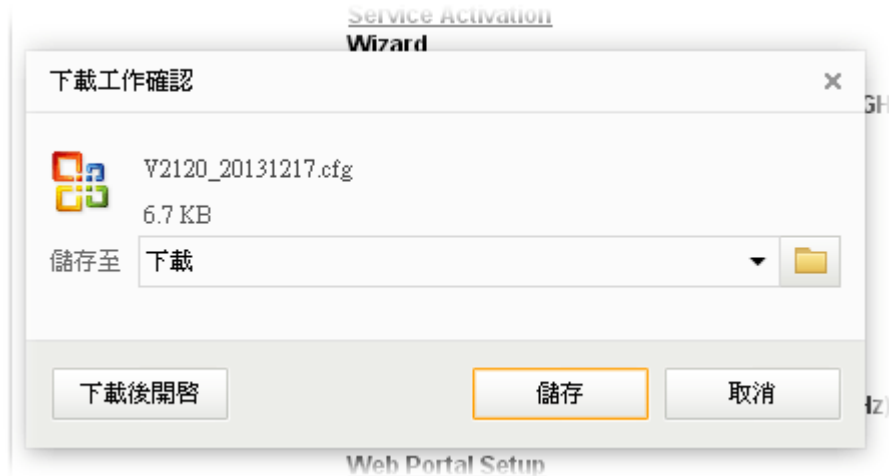


1.7.6 Config Backup



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.

1.7.7 Logout



Click this icon to exit the web user interface.

1.8 Online Status

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 2:32:26
IPv4			IPv6			
LAN Status						
IP Address		Primary DNS: 8.8.8.8		Secondary DNS: 8.8.4.4		
192.168.1.1		TX Packets 3946	RX Packets 74458			
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		Static IP	0:11:25		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
172.16.3.130	172.16.3.1	8	3	2152	274	
WAN 2 Status >> Dial PPP						
Enable	Line	Name	Mode	Up Time	Signal	
No	USB		---	00:00:00	-	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	

Physical Connection for IPv6 Protocol

Online Status

Physical Connection						System Uptime: 0day 2:34:16
IPv4			IPv6			
LAN Status						
IP Address FE80::21D:AFF:FE9C:F734/64 (Link)						
TX Packets	RX Packets	TX Bytes	RX Bytes			
49	0	5268	0			
WAN IPv6 Status						
Enable	Mode	Up Time				
No	Offline	---				
IP	Gateway IP					
---	---					

Detailed explanation (for IPv4) is shown below:

Item	Description
LAN Status	<p>Primary DNS-Displays the primary DNS server address for WAN interface.</p> <p>Secondary DNS -Displays the secondary DNS server address for WAN interface.</p> <p>IP Address-Displays the IP address of the LAN interface.</p> <p>TX Packets-Displays the total transmitted packets at the LAN interface.</p> <p>RX Packets-Displays the total received packets at the LAN interface.</p>
WAN1/WAN2	Enable – Yes in red means such interface is available but not

Item	Description
	<p>enabled. Yes in green means such interface is enabled.</p> <p>Line – Displays the physical connection (Ethernet, or USB) of this interface.</p> <p>Name – Display the name of the router.</p> <p>Mode - Displays the type of WAN connection (e.g., PPPoE).</p> <p>Up Time - Displays the total uptime of the interface.</p> <p>IP - Displays the IP address of the WAN interface.</p> <p>GW IP - Displays the IP address of the default gateway.</p> <p>TX Packets - Displays the total transmitted packets at the WAN interface.</p> <p>TX Rate - Displays the speed of transmitted octets at the WAN interface.</p> <p>RX Packets - Displays the total number of received packets at the WAN interface.</p> <p>RX Rate - Displays the speed of received octets at the WAN interface.</p>

Detailed explanation (for IPv6) is shown below:

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

1.9 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.

This page is left blank.

2

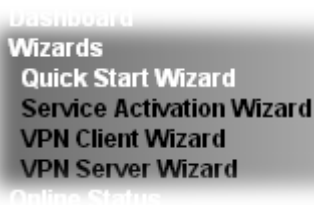
Quick Setup

There are several setup wizards offered for you to configure the router simply and quickly.

- **Quick Start Wizard** – used for building network connection, Internet access.
- **Service Activation Wizard** – used for activating the web content filter service.
- **VPN Client Wizard** – used for establishing VPN tunnel; the router is treated as a VPN client.
- **VPN Server Wizard** – used for establishing VPN tunnel; the router is treated as a VPN server.

2.1 Quick Start Wizard

The **Quick Start Wizard** is designed for you to easily set up your router for Internet access. Open **Wizards>>Quick Start Wizard**.



It can help you to deploy and use the router easily and 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 23 characters).

Old Password	<input type="password" value="••••"/>
New Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>

< Back Next > Finish Cancel

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

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1 ▾
Display Name:	<input type="text"/>
Physical Mode:	Ethernet
Physical Type:	Auto negotiation ▾

< Back

Next >

Finish

Cancel

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

2.1.1 For WAN1 (Ethernet)

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

Quick Start Wizard

WAN Interface

WAN Interface:	WAN1 ▾
Display Name:	<input type="text"/>
Physical Mode:	Ethernet
Physical Type:	Auto negotiation ▾

< Back Next > Finish Cancel

2.1.1.1 PPPoE

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.
2. Choose **WAN1** as the WAN Interface and click the **Next** button.
3. The following page will be open for you to specify Internet Access Type. Click **PPPoE** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

- PPPoE
- PPTP
- L2TP
- Static IP
- DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

PPPoE Client Mode

WAN 1
Enter the user name and password provided by your ISP.

Service Name (Optional)

Username

Password

Confirm Password

Available settings are explained as follows:

Item	Description
Service Name	Type the service information for identifying ISP.
Username	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

- A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
 Physical Mode: Ethernet
 Internet Access: PPPoE

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

6. Click **Finish**. A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.2 PPTP/L2TP

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.
2. Choose **WAN1** as the WAN Interface and click the **Next** button.
3. The following page will be open for you to specify Internet Access Type. Click **PPTP/L2TP** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

4. 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

PPTP Client Mode

WAN 1
Enter the username, password, WAN IP configuration and PPTP server IP provided by your ISP.

Username
 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
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.

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

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Internet Access:	PPTP
<p>Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.</p>	

6. Click **Finish**. A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.3 Static IP

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.
2. Choose **WAN1** as the WAN Interface and click the **Next** button.
3. The following page will be open for you to specify Internet Access Type. Click **Static IP** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

Static IP Client Mode

WAN 1
Enter the Static IP configuration provided by your ISP.

WAN IP
Subnet Mask
Gateway
Primary DNS
Secondary DNS (optional)

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.

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

5. A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
 Physical Mode: Ethernet
 Internet Access: Static IP

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

6. Click **Finish**. A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

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

2.1.1.4 DHCP

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**.
2. Choose **WAN1** as the WAN Interface and click the **Next** button.
3. The following page will be open for you to specify Internet Access Type. Click **DHCP** as the Internet Access Type. Then click **Next** to continue.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

< Back Next > Finish Cancel

4. Click **DHCP** as the Internet Access type. Simply click **Next** to continue. Then click **Next** for viewing summary of such connection.

Quick Start Wizard

DHCP Client Mode

WAN 1
If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name (optional)
MAC (optional)

< Back Next > Finish Cancel

Available settings are explained as follows:

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

	enter the MAC address.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

- A summary page will be displayed as follows.

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
 Physical Mode: Ethernet
 Internet Access: DHCP

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.

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

2.1.2 For WAN2 (USB)

WAN2 is dedicated to physical mode in USB.

1. Open **Wizards>>Quick Start Wizard**. Finish the password settings and click **Next**
2. Choose **WAN1** as the WAN Interface and click the **Next** button.

Quick Start Wizard

WAN Interface

WAN Interface:	WAN2
Display Name:	<input type="text"/>
Physical Mode:	USB

< Back Next > Finish Cancel

3. In the following page, fill in the information for 3G/4G USB Modem.

Quick Start Wizard

Connect to Internet

WAN 2	
Internet Access :	3G/4G USB Modem(PPP mode)
3G/4G USB Modem(PPP mode)	
SIM PIN code	<input type="text"/>
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	<input type="text"/> <input type="button" value="Apply"/>

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Internet Access	Choose a protocol for accessing the Internet.
3G/4G USB Modem (PPP mode)	<p>SIM Pin code –Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.</p> <p>Modem Initial String – Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP. The maximum length</p>

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

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN2
Physical Mode:	USB
Internet Access:	PPP
<p>Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.</p>	

- Click **Finish**. A page of **Quick Start Wizard Setup OK!!!** will appear.

Quick Start Wizard Setup OK!

- Now, you can enjoy surfing on the Internet.

2.2 Service Activation Wizard

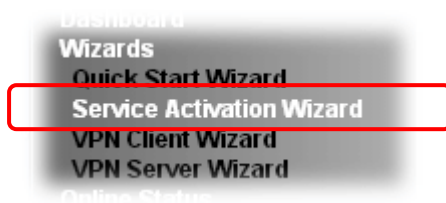
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. **For the Service Activation Wizard is only available for admin operation, therefore, please type “admin/admin” on Username/Password while Logging into the web user interface.**

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 **Wizards>>Service Activation Wizard**.



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

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
 Formal edition with license key

Free trial edition: it offers a period of trial for you to get acquainted with WCF function.

Formal edition with license key: you can extend the license valid time manually.

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

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

Service Activation Wizard

Select the service type that you want to activate

This product provides 30 days of free trial, please choose the item(s) you want to use.

WCF service:

Web Content Filter (BPjM)
BPjM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPjM WCF service. This is a free service without guarantee.
Activation Date : 2013-02-18

Web Content Filter (Commtouch) [License Agreement](#)
Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.
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.

< Back **Next >** Finish Cancel

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> .

4. 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.

< Back **Next >** Finish Cancel

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

Service Activation Wizard

Connection Succeeded!

Please check the following item(s) to enable services on your router.

Enable Web Content Filter

Next >

Finish

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

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

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

Service Activation Wizard

Server Enabled!

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2013-02-18	2013-03-21	Commtouch

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

Copyright © DrayTek Corp. All Rights Reserved.

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

Formal edition with license key

Next >

Finish

Cancel

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 (CommTouch)

License Agreement

CommTouch is the web content filter based on CommTouch operated in the worldwide.

Enter your License key:

Activation Date : 2013-03-22 select

Web Content Filter (fragFINN)

License Agreement

Enter your License key:

Activation Date : 2013-02-18 select

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.

< Back

Next >

Finish

Cancel

2.3 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: Route Mode ▾

Please choose a LAN-to-LAN Profile: [Index] [Status] [Name] ▾

Note: For a typical LAN-to-LAN tunnel, please select Route Mode.
 If the remote network is expecting only a single client or ip and is not configured to route the subnet and then select NAT mode.
 If in doubt then select Route Mode

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode. <div style="border: 1px solid #ccc; padding: 2px; width: fit-content;"> Route Mode ▾ Route Mode NAT Mode </div>
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

[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)	Throughput ranking (1 is the highest; 5 is the lowest)
1. L2TP over IPsec	1. PPTP (None Encryption)
2. IPsec	2. L2TP
3. PPTP (Encryption)	3. IPsec
4. L2TP	4. L2TP over IPsec
5. PPTP (None Encryption)	5. PPTP (Encryption)

Select VPN Type:

- PPTP (None Encryption)
- PPTP (Encryption)
- IPsec
- L2TP
- L2TP over IPsec (Nice to Have)
- L2TP over IPsec (Must)

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

Note: The following descriptions for VPN Type are based on the **Route Mode** specified in **LAN-to-LAN Client Mode Selection**.

- When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP Encryption Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	●●●●●●
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **IPsec**, you will see the following graphic:

VPN Client Wizard

VPN Client IPsec Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE 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)	DES without Authenticator
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP**, you will see the following graphic:

VPN Client Wizard

VPN Client L2TP Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

- When you choose **L2TP over IPsec (Nice to Have)** or **L2TP over IPsec (Must)**, you will see the following graphic:

VPN Client Wizard

VPN Client L2TP over IPsec (Nice to Have) Settings

Profile Name	???
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE 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)	DES without Authenticator
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
Always On	Check to enable router always keep VPN connection.
Server IP/Host Name for VPN	Type the IP address of the server or type the host name for such VPN profile.
IKE Authentication Method	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. Pre-Shared Key- Specify a key for IKE authentication. Confirm Pre-Shared Key- Confirm the pre-shared key.
Digital Signature (X.509)	Click Digital Signature to invoke this function. Peer ID – Choose the peer ID selection from the drop down list. Local ID – Choose Alternative Subject Name First or Subject Name First . Local Certificate – Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in Certificate Management >> Local Certificate . Otherwise, the setting you choose here will not be effective.
IPsec Security Method	Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the use name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

- 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 Client Wizard

Please confirm your settings

LAN-to-LAN Index: 3
Profile Name: VPN_Jim
VPN Connection Type: L2TP over IPsec (Nice to Have)
Always on: No
Server IP/Host Name: 172.16.3.8
IKE Authentication Method: Pre-Shared Key
IPsec Security Method: AH-SHA1
Remote Network IP: 172.16.3.99
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
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

2.4 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 Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection: Remote Dial-in User (Teleworker) ▾

Please choose a LAN-to-LAN Profile: 1 x ??? ▾

Please choose a Dial-in User Accounts: 8 x ??? ▾

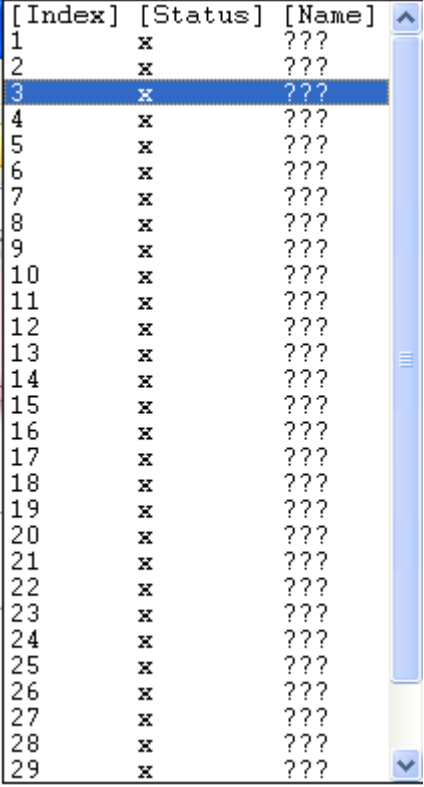
Allowed Dial-in Type:

- PPTP
- IPsec
- L2TP with IPsec Policy None ▾
- SSL Tunnel

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	<p>Choose the direction for the VPN server.</p> <p>Site to Site VPN – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.</p> <p>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.</p> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> ▾ <p>Site to Site VPN (LAN-to-LAN)</p> <p style="background-color: #e0e0e0;">Site to Site VPN (LAN-to-LAN)</p> <p>Remote Dial-in User (Teleworker)</p> </div>
Please choose a LAN-to-LAN Profile	<p>This item is available when you choose Site to Site VPN (LAN-to-LAN) as VPN server mode. 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	???																																																																																									
<p>Please choose a Dial-in User Accounts</p>	<p>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.</p>																																																																																										
<p>Allowed Dial-in Type</p>	<p>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).</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy <input checked="" type="checkbox"/> SSL Tunnel <div style="border: 1px solid gray; padding: 2px; display: inline-block;"> None ▼ None Nice to Have Must </div> <p>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.</p>																																																																																										

- 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 Server Wizard

VPN Authentication Setting

Profile Name	<input type="text"/>
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	<input data-bbox="995 405 1270 434" type="text" value="???"/>
Password	<input type="text"/>
Peer IP/VPN Client IP	<input type="text"/>
Site to Site Information	
Remote Network IP	<input type="text"/>
Remote Network Mask	<input type="text"/>

- 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 Server Wizard

VPN Authentication Setting

Profile Name	<input data-bbox="1002 1122 1276 1151" type="text" value="???"/>
PPTP / L2TP / L2TP over IPsec / SSL Tunnel Authentication	
Username	<input data-bbox="1002 1180 1276 1209" type="text" value="???"/>
Password	<input type="text"/>
IPsec / L2TP over IPsec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	<input type="text"/>
Confirm Pre-Shared Key	<input type="text"/>
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	<input data-bbox="1008 1368 1283 1397" type="text" value="None"/>
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	<input type="text"/>
Peer ID	<input type="text"/>
Site to Site Information	
Remote Network IP	<input data-bbox="1002 1579 1276 1608" type="text" value="0.0.0.0"/>
Remote Network Mask	<input data-bbox="1002 1615 1276 1644" type="text" value="255.255.255.0"/>

- When you check **IPsec**, you will see the following graphic:

VPN Server Wizard

VPN Authentication Setting

Profile Name	???
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

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
Pre-Shared Key	For IPsec/L2TP IPsec authentication, you have to type a pre-shared key. The length of the name is limited to 64 characters.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Peer ID – Choose the peer ID selection from the drop down list. Local ID – Choose Alternative Subject Name First or Subject Name First .
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client. The length of the name is limited to 47 characters.

Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

3. After finishing the configuration, please click **Next**. The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

VPN Server Wizard

Please Confirm Your Settings

VPN Environment:	Site to Site VPN (LAN-to-LAN)
Index:	2
Profile Name:	???
Username:	???
Allowed Service:	PPTP+L2TP with IPsec Policy
Peer IP/VPN Client IP:	
Peer ID:	456
Remote Network IP:	172.16.3.56
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 Server Wizard setup.
- View more detailed configurations.

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

2.5 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.

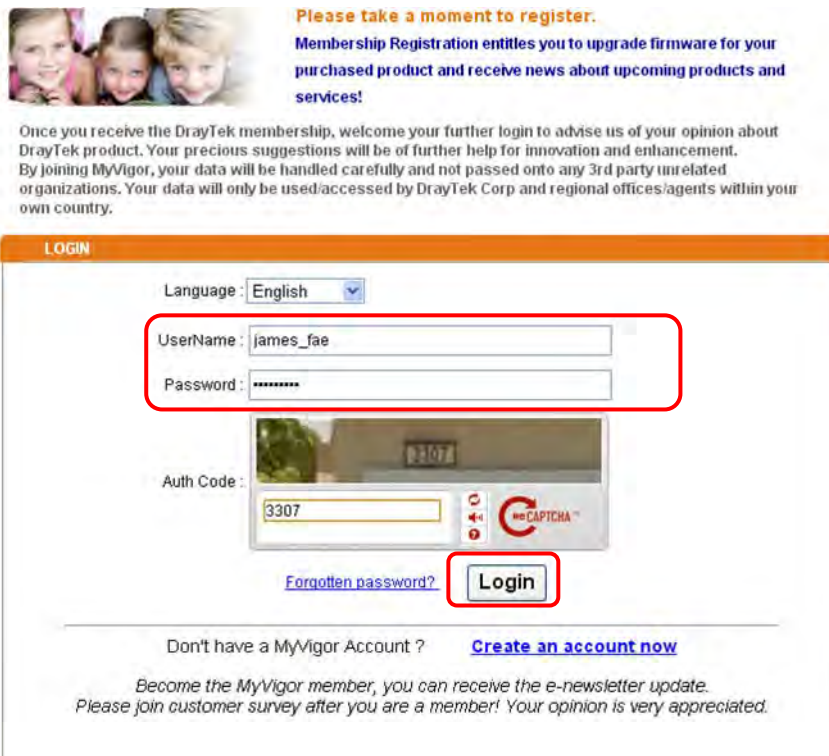
- 1 Please login the web configuration interface of Vigor router by typing “**admin/admin**” as User Name / Password.



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

Support Area
Product Registration

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



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

DrayTek MyVigor

Home Search

My Information

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

RowNo : 5 PageNo : 1 **Add**

Your Device List

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

Product Registration

- 4 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**.

DrayTek MyVigor

Home Search GO

My Product Search for this site GO

Registration Device

Serial number : [2011082214320301](#)

Nickname : *

Registration Date :

Usage :

Product Rating : [Your opinion so far]

No. of Employees : [In total within your company]

Supplier : [Where you bought it from]

Date of Purchase : [mm-dd-yyyy]

Internet Connection : *

Cable ADSL VDSL Fiber

3G WIMAX LTE

Cancel **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.

The screenshot shows the MyVigor website interface. The left sidebar contains navigation links: Home, About Us, Product, My Information, VigorACS SI, Vigor Series, Management, and Customer Survey. The main content area displays 'My Information' with user details and a 'Your Device List' table. The table has columns for Serial Number / Host ID, Device Name, Model, and Note. The last row, with serial number 2011082214320301, is highlighted with a red box.

Serial Number / Host ID	Device Name	Model	Note
20100707144801	Vigor3300V	Vigor3300	-
20100708105301	Vigor2820	Vigor2820	-
20101005104801	Vigor2710vn	Vigor2710	-
2010121707335201	Vigor2380	Vigor2830	-
2011082214320301	Vigor 2120	Vigor 2120	-

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

The screenshot shows the 'My Product' page. Under 'Device Information', there are buttons for 'Rename', 'Transfer', and 'Back'. Below this, there are two tabs: 'Device's Service' (selected) and 'Expired License'. A table lists services with columns for Service, Provider, Action, Status, Start Date, and Expired Date. The 'Trial' button in the 'Action' column is highlighted with a red box. Below the table, there is a note about the trial service.

Service	Provider	Action	Status	Start Date	Expired Date
WCF	Commtouch	Trial	On	-	-

The [Commtouch GlobalView Web Filter](#) is provided for Vigor router with only 1-month trial. After trial period, please purchase the official package from your local DrayTek dealer/distributor.

BPM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPM/WCF service. This is a free service without guarantee.

- 9 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**.

- 10 When this page appears, click **Register**.

- 11 Wait for a moment until the following page appears.

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2013-08-24	2013-09-23	Commtouch

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

Copyright © DrayTek Corp. All Rights Reserved.

- 12 Click **Close**.

3

Tutorials and Applications

3.1 How to configure settings for IPv6 Service in Vigor2120

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 Vigor2120, 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 Vigor2120, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

1. Access into the web user interface of Vigor2120. 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	Static or Dynamic IP	Details Page IPv6
WAN2		USB	None	Details Page IPv6

Note: Only one WAN interface support IPv6 service at one time. In this example, WAN1 is chosen as the one supporting IPv6 service.

- In the following figure, use the drop down list to choose a proper connection type.

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type

Offline

Offline

PPP

TSPC

AICCU

DHCPv6 Client

Static IPv6

6in4 Static Tunnel

6rd

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.

Internet Access >> PPPoE

PPPoE Client Mode

PPPoE Setup

PPPoE Link Enable Disable

ISP Access Setup

ISP Name: Hinet

Username: 73168525@hinet.net

Password:

Index(1-15) in **Schedule** Setup:
=> [] , [] , [] , []

WAN Connection Detection

Mode: ARP Detect

Ping IP: []

TTL: []

PPPoE Pass-through

For Wired LAN

For Wireless LAN

PPP/MP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP) WAN IP Alias

Fixed IP: Yes No (Dynamic IP)

Fixed IP Address: []

Default MAC Address

Specify a MAC Address

MAC Address: 00 : 1D : AA : 9C : F7 : 35

OK

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type: PPP

Note : IPv4 WAN setting should be PPPoE client.

OK

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 >> Dial PPPoE						
Enable	Line	Name	Mode	Up Time		
Yes	ADSL		PPPoE	00:00:00		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
---	---	0	0	0	0	
WAN 2 Status >> Drop PPPoE						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:00:54		
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)	
114.44.49.54	168.95.98.254	800	4761	821	6617	

Online Status

Physical Connection						System Uptime: 0:2:32
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 >> Drop PPP						
Enable	Mode	Up Time				
Yes	PPP	0:02:08				
IP	Gateway IP					
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)	FE80::90:1A00:242:AD52					
FE80::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.)

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode	
Connection Type	TSPC
TSPC Configuration	
Username	cacahsu
Password	*****
Confirm Password	*****
Tunnel Broker	broker.freenet6.net
OK	

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		
LAN Status			
IP Address			
2001:5C0:1502:D00:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
88	121	15596	10249
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	TSPC	0:01:40	
IP			Gateway IP
2001:5C0:1400:B::10B9/128 (Global)			---
FE80::722C:3559/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
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.)

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode

Connection Type: AICCU

AICCU Configuration

Always On

Username: JCR3-SIXXS

Password: *****

Confirm Password: *****

Tunnel Broker: tic.sixxs.net

Subnet Prefix: 2001:4DD0:FF00:8805::2 / 64

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

OK

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

Online Status

System Uptime: 0:1:18

Physical Connection		IPv4	IPv6
LAN Status			
IP Address			
2001:4DD0:FF00:83E4:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
147	187	34205	19176
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	AICCU	0:00:48	
IP		Gateway IP	
2001:4DD0:FF00:3E4::2/64 (Global)		---	
FE80::4CD0:FF00:3E4:2/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
186	137	16438	33093

- **DHCPv6 Client**

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode	
Connection Type	DHCPv6 Client
DHCPv6 Client Configuration	
Identity Association	<input type="radio"/> Prefix Delegation <input checked="" type="radio"/> Non-temporary Address
IAID (Identity Association ID)	1779026617
OK	

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: 0:0:50	
IPv4		IPv6	
LAN Status			
IP Address			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
6	2	588	156
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	DHCPv6 Client	0:00:40	
IP			Gateway IP
2001:B010:7300:201:21D:AFF:FEA6:256A/64 (Global)			---
2001:1111:2222:5555:21D:AFF:FEA6:256A/64 (Global)			
2001:1111:2222:3333::1111/128 (Global)			
FE80::21D:AFF:FEA6:256A/64 (Link)			
DNS IP			
2001:4860:4860::8888			
2001:4860:4860::8844			
TX Packets	RX Packets	TX Bytes	RX Bytes
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 Add Delete

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	
Yes	Static IPv6	0:03:56	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/64 (Global)		---	
2001:1111:2222:5555:21D:AFF:FEA6:256A/64 (Global)			
FE80::21D:AFF:FEA6:256A/64 (Link)			
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 Vigor2120. Open **LAN>> General Setup**. Click the **IPv6** button to display the following page.

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

LAN >> General Setup

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

Router Advertisement Server

Enable Disable

Advertisement Lifetime Seconds (Range : 600 - 9000)

DHCPv6 Server

Enable Server Disable Server

Start IPv6 Address

End IPv6 Address

DNS Server IPv6 Address

Primary DNS Server

Secondary DNS Server

Static IPv6 Address configuration

IPv6 Address / Prefix Length

 /

Current IPv6 Address Table

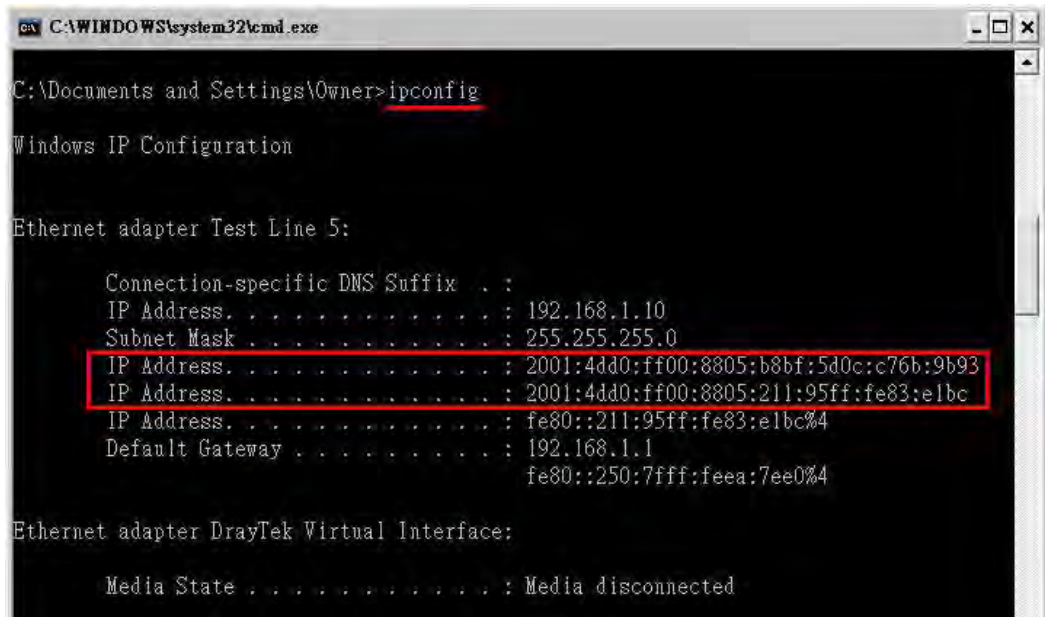
Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FEA6:2568/64	Link

2. In the field of **Router Advertisement Server**, 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 **DHCPv6 Server**, 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:

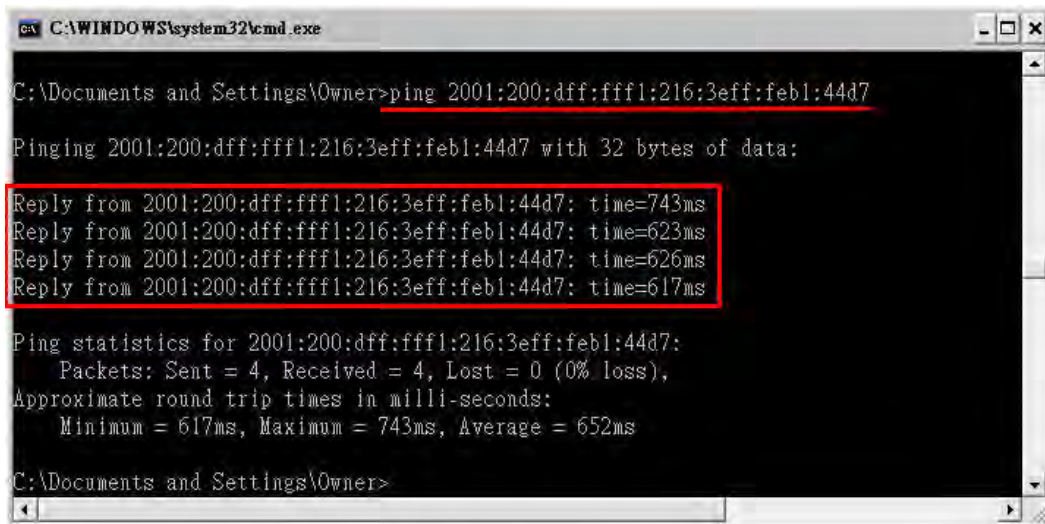
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.10
    Subnet Mask . . . . .            : 255.255.255.0
    IP Address. . . . .               : 2001:4dd0:ff00:8805:b8bf:5d0c:c76b:9b93
    IP Address. . . . .               : 2001:4dd0:ff00:8805:211:95ff:fe83:e1bc
    IP Address. . . . .               : fe80::211:95ff:fe83:e1bc%4
    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 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. 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 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 or FTP server.

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 Device Status

Disk	Modem	Printer	Refresh
USB Mass Storage Device Status			
Connection Status: Disk Connected		<input type="button" value="Disconnect USB Disk"/>	
Write Protect Status: No			
Disk Capacity: 2009 MB			
Free Capacity: 1212 MB <input type="button" value="Refresh"/>			
USB Disk Users Connected			
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it

2. 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

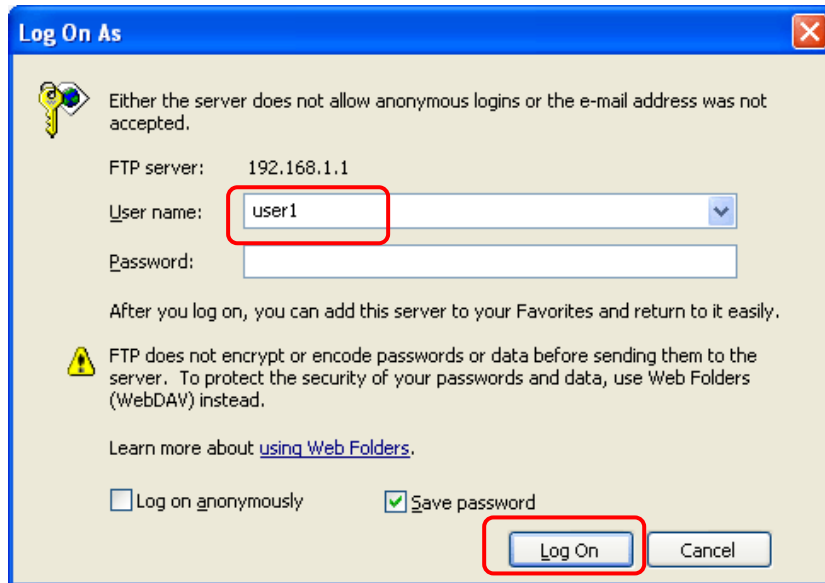
Profile Index: 1

FTP/Samba User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="text"/> (Maximum 11 Characters)
Confirm Password	<input type="text"/>
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

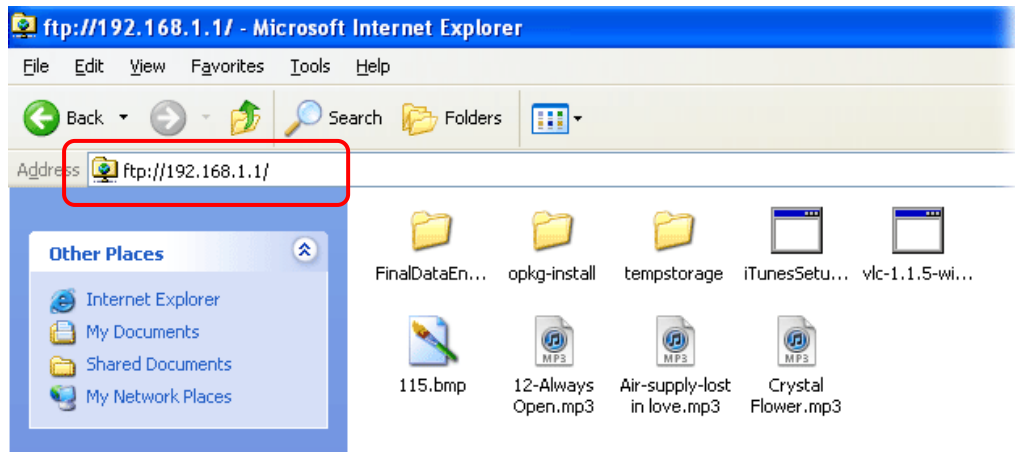
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

3. 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.



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



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

USB Application >> USB Device Status

Disk	Modem	Printer	Refresh	
USB Mass Storage Device Status				
Connection Status: Disk Connected				Disconnect USB Disk
Write Protect Status: No				
Disk Capacity: 2009 MB				
Free Capacity: 1212 MB Refresh				
USB Disk Users Connected				
Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.10(1963)	user1	Drop

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.

Now, users in LAN of Vigor2120 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**.

3.3 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 Trunk

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"/>	---

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:

VPN Dial-Out Through:

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block

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

2. Dial-Out Settings

- 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

<p>Allowed Dial-In Type</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 None</p> <hr/> <p><input checked="" type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP <input type="text" value="218.242.130.19"/></p> <p>or Peer ID <input type="text"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password <input style="width: 100px;" type="password"/></p> <p>VJ Compression <input type="radio"/> On <input checked="" type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p><input type="button" value="IKE Pre-Shared Key"/> <input style="width: 100px;" type="text"/></p> <p><input checked="" type="checkbox"/> Digital Signature(X.509)</p> <p>None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>
---	---

4. Gre over IPsec Settings

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

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction Disable
Remote Gateway IP <input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do
<input checked="" type="checkbox"/> Remote Network IP <input type="text" value="192.168.1.0"/>	<input type="button" value="Route"/>
<input checked="" type="checkbox"/> Remote Network Mask <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
<input type="checkbox"/> Local Network IP <input type="text" value="192.168.1.9"/>	
<input type="checkbox"/> Local Network Mask <input type="text" value="255.255.255.0"/>	
<input type="button" value="More"/>	

- 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 Seconds : 5

VPN Connection Status
Current Page: 1 Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
1 (VPN Server)	IPSec Tunnel DES-SHA1 Auth	218.242.130.19	192.168.1.0/24	353	3	291	3	0:13:58 <input type="button" value="Drop"/>

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

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: [Set to Factory Default](#)

View: All Trunk

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

- 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 Call Direction Both Dial-Out Dial-in

Enable this profile Always on

Netbios Naming Packet Pass Block

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

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.

2. Dial-Out Settings

<p>Type of Server I am calling</p> <p><input type="radio"/> PPTP</p> <p><input checked="" type="radio"/> IPsec Tunnel</p> <p><input type="radio"/> L2TP with IPsec Policy None</p> <p>Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)</p> <p>218.242.133.91</p>	<p>Username ???</p> <p>Password</p> <p>PPP Authentication PAP/CHAP</p> <p>VJ Compression <input type="radio"/> On <input checked="" type="radio"/> Off</p> <p>IKE Authentication Method</p> <p><input checked="" type="radio"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key ●●●●●●●●</p> <p><input type="radio"/> Digital Signature(X.509)</p> <p>Peer ID None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <p>IPsec Security Method</p> <p><input type="radio"/> Medium(AH)</p> <p><input checked="" type="radio"/> High(ESP) 3DES with Authentication</p> <p>Advanced</p> <p>Index(1-15) in <u>Schedule</u> Setup:</p> <p><input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p>
---	--

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

My WAN IP 0.0.0.0	RIP Direction Disable
Remote Gateway IP 0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP 172.17.1.0	Route
Remote Network Mask 255.255.255.0	
Local Network IP 192.168.1.9	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
Local Network Mask 255.255.255.0	
More	

OK Clear 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 Seconds : Refresh

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime	
1 (VPN Client)	IPSec Tunnel DES-SHA1 Auth	218.242.133.91	172.17.1.0/24	8	3	132	36	0:6:41	<input type="button" value="Drop"/>

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

3.4 How to Optimize the Bandwidth through QoS Technology

Have you ever gotten any problems in uploading/downloading files (Voice, video or email/data only) with the narrow/districted bandwidth you may share from the common Internet connection line? The advanced bandwidth management technology-QoS (Quality of Service) helps you to well allocate the bandwidth upon your demand of Voice, Video, or Data transferring. Let's see how to get the optimum bandwidth per your request by using DrayTek Vigor router as below.

Scenario: The Internet connection you got from ISP line is 2MB/512Kb. There are VoIP telephony network, IPTV set top box and data server at your home. Assume you want to allocate 30% of the bandwidth you got to VoIP demand, 50% for IPTV, 15% for mail/data, 5% for others. Let's see how easily it is to do the setting as below:

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



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

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

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

Bandwidth Management >> Quality of Service

Class Index #1

Name: Tag packets as:

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

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

Rule Edit

<input checked="" type="checkbox"/> ACT	
Ethernet Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Local Address	Any <input type="button" value="Edit"/>
Remote Address	Any <input type="button" value="Edit"/>
DiffServ CodePoint	ANY
Service Type	---Predefined---

Note: Please choose/setup the **Service Type** first.

- 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.

Ethernet Type: IPv4

Address Type	Range Address
Start IP Address	172.16.1.240
End IP Address	172.16.1.241
Subnet Mask	0.0.0.0

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

Rule Edit

<input checked="" type="checkbox"/> ACT	
Ethernet Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Local Address	172.16.1.240~172.16.1.241 <input type="button" value="Edit"/>
Remote Address	Any <input type="button" value="Edit"/>
DiffServ CodePoint	ANY
Service Type	---Predefined---

Note: Please choose/setup the **Service Type** first.

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

Bandwidth Management >> Quality of Service

Class Index #1
 Name Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY

8. 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 #2
 Name Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY

and

Bandwidth Management >> Quality of Service

Class Index #3
 Name Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	IP precedence 2	ANY

9. Assuming you get 2MB/512Kb Internet line. You can click the **Setup** link of WAN1 to set up the bandwidth for different groups among VoIP, IPTV and Data/Email.

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	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	
Class 2	IPTV	Edit	Edit
Class 3	Data/Email	Edit	

10. In the Setup page, check the box of **Enable the QoS Control**. Type 30, 50 and 15 in the boxes for VoIP, IPTV and Data/Email respectively. Check the box of **Enable UDP Bandwidth Control**.

Bandwidth Management >> Quality of Service

General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth Kbps Mbps

WAN Outbound Bandwidth Kbps Mbps

Index	Class Name	Reserved Bandwidth Ratio
Class 1	VoIP	<input type="text" value="30"/> %
Class 2	IPTV	<input type="text" value="50"/> %
Class 3	Data/Email	<input type="text" value="15"/> %
	Others	<input type="text" value="5"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %

Outbound TCP ACK Prioritize

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.

11. 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	100000Kbps/100000Kbps	Outbound	30%	50%	15%	5%	Active	Status	Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	VoIP	Edit	Edit
Class 2	IPTV	Edit	
Class 3	Data/Email	Edit	


3.5 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.

3.5.1 Create an Account via Vigor Router

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

CSM >> Web Content Filter Profile 

Web-Filter License **Activate**
[Status:Not Activated]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

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

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

Administration Message (Max 255 characters) Default Message Cache : L1 + L2 Cache

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%  
<br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.  
<p>Please contact your system administrator for further information.</center></body>
```

Or

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

System Maintenance >> Activation Activate via interface : auto-selected

Web-Filter License **Activate**
[Status:Not Activated]

Authentication Message

```
Activation authenticate fail, contact with support@draytek.com, 2012-10-30 16:17:01
```

2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.



Please take a moment to register.

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

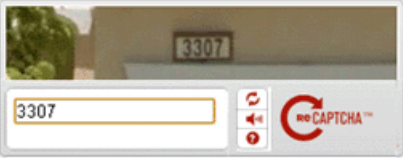
Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

LOGIN

Language :

UserName :

Password :

Auth Code : 

[Forgotten password?](#)

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

*Become the MyVigor member, you can receive the e-newsletter update.
Please join customer survey after you are a member! Your opinion is very appreciated.*

3. Click the link of **Create an account now**.
4. Check to confirm that you accept the Agreement and click **Accept**.

Register

Create an account - Please enter personal profile.

- 1 Agreement**
- 2 Personal Information
- 3 Preferences
- 4 Completion

===== MyVigor Agreement =====

1. Agreement
Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the modifications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration
To use this service, you have to agree the following conditions:
(a) Provide your complete and correct information according to the registration steps of this service.
(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your account.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

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

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

- 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**.

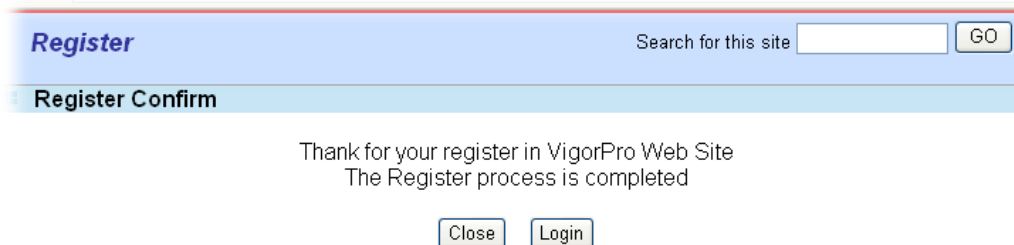
***** This is an automated message from myvigor.draytek.com. *****

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

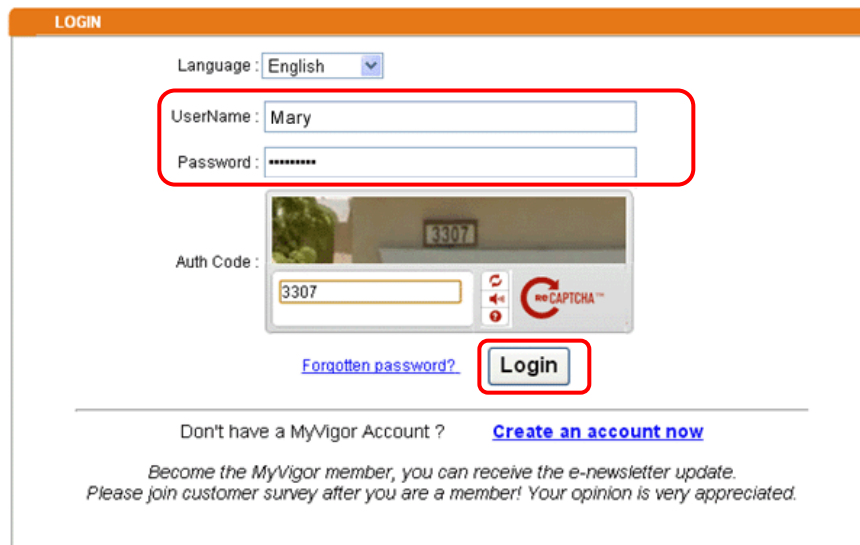
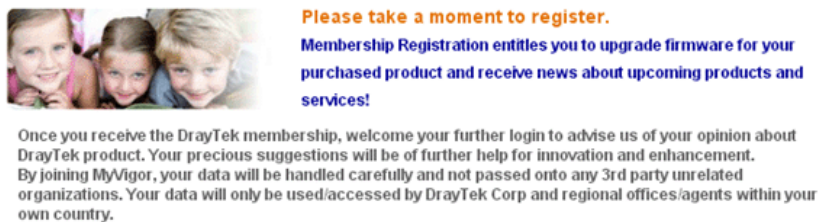
Please click on the activation link below to activate your account

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**.



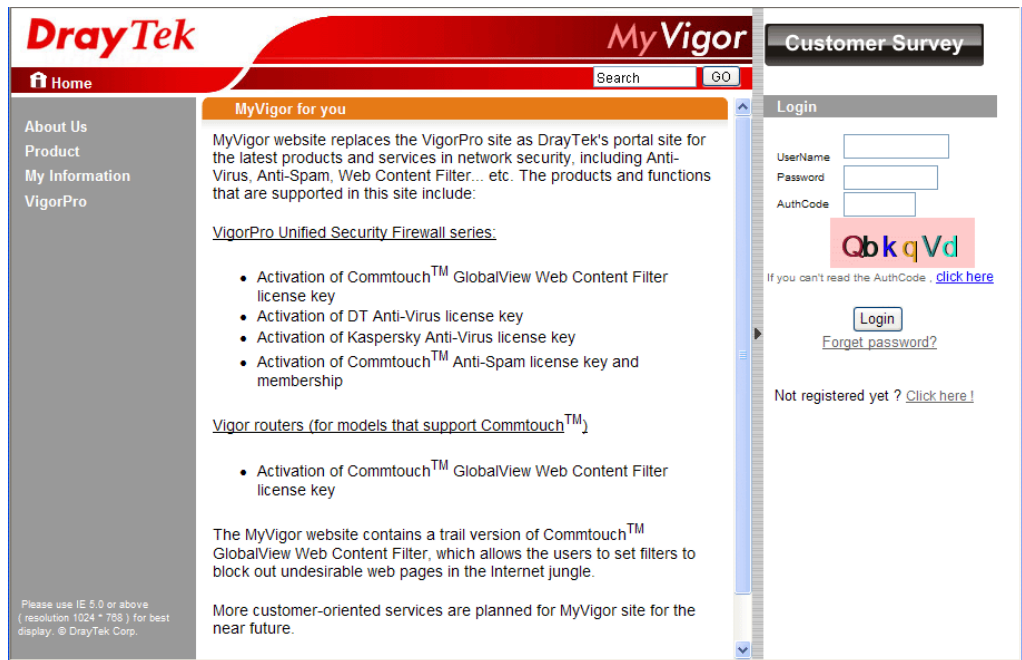
10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.



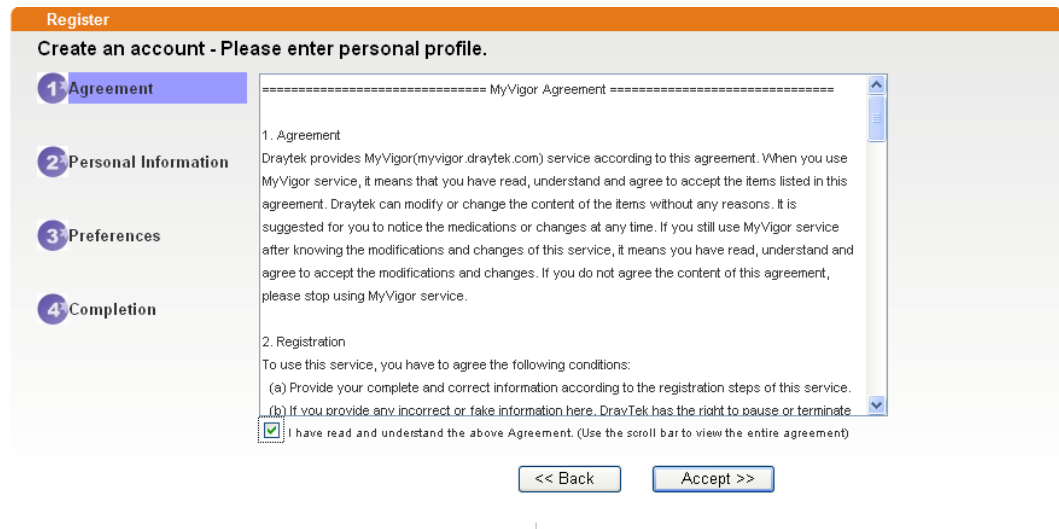
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

3.5.2 Create an Account via MyVigor Web Site

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



2. Check to confirm that you accept the Agreement and click **Accept**.



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

Register
Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:* Mary
(3 ~ 20 characters)

Password:*
(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:*

Personal Information

First Name:* Mary

Last Name:* Ted

Company Name: Tech Ltd.

Email Address:* mary_ted@tech.com
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country:* SWITZERLAND

Career:* Supervisor

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

Register
Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

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

Register
Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Completion

A confirmation email has been sent to **mary_ted@tech.com**
Please click on the activation link in the email
to activate your account

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**.

Register Search for this site

Register Confirm

The Confirm message of New Owner(Mary) maybe timeout
Please try again or contact to draytek.com

Close 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!


Once you receive the DrayTek membership, welcome your further login to advise us of your opinion about DrayTek product. Your precious suggestions will be of further help for innovation and enhancement. By joining MyVigor, your data will be handled carefully and not passed onto any 3rd party unrelated organizations. Your data will only be used/accessed by DrayTek Corp and regional offices/agents within your own country.

LOGIN

Language : English

UserName : Mary

Password : *****

Auth Code :  3307

Forgotten password? Login

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

Become the MyVigor member, you can receive the e-newsletter update.
Please join customer survey after you are a member! Your opinion is very appreciated.

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

3.6 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
<u>1.</u>		kotsms.com.tw (TW)
<u>2.</u>		kotsms.com.tw (TW)
<u>3.</u>		kotsms.com.tw (TW)
<u>4.</u>		kotsms.com.tw (TW)
<u>5.</u>		kotsms.com.tw (TW)
<u>6.</u>		kotsms.com.tw (TW)
<u>7.</u>		kotsms.com.tw (TW)
<u>8.</u>		kotsms.com.tw (TW)
<u>9.</u>	Custom 1	
<u>10.</u>	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	<input type="text" value="Local number"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/> ▼
Username	<input type="text" value="abc5026"/>
Password	<input type="password" value="●●●"/>
Quota	<input type="text" value="3"/>
Sending Interval	<input type="text" value="3"/> (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

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
1.	Local number	kotsms.com.tw (TW)	
2.		kotsms.com.tw (TW)	
3.		kotsms.com.tw (TW)	
4.		kotsms.com.tw (TW)	
5.		kotsms.com.tw (TW)	
6.		kotsms.com.tw (TW)	
7.		kotsms.com.tw (TW)	
8.		kotsms.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

			Set to Factory Default
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		<input type="text" value="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	

- 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		
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 <input checked="" type="checkbox"/>	1 - Local number	0912345678	1 - WAN_Notify	<input type="text"/> <input type="text"/>
2 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
3 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
4 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
5 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
6 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
7 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
8 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
9 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>
10 <input type="checkbox"/>	1 - Local number		1 - WAN_Notify	<input type="text"/> <input type="text"/>

- 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.

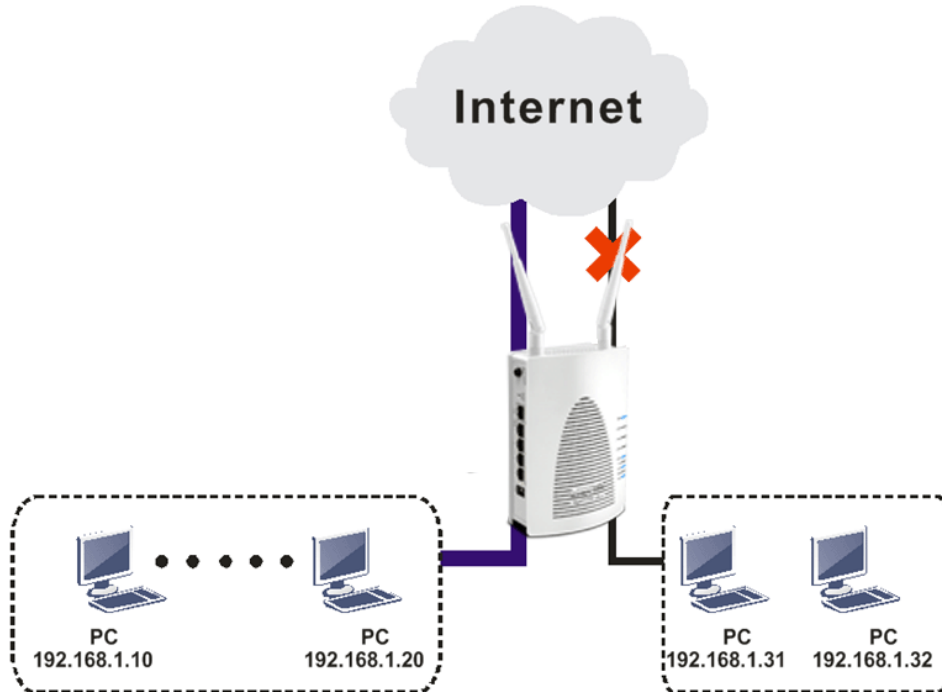
Object Settings >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text" value="clickatell"/>
<div style="border: 1px solid gray; height: 50px; width: 100%;"></div>	
Please contact with your SMS provide to get the exact URL String eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username===txtUser### &password===txtPwd###&msisdn===txtDest###&message===txtMsg###	
Username	<input type="text" value="ilan123"/>
Password	<input type="password" value="••••••"/>
Quota	<input type="text" value="3"/>
Sending Interval	<input type="text" value="3"/> (seconds)

3.7 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

Filter Setup				Set to Factory Default
Set	Comments	Set	Comments	
1.	Default Call Filter	7.		
2.	Default Data Filter	8.		
3.		9.		
4.		10.		
5.		11.		
6.		12.		

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
2	<input type="checkbox"/>		UP	Down
3	<input type="checkbox"/>		UP	Down
4	<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:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Sessions Control:

Syslog:

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:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

Syslog:

- 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

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

Filter Set 2 Rule 3

<input checked="" type="checkbox"/> Check to enable the Filter Rule		
Comments:	open_ip	
Index(1-15) in Schedule Setup:	, , ,	
Clear sessions when schedule ON:	<input type="checkbox"/> Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	192.168.1.10~192.168.1.20	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care	
Application	Action/Profile	Syslog
Filter:	Pass Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	


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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		<u>Down</u>
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	block_all	<u>UP</u>	<u>Down</u>
<input type="text" value="3"/>	<input checked="" type="checkbox"/>	open_ip	<u>UP</u>	<u>Down</u>
<input type="text" value="4"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" value="5"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" value="6"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="text" value="7"/>	<input type="checkbox"/>		<u>UP</u>	

Next Filter Set 

9. Now, all the settings are configured well. Only the computers with the IP addresses within 192.168.1.10 ~ 192.168.1.20 can access to Internet.

3.8 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter

There are two ways to block the facebook service, Web Content Filter and URL Content Filter.

Web Content Filter,

Benefits: Easily and quickly implement the category/website that you want to block.

Note: License is required.

URL Content Filter,

Benefits: Free, flexible for customize webpage.

Note: Manual setting (e.g., one keyword for one website.)

I. Via Web Content Filter

1. Make sure the Web Content Filter (powered by Commtouch) license is valid.

CSM >> Web Content Filter Profile

Web-Filter License [Activate](#)
[Status: **Commtouch**] [Start Date: **2012-12-31** Expire Date: **2013-01-08**]

Setup Query Server	<input type="text" value="auto-selected"/>	Find more
Setup Test Server	<input type="text" value="auto-selected"/>	Find more

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

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

Administration Message (Max 255 characters) Cache :

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%  
<br>that is categorized with %CLI% <br>has been blocked by %RNAME% Web Content  
Filter.<p>Please contact your system administrator for further  
information.</center></body>
```

How to register/activate Web Content Filter (WCF) license? Please visit for getting more information:

***How to Register AI/AV/AS/WCF Service (Service Activation Wizard)**
(<http://www.draytek.com/user/SupportFAQDetail.php?ID=1955>)

***How to Activate Anti-Virus/Anti-Intrusion/Anti-Spam Service**
(<http://www.draytek.com/user/SupportFAQDetail.php?ID=286>)

How to use the Web Content Filter (WCF)
(<http://www.draytek.com/user/SupportFAQDetail.php?ID=1953>)

*** What the Web Content Filter (WCF) license benefits are,**
(<http://www.draytek.com/user/PdInfoDetail.php?Id=110>)

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

Child Abuse Images

Leisure

Select All
Clear All

Entertainment Games Sports
Travel Leisure & Recreation Fashion & Beauty

Business

Select All
Clear All

Business Job Search Web-based Mail

Chatting

Select All
Clear All

Chat Instant Messaging

Computer-Internet

Select All
Clear All

Anonymizers Forums & Newsgroups Computers
Download Sites Streaming, Downloads Phishing & Fraud
Search Engine, Portals **Social Networking** Spam Sites
Malware Botnets Hacking
Illegal Software Information Security Peer-to-Peer

Other

Select All

Adv & Pop-Ups Arts Transportation
Compromised Dating & Personals Education

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

Firewall >> General Setup

General Setup

General Setup Default Rule

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
Sessions Control	19 / 32000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>

Advance Setting

None
[Create New]
1-Default

OK Cancel

- 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.

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text" value="Facebook"/>
Contents	<input type="text" value="facebook"/>

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

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

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

- 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: Group/Object Selections:

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.

General Setup

General Setup Default Rule

Actions for default rule:	Action/Profile	Syslog
Application		
Filter	<input type="text" value="Pass"/>	<input type="checkbox"/>
Sessions Control	21 / <input type="text" value="32000"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter	<input type="text" value="1-Facebook"/>	<input type="checkbox"/>
Web Content Filter	<input type="text" value="None"/>	<input type="checkbox"/>
Advance Setting	<input type="button" value="Edit"/>	

B. Disallow users to play games on Facebook

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

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name	facebook-apps
Contents	apps.facebook

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

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

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

OK Clear Cancel

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:	face.apps		
Priority:	Either : URL Access Control First	Log:	None
1.URL Access Control			
<input checked="" type="checkbox"/> Enable URL Access Control		<input type="checkbox"/> Prevent web access from IP address	
Action:		Group/Object Selections	
Block		facebook..	
2.Web Feature			
<input type="checkbox"/> Enable Restrict Web Feature			
Action:			
Pass		<input type="checkbox"/> Cookie	<input type="checkbox"/> Proxy
		<input type="checkbox"/> 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

General Setup	Default Rule	
Actions for default rule:		
Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
Sessions Control	21 / 32000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	2-face.apps	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Advance Setting	<input type="button" value="Edit"/>	

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.

DrayTek Vigor2120 Series

Dashboard

System Information

Model Name	Vigor2120n+	System Up Time	0:37:47
Router Name		Current Time	2000 Jan 1 Sat 0:37:43
Firmware Version	3.7.5.1	Build Date/Time	Jul 31 2014 21:33:32
LAN MAC Address	00-1D-AA-9C-F7-3C		

IPv4 Internet Access

Line / Mode	IP Address	MAC Address	Up Time
WAN1 Ethernet / ---	Disconnected	00-1D-AA-9C-F7-3D	00:00:00
WAN2 USB / ---	Disconnected	00-1D-AA-9C-F7-3E	00:00:00

Interface

WAN	Connected :0	WAN1	WAN2
LAN	Connected :0	LAN1	LAN2
WLAN	Connected :0	LAN3	LAN4
WLAN5G	Connected :0		

Security

VPN	Connected : 0	Remote Dial-in User / LAN to LAN
MyVigor	Activate : 0	

System Resource

Current CPU Usage:	50%
--------------------	-----

Quick Access

- System Status
- Dynamic DNS
- TR-069
- IMP2P Block
- Schedule
- SysLog / Mail Alert
- RADIUS
- Firewall Object Setting
- Data Flow Monitor

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, Vigor2120 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2120, it can support HSDPA/ UMTS/EDGE/ GPRS/ GSM and the future 3G standard (HSUPA, etc). Vigor2120 n 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 Vigor2120 n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2120 n series.



After connecting into the router, 3G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN3 also can be used as backup device. Therefore,

when WAN1 and WAN2 are not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.

WAN
 General Setup
 Internet Access
 Multi-VLAN

4.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 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 and WAN2 settings. WAN1 is fixed with physical mode of Ethernet.

WAN >> General Setup

General Setup	
WAN1	WAN2
Enable: <input type="button" value="Yes"/>	Enable: <input type="button" value="No"/>
Display Name: <input type="text"/>	Display Name: <input type="text"/>
Physical Mode: Ethernet	Physical Mode: USB
Physical Type: <input type="button" value="Auto negotiation"/>	Active Mode: Backup
VLAN Tag insertion: <input type="button" value="Disable"/>	
Tag value: <input type="text" value="0"/> (0~4095)	
Priority: <input type="text" value="0"/> (0~7)	
<input type="button" value="OK"/>	

Available settings are explained as follows:

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

	
VLAN Tag insertion	<p>Enable – 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>Disable – Disable the function of VLAN with tag.</p> <p>Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
Active Mode	Display that WAN2 will be activated as Backup interface.

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) 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 or Dynamic IP	Details Page	IPv6
WAN2		USB	None PPPoE Static or Dynamic IP PPTP/L2TP	Details Page	IPv6

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN2		USB	None None 3G/4G USB Modem(PPP mode) 4G USB Modem(DHCP mode)	Details Page	IPv6

Available settings are explained as follows:

Item	Description
Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1/WAN2 (Ethernet) /WAN3 (USB) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. Then, click Details Page for accessing the settings page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface. Note that Details Page will be changed slightly based on physical mode specified on WAN>>General Setup .
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface. If IPv6 service is active on this WAN interface, the color of “IPv6” will become green.

4.1.3.1 Details Page for PPPoE in WAN1

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

Internet Access >> PPPoE

PPPoE Client Mode

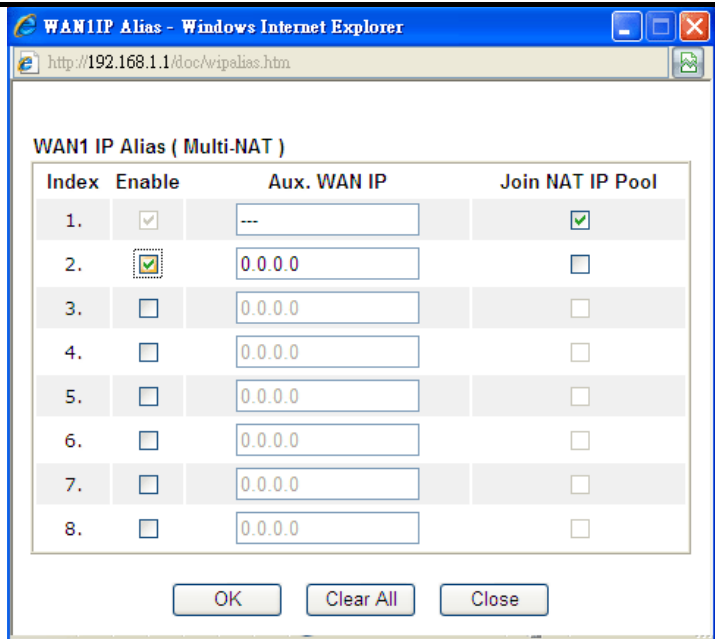
<p>PPPoE Setup PPPoE Link <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>ISP Access Setup ISP Name <input type="text"/> Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <p>WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/> TTL: <input type="text"/></p> <p>MTU <input type="text" value="1492"/> (Max:1492)</p> <p>PPPoE Pass-through <input type="checkbox"/> For Wired LAN <input type="checkbox"/> For Wireless LAN</p>	<p>PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/> Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/></p> <hr/> <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="9C"/> <input type="text" value="F7"/> <input type="text" value="35"/>
---	--

OK

Available settings are explained as follows:

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

	<p>to execute for WAN detection.</p> <p>Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</p>
MTU	<p>It means Max Transmit Unit for packet. The default setting is 1492.</p>
PPPoE Pass-through	<p>The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.</p> <p>For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p> <p>For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.</p>
PPP/MP Setup	<p>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method (IPCP)	<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>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click OK 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.

4.1.3.2 Details Page for Static or Dynamic IP in WAN1

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.

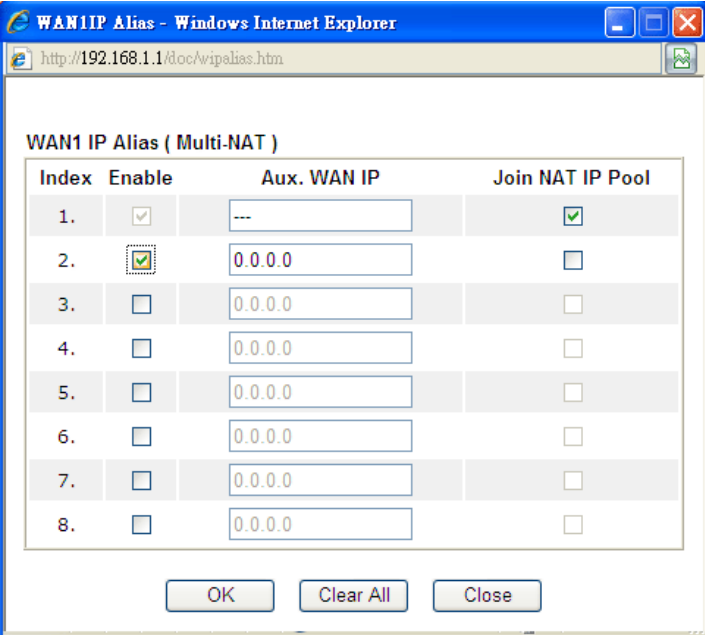
To use **Static or Dynamic IP** as the accessing protocol of the internet, please click the **Static or Dynamic IP** tab. The following web page will be shown.

Static or Dynamic IP

<p>Access Control Broadband Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text" value="0.0.0.0"/> PING Interval <input type="text" value="0"/> minute(s)</p> <p>WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/> TTL:</p> <p>MTU <input type="text" value="1492"/> (Max:1500)</p> <p>RIP Protocol <input type="checkbox"/> Enable RIP</p>	<p>WAN IP Network Settings <input type="text" value="WAN IP Alias"/></p> <p><input type="radio"/> Obtain an IP address automatically (DHCP Client) Router Name <input type="text" value="Vigor"/> * Domain Name <input type="text"/> * * : Required for some ISPs</p> <p>DHCP Client Identifier for some ISP <input type="checkbox"/> Enable Username <input type="text"/> Password <input type="text"/></p> <p><input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.130"/> Subnet Mask <input type="text" value="255.255.255.0"/> Gateway IP Address <input type="text" value="172.16.3.1"/></p> <p><input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> · <input type="text" value="1D"/> · <input type="text" value="AA"/> · <input type="text" value="9C"/> · <input type="text" value="F7"/> · <input type="text" value="35"/></p> <p>DNS Server IP Address Primary IP Address <input type="text" value="8.8.8.8"/> Secondary IP Address <input type="text" value="8.8.4.4"/></p>
--	---

Available settings are explained as follows:

Item	Description
Broadband Access	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU	It means Max Transmit Unit for packet.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.</p>  <p>Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use Dynamic IP mode.</p> <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. <p>DHCP Client Identifier for some ISP</p> <ul style="list-style-type: none"> ● Enable: Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. <p>Specify an IP address – Click this radio button to specify some data if you want to use Static IP mode.</p> <ul style="list-style-type: none"> ● IP Address: Type the IP address.

	<ul style="list-style-type: none"> ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. <p>Default MAC Address: Click this radio button to use default MAC address for the router.</p> <p>Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.</p>
DNS Server IP Address	Type in the primary IP address for the router if you want to use Static IP 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.

4.1.3.3 Details Page for PPTP/L2TP in WAN1

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

Internet Access >> PPTP/L2TP

PPTP/L2TP Client Mode

<p>PPTP/L2TP Setup</p> <p>PPTP/L2TP Link <input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable</p> <p>Server Address <input type="text"/></p> <p>Specify Gateway IP Address <input type="text" value="172.16.3.1"/></p> <p>ISP Access Setup</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <hr/> <p>MTU <input type="text" value="1460"/> (Max:1460)</p>	<p>PPP Setup</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/> <input type="button" value="v"/></p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address Assignment Method (IPCP)</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p> <p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text" value="172.16.3.130"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p>
--	---

Available settings are explained as follows:

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

	Specify Gateway IP Address – Specify the gateway IP address for DHCP server.
ISP Access Setup	<p>Username -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>Password -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.</p> <p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>
MTU	It means Max Transmit Unit for packet.
PPP Setup	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method(IPCP)	<p>Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same 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 Yes to use this function and type in a fixed IP address in the box.</p> <p>Fixed IP Address -Type a fixed IP address.</p>
WAN IP Network Settings	<p>Obtain an IP address automatically – Click this button to obtain the IP address automatically.</p> <p>Specify an IP address – Click this radio button to specify some data.</p> <ul style="list-style-type: none"> ● IP Address – Type the IP address. ● Subnet Mask – Type the subnet mask.

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

4.1.3.4 Details Page for 3G/4G USB Modem (PPP mode) in WAN2

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 WAN2. The following web page will be shown.

WAN >> Internet Access



[Modem Support List](#)

WAN 2

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

SIM PIN code

Modem Initial String
(Default: AT&FE0V1X1&D2&C1S0=0)

APN Name

Modem Initial String2

Modem Dial String
(Default: ATDT*99#, CDMA: ATDT#777, TD-SCDMA: ATDT*98*1#)

Service Name (Optional)

PPP Username (Optional)

PPP Password (Optional)

PPP Authentication

Index(1-15) in **Schedule** Setup:
=> , , ,

WAN Connection Detection

Mode

Ping IP

TTL:

Available settings are explained as follows:

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

APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply . The maximum length of the name you can set is 43 characters.
Modem Initial String2	The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings. The maximum length of the string you can set is 47 characters.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. The maximum length of the string you can set is 31 characters.
Service Name	Enter the description of the specific network service.
PPP Username	Type the PPP username (optional). The maximum length of the name you can set is 63 characters.
PPP Password	Type the PPP password (optional). The maximum length of the password you can set is 62 characters.
PPP Authentication	Select PAP only or PAP or CHAP for PPP.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for ping. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

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

4.1.3.5 Details Page for 4G USB Modem (DHCP mode) in WAN2

To use **4G USB Modem (DHCP mode)** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **4G USB Modem (DHCP mode)** for WAN2. The following web page will be shown.

WAN >> Internet Access



WAN 2 | [Modem Support List](#)

4G USB Modem(DHCP mode) Enable Disable

SIM PIN code

Network Mode (Default: 4G/3G/2G)

APN Name

MTU (Default: 1380)

LTE software version ---

LTE hardware version ---

WAN Connection Detection

Mode

Ping IP

TTL:

Available settings are explained as follows:

Item	Description
4G USB Modem (DHCP mode)	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet. The maximum length of the PIN code you can set is 15 characters.
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply . The maximum length of the name you can set is 43 characters.
MTU	It means Max Transmit Unit for packet. The default setting is 1380.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for ping.

	TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
--	---

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

4.1.3.6 Details Page for IPv6 – Offline in WAN1/WAN2

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode	
Connection Type	Offline <input type="button" value="v"/>
<input type="button" value="OK"/>	

4.1.3.7 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/L2TP	IPv6
Internet Access Mode			
Connection Type		PPP <input type="button" value="v"/>	
Note : IPv4 WAN setting should be PPPoE client.			
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>	

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

Online Status

Physical Connection		System Uptime: 0:2:32	
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			>> Drop PPP
Enable	Mode	Up Time	
Yes	PPP	0:02:08	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
DNS IP			
2001:8000:168::1			
2001:8000:168::2			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	9	544	1126

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

4.1.3.8 Details Page for IPv6 – TSPC in WAN1/WAN2

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 i

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		TSPC ▼	
TSPC Configuration			
Username	<input type="text"/>		
Password	<input type="password"/>		
Confirm Password	<input type="password"/>		
Tunnel Broker	<input type="text"/>		
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>	

Available settings are explained as follows:

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

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

4.1.3.9 Details Page for IPv6 – AICCU in WAN1/WAN2

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
<p>Internet Access Mode</p> <p>Connection Type: <input type="text" value="AICCU"/></p> <p>AICCU Configuration</p> <p><input type="checkbox"/> Always On</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Confirm Password: <input type="text"/></p> <p>Tunnel Broker: <input type="text" value="tic.sixxs.net"/></p> <p>Subnet Prefix: <input type="text"/> / <input type="text"/></p> <p>Note : If "Always On" is not enabled,AICCU connection would only retry three times.</p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>			

Available settings are explained as follows:

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

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

4.1.3.10 Details Page for IPv6 – DHCPv6 Client in WAN1

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

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		DHCPv6 Client	
DHCPv6 Client Configuration			
Identity Association		<input checked="" type="radio"/> Prefix Delegation <input type="radio"/> Non-temporary Address	
IAID (Identity Association ID)		1595978305	
OK		Cancel	

Available settings are explained as follows:

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

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

4.1.3.11 Details Page for IPv6 – Static IPv6 in WAN1

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

Internet Access >> IPv6

IPv6 Mode

Internet Access Mode
Connection Type:

Static IPv6 Address Configuration
IPv6 Address: / Prefix Length:

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
-------	----------------------------	-------

Available settings are explained as follows:

Item	Description
Static IPv6 Address configuration	IPv6 Address – Type the IPv6 Static IP Address. Prefix Length – Type the fixed value for prefix length. Add – Click it to add a new entry. Delete – Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.

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

4.1.3.12 Details Page for IPv6 – 6in4 Static Tunnel in WAN1

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/L2TP	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"/>	/ <input type="text"/> (default:64)
LAN Routed Prefix		<input type="text"/>	/ <input type="text"/> (default:64)
Tunnel TTL		<input type="text"/>	(default:255)
OK		Cancel	

Available settings are explained as follows:

Item	Description
Remote Endpoint IPv4 Address	Type the static IPv4 address for the remote server.
6in4 IPv6 Address	Type the static IPv6 address for IPv4 tunnel with the value for prefix length.
LAN Routed Prefix	Type the static IPv6 address for LAN routing with the value for prefix length.
Tunnel TTL	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		
LAN Status			
IP Address			
2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
14	80	1244	6815
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6in4 Static Tunnel	0:04:07	
IP		Gateway IP	
2001:4DD0:FF10:83E4::2131/64 (Global)		---	
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
3	26	211	2302

4.1.3.13 Details Page for IPv6 – 6rd in WAN1

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

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type		6rd	
6rd Settings			
6rd Mode		<input type="radio"/> Auto 6rd <input checked="" type="radio"/> Static 6rd	
Static 6rd Settings			
IPv4 Border Relay:		192.168.101.111	
IPv4 Mask Length:		0	
6rd Prefix:		2001:E41::	
6rd Prefix Length:		32	
OK		Cancel	

Available settings are explained as follows:

Item	Description
6rd Mode	<p>Auto 6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP".</p> <p>Static 6rd - Set 6rd options manually.</p>
IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.
IPv4 Mask Length	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.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	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 0:9:15	
IPv4		IPv6	
LAN Status			
IP Address			
2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
15	113	1354	18040
WAN1 IPv6 Status			
Enable	Mode	Up Time	
Yes	6rd	0:09:06	
IP			Gateway IP
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global)			---
FE80::C0A8:651D/128 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
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.

WAN >> Multi-VLAN

Multi-VLAN

General

Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
3. WAN3	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
4. WAN4	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
5. WAN5	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
6.	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
7.	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
8.	No	Ethernet(WAN1)	None	<input type="checkbox"/> Enable <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

OK

Cancel

Available settings are explained as follows:

Item	Description
Channel	Display the number of each channel. Channels 1 and 2 are used by the Internet Access web user interface and can not be configured here. Channels 3 ~ 8 are configurable.
Enable	Display whether the settings in this channel are enabled (Yes) or not (No).
WAN Type	Displays the physical medium that the channel will use.
VLAN Tag	Displays the VLAN tag value that will be used for the packets traveling on this channel.
Port-based Bridge	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. Enable - Check this box to enable the port-based bridge function on this channel. P1 ~ P4 – Check the box(es) to build bridge connection on LAN.

Click any index (6~ 8) to get the following web page:

Multi-VLAN Channel 6: **Enable** **Disable**

WAN Type : Ethernet(WAN1) ▾

General Settings

VLAN Header

VLAN Tag:

Priority: 0 ▾

Note: Tag value must be set between 1~4095 and unique for each channel.
Only one channel can be untagged (equal to 0) at a time.

Bridge mode

Enable

Physical Members

P1 P2 P3 P4

Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.

OK
Cancel

Available settings are explained as follows:

Item	Description
Multi-VLAN Channel (6~8)	<p>Enable – Click it to enable the configuration of this channel.</p> <p>Disable – Click it to disable the configuration of this channel.</p>
WAN Type	<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>
General Settings	<p>VLAN Tag – 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>Priority – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
Bridge mode	<p>Enable – Click it to enable Bridge mode for such channel.</p> <p>Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.</p>

Moreover, WAN link for Channel 3~5 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 3~5 to configure your router.

Multi-VLAN Channel 5: Enable Disable

WAN Type :

General Settings

VLAN Header

VLAN Tag:

Priority:

Note: Tag value must be set between 1~4095 and unique for each channel.
Only one channel can be untagged (equal to 0) at a time.

Open Port-based Bridge Connection for this Channel

Physical Members

P1 P2 P3 P4

Note: P1 is reserved for NAT use, and cannot be configured for bridge mode.

Open WAN Interface for this Channel

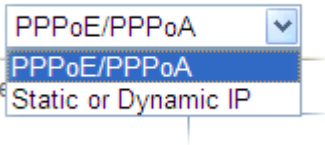
WAN Application:

WAN Setup:

<p>ISP Access Setup</p> <p>ISP Name <input type="text"/></p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p><input checked="" type="checkbox"/> Always On</p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address From ISP</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p>	<p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name <input type="text" value="Vigor"/>*</p> <p>Domain Name <input type="text"/>*</p> <p><small>*: Required for some ISPs</small></p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Gateway IP Address <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text" value="8.8.8.8"/></p> <p>Secondary IP Address <input type="text" value="8.8.4.4"/></p>
---	---

Available settings are explained as follows:

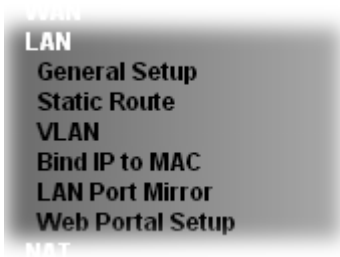
Item	Description
Multi-VLAN Channel (3~5)	Enable – Click it to enable the configuration of this channel. Disable – Click it to disable the configuration of this channel.
WAN Type	The connections and interfaces created in every channel may select a specific WAN type to be built upon. In the Multi-VLAN application, only the Ethernet WAN type is available. The user will be able to select the physical WAN interface the channel shall use here.
General Settings	VLAN Tag – Type the value as the VLAN ID number. Valid settings are in the range from 1 to 4095. The network

	<p>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>Priority – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.</p>
<p>Open Port-based Bridge Connection for this Channel</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>Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.</p>
<p>Open WAN Interface for this Channel</p>	<p>Check the box to enable relating function.</p> <p>WAN for Router-borne Application - Management 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>IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.</p> <p>WAN Setup – Choose PPPoE/PPPoA or Static or Dynamic IP to determine what WAN settings must be configured.</p> 
<p>ISP Access Setup, IP Address From ISP, WAN IP Network Settings, DNS Server IP Address</p>	<p>For other settings, refer to Details Page for PPPoE / Static or Dynamic IP in WAN1.</p>

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

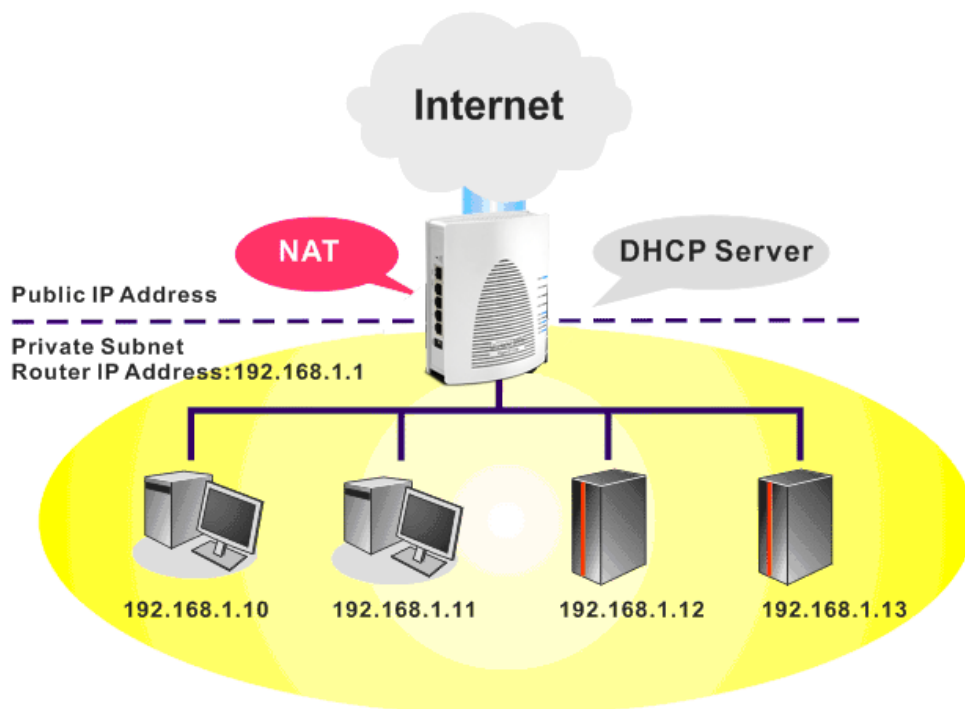
4.2 LAN

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.

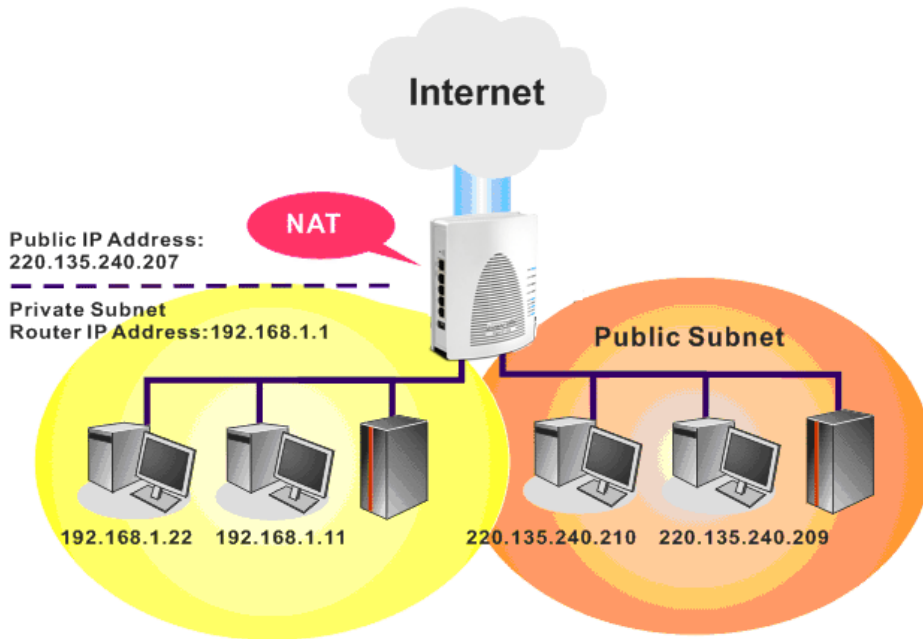


4.2.1 Basics of LAN

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 8 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 two subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN2). 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 can be operated under **NAT** or **Route** mode. IP Routed Subnet can be operated under Route mode.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

[Advanced](#) You can configure DHCP options here.

Inter-LAN Routing

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

Note: LAN 2 is available when VLAN is enabled.

[OK](#)

Each item is explained as follows:

Item	Description
General Setup	<p>Allow to configure settings for each subnet respectively.</p> <p>Index - Display all of the LAN items.</p> <p>Status- Basically, LAN1 status is enabled in default. LAN2, LAN3, LAN3 and IP Routed Subnet can be observed by checking the box of Status.</p> <p>DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.</p> <p>IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it.</p> <p>Details Page - Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet.</p> <p>IPv6 – Click it to access into the settings page of IPv6.</p>

Advanced

When the router receives the DHCP request from LAN client, the router will assign an IP with the DHCP packets adding option number and data information.

LAN >> General Setup

DHCP Server Options Status

Enable	Interface	Option	Type	Data
--------	-----------	--------	------	------

Enable:

Interface: All LAN1 LAN2 IP Routed Subnet

Option Number:

DataType: ASCII Character (EX :Option:18, Data:/path)
 Hexadecimal Digit (EX: Option:18, Data:2f70617468)
 Address List (EX :Option:44, Data:172.16.2.10,172.16.2.20...)

Data:

Enable – Check the box to enable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,

Option number:100

Data: abcd

When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.

Interface – Choose the interface for applying such option.

Option Number – Type a number for such function.

DataType – Choose the type (ASCII or Hex or Address) for the data to be stored.

Data – Type the content of the data to be processed by the function of DHCP option.

Inter-LAN Routing

Check the box to link two or more different subnets (LAN and LAN).

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

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

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
<p>Network Configuration For NAT Usage</p> <p>IP Address <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <hr/> <p>RIP Protocol Control <input type="button" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p><input type="checkbox"/> Enable Relay Agent</p> <p>Start IP Address <input type="text" value="192.168.1.10"/></p> <p>IP Pool Counts <input type="text" value="200"/></p> <p>Gateway IP Address <input type="text" value="192.168.1.1"/></p> <p>Lease Time <input type="text" value="86400"/> (s)</p> <p><input checked="" type="checkbox"/> Retrieve IPs from inactive clients periodically</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>
<input type="button" value="OK"/>	

Available settings are explained as follows:

Item	Description
LAN IP Network Configuration	<p>For NAT Usage,</p> <ul style="list-style-type: none"> ● IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1). ● Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) <p>RIP Protocol Control,</p> <ul style="list-style-type: none"> ● Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) ● Enable activates the RIP protocol.
DHCP Server Configuration	<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>Enable Server - Let the router assign IP address to every host in the LAN.</p> <p>Disable Server – Let you manually assign IP address to</p>

	<p>every host in the LAN.</p> <p>Enable Relay Agent – Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <p>DHCP Server IP Address – It is available when Enable Relay Agent 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>Start IP Address - 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>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.</p> <p>Gateway IP Address - 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>Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.</p> <p>Retrieve IPs from inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).</p>
<p>DNS Server IP Address</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>Primary IP Address - 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>Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.</p> <p>The default DNS Server IP address can be found via Online Status:</p>

Physical Connection				System Uptime: 22:22:45
IPv4		IPv6		
LAN Status		Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	
IP Address		TX Packets	RX Packets	
192.168.1.1		0	41533	

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

4.2.2.2 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

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

Router Advertisement Server

Enable Disable

Advertisement Lifetime Seconds (Range : 600 - 9000)

DHCPv6 Server

Enable Server Disable Server

Start IPv6 Address

End IPv6 Address

DNS Server IPv6 Address

Primary DNS Server

Secondary DNS Server

Static IPv6 Address

IPv6 Address / Prefix Length

Current IPv6 Address Table

Index	IPv6 Address/Prefix Length	Scope
1	FE80::21D:AAFF:FE9C:F734/64	Link

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
Router Advertisement Server	<p>Enable – Click it to enable router advertisement server. The router advertisement daemon 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>Disable – Click it to disable router advertisement server.</p> <p>Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.</p>
DHCPv6 Server Configuration	<p>Enable Server –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.</p> <p>Disable Server –Click it to disable DHCPv6 server.</p> <p>Start IPv6 Address / End IPv6 Address –Type the start and end address for IPv6 server.</p>
DNS Server IPv6 Address	<p>Primary DNS Sever – Type the IPv6 address for Primary DNS server.</p> <p>Secondary DNS Server –Type another IPv6 address for DNS server if required.</p>
Static IPv6 Address configuration	<p>IPv6 Address –Type static IPv6 address for LAN.</p> <p>Prefix Length – Type the fixed value for prefix length.</p> <p>Add – Click it to add a new entry.</p> <p>Delete – Click it to remove an existed entry.</p>
Current IPv6 Address Table	Display current used IPv6 addresses.

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.

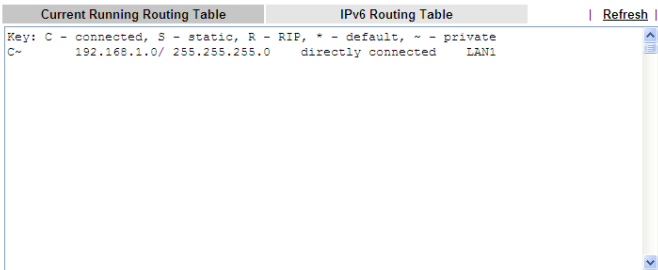
Static Route for IPv4

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.	???	?		

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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
View Routing Table	<p>Displays the routing table for your reference.</p> <p>Diagnostics >> View Routing Table</p> 
Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.

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
- LAN2
- WAN1
- WAN2

Available settings are explained as follows:

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

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

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

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

Each item is explained as follows:

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

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

LAN >> Static Route Setup

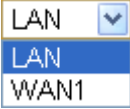
Index No. 1

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

OK Cancel Delete

Available settings are explained as follows:

Item	Description
Enable	Check it to enable this profile.

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

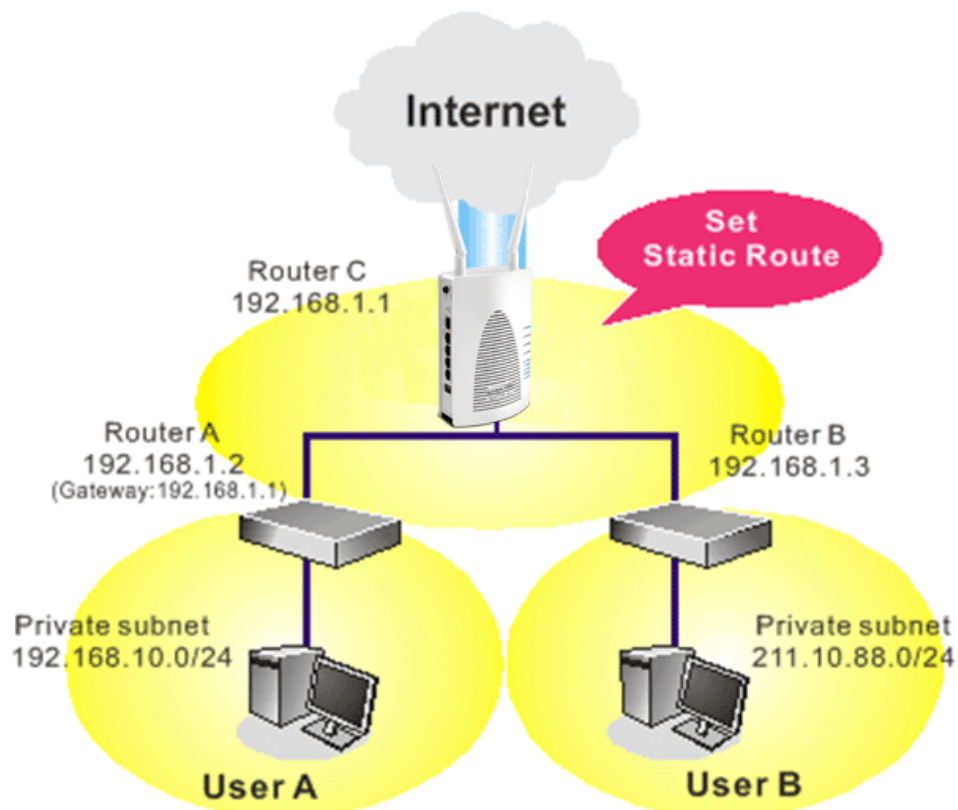
After finishing all the settings here, please click **OK** to save the configuration.

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

<input checked="" type="checkbox"/> Enable	
Destination IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN1

OK Cancel Delete

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

<input checked="" type="checkbox"/> Enable	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN1

OK Cancel Delete

- 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 - RIP, * - default, ~ - private				
S~	192.168.10.0/ 255.255.255.0	via 192.168.1.2	LAN1	
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1	
S~	211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1	

4.2.4 VLAN

With the 4-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 (Vigor2120n-plus), 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 ~ P4) 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.

VLAN Configuration

<input checked="" type="checkbox"/> Enable																
	LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<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"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
3. Each VID must be unique.

OK Clear Cancel

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

Available settings are explained as follows:

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 – P4 – Check the LAN port(s) to be grouped under the selected VLAN.
Wireless LAN (2.4GHz)	SSID1 – SSID4 – Check the SSID boxes to group them under the selected VLAN.
Wireless LAN (5GHz)	SSID1 – SSID4 – Check the SSID boxes to group them under the selected VLAN.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> LAN 1 LAN 1 LAN 2 </div>

VLAN Tag	<p>Enable – Check the box to enable the function of VLAN with tag.</p> <p>The router will add specific VLAN number to all packets on the LAN while sending them out.</p> <p>Please type the tag value and specify the priority for the packets sending by LAN.</p> <p>VID – Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
-----------------	--

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

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

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4. VLAN0 and VLAN1 are configured with different subnets.
2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below. Click **OK** to save the settings.

LAN >> VLAN Configuration

VLAN Configuration

<input checked="" type="checkbox"/> Enable															
LAN				Wireless LAN(2.4GHz)				Wireless LAN(5GHz)				VLAN Tag			
P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
<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"/>	LAN 1	<input type="checkbox"/>	0	0
<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"/>	LAN 1	<input type="checkbox"/>	0	0
<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"/>	LAN 1	<input type="checkbox"/>	0	0
<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"/>	LAN 1	<input type="checkbox"/>	0	0
<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"/>	LAN 1	<input type="checkbox"/>	0	0

1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.
2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected.
3. Each VID must be unique.

OK Clear Cancel

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

4.2.5 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

Bind IP to MAC

Enable
 Disable
 Strict Bind

ARP Table		IP Bind List (Limit: 300 entries)	
IP Address	Mac Address	Index	Mac Address
192.168.1.10	E0-CB-4E-DA-48-79		

Show Comment

Note: IP-MAC binding presets DHCP Allocations.
If you select Strict Bind, unspecified LAN clients cannot access the Internet.

OK

Backup IP Bind List : Upload From File: No file chosen

Available settings are explained as follows:

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Select All	Click this link to select all the items in the ARP table.
Sort	Reorder the table based on the IP address.

Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
Add or Update	<p>IP Address – Type the IP address that will be used for the specified MAC address.</p> <p>Mac Address – Type the MAC address that is used to bind with the assigned IP address.</p> <p>Comment – Type a brief description for the entry.</p> <p>Show Comment – Check this box to display the comment on IP Bind List box.</p>
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List .
Update	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in IP Bind List . Simply click and select the one, and click Delete . The selected item will be removed from the IP Bind List .
Backup	Store the configuration for Bind IP to MAC as a file.
Restore	Restore the previously stored configuration file and apply to such page.

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:
 P2 P3 P4

Mirrored port:
 P1 P2 P3 P4

Note: The selected mirror port will only serve debug purposes and should not be used as a part of the LAN.

Available settings are explained as follows:

Item	Description
Port Mirror	Check Enable to activate this function. Or, check Disable 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	
<u>1.</u>	Disable	None	<input type="button" value="Preview"/>
<u>2.</u>	Disable	None	<input type="button" value="Preview"/>
<u>3.</u>	Disable	None	<input type="button" value="Preview"/>
<u>4.</u>	Disable	None	<input type="button" value="Preview"/>

Note: Internet access must be enabled while webpage redirection is about to enable.

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 interfaces of the profile.
Preview	Open a preview window according to the configured settings.

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

LAN >> Web Portal Setup

Profile Index: 1

Disable
 URL Redirect
 Message

e.g. http://www.draytek.com

(Max 511 characters)

Applied Interfaces

LAN1 LAN2
 SSID1 SSID2 SSID3 SSID4
 SSID1 SSID2 SSID3 SSID4

OK

Cancel

Available settings are explained as follows:

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

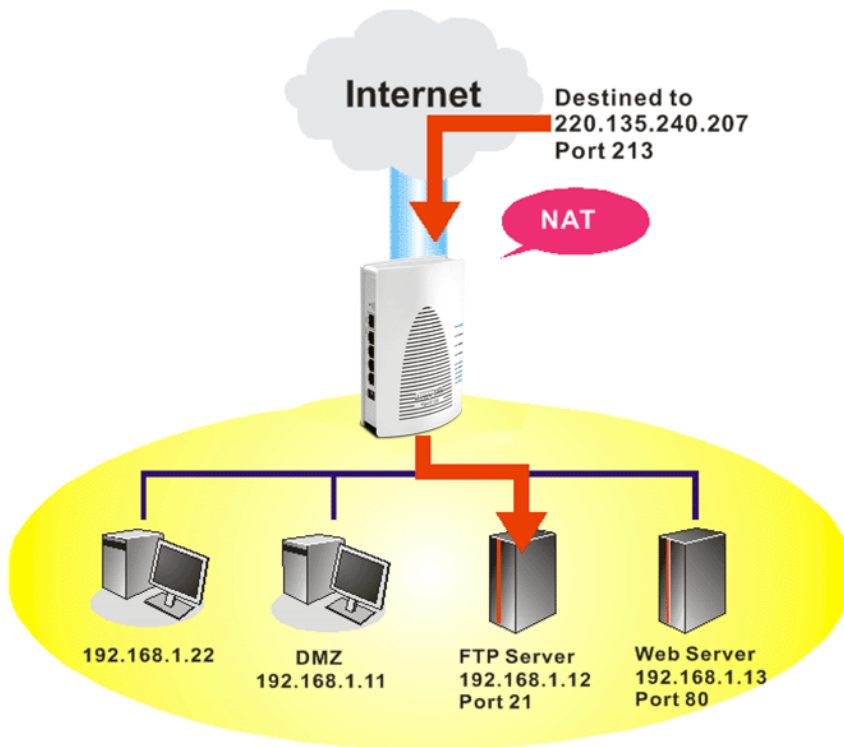
Note: On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

Below shows the menu items for NAT.

LAN
 NAT
 Port Redirection
 DMZ Host
 Open Ports
 Address Mapping
 Port Triggering
 Firewall

4.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Port Redirection

[Set to Factory Default](#)

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

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

[Next](#) >>

Note: The configured ports in the **Management** and **SSL VPN** webUIs will be used by the router and not be sent to the local computer defined here.

Each item is explained as follows:

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

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

NAT >> Port Redirection

Index No. 1

Enable

Mode Range

Service Name Single

Protocol Range

WAN IP ---

Public Port 1.All

Private IP 0 -

Private Port -

Private Port 0

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:

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

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

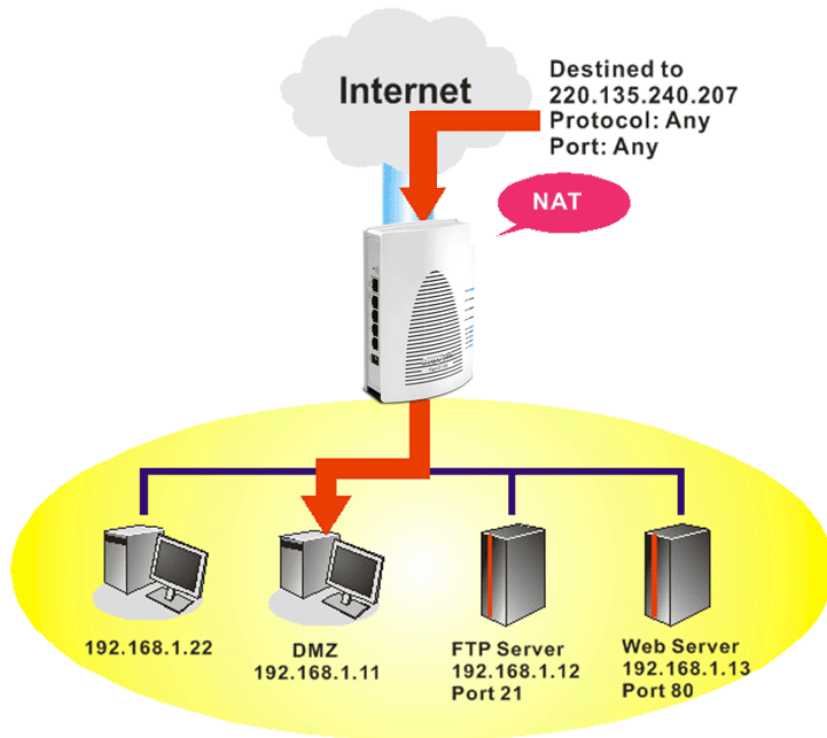
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

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

IPv4 Management Setup	IPv6 Management Setup												
<p>Router Name <input type="text"/></p> <p><input type="checkbox"/> Default: Disable Auto-Logout</p> <hr/> <p>Internet Access Control</p> <p><input type="checkbox"/> Allow management from the Internet</p> <ul style="list-style-type: none"> <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"/> TR069 Server <input type="checkbox"/> SSH Server <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List from the Internet</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>Management Port Setup</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>FTP Port <input type="text" value="21"/> (Default: 21)</p> <p>TR069 Port <input type="text" value="8069"/> (Default: 8069)</p> <p>SSH Port <input type="text" value="22"/> (Default: 22)</p> <hr/> <p>External Device Control</p> <p><input checked="" type="checkbox"/> No respond to External Device</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"/> ▾											

4.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1

WAN 1

None

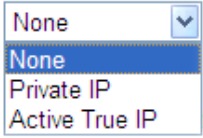
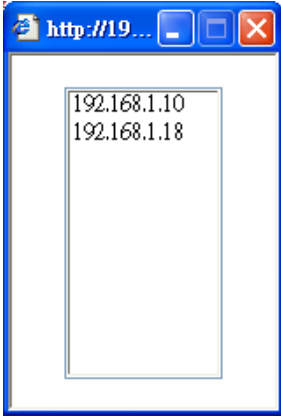
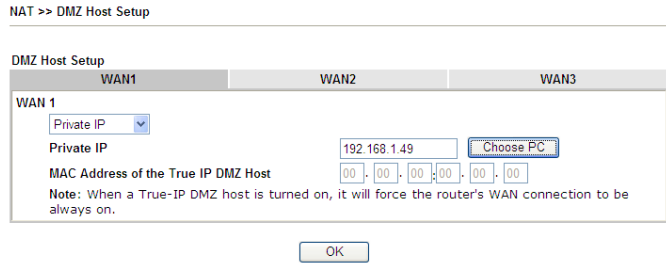
Private IP Choose IP

MAC Address of the True IP DMZ Host

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

OK

Available settings are explained as follows:

Item	Description
<p>WAN 1</p> 	<p>Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.</p>
<p>Private IP</p>	<p>Enter the private IP address of the DMZ host, or click Choose PC to select one.</p>
<p>Choose PC</p>	<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 OK to save the setting.</p> 


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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1				
WAN 1				
Index	Enable	Aux. WAN IP	Private IP	
1.	<input type="checkbox"/>	172.16.3.130	<input type="text" value="0.0.0.0"/>	<input type="button" value="Choose IP"/>
2.	<input type="checkbox"/>	172.16.3.149	<input type="text" value="0.0.0.0"/>	<input type="button" value="Choose IP"/>

Available settings are explained as follows:

Item	Description																									
Enable	Check to enable the DMZ Host function.																									
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.																									
Choose PC	<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 OK to save the setting.</p>																									
	<p>NAT >> DMZ Host Setup</p> <p>DMZ Host Setup</p> <table border="1"> <thead> <tr> <th colspan="5">WAN1</th> </tr> <tr> <th colspan="5">WAN 1</th> </tr> <tr> <th>Index</th> <th>Enable</th> <th>Aux. WAN IP</th> <th>Private IP</th> <th></th> </tr> </thead> <tbody> <tr> <td>1.</td> <td><input type="checkbox"/></td> <td>172.16.3.130</td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="button" value="Choose IP"/></td> </tr> <tr> <td>2.</td> <td><input checked="" type="checkbox"/></td> <td>172.16.3.149</td> <td><input type="text" value="192.168.1.10"/></td> <td><input type="button" value="Choose IP"/></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Clear"/> </p>	WAN1					WAN 1					Index	Enable	Aux. WAN IP	Private IP		1.	<input type="checkbox"/>	172.16.3.130	<input type="text" value="0.0.0.0"/>	<input type="button" value="Choose IP"/>	2.	<input checked="" type="checkbox"/>	172.16.3.149	<input type="text" value="192.168.1.10"/>	<input type="button" value="Choose IP"/>
WAN1																										
WAN 1																										
Index	Enable	Aux. WAN IP	Private IP																							
1.	<input type="checkbox"/>	172.16.3.130	<input type="text" value="0.0.0.0"/>	<input type="button" value="Choose IP"/>																						
2.	<input checked="" type="checkbox"/>	172.16.3.149	<input type="text" value="192.168.1.10"/>	<input type="button" value="Choose IP"/>																						

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

4.3.3 Open Ports

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

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

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

NAT >> Open Ports

Open Ports Setup					Set to Factory Default
Index	Comment	WAN Interface	Aux. WAN IP	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](#) >>

Note:The configured ports in the **Management** and **SSL VPN** webUIs will be used by the router and not be sent to the local computer defined here.

Available settings are explained as follows:

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

<input checked="" type="checkbox"/> Enable Open Ports							
Comment	P2261						
WAN Interface	WAN1						
WAN IP	172.16.3.130						
Private IP	192.168.1.10					Choose IP	
1.	Protocol	Start Port	End Port	2.	Protocol	Start Port	End Port
	TCP	80	80		----	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

OK Clear Cancel

Available settings are explained as follows:

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

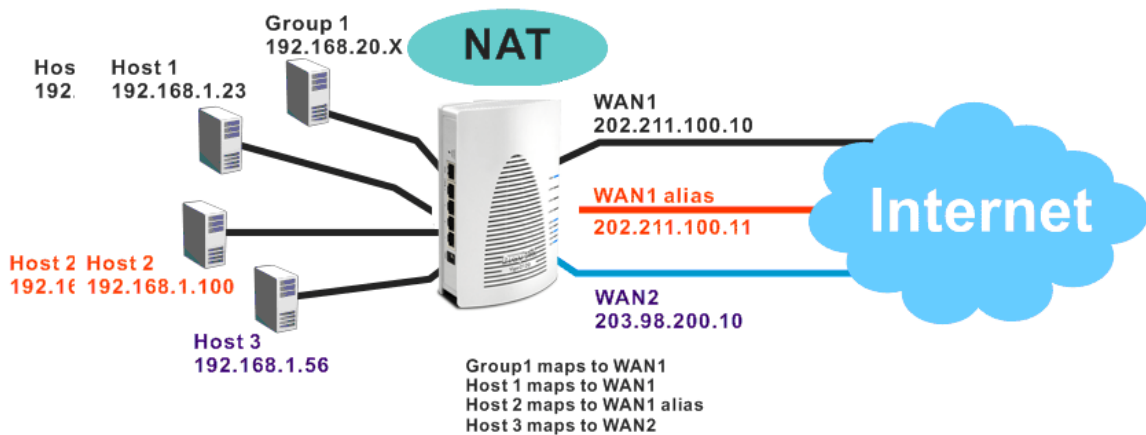
After finishing all the settings here, please click **OK** to save the configuration.

NAT >> Open Ports

Open Ports Setup					Set to Factory Default
Index	Comment	WAN Interface	Aux. WAN IP	Local IP Address	Status
1.	P2261	WAN1	172.16.3.130	192.168.1.10	√
2.					×
3.					×
4.					×
5.					×
6.					×
7.					√

4.3.4 Address Mapping

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



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

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11
 WAN2: 203.98.200.10

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

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

NAT >> Address Mapping

Address Mapping Setup					Set to Factory Default
Index	Protocol	Public IP	Private IP	Mask	Status
1.	ALL	---		/32	x
2.	ALL	---		/32	x
3.	ALL	---		/32	x
4.	ALL	---		/32	x
5.	ALL	---		/32	x

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to configure. You should click the appropriate index number to edit or clear the corresponding entry.
Protocol	Display the protocol used for this address mapping.
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10.
Mask	Display the subnet mask selected for this address mapping.
Status	Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1

Enable

Protocol: ALL ▾

WAN Interface: WAN1 ▾

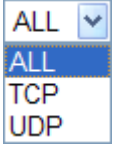
WAN IP: 1-172.16.3.130 ▾

Private IP:

Subnet Mask: /32 ▾

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.

Protocol	Specify the transport layer protocol. It could be TCP , UDP , or ALL for selection. 
WAN Interface	Choose the WAN interface for such address mapping profile.
WAN IP	This is the source IP of a packet captured on the WAN side and sent by a NAT host specified in the Private IP field. The drop down menu contains WAN interface IPs and WAN IP alias IPs.
Private IP	This is the source IP of a NAT host which wishes to send packets to the WAN side and have source address as configured in the WAN IP field.
Subnet Mask	Select a value of subnet mask for private IP address.

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

4.3.5 Port Triggering

Port Triggering is a variation of open ports function.

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

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

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

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

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

Click the index number link to open the configuration page.

No. 1

Enable

Service User Defined ▾

Comment

Triggering Protocol TCP ▾

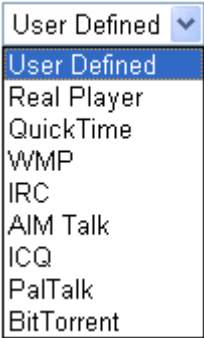


Triggering Port

Incoming Protocol UDP ▾

Incoming Port

Note: The Triggering Port and Incoming Port should be input like this :
123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile. 
Comment	Type the text to memorize the application of this rule.
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile. 
Triggering Port	Type the port or port range for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile. 
Incoming Port	Type the port or port range for the incoming packets.

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

4.4 Firewall

4.4.1 Basics for Firewall

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

Firewall Facilities

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

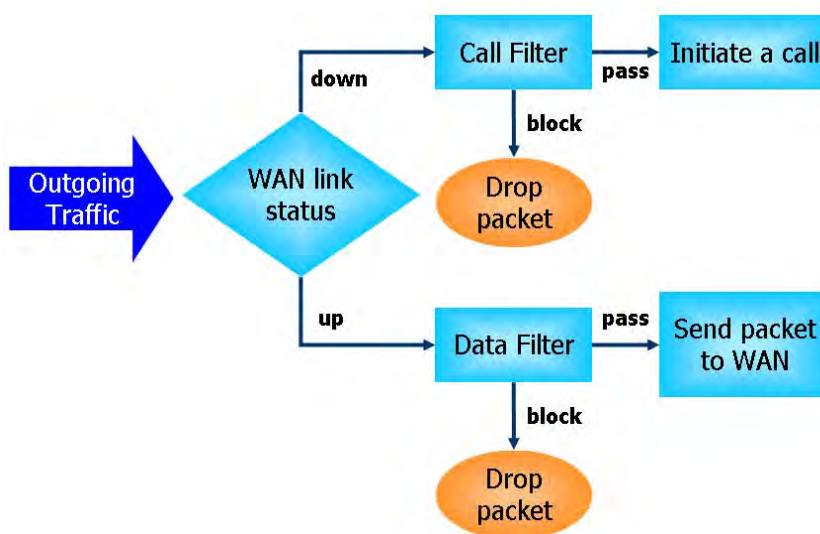
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

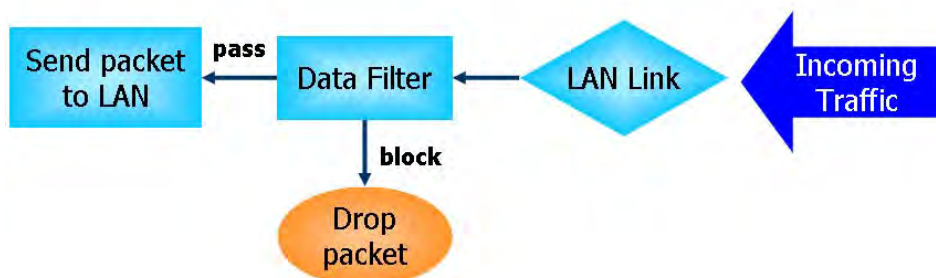
IP Filters

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

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

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





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.

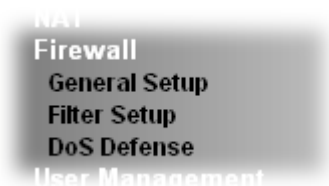
The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog 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. Unassigned numbers |
| 8. Trace route | |

Below shows the menu items for Firewall.



4.4.2 General Setup

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

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

4.4.2.1 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

General Setup

General Setup
Default Rule

Call Filter Enable Start Filter Set

Disable

Data Filter Enable Start Filter Set

Disable

Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)

Enable Strict Security Firewall

Block routing packet from WAN

IPv4 IPv6

Note: The packets will be filtered by the following firewall functions sequentially:

1. Data Filter Sets and Rules
2. Block routing packets from WAN
3. Default Rule

Available settings are explained as follows:

Item	Description
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.

Accept large incoming...	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable “ Accept large incoming fragmented UDP or ICMP Packets ”. By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable “ Accept large incoming fragmented UDP or ICMP Packets ”.
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission. Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router’s firewall will block the packets directly.
Block routing packet from WAN	Usually, IPv6 network sessions/traffic from WAN to LAN are allowed in default. IPv6 - Check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT. IPv4 - Check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.

4.4.2.2 Default Rule Page

Such page allows you to choose filtering profiles including QoS, Policy Route, WCF, APP Enforcement, and URL Content Filter for data transmission via Vigor router.

Firewall >> General Setup


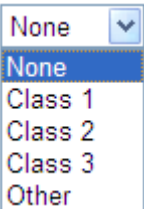
General Setup

General Setup
Default Rule

Actions for default rule:	Action/Profile	Syslog
Application		
Filter	Pass <input type="button" value="v"/>	<input type="checkbox"/>
Sessions Control	29 / <input type="text" value="32000"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>

Advance Setting

Available settings are explained as follows:

Item	Description
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter </p>
Sessions Control	<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>
Quality of Service	<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> 
APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] 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 APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Advance Setting	<p>Click Edit to open the following window. However, it is</p>

strongly recommended to use the default settings here.

Firewall >> General Setup

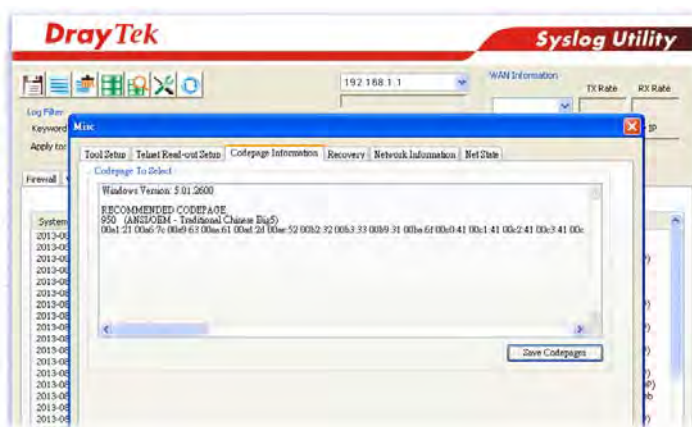
Advance Setting

Codepage	ANSI(1252)-Latin I	
Window size:	65535	
Session timeout:	1440	Minute

OK Close

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

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



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.

4.4.3 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
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

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
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios		Down
<input type="button" value="2"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="3"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="4"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="5"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="6"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="7"/>	<input type="checkbox"/>		UP	

Next Filter Set

Available settings are explained as follows:

Item	Description
Filter Rule	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.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Move Up/Down	Use Up or Down link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

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

Filter Set 3 Rule 1

Check to enable the Filter Rule

Comments:

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

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application	Action/Profile	Syslog
Filter:	<input type="text" value="Pass Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	0 / <input type="text" value="32000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
<u>Quality of Service</u>	<input type="text" value="None"/>	<input type="checkbox"/>
<u>APP Enforcement:</u>	<input type="text" value="None"/>	<input type="checkbox"/>
<u>URL Content Filter:</u>	<input type="text" value="None"/>	<input type="checkbox"/>
<u>Web Content Filter:</u>	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

Available settings are explained as follows:

Item	Description
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear the sessions when the above schedule profiles are applied.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <input type="text" value="LAN/RT/VPN -> WAN"/> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <input type="text" value="LAN/RT/VPN -> WAN"/> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <input type="text" value="WAN -> LAN/RT/VPN"/> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <input type="text" value="LAN/RT/VPN -> LAN/RT/VPN"/> </div> <p>Note: RT means routing domain for 2nd subnet or other</p>

LAN.

Source/Destination IP

Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.

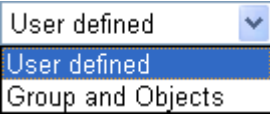
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.

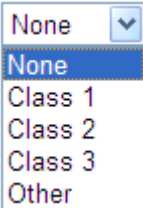
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

Click **Edit** to access into the following dialog to choose a suitable service type.

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In

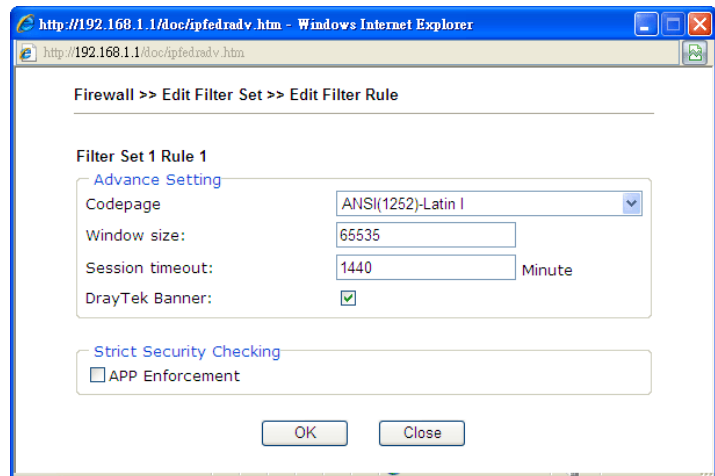
	<p>addition, if you want to use the service type from defined groups or objects, please choose Group and Objects as the Service Type.</p>  <p>Protocol - Specify the protocol(s) which this filter rule will apply to.</p> <p>Source/Destination Port –</p> <p>(=) – when the first and last value are the same, 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.</p> <p>(!=) – 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.</p> <p>(>) – the port number greater than this value is available.</p> <p>(<) – the port number less than this value is available for this profile.</p> <p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
Fragments	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p><i>Don't care</i> -No action will be taken towards fragmented packets.</p> <p><i>Unfragmented</i> -Apply the rule to unfragmented packets.</p> <p><i>Fragmented</i> - Apply the rule to fragmented packets.</p> <p><i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.</p>
Filter	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	<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>
Sessions Control	<p>The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The</p>

	default setting is 60000.
MAC Bind IP	<p>Strict – Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP be bound for applying such filter rule.</p> <p>No-Strict - no limitation.</p>
Quality of Service	<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> 
APP Enforcement	<p>Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] 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 APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
URL Content Filter	<p>Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the</p>

Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

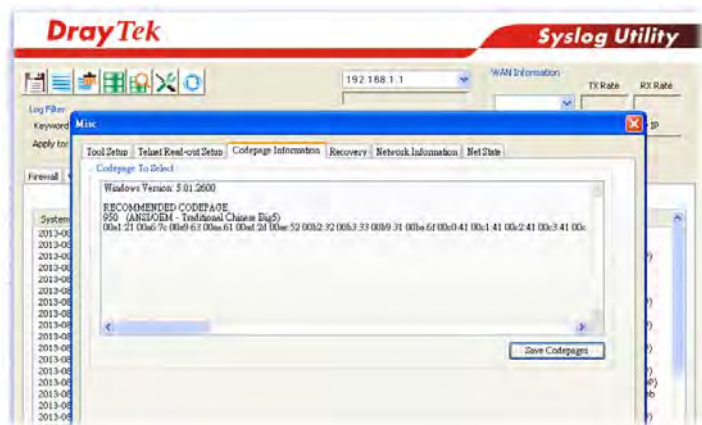
Advance Setting

Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

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



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.

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

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.

The image shows a sequence of screenshots from the DrayTek Firewall configuration interface, illustrating the setup of call and data filters. Red arrows indicate the flow from the General Setup screen to the Filter Setup screen, and then to the Edit Filter Rule screen.

Firewall >> General Setup

General Setup

General Setup | Default Rule

Call Filter: Enable, Disable. Start Filter Set: Set#1

Data Filter: Enable, Disable. Start Filter Set: Set#2

Accept large incoming fragmented UDP or ICMP packets (for some of the...)

Enable Strict Security Firewall

OK | Cancel

Firewall >> Filter Setup

Filter Set

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Set to Factory Default

OK | Cancel

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments: Default Call Filter

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

OK | Clear | Cancel

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments:

Index(1-15) in Schedule Setup: [] [] [] []

Clear sessions when schedule ON: Enable

Direction: LAN/RT/VPN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: Any [Edit]

Fragments: Don't Care

Application: Filter: Pass Immediately [Edit]

Branch to Other Filter Set: None

Sessions Control: 0 / 32000

MAC Bind IP: Non-Strict

Quality of Service: None

APP Enforcement: None

URL Content Filter: None

Web Content Filter: None

Advance Setting [Edit]

OK | Clear | Cancel

4.4.4 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

Enable DoS Defense Select All

<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

Block IP options
 Block Land
 Block Smurf
 Block trace route
 Block SYN fragment
 Block Fraggle Attack

Block TCP flag scan
 Block Tear Drop
 Block Ping of Death
 Block ICMP fragment
 Block Unassigned Numbers

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

OK
Clear All
Cancel

Available settings are explained as follows:

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	<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 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router

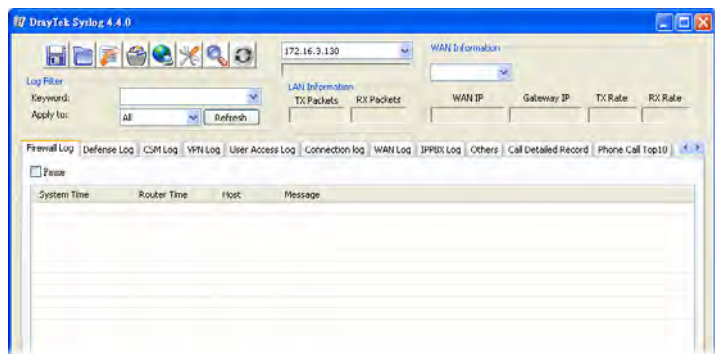
	<p>will start to randomly discard the subsequent UDP packets for a period defined in Timeout.</p> <p>The default setting for threshold and timeout are 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<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 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable PortScan detection	<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 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as “attack event”.</p>
Block IP options	<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>
Block Land	<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>
Block Smurf	<p>Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.</p>
Block trace router	<p>Check the box to enforce the Vigor router not to forward any trace route packets.</p>
Block SYN fragment	<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>
Block Fraggle Attack	<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>
Block TCP flag scan	<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>
Block Tear Drop	<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>
Block Ping of Death	<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>
Block ICMP Fragment	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>
Block Unassigned Numbers	<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>
Warning Messages	<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 DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected.</p>

SysLog / Mail Alert Setup

SysLog Access Setup	Mail Alert Setup
<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/>
Syslog Save to:	SMTP Server <input type="text"/>
<input checked="" type="checkbox"/> Syslog Server	SMTP Port <input type="text" value="25"/>
<input type="checkbox"/> USB Disk	Mail To <input type="text"/>
Router Name <input type="text"/>	Return-Path <input type="text"/>
Server IP Address <input type="text"/>	<input type="checkbox"/> Use SSL
Destination Port <input type="text" value="514"/>	<input type="checkbox"/> Authentication
Mail Syslog <input type="checkbox"/> Enable	Username <input type="text"/>
Enable syslog message:	Password <input type="text"/>
<input checked="" type="checkbox"/> Firewall Log	Enable E-Mail Alert:
<input checked="" type="checkbox"/> VPN Log	<input checked="" type="checkbox"/> DoS Attack
<input checked="" type="checkbox"/> User Access Log	<input checked="" type="checkbox"/> IM-P2P
<input checked="" type="checkbox"/> WAN Log	<input checked="" type="checkbox"/> VPN LOG
<input checked="" type="checkbox"/> Router/DSL information	

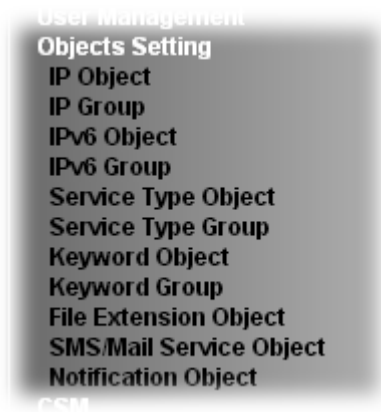
Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
3. We only support secured SMTP connection on port 465.



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

4.5 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).



4.5.1 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](#) | [33-64](#) | [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:

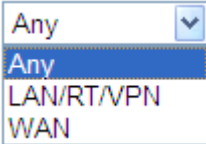
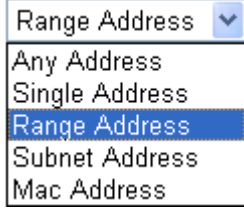
Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.59
End IP Address:	192.168.1.65
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

OK Clear Cancel

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 Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN/RT/VPN or any IP address. If you choose LAN/RT/VPN as the Interface here, and choose LAN/RT/VPN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN/RT/VPN interface will be opened for you to choose in Edit Filter Rule page.</p>
Address Type	<p>Determine the address type for the IP address.</p> <p>Select Single Address if this object contains one IP address only.</p> <p>Select Range Address if this object contains several IPs within a range.</p> <p>Select Subnet Address if this object contains one subnet for IP address.</p> <p>Select Any Address if this object contains any IP address.</p> <p>Select Mac Address if this object contains Mac address.</p> 
MAC Address	Type the MAC address of the network card which will be controlled.

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

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

Objects Setting >> IP Object

IP Object Profiles:

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

4.5.2 IP Group

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

Objects Setting >> IP Group

IP Group Table:

[Set to Factory Default](#)

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

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

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

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface:

Available IP Objects

1-RD Department
 2-Financial Dept
 3-HR Department

Selected IP Objects

(Empty)

Available settings are explained as follows:

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

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

4.5.3 IPv6 Object

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

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

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

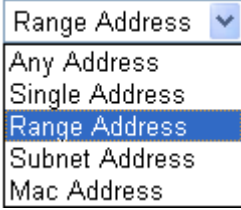
1. Click the number (e.g., #1) under Index column for configuration in details.
2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="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
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	<p>Determine the address type for the IPv6 address.</p> <p>Select Single Address if this object contains one IPv6 address only.</p> <p>Select Range Address if this object contains several IPv6s within a range.</p> <p>Select Subnet Address if this object contains one subnet for IPv6 address.</p> <p>Select Any Address if this object contains any IPv6 address.</p> <p>Select Mac Address if this object contains Mac address.</p> 
Mac Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Prefix Len	Type the number (e.g., 64) for the prefix length of IPv6 address.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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

4.5.4 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
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

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

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

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

4.5.5 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
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:

- Click the number (e.g., #1) under Index column for configuration in details.

- The configuration page will be shown as follows:

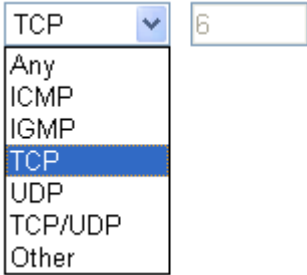
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	www	
Protocol	TCP	6
Source Port	=	1 ~ 65535
Destination Port	=	1 ~ 65535

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to. 
Source/Destination Port	Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number. (=) – 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
<u>1.</u>	www	<u>17.</u>
<u>2.</u>	SIP	<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>

4.5.6 Service Type Group

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

Objects Setting >> Service Type Group

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

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

Available settings are explained as follows:

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

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

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

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects

1-www

2-SIP

>>

<<

Selected Service Type Objects

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Available Service Type Objects	All the available service objects that you have added on Objects Setting>>Service Type Object will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

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

4.5.7 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](#) >> [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 >> Keyword Object Setup

Profile Index : 1

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

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

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

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

Available settings are explained as follows:

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

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

4.5.8 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
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

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

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

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

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

<p>Available Keyword Objects</p> <p>1-Key-1 2-Key-2</p>	<p>>></p> <p><<</p>	<p>Selected Keyword Objects(Max 16 Objects)</p>
--	---------------------------------	--

Available settings are explained as follows:

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

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

4.5.9 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
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Available settings are explained as follows:

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

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
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrm
Compression <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Available settings are explained as follows:

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

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

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

Each item is explained as follows:

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

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

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

Object Settings >> SMS / Mail Service Object

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

- The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Line_down"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="line1"/>
Password	<input type="password" value="••••"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Available settings are explained as follows:

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

- 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.	Line_down	kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)

Customized SMS Service

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

Object Settings >> SMS / Mail Service Object

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

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

Object Settings >> SMS / Mail Service Object

Profile Index: 9

Profile Name	<input type="text" value="Custom 1"/>
Service Provider	<input type="text"/>
<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>	
<p>Please contact with your SMS provide to get the exact URL String eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username=###txtUser### &password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###</p>	
Username	<input type="text"/>
Password	<input type="text"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

Available settings are explained as follows:

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

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

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

Mail Service Object

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

Object Settings >> SMS / Mail Service Object

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

Each item is explained as follows:

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

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

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
Index	
<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	<input type="text" value="Mail_Notify"/>
SMTP Server	<input type="text" value="192.168.1.98"/>
SMTP Port	<input type="text" value="465"/>
Sender Address	<input type="text" value="carrieni@draytek.com"/>
<input checked="" type="checkbox"/> Use SSL	
<input checked="" type="checkbox"/> Authentication	
Username	<input type="text" value="john"/>
Password	<input type="password" value="••••"/>
Sending Interval	<input type="text" value="0"/> (seconds)

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Type the IP address of the mail server. The maximum length of the name you can set is 63 characters.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Use SSL	Check this box to enable such function.

Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function. Username – Type a name for authentication. The maximum length of the name you can set is 31 characters. Password – Type a password for authentication. The maximum length of the password you can set is 31 characters.
Sending Interval	Define the interval for the system to send the SMS out.

- 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	
<u>1.</u>	Mail_Notify	
<u>2.</u>		
<u>3.</u>		

4.5.11 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
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile	Display the name for such mail server profile.
Settings	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
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

2. The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Index: 4

Profile Name	Notify_attack	
Category	Status	
WAN	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected
VPN Tunnel	<input type="checkbox"/> Disconnected	<input type="checkbox"/> Reconnected

Available settings are explained as follows:

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

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

Object Settings >> Notification Object

Index	Profile Name	Settings
<u>1.</u>	Notify_attack	WAN VPN
<u>2.</u>		
<u>3.</u>		

[Set to Factory Default](#)

4.6 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.

Note: 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

4.6.1 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
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
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.

There are four tabs IM, P2P, Protocol and OTHERS 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="button" value="Select All"/>	<input type="button" value="Clear All"/>		
Protocol			
Enable	APP Name	Version	Note
<input type="checkbox"/>	DB2		DB2 is a relational database management system (RDBMS) offered by IBM.
<input type="checkbox"/>	DNS		Domain Name System (DNS) protocol is used to translate easily memorized domain names to numerical IP addresses needed for the purpose of locating computer services and devices worldwide.
<input type="checkbox"/>	FTP		File Transfer Protocol (FTP) is used to transfer files from one host to another host over networks.
<input type="checkbox"/>	HTTP	1.1	Hypertext Transfer Protocol (HTTP) is the data communication protocol for the World Wide Web.
<input type="checkbox"/>	IMAP	4.1	Internet message access protocol (IMAP) is a protocol for e-mail retrieval.
<input checked="" type="checkbox"/>	IRC	2.4.0	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat), synchronous conferencing and file sharing.
<input type="checkbox"/>	Informix		Informix is a relational database management system (RDBMS) offered by IBM.
<input type="checkbox"/>	MSSQL		Microsoft SQL Server is a relational database

Available settings are explained as follows:

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

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.

4.6.2 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.

CSM >> URL Content Filter Profile

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

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

Administration Message (Max 255 characters)

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

Each item is explained as follows:

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

Administration Message	You can type the message manually for your necessity. Default Message - 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 Administration Message .
-------------------------------	--

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: Log:

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

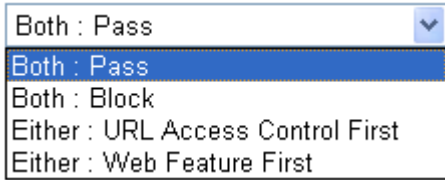
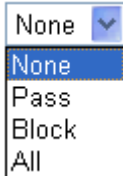

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload File Extension Profile:

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass – 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>Both: Block –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>Either: URL Access Control First – 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>Either: Web Feature First –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>Log</p>	<p>None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog. All – All the actions (Pass and Block) will be recorded in Syslog.</p> 
<p>URL Access Control</p>	<p>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</p> <p>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p> <p>Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected.</p> <p>Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>Block - 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>Group/Object Selections – 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.

Object/Group Edit

<u>Keyword Object</u>	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or <u>Keyword Group</u>	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None

OK Close

Web Feature

Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

Action - This setting is available only when **Either: URL Access Control First** or **Either: Web Feature Firs** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below.

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

If the web pages do not match with the specified feature set here, it will be processed with reverse action.

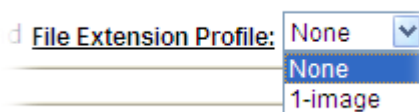
Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.

Upload - Check the box to block the file upload by way of web page.

File Extension Profile - Choose one of the profiles that you configured in **Object Setting>> File Extension**

Objects previously for passing or blocking the file downloading.



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

4.6.3 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.

Note 1: Web Content Filter (WCF) is not a built-in service of Vigor router but a service powered by **Commtouch**. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer/distributor for detailed information.

Note 2: Commtouch is merged by **Cyren**, and **GlobalView** services will be continued to deliver powerful cloud-based information security solutions! Refer to: <http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html>

Web-Filter License [Activate](#)
 [Status:Not Activated]

Setup Query Server	<input type="text" value="auto-selected"/>	Find more
Setup Test Server	<input type="text" value="auto-selected"/>	Find more

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

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

Administration Message (Max 255 characters) Cache :

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

Legend:
 %SIP% - Source IP , %DIP% - Destination IP , %URL% - URL
 %CL% - Category , %RNAME% - Router Name

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.
Default Message	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 Administration Message .

Cache	<p>None – 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>L1 – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.</p> <p>L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.</p> <p>L1+L2 Cache – 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: Log:

Black/White List

Enable

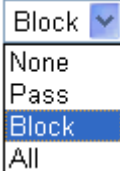
Action: Group/Object Selections

Action:

Groups	Categories		
Child Protection <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> Alcohol & Tobacco	<input checked="" type="checkbox"/> Criminal Activity	<input checked="" type="checkbox"/> Gambling
	<input checked="" type="checkbox"/> Hate & Intolerance	<input checked="" type="checkbox"/> Illegal Drug	<input checked="" type="checkbox"/> Nudity
	<input checked="" type="checkbox"/> Porn & Sexually	<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Weapons
	<input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Tasteless

<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs	<input type="checkbox"/> Personal Sites
<input type="checkbox"/> Politics	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion
<input type="checkbox"/> Restaurants & Dining	<input type="checkbox"/> Shopping	<input type="checkbox"/> Translators
<input type="checkbox"/> General	<input type="checkbox"/> Cults	<input type="checkbox"/> Greeting cards
<input type="checkbox"/> Image Sharing	<input type="checkbox"/> Network Errors	<input type="checkbox"/> Parked Domains
<input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> Uncategorized Sites	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	<p>Enable – Activate white/black list function for such profile.</p> <p>Group/Object Selections – Click Edit to choose the group or object profile as the content of white/black list.</p> <p>Pass - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. 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>Block - restrict accessing into the corresponding webpage with the characters listed on Group/Object Selections. 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>
Action	<p>Pass - allow accessing into the corresponding webpage with the categories listed on the box below.</p> <p>Block - 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>
Log	<p>None – There is no log file will be recorded for this profile.</p> <p>Pass – Only the log about Pass will be recorded in Syslog.</p> <p>Block – Only the log about Block will be recorded in Syslog.</p> <p>All – All the actions (Pass and Block) will be recorded in Syslog.</p> 

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

4.6.4 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.

CSM >> DNS Filter

DNS Filter

DNS Filter	<input type="checkbox"/> Enable
Syslog	None
Service	None
Cache Time(hour)	1
Enable Block Page	<input checked="" type="checkbox"/> Enable

Administration Message (Max 255 characters)

Default Message

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% DNS Filter.<p>Please contact your system administrator for further information.</center></body>
```

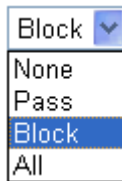
Legend:

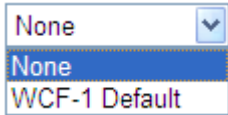
%SIP% - Source IP , %URL% - URL
%CL% - Category , %RNAME% - Router Name

OK

Cancel

Available settings are explained as follows:

Item	Description
DNS Filter	Check Enable to enable such feature.
Syslog	<p>The filtering result can be recorded according to the setting selected for Syslog.</p> <p>None – There is no log file will be recorded for this profile.</p> <p>Pass – Only the log about Pass will be recorded in Syslog.</p> <p>Block – Only the log about Block will be recorded in Syslog.</p> <p>All – All the actions (Pass and Block) will be recorded in Syslog.</p> 

Service	Set the filtering conditions. Specify one of the WCF profiles as Service.  Choose the WCF profiles to apply DNS filter.
Cache Time (hour)	Set the time for DNS query.
Enable Block Page	If such function is enabled, when DNS packets are blocked by DNS filter, a web page containing the description listed on Administration Message will be shown on the screen.
Administration Message	Type the words or sentences which will be displayed when a web page is blocked by Vigor router.

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

4.6.5 APPE Support List

Such page lists all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.

CSM >> APPE Support List

This charts lists out the APP Enforcement supported by Vigor routers.
Last update on 2014-06-16

IM	P2P	PROTOCOL	OTHERS
APP Type	APP Name	Version	Note
IM	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.
	AliiWW	2008	
	Ares	2.0.9	
	BaiduHi	37378	
	Fetion	2010	
	GaduGadu Protocol		
	Google Chat		
	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or former versions, Videos and Voices can be blocked separately.
	ICU2	8.0.6	
	Jabber Protocol/Google Talk		
	KC	2008	
	LINE	4.4.1	To block LINE for PC (v3.6.0.32) and mobile phone (v4.4.1).
	Lava-Lava	2007	
	MSN	2011	
MobileMSN			

4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.



4.7.1 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:

Limitation List

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Administration Message (Max 256 characters)

Time Schedule

Index(1-15) 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
Session Limit	<p>Enable - Click this button to activate the function of limit session.</p> <p>Disable - Click this button to close the function of limit</p>

	<p>session.</p> <p>Default session limit - Defines the default session number used for each computer in LAN.</p>
Limitation List	<p>Displays a list of specific limitations that you set on this web page.</p>
Specific Limitation	<p>Start IP- Defines the start IP address for limit session.</p> <p>End IP - Defines the end IP address for limit session.</p> <p>Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.</p> <p>Add - Adds the specific session limitation onto the list above.</p> <p>Edit - Allows you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Administration Message	<p>Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.</p> <p>Default Message - Click this button to apply the default message offered by the router.</p>
Time Schedule	<p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>

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

4.7.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

Enable
 IP Routed Subnet
 Disable

Default TX Limit: Kbps
 Default RX Limit: Kbps

Allow auto adjustment to make the best utilization of available bandwidth.

Limitation List

Index	Start IP	End IP	TX limit	RX limit	Shared

Specific Limitation

Start IP: End IP:

Each
 Shared
 TX Limit: Kbps
 RX Limit: Kbps

Smart Bandwidth Limit

For any LAN IP Not in Limitation List, when session number exceeds

TX Limit : Kbps
 RX Limit : Kbps

Note : For TX/RX, a setting of "0" means unlimited bandwidth.

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Available settings are explained as follows:

Item	Description
Bandwidth Limit	<p>Enable - Click this button to activate the function of limit bandwidth.</p> <p>Apply to 2nd Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup.</p> <p>Disable - Click this button to close the function of limit bandwidth.</p> <p>Default TX limit - Define the default speed of the upstream for each computer in LAN.</p> <p>Default RX limit - Define the default speed of the</p>

	<p>downstream for each computer in LAN.</p> <p>Allow auto adjustment... - Check this box to make the best utilization of available bandwidth.</p>
Limitation List	<p>Display a list of specific limitations that you set on this web page.</p>
Specific Limitation	<p>Start IP - Define the start IP address for limit bandwidth.</p> <p>End IP - Define the end IP address for limit bandwidth.</p> <p>Each /Shared - Select Each to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select Shared to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>Add - Add the specific speed limitation onto the list above.</p> <p>Edit - Allow you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Smart Bandwidth Limit	<p>Check this box to have the bandwidth limit determined by the system automatically.</p> <p>TX limit - Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p>
Time Schedule	<p>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.</p>

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

4.7.3 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?

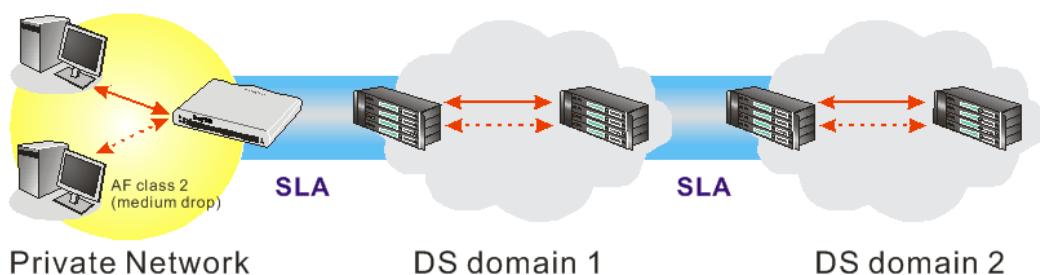
There are two components within Primary configuration of QoS deployment:

- **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.

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	80000Kbps/85000Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup	
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup	

Class Rule			
Index	Name	Rule	Service Type
Class 1	E-mail	Edit	Edit
Class 2	IPTV	Edit	
Class 3	Data/Email	Edit	

Available settings are explained as follows:

Item	Description
General Setup	<p>Index - Display the WAN interface number that you can edit.</p> <p>Status - Display if the WAN interface is available for such function or not.</p> <p>Bandwidth - Display the inbound and outbound bandwidth setting for the WAN interface.</p> <p>Direction - Display which direction that such function will influence.</p> <p>Class 1/Class2/Class 3/Others - Display the bandwidth percentage for each class.</p> <p>UDP Bandwidth Control - Display the UDP bandwidth control is enabled or not.</p> <p>Online Statistics - Display an online statistics for quality of service for your reference</p> <p>Setup - Allow to configure general QoS setting for WAN interface.</p>
Class Rule	<p>Index - Display the class number that you can edit.</p> <p>Name - Display the name of the class.</p> <p>Rule - Allow to configure detailed settings for the selected Class.</p> <p>Service Type - Allow to configure detailed settings for the service type.</p>

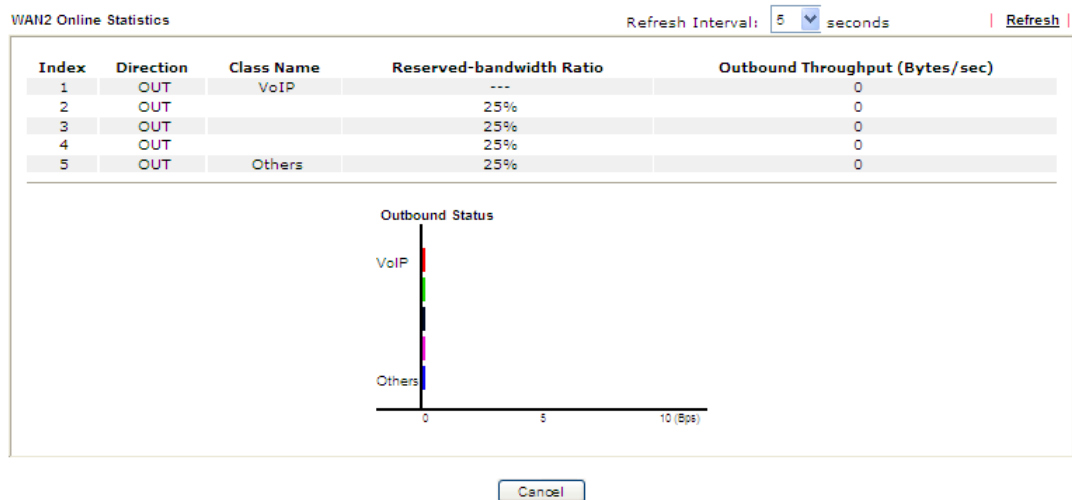
This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

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

General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth	<input type="text" value="80"/>	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps
WAN Outbound Bandwidth	<input type="text" value="85"/>	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	<input type="text" value="25"/> %
Class 2	IPTV	<input type="text" value="25"/> %
Class 3	Data/Email	<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %

Outbound TCP ACK Prioritize

Note:1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.

2. You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

Available settings are explained as follows:

Item	Description
Enable the QoS Control	<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>IN - apply to incoming traffic only.</p> <p>OUT - apply to outgoing traffic only.</p> <p>BOTH - apply to both incoming and outgoing traffic.</p> <p>Check this box and click OK, then click Setup link again. You will see the Online Statistics link appearing on this page.</p>
WAN Inbound Bandwidth	<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>
WAN Outbound Bandwidth	<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>
Reserved Bandwidth Ratio	<p>It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed.</p>
Enable UDP Bandwidth Control	<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>
Outbound TCP ACK Prioritize	<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>
Limited_bandwidth Ratio	<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	UDP Bandwidth Control	Online Statistics
WAN1	Enable	80000Kbps/85000Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

- 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 Tag packets as: ▼

NO	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

ACT

Ethernet Type IPv4 IPv6

Local Address

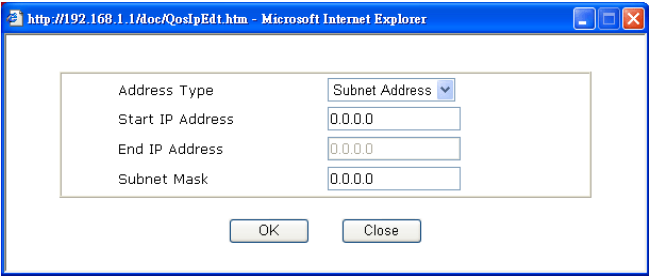
Remote Address

DiffServ CodePoint ▼

Service Type ▼

Note: Please choose/setup the Service Type first.

Available settings are explained as follows:

Item	Description
ACT	Check this box to invoke these settings.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.
Remote Address	<p>Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.</p>  <p>Address Type – Determine the address type for the source address.</p> <p>For Single Address, you have to fill in Start IP address.</p> <p>For Range Address, you have to fill in Start IP address and End IP address.</p> <p>For Subnet Address, you have to fill in Start IP address and Subnet Mask.</p>
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

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 Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	ANY
2 <input type="radio"/>	Active	192.168.1.12	192.168.1.56	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 [Set to Factory Default](#)

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics
WAN1	Enable	80000Kbps/85000Kbps	Both	25%	25%	25%	25%	Inactive	Status Setup
Backup WAN	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

- 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	<input type="text"/>
Service Type	TCP <input type="button" value="v"/> <input type="text" value="6"/>
Port Configuration	
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range
Port Number	<input type="text" value="0"/> - <input type="text" value="0"/>

Available settings are explained as follows:

Item	Description
Service Name	Type in a new service for your request. The maximum length of the name you can set is 11 characters.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	<p>Type - Click Single or Range as the Type. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.</p> <p>Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.</p>

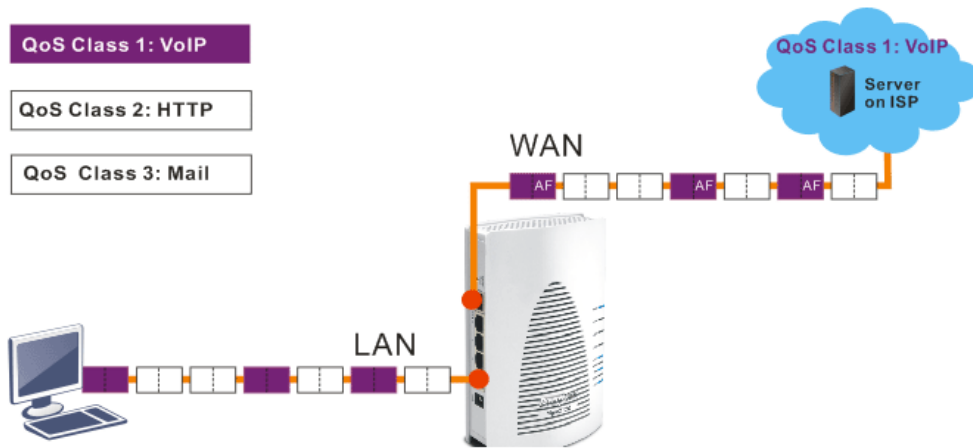
- After finishing all the settings here, please click **OK** to save the configuration.

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.



Bandwidth Management >> Quality of Service

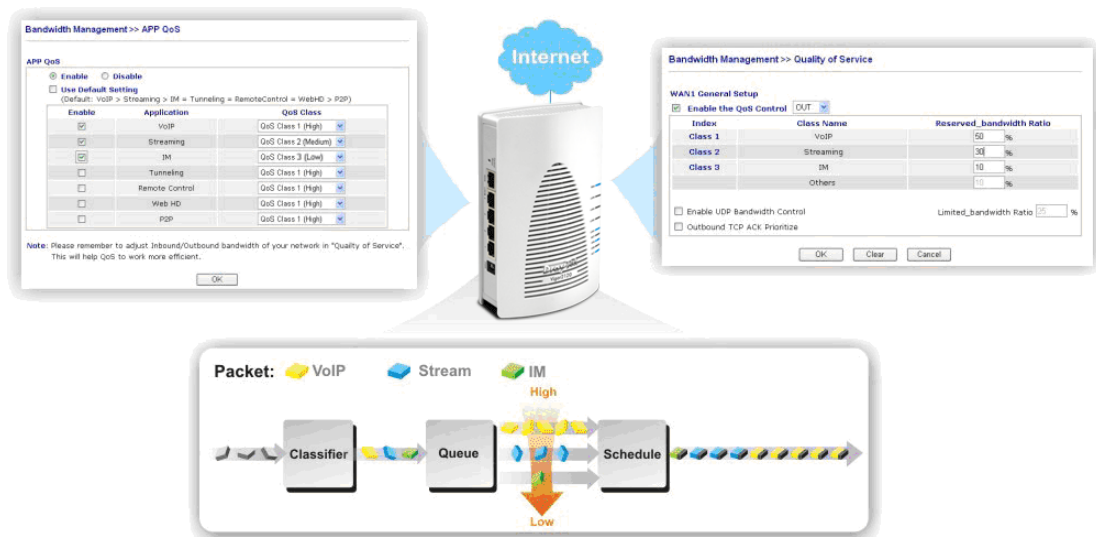
Class Index #1
 Name: VoIP Tag packets as: AF Class1 (High Drop)

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	<input type="radio"/> Active	Any	Any	ANY	ANY

4.7.4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as IM or P2P without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect several types of software in application layer. By combining the function of QoS, Vigor router can perform the bandwidth management for the application of VoIP, Streaming, IM, P2P and so on.



Open **Bandwidth Management>>APP QoS** to display the following page. The following shows web page under Traceable.

APP QoS

Enable Disable

 Apply to all: QoS Class 1 (High) ▾

Enable	Protocol	Action
<input type="checkbox"/>	DNS	QoS Class 1 (High) ▾
<input type="checkbox"/>	FTP	QoS Class 1 (High) ▾
<input type="checkbox"/>	HTTP	QoS Class 1 (High) ▾
<input type="checkbox"/>	IMAP	QoS Class 1 (High) ▾
<input type="checkbox"/>	IRC	QoS Class 1 (High) ▾
<input type="checkbox"/>	NNTP	QoS Class 1 (High) ▾
<input type="checkbox"/>	POP3	QoS Class 1 (High) ▾
<input type="checkbox"/>	SMB	QoS Class 1 (High) ▾
<input type="checkbox"/>	SMTP	QoS Class 1 (High) ▾
<input type="checkbox"/>	SNMP	QoS Class 1 (High) ▾
<input type="checkbox"/>	SSH	QoS Class 1 (High) ▾
<input type="checkbox"/>	SSL/TLS	QoS Class 1 (High) ▾
<input type="checkbox"/>	TELNET	QoS Class 1 (High) ▾

Note: Please remember to adjust Inbound/Outbound bandwidth of your network in "Quality of Service".
 This will help QoS to work more efficient.

The following shows web page under Untraceable.

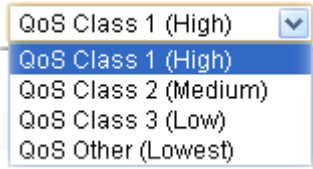
APP QoS

Enable Disable

 Action: QoS Class 1 (High) ▾

Enable	IM
<input type="checkbox"/>	AIM
<input type="checkbox"/>	AliWW
<input type="checkbox"/>	Ares
<input type="checkbox"/>	BaiduHi
<input type="checkbox"/>	Fetion
<input type="checkbox"/>	GaduGadu Protocol
<input type="checkbox"/>	Google Chat
<input type="checkbox"/>	ICQ
<input type="checkbox"/>	ICU2
<input type="checkbox"/>	Jabber Protocol/Google Talk
<input type="checkbox"/>	KC
<input type="checkbox"/>	LINE
<input type="checkbox"/>	Lava-Lava
<input type="checkbox"/>	MSN
<input type="checkbox"/>	MobileMSN
<input type="checkbox"/>	POCO
<input type="checkbox"/>	Paltalk
<input type="checkbox"/>	QQ/TM
<input type="checkbox"/>	Qq

Available settings are explained as follows:

Item	Description
Enable/Disable	Click Enable to activate APP QoS function. Click Disable to deactivate APP QoS function.
Select All	Click it to choose all of the items in this page.
Clear All	Uncheck all the selected boxes.
Action	The APP can be specified with different QoS Class. 

4.8 Applications

Below shows the menu items for Applications.



4.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.

Dynamic DNS Setup
| [Set to Factory Default](#) |

Enable Dynamic DNS Setup

Auto-Update interval Min(s) (1~14400)

Accounts:

Index	Domain Name	Active
1.		x
2.		x
3.		x

Available settings are explained as follows:

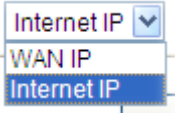
Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display the WAN interface used.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.

- 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

<input checked="" type="checkbox"/> Enable Dynamic DNS Account		
Service Provider	dyndns.org (www.dyndns.org) ▼	
Service Type	Dynamic ▼	
Domain Name	chronic6653	dyndns.org ▼
Login Name	chronic6653	(max. 64 characters)
Password	••••••••	(max. 23 characters)
<input type="checkbox"/> Wildcards		
<input type="checkbox"/> Backup MX		
Mail Extender		
Determine Real WAN IP	Internet IP ▼	

Available settings are explained as follows:

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine Real WAN IP	<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> <div style="text-align: center;">  </div> <p>WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.</p> <p>Internet IP - If it is selected and the WAN IP of Vigor</p>

	router is private, it will be converted to public IP before DDNS update takes place.
--	--

- 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.

4.8.2 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 Resolution | [Set to Factory Default](#) |

Enable	Index	Profile	Domain Name
<input type="checkbox"/>	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.		

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

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable	Check the box to enable the selected profile.
Index	Click the number below Index to access into the setting page.
Profile	Display the name of the LAN DNS profile.
Domain Name	Display the domain name of the LAN DNS profile.

You can set up to 20 LAN DNS profiles.

To create a LAN DNS profile:

- Click any index, say Index No. 1.
- The detailed settings with index 1 are shown below.

Profile Index : 1

Enable

Profile:

Domain Name:

IP Address List

Index	IP Address	Same Subnet Reply

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile.
Domain Name	Type the domain name for such profile.
IP Address List	<p>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.</p> <p>Add – Click it to open a dialog to type the host's IP address.</p> <div style="border: 1px solid blue; padding: 5px; margin: 5px 0;"> <p style="font-size: small;">Host's IP Address - Windows Internet Explorer</p> <p style="font-size: x-small;">http://192.168.1.1/doc/landnshost.htm</p> <p>Host's IP Address</p> <p><input style="width: 150px;" type="text" value="192.1368.1.86"/></p> <p><input checked="" type="checkbox"/> Only responds to the DNS request when the sender is in the same subnet.</p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> </div> <p>● 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.</p> <p>Delete – Click it to remove an existed IP address on the list.</p>

3. Click **OK** button to save the settings.

- A new LAN DNS profile has been created.

Applications >> LAN DNS

LAN DNS Resolution | [Set to Factory Default](#) |

Enable	Index	Profile	Domain Name
<input checked="" type="checkbox"/>	1.	sales_1	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

4.8.3 Schedule

The Vigor router has a built-in 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: | [Set to Factory Default](#) |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.

Status	Display if this schedule setting is active or inactive.
---------------	---

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN and Remote Access** >> **LAN-to-LAN** settings.

To add a schedule:

1. Click any index, say Index No. 1.
2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1

Enable Schedule Setup

Start Date (yyyy-mm-dd) 2000 . 1 . 1

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

OK Clear Cancel

Available settings are explained as follows:



Item	Description
Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	Specify which action Call Schedule should apply during the period of the schedule. Force On -Force the connection to be always on. Force Down -Force the connection to be always down. Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field. Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

Idle Timeout	Specify the duration (or period) for the schedule. How often -Specify how often the schedule will be applied Once -The schedule will be applied just once Weekdays -Specify which days in one week should perform the schedule.
---------------------	---

3. Click **OK** button to save the settings.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office
Hour:  
(Force On)
Mon - Sun **9:00 am** to **6:00 pm**

1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

4.8.4 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

Enable

Server IP Address

Destination Port

Shared Secret

Confirm Shared Secret

Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature.
Server IP Address	Type the IP address of RADIUS server
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

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

4.8.5 UPnP

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

Applications >> UPnP

UPnP

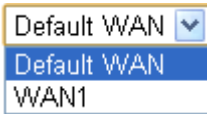
Enable UPnP Service Default WAN ▾

Enable Connection Control Service

Enable Connection Status Service

Note: To allow NAT pass-through to a UPnP-enabled client on the LAN, enable UPnP service above and ensure that the used connection service is also ticked.

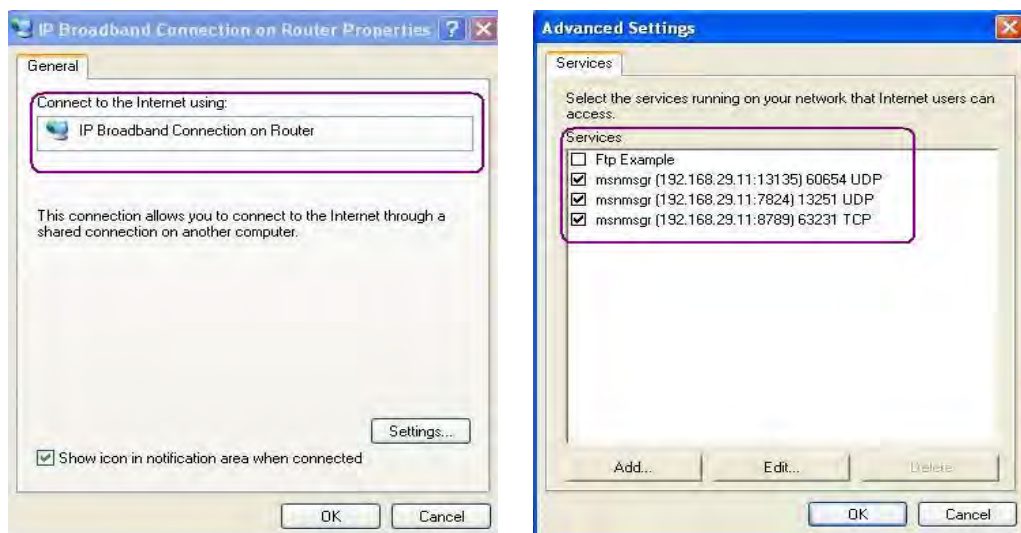
Available settings are explained as follows:

Item	Description
Enable UPnP Service	Accordingly, you can enable either the Connection Control Service or Connection Status Service .
Default WAN	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.

4.8.6 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications >> IGMP

IGMP

Enable IGMP Proxy WAN1 ▾
 IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function **take no effect when Bridge Mode is enabled**.

Enable IGMP Snooping
 Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group.
 Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

[Refresh](#)

Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4

Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> WAN1 ▾ WAN1 PVC </div>
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

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

4.8.7 Wake on LAN

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

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

Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with **Bind IP to MAC** function, only binded PCs can wake up through IP.

Wake by:

IP Address:

MAC Address:

Result

Available settings are explained as follows:

Item	Description
Wake by	<p>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.</p> <p>Wake by: <input type="text" value="MAC Address"/></p>
IP Address	<p>The IP addresses that have been configured in Firewall>>Bind IP to MAC will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.</p>
MAC Address	<p>Type any one of the MAC address of the bound PCs.</p>
Wake Up	<p>Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.</p>

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: : : : : :

Result

Send command to client done.

4.8.8 SMS / Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

SMS Provider

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

| [Set to Factory Default](#) |

Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 <input checked="" type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
2 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
3 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
4 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
5 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
6 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
7 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
8 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
9 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>
10 <input type="checkbox"/>	1 - Line_down <input type="button" value="v"/>	<input type="text"/>	1 - Notify_attack <input type="button" value="v"/>	<input type="text"/> <input type="text"/>

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 SMS Provider link to define the SMS server.

Recipient	Type the name of the one who will receive the SMS.
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the SMS.
Schedule	Type the schedule number that the SMS will be sent out. You can click the Schedule(1-15) 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

SMS Provider		Mail Server			Set to Factory Default	
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)		
1 <input checked="" type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
2 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
3 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
4 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
5 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
6 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
7 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
8 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
9 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	
10 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - Notify_attack	<input type="text"/>	<input type="text"/>	

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
Mail Service	Use the drop down list to choose mail service provider. You can click Mail Service link to define the mail server.
Recipient	Type the e-mail address of the one who will receive the notification message.
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the Notify Profile link to define the content of the mail message.

Schedule	Type the schedule number that the notification will be sent out. You can click the Schedule(1-15) link to define the schedule.
-----------------	--

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

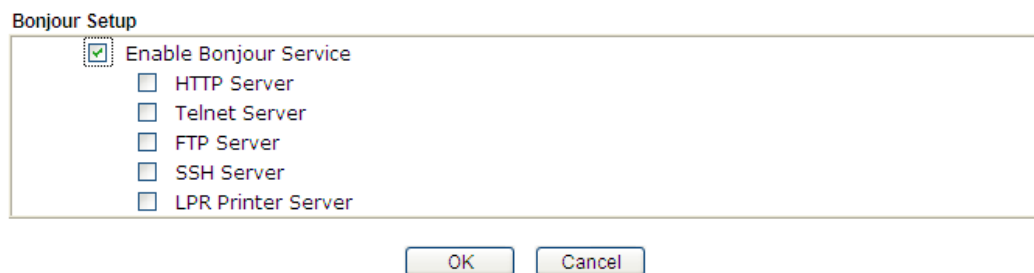
4.8.9 Bonjour

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.

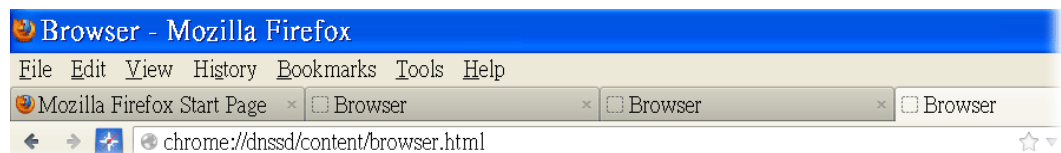
To enable the Bonjour service, click **Application>>Bonjour** to open the following page. Check the box(es) of the server service(s) that you want to share to the LAN clients.

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.



2. Open the web browse, Firefox. If Bonjour and DNSSD have been installed, you can open the web page (DNSSD) and see the following results.

DNSSD for Firefox

Browser Configuration Options Diagnostic Information

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http_tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http_tcp.	local.	
2	HP LaserJet 1300	_ipp_tcp.	local.	
2	tctseng-virtual-machine	_udisks-ssh_tcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation_tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation_tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation_tcp.	local.	

- Open **System Maintenance>>Management**. Type a name (e.g., Dray_2925) as the Router Name and click **OK**.

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup												
Router Name <input type="text" value="Vigor Router"/> <input type="checkbox"/> Default: Disable Auto-Logout Internet Access Control <input checked="" 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 checked="" type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet Access List from the Internet <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"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports 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) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22) External Device Control <input checked="" type="checkbox"/> No respond to External Device
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"/>											

OK

- Next, open **Applications>>Bonjour**. Check the service that you want to use via Bonjour.

Applications >> Bonjour

Bonjour Setup

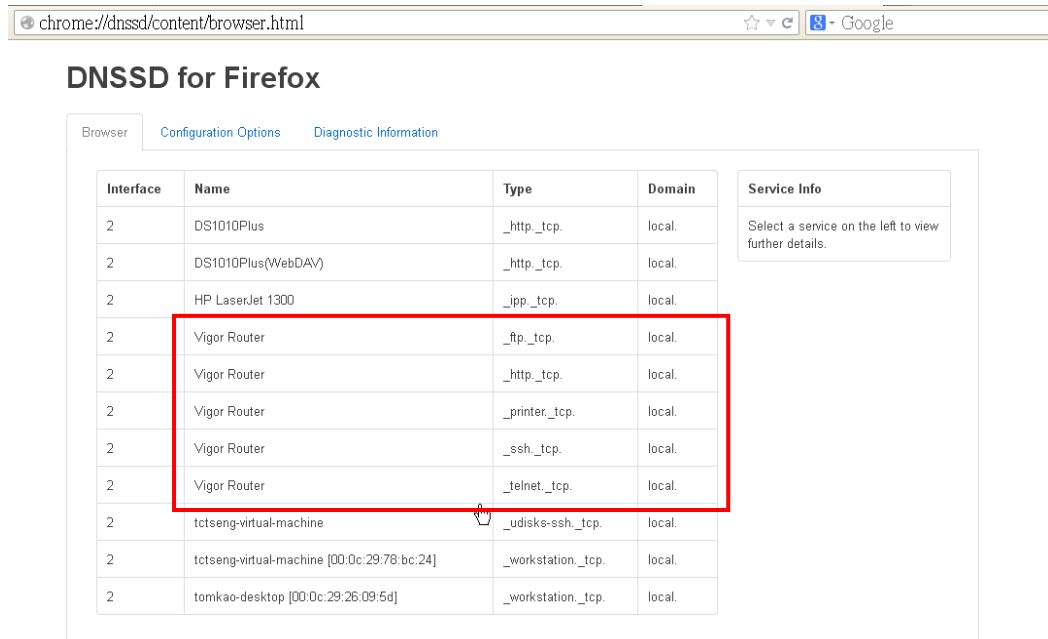
Enable Bonjour Service

- HTTP Server
- Telnet Server
- FTP Server
- SSH Server
- LPR Printer Server

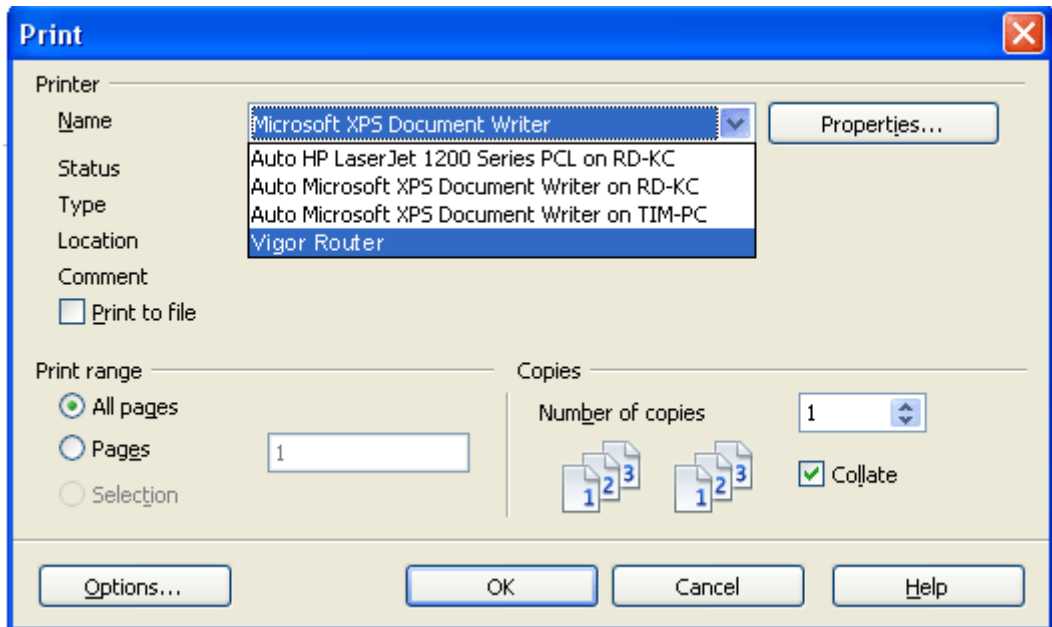
OK

Cancel

- 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).



4.9 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.



4.9.1 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

Note: To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT [Open Ports](#) or [Port Redirection](#) is also configured.

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

4.9.2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.


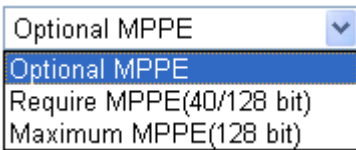
VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol	
Dial-In PPP Authentication	PAP/CHAP/MS-CHAP/MS-CHAPv2
Dial-In PPP Encryption(MPPE)	Optional MPPE
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	<input type="text"/>
Password	<input type="text"/>
IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Assigned IP start	LAN 1 192.168.1.200
	LAN 2 192.168.2.200

OK

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	<p>PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol.</p> <p>PAP /CHAP/MS-CHAP/MS-CHAPv2 - 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> 
Dial-In PPP Encryption (MPPE)	<p>Optional MPPE - 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>Require MPPE (40/128bits) - 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>Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.</p>

Mutual Authentication (PAP)	<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 Username and Password of the mutual authentication peer.</p> <p>The length of the name/password is limited to 23/19 characters.</p>
Assigned IP Start	<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>

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

4.9.3 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

VPN IKE/IPsec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Certificate for Dial-in None ▾

Pre-Shared Key

Pre-Shared Key

Confirm Pre-Shared Key

IPsec Security Method

Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPsec-related VPN connections such as L2TP over IPsec and IPsec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming

	<p>from remote dial-in user, Certificate (X.509) and Pre-Shared Key.</p> <p>Certificate for Dial-in –Choose one of the local certificates from the drop down list.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.</p> </div>
<p>IPsec Security Method</p>	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High (ESP) - 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.

4.9.4 IPsec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPsec Peer Identity

X509 Peer ID Accounts: [Set to Factory Default](#)

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	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

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPsec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

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
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.
Enable this account	Check it to enable such account profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address, Domain, or E-mail Address . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E) .

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

4.9.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

VPN and Remote Access >> Remote Dial-in User



Remote Access User Accounts:				Set to Factory Default			
Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	<input type="checkbox"/>	---	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	???	<input type="checkbox"/>	---	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	???	<input type="checkbox"/>	---	<u>19.</u>	???	<input type="checkbox"/>	---
<u>4.</u>	???	<input type="checkbox"/>	---	<u>20.</u>	???	<input type="checkbox"/>	---
<u>5.</u>	???	<input type="checkbox"/>	---	<u>21.</u>	???	<input type="checkbox"/>	---
<u>6.</u>	???	<input type="checkbox"/>	---	<u>22.</u>	???	<input type="checkbox"/>	---
<u>7.</u>	???	<input type="checkbox"/>	---	<u>23.</u>	???	<input type="checkbox"/>	---
<u>8.</u>	???	<input type="checkbox"/>	---	<u>24.</u>	???	<input type="checkbox"/>	---
<u>9.</u>	???	<input type="checkbox"/>	---	<u>25.</u>	???	<input type="checkbox"/>	---
<u>10.</u>	???	<input type="checkbox"/>	---	<u>26.</u>	???	<input type="checkbox"/>	---
<u>11.</u>	???	<input type="checkbox"/>	---	<u>27.</u>	???	<input type="checkbox"/>	---
<u>12.</u>	???	<input type="checkbox"/>	---	<u>28.</u>	???	<input type="checkbox"/>	---
<u>13.</u>	???	<input type="checkbox"/>	---	<u>29.</u>	???	<input type="checkbox"/>	---
<u>14.</u>	???	<input type="checkbox"/>	---	<u>30.</u>	???	<input type="checkbox"/>	---
<u>15.</u>	???	<input type="checkbox"/>	---	<u>31.</u>	???	<input type="checkbox"/>	---
<u>16.</u>	???	<input type="checkbox"/>	---	<u>32.</u>	???	<input type="checkbox"/>	---

OK Cancel

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
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 enable the selected profile.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

Index No. 12

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</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"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <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 IGMP, IP-Camera, DHCP Relay...etc.)</p> <hr/> <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> <hr/> <p>SSL VPN</p> <p><input type="button" value="Set SSL Application"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
---	--

Available settings are explained as follows:

Item	Description
<p>User account and Authentication</p>	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- 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>
<p>Allowed Dial-In Type</p>	<p>PPTP - 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>IPsec Tunnel - Allow the remote dial-in user to make an IPsec VPN connection through Internet.</p> <p>L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.

	<ul style="list-style-type: none"> ● Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. ● Must -Specify the IPsec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel – Allow the remote dial-in user to make an SSL VPN connection through Internet.</p> <p>Specify Remote Node -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 general settings.</p> <p>Netbios Naming Packet -</p> <ul style="list-style-type: none"> ● 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. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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. <p>User Name - 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>Password - 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>Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.</p> <p>PIN Code – Type the code for authentication (e.g, 1234).</p> <p>Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p> <p>Assign Static IP Address – Please type a static IP address for the subnet you specified.</p>
SSL VPN	<p>Set SSL Application – Choose the SSL application profile to be applied by such dial-in user profile.</p>
IKE Authentication Method	<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</p>

	<p>or without specify the IP address of the remote node.</p> <p>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.</p> <p>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.</p>
IPsec Security Method	<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>Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p>High-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> <p>Local ID (Optional)- 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.

4.9.6 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](#) |

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"/>	---
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"/>	---

Available settings are explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Active	V – means the profile has been enabled. X – mans the profile has not been enabled.
Status	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.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Username <input type="text" value="???"/> Password(Max 15 char) <input type="text"/> PPP Authentication <input type="text" value="PAP Only"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input type="text"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

Available settings are explained as follows:

Item	Description
Common Settings	<p>Profile Name – Specify a name for the profile of the LAN-to-LAN connection.</p> <p>Enable this profile - Check here to activate this profile.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● 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. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass – Click this button to let multicast packets pass

	<p>through the router.</p> <ul style="list-style-type: none"> ● Block – This is default setting. Click this button to let multicast packets be blocked by the router. <p>Call Direction - Specify the allowed call direction of this LAN-to-LAN profile.</p> <ul style="list-style-type: none"> ● Both:-initiator/responder ● Dial-Out- initiator only ● Dial-In- responder only. <p>Always On-Check to enable router always keep VPN connection.</p> <p>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</p> <p>Enable PING to keep alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.</p> <p>Enable PING to keep alive 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>PING to the IP - Enter the IP address of the remote host that located at the other-end of the VPN tunnel.</p>
<p>Dial-Out Settings</p>	<p>Type of Server I am calling –</p> <p>PPTP - 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>IPsec Tunnel - Build an IPsec VPN connection to the server through Internet.</p> <p>L2TP with IPsec Policy - 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"> ● None: Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection. ● Nice to Have: Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. ● Must: Specify the IPsec policy to be definitely

applied on the L2TP connection.

User Name - 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.

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 15 characters.

PPP Authentication - This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to wild compatibility.

VJ compression - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **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:

IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

- **IKE phase 1 proposal**-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
- **IKE phase 2 proposal**-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
- **IKE phase 1 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
- **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.
- **Perfect Forward Secret (PFS)**-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Index(1-15) - Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

3. Dial-In Settings

<p>Allowed Dial-In Type</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 None</p> <p><input type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP <input style="width: 100px;" type="text"/></p> <p>or Peer ID <input style="width: 100px;" type="text"/></p>	<p>Username <input data-bbox="1161 456 1380 488" style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 11 char) <input data-bbox="1161 501 1380 533" style="width: 100px;" type="text"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1161 663 1380 694" style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p> <p>Local ID</p> <p><input checked="" type="radio"/> Alternative Subject Name First</p> <p><input type="radio"/> Subject Name First</p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>
--	---

4. TCP/IP Network Settings

<p>My WAN IP <input data-bbox="663 1032 882 1064" style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input data-bbox="663 1077 882 1108" style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input data-bbox="663 1122 882 1153" style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network Mask <input data-bbox="663 1167 882 1198" style="width: 100px;" type="text" value="255.255.255.0"/></p> <p>Local Network IP <input data-bbox="663 1211 882 1243" style="width: 100px;" type="text" value="192.168.1.1"/></p> <p>Local Network Mask <input data-bbox="663 1256 882 1288" style="width: 100px;" type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do</p> <p style="text-align: center;">Route</p> <hr/> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)</p>
--	--

Available settings are explained as follows:

Item	Description
Dial-In Settings	<p>Allowed Dial-In Type - Determine the dial-in connection with different types.</p> <ul style="list-style-type: none"> ● PPTP - 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. ● IPsec Tunnel- Allow the remote dial-in user to trigger an IPsec VPN connection through Internet. ● L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below: <ul style="list-style-type: none"> ■ None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the

L2TP without IPsec policy can be viewed as one pure L2TP connection.

- **Nice to Have** - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.
- **Must** - Specify the IPsec policy to be definitely applied on the L2TP connection.

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.
- **High-** 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.

TCP/IP Network Settings

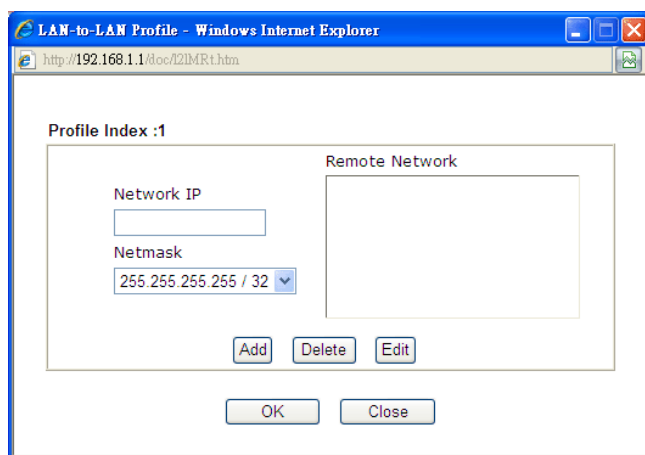
My WAN IP –This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, 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.

Remote Network IP/ Remote Network Mask - 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.

Local Network IP / Local Network Mask - Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.

More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



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.

4.9.7 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

VPN Connection Status Page No.

Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime

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

Available settings are explained as follows:

Item	Description
Dial-out Tool	<p>Dial - Click this button to execute dial out function.</p> <p>Refresh Seconds - Choose the time for refresh the dial information among 5, 10, and 30.</p> <p>Refresh - Click this button to refresh the whole connection status.</p>

4.10 Certificate Management

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

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

Here you can 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.



4.10.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

Available settings are explained as follows:

Item	Description
Generate	Click this button to open Generate Certificate Request window. Type in all the information that the window requests. Then click Generate again.
Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.
Delete	Click this button to delete selected name with certification information.

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Generate Certificate Signing Request

Subject Alternative Name	
Type	IP Address <input type="button" value="v"/>
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 <input type="button" value="v"/>
Key Size	1024 Bit <input type="button" value="v"/>

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	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

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:
 Click **Import** to upload the local certificate.

Upload PKCS12 Certificate
 Select a PKCS12 file.
 PKCS12 file:
 Password:
 Click **Import** to upload the PKCS12 file.

Upload Certificate and Private Key
 Select a certificate file and a matchable Private Key.
 Certificate file:
 Key file:
 Password:
 Click **Import** to upload the local certificate and private key.

Available settings are explained as follows:

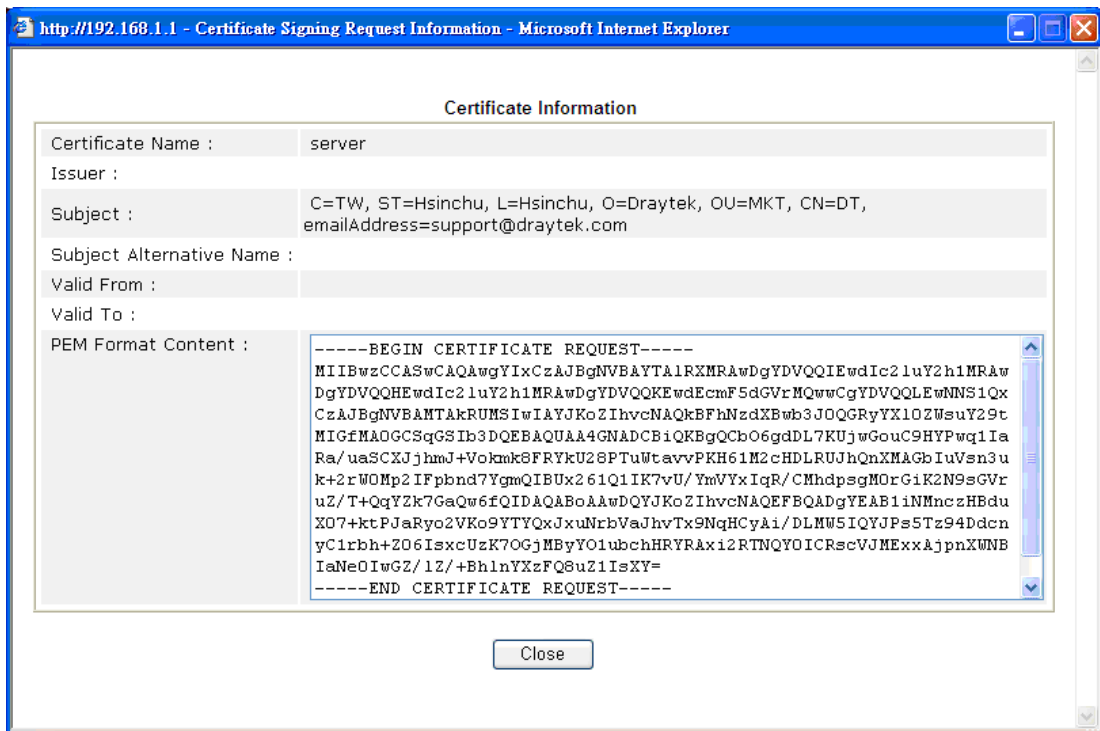
Item	Description
Upload Local Certificate	It allows users to import the certificate which is generated by vigor router and signed by CA server. If you have done well in certificate generation, the Status of the certificate will be shown as “ OK ”.
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. Note: PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.



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.

4.10.2 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	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

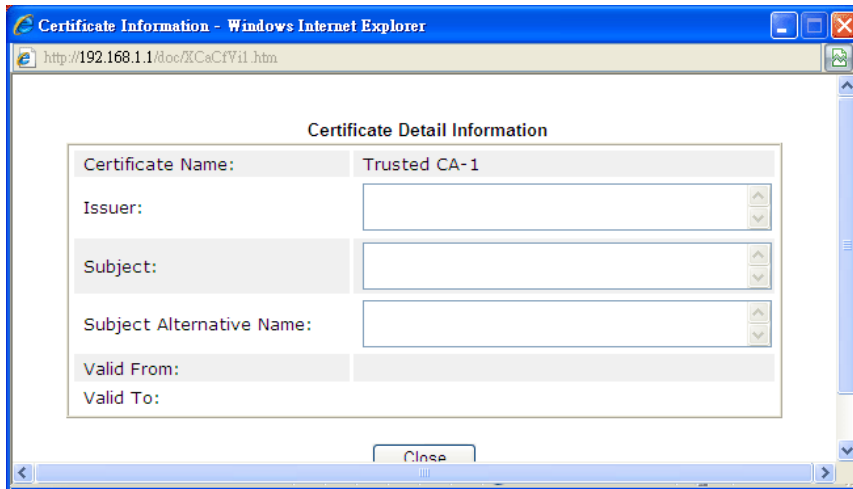
To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click [Import](#) to upload the certification.

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.



4.10.3 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

<p>Backup</p> <p>Encrypt password: <input type="text"/></p> <p>Confirm password: <input type="text"/></p> <p>Click <input type="button" value="Backup"/> to download certificates to your local PC as a file.</p>
<p>Restoration</p> <p>Select a backup file to restore.</p> <p><input type="text"/> <input type="button" value="Browse.."/></p> <p>Decrypt password: <input type="text"/></p> <p>Click <input type="button" value="Restore"/> to upload the file.</p>

4.11 Wireless LAN(2.4GHz/5GHz)

This function is used for “n” models only.

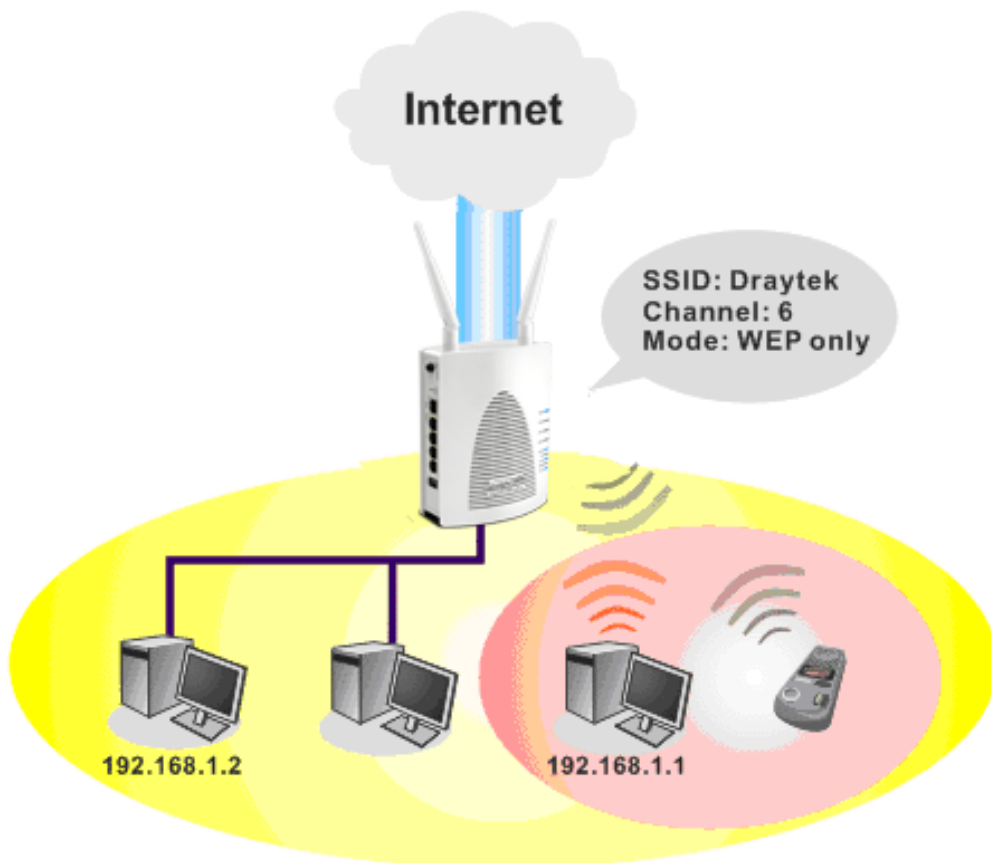
4.11.1 Basic Concepts

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.

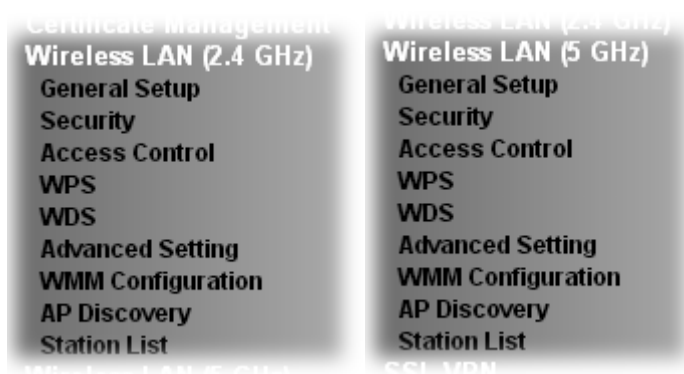
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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.



In this section, we take Wireless LAN (2.4G) as the examples of function explanations.

4.11.2 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.

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode :

Channel:

	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="DrayTek_Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note:
Enabling the Isolate Member configuration will forbid the wireless clients associated to the same SSID from connecting to each other.

The isolate VPN configuration will isolate the wireless traffic from VPN connections and thus, wireless clients will not be able to access the VPN network under this setting.

Rate Control

	Enable	Upload	Download
SSID 1	<input type="checkbox"/>	<input type="text" value="30000"/> kbps	<input type="text" value="30000"/> kbps
SSID 2	<input type="checkbox"/>	<input type="text" value="30000"/> kbps	<input type="text" value="30000"/> kbps
SSID 3	<input type="checkbox"/>	<input type="text" value="30000"/> kbps	<input type="text" value="30000"/> kbps
SSID 4	<input type="checkbox"/>	<input type="text" value="30000"/> kbps	<input type="text" value="30000"/> kbps

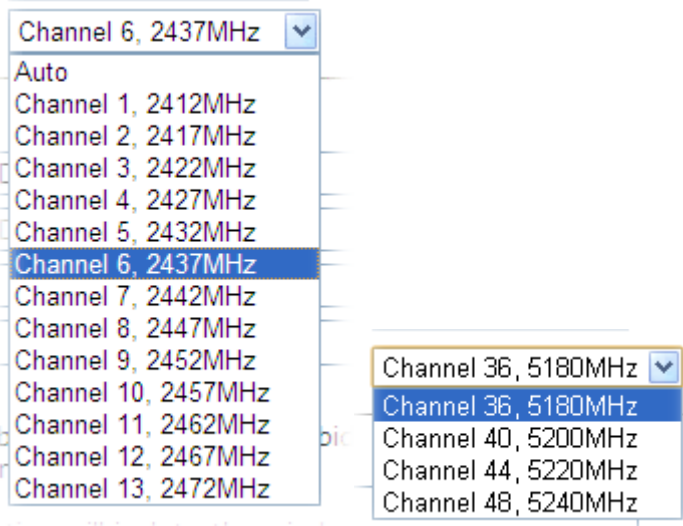
Note:
Configurable upload and download rates are from 100 to 50,000(kbps).

Associated Schedule Profiles: , , ,

Note:
Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored. Valid settings are profile indexes 1 to 15.

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	<p>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> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p>2.4G</p> </div> <div style="text-align: center;"> <p>5G</p> </div> </div>

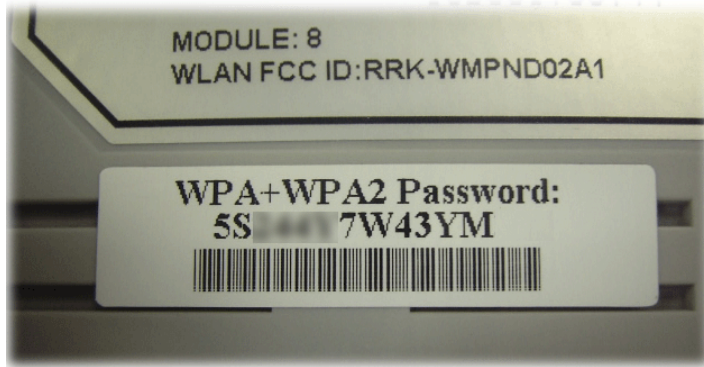
<p>Channel</p>	<p>Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.</p>  <p style="text-align: center;">2.4G 5G</p>
<p>Hide SSID</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>SSID</p>	<p>Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.</p>
<p>Isolate</p>	<p>Member – Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. VPN – Check this box to restrict the wireless clients (stations) to access VPN network.</p>
<p>Rate Control</p>	<p>It controls the data transmission rate through wireless connection. Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. Download – Type the transmitting rate for data download. Default value is 30,000 kbps.</p>
<p>Schedule</p>	<p>Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.</p>

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

4.11.3 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 (2.4 GHz) >> Security Settings

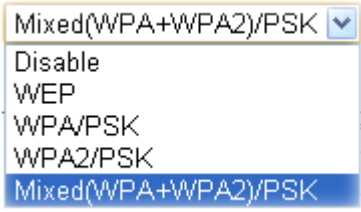
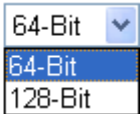
SSID 1	SSID 2	SSID 3	SSID 4
<p>Mode: Mixed(WPA+WPA2)/PSK ▼</p> <p><u>WPA</u></p> <p>Encryption Mode: TKIP for WPA/AES for WPA2</p> <p>Pre-Shared Key(PSK): <input type="text" value="*****"/></p> <p>Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".</p> <p><u>WEP</u></p> <p>Encryption Mode: 64-Bit ▼</p> <p><input checked="" type="radio"/> Key 1 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 2 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 3 : <input type="text" value="*****"/></p> <p><input type="radio"/> Key 4 : <input type="text" value="*****"/></p> <p>Note:</p> <p>For 64 bit WEP key configurations, please insert 5 ASCII characters or 10 Hexadecimal digits leading by "0x". Examples are "AB312" or "0x4142333132".</p> <p>For 128 bit WEP key configurations, please insert 13 ASCII characters or 26 Hexadecimal digits leading by "0x".</p>			

OK

Cancel

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.

	 <p>Disable - Turn off the encryption mechanism.</p> <p>WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.</p> <p>WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.</p> <p>Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.</p>
WPA	<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 authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p> <p>Type - Select from Mixed (WPA+WPA2) or WPA2 only.</p> <p>Pre-Shared Key (PSK) - Either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").</p>
WEP	<p>64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)</p> <p>128-Bit - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x414243444546474849A4B4C4D).</p> <p>Encryption Mode: </p> <p>All wireless devices must support the same WEP encryption bit size and have the same key. Four keys 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.

4.11.4 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 : : : : : :

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

Available settings are explained as follows:

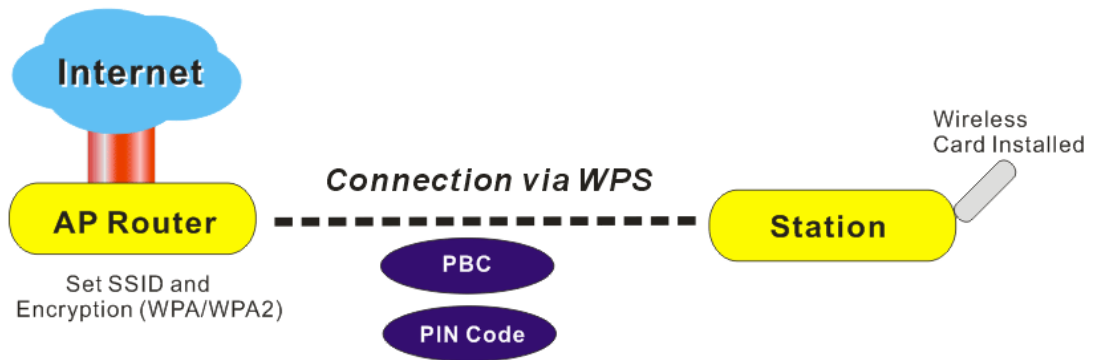
Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.

Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

4.11.5 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.

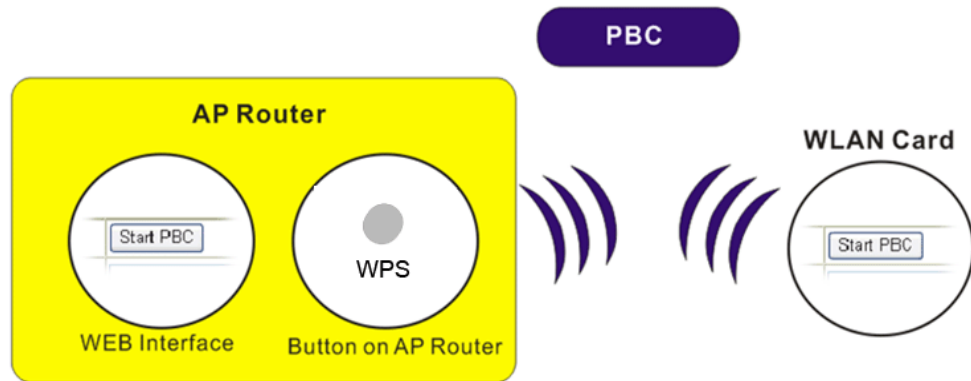


Note: Such function is available for the wireless station with WPS supported.

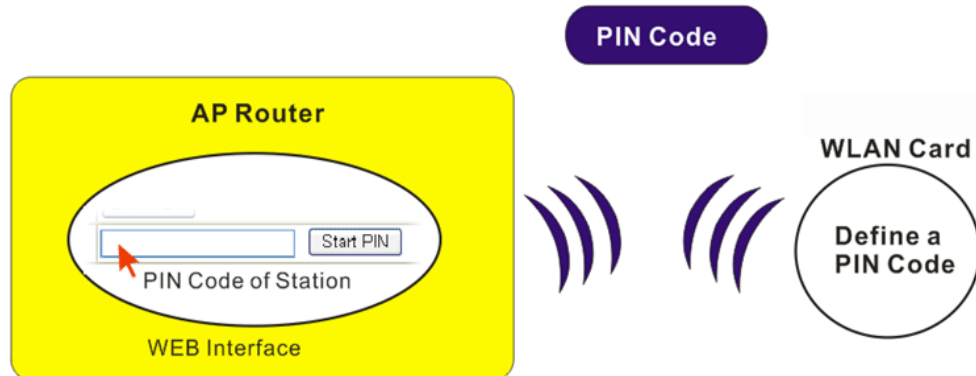
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for 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*.

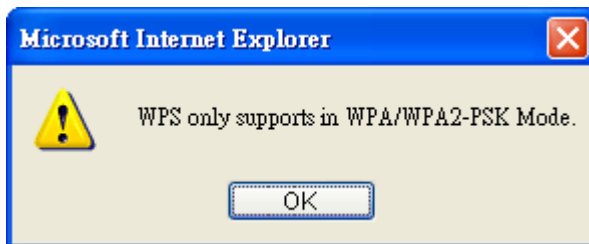
- On the side of Vigor2120 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- 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 (2.4 GHz) >> WPS (Wi-Fi Protected Setup)

Enable WPS

Wi-Fi Protected Setup Information


WPS Status	Configured
SSID	DrayTek
Authentication Mode	Mixed(WPA+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: Wireless LAN is NOT enabled!!

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:

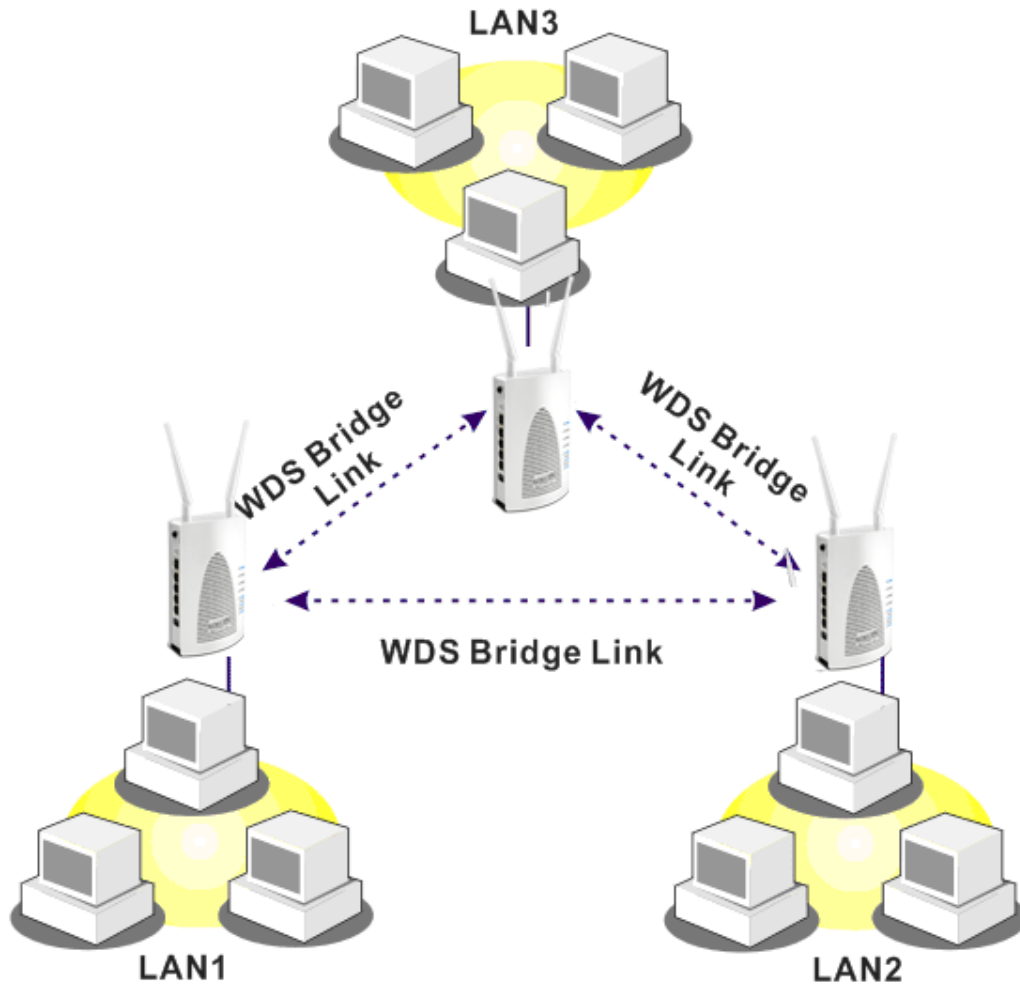
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN 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)

4.11.6 WDS

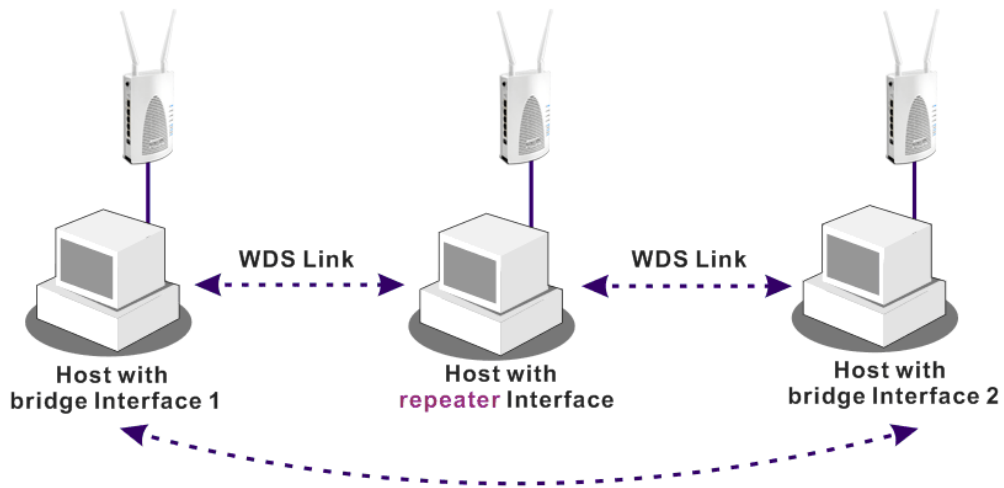
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:

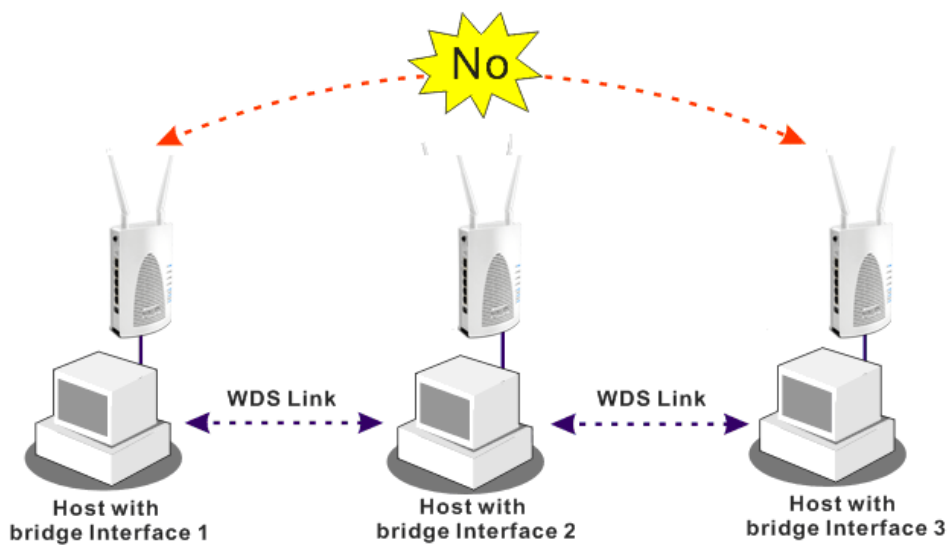


The application for the WDS-Repeater mode is depicted as below:



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.

WDS Settings | [Set to Factory Default](#) |

Mode: Bridge ▾

Security:

Disable WEP Pre-shared Key

WEP:

Use the same WEP key set in [Security Settings](#).

Pre-shared Key:

Type:

WPA WPA2

Key :

Note: WPA and WPA2 are not compatible with DrayTek WPA.

Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".

Bridge

Enable Peer MAC Address

<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Note: Disable unused links to get better performance.

Repeater

Enable Peer MAC Address

<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Access Point Function:

Enable Disable

Status:

Send "Hello" message to peers.

Note: The status is valid only when the peer also supports this function.

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. Disable mode will not invoke any WDS setting. Bridge mode is designed to fulfill the first type of application. Repeater mode is for the second one. <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Disable ▾ Disable Bridge Repeater </div>
Security	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
Pre-shared Key	Type – There are some types for you to choose. WPA and WPA2 are used for WDS devices (e.g.2120n-plus wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. Key - Type 8 ~ 63 ASCII characters or 64 hexadecimal

	digits leading by “0x”.
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

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

4.11.7 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.

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 checked="" type="radio"/> Disable <input type="radio"/> Enable
Packet-OVERDRIVE™ TX Burst	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

OK

2.4G

Wireless LAN (5 GHz) >> Advanced Setting

Physical Mode

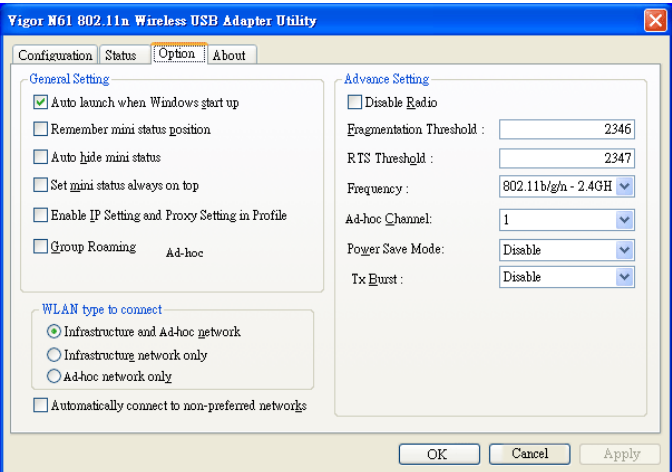
Operation Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

OK

5G

Available settings are explained as follows:

Item	Description
Operation Mode	<p>Mixed Mode – 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>Green Field – 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>
Channel Bandwidth	<p>20- the router will use 20MHz for data transmission and receiving between the AP and the stations.</p> <p>20/40 – 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 transmission.</p>
Guard Interval	<p>It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto 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.</p>

Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable .
Long Preamble	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 Enable to use Long Preamble if needed to communicate with this kind of devices.
Packet-OVERDRIVE	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). 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>Note: 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 Enable for TxBURST on the tab of Option).</p>  <p>Tx Burst : Disable Disable Enable</p> <p>Note: * 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.

4.11.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.

WMM Configuration | [Set to Factory Default](#) |

WMM Capable Enable Disable

APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable radio button.
APSD Capable	The default setting is Disable .
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	CWMin means contention Window-Min and CWMax 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.

Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. Note: Vigor2120 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	“Uncheck” (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. “Check” the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

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

4.11.9 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 APs in the neighborhood.

Access Point List

BSSID	Channel	SSID

See [Statistics](#).

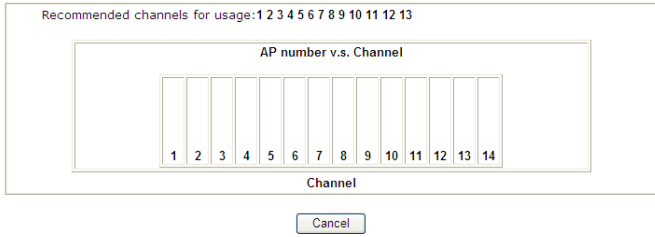
Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to [WDS Settings](#) :

AP's MAC address : : : : :

 Bridge Repeater

Available settings are explained as follows:

Item	Description
Scan	It is used to discover AP(s) in the neighborhood. The results will be shown on the box above this button.
Statistics	<p>It displays the statistics for the channels used by APs.</p> <p>Wireless LAN >> Site Survey Statistics</p> 
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 Add to . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

4.11.10 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.

Station List

Status	MAC Address	Associated with

Status Codes :
 C: Connected, No encryption.
 E: Connected, WEP.
 P: Connected, WPA.
 A: Connected, WPA2.
 B: Blocked by Access Control.
 N: Connecting.
 F: Fail to pass WPA/PSK authentication.

Note: After 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 : : : : :

Available settings are explained as follows:

Item	Description
Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into Access Control .

4.11.11 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect Vigor router. If such function is not enabled, the wireless client can connect Vigor router until the router shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

Note: Up to 300 Wireless Station records are supported by Vigor router.

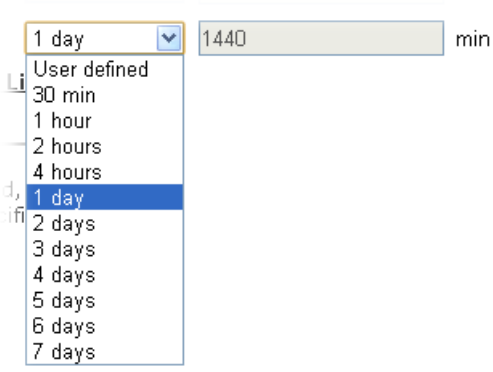
Wireless LAN (2.4 GHz) >> Station Control

SSID 1	SSID 2	SSID 3	SSID 4
SSID	DrayTek		
Enable	<input type="checkbox"/>		
Connection Time	1 hour	60	min
Reconnection Time	1 day	1440	min
Display All Station Control List			
WEB Portal Setup			

Note: Once the feature is enabled, the Internet accessibility will be restricted by the wireless station MAC address with the specific connection time.

OK Cancel

Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor router. Or, type the duration manually when you choose User defined . 
Display All Station Control List	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.
WEB Portal Setup	Click it to access in to LAN>>Web Portal Setup page for

modifying the settings if required.

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

4.12 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.



Wireless LAN (802.11n)
SSL VPN
General Setup
SSL Application
User Account
Online User Status
USB Application

4.12.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

SSL VPN General Setup

Port	<input type="text" value="443"/> (Default: 443)
Server Certificate	<input type="text" value="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 act on all SSL applications.

OK

Cancel

Available settings are explained as follows:

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in System Maintenance>>Management . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose Self-signed to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

Encryption Key Algorithm	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.

4.12.2 SSL Application

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

SSL VPN >> SSL Application

SSL Applications Profiles: [Set to Factory Default](#)

Index	Name	Host Address	Service	Active
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP or SAMBA path.
Service	Display the type of the service selected, e.g., VNC/RDP/SAMBA.
Active	Display current status (active or inactive) of the selected profile.

To create a new SSL application profile:

1. Click number link under Index filed to set detailed configuration.

SSL VPN >> SSL Application

SSL Applications Profiles:

Index	Name	Host
1.		
2.		
3.		
4.		

- The following page will appear.

SSL VPN >> SSL Application

Profile Index : 8

Enable Application Service

Application Name

Application Virtual Network Computing (VNC) ▾
---Please Select---
Virtual Network Computing (VNC)
Remote Desktop Protocol (RDP)

IP Address

Port

Idle Timeout second(s)

Scaling 100% ▾

Available settings are explained as follows:

Item	Description
Enable Application Server	Check the box to enable such profile.
Application Name	Type a name for such application. The length of the name is limited to 23 characters.
Application	<p>There are three types offered for you to create an application profile.</p> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;"> Virtual Network Computing (VNC) ▾ ---Please Select--- Virtual Network Computing (VNC) Remote Desktop Protocol (RDP) </div> <p>Virtual Network Computing (VNC) – It allows you to access and control a remote PC through VNC protocol.</p> <p>Remote Desktop Protocol (RDP) – It allows you to access and control a remote PC through RDP protocol.</p>
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
Screen Size	If you choose RDP, you have to choose the screen size for such application.

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

SSL Applications Profiles: [Set to Factory Default](#)

Index	Name	Host Address	Service	Active
<u>1.</u>	VNC_1	192.168.1.51:5900	VNC	v
<u>2.</u>				x
<u>3.</u>				x

4.12.3 User Account

With SSL VPN, Vigor2120 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, Vigor2120 series 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**.

Remote Access User Accounts: [Set to Factory Default](#)

Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???	<input type="checkbox"/>	---	<u>17.</u>	???	<input type="checkbox"/>	---
<u>2.</u>	???	<input type="checkbox"/>	---	<u>18.</u>	???	<input type="checkbox"/>	---
<u>3.</u>	???	<input type="checkbox"/>	---	<u>19.</u>	???	<input type="checkbox"/>	---
<u>4.</u>	???	<input type="checkbox"/>	---	<u>20.</u>	???	<input type="checkbox"/>	---
<u>5.</u>	???	<input type="checkbox"/>	---	<u>21.</u>	???	<input type="checkbox"/>	---
<u>6.</u>	???	<input type="checkbox"/>	---	<u>22.</u>	???	<input type="checkbox"/>	---
<u>7.</u>	???	<input type="checkbox"/>	---	<u>23.</u>	???	<input type="checkbox"/>	---
<u>8.</u>	???	<input type="checkbox"/>	---	<u>24.</u>	???	<input type="checkbox"/>	---
<u>9.</u>	???	<input type="checkbox"/>	---	<u>25.</u>	???	<input type="checkbox"/>	---
<u>10.</u>	???	<input type="checkbox"/>	---	<u>26.</u>	???	<input type="checkbox"/>	---
<u>11.</u>	???	<input type="checkbox"/>	---	<u>27.</u>	???	<input type="checkbox"/>	---
<u>12.</u>	???	<input type="checkbox"/>	---	<u>28.</u>	???	<input type="checkbox"/>	---
<u>13.</u>	???	<input type="checkbox"/>	---	<u>29.</u>	???	<input type="checkbox"/>	---
<u>14.</u>	???	<input type="checkbox"/>	---	<u>30.</u>	???	<input type="checkbox"/>	---
<u>15.</u>	???	<input type="checkbox"/>	---	<u>31.</u>	???	<input type="checkbox"/>	---
<u>16.</u>	???	<input type="checkbox"/>	---	<u>32.</u>	???	<input type="checkbox"/>	---

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

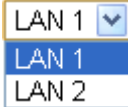
Click each index to edit one remote user profile.

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</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"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <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 IGMP,IP-Camera,DHCP Relay..etc.)</p> <hr/> <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> <hr/> <p>SSL VPN</p> <p><input type="button" value="Set SSL Application"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
--	--

Available settings are explained as follows:

Item	Description
User account and Authentication	<p>Enable this account - Check the box to enable this function.</p> <p>Idle Timeout- 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>
Allowed Dial-In Type	<p>PPTP - 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>IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.</p> <p>L2TP with IPSec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:</p> <ul style="list-style-type: none"> ● None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. ● Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

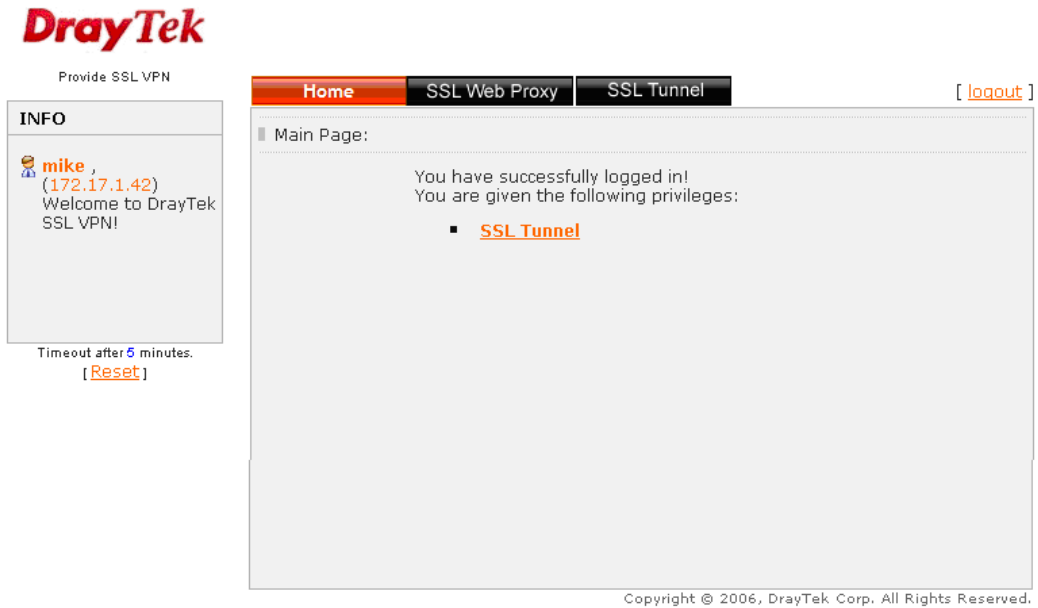
Item	Description
	<ul style="list-style-type: none"> ● Must -Specify the IPSec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p>Specify Remote Node - 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 general settings.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● 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. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● 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.
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p>  <p>Assign Static IP Address – Please type a static IP address for the subnet you specified.</p>
SSL VPN	Set SSL Application - Choose the SSL application profile to be applied by such dial-in user profile.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Enable Mobile One-Time Passwords (mOTP)	<p>Check this box to make the authentication with mOTP function.</p> <p>PIN Code – Type the code for authentication (e.g, 1234).</p> <p>Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
IKE Authentication	This group of fields is applicable for IPSec Tunnels and L2TP

Item	Description
Method	<p>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>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.</p> <p>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.</p>
IPSec Security Method	<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>Medium-Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.</p> <p>High-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> <p>Local ID - 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.

3.12.4 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
Kate	192.168.30.14	299	<input type="button" value="Drop"/>

Available settings are explained as follows:

Item	Description
Active User	Display current user who visit SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click Drop to drop certain login user from the router's SSL Portal UI.

4.13 USB Application

USB storage disk connected on Vigor router can be regarded as a server or WAN interface. 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.

Note: USB ports on Vigor router are allowed to connect to USB modem. Models of the modems supported by Vigor router can be seen from **USB Application>>Modem Support List**. For network connection via USB modem, refer to **WAN>>Internet Access** and **WAN>>General Setup** for detailed information.



4.13.1 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 Connections	<input type="text" value="5"/> (Maximum 6)
Default Charset	<input type="text" value="English"/>

Note: 1. If Charset is set to "English", only English long file name is supported.
 2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.

OK

Available settings are explained as follows:

Item	Description
General Settings	<p>Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.</p> <p>Default Charset - At present, Vigor router supports four types of character sets. Default Charset is for English based file name.</p>



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

4.13.2 USB User Management

This page allows you to set profiles for FTP 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 | [Set to Factory Default](#)

Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		

Click index number to access into configuration page.

USB Application >> USB User Management


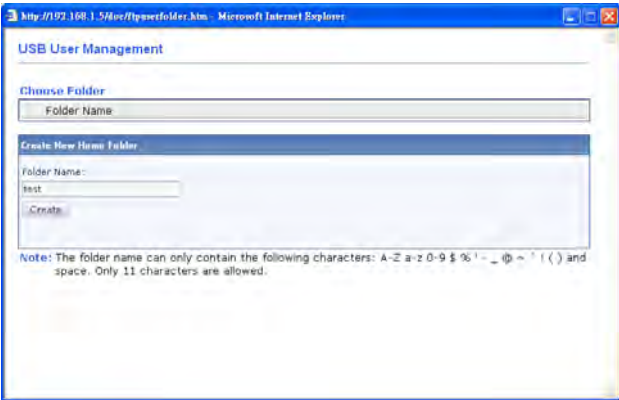
Profile Index: 1

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

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

Available settings are explained as follows:

Item	Description
FTP/Samba User	Enable – Click this button to activate this profile (account) for FTP service. Later, the user can use the username

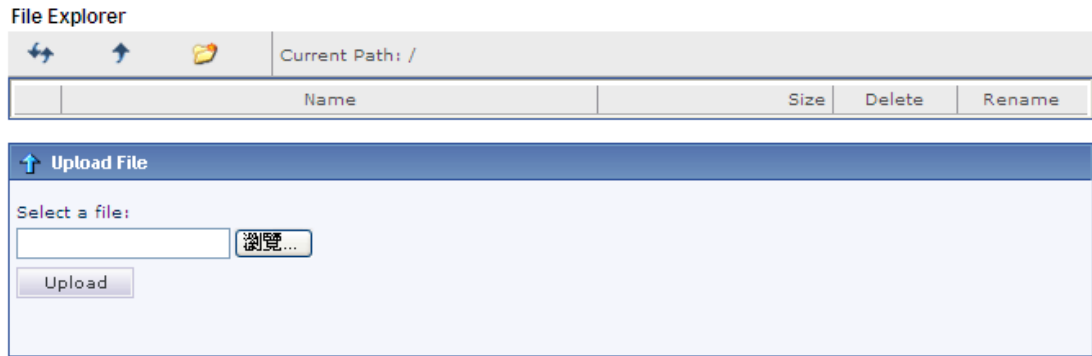
	<p>specified in this page to login into FTP server.</p> <p>Disable – Click this button to disable such profile.</p>
Username	<p>Type the username for FTP users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk. The length of the name is limited to 11 characters.</p> <p>Note: “Admin” could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.</p> <p>Note: FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.</p>
Password	<p>Type the password for FTP users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.</p>
Confirm Password	<p>Type the password again to make confirmation.</p>
Home Folder	<p>It determines the folder for the client to access into.</p> <p>The user can enter a directory name in this field. Then, after clicking OK, the router will create the specific/new folder in the USB storage disk. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB storage disk.</p> <p>Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. 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>The screenshot shows a web browser window titled "USB User Management" with two main sections. The "Choose Folder" section has a text input field labeled "Folder Name". The "Create New Home Folder" section has a text input field labeled "Folder Name" with the value "test" entered, and a "Create" button below it. A note at the bottom states: "Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' _ - ~ ^ ! () and space. Only 11 characters are allowed."</p>
Access Rule	<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>File – Check the items (Read, Write and Delete) for such profile.</p> <p>Directory –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.

4.13.3 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



Note: The folder can not be deleted when it is not empty.

Available settings are explained as follows:

Item	Description
 Refresh	Click this icon to refresh files list.
 Back	Click this icon to return to the upper directory.
 Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

4.13.4 USB Device 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 Device Status

Disk	Modem	Printer	Refresh
USB Mass Storage Device Status			
Connection Status: No Disk Connected			Disconnect USB Disk
Disk Capacity: 0 MB			
Free Capacity: 0 MB Refresh			
USB Disk Users Connected			
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Available settings are explained as follows:

Item	Description
Connection Status	If there is no USB storage disk connected to Vigor router, “ No Disk Connected ” will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click Refresh at any time to get new status for free capacity.
Index	It displays the number of the client which connecting to FTP server.
IP Address	It displays the IP address of the user’s host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

USB Application >> USB Device Status

Disk	Modem	Printer	Refresh
USB Mass Storage Device Status			
Connection Status: Disk Connected			Disconnect USB Disk
Write Protect Status: No			
Disk Capacity: 2009 MB			
Free Capacity: 925 MB Refresh			
USB Disk Users Connected			
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

4.13.5 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

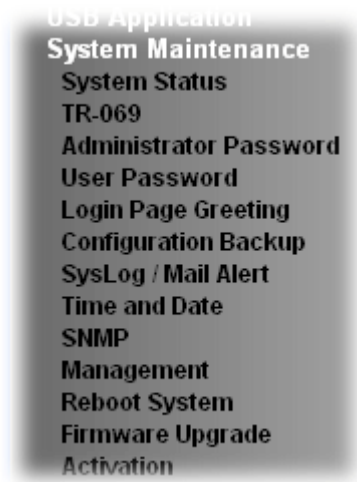
The following compatibility test lists 3.5G/LTE modems **supported by Vigor router under certain environment or countries**. If the LTE modem you have is on the list but cannot work properly, please write an e-mail to support@draytek.com or consult your dealer for further information.

PPP mode		DHCP mode	
Brand	Model	LTE	Status
Aiko	Aiko 83D		Y
Alcatel	Alcatel L100V		Y
Alcatel	Alcatel W100		Y
BandRich	Bandlux C170		Y
BandRich	Bandlux C270		Y
BandRich	Bandlux C321		Y
BandRich	Bandlux C330		Y
BandRich	Bandlux C502		Y
Huawei	Huawei E169u		Y
Huawei	Huawei E220		Y
Huawei	Huawei E3030		Y
Huawei	Huawei E3131		Y

4.14 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, SNMP, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.



4.14.1 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 : Vigor2120n+
Firmware Version : 3.7.5.1
Build Date/Time : Jul 31 2014 21:33:32

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-9C-F7-3C	192.168.1.3	255.255.255.0	No	8.8.8.8
LAN2	00-1D-AA-9C-F7-3C	192.168.2.1	255.255.255.0	Yes	8.8.8.8
IP Routed Subnet	00-1D-AA-9C-F7-3C	192.168.0.1	255.255.255.0	Yes	8.8.8.8

Wireless LAN			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-9C-F7-3C	Europe	2.7.1.5	DrayTek

Wireless LAN(5GHz)			
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-9C-F7-3E	Europe	2.7.1.5	DrayTek_5G

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-9C-F7-3D	---	---	---
WAN2	Disconnected	00-1D-AA-9C-F7-3E	---	---	---

IPv6			
	Address	Scope	Internet Access Mode
LAN	FE80::21D:A AFF:FE9C:F73C/64	Link	---

User Mode is OFF now.

Available settings are explained as follows:

Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	<p>MAC Address - Display the MAC address of the LAN Interface.</p> <p>IP Address - Display the IP address of the LAN interface.</p> <p>Subnet Mask - Display the subnet mask address of the LAN interface.</p> <p>DHCP Server - Display the current status of DHCP server of the LAN interface</p> <p>DNS - Display the assigned IP address of the primary DNS.</p>
WAN	<p>Link Status - Display current connection status.</p> <p>MAC Address - Display the MAC address of the WAN Interface.</p> <p>Connection - Display the connection type.</p> <p>IP Address - Display the IP address of the WAN interface.</p> <p>Default Gateway - Display the assigned IP address of the default gateway.</p>
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.</p> <p>Internet Access Mode – Display the connection mode chosen for accessing into Internet.</p>

4.14.2 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	Internet
ACS Server	
URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Test With Inform"/>	Event Code PERIODIC
Last Inform Response Time : (NA)	●
CPE Client	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
URL	<input type="text"/>
Port	8069
Username	vigor
Password	*****

Periodic Inform Settings

<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Interval Time	900 second(s)

STUN Settings

<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Server Address	<input type="text"/>
Server Port	3478
Minimum Keep Alive Period	60 second(s)
Maximum Keep Alive Period	-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	<p>URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.</p> <p>Test With Inform – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.</p> <p>Event Code – Use the drop down menu to specify an event</p>

	to perform the test. Last Inform Response Time – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Client	Such information is useful for Auto Configuration Server. Enable/Disable – Allow/Deny the CPE Client to connect with Auto Configuration Server. Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification.
STUN Settings	The default is Disable . If you click Enable , please type the relational settings listed below: Server IP – Type the IP address of the STUN server. Server Port – Type the port number of the STUN server. Minimum Keep Alive Period – 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”. Maximum Keep Alive Period – 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.

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

4.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>	
New Password	<input type="text"/>	(Max. 23 characters allowed)
Confirm Password	<input type="text"/>	(Max. 23 characters allowed)

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

Available settings are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is “ admin ”.

New Password	Type in new password in this field. The length of the password is limited to 23 characters.
Confirm Password	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

4.14.4 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="text"/>
Confirm Password	<input type="text"/>

Note: 1.Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()

2.Password can't be only *.Example: '*!' or '!***!' or '!***!' is illegal, but '!23*!' or '!*45!' is OK.

OK

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web use interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

Below shows an example for accessing into User Operation with User Password.

1. Open **System Maintenance>>User Password**.
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
Confirm Password

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

OK

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password

Active Configuration

Password	: *****
----------	---------

4. Log out Vigor router web user interface by clicking the Logout button.



5. The following window will be open to ask for username and password. Type the new user password in the field of **Password** and click **Login**.

DrayTek **Vigor2120 Series**

Login

Username

Password

Login

Copyright © 2013 DrayTek Corp. All Rights Reserved.

6. The main screen with User Mode will be shown as follows.

DrayTek Vigor2120 Series

Auto Logout IP6

Dashboard

System Information

Model Name	Vigor2120n+	System Up Time	174:11:48
Router Name		Current Time	2014 Jan 14 Tue 9:6:25
Firmware Version	3.7.5_RC2	Build Date/Time	Jan 3 2014 17:15:11
LAN MAC Address	00-1D-AA-9C-F7-34		

IPv4 Internet Access

	Line / Mode	IP Address	MAC Address	Up Time
WAN1	Ethernet / Static IP	172.16.3.130	00-1D-AA-9C-F7-35	171:50:47
WAN2	USB / ---	Disconnected	00-1D-AA-9C-F7-36	00:00:00

Interface

WAN	Connected : 1, <input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2
LAN	Connected : 0, <input checked="" type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4
WLAN	Connected : 0
WLAN5G	Connected : 0

System Resource

Current Status :	CPU Usage: 3%
	Memory Usage: 73%

Quick Access

- System Status
- Dynamic DNS

WLAN
LAN
NAT
Applications
Wireless LAN (2.4 GHz)
Wireless LAN (5 GHz)
System Maintenance
Diagnostics

All Rights Reserved.

User mode
Status: Settings Saved

WLAN
LAN4
LAN3
LAN2
LAN1
5G
2.4G
USB
ACT

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.

4.14.5 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](#) |

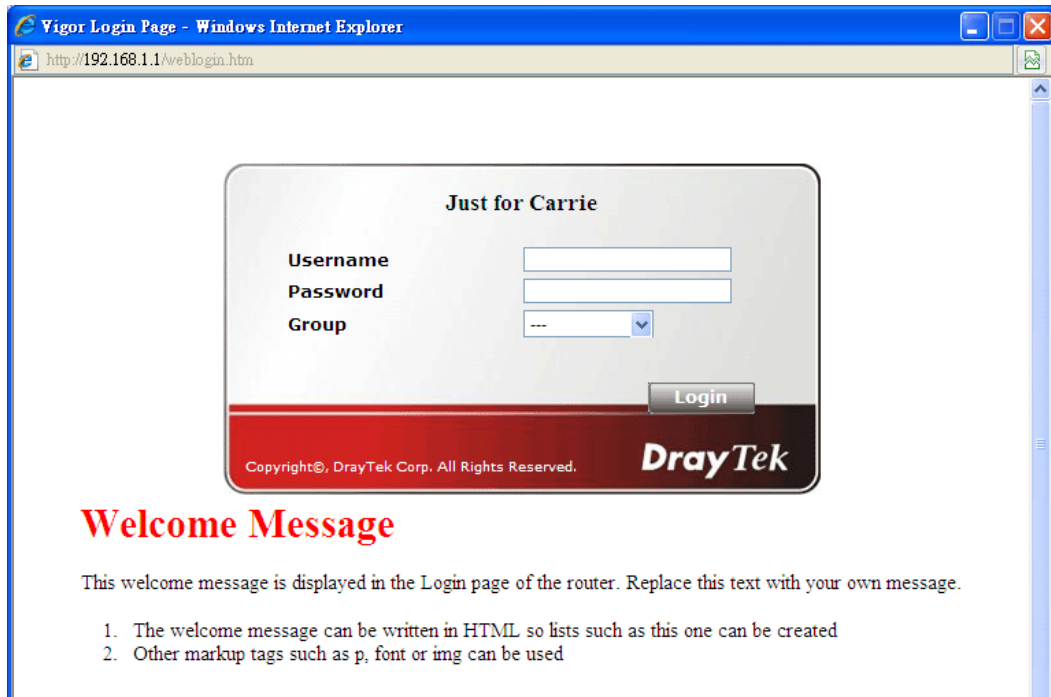
```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p><ol><li>The welcome message can be written in HTML so lists such as this one can be created </li><li>Other markup tags such as p, font or img can be used</li></ol>
```

Examples of Welcome Message and Bulletin:
 <h1>Welcome Message</h1>
 <p>Message</p>

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	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.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.



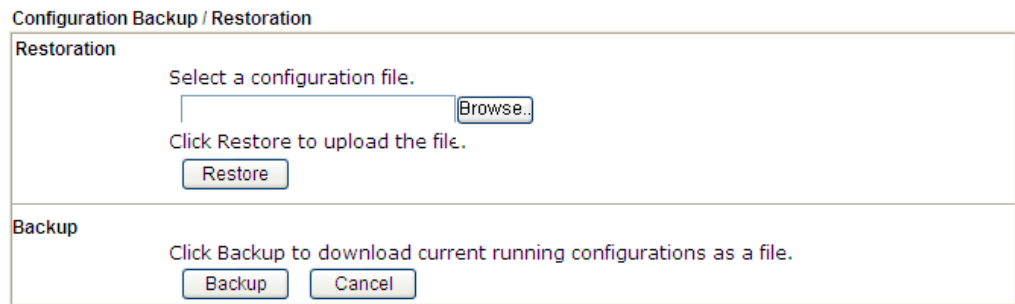
4.14.6 Configuration Backup

Backup the Configuration

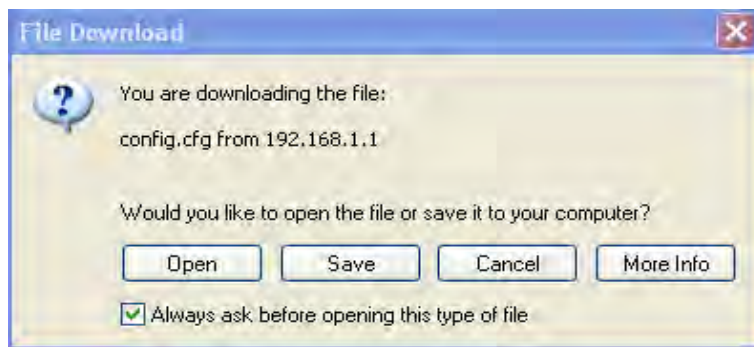
Follow the steps below to backup your configuration.

1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

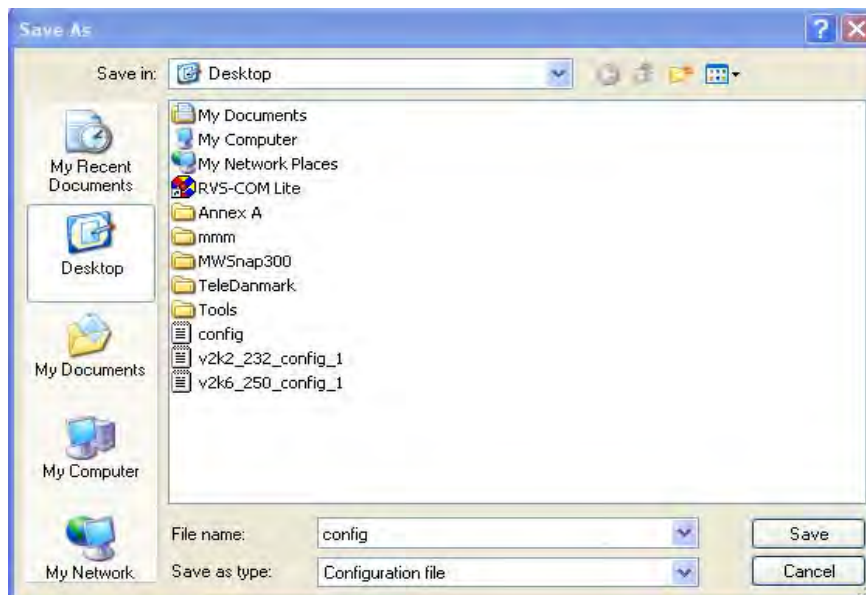
System Maintenance >> Configuration Backup



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

Configuration Backup / Restoration

Restoration

Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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.

4.14.7 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>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input type="text"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>SMTP Port <input type="text" value="25"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> VPN LOG</p>
--	---

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".
 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
 3. We only support secured SMTP connection on port 465.

Available settings are explained as follows:

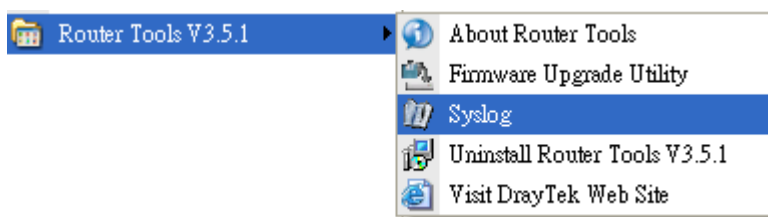
Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to – Check Syslog Server to save the log to Syslog server.</p> <p>USB Disk - Check USB Disk to save the log to the attached USB storage disk.</p> <p>Router Name - Display the name for such router configured in System Maintenance>>Management. If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>Mail Syslog – Check the box to recode the mail event on Syslog.</p> <p>Enable syslog message - Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.</p>

<p>Mail Alert Setup</p>	<p>Check Enable to activate function of mail alert.</p> <p>Send a test e-mail - 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>SMTP Server/SMTP Port - The IP address/Port number of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Return-Path - Assign a path for receiving the mail from outside.</p> <p>Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.</p> <p>Authentication - Check this box to activate this function while using e-mail application.</p> <ul style="list-style-type: none"> ● User Name - Type the user name for authentication. ● Password - Type the password for authentication. <p>Enable E-mail Alert - Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.</p>
--------------------------------	---

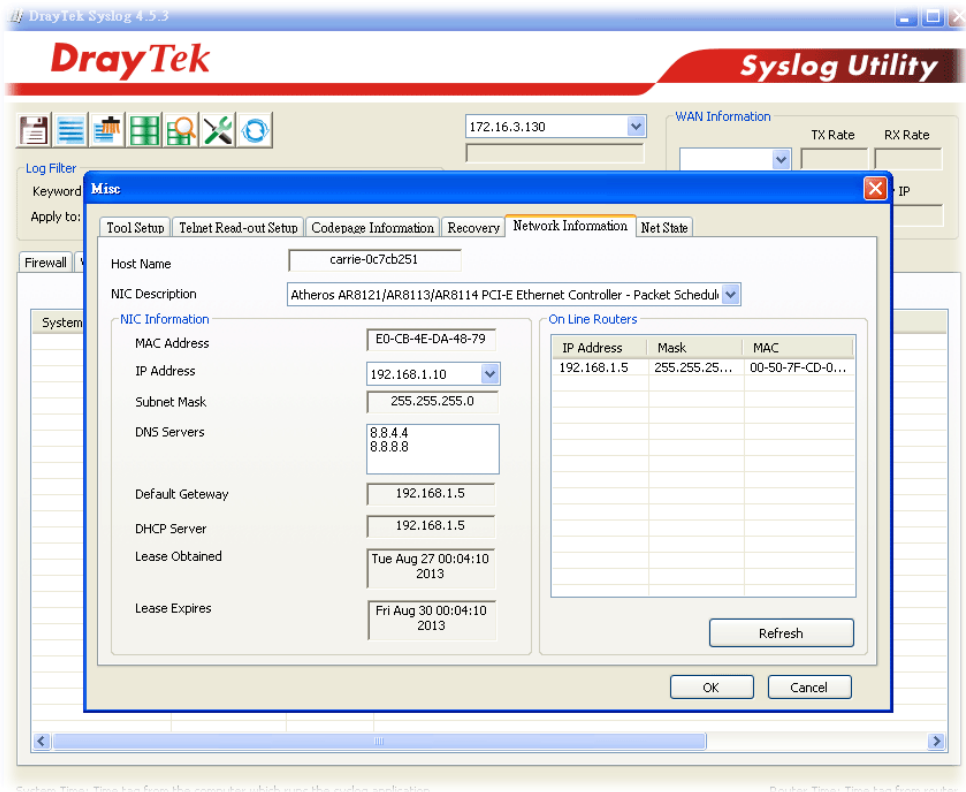
Click **OK** to save these settings.

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.



Custom Time: Time has from the computer which runs this custom application.

Default Time: Time has from router.

4.14.8 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

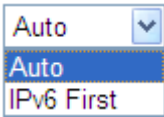
Current System Time	2013 Dec 19 Thu 7 : 2 : 29	Inquire Time
---------------------	----------------------------	--------------

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
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Server	Type the IP address or domain name of the time server.
Priority	<p>IPv6 First – If the time server configured with a domain name that supports IPv6; such option will be the first choice.</p> <p>Auto – It is the default setting. If you have no idea whether the time server supports IPv6 or IPv4, simply choose Auto as the priority.</p> 
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.14.9 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.

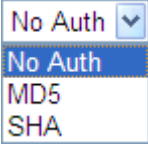
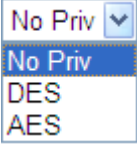
Applications >> SNMP

SNMP Setup

<input checked="" type="checkbox"/> Enable SNMP Agent	
Get Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
Manager Host IP(IPv4)	<input type="text"/>
Manager Host IP(IPv6)	<input type="text"/>
Trap Community	<input type="text" value="public"/>
Notification Host IP(IPv4)	<input type="text"/>
Notification Host IP(IPv6)	<input type="text"/>
Trap Timeout	<input type="text" value="10"/>
<input type="checkbox"/> Enable SNMPV3 Agent	
USM User	<input type="text"/>
Auth Algorithm	<input type="text" value="No Auth"/>
Auth Password	<input type="text"/>
Privacy Algorithm	<input type="text" value="No Priv"/>
Privacy Password	<input type="text"/>

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public . The maximum length of the text is limited to 23 characters.
Set Community	Set community by typing a proper name. The default setting is private . The maximum length of the text is limited to 23 characters.
Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public . The maximum length of the text is limited to 23 characters.
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.

Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. 
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

4.14.10 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												
Router Name <input type="text"/> <input type="checkbox"/> Default: Disable Auto-Logout Internet Access Control <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"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet Access List from the Internet <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"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports 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) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22) External Device Control <input checked="" type="checkbox"/> No respond to External Device
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"/>											

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	If it is enabled, the function of auto-logout for web user interface will be disabled.  The web user interface will be open until you click the Logout icon manually. 
Internet Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the

	<p>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>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</p>
Access List from the Internet	<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>List IP - Indicate an IP address allowed to login to the router.</p> <p>Subnet Mask - Represent a subnet mask allowed to login to the router.</p>
Management Port Setup	<p>User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
External Device Control	<p>No respond to External Device – Check the box to make Vigor2120 not being detected by other router and not being displayed as an external device.</p>

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

For IPv6

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
<p>Management Access Control</p> <p>Allow management from the Internet</p> <p><input type="checkbox"/> Telnet Server (Port : 23)</p> <p><input type="checkbox"/> HTTP Server (Port : 80)</p> <p><input type="checkbox"/> HTTPS Server (Port : 443)</p> <p><input type="checkbox"/> SSH Server (Port : 22)</p> <p><input type="checkbox"/> Enable PING from the Internet</p> <hr/> <p>Access List</p> <p>List IPv6 Address / Prefix Length</p> <p>1. <input type="text"/> / <input type="text" value="128"/></p> <p>2. <input type="text"/> / <input type="text" value="128"/></p> <p>3. <input type="text"/> / <input type="text" value="128"/></p> <p>Note : Telnet / Http server port is the same as IPv4.</p>	

OK

Available settings are explained as follows:

Item	Description
Management Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system

	<p>to allow you managing the router from Internet. Check the box(es) to specify.</p> <p>Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.</p>
Access List	<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>IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.</p>

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

4.14.11 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

Reboot Now

Auto Reboot Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

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.

4.14.12 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 (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.

未選擇檔案

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.5

Firmware Upgrade Procedures:


1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, 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 a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

4.14.13 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>.

System Maintenance >> Activation Activate via interface : auto-selected ▾

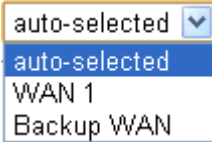
Web-Filter License [Activate](#)
 [Status:Not Activated]

Authentication Message

```
WebFilter, service not activate 2013-12-19 07:11:49
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
 If you change the service provider, the configuration of the function will be reset.

Available settings are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter. 
Activate	The Activate link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of web filter , the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation

Activate via interface: auto-selected ▾

Web-Filter License

[Activate](#)

[Status: **Commtouch**] [Start Date: **2011-03-28** Expire Date: **2011-04-27**]

```
Authentication Message
WebFilter, Activation authenticate fail, contact with support@draytek.com, 20
01 00:00:24
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

4.15 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.15.1 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
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

Available settings are explained as follows:

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

4.15.2 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
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
C~	192.168.1.0/ 255.255.255.0	directly connected LAN1

And,

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	Refresh		
Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN	U	256	
FF00::/8	LAN	U	256	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.15.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

Ethernet ARP Cache Table				Clear Refresh
IP Address	MAC Address	Netbios Name	Interface	
192.168.1.5	00-50-7F-CD-07-48		LAN1	
192.168.1.49	E0-CB-4E-DA-48-79	CARRIE-0C7CB251	LAN1	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.15.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Diagnostics >> View IPv6 Neighbour Table

IPv6 Neighbour Table			Refresh
IPv6 Address	Mac Address	Interface	
FF02::2	33-33-00-00-00-02	LAN	
FF02::1:3	33-33-00-01-00-03	LAN	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	
FF02::1	33-33-00-00-00-01	LAN	
FF02::1	00-00-00-00-00-00	USB2	
FF02::1:2	00-00-00-00-00-00	USB2	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.15.5 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
LAN1 : 192.168.1.1/255.255.255.0, DHCP server: On					
Index	IP Address	MAC Address	Leased Time	HOST ID	

Show Comment

And,

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table		DHCPv6 IP Assignment Table		Refresh
DHCPv6 server binding client:				
Index	IPv6 Address	MAC Address	Leased Time	

Show Comment

Available settings are explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.

Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

4.15.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

[Diagnostics](#) >> [NAT Sessions Table](#)

NAT Active Sessions Table | [Refresh](#) |

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
192.168.1.11 2491	52078	24.9.93.189 443	WAN1
192.168.1.11 2493	52080	207.46.25.2 80	WAN1
192.168.1.10 3079	52665	207.46.5.10 80	WAN1

Available settings are explained as follows:

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

4.15.7 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis

IPV4 IPV6
 Ping to: Host / IP
Host / IP
DNS
Gateway

Result | [Clear](#) |

And,

Diagnostics >> Ping Diagnosis

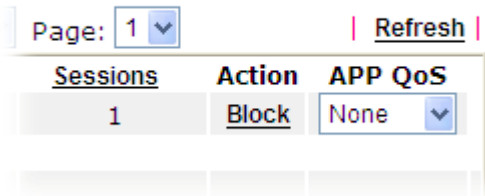
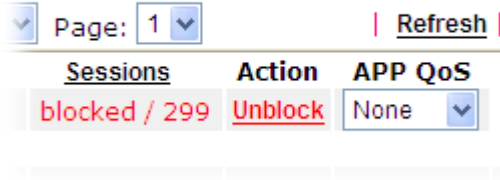
Ping Diagnosis

IPV4 IPV6
 Ping IPv6 Address:
Run

Result | [Clear](#) |

Available settings are explained as follows:

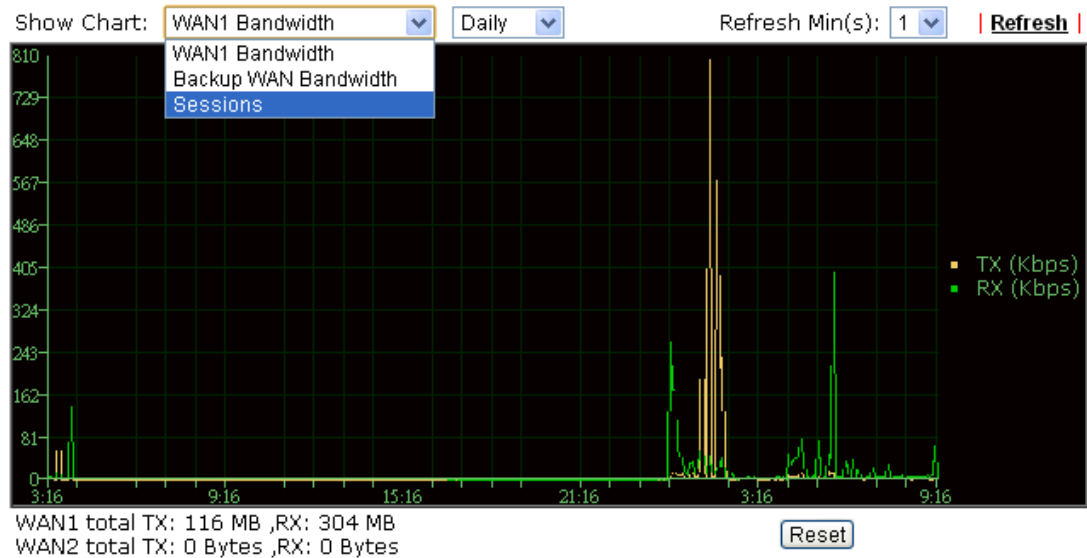
Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

	<p>automatically.</p> <p>Refresh Seconds: <input type="text" value="10"/> <input type="button" value="v"/> <input type="text" value="10"/> <input type="text" value="15"/> <input type="text" value="30"/></p>
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	<p>Block - can prevent specified PC accessing into Internet within 5 minutes.</p>  <p>Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.</p> 
Current /Peak/Speed	<p>Current means current transmission rate and receiving rate for WAN interface.</p> <p>Peak means the highest peak value detected by the router in data transmission.</p> <p>Speed means line speed specified in WAN>>General Setup. If you do not specify any rate at that page, here will display Auto for instead.</p>

4.15.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth, Backup WAN 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.

Diagnostics >> Traffic Graph



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1 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.

4.15.10 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

Protocol: ICMP ▾

Host / IP Address:

Result | [Clear](#) |

And,

Diagnostics >> Trace Route

Trace Route

IPV4 IPV6

Trace Host / IP Address:

Result | [Clear](#) |

Available settings are explained as follows:

Item	Description
IPv4 / IPv6	Click one of them to display corresponding information for it.
Protocol	Use the drop down list to choose the protocol that you want to ping through.

Host/IP Address	It indicates the IP address of the host.
Trace Host/IP Address	It indicates the IPv6 address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

4.15.11 System Explorer


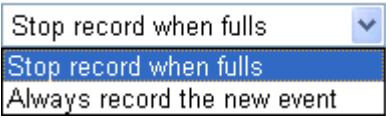
Such page provides real-time syslog and displays the information on the screen.

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.

Diagnostics >> Syslog Explorer

Available settings are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. 
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose.  Stop record when fulls – when the capacity of syslog is full, the system will stop recording. Always record the new event – only the newest events

	will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

USB Application >> Syslog Explorer

Web Syslog	USB Syslog
------------	------------

Note: The syslog will show while the saved syslog file size is over 1MB.

Folder: n/a File: n/a Page: n/a Log Type: n/a

Time	Log Type	Message
------	----------	---------

Available settings are explained as follows:

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

4.15.12 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.

Diagnostics >> IPv6 TSPC Status

WAN	Refresh
TSPC Disabled	

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

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

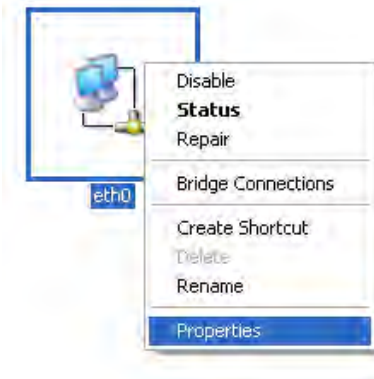


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

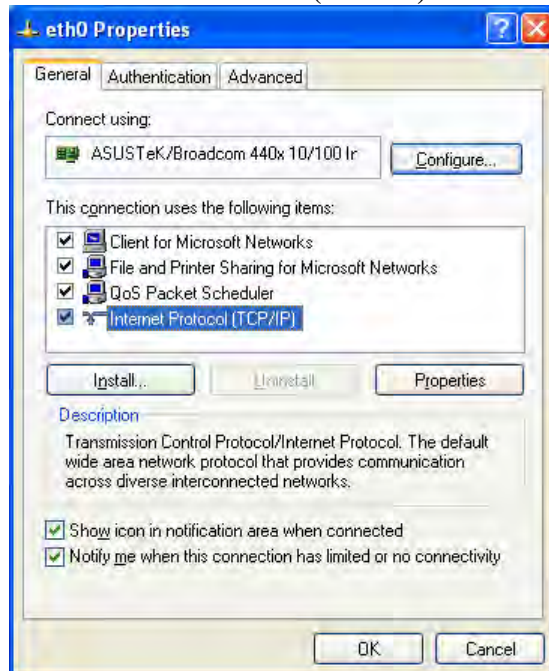
1. Go to **Control Panel** and then double-click on **Network Connections**.



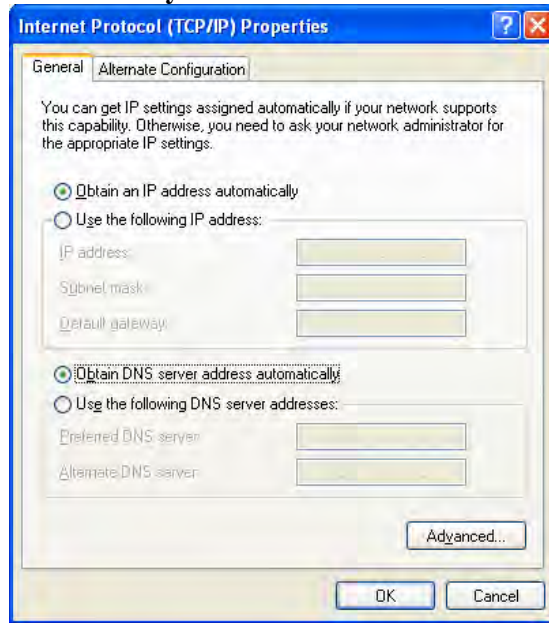
2. Right-click on **Local Area Connection** and click on **Properties**.



3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.

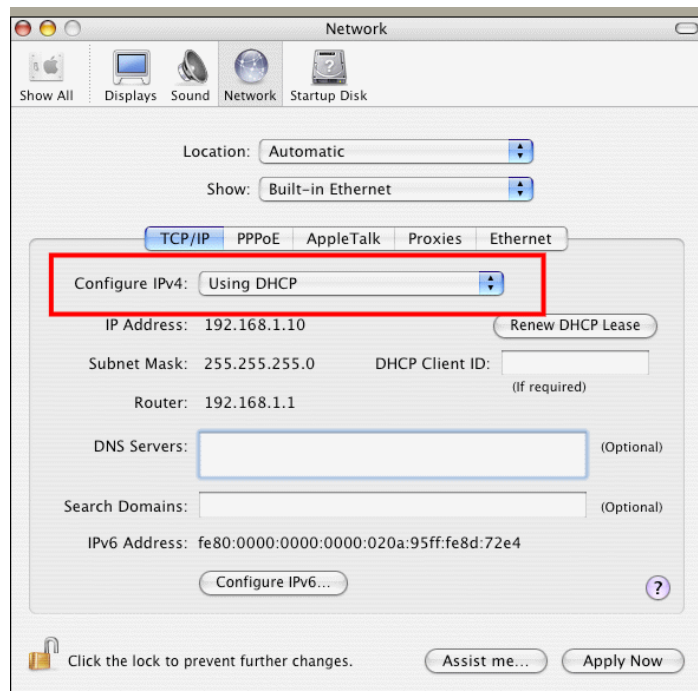


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



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.



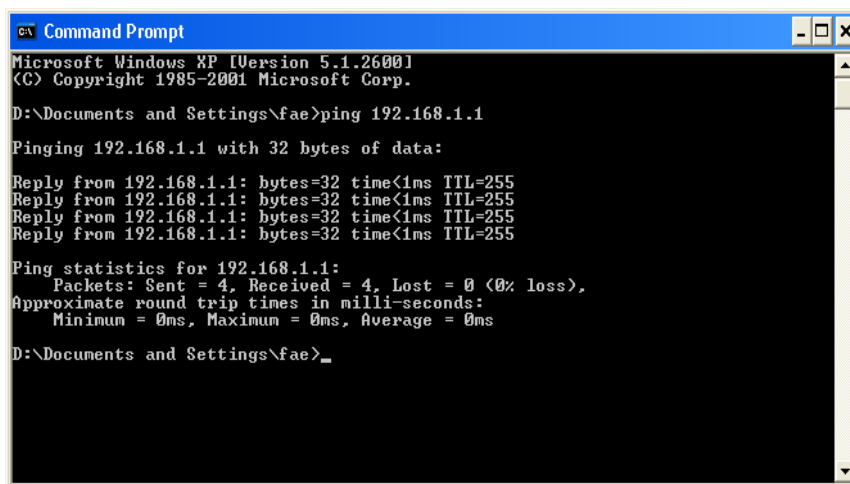
5.3 Pinging the Router from Your Computer

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.



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of “**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For Mac OS (Terminal)

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.

```

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-WAN2 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN2		USB	None PPPoE Static or Dynamic IP PPTP/L2TP	Details Page	IPv6

5.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2120. 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 Vigor2120.

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.

The screenshot shows the DrayTek Syslog Utility interface. At the top, there is a navigation bar with the DrayTek logo and the title 'Syslog Utility'. Below this, there are several icons and a dropdown menu showing the IP address '172.16.3.130'. The interface is divided into sections for 'Log Filter' (with a keyword field and an 'Apply to' dropdown set to 'All'), 'LAN Information' (with TX and RX packets fields), and 'WAN Information' (with TX and RX rates and WAN IP/Gateway IP fields). The main content area has tabs for 'Firewall', 'VPN', 'User Access', 'Connection', 'WAN', 'IPPBX', and 'Others'. The 'WAN' tab is active, and it contains a 'Show Syslog List' button and a 'Show Traffic Graph' button. Below these is a table with the following data:

System Time	Router Time	Host	Message
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: Session Usage: 123 (5 min average)
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: WAN1: Tx 81 Kbps, Rx 12 Kbps (5 min average)
2013-08-27 15:10:07	Aug 27 07:09:51	Vigor-router	[USB]Host Controller Driver: OTG
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=82 (in), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=01 (out), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Mass Storage device class
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface Class:SubClass:Protocol = [08:06:50]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface: 0
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Per-interface classes
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Device Class:SubClass:Protocol = [00:00:00]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]SerialNumber:[3] ED96E018
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Product:[2] Mass Storage
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Manufacturer:[1] Generic
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Usb new device: Vendor ID [058F], Product ID: [6387]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]num of interfaces=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb_set_configuration=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Usb Device Connected at Port 0

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 Vigor2120. 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(1-15) in Schedule Setup: , , ,

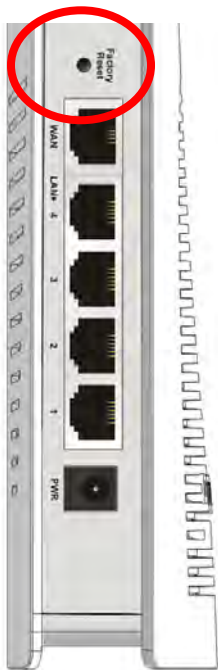
Note: Action and Idle Timeout settings will be ignored.

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 DrayTek

If the router still cannot work correctly after trying many efforts, please feel free to send e-mail to support@DrayTek.com.