



Your reliable networking solutions partner

User's Guide

Delight

V1.01

Vigor2760 Series VDSL2 Security Firewall User's Guide

Version: 1.01 Firmware Version: V3.7.5.1 (For future update, please visit DrayTek web site) Date: May 12, 2014



Copyright Information

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



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303Product:Vigor2760 Series Router

DrayTek Corp. declares that Vigor2760 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 the DSL and 2.4GHz/5GHz WLAN network throughout the EC region. Please see the user manual for the applicable networks on your product.

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.

RF Exposure Warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Caution

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

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

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







Table of Contents



Introduction	1
1.1 Features	2
1.2 Package and Content	4
1.3 LED Indicators and Connectors	5
1.3.1 For Vigor2760 1.3.2 For Vigor2760n 1.3.3 For Vigor2760Vn	7
1.4 Hardware Installation	11
1.5 Printer Installation	12
1.6 Accessing Web Page	20
1.7 Changing Password	21
1.8 Introducing Dashboard	22
1.8.1 Virtual Panel 1.8.2 Name with a Link	23
 1.8.3 Quick Access for Common Used Menu 1.8.4 GUI Map 1.8.5 Web Console 1.8.6 Config Backup 1.8.7 Logout 	25 26 27
1.9 Online Status	27
1.9.1 Physical Connection 1.9.2 Virtual WAN	27 30
1.10 Saving Configuration	31



Quick Setup	33
2.1 Quick Start Wizard	33
2.1.1 For WAN1 (ADSL/VDSL2) 2.1.2 For WAN2 (Ethernet) 2.1.3 For WAN3 (USB)	35
2.1.2 For WAN2 (Ethernet)	41
2.1.3 For WAN3 (USB)	50
2.2 Service Activation Wizard	52
2.3 VPN Client Wizard	56
2.4 VPN Server Wizard	62
2.5 Wireless Wizard	67
2.6 VoIP Wizard	
2.7 Registering Vigor Router	





Advanced Configuration	77
3.1 WAN	77
 3.1.1 Basics of Internet Protocol (IP) Network. 3.1.2 General Setup. 3.1.3 Internet Access 3.1.4 Multi-PVC. 	79 84
3.2 LAN	
3.2.1 Basics of LAN	
 3.2.2 General Setup	. 124 . 134 . 139 . 142 . 144
3.2.7 Web Portal Setup 3.3 Route Policy	
3.4 NAT	
3.4.1 Port Redirection 3.4.2 DMZ Host 3.4.3 Open Ports	. 156
3.4.4 Port Triggering	
3.5 Firewall	. 164
 3.5.1 Basics for Firewall 3.5.2 General Setup 3.5.3 Filter Setup 3.5.4 DoS Defense 	. 166 . 171
3.6 Objects Settings	. 183
3.6.1 IP Object 3.6.2 IP Group 3.6.3 IPv6 Object 3.6.4 IPv6 Group	. 186 . 188 . 190
3.6.5 Service Type Object 3.6.6 Service Type Group 3.6.7 Keyword Object 3.6.8 Keyword Group	. 193 . 195 . 197
3.6.9 File Extension Object 3.6.10 SMS/Mail Service Object 3.6.11 Notification Object	. 200 . 205
3.7 CSM Profile	
 3.7.1 APP Enforcement Profile	. 211 . 215 . 219
3.8 Bandwidth Management	. 221
3.8.1 Sessions Limit3.8.2 Bandwidth Limit3.8.3 Quality of Service3.8.4 APP QoS	. 223 . 225



3.9 Applications	. 236
3.9.1 Dynamic DNS 3.9.2 LAN DNS 3.9.3 Schedule	. 239
3.9.4 RADIUS	. 245
3.9.5 UPnP	
3.9.6 IGMP	
3.9.7 Wake on LAN 3.9.8 SMS / Mail Alert Service	
3.9.9 Bonjour.	
3.10 VPN and Remote Access	
3.10.1 Remote Access Control	
3.10.2 PPP General Setup 3.10.3 IPsec General Setup	
3.10.4 IPsec Peer Identity	
3.10.5 Remote Dial-in User	
3.10.6 LAN to LAN	
3.10.7 Connection Management	
3.11 Certificate Management	. 273
3.11.1 Local Certificate	
3.11.2 Trusted CA Certificate	
3.11.3 Certificate Backup	
3.12 VoIP	
3.12.1 DialPlan 3.12.2 SIP Accounts	
3.12.2 SIP Accounts	
3.12.4 Status	
3.13 Wireless LAN	
3.13.1 Basic Concepts	. 299
3.13.2 General Setup	. 301
3.13.3 Security	
3.13.4 Access Control.	
3.13.5 WPS 3.13.6 WDS	
3.13.7 Advanced Setting	
3.13.8 WMM Configuration	
3.13.9 AP Discovery	
3.13.10 Station List	
3.14 USB Application	
3.14.1 USB General Settings	
3.14.2 USB User Management	
3.14.3 File Explorer	
3.14.4 USB Device Status 3.14.5 Modem Support List	
3.15 System Maintenance	
3.15.1 System Status	
3.15.2 TR-069 3.15.3 Administrator Password	. 327 ຊາຍ
3.15.4 User Password	
3.15.5 Login Page Greeting	
3.15.6 Configuration Backup	
3.15.7 Syslog/Mail Alert	
3.15.8 Time and Date	



3.15.9 SNMP	339
3.15.9 SNMP 3.15.10 Management	
3.15.11 Reboot System	344
3.15.12 Firmware Upgrade	
3.15.13 DSL Firmware Upgrade	
3.15.14 Activation	
3.16 Diagnostics	
3.16.1 Dial-out Triggering	
3.16.2 Routing Table	
3.16.3 ARP Cache Table	350
3.16.4 IPv6 Neighbour Table	
3.16.5 DHCP Table	351
3.16.6 NAT Sessions Table	352
3.16.7 Ping Diagnosis	353
3.16.8 Data Flow Monitor	
3.16.9 Traffic Graph	356
3.16.10 Trace Route	357
3.16.11 Syslog Explorer	358
3.16.12 IPv6 TSPC Status	



Tutorials and Applications	.361
4.1 How to configure settings for IPv6 Service in Vigor2760	. 361
4.2 How can I get the files from USB storage device connecting to Vigor router?	. 373
4.3 How to Build a LAN-to-LAN VPN Between Remote Office and Headquarter via IPsec Tu (Main Mode)	
4.4 How to Optimize the Bandwidth through QoS Technology	. 379
4.5 QoS Setting Example	. 383
4.6 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection	. 388
4.7 How to Create an Account for MyVigor	. 392
4.7.1 Create an Account via Vigor Router 4.7.2 Create an Account via MyVigor Web Site	
4.8 How to Setup Address Mapping	. 400
4.9 How to Configure Certain Computers Accessing to Internet	. 402
4.10 How to Block Facebook Service Accessed by the Users via Web Content Filter / URL Content Filter	. 406



Trouble Shooting	
5.1 Checking If the Hardware Status Is OK or Not	411
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	412
5.3 Pinging the Router from Your Computer	415
5.4 Checking If the ISP Settings are OK or Not	416
5.5 Problems for 3G Network Connection	416



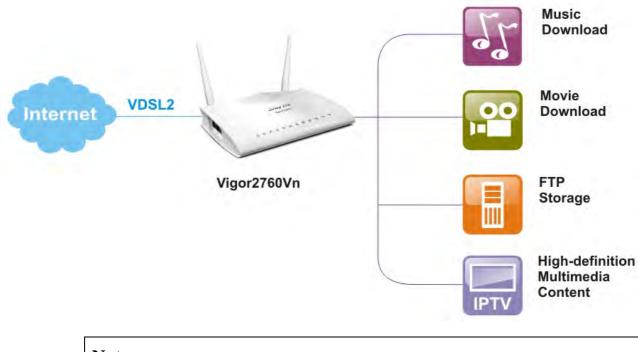
5.6 Backing to Factory Default Setting If Necessary	····· ·	417
5.7 Contacting DrayTek		418



Vigor2760 series is a VDSL2 router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

With the development of NGN (Next Generation Network), you may recently hear the news about FTTx deployment in your local area or even have already subscribed the unbundling last mile service (e.g. VDSL2) from local ITSP for FTTx. As adopting FTTx, the main question for end users is whether your legacy router could fully utilize its bandwidth or not.

DrayTek launches Vigor 2760 series – High speed router, perfectly complied with VDSL2 environment including Vigor2760, Vigor2760n and Vigor2760Vn for speed-wanted customers. With high throughput performance and secured broadband connectivity provided by Vigor 2760 series, you can simultaneously engage these bandwidth-intensive applications, such as high-definition video streaming, online gaming, and Internet telephony / access.



Note: This manual is written based on the standard firmware version of Vigor2760 series and suitable for all of the countries except for UK area. For product enquiries in the UK, Ireland and Channel Islands, please contact the UK office.

DrayTek UK Office

Sales Tel: 020 8381 5500

Email: info@draytek.co.uk



1.1 Features

ADSL2/2+ &	Compliant with ITU-T G.993.2 & G.997.1
VDSL2	Support Band Plan 998 & 997
	Support Annex A / Annex B
	VDSL2 Profile 8a/8b/8c/8d/12a/12b/17a/30a
	Capability Fall-back to ADSL2/2+
	Multi-VLAN
	Multi-PVC
Internet	Support IPv4 & IPv6
	Support PPPoE/PPPoA
	Support DHCP/Static IP
	Internet connection over 3G/4G USB Dongle
	Multi-VLAN/Multi-PVC for triple play
VPN	2 VPN Tunnels
	Built-in PPTP/L2TP/IPsec VPN server
	VPN Passthough (PPTP/L2TP/IPsec)
	IPsec Main/Aggressive Mode
	IKE Authentication (PSK & X.509)
	PPTP MPPE
	L2TP over IPsec
Security	Object-based Firewall
	MAC Address Filter
	SPI (Stateful Packet Inspection)
	DoS/DDoS Prevention
	IM/P2P Applications Filter
	URL Content Filter
	Global View Web Content Filter
	Bind IP to MAC
NAT/Routing	DMZ Host
	Port Forwarding & Redirection
	Route Policy
	Static Route
	RIPv2
Network Feature	• Two subnets(VLAN)
	LAN Port Mirror
	Bandwidth/Session Management
	• QoS by IP, Port, Applications
	• Dynamic DNS
	LAN DNS
	• UPnP
	 IGMP proxy & snooping Wake on LAN
	• Wake on LAN
	• Bonjour



Sharing
Sharing
erver for File Sharing by a USB Memory Stick/USB
with FAT32 Format
yslog
HTTPS User Interface
ver Telnet/SSH/Web UI
uration Backup/Restore
istrator Access Control
ted User Mode
Aonitor
n Diagnostic Function
/SMS Alert
v1/v2c
9 (Compliance with VigorACS SI)
rt 2T2R 2.4GHz, Single Band
02.11n Compliant
-bit WEP, WPA/WPA2
Wireless Distribution System)
Address Access Control
ss Client List
Point Discovery
n SSID
le SSID
ol: SIP, RTP/RTCP
Registrars
Line Echo-cancellation
Status
Loop Through
Features :
δ.711 A/μ law δ.723.1
3.726
3.729 A/B
/AD/CNG
Relay :
n Band
Out Band (RFC-2833)
IP Info
Aodem Support :
3.711 Pass-through
38 for fax Sending/Receiving
mental Services :
Call Hold/Retrieve
Call Waiting
LIR (Calling Line Identification Restriction)

-

- Call Barring (Incoming / Outgoing)
- ➤ Hotline
- DND (Do Not Disturb)
- ➢ Call Transfer
- MWI (Message Waiting Indicator) (RFC-3842)

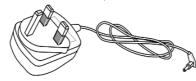
Note: If you are using Linux-platform firmware and plan to upgrade DrayOS-platform, please feel free to contact <u>support@draytek.com</u> to assure your expected features can be performed.

1.2 Package and Content

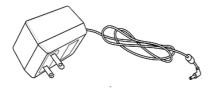




The type of the power adapter depends on the country that the router will be installed. * The maximum power consumption is *17-23 Watt*.



UK-type Power Adapter



USA/Taiwan-type Power Adapter



EU-type Power Adapter

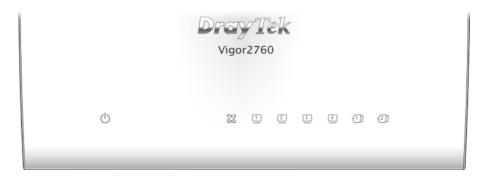


AU/NZ-type Power Adapter

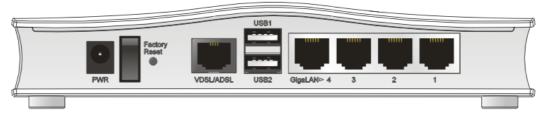
1.3 LED Indicators and Connectors

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

1.3.1 For Vigor2760



LED	Status	Explanation
(¹)	Blinking	The router is powered on and running normally.
(ACT)	Off	The router is powered off.
72	On	The DSL port is connected.
DSL (Green)	Blinking (Slowly)	The router is ready.
	Blinking (Quickly)	The connection is training.
	On (Green)	The port is connected.
LAN1/2/3/4	Blinking (Green)	The data is transmitting.
-(1)] ~ -(2)]	On	A USB device is connected and active.
USB1/2		

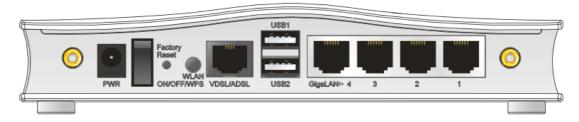


Interface	Description
PWR	Connector for a power adapter.
I / O	Power switch.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
VDSL/ADSL	Connector for accessing the Internet.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
LAN (1-4)	Connectors for local network devices.

1.3.2 For Vigor2760n

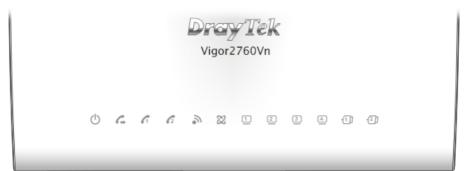
	Dray Tek Vigor2760n	
Ċ		

LED	Status	Explanation
(¹)	Blinking	The router is powered on and running normally.
(Activity)	Off	The router is powered off.
2	On (Green)	The wireless access point is ready.
(Wireless LAN	Blinking (Green)	The data is transmitting via wireless connection.
On/Off/WPS)	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
	Off	The wireless access point is turned off.
72	On	The DSL port is connected.
DSL (Green)	Blinking (Slowly)	The router is ready.
	Blinking (Quickly)	The router is trying to connect to Internet.
1~4	On	The port is connected.
LAN1/2/3/4	Blinking (Green)	The data is transmitting.
-(1) ~ -(2)	On	A USB device is connected and active.
USB1/2		

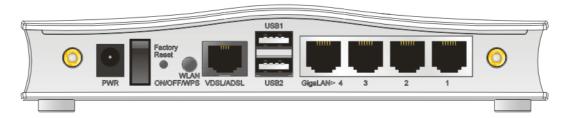


Interface	Description
PWR	Connector for a power adapter.
Ι/Ο	Power switch.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WLAN ON/OFF/WPS	WLAN WPS - Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on.
	WLAN ON/OFF - Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
VDSL/ADSL	Connector for accessing the Internet.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
LAN (1-4)	Connectors for local network devices.

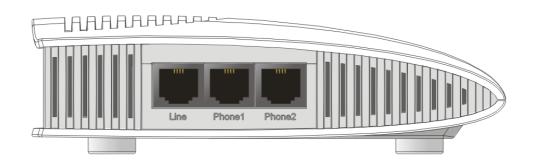
1.3.3 For Vigor2760Vn



LED	Status	Explanation
(b)	Blinking	The router is powered on and running normally.
(ACT)	Off	The router is powered off.
G	On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off for awhile.
(LINE)	Off	There is no PSTN phone call.
66	On	The phone connected to this port is off-hook.
€1 €2	Off	The phone connected to this port is on-hook.
(Phone1/Phone2)	Blinking	A phone call comes.
2	On (Green)	The wireless access point is ready.
(Wireless LAN	Blinking (Green)	The data is transmitting via wireless connection.
On/Off/WPS)	Blinking (Orange)	Blinks with one second cycle for two minutes. The WPS function is active.
	Off	The wireless access point is turned off.
247	On	The DSL port is connected.
DSL (Green)	Blinking (Slowly)	The router is ready.
	Blinking (Quickly)	The router is trying to connect to Internet.
	On	The port is connected.
LAN1/2/3/4	Blinking (Green)	The data is transmitting.
-(1) ~ -(2)	On	A USB device is connected and active.
USB1/2		



Interface	Description
PWR	Connector for a power adapter.
I / O	Power switch.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WLAN ON/OFF/WPS	 WLAN WPS - Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS connection will be on. WLAN ON/OFF - Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
VDSL/ADSL	Connector for accessing the Internet.
USB (1-2)	Connector for USB storage device (Pen Driver/Mobile HD) or printer or 3G backup.
LAN (1-4)	Connectors for local network devices.



Interface	Description
LINE	Connector for PSTN life line.
Phone1/Phone2	Connector of analog phone for VoIP communication.

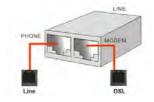




1.4 Hardware Installation

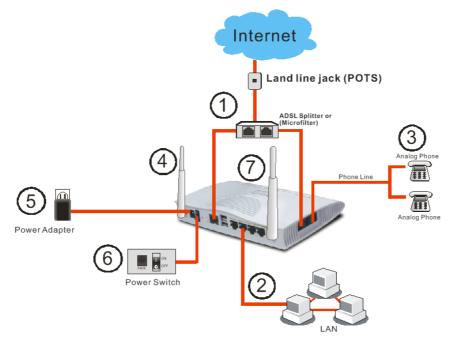
Before starting to configure the router, you have to connect your devices correctly.

1. Connect the xDSL interface to the external XDSL splitter with an XDSL line cable for all models. For Vigor2760Vn, also connect Line interface to external XDSL splitter.



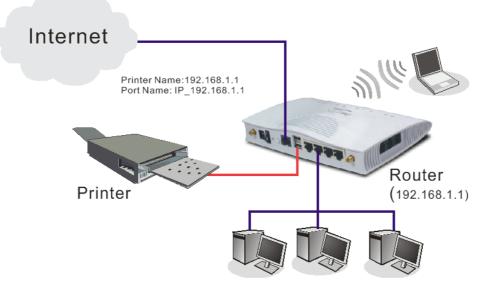
- 2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
- 3. Connect Phone port to a conventional analog telephone (for V model only).
- 4. Connect detachable antennas to the router for Vigor2760 series (for n model only).
- 5. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
- 6. Power on the router.
- 7. Check the ACT and DSL, LAN LEDs to assure network connection.

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



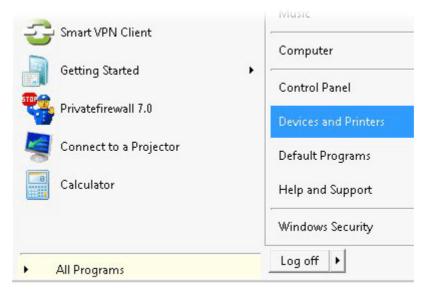
1.5 Printer Installation

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 7. For installation on other Windows systems, please visit **www.DrayTek.com**.

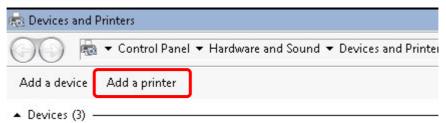


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

- 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.

/ =	Add Printer t type of printer do you want to install?
•	Add a local printer Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)
•	Add a network, wireless or Bluetooth printer
	Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

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**.

Add Printer		
🖶 Add Printer		
Choose a printer port		
A printer port is a type of con	nection that allows your computer to exchange informatio	n with a printer.
○ Use an existing port:	LPT1: (Printer Port)	
• Greate a new part. Type of port:	Standard TCP/IP Port	
Type of port.	Journal a rol Jarron	
	Ne	d Cance

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**.

Type a printer hostname or IP	P address	
Device type:	TCP/IP Device	
Hostname or IP address:	192.168.1.1	
Port name:	192.168.1.1	

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

n	
🖶 Add Printer	
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.	
 The device is properly configured. The address on the previous page is correct. 	
. The address on the previous page is contect.	
If you think the address is not correct, click Back to re	
If you think the address is not correct, click Back to re address and perform another search on the network.	
If you think the address is not correct, click Back to re	
If you think the address is not correct, click Back to re address and perform another search on the network. device type below.	If you are sure the address is correct, select th
If you think the address is not correct, click Back to re address and perform another search on the network. device type below.	
If you think the address is not correct, click Back to re address and perform another search on the network. device type below.	If you are sure the address is correct, select th
If you think the address is not correct, click Back to re address and perform another search on the network. device type below. Device Type © Standard Generic Network Card	If you are sure the address is correct, select th
If you think the address is not correct, click Back to re address and perform another search on the network. device type below. Device Type © Standard Generic Network Card	If you are sure the address is correct, select th

8. 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**.

Install th	he printer driver					
17	Choose your print	er from the	list. Click Wi	ndows Update to se	e more mod	els.
S	T					
	To install the drive	er from an ir	istallation CL	, click Have Disk.		
	fuctorer		Deintere			
Brothe	er		🖏 Brother D	CP-116C		
Canor	1		🔄 Brother D	CP-117C		
DrayT	ek		🔄 Brother D	CP-128C		
Epson			🔄 Brother D			
Fuii Xe	erox	<u> </u>	🗔 Brother D	CP-130C		<u>•</u>
📷 Th	nis driver is digitally si	ianed.		Windows Up	odate	Have Disk
	II me why driver sign		rtant			
10	in the only ander sign	ing is impo	rearre			

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

n Add Printer					
🗿 🖶 Add Pri	ter				
Type a print	er name				
Printer nam	::	ner DCP-116C		 	
This printer	will be installed w	vith the Brother DCF	-116C driver.		
					<u> </u>
				Next	Cance

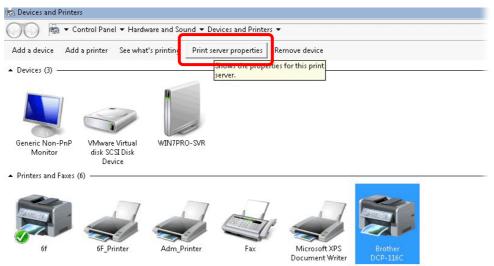
10. Choose **Do not share this printe**r and click **Next**.

Printer Sharing				
(f you want to share th				suggested name o
type a new one. The s	hare name will be vis	ible to other netwo	'k users.	
O not share this p	orinter			
C Share this printer :	o that others on your	r network can find a	nd use it	
Share name:				
Location:				
Comment:				

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

# A	Add Printer	>
0	🖶 Add Printer	
	You've successfully added Brother DCP-116C	
	Set as the default printer	
	To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.	
	Print a test page	
	Finish Cancel	

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.

Port Description Printer TS002 Inactive TS Port TS001 Inactive TS Port TPVM: ThinPrint Print Port fo 172.16.2.2 Standard TCP/IP Port 6f LPR_local Standard TCP/IP Port Adm_Printer LPR_local Standard TCP/IP Port 192.168.1.1 Standard TCP/IP Port Brother DCP-116C XPSPort: Local Port	Ports on this	1	1
I DR. Jocal Standard TCP/IP Port 6E Printer 192.168.1.1 Standard TCP/IP Port Brother DCP-116C	TS002 TS001 TPVM:	Inactive TS Port Inactive TS Port ThinPrint Print Port fo	
APSPort: Local Port Microsoft APS Document Writer	1 PB_local 192.168.1.1	Standard TCP/IP Port Standard TCP/IP Port	6E_Drinter Brother DCP-116C
Add Port Delete Port Configure Port	1	1	

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.

	-				
	Configure Standard TCP/IF	' Port Monit	or		
F	Port Settings				
j.	Port Name:		192.168.1.1		
ſ	Printer Name or IP Add	lress:	192.168.1.1		
	Protocol		,		
	C Raw			€ LPR	
	Raw Settings]
	Port Number:	9100			
	LPR Settings				
-	Queue Name:	рЦ			
	🔲 LPR Byte Countin	g Enabled			
	SNMP Status Enal	bled —			
	Community Name:	public	6		
_	SNMP Device Index:	1			

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



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

About DrayTek Pro	ducts Supports Solutions Multi-Media Demo Contact Us Q Search	
AQ / Application	You are here: Home + Supports + FAQ / Application Notes + Printer Server	
Latest EAO/Application		D
USB		
Printer Server		
3G/4G Internet		
Connection		
	hat types of printers are compatible with Viger rout.	ne link
	hat types of printers are compatible with Vigor rout	er? link.
n, click the W	hat types of printers are compatible with Vigor routo	e r ? link.
n, click the W		er?link. ₅
n, click the W		er? link. ₪
n, click the W Q / Application est FAQ/Application sic	You are here: Home > Supports > FAQ / Application Notes > Printer Server	er? link. ₪
n, click the W Q / Application test FAQ/Application	You are here: Home > Supports > FAQ / Application Notes > Printer Server	er? link. ₪ 2012/01/12
n, click the W Q / Application est FAQ/Application sic rmware Upgrade	You are here: Home + Supports + FAQ / Application Notes + Printer Server Printer Server	5
n, click the W Q / Application est FAQ/Application sic rmware Upgrade	You are here: Home + Supports + FAQ / Application Notes + Printer Server Printer Server What types of printers are compatible with Vigor router?	S 2012/01/12

1.6 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.

Dray Tek	Vigor2760 Series
Login	
Username Password	admin ••••• Login
	oyright © 2013 DrayTek Corp. All Rights erved.

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.

Dray Tek	Vigo	r2760 Serie	95			1 111	🗄 🕞 Deligh
Auto Logout 💌 🛛 🛛 🛛 🖉	Dashboar	rd					
Dashboard Wizards Online Status WAN LAN Route Policy		<u> </u>	A 4		-Vn	0 0 0	ді <i>(</i> Ді
NAT Firewall Objects Setting CSM Bandwidth Management	System I Model Na Router Na		IVn	System Up Time	1:3:22 2000 Jap 1	. Sat 1:3:20	Quick Access System Status Dynamic DNS
Applications VPN and Remote Access Certificate Management VoIP	Firmware DSL Versi	Version 3.7.5.1	-04-00-01	Build Date/Time	Mar 31 201	14 10:02:56	TR-069 IM-P2P Block Schedule
Wireless LAN USB Application	IF V4 INLE	Line / Mode	IP Address	MAC Addres	s	Up Time	SysLog / Mail Alert RADIUS
System Maintenance	WAN1	ADSL / PPPoA	Disconne			00:00:00	Firewall Object Setting
Diagnostics	WAN2	Ethernet /	Disconne	cted 00-1D-AA-B	38-15-02	00:00:00	Data Flow Monitor
	WAN3	USB /	Disconne	cted 00-1D-AA-8	38-15-03	00:00:00	
Support Area							
Product Registration	IPv6 Inte	rnet Access	1.4.44		10		
	LAN	Mode RADVD / DHCPv6	Address	FF:FEB8:1500/64	Scope Link	Up Time	
All Rights Reserved.	LAN	TRADVD / DHCPV6	FE80::210:AA	FF:FEB8:1000/64	Link		1
	Interface						1
	DSL		n Stream : OKb	os / Up Stream : OKb	ps		1
	WAN	Connected : 0,	WAN1 WA				1
	CI LAN	Connected : 0,	LAN1 CLAM	12 @LAN3 @LA	NA.		1

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

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

Auto Logout 💌	
Auto Logout	
Off	
1 min	
3 min	9 F
5 min	91
10 min	

1.7 Changing Password

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

- 1. Open a web browser on your PC and type http://192.168.1.1. A pop-up window will open to ask for username and password.
- 2. Please type "admin/admin" as Username/Password for accessing into the web user interface with admin mode.
- 3. Go to System Maintenance page and choose Administrator Password.



System Maintenance >> Administrator Password Setup

Administrator Password		
Old Password		
New Password		(Max. 23 characters allowed)
Confirm Password		(Max. 23 characters allowed)
Note: Password can contain only a	a-z A-Z O-9 , ; : . " < :	> * + = \ ? @ # ^ ! ()

	_
OK	

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

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

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

DrayTek Vigor2760 Series
Login
Username admin Password •••••
Login
Delight Copyright © 2013 DrayTek Corp. All Rights Reserved.

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

1.8 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:

ashboar	d							
		<u> </u>	C	6	Drey Te Vigor2760	~~	• • •	
						_		
	nformati							Quick Access
todel Na		Vigor2760	vn		rstem Up Time Irrent Time	1:3:22	Sat 1:3:20	System Status
	Version	2751			ild Date/Time		4 10:02:56	Dynamic DNS TR-069
SL Versi		05-04-04-	04-00-01		N MAC Address	00-1D-AA-8	8-15-00	IM/P2P Block Schedule SysLog / Mail Alert
	Line / M		IP /	Address	MAC Address		Up Time	RADIUS
				sconnected	00-1D-AA-B	-	00:00:00	Firewall Object Setting
WAN1	ADSL /	PPPoA						Data Flow Monitor
WAN1 WAN2	ADSL / Etherne			sconnected	00-1D-AA-B	8-15-02	00:00:00	
-		et /	Dis	sconnected sconnected	00-1D-AA-8 00-1D-AA-8		00:00:00 00:00:00	Data Pion Monitor
WAN2 WAN3	Etherne USB / -	et / 	Dis					
WAN2 WAN3	Etherne	et / 	Dis	sconnected		8-15-03	00:00:00	
WAN2 WAN3 V6 Inte	Etherno USB / - ernet Acc Mode	et / :ess	Address	sconnected	00-1D-AA-B	8-15-03 Scope		
WAN2 WAN3 Pv6 Inte	Etherni USB / - ernet Acc Mode RADVD	et / :ess	Address	sconnected		8-15-03	00:00:00	
WAN2 WAN3 Pv6 Inte	Etherne USB / - ernet Acc Mode RADVD	et / cess / DHCPv6	Address FE80::2	sconnected 21D:AAFF:FE	00-1D-AA-B B8:1500/64	8-15-03 Scope Link	00:00:00	
WAN2 WAN3 Pv6 Inte	Etherne USB / - ernet Acc Mode RADVD	et / cess / DHCPv6 cted : Down	Address FE80::2	sconnected 21D:AAFF:FE	00-1D-AA-B	8-15-03 Scope Link	00:00:00	

1.8.1 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.



The LED lights or blinks according to the physical connection on the router. For detailed information about the LED display, refer to **1.2 LED Indicators and Connectors**.

1.8.2 Name with a Link

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

System Informati Model Name	Vigor2760n		System Up Time	117:48:57
Router Name			Current Time	2014 Jan 21 Tue 3:50:10
Firmware Version	3.7.5_RC1		Build Date/Time	Dec 31 2013 15:53:08
DSL Version			LAN MAC Address	00-1D-AA-A9-5E-58
IPv4 Internet Acc	ess			



1.8.3 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								
DSL	Connected : Do [.]	Connected : Down Stream : OKbps / Up Stream : OKbps						
WAN	Connected : 1,	WAN1	WAN2	WAN3				
AN I	Connected : 0,	LAN1	LAN2	LAN3	LAN4			
VLAN	Connected : O							
USB	Connected : 0,	OUSB 1						
	U, U,	OUSB 2						
Security								

security			
📑 VPN	Connected : O	<u>Remote Dial-in User</u> /	LAN to LAN

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

Security					
VPN	Connected : 1		<u>Remote Dial-in l</u>	Jser / LAN to LAN	
	Current Page: 1		Page No. 🛽 🛩 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.

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).



1.8.4 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		VPN and Remote Access
Wizards		Remote Access Control
	<u>Quick Start Wizard</u>	PPP General Setup
	Service Activation Wizard	IPsec General Setup
	VPN Client Wizard	IPsec Peer Identity
	VPN Server Wizard	Remote Dial-in User
	Wireless Wizard	LAN to LAN
	VoIP Wizard	Connection Manageme
Online Status		Certificate Management
	Physical Connection	Local Certificate
	Virtual WAN	Trusted CA Certificate
WAN		Certificate Backup
	<u>General Setup</u>	Wireless LAN
	Internet Access	<u>General Setup</u>
	Multi-PVC	Security
LAN		Access Control
	<u>General Setup</u>	WPS
	Static Route	WDS
	VLAN	Advanced Setting
	Bind IP to MAC	WMM Configuration
	LAN Port Mirror	AP Discovery
	<u>Web Portal Setup</u>	Station List
NAT		USB Application
	Port Redirection	USB General Settings
	DMZ Host	USB User Management
	<u>Open Ports</u>	File Explorer
	<u>Address Mapping</u>	USB Device Status
	<u>Port Triggering</u>	Modem Support List
Firewall		System Maintenance
	<u>General Setup</u>	System Status
	Filter Setup	TR-069

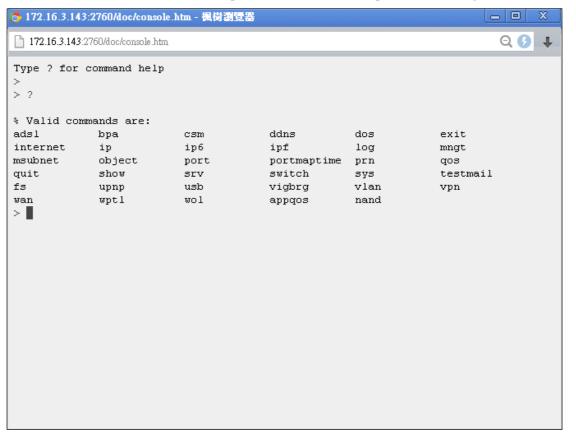
Dray Tek

1.8.5 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.



Dray Tek

1.8.6 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.

pening ¥2860_20140402.cfg	
You have chosen to open:	
₩2760_20140402.cfg which is: cfg File (8.8 KB) from: http://172.16.3.133:2860	
What should Firefox do with this file?	
 Save File 	
Do this automatically for files like this from now on.	
OK	Cancel

Click **Save** to store the setting.

1.8.7 Logout



Click this icon to exit the web user interface.

1.9 Online Status



1.9.1 Physical Connection

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



Physical Connection for IPv4 Protocol

Online Status

Physical Connection	on			System Upt	ime: 4days 23:49:2
	IPv4		IPv6		
LAN Status Primary		ary DNS: 10.39	.0.1	Secondary D	NS: 8.8.4.4
IP Address	TX Packets	RX Pac	kets		
192.168.1.1	63074	88053			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
No	ADSL			00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
NAN 2 Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	118:46:03	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
10.39.0.13	10.39.0.1	44744	7264	25837	530
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	-
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
ADSL Information	(ADSL Firmware	Version:)			
ATM Statistics	TX Cells	RX Cells	TX CRC err	rs RX C	RC errs
	0	0	0	0	
ADSL Status M	lode State	Up Speed	Down Speed	SNR Margin	Loop Att.
		0	0	0	0

Note: If the firmware which supports Vectoring has been installed to your Vigor router, you will see a short message of "with Vectoring support" near to VDLS2 Information. Such feature is available for VDSL2 only.

	to see a	0	0	0	0.
WAN 3 Sta	itus				
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	-
IP	GW IP	TX Pac	kets TX Rate(E	Bps) RX Packets	RX Rate(Bps)
	TTT	0	0	0	0
VDSL2 Inf	ormation (VDS	L2 Firmware Version:	05-06-06-02-00	0-07 with Vector	ing support)
Profile	State	UP Speed	Down Speed	SNR Upstream	SNR Downstream
30A	SHOWTIME	93898 (Kbps)	101058 (Kbps)	6 (0.1dB)	19 (0.1dB)

Physical Connection for IPv6 Protocol

Online Status

Physical Connecti	on			System (Jptime: 4days 23:51:32
	IPv4		IP∨6		
LAN Status					
IP Address					
FE80::21D:AAI	FF:FEA9:5E58/64 (Lin	k)			
TX Packets	RX Packets	TX Bytes	RX Bytes		
1702	200	134202	48922		
WAN IPv6 Status					
Enable	Mode	Up Time			
No	Offline				
IP			Ga	iteway IP	
				-	

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

Detailed explanation (for IPv4) is shown below:

Detailed explanation (for IPv6) is shown below:

Item Description



Item	Description		
LAN Status	IP Address - Displays the IPv6 address of the LAN interface.		
	TX Packets -Displays the total transmitted packets at the LAN interface.		
	RX Packets -Displays the total received packets at the LAN interface.		
	TX Bytes - Displays the speed of transmitted octets at the LAN interface.		
	RX Bytes - Displays the speed of received octets at the LAN interface.		
WAN IPv6 Status	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.		
	Mode - Displays the type of WAN connection (e.g., TSPC).		
	Up Time - Displays the total uptime of the interface.		
	IP - Displays the IP address of the WAN interface.		
	Gateway IP - Displays the IP address of the default gateway.		

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

1.9.2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

/irtual WAN System Uptime: 119:52:					
WAN 4 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 5 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 6 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0

1.10 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.

Vigor2760 Series User's Guide

Dray Tek



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.
- Wireless Wizard used for building wireless LAN connection.
- VoIP Wizard used for establishing VoIP profile.

2.1 Quick Start Wizard

Quick Start Wizard 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

login password		
Please enter an alpha-num	ric string as your Password (Max 23 characters).	
Old Password	••••	
New Password	••••	
Confirm Password	••••	

Dray Tek

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

WAN Interface	
WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL / VDSL2
Physical Type:	Auto negotiation
VLAN Tag insertion	Enable 💌
Tag value	0 (0~4095)
Priority	0 (0~7)
	< Back Next > Finish Cancel

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



2.1.1 For WAN1 (ADSL/VDSL2)

WAN1 is specified for ADSL or VDSL2 connection.

Quick Start Wizard

WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL / VDSL2
Physical Type:	Auto negotiation
VLAN Tag insertion	Enable 💌
Tag value	0 (0~4095)
Priority	0 (0~7)

Available settings are explained as follows:

Item	Description
Display Name	Type a name to identify such WAN.
VLAN Tag insertion	The settings configured in this field are available for WAN1 and WAN2.
	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.
	Disable – Disable the function of VLAN with tag.
	Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.

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

PPPoE/PPPoA

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

Quick Start Wizard

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

Item	Description
Protocol	There are two modes offered for you to choose for WAN1 interface. PPPoE / PPPoA PPPoE / PPPoA MPoA / Static or Dynamic IP Choose PPPoE/PPPoA as the protocol.
For ADSL Only	Such field is provided for ADSL only. You have to choose encapsulation and type the values for VPI and VCI. Or, click Auto detect to find out the best values. PPPoE LLC/SNAP PPPoE LLC/SNAP PPPoA VC MUX PPPoA VC MUX
Fixed IP	Click Yes to enable Fixed IP feature.
IP Address	Type the IP address if Fixed IP is enabled.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.



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

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

Quick Start Wizard	

Set PPPoE / PPPoA	
WAN 1	
Service Name (Optional)	2760
Username	84005755@hinet.net
Password	••••••
Confirm Password	••••••
	<pre>< Back Next > Finish Cancel</pre>

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
User Name	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.
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.

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

Quick Start Wizard

ease confirm your settings: WAN Interface: Physical Mode: VPI: VCI: Protocol / Encapsulation: Fixed IP: Primary DNS: Secondary DNS:	WAN1 ADSL / VDSL2 8 35 PPPoE / LLC No 8.8.8 8.8.4.4
	< Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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



MPoA / Static or Dynamic IP

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

t to Internet	
WAN 1	
Protocol	MPoA / Static or Dynamic IP
For ADSL Only:	
Encapsulation	1483 Bridged IP LLC
VPI	0 Auto detect
VCI	88
Fixed IP	• Yes ONo(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

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

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

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

Quick Start Wizard

Please confirm your settings: WAN Interface: WAN1 Physical Mode: ADSL / VDSL2 VPI: 8 35 VCI: 1483 Bridge LLC Protocol / Encapsulation: Fixed IP: No Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4 < Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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

Dray Tek

2.1.2 For WAN2 (Ethernet)

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

Quick Start Wizard

WAN Interface:	WAN2 🔽
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 💌
VLAN Tag insertion	Disable 💌

Available settings are explained as follows:

Item	Description
Display Name	Type a name for the router.
VLAN Tag insertion	The settings configured in this field are available for WAN1 and WAN2.
	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 WAN2.
	Disable – Disable the function of VLAN with tag.
	Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.

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

PPPoE

Quick Start Wizard

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

WAN 2				
Select one of th	e following Internet A	Access types provided	by your ISP.	
	PPPoE			
	🔘 РРТР			
	🔘 Static II	P		
	🔘 DHCP			

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

Quick Start Wizard

WAN 2	
Enter the user name and pas:	sword provided by your ISP.
Service Name (Optional)	2760
Username	84005657@hinet.net
Password	
Confirm Password	

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
User Name	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.

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.

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

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
settings and restart the V	

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

Quick Start Wizard Setup OK!

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

Quick Start Wizard

PPTP

Quick Start Wizard

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

ccess types provided by your ISP.
)

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

Quick Start Wizard

WAN 2		
by your ISP.	word, WAN IP configuration and PPTP serve	r IP provided
Username	5477aec	
Password	•••••	
Confirm Password		
WAN IP Configuration		
💿 Obtain an IP addres:	automatically	
🔵 🔘 Specify an IP addres	S	
IP Address	10.39.0.13	
Subnet Mask	255.255.255.0	
Gateway	10.39.0.1	
Primary DNS	8.8.8.8	
Second DNS	8.8.4.4	
PPTP Server		

Item	Description
User Name	Assign a specific valid user name provided by the ISP. Note: The maximum length of the user name you can set is 63 characters.
Password	Assign a valid password provided by the ISP. Note: The maximum length of the password you can set is 62 characters.



Confirm Password	Retype the password.
WAN IP Configuration	Obtain an IP address automatically – the router will get an IP address automatically from DHCP server.
	Specify an IP address – you have to type relational settings manually.
	IP Address - Type the IP address.
	Subnet Mask – Type the subnet mask.
	Gateway – Type the IP address of the gateway.
	Primary DNS – Type in the primary IP address for the router.
	Second DNS –Type in secondary IP address for necessity in the future.
PPTP 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.

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

ck Start Wizard	
use comminy your settings.	
WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	рртр
Click Back to modify char settings and restart the V	nges if necessary. Otherwise, click Finish to save the current rigor router.

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

Quick Start Wizard Setup OK!

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



Static IP

Quick Start Wizard

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

WAN 2				
Select one of the	e following Internet Ad	ccess types provi	ided by your ISP.	
	🔘 PPPoE			
	🔘 РРТР			
	💿 Static IP	I Contraction of the second		
	O DHCP			

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

Quick Start Wizard

WAN 2			
Enter the Static IP config	juration pr <mark>ovided by your I</mark> S	iP.	
WAN IP	10.39.0.13		
Subnet Mask	255.255.255.0		
Gateway	10.39.0.1		
Primary DNS	8.8.8.8		
Secondary DNS	8.8.4.4 (opt	(optional)	tional)

Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.



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

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

Quick Start Wizard

Please confirm your settings:	
WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
	ges if necessary. Otherwise, click Finish to save the current
settings and restart the Vi	gor router.
	< Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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

DHCP

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

WAN 2		
Select one of the	following Internet Access types provided by yo	our ISP.
	O PPPoE	
	O PPTP	
	🔘 Static IP	
	O DHCP	

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

Quick Start Wizard

Quick Start Wizard

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

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

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

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

Quick Start Wizard

Please confirm your settings:	
WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
settings and restart the Vi	iges if necessary. Otherwise, click Finish to save the current igor router.
	< Back Next > Finish Cancel

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

Quick Start Wizard Setup OK!

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

2.1.3 For WAN3 (USB)

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

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

Quick Start Wizard

Interface	
WAN Interface:	WAN3 💌
Display Name:	
Physical Mode:	USB

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

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

Item	Description
Internet Access	Choose one of the selections as the protocol of accessing the internet.
3G/4G USB Modem (PPP mode)	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.
4G USB Modem (DHCP mode)	SIM Pin code –Type PIN code of the SIM card that will be used to access Internet.
	Network Mode – Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.
	APN Name – APN means Access Point Name which is provided and required by some ISPs.

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

Quick Start Wizard

Please confirm your setti	ings:				
WAN Interface: Physical Mode: Internet Access Click Back to m	: WAN3 USB	γ. Otherwise, diα	ck Finish to :	save the cur	rent
		< Back	Next >	Finish	Cancel

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

Quick Start Wizard Setup OK!

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

2.2 Service Activation Wizard

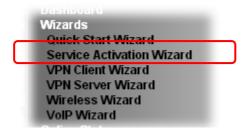
Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web user interface.

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 <u>http://myvigor.draytek.com</u>. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for detailed information.

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

Note: Such function is available only for Admin Mode.

1. Open Wizards>>Service Activation Wizard.



Service Activation Wizard

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

This wizard is - Web Conten Please choose	t Filter	-			
		 Free trial edition Formal edition with 	th 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**.

This	product provides 30 days of free trial, please choose the item(s) you want to use.	
	service:	
01	Veb Content Filter (BPiM)	
E	BPJM is the web content filter based on service operated in Germany. We recommend only users live in Sermany to try the BPJM WCF service. This is a free service without guarantee.	
	Activation Date : 2013-02-18	
t	Web Content Filter (Commtouch) License Agreement Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day rial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets. Activation Date : 2013-02-18	
		Activation
0 1	Web Content Filter (HagF1MM) License	Date : 2013-02-18

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

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 <u>http://www.draytek.de/jugendschutz</u>.

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

Service Activation Wizard

Pleas	e confirm your settings	
	Sevice Type : Sevice Activated :	Trial version Web Content Filter (Commtouch)
	Please click Back to re-se	lect service type you to activate.
		< Back Next > Finish Cancel

Dray Tek

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

Service Activation Wizard

Service Activation Wizard

Please check the		n(s) to enable services	on your router.	
Thease aneak and	-			
	✓ E	nable Web Content Filt	ter	

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

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

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

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



Dray Tek

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.

AN-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, pleas If the remote network is expecting only subnet and then select NAT mode. If in doubt then select Route Mode	e select Route Mode. y a single client or ip and is not configured to route the

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. Route Mode Route Mode NAT Mode
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.



[Index] [Status] [Name]	~
1	x	???	
	x	???	
2 3	X	???	
4	x	???	
5	х	???	
4 5 6 7	х	???	
7	х	???	
18	х	???	
19	х	???	
10	х	???	
111	х	???	
12	x	???	
13	х	???	=
14	x	???	
15	х	???	
16	х	???	
17	х	???	
18	х	???	
19	х	???	
20	х	???	
21	х	???	
22	x	???	
23	х	???	
24	х	???	
25	х	???	
26	х	???	_
27	x	???	
28	х	???	_
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

PN 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
PPTP (Encryption)	3. IPsec
4. L2TP	L2TP over IPsec
PPTP (None Encryption)	5. PPTP (Encryption)
IP L2 L2	PTP (None Encryption) PTP (Encryption) 'sec 2TP 2TP over IPsec (Nice to Have) 2TP over IPsec (Must)
	< Back Next > Finish Cancel

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



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

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

VPN Client Wizard

VPN Client PPTP None Encryption Settings	
Profile Name	???
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
L	
	<pre>< Back Next > Finish Cancel</pre>

• When you choose **IPsec**, you will see the following graphic: **VPN Client Wizard**

PN Client IPsec Settings	
Profile Name	???
🗌 Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89) IKE Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔘 Digital Signature (X.509)	
Peer ID	None 😪
Local ID	
Alternative Subject Name First	
O Subject Name First	
IPsec Security Method	
	DES without Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

VPN Client Wizard

VPN Client L2TP Settings	
Profile Name	???
🔲 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
	Sack Next > Finish Cancel

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

VPN Client Wizard

rofile Name	???
Always on	
erver IP/Host Name for VPN e.g. draytek.com or 123.45.67.89) KE Authentication Method	
Pre-Shared Key	
Confirm Pre-Shared Key	
🔘 Digital Signature (X.509)	
Peer ID	None 🔽
Local ID	
Alternative Subject Name First	
O Subject Name First	
Psec Security Method	
 Medium (AH) High (ESP) 	DES without Authentication 🗸
Jsername	???
assword	
emote Network IP	0.0.0.0
lemote Network Mask	255.255.255.0

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- Confirm Pre-Shared Key-Confirm the pre-shared key.
Digital Signature	Click Digital Signature to invoke this function.
(X.509)	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.

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



VPN and Remote Access >> VPN Client Wizard

I AN-to-I AN Index:	20		
Profile Name:	VPN-2		
VPN Connection Type:	L2TP over IPsec (Nice to Have)		
VPN Dial-Out Through: Always on:	WAN1 First No 172.16.3.8		
IKE Authentication Method:			
IPsec Security Method:	AH-SHA1		
Remote Network IP:	0.0.0.0		
Remote Network Mask:	255.255.255.0		
en la la la la la			
	 Go to the VPN Connection Management. 		
	, , ,		
	Go to the VPN Connection Management.		
Click Back to modify changes if ne proceed to the following action:	 Go to the VPN Connection Management. Do another VPN Client Wizard setup. 		

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.

PN Server Mode Selection:	Remot	te Dial-in Us	er (Teleworker) 🔽	
ease choose a LAN-to-LAN Profile:	3	х	222	~	
ease choose a Dial-in User Accounts:	2	x	???	~	
lowed Dial-in Type:	♥ PP ♥ IP: ♥ L2		sec Policy [None	~

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. Site to Site VPN – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.
	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.
	Site to Site VPN (LAN-to-LAN) Site to Site VPN (LAN-to-LAN) Remote Dial-in User (Teleworker)
Please choose a LAN-to-LAN Profile	This item is available when you choose Site to Site VPN (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.



	[Indew] [Statue] [Name]		
	[Index] [Status] [Name] 1 x ???		
	2 x ???		
	3 x ??? 4 x ???		
	6 x ???		
	7 x ???		
	8 x ??? 9 x ???		
	10 x ???		
	11 x ???		
	12 x ??? 13 x ??? =		
	14 x ???		
	15 x ???		
	16 x ??? 17 x ???		
	18 x ???		
	19 x ???		
	20 x ??? 21 x ???		
	22 x ???		
	23 x ???		
	24 x ??? 25 x ???		
	26 x ???		
	27 x ???		
	28 x ??? 29 x ??? ✓		
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.		
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).		
	🗹 РРТР		
	✓ IPsec		
	L2TP with IPsec Policy None None None Nice to Have Must		
	Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (Site to Site VPN and Remote Dial-in User) selected.		

2. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made.

Here we take the examples of choosing **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	???
PPTP / L2TP / L2TP over IPsec Authentication	
Username	???
Password	
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0
	< Back Next > Finish Cancel

• 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

/PN Authentication Setting	
Profile Name	???
PPTP / L2TP / L2TP over IPsec Authentication	
Username	???
Password	
IPsec / L2TP over IPsec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🔲 Digital Signature (X.509)	
Peer ID	None 🗸
Local ID	
Alternative Subject Name First	
🔘 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

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

VPN Server Wizard

Profile Name	???
IPsec / L2TP over IPsec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🗖 Digital Signature (X.509)	
Peer ID	None
Local ID	
Alternative Subject Name First	
🔘 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

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	Check the box of Digital Signature to invoke this function.
(X.509)	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: ??? PPTP+L2TP with IPsec Policy Allowed Service: 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: O to the VPN Connection Management. O Do another VPN Server Wizard setup. O View more detailed configurations. < Back Next > Finish Cancel

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 Wireless Wizard

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

Follow the steps listed below:

1. Open Wireless Wizard.



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

Wireless	Wizar	d
----------	-------	---

lost AP Configuration	
Name:	DrayTek
Mode:	Mixed(11b+11g+11n) 💌
Channel:	Channel 6, 2437MHz 🔽
Password:	*****
NOLE: THE HOST AF	^o configured here will be used for home or internal company use.
	Sack Next > Finish Cancel

Item	Description
Name	Type the SSID name of this router. The default name is defined with DrayTek. Change the name if required.
Mode	At present, the router can connect to 11b Only, 11n Only, 11g Only, Mixed (11b+11g), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

	Mixed(11b+11g+11n) ✓ 11b Only 11g Only 11n Only (2.4 GHz) Mixed(11b+11g) Mixed(11b+11g+11n)
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Password	 The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Guest AP Configuration
CEnable
Note: The configured guest AP will not be able to access VPN connections or communicate with wireless devices connecting to the router's other APs. The guest AP will be configured to be not able to connect to LAN interfaces also. However if the VLAN configurations were already made, then the guest AP will be able to connect to LAN ports belonging in the same VLAN group. This AP interface is by default configured for Internet access only.
Sack Next > Finish Cancel

Item	Description
Enable/Disable	Click it to enable or disable settings in this page.
Name	Type the SSID name of this router. (SSID1)

Password	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Rate Control	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.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

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

Wireless Wizard

Basic Wireless Settings		
Mode:Mixed(11b+11g+11n) Channel:Channel 6, 2437MHz		
Host AP Configurations		
Name:DrayTek Password:***********		
Guest AP Configurations		
Status:Disabled		
Name:DrayTek_Guest Password:***********		
Rate Control:Disabled		

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

2.6 VoIP Wizard

Vigor router offers a quick method to configure settings for VoIP application. Follow the steps listed below.

1. Open Wizards>>VoIP Wizard.



2. The screen of VoIP Wizard will be shown as follows.

VoIP Wizard

Set VoIP service provider domain			
VoIP service provider	draytel.org 🛛 💙	draytel.org (63 char max).	
SIP Port	5060		
Set Account quickly			
Phone 1 (default mapping to Account 1)			
Account Number/Name		(63 char max).	
Password		(63 char max).	

Account Number/Name	(63 char max).
Password	(63 char max).

Item	Description
Set VoIP service provider domain	VoIP service provider - Use the drop down list to choose the ISP which offers the VoIP service for your router.
	SIP Port – Use the default setting (5060).
Set Account quickly	Account Number/Name – Type the account number/name registered to your ISP.
	Password – Type the password for the account registered to your ISP.
	Use the same Account as phone 1 – If you don't need to configure Phone 2 settings, simply check this box.
Next	Click it to get into the next setting page.



Cancel	Click it to give up the quick start wizard.
--------	---

 After finished the settings above, click Next for viewing summary of such connection. VolP Wizard

SIP Port		
SIP PUR	5060	
Phone 1 Account	5060	
Phone 2 Account	5060	
Click Back to modify change	if necessary. Otherwise, click Finish to save current settings.	

4. Click **Finish.** A page of **VoIP Wizard Setup OK!!!** will appear.

VoIP Wizard Setup OK!

2.7 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.

Dray Tek	Vigor2760 Series
Login	
Username Password	admin
	Login
	oyright © 2013 DrayTek Corp. All Rights served.

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



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

C.		Please take a mom Membership Regis for your purchased upcoming product	tration entitles you product and rece	to upgrade firmware ive news about
LO	DGIN			
	UserName :	james_fae]	
	Password :	•••••]	
	Auth Code :	txxhdd	t x x h d d	
		If you cannot read the word,	click here	
		Forgotten password?	Login	
	Don't have a M	yVigor Account ?	Create an account	now
L				

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

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

5 When the following page appears, please type in Nickname (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.

About Us Product	My Product		Search for th	nis site GO
My Information	🛤 Registration Device	I		
VigorACS SI VigorPro	Serial number : Nickname : *	201103160920 Vigor2760	0201	
Product Registration Customer Survey	Registration Date :	03-16-2011		
	Usage :	Select	*	
	Product Rating :	Select	📝 (Your opinion so fa	r)
	No. of Employees :	Select	🞽 (In total within your	company)
	Supplier :		(Where	you bought it from)
	Date of Purchase :		(mm-dd	- УУУУ)
	Internet Connection : *			
	🔲 Cable	🗹 ADSL	VDSL	🔲 Fiber
	🔲 3G	🔲 WIMAX	🔲 LTE	
Please use IE 5.0 or above (resolution 1024 * 768) for best display. © DrayTek Corp.				Cancel Submit

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

Your device has been successfully added to the database.



7 Now, you have finished the product registration.



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

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

1 Home		Search GO
About Us Product My Information VigorACS SI VigorPro Customer Survey	My Information Welcome.james_fae Last Login Time : 2011-03-16 01:45:09 Last Login From : 172.16.2.180 Current Login Time : 2011-03-16 18:20:31 Current Login From : 172.16.3.148 Your Device List	RowNo : 5 Y PageNo : 1 Y
	Serial Number / Host ID Device Name	Model Note
	2011031609200201 Vigor2760	Vigor2760 -

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

	My Product
About Us Product	Device Information
My Information VigorACS SI VigorPro Customer Survey	Nickname : Vigor2760 Serial : 2011031609200201 Model : Vigor2760 Series Rename Transfer Back
	Device's Service Expired License
	Service Provider Action Status Start Date Expired Date
	<u>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.</u>
	BPJM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPJM WCP service. This is a free service without guarantee.

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

About Us Product	Confirm Messag	e		Cancel
My Information	User Name :	james_fae		
VigorACS SI	Serial :	201103160920020		
VigorPro	Model:	Vigor2760		
Customer Survey	Licens	se Number	Service Provider	Status
	PLEASE READ CAREFULLY B BY DOWNLOAD AGREEING TO NOT AGREE TO	EFORE DOWNLOADING ING, INSTALLING C BE BOUND BY THE	CENSE AGREEMENT (?LICENSE?) OR OTHERWISE USING THE SOFT R USING THE SOFTWARE, YOU AF TERMS OF THIS LICENSE. IF YO IS LICENSE, YOU ARE NOT AUTH WARE.	RE DU DO
	1. Scope.	☑ I have read and accept	the above Agreement. (Please check this bo).	Next

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



12 Wait for a moment until the following page appears.

DrayTek Service Activation

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

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

Copyright © DrayTek Corp. All Rights Reserved.

Close

13 Click Close.

This page is left blank.

Vigor2760 Series User's Guide

Dray Tek



This chapter will guide users to execute web configuration.

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

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

Dray Tek	Vigo	r270	50 Serie	5					1	1 13	G	Delight
Auto Logout 💌 🛛 IR:6	Dashboa	rd										^
Dashboard Wizards Online Status WAN LAN Route Policy			<u>o</u> e		a a		27-539-21 Vigor2760	Vn.	00	Ð	Ð	
NAT Firewall Objects Setting	System I		ti o m	_						_	Quick Access	
CSM	Model Na		Vigor2760	0.00		Syste	em Up Time	1:3:22			System Status	
Bandwidth Management	Router Na		Vigor2760	WH			ent Time		1 Sat 1:3:20	- 1	Dynamic DNS	
Applications	Firmware		3.7.5.1				Date/Time		014 10:02:56	- 1	TR-069	
VPN and Remote Access Certificate Management VoIP	DSL Versi	ion	05-04-04-	04-0	0-01		MAC Address				M/P2P Block Schedule	
Wireless LAN	IPv4 Inte	ernet Ad	cess								SysLog / Mail Aler	t
USB Application		Line / I	Mode		IP Address		MAC Addres	s	Up Time		RADIUS	
System Maintenance	WAN1		/ PPPoA		Disconnec		00-1D-AA-8		00:00:00		Firewall Object Se	tting
Diagnostics	WAN2		net /		Disconnec		00-1D-AA-8		00:00:00		Data Flow Monitor	
	WAN3	USB /			Disconnec	ted	00-1D-AA-8	8-15-03	00:00:00			
Support Area	ID. O. Lot.			_		_						
Product Registration	IPv6 Inte	Mode	cess		ress			Coone	Up Time			
	LAN		D / DHCPv6		ress 30::21D:AAF	E-EEBO	1500/64	Scope	Up Time	-		
All Rights Reserved.	LAN	TRADVI	0 / UNCPIO	FEO	0210.445	r.rcbo	.1300/04	LINK				
	Interface	e										
	DSL		ected : Dow	n Str	eam : OKbn	s / Up !	Stream : OKb	ps				
	WAN		ected : 0,	WA			WAN3					
	🗔 LAN	Conne	ected : 0, (ULAN	11 @LAN:	2 🌒	LAN3 @LA	N4				~
	and the second second											Long to

3.1 WAN

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

3.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address



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, Vigor2760 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2760, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2760n 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 Vigor2760n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2760n 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-PVC

3.1.2 General Setup

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

This router supports multiple-WAN function. It allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1, WAN2, and WAN3 settings.

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

WAN >> General Setup

Setup		
Index	Enable	Physical Mode/Type
WAN1	-	ADSL/-
WAN2	V	Ethernet/Auto negotiation
WAN3	V	USB/-

Note: WAN1 and WAN2 cannot work simultaneously, so when one of the interfaces is enabled, the other will be disabled. WAN3 can only serve as the backup WAN for WAN1 or WAN2, depending on which is active.

OK]

Available settings are explained as follows:

Description
Click the WAN interface link under Index to access into the WAN configuration page.
V means such WAN interface is enabled and ready to be used.
Display the physical mode and physical type of such WAN interface.

Note: In default, each WAN port is enabled.

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



WAN1 with ADSL/VDSL

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

WAN >> General Setup

WAN 1	
Enable:	Yes 💌
Display Name:	
Physical Mode:	ADSL
DSL Mode:	Auto 💌
Physical Type:	Auto negotiation 👻
DSL Modem Code:	Default
VLAN Tag insertion (ADSL):	Disable 👻 (Please configure Internet Access setting first)
Tag value:	0 (0~4095)
Priority:	0 (0~7)
VLAN Tag insertion (VDSL2):	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)

Note:

 WAN1 and WAN2 cannot work simultaneously, so when one of the interfaces is enabled, the other will be disabled. WAN3 can only serve as the backup WAN for WAN1 or WAN2, depending on which is active.
 In DSL auto mode, the router will reboot automatically while switching between VDSL2 and ADSL lines.



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 interface.	
Physical Mode	Display the physical mode of such interface. If VDSL2 is detected, this field will display " VDSL2 "; if ADSL is detected, it will display " ADSL ".	
DSL Mode	Specify the physical mode (VDSL or ADSL) for such router manually.	
Physical Type	For such interface, no type can be selected.	
DSL Modem Code	Choose the correct DSL modem code for ensuring the network connection. Default Default AnnexA_560816_552011 AnnexA_548006_544401 If you have no idea about the selection, simply choose	

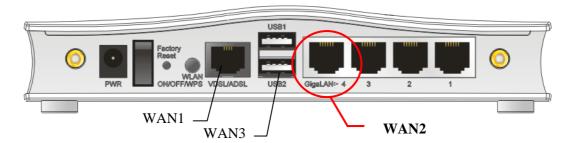


	Default or contact the dealer for assistance.
VLAN Tag insertion	The settings configured in this field are available for ADSL.
(ADSL)	Enable – Enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the WAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by WAN1.
	Disable – Disable the function of VLAN with tag.
	Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.
VLAN Tag insertion (VDSL2)	The settings configured in this field are available for VDSL2.
	Enable – Enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the WAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by WAN1.
	Disable – Disable the function of VLAN with tag.
	Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.

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

WAN2 with Ethernet

The physical LAN4 port can be treated as a WAN interface, named WAN2.



When WAN2 is enabled, WAN1 (DSL) will be disabled automatically.

WAN >> General Setup

Enable:	Yes 💌
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 💌
VLAN Tag insertion :	Disable 💌 (Please configure Internet Access setting first)
Tag value:	0 (0~4095)
Priority:	0 (0~7)

Note:

1. WAN1 and WAN2 cannot work simultaneously, so when one of the interfaces is enabled, the other will be disabled. WAN3 can only serve as the backup WAN for WAN1 or WAN2, depending on which is active. 2. When WAN2 is enabled, LAN P4 port will be used as WAN2.

OK	Cancel

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. Current Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M full duplex 100M full duplex 1000M full duplex 1000M full duplex	
VLAN Tag insertion	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.
Disable – Disable the function of VLAN with tag.
Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.
Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.

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

WAN3 with USB

To use 3G/4G network connection through 3G/4G USB Modem, please configure $\ensuremath{\textbf{WAN3}}$ interface.

WAN >> General Setup

WAN 3

Enable:	Yes 💌	
Display Name:		
Physical Mode:	USB	

Note:

WAN1 and WAN2 cannot work simultaneously, so when one of the interfaces is enabled, the other will be disabled. WAN3 can only serve as the backup WAN for WAN1 or WAN2, depending on which is active.



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.

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

3.1.3 Internet Access

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

WAN	>>	Internet	Access
-----	----	----------	--------

Internet Access

Display Name	Physical Mode	Access Mode	
	ADSL / VDSL2	None 🔽	Details Page IPv6
	Ethernet	None PPPoE / PPPoA	Details Page IPv6
	USB	MPoA / Static or Dynamic IP None	Details Page IPv6
	Display Name	Ethernet	ADSL / VDSL2 None Ethernet PPPoE / PPPoA MPoA / Static or Dynamic IP

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	None	$\mathbf{\vee}$	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	¥	Details Page IPv6
WAN3		USB	None PPPoE		Details Page IPv6
Note: Or	nly one WAN can	support IPv6.	Static or Dynamic IP PPTP		

Advanced You can configure DHCP client options here.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		ADSL / VDSL2	None	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP 🛛 👻	Details Page IPv6
WAN3		USB	None	Details Page IPv6
Note: On	Ily one WAN can	support IPv6.	None 3G/4G USB Modem(PPP mode) 4G USB Modem(DHCP mode)	
Advanc	ed You can conf	igure DHCP client (options here.	

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(ADSL/VDSL2) /WAN2 (Ethernet) /WAN3 (3G/4G USB Modem) according to the real network connection.	
Access Mode	Use the drop down list to choose a proper access mode. The	



	details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page (based on IPv4) according to the access mode that you choose in WAN interface.
	Note that Details Page will be changed slightly based on ADSL/VDSL2 physical mode specified on WAN>>General Setup .
IPv6	This button will open different web page (based on Physica Mode) to setup IPv6 Internet Access Mode for WAN interface.
	If IPv6 service is active on this WAN interface, the color o "IPv6" will become green.
Advanced	This button allows you to configure DHCP client options. DHCP packets can be processed by adding option number and data information when such function is enabled and configured.
	DHCP Client Options Status Options List Enable Interface Option Type Data
	Enable: Interface: All WAN1 WAN2 WAN3 WAN4 WAN5 WAN6 Interface: Option Number: DataType: OASCII Character (EX: Option:18, Data:/path) Hexadecimal Digit (EX: Option:18, Data:270617468) Address List (EX: Option:44, Data:172.16.2.10,172.16.2.20) Data: Add Update Delete
	Note: Option 61 has been given a default value. You can configure option 61(Client Identifier) in "WAN >> Internet Access" page. If you choose to configure option 61 here, the settings in "WAN >> Internet Access, Details Page" will be overwritten. Option 12 is reserved, you cannot configure it here but you can configure it in "Router Name" field of "WAN >> Internet Access". OK
	Enable/Disable – Enable/Disable the function of DHCP
	Option. Each DHCP option is composed by an option
	number with data. For example, Option number:100
	Data: abcd
	When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.
	Interface – Specify the WAN interface(s) that will be overwritten by such function. WAN4 ~ WAN6 can be located under WAN>>Multi-PVC .
	Option Number – Type a number for such function.
	Note: If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.
	DataType – Choose the type (ASCII or Hex) for the data to be stored.

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

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

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

WAN	>>	Internet	Access
		micritici	ACCUSS

WAN 1				
PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
Enable	O Disable		IP Setup	PAP or CHAP 🗸
ISP Access Set Username Password	up	Idle T	imeout dress Assignment Meth	-1 second(s)
Index(1-15) in =>,	Schedule Setup:		IP: ○ Yes ⊙ No (IP Address [Dynamic IP)
WAN Connectio Mode Ping IP TTL:	ARP Detect 💌	O Sp	efault MAC Address becify a MAC Address Address: 00 •1D	• •AA :A8 •B7 •69
МТО	1442 (Max:1492)			
	OK	Ca	ncel	

Item	Description
Enable/Disable	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	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	Username – Type in the username provided by ISP in this field.
	Password – Type in the password provided by ISP in this field.
	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 pinging.				
	TTL (Time to Live) – Displays value for your reference.				
	TTL value is set by telnet command.				
MTU	It means l is 1442.	It means Max Transmit Unit for packet. The default setting is 1442.			
PPP/MP Setup	PPP Aut for PPP.	hentica	tion – Select PAP o	nly or PAP or CHA	
			Set the timeout for be sing through the tim	reaking down the e without any action.	
IP Address Assignment Method (IPCP)	time you provides a whenever address ir you want WAN IP and would use WAN	connect service you rea the Fiz to use t Alias - d like to IP Alia	to always assign you quest. In this case, y ked IP field. Please c his function. If you have multiple o utilize them on the as. You can set up to	some case, your ISP the same IP address ou can fill in this IP contact your ISP befo e public IP addresses WAN interface, plea o 8 public IP addresses	
	other than		rrent one you are usi	ng.	
	172.16.3.1				
	WAN1 IP #	Alias (Mu	lti-NAT)		
	Index E		Aux. WAN IP	Join NAT IP Pool	
	1.				
	2.		0.0.0.0		
	3.		0.0.0.0		
	4.		0.0.0.0		
	5.		0.0.0.0		
	5. 6.		0.0.0.0		
	5. 6. 7.		0.0.0.0		
	5. 6. 7. 8.		0.0.0.0		
	5. 6. 7. 8.		0.0.0.0		
	5. 6. 7. 8. << <u>18</u> 9 Fixed IP a	- <u>16</u> <u>17-2</u> - <u>16</u> <u>17-2</u> - Click	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0 0.0	Close Close	
	5. 6. 7. 8. << 18 9 Fixed IP fixed IP a Default M Address of 10	- Click ddress MAC A MAC A	0.0.0.0 0.0.0.0 <td< td=""><td>Close Close Address. Se Default MAC dress by typing on the</td></td<>	Close Close Address. Se Default MAC dress by typing on the	

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

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

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

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
🔘 Enable	 Disable 	WAN IP Network Settings	WAN IP Alias
Keep WAN Con Enable PING FING to the IP PING Interval	nection G to keep alive 0 minute(s)	 Obtain an IP address a Router Name Domain Name * : Required for some IS Specify an IP address 	Vigor
WAN Connectio Mode Ping IP TTL:	n Detection	IP Address Subnet Mask Gateway IP Address	
MTU	1442 (Max:1500)	 Default MAC Address Specify a MAC Address 	
RIP Protocol		MAC Address: 00 .1D DNS Server IP Address Primary IP Address Secondary IP Address	•AA A8 •B7 •69 8.8.8.8 8.8.4.4

WAN >> Internet Access

Item	Description
Enable/Disable	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.
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.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.



Bridge Mode	If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.			
WAN IP Network Settings	 This group allows you to obtain an IP address automatically and allows you type in IP address manually. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog. 			
		2.168.1.1/doc	ndows Internet Explorer Wipalias.htm	
		P Alias (M Enable	Aux. WAN IP	Join NAT IP Pool
	1.			
	2.		0.0.0.0	
	з.		0.0.0.0	
	4.		0.0.0.0	
	5.		0.0.0.0	
	6.		0.0.0.0	
	7.		0.0.0.0	
	8.		0.0.0.0	
			OK Clear All	Close
		e IP add Route provie Doma	ress automatically. er Name – Type in the ded by ISP.	y – Click this button to ne router name the domain name that
	Specify some dat	ta.		idio button to specify
			ldress – Type in the et Mask – Type in the	-
	 Subnet Mask – Type in the subnet mask. Gateway IP Address – Type in gateway IP address. 			
	router. Y another	You can w MAC ad	ddress – Type in M. use Default MAC A dress for your necess	ddress or specify sity.
	Specify a MAC Address – Type in the MAC address for the router manually.			
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.			

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

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

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

WAN 1		
PPPoE	Static or Dynamic IP	PPTP/L2TP IPv6
O Enable F	PPTP 🔿 Enable L2TP 💿 Disable	PPP Setup
Server Address	3	PPP Authentication PAP or CHAP 👻
Specify Gatew	ay IP Address	Idle Timeout -1 second(s)
		IP Address Assignment Method (IPCP) WAN IP Alias
ISP Access Set	qu	Fixed IP: 🔿 Yes 💿 No (Dynamic IP)
Username		Fixed IP Address
Password		WAN IP Network Settings
Index(1-15) in	Schedule Setup:	Obtain an IP address automatically
=> ,	, , ,	Specify an IP address
		IP Address
МТО	1442 (Max:1460)	Subnet Mask
	ОК	Cancel

WAN >> Internet Access

Item	Description
PPTP/L2TP	Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
	Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.
	Disable – Click this radio button to close the connection through PPTP or L2TP.
	Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
	Specify Gateway IP Address – Specify the gateway IP address for DHCP server.
ISP Access Setup	Username -Type in the username provided by ISP in this field.
	Password -Type in the password provided by ISP in this field.
	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.
MTU	It means Max Transmit Unit for packet. The default setting



	is 1442.			
PPP Setup	for PPP. Idle Tim	 PPP Authentication - Select PAP only or PAP or CHAP for PPP. Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. 		
IP Address Assignment Method(IPCP)	and woul use WAN	d like t I IP Al	o utilize them on the	e public IP addresses WAN interface, please o 8 public IP addresses ing.
	S WAN1IP	Alias - 撮	樹潮覽器	
	172.16.3.	143:2860/d	oc/wipalias.htm	6 +
	WAN1 IP	Alias (Mu	ulti-NAT)	·
	Index E	,	Aux. WAN IP	Join NAT IP Pool
	1.			
	2.		0.0.0.0	
	з.		0.0.0.0	
	4.		0.0.0.0	
	5.		0.0.0.0	
	6.		0.0.0.0	
	7.		0.0.0.0	
	8.		0.0.0.0	
			24 25-32 >> OK Clear All	Close
	you each your ISP address v this IP ad before yo function	time y provid whenev dress i ou want and typ	ou connect to it and es service to always er you request. In thi n the Fixed IP field.	
WAN IP Network Settings	obtain the	e IP ad	dress automatically.	\mathbf{y} – Click this button to
	Specify a some dat	a.		adio button to specify
			ddress – Type the IF	
		Subn	et Mask – Type the	subnet mask.

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

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

WAN >> Internet Access

WAN 1

PPPoE / PPPoA	MPoA / Static or	Dynamic IP	IPv6
💿 Enable 🛛 Disal	ble	ISP Access Setup	
		Username	
Modem Settings (for ADSL		Password	
Multi-PVC channel	Channel 1	Separate Account f	or ADSL
VPI	0	PPP Authentication	PAP or CHAP
VCI	33		
Encapsulating Type	LLC/SNAP 💌	Idle Timeout	-1 second(s)
Protocol	PPPoE V	IP Address From ISP	WAN IP Alias
Modulation	Multimode 🗸	Fixed IP 🛛 🔘 Yes 💿	No (Dynamic IP)
		Fixed IP Address	
PPPoE Pass-through			
For Wired LAN		Default MAC Addres	
📃 For Wireless LAN		Specify a MAC Add	
		MAC Address: 00 .	1D .AA A8 .B7 .69
WAN Connection Detection	-	Tenders (d. d.C.) in Cale a de	de Celerer
Mode	ARP Detect 🛩	Index(1-15) in <u>Schedu</u>	IIE Setup:
Ping IP		; =>,	rr
TTL:			
мти	1442 (Max:1492)		
	OK	Cancel	

Item	Description
Enable/Disable	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.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	VPI - Type in the value provided by ISP.
	VCI - Type in the value provided by ISP.
	Encapsulating Type - Drop down the list to choose the type provided by ISP.
	Protocol - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP.
	If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group.



	Modulation –Default	setting is Multimode. Choose the one		
	that fits the requirement of your router.			
	Modulation	Multimode T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode		
PPPoE Pass-through	also can establish the clients to your ISP via protocol is selected, th will be transformed in server. Thus, the PC c direction.			
	network can use anoth	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.		
	For Wireless LAN – It is available for n model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.			
	Note: To have PPPoA Pass-through, please choose PPPoA protocol and check the box(es) here. The router will behave like a modem which only serves the PPPoE client on the LAN. That's, the router will offer PPPoA dial-up connection.			
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.			
	Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.			
	Ping IP – If you choo	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) - TTL value is set by te	 Displays value for your reference. Inet command. 		
MTU	It means Max Transm is 1442.	It means Max Transmit Unit for packet. The default setting is 1442.		
ISP Access Setup	parameters according ISP.	sername, password and authentication to the information provided by your		
	field.	the username provided by ISP in this		
	field.	he password provided by ISP in this		
	_	r ADSL – In default, WAN1 supports sets the same PPPoE account and		

IP Address From ISP	 password for connection. If required, you can configure another account and password for ADSL connection by checking this box. If it is checked, the system will ask you to type another group of account and password additionally. PPP Authentication – Select PAP only or PAP or CHAP for PPP. Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. 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. WAN IP Alias - If you have multiple public IP addresses 				
	and would like	\mathbf{s} - If you have multiple to utilize them on the V lias. You can set up to	WAN interface, please		
	other than the	current one you are usin	•		
	👌 WAN1IP Alias -	楓樹潮覽器			
	172.16.3.143:2860)/doc/wipalias.htm	•		
	WAN1 IP Alias (Multi-NAT)			
	Index Enable	Aux. WAN IP	Join NAT IP Pool		
	1. 🗹				
	2. 🗖	0.0.0.0			
	3. 🗌	0.0.0.0			
	4.	0.0.0.0			
	5.	0.0.0.0			
	6. 🗌	0.0.0.0			
	7.	0.0.0.0			
	8.	0.0.0.0			
	<< <u>1-8 9-16 1</u>	11-24 20-32 >>	<u>Next</u> >>		
	OK Clear All Close				
	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.				
	Index (1-15) in of time schedu set previously	n Schedule Setup - Yo le for your request. All in Applications >> Scl e number that you have	the schedules can be nedule web page and		

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



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

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

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

PPPoE / PPPoA	MPoA / Static or	Dynamic IP	IPv6
🔘 Enable 🛛 💿 Di	sable	WAN IP Network Settings	WAN IP Alias
Modem Settings (for AD	SL only)	◯ Obtain an IP address a	-
Multi-PVC channel	Channel 2	Router Name	Vigor
Encapsulation		Domain Name	
148	33 Bridged IP LLC 🛛 🗸	* : Required for some I	SPs
VPI	0	Specify an IP address	
VCI	88	IP Address	
Modulation	Multimode 🗸	Subnet Mask	
Modulation	Wultimode Y	Gateway IP Address	
WAN Connection Detect	ion		
Mode	ARP Detect 💙	Oefault MAC Address	
Ping IP		Specify a MAC Addre	SS
TTL:		MAC Address: 00 .10	.AA A8 .B7 .69
мти	1442 (Max:1500)	DNS Server IP Address	
	(Max 1900)	Primary IP Address	8.8.8.8
RIP Protocol		Secondary IP Address	8.8.4.4
Enable RIP		,	
Bridge Mode			
Enable Bridge Mode	1		

Available settings are explained as follows:

WAN >> Internet Access

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

	VPI - Type in the value provided by ISP.		
	VCI - Type in the value provided by ISP.		
	Modulation –Default setting is Multimode. Choose the one		
	that fits the requirement of your router.		
	Modulation	Multimode T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode	
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.		
	Mode – Choose ARP Detector to execute for WAN detection	t or Ping Detect for the system on.	
	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) – Disp. TTL value is set by telnet co	lays value for your reference.	
MTU	It means Max Transmit Unit is 1492.	t for packet. The default setting	
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.		
Bridge Mode	If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.		
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.		
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.		



O WAN1	IP Alias - 🐻	樹潮覽器	
172.16	5. 3.143 :2860/a	oc/wipalias.htm	6 🕇
WANT I	D Alles (M		^
	P Alias (M Enable	Aux. WAN IP	Join NAT IP Pool
1.			
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
<< <u>1-8</u>	<u>9-16 17</u>	-24 25-32 >>	<u>Next</u> >>
		OK Clear All ddress automaticall dress automatically.	y – Click this button to
	he IP ade Rout	ddress automaticall dress automatically. t er Name – Type in t	y – Click this button to
	he IP ado Rout provi Dom	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in	y – Click this button to
obtain t	he IP add Rout provi Dom you h	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned.	y – Click this button to he router name the domain name that
obtain t	he IP add Rout provi Dom you h	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned.	y – Click this button to he router name
obtain t	he IP ado Rout provi Dom you h y an IP a ata.	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned.	y – Click this button to he router name the domain name that adio button to specify
obtain t	he IP add Rout provi Dom you h y an IP a ata. IP Ad Subn	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned. ddress – Click this r ddress – Type in the net Mask – Type in t	y – Click this button to he router name the domain name that adio button to specify private IP address. he subnet mask.
obtain t	he IP add Rout provi Dom you h y an IP a ata. IP Ad Subn	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned. ddress – Click this r ddress – Type in the net Mask – Type in t	y – Click this button to he router name the domain name that adio button to specify private IP address. he subnet mask.
obtain t Specify some da Default router.	he IP add Rout provi Dom you h y an IP a ata. IP Ad Subm Gate addre t MAC A You can	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned. ddress – Click this r ddress – Type in the net Mask – Type in t tway IP Address – T ess. Address – Type in M use Default MAC A	y – Click this button to he router name the domain name that adio button to specify private IP address. he subnet mask. 'ype in gateway IP AC address for the address or specify
obtain t Specify some da Default router. another Specify	he IP add Rout provi Dom you h y an IP a ata. IP Ad Subm Gate addre t MAC A You can	ddress automaticall dress automatically. ter Name – Type in t ided by ISP. ain Name – Type in nave assigned. ddress – Click this r ddress – Type in the net Mask – Type in t way IP Address – T ess. Address – Type in M use Default MAC A ddress for your necess	y – Click this button to he router name the domain name that adio button to specify private IP address. he subnet mask. 'ype in gateway IP AC address for the address or specify

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

Details Page for PPPoE in WAN2

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

PPPoE	Static or Dynamic IP	PPT	FP/L2TP	IPv6
🔘 Enable 💿 Disa	ble	PPP/MP Setup		
ISP Access Setup Username Password Index(1-15) in <u>Schedule</u> =>,,	 Setup: ,	PPP Authenticat Idle Timeout IP Address Assign WAN IP Alias Fixed IP: O Yes Fixed IP Address	-1 Iment Method	
WAN Connection Detectio Mode Ping IP TTL:	ARP Detect	 Default MAC Specify a MA MAC Address: 	AC Address	A: A8 .B7 .6A
MTU	1442 (Max:1492)			

WAN >> Internet Access

Item	Description
Enable/Disable	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	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	Username – Type in the username provided by ISP in this field.
	The maximum length of the user name you can set is 63 characters.
	Password – Type in the password provided by ISP in this field.
	The maximum length of the password you can set is 62 characters.
	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 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. The default setting is 1492.					
PPP/MP Setup	PPP Aut for PPP.	thentica	ntion – Select PAP o	only or PAP or CHAP		
			Set the timeout for b using through the time	reaking down the ne without any action.		
IP Address Assignment Method (IPCP)	time you provides wheneve address i you want WAN IP and woul use WAN	connect service or you re n the Fi t to use Alias - Id like to N IP Ali	to always assign you quest. In this case, y xed IP field. Please of this function. If you have multiple o utilize them on the	a some case, your ISP u the same IP address ou can fill in this IP contact your ISP befor e public IP addresses WAN interface, pleas o 8 public IP addresses		
	additiona	al WAN		k the Enable box. The		
	S WAN2IF		•	_ O X		
	172.16.3	. 143 :2860/da	c/wipalias.htm	6 1		
		A.I	14: N.S.T.)	2		
		Alias (Mu Enable	Aux. WAN IP	Join NAT IP Pool		
	1.		10.39.0.10			
	2.	V	10.39.0.150			
	З.		0.0.0.0			
	4.		0.0.0.0			
	5.		0.0.0.0			
	5.		0.0.0.0			
		_				
	6.		0.0.0.0			
	6. 7. 8.		0.0.0.0			
	6. 7. 8. << <u>18</u>	9-16 17- - Click address	0.0.0.0	Close Next >> Close		
	6. 7. 8. << 18 1 Fixed IP fixed IP fixed IP fixed IP	9-16 17- - Click address MAC A or spec	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0	Close Next >> Close		

router manually.

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

Details Page for Static or Dynamic IP in WAN2

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

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

WAN 2			
PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Enable	O Disable	WAN IP Network Settings	WAN IP Alias
Keep WAN Con	nection	🔘 Obtain an IP address a	utomatically
	G to keep alive	Router Name	*
PING to the IP		Domain Name	*
		* : Required for some IS	SPs
PING Interval	0 minute(s)	DHCP Client Identifier for s	ome ISP
WAN Connectio	n Detection	Enable	
Mode	ARP Detect V	Username	
Ping IP		Password	
TTL:		Specify an IP address	
		IP Address	172.16.3.130
мти	1442 (Max:1500)	Subnet Mask	255.255.0.0
RIP Protocol		Gateway IP Address	172.16.1.1
Enable RIP			
		Oefault MAC Address	
		Specify a MAC Addres	s
		MAC Address: 00 .1D	.AA A8 .B6 .AA
		DNS Server IP Address	
		Primary IP Address	168.95.1.1
		Secondary IP Address	8.8.4.4
	OK	Cancel	

WAN >> Internet Access

Item	Description
Enable / Disable	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



	PING t specify alive. PING I	PING Interval - Enter the interval for the system to execute the PING operation.			
WAN Connection Detection	connect Detect.	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping			
	to execu	ute for W	AN detection.		
	0	•	address in this field f	as detection mode, yo for pinging.	
	TTL (1	Time to		ue for your reference.	
MTU	It mean is 1492		ransmit Unit for pac	ket. The default setting	
RIP Protocol	(RFC tables in	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.			
Settings	WAN I and wor use WA other th	P Alias uld like t N IP Al	o utilize them on the ias. You can set up t urrent one you are us	le public IP addresses WAN interface, pleas o 8 public IP addresses	
	172.16	.3.143:2860/ð	oc/wipalias.htm	() +	
		P Alias (M Enable	ulti-NAT) Aux. WAN IP	Join NAT IP Pool	
	1.		10.39.0.10		
	2.		10.39.0.150		
	з.		0.0.0.0		
	4.		0.0.0.0		
			0.0.0.0		
	5.		0.0.0.0		
	5.		0.0.0.0		
	6.		0.0.0.0		
	6. 7. 8.		0.0.0.0		
	6. 7. 8.		0.0.0.0		

	Dynamic IP mode.
	• Router Name : Type in the router name provided by ISP.
	• Domain Name : Type in the domain name that you have assigned.
	DHCP Client Identifier for some ISP
	• 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.
	Specify an IP address – Click this radio button to specify some data if you want to use Static IP mode.
	• IP Address : Type the IP address.
	• Subnet Mask : Type the subnet mask.
	• Gateway IP Address: Type the gateway IP address.
	Default MAC Address : Click this radio button to use default MAC address for the router.
	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.
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.

Details Page for PPTP/L2TP in WAN2

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

WAN >> Internet Access

PPPoE	Static or Dynam	ic IP	PPTP	IPv6
🔘 Enable 💿 D)isable	PPP Setup		
PPTP Server		PPP Authentica	tion PA	P or CHAP 🔽
Specify Gateway IF	P Address	Idle Timeout	-1	second(s)
10.3	9.0.1	IP Address Assig	inment Method	(IPCP)
		WAN IP Alias		
SP Access Setup		Fixed IP: 🔘 Y	íes 💿 No (D	ynamic IP)
Username		Fixed IP Addres	ss 🗍	
Password		WAN IP Network	Settings	
Index(1-15) in <u>Sch</u>	iedule Setup:	💿 Obtain an I	P address au	tomatically
=>,	,, ,,	🔘 🔘 Specify an I	(P address	
		IP Address	10.	39.0.13
мти	1460 (Max:1460)	Subnet Mask	25:	5.255.255.0

Available settings are explained as follows:

Item	Description
PPTP/L2TP	Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
	Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.
	Disable – Click this radio button to close the connection through PPTP or L2TP.
	Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
	Specify Gateway IP Address – Specify the gateway IP address for DHCP server.
ISP Access Setup	Username -Type in the username provided by ISP in this field. The maximum length of the user name you can set is 63 characters.
	Password -Type in the password provided by ISP in this field. The maximum length of the password you can set is 62 characters.
	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.
MTU	It means Max Transmit Unit for packet. The default setting is 1460.
PPP Setup	PPP Authentication - Select PAP only or PAP or CHAP

Dray Tek

	for PPF)				
			Set the timeout for b	reaking down the		
				ne without any action.		
IP Address Assignment Method(IPCP)	and wo use WA other th	ould like t AN IP Al nan the cu	o utilize them on the as. You can set up t urrent one you are us	le public IP addresses e WAN interface, pleas o 8 public IP addresses sing.		
		21P Alias - 拥				
	172.1	5.3.143:2860/d	oc/wipalias.htm	9 +		
	WAN2	P Alias (M	ulti-NAT)	2		
		Enable	Aux. WAN IP	Join NAT IP Pool		
	1.	V	10.39.0.10			
	2.	✓	10.39.0.150			
	з.		0.0.0.0			
	4.		0.0.0.0			
	5.		0.0.0.0			
	6.		0.0.0.0			
	7.		0.0.0.0			
	8.		0.0.0.0			
	<< <u>1.8 9.16 17.24 25.32 >> Next</u> >>					
		OK Clear All Close				
	you ead your IS address this IP before functio	ch time yo P provides whenever address in you want n and typ	ou connect to it and es service to always er you request. In the n the Fixed IP field.			
WAN IP Network Settings	obtain	the IP add y an IP a	dress automatically.	ly – Click this button to radio button to specify		
	Some u		ddress – Type the II	P address.		
			et Mask – Type the			

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

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

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

AN 3	Modern Support Li
3G/4G USB Modem(PPP mode)	◯Enable ⊙Disable
SIM PIN code	
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	Apply
Modem Initial String2	AT
Modem Dial String	ATDT*99#
	(Default:ATDT*99#, CDMA:ATDT#777, TD- SCDMA:ATDT*98*1#)
Service Name	(Optional)
PPP Username	(Optional)
PPP Password	(Optional)
PPP Authentication	PAP or CHAP
Index(1-15) in <u>Schedule</u> Setup: =>,,,,	
WAN Connection Detection	
Mode	ARP Detect 😒
Ping IP	
TTL:	

Available settings are explained as follows:

Item	Description		
Modem Support List	It lists all of the modems supported by such router.		
	n2 hily //1921.06 1.1.1/sociengii:030 hila - Wandows Internet Explorer		
	4G Modern Support List		
	Last updated on 2013-05-13		
	Standard Brand Module Status		
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 pinging. 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.



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

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

AN 3	Modem Support Li
4G USB Modem(DHCP mode)	💿 Enable i 🔿 Disable
SIM PIN code	
Network Mode	46/36/26 💌 (Default:46/36/26)
APN Name	
MTU	1380 (Default:1380)
LTE software version	
LTE hardware version	
WAN Connection Detection	
Mode	ARP Detect 💌
Ping IP	
TTL:	

Item	Description		
Modem Support List	It lists all of the moderns supported by such router.		
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 19 characters.		
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.		
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply . The maximum length of the name you can set is 47 characters.		

MTU	It means Max Transmit Unit for packet. The default setting is 1380.
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.

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

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

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

WAN >> Internet Access

Static or Dynamic IP	PPTP	IPv6
Offline	*	
	Offline	

Details Page for IPv6 – PPP in WAN1/WAN2

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

No need to type any other information for PPP mode.

WAN >> Internet Access

PPPoE	Static or Dynamic IP		PPTP	IPv6
Internet Access	ode			
Connection Typ		PPP	~	
Note : IPv4 WAN	setting should be PPP	oE client.		

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



Online Status

Physical Connecti	ion			System Uptime: 0:2:32
	IPv4	IF	PV6	
LAN Status				
IP Address				
	00:201:21D:AAFF:F FF:FEA6:2568/64 (L	FEA6:2568/64 (Global) Link)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
7	4	690	328	
WAN2 IPv6 Status	3			>> Drop PPP
Enable	Mode	Up Time		
Yes	PPP	0:02:08		
IP			Gateway IP	
	00:201:21D:AAFF:F F:FEA6:256A/128 (L	FEA6:256A/128 (Global) Link)	FE80::90:1A00:2	42:AD52
DNS IP				
2001:B000:16 2001:B000:16				
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.

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

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

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

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

WAN >> Internet Access

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type	TSPC	~	
TSPC Configuration			
Username			
Password			
Confirm Password			
Tunnel Broker			



Item	Description
Username	Type the name obtained from the broker. It is suggested for you to apply another username and password for <u>http://gogonet.gogo6.com/page/freenet6-account</u> . The maximum length of the name you can set is 63 characters.
Password	Type the password assigned with the user name. The maximum length of the name you can set is 19 characters.
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.

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

PPPoE	Static or Dynamic I	Р	PPTP	IP∨6
nternet Access Mode				
Connection Type		AICCU	*	
AICCU Configuration				
📃 Always On				
Username				
Password				
Confirm Password				
Tunnel Broker	tic.sixxs.net			
Subnet Prefix			1	
If "Always On" is not e	nabled. AICCU conne	ection would only	retry three time	s.

Available settings are explained as follows:

WAN >> Internet Access

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



0

Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address getting from service provider. The maximum length of the prefix you can set is 128 characters.

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

Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2

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

WAN	>>	Internet Access

PPPoE	Sta	tic or Dynamic I	Р	PPTP	IPv6
Internet Acc	ess Mode				
Connection	Туре		DHCPv6 Client	•	
DHCPv6 Clie	nt Configuration				
Identity A	ssociation 🧕 🧕) Prefix Delegat	tion 🔘 Non-tem	porary Address	
IAID (Iden	tity Association ID)	4230640032			

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.

Details Page for IPv6 – Static IPv6 in WAN1/WAN2

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

WAN	>>	Internet Access
VVAN	_	Internet Access

PPoE	Static or Dynamic	IP	PPTP	IPv6
Internet Acc	ess Mode			
Connection	Туре	Static IPv6	~	
Static IPv6 A	ddress configuration			
IPv6 Addre	ess	/ Prefix	Length	
		/	Add	Delete
Current IP	/6 Address Table			
	ateway configuration			
	ateway configuration way Address	7		
]		

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.			
Static IPv6 Gateway Configuration	IPv6 Gateway Address - Type your IPv6 gateway address here.			

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

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

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

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

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

WAN >> Internet Access

WAN 1					
PPPoE	Static or Dyna	amic IP	PPTP/L	.2TP	IPv6
Internet A	ccess Mode				
Connectio	on Type	6in4 S	tatic Tunnel 💌		
6in4 Statio		[
Remote	Endpoint IPv4 Address				
6in4 IPv	6 Address			/ 64 (default:64)
LAN Rou	ited Prefix			/ 64 (default:64)
Tunnel 1	TTL	255 (default	:255)		
	(OK Ca	ncel		

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.

0

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

Online Status

Physical Connection IPv4				System Uptime: 0day 0:4:16
		IPv6		
LAN Status				
IP Address				
	00:83E4:21D:AAFF:FE FF:FE83:11B4/64 (Link		Global)	
TX Packets	RX Packets	TX Bytes	RX Bytes	
14	80	1244	6815	
WAN1 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	6in4 Static Tunnel	0:04:07		
IP			Gateway IP	
		lobal)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
3	26	211	2302	

Details Page for IPv6 – 6rd in WAN1/WAN2

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

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access	s Mode		
Connection Ty	ре	6rd 💌	
6rd Settings			
6rd Mode	O Auto 6rd I S	tatic 6rd	
Static 6rd Setti	ngs		
IPv4 Border I	Relay: 192.168.101.	111	
IPv4 Mask Le	ength: 0		
6rd Prefix:	2001:E41::		
6rd Prefix Ler	ngth: 32		
	ОК	Cancel	

Item	Description
6rd Mode	Auto 6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP". Static 6rd - Set 6rd options manually.
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 Connect	ion			System Uptime: 0day 0:9:18
	IPv4		IPv6	and the second
LAN Status				
IP Address				
	5:1D00:21D:AAFF: FF:FE83:11B4/64 (lobal)	
TX Packets	RX Packets	TX Bytes	RX Bytes	
15	113	1354	18040	
WAN1 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	6rd	0:09:06		
IP			Gateway IP	
(Global)	5:1D01:21D:AAFF: 51D/128 (Link)	FE83:11B5/128	<u> </u>	
TX Packets	RX Packets	TX Bytes	RX Bytes	
13	29	967	2620	

3.1.4 Multi-PVC

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

General

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

WAN >> Multi-PVC

•	ulti	D\/	IC.
	սոս	-F V	6

Adv	anced			
Enable	WAN Type	VPI/VCI	VLAN Tag	Port-based Bridge
Yes	ADSL	8/35	None	
No	Ethernet(WAN2)		None	
No	ADSL	1/43	None	
No	ADSL	1/44	None	□ Enable □ P1 □ P2 □ P3 □ P4
No	ADSL	1/45	None	Enable P1 P2 P3 P4
No	ADSL	1/46	None	□ Enable □ P1 □ P2 □ P3 □ P4
No	ADSL	1/47	None	Enable P1 P2 P3 P4
No	ADSL	1/48	None	□ Enable □ P1 □ P2 □ P3 □ P4
	Enable Yes No No No No No	YesADSLNoEthernet(WAN2)NoADSLNoADSLNoADSLNoADSLNoADSLNoADSL	Enable WAN Type VPI/VCI Yes ADSL 8/35 No Ethernet(WAN2) 1/43 No ADSL 1/43 No ADSL 1/44 No ADSL 1/45 No ADSL 1/46 No ADSL 1/46 No ADSL 1/46 No ADSL 1/46 No ADSL 1/47	EnableWAN TypeVPI/VCIVLAN TagYesADSL8/35NoneNoEthernet(WAN2)NoneNoADSL1/43NoneNoADSL1/44NoneNoADSL1/45NoneNoADSL1/46NoneNoADSL1/46NoneNoADSL1/47None



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 4 ~ 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.
VPI/VCI	Display the value for VPI and VCI.
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 (7~8) to get the following web page:

WAN >> Multi-PVC >> Channel 7

General Settings		ATM QoS	
VPI	1	QoS Type	UBR 💌
VCI	47	PCR	0
Protocol	PPPoA 🔽	SCR	0
Encapsulation	VC MUX 💌	MBS	0
🗌 Add VLAN Header			
VLAN Tag	0		
Priority	0		
Bridge mode			
Enable			
Physical Members			
□P1 □P2 □P3	P4		

OK Cancel

Item	Description	
Multi-VLAN Channel 7/8	Enable – Click it to enable the configuration of this channel.	
	Disable –Click it to disable the configuration of this channel.	
General Settings	VPI - Type in the value provided by your ISP.	
	VCI - Type in the value provided by your ISP.	
	Protocol - Select a proper protocol for this channel.	
	Encapsulation - Choose a proper type for this channel. types will be different according to the protocol setting you choose.	
	1483 Route IP LLC 1483 Bridged IP LLC 1483 Route IP LLC 1483 Route IP LLC 1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux 1483 Routed IP VC-Mux(IPoA) 1483 Bridged IP(IPoE)	
	Add VLAN Header – Check the box to enable the following two options.	
	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.	
	Priority – Choose the number to determine the packet	

	priority for such VLAN. The range is from 0 to 7.
ATM OoS	Such option is available only when WAN1 is connected with the type of ADSL.
	QoS Type - Select a proper QoS type for the channel.
	Type the values for PCR, SCR and MBS respectively.
Bridge mode	Enable – Click it to enable Bridge mode for such channel.
	Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the bridge connection.

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

WAN links for Channel 4, 5 and 6 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 4, 5 and 6 to configure your router.

Dray Tek

WAN >> Multi-PVC >> Channel 4

General Settings VPI 1 VCI 44 Protocol Encapsulation	ATM QoS QoS Type PCR SCR	UBR 💌
VCI 44 Protocol PPPoA V Encapsulation VC MUX V	PCR	
Protocol PPPoA Protocol PPOA PPOA Protocol PPOA Protocol PPOA PPOA Protocol PPOA PPOA		0
Encapsulation VC MUX 💌	SCR	
		0
	MBS	0
🗌 Add VLAN Header		
VLAN Tag D		
Priority		
Open Port-based Bridge Connection for this Char Physical Members P1 P2 P3 P4	mel	
□ Open WAN Interface for this Channel WAN Application: Management ▼ WAN Connection Detection		
Mode ARP Detect 💌		
Ping IP		
PPPoE/PPPoA Client	MPoA (RFC1483/2684)	
ISP Access Setup	○ Obtain an IP addres	s automatically
ISP Name	Router Name	∨igor *
Username	Domain Name	*
Password	*: Required for some	ISPs
PPP Authentication PAP or CHAP	Specify an IP addres	\$\$
🗹 Always On	IP Address	
Idle Timeout -1 second(s)	Subnet Mask	
IP Address From ISP	Gateway IP Address	
Fixed IP 🛛 Yes 💿 No (Dynamic IP)	DNS Server IP Address	
Fixed IP Address	Primary IP Address	8.8.8
	Secondary IP Address	8.8.4.4

Item	Description
Multi-VLAN Channel 4/5/6	Enable – Click it to enable the configuration of this channel. Disable –Click it to disable the configuration of this channel.
General Settings	VPI - Type in the value provided by your ISP.

	VCI - Type in the value provided by your ISP.
	Protocol - Select a proper protocol for this channel.Encapsulation - Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.
	VC MUX ▼ VC MUX LLC/SNAP
	Add VLAN Header – Check the box to enable the following two options.
	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.
	Priority – Choose the number to determine the packet priority for such VLAN. The range is from 0 to 7.
Open Port-based Bridge Connection for this Channel	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.
	Physical Members – Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection.
Open WAN Interface for	Check the box to enable relating function.
this Channel	WAN Application –
	 Management – It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web configuration/telnet/TR069.
	-
	• IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.
	e
ISP Access Setup for PPPoE/PPPoA Client	 interface to send IGMP packets to IPTV servers. VoIP - The VoIP configuration will allow the WAN
_	 interface to send IGMP packets to IPTV servers. VoIP - The VoIP configuration will allow the WAN interface to send VoIP packets to servers. Enter your allocated username, password and authentication parameters according to the information provided by your
_	 interface to send IGMP packets to IPTV servers. VoIP - The VoIP configuration will allow the WAN interface to send VoIP packets to servers. Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
_	 interface to send IGMP packets to IPTV servers. VoIP - The VoIP configuration will allow the WAN interface to send VoIP packets to servers. Enter your allocated username, password and authentication parameters according to the information provided by your ISP. ISP Name – Type in the name of your ISP. Username – Type in the username provided by ISP in this field. The maximum length of the name you can set is 80
_	 interface to send IGMP packets to IPTV servers. VoIP - The VoIP configuration will allow the WAN interface to send VoIP packets to servers. Enter your allocated username, password and authentication parameters according to the information provided by your ISP. ISP Name – Type in the name of your ISP. Username – Type in the username provided by ISP in this field. The maximum length of the name you can set is 80 characters. Password – Type in the password provided by ISP in this field. The maximum length of the password you can set is



	always. Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.	
	Fixed IP – Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address .	
WAN IP Network Settings for Static or Dynamic IP	Obtain an IP address automatically – Click this button to obtain the IP address automatically.	
	• Router Name – Type in the router name provided by ISP.	
	• Domain Name – Type in the domain name that you have assigned.	
	Specify an IP address – Click this radio button to specify some data.	
	• IP Address – Type in the private IP address.	
	• Subnet Mask – Type in the subnet mask.	
	• Gateway IP Address – Type in gateway IP address.	
	DNS Server IP Address - Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.	

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

Advanced

WAN >> Multi-PVCs

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

Note that such web page is available only when ADSL is selected as WAN type.

General	Advance	d			
		А	TM QoS		_
Channel	QoS Type	PCR	SCR	MBS	PVC to PVC Binding
1.	UBR 🖌	0	0	0	Disable 😽
2.	UBR 🗸	0	0	0	Disable 😪
з.	UBR 🗸	0	0	0	Disable 💌
4.	UBR 🗸	0	0	0	Disable 😪
5.	UBR 🗸	0	0	0	Disable 😽
6.	UBR 🗸	0	0	0	Disable 😽
7.	UBR 🗸	0	0	0	Disable 😽
8.	UBR 🗸	0	0	0	Disable 🗸

Note:1.If the parameters in the ATM QoS settings are set to zero,then their default settings will be used. Also,PCR(max)=ADSL Up Speed /53/8 .

2.Multiple channels may use the same ADSL channel link through the PVC Binding configuration. The PVC Binding configuration is only supported for channels using ADSL,please make sure the channel that you are binding to is using ADSL as its WAN type.The binding will work only under PPPoE and MPoA 1483 Bridge mode.





Item	Description			
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides.			
PCR	It represents Peak Cell Rate. The default setting is "0".			
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.			
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.			
PVC to PVC Binding	It allows the PVC channel to use the same ADSL connection settings of another PVC channel. Please choose the PVC channel (must be enabled first) via the drop down list. This option is available only when the PVC channel is enabled on the General tab.			

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

3.2 LAN

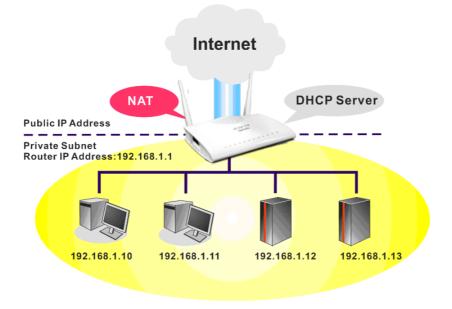
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

LAN
General Setup
Static Route
VLAN
Bind IP to MAC
LAN Port Mirror
Web Portal Setup
NAT

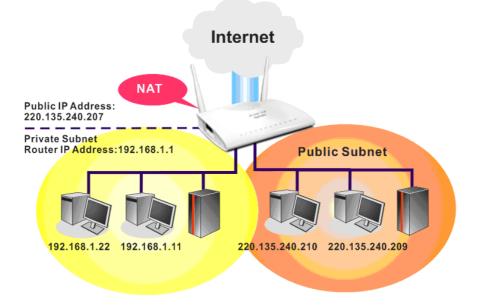
3.2.1 Basics of LAN

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





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



What is Routing Information Protocol (RIP)

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

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.



What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 8 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.

3.2.2 General Setup

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

There are six 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	V	V	192.168.1.1	Details Page	IPv6
LAN 2	✓		10.39.0.13	Details Page	
IP Routed Subnet			192.168.0.1	Details Page	

Advanced You can configure DHCP server options here.

Force router to use "DNS server IP address" settings specified in LAN1

Inter-LAN Routing	

Subnet	LAN 1	LAN 2
LAN 1	V	
LAN 2		V

Note: LAN 2 is available when VLAN is enabled.

OK

Item	Description
General Setup	Allow to configure settings for each subnet respectively.
	Index - Display all of the LAN items.
	Status- Basically, LAN1 status is enabled in default. LAN2 –LAN6 and IP Routed Subnet can be observed by checking the box of Status .
	DHCP- LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.
	IP Address - Display the IP address for each LAN item. Such information is set in default and you can not modify it.
	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.
	IPv6 – Click it to access into the settings page of IPv6.
Advanced	DHCP packets can be processed by adding option number and data information when such function is enabled.



	LAN >> General Setup
	DHCP Options Status
	O Enable Obisable Options List
	Index Option Number Ascii/Hex Data
	Option Number:
	DataType:
	Add Delete
	Note: Maximum number of custom DHCP option is five.
	OK
	Enable/Disable – Enable/Disable the function of DHCP
	Option. Each DHCP option is composed by an option
	number with data. For example,
	Option number:100
	Data: abcd
	When such function is enabled, the specified values for
	DHCP option will be seen in DHCP reply packets.
	Option Number – Type a number for such function.
	DataType – Choose the type (ASCII or Hex) for the data to
	be stored.
	Data – Type the content of the data to be processed by the function of DHCP option.
Force router to use DNS	Force Vigor router to use DNS servers configured in
server IP address	LAN1/LAN2/LAN3/LAN4/LAN5/LAN6 instead of DNS
	servers given by the Internet Access server (PPPoE, PPTP,
	L2TP or DHCP server).
Inter-LAN Routing	Check the box to link two or more different subnets (LAN
	and LAN).

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

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

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

LAN 1 Ethernet TCP / IP a	nd DHCP Setup	LAN 1 IPv6 Setup			
Network Configuration		DHCP Server Configuration			
For NAT Usage		💿 Enable Server 🔘 Dis	able Se	rver	
IP Address	192.168.1.1	Enable Relay Agent			
Subnet Mask	255.255.255.0	Start IP Address	192.16	3.1.10	
		IP Pool Counts	200		
RIP Protocol Control	Disable 💙	Gateway IP Address	192.16	3.1.1	
Note: Disable LAN & Enable LAN shouldn't be in the same subnet.		Lease Time	86400		(s)
		Retrieve IPs from inactive clients periodically			
		DNS Server IP Address			
		Primary IP Address			
		Secondary IP Address			
		· ·			

LAN >> General Setup

_		_
()	017	
	- NK	

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



	request to.
	• 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.
	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.
	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.
	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.
	Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.
	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 DHCF 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).
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	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.
	Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:

Online Status			
Physical Connection	.4	IPv6	System Uptime: 22:22:45
LAN Status		/ DNS: 8.8.8.8	Secondary DNS: 8.8.4.4
IP Address	TX Packets	RX Packets	Secondary DNS: 0.0.4.4
192.168.1.1	0	41533	
left empty, th users as a DI If the IP add cache, the ro Otherwise, th	the router with NS proxy set ress of a do uter will re- the router for S server by	ill assign its or erver and main omain name is solve the dom orwards the DM establishing a	IP Address fields are wn IP address to local ntain a DNS cache. already in the DNS nain name immediately. NS query packet to the wAN (e.g.

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

Details Page for LAN1 – IPv6 Setup

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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Router Advertisement Server	
⊙Enable ○Disable	
Advertisement Lifetime 1800	Seconds (Range : 600 - 9000)
DHCPv6 Server	
O Enable Server O 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 / Add Delete	
Current IPv6 Address Table	
Index IPv6 Address/Prefix 1 FE80::21D:AAFF:FEB8	
	V

OK

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

Item	Description
Router Advertisement Server	 Enable – Click it to enable router advertisement server. The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration. Disable – Click it to disable RADVD server.
	Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.
DHCPv6 Server	Enable Server –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.
	Disable Server –Click it to disable DHCPv6 server.
	Start IPv6 Address / End IPv6 Address – Type the start and end address for IPv6 server.
DNS Server IPv6 Address	Primary DNS Sever – Type the IPv6 address for Primary DNS server.
	Secondary DNS Server – Type another IPv6 address for DNS server if required.
Static IPv6 Address	IPv6 Address – Type static IPv6 address for LAN.
configuration	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 used IPv6 addresses.

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

Details Page for LAN2

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup			
Network Configuration		DHCP Server Configuration	
○ Enable		⊙Enable Server ○Disable Server	
⊙ For NAT Usage	○ For Routing Usage	🔲 Enable Relay Agent	
IP Address	192.168.2.1	Start IP Address	192.168.2.10
Subnet Mask	255.255.255.0	IP Pool Counts	100
Note: Disable LAN & Enable LAN shouldn't be in the same subnet.		Gateway IP Address	192.168.2.1
		Lease Time	259200 (s)
		🗹 Retrieve IPs from ina	active clients periodically
		DNS Server IP Address	
		Primary IP Address	0.0.0.0
		Secondary IP Address	0.0.0.0

ОК

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.
	For NAT Usage - Click this radio button to invoke NAT function.
	For Routing Usage - Click this radio button to invoke this function.
	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)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server – Let you manually assign IP address to every host in the LAN.
	Enable Relay Agent - 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.
	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.
	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.
	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.
	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.
	Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.
	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).
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	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.
	Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
	The default DNS Server IP address can be found via Online Status:
	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
	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.

Details Page for IP Routed Subnet

LAN >> General Setup

TCP/IP and DHCP Setup	for IP Routed Subnet		
Network Configuration		DHCP Server Configuration	
○Enable ⊙Disable For Routing Usage		Start IP Address	
IP Address	192.168.0.1	IP Pool Counts	0 (max. 32)
Subnet Mask	255.255.255.0	Lease Time	259200 (s)
RIP Protocol Control Note: Disable LAN & En the same subnet.	Disable 💙 able LAN shouldn't be in	Use LAN Port Use MAC Address Index Matched MAC Add	P1 P2
		Add Delete	Edit Cancel
		OK	

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.
	For Routing Usage,
	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)
	RIP Protocol Control,
	Disable - deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	Enable – activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your



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

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

3.2.3 Static Route

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

Static Route for IPv4

LAN >> Static Route Setup

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

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

Item	Description		
Index	The number (1 to 10) under Index allows you to open next page to set up static route.		
Destination Address	Displays the destination address of the static route.		
Status	Displays the status of the static route.		
Set to Factory Default	Clear all of the settings and return to factory default settings.		
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table Current Running Routing Table IPv6 Routing Table Refresh Key: C - connected, S - static, R - RIP, * - default, ~ - private Image: C - 192.168.1.0/ 255.255.258.0 Image: C - 192.168.1.0/ 255.255.258.0		

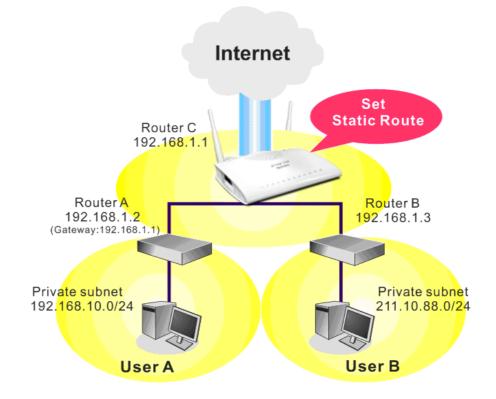
Available settings are explained as follows:

Add Static Routes to Private and Public Networks

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

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

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



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

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

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

LAN >> Static Route Setup

Index No. 1		
🗹 Enable		
	Destination IP Address	192.168.1.10
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN1 💌

Available settings are explained as follows:

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

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

LAN	>>	Static	Route	Setup

Index No. 2 Image: Second se	
Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN1 💌
Note: WAN4, WAN5, WAN6 are router-borne WAN	s.
OK (Cancel Delete

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

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
S~ 192.168.10.0/ 255.255.2 C~ 192.168.1.0/ 255.255.2	R - RIP, * - default, ~ - private 55.0 via 192.168.1.2 LAN1 55.0 directly connected LAN1 55.0 via 192.168.1.3 LAN1	
		~

Static Route for IPv6

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

LAN >> Static Route Setup

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

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

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

Available settings are explained as follows:

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

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

LAN >> Static Route Setup

Index No. 1		
Destination IPv6 Address / Prefix Len	::	/ 0
Gateway IPv6 Address]
Network Interface	LAN 💌	
ОК	Cancel Delete	

Available settings are explained as follows:

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

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



3.2.4 VLAN

With the 6-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 models (Vigor2760n/Vigor2760Vn), each of the wireless SSIDs can also be grouped within one of the VLANs.

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.

Below is an example page in Vigor2760n:

VLAN Configuration 🗹 Enable LAN Wireless LAN P1 P2 Ρ3 P4 SSID1 SSID2 SSID3 SSID4 Subnet VLAN0 **~ ~ ~** \checkmark **V** \checkmark **V** LAN 1 🔽 VLAN1 **~** LAN 2 🔽 VLAN2 LAN 1 🔽 VLAN3 LAN 1 🔽 VLAN4 LAN 1 🔽 VLAN5 LAN 1 🔽 VLAN6 LAN 1 🔽 VLAN7 LAN 1 🔽



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

Item	Description
Enable	Click it to enable VLAN configuration.
LAN	P1 - P4 – Check the LAN port(s) to group them under the selected VLAN.
Wireless LAN	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.

LAN	1	*
LAN	1	
LAN	2	

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

Vigor2760 series features a hugely flexible VLAN system. In its simplest form, each of the Gigabit LAN ports can be isolated from each other, for example to feed different companies or departments but keeping their local traffic completely separated.

Configuring port-based VLAN for wireless and non-wireless clients

- 1. All the wire network clients are categorized to group VLAN0 in subnet 192.168.1.0/24 (LAN1).
- 2. All the wireless network clients are categorized to group VLAN1 in subnet 192.168.2.0/24 (LAN2).
- 3. Open LAN>>VLAN Configuration. Check the boxes according to the statement in step 1 and Step 2.

LAN >> VLAN Configuration

		L	AN			Wirele	ss LAN		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet
VLAN0	~	~	~	✓					LAN 1 🔽
VLAN1					~	~	~	~	LAN 2 🔽
VLAN2									LAN 1 💌
VLAN3									LAN 1 💌
VLAN4									LAN 1 💌
VLAN5									LAN 1 💌
VLAN6									LAN 1 💌
VLAN7									LAN 1 💌

- 4. Click **OK**.
- 5. Open LAN>>General Setup. If you want to let the clients in both groups communicate with each other, simply activate Inter-LAN Routing by checking the box between LAN1 and LAN2.



LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2		~	192.168.2.1	Details Page	
IP Routed Subnet			192.168.0.1	Details Page	

Advanced You can configure DHCP server options here.

Force router to use "DNS server IP address" settings specified in LAN1 📝

Inter-LAN Routing				
Subnet	LAN 1	LAN 2		
LAN 1	\checkmark			
LAN 2	\checkmark			

Note: LAN 2 is available when VLAN is enabled.

OK 🗌

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

3.2.5 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

Bind IP to MAC							
🔘 Enable 🧕 🧕	🛛 Disable 🛛 Strict Bind						
ARP Table	<u>Select All</u> Sort Refre	sh	IP Bind I	List (Limit: 30	0 entries)	Selec	<u>:t All Sort</u>
IP Address	Mac Address	^	Index	IP Address	Mac	Address	~
10.28.60.12	00-50-7F-22-33-43	>					
Add or Update							
IP Address							
Mac Address							
Comment							~
						📃 Shov	v Comment
	Add		Update	Delete			

Note: IP-MAC binding presets DHCP Allocations.

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

Backup IP Bind List :	Upload From File: (選擇檔案) 未選擇檔案
Backup	Restore

OK

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking 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	 IP Address – Type the IP address that will be used for the specified MAC address. Mac Address – Type the MAC address that is used to bind with the assigned IP address. Comment – Type a brief description for the entry.
	Show Comment – Check this box to display the comment on IP Bind List box.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in 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.

3.2.6 LAN Port Mirror

LAN port mirror can be applied for the users in LAN. Generally speaking, this function copies traffic from one or more specific ports to a target port. This mechanism helps manager track the network errors or abnormal packets transmission without interrupting the flow of data access the network. By the way, user can apply this function to monitor all traffics which user needs to check.

There are some advantages supported in this feature. First, it is more economical without other detecting equipments to be set up. Second, it may be able to view traffic on one or more ports within a VLAN at the same time. Third, it can transfer all data traffics to be mirrored to one analyzer connect to the mirroring port. Last, it is more convenient and easy to configure in user's interface.

LAN >> LAN Port Mirror

LAN Port Mirror				
Port Mirror:				
💿 Enable 🔘 Disabl	e			
Mirror port:				
○P1	○ P2	Орз	○ P4	
Mirrored port:				
P 1	P 2	🗖 РЗ	P 4	
		OK		

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.



3.2.7 Web Portal Setup

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

LAN >> Web Portal Setup

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

Each item is explained as follows:

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

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

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

```
Profile Index: 1
```

💿 Disable						
◯ URL Redirect	http://					
	e.g. http://www.draytek.com					
○ Message	<h1>Vigor</h1> <h2> - Reliable connectivity</h2> <h2> - Robust firewall protection</h2> <h2> - Multi-site secure communication</h2>					
Applied Interfaces	(Max 511 characters)					
Applica Interfaces						
2.4G SSID	SSID1 SSID2 SSID3 SSID4					



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.

3.3 Route Policy

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

Route P	olicy											•
Route P	olicy								<u> </u>	et to Fa	ctory D	<u>efault</u>
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Dowr
1		Any	WAN1									Down
2		Any	WAN1								<u>UP</u>	Dowr
<u>3</u>		Any	WAN1								<u>UP</u>	Dowr
<u>4</u>		Any	WAN1								<u>UP</u>	Dowr
<u>5</u>		Any	WAN1								<u>UP</u>	Down
<u>6</u>		Any	WAN1								<u>UP</u>	Down
<u>7</u>		Any	WAN1								<u>UP</u>	Down
<u>8</u>		Any	WAN1								<u>UP</u>	Down
<u>9</u>		Any	WAN1								<u>UP</u>	Dowr
<u>10</u>		Any	WAN1								<u>UP</u>	Down

Wizard Mode: most frequently used settings in three pages

O Advance Mode: all settings in one page

OK

Available settings are explained as follows:

Item	Description
Index	Click the number of index to access into the configuration web page.

Enable	Check this has to anable this policy					
Lilable	Check this box to enable this policy.					
Protocol	Display the protocol used for this policy.					
Interface	Display the interface to send packets to once the policy is matched.					
Interface Address	Display the WAN IP or WAN IP alias address which is used as source IP of the outgoing packets.					
Src IP Start	Displays the IP address for the start of the source IP.					
Src IP End	Displays the IP address for the end of the source IP.					
Dest IP Start	Displays the IP address for the start of the destination IP.					
Dest IP End	Displays the IP address for the end of the destination IP.					
Dest Port Start	Displays the IP address for the start of the destination port.					
Dest Port End	Displays the IP address for the end of the destination port.					
Move UP/Move Down	Use Up or Down link to move the order of the policy.					
Wizard Mode	Allows to configure frequently used settings of route policy via three setting pages					
Advance Mode	Allows to configure detailed settings of route policy.					

To use Wizard Mode, simple do the following steps:

- 1. Click the **Wizard Mode** radio button.
- 2. Click **Index 1**. The setting page will appear as follows:

Route Policy

Index: 1 Criteria		
Load-Balance/Rou	ute Policy applies to pack	xets that meet the following criteria
Source IP	💿 Any	
	🔘 Src IP Start	Src IP End
		~
Destination IP	🔘 Any	
	💿 Dest IP Start	Dest IP End
	192.168.1.6	~ 192.168.1.66
		<pre>< Back Next > Finish Cancel</pre>

Item	Description			
Source IP	Any – Any IP can be treated as the source IP.			
	Src IP Start - Type the source IP start for the specified WAN interface.			
	Src IP End - Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN			

	interface.
Destination IP	Any – Any IP can be treated as the destination IP.
	Dest IP Start- Type the destination IP start for the specified WAN interface.
	Dest IP End - Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

3. Click **Next** to get the following page.

Index: 1 Interface								
Load-Balance/Route Policy d	lirects the packet	ts to	the int	terface	below			
Interface	LAN1	~						
	LAN2 IP Routed Subnet WAN1 WAN2 WAN3 WAN4	: E	3ack	Ne	xt >	Fin	ish	Cancel

Available settings are explained as follows:

Item	Description
Interface	Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.

4. After specifying the interface, click **Next** to get the following page.

Route Policy

: 1 NAT or Ro	uting
Based or NAT	n the settings in the previous pages, we guess you want to have: Force
The curre	ent setting is:
\odot	Force NAT
0	Force Routing

< Back Next > Finish Cancel

Item	Description
Force NAT /Force Routing	It determines which mechanism that the router will use to forward the packet to WAN.

5. After choosing the mechanism, click **Next** to get the summary page for reference.

Route Policy

Criteria	
Source IP	Any
Destination IP	$192.168.1.6 \sim 192.168.1.66$
Interface	
WAN1	
More options	
Force NAT	

6. If there is no error, click **Finish** to complete wizard setting.

Route P	olicy											0
Route Policy Set to Factory Default												
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	IP	Dest IP Start	Dest IP End	Dest Port Start		Move Up	Move Down
<u>1</u>	~	Any	WAN1		Any	Any	192.168.1.6	192.168.1.66	Any	Any		<u>Down</u>
2		Any	WAN1								<u>UP</u>	Down
<u>3</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
4		Any	WAN1								UP	Down
<u>5</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>6</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
7		Any	WAN1								<u>UP</u>	<u>Down</u>
8		Any	WAN1								UP	Down
<u>9</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>10</u>		Any	WAN1								<u>UP</u>	<u>Down</u>

• Wizard Mode: most frequently used settings in three pages

O Advance Mode: all settings in one page

OK

To use Advance Mode, do the following steps:

- 1. Click the Advance Mode radio button.
- 2. Click **Index 1** to access into the following page.

Protocol	Any 🗸	
Source IP	Any	
	<u> </u>	Src IP End
	~	
Destination IP	Any	
	🔘 Dest IP Start 🛛 🛛	Dest IP End
	~	
	💿 Any	
Destination Port	🔵 Dest Port Start 🛛 🛛	Dest Port End
	~	
Send to if Criteria Matched		
Interface	WAN1	
Gateway IP	🕟 Default Gateway	
	🍈 Specific Gateway 🗌	
More Options		
Auto Failover to the Oth	er WAN	
Packet Forwarding to WAN	Force NAT	
via	O Force Routing	

Note: 1. Force NAT(Routing): NAT(Routing) will be performed on outgoing packets, regardless of which type of subnet (NAT or IP Routing) they originate from.
 2. Please use the "Any" with caution. The settings applied here have higher priority than the static routes rules and the routes in the routing table.

Item	Description
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source IP	 Any – Any IP can be treated as the source IP. Src IP Start - Type the source IP start for the specified WAN interface. Src IP End - Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.



Destination IP	Any – Any IP can be treated as the destination IP.
	Dest IP Start- Type the destination IP start for the specified WAN interface.
	Dest IP End - Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Destination Port	Any – Any port number can be treated as the destination port.
	Dest Port Start - Type the destination port start for the destination IP.
	Dest Port End - Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if criteria matched	Interface – Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.
	Gateway IP – Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.
More options	Auto Failover To The Other WAN – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is down.
	Packet Forwarding to WAN via – Choose Force NAT or Force Routing .

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

Route P	olicy								Se	t to Fac	ctory E	Default
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Port '		Move Down
1	V	Any	WAN1		Any	Any	192.168.1.6	192.168.1.66	Any	Any		<u>Down</u>
2	~	TCP	WAN2		192.168.1.11	192.168.1.11	Any	Any	Any	Any	<u>UP</u>	Down
3		Any	WAN1								<u>UP</u>	<u>Down</u>
4		Any	WAN1								<u>UP</u>	Down
<u>5</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
6		Any	WAN1								<u>UP</u>	Down
Z		Any	WAN1								<u>UP</u>	<u>Down</u>
8		Any	WAN1								<u>UP</u>	Down
<u>9</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>10</u>		Any	WAN1								<u>UP</u>	<u>Down</u>

🔘 Wizard Mode: most frequently used settings in three pages

● Advance Mode: all settings in one page

OK)

0

3.4 NAT

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

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

The benefit of the NAT includes:

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

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

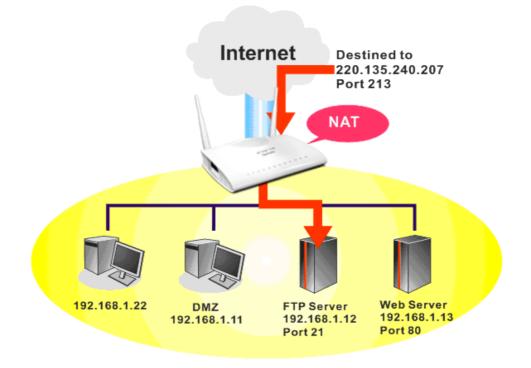
Below shows the menu items for NAT.



3.4.1 Port Redirection

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





The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 40 port-mapping entries for the internal hosts.

Port Red	Port Redirection Set to Factory Default							
Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status		
<u>1.</u>		All				×		
<u>2.</u>		All				×		
<u>3.</u>		All				×		
4.		All				×		
<u>5.</u>		All				×		
<u>6.</u>		All				×		
<u>7.</u>		All				×		
<u>8.</u>		All				×		
<u>9.</u>		All				×		
<u>10.</u>		All				×		
< <u> 1-10</u>	<u>11-20 21-30 31-</u>	<u>40</u> >>				<u>Next</u> >>		

NAT >> Port Redirection

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

Item Description			
IndexDisplay 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.		

Each item is e	xplained as follows:
----------------	----------------------



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 Range
Protocol	[×]
WAN IP	1.All 💌
Public Port	0
Private IP	-
Private Port	0

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

OK	Clear	Cancel

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.

System Maintenance >> Management

	IPv4 Management	Setup	IPv6 Management Setup		
Route	r Name		Management Port Setu	р	
			🔄 💿 User Define Ports	🔘 Defa	ault Ports
	efault:Disable Auto-L	ogout	Telnet Port	23	(Default: 23)
Intern	et Access Control		HTTP Port	8276	(Default: 80)
🗹 🖂	low management fro	m the Internet	HTTPS Port	443	(Default: 443)
	FTP Server		FTP Port	21	(Default: 21)
I –	HTTP Server		TR069 Port	8069	(Default: 8069)
I –	HTTPS Server		SSH Port	22	(Default: 22)
	Telnet Server			~~	
	TR069 Server SSH Server		External Device Control	I	
	sable PING from the	Internet	No respond to Exte	rnal Devi	ce
	sable Ping from the	Internet	_		
LAN A	ccess Control				
🗹 🗹	low management fro	m LAN			
	FTP Server				
	HTTP Server				
	HTTPS Server				
	Telnet Server				
	SSH Server				
	оју То				
	LAN2				
	IP Routed Subnet				
Acces	s List from the Interne	et			
List	IP	Subnet Mask			
1		~			
2		~			
з [*			
		od to poposs all the rou			

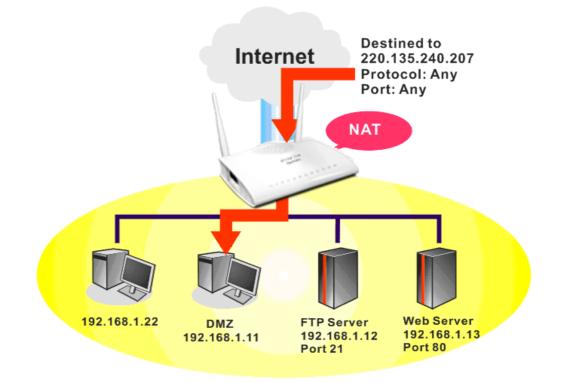
Note: LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.

OK



3.4.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

DMZ Host Setup		
WAN1	WAN2	WAN3
WAN 1		
None 💌		
Private IP		Choose IP
MAC Address of the True IP D	MZ Host 00 · 00 · 00 · 00 · 00	
Note : When a True-IP DMZ H always on.	nost is turned on, it will force the ro	outer's WAN connection to be

ΟK

Available settings are explained as follows:
--

Item	Description
WAN 1 None Private IP Active True IP	Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. Impulsion Impulsion 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. Imput Host Setup Imput Host Inter IP DMZ Host is turned on , it will force the router's WAM connection to be Imput Host Setup Imput Host Inter IP DMZ Host is turned on , it will force the router's WAM connection to be Imput Host Setup Imput Host Inter IP DMZ Host is turned on , it will force the router's WAM connection to be Imput Host Setup Imput Host Inter IP DMZ Host is turned on , it will force the router's WAM connection to be Imput Host Setup

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

See the following figure.

)MZ Host Setup		
WAN1	WAN2	WAN3
WAN 2		
Enable	Private IP	
	0.0.0	Choose 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.

MZ Host S	etup			
	WAN1		WAN2	WAN3
WAN 2 Index	Enable	Aux. WAN IP	Private IP	
1.		10.39.0.10	0.0.0.0	Choose IP
2.		10.39.0.150	0.0.0	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	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host. The selection of the selected one private IP from the above dialog, the IP address will be shown on the screen. Click OK to save the setting.

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



3.4.3 Open Ports

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

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

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

NAT	>>	Open	Ports
-----	----	------	-------

Open Ports Setup		Set	to Factory Default
Index	Comment	Local IP Address	Status
<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>			×
<< <u>1-10 11-20 21-30</u>	<u>) 31.40 >></u>		<u>Next</u> >>

Note: The configured ports in the $\underline{Management}$ webUIs will be used by the router and not be sent to the local computer defined here.

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.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
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.

NAT >> Open Ports >> Edit Open Ports

🗹 E	nable Open Por	ts				
	Com	ment	P226			
	Priva	ate IP	10.39.0.	11 Choos	e IP	
	Protocol	Start Port	End Port	Protocol	Start Port	End Port
1.	TCP 💌	80	80 :	2 💌	0	0
з.	💙	0	0	4. 🔤 🕶	0	0
5.	💙	0	0	5 💌	0	0
7.	¥	0	0	3 💙	0	0
9.	¥	0	0 1	0. 🔤	0	0

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.
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	Local IP Address	Status
<u>1.</u>	P226	10.39.0.11	v
<u>2.</u>			×
<u>3.</u>			×
<u>4.</u>			×
<u>5.</u>			×
<u>6.</u>			×
<u>7.</u>			х
<u>8.</u>			×
<u>9.</u>			х
<u>10.</u>			×
<< 1-10 11-20 21-3	<< 1-10 11-20 21-30 31-40 >> Nex		

Note: The configured ports in the <u>Management</u> webUIs will be used by the router and not be sent to the local computer defined here.

3.4.4 Port Triggering

Port Triggering is a variation of open ports function.

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

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

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAT >> Port Triggering

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

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.

NAT >> Port Triggering

No. 1

Enable	
Service	User Defined 💌
Comment	
Triggering Protocol	TCP 💌
Triggering Port	80
Incoming Protocol	UDP 🗸
Incoming Port	1024
Note: The Triggering Port and Incoming P 123-456,777-789 (legal),123-456,789 (le	
	ear Cancel

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile. User Defined User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent
Comment	Type the text to memorize the application of this rule.



Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.
Triggering Port	Type the port or port range for such triggering profile.
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.
Incoming Port	Type the port or port range for the incoming packets.

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

3.5 Firewall

3.5.1 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:

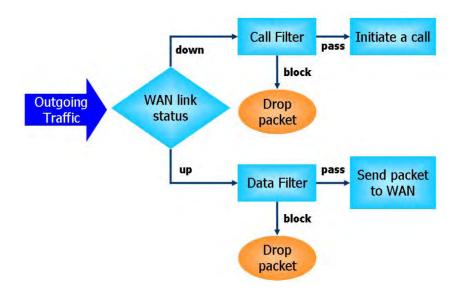
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

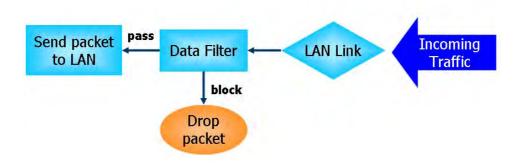
IP Filters

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

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

Below shows the menu items for Firewall.

Firewall General Setup Filter Setup DoS Defense



3.5.2 General Setup

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

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

General Setup Page

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

Firewall >> General Setup

eneral Setup	Default Rule	
Call Filter	 Enable 	Start Filter Set 🛛 Set#1 🛛 👻
	🔘 Disable	
Data Filter	💿 Enable	Start Filter Set 🛛 Set#2 🛛 🐱
	🔘 Disable	
CS) 🗹 Enable Str	ge incoming fragmented ict Security Firewall) packet from WAN	l UDP or ICMP packets (for some games, ex.
CS) CS) Enable Str Accept routing IPv4	ict Security Firewall 3 packet from WAN IPv6	
CS) Enable Str Accept routing IPv4 Note: The pack	ict Security Firewall 9 packet from WAN IPv6 <ets be="" filtered="" td="" will="" with<=""><td>the follow function sequentially:</td></ets>	the follow function sequentially:
CS) Enable Str Accept routing IPv4 Note: The pack 1. Accept I 2. Data Fil	ict Security Firewall) packet from WAN IPv6 kets will be filtered with Routing Packet from WA ter Set and Rule in Fire	the follow function sequentially: N
CS) Enable Str Accept routing IPv4 Note: The pack 1. Accept I 2. Data Fil	ict Security Firewall 9 packet from WAN IPv6 kets will be filtered with Routing Packet from WA	the follow function sequentially: N

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.
Accept routing packet from WAN	 Usually, IPv6 network sessions/traffic from WAN to LAN will be blocked by IPv6 firewall to prevent remote client accessing into the PCs on LAN in default. IPv6 - Check the box to make the packets (routed from WAN to LAN) via IPv6 being accepted 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 accepted by such router. It is effective only for the packet the incoming packets via IPv4 being accepted by such router.
	IPv4 being accepted by such router. It is effective only for the packets routed but not for packets translated by NAT.

Default Rule Page

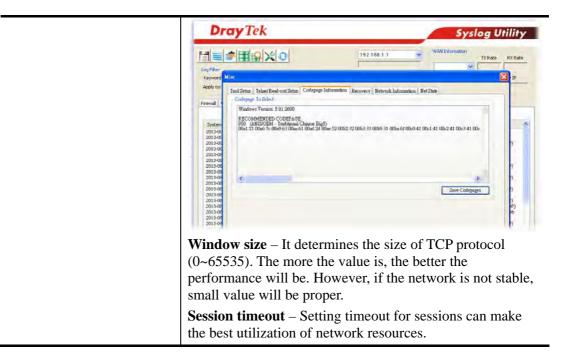
Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

eneral Setup Default R	uie		
Actions for default rule:			
Application	Action/Profile	Syslog	
Filter	Pass 💌		
Sessions Control	0 / 32000		
Quality of Service	None 💌		
APP Enforcement	None 💌		
URL Content Filter	None 💌		
Web Content Filter	None 💌		
Advance Setting	Edit		

Item	Description	
Filter	Select Pass or Block for the packets that do not match with the filter rules.	
	Filter Pass V Pass Block	
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None None Class 1 Class 2 Class 3 Default	
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select,	



	page to create a new follow the standard of profile selected here. section of APP Enfo troubleshooting need for IM/P2P by check	te New] from the drop down list in this profile. All the hosts in LAN must configured in the APP Enforcement . For detailed information, refer to the prement profile setup. For ls, you can specify to record information ting the Log box. It will be sent to the refer to section Syslog/Mail Alert for nation.
URL Content Filter	(created in CSM>> 1 this router. Please set CSM>> URL Conte [Create New] from t a new profile. For tro record information for the Log box. It will b	L Content Filter profile settings URL Content Filter) for applying with t at least one profile for choosing in ent Filter web page first. Or choose the drop down list in this page to create publeshooting needs, you can specify to or URL Content Filter by checking be sent to Syslog server. Please refer to Alert for more detailed information.
Web Content Filter	(created in CSM>> this router. Please set CSM>> Web Conte [Create New] from t a new profile. For tro record information for Log box. It will be set	b Content Filter profile settings Web Content Filter) for applying with t at least one profile for anti-virus in ent Filter web page first. Or choose the drop down list in this page to create publeshooting needs, you can specify to or Web Content Filter by checking the ent to Syslog server. Please refer to Alert for more detailed information.
Advance Setting	-	ne following window. However, it is ded to use the default settings here.
	Advance Setting Codepage Window size: Session timeout:	ANSI(1252)-Latin I
	among different lang help the system obtain from URL and enhar Filter. The default van I. If you do not choor URL will be procession choose a codepage. If you do not have an please open Syslog.	OK Close Action is used to compare the characters guages. Choose correct codepage can ining correct ASCII after decoding data ace the correctness of URL Content lue for this setting is ANSI 1252 Latin se any codepage, no decoding job of ed. Please use the drop-down list to ny idea of choosing suitable codepage, From Codepage Information of Setup the recommended codepage listed on



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



3.5.3 Filter Setup

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

Firewall >> Filter Setup

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1					
Comments :	Default Call Filter]			
Filter Rule	e Active	Comments		Move Up Mo	ove Down
1	\checkmark	Block NetBios			<u>Down</u>
2				<u>UP</u>	<u>Down</u>
3				<u>UP</u>	<u>Down</u>
4				<u>UP</u>	<u>Down</u>
5				<u>UP</u>	<u>Down</u>
6				<u>UP</u>	<u>Down</u>
7				<u>UP</u>	
				Next Filter Set	None 💌
	C	K Clear	Cancel		

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered $(1 \sim 7)$ to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23-character long.
Move Up/Down	Use 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.

Dray Tek

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

Firewall >> Edit Filter Set >> Edit Filter Rule

🗹 Check to enable the Filter Rul	le	
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule ON:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to any	Edit
Fragments:	Don't Care 🔽	
Application	Action/Profile	Syslog
Filter:	Block Immediately 🛛 👻	
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	

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. LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN



Source/Destination IP	Click Edit to access into the following dialog to choose
	source/destination IP or IP ranges.
	/ IP Address Edit - Windows Internet Explorer
	http://192.168.1.1/doc/pfipedt.htm
	IP Address Edit
	Address Type Any Address 💌
	Start IP Address 0.0.0.0
	End IP Address 0.0.0.0
	Subnet Mask 0.0.0.0
	Invert Selection
	or IP Object None
	or IP Object None 🗸
	or IP Object None
	or IPv6 Object None
	or IPv6 Object None
	or IPv6 Object None
	OK Close
	To set the IP address manually, please choose Any
	addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects as
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects ♥ Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose
Service Type	 groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type.
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type.
Service Type	 groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type.
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Subnet Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit - Windows Internet Explorer Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit - Windows Internet Explorer Intry/192.1681.1/doc/ptext.txx
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. ✓ Service Type Edit - Windows Internet Explorer Service Type Edit Service Type Edit Service Type Edit Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. ✓ Service Type Edit - Windows Internet Explorer Imp/1921681.1dec/nptedthm Service Type Edit Service Type Edit Service Type Edit Service Type Edit Imp/1921681.1dec/nptedthm
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. ✓ Service Type Edit - Windows Internet Explorer Imput/19216811/doc/nteel.htm Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. ✓ Service Type Edit - Windows Internet Explorer Imp/1921681.1doc/ntedthen Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit None Image Service Object None Image Service Object
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Range Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit Service Type Edit
Service Type	groups or objects, please choose Group and Objects as Address Type. Group and Objects Any Address Single Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that y want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose suitable service type. Service Type Edit Service Type Edit Service Type Edit Service Object None or Service Object

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



	default setting is 60000.
MAC Bind IP	Strict - Make the MAC address and IP address settingsconfigured in IP Object for Source IP and Destination IPbe bound for applying such filter rule.No-Strict - no limitation.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default
APP Enforcement	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.
URL Content Filter	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.
URL Content Filter	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.
Web Content Filter	 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.
Advance Setting	Click Edit to open the following window. However, it is strongly recommended to use the default settings here. Firewall >> Edit Filter Set >> Edit Filter Rule
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Compare the security Checking Strict Security Checking APP Enforcement
	OKCloseCodepage - 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
	Dray Tek Syslag Utility Image: State S
	 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.
The requested Web page has been blocked by Web Content Filter.
The requested web page has been blocked by web content riter.
Please contact your system administrator for further information.
[Powered by Draytek]
v
Strict Security Checking - All the packets, while
•
transmitting through Vigor router, will be filtered by
firewall settings configured by Vigor router. When the
resource is inadequate, the packets will be blocked if Strict
Security Checking is enabled. If Strict Security Checking is
not enabled, then the packets will pass through the router.

Example

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

al Setup					
General Setup	Default Rule				
Call Filter	Enable Disable	Start Filter Set Set#1 v			
Data Filter	 Enable Disable 	Start Filter Set Set#2 🛩			
	e incoming fragmented l ct Security Firewall	JOP or ICMP packets (for some gi	Firewall >> Filter Setup		
			Filter Setup		Set to Factory Defa
			Set Comments	Set	Comments
			1. Default Call Filter	1.	
	OK	Cancel	 Default Data Filter 3. 	<u>8.</u> 2.	
			4	10.	
			5.	11.	
			6.	12.	
Firewall >> F Filter Set 1 Comments :	Ilter Setup >> Edit Filter S		Firewall>> Edit Fifter Set >> Edit Fifter Rule		
Filter Set 1 Comments :	Default Call Filter Active	Comments	Filter Set 1 Rule 1		
Filter Set 1 Comments :	Default Call Filter	2		le	
Filter Set 1 Comments :	Default Call Filter Active	Comments	Filter Set 1 Rule 1		
Filter Set 1 Comments :	Default Call Filter Active	Comments	Filter Set 1 Rule 1 Check to enable the Filter Ru Comments: Index(1-15) in <u>Schedule</u> Setup: Clear sequences when schedule	le	
Filter Set 1 Comments : 1 2 3 4	Default Call Filter Active I	Comments	Filter Set 1 Bute 1 Filter Set 1 Comments: Comments: Index(1-15) in <u>Schedule</u> Setup: Clear sessions when schedule ON:	le Block NetBins	
Filter Set 1 Comments : Ther Rom	Default Call Filter Active (2)	Comments	Filter Set 1 Rule 1 Check to enable the Filter Ru Comments: Index(1-15) in <u>Schedule</u> Setup: Clear sequences when schedule	Block NetBios	Edd
Filter Set 1 Comments : 1 2 3 4	Defaul Call Filter Active (2)	Comments	Filter Set I Rule 1 Check to enable the Filter Ru Commonts: Index(1-15) in <u>Schedule</u> Setup: Clear sessons when schedule OR: Direction:	le Black NatBins Prable LANRTWPN -> WAN	Edit
Filter Set 1 Comments : Inter Kom 1 2 3 4 5	Defaul Call Filter Active U	Comments	Filter Sei 1 Rule 1 P Check to enable the Filter Ru Commonits: Index(1-15) in <u>Schedule</u> Setup: Clear sessens when schedule ON: Direction: Source IP: Destination IP: Service Type:	le Black NetBins Deck NetBins D	
Filter Set 1 Comments : Ther roun 2 3 4 5 5	Oetsut vali Filter Active I I I I I I I I I I I I	Comments	Filter Set 1 Rule 1 Comments: Index(1-15) in Schedule Setup: Clear seisons when schedule ON: Direction: Source IP: Direction IP:	le Black MatBlans , , , , , , , , , , , , , , , , , , ,	Edit
Filter Set 1 Comments : Ther rous 2 3 4 5 5	Defaul Call Filter Active U	Comments	Files Sei 1 Rule 1 Check to enable the Filter Ru Camments: Index(1-15) in Schedule Setup: Cher sessons when schedule OR: Direction: Source IP: Destanation IP: Fragminet: Fragminet: Application	le Binck NotBins Binck NotBins Enable LANRTUNPL + WAR Any Any Any Any Any Any Action Profile	Edit
Filter Set 1 Comments : Ther roun 2 3 4 5 5	Defaul Call Filter Active U	Comments	Filter Set 1 Rule 1 Comments: Index(1-15) in Schedule Setup: Chair seisions: when schedule OK: Direction: Source IP: Dustriation IP: Survio: Typu: Fragmonic: Application Fiber:	le Btock NetBins Deck Intelline Enable LevelTVPN-> VVAN Any Any Any CCPAUDP, Part from 137-138 to any Don't Gare Action Profile Biock Immediately	Edit
Filter Set 1 Comments : Ther rous 2 3 4 5 5	Defaul Call Filter Active U	Comments Block NetDios	Filter Set 1 Rule 1 P Check to enable the Filter Pu Communits: Index(1-15) in <u>Schedule</u> Setup: Clear dessens when schedule ON: Direction: Source IP: Dostination IP: Service Type: Fragilization Filter Branch to Other Filter Set:	le Black NutBins D-Read Read Read Read Read Read Read Read	Edit
Filter Set 1 Comments : Ther rous 2 3 4 5 5	Defaul Call Filter Active U	Comments Block NetDios	Filter Set 1 Rule 1 Comments: Index(1-15) in Schedule Setup: Chair seisions: when schedule OK: Direction: Source IP: Dustriation IP: Survio: Typu: Fragmonic: Application Fiber:	le Btock NetBins Deck Intelline Enable LevelTVPN-> VVAN Any Any Any CCPAUDP, Part from 137-138 to any Don't Gare Action Profile Biock Immediately	Edit Edit Syslog
Filter Set 1 Comments : Ther rear 2 3 4 5 5 5	Defaul Call Filter Active U	Comments Block NetDios	Files Sei 1 Rule 1 Check to enable the Filter Ru Camments: Index(1-15) in Schedule Setup: Cher sessons when schedule OR: Direction: Source IP: Destination IP: Fragminet: Fragminet: Application Filter: Branch to Other Filter Set: Session Scontrol	le Binck NotBins Binck NotBins Enable LANRTKVPN + WAN Any Any Any Any Any Any Action Profile Biock kimmediately California	Edit Edit Syslog
Filter Set 1 Comments : Ther rear 2 3 4 5 5 5	Defaul Call Filter Active U	Comments Block NetDios	Filter Set 1 Rule 1 Place Set 1 Rule 1 Place Set 1 Schedule Setup: Chair sessions when schedule OK: Direction: Source IP: Destination IP: Styrical Type: Progenities: Progenities: Progenities: Branch to Other Filter Set: Sessions Control MAC Bind IP	le Black NetBlans File Black NetBlans File Enable LevelTVDN-> VVAN Any Any Any Any CCPAUDP, Port from 137-138 to any Don't Gare Action Profile Block immediately File File File File File File File File	Edit Edit Syslog
Filter Set 1 Comments : Ther road	Defaul Call Filter Active U	Comments Block NetDios	Filter Set 1 Rule 1 Commonts: Index(1-15) in Schedule Setup: Char sessions when schedule OR: Direction: Source IP: Destination IP: Service Type: Progenitisk: Application Filter: Branch to Other Filter Set: Sessions Control MAC Bind IP Cuality of Service APP Enforcement: UBL Content Filter:	le Block NetBins Field NetBins	Systeg
Filter Set 1 Comments : Ther road	Defaul Call Filter Active U	Comments Block NetDios	Files Sei 1 Rule 1 Check to enable the Filter Ru Cammonits: Index(1-15) in Schedule Setup: Cherr sessions when schedule Oh: Direction: Source IP: Destination IP: Braydination Fragilization Fragilization Filter Branch to Other Filter Set: Sessions Control MaC Bind IP Gually of Service APP Enforcements:	le Bicki NotBins	Edit Edit Syslog

Dray Tek

3.5.4 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			
🗌 Enable SYN flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
Enable UDP flood defense	Threshold	2000	packets / sec
	Timeout	10	sec
Enable ICMP flood defense	Threshold	250	packets / sec
	Timeout	10	sec
Enable Port Scan detection	Threshold	2000	packets / sec
🔲 Block IP options	📃 Block TCP flag	scan	
Block Land	📃 Block Tear Dro	р	
Block Smurf	📃 Block Ping of D	eath	
📃 Block trace route 📃 Block ICMP fragment			
📃 Block SYN fragment 📃 Block Unassigned Numbers			
Block Fraggle Attack			
Enable DoS defense function to preven crackers.	nt the attacks fro	om hacker	or //
OK Clea	r All Cancel		

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 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.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout.
	The default setting for threshold and timeout are 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.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 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.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning.
	By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.
	Activating the DoS/DDoS defense functionality might



	the fraggle attack defense, a	e blocked. Therefore, the RIP	
Block TCP flag scan	Check the box to activate the Block TCP flag scan function Any TCP packet with anomaly flag setting is dropped. Thos scanning activities include <i>no flag scan</i> , <i>FIN without ACK</i> <i>scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .		
Block Tear Drop	(packets) that exceed the ma	when receiving ICMP datagrams aximum length. To avoid this ter is designed to be capable of	
Block Ping of Death	This attack involves the perp packets to the target hosts so	that those target hosts will the packets. The Vigor routers	
Block ICMP Fragment	Check the box to activate the function. Any ICMP packets dropped.	e Block ICMP fragment s with more fragment bit set are	
Block Unassigned Numbers	the upper layer. However, th are reserved and undefined a		
Warning Messages	We provide Syslog function from Vigor router. The user, the report sending from Vigo Client.	as a Syslog Server, shall receive	
		lated to DoS Defense will be	
		iew it through Syslog daemon. n the message, followed by a	
	name to indicate what kind of attacks is detected.		
	System Maintenance >> SysLog / Mail Alert Setup		
	SysLog / Mail Alert Setup SysLog Access Setup ♥ Enable Syslog Save to: ♥ USB Disk Router Name Server IP Address Destination Port 514 Mail Syslog Enable Enable syslog message: ♥ VPN Log ♥ User Access Log ♥ WAN Log ♥ Acuter/DSL information Note: 1. Mail Syslog cannot be activated unless 2. Mail Syslog feature sends a Syslog file when 3. We only support secured SMTP connection o	its size reaches 1M Bytes.	

Visit State Visit State Reported Repor	Image: State State State Internation Image: State State State State Internation Image: State	Dray Te	Dra	Tek			Swa	log Utility
O Show Syday Lat O Show Syday Lat P Refer log CSMLug: Defense Log System time Router Time System time Router Time System System time System Router Ti	Others Start Correction Others Let P Filter Log CSHLug) Defense Log System Time Floar Time Floar Time System Time Floar Time Floar Time Time Time Time Time Time Time Time	al 📰 👘 🔛 😡	Log Piker Keyword:		×	LAN Information	WWW Information	TX Rate RX Rate
IP Filter log CSMLog Defense Log System time Rotzer Time Host Message 2013-04/20 11/573/4 Aug 2017/5720 Spectram time Rotzer Time 2013-04/20 11/573/4 Aug 2017/5720 Spectram time Inter-Srid 2013-04/20 11/573/4 Aug 2017/5720 Spectram time Docs Tools Tifnogh extra01 10:0.0.0.069-5255, 525.255 / 256 / 710/01 Titesmen20, Titem-Srid 2013-04/20 11/573/4 Aug 2017/520 Vigori rotzer Docs Tools Tifnogh extra01 10:0.0.0.069-5255, 525.255 / 576 / 710/01 Titesmen20, Titem-Srid 2013-04/20 11/573/4 Aug 2017/520 Vigori rotzer Docs Tools Tifnogh extra01 10:0.0.0.069-5255, 525.255 / 576 / 710/01 Titesmen20, Titem-Srid 2013-04/20 11/573/4 Aug 2017/520 Vigori rotzer Docs Tools Tifnogh extra01 10:0.0.0.069-5255, 525.255 / 576 / 710/01 Titesmen20, Titem-Srid 2013-04/20 11/573/4 Aug 2017/520 Vigori rotzer Docs Tools Tifnogh extra01 10:0.0.0.0.069 / 5755, 575 / 255 / 575 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 / 255 / 775 /	P Filter Tog CSMLog Defense Log System Time Rouzer Time Host Message 2013-08-2011/57.07 Mag 2010/57.05 Moor-ouzer [Oor-Outer] 2013-08-2011/57.04 Mag 2010/57.05 Moor-ouzer [Oor-Outer] 2013-08-2011/57.04 Mag 2010/57.05 Moor-ouzer [Oor-Outer]		and a second	Access Connection				
System time Rodar Time Host Message 2010-04/2011/57/47 Aug 2010/57/05 Woorrouter [D00[Inio][Fragde attack[0.00.0469-52/5.255.255.255.07[OutP][Lem=20], Item-570] 2010-04/2011/57/47 Aug 2010/57/05 Woorrouter [D00[Inio][Fragde attack[0.00.0469-52/5.255.255.255.07[OutP][Lem=20], Item-570] 2010-04/2011/57/47 Aug 2010/57/05 Woorrouter [D00[Inio][Fragde attack[0.00.0469-52/5.255.255.255.07[OutP][Lem=20], Item-570] 2010-04/2011/57/47 Aug 2010/57/00 Woorrouter [D00[Inio][Fragde attack[0.00.0469-52/5.355.255.255.0597[OutP][Lem=20], Item-570] 2010-04/2011/57/47 Mog 2010/57/00 Woorrouter [D00[Inio][Fragde attack[0.00.0469-52/5.355.255.255.0597[OutP][Lem=20], Item-570]	Control Trans. Control				O Show Defen	os Alect TOP10		
System Time Router Time Host Message 2019-04/20 11:57:47 Aug 20 00:57:05 Money-code [Doc0]Diolog/Traggle_attask [0:0:0:0:04-52:55:25:55:25:56/TUCP]1tem=20; Item=576] 2019-04/20 11:57:47 Aug 20 00:55:00 Money-code [Doc0]Diolog/Traggle_attask [0:0:0:0:04-52:55:25:55:25:55:07/TUCP]1tem=20; Item=576] 2019-04/20 11:57:46 Aug 20 00:55:00 Money-code [Doc0]Diolog/Traggle_attask [0:0:0:0:04-52:55:25:25:55:25:59/TUCP]1tem=20; Item=576] 2013-04/20 11:57:46 Aug 20 00:55:00 Money-code [Doc0]Diolog/Traggle_attask [0:0:0:0:0:45:25:25:25:25:55:25:59/TUCP]1tem=20; Item=576]	System Time Router Time Host Message 2019-04/20 11:57:47 Aug 20 07:57:05 Bioencoder [D00]Illiod[Tragde_stab][10:0.0.044-925:525:525:525:57]U0*][Len=z0, ILlin=57e] 2019-04/20 11:57:47 Aug 20 07:57:05 Bioencoder [D00]Illiod[Tragde_stab][10:0.0.044-925:525:525:525:57]U0*][Len=z0, ILlin=57e] 2019-04/20 11:57:46 Aug 20 05:55:05 Bioencoder [D00]Illiod[Tragde_stab][10:0.044-925:525:525:525:57]U0*][Len=z0, ILlin=57e] 2013-04/20 11:57:46 Aug 20 05:55:05 Bioencoder [D00]Illiod[Tragde_stab][10:0.064-925:525:525:525:57]U0*][Len=79][Len=79] 2013-04/20 11:57:46 Aug 20 05:55:05 Bioencoder [D00]Illiod[Tragde_stab][10:0.064-925:57] Stab][10:0.064-925:55:57] 2013-04/20 11:57:46 Aug 20 05:55:00 Bioencoder [D00]Illiod[Tragde_stab][10:0.064-925:57] Stab][10:0.064-925:57] 2013-04/20 11:57:46 Aug 20 05:55:00 Bioencoder [D00]Illind[Tragde_stab][10:0.064-925:57] Stab][10:0.064-925:57]	IP Filter Log CSMLog D	IP Filter Log	Jog Defense Log				TParent .
2013-04/30 (1.57):47 Aug 2010;5705 - Speercoze [Doc3[Biod]fragde atta6 [0.0.004-552, 55, 55, 25):67 DeP[Len-20, 1.6m-570] 2013-04/50 (1.57):47 Aug 2010;5305 - Speercoze [Doc3[Biod]fragde atta6 [0.0.004-552, 55, 55, 25):67 DeP[Len-20, 1 2013-04/50 (1.57):48 Aug 2010;5303 - Speercoze [Doc3[Biod]fragde atta6 [0.0.064-552, 55, 55, 25):57 SPT[DeP[Len-20, 1.105]] 2013-04/50 (1.57):48 Aug 2010;5303 - Speercoze [Doc3[Biod]fragde atta6 [0.0.064-552, 55, 55, 55):57 SPT[DeP[Len-20, 1.105]]	2013-04/31 (1-5747) App 2010/5205 (Separate DOS)(Dirio) (Fragde ettas) (20.0.0.048-525,525,525,5267) (UPF) tee-20, 11ee-276] 2013-04/51 (1-5747) App 2010/5305 (Separate DOS)(Dirio) (Fragde ettas) (20.0.048-525,525,525,5267) (UPF) tee-20, 11ee-276] 2013-04/51 (1-574) App 2010/5305 (Separate DOS)(Dirio) (Fragde ettas) (1-2, 104, 1, 0, 447-525,525,525,5267) (UPF) tee-20, 11ee-276] 2013-04/51 (1-574) App 2010/5305 (Separate DOS)(Dirio) (Fragde ettas) (1-2, 104, 1, 0, 447-525,525,525,5267) (UPF) tee-20, 11ee-276]	Sustem Time	Suctany Time	Router Time	HIND	Messane	L	Trees
		2013-08-2011:53:47 2013-08-2011:53:46 2013-08-2811:53:44	2013-08-291 2013-08-281 2013-08-281	3:47 Aug 28 03:53:0 3:46 Aug 28 03:53:0 3:44 Aug 28 03:53:0	25 Vigor-router 23 Vigor-router 22 Vigor-router	[DC5][Block][fraggle_attack][0.0.0.066- [DC5][Block][fraggle_attack][192.166.1. [DD5][Block][fraggle_attack][0.0.0.068-	->255.255.255.255.255.67TUOPT 10:4744->255.255.255.255.255:9 >255.255.255.255.255.255.255.9	Hen=20, ILen=576] 997[UDP][Hen=20, T Hen=20, TLen=576]

DrayTek

3.6 Objects Settings

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

Objects Setting
IP Object
IP Group
IPv6 Object
IP∨6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
SMS/Mail Service Object
Notification Object

3.6.1 IP Object

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

Ob	iects	Setting	>>	IP Ob	iect
~~~	0000	ooung			1000

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

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

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

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

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



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

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

Objects Setting >> IP Object

IP Object Profiles:

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

### 3.6.2 IP Group

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

Objects Setting >> IP Group

P 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 >> IP Group

Profile Index : 1	
Name:	Administration
Interface:	Any 🗸
Available IP Objects	Selected IP Objects
1-RD Department 2-Financial Dept 3-HR Department	>> <<
	OK Clear Cancel

Available settings are explained as follows:

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

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

### 3.6.3 IPv6 Object

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

Objects Setting >> IPv6 Object

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

Available settings are explained as follows:

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

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

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

Objects Setting >> IPv6 Object

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

Vigor2760 Series User's Guide

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

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

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

### 3.6.4 IPv6 Group

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

Objects Setting >	>> IPv6	Group
-------------------	---------	-------

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

Available settings are explained as follows:

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

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

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

Objects Setting >> IPv6 Group

ofile Index : 1	
Name:	
Available IPv6 Objects	Selected IPv6 Objects
	>>
	<u> </u>
	OK Clear Cancel



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

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

# 3.6.5 Service Type Object

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

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

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

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

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

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

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

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

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         IGMP       7         UDP       TCP/UDP         Other       6
Source/Destination Port	<ul> <li>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</li> <li>(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.</li> <li>(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.</li> <li>(&gt;) – the port number greater than this value is available.</li> <li>(&lt;) – the port number less than this value is available for this profile.</li> </ul>

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

Objects Setting >> Service Type Object

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

### 3.6.6 Service Type Group

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

Objects Setting >> Service Type Group

Service Type	e 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>		28.	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

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

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

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

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

Objects Setting >> Service Type Group Setup

Available settings are explained as follows:

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

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

### 3.6.7 Keyword Object

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

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

Objects Setting >> Keyword Object

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

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

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

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

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

### 3.6.8 Keyword Group

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

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

Objects Setting >> Keyword Group

Available settings are explained as follows:

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

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

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

Objects Setting >> Keyword Group Setup

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

**Dray** Tek

Available settings are explained as follows:

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

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

### 3.6.9 File Extension Object

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

Objects Setting >> File Extension Object

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

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

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

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

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

Objects Setting >> File Extension Object Setup

Available settings are explained as follows:

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

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

### 3.6.10 SMS/Mail Service Object

#### **SMS Service Object**

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

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

Object Settings >> SMS / Mail Service Object

Each item is explained as follows:

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

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

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

Object Settings >> SMS / Mail Service Object

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

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

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

Available settings are explained as follows:

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

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

Object Settings >> SMS / Mail Service Object

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

#### **Customized SMS Service**

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

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

Object Settings >> SMS / Mail Service Object

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

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

Profile Name	Custom 1	
Service Provider		
		<u>_</u>
	MS provide to get the exact URL String 7/eapi/submission/send_sms/2/2.0?userna	
eg:bulksms.vsms.net:5567		
eg:bulksms.vsms.net:5567 &password=###txtPwd#	7/eapi/submission/send_sms/2/2.0?userna	
eg:bulksms.vsms.net:5567 &password=###txtPwd# Username	7/eapi/submission/send_sms/2/2.0?userna	

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



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

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

### **Mail Service Object**

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

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

Object Settings >> SMS / Mail Service Object

Each item is explained as follows:

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

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

Object Settings >> SMS / Mail Service Object

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

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:

Profile Index: 1		
Profile Name	Mail_Notify	
SMTP Server	192.168.1.98	
SMTP Port	25	
Sender Address	carrie_ni@draytek.com	
Use SSL		
Authentication		
Username	John	
Password	••••	
Sending Interval	0 (seconds)	
	OK Clear Cancel	

Object Settings >> SMS / Mail Service Object

Item	Description
Profile Name	Type a name for such mail service profile. The maximum length of the name you can set is 31 characters.
SMTP Server	Type the IP address of the mail server. The maximum length of the name you can set is 63 characters.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function.
	<b>Username</b> – Type a name for authentication. The maximum length of the name you can set is 31 characters.
	<b>Password</b> – Type a password for authentication. The maximum length of the password you can set is 31



	characters.
Sending Interval	Define the interval for the system to send the SMS out.

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

Object Settings >> SMS / Mail Service Object

SMS Pro	vider	Mail Server		Set to Factory Default
Index			Profile Name	
<u>1.</u>			Mail_Notify	
<u>2.</u>				
3.				

### 3.6.11 Notification Object

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

You can set an object with different monitoring situation.

Object Settings >> Notification Object

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

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

Object Settings >> Notification Object

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

**Dray** Tek

2. The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Name	Notify_attack		
Category		Status	
WAN	Disconnected Reconnected		
VPN Tunnel	Disconnected	Reconnected	

Available settings are explained as follows:

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

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

Object Settings >> Notification Object

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

# 3.7 CSM Profile

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

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

### **APP Enforcement Filter**

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

### **URL Content Filter**

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

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

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

#### Web Content Filter

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

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

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



Objects Setting
CSM
APP Enforcement Profile
URL Content Filter Profile
Web Content Filter Profile
DNS Filter
APPE Support List

### 3.7.1 APP Enforcement Profile

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

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

CSM >> APP Enforcement Profile

Available settings are explained as follows:

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

Click the number under Index column for settings in detail.

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



Below shows the items which are categorized under Protocol.

CSM >> APP Enfo	rcement Profile					
Profile Index : 1	Profile Name:					
IM	P2P	Protocol	OTHERS			
Select All	Clear All		Support List		Action : Bl	ock 💌
			Protocol			
DNS	FTP		HTTP	IMAP	IRC IRC	
<b>NNTP</b>	РОРЗ		SMB	SMTP	SNMP	
SSH .	SSL/TLS		TELNET	MSSQL	MySQL	
Oracle	PostgreSQL		Sybase	DB2	🗌 Informix	
			OK Cancel			

Available settings are explained as follows:

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

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

Below shows the items which are categorized under IM.

CSM >> APP Enforcement Profile

Profile Index : 1 F	Profile Name:					
IM	P2P	Protocol	OTHERS			
Select All C	lear All			Support L	<u>.ist</u>	
		Advanc	ed Management			
Activity /	Application	MSN	YahooIM	DIM AIM(<= v5.9) I		
L L	ogin					
Me	ssage					
File 1	Fransfer					
G	iame					
Conference	e(Video/Voice)					
Other	Activities					
		IM Application			VoIP	
AIM6/7	QQ/TM	iChat		ober/GoogleTalk	Skype Kubao	
GoogleChat	XFire	GaduGad	du 🗌 Pa	Italk	Gizmo SIP/RTP	
Qnext	ПРОСО/РРЗ6	5 🗌 AresCha	t 🗌 Ali	WW	TelTel TeamSpeak	k
Lava-Lava	LCU2	🗌 iSpQ				~
MobileMSN	BaiduHi	Fetion		NE	RaidCall	
		Web IM ( * =	more than one ad	dress)		
				<u>Buddy ILove</u> Nhaha* getN	<u>elM*</u> 1essenger	
WebIM URLs				SN2GO* Kool		
	·	MessengerAdictos				
-	-					
		[ OI	< Cancel			

**Dray** Tek

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

#### CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:				
IM P2P	Protocol	OTHERS		
Select All Clear All			Support	List
Protocol			Applications	
SoulSeek	SoulSeek			
eDonkey	eDonkey, eM	ule, Shareaza		
■ FastTrack	KazaA, BearS	ihare, iMesh		
OpenFT	KCeasy, FileP	'ipe		
Gnutella	BearShare, Li	imewire, Shareaza	a, Foxy, KCeasy	
OpenNap	Lopster, XNa	p, WinLop		
BitTorrent	BitTorrent, Bi	tSpirit, BitComet		
	Othe	er P2P Applications		
Xunlei Vag	а [	PP365	<b>П</b> РОСО	Clubbox
Ares ezPe	er 🛛	Pando	Huntmine	Kuwo

OK Cancel

# The items categorized under OTHERS-----

#### CSM >> APP Enforcement Profile

Profile Index : 1	Profile Name:				
IM	P2P	Protocol	OTHERS		
Select All C	Clear All			Support	List
			Tunneling		
Socks4/5	PGPNet	Пн	TTP Proxy	Tor	
SoftEther	MS TEREDO		/ujie/UltraSurf	Hamachi	HTTP Tunnel
Ping Tunnel	TinyVPN	□R	ealTunnel	DynaPass	UltraVPN
FreeU	Skyfire	Пн	otspot Shield		
			Streaming		
MMS	RTSP	Пт	/Ants	PPStream	
🗌 FeiDian	UUSee	🗆 N	SPlayer	PCAST	Τνκοο
SopCast	UDLiveX	Пт	/UPlayer	MySee	Joost
FlashVideo	SilverLight	s	ingbox	QVOD	
L		F	Remote Control		
	Radmin	S	pyAnywhere	ShowMyPC	LogMeIn
TeamViewer	Gogrok	R	emoteControlPro	CrossLoop	WindowsRDP
pcAnywhere	🗌 Timbuktu	v	/indowsLiveSync	SharedView	
			Weh HD		
HTTP Upload			S SkyDrive	GDoc Uploader	ADrive
MyOtherDrive	_ ′	Шв	oxNet	OfficeLive	DropBox
Google Servi	ce liCloud				
			OK Cancel		

## 3.7.2 URL Content Filter Profile

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

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

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

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

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

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

L Content Filter F			Set to Factory Det	
Profile	Name	Profile	Name	
<u>1.</u>		<u>5.</u>		
<u>2.</u>		<u>6.</u>		
<u>3.</u>		<u>7.</u>		
4.		8.		

CSM >> URL Content Filter Profile

Administration Message (Max 255 characters)	Default Message	
<pre><body><center> The requested Web page has been blocked by URL Filter.Please contact your system administrator for further information.</center></body></pre>	Content	~
		~

0K

Each item is explained as follows:

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

**Dray** Tek

0

Administration Message	You can type the message manually for your necessity.	
	<b>Default Message</b> - You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of <b>Administration</b> <b>Message</b> .	

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

Profile Name:			
Priority:	Both : Pass	V Log:	None 💌
1.URL Access	Control		
🗆 Enab	le URL Access Control	Prevent w	veb access from IP address
Actio	n:	Group/Obje	ct Selections
Pass	*		Edit
2.Web Feature			
🗌 Enab	le Restrict Web Feature		
Actio	n:		
Pass	🗹 🗌 Cookie 🔲 Proxy	Upload File E	xtension Profile: None 💌
1			

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



	Either: Web Feature 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 web feature first, then URL second.
	Either : Web Feature First
Log	None – There is no log file will be recorded for this profile. Pass – Only the log about Pass will be recorded in Syslog. Block – Only the log about Block will be recorded in Syslog. All – All the actions (Pass and Block) will be recorded in Syslog. None Pass Block
URL Access Control	All         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. <b>Prevent web access from IP address</b> - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.
	Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. <i>Pass</i> - Allow accessing into the corresponding webpage with the keywords listed on the box below.
	<b>Block</b> - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. Action:
	Block         Pass         Block         Group/Object Selections – The Vigor router provides         several frames for users to define keywords and each frame

supports multiple keywords. The keyword could be a noun,
a partial noun, or a complete URL string. Multiple
keywords within a frame are separated by space, comma, or
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

bjec	t/Group Edit	
	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 Keyword Object	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 💌

Web Feature	<b>Enable Restrict Web Feature -</b> 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.
	<ul><li><i>Block</i> - Restrict accessing into the corresponding webpage with the keywords listed on the box below.</li><li>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</li></ul>
	<b>Cookie</b> - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
	<b>Proxy</b> - 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.
	<b>Upload</b> – Check the box to block the file upload by way of web page.
	<b>File Extension Profile</b> – Choose one of the profiles that you configured in <b>Object Setting&gt;&gt; File Extension</b>



<b>Objects</b> previously for passing or blocking the file downloading.		
d File Extension Profile:	None None 1-image	

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

### 3.7.3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (*MyVigor*) located on <u>http://myvigor.draytek.com</u>.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (*MyVigor*) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

**Note:** If you have used **Service Activation Wizard** to activate WCF service, you can skip this section.

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

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

**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.

#### CSM >> Web Content Filter Profile

Web-Filter L [Status:No	.icense ot Activated]					<u>Activate</u>
Setup Quer	ry Server	auto-selected			Find more	
Setup Test	Server	auto-selected			Find more	
Web Conten	nt Filter Profile Table:				Set	to Factory Default
Profile	Na	me	Profile		Name	
<u>1.</u>	Def	ault	<u>5.</u>			
<u>2.</u>			<u>6.</u>			
<u>3.</u>			<u>7.</u>			
<u>4.</u>			<u>8.</u>			
Administration Message (Max 255 characters) Default Message Cache : L1 + L2 Cache <body><center> &gt;body&gt;<center> &gt;br&gt; &gt;categorized with %CL% has been blocked by %RNAME% Web Content Filter.Please contact your system administrator for further information.</center></center></body>						
	Source IP,%DIP% Category , %RNAME	,	%URL% -	URL		

0K

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 <b>Administration Message</b> .



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

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.

Profile Index: 1			
Profile Name: Default			Log: Block
Black/White List			
Enable			
Action:	G	roup/Object Selections	
Block 🛩			Edit
Action: Block 💌			
Groups	Categories		
Child Protection	Alcohol & Tobacco	Criminal Activity	🗹 Gambling
Select All	Hate & Intolerance	🗹 Illegal Drug	✓ Nudity
Clear All	Porn & Sexually	✓ Violence	✓ Weapons
	School Cheating	Sex Education	✓ Tasteless
	émilia.	ward and a second second	and the state of the solution."
	News	Non-profits & NGOs	Personal Sites
	Politics	Real Estate	Religion
	Restaurants & Dining	Shopping	Translators
	General	Cults	Greeting cards
	Image Sharing	Network Errors	Parked Domains
	Private IP Addresses	Uncategorised Sites	

**Dray** Tek

Item	Description
Profile Name	Type a name for the CSM profile. The maximum length of the name you can set is 15 characters.
Black/White List	<b>Enable</b> – Activate white/black list function for such profile. <b>Group/Object Selections</b> – Click <b>Edit</b> to choose the group or object profile as the content of white/black list.
	<b>Pass</b> - <b>allow</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
	<ul><li>Block - restrict accessing into the corresponding webpage with the characters listed on Group/Object Selections.</li><li>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.</li></ul>
Action	<b>Pass</b> - allow accessing into the corresponding webpage with the categories listed on the box below.
	<b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.
	If the web pages do not match with the specified feature set here, it will be processed with reverse action.
Log	<ul> <li>None – There is no log file will be recorded for this profile.</li> <li>Pass – Only the log about Pass will be recorded in Syslog.</li> <li>Block – Only the log about Block will be recorded in Syslog.</li> <li>All – All the actions (Pass and Block) will be recorded in Syslog.</li> <li>Block Mone</li> <li>Pass</li> <li>Block</li> <li>All</li> </ul>

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

## 3.7.4 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	Enable
Syslog	None 💌
Service	None
Cache Time(hour)	1 💌
Administration Message (Max 255 charact	ers) Default Message
that is categorized with %CL% d	uested Web page from %SIP% to %URL% r>has been blocked by %RNAME% DNS Filter.Please r further information.
Legend: %SIP% - Source IP , %URL% - U %CL% - Category , %RNAME% - R(	RL outer Name OK Cancel

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

Service	Set the filtering conditions. Specify one of the WCF profiles as Service.		
	None None WCF-1 Default		
	Choose the WCF profiles to apply DNS filter.		
Cache Time (hour)	Set the time for DNS query.		
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.

# 3.7.5 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 2013-12-11  $\,$ 

IM	P2P		PROTOCOL	OTHERS	
APP Type	APP Name	Version		Note	
	AIM	5.9			
	AIM	6/7	Only block Logi services can no	n. If users have alre t be blocked.	ady logged in, AIM
	AliWW	2008			
	Ares	2.0.9			
	BaiduHi	37378			
	Fetion	2010			
	GaduGadu Protocol				
	Google Chat				
	ICQ	7	at the same tim	os are blocked, Voic ne. In ICQ5 or forme be blocked separati	r versions, Videos
	ICU2	8.0.6			
	Jabber Protocol/Google Talk				

# 3.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.



Bandwidth Management >> Sessions Limit

### 3.8.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

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

🔘 Enable 💿 Disable			
Default Max Sessions: 1	00		
Limitation List			
Index Start IP	End IP	Max Sessions	
Specific Limitation	End IP:		
Maximum Sessions:			
Maximum Sessions.	Add	Edit Delete	
inistration Message (Max 25)	5 characters)		Default Message
2 .			
			~
e Schedule			
Index(1-15) in Schedule S	etup:  ,	, ,	

To activate the function of limit session, simply click **Enable** and set the default session limit. Available settings are explained as follows:

Item	Description		
Session Limit	<b>Enable -</b> Click this button to activate the function of limit session.		



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

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



## 3.8.2 Bandwidth Limit

Bandwidth Management >> Bandwidth Limit

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

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

🔘 Enable 🗌 IP Ro	uted Subnet 🤇	Disable		
Default TX Limit: 200	0 Kbps 🔽	Default RX Lim	it: 8000	Kbps 🐱
🔲 Allow auto adjus	stment to make	the best utilizatio	on of <u>availat</u>	e bandwidth.
Limitation List				
Index Start IP	End IP	TX limit	RX limit	Shared
Specific Limitation				
Start IP:	En	d IP:		
⊙ Each ○ Shared	TX Limit:	Kbps 💌 RX L	.imit:	Kbps 🐱
	Add	Edit Delete		
Smart Bandwidth L	imit			
For any LAN IP Not	in Limitation Lis	t, when session r	number exc	eeds 1000
TX Limit : 200	Kbps 🔽 RX Li	imit : 800 K	bps 😽	
For TX/RX, a setting of "0				
Schedule				
ndex(1-15) in <u>Schedule</u> Se lote: Action and Idle Timed				
		boloporod		

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

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

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

## 3.8.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.





However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the Bandwidth Management menu, click Quality of Service to open the web page.

ndex Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1 Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN2 Disable 10	0000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3 Disable 10	0000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Class 1							Edit		,,,,
Index Class 1		ame					Rule Edit	Service T	, , ,
	2				Edit Edit				
Class 2							Edit		
Class 2 Class 3							<u></u>		
							Lun		
Class 3	Priority for VoIP SIP/RTP:								

Bandwidth Management >> Quality of Service

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



Item	Description
for VoIP SIP/RTP	be sent with highest priority.
	<b>SIP UDP Port</b> - Set a port number used for SIP.

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

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

### **Online Statistics**

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.

12 Online	Statistics			Refresh Interval: 5 🔽 seconds 🛛 🕴 Refre
Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)
1	OUT	VoIP		0
2	OUT		25%	0
3	OUT		25%	0
4	OUT		25%	0
5	OUT	Others	25%	0
			VoIP Others	

#### **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.

**Dray** Tek

#### Bandwidth Management >> Quality of Service

WAN2 General Setup					
	WAN Inbound Bandwidth	100	Kbps 🖲 Mbps		
	WAN Outbound Bandwidth	100	Kbps 🖲 Mbps		
Index	Class Name		Reserved_bandwidth Ratio		
Class 1			25 %		
Class 2			25 %		
Class 3			25 %		
	Others		25 %		
🗌 Enable UDI	9 Bandwidth Control		Limited_bandwidth Ratio 25 %		
🗆 Outbound	TCP ACK Prioritize				
Note:1.Before a bandwidth is n		eal bandwid	th first. QoS may not work properly if the		

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

ΟK

Clear

Cancel

Item	Description
Enable the QoS Control	The factory default for this setting is checked.
	Please also define which traffic the QoS Control settings will apply to.
	<b>IN-</b> apply to incoming traffic only.
	OUT-apply to outgoing traffic only.
	<b>BOTH-</b> apply to both incoming and outgoing traffic.
	Check this box and click <b>OK</b> , then click <b>Setup</b> link again. You will see the <b>Online Statistics</b> link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN2/WAN3. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN2/WAN3. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of <b>reserved bandwidth to upstream speed</b> and <b>reserved bandwidth to downstream speed</b> .
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.



Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

**Note:** The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

### Edit the Class Rule for QoS

1. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

Bandwidth Management >> Quality of Service

General Setup							Set t	o Factory D	efault
Index Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	;
WAN1 Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2 Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3 Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

#### Class Rule

Class 1     Edit       Class 2     Edit	Index	le Service Type
	Class 1	lit
	Class 2	lit <u>Edit</u>
Class 3 Edit	Class 3	lit

Enable the First Priority for VolP SIP/RTP:     SIP UDP Port: 5060 (Default:5060)	
	OK

2. After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.

Bandwidth Management >> Quality of Service

Class Inc	lex #1					
Name	Test			Tag packets as:	Default	*
NO	Status	Local Address	Remote Address	DiffServ CodeP	oint Servi	ісе Туре
1	Empty	-	-	-		-
		,	Add Edit Delet	e		
			OK Cancel			

**Dray** Tek

3. For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY 🔽	
Service Type	Predefined	*

OK Cancel

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 <b>Edit</b> button to set the local IP address (on LAN) for the rule.
Remote Address	Click the <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.
	Address Type       Subnet Address         Start IP Address       D.0.0         End IP Address       D.0.0         Subnet Mask       D.0.0         OK       Close         Address Type – Determine the address type for the source address.         For Single Address, you have to fill in Start IP address.         For Range Address, you have to fill in Start IP address and End IP address.         For Subnet Address, you have to fill in Start IP address and End IP address.         For Subnet Address, you have to fill in Start IP address and End IP address.
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.

Class Index #1 Name Test 🔲 Tag packets as: Default DiffServ NO Status Local Address Remote Address Service Type CodePoint ANY 1 🔿 Active Any Any ANY Add Edit Delete ΟK Cancel

#### Bandwidth Management >> Quality of Service

#### Edit the Service Type for Class Rule

1. To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

Bandwidth Management >> Quality of Service

General	Setup							<u>Set t</u>	o Factory De	efault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

#### Class Rule

Index	Name	Rule	Service Type
Class 1	Test	Edit	
Class 2		<u>Edit</u>	<u>Edit</u>
Class 3		<u>Edit</u>	

✓ Enable the First Priority for VoIP SIP/RTP:	
SIP UDP Port: 5060 (Default: 5060)	
	OK

2. After you click the **Edit** link, you will see the following page.

Bandwidth Management >> Quality of Service

User Defined Ser	rvice Type		
NO	Name	Protocol	Port
1	Empty	-	-
		Add Edit Delete	
		Cancel	

3. For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Name	
Service Type	TCP 6
Port Configuration	
Туре	💿 Single 🔘 Range
Port Number	0 - 0

Available settings are explained as follows:

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

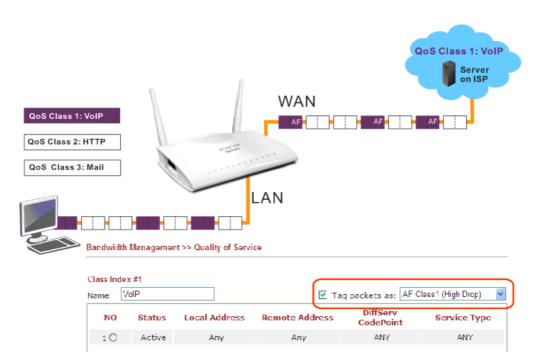
5. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

#### **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.



### 3.8.4 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 VNC or PPTV without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbond bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click **Bandwidth Management>>APP QoS** to open the following page.

Bandwidth Management >> APP QoS

Enable I Traceable	Disable Untraceable				
Select All	Clear All	Apply to all:	QoS Cla	ss 1 (High) 🛛 🔽	Apply
Enable		Protocol		Action	
	DNS			QoS Other (Lowest	) 🔽
	FTP			QoS Other (Lowest	) 🔽
	HTTP			QoS Other (Lowest	) 🗸
	IMAP			QoS Other (Lowest	) 🗸
	IRC			QoS Other (Lowest	) 🗸
	NNTP			QoS Other (Lowest	) 🔽
	POP3			QoS Other (Lowest	) 🔽
	SMB			QoS Other (Lowest	) 🔽
	SMTP		Ī	QoS Other (Lowest	) 🔽
	SNMP			QoS Other (Lowest	) 🔽
	SSH			QoS Other (Lowest	) 🔽
	SSL/TLS			QoS Other (Lowest	
	TELNET			QoS Other (Lowest	) 🗸

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

ΟK

Item	Description	
Enable/Disable	Click <b>Enable</b> to activate APP QoS function. Click <b>Disable</b> to deactivate APP QoS function.	
Traceable	The protocol listed below is traceable by Vigor router. Each tab offers different types of protocols to fit your request.	
Untraceable	The protocol listed below is not easy to trace by Vigor router. Each tab offers different types of protocols to fit your request.	
Select All	Click it to select all of the protocols.	



Clear All	Click it to de-select all of the protocols.		
Apply to all	Choose one of the actions from the drop down list. It is prepared for applying to all protocols.           Apply to all:         QoS Class 1 (High)         Apply		
	ol QoS Class 1 (High) QoS Class 2 (Medium) QoS Class 3 (Low) DefaultClass (Lowest) ↓ ↓		
	<b>Apply</b> – Click it to make the selected action be applied all of the selected protocols immediately.		
Action	There are many protocols which can be specified with different QoS Class.		
	Action QoS Class 1 (High) QoS Class 1 (High) QoS Class 2 (Medium) QoS Class 3 (Low) DefaultClass (Lowest) QoS Class 1 (High)		

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

# 3.9 Applications

Below shows the menu items for Applications.

banuwiuth management
Applications
Dynamic DNS
LAN DNS
Schedule
RADIUS
UPnP
IGMP
Wake on LAN
SMS/Mail Alert Service
Bonjour

### 3.9.1 Dynamic DNS

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

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

#### Enable the Function and Add a Dynamic DNS Account

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

)ynamic DNS Setup		Set to Factory Default
📃 Enable Dynamic DN	IS Setup	View Log Force Update
Auto-Update interval	14400 Min(s) (1~14400)	
Accounts:		
Index	Domain Name	Active
<u>1.</u>		×
<u>2.</u>		×
<u>3.</u>		X
	OK Clear All	

#### Applications >> Dynamic DNS Setup

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.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.

```
Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup
```

ndex : 1 Enable Dynamic DNS	Account	
Service Provider	dyndns.org (www.dyndns.org)	¥
Service Type	Dynamic 😽	
Domain Name	chronic6653 dyndns.org	dyndns.org 🖌
Login Name	chronic6653	(max. 64 characters)
Password	•••••	(max. 23 characters)
Wildcards		
Backup MX		
Mail Extender		
Determine Real WAN IP	Internet IP 💙	

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.

Item	Description
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	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. 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. There are two methods offered for you to choose: Internet IP WAN IP Internet IP II is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. Internet IP – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.

4. Click **OK** button to activate the settings. You will see your setting has been saved.

#### Disable the Function and Clear all Dynamic DNS Accounts

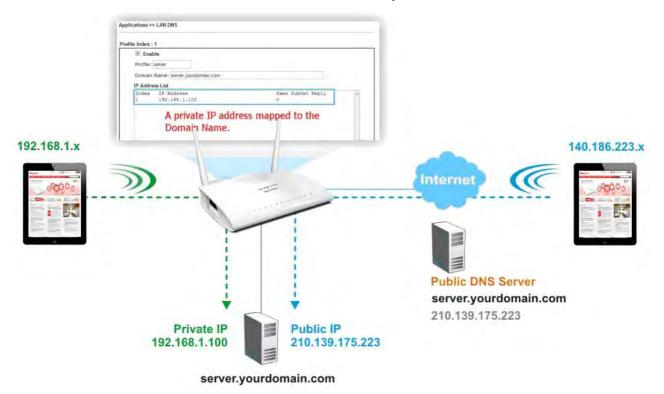
In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

#### **Delete a Dynamic DNS Account**

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

### 3.9.2 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.



Simply click **Application>>LAN DNS** to open the following page.

					<b>D</b> 110
Ap	plica	tions	>>	LAN	DNS

LAN DNS Re	solution		Set to Factory Default
Enable	Index	Profile	Domain 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>		
<< <u>1-10   1</u>	1- <u>20</u> >>		

OK

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:

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

#### Applications >> LAN DNS

🗹 Enat	ble		
Profile:	MAIL		
Domain	Name: ms.draytek.com		
IP Addre	ss List		
Index	IP Address	Same Subnet Reply	~
1	172.16.3.8		
			~
Add	Delete		

OK Clear

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	The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name. Add – Click it to open a dialog to type the host's IP address.

o Host's IP Address - 楓樹湖覽器	X 0 -
172.16.3.133:2860/doc/landnshost.htm	Q 🕑 🕴
Host's IP Address 172.16.3.8 Only responds to the DNS request when the sender is in t subnet. OK Close	the same
• Only responds to the DNS – Difference can share the same domain name. Howe to check this box to make the router ider respond the IP address for the DNS quer from different LAN PC.	ver, you have ntify &
Delete – Click it to remove an existed IP addr	ress on the list.

- 3. Click **OK** button to save the settings.
- 4. A new LAN DNS profile has been created.

#### Applications >> LAN DNS

LAN DNS Re	solution		Set to Factory Default
Enable	Index	Profile	Domain Name
	<u>1.</u>	MAIL	ms.draytek.com
	<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>		
<< <u>1-10   1</u>	<u>1-20</u> >>		

OK )

**Dray** Tek

## 3.9.3 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.

ule:			Set to Factory Def
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	х
<u>2.</u>	x	<u>10.</u>	х
<u>3.</u>	х	<u>11.</u>	х
<u>4.</u>	x	<u>12.</u>	х
<u>5.</u>	х	<u>13.</u>	х
<u>6.</u>	х	<u>14.</u>	х
<u>7.</u>	х	<u>15.</u>	х
8.	×		

Applications >> Schedule

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

Available settings are 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
ОК	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.	
	<b>Enable Dial-On-Demand -</b> Specify the connection to be dial-on-demand and the value of idle timeout should be specified in <b>Idle Timeout</b> field.	
	<b>Disable Dial-On-Demand -</b> Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.	
Idle Timeout	Specify the duration (or period) for the schedule.	
	How often -Specify how often the schedule will be applied Once -The schedule will be applied just once	
	<b>Weekdays</b> -Specify which days in one week should perform the schedule.	

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



#### Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).



- 1. Make sure the PPPoE connection and **Time Setup** is working properly.
- 2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- 3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

# **3.9.4 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	1812
Shared Secret	
Confirm Shared Secret	
ОК	Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature.
Server IP Address	Enter the IP address of RADIUS server
<b>Destination Port</b>	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

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

# 3.9.5 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
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 <b>Connection Control</b> <b>Service</b> or <b>Connection Status Service</b> .

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

	Broadband	😨 IP Broadband Connection (	
Network Tasks         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create new connection	hinet Disconnected WAN Miniport (PPPOE) Dial-up	General Internet Gateway Status:	Connected
ee Also	test Disconnected DrayTek ISDN PPP	Duration: Speed: Activity	00:19:06 100.0 Mbps
Ither Places     Image: Control Panel       My Network Places       My Documents       My Computer	Internet Gateway IP Broadband Connection on Router Enabled LAN or High-Speed Internet	Packets: Sent: 404 Received: 1.115	734
Vetails (*) Network Connections	Local Area Connection Enabled Realter RTL8139/810x Family	Properties Disable	Close

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.



ieneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
Section on Router	(Services
This connection allows you to connect to the Internet through a shared connection on another computer.	<ul> <li>Ftp Example</li> <li>msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>msnmsgr (192.168.29.11:8789) 63231 TDP</li> </ul>
Settings	

The reminder as regards concern about Firewall and UPnP

#### Can't work with Firewall Software

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

#### **Security Considerations**

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

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

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

# 3.9.6 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications >> IGMP					
IGMP					
Enable IGMP	Proxy WAN1 🔽				
	is to act as a multicast proxy any multicast group. But this f				
Enable IGMP	Snooping				
	Snooping, multicast traffic is				
Disable IGMP	snooping, multicast traffic is	treated in the	same manner a	is broadcast tra	affic.
		OK Can	cel		
					<u>Refresh</u>
Working Multic	ast 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.
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.



# 3.9.7 Wake on LAN

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

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

Application >> Wake on LAN

wake up through	AN integrates with <u>Bind IP to MAC</u> function, only binded PCs can h IP.
Wake by:	MAC Address 🗸
IP Address:	🗸
MAC Address:	: : : : : Wake Up!
Result	

Available settings are explained as follows:

Item	Description	
Wake by	Two types provide for you to wake up the bound IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.         Wake by:       MAC Address v         MAC Address       IP Address         IP Address       IP Address	
IP Address	The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.	
MAC Address	Type any one of the MAC address of the bound PCs.	
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.	

**Dray** Tek

Wal	ke	on	Т	A	V .

Wake by:	MAC Address 🗸
IP Address:	*
MAC Address:	: : : : Wake Up!
Result	

## 3.9.8 SMS / Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

#### **SMS Provider**

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

SMS Provider	Mail Server		<u></u>	Set to Factory Default
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 🔽	1 - Line_down 💌		1 - Notify_attack 💌	
2 🔲	1 - Line_down 🗸		1 - Notify_attack 🗸	
3 🗌	1 - Line_down 👻		1 - Notify_attack 💌	
4	1 - Line_down 💉		1 - Notify_attack 💙	
5 🗌	1 - Line_down 😽		1 - Notify_attack 💌	
6	1 - Line_down 💉		1 - Notify_attack 💙	
7 🗌	1 - Line_down 😽		1 - Notify_attack 🗸	
8	1 - Line_down 😽		1 - Notify_attack 💙	
9 🗌	1 - Line_down 👻		1 - Notify_attack 💌	
10 🔲	1 - Line_down 😽		1 - Notify_attack 💙	

Application >> SMS / Mail Alert Service

Available settings are explained as follows:

Item	Description
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click <b>SMS Provider</b> link to define the SMS server.

Cancel

OK

Recipient	Type the name of the one who will receive the SMS.	
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the SMS.	
Schedule	Type the schedule number that the SMS will be sent out. You can click the <b>Schedule(1-15)</b> link to define the schedule.	

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

### **Mail Server**

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

SMS Provider	Mail Server	<u> </u>	<u> </u>	Set to Factory Defa
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)
1 🔽	1 - Mail_Notify 💙		1 - Notify_attack 💌	
2	1 - Mail_Notify 🗸		1 - Notify_attack 🗸	
3 🗌	1 - Mail_Notify 🗸		1 - Notify_attack 👻	
4	1 - Mail_Notify 🗸		1 - Notify_attack 💙	
5 🗌	1 - Mail_Notify 💙		1 - Notify_attack 👻	
6	1 - Mail_Notify 💙		1 - Notify_attack 💙	
7 🗆	1 - Mail_Notify 🗸		1 - Notify_attack 👻	
8	1 - Mail_Notify 💙		1 - Notify_attack 👻	
9 🔲	1 - Mail_Notify 💙		1 - Notify_attack 👻	
10 🗌	1 - Mail_Notify 🗸		1 - Notify_attack 🗸	

Cancel

OK

Application >> SMS / Mail Alert Service

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 <b>Mail Service</b> link to define the mail server.
Recipient	Type the e-mail address of the one who will receive the notification message.
Notify	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the mail message.

Schedule	Type the schedule number that the notification will be sent out.
	You can click the <b>Schedule</b> ( <b>1-15</b> ) link to define the schedule.

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

### 3.9.9 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 software 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				
Bonjour Setup				
Enable Bonjour Service				
HTTP Server				
Telnet Server				
FTP Server				
SSH Server				
LPR Printer Server				
	OK Cancel			

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.

Browser - Mozilla Firefox				
<u>File Edit V</u> iew Hi <u>s</u> tory <u>B</u> o	okmarks <u>T</u> ools <u>H</u> elp			
🥹 Mozilla Firefox Start Page 🛛 🛛	Browser	× 🖂 Browser	× 🖾 Browser	
🔶 🔶 🛃 🕝 chrome://dnssd/	content/browser.html		☆ ▼	



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.

rome://dnssd/cor	ne://dnssd/content/browser.html		☆ ▼ C Google		
DNSSD	for Firefox				
Browser Co	nfiguration Options Diagnostic Information				
Interface	Name	Туре	Domain	Service Info	
2	DS1010Plus	_httptcp.	local.	Select a service on the left to view further details.	
2	DS1010Plus(WebDAV)	_httptcp.	local.	further details.	
2	HP LaserJet 1300	_ipptcp.	local.		
2	tctseng-virtual-machine	udisks-sshtcp.	local.		
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstationtcp.	local.		
2	tomkao-desktop (00:0c:29:26:09:5d)	_workstationtcp.	local.		

3. Open **System Maintenance>>Management**. Type a name (e.g., Dray_2925) as the Router Name and click **OK**.

IPv4 Manageme	ent Setup	IPv6 Management Setup	
Router Name	Vigor Router	Management Port Setu	p
		💿 User Define Ports	O Default Ports
Management Access Co	ntrol	Telnet Port	23 (Default: 23)
Allow management	from the Internet	HTTP Port	80 (Default: 80)
FTP Server		HTTPS Port	443 (Default: 443)
HTTP Server		FTP Port	21 (Default: 21)
HTTPS Server		SSH Port	22 (Default: 22)
✓ Telnet Server			(Default: 22)
SSH Server			
Disable PING from t	ne Internet	_	
Access List			
List IP	Subnet Mask		
1	*		
2	~		
3	×		
1		·	
		ОК	

System Maintenance >> Management

4. Next, open Applications>>Bonjour. Check the service that you want to use via Bonjour.

Bonjour Setup	
Enable Bonjour Service	
HTTP Server	
Telnet Server	
FTP Server	
SSH Server	
LPR Printer Server	



5. 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.

☆ マ C 🛛 - Google

wser Co	nfiguration Options Diagnostic Information			
Interface	Name	Туре	Domain	Service Info
2	DS1010Plus	_httptcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_httptcp.	local.	
2	HP LaserJet 1300	_ipptcp.	local.	_
2	Vigor Router	_ftptcp.	local.	
2	Vigor Router	_httptcp.	local.	
2	Vigor Router	_printertcp.	local.	
2	Vigor Router	_sshtcp.	local.	
2	Vigor Router	_telnettcp.	local.	
2	tctseng-virtual-machine	_udisks-sshtcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstationtcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstationtcp.	local.	

#### **DNSSD** for Firefox

◎ chrome://dnssd/content/browser.html

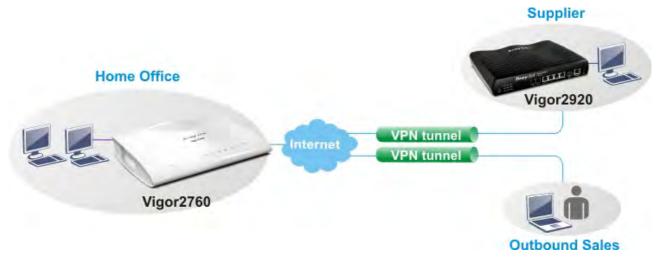
6. Now, any page or document can be printed out through Vigor router (installed with a printer).

Print		
Printer <u>N</u> ame Status Type Location Comment	Microsoft XPS Document Writer Auto HP LaserJet 1200 Series PCL on RD-KC Auto Microsoft XPS Document Writer on RD-KC Auto Microsoft XPS Document Writer on TIM-PC Vigor Router	Properties
Print to file Print range O All pages Pages Selection	Copies Number of copies	1 🗢
Options	OK Cancel	

# **Dray** Tek

# 3.10 VPN and Remote Access

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



Below shows the menu items for VPN and Remote Access.

VPN and Remote Access Remote Access Control PPP General Setup IPsec General Setup IPsec Peer Identity Remote Dial-in User LAN to LAN Connection Management

### 3.10.1 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.

Remote Access Control Setur	
	Enable PPTP VPN Service
	Enable IPSec VPN Service
	Enable L2TP 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 <u>Open Ports</u> or <u>Port Redirection</u> is also configured.

OK Clear Cancel
-----------------

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



# 3.10.2 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
	Dial-In PPP Encryption(MPPE) Optional MPPE 💙
	Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No
	Username
	Password
	IP Address Assignment for Dial-In Users (When DHCP Disable set)
	Assigned IP start LAN 1 192.168.1.200
	LAN 2 10.39.0.200

OK

Available settings are explained as follows:

Item	Description	
Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.	
	<b>PAP/CHAP/MS-CHAP/MS-CHAPv2</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.	
<b>Dial-In PPP Encryption</b> (MPPE)	<b>Optional MPPE</b> - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.	
	Optional MPPE	
	Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit)	
	<b>Require MPPE (40/128bits) -</b> Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.	
	Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.	



Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer. The length of the name/password is limited to 23/19 characters.
Assigned IP Start	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. You can configure up to four start IP addresses for LAN1 ~ LAN6.

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

### 3.10.3 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	
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.	

OK Cancel

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 c			
	There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote dial-in user, <b>Certificate (X.509)</b> and <b>Pre-Shared Key</b> .			
	Pre-Shared Key- Specify a key for IKE authentication.			
	<b>Confirm Pre-Shared Key-</b> Retype the characters to confirm the pre-shared key.			
	Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.			
IPsec Security Method	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.			
	<b>High (ESP)</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.			

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

# 3.10.4 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.

(509 Peer ID A	Accounts:			Set to Facto	ry Default
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	Х	<u>17.</u>	???	Х
<u>2.</u>	???	Х	<u>18.</u>	???	х
<u>3.</u>	???	Х	<u>19.</u>	???	Х
<u>4.</u>	???	Х	<u>20.</u>	???	х
<u>5.</u>	???	Х	<u>21.</u>	???	Х
<u>6.</u>	???	Х	<u>22.</u>	???	х
<u>7.</u>	???	Х	<u>23.</u>	???	Х
<u>8.</u>	???	Х	<u>24.</u>	???	х
<u>9.</u>	???	Х	<u>25.</u>	???	Х
<u>10.</u>	???	Х	26.	???	х
<u>11.</u>	???	Х	<u>27.</u>	???	Х
<u>12.</u>	???	х	<u>28.</u>	???	х
<u>13.</u>	???	Х	<u>29.</u>	???	Х
<u>14.</u>	???	х	<u>30.</u>	???	х
<u>15.</u>	???	Х	<u>31.</u>	???	Х
<u>16.</u>	???	х	<u>32.</u>	???	х

VPN and Remote Access >> IPsec Peer Identity

Available settings are explained as follows:

Item Description	
Set to Factory Default Click it to clear all indexes.	
Index	Click the number below Index to access into the setting page of IPsec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

#### VPN and Remote Access >> IPsec Peer Identity

Profile Index : 1					
rofile Name ???					
Enable this account					
O Accept Any Peer ID					
○ Accept Subject Alternative Name					
Туре	IP Address				
IP					
Domain Name					
E-Mail					
O Accept Subject Name					
Country (C)					
State (ST)					
Location (L)					
Orginization (O)					
Orginization Unit (OU)					
Common Name (CN)					
Email (E)					
	OK Clear Cancel				

Available settings are explained as follows:

Item	Description		
Profile Name	Type the name of the profile. The maximum length of the name you can set is 32 characters.		
Enable this account	Check it to enable such account profile.		
Accept Any Peer ID	Click to accept any peer regardless of its identity.		
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be <b>IP</b> <b>Address, Domain,</b> or <b>E-mail Address</b> . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.		
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes <b>Country (C), State (ST), Location (L), Organization (O),</b> <b>Organization Unit (OU), Common Name (CN),</b> and <b>Email (E)</b> .		

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



# 3.10.5 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.

ndex	User	Active	Status	Index	User	Active	Status
<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>	???		
16.	???			<u>32.</u>	???		

VPN and Remote Access >> Remote Dial-in User



Available settings are explained as follows:

Item	Description	
Set to Factory Default	Click to clear all indexes.	
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 <b>???</b> represents that the profile is empty.	
Active	Check the box to activate such 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.



0

VPN and Remote Access >> Remote Dial-in User

Index No. 1	
User account and Authentication  Enable this account Idle Timeout  Allowed Dial-In Type  PPTP  IPsec Tunnel	Username ??? Password(Max 19 char) Enable Mobile One-Time Passwords(mOTP) PIN Code Secret KE Authentication Method
L2TP with IPsec Policy None     Specify Remote Node Remote Client IP     or Peer ID     Netbios Naming Packet      Pass      Block Multicast via VPN     Pass      Block (for some IGMP,IP-Camera,DHCP Relayetc.)	Pre-Shared Key          IKE Pre-Shared Key         Digital Signature(X.509)         None         IPsec Security Method         Medium(AH)         High(ESP)         DES         JDES         Local ID (optional)
Subnet LAN 1  Assign Static IP Address 0.0.0.0 OK CI	ear Cancel

Available settings are explained as follows:

Item	Description		
User account and Authentication	<b>Enable this account</b> - Check the box to enable this function.		
	<b>Idle Timeout-</b> If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.		
Allowed Dial-In Type	<b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.		
	<b>IPsec Tunnel</b> - Allow the remote dial-in user to make an IPsec VPN connection through Internet.		
	<b>L2TP with IPsec Policy</b> - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:		
	• None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.		
	• Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.		
	• <b>Must</b> -Specify the IPsec policy to be definitely		



	applied on the L2TP connection.	
	Specify Remote Node -You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).	
	Uncheck the checkbox means the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .	
	Netbios Naming Packet -	
	• <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.	
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.	
	<b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.	
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.	
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.	
	<b>User Name</b> - This field is applicable when you select PPTF or L2TP with or without IPsec policy above. The length of the name is limited to 23 characters.	
	<b>Password</b> - This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 19 characters.	
	<b>Enable Mobile One-Time Passwords (mOTP) -</b> Check this box to make the authentication with mOTP function.	
	<b>PIN Code</b> – Type the code for authentication (e.g, 1234). <b>Secret</b> – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).	
Subnet	Chose one of the subnet selections for such VPN profile.	
	<b>Assign Static IP Address</b> – Please type a static IP address for the subnet you specified.	
IKE Authentication Method	This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.	
	of without specify the fir address of the remote houe.	
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.	
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters	

<ul> <li>with IPsec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.</li> <li>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.</li> </ul>
<b>High-Encapsulating Security Payload (ESP)</b> means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
<b>Local ID (Optional)-</b> Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

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

## 3.10.6 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.

VPN and Remote Access >> LAN to LAN

ndex	Name	Active	Status	Index	Name	Active	Status
<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>	???		
16.	???			<u>32.</u>	???		

Available settings are explained as follows:

Item	Description	
Set to Factory Default	Click to clear all indexes.	

0

Name	Indicate the name of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.
Active	<ul><li>V – means the profile has been enabled.</li><li>X – mans the profile has not been enabled.</li></ul>
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

To edit each profile:

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name ??? Enable this profile Netbios Naming Packet  Pass OBlock	Call Direction   Both Dial-Out Dial-in  Always on  Idle Timeout  300 second(s)
Multicast via VPN OPass OBlock (for some IGMP,IP-Camera,DHCP Relayetc.)	Enable PING to keep alive PING to the IP
2. Dial-Out Settings	
Type of Server I am calling          PPTP         IPsec Tunnel         L2TP with IPsec Policy None         Server IP/Host Name for VPN.         (such as draytek.com or 123.45.67.89)	Username ??? Password(Max 15 char) PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 V VJ Compression O Off IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) Peer ID None V Local ID O Alternative Subject Name First Subject Name First
	IPsec Security Method ● Medium(AH) ● High(ESP) DES without Authentication Advanced Index(1-15) in <u>Schedule</u> Setup: ,,,,

**Dray** Tek

Available settings are explained as follows:

Item	Description			
Common Settings	<b>Profile Name</b> – Specify a name for the profile of the LAN-to-LAN connection.			
	Enable this profile - Check here to activate this profile.			
	Netbios Naming Packet			
	<ul> <li>Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</li> </ul>			
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.			
	<b>Multicast via VPN -</b> Some programs might send multicast packets via VPN connection.			
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.			
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.			
	<b>Call Direction -</b> Specify the allowed call direction of this LAN-to-LAN profile.			
	• <b>Both</b> :-initiator/responder			
	• <b>Dial-Out</b> - initiator only			
	• <b>Dial-In-</b> responder only.			
	<b>Always On-</b> Check to enable router always keep VPN connection.			
	<b>Idle Timeout:</b> The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.			
	<ul> <li>Enable PING to keep alive - This function is to help the router to determine the status of IPsec VPN connection, especially useful in the case of abnormal VPN IPsec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.</li> </ul>			
	<b>Enable PING to keep alive</b> is used to handle abnormal IPsec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).			
	<b>PING to the IP -</b> Enter the IP address of the remote host that located at the other-end of the VPN tunnel.			



Dial-Out Settings	<b>Type of Server I am calling - PPTP</b> - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
	<b>IPsec Tunnel</b> - Build an IPsec VPN connection to the server through Internet.
	<b>L2TP with IPsec Policy -</b> Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:
	• None: Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.
	• Nice to Have: Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.
	<b>Must:</b> Specify the IPsec policy to be definitely applied on the L2TP connection.
	<b>User Name -</b> This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 49 characters.
	<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 15 characters.
	<b>PPP Authentication -</b> This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. PAP/CHAP is the most common selection due to wild compatibility.
	<b>VJ compression -</b> This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to <b>Yes</b> to improve bandwidth utilization.
	<b>IKE Authentication Method -</b> This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy.
	• <b>Pre-Shared Key</b> - Input 1-63 characters as pre-shared key.
	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPsec Peer Identity.</li> </ul>
	<b>Peer ID</b> - Select one of the predefined Profiles set in <b>VPN and Remote Access</b> >> <b>IPsec Peer Identity.</b>
	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.
	<ul> <li>Local Certificate – Select one of the profiles set in Certificate Management&gt;&gt;Local Certificate.</li> </ul>
	<b>IPsec Security Method -</b> This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy.

• Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.
• High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:
• <b>DES without Authentication</b> -Use DES encryption algorithm and not apply any authentication scheme.
• <b>DES with Authentication-</b> Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
• <b>3DES without Authentication</b> -Use triple DES encryption algorithm and not apply any authentication scheme.
• <b>3DES with Authentication-</b> Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
• <b>AES without Authentication</b> -Use AES encryption algorithm and not apply any authentication scheme.
• <b>AES with Authentication-</b> Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
<b>Advanced -</b> Specify mode, proposal and key life of each IKE phase, Gateway, etc.
The window of advance setup is shown as below:
IKE advanced settings
IKE phase 1 mode          O Man mode         O Aggressive mode            IKE phase 1 proposal          Asco         O         MAAC_SNATINIAC_MOS         O         (s000 - \$6400)         IKE phase 1 key lifetime         28000         (s000 - \$6400)         IKE phase 2 key lifetime         38600         (6600 - \$6400)         Particel Ferward Secret         O Disable         O Disable         O Disable         O         Enable
Note If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negratiste with the remote vie. The proposals include DES_(MD5 SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_MD5_SHA]_G5, AES125_MD5_G2, G5), AES256_SHA_G2, G5), AES256_SHA_G14 [OK] [Otem]
<b>IKE phase 1 mode -</b> Select from <b>Main</b> mode and <b>Aggressive</b> mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPsec session. However, the <b>Aggressive</b> mode is faster. The default value in Vigor router is Main mode.
• <b>IKE phase 1 proposal-</b> 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 <b>Main</b> mode. We suggest you select the combination that covers the most schemes.
• <b>IKE phase 2 proposal-</b> 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

Allowed Dial-In Type		Username	???		
PPTP			r r r		
		Password(Max 11 char)			
IPsec Tunnel		VJ Compression	💿 On 🔘 Off		
L2TP with IPsec Pol	licy None 🔽	IKE Authentication Method			
🔲 Specify Remote VPN	Gateway	Pre-Shared Key			
Peer VPN Server IP		[IKE Pre-Shared Key]			
		Digital Signature(X.5	09)		
or Peer ID		None 🗸			
		Local ID			
		<ul> <li>Alternative Subje</li> </ul>	ect Name First		
		🔾 Subject Name First			
			IPsec Security Method		
		✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES			
		High(ESP) 🗹 DES 🗹	3DES 🗹 AES		
4. TCP/IP Network Settings					
My WAN IP	0.0.0	RIP Direction	Disable 🔽		
Remote Gateway IP	0.0.0	From first subnet to rem	ote network, you have		
Remote Network IP	0.0.0.0	to do	Deute III		
Remote Network Mask	255.255.255.0		Route 💌		
Local Network IP	192.168.1.1	Change default rout	e to this VPN tunnel (		
Local Network Mask	255.255.255.0	Only single WAN suppor	ts this )		
	More				
		Clear			

Available settings are explained as follows:

Item	Description
Dial-In Settings	<b>Allowed Dial-In Type -</b> Determine the dial-in connection with different types.
	• <b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set

the User Name and Password of remote dial-in user below.
• <b>IPsec Tunnel-</b> Allow the remote dial-in user to trigger an IPsec VPN connection through Internet.
• L2TP with IPsec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:
None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.
Nice to Have - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.
Must - Specify the IPsec policy to be definitely applied on the L2TP connection.
<b>Specify Remote VPN Gateway -</b> 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.
<b>User Name -</b> This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the name is limited to 11 characters.
<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPsec policy above. The length of the password is limited to 11 characters.
<b>VJ Compression -</b> 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.
<b>IKE Authentication Method -</b> 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.
• <b>Pre-Shared Key</b> - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
<ul> <li>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 &gt;&gt;IPsec Peer Identity.</li> </ul>
<ul> <li>Local ID – Specify which one will be inspected first.</li> </ul>



	<ul> <li>Alternative Subject Name First – The alternative subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> <li>Subject Name First – The subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
	<b>IPsec Security Method -</b> This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.
	• <b>Medium-</b> Authentication Header (AH) means data will be authenticated, but not be encrypted. By default this option is active.
	• <b>High-</b> Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
TCP/IP Network Settings	<ul> <li>My WAN IP –This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP</li> <li>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, 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 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 is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the 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.</li> </ul>
	<b>Remote Network IP/ Remote Network Mask -</b> Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.
	<b>Local Network IP / Local Network Mask -</b> Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required.
	<b>More -</b> Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

🧭 LAN-to-LAN Profile - Windows Internet Explorer
http://192.168.1.1/doc/l2IMRt.htm
Profile Index :1
Remote Network
Network IP Netmask 255.255.255.255/32
Add Delete Edit
OK Close
and the second
<b>RIP Direction -</b> 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
<b>do</b> - If the remote network only allows you to dial in with single IP, please choose <b>NAT</b> , otherwise choose <b>Route</b> .
<b>Change default route to this VPN tunnel -</b> 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.

# 3.10.7 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.

			Dial-out Tool Refresh Seconds : 10 💌 Refres						
			Dial						
<b>VPN Conne</b> Current P	ection Status lage: 1					Pag	e No.	Go >>	
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	

Available settings are explained as follows:

VPN and Remote Access >> Connection Management

Item	Description			
Dial-out Tool	<b>Dial -</b> Click this button to execute dial out function.			
	<b>Refresh Seconds -</b> Choose the time for refresh the dial information among 5, 10, and 30.			
	<b>Refresh -</b> Click this button to refresh the whole connection status.			



# 3.11 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.



## 3.11.1 Local Certificate

Certificate Management >> Local Certificate

(509 Local Certific	cate Configuration		
Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		
X509 Loca	al Certificate		

Available settings are explained as follows:

Item	Description
Generate	Click this button to open Generate Certificate Request window.



	Certificate Management >> Local Certificate			
	Generate Certificate Signing Request			
	Subject Alternative Name			
	Туре	IP Address		
	IP			
	Subject Name			
	Country (C)			
	State (ST)			
	Location (L)			
	Organization (O)			
	Organization Unit (OU)			
	Common Name (CN)			
	Email (E)			
	Кеу Туре	RSA 💙		
	Key Size	1024 Bit 💌		
	Generate Note: Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.			
	Type in all the informa click <b>Generate</b> again.	ation that the window requests. Then		
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 vie request.	ew the detailed settings for certificate		
Delete	Click this button to delete selected name with certification information.			

After clicking **GENERATE**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/ST=HC/L=HC/O=Draytek/0	Requesting	View Delete
GENERATE X509 Lo	IMPORT REFRESH		
MIIBq EwJIQ CQEWE AoGBA a1X// m6+Of hkiG9 9yojH eorpD	BEGIN CERTIFICATE REQUEST jCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAd zEQMA4GA1UEChMHRHJheXR1azELMAkGA1UU 3N1cHBvcnRAZHJheXR1ay5jb2Owg28wDQVd LMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw6 fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wH 4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkq w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJs pstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMo a1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vU END CERTIFICATE REQUEST	SCXMCURQXIjAg JKoZIhvcNAQEB ByTU5HQvXpAzc HwCalAZQoGvIi gnQ1QNSuFAgMB sVzu7JHafSSeU FoQFx/LWdaEPU	BgkqhkiG9w0B BQADgY0AMIGJ rgJBGrikTUBX ODMC7f5w9xA8 AAGgADANBgkq naYDZefCmGfX 5LqryBKKgC9t

# 3.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate	Management	>>	Trusted	CA	Certificate
-------------	------------	----	---------	----	-------------

#### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete
1		REFRESH	

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

Impo	ort X509	Trusted	CA	Certificate
in the second se		1100000	00	Continuouto

Select a trusted CA certificate file.	
Browse.	
Click Import to upload the certification.	
Import Cancel	

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

Cer	tificate Information - Windows Interne	t Explorer 📃	
🦲 http	:// <b>192.168.1.1</b> /doc/XCaCfVi1.htm		
			^
	Certi	ficate Detail Information	
	Certificate Name:	Trusted CA-1	
	Issuer:		
	Subject:		
	Subject Alternative Name:		
	Valid From:		
	Valid To:		
	•	Close	~
<			

**Dray** Tek

# 3.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Backup	
	Encrypt password:
	Confirm password:
	Click Backup to download certificates to your local PC as a file.
Restoration	
	Select a backup file to restore.
	Browse.
	Decrypt password:
	Click Restore to upload the file.

# **Dray** Tek

# 3.12 VoIP

Note: This function is used for "V" models.

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

#### sip: user:password @ host: port

Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ $\mu$ -law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

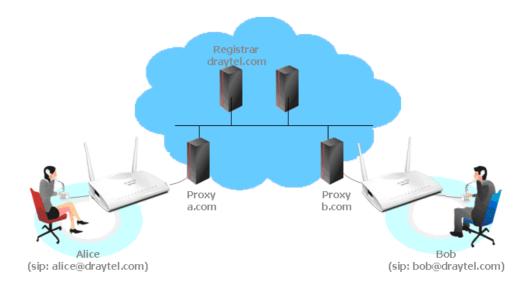
Usually there will be two types of calling scenario, as illustrated below:

#### • Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

If you both register to the same SIP Registrar, then it will be illustrated as below:

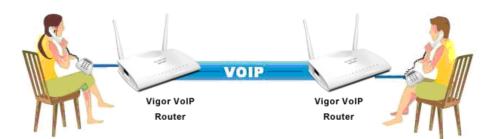
**Dray** Tek



The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



• Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



## 3.12.1 DialPlan

This page allows you to set phone book, digit map, call barring, regional settings and PSTN setup for the VoIP function. Click the links on this page to access into next pages for detailed settings.

VoIP >> DialPlan Setup		
DialPlan Configuration		
	<u>Phone Book</u>	
	<u>Digit Map</u>	
	Call Barring	
	<u>Regional</u>	
	<u>PSTN Setup</u>	

#### Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor2830Vn for setting the phone book.

VoIP >> DialPlan Setup

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
<u>1.</u>				Default	None		х
<u>2.</u>				Default	None		х
<u>3.</u>				Default	None		х
<u>4.</u>				Default	None		х
<u>5.</u>				Default	None		х
<u>6.</u>				Default	None		х
7.				Default	None		×
10.				Detault	None		
<u>16.</u>				Default	None		х
<u>17.</u>				Default	None		х
<u>18.</u>				Default	None		х
<u>19.</u>				Default	None		х
20.				Default	None		×

<< <u>1-20</u> | <u>21-40</u> | <u>41-60</u> >>
Status: v --- Active, x --- Inactive

Click any index number to display the dial plan setup page.

#### VoIP >> DialPlan Setup

Phone Book Inc	lex No. 1	
🗹 Enable		
	Phone Number	1
	Display Name	Polly
	SIP URL	1112 @ fwd.pulver.com
	Dial Out Account	Default 💌
	Loop through	PSTN V
	Backup Phone Number	PSTN
	ОК	Clear Cancel

Available settings are explained as follows:

Item	Description	
Enable	Click this to enable this entry.	
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits <b>0-9</b> and *.	
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.	
SIP URL	Enter your friend's SIP Address.	
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.	
Loop through	Choose PSTN to enable loop through function.	
Backup Phone Number	When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number for this VoIP phone setting.	

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



**Note:** If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

## Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

#	Enable	Match Prefix	Mod	le	OP Number	Min Len	Max Len	Route	Move Up	Mov Dow
1		03	Replac	e 💌	8863	7	8	PSTN 🔽		Dow
2	✓	886	Strip	۷	886	9	10	PSTN 🔽	UP	Dow
3			None	~		0	0	PSTN 🔽	UP	Dow
4			None	~		0	0	PSTN 🔽	UP	Dow
5			None	~		0	0	PSTN 🔽	UP	Dow
6			None	~		0	0	PSTN 🔽	UP	Dow
7			None	~		0	0	PSTN 🔽	UP	Dow
			Mono			O.	0	DOTN 5		
			None			U	U	POIN E	<u>UP</u>	Dow
17			None	$\sim$		0	0	PSTN 🔽	<u>UP</u>	Dow
8			None	×		0	0	PSTN 🔽	<u>UP</u>	Dow
.9			None	v		0	0	PSTN 🔽	<u>UP</u>	Dow
20			None	$\sim$		0	0	PSTN 🗸	<u>UP</u>	

Item	Description
Enable	Check this box to invoke this setting.
Match Prefix	It is used to match with the number you dialed and can be modified with the <b>OP Number</b> by the mode (add, strip or replace).
Mode	None - No action. Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
	<b>Strip</b> - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set

	with 886.	
	Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to SIP server. Mode Replace None Add Strip Replace	
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.	
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.	
Max Len	Set the maximum length of the dial number for applying the prefix number settings.	
Route	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in <b>VoIP&gt;&gt; Phone Settings</b> .	
Move UP /Move Down	Click the link to move the selected entry up or down.	

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

# **Call Barring**

Call barring is used to block phone calls coming from the one that is not welcomed.

VoIP >> DialPlan Setup

0

Call Barr	ing Setup			5	Set to Factory	<u>Default</u>
Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Schedule	Status
1.						х
<u>2.</u>						×
<u>3.</u>						х
<u>4.</u>						×
<u>5.</u>						×
<u>6.</u>						×
<u>7.</u>						×
<u>8.</u>						×
<u>9.</u>						×
<u>10.</u>						×
<< <u>1-10</u>	<u>11-20</u> >>					<u>Next</u> >>

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u>

Click any index number to display the dial plan setup page.

```
VoIP >> DialPlan Setup
```

Call Barring Index No. 1	
🗹 Enable	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Route	All 💌
Index(1-15) in <u>Schedule</u> Setup	,,,
Note: Wildcard '?' is supported.	
OK	Cancel

Item	Description		
Enable	Check it to enable this entry.		
Call Direction	Check it to enable this entry. Determine the direction for the phone call, IN – income call, OUT-outgoing call, IN & OUT – both incoming a outgoing calls. IN OUT IN & OUT		

Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number	
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.	
Route	All means all the phone calls will be blocked with such mechanism.	
Index (1-15) in Schedule	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section <b>Applications&gt;&gt;Schedule</b> for detailed configuration.	

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup					
Call Barring Block Anonymous					
Route	Phone1 Phone2				
Index(1-15) in <u>Schedule</u> Setup					
Note:Block the incoming calls which do not have the caller ID.					
OK	Cancel				

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup

Call Barring Block Unknown Domain		
Route	Phone1 Phone2	
Index(1-15) in <u>Schedule</u> Setup	, , , , , , , , , , , , , , , , , , , ,	
Newsylf also also also also in a subject to a set the difference	A frame the demote formed in CTR and such that will also de-	

Note: If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked.



For **Block IP Address** – this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup

Call Barring Block IP Address	
Route	Phone1 Phone2
Index(1-15) in <u>Schedule</u> Setup	
Note: The incoming calls by means of IP dialing (e	g.#192*168*1*1#) should be blocked.
OK	Cancel

## Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

#### VoIP >> DialPlan Setup

🗹 Enable Regional		Ι.	Set to Factory Default
Last Call Return [Miss]:	*69		
Last Call Return [In]:	*12	Last Call Return [Out]:	*14
Call Forward [All] [Act]:	*72 +number+#	Call Forward [Deact]:	*73 +#
Call Forward [Busy] [Act]:	*90 +number+#	Call Forward [No Ans] [Act]:	*92 +number+#
Do Not Disturb [Act]:	*78 +#	Do Not Disturb [Deact]:	*79 +#
Hide caller ID [Act]:	*67 +#	Hide caller ID [Deact]:	*68 +#
Call Waiting [Act]:	*56 +#	Call Waiting [Deact]:	*57 +#
Block Anonymous [Act]:	*77 +#	Block Anonymous [Deact]:	*87 +#
Block Unknow Domain [Act]:	*40 +#	Block Unknow Domain [Deact]:	*04 +#
Block IP Calls [Act]:	*50 +#	Block IP Calls [Deact]:	*05 +#
Block Last Calls [Act]:	*60 +#		

Available settings are explained as follows:

Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number

Cancel



ΟK

	typed in this field to call back to that one.
Last Call Pature [Out]	
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

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



## **PSTN Setup**

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Check the **Enable** box to make the PSTN number available for dial whenever you need and type the number in the field of **phone number for PSTN relay**.

VoIP >> PSTN Setup	
--------------------	--

Enable	phone number for PSTN relay	

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

# 3.12.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an Account Name or user name, SIP Registrar, Proxy, and Domain name. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in Account Name@ Domain name

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Note: Selection items for Ring Port will differ according to the router you have.

VoIP >>	SIP Acco	unts					Contraction
SIP Acc	ounts Lis	t					Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	e Codec	Ring Port	Status
1					G.729A/B	🗌 Phone1 🗌 Phone2	-
2					G.729A/B	🗌 Phone1 📃 Phone2	-
<u>3</u>					G.729A/B	🗌 Phone1 🗌 Phone2	-
4					G.729A/B	🗌 Phone1 📃 Phone2	-
<u>5</u>					G.729A/B	🗌 Phone1 🗌 Phone2	-
<u>6</u>					G.729A/B	🗌 Phone1 📃 Phone2	-
NAT Tra	versal Se	etting			se	success registered on S rver fail to register on SIP se	
	STUN	l Server:					
	Exte	rnal IP:					
	SIP F	PING Interval:		150 se	с		

Available settings are explained as follows:

Item	Description
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Codec	Display the codec type for the account.
Ring Port	Specify which port will ring when receiving a phone call.
Status	Show the status for the corresponding SIP account. <b>R</b> means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.



A

STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.

Click any index link to access into the following page for configuring SIP account.

#### VoIP >> SIP Accounts

Profile Name	(11 char max.)
Register via	None 💌 🗌 Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
Act as outbound pro	xy
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 🕑 3600 sec
NAT Traversal Support	None 💌
Call Forwarding	Disable 💌
SIP URL	
Time Out	30 sec
Ring Port	Phone1 Phone2
Ring Pattern	1 💌
Prefer Codec	G.729A/B (8Kbps) 💌 🗌 Single Codec
Packet Size	20ms 💌
Voice Active Detector	Off 🖌

Item	Description
Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose <b>None</b> and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of <b>Call without Registration</b> . Choosing <b>Auto</b> is recommended. The system will select a proper way for your VoIP call.

	None None Auto WAN1 WAN2 LAN/VPN PVC				
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is <b>5060.</b> Your peer must set the same value in his/her Registrar.				
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.				
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type <b>:port number</b> after the domain name to specify that port as the destination of data transmission (e.g., <b>nat.draytel.org:5065</b> )				
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.				
Display Name	The caller-ID that you want to be displayed on your friend's screen.				
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.				
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.				
Password	The password provided to you when you registered with a SIP service.				
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.				
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.				
	NAT Traversal Support None  None Stun Manual Nortel				
	<b>None</b> – Disable this function.				
	<b>Stun</b> – Choose this option if there is Stun server provided for your router.				
	Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.				
	<b>Nortel</b> – If the soft-switch that you use supports Nortel solution, you can choose this option.				



Call Forwarding	There are four options for you to choose. <b>Disable</b> is to close call forwarding function. <b>Always</b> means all the incoming calls will be forwarded into SIP URL without any reason. <b>Busy</b> means the incoming calls will be forwarded into SIP URL only when the local system is busy. <b>No Answer</b> means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out. Disable Always Busy No Answer Busy or No Answer SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. <b>Time Out</b> – Set the time out for the call forwarding. The default setting is 30 sec.
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern  1 2 3 4 5 6
Prefer Codec	Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711. G.729A/B (8Kbps) G.711MU (64Kbps) G.723 (6.4kbps) G.723 (6.4kbps) G.726_32 (32kbps) Single Codec – If the box is checked, only the selected Codec will be applied.
Packet Size	The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

**Dray** Tek

	Packet Size	20ms V 10ms 20ms 30ms 40ms 50ms 60ms
Voice Active Detector	or not. If not, the router will	lick On to invoke this function;

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

# 3.12.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

```
VoIP >> Phone Settings
```

Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	User Defined	5/5		OutBand
2	Phone2	CW,CT,	User Defined	5/5		OutBand

RTP

Symmetric RTP	
Dynamic RTP Port Start	10050
Dynamic RTP Port End	15000
RTP TOS	IP precedence 5

Item	Description
Phone List	<b>Port</b> – there are two phone ports provided here for you to configure. <b>Phone1/Phone2</b> allows you to set general settings for PSTN phones.
	<b>Call Feature</b> – A brief description for call feature will be shown in this field for your reference.
	<ul><li>Tone - Display the tone settings that configured in the advanced settings page of Phone Index.</li><li>Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.</li></ul>
	<b>Default SIP Account</b> – "draytel_1" is the default SIP account. You can click the number below the Index field to



	change SIP account for each phone port. <b>DTMF Relay</b> – Display DTMF mode that configured in the advanced settings page of Phone Index.			
RTP	Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remo router to the private IP of local router), you can check this box to solve this problem.			
	<b>Dynamic RTP Port Start</b> - Specifies the start port for RT stream. The default value is 10050.			
	<b>Dynamic RTP Port End</b> - Specifies the end port for RTP stream. The default value is 15000.			
	<b>RTP TOS</b> – It decides the level of VoIP package. Use the drop down list to choose any one of them.			
	ManualIP precedence 1IP precedence 2IP precedence 3IP precedence 4IP precedence 5IP precedence 6IP precedence 7AF Class1 (Low Drop)AF Class1 (Medium Drop)AF Class1 (High Drop)AF Class2 (Low Drop)AF Class2 (Low Drop)AF Class3 (Medium Drop)AF Class3 (Low Drop)AF Class3 (Medium Drop)AF Class3 (Medium Drop)AF Class4 (Low Drop)AF Class4 (Low Drop)AF Class4 (Medium Drop)AF Class4			
	RTP TOS Manual			

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

## **Detailed Settings for Phone Port**

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Phone1							
Call Feature		Defa	IIt SIP Acc	count			~
🔲 Hotline			Dlav dial t		when a	ccount n	eqistered
Session Timer	90 sec		nay ular t	one only	when a	ccount n	systered
🔲 T.38 Fax Function							
Error Correction Mode	REDUNDANCY 🔽						
DND(Do Not Disturb) N Index(1-15) in <u>Sche</u>							
Note: Action and Id be ignored.	le Timeout settings will						
Index(1-60) in <u>Phon</u>	e Book as Exception List:						
	,,,,,						
CLIR (hide caller ID)							
🗹 Call Waiting							
🗹 Call Transfer							
	OK Ca	ncel	Advan	ced			

Item	Description			
Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.			
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.			
T.38 Fax Function	Check the box to enable T.38 fax function. <b>Error Correction Mode</b> – choose a mode for error correction.			
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.			
	<ul> <li>Index (1-15) in Schedule - Enter the index of schedule</li> <li>profiles to control when the phone will ring and when will</li> <li>not according to the preconfigured schedules. Refer to</li> <li>section Application &gt;&gt;Schedule for detailed configuration</li> </ul>			
	<b>Index (1-60) in Phone Book -</b> Enter the index of phone book profiles. Refer to section <b>DialPlan – Phone Book</b> for detailed configuration.			
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.			
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your			



	response. Click hook flash to pick up the waiting phone call.
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.
Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. Play dial tone only when account registered - Check this box to invoke the function.

In addition, you can press the Advanced button to configure tone settings, volume gain, MISC and DTMF mode. Advanced setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

VoIP >> Phone Settings

Advance	Settings >>	Phone 1

Tone Settings							
Region User Defined	*		Call	er ID Type	FSK_ETSI		
	Low Freq(Hz)	High Freq(Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)	
Dial tone	350	440	0	0	0	0	
<b>Ringing tone</b>	400	450	400	200	400	2000	
Busy tone	400	0	375	375	0	0	
Congestion tone	0	0	0	0	0	0	
Volume Gain			DTMF				
Mic Gain(1-10)	5		DTMF Mod	le	OutBand ( R	FC2833) 🛛 🔽	
Speaker Gain(1-10)	5		Payload T (RFC2833)	ype ) (96 - 127)	101		
MISC							
Dial Tone Power Level	(1 - 50) 27	7					
Ring Frequency (10 -	50HZ) 25	ō					
Call Waiting Tone Pow (1 - 30)	ver Level 13	3					
Interdigit Timeout (1	- 10 sec) 4						

Available settings are explained as follows:

Item	Description
Region	Select the proper region which you are located. The common settings of <b>Caller ID Type</b> , <b>Dial tone</b> , <b>Ringing tone</b> , <b>Busy tone</b> and <b>Congestion tone</b> will be shown automatically on the page. If you cannot find out a suitable

Cancel

**Dray** Tek

ΟK

	one, please choose <b>User Defined</b> and fill out the				
	corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.				
	ango				
	User Defined 💌				
	User Defined				
	US				
	^a Denmark				
	li Italy				
	Germany				
	S Netherlands ID Portugal				
	es Sweden				
	Australia				
	G Slovenia				
	Czech				
	Slovakia				
	G Hungary Switzerland				
	France				
	China				
	I Taiwan HZ				
	ting Tope Power Le				
	Also, you can specify each field for your necessity. It is				
	recommended for you to use the default settings for VoIP				
	communication.				
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume				
, on the Guin	of microphone and speaker by entering number from 1-10.				
	The larger of the number, the louder the volume is.				
MISC	<b>Dial Tone Power Level</b> - This setting is used to adjust the				
	loudness of the dial tone. The smaller the number is, the				
	louder the dial tone is. It is recommended for you to use the				
	default setting.				
	<b>Ring Frequency</b> - This setting is used to drive the				
	frequency of the ring tone. It is recommended for you to use				
	the default setting.				
	Call Waiting Tone Power Level - This setting is used to				
	adjust the loudness of the call waiting tone. The smaller the				
	number is, the louder the tone is. It is recommended for you				
	to use the default setting.				
	<b>Interdigit Timeout</b> Type a value in this field to enacity				
	<b>Interdigit Timeout</b> – Type a value in this field to specify time limit for interdicit				
	time limit for interdigit.				
DTMF	time limit for interdigit. DTMF Mode – There are four DTMF modes for you to				
DTMF	time limit for interdigit.				
DTMF	time limit for interdigit. DTMF Mode – There are four DTMF modes for you to				
DTMF	<ul><li>time limit for interdigit.</li><li>DTMF Mode – There are four DTMF modes for you to choose.</li></ul>				
DTMF	time limit for interdigit.          DTMF Mode – There are four DTMF modes for you to choose.         DTMF mode         InBand         OutBand (RFC2833)				
DTMF	time limit for interdigit.       DTMF Mode – There are four DTMF modes for you to choose.      DTMF mode      InBand				



• <i>InBand</i> - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone.
• <b>OutBand</b> - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.
• <i>SIP INFO</i> - Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.
<b>Payload Type (rfc2833)</b> - Type a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

# 3.12.4 Status

From this page, you can find codec, connection and other important call status for each port.

VoIP >> Status

Status								Refresh	Secon	ds: 1	0 💌	Refresh
Port	Status	Codec	PeerID	Elapse(hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter(ms)	In Calls	Out Calls	Miss Calls	Speaker Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5

Date		Time	Duration	In/Out/Miss	Account ID	Peer ID
(mm-dd-y	ууу)	(hh:mm:ss)	(hh:mm:ss)			
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	
						,

xxxxxxxx : VoIP is encrypted. xxxxxxxxx : VoIP isn't encrypted.

Available settings are explained as follows:

Item	Description
Refresh Seconds	Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.

**Dray** Tek

	Refresh Seconds : 10 🛩 5 10 30			
Port	It shows current connection status for Phone(s) ports.			
Status	It shows the VoIP connection status.			
	<b>IDLE -</b> Indicates that the VoIP function is idle.			
	<b>HANG_UP</b> - Indicates that the connection is not established (busy tone).			
	<b>CONNECTING -</b> Indicates that the user is calling out.			
	<b>WAIT_ANS</b> - Indicates that a connection is launched and waiting for remote user's answer.			
	<b>ALERTING -</b> Indicates that a call is coming.			
	<b>ACTIVE-</b> Indicates that the VoIP connection is launched.			
Codec	Indicates the voice codec employed by present channel.			
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).			
Elapse(hh:mm:ss)	The format is represented as hours:minutes:seconds.			
Tx Pkts	Total number of transmitted voice packets during this connection session.			
Rx Pkts	Total number of received voice packets during this connection session.			
Rx Losts	Total number of lost packets during this connection session.			
Rx Jitter	The jitter of received voice packets.			
In Calls	Accumulation for the times of in call.			
Out Calls	Accumulation for the times of out call.			
Miss Calls	Accumulation for the times of missing call.			
Speaker Gain	The volume of present call.			
Log	Display logs of VoIP calls.			

# **3.13 Wireless LAN**

This function is used for "n" models only.

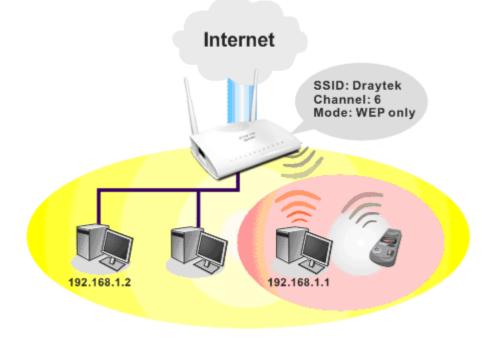
## 3.13.1 Basic Concepts

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.

# **Dray** Tek

## **Security Overview**

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Wireless LAN General Setup Security Access Control WPS WDS Advanced Setting WMM Configuration AP Discovery Station List

Vigor2760 Series User's Guide

# 3.13.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN(2.4GHz) >> General Setup
---------------------------------------

able Wireless L	AN			
Mode :	1	Mixed(11b+11g+11n) 🔽		
Channel:		Channel 6, 2437MHz 🛛 👻		
Enable Hid	le SSID	SSID	Isolate Member	Isolate VPN
1	D	rayTek		
2		rayTek_Guest		
3				
4				
the same SSII The isolate VP	) from conne N configurati	er configuration will forbid th cting to each other. on will isolate the wireless t ot be able to access the VP	raffic from VPN conn	ections and
Enabling the I the same SSII The isolate VP	D from conne N configurati clients will n	cting to each other. on will isolate the wireless t ot be able to access the VPI	raffic from VPN conn N network under this	ections and s setting.
Enabling the I the same SSII The isolate VP thus, wireless Rate Control	) from conne N configurati	cting to each other. on will isolate the wireless t ot be able to access the VPI	raffic from VPN conn N network under this Downloa	ections and s setting.
Enabling the I the same SSII The isolate VP thus, wireless Rate Control SSID 1	D from conne N configurati clients will n	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps	raffic from VPN conn N network under this Downloa 30000	ections and setting. ad kbps
Enabling the I the same SSII The isolate VP thus, wireless Rate Control SSID 1 SSID 2	D from conne N configurati clients will n	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps 30000 kbps	raffic from VPN conn N network under this Downloa 30000 30000	ections and s setting. ad kbps kbps
Rate Control SSID 1 SSID 2 SSID 3	D from conne N configurati clients will n Enable	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps 30000 kbps 30000 kbps	raffic from VPN conno N network under this Downloa 30000 30000 30000	ections and s setting. ad kbps kbps kbps
Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note:	D from conne N configurati clients will n Enable	cting to each other. on will isolate the wireless to ot be able to access the VPI Upload 30000 kbps 30000 kbps 30000 kbps 30000 kbps	raffic from VPN conno N network under this Downloa 30000 30000 30000 30000	ections and s setting. ad kbps kbps
Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note:	D from conne N configurati clients will n Enable	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps 30000 kbps 30000 kbps	raffic from VPN conno N network under this Downloa 30000 30000 30000 30000	ections and s setting. ad kbps kbps kbps
Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note:	D from conne N configurati clients will n Enable	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps 30000 kbps 30000 kbps 30000 kbps 00000 kbps	raffic from VPN conno N network under this Downloa 30000 30000 30000 30000	ections and s setting. ad kbps kbps kbps
Enabling the I the same SSII The isolate VP thus, wireless Rate Control SSID 1 SSID 2 SSID 3 SSID 4 Note: Configurable u Associated Sc Note:	D from conne N configurati clients will n Enable D D D D D D D D D D D D D D D D D D D	cting to each other. on will isolate the wireless t ot be able to access the VPI Upload 30000 kbps 30000 kbps 30000 kbps 30000 kbps 00000 kbps	raffic from VPN conno N network under this Downloa 30000 30000 30000 to 50,000(kbps).	ections and setting. d kbps kbps kbps kbps kbps

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	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.

Cancel

ΟK

Channel	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only (2.4 GHz) Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Mixed(11b+11g+11n) Channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. Channel 6, 2437MHz Channel 7, 2412MHz Channel 1, 2412MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz
	Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz mber configuration will forb
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
Isolate	<ul> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> <li>VPN – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</li> </ul>
Rate Control	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.
Schedule	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules



	pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
--	--------------------------------------------------------------------------------------------------------------------------------------------

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

# 3.13.3 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.



**Note:** All wireless devices must support the same encryption bit length and share the same key. If WEP mode is selected, only one of four preset keys can be selected at one time.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

#### Wireless LAN >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4	
Mode:			Mixed(WPA+	WPA2)/PSK 💌
<u>WPA</u>				
	Encryption Mode	:	TKIP for WPA	VAES for WPA2
	Pre-Shared Key(	PSK):	******	
	Type 8~63 ASCI "cfgs01a2" or			digits leading by "0x", for example
WEP				
	Encryption Mode	:	64-Bit 🔽	
			******	
	○Кеу 2 :		**********	
	○Кеу 3 :		*********	
	○Кеу 4 :		*****	
Note:				
	bit WEP key con eading by "Ox". E			II characters or 10 Hexadecimal 2333132".
	3 bit WEP key co eading by "Ox".	nfigurations, ple	ase insert 13 A	SCII characters or 26 Hexadecimal

OK

Cancel

Item	Description
Item Mode	Description         There are several modes provided for you to choose.         Mixed(WPA+WPA2)/PSK         Disable         WEP         WPA/PSK         WPA2/PSK         Mixed(WPA+WPA2)/PSK         Hevadecimal digits leading by         Disable - Turn off the encryption mechanism.         WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.
	<ul> <li>WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.</li> <li>WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.</li> </ul>
	<b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such



	as "0x321253abcde").
	<b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only. <b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
WEP	<b>64-Bit</b> - For 64 bits WEP key, either <b>5</b> ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
	<b>128-Bit</b> - For 128 bits WEP key, either <b>13</b> ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).
	Encryption Mode: 64-Bit 64-Bit 128-Bit
	All wireless devices must support the same WEP encryption bit size and have the same key. <b>Four keys</b> can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

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

## 3.13.4 Access Control

Wireless LAN(2.4GHz) >> Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Enable Mac Address Filter	SSID 1 White List	SSID 2 White List V
	SSID 3 White List	SSID 4 White List
	MAC Address Filt	er
Index Attribute	MAC Address	Apply SSID
	s MAC Address : : : : : :	
	s MAC Address : : : : : :	
Apply SSID		SSID 3 SSID 4

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.

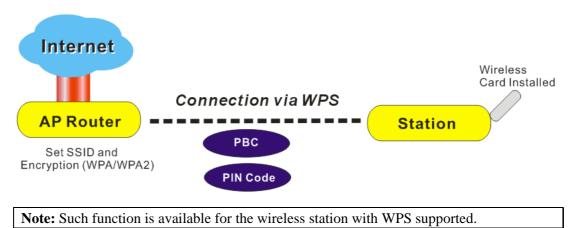


Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

## 3.13.5 WPS

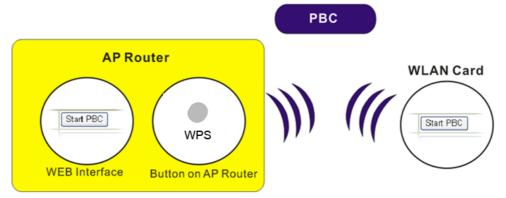
**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



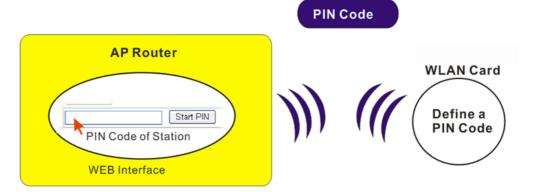
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 2760 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



• If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

#### Below shows Wireless LAN>>WPS web page:

#### Wireless LAN >> WPS (Wi-Fi Protected Setup)

🗹 Enable WPS 🗘

#### Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Mixed(WPA+WPA2)/PSK

#### Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Ready

Note: WPS can help your wireless client automatically connect to the Access point.

♀: WPS is Disabled.

♥: WPS is Enabled.

🔅 : Waiting for WPS requests from wireless clients.

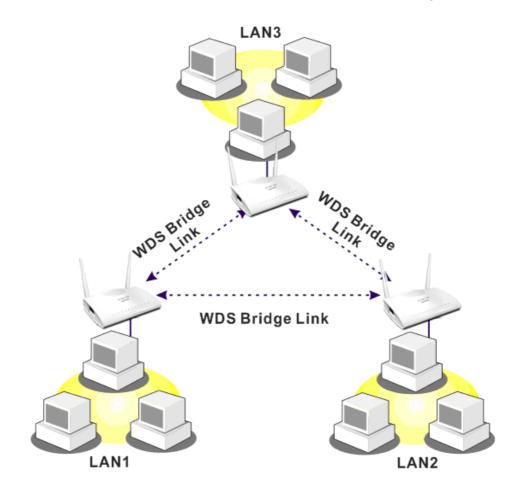
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

## 3.13.6 WDS

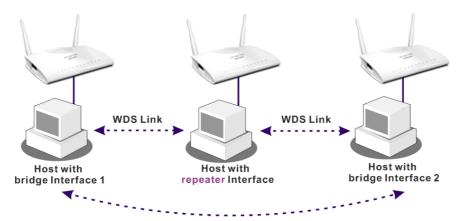
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

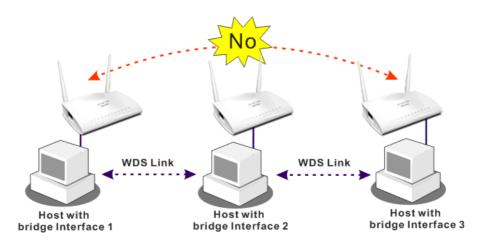


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

Wireless LAN >> WDS Settings

Mode: Disable V	Bridge
Mode: Disable Security: Disable WEP Pre-shared Key WEP: Use the same WEP key set in Security Settings. Pre-shared Key: Type: DrayTek WPA WPA WPA2 Key : Type 8~63 ASCII characters or 64 hexadecimal digits leading by "Dx", for example "cfgs01a2"	Bridge Enable Peer MAC Address  Enable Peer MAC Address  Enable Peer MAC Address  Repeater Enable Peer MAC Addess  Enable Peer MAC Addess  Enable Peer MAC Addess  Access Point Function:  Enable Disable
	Status: Send "Hello" message to peers. Link Status Note: The status is valid only when the peer als supports this function.

Item	Description
Mode	Choose the mode for WDS setting. <b>Disable</b> mode will not invoke any WDS setting. <b>Bridge</b> mode is designed to fulfill the first type of application. <b>Repeater</b> mode is for the

	second one.
	Disable Disable Bridge Repeater
Security	There are three types for security, <b>Disable</b> , <b>WEP</b> and <b>Pre-shared key</b> . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in <b>Security Settings</b> page. If you did not set any key in <b>Security Settings</b> page, this check box will be dimmed.
Pre-shared Key	<b>Type</b> – There are some types for you to choose. <b>WPA</b> and <b>WPA2</b> are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. <b>Key</b> - Type 8 ~ 63 ASCII characters or 64 hexadecimal 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 <b>Enable</b> 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 <b>Enable</b> box in the front of the MAC address after typing.
Access Point Function	Click <b>Enable</b> to make this router serving as an access point; click <b>Disable</b> to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

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

## 3.13.7 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	💿 Mixed Mode 🔘 Green Field
Channel Bandwidth	O 20 💿 20/40
Guard Interval	🔘 long 💿 auto
Aggregation MSDU(A-MSDU)	🔿 Disable 💿 Enable
Long Preamble	💿 Disable 🔘 Enable
Packet-OVERDRIVE TM TX Burst	💿 Disable 🔘 Enable

OK

Item	Description
Operation Mode	<b>Mixed Mode</b> – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
	<b>Green Field</b> – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	<b>20-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.
	<b>20/40</b> – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose <b>auto</b> as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable.</b>
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 <b>Enable</b> to use <b>Long Preamble</b> if needed to communicate with this kind of devices.
Packet-OVERDRIVE	This feature can enhance the performance in data

transmission about 40%* more (by checking <b>Tx Burs</b> t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.		
<b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b> ).		
Vigor N61 802.11n Wireless USB Adapter Utility		
Configuration Status Option About		
-General Setting	Advance Setting	
🔽 Auto launch when Windows start up	🔲 Disable <u>R</u> adio	
Remember mini status position	Fragmentation Threshold :	2346
🔲 Auto <u>h</u> ide mini status	RTS Threshold :	2347
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH 🐱
Enable IP Setting and Proxy Setting in Profile	Ad-hoc Channel:	1
Group Rosming Ad-hoc	Power Save Mode:	Disable
	Tx Burst :	Disable
WLAN type to connect <ul> <li>Infrastructure and Ad-hoc network</li> <li>Infrastructure network only</li> <li>Ad-hoc network only</li> </ul>	, <u>-</u>	
Automatically connect to non-preferred networks		
Tx <u>B</u> urst : Diss Diss Ena	lble	Cancel Apply
Note: * means the real tran	smission rate of	lepends on the
environment of the network		1

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



## 3.13.8 WMM Configuration

Wireless LAN(2.4GHz) >> 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.

VMM Configura	MM Configuration Set to Factory Default					
WMM Capable	2	Enable	🔿 Disable			
PSD Capable	2	🔘 Enable	Oisable			
VMM Paramete	ers of Access Poi	int				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
AC_BK	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
VMM Paramete	ers of Station					
	Aifsn	CWMin	1	CWMax	Тхор	ACM
AC_BE	3	4		10	0	
AC_BK	7	4		10	0	
AC_VI	2	3		4	94	
AC_VO	2	2	]	3	47	

0K

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
APSD Capable	The default setting is <b>Disable</b> .
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference

	between AC_BE and AC_BK categories must be greater.
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
АСМ	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> Vigor2760 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.

## 3.13.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List			
	BSSID	Channel	SSID
			~
			<u></u>
		Scan	]
See <u>St</u>	atistics.		
	ouring the scanning proc e router.	ess (~5 secor	ids), no station is allowed to connect
Add to	WDS Settings :		
AP's MA	AC address	::	
Add t	to	💿 Bridge	O Repeater

Wireless LAN >> Access Point Discovery

Item	Description	
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.	
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics           Recommended channels for usage:12345678910111213         AP number v.s. Channel         1 2 3 4 5 6 7 8 9 10 11 12 13 14         Channel	
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click <b>Add to</b> . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.	

## 3.13.10 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	
		Refresh		
	Status Codes : C: Connected, N E: Connected, W B: Connected, W	EP.		
	P: Connected, W A: Connected, W	PA2.		
	B: Blocked by Ac N: Connecting.	cess Control.		
	F: Fail to pass W	PA/PSK authentication.		
		e. In that case, it will still	r successfully, it may be turned be on the list until the	
	Add to Access Co	ntrol :		
	Client's MAC add	ress ::::	: : : : : : : : : : : : : : : : : : : :	
		Add	1	

Wireless LAN(2.4GHz) >> Station List

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.

## **3.14 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.

USB Application USB General Settings USB User Management File Explorer USB Device Status Modem Support List

## 3.14.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server. 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	5 (Maximum 6)
Default Charset	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 multiconnection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.

OK

Item	Description
General Settings	<b>Simultaneous FTP Connections -</b> This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.
	<b>Default Charset -</b> At present, Vigor router supports four types of character sets. Default Charset is for English based file name.



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

## 3.14.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

USB User Mar	nagement			1	Set to Factory Default
Index	Username	Home Folder	Index	Username	Home Folder
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

Click index number to access into configuration page.

USB Application >> USB User Management

Profile Index: 1	
FTP/Samba User	🔘 Enable 🛛 💿 Disable
Username	
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	2
Access Rule	
File	🗌 Read 📃 Write 🔛 Delete
Directory	🗌 List 📃 Create 📃 Remove
Note: The folder name can only contair and space.	h the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) /
01	Clear Cancel

Item	Description
FTP/Samba User	<b>Enable</b> – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.



	<b>Disable</b> – Click this button to disable such profile.			
Username	<ul> <li>Type the username for FTP/Samba users for accessing in FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you cat 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.</li> <li>Note: "Admin" could not be typed here as username, for</li> </ul>			
	the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.			
	<b>Note:</b> FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.			
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk. The length of the password is limited to 11 characters.			
Confirm Password	Type the password again to make confirmation.			
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk. Note: When write protect status for the USB storage disk is <b>ON</b> , you cannot type any new folder name in this field. Only "/" can be used in such case. You can click <b>?</b> to open the following dialog to add any new folder which can be specified as the Home Folder. <b>Volue thangement</b> <b>Volue thangement</b> <b>Volue</b>			
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.         File – Check the items (Read, Write and Delete) for such profile.         Directory –Check the items (List, Create and Remove) for such profile.			

Before you click **OK**, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

## 3.14.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Appl	USB Application >> File Explorer								
File Explo	orer								
<del>49</del>	•	<b>2</b>	Current Path: /						
			Name				Size	Delete	Rename
🚹 Uplo	ad File								
Select a		<b>*</b>	覽						

Note: The folder can not be deleted when it is not empty.

Item	Description
** Refresh	Click this icon to refresh files list.
→ Back	Click this icon to return to the upper directory.
🧭 Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

## 3.14.4 USB 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.

Disk	Modem	Printer	<u>Refresh</u>
USB Mass Storag	ge Device Status		
Connection Sta	atus: No Disk Conne	cted	Disconnect USB Disk
Disk Capacity:	0 MB		
Free Capacity:	0 MB <u>Refresh</u>		
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.

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 <b>Refresh</b> at any time to get new status for free capacity.		
Index	It displays the number of the client which connecting to FTP server.		
IP Address	It displays the IP address of the user's host which connecting to the FTP server.		
Username	It displays the username that user uses to login to the FTP server.		

Available settings are explained as follows:

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

Disk	Modem	Printer		Refresh
USB Mass Storage	e Device Status			
Connection Status: Disk Connected Disconnect USB Disk Write Protect Status: No				
Disk Capacity: 2009 MB Free Capacity: 925 MB <u>Refresh</u>				
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.



## 3.14.5 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.

3.5G	LTE	WIMAX	
Brand		Module	Status
4G system	XSPlug P	3	С
Aiko	Aiko 76E		Y
Aiko	Aiko 83D		Y
Alcatel	×080S		м
Alcatel	×230		м
Alcatel	×500		С
Alfa	Fly3G		Y
Amoi	Amoi H01	L	Y
AnyDATA	ADU-300		Y
AnyDATA	ADU-500	A	Y
AnyDATA	ADU-510	A	м
ASUS	ASUS T5	00	м
BandRich	Bandluxe	C100	м
BandRich	Bandluxe	C100S[1]	м
BandRich	Bandluxe	Bandluxe C170	
RandDich	Randluve	C270	$\sim$

## 3.15 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog /Mail Alert, Time and Date, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

and the second se
System Maintenance
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
DSL Firmware Upgrade
Activation

## 3.15.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

#### System Status

Model Name	: Vigor2760Vn
Firmware Version	: 3.7.5.1
Build Date/Time	: Mar 31 2014 10:02:56

		LAN			
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1 LAN2	00-1D-AA-B8-15-00	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-1D-AA-B8-15-00	192.168.2.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-1D-AA-B8-15-00	192.168.0.1	255.255.255.0	ON	8.8.8.8

	Wireless LA	N	
MAC Address	Frequency Domain	Firmware Version	SSID
00-1D-AA-B8-15-00	Europe	2.7.1.5	DrayTek

WAN				
Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1 Disconnected	00-1D-AA-B8-15-01	PPPoE		
WAN2 Disconnected	00-1D-AA-B8-15-02			
WAN3 Disconnected	00-1D-AA-B8-15-03			

	I	P∨6		
Addre:	SS	Scope	Internet Access Mode	
LAN FE80::	:21D:AAFF:FEB8:1500/64	Link		
	v	/oIP		
Port Phone1	Profile	Reg.	In/Out	
Phone1		No	0/0	
Phone2		No	0/0	

User Mode is OFF now.



Item	Description
Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN	MAC Address
	- Display the MAC address of the LAN Interface.
	IP Address
	- Display the IP address of the LAN interface.
	Subnet Mask
	- Display the subnet mask address of the LAN interface.
	DHCP Server
	- Display the current status of DHCP server of the LAN
	interface
	DNS
	- Display the assigned IP address of the primary DNS.
WAN	Link Status
	- Display current connection status.
	MAC Address
	- Display the MAC address of the WAN Interface.
	Connection
	- Display the connection type.
	IP Address
	- Display the IP address of the WAN interface.
	Default Gateway
	- Display the assigned IP address of the default gateway.
IPv6	Address - Display the IPv6 address for LAN.
	<b>Scope -</b> Display the scope of IPv6 address. For example, IPv6 <b>Link Local</b> could only be used for direct IPv6 link. It can't be used for IPv6 internet.
	<b>Internet Access Mode</b> – Display the connection mode chosen for accessing into Internet.

## 3.15.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

System Maintenance >> TR-069 Setting	
--------------------------------------	--

ACS and CPE Settings	
ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
	Test With Inform Event Code PERIODIC
Last Inform Respor	ise Time :(NA) 🥌
CPE Client O Enable 💿 D	isable
URL	
Port	8069
Username	vigor
Password	••••••
Periodic Inform Settings	
💿 Disable	
🔘 Enable	
Interval Time	900 second(s)
STUN Settings	
<ul> <li>Disable</li> </ul>	
🔘 Enable	
Server Address	
Server Port	3478
Minimum Keep /	Alive Period 60 second(s)
Maximum Keep	Alive Period -1 second(s)
	OK

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
	<b>Test With Inform</b> – Specify the Event Code from the drop down list. Click this button to make a test for the response from VigorACS.
	<b>Last Inform Response Time -</b> Display the response time informed by VigorACS.

CPE Client	Such information is useful for Auto Configuration Server. <b>Enable/Disable</b> – Allow/Deny the CPE Client to connect with Auto Configuration Server.		
	<b>Port</b> – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.		
Periodic Inform Settings	The default setting is <b>Enable</b> . Please set <b>interval time</b> or schedule time for the router to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.		
STUN Settings	The default is <b>Disable</b> . If you click <b>Enable</b> , please type the relational settings listed below:		
	<b>Server IP</b> – Type the IP address of the STUN server.		
	<b>Server Port</b> – Type the port number of the STUN server.		
	<b>Minimum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".		
	<b>Maximum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.		

## 3.15.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password	
Old Password	
New Password	(Max. 23 characters allowed)
Confirm Password	(Max. 23 characters allowed)
Note: Password can contain only a	a-z A-Z O-9,;:."<>*+=\ ?@#^!()

OK

Available settings are explained as follows:

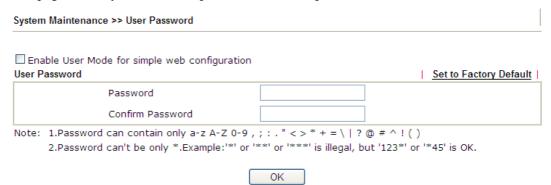
Item	Description
Old Password	Type in the old password. The factory default setting for password is <b>"admin"</b> .
New Password	Type in new password in this field.
Confirm Password	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.



## 3.15.4 User Password

This page allows you to set new password for user operation.



Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration.
	The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Type in the new password again.
Set to Factory Default	Click to return to the factory default setting.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

Below shows an example for accessing into User Operation with User Password.

1. Open System Maintenance>>User Password.

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**.

Jser Passwor	er Mode for simple web configur d		Set to Factor
	Password	••••	]
	Confirm Password	•••••	]
Note: 1.Pas	Confirm Password		@ # ^ ! ( )
	sword can't be only *.Example:'		

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password						
Active Configuration						
Password	. *****					

4. Log out Vigor router web user interface by clicking the Logout button.



5. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.

<b>Dray</b> Tek	Vigor2760 Series
Login	
Username Password	•••••
Delight _{Cor}	Login byright © 2013 DrayTek Corp. All Rights Reserved

6. The main screen with User Mode will be shown as follows.

<b>Dray</b> Tek	k v	ligor	2760 Ser	ies					Delight
Auto Logout 💌 🛛 🥵	Dashboar	d							
Dashboard Wizards Online Status WAN LAN Route Policy NAT			o		`	Algor2760		000	D (D)
Applications Wireless LAN	Queters la	5	ine		_				Ouisk Assess
System Maintenance Diagnostics	System in								Quick Access
brughtanca	Model Nam		Vigor2760Vn		System Up Time		2:27:33 2000 Jan 1 Sat 2:27:29		System Status Dynamic DNS
		Router Name Firmware Version					4 10:02:56	<u>Dynamic DNS</u>	
	DSL Versio		3.7.5 05-04-04-04-04	D-01		IAC Address	00-1D-AA-		
	IPv4 Inter	net Aco	ess		-				1
		Line / I	Node	IP Address		MAC Addres	s	Up Time	
	WAN1	ADSL /	PPPoE	Disconnecte	d	00-1D-AA-B	8-15-01	00:00:00	1
	WAN2	Ethern	et /	Disconnecte	ed	00-1D-AA-B	8-15-02	00:00:00	
	WAN3	USB /		Disconnecte	d	00-1D-AA-B	8-15-03	00:00:00	
	IPv6 Inter	net Aco	ess						
All Rights Reserved.		Mode	Add	lress	Scope		Up Time		
	LAN	RADVD	/ DHCPv6 FE8	0::21D:AAFF	FEB8:	1500/64	Link		]
	Interface								
	DSL	Conneo	cted : Down Stre	am : OKbps /	Up Str	eam : OKbps			1
	WAN		cted : 0, 🛛 🔍 WAI			VAN3			1

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

Note: Setting in User Mode can be configured as same as in Admin Mode.

## 3.15.5 Login Page Greeting

System Maintenance >> 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.

Enable			
Login Page Title	Router Login	(31 char max.)	
Welcome Message	and Bulletin (Max 511 characters)	Preview Set to Factory D	<u>efault</u>
HTML so lists s	ich as this one can be create or img can be used		





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.

🖉 Vigor Login Page - Windows Internet Explorer 📃 🗖 🔀
🔊 http://192.168.1.1/weblogin.htm
Just for Carrie Username Password Group V Login Copyright@, DrayTek Corp. All Rights Reserved.
Welcome Message
This welcome message is displayed in the Login page of the router. Replace this text with your own message.
<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>

## 3.15.6 Configuration Backup

### **Backup the Configuration**

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

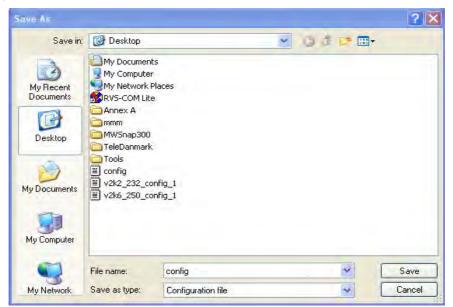
System	Maintenance	>>	Configuration	Backup
--------	-------------	----	---------------	--------

Configuration Backup / Restoration			
Restoration			
	Select a configuration file.		
	Select		
	Click Restore to upload the file.		
	Restore		
Backup			
	Click Backup to download current running configurations as a file.		
	Backup Cancel		

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Dov	wnload 🛛 🔀
2	You are downloading the file: config.cfg from 192,168.1.1 Would you like to open the file or save it to your computer? Open Save Cancel More Info I Always ask before opening this type of 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.

ystem Maintenance >> Configuration Backup		
Configuration	Backup / Restoration	
Restoration		
	Select a configuration file.	
	Select	
	Click Restore to upload the file.	
	Restore	
Backup		
	Click Backup to download current running configurations as a file.	
	Backup Cancel	

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

## 3.15.7 Syslog/Mail Alert

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.

SysLog / Mail Alert Setup				
SysLog Access Setup		Mail Alert Setup		
🗹 Enable		🗹 Enable	Send a test e-mail	
Syslog Save to: Syslog Server		SMTP Server		
USB Disk		SMTP Port	25	
Router Name		Mail To		
Server IP Address		Return-Path		
Destination Port	514	Use SSL		
Mail Syslog	🗖 Enable	Authentication		
Enable syslog message:		Username		
🗹 Firewall Log		Password		
VPN Log		Enable E-Mail Alert:		
✓ User Access Log		DoS Attack		
✓ Call Log		IM-P2P		
WAN Log				
🗹 Router/DSL inform	ation	VPN LOG		

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to".

Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.
 We only support secured SMTP connection on port 465.



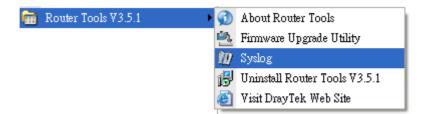
Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog.
	<b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.
	Check <b>USB Disk</b> to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in <b>System</b> <b>Maintenance&gt;&gt;Management.</b>
	If there is no name here, simply lick the link to access into <b>System Maintenance&gt;&gt;Management</b> to set the router name.
	Server IP Address - The IP address of the Syslog server.
	<b>Destination Port -</b> Assign a port for the Syslog protocol.
	<b>Mail Syslog</b> – Check the box to recode the mail event on Syslog.
	<b>Enable syslog message -</b> Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.

Mail Alert Setup	Check <b>Enable</b> to activate function of mail alert.
	<b>Send a test e-mail -</b> Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
	<b>SMTP Server/SMTP Port -</b> The IP address/Port number of the SMTP server.
	Mail To - Assign a mail address for sending mails out.
	<b>Return-Path</b> - Assign a path for receiving the mail from outside.
	<b>Use SSL -</b> Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
	Authentication - Check this box to activate this function while using e-mail application.
	User Name - Type the user name for authentication.
	<b>Password -</b> Type the password for authentication.
	<b>Enable E-mail Alert -</b> Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



	ayTek ≢≣₽ש	172.16.3.1	30 💌	- WAN Inform	Syslog U nation TX Rate	RX Rate
-	Mise					P IP
Apply to:	Tool Setup Telnet Read-out Setup	Codepage Information Recovery Net	twork Information	Net State		
irewall	Host Name	carrie-0c7cb251				
	NIC Description Al	heros AR8121/AR8113/AR8114 PCI-E Eti	hernet Controller - P	acket Schedul 🗸		
System	NIC Information		On Line Routers			
	MAC Address	E0-CB-4E-DA-48-79	IP Address	Mask	MAC	
	IP Address	192.168.1.10	192.168.1.5	255.255.25	00-50-7F-CD-0	
	Subnet Mask	255.255.255.0				
	DNS Servers	8.8.4.4 8.8.8.8				
	Default Geteway	192.168.1.5				
	DHCP Server	192.168.1.5				
	Lease Obtained	Tue Aug 27 00:04:10 2013				
	Lease Expires	Fri Aug 30 00:04:10 2013			Refresh	
				ОК	Cancel	

System Time: Time tag from the computer which runs the syslog application

Router Time: Time tag from route

## 3.15.8 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Time and Date

#### Time Information

Current System Time 2014 Jan 2	22 Wed 15 : 18 : 53 Inquire Time
Time Setup	
🔘 Use Browser Time	
💿 Use Internet Time	
Time Server	pool. ntp. org
Priority	Auto 💌
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	
Automatically Update Interval	30 min 💌
	OK Cancel

Available settings are explained as follows:

Item	Description	
Current System Time	Click <b>Inquire Time</b> to get the current time.	
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.	
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.	
Time Server	Type the IP address of the time server.	
Priority	Choose Auto or IPv6 First as the priority.	
Time Zone	Select the time zone where the router is located.	
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.	
Automatically Update Interval	Select a time interval for updating from the NTP server.	

Click **OK** to save these settings.

### 3.15.9 SNMP

Applications >> 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.

Enable SNMP Agent	
Get Community	public
Set Community	private
Manager Host IP(IPv4)	
Manager Host IP(IPv6)	
Trap Community	public
Notification Host IP(IPv4)	
Notification Host IP(IPv6)	
Trap Timeout	10
Enable SNMPV3 Agent	
USM User	
Auth Algorithm	No Auth 🗸
Auth Password	
Privacy Algorithm	No Priv 🗸
Privacy Password	

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 <b>public.</b>	
	The maximum length of the text is limited to 23 characters.	
Set Community	Set community by typing a proper name. The default setting is <b>private.</b>	
	The maximum length of the text is limited to 23 characters.	
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 <b>public.</b>	
	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.           No Auth         No Auth           MD5         SHA
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. No Priv V DES AES
Privacy Password	Type a password for privacy. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

## 3.15.10 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, and External Device Control.

The management pages for IPv4 and IPv6 protocols are different.

### For IPv4

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Se	tup	
Router Name			
Default:Disable Auto-Logout	Management Port S	etup	
	💽 User Define P	orts	
Internet Access Control	🔘 Default Ports		
Allow management from the Internet	Telnet Port	23	(Default: 23)
FTP Server	HTTP Port	80	(Default: 80)
🗹 HTTP Server	HTTPS Port	443	(Default: 443)
HTTPS Server	FTP Port	21	(Default: 21)
Telnet Server	TR069 Port	8069	 (Default: 8069)
🗹 TR069 Server	SSH Port	22	(Default: 22)
SSH Server		22	
🗹 Disable PING from the Internet	External Device Con	trol	
LAN Access Control	No respond to	External De	vice
Allow management from LAN			
FTP Server			
Telnet Server			
Apply To Subnet			
VLAN2			
✓ IP Routed Subnet			
Access List from the Internet List IP Subnet Mask			
1 Subnet Mask			
2	×		
3	~		

Note: Subnet LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.

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.

	Logout
Internet Access Control	<ul> <li>Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.</li> <li>Disable PING from the Internet - Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.</li> </ul>
LAN Access Control	<ul> <li>Allow management from LAN- Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.</li> <li>Apply To – Check the LAN interface for the administrator to use for accessing into web user interface of Vigor router.</li> </ul>
Access List from the Internet	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. List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.
Management Port Setup	<ul> <li>User Define Ports - Check to specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.</li> <li>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</li> </ul>
External Device Control	<b>No respond to External Device</b> – Check the box to make Vigor2760 not being detected by other router and not being displayed as an external device.

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



## For IPv6

System Maintenance >> Management

IP\	/4 Management Setup	IPv6 Management Setup	
Manag	jement Access Control		
Allov	w management from the Intei	rnet	
	Telnet Server ( Port : 23)		
	🔲 HTTP Server ( Port : 2860)	)	
	📃 HTTPS Server ( Port : 443)	)	
	SSH Server ( Port : 22)		
<b>[</b> ]	Enable PING from the Interne	t	
Acces	is List		
List	IPv6 Address / Prefix Lengtł	า	
1.		/ 128	
2.		/ 128	
з.		/ 128	
Note :	Telnet / Http server port is th	ne same as IPv4.	

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 to allow you managing the router from Internet. Check the box(es) to specify.
	<b>Enable PING from the Internet</b> - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	<b>IPv6 Address /Prefix Length-</b> Indicate the IP address(es) allowed to login to the router.

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

## 3.15.11 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 ?
	Osing current configuration
	O Using factory default configuration
Auto Reboot Time Sch	Reboot Now
Inde	x(1-15) in <u>Schedule</u> 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.

## 3.15.12 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.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

Web Firmware Upgrade

Select a firmware file. Select Click Upgrade to upload the file. Upgrade

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.7.5.1	
Firmware Upgrade Procedures:	
<ol> <li>Click "OK" to start the TFTP server.</li> <li>Open the Firmware Upgrade Utility or other 3-party TFTP client software.</li> <li>Check that the firmware filename is correct.</li> <li>Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.</li> <li>After the upgrade is compelete, the TFTP server will automatically stop running.</li> </ol>	
Do you want to upgrade firmware ? OK	

Click OK. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade



For the detailed information about firmware update, please go to Chapter 5.

## 3.15.13 DSL Firmware Upgrade

This function is used to upgrade modem code if you find built-in modem code is not suitable for Vigor router. Contact with your dealer for further assistance if required.

## System Maintenance >> Modem Code Upgrade Web DSL Modem Code Upgrade Select a modem code file. Select Click Upgrade to upload the file. Upgrade

### 3.15.14 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

System Maintenance >> Activation	Activate via interface : auto-selected 💌
Web-Filter License [Status:Not Activated]	Activate
Authentication Message	
Note: If you want to use email alert or syslog, plea If you change the service provider, the confi	

OK Cancel

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter. auto-selected WAN 1 WAN 2
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 <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation	Activate via interface : auto-selected 🗸
Web-Filter License [Status:Commtouch] [Start Date:2011-03-28 Expire Date:	Activate 2011-04-27]
Authentication Message	-
WebFilter, Activation authenticate fail, contact w O1 00:00:24	rith support@draytek.com, 2C 🖉
Note: If you want to use email alert or syslog, please configure t If you change the service provider, the configuration of the	
OK Cancel	)

## 3.16 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.

Diagnostics Dial-out Triggering Routing Table ARP Cache Table IPv6 Neighbour Table DHCP Table NAT Sessions Table Ping Diagnosis Data Flow Monitor Traffic Graph Trace Route Syslog Explorer IPv6 TSPC Status

## 3.16.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

```
Diagnostics >> Dial-out Triggering
```

HEX Format:	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00 00 00 00 00 00 00	
Decoded Format:	
0.0.0.0 -> 0.0.0.0	
Pr 0 len 0 (0)	

Item	Description	
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.	
Refresh	Click it to reload the page.	

# 3.16.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
	0 directly connected LAN2 0 directly connected LAN1	
		•

Note: WAN4, WAN5, WAN6 are router-borne WANs.

#### Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 R	outing Table		1	Refres	<u>h</u>
Destination FE80::/64 FF00::/8	Interface LAN LAN	υ	Metric 256 256	Next Hop		^
<					N	~

Item	Description
Refresh	Click it to reload the page.

## 3.16.3 ARP Cache Table

Click Diagnostics and click ARP Cache Table to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

```
Diagnostics >> View ARP Cache Table
```

Ethernet ARP Cache	Table			Clear Refresh
IP Address 192.168.1.5	MAC Address 00-50-7F-CD-07-48	Netbios Name	Interface LAN1	<u>^</u>
192.168.1.49	E0-CB-4E-DA-48-79	CARRIE-0C7CB251	LAN1	
				<u>~</u>

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

### 3.16.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Diagnostics >> View IPv6 Neighbour Table

IPv6 Address	Mac Address	Interface
FF02::2	33-33-00-00-00-02	LAN
FF02::1:3	33-33-00-01-00-03	LAN
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN
FF02::1	33-33-00-00-00-01	LAN
FF02::1	00-00-00-00-00	USB2
FF02::1:2	00-00-00-00-00-00	USB2
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN
<		>

<b>_</b>
----------



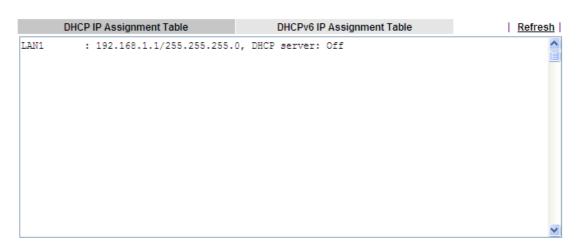
Refresh	Click it to reload the page.
---------	------------------------------

## 3.16.5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

Diagnostics >> View DHCP Assigned IP Addresses



#### Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table	DHCPv6 IP Assignment Table	<u>Refresh</u>
DHCPv6 server binding client: Index IPv6 Address	MAC Address Leased Time	
<		∑ ×

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.



HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

## 3.16.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

Diagnostics >> NAT Sessions Table

```
NAT Active Sessions Table

        Private IP :Port #Pseudo Port
        Peer IP :Port Interface

        192.168.1.11
        2491
        52078
        24.9.93.189
        443
        WAN1

        192.168.1.11
        2493
        52080
        207.46.25.2
        80
        WAN1

        192.168.1.10
        3079
        52665
        207.46.5.10
        80
        WAN1
```

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

# 3.16.7 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis			
⊙ IPV4 O	IPV6		
		a LAN PC or you don't want to spec ct "Unspecified".	fy which WAN to
Ping thre	ough: Unspecifi	ied 💌	
Ping to:	Host/IP V Host/IP DNS	IP Address:	
Result	Gateway 1 Gateway 2 Gateway 3		Clear
			<b>y</b>

#### Diagnostics >> Ping Diagnosis

Ping Diagnosis	
○ IPV4 ③ IPV6	
Ping IPv6 Address:	
Run	
Result	Clear
	$\sim$

Item	Description	
IPV4/IPV6	Choose the interface for such function.	
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose <b>Unspecified</b> to be determined by the router automatically.	
Ping to	Use the drop down list to choose the destination that you want to ping.	
IP Address	Type the IP address of the Host/IP that you want to ping.	
Ping IPv6 Address	Type the IPv6 address that you want to ping.	



Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

## 3.16.8 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Bandwidth	Management >>	Sessions Limit
-----------	---------------	----------------

📀 Enab	le 🔘 Disable	
Default	Max Sessions:	100
imitatio.	n List	
Index	Start IP	End IP

Click Diagnostics and click Data Flow Monitor to open the web page. You can click IP Address, TX rate, RX rate or Session link for arranging the data display.

Diagnostics >> Data Flow Monitor

		Refresh Seco	nds: 10 🚩 Page	: 1 🕶		Refresh
Index	IP Address	TX rate(Kbps)	RX rate(Kbps) 😪	Sessions	Action	APP QoS
1	192.168.1.10_CARRIE- 0C7CB251	34	1	138	Block	None 💌
		0 (ID ) (	0 / ID   I	<b>6</b>		
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak		
WAN1	172.16.3.130	40 / 2476 / Auto	9 / 4022 / Auto	138		
WAN2			0 / 0 / Auto	0		
WAN3			0 / 0 / Auto	0		
Total		4ባ / 2476 / Auto	9 / 4022 / Auto	138,/395		

Enable Data Flow Monitor

2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

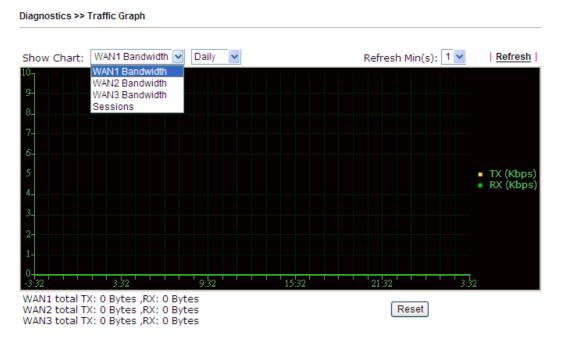
3. (Kbps): shared bandwidth

+ : residual bandwidth used Current/Peak are average.

Item	Description		
Enable Data Flow Monitor	Check this box to enable this function.		
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 10 • 10 15 30		
Refresh	Click this link to refresh this page manually.		
Index	Display the number of the data flow.		
IP Address	Display the IP address of the monitored device.		
TX rate (kbps)	Display the transmission speed of the monitored device.		
RX rate (kbps)	Display the receiving speed of the monitored device.		
Sessions	Display the session number that you specified in Limit Session web page.		
	within 5 minutes. Page: 1 V   Refresh   Sessions Action APP QoS 1 Block None V Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column. Page: 1 V   Refresh   Sessions Action APP QoS blocked / 299 Unblock None V		
Current /Peak/Speed	<ul> <li>Current means current transmission rate and receiving rate for WAN interface.</li> <li>Peak means the highest peak value detected by the router in data transmission.</li> <li>Speed means line speed specified in WAN&gt;&gt;General Setup. If you do not specify any rate at that page, here will display Auto for instead.</li> </ul>		

# 3.16.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.



## 3.16.10 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

Diagnostics >	> Trace Route		
Trace Route			
		Jnspecified 🗸	
	Protocol: II Host / IP Address:	CMP 🗸	
	Result		 Clear
			V

#### or

Diagnostics >> Trace Route

○ IPV4		
Trace Host / IP Address:		
	Run	
Result		Clear
		~

Item	Description	
IPv4 / IPv6	Click one of them to display corresponding information for it.	
Trace through	Use the drop down list to choose the interface that you want to ping through.	



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.

# 3.16.11 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

## For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Diagnostics >> Syslog Explorer

Time	Ν	lessage
	Syslog Type User 👻 Display Mode	e Stop record when fulls
Enable Web Syslog		Export   Refresh   Clear
Web Syslog	USB Syslog	

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. User User Firewall Call WAN VPN All
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose.

	Stop record when fulls Stop record when fulls Always record the new event
	<b>Stop record when fulls</b> – when the capacity of syslog is full, the system will stop recording.
	Always record the new event – only the newest events will be recorded by the system.
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.

Diagnostics >> Syslog Explorer

Web Syslog

USB Syslog

· · ·	show while the saved s	· ·		
Folder: n/a	File: n/a	Page: n/a	Log Type: n/a	
Time	Log Type		Message	

Item	Description
Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

# 3.16.12 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

WAN1	WAN2	WAN3		<u>Refres</u>
TSPC Enabled				
TSPC Connectio	n Status			
Local Endpoin	tv4 Address:	114.44.54.220		
Local Endpoin	tv6Address:	2001:05c0:1400:00	)0b:0000:0000:0000:10b9	
Router DNS na	me:	88886666.broker.fre	eenet6.net	
Remote Endpo	oint v4 Address :	81.171.72.11		
Remote Endpo	ointv6 Address :	2001:05c0:1400:00	)0b:0000:0000:0000:10b8	
Tspc Prefix :		2001:05c0:1502:0c	100:0000:0000:0000:0000	
Tspc Prefixlen	:	56		
Tunnel Broker	:	amsterdam.freenet	6.net	
Tunnel Status	:	Connected		

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.



# 4.1 How to configure settings for IPv6 Service in Vigor2760

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 Vigor2760, 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 Vigor2760, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client, Static IPv6, 6in4 Static Tunnel and 6rd.

1. Access into the web user interface of Viogr2760. 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		ADSL / VDSL2	None	~	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page IPv6
WAN3		USB	None	*	Details Page IPv6

Note: Only one WAN can support IPv6.



**Note:** Only one WAN interface support IPv6 service at one time. In this example, WAN2 is chosen as the one supporting IPv6 service.

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

WAN 2				
PPPoE	Static or Dynamic IP		РРТР	IPv6
Internet Acc	ess Mode			
Connection	Туре	Offline	~	
		Offline		
		PPP		
		TSPC		
		AICCU		
		DHCPv6 Client		
	OK	Static IPv6		
		6in4 Static Tunnel		
		6rd		

Different connection types will bring out different configuration page. Refer to the following:

• PPP – Dual Stack application, IPv4 and IPv6 services can be utilized at the same time

Choose PPP and type the information for PPPoE of IPv4.

WAN >> Internet Access

PPPoE Static or Dynamic IP	PPTP/L2TP IPv6
Enable     Disable       ISP Access Setup	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)
<pre>=&gt; , , , , , , , , , , , , , , , , , ,</pre>	Fixed IP Address  Default MAC Address  Specify a MAC Address MAC Address: 00 ·1D ·AA :A8 ·B7 ·6A

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

PPPoE	Static or Dynamic IP	l i i i i i i i i i i i i i i i i i i i	PPTP/L2TP	IPv6
Internet Ac	cess Mode			
Connectio	n Type	PPP	*	
Note : IPv4	WAN setting should be PPPoE clie	nt.		

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.

Physical Connectio	'n			Sy	stem Uptime: 0:1:11
	IPv4		IPv6		
LAN Status	Prim	ary DNS: 168.95	5,192,1	Secondary D	<b>IS:</b> 168.95.1.1
IP Address	TX Packets	RX Pac	kets		
192,168,1,1	0	3085			
WAN 1 Status					>> Dial PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	00:00:00	
IP	GW IP	<b>TX Packets</b>	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
		0	0	0	O
WAN 2 Status					>> Drop PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:54	
IP	GW IP	<b>TX Packets</b>	TX Rate(Bps)	<b>RX</b> Packets	RX Rate(Bps)
114.44.49.54	168.95.98.254	800	4761	821	6617
WAN 3 Status	1				
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	÷
IP	GW IP	<b>TX Packets</b>	TX Rate(Bps)	<b>RX Packets</b>	RX Rate(Bps)
-		0	0	0	0
ADSL Information	( ADSL Firmware	Version: 05-0	4-04-04-00-01)		
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RXC	RC errs
	0	0	0	0	
ADSL Status M	ode State	Up Speed	Down Speed	SNR Margin	Loop Att.
	READY	0	n	0	n

#### **Online Status**

Physical Connecti	ion			System Uptime: 0:2:32
	IPv4		IPv6	
LAN Status				the second second
IP Address				
2001:B010:73	00:201:21D:AAFF:F	EA6:2568/64 (Glo	pal)	
FE80::21D:AA	FF:FEA6:2568/64 (L	.ink)	and the second second	
TX Packets	<b>RX Packets</b>	TX Bytes	RX Bytes	
7	4	690	328	
WAN2 IPv6 Status	5			>> Drop PPP
Enable	Mode	Up Time		
Yes	PPP	0:02:08		
1P			Gateway IP	
2001:B010:73	00:201:21D:AAFF:F	EA6:256A/128 (Gl	obal) FE80::90:1A00:2	242:AD52
	F:FEA6:256A/128 (L	.ink)		
DNS IP				
2001:B000:16 2001:B000:16				
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
7	9	544	1126	

#### • TSPC – Tunnel application, both IPv6 hosts communicate through IPv4 network

Choose **TSPC** and type the information for TSPC service.

WAN >> Internet Access

**Note:** While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the TSPC information is obtained from <u>http://gogo6.com/</u> after applied for the service.)

PPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access Mode			
Connection Type	Т	SPC 🔽	
TSPC Configuration			
Username	cacahsu		
Password	•••••		
Confirm Password	•••••		
Tunnel Broker	broker.freenet6.ne	t	

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

Physical Connect	ion			System Uptime: 0:2:3
	IPv4		IPv6	
LAN Status				
IP Address			_	
	2:D00:21D:AAFF:FE		al	
	FF:FEA6:2568/64 (L		Barran Co.	
TX Packets	RX Packets	TX Bytes	RX Bytes	
88	121	15596	10249	
WAN2 IPv6 Status	3			
Enable	Mode	Up Time		
Yes	TSPC	0:01:40		
IP			Gateway IP	
2001:5C0:140	10(B):10B9/128 (Gld	(bal)		
FE80::722C:3		and to do one		
TX Packets	<b>RX Packets</b>	TX Bytes	RX Bytes	
127	89	9219	15866	

#### • AICCU – Tunnel application

WAN >> Internet Access

Choose AICCU and type the information for AICCU of IPv6.

**Note:** While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the AICCU information is obtained from <u>https://www.sixxs.net/main/</u> after applied for the service.)

PPPoE	Static or Dynamic IP		PPTP/L2TP	IPv6
Internet Access Mode				
Connection Type		AICCU	~	
AICCU Configuration				
🗌 Always On				_
Username	JCR3-SIXXS			
Password	••••			
Confirm Password	••••			
Tunnel Broker	tic.sixxs.net			
Subnet Prefix	2001:4DD0:FF00:8	3805::2	/ 64	

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

Online Status				
Physical Connect	ion			System Uptime: 0:1:18
	IPv4		IPv6	
LAN Status				
IP Address				
2001:4DD0:FF	00:83E4:21D:AAFF	:FEA6:2568/64 (Gl	obal)	
	FF:FEA6:2568/64 (L		Contain	
TX Packets	RX Packets	TX Bytes	RX Bytes	
147	187	34205	19176	
WAN2 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	AICCU	0:00:48		
IP			Gateway IP	
2001:4DD0:FF	00:3E4::2/64 (Glob	al)		
FE80::4CD0:F	F00:3E4:2/64 (Link)	)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
186	137	16438	33093	

#### • DHCPv6 Client

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

N 2 PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6
Internet Access	Mode		
Connection Typ	DHC DHC	Pv6 Client 💌	
DHCPv6 Client C	onfiguration		
Identity Asso	ciation O_Prefix Delegation	Non-temporary Address	
IAID (Identity	Association ID) 972573680	]	

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

Online Status				
Physical Connect	ion			System Uptime: 0:0:50
	IPv4		IPv6	
LAN Status IP Address				
FE80::21D:AA	FF:FEA6:2568/64 (Lii	nk)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
6	2	588	156	
WAN2 IPv6 Status	3			
Enable	Mode	Up Time		
Yes	DHCPv6 Client	0:00:40		
IP		1000	Gateway IP	
2001:B010:73	00:201:21D:AAFF:FE	EA6:256A/64 (Glol	bal)	
2001:1111:22	22:5555:21D:AAFF:F 22:3333::1111/128 FF:FEA6:256A/64 (Lii	(Global)	obal)	
DNS IP				
2001:4860:48 2001:4860:48				
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
14	5	1174	694	

Vigor2760 Series User's Guide

#### • Static IPv6

**Online Status** 

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

WAN 2	>> Inter	net Ac	cess

PPoE	Static or Dynamic IP		PPTP/L2TP	-	IPv6
Internet Access	s Mode		-		
Connection Ty	pe	Static IPv6	*		
Static IPv6 Add	ress configuration				
IPv6 Address	a subscription of the second	/ Pre	fix Length		
2001:B010:7300	D:201:21D:AAFF:FEA6:256A	/ 64	Add	Delete	
Current IPv6 A	ddress Table				-
Index IPv6	Address/Prefix Length		Scope		
	B010:7300:201:21D:AAFF:FE	A6:256A/64	Global		
2 2001:	1111:2222:5555:21D:AAFF:F	EA6:256A/64	Global		
3 FE80:	:21D:AAFF:FEA6:256A/64		Link		
Ctatic IDs & Cata	urar a ordinus ation				
IPv6 Gatewa	eway configuration				
IPVD Gatewa	Audress	_			
3					

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

Physical Connect	ion			System Uptime: 0:4:2
	IPv4		IPv6	
LAN Status IP Address				
FE80):21D(AA	FF:FEA6:2568/64 (L	.ink)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
4	0	312	0	
WAN2 IPv6 Statu:	\$			
Enable	Mode	Up Time		
Yes	Static IPv6	0:03:56		
IP			Gateway IP	
2001:B010:73	00:201:21D:AAFF:F	EA6:256A/64 (Glob	al)	
	:22:5555:21D:AAFF FF:FEA6:256A/64 (L		bal)	
TX Packets	<b>RX</b> Packets	TX Bytes	RX Bytes	
8	2	608	364	

#### • 6in4 Static Tunnel

Choose 6in4 Static Tunnel. Type remote endpoint IPv4 address, 6in4 IPv6 Address, LAN Routed Prefix and Tunnel TTL.

PPoE	Static or Dynamic I	Р	PPT	P/L2	TP		IPv6
Internet Access Mode Connection Type		6in4	Static Tunnel	~			
6in4 Static Tunnel Remote Endpoint IPv	/4 Address						
' 6in4 IPv6 Address				_/	64	(default:6	4)
LAN Routed Prefix				1	64	(default:6	4)
Tunnel TTL	255	(defau	lt:255)				

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

```
Online Status
```

Physical Connect	ion			System Uptime: 0day 0:4:16
IPv4			IPv6	
LAN Status				
IP Address				
2001:4DD0:FF	00:83E4:21D:AAF	E:FE83:11B4/64 (0	Global)	
	FF:FE83:11B4/64 (			
TX Packets	RX Packets	TX Bytes	RX Bytes	
14	80	1244	6815	
WAN1 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	6in4 Static Tunr	nel 0:04:07		
IP		and the first second second	Gateway IP	
	F10:83E4::2131/64	(Global)		
FE80::C0A8:6	51D/128 (Link)			
TX Packets	<b>RX Packets</b>	TX Bytes	RX Bytes	
3	26	211	2302	

#### • 6rd

Choose 6rd. Type IPv4 Border Relay, IPv4 Mask Length, 6rd Prefix and 6rd Prefix Length.

Static or Dynamic IP	PPTP/L2TP	IPv6
e		
61	• t	
Auto 6rd Stat	ic 6rd	
: 192.168.101.11		
192.168.101.11		
		le The second seco

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

#### **Online Status**

Physical Connect	ion			System Uptime: 0day 0:9:15
	IPv4		IPv6	
LAN Status				
IP Address				
2001:E41:A86	5:1000:21D:AAFE:	FF83:11B4/64 (Glo	bal)	
	FF:FE83:11B4/64 (		Solid	
TX Packets	RX Packets	TX Bytes	RX Bytes	
15	113	1354	18040	
WAN1 IPv6 Statu	5			
Enable	Mode	Up Time		
Yes	6rd	0:09:06		
IP	1.1.1.1.177.4		Gateway IP	
2001:E41:A86 (Global)	5:1D01:21D:AAFF:	FE83:11B5/128		
FE80::COA8:6	51D/128 (Link)		-	
TX Packets	<b>RX Packets</b>	TX Bytes	RX Bytes	
13	29	967	2620	

## **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 Viogr2760. Open LAN>> General Setup. Click the IPv6 button. Then, click LAN1 IPv6 Setup tab.

Note: Only the subnet of LAN 1 supports IPv6 feature.

	etup	LAN 1 IPv6		
<u>Router Adver</u> tisement Se	rver			
🖲 Enable 🛛 🔿 Disable	<i>2</i>			
Advertisement Lifetime [1	.800 Seconds (F	Range : 600	) - 9000)	
HCPv6 Server Configuration				
an a	)isable Server			-
Start IPv6 Address	2001:1111:2222:3	0.03000.005		_
End IPv6 Address	2001:1111:2222:3	3333::2222		
NS Server IPv6 Address	0001 1050 1050			
Primary DNS Server	2001:4860:4860::			
Secondary DNS Server	2001:4860:4860::	8844		
tatic IPv6 Address configur	ation			
IPv6 Address	adon	/ Pret	fix Length	
		ΠÍΓ	Add	Delete
Current IPv6 Address Table	6)			
Index IPv6 Address/Pre	그 같은 것은 것을 가지 않는 것이 같은 것을 했다.		Scope	~
1 FE80::21D:AAFF:1	EA6:2568/64		Link	

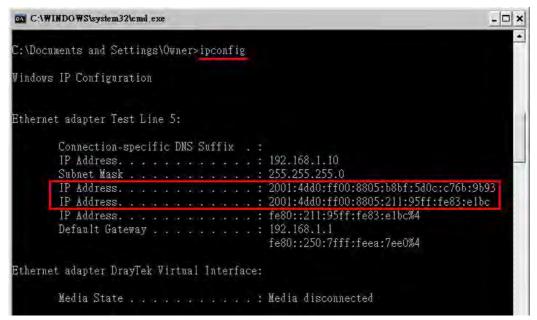
- 2. In the field of **Router Advertisement Server**, the default setting is **Enable**. The client's PC will ask router advertisement service for the Prefix of IPv6 address automatically, and generate an Interface ID by itself to compose a full and unique IPv6 address.
- 3. In the field of **HCPv6 Server Configuration**, when DHCPv6 service is enabled, you can assign available IPv6 address for the client manually.

**Note:** When both mechanisms are enabled, the client can determine which mechanism to be used (e.g., the default mechanism for Windows7 is Router Advertisement Server ).



## III. Confirming IPv6 Service Run Successfully

1. Make sure you have get the correct IPv6 IP address. Get into MS-DOS interface and type the command of "ipconfig". Refer to the following figure.



From the above figure we can see IPv6 IP address has been captured by the system.

2. Use the Ping command to ping any IPv6 address indicating an IPv6 website. For example, <u>www.kame.net</u> is a website supporting IPv4 IP and IPv6 IP services. Its IPv6 address is seen with a format of 2001:200:dff:fff1:216:3eff:feb1:44d7.

C:\WINDOWS\system32\cmd.exe	- 🗆 ×
C:\Documents and Settings\Owner>ping 2001:200:dff:fff1:216:3eff:feb1:44d7	<u>*</u>
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	1
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., <u>www.kame.net</u>. If your computer accesses into the website by using IPv6 address, you may see a turtle dancing on the screen. If not, only a steady turtle will be seen.



If you can see a turtle dancing on the screen, that means IPv6 service is ready for you to access and utilize.



# 4.2 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through FTP server.

You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

JSB Applicatio	on >> USB Disk Status		
USB Mass Stor	rage Device Status	_	
Connection 9	Status Disk Connecte	ed	Disconnect USB Disk
Write Protec	t Status: No		
Disk Capacity	y: 2009 MB		
USB Disk Use	rs Connected		Refresh
Index	Service	IP Address(Port)	Username

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

2. Setup a user account for the FTP service by using USB Application >>USB User Management. Click Enable to enable FTP account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

FTP	💿 Enable	O Disable
Username	user1	
Password		(Maximum 11 Characters)
Confirm Password		
Home Folder		<b>2</b>
Access Rule		
File	🗹 Read	Write Delete
Directory	🗹 List	Create Remove
The folder name can only c	ontain the following	characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( )
and space.		

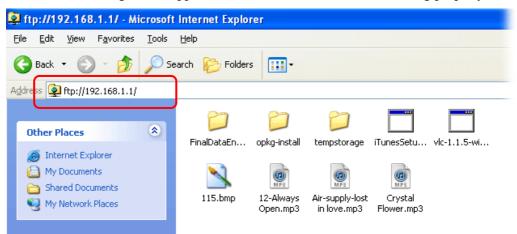
3. Click **OK** to save the configuration.

USB Application >> USB User Management

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

Log On	As 🔀
?	Either the server does not allow anonymous logins or the e-mail address was not accepted.
	FTP server: 192.168.1.1
	User name: user1
	Password:
	After you log on, you can add this server to your Favorites and return to it easily.
A	FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.
	Learn more about using Web Folders.
	Log on anonymously
	Log On Cancel

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



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

USB Application >> USB Disk Status

USB Mass Sto	orage Device Stat	tus			
Connection Status: Disk Connected Disconnect USB Disk					
Write Protect Status: No					
Disk Capaci	ty: 2009 MB				
USB Disk Us	ers Connected			Refresh	
Index	Service	IP Address(Port)	Username		
1.	FTP	192.168.1.10(1963)	user1	Drop	

Now, users in LAN of Vigor2710 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application** >>**USB User Management.** 



# 4.3 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. The following settings are for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

VPN and Remote Access >> LAN to LAN

_AN-to-LA	N Profiles:					Set to	Factory Default
Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	???			<u>17.</u>	???		
<u>2.</u>	???			<u>18.</u>	???		
<u>3.</u>	???			<u>19.</u>	???		
<u>4.</u>	777			<u>20.</u>	???		
<u>5.</u>	777			<u>21.</u>	???		

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Server*), and check the box of **Enable This Profile**. For Vigor router will be set as a **server**, the call direction shall be set as **Dial-in** and set 0 as **Idle Timeout**.

Profile Index : 1 1. Common Settings		
Profile Name VPN Server		Call Direction O Both O Dial-Out O Dial-in
VPN Dial-Out Through WAN1 First Netbios Naming Packet ③Pass 〇 Block	*	Idle Timeout 0 second(s) Enable PING to keep alive PING to the IP
Multicast via VPN  Pass O Block (for some IGMP,IP-Camera,DHCP Relayetc.)		PING to the IP
2. Dial-Out Settings		

**Dray** Tek

0

4. Now navigate to the next section, **Dial-In Settings** to check PPTP, IPsec Tunnel and L2TP boxes. Check the box of **Specify Remote...** and type the **Peer VPN Server IP** (e.g., 218.242.130.19 in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

3. Dial-In Settings	
Allowed Dial-In Type	Username ???
✓ РРТР	Password
✓ IPsec Tunnel	VJ Compression On Off
🗹 L2TP with IPsec Policy None 🛛 👻	
	IKE Authentication Method
Specify Remote VPN Gateway	✓ Pre-Shared Key
Peer VPN Server IP	IKE Pre-Shared Key
218.242.130.19	✓ Digital Signature(X.509)
or Peer ID	None 🛩
	Local ID
	<ul> <li>Alternative Subject Name First</li> </ul>
	🔿 Subject Name First
	IPsec Security Method
	Medium(AH)
	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
4. Gre over IPsec Settings	

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

My WAN IP	0.0.0.0	RIP Direction Disable
Remote Gateway IP	0.0.0	From first subnet to remote network, you have to do
Remote Network IP	192.168.1.0	Route 🛩
Remote Network Mask	255.255.255.0	
Local Network IP	192.168.1.9	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	
	More	

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

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

Dial-out Tool					Refresh Seconds : 5 🗙 Refre				5 🔽 Refresh	
		( V2920 )	172.16.2	2.145		✓ Di	al			
/PN Connecti	on Status									
Current Page	: 1							Pag	je No.	Go >
VPN	Туре	Remote IP	Virtua	I Network	Tx Pkts	Tx R (Bp		Rx Pkts	Rx Ra (Bps	Unlime
1 (VPN Server)	IPSec Tunnel DES-SHA1 Auth	218.242.1	30.19	192.168.1.0	0/24	353	3	291	з	0:13:58 Drop
					XX	XXXXXX	: Da	ita is e	norypti	ed.

VPN and Remote Access >> Connection Management

#### Configuration on Vigor Router for Branch Office

- 1. Log into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>LAN to LAN** to create a LAN-to-LAN profile. The following settings are for a permanent VPN connection.

VPN and Remote Access >> LAN to LAN

VPN and Remote Access >> LAN to LAN

LAN-to-LA	N Profiles:					Set to	Factory Default
Index	Name	Active	Status	Index	Name	Active	Status
<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>	???		

3. Click any index number to open the configuration page. Type a name which is easy for identification for such profile (in this case, type *VPN Client*), and check the box of **Enable This Profile**. For such Vigor router will be set as a **client**, the call direction shall be set as **Dial-out**. Check the box of **Always on** for a permanent VPN connection.

Profile Index : 1 1. Common Settings	
Profile Name VPN Client	Call Direction 🛛 Both 💿 Dial-Out 🔿 Dial-in
☑ Enable this profile	Always on
	Idle Timeout -1 second(s)
VPN Dial-Out Through WAN1 First	Enable PING to keep alive
Netbios Naming Packet ③ Pass 〇 Block	PING to the IP
Multicast via VPN  Image: Pass O Block	
(for some IGMP, IP-Camera, DHCP Relayetc.)	
2. Dial-Out Settings	

**Dray** Tek

0

4. Now navigate to the next section, **Dial-Out Settings** to select the **IPsec Tunnel** service and type the remote server IP/host name (e.g., 218.242.133.91, in this case). Press the **IKE Pre-Shared Key** button to set the **PSK**; and select **Medium (AH)** or **High (ESP)** as the security method.

2. Dial-Out Settings	
Type of Server I am calling	Username ???
О РРТР	Password
<ul> <li>IPsec Tunnel</li> </ul>	PPP Authentication PAP/CHAP
O L2TP with IPsec Policy None	VJ Compression On
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 218.242.133.91	IKE Authentication Method <ul> <li>Pre-Shared Key</li> <li>IKE Pre-Shared Key</li> </ul>
	O Digital Signature(X.509)
	Peer ID None 🗸
	Local ID
	Iternative Subject Name First
	🔿 Subject Name First
	IPsec Security Method
	O Medium(AH)
	High(ESP) 3DES with Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:

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

Enable IPsec Dial-Ou	t function GRE over IPsed	<u> </u>
Logical Traffic	My GRE IP	Peer GRE IP
5. TCP/IP Network Setting	IS	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	172.17.1.0	Route 💙
Remote Network Mask	255.255.255.0	
Local Network IP	192.168.1.9	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	single ward supports this y
	More	

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

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

Dial-out Tool				Refresh Seconds : 5 💌 Re				<ul> <li>Refresh</li> </ul>	
		( V2920 ) 17	72.16.2.1	45	•	<ul> <li>Dial</li> </ul>			
PN Connecti	on Status								
urrent Page	: 1						Pag	je No.	G0 >:
					_				
VPN	Туре	Remote IP	Virtual	Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rat (Bps)	Unlime

VPN and Remote Access >> Connection Management

# 4.4 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

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
lass Ru	ule									
Ind	ex		Name				<u> </u>	Rule	Service T	ype

Class 1 Class 2 Class 3 Edit Edit Edit	Index	Name	Rule	Service Type
	Class 1		<u>Edit</u>	
Class 3 Edit	Class 2		Edit	<u>Edit</u>
	Class 3		<u>Edit</u>	

OK

#### ☑ Enable the First Priority for VoIP SIP/RTP:

SIP UDP Port: 5060 (Default: 5060)



3. In the following page, type a name (e.g., VoIP) for such class and click Add. Bandwidth Management >> Quality of Service

			packets as: Defau	
Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
Empty	-	-	-	-
		Empty -	Empty	Empty CodePoint

 Check the box of ACT. Click Edit to specify the local address. Bandwidth Management >> Quality of Service

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	
Service Type	Predefined	
Note: Please choose/se	tup the <u>Service Type</u> first.	

5. In the pop-up window, choose **Range Address** as the **Address Type** and type the start IP address and end IP address in relational fields. Click **OK** to save the settings and exit the window.

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

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

Bandwidth Management >> Quality of Service

Rule Edit		
	ACT	
	Ethernet Type	● IPv4 ○ IPv6
	Local Address	172.16.1.240~172.16.1.241
	Remote Address	Any Edit
	DiffServ CodePoint	ANY
	Service Type	Predefined
	Note: Please choose/setup th	e <u>Service Type</u> first.
	ſ	OK Cancel

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

Bandwidth Management >> Quality of Service

Class Index #1 Jame VolP								
NO Status Local Address Remote Address CodePoint Service Type								
1 ()	Active	172.16.1.240 ~ 172.16.1.241	Any	ANY	ANY			
Add Edit Delete								
			OK Cancel					

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

Name IPTV 🗌 Tag packets as: Default								
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1 ()	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY			
		A	Add Edit Delete					
		Г	OK Cancel	ן				

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

DiffServ		ets as: Default				ata/Email	ss Inde	
	vice Type	ffServ		Re	Local Address			
	ANY						1 ()	
Add Edit Delete								

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 Status	Bandwidth	Direction	Class	Class	Class	Othors	UDP Bandwidth	<u>o Factory (</u> Online	
muex	ətatus	Banuwiuth	Direction	1	2	3	others	Control	Statistic	5
WAN1	Enable	Kbps/Kbps	Outbound	30%	50%	15%	5%	Active	<u>Status</u>	<u>Setup</u>
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

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

 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.

WAN1 General Setup		
Enable the QoS	Control OUT 💌	
Index	Class Name	Reserved_bandwidth Ratio
Class 1	VoIP	30 %
Class 2	IPTV	50 %
Class 3	Data/Email	15 %
	Others	5 %
Enable UDP Band	dwidth Control	Limited_bandwidth Ratio 25 %
Outbound TCP A	CK Prioritize	
	OK Clear	Cancel

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

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

General Setup								<u>Set t</u>	o Factory D	efault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	30%	50%	15%	5%	Active	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

Class Rule			
Index	Name	Rule	Service Type
Class 1	E-mail	Edit	
Class 2	HTTPS	<u>Edit</u>	<u>Edit</u>
Class 3		<u>Edit</u>	

# 4.5 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or V PN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

#### 1. Go to **Bandwidth Management>>Quality of Service.**

Bandwidth Management >> Quality of Service

General	Setup								o Factory De	efault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	Kbps/Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

#### Class Rule

Index	Name	Rule	Service Type
Class 1		<u>Edit</u>	
Class 2		<u>Edit</u>	<u>Edit</u>
Class 3		<u>Edit</u>	

Enable the First Priority for VoIP SIP/RTP:	
SIP UDP Port: 5060 (Default: 5060)	
	ОК

2. Click **Setup** link of WAN(1/2/3). Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.

Bandwidth Management >> Quality of Service

#### WAN2 General Setup

<b>~</b>	Enable the QoS Control	BOTH 🔽	
	WAN Inboun	IN OUT	jth
	WAN Outbou	BOTH	vidth

3. Set Inbound/Outbound bandwidth.

Bandwidth	Management >>	Quality	of Service
-----------	---------------	---------	------------

WAN2 General Setup								
	VAN Inbound Bandwidth VAN Outbound Bandwidth	100000 Кbps 100000 Кbps						
Index Class 1	Class Name VoIP	Reserved_bandwidth Ratio						



**Note:** The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

4. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1. Click **OK** to save the settings.

Class II	ndex	#1					
Name E-mail		🗌 Tag packets as: Default 🛛 💌					
NC	)	Status	Local Addres	s	Remote Address	DiffServ CodePoint	Service Type
1 (	)	Active	Any		Any	ANY	ANY
	Add Edit Delete						
OK Cancel							

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

5. Click the **Setup** link for WAN2. The user can set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP. Click **OK** to save the settings.

Enable the QoS Control BOTH								
WAN In	bound Bandwidth	100000 Kbps						
WAN OU	Itbound Bandwidth	100000 Kbps						
Index	Class Name	Reserved_bandwidth_Ratio						
Class 1	E-mail	25 %						
Class 2		25 %						
Class 3		25 %						
	Others	25 %						
Enable UDP Bandwid	ith Control	Limited_bandwidth Ratio 25						
Outbound TCP ACK	Prioritize							

6. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth for **HTTPS**. And click **OK**.

Class Index Name H	<b>x #2</b> TTPS		🗆 Та	ag packets as: Defau	ılt 💌	
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1	Active	172.16.1.242 ~ 172.16.1.249	Any	ANY	ANY	
Add Edit Delete						
OK Cancel						

#### 7. Click **Setup** link for WAN2.

Bandwidth Management >> Quality of Service

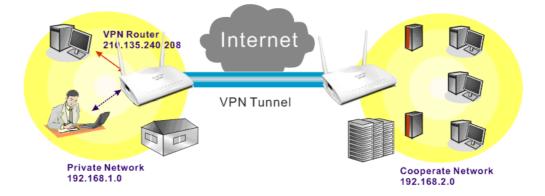
Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Both	25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
								_	<b>F</b> .14	
Class	51		E-mail					<u>Edit</u>		
Class			HTTPS					<u>Edit</u>	<u>Edit</u>	
Class	53							<u>Edit</u>		
		First Priority for VolP SIP/R ort: 5060 (Default: 506)								

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

Enable the QoS Co	ntrol BOTH 🛩			
WAN I	nbound Bandwidth	100000 Kbps		
WAN C	outbound Bandwidth	100000 Kbps		
Index	Class Name	Reserved_bandwidth Ratio		
Class 1	E-mail	25 %		
Class 2	HTTPS	25 %		
Class 3		25 %		
	Others	25 %		
Enable UDP Bandw		Limited_bandwidth Ratio 25 9		

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the



Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.

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

Bandwidth Management >> Quality of Service

Class In	dex #3				
Name	VPN		🗌 Ta	ag packets as: Defa	ult 💌
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
		7	Add Edit Delet	e	
		ſ	OK Cancel		

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

Bandwidth Management >> Quality of Service

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	
Service Type	Predefined	
Note: Please choose/setup t	he <u>Service Type</u> first.	

12. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	192.168.1.0	Edit
Remote Address	192.168.2.0	Edit
DiffServ CodePoint	ANY	
Service Type	Predefined	
Note: Please choose/set	up the <u>Service Type</u> first.	

Bandwidth Management >> Quality of Service

# 4.6 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.

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

Object Settings >> SMS / Mail Service Object

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.

rofile Name	Local number
Service Provider	kotsms.com.tw (TW)
Isername	abc5026
assword	•••
uota	3
ending Interval	3 (seconds)

Object Settings >> SMS / Mail Service Object

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

SMS Provider	Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider
<u>1.</u>	Local number	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	

Object Settings >> SMS / Mail Service Object

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

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

Object Settings >> Notification Object

6. 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

rofile Name	WAN_Notify	
Category		Status
WAN	Disconnected	Reconnected
VPN Tunnel	Disconnected	Reconnected

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

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

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).

Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - Local number 💌	0912345678	1 - WAN_Notify 💙	
2	1 - Local number 👻		1 - WAN_Notify 💙	
3 🗌	1 - Local number 👻		1 - WAN_Notify 💙	
4	1 - Local number 😪		1 - WAN_Notify 💙	
5 🗌	1 - Local number 😪		1 - WAN_Notify 💙	
6	1 - Local number 👻		1 - WAN_Notify 🗸	
7 🗌	1 - Local number 👻		1 - WAN_Notify 🗸	
8	1 - Local number 👻		1 - WAN_Notify 🗸	
9 🔲	1 - Local number 👻		1 - WAN_Notify 💙	
10 🗌	1 - Local number \vee		1 - WAN_Notify 🛩	

Application >> SMS / Mail Alert Service

9. 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.

Profile Name	Custom 1		
Service Provider	clickatell		
			~
eg:bulksms.vsms.net:5567,		/2.0?username=###txtUser###	~
eg:bulksms.vsms.net:5567,		/2.0?username=###txtUser###	~
eg:bulksms.vsms.net:5567, &password=###txtPwd##	/eapi/submission/send_sms/2, #&msisdn=###txtDest###&r	/2.0?username=###txtUser###	×
eg:bulksms.vsms.net:5567, &password=###txtPwd## Username	/eapi/submission/send_sms/2, #&msisdn=###txtDest###&r ilan123	/2.0?username=###txtUser###	×

Object Settings >> SMS / Mail Service Object

# 4.7 How to Create an Account for MyVigor

The website of MyVigor (a server located on <u>http://myvigor.draytek.com</u>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

# 4.7.1 Create an Account via Vigor Router

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

Web-Filter License [Status:Not Activated]			Acti	vat
Setup Query Server	auto-selected		Find more	
Setup Test Server	auto-selected		Find more	
Web Content Filter Profil	le Table:		Set to Factory Defa	<u>ult</u>
Profile	Name	Profile	Name	
<u>1.</u>	Default	<u>5.</u>		
<u>2.</u>		<u>6.</u>		
<u>3.</u>		<u>7.</u>		
<u>4.</u>		<u>8.</u>		
that is categor: Filter.Please co:	ized with %CL% <br: ntact your system a</br: 	whas been blocked by administrator for fur		
 br>that is categor. Filter.Please co; information.	ized with %CL% htact your system a r>	has been blocked by	rom %SIP% to %URL% %RNAME% Web Content ther	
<pre> that is categor. Filter.Please component information.</pre> /cente:	ized with %CL% ntact your system a r>	OK OK OK	rom %SIP% to %URL% %RNAME% Web Content ther	
<pre>    Filter.Please components of the second second</pre>	ized with %CL% ntact your system a r>	OK OK OK	From \$SIP\$ to \$URL\$ \$RNAME\$ Web Content ther owing page.	d
 br>that is categor. Filter.Please co; information.	ized with %CL% ntact your system a r> enance>>Activat	OK OK	From \$SIP% to %URL% %RNAME% Web Content ther owing page.	d

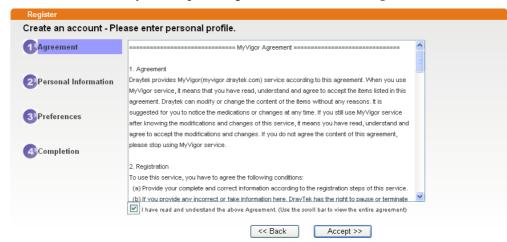


2. Click the Activate link. A login page for MyVigor web site will pop up automatically.

	Please take a moment to register. Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!
LOGIN	
UserName :	
Password :	
Auth Code :	t xxhdd
	If you cannot read the word, <u>click here</u>
	Forgotten password? Login
Don't have a M	yVigor Account ? Create an account now
L	

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

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



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

	Account Informati	ion	
Agreement	UserName:*	Mary Check Account	
		(3 ~ 20 oharaoters)	
Damand	Password:*	••••	
Personal		(4 ~ 20 characters : Do not set the same as the username.)	
intormation	Confirm Password:*	••••	
	Personal Informat	tion	
Preferences	First Name:"	Mary	
	Last Name:*	Ted	
Completion	Company Name:	Tech Ltd.	
	Email Address:*	mary ted@tech.com	
		Please note that a valid E-mail address is required to receive the Subscription Code." need this code to activate your account.	You will
	Tel:	0	
	Country:*	SWITZERLAND	
	Career.*	Supervisor	

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

Register		
Create an account -	Please enter personal profile.	
	How did you find out about this website?	Internet
	What kind of anti-virus do you use?	AntiVir 🗸
2 Personal Information	l 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	Global Server 👻
3 Preferences	verification mail.	
Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

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

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site GO
Register Confirm	
	Thank for your register in VigorPro Web Site The Register process is completed
	Close Login

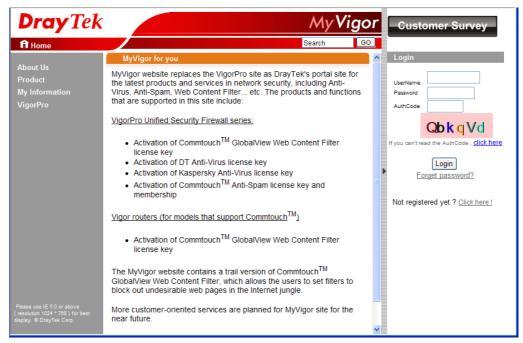
10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

	Please take a moment to register. Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!
LOGIN	
UserName :	Mary
Password :	••••
Auth Code :	T4he1C
	If you cannot read the word, <u>click here</u>
	Forgotten password? Login
Don't have a l	MyVigor Account ? Create an account now
lf you a	re having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

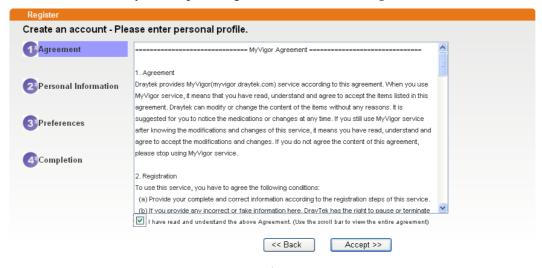
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

### 4.7.2 Create an Account via MyVigor Web Site

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



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



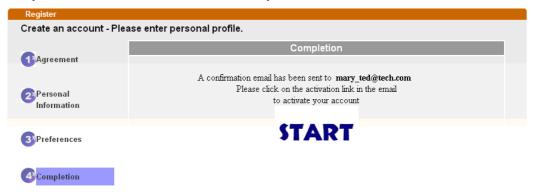
3. Type your personal information in this page and then click Continue.

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
	Password:*	(3 ~ 20 characters)
Personal	Password.	(4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	
	Personal Informat	tion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SVMTZERLAND 🗸
	Career:*	Supervisor

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

Register		
Create an account	- Please enter personal profile.	
	How did you find out about this website?	Internet
Agreement	What kind of anti-virus do you use?	AntiVir
2 Personal	l would like to subscribe to the MyVigor e-letter.	
Information	l would like to receive DrayTek product news.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
Completion		<< Back Continue >>

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



6. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

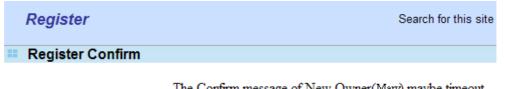
***** This is an automated message from myvigor draytek.com.*****

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



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

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

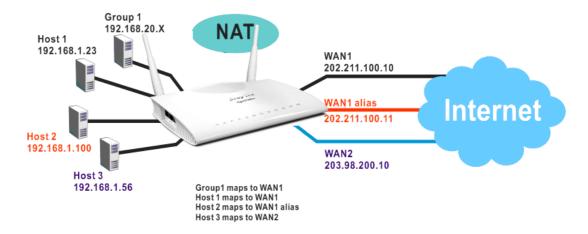
	Please take a moment to register. Membership Registration entitles you to upgrade firm for your purchased product and receive news about upcoming products and services!	ware
LOGIN		
UserName :	Mary	
Password :	••••	
Auth Code :	T4he1C	
	If you cannot read the word, <u>click here</u>	
	Forgotten password? Login	
Don't have a N	MyVigor Account ? Create an account now	_
L		

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

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

# 4.8 How to Setup Address Mapping

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



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

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11 WAN2: 203.98.200.10

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

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host 1 to always map to 202.211.100.10 (WAN1); Host 2 to always map to 202.211.100.11 (WAN1 alias); Host 3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

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

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

- 1. Log into the web user interface of Vigor2760.
- 2. Open WAN>>Internet Access. For WAN1, choose MPoA/Static or Dynamic IP as the Access Mode.

WAN >> Internet Access

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

Note : Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

3. Click the **Details Page** of WAN 1 to open the following page. From the above figure, set main WAN IP address as 202.211.100.10.

WAN 1 PPPoE / PPPoF	MPoA / Static or	Dynamic IP	IPv6
🛞 Enable 🔇	) Disable	WAN IP Network Settings	WAN IP Alias
Modem Settings (for Multi-PVC channel Encapsulation VPI VCI Modulation		Obtain an IP address a Router Name Domain Name * : Required for some DHCP Client Identifier for s Enable Username Password	Vigor *
WAN Connection De Mode Ping IP TTL:	ARP Detect	Specify an IP address IP Address Subnet Mask Gateway IP Address	202.211.100.10 255.255.255.0
MTU RIP Protocol	1492 (Max:1500)	<ul> <li>Default MAC Address</li> <li>Specify a MAC Address</li> <li>MAC Address: 00 -11</li> </ul>	855

Click the **WAN IP Alias** button to configure the other P address which is 202.211.100.11. Make sure **Join IP NAT Pool** is not checked. Click **OK** to save the settings.

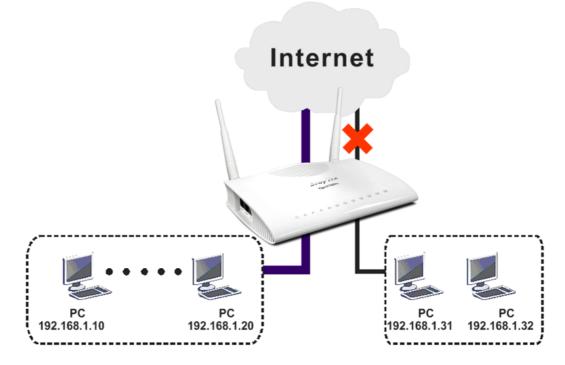
#### WAN1 IP Alias ( Multi-NAT )

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.		202.211.100.10	$\checkmark$
2.		202.211.100.11	
З.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
	(	OK Clear All	Close

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

# 4.9 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 Setu	ID.		Set to	Factory Default
Set	Comments	Set	Comments	
_1_	Default Call Filter	<u>7.</u>		
<u>2.</u>	Default Data Filter	<u>8.</u>		
		<u>9.</u>		
4		<u>10.</u>		
5		<u>11.</u>		
<u>6</u> .		<u>12.</u>		
Firewa > Filter S t Comment				
Filte	Rule Active	Comments	Move Up	Move Down
		xNetBios -> DNS		<u>Down</u>
2			UP	<u>Down</u>
3			UP	<u>Down</u>
4			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**.

🗹 Check to enable the Filter Rul	9	
Comments:	block_all	
ndex(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule DN:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care 🐱	
Application	Action/Profile	Syslog
Filter:	Block If No Further Match 🔽	

**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.

Firewall >> Edit Filter Set >> Edit Filter Rule

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**.

ar Sat 2 Rula 3	_	
🗹 Check to enable the Filter Ru	le	
Comments:	open_ip	
Index(1-15) in <u>Schedule</u> Setup:		
Clear sessions when schedule ON:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	Any	Edit
Fragments:	Don't Care 🛛 👻	
Application	Action/Profile	Syslog
Filter:	Block Immediately 🛛 👻	
Branch to Other Filter Set:	None 💀	

6. A dialog box will be popped up. Choose **Range Address** as **Address Type** by using the drop down list. Type 192.168.1.10 in the field of **Start IP**, and type 192.168.1.20 in the field of **End IP**. Then, click **OK** to save the settings. The computers within the range can access into the Internet.

Address Type	Range Address 🛛 👻
Start IP Address	192.168.1.10
End IP Address	192.168.1.20
Subnet Mask	0.0.0.0
Invert Selection	
IP Group	None 🔽
or <u>IP Object</u>	None 🔽
or IP Object	None 🐱
or IP Object	None 🔽
IPv6 Group	None 🐱
or <u>IPv6 Object</u>	None 🔽
or IPv6 Object	None 🔽
or IPv6 Object	None 🗸

7. Now, check the content of **Source IP** is correct or not. The action for **Filter** shall be set with **Pass Immediately.** Then, click **OK** to save the settings.

Firewall >	> Edit	Filter	Set >>	Edit	Filter	Rule
		THUCK I	300	L'une	i neoi	1 Marc

er Set 2 Rule 3					
Check to enable the Filter Ru Comments:	lle open_ip				
Index(1-15) in <u>Schedule</u> Setup: Clear sessions when schedule ON:	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, _,				
Direction:	LAN/RT/VPN -> WAN				
Source IP:	192.168.1.10~192.168.1.20	Edit			
Destination IP:	Any	Edit			
Service Type:	Any	Edit			
Fragments:	Don't Care 🔽				
Application	Action/Profile	Syslog			
Filter:	Pass Immediately 🔽				
Branch to Other Filter Set:	None 😒				

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

Firewall >> Filter Setup >> Edit Filter Set	
---------------------------------------------	--

Filter Set 2				
Comments :	Default Data Filter			
Filter Rule	e Active	Comments	Move Up	Move Down
1		xNetBios -> DNS		<u>Down</u>
2		block_all	<u>UP</u>	<u>Down</u>
3		open_ip	<u>UP</u>	<u>Down</u>
4			<u>UP</u>	<u>Down</u>
5			UP	<u>Down</u>
6			<u>UP</u>	<u>Down</u>
7			<u>UP</u>	
			Next Filter Se	et None 🔽
		OK Clear	Cancel	

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

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

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

#### Web Content Filter,

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

Note: License is required.

#### **URL Content Filter,**

Benefits: Free, flexible for customize webpage.

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

# I. Via Web Content Filter

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

<b>/eb-Filter License</b> Status: Commtou		:2012-12-31 Expire	Date:2013-01-		<u>tivat</u> :
Setup Query Serve	ər	auto-selected		Find more	
Setup Test Server		auto-selected		Find more	
/eb Content Filter	Profile Table:			Set to Factory Def	ault
Profile	Na	me	Profile	Name	
<u>1.</u>	Det	ault	<u>5.</u>		
<u>2.</u>			<u>6.</u>		
<u>3.</u>			<u>7.</u>		
<u>4.</u>			<u>8.</u>		
br>that is cat	br> <	The requested th %CL% has b our system admini	een blocked	Cache : L1 + L2 Cac > from %SIP% to %URL% by %RNAME% Web Content further	he 💙

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

Off   R6  Dashboard Wizards		Business Select All Clear All	Business	Job Search	Uweb-based Mail
Online Status WAN LAN NAT Firewall		Chating Select All Clear All	Chat	□ Instant Messaging	
Objects Setting CSM APP Enforcement Profile URL Content Filter Profile Web Content Filter Profile DNS Filter APPE Support List	Ξ	Computer-Internet Select All Clear All	Anonymizers Download Sites Search Engine,Portals Malware Illegal Software	Forums & Newsgroups     Streaming, Downloads     Social Networking     Botnets     Information Security	Computers Phishing & Fraud Spam Sites Hacking Peer-to-Peer
Bandwidth Management Applications VPN and Remote Access Certificate Management Wireless LAN USB Application System Maintenance Diagnostics		Other Select All Clear All	Adv & Pop-Ups Compromised Finance News Politics Restaurants & Dining General	Arts Dating & Personals Government Non-profits & NGOs Real Estate Shopping Cults	Transportation Education Health & Medicine Personal Sites Religion Translators Greeting cards
Support Area Product Registration All Rights Reserved.	~		☐ General ☐ Image Sharing ☐ Private IP Addresses	Network Errors	Parked Domains

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

Off <b>IR6</b> Dashboard Nizards	General Setup				
Online Status	General Setup	Default Rule			
NAN AN NAT Firewall General Setup	Actions for defa Application	ult rule:	Action/Profile	Syslog	
Filter Setup DoS Defense	Filter		Pass 💌		
bjects Setting SM	Sessions Contro	ı	0 / 32000		
andwidth Management	Quality of Servi	ce	None 💌		
pplications PN and Remote Access	APP Enforceme	nt	None 💌		
ertificate Management /ireless LAN	URL Content Fil	ter	None 💌		
SB Application System Maintenance	Web Content Fi	<u>ter</u>	1-Default		
liagnostics	Advance Settir	ıg	Edit		
upport Area roduct Registration					
All Rights Reserved.					

4. Next time when someone accesses facebook via this router, the web page would be blocked and the following message would be displayed instead.

The requested Web page from 192.168.2.114 to www.facebook.com/ that is categorized with [Social Networking] has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by DrayTek]



# **II. Via URL Content Filter**

Objects Setting >> Keyword Object Setup

#### A. Block the web page containing the word of "Facebook"

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

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

CSM >> URL Content Filter Profile

Profile Name:	Facebook	
Priority:	Either : URL Access Control	First 🕶 Log: None 💌
1.URL Access	Control	
🗹 Enab	le URL Access Control	Prevent web access from IP address
Actio	on:	Group/Object Selections
Block	Y Facebook	Edit
2.Web Featur	e	
🗌 Enat	le Restrict Web Feature	
Actio	in:	
Pass	🖌 🗌 Cookie 🔲 Proxy	🗌 Upload <u>File Extension Profile:</u> None 🛛 👻

5. When you finished the above steps, click **OK**. Then, open **Firewall>>General Setup**.

6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of **URL Content Filter**. Now, users cannot open any web page with the word "facebook" inside.

hboard	General Setup			
ards ine Status				
	General Setup	Default Rule		
N				
	Actions for defa	ult rule:		
wall neral Setup	Application		Action/Profile	Syslog
er Setup	Filter		Pass 💌	
S Defense ects Setting	Sessions Contro		0 / 32000	
dwidth Management lications	Quality of Serv	ice	None 🎽	
and Remote Access	APP Enforceme	ent	None 💌	
ificate Management eless LAN	URL Content Fi	lter	1-Facebook 😽	
Application	web Content F	liter		
em Maintenance nostics				
Juosucs	Advance Setti	na	Edit	
		.9		

#### 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.

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

Objects Setting >> Keyword Object Setup

```
Dray Tek
```

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

Firewall >> General Setup

Profile Index: 2	
Profile Name:	face.apps
Priority:	Either : URL Access Control First 👻 Log: None 💌
1.URL Acces	s Control
🗹 Ena	ble URL Access Control
Acti	on: Group/Object Selections
Bloc	k 💌 facebook
2.Web Featu	re
Ena	ble Restrict Web Feature
Acti	on:
	🛛 🔍 🗌 Cookie 🔲 Proxy 📄 Upload <u>File Extension Profile:</u> None 👻
Pass	

- 5. When you finished the above steps, please open **Firewall>>General Setup**.
- 6. Click the **Default Rule** tab. Choose the profile just configured from the drop down list in the field of URL Content Filter. Now, users cannot open any web page with the word "facebook" inside.

al Setup				
General Setup	Default Rule			
Actions for defa	ault rule:			
Application		Action/Profile	Syslog	
Filter		Pass 😽		
Sessions Contro	ol	0 / 60000		
Quality of Serv	ice	None 😽		
APP Enforceme	ent	None 💌		
URL Content Fi	lter	2-face.apps 😽		
Web Content F	<u>ilter</u>	None 😽		
Advance Setti	ng	Edit		

Vigor2760 Series User's Guide

# **5** Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

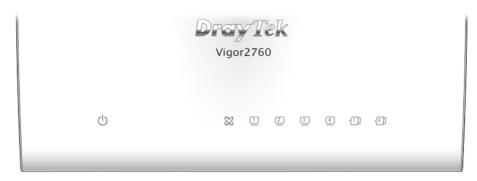
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

# 5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**1.3 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to "1.3 Hardware Installation" to execute the hardware installation again. And then, try again.

# **5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not**

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

#### **For Windows**



The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

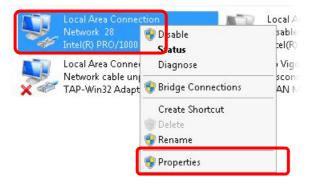
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



2. In the following window, click Change adapter settings.



3. Icons of network connection will be shown on the window. Right-click on Local Area Connection and click on Properties.



4. Select Internet Protocol Version 4 (TCP/IP) and then click Properties.

Local Area Connect	ion Properties	
Networking Sharing		
Connect using:		
11 Intel(R) PRO/11	000 MT Network Conne	ection
· • • •		Configure
This connection uses	the following items:	
🗹 📑 Client for Mic		
Privacyware		
🗹 📙 QoS Packet		
	er Sharing for Microsoft	
	col Version 6 (TCP/IP)	
	ocol Version 4 (TCP/IP)	
	opology Discovery Map	
Link-Layer T	opology Discovery Res	ponder
Install	Uninstall	Properties
- Description		

5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.

ou can get IP settings assigned au is capability. Otherwise, you need r the appropriate IP settings.					
Obtain an IP address automati	ically	ן			
Use the following IP address:-		•			
IP address:		1	ġ.	i.	
Subnet mask:			2		
Default gateway:					
Obtain DNS server address au	tomatio	ally			
O Use the following DNS server a	address	ses:			
Preferred DNS server:		8	÷.	Ξ.	
Alternate DNS server:	Γ	2	1		
🗖 Validate settings upon exit				٨d٧	anced

# For Mac OS

- 1. Double click on the current used Mac OS on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

) 🖯 🖯			Netw	vork		
ihow All	Displays Sou	nd Network	Startup Dis	k		
	L	_	utomatic		•	
	_		uilt-in Ethe			
	TCP/			alk Proxies	Ethernet	
	igure IPv4:	Using DH0				HCP Lease
	bnet Mask:			DHCP Client I		
	Router:	192.168.1	.1		(If requir	ed)
DI	NS Servers:					(Optional)
Search	n Domains:					(Optional)
IPv	6 Address:	fe80:0000:0	0000:0000	0:020a:95ff:fe80	d:72e4	
		Configure	IPv6)			?

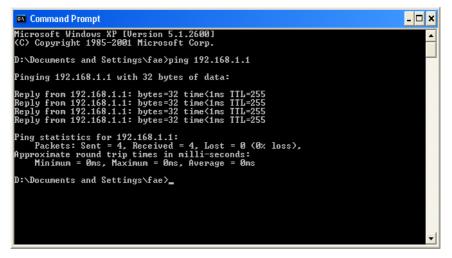
# **5.3 Pinging the Router from Your Computer**

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

### **For Windows**

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

#### For Mac OS (Terminal)

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the Application folder and get into Utilities.
- 3. Double click **Terminal**. The Terminal window will appear.
- 4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

000	Terminal - bash - 80x24	
64 bytes from 192.160 64 bytes from 192.160 64 bytes from 192.160 64 bytes from 192.160 64 bytes from 192.160		8
In the second	statistics 1, 5 packets received, 0% packet loss ax = 0.697/0.723/0.755 ms	

# 5.4 Checking If the ISP Settings are OK or Not

Open **WAN** >> **Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1-WAN3 to review the settings that you configured previously.

WAN >> Internet Access

Internet	Access				
Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL / VDSL2	None	*	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	$\sim$	Details Page IPv6
WAN3		USB	None	*	Details Page IPv6
Nata Or	ly one WAN can	support IDus			

Note: Only one WAN can support IPv6.

Advanced You can configure DHCP client options here.

# 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 Vigor2760. 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 Vigor2760.

#### 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.



Dray Tek Syslog Utility					
Log Filter Keyword: Apply to: A Firewall VPN User Ad		<ul> <li>Refresh</li> <li>WAN IPPBX</li> </ul>			
Show Syslog List		🔵 Show Tra	affic Graph 🔲 Pause		
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			
2013-08-27 15:10:07	Aug 27 07:09:51	Vigor-router			
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			
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router			
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			
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			
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router			
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router			
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router			
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 Vigor2760. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

# 5.6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.



**Warning:** After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

### Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

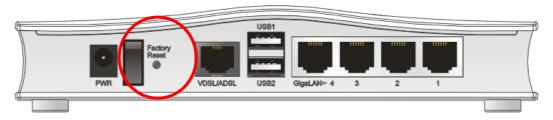
Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System	
Do you v	want to reboot your router ?
<ul> <li>Usin</li> </ul>	g current configuration
🔿 Usin	g factory default configuration
	Reboot Now
Auto Reboot Time Schedule	
Index(1-15) in	Schedule Setup:,,,,
Note: Action and	d 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 contact Draytek or your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

**Note:** If synchronization issue for xDSL happened to the router, please send an e-mail to support@DrayTek.com.

