

Vigor2830 Series

ADSL2 + Security Firewall



Your reliable networking solutions partner

User's Guide

Vigor2830 Series ADSL2+ Security Firewall User's Guide

Version: 2.3 Firmware Version: V3.6.7 Date: June 16, 2014



Copyright Information

Copyright Declarations	© 2014 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc.

• Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

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



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303Product:Vigor2830 Series Router

DrayTek Corp. declares that Vigor2830 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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, POTS, 2.4GHz/5GHz WLAN network throughout the EC region and Switzerland with restrictions in France. 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.

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 LED Indicators and Connectors	2
1.1.1 For Vigor2830 1.1.2 For Vigor2830n/ Vigor2830n-plus 1.1.3 For Vigor2830Vn/Vigor2830Vn-plus	2 4 6
1.2 Hardware Installation	8
1.3 Printer Installation	9
1.4 Accessing Web Page	16
1.5 Changing Password	17
1.6 Online Status	19
1.6.1 Physical Connection 1.6.2 Virtual WAN	19 21
1.7 Saving Configuration	21



Quick Setup	23
2.1 Quick Start Wizard	23
2.1.1 For WAN1 (ADSL) 2.1.2 For WAN2 (Ethernet) 2.1.3 For WAN3 (USB)	
2.2 Service Activation Wizard	
2.3 VPN Client Wizard	44
2.4 VPN Server Wizard	50
2.5 Wireless Wizard	55
2.6 VoIP Wizard	58
2.7 Registering Vigor Router	59



Advanced Configuration	63
3.1 WAN	63
 3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 General Setup	65 71
3.2 LAN	103
3.2.1 Basics of LAN 3.2.2 General Setup 3.2.3 Static Route	105



 3.2.4 VLAN (Multi-Subnet) 3.2.5 Bind IP to MAC	. 121 . 122 . 123
3.3 Load-Balance /Route Policy	
3.4 NAT	
3.4.1 Port Redirection	
3.4.3 Open Ports	
3.4.4 Port Triggering	
3.5 Firewall	. 143
3.5.1 Basics for Firewall	143
3.5.2 General Setup	
3.5.3 Filter Setup	
3.5.4 DoS Defense	. 158
3.6 User Management	. 161
3.6.1 General Setup	. 162
3.6.2 User Profile	
3.6.3 User Group	
3.6.4 User Online Status	
3.7 Objects Settings	. 170
3.7.1 IP Object	
3.7.2 IP Group	
3.7.3 IPv6 Object	
3.7.4 IPv6 Group 3.7.5 Service Type Object	
3.7.6 Service Type Group	
3.7.7 Keyword Object	. 183
3.7.8 Keyword Group	
3.7.9 File Extension Object 3.7.10 SMS/Mail Service Object	
3.7.11 Notification Object	
3.8 CSM Profile	
3.8.1 APP Enforcement Profile	
3.8.2 URL Content Filter Profile	
3.8.3 Web Content Filter Profile	
3.8.4 DNS Filter	
3.8.5 APPE Support List	. 209
3.9 Bandwidth Management	. 210
3.9.1 Sessions Limit	. 210
3.9.2 Bandwidth Limit	
3.9.3 Quality of Service	
3.10 Applications	. 223
3.10.1 Dynamic DNS	
3.10.2 LAN DNS	
3.10.3 Schedule 3.10.4 RADIUS	
3.10.5 Active Directory/LDAP	
3.10.6 UPnP	. 235
3.10.7 IGMP	
3.10.8 Wake on LAN	. ∠38



3.10.9 SMS/Mail Alert Service	239
3.11 VPN and Remote Access	241
3.11.1 Remote Access Control	242
3.11.2 PPP General Setup	
3.11.3 IPSec General Setup	
3.11.4 IPSec Peer Identity	
3.11.5 Remote Dial-in User	
3.11.6 LAN to LAN	
3.11.7 VPN TRUNK Management	
3.11.8 Connection Management	
3.12 Certificate Management	268
3.12.1 Local Certificate	268
3.12.2 Trusted CA Certificate	
3.12.3 Certificate Backup	273
3.13 VoIP	273
3.13.1 DialPlan	275
3.13.2 SIP Accounts	-
3.13.3 Phone Settings	288
3.13.4 Status	293
3.14 Wireless LAN	295
3.14.1 Basic Concepts	
3.14.2 General Setup	
3.14.3 Security 3.14.4 Access Control	
3.14.5 WPS	
3.14.6 WDS	
3.14.7 Advanced Setting	
3.14.8 WMM Configuration	
3.14.9 AP Discovery	
3.14.10 Station List	
3.14.11 Bandwidth Management	
3.15 SSL VPN	316
3.15.1 General Setup	316
3.15.2 SSL Web Proxy	317
3.15.3 SSL Application	
3.15.4 User Account	
3.15.5 User Group 3.15.6 Online User Status	
3.16 USB Application	328
3.16.1 USB General Settings	
3.16.2 USB User Management	
3.16.3 File Explorer	
3.16.4 USB Device Status	
3.16.5 Modem Support List	
3.17 System Maintenance	334
3.17.1 System Status	
3.17.2 TR-069	
3.17.3 Admin Setting	
3.17.4 User Password	
3.17.5 Login Page Greeting	
3.17.6 Configuration Backup 3.17.7 Syslog/Mail Alert	
3.17.7 Systog/Mail Alert	
	~~~~



3.17.9 SNMP	
3.17.10 Management	
3.17.11 Reboot System	
3.17.12 Firmware Upgrade	
3.17.13 Activation	
3.18 Diagnostics	
3.18.1 Dial-out Triggering	
3.18.2 Routing Table	
3.18.3 ARP Cache Table	
3.18.4 IPv6 Neighbour Table	
3.18.5 DHCP Table	
3.18.6 NAT Sessions Table	
3.18.7 Ping Diagnosis	
3.18.8 Data Flow Monitor	
3.18.9 Traffic Graph	
3.18.10 Trace Route	
3.18.11 Syslog Explorer	
3.18.12 IPv6 TSPC Status	
3.19 External Devices	



Application and Examples	371
4.1 How to Configure Multiple Services with PVC to PVC Binding	371
4.2 How to Configure Multi-Subnet in Vigor2830	375
4.3 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Ro	
4.4 How to Send a Notification to Specified Phone Number via SMS Service in WAN Disconnection	385
4.5 Web Portal Log-In Application for Wireless Client	389
4.6 How to Customize Your Login Page	393
4.7 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	396
4.8 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	404
4.9 QoS Setting Example	408
4.10 Upgrade Firmware for Your Router	413
4.11 Request a certificate from a CA server on Windows CA Server	416
4.12 Request a CA Certificate and Set as Trusted on Windows CA Server	420
4.13 Creating an Account for MyVigor	422
4.13.1 Creating an Account via Vigor Router 4.13.2 Creating an Account via MyVigor Web Site	422 426
4.14 How to Implement the LDAP/AD Authentication for User Management?	430
4.15 How to Implement the LDAP/AD Authentication for VPN?	433
4.16 How to Setup Address Mapping	436
4.17 How to setup Load Balance for Packets?	440





Trouble Shooting	443
5.1 Checking If the Hardware Status Is OK or Not	443
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	444
5.3 Pinging the Router from Your Computer	447
5.4 Checking If the ISP Settings are OK or Not	448
5.5 Problems for 3G Network Connection	448
5.6 Backing to Factory Default Setting If Necessary	449
5.7 Contacting DrayTek	450
Appendix I: VLAN Applications on Vigor Router	451
Appendix II: Release Note	459



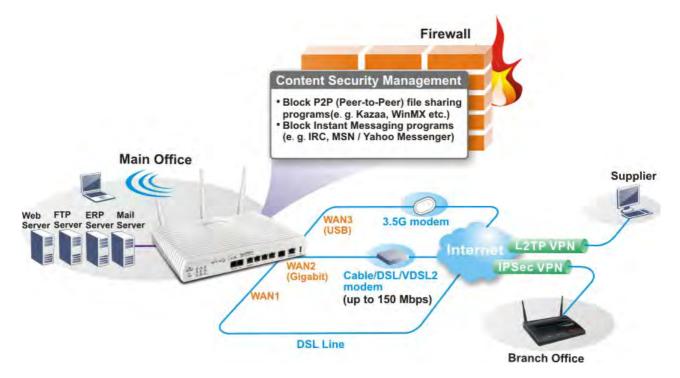
Vigor2830 series is an ADSL2+ router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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

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

Object-based firewall is flexible and allows your network be safe. In addition, Vigor2830 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files.

Vigor2830 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.



# **1.1 LED Indicators and Connectors**

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

### 1.1.1 For Vigor2830



LED		Status	Explanation				
ACT (Activity)		Blinking	The router is powered on and running normally.				
		Off	The router is powered off.				
USB		On	USB device is connected and ready for use.				
CSM		Blinking	<u> </u>				
		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filte application is enabled from <b>Firewall &gt;&gt;General</b> <b>Setup</b> . (Such profile must be established under <b>CSM</b> menu).				
WCF		On	The Web Content Filter is active. (It is enabled from <b>Firewall &gt;&gt; General Setup</b> ).				
DSL		On	The router is ready to access Internet through DSL link.				
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is tranning.				
WAN2 DoS		On	The WAN2 connection is ready.				
		Blinking	It will blink while transmitting data.				
		On	The DoS/DDoS function is active.				
		Blinking	It will blink while an attack is detected.				
VPN		On	The VPN tunnel is active.				
QoS		On	The QoS function is active.				
LED on Conned	ctor						
	Left LED	On	The port is connected.				
GigaLAN	(Green)	Off	The port is disconnected.				
1/2/3/4		Blinking	The data is transmitting.				
	Right LED	On	The port is connected with 1000Mbps.				
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.				
	Left LED	On	The port is connected.				
WAN 2 (Giga)	(Green)	Off	The port is disconnected.				
		Blinking	The data is transmitting.				
	Right LED	On	The port is connected with 1000Mbps.				
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.				



	or <b>2830</b> - Security Firewall								
•									I ON
eset	GigaLAN ► 1	2	3	4	DSL	WAN2(Giga)	USB //	PWR	O OFF

Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking).
	Press the hole and keep for more than 5 seconds. When you see the ACT LED
	begins to blink rapidly than usual, release the button. Then the router will
	restart with the factory default configuration.
GigaLAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

# 1.1.2 For Vigor2830n/ Vigor2830n-plus

Wireless LAN ONICIFINPES ACT WILAN Dos Esclory Factory Reset CSM WANZ Oct		Vigor283 ADSL2+ Securit	30n y Firewall IgaLAN + 1 2 3 4 DSL WAN2(Giga) USB
WHEIBEE LAN DINFEPTIVEDS ACT WLAN DOS DISL VEN Factory Reset CSM WANZ DOS	-	Vigor28. ADSL2+ Securit	30n-plus y Firewall IgeLAN+1 2 3 4 DSL WANZ(Gige) USB
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
(1001(10 <u>)</u> )		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application is enabled from <b>Firewall</b> >> <b>General</b> <b>Setup</b> . (Such profile must be established under <b>CSM</b> menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink slowly while wireless traffic goes through. If ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The data is transmitting.
WAN2		On	The WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while an attack is detected.
VPN		On	The VPN tunnel is active.
QoS		On	The QoS function is active.
LED on Connecto	or		
	Left LED	On	The port is connected.
GigaLAN 1/2/3/4	(Green)	Off	The port is disconnected.
0		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.
	Left LED	On	The port is connected.
WAN 2 (Giga)	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.





actor



Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on)
	or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
GigaLAN (1-4)	Connecters for local network devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

# 1.1.3 For Vigor2830Vn/Vigor2830Vn-plus



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
USB	On	USB device is connected and ready for use.
	Blinking	The data is transmitting.
CSM	On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from <b>Firewall</b> >> <b>General Setup</b> . (Such profile must be established under <b>CSM</b> menu).
WLAN	On	Wireless access point is ready.
	Blinking	It will blink slowly while wireless traffic goes through. If ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The DSL connection is ready. Quickly: The connection is tranning.
WAN2	On	The WAN2 connection is ready.
	Blinking	It will blink while transmitting data.
Line	On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off.
	Off	There is no PSTN phone call.
Phone 1/2	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
	Blinking	A phone call comes.
LED on Connector		

	Left LED	On	The port is connected.
GigaLAN 1/2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.
	Left LED	On	The port is connected.
WAN2 (Giga)	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.

Right LED	On	The port is connected with 1000Mbps.
(Green)	Off	The port is connected with 10/100Mbps when left
		LED is on.

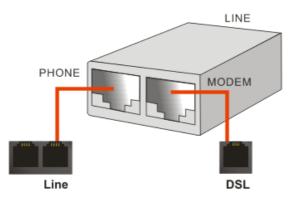
Wireless LAN	ADSL2+ Security Firewall	
ON/OFF/WPS		
Reset	Phone1/2 Line GigaLAN + 1 2 3 4 DSL WAN2(Giga)	USB

Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device
ON/OFF/WPS	making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking).
	Press the hole and keep for more than 5 seconds. When you see the ACT LED
	begins to blink rapidly than usual, release the button. Then the router will
	restart with the factory default configuration.
Phone 1/2	Connecter for analog phone(s).
Line	Connector for PSTN life line.
GigaLAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

# **1.2 Hardware Installation**

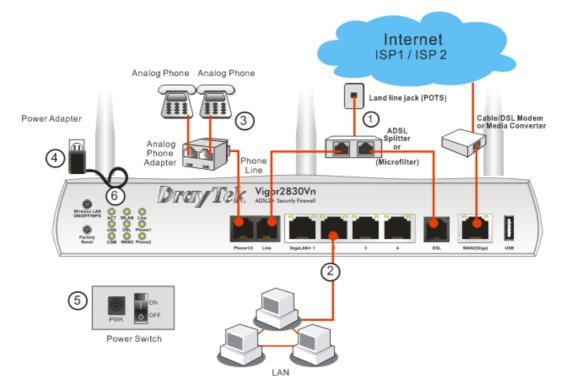
Before starting to configure the router, you have to connect your devices correctly.

1. Connect the ADSL interface to the external ADSL splitter with an ADSL line cable for all models. For Vigor2830Vn, also connect Line interface to external ADSL splitter.



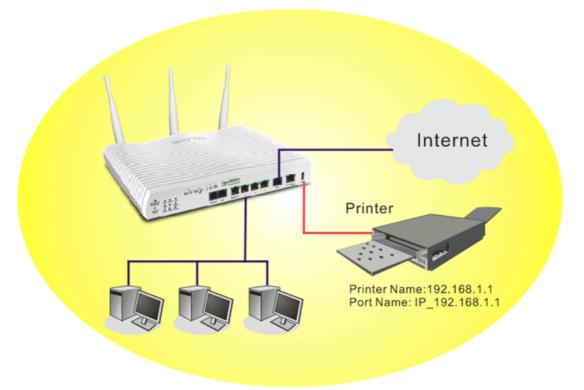
- 2. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 3. Connect the telephone set with phone lines (for using VoIP function). For the model without phone ports, skip this step.
- 4. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
- 5. Power on the device by pressing down the power switch on the rear panel.
- 6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

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



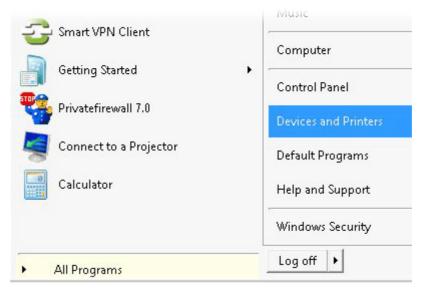
# **1.3 Printer Installation**

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**.

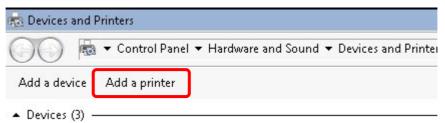


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

- 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	
	Add Printer	
v	Vhat 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.	_
	Next Canci	el

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 information with a printer.
C Use an existing port:	LPT1: (Printer Port)
Type of port:	Standard TCP/IP Port
.,,,	
	Next Cancel

Vigor2830 Series User's Guide



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 IF	address	
Device type:	TCP/IP Device	
Hostname or IP address:	192.168.1.1	
Port name:	192.168.1.1	
	omatically select the driver to use	

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

ఉ Add Printer	
Additional port info	rmation required
The device is not t	found on the network. Be sure that:
1. The device is t	urned on.
2. The network is	i connected.
3. The device is p	properly configured. n the previous page is correct.
<ol> <li>The device is p</li> <li>The address or</li> <li>If you think the ac address and perfo</li> </ol>	n the previous page is correct. Idress is not correct, click Back to return to the previous page. Then correct the rm another search on the network. If you are sure the address is correct, select t
<ol> <li>The device is p</li> <li>The address or</li> <li>If you think the ac</li> </ol>	n the previous page is correct. Idress is not correct, click Back to return to the previous page. Then correct the rm another search on the network. If you are sure the address is correct, select t
<ol> <li>The device is p</li> <li>The address or</li> <li>If you think the ac address and perfo device type below</li> </ol>	n the previous page is correct. Idress is not correct, click Back to return to the previous page. Then correct the rm another search on the network. If you are sure the address is correct, select t
<ol> <li>The device is p</li> <li>The address or</li> <li>If you think the ac address and perfordevice type below</li> </ol>	n the previous page is correct. Idress is not correct, click Back to return to the previous page. Then correct the rm another search on the network. If you are sure the address is correct, select t

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	ne printer driver					
-				ndows Update to see	more moc	lels.
	To install the drive	r from an II	nstallation CL	, CIICK Have DISK.		
-	octarer		Deintere			<b></b>
Brothe	r		🔄 Brother D	CP-116C		
Canon	8		🔄 Brother D	ICP-117C		
DrayTe	:k		🔄 Brother D			
Epson		-	🔄 Brother D			
Fuii Xe	rox	-	🗔 Brother D	CP-130C		•
📷 Th	is driver is digitally si	igned.		Windows Up	date	Have Disk
	II me why driver sign					

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

Add Printer	
📕 🖶 Add Printer	
Type a printer name	
Printer name: Brother DCP-116C	
This printer will be installed with the Brother DCP-116C dri	ver.
	Next Can

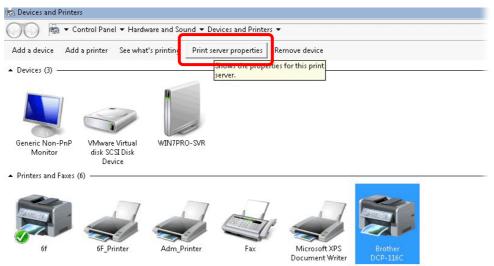
10. Choose **Do not share this printe**r and click **Next**.

🚽 Add Printer			
Printer Sharing			
If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.			
• Do not share this printer	]		
C Share this printer so that o	thers on your network can fi	ind and use it	
Share name:			
Location:			
Comment:			

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

🦟 A	Add Printer
0	and 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.

Ports on thi	1		
Port TS002	Description Inactive TS Port	Printer	<u> </u>
TS002	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	
I PR_local	Standard TCD/ID Port	6E_Drinter	
192.168.1.	Standard TCP/IP Port	Brother DCP-116C	
XPSPort:	Local Port	Microsoft XPS Docur	nent Writer 🚽
Add	Port Dele	te Port Con	figure Port
			-

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

Ĩ	Configure Standard TCP/IP	Dort Monit	or	
_	Port Settings	r ore morne	01	
F	Port Name:		192.168.1.1	
-	Printer Name or IP Addr	a <i>re</i> ,	192.168.1.1	
- 11	- Protocol	ess:	192.108.1.1	
- 11	C Raw			
- 11	Raw Settings			
- 11	Port Number:	9100		
1	LPR Settings			 
-	Queue Name:	рЦ		
	LPR Byte Counting	Enabled		
	SNMP Status Enab	led —		
	Community Name:	public	8	
_	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**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

<b>Dray</b> Tek	MyVigor Register E-newsletter DrayTek.HQ Media Center Global (	(English) 💌 Log
About DrayTek Produc	ts Supports Solutions Multi-Media Demo Contact Us	<b>Q</b> Search
FAQ / Application	You are here: Home > Supports > FAQ / Application Notes > Printer Server	
Basic		<b>N</b>
Firmware Upgrade	Printer Server	
WAN		
IPv6	1. What types of printers are compatible with Vigor router?	2012/01/12
Triple-Play	2. How do I configure LPR printing on Windows7?	2012/08/20
Dual WAN	3. How do I configure LPR printing on My Windows Vista ?	2009/01/20
LAN		
DHCP	4. How do I configure LPR printing on Linux boxes ?	2009/01/20
NAT	5. How do I configure LPR printing on Windows2000/XP ?	2010/04/06

# 1.4 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.

Username Password	Login
Copyright©, DrayTek Corp. All Rights Reserved.	<b>Dray</b> Tek

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



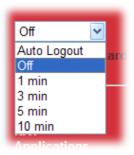
**Notice:** If you fail to access to the web configuration, please go to "Trouble Shooting" for detecting and solving your problem.

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

Vigor2830 ADSL2 + Security F	Series Firewall				Dro	ay Te
Off 💌 🕫	System Status					
zards line Status	Model Name Firmware Version Build Date/Time	: Vigor2830Vn : 3.6.7_db : Mar 24 2014 15	5:47:36			
AN			LAN			
oad-Balance/Route Policy AT irewall ser Management	LAN1 LAN2 LAN3	MAC Address 00-50-7F-6A-FB-1 00-50-7F-6A-FB-1 00-50-7F-6A-FB-1	8 192.168.2.1	255.255.255.0	DHCP Server ON ON ON	DNS 8.8.8.8 8.8.8.8 8.8.8.8
lbjects Setting ISM ≣ andwidth Management	LAN4 IP Routed Subnet	00-50-7F-6A-FB-1 t 00-50-7F-6A-FB-1	8 192.168.0.1	255.255.255.0 255.255.255.0	ON ON	8.8.8.8 8.8.8.8
pplications PN and Remote Access ertificate Management oIP	MAC Address 00-50-7F-6A		Wireless LAN ncy Domain	Firmware Versic "2.2.0.7"	n SSID DrayT	Tek
Vireless LAN SL VPN			WAN			
B Application stem Maintenance ignostics ternal Devices	Link Statu WAN1 Disconned WAN2 Disconned WAN3 Disconned	oted 00-50-7F-6A-F oted 00-50-7F-6A-F	B-1A	ction IP Address	5 Default Gat  	teway
ipport Area			IPv6			
oduct Registration	Address LAN FE80::250:	7FFF:FE6A:FB18/64	Sc Lir		ccess Mode	
			VoIP			
	Port	Profile	Re	g. In	/Out	

**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.



# **1.5 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 the Username/Password and click Login.
- 3. Go to **System Maintenance** page and choose **Admin Setting**.



System Maintenance >> Admin Se	etting
Administrator Password	
Old Password	
New Password	(Max. 23 characters allowed)
Confirm Password	(Max. 23 characters allowed)
Note:Password can contain only	·a-z A-Z O-9 , ; : . " < > * + = \   ? @ # ^ ! ( )
Administrator Local User	
🗖 Local User	
Local User List	
Index User Name	

- 4. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.
- 5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.

Username Password	
	Login
Copyright@, DrayTek Corp. All Rights Reserved.	<b>Dray</b> Tek

# 1.6 Online Status

Online Sta	atus
Physical	Connection
Virtual W	AN

#### **1.6.1 Physical Connection**

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

#### **Physical Connection for IPv4 Protocol**

**Online Status** 

Physical Connectio	en la			2	ystem Uptime: 4:7
	IPv4		IPv6		
LAN Status	Prima	nry DNS: 8.8.8.8	3	Secondary D	NS: 8.8.4.4
IP Address	TX Packets	RX Pac	kets		
192.168.1.1	53964	729498			
WAN 1 Status					>> <u>Dial PPP</u>
Enable	Line	Name	Mode	Up Time	
Yes	VDSL		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
Message [ PPP Sh	iutdown ]				
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	4:07:44	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172.16.3.103	172.16.1.1	29011	351	125630	1230
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

#### **Physical Connection for IPv6 Protocol**

#### **Online Status**

Physical Connect	ion			System Uptime: 4:8:42
	IPv4		IPv6	
LAN Status				
IP Address				
FE80::250:7FF	F:FEEA:7EC8/64 (Lin	k)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
2	0	156	0	
WAN IPv6 Status				
Enable	Mode	Up Time		
No	Offline			
IP			Gateway	IP

Detailed explanation (for IPv4) is shown below:



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

Detailed explanation (for IPv6) is shown below:

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



Item	Description
	<b>Up Time</b> - Displays the total uptime of the interface.
	<ul><li>Up Time - Displays the total uptime of the interface.</li><li>IP - Displays the IP address of the WAN interface.</li></ul>
	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.

#### 1.6.2 Virtual WAN

Such page displays the virtual WAN connection information.

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

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

Online Status	0n	line	Status
---------------	----	------	--------

Virtual WAN				Sys	tem Uptime: 69:
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
WAN 7 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

# **1.7 Saving Configuration**

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



**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.



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

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

•••
•••
•••

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.



ick Start Wizard	
AN Interface	
WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL
Physical Type:	Auto negotiation 💟
	< Back Next > Finish Cance

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

#### 2.1.1 For WAN1 (ADSL)

WAN1 is specified for ADSL connection. Please select the appropriate Internet access type **according to the information from your ISP**.

Interface	
WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL
Physical Type:	Auto negotiation 😒

#### 2.1.1.1 PPPoE/PPPoA

**PPPoE/PPPoA:** PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.



1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page. Choose **PPPoE XXXX or PPPoA XXXXX** as the protocol.

ect to Internet	
WAN 1	
VPI	8 Auto detect
VCI	35
Protocol / Encapsulation	PPPoA VC MUX
Fixed IP	◯Yes ④No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	8.8.8.8
Second DNS	8.8.4.4

Available settings are explained as follows:

Item	Description
VPI	Type in the value provided by ISP. <b>Auto detect</b> – Click this button to have the VPI and VCI to be detected by the system automatically
VCI	Type in the value provided by ISP.
Protocol / Encapsulation	There are several modes offered for you to choose for WAN1 interface. PPPoE LLC/SNAP PPPoE VC MUX PPPoA LLC/SNAP PPPoA VC MUX 1483 Bridged IP LLC 1483 Routed IP LLC 1483 Routed IP VC-Mux 1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE)
Fixed IP	Click <b>Yes</b> to enable Fixed IP feature.
IP Address	Type the IP address if <b>Fixed IP</b> is enabled.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

2. After finished the above settings, simply click **Next.** 

Quick Start Wizard

WAN 1	
Service Name (Optional)	84005755@hinet.net
Username	84005755
Password	•••••
Confirm Password	

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
User Name	Type in the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Type a valid password provided by the ISP.
<b>Confirm Password</b>	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

#### Quick Start Wizard

WAN Interface:	WAN1
Physical Mode:	ADSL
Physical Type:	Auto negotiation
VPI:	0
VCI:	33
Protocol / Encapsulation:	PPPoE / LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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.

### 1483 Bridged IP /1483 Routed IP

1. Choose **WAN1** as WAN Interface and click the **Next** button; you will get the following page. Choose **1483 Bridged IP** /**1483 Routed IP** as the protocol.

Quick Start Wizard

WAN 1	
VPI	8 Auto detect
VCI	35
Protocol / Encapsulation	1483 Routed IP LLC
Fixed IP	🔿 Yes 🛛 💿 No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	8.8.8.8
Second DNS	8.8.4.4
	<pre>&lt; Back Next &gt; Finish Can</pre>

Available settings are explained as follows:

Item	Description

VPI	Type in the value provided by ISP. <b>Auto detect</b> – Click this button to have the VPI and VCI to be detected by the system automatically
VCI	Type in the value provided by ISP.
Protocol / Encapsulation	There are several modes offered for you to choose for WAN1 interface.
Fixed IP	Click <b>Yes</b> to enable Fixed IP feature.
IP Address	Type the IP address if <b>Fixed IP</b> is enabled.
Subnet Mask	Type the subnet mask.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

e confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	ADSL
Physical Type:	Auto negotiation
VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	8.8.8.8
Secondary DNS:	8.8.4.4

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

#### Quick Start Wizard Setup OK !!!

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

## 2.1.2 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

l Interface	
WAN Interface:	WAN2 💌
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 🔽
	Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex

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.

#### Quick Start Wizard

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

### **PPPoE**

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.



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.

ect to Internet				
WAN 2				
Select one of the	following Internet Ac	cess types provi	ded by your ISP.	
	PPPoE			
	🔘 РРТР			
	🔘 L2TP			
	🔘 Static IF			
	O DHCP			
	-			

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

#### Quick Start Wizard

PPPoE Client Mode	
WAN 2	
Enter the user name and p	assword provided by your ISP.
User Name	84005657@hinet.net
Password	•••••
Confirm Password	•••••
	< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
User Name	Type in the valid user name (maximum 63 characters) provided by the ISP in this field.
Password	Type a valid password provided by the ISP.
Confirm Password	Retype the password.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.



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

Quick Start Wizard	
Please confirm your settings:	
WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
Click <b>Back</b> to modify char settings and restart the V	nges if necessary. Otherwise, click <b>Finish</b> to save the current rigor router.
	<pre>&lt; Back Next &gt; Finish Cancel</pre>

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

### Quick Start Wizard Setup OK !!!

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

### PPTP/L2TP

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 follow	wing Internet Acce:	ss types provid	ded by your ISP.	
	O PPPoE			
	💽 РРТР			
	O L2TP			
	🔘 Static IP			
	🔘 DHCP			

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

Quick Start Wizard

WAN 2 Enter the user name, pass your ISP.	vord, WAN IP configuration and L2TP server IP provi	ided by
Úser Name	test	
Password	••••	
Confirm Password	••••	
WAN IP Configuration		
💿 Obtain an IP address	automatically	
🔘 Specify an IP address		
IP Address		
Subnet Mask		
Gateway	undefined	
Primary DNS		
Second DNS		
L2TP Server		

Available settings are explained as follows:

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

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



Qui	ick	Start	Wizar	d

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	L2TP
settings and restart the Vi	ges if necessary. Otherwise, click <b>Finish</b> to save the current igor router.

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

### Quick Start Wizard Setup OK !!!

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

### 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	following Internet Ac	cess types provid	led by your ISP.	
	🔘 PPPoE			
	🔘 РРТР			
	🔘 L2TP			
	💿 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 <u>ovided by your</u> IS	βP.	
WAN IP	172.16.3.102		
Subnet Mask	255.255.0.0		
Gateway	172.16.1.1		
Primary DNS	8.8.8.8		
Secondary DNS	8.8.4.4	(optional)	

Available settings are explained as follows:

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

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

iick Start Wizard		
ease confirm your settings:		
WAN Interface:	WAN2	
Physical Mode:	Ethernet	
Physical Type:	Auto negotiation	
Internet Access:	Static IP	
Click <b>Back</b> to modify chan settings and restart the V	nges if necessary. Otherwise, click <b>Finish</b> to save the current igor router.	
	<pre>&lt; Back Next &gt; Finish Cance</pre>	

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

### Quick Start Wizard Setup OK !!!

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

## 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.

ect to Internet				
WAN 2				
Select one of the followir	ng Internet Acce	ss types provi	ded by your ISP.	
	○ PPPoE			
	🔘 РРТР			
	🔘 L2TP			
	🔘 Static IP			
	OHCP			
	-			

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

Quick Start Wizard

WAN 2	
If your ISP requenter it in.	uires you to enter a specific host name or specific MAC address, please
Host Name	(optional)
MAC	00 -50 -7F -00 -00 -02 (optional)

Available settings are explained as follows:

Item	Description
Host Name	Type the name of the host.
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.

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 <b>Finish</b> 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)

To use 3G USB modem for network connection, please choose WAN3.

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

ck Start Wizard			
l Interface			
WAN Interface:	WAN3 V		
Display Name:			
Physical Mode:	USB		
	<pre></pre>		

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

Quick Start Wizard

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

Available settings are explained as follows:

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



	<ul> <li>question, please contact to your ISP. The maximum length of the string you can set is 47 characters.</li> <li>APN Name – APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.</li> </ul>
4G USB Modem (DHCP mode)	<ul> <li>SIM Pin code –Type PIN code of the SIM card that will be used to access Internet.</li> <li>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.</li> <li>APN Name – APN means Access Point Name which is provided and required by some ISPs.</li> </ul>

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

Quick Start Wizard

WAN Interface:	WAN3
Physical Mode:	USB
Internet Access:	DHCP
	/igor router.
	-

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

### Quick Start Wizard Setup OK !!!

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

# 2.2 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.

#### 1. Open Service Activation Wizard.



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

Service Activation Wizard	
Select the service type that you want to activate	
This wizard is used for activating - Web Content Filter Please choose the edition you need.	sense key
	Next > Finish Cancel

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

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



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:	
o w	/eb Content Filter (BPjM)	
	PjM is the web content filter based on service operated in Germany. We recommend only users live in ermany to try the BPjM WCF service. This is a free service without guarantee.	
	Activation Date : 2013-02-18	
Co tri	Ide Content Filter (Commtouch)         License           Agreement         Agreement           ommtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day lal period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from tailing outlets.         base of the trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from tailing outlets.	
	Activation Date : 2013-02-18	
0 w	Elense	Activation Date : 2013-02-18

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

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**.

ease confirm your settings		
Sevice Type : Sevice Activated :	Trial version Web Content Filter ( Commtouch	)
Please click Back to re-so	elect service type you to activate.	
	< Back Next >	Finish Canc

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

. . . . ...



Service Activation Wizard		
Connection Succeeded!		
Please check the following item(s) to enable services on your router.		
Enable Web Content Filter		
1	Next>	Finish

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

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

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

ibled!			
	DrayTek Service	e Activation	
Service Name	Start Date	Expire Date	Status
Web Content filter	2011-09-21	2011-10-22	Commtouch
lease check if the licen ormal operation for you			

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**.

lect the service type that you want to a	ctivate				
This wizard is used for activating - Web Content Filter Please choose the edition you nee	ed.				
⊖ Fr	ee trial edition				
⊙ Fo	ormal edition wit	h license key	>		
		Nex	t > Finish	Cance	
		INCA		Cance	
vice Activation Wizard					
ect the service type that you want to activat	e				
Please choose the item you want to use. WCF service:					
Web Content Filter (Commtouch) Commtouch is the web content filter based purchase DrayTek's prepared Commtouch of	License Action on Commtouch cler GlobalView WCF pack		. There is a 30-day tri tlets.	al period. After tr	rial, you can
Enter your License key:			Activation Date :	2010-11-02	<u>select</u>
I have read and accept the above Ag	eement. (Please )	check this box).			
		,			

# 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.

oose VPN Establishment Environment	
LAN-to-LAN VPN Client Mode Selection:	Route Mode 🛩
Please choose a LAN-to-LAN Profile:	[Index] [Status] [Name] 🗸
Note: For a typical LAN-to-LAN tunnel, please If the remote network is expecting only the subnet and then select NAT mode. If in doubt then select Route Mode	y a single client or ip and is not configured to route
If the remote network is expecting only the subnet and then select NAT mode.	y a single client or ip and is not configured to route

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode. 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 ??? 2 x ??? 3 x ??? 4 x ??? 5 x ??? 6 x ??? 7 x ??? 8 x ??? 9 x ??? 10 x ??? 11 x ??? 12 x ??? 13 x ??? 14 x ??? 15 x ??? 16 x ??? 16 x ??? 18 x ??? 18 x ???
2 x ??? 3 x ??? 4 x ??? 5 x ??? 6 x ??? 7 x ??? 8 x ??? 9 x ??? 10 x ??? 10 x ??? 11 x ??? 13 x ??? 13 x ??? 14 x ??? 15 x ??? 16 x ??? 18 x ???
3       ×       ???         4       ×       ???         5       ×       ???         6       ×       ???         7       ×       ???         8       ×       ???         9       ×       ???         10       ×       ???         11       ×       ???         12       ×       ???         13       ×       ???         14       ×       ???         16       ×       ???         17       ×       ???         18       ×       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
10       x       ???         11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
11       x       ???         12       x       ???         13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
13       x       ???         14       x       ???         15       x       ???         16       x       ???         17       x       ???         18       x       ???
14         x         ???           15         x         ???           16         x         ???           17         x         ???           18         x         ???
16 x ??? 17 x ??? 18 x ???
16 x ??? 17 x ??? 18 x ???
18 x ???
18 x ???
19 x ???
20 x ???
21 x ???
22 x ???
23 x ???
24 x ???
25 x ???
26 🗴 ??? 🕇
27 x ???
28 🗴 ??? 🔔
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

ecurity ranking (1 is the highest; 5 is the	lowest) Throughput ranking (1 is the highest; 5 is the lowest
<ol> <li>L2TP over IPSec</li> <li>IPSec</li> <li>PPTP (Encryption)</li> <li>L2TP</li> <li>PPTP (None Encryption)</li> </ol>	1. PPTP (None Encryption) 2. L2TP 3. IPSec 4. L2TP over IPSec 5. PPTP (Encryption)
Select VPN T	ype: PPTP (None Encryption) PPTP (None Encryption) PPTP (Encryption) IPSec L2TP L2TP over IPSec (Nice to Have) L2TP over IPSec (Must)

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



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

Profile Name	???
/PN Dial-Out Through	WAN1 First
Always on	
Server IP/Host Name for VPN e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Jsername	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

VPN and Remote Access >> VPN Client Wizard

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

VPN and Remote Access >> VPN Client Wizard

Profile Name	???
VPN Dial-Out Through	WAN1 First
Always on	
Server IP/Host Name for VPN (e.g. 5551234, 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	
🔘 Subject Name First	
IPSec Security Method	
💿 Medium (AH)	
🔿 High (ESP)	DES without Authentication 💌
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0



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

VPN and Remote Access >> VPN Client Wizard

ofile Name	VPN-1
/PN Dial-Out Through	WAN1 First
Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Jsername	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

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

VPN and Remote Access >> VPN Client Wizard

rofile Name	VPN-2
PN Dial-Out Through	WAN1 First
Always on	
erver IP/Host Name for VPN 9.q. 5551234, draytek.com or 123.45.67.89)	
E Authentication Method	
O Pre-Shared Key	
Confirm Pre-Shared Key	
🔘 Digital Signature (X.509)	
Peer ID	None 🗸
Local ID	
💿 Alternative Subject Name First	
🔘 Subject Name First	
Sec Security Method	
💿 Medium (AH)	
🔿 High (ESP)	DES without Authentication 😒
sername	???
assword	
emote Network IP	0.0.0.0
emote Network Mask	255.255.255.0

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.

VPN Dial-Out Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.		
Through	WAN1 First		
	WAN1 First		
	WAN1 Only		
	WAN2 First		
	WAN2 Only WAN1 Only: Backup WAN2		
	WAN1 Only: Backup WAN2 WAN2 Only: Backup WAN1		
	WAN3 First		
	WAN3 Only		
	WAN1 First/ WAN2 First/ WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for VPN connection. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.		
	WAN Interface instead. WAN1 Only /WAN2 Only/WAN 3 Only- While		
	connecting, the router will use WAN1/WAN2/WAN3 as		
	the only channel for VPN connection.		
	<b>WAN1 Only: Backup WAN2</b> - While connecting, the router will use WAN2 for VPN connection. If WAN2 fails, the router will use backup WAN1 interface instead.		
	WAN2 Only: Backup WAN1 - While connecting, the router will use WAN1 for VPN connection. If WAN1 fails, the router will use backup WAN2 interface instead.		
Always On	Check to enable router always keep VPN connection.		
Pre-Shared Key	<b>IKE Authentication Method</b> usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.		
	Pre-Shared Key- Specify a key for IKE authentication.		
	Confirm Pre-Shared Key-Confirm the pre-shared key.		
Digital Signature (X.509)	Click <b>Digital Signature</b> to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local Certificate.</b> Otherwise, the setting you choose here will not be effective.		
	<b>Peer ID</b> – Choose the peer ID selection from the drop down list.		
	<b>Local ID</b> – Choose <b>Alternative Subject Name First</b> or <b>Subject Name First</b> .		
IPSec Security Method	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.		
	<b>High</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.		



User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
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.

ease confirm your settings		
LAN-to-LAN Index:	3	
Profile Name:	VPN-1	
VPN Connection Type:	L2TP over IPSec (Must)	
VPN Connection Through:	WAN1 First	
Always on:	No	
Server IP/Host Name:	draytek.com	
IKE Authentication Method:	Digital Signature (X.509)	
IPSec Security Method:	AH-SHA1	
Remote Network IP:	192.168.1.6	
Remote Network Mask:	255.255.255.0	
Click <b>Back</b> to modify changes if nece and proceed to the following action	essary. Otherwise, click <b>Finish</b> to save the current settings :	
	So to the VPN Connection Management.	
	O Do another VPN Client Wizard setup.	
	<ul> <li>View more detailed configurations.</li> </ul>	
	< Back Next > Finish Canc	

Available settings are explained as follows:

VPN and Remote Access >> VPN Client Wizard

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

# 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: /lease choose a LAN-to-LAN Profile:	Site to Site VPN (LAN-to-LAN)
anco obanco a LAN-to-LAN Brafilor	
TEASE CHOOSE & LAN-TO-LAN PROME:	1 x ??? 💌
lease choose a Dial-in User Accounts:	[Index] [Status] [Name] 🕑
llowed Dial-in Type:	
	<ul> <li>✓ PPTP</li> <li>✓ IPsec</li> </ul>
	✓ IPsec ✓ L2TP with IPsec Policy None
	SSL Tunnel

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. <b>Site to Site VPN</b> – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. <b>Remote Dial-in User</b> –You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. Site to Site VPN (LAN-to-LAN) <u>Site to Site VPN (LAN-to-LAN)</u> <u>Remote Dial-in User (Teleworker)</u>

Please choose a LAN-to-LAN Profile	This item is available when you choose <b>Site to Site VPN</b> (LAN-to-LAN) as VPN server mode. There are 32 VPN
LAN-to-LAN Profile	(LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set. $\begin{bmatrix} Index \end{bmatrix} \begin{bmatrix} Status \end{bmatrix} \begin{bmatrix} Name \end{bmatrix} \\ 1 \\ x \\ ??? \\ 2 \\ x \\ ??? \\ 3 \\ x \\ ??? \\ 4 \\ x \\ ??? \\ 5 \\ x \\ ??? \\ 6 \\ x \\ ??? \\ 7 \\ x \\ ??? \\ 8 \\ x \\ ??? \\ 9 \\ x \\ ??? \\ 10 \\ x \\ ??? \end{bmatrix}$
	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$
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). <ul> <li>PPTP</li> <li>IPsec</li> <li>L2TP with IPsec Policy</li> <li>None</li> <li>Nice to Have</li> <li>Must</li> </ul>
	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 ( <b>Site to Site</b> <b>VPN</b> and <b>Remote Dial-in User</b> ) 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 **Remote-Dial-in User** 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 / SSL Tunnel Aut	hentication
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:

erver1
lone 🗸
92.168.1.99
Next > Finish Cancel
1

VPN and Remote Access >> VPN Server Wizard

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

VPN and Remote Access >> VPN Server Wizard

IPSec / L2TP over IPSec Authentication			
🗹 Pre-Shared Key			
Confirm Pre-Shared Key			
📃 Digital Signature (X.509)			
Peer ID	None	*	
Peer IP/VPN Client IP			
Peer ID			

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Pre-Shared Key	For IPSec/L2TP IPSec authentication, you have to type a pre-shared key.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local</b> <b>Certificate.</b> Otherwise, the setting you choose here will not be effective.
Peer IP/VPN Client IP	Type the WAN IP address or VPN client IP address for the remote client.
Peer ID	Type the ID name for the remote client.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

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

Please Confirm Your Settings			
VPN Environment: Index: Profile Name:	Site to Site VPN (LAN-to-LAN) 3 VPN-Ser1		
Username: Allowed Service: Peer IP/VPN Client IP: Peer ID:	server1 PPTP+IPSec		
Remote Network IP: Remote Network Mask:	0.0.0.0 255.255.255.0		
Click <b>Back</b> to modify changes if and proceed to the following ac	necessary. Otherwise, click <b>Finish</b> to save the current settings ction:		
	<ul> <li>Go to the VPN Connection Management.</li> <li>Do another VPN Server Wizard setup.</li> <li>View more detailed configurations.</li> </ul>		
	O Do another VPN Server Wizard setup.		

Available settings are explained as follows:

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

# 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).

Note: This wizard is available for "n" model only.

Follow the steps listed below:

1. Open Wireless Wizard.



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

#### Wireless Wizard

Name:DrayTekMode:Mixed(11b+11g+11n) ♥Channel:Channel 6, 2437MHz ♥Password:1235678996Note:The host AP configured here will be used for home or internal company use.	AP Configuration	
Channel: Channel 6, 2437MHz Password: 1235678996	Name:	DrayTek
Password: 1235678996	Mode:	Mixed(11b+11g+11n)
	Channel:	Channel 6, 2437MHz 🛛 🖌
Note:The host AP configured here will be used for home or internal company use.	Password:	1235678996

Available settings are explained as follows:

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

-

	Mixed(11b+11g+11n)       Mixed(11b+11g+11n)         11b Only       11g Only         11g Only       11n Only (2.4 GHz)         Mixed(11b+11g)       Mixed(11b+11g)         Mixed(11g+11n)       Mixed(11a+11n 5 GHz)         Mixed(11b+11g+11n)       or		
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 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").		
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.

🔍 Enable 🛛 🖲 🖸	Disable
Name:	DrayTek_Guest
Password:	
Rate Control:	Enable Upload30000 kbps Download30000 kbps
	ith wireless devices connecting to the router's other APs. The guest gured to be not able to connect to LAN interfaces also. However if the tions were already made, then the guest AP will be able to connect to

Available settings are explained as follows:

Wireless Wizard

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

Password	<ul> <li>The wireless mode offered by this wizard is WPA2/PSK.</li> <li>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.</li> <li>Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").</li> </ul>	
Rate Control	<ul> <li>It controls the data transmission rate through wireless connection.</li> <li>Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.</li> <li>Download – Type the transmitting rate for data download. Default value is 30,000 kbps.</li> </ul>	
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

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.

Note: This wizard is available for "V" model only.

1. Open VoIP Wizard.



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

VoIP service provider d	omain			
VoIP service provider	draytel.org 🛛 👻	draytel.org	(63 char max).	
SIP Port	5060			
t Account quickly				
Phone 1 (default mappi	ng to Account 1)			
Account Number/Name		(63 char max).		
Password		(63 char max).		
Phone 2 (default mappi	ng to Account 2)			
🗹 use the same Acco	unt as phone1			
Account Number/Name		(63 char max).		
Password		(63 char max).		

Available settings are explained as follows:

Item	Description	
Set VoIP service provider domain	<ul><li>VoIP service provider - Use the drop down list to choose the ISP which offers the VoIP service for your router.</li><li>SIP Port – Use the default setting (5060).</li></ul>	
Set Account quickly	Account Number/Name – Type the account number/name registered to your ISP.	
	<b>Password</b> – Type the password for the account registered to your ISP.	
	<b>Use the same Account as phone 1</b> – 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.	



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

VoIP Wizard	
Please confirm your settings:	
VoIP Service Provider	draytel.org
SIP Port	5060
Phone 1 Account	5633s
Phone 2 Account	5633s
Click <b>Back</b> to modify char	ges if necessary. Otherwise, click Finish to save current settings.
	< Back Next > Finish Cancel

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.

		Login
Password	••••	Login
Username	admin	

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. If not, please refer to section 4.13 Creating an Account for MyVigor.

	Please take a moment to register. Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!			
LOGIN				
UserName :	james_fae			
Password :	******			
Auth Code :	txxhdd t x x h d d			
If you cannot read the word, <u>click here</u>				
	Forgotten password? Login			
Don't have a	MyVigor Account ? Create an account now			

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

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

<b>Dray</b> Tel				М
1 Home				Searc
D About Us Product My Information VigorACS SI Vigor Series	My Information Welcome,james Last Login Time : Last Login From : Current Login Tim Current Login From Your Device List	<mark>_fae</mark> 2011-08-24 09:3 123.110.144.22 e: 2011-08-24 2 m: 114.37.142.1	0 3:01:15	Add
Management Product Registration	Serial Number / Host ID 104001703857	Device Name Vigor2710	Model Vigor2710	Note
🌡 Customer Survey	200807100001	VigorPro5300	VigorPro5300	-
	200911030001	ryan	VigorPro5300	-

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**.

<b>Dray</b> Tek					My	Vigor
Home					Search	GO
D About Us	My Product		S	earch for t	his site	GO
My Information	Registration Device					
VigorACS SI	Serial number :	20110822143	20301			
Vigor Series	Nickname : *	vigor2830				
🌣 Management	Registration Date : *	08-24-2011				
Product Registration	Usage :	- Select -	<b>~</b>			
Customer Survey	Product Rating :	- Select -	🔁 ( Your	opinion so	far )	
	No. of Employees :	- Select -	📔 ( In tota	al within yo	ur company )	
	Supplier :			(Wher	e you bought it from )	
	Date of Purchase :			( mm-d	d-yyyy ]	
	Internet Connection : *					
	Cable	ADSL		/DSL	🗌 Fiber	
	🔲 3G	🗆 WIMAX		LTE		
Convictors @ DravTek Com					Cancel Su	bmit

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

Your device has been successfully added to the database.

OK
----

- 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.

<b>Dray</b> Tek	C		/	MyVigo
1 Home			Se	arch G
D	My Information			
About Us Product	Welcome, draytekfae Last Login Time : 2011-08-24			
My Information	Last Login From : 123.110.14 Current Login Time : 2011-08			
VigorACS SI	Current Login From : 114.37.1			
Vigor Series	Your Device List		RowNo : 5 👱 Pa	sgeNo : Z 🞽
Management	0.1111.1.111.110			
Customer Survey	Serial Number / Host ID	Device Name	Model	Note
,	20100707144801	Vigor3300V	Vigor3300	-
	20100708105301	Vigor2820	Vigor2828	-
	20101005104801	Vigor2710vn	Vigor2710	-
	2010121707335201	Vigor2920	Vigor2928	-
	2011082214320301	Vigor2830	Vigor2830	-
	2011082214320301	Vigor2830	Vigor2830	

**Dray** Tek

This page is left blank.

#### Vigor2830 Series User's Guide

# **Dray** Tek



This chapter will guide users to execute advanced 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.

Vigor2830 Se ADSL2 + Security Fire					Dro	<b>ay</b> Tek
Off 💌 1166	System Status					^
Wizards Online Status	Model Name Firmware Version Build Date/Time	: Vigor2830Vn : 3.6.7_db : Mar 24 2014 15:47:3	86			
WAN			LAN			
LAN Load-Balance/Route Policy NAT	LAN1	MAC Address 00-50-7F-6A-FB-18	IP Address 192.168.1.1	Subnet Mask 255,255,255,0	DHCP Server ON	DNS 8.8.8.8
Firewall	LAN2	00-50-7F-6A-FB-18	192.168.2.1	255.255.255.0	ON	8.8.8.8
User Management Objects Setting	LAN3 LAN4	00-50-7F-6A-FB-18 00-50-7F-6A-FB-18	192.168.3.1 192.168.4.1	255.255.255.0 255.255.255.0	ON ON	8.8.8.8
CSM	IP Routed Subnet	00-50-7F-6A-FB-18	192.168.0.1	255.255.255.0	ON	8.8.8.8
Bandwidth Management Applications			Wireless LAN			
VPN and Remote Access	MAC Address	Frequency		Firmware Versio	n SSID	
Certificate Management	00-50-7F-6A-F		bomain	2.2.0.7	DrayT	ek
VolP Wireless I AN						
SSL VPN	Link Status	MAC Address	WAN Connect	tion IP Address	; Default Gat	
USB Application	WAN1 Disconnecte					eway
System Maintenance Diagnostics	WAN2 Disconnecte					
External Devices	WAN3 Disconnecte	d 00-50-7F-6A-FB-1E	3			
Support Area			IPv6			
Product Registration	Address LAN FE80::250:7F	FF:FE6A:FB18/64	Scc Link		ccess Mode	
			VolP			
	Port	Profile	Req	. In,	/Out	

# 3.1 WAN

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

# 3.1.1 Basics of Internet Protocol (IP) Network

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

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



### What are Public IP Address and Private IP Address

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

# Get Your Public IP Address from ISP

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

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

### Network Connection by 3G/4G USB Modem

For 3G/4G mobile communication through Access Point is popular more and more, Vigor2830 adds the function of 3G/4G network connection for such purpose. By connecting 3G/4G USB Modem to the USB port of Vigor2830, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2830n with 3G/4G 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 Vigor2830n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2830n series.



After connecting into the router, 3G/4G 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/4G 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/4G 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

### 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.

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

0K

Note:Line Speed only used for load balance mode: according to Line Speed

Available settings are explained as follows:

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

**Dray** Tek

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

Note: In default, each WAN port is enabled.

## WAN1 with ADSL

WAN1 is fixed with physical mode of ADSL.

#### WAN >> General Setup

WAN 1	
Enable:	Yes 💌
Display Name:	
Physical Mode:	ADSL
Physical Type:	Auto negotiation 🖂
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion :	Disable 💌 (Please configure Internet Access setting first)
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Backup 💌 Load Balance: 🗹
	🗌 WAN 1 🗖 WAN 2 🗖 WAN 3
Backup Type (Only if acting as backup for multiple WAN):	<ul> <li>When any of selected WAN disconnect</li> <li>When all of selected WAN disconnect</li> </ul>

Note:Line Speed only used for load balance mode: according to Line Speed



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

VLAN Tag insertion	<b>Enable</b> – Enable the function of VLAN with tag.	
	The router will add specific VLAN number to all packets on the WAN while sending them out.	
	Please type the tag value and specify the priority for the packets sending by WAN1.	
	<b>Disable</b> – Disable the function of VLAN with tag.	
	<b>Tag value</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.	
	<b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.	
Active Mode	Choose <b>Always On</b> to make the WAN1 connection being activated always.	
	Always On <mark>↓</mark> Always On Backup	
	<b>Load Balance</b> : Check this box to enable <b>auto</b> load balance function for such WAN interface.	
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.	
Backup Type	If you choose <b>Backup</b> as the <b>Active Mode</b> , Backup WAN will be changed into <b>Backup Type</b> . You have to specify which role the WAN interface should play if you want to backup multiple WANs. However, ignore this setting if you want to backup a single WAN.	
	Active Mode: Backup  WAN 1 WAN 2 WAN 3	
	Backup Type (Only if acting as backup for multiple WAN):	
	When any of selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.	
	When all of selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.	

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

# WAN2 with Ethernet

WAN2 is fixed with physical mode of Ethernet.

### WAN >> General Setup

WAN 2	
Enable:	Yes 🛩
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 🐱
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion :	Disable 👻 (Please configure Internet Access setting first)
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Backup 🔽 Load Balance: 🗹
	WAN 1 WAN 2 WAN 3
Backup Type (Only if acting as backup for multiple WAN):	When any of selected WAN disconnect     When all of selected WAN disconnect
Note:Line Speed only used for load b	palance mode: according to Line Speed

OK Cancel

Item	Description		
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.		
Display Name	Type the description for such WAN interface.		
Physical Mode	Display the physical mode of such WAN interface.		
Physical type	You can change the physical type for WAN2 or choose <b>Auto negotiation</b> for determined by the system.		
	Physical Type: Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex		
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load</b> <b>Balance Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.		
VLAN Tag insertion	<b>Enable</b> – Enable the function of VLAN with tag.		
	The router will add specific VLAN number to all packets on the WAN while sending them out.		
	Please type the tag value and specify the priority for the packets sending by WAN1.		
	<b>Disable</b> – Disable the function of VLAN with tag.		
	Tag value – Type the value as the VLAN ID number. The		



	range is form 0 to 4095.		
	<b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.		
Active Mode	Choose Always On to make such WAN connection being activated always. Always On Backup Load Balance: Check this box to enable auto load balance function for such WAN interface.		
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.		
Backup Type	If you choose <b>Backup</b> as the <b>Active Mode</b> , Backup WAN will be changed into <b>Backup Type</b> . You have to specify which role the WAN interface should play if you want to backup multiple WANs. However, ignore this setting if you want to backup a single WAN.		
	Active Mode: Backup V WAN 1 WAN 2 WAN 3 When any of selected WAN disconnect (Only if acting as backup for multiple WAN):		
	When any of selected WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.		
	When all of selected WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.		

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

# WAN3 with USB

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

WAN >> General Setup

WAN 3	
Enable:	Yes 💌
Display Name:	
Physical Mode: Line Speed(Kbps):	USB
DownLink	0
UpLink	0
Active Mode:	Backup 💌 Load Balance: 🗹
	🗌 WAN 1 🗌 WAN 2 🗌 WAN 3
Backup Type (Only if acting as backup for multiple WAN):	When any of selected WAN disconnect     When all of selected WAN disconnect
Physical Mode: Line Speed(Kbps): DownLink UpLink Active Mode: Backup Type (Only if acting as backup for multiple WAN):	D D Backup ♥ Load Balance: ♥ WAN 1 ₩AN 2 ₩AN 3 When any of selected WAN disconnect

Note:Line Speed only used for load balance mode: according to Line Speed

OK Cancel

Item	Description
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
Display Name	Type the description for such WAN interface.
Physical Mode	Display the physical mode of such WAN interface.
Physical type	In such WAN interface, no type can be selected.
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load</b> <b>Balance Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	Choose Always On to make such WAN connection being activated always. Always On ✓ Always On ✓ Always On ✓ Backup Load Balance: Check this box to enable auto load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.

Backup Type	will be changed into <b>Back</b> which role the WAN inter	the Active Mode, Backup WAN <b>cup Type</b> . You have to specify face should play if you want to However, ignore this setting if you VAN.	
	Send <u>Mail Alert</u> if line drops out Active Mode:	Backup	
	Backup Type (Only if acting as backup for multiple WAN):	<ul> <li>When any of selected WAN disconnect</li> <li>When all of selected WAN disconnect</li> </ul>	
	When any of selected WAN disconnect – Such I WAN will be activated when any master WAN in disconnects.		
	When all of selected WA WAN will be activated or interfaces disconnect.	N disconnect – Such backup Ily when all master WAN	

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

### 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 Index Display Name Physical Mode Access Mode WAN1 ADSL PPPoE / PPPoA × Details Page IPv6 None WAN2 Ethernet Details Page IPv6 PPPoE / PPPoA MPoA (RFC1483/2684) WAN3 USB None Y Details Page IPv6

Note : Only one WAN can support IPv6.

#### WAN >> Internet Access

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

#### WAN >> Internet Access

Index Display Na	ime Physical Mode	Access Mode	
WAN1	ADSL	None	Details Page IPv6
WAN2	Ethernet	Static or Dynamic IP 🛛 👻	Details Page IPv6
WAN3	USB	None	Details Page IPv6
ote : Only one WAN	can support IPv6.	None 3G/4G USB Modem(PPP mode) 4G USB Modem(DHCP mode)	

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)/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 according to the access mode that you choose in WAN interface
IPv6	<ul><li>This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface.</li><li>If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.</li></ul>
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.

# **Dray** Tek

WAN >> Internet Access
DHCP Client Options Status
Options List
Enable Interface Option Type Data
Enable: @
Interface: WAN1 WAN2 WAN3 WAN5 WAN6 WAN7
Option Number:
DataType:  String  Raw Byte in Hex. (Example of Raw Byte Data Type Input Format:2f T0 61 74 68 31)
Data: Add Update Delete
Note:
Option 61 has been given a default value. You can configure option 61(Client Identifier) in "WAN >> Interface Access" page. If you choose to configure option 61 here, the settings in "WAN >> Interface Access,Details Darce" will be exemptified by the exemptified of the exemptifie
Page" will be overwritten. Option 12 is reserved, you cannot configure it here but you can configure it in "Router Name" field of "WAN >> Interface 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.
<b>Interface</b> – Specify the WAN interface(s) that will be overwritten by such function. WAN5 ~ WAN7 can be located under <b>WAN&gt;&gt;Multi-PVCs</b> .
<b>Option Number</b> – Type a number for such function.
<b>Note:</b> If you choose to configure option 61 here, the detailed settings in WAN>>Interface Access will be overwritten.
<b>DataType</b> – Choose the type (ASCII or Hex) for the data t be stored.
<b>Data</b> – Type the content of the data to be processed by the function of DHCP option.

# Details Page for PPPoE/PPPoA in WAN1

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

PPPoE / PPPoA	MPoA (RFC	1483/2684)	IPv6
Enable Dis     Dis     DSL Modem Settings Multi-PVC channel VPI VCI Encapsulating Type Protocol Modulation PPPoE Pass-through     For Wireless LAN WAN Connection Detectio Mode	Channel 1 V Channel 1 V 33 LLC/SNAP V PPPoE V Multimode V	Fixed IP O Yes O M Fixed IP Address O Default MAC Addres MAC Address: 00 .50 Index(1-15) in <u>Schedule</u>	PAP or CHAP  PAP o
Ping IP TTL: Bridge Mode Enable Bridge Mode		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, ,, ,, ,, ,, , _, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, , ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, , ,, , ,, , ,, , ,, , , ,, , , , , , , , , , , , , , , , , , , ,	J []

WAN >> Internet Access

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



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



			ser name (maximum 63	
		provided by the ISP i		1
	<b>Password</b> – Type in the password provided by ISP in this field.			
		you want to connect t	AP only or PAP or CHA to Internet all the time, yo	
		•	for breaking down the	
			e time without any action.	
IP Address From ISP	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your I provides service to always assign you the same IP addr whenever you request. In this case, you can fill in this I address in the Fixed IP field. Please contact your ISP b you want to use this function.			
	WAN IP A	l <b>ias</b> - If you have mu	ltiple public IP addresses	
			the WAN interface, plea	
		P Alias. You can set in current one you ar	up to 8 public IP addresse	S
	State in the initial initia initial initial initial initial initial initial initi	•		
	() 192.168.1.5/doo	:/wipalias.htm	0	
	WAN1 IP Alia	s ( Multi-NAT )		
	Index Enab		Join NAT IP Pool	
	1. 🗹			
	2. 🗹	0.0.0		
	3. 🗖			
	4.	0.0.0		
	5.			
	6.	0.0.0		
	7.	0.0.0		
	8.	0.0.0.0		
		OK Clear All	Close	
			function and type in a	
		ress in the box of <b>Fi</b>		
	<b>Default MAC Address</b> – You can use <b>Default MAC</b> <b>Address</b> or specify another MAC address by typing on the boxes of MAC Address for the router.			
			e the MAC address for the	e
	router manu	• •		
	of time sche set previous	dule for your reques ly in <b>Applications</b> >	- You can type in four se t. All the schedules can be > <b>Schedule</b> web page and have set in that web page	e d

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



## Details Page for MPoA (RFC1483/2684) in WAN1

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** as the accessing protocol of the Internet, select **MPoA** from the **WAN>>Internet Access >>WAN1** page. The following web page will appear.

PPPoE / PPPoA	MPoA (RF	C1483/2684)	IPv6
🔍 Enable 🛛 🖲 Dis	able	WAN IP Network Settings	WAN IP Alias
DSL Modem Settings		Obtain an IP address a	utomatically
Multi-PVC channel	Channel 2	Router Name	Vigor
Encapsulation		Domain Name	
	3 Bridged IP LLC	* : Required for some	ISPs
		DHCP Client Identifier for s	ome ISP
VPI	8	🔲 Enable	
VCI	88	Username	
Modulation	Multimode 🛛 🔽	Password	
		Specify an IP address	
WAN Connection Detection		IP Address	202.211.100.10
Mode	ARP Detect 💌	Subnet Mask	255.255.255.0
Ping IP		Gateway IP Address	
TTL:			
RIP Protocol		🗌 🖲 Default MAC Addres	s
Enable RIP		🔹 🔍 Specify a MAC Addre	355
		MAC Address: 00 ·10	D AA A8 42 5
Bridge Mode			
🔲 Enable Bridge Mod	e	DNS Server IP Address	
		Primary IP Address	8.8.8.8
		Secondary IP Address	8.8.4.4

WAN >> Internet Access

Item	Description
Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >>Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	<b>VPI</b> - Type in the value provided by ISP.
	<b>VCI</b> - Type in the value provided by ISP.
	<b>Encapsulating</b> - Drop down the list to choose the type provided by ISP.
	<b>Modulation</b> –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	<ul> <li>Such function allows you to verify whether network</li> <li>connection is alive or not through ARP Detect or Ping</li> <li>Detect.</li> <li>Mode – Choose ARP Detect or Ping Detect for the system</li> <li>to execute for WAN detection.</li> </ul>	
	<ul> <li>Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</li> <li>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</li> </ul>	
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.	
Bridge Mode	If you choose <b>Bridged IP</b> as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.	
WAN IP Network Settings	<ul> <li>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</li> <li>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.</li> </ul>	

) 192.168	3.1.5/doc/wipali	ias.htm	C
	P Alias ( Mu	Ilti-NAT ) Aux. WAN IP	Join NAT IP Pool
Index	Enable V	AUX. WAN IP	JOIN NAT IP POOL
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	
htain	an IP a	OK Clear All	Close
	he IP ad	ddress automatically	lly – Click this but
	he IP ad <b>Rou</b> t	ddress automatica	lly – Click this but
	he IP ad Rout provi Dom	<b>ddress automatica</b> dress automatically <b>ter Name</b> – Type in	Ily – Click this but 1 the router name
tain ti ●	he IP ad Rout provi Dom you l	ddress automatica dress automatically ter Name – Type in ided by ISP. aain Name – Type i	Illy – Click this but 1 the router name n the domain name
tain ti ●	he IP ad Rout provi Dom you l Client I Enal	ddress automatica dress automatically ter Name – Type in ided by ISP. tain Name – Type i have assigned.	Ily – Click this but h the router name n the domain name ISP to specify usernam

• **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.

- **IP** Address Type in the private IP address.
- **Subnet Mask** Type in the subnet mask.
- Gateway IP Address Type in gateway IP address.

**Default MAC Address** – Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.

**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 necessary,
	type in secondary IP address for necessity in the future.

### **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.

#### WAN >> Internet Access

O Enable 💿 Disable		
ISP Access Setup         Service Name (Optional)         Username         Password         Index(1-15) in Schedule Setup:         =>         ,       ,         WAN Connection Detection         Mode       ARP Detect          Ping IP         TTL:         MTU       1442 (Max:1492)	Idle Timeout 1 IP Address Assignment Method WAN IP Alias Fixed IP: O Yes O No (Dyn Fixed IP Address O Default MAC Address O Specify a MAC Address	

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



	TTL (Time	· • •	value for your reference.	
	TTL value is set by telnet command.			
MTU	It means Max Transmit Unit for packet. The default setting is 1442.			
PPP/MP Setup	<ul> <li>PPP Authentication – Select PAP only or PAP or CHAP for PPP. If you want to connect to Internet all the time, you can check Always On.</li> <li>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</li> </ul>			
IP Address Assignment Method (IPCP)	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 to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click <b>OK</b> to exit the dialog.			
	🛃 未命名 - 楓樹	•		
	(© 192.168.1.5/doc/wipalias.htm (©) WAN1 IP Alias ( Multi-NAT )			
	Index Enab		Join NAT IP Pool	
	1. 🗹			
	2. 🗹	0.0.0.0		
	з. 🗆	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	
	fixed IP add	ress in the box of <b>Fi</b> x		
	Address or		an use <b>Default MAC</b> C address by typing on the puter.	
	Specify a M router manu	• •	e the MAC address for the	

After finishing all the settings here, please click  $\mathbf{O}\mathbf{K}$  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	<ul> <li>Disable</li> </ul>	WAN IP	Network Settings	WAN IP Alias
Keep WAN Conne Enable PING PING to the IP PING Interval WAN Connection Mode	) to keep alive 0 minute(s)	Obt Route Doma	ain an IP address a er Name in Name quired for some I lient Identifier for so able	utomatically * * * * * * * * * * * * * * *
Ping IP TTL: MTU	1442 (Max:1500)	- IP Add	cify an IP address	
RIP Protocol		● Def	vay IP Address fault MAC Address ecify a MAC Addre Address: 00 ·50	- :55
		Primary	r <b>ver IP Address</b> / IP Address lary IP Address	8.8.8.8 8.8.4.4

WAN >> Internet Access

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



WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.			
	<ul> <li>Ping IP – If you choose Ping Detect as detection mode, y have to type IP address in this field for pinging.</li> <li>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</li> </ul>			
MTU	It means Max Transmit Unit for packet. The default setting is 1442.			
RIP Protocol	Routing Information Protocol is abbreviated as RIP(RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.			
Settings	<ul> <li>This group allows you to obtain an IP address automatical and allows you type in IP address manually.</li> <li>WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, ple use WAN IP Alias. You can set up to 8 public IP address other than the current one you are using.</li> </ul>			
	★ 未命名 - 楓樹瀏覽器 ⑤ 192.168.1.5/doc/wipalias.htm			
	WAN1 IP Alias (Multi-NAT)			
	Index     Enable     Aux. WAN IP     Join NAT IP Pool       1.     Image: Comparison of the second sec			
	1.     ✓       2.     ✓			
	3.			
	4. 0.0.0.0			
	5. 0.0.0.0			
	6. 0.0.0.0			
	7. 0.0.0.0			
	8. 0.0.0.0			
	OK Clear All Close			
	<b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically if you want to use <b>Dynamic IP</b> mode.			
	• <b>Router Name</b> : Type in the router name provided by ISP.			
	• <b>Domain Name</b> : Type in the domain name that you have assigned.			
	<ul> <li>DHCP Client Identifier for some ISP</li> <li>Enable: Check the box to specify username and password as the DHCP client identifier for some</li> </ul>			

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

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

# Details Page for PPTP/L2TP in WAN2

WAN >> Internet Access

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

PPPoE	Static or Dynamic IP	PPTP/L21	P	IPv6
Server Addres Specify Gatev ISP Access Set Username Password	vay IP Address	PPP Setup PPP Authentication Idle Timeout IP Address Assignment WAN IP Alias Fixed IP: Yes Fixed IP Address WAN IP Network Setting Obtain an IP add Specify an IP add IP Address Subnet Mask	-1 Method ( ) No (Dyn <b>Js</b> ress auto	namic IP)

Detailed explanation is shown below:

Item	Description
PPTP/L2TP	Enable PPTP- Click this radio button to enable a PPTP



	client to esta interface.	blish a tunnel to a DS	L modem on the WAN		
	<b>Enable L2TP</b> - Click this radio button to enable a L2T client to establish a tunnel to a DSL modem on the WA interface.				
	<b>Disable</b> – Cl through PPT		o close the connection		
		ress - Specify the IP a enable PPTP/L2TP c	ddress of the PPTP/L21 lient mode.		
	<b>Specify Gateway IP Address</b> – Specify the gateway IP address for DHCP server.				
ISP Access Setup	Username - field.	Type in the username	provided by ISP in this		
	<b>Password</b> -Type in the password provided by ISP in this field.				
	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.				
MTU	It means Max Transmit Unit for packet. The default setting is 1442.				
PPP Setup	<ul> <li>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</li> <li>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</li> </ul>				
IP Address Assignment Method(IPCP)	<b>WAN IP Alias</b> - If you have multiple public IP addresses and would like to utilize them on the WAN interface, pleas use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.				
	중 未命名 - 楓樹都 ◎ 192.168.1.5/doc				
	WAN1 IP Alias				
	Index Enabl	· · · · · ·	Join NAT IP Pool		
	1. 🗹				
	2. 🗹	0.0.0.0			
	з. 🗆	0.0.0			
	4. 🗆	0.0.0			
	4. 🗌 5. 🗌	0.0.0.0			
	5. 🗆 6. 🗖	0.0.0.0			
	5.        6.        7.	0.0.0.0			
	5. 🗆 6. 🗖	0.0.0.0			
	5.        6.        7.	0.0.0.0			
	5. 6. 7. 8. Fixed IP - U	OK Clear All			

	your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click <b>Yes</b> to use this function and type in a fixed IP address in the box. <b>Fixed IP Address -</b> Type a fixed IP address.
WAN IP Network Settings	<b>Obtain an IP address automatically</b> – Click this button to obtain the IP address automatically.
	<b>Specify an IP address</b> – Click this radio button to specify some data.
	<b>IP Address</b> – Type the IP address.
	<b>Subnet Mask</b> – Type the subnet mask.

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

# **Dray** Tek

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

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN2. The following web page will be shown.

N 3	
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#)
PPP Username	(Optional)
PPP Password	(Optional)
PPP Authentication	PAP or CHAP 🗸
Index(1-15) in <u>Schedule</u> Setup:	<u>.</u>
=>,,,	
WAN Connection Detection	
Mode	ARP Detect 🔛
Ping IP	
TTL:	

Item	Description
3G/4G USB Modem (PPP mode)	<b>Enable / Disable -</b> Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
	<b>SIM PIN code -</b> Type PIN code of the SIM card that will be used to access Internet.
	<b>Modem Initial String -</b> Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
	<b>APN Name -</b> APN means Access Point Name which is provided and required by some ISPs. Type the name and click <b>Apply</b> .
	<b>Modem Initial String2 -</b> The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings.
	<b>Modem Dial String -</b> Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
	<b>PPP Username -</b> Type the PPP username (optional).

	<b>PPP Password -</b> Type the PPP password (optional).
	<b>PPP Authentication</b> - Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.
	<b>Index (1-15) in Schedule Setup</b> - You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	<b>TTL</b> ( <b>Time to Live</b> ) – Displays value for your reference. TTL value is set by telnet command.

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

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

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

WAN >> Internet Access

13	Modem Support L
4G USB Modem(DHCP mode)	💿 Enable 🛛 Disable
SIM PIN code	
Network Mode	40/30/20 💌 (Default:4G/3G/2G)
APN Name	
MTU	1380 (Default:1380)
LTE software version LTE hardware version	
WAN Connection Detection	
Mode	ARP Detect 💌
Ping IP	
TTL:	

### Available settings are explained as follows:

Item	Description
4G USB Modem (DHCP mode)	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.



0

SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.		
	The maximum length of the PIN code you can set is 19 characters.		
Network Mode	Force Vigor router to connect Internet with the mode specified here. If you choose 4G/3G/2G as network mode, the router will choose a suitable one according to the actual wireless signal automatically.		
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click <b>Apply</b> . The maximum length of the name you can set is 47 characters.		
MTU	It means Max Transmit Unit for packet. The default setting is 1380.		
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.		
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.		
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.		
	<b>TTL (Time to Live)</b> – Displays value for your reference. TTL value is set by telnet command.		
Modem Support List	It lists all of the modems supported by such router. 46 Modem Support List		
	Last updated on 2013-03-26		
	Standard Brand Module Status		
	LTE LG VL600 Y		
	WIMAX Samsung swc-u200 Y		
	Y:Tested and is supported. M:Has not been tested but might be supported.		

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

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

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

WAN >> Internet Access

WAN 1
PPPoE / PPPoA MPoA (RFC1483/2684) IPv6
Internet Access Mode
Connection Type Offline 
OK Cancel

Details Page for IPv6 – PPP in WAN1/WAN2



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

No need to type any other information for PPP mode.

ΡΡΡοΕ / ΡΡΡοΑ	MPoA (RFC1483/2684)	IPv6
Internet Access Mode		
Connection Type	PPP 💌	
Note : IPv4 WAN setting sh	ould be <b>PPPoE</b> client.	

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

Physical Connect	ion			System Uptime: 0:0:30
	IPv4		IPv6	
LAN Status				
IP Address				
	300:200:21D:AAFF:F FF:FE7A:3E58/64 (L	E7A:3E58/64 (Global) ink)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
7	8	618	672	
WAN2 IPv6 Statu	5			
Enable	Mode	Up Time		
Yes	PPP	0:00:11		
IP			Gateway IP	
	300:200:21D:AAFF:F F:FE7A:3E5A/128 (L		FE80::90:1A00:242:AD52	
DNS IP				
2001:B000:10 2001:B000:10				
TX Packets	RX Packets	TX Bytes	RX Bytes	
7	4	544	616	

**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.

Online Status



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

ΡΡΡοΕ / ΡΡΡοΑ	MPoA (RFC1483/2684)	IPv6
Internet Access Mode		
Connection Type	TSPC	
TSPC Configuration		
Username		
Password		
Confirm Password		
Tunnel Broker		

Available settings are explained as follows:

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

Cancel

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

ΟK

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

	MD - A (DE C1402/2004)	ID-C
ΡΡΡοΕ / ΡΡΡοΑ	MPoA (RFC1483/2684)	IPv6
nternet Access Mode		
Connection Type	AICCU	
AICCU Configuration		
🗌 Always On		
Username		
Password		
Confirm Password		
Tunnel Broker	tic.sixxs.net	
Subnet Prefix		/

### Available settings are explained as follows:

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

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

# 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 / PPPoA	MPoA (RFC1483/2684)	IP∨6
nternet Access Mode		
onnection Type	DHCPv6 Client 🚩	
HCPv6 Client Configuratio	on	
Identity Association	💿 Prefix Delegation 🗢 Non-tempo	rary Address
IAID (Identity Associatio	on ID) 11570169	

UK Cancel
-----------

Available settings are explained as follows:

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

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

**Dray** Tek

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

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

WAN	>>	Internet	Access
			100000

PPPoE / PPPoA	MPoA (RF	C1483/2684)	IP∨6
Internet Access Mode			
Connection Type		Static IPv6 🛛 👻	
Static IPv6 Address configu	ration		
IPv6 Address		/ Prefix Lengt	:h
			Add Delete
Current IPv6 Address Tabl	e		
			X
Static IPv6 Gateway configu IPv6 Gateway Address	ıration		
-		7	
::			

Available settings are explained as follows:

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

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

### 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.

>> Internet Access		
1		
PPPoE / PPPoA	MPoA (RFC1483/2684)	IPv6
Internet Access Mode		
Connection Type	6in4 Static Tunn	el 💌
6in4 Static Tunnel		
Remote Endpoint IPv4 Address		
6in4 IPv6 Address		/ 64 (default:64)
LAN Routed Prefix		/ 64 (default:64)
Tunnel TTL	255 (default:255)	
	OK Cancel	

Available settings are explained as follows:

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

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

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

#### **Online Status**

Physical Connect	ion			System Uptime: 0day 0:4:16
IPv4		IPv6		A REAL PROPERTY OF THE DESIGN STATE
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	
	-10:83E4::2131/64 (G 51D/128 (Link)	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 >> Internet Access			0
WAN 1			
ΡΡΡοΕ / ΡΡΡοΑ	MPoA (RFC1483/2684)	IPv6	
Internet Access Mode			
Connection Type	6rd 💌		
6rd Settings			
6rd Mode	🔾 Auto 6rd 🛛 🥑 Static 6rd		
Static 6rd Settings			
IPv4 Border Relay:			
IPv4 Mask Length:	0		
6rd Prefix:			
6rd Prefix Length:	0		
	OK Cancel		

Item	Description	
6rd Mode	<ul> <li>Auto 6rd – Retrieve 6rd prefix automatically from 6rd service provider. The IPv4 WAN must be set as "DHCP".</li> <li>Static 6rd - Set 6rd options manually.</li> </ul>	
IPv4 Border Relay	Type the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.	



IPv4 Mask Length	Type a number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. It may be any value between 0 and 32.
6rd Prefix	Type the 6rd IPv6 address.
6rd Prefix Length	Type the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.

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

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

### **Online Status**

Physical Connection IPv4				System Uptime: 0day 0:9:15
			IPv6	
LAN Status				
IP Address				
	55:1D00:21D:AAFF: FF:FE83:11B4/64 (		obal)	
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			Gateway IP	
(Global)	5:1D01:21D:AAFF: 51D/128 (Link)	FE83:11B5/128		
TX Packets	RX Packets	TX Bytes	RX Bytes	
13	29	967	2620	

### 3.1.4 Multi-PVCs

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

### General

WAN >> Multi-PVCs

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

General ATM QoS Port-based Bridge					PVC to PVC Binding/Add Tag			
Channel		Enable	VPI	VCI	QoS T	ype	Protocol	Encapsulation
1.		<b>~</b>	0	33	UBR	*	PPPoE 💌	LLC/SNAP 💌
2.		<b>~</b>	0	88	UBR	*	MPoA 🔽	1483 Bridged IP LLC 🛛 💌
з.			1	43	UBR	~	PPPoA 🔽	VC MUX
4.			1	44	UBR	~	PPPoA 🔽	VC MUX
5.	WAN		1	45	UBR	*	PPPoA 🔽	VC MUX
6.	WAN		1	46	UBR	~	PPPoA 🔽	VC MUX
7.	<u>WAN</u>		1	47	UBR	~	PPPoA 🔽	VC MUX
8.			1	48	UBR	~	PPPoA 🔽	VC MUX

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

OK Clear Cancel

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



	PPPoE V PPPoE MPoA
Encapsulation	Choose a proper type for this channel. The types will be different according to the protocol setting that you choose. 1483 Route IP LLC 1483 Bridged IP LLC 1483 Bridged IP LLC 1483 Bridged IP VC-Mux 1483 Route IP VC-Mux 1483 Routed IP VC-Mux(IPoA) 1483 Bridged IP(IPoE)

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

WAN for Router-borne Application: 🛛 Management 💌	
🔘 Enable 💿 Disable	
DSL Modern Settings	
VPI 1 QoS Type	UBR 💌 PVC Binding Disable 💌
VCI 45 Protocol	PPPoA 🐱 Add Tag 🗌 0
Encapsulation	VC MUX
WAN Connection Detection	
Mode ARP Dete	ct 🐱
Ping IP	
TTL:	
PPPoE/PPPoA Client	MPoA (RFC1483/2684)
ISP Access Setup	Obtain an IP address automatically
ISP Name	Router Name Vigor *
Username	Domain Name *
Password	*: Required for some ISPs
PPP Authentication PAP or CHAP 🔽	Specify an IP address
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 8.8.8.8
	Secondary IP Address 8.8.4.4
ОК	Cancel

WAN >> Multi-PVCs >> PVC Channel 5

# **Dray** Tek

Available settings are explained as follows:

Item	Description
WAN for Router-borne Application	Choose the router service for channel 5, 6 or 7. <b>Management</b> - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR069.
	<ul> <li>VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this PVC will be effective for VoIP data transmitting and receiving.</li> <li>IPTV - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.</li> </ul>

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

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

### ATM QoS

WAN >> Multi-PVCs

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

ieneral	ATM QoS	Port-based Bridge	PVC to PVC	Binding/Add Tag
Channel	QoS Type	PCR	SCR	MBS
1.	UBR 🔽	0	0	0
2.	UBR 💌	0	0	0
з.	UBR 💌	0	0	0
4.	UBR 💌	0	0	0
5.	UBR 💌	0	0	0
6.	UBR 💌	0	0	0
7.	UBR 💌	0	0	0
8.	UBR 💌	0	0	0

2.PCR(max) = ADSL Up Speed / 53 / 8.

Clear Cancel ΟK

Item	Description				
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides.				



PCR	It represents Peak Cell Rate. The default setting is "0".
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.

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

## **Port-based Bridge**

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

WAN >> Multi-PVCs

neral ATM	QoS P	ort-based E	Bridge		PVC to P	VC Binding/Add Tag
Channel	Enable	P1	P2	P3	P4	Service Type
1.						Normal 💌
2.						Normal 💌
з.						Normal 💌
4.						Normal 💌
5.						Normal 💌
6.						Normal 💌
7.						Normal 💌
8.						IGMP 💌

Cancel

(	OK	Clear
Available settings are explained	ed as follo	ws:

Item	Description	
Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT using.	
P1 to P4	It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8.	
Service Type	Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. Such feature is used for specific application. Please choose <b>Normal</b> as the <b>Service Type</b> .	
	Normal – It means that the PVC can accept all packets. IGMP –It means that such PVC can accept IGMP packets only. Such type just meets a specific environment on some ISPs. Data and IGMP packets will be transmitted and received with different PVC.	

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

### PVC to PVC Binding/Add Tag

This feature can direct certain services (such as Internet, IPTV and so on) from other channels into a single channel.

Multi-PVCs				
General	ATM QoS	Port-based Bridge	PVC to PVC B	inding/Add Tag
Channe	÷I	PVC Binding	Add Tag	Priority
1.		Disable 💌		0
2.		Disable 💙	0	0
з.		Disable 💌	0	0
4.		Disable 1	0	0
5.		2 3	0	0
6.		4 5	0	0
7.		6		0
8.		8	0	0

WAN >> Multi-PVCs

Note: Multiple channels may use the same channel link through the PVC Binding configuration. PVC to PVC Binding only supports PPPoE and MPoA 1483 Bridge mode.



Available settings are explained as follows:

Item	Description
PVC Binding	Data transmitted through the selected channel will be redirected and transmitted via the channel configured in the field of PVC Binding.
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

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

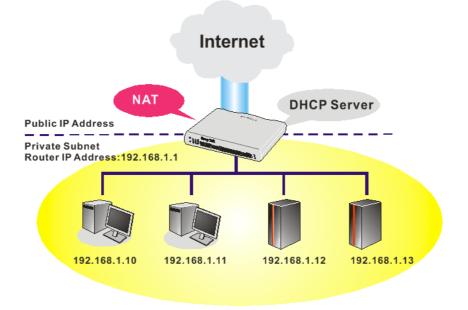
# 3.2 LAN

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.



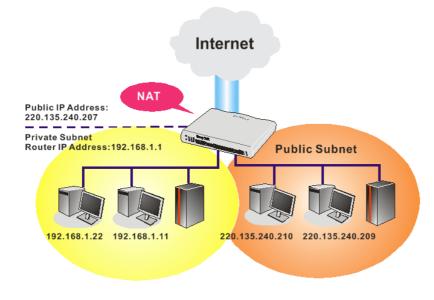
### 3.2.1 Basics of LAN

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.

**Dray** Tek



### What is Routing Information Protocol (RIP)

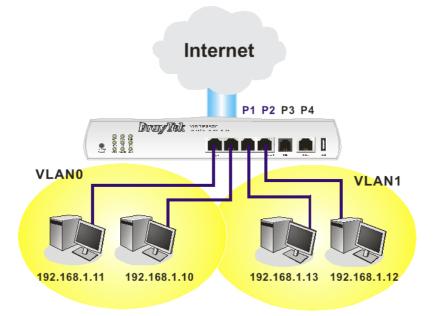
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### What is Static Route

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

### What are Virtual LANs and Rate Control

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



# **Dray** Tek

# 3.2.2 General Setup

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

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN4). 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 – LAN4 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		1	192.168.2.1	Details Page	
LAN 3		1	192.168.3.1	Details Page	
LAN 4		1	192.168.4.1	Details Page	
IP Routed Subnet		1	192.168.0.1	Details Page	

Advanced You can configure DHCP options here.

Force router to use "DNS server IP address" settings specified in LAN1
 Inter-LAN Routing

Inter-LAN Notiting				
Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	1			
LAN 2		<b>V</b>		
LAN 3			1	
LAN 4				<b>V</b>

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



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

	LAN >> General Setup
	DHCP Options Status O Enable  O Disable
	Options List
	Index Option Number Ascii/Hex Data
	Option Number:
	DataType:      O Ascii O Hex (Example of Hex Data Type Input Format:0xff 0x00 0xc0 0xa8)  Data:
	Add Delete
	Note: Maximum number of custom DHCP option is five.
	OK
	<b>Enable/Disable</b> – Enable/Disable the function of DHCP
	Option. Each DHCP option is composed by an option
	number with data. For example,
	Option number:100
	Data: abcd
	When such function is enabled, the specified values for
	DHCP option will be seen in DHCP reply packets.
	<b>Option Number</b> – Type a number for such function.
	<b>DataType</b> – Choose the type (ASCII or Hex) for the data to
	be stored.
	<b>Data</b> – Type the content of the data to be processed by the
	function of DHCP option.
Force router to use "DNS	Force Vigor router to use DNS servers configured in
server IP address"	LAN1/LAN2/LAN3/LAN4 instead of DNS servers given
settings as specified in	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).

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

To configure LAN 1 ~ LAN 4, or IP Routed Subnet, simply click **Details Page** to open the settings page.

# **Details Page for LAN1**

LAN1 is the default configuration for basic host connection.

#### LAN >> General Setup

LAN 1 Ethernet TCP / IP	and DHCP Setup	LAN 1 IPv6 Setup		
Network Configuration		DHCP Server Configuratio	n	
For NAT Usage		💿 Enable Server 🔘 Di	sable Server	
IP Address	192.168.1.1	Enable Relay Agent		
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
		IP Pool Counts	200	
RIP Protocol Control	Disable 🔽 nable LAN shouldn't be	Gateway IP Address	192.168.1.1	
the same subnet.	nable LAN Shoulunit be	" Lease Time	86400	(s)
		🗹 Retrieve IPs from ir	active clients pe	eriodically
		DNS Server IP Address		
		Primary IP Address		
		Secondary IP Address		
		OK		

Item	Description	
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	<b>Disable -</b> deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)	
	<b>Enable</b> – activate the RIP protocol.	
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.	
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.	
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.	
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.	
	<b>Enable Relay Agent</b> –Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.	
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.	
	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.
	<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
	<b>Lease Time</b> – Enter the time to determine how long the IP address assigned by DHCP server can be used.
	<b>Retrieve IPs from inactive clients periodically</b> – 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 Configuration	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	<b>Primary IP Address -</b> You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
	<b>Secondary IP Address -</b> You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
	The default DNS Server IP address can be found via Online Status:
	System Status         System Uptime: 71:47:46           LAN Status         Primary DNS: 194.109.6.66         Secondary DNS: 168.95.1.1           IP Address         TX Packets         RX Packets           192.168.1.1         347390         214004
	If both the Primary IP and Secondary IP Address fields are left empty, the router will use the DNS server assigned by ISP. If not, the router will assign its own IP address to local users as a DNS proxy server.
	<b>Force router to use address for DNS-</b> Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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



### Details Page for LAN1 – IPv6 Setup

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

Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup	
RADVD Configuration		
◯ Enable 🛛 💿 Disable		
Advertisement Lifetime 1800	Seconds (Range : 600 - 9000)	
DHCPv6 Server Configuration		
◯ Enable Server 💿 Disable 🤅	Server	
Start IPv6 Address		]
End IPv6 Address		]
DNS Server IPv6 Address		_
Primary DNS Server		]
Secondary DNS Server		]
Static IPv6 Address configuration IPv6 Address Current IPv6 Address Table Index IPv6 Address/Prefix 1 FE80::250:7FFF:FEEA:		Delete

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

Item	Description
RADVD Configuration	<ul> <li>Enable – Click it to enable RADVD server. The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.</li> <li>Disable – Click it to disable RADVD server.</li> </ul>
	Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router

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

# Details Page for LAN2/LAN3/LAN4

LAN >> General Setup

Lan 2 Ethernet TCP / IP and	IDHCP Setup			
Network Configuration		DHCP Server Configuratio	n	
○Enable ⊙Disable		⊙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 & En the same subnet.	able LAN shouldn't be in	Gateway IP Address	192.168.2.1	
rne same subner.		Lease Time	259200 (s)	
		Retrieve IPs from inactive clients periodically		
		DNS Server IP Address		
		Primary IP Address		
		Secondary IP Address		
		ok ]		

Item	Description
Network Configuration	<b>Enable/Disable</b> - Click <b>Enable</b> to enable such configuration. Click <b>Disable</b> to disable such configuration.
	<b>For NAT Usage -</b> Click this radio button to invoke NAT function.
	<b>For Routing Usage -</b> Click this radio button to invoke this function.
	<b>IP Address -</b> Type in private IP address for connecting to a local private network (Default: 192.168.1.1).



	<b>Subnet Mask -</b> Type in an address code that determines the size of the network. (Default: 255.255.255.0/24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
	<b>Lease Time</b> – 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 Configuration	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	<b>Primary IP Address -</b> You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not

provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.			
<b>Secondary IP Address -</b> You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.			
The default DNS Server IP address can be found via Online Status:			
System Status         System Uptime: 71:47:46           LAN Status         Primary DNS:         194.109.6.66         Secondary DNS:         168.95.1.1           IP Address         TX Packets         RX Packets           192.168.1.1         347390         214004			
If both the Primary IP and Secondary IP Address fields are left empty, the router will use the DNS server assigned by ISP. If not, the router will assign its own IP address to local users as a DNS proxy server.			
<b>Force router to use address for DNS-</b> Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).			

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

# Details Page for IP Routed Subnet

LAN >> General Setup

TCP/IP and DHCP Setup for	ir Routeu Subilet				
Network Configuration		DHCP Set	rver Configuration		
OEnable ODisable		Start IP	Address		
For Routing Usage		IP Pool (	Counts	0	(max. 32)
IP Address	192.168.0.1	Lease Ti	ime	259200	) (s)
Subnet Mask	255.255.255.0		LAN Port	P1	
RIP Protocol Control	Disable 🗸	1	MAC Address		U F2
Note: Disable LAN & Enable LAN shouldn't be in the same subnet.		Index	Matched MAC Add	iress	given IP Address
		MAC A	ddress :	1-1	
			Add Delete	Edit	Cancel
		ok ]			

### TCP/IP and DHCP Setup for IP Routed Subnet

Item	Description
Network Configuration	<b>Enable/Disable -</b> Click <b>Enable</b> to enable such configuration. Click <b>Disable</b> to disable such configuration.
	For Routing Usage - Click this radio button to invoke this



	function.
	<b>IP Address -</b> Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask -</b> Type in an address code that determines the size of the network. (Default: 255.255.0/24).
	RIP Protocol Control –
	<b>Disable -</b> Deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	<b>Enable</b> – Activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. It the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Lease Time</b> - Enter the time to determine how long the IP address assigned by DHCP server can be used.
	<b>Use LAN Port</b> – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.
	Use MAC Address - Check such box to specify MAC address.
	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.
	<b>Add</b> – Type the MAC address in the boxes and click this button to add.
	<b>Delete</b> – Click it to delete the selected MAC address.
	Edit – Click it to edit the selected MAC address.
	<b>Cancel</b> – Click it to cancel the job of adding, deleting and

editing.	
----------	--

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

# 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	4	IPv6		Set	to Factory Default   View R	outing Table
Index	Destir	ation Address	Status	Index	Destination Address	Status
<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			
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  Ref: C - connected, S - static, R - RIP, * - default, ~ - private * 0.0.0.0/ 0.0.00 via 172.16.3.1, WAN1 C - 192.166.1.0/ 255.255.0 is directly connected, LAN C 172.16.3.0/ 255.255.255.0 is directly connected, WAN1			
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.			



# **Static Route for IPv6**

You can set up to 40 profiles for IPv6 static route.

#### LAN >> Static Route Setup

IPv	4	IPv6		Set to Fa	ctory Default   <u>View IPv6 R</u>	outing Table
Index	Destir	ation Address	Status	Index	Destination Address	Status
<u>1.</u>		::/0	×	<u>11.</u>	::/0	×
<u>2.</u>		::/0	×	<u>12.</u>	::/0	×
<u>3.</u>		::/0	×	<u>13.</u>	::/0	×
<u>4.</u>		::/0	×	<u>14.</u>	::/0	×
<u>5.</u>		::/0	×	<u>15.</u>	::/0	×
<u>6.</u>		::/0	×	<u>16.</u>	::/0	×
<u>7.</u>		::/0	×	<u>17.</u>	::/0	×
<u>8.</u>		::/0	×	<u>18.</u>	::/0	×
<u>9.</u>		::/0	×	<u>19.</u>	::/0	×
<u>10.</u>		::/0	×	<u>20.</u>	::/0	×
<< <u>1 - 20   2</u>	<u>21 - 40</u> >>					<u>Next</u> >>

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

### Each item is explained as follows:

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

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

#### LAN >> Static Route Setup

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

|--|



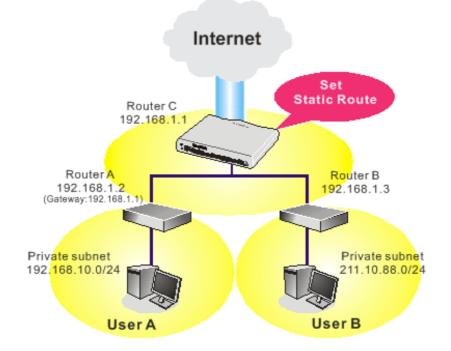
Enable	Click it to enable this profile.			
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.			
Gateway IPv6 Address	Type the gateway address for this entry.			
Network Interface	Use the drop down list to specify an interface for this static route.			

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

Here is an example 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.

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

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

ndex No. 2		
🗹 Enable		
	Destination IP Address	211.100.88.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.3
	Network Interface	LAN1 💌
Note: WAN5,	WAN6, WAN7 are router-borne WANs.	

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

Diagnostics >> View Routing Table

LAN >> Static Route Setup

LAN >> Static Route Setup

	Current Running Rou	ting Table	IPv6 Routing Tab	le	I	<u>Refresh</u>
Key:	C - connected, S	- static, R	- RIP, * - default, ~ -	private		~
*	0.0.0/	0.0.0.0	via 172.16.1.1	UAN2		
S~	192.168.10.0/	255.255.255.	0 via 192.168.1.2	LAN1		
C~	192.168.1.0/	255.255.255.	0 directly connected	LAN1		
С	172.16.0.0/	255.255.0.0	directly connected	WAN2		
ສ~	211.100.88.0/	255.255.255.	0 via 192.168.1.3	LAN1		
						~

Note: WAN5, WAN6, WAN7 are router-borne WANs.



# 3.2.4 VLAN (Multi-Subnet)

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

### Tagged VLAN

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

### **Port-Based VLAN**

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

LAN >> VLAN Configuration

VLAN Cor	LAN Configuration											
🗹 Enab	✓ Enable											
	LAN			Wireless LAN				VLAN Tag				
	P1	P2	Р3	<b>P4</b>	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0									LAN 1 🔽		0	0 🐱
VLAN1									LAN 1 💌		0	0 🐱
VLAN2									LAN 1 💌		0	0 🗸
VLAN3									LAN 1 💌		0	0 💌
VLAN4									LAN 1 🔽		0	0 🗸
VLAN5									LAN 1 🔽		0	0 💌
VLAN6									LAN 1 💌		0	0 🗸
VLAN7									LAN 1 🔽		0	0 🕶

Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;

2. The checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;

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

OK Clear Cancel

**Note:** Such page will be different slightly in accordance with the type of the router you have and settings in this page only applied to LAN port but not WAN port.

Item	Description					
Enable	Check this box to enable such function.					
LAN	<b>P1</b> – <b>P4</b> – Check the LAN port(s) to be grouped under the selected VLAN.					
Wireless LAN	<b>SSID1 – SSID4</b> – Check the SSID box(es) for the wireless					



	clients to be grouped under the selected VLAN.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address(es) that specified by the subnet.
VLAN Tag	<b>Enable</b> – Check it to enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the LAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN.
	<b>VID</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.
	<b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.
Permit untagged device in P1 to access router	It can help users to communicate with the router still even though configuring wrong VLAN tag setting. For Vigor router has one LAN physical port only, it is recommended to enable the management port (LAN 1) to ensure the data transmission is unimpeded.

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

Vigor2830 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.

**Dray** Tek

#### LAN >> VLAN Configuration

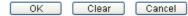
VLAN	Conf	igurat	ion

VLANCO	<u> </u>											
🗹 Enab	ole											
	LAN			Wireless LAN					VLAN Tag	J		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<b>V</b>	<b>~</b>	<b>~</b>	✓					LAN 1 🔽		0	0 🗸
VLAN1					<b>~</b>	<b>~</b>	<b>~</b>	<b>~</b>	LAN 2 🔽		0	0 🗸
VLAN2									LAN 3 🔽		0	0 🗸
VLAN3									LAN 1 🔽		0	0 🗸
VLAN4									LAN 1 💌		0	0 🗸
VLAN5									LAN 1 🔽		0	0 🗸
VLAN6									LAN 1 💌		0	0 🗸
VLAN7									LAN 1 🔽		0	0 🗸

Permit untagged device in P1 to access router

1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic.

2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected. 3. Each VID must be unique.



### 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.

General Setup					
Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2		<b>~</b>	192.168.2.1	Details Page	
LAN 3		<b>V</b>	192.168.3.1	Details Page	
LAN 4		<b>~</b>	192.168.4.1	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 🗔 🖂

Inter-		

LAN >> General Setup

inter Entrietting				
Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	$\checkmark$			
LAN 2	<ul> <li>Image: A set of the set of the</li></ul>	×		
LAN 3			<b>V</b>	
LAN 4				$\checkmark$

0K

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

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.

**Note:** As for the VLAN applications, refer to "Appendix I: VLAN Application on Vigor Router" for more detailed information.



# 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	ARP Table   <u>Select All</u>   <u>Sort</u>   <u>Refresh</u>   IP Bind List   <u>Select All</u>   <u>Sort</u>						
IP Address	Mac Address	Index I	P Address	Mac Address	<u>~</u>		
192.168.1.10	E0-CB-4E-DA-48-79						
	~						
Add or Update							
IP Address							
Mac Address							
Comment [					~		
				Show C	Comment		
	Add	Update (	Delete				

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

_		
	OK	
	00	

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



	ARP table information.						
Add and Update	<ul> <li>IP Address – Type the IP address that will be used for the specified MAC address.</li> <li>Mac Address – Type the MAC address that is used to bind with the assigned IP address.</li> </ul>						
	<b>Comment</b> – Type a brief description for the entry.						
	<b>Show Comment</b> – Check it to display the content of the comment.						
IP Bind List	It displays a list for the IP bind to MAC information.						
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .						
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 <b>IP Bind List</b> . Simply click and select the one, and click <b>Delete</b> . The selected item will be removed from the <b>IP Bind List</b> .						

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

### 3.2.6 LAN Port Mirror

LAN >> 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. Next, it is more convenient and easy to configure in user's interface. Last, connect a PC with Smart Monitor installed to the mirror port of this router to capture monitored information.

LAN Port Mirror				
Port Mirror:				
OEnable ODisa	ble			
Mirror port:				
OP2	ОРЗ	○ P4		
Mirrored port:				
<b>P</b> 1	<b>P</b> 2	🗖 РЗ	<b>P</b> 4	
Note :The selected	mirror port will only ser	e debug nurnoses and sho	uld not he used as a nar	t of the

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

OK

Available settings are explained as follows:

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

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

### 3.2.7 Wired 802.1x

IEEE 802.1x is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism for the device that is attached to a LAN or WLAN.

Wired 802.1x provides authentication for one network device on each LAN port. The RADIUS Server settings must be configured before enabling 802.1x because the EAP (Extensible Authentication Protocol) Authenticator relies on the RADIUS Server in its authentication process. Each LAN port with Wired 802.1x configured will only forward 802.1x packets and block all other packets until the authentication has successfully completed.

LAN	>>	W	ired	80	2.1	x

Wired 802.1x				
LAN 802.1x:				
Enable				
802.1x ports:				
□ P1	□ P2	🗆 РЗ	□ P4	

Please note that 802.1x enabled LAN ports will support EAPOL authentication for one network device only. Therefore,802.1x enabled LAN ports will have issues when connecting to a L2 switch. If you want 802.1x support for multiple network devices, please disable 802.1x here and configure 802.1x on the connecting switch. This feature supports PEAP and EAP-TLS.

OK

Available settings are explained as follows:

Item	Description			
Enable	Check the box to enable LAN 802.1x function.			
802.1x ports	After enabling the function, simply specify the LAN port(s) to apply such function.			

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

# 3.2.8 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	ible:		
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

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

Each item is explained as follows:
------------------------------------

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

# **Dray** Tek

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

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

💿 Disable					
◯ URL Redirect	http://				
	e.g. http://www.draytek.com Note : If the User Management application is enabled, it will override the Web Portal settings seen here.				
○ Message	<h1><font color="red">Vigor</font></h1> <h2> - Reliable connectivity</h2> <h2> - Robust firewall protection</h2> <h2> - Multi-site secure communication</h2>				
Applied Interfaces	(Max 255 characters)				
	LAN1 LAN2 LAN3 LAN4				
	SSID1 SSID2 SSID3 SSID4				

Cancel

ОK

Available settings are explained as follows:

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

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

# 3.3 Load-Balance /Route Policy

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

oad-B	oad-Balance/Route Policy   Set to Factory Default						<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	Mov Dow
1		Any	WAN1									Dow
2		Any	WAN1								<u>UP</u>	Dow
<u>3</u>		Any	WAN1								<u>UP</u>	<u>Dow</u>
<u>4</u>		Any	WAN1								<u>UP</u>	Dow
<u>5</u>		Any	WAN1								<u>UP</u>	<u>Dow</u>
<u>6</u>		Any	WAN1								<u>UP</u>	Dow
Z		Any	WAN1								<u>UP</u>	Dow
<u>8</u>		Any	WAN1								UP	Dow
<u>9</u>		Any	WAN1								<u>UP</u>	<u>Dow</u>
<u>10</u>		Any	WAN1								UP	Dow

◎ Wizard Mode: most frequently used settings in three pages

O Advance Mode: all settings in one page

### ΟK

Available settings are explained as follows:

Item	Description	
Index	Click the number of index to access into the configuration web page.	
Enable	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 <b>Up</b> or <b>Down</b> link to move the order of the policy.	



Wizard Mode	This mode will guide you to configure the common settings with several pages.
Advance Mode	This mode allows you to modify all the settings in one page.

Click **Index 1** to access into the following page for configuring load-balance policy. Here we choose **Advance Mode** as an example.

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:

Load-Balance/Route Policy

dex: 1 Criteria	
Load-Balance/Rou	ute Policy applies to packets that meet the following criteria
Source IP	O Any
	Src IP Start     Src IP End
Destination IP	O Any
	<ul> <li>Dest IP Start</li> <li>Dest IP End</li> </ul>
	< Back Next > Finish Cancel

Available settings are explained as follows:

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

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

#### Load-Balance/Route Policy

Index: 1 Interface			
Load-Balance/Route	Policy directs the pack	ets	; to the interface below
Interface	WAN1	~	
	LAN1	~	
	LAN2		
	LAN3		Back Next > Finish Cancel
	LAN4		
	IP Routed Subnet		
	WAN1	1	

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.

Load-Balance/Route Policy

Index: '	1 NAT or Rout	ing					
	Based on t Force NAT	he settings in the	e previous p	ages, we gues	s you wai	nt to have	:
	The current	t setting is:					
	۲	Force NAT					
	Õ	Force Routing					
				< Back	Next ≻	Finish	Cancel

Available settings are explained as follows:

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.

Load-Balance/Route Policy

Criteria	
Source IP	Any
Destination IP	192.168.1.6 ~ 192.168.1.66
Interface	
WAN1	
More options	
Force NAT	
	Sack Next > Finish C

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

Load-Ba	.oad-Balance/Route Policy											
Load-B	alance/R	oute Policy	/						Set	t to Fa	ctory D	efault
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<b>~</b>	Any	WAN1		Any	Any	Any	Any	Any	Any		<u>Down</u>
2		Any	WAN1								<u>UP</u>	<u>Down</u>
3		Any	WAN1								UP	Down

To use Advance Mode, do the following steps:

1. Click the Advance Mode radio button.

Load-Balance/Route Policy

2. Click **Index 1** to access into the following page.

Protocol	Any
Source IP	O Any
	Src IP Start Src IP End
	~
Destination IP	🔿 Any
	Dest IP Start Dest IP End
	~
	🔿 Any
Destination Port	Oest Port Start Dest Port End
	~
Send to if Criteria Matched	
Interface	WAN1
Gateway IP	Default Gateway
	🚫 Specific Gateway
More Options	
 Auto failover to other	. 141481
Packet Forwarding to WA	
via	Force Routing

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable this policy.

**Dray** Tek

Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.
Source IP	<ul> <li>Any – Any IP can be treated as the source IP.</li> <li>Src IP Start - Type the source IP start for the specified WAN interface.</li> <li>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.</li> </ul>
Destination IP	<ul> <li>Any – Any IP can be treated as the destination IP.</li> <li>Dest IP Start- Type the destination IP start for the specified WAN interface.</li> <li>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.</li> </ul>
Destination Port	<ul> <li>Any – Any port number can be treated as the destination port.</li> <li>Dest Port Start - Type the destination port start for the destination IP.</li> <li>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.</li> </ul>
Send to if criteria matched	<ul> <li>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.</li> <li>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.</li> </ul>
More options	<ul> <li>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.</li> <li>Packet Forwarding to WAN via – Choose Force NAT or Force Routing.</li> </ul>



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

Load-B	oad-Balance/Route Policy											
Load-B	alance/R	oute Policy	y						Set	t to Fa	ctory E	)efault
Index	: Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<b>~</b>	Any	WAN1		Any	Any	Any	Any	Any	Any		<u>Down</u>
2		Any	WAN1								UP	<u>Down</u>
3		Anv	WAN1								UP	Down

# 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.

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.

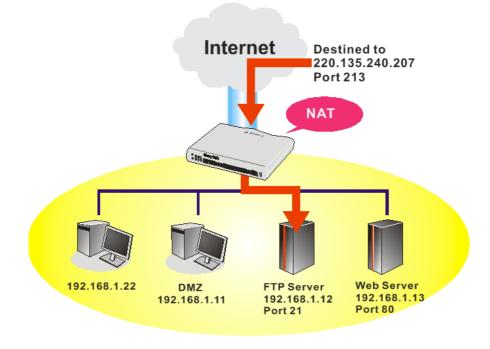
Below shows the menu items for NAT.



### **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 20 port-mapping entries for the internal hosts.

Port Red					Set to Facto	
Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
<u>1.</u>		All				Х
<u>2.</u>		All				х
<u>3.</u>		All				×
<u>4.</u>		All				×
<u>5.</u>		All				×
<u>6.</u>		All				×
<u>7.</u>		All				X
<u>8.</u>		All				×
<u>9.</u>		All				X
10.		All				×
< 1-10	11-20 >>					Next >>

#### 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		
Index Display the number of the profile.		
Service Name	Display the description of the specific network service.	
WAN InterfaceDisplay the WAN IP address used by the profile.		



Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified <b>Private IP and Port</b> 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.

ΝΛΤ	~~	Port	Rad	irection
NA I	~	FOIL	rea	nection

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

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

Private IP	Specify the private IP address of the internal host providing the service. If you choose <b>Range</b> as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.

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

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

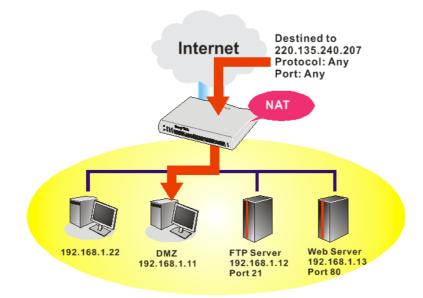
IPv4 Management Setup	Pv6 Management Setup		
Router Name	Management Port Setup		
	- 💿 User Define Ports	🔘 Def	ault Ports
🔲 Default:Disable Auto-Logout	Telnet Port	23	(Default: 23)
Internet Access Control	HTTP Port	80	(Default: 80)
Allow management from the Internet	HTTPS Port	443	(Default: 443)
FTP Server	FTP Port	21	(Default: 21)
HTTP Server	TR069 Port	8069	(Default: 8069)
HTTPS Server	SSH Port	22	(Default: 22)
🗹 Telnet Server	Estamol Device Control		
🗹 TR069 Server	External Device Control		iaa
SSH Server	No respond to Exte	ernai Dev	ice
Disable PING from the Internet			
LAN Access Control	-		
🗹 Allow management from LAN			
FTP Server			
HTTP Server			
HTTPS Server			

3.4.2 DMZ Host

System Maintenance >> Management

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:

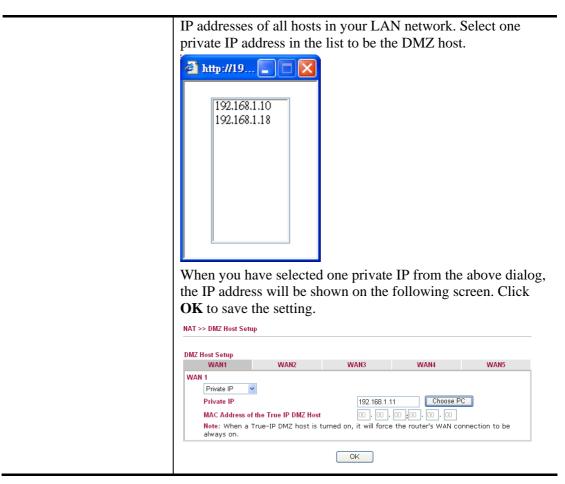
#### NAT >> DMZ Host Setup

WAN1	WAN2	WAN3
/AN 1		
None 💌		
Private IP		Choose PC
MAC Address of the True I	P DMZ Host 00 . 00	
<b>Note</b> : When a True-IP DN always on.	1Z host is turned on, it will for	ce the router's WAN connection to be

OK

Item	Description	
WAN 1 None	Choose <b>Private IP</b> or <b>Active True IP</b> first. <b>Active True IP</b> selection is available for WAN1 only. WAN 1 None Private IP Active True IP None	
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	





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

NAT >> DMZ Host Setup	

WAN1	WAN2	WAN3
WAN 2		
Enable	Private IP	
	0.0.0.0	Choose PC

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



#### NAT >> DMZ Host Setup

	WAN1		WAN2	WAN3
VAN 2 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.102	0.0.0	Choose PC
2.		172.16.3.200	0.0.0.0	Choose PC

Available settings are explained as follows:

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.
	Image: Walk isotropy
	WAN 2         Index         Enable         Aux. WAN IP         Private IP           1.         Image: Character and the state of the
	2. 172:16.3.200 0.0.0 Choose PC

After finishing all the settings here, please click  $\mathbf{OK}$  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

Index	Comment	WAN Interface	Local IP Address	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>				Х

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
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	Display the name for the defined network service.
WAN Interface	Display the WAN interface of the profile.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the <b>Inactive</b> or <b>Active</b> state.

Available settings are explained as follows:

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

Ind	еx	No.	1

🗹 Enable Oper						
	Comment	P2P				
	WAN Interface	WAN	1 💌			
	Local Computer	192.1	68.1.10	Cho	ose PC	
Protocol	Start Port	End Port		Protocol	Start Port	End Port
1. TCP 🛩	4500	4700	6.	💙	0	0
2. UDP 🔽	4500	4700	7.	💙	0	0
3 💌	0	0	8.	💙	0	0
4. 🛛 🕶	0	0	9.	💙	0	0
5 💙	0	0	10.	💙	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.
WAN Interface	Choose a WAN interface for this profile.
Local Computer	Enter the private IP address of the local host or click <b>Choose PC</b> to select one.
	<b>Choose PC -</b> Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be <b>TCP</b> , <b>UDP</b> , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

# 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

					-	
Index	Comment	<b>Triggering Protocol</b>	Triggering Port	Incoming Protocol	Incoming Port	Status
<u>1.</u>						x
<u>2.</u>						x
<u>3.</u>						x
<u>4.</u>						х
<u>5.</u>						х
<u>6.</u>						х
<u>7.</u>						х
<u>8.</u>						х
<u>9.</u>						х
<u>10.</u>						х

<< <u>1-10</u> | <u>11-20</u> >>

<u>Next</u> >:

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

Available settings are explained as follows:

Click the index number link to open the configuration page.



No. 1	
Enable	
Service	User Defined 💌
Comment	
Triggering Protocol	🗸
Triggering Port	
Incoming Protocol	💌
Incoming Port	
Note: The Triggering Port and Incoming Port 123-456,777-789 (legal),123-456,789 (legal)	
OK	ear Cancel

Item	Description
Enable	Check to enable this entry.
Service	Choose the <b>predefined</b> service to apply for such trigger profile. User Defined Weal 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 trigger 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.

	V TCP UDP TCP/UDP
Incoming Port	Type the port or port range for the incoming packets.

# 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:

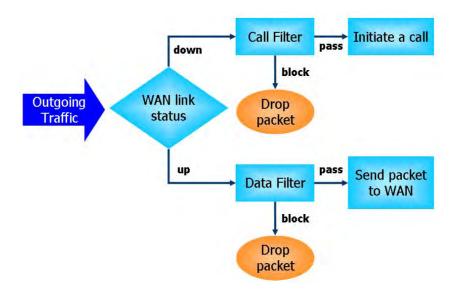
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

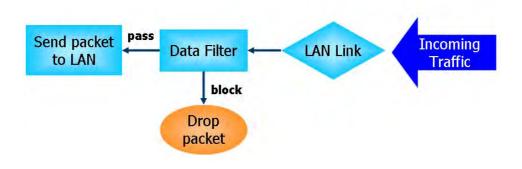
#### **IP Filters**

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.





### 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	
✓ Accept lar CS )		UDP or ICMP packets ( for some games, ex.

Available settings are explained as follows:

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

Cancel

ΟK

	fragmented UDP or ICMP Packets".
Enable Strict Security Firewall	Check the box to enable such function. All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router if such feature is enabled. If the firewall system does not have any response (pass or block) for these packets, such as no response coming from web content filter, then the router's firewall will block the packets directly.
Accept routing packet from WAN	<ul> <li>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.</li> <li>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</li> </ul>
	<ul> <li>translated by NAT.</li> <li><b>IPv4</b> - Check the box to make the incoming packets via IPv4 being accepted by such router. It is effective only for the packets routed but not for packets translated by NAT.</li> </ul>

### **Default Rule Page**

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

Firewall >> General Setup

General Setup	Default Rule			
Actions for defau	lt rule:			
Application		Action/Profile	Syslog	
Filter		Pass 💌		
Sessions Control		141 / 60000		
Quality of Service	<u>+</u>	None 💌		
Load-Balance pol	licy	Auto-Select 🐱		
<u>User Managemer</u>	<u>nt</u>	None 🗸 🗸		
APP Enforcement	<u>t</u>	None 😽		
URL Content Filter	Ľ	None 😽		
Web Content Filte	<u>۲</u>	None 💌		
Advance Settin(	9	Edit		

Item	Description
Filter	Select <b>Pass</b> or <b>Block</b> for the packets that do not match with the filter rules.



	Filter Pass V Pass Block	
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default	
Load-Balance Policy	Choose the WAN interface for applying Load-Balance Policy. Auto-Select WAN1 WAN2 WAN3	
User Management	Such item is available only when <b>Rule-Based</b> is selected in User <b>Management&gt;&gt;General Setup</b> . The general firewall rule will be applied to the user/user group/all users specified here. None User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile existed, <b>Create New User</b> or <b>Create New Group</b> item will appear for you to click to create a new one.	
APP Enforcement	Select an <b>APP Enforcement</b> profile for global IM/P2P application blocking. If there is no profile for you to select, please choose <b>[Create New]</b> from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the <b>APP Enforcement</b> profile selected here. For detailed information, refer to the section of <b>APP Enforcement</b> profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.	
URL Content Filter	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 <b>CSM&gt;&gt; URL Content Filter</b> web page first. Or choose [ <b>Create New</b> ] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for <b>URL Content Filter</b> by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.		
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			
	Image: Second		
	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.
<b>Session timeout</b> – Setting timeout for sessions can make the best utilization of network resources.

# 3.5.3 Filter Setup

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

Firewall >> Filter Setup

ilter 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 : De	fault Call Filter				
Filter Rule	Active	Comments		Move Up	Move Down
1		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 🔽
		OK Clear	Cancel		

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



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

Firewall >> Edit Filter Set >> Edit Filter Rule

Check to enable the Filter Ru	le	
Comments:		
Index(1-15) in <u>Schedule</u> Setup:	,,,,	
Clear sessions when schedule ON	I: 🗌 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:	Pass Immediately	
Branch to Other Filter Set:	None 💙	
Sessions Control	o / 60000	
MAC Bind IP	Non-Strict 💌	
Quality of Service	None 💌	
Load-Balance policy	Auto-Select 💌	
<u>User Management</u>	None 💌	
APP Enforcement:	None 💌	
URL Content Filter:	None 💌	
Web Content Filter:	None 💌	
Advance Setting	Edit	

Available settings are explained as follows:

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

Source/Destination IP	LAN.	domain for 2nd subnet or other the following dialog to choose the P ranges.
	IP Address Edit	Course and Objects as
	Address Type	Group and Objects
	Start IP Address	0.0.0.0
	End IP Address	0.0.0.0
	Subnet Mask	0.0.0.0
	Invert Selection IP Group	None V
	or IP Object	None
	or IP Object	None
	or IP Object	1-RD Department 2-Financial Dept.
	40	Close
	as the Address Type and addition, if you want to u groups or objects, please Address Type. Group and Objects V Any Address	nually, please choose <b>Any</b> / <b>Range Address/Subnet Address</b> type them in this dialog. In se the IP range from defined choose <b>Group and Objects</b> as the
		down list, choose the one that you <b>IP Object</b> drop down list to a want.
Service Type	Click <b>Edit</b> to access into suitable service type.	the following dialog to choose a

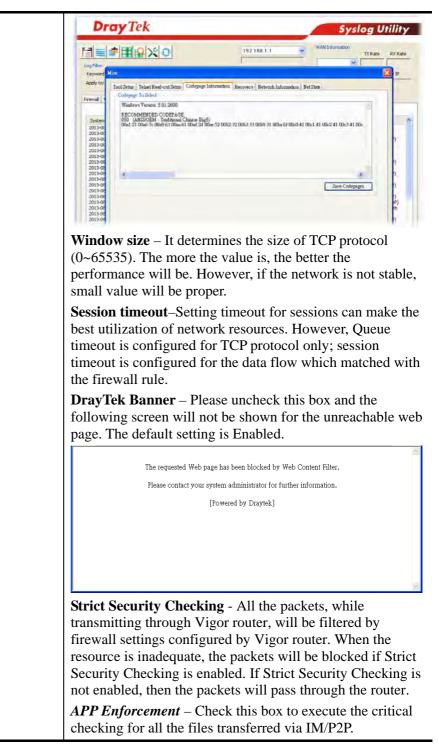


	🗿 Service Type Edit - Microsoft Internet Explorer
	Service Type Edit Service Type Group and Objects V Protocol TCP/UDP V Source Port = V 137 ~133 Destination Port = V 137 ~133 Service Group None V or Service Object None or Service Object 1-SIP or Service Object 2_RTP OK Close
	To set the service type manually, please choose User defined as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose Group and Objects as the Service Type. 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.
	<ul> <li>(&lt;) – the port number less than this value is available for this profile.</li> <li>Service Group/Object - Use the drop down list to choose the one that you want.</li> </ul>
Fragments	Specify the action for fragmented packets. And it is used for <b>Data Filter</b> 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.
	<b>Block Immediately -</b> Packets matching the rule will be dropped immediately.

	<b>Pass Immediately -</b> Packets matching the rule will be passed immediately.
	<b>Block If No Further Match -</b> A packet matching the rule, and that does not match further rules, will be dropped.
	<b>Pass If No Further Match -</b> 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	<ul> <li>Strict - Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP be bound for applying such filter rule.</li> <li>No-Strict - no limitation.</li> </ul>
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default
Load-Balance policy	Choose the WAN interface for applying Load-Balance Policy.
User Management	uch item is available only when <b>Rule-Based</b> is selected in User <b>Management&gt;&gt;General Setup</b> . The general firewall rule will be applied to the user/user group/all users specified here. None User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile existed, <b>Create New User</b> or <b>Create New Group</b> item will appear for you to click to create a new one
APP Enforcement	Select an <b>APP Enforcement</b> profile for global IM/P2P application blocking. If there is no profile for you to selelct, please choose [ <b>Create New</b> ] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the <b>APP Enforcement</b>



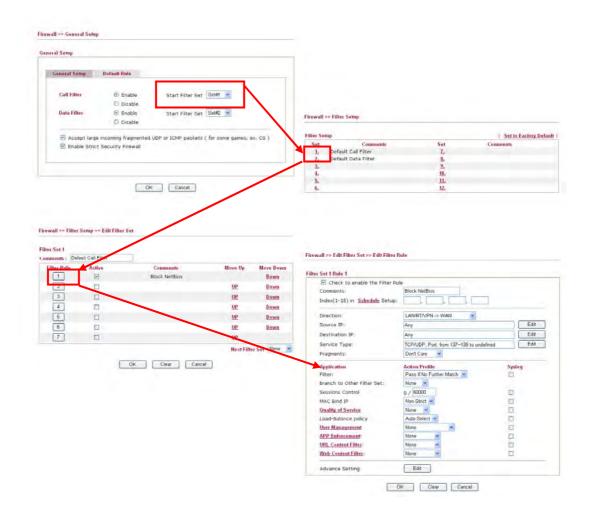
	<ul> <li>profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</li> </ul>
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	<ul> <li>Select one of the Web Content Filter profile settings         (created in CSM&gt;&gt; Web Content Filter) for applying with         this router. Please set at least one profile for anti-virus in         CSM&gt;&gt; Web Content Filter web page first. Or choose         [Create New] from the drop down list in this page to create         a new profile. For troubleshooting needs, you can specify to         record information for Web Content Filter by checking the         Log box. It will be sent to Syslog server. Please refer to         section Syslog/Mail Alert for more detailed information.</li> </ul>
Advance Setting	Click Edit to open the following window. However, it is strongly recommended to use the default settings here. 192.168.1.1/doc/spfedredv.htm ####################################



### 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.





### 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	

Dos derense 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 Drop					
Block Smurf	Block Smurf Block Ping of Death				
Block trace route	🔲 Block ICMP fra	gment			
Block SYN fragment	🔲 Block Unassigr	ned Numb	ers		
🔲 Block Fraggle Attack					
Enable DoS defense function to preve crackers.	nt the attacks fr	om hacker	or		
			1		

OK Clear 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



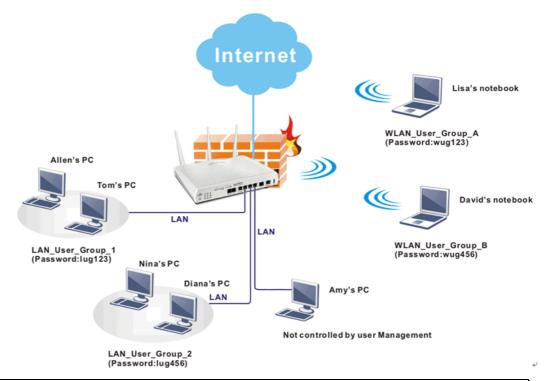
	manne when 2000 methods not accord received they will be
	means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood 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 Port Scan 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 block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets

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

Log Flow Keyward: Agoly to:		Refresh	LAN Information TX Packets		WAN b formation	Galeway IP	TX Rate	RXRate
Finewal Log Defe Preme System Time	Router Time	Ilost	FLog Connection I Message	og WANLog 1	IPPEX Log   Others   C	all Detailed Recor	d [ Phone Cal	Top10

# 3.6 User Management

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



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

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





# 3.6.1 General Setup

General Setup can determine the standard (rule-based or user-based) for the users controlled by User Management. The mode (standard) selected here will influence the contents of the filter rule(s) applied to every user.

#### User Management >> General Setup

al Setup	
Mode: Rule-Based 💌 Display IP Address on tracking window: Off	×
<ul> <li>Web Authentication: HTTPS </li> <li>Notice :</li> <li>1. User Management will refer to active rules in in user-based firewall mode.</li> <li>2. Users match the above lists will not be required for users match the above lists will valid.</li> <li>3. Otherwise, authentication required for users The firewall rules designated in the user pro-</li> </ul>	ired for authentication. 5 not matched the above lists.
Landing Page (Max 255 characters)	Preview Set to Factory Default
<body stats="l"><script <="" http:="" language="javascript&lt;br&gt;window.location=" td="" www.draytek.com'<=""><th></th></tr><tr><td>OK Clear</td><th>Cancel</th></tr></tbody></table></script></body>	

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



### 3.6.2 User Profile

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

ser Profile Table			Set to Factory Defaul
Profile	Name	Profile	Name
<u>1.</u>	admin	<u>17.</u>	
<u>2.</u>	Dial-In User	<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>	

User Management >> User Profile

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

le Index 3		
🗹 Enable this account		_
User Name		
Password		]
Confirm Password		]
Idle Timeout	10	min(s) 0:Unlimited
Max User Login	0	0:Unlimited
External Server Authentication	None 💌	
Log	None 💌	
Pop Browser Tracking Window	<b>v</b>	
Authentication	🗹 Web 🛛 🗹 Alert Te	ool 🗹 Telnet
Landing Page		
Index(1-15) in <u>Schedule</u> Setup:	,,,,	,
Enable Time Quota 0	min. +-0	min.
📃 Enable Data Quota 🛛 0	MB V +-0	MB
	chedulina time expired	
Enable Default Time Que		fault Data Quota 🛛 🛛 ME

User Management >>User Profile



Item	Description	
Enable this account	Check this box to enable such user profile.	
User Name	Type a name for such user profile (e.g.,LAN_User_Group_1, WLAN_User_Group_A,WLAN_User_Group_B, etc). When a user tries to accessInternet through this router, an authentication step must beperformed first. The user has to type the User Namespecified here to pass the authentication. When the userpasses the authentication, he/she can access Internet via thisrouter. However the accessing operation will be restrictedwith the conditions configured in this user profile.	
Password	Type a password for such profile (e.g., <i>lug123</i> , <i>wug123</i> , <i>wug456</i> , etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.	
<b>Confirm Password</b>	Type the password again for confirmation.	
Idle Timeout	If the user is idle over the limitation of the timer, the <b>network connection will be stopped for such user.</b> By default, the Idle Timeout is set to 10 minutes.	
Max User Login	Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.	
Policy	It is available only when User-Based mode selected in User Management>>General Setup. Default [Create New Policy]	
	<ul> <li>Default – If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile.</li> <li>Create New Policy – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.</li> </ul>	



Item	Description	
	Firewall >> Edit Filter Set >> Edit Filter Rule	
	Filter Set 1 Rule 2	
	Comments:	
	Index(1-15) in <u>Schedule</u> Setup:	,,,,
	Direction:	LAN/RT/VPN -> WAN
	Source IP:	Any
	Destination IP:	Any
	Service Type:	Any
	For the detailed configuration, si <b>Firewall&gt;&gt;Filter Rule</b> . The fire selected in <b>Firewall&gt;&gt;General&gt;</b> available for use in <b>User Manag</b>	wall filter rules that are not >>Default rule can be
External Service Authentication	The router will authenticate the dial-in user by itself or by external service such as Radius server. If Radius is selected here, it is not necessary to configure the password setting above.	
Log	Time of login/log out, block/unb sent to and displayed in Syslog. the log items to take down relation None Login Event All	Please choose any one of
Pop Browser Tracking Window	If such function is enabled, a pop displayed on the screen with tim if Idle Timeout is set. However, time periodically to keep the con Idle Timeout will not interrupt th	e remaining for connection the system will update the nection always on. Thus,
Authentication	Any user (from LAN side or WL to Internet via Vigor router must router first. There are three ways the user to choose for authentica	be authenticated by the offered by the router for
	Web – If it is selected, the use carouter from any browser. Then, a popped up and ask the user to typ password for authentication. If selected with the selected of the select	a login window will be pe the user name and ucceed, a <b>Welcome</b> anagement >> General authentication, the
	Alert Tool – If it is selected, the and type the user name and pass	

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



Item	Description
	such profile. - Click this box to decrease the data quota for such profile.
Reset quota to default when scheduling time expired	Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically.
	<b>Enable</b> – Check it to use the default setting for time quota and data quota.
	<b>Default Time Quota</b> – Type the value for the time manually.
	<b>Default Data Quota</b> – Type the value for the data manually.

# 3.6.3 User Group

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

User 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>	

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

#### User Management >> User Group

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

Available settings are explained as follows:

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

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

# 3.6.4 User Online Status

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

User Management >> User Online Status

Current Time : 11-01 02:53:00			Refresh Seconds: 10 💌 Page: 1 💌   <u>Refresh</u>				
Index	Profile V	IP Address	User	Last Login Time	Expired Time	Idle Time	Action
1	<u>admin</u>	192.168.1.10	admin	10-31 08:50:50	Unlimited	Unlimited	Block Logout

Total Number : 1

Available settings are explained as follows:

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

# 3.7 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).

User management
Objects Setting
▶ IP Object
▶ IP Group
▶ IPv6 Object
▶IPv6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
SMS/Mail Service Object
Notification Object
CSM

# 3.7.1 IP Object

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

#### Objects Setting >> IP Object

P 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>	
< <u>1-32   33-64   6</u>	<u>5-96   97-128   129-160   161-</u>	<u>192</u> >>	<u>Next</u> >>

Available settings are explained as follows:

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

# **Dray** Tek

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

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

Objects Setting >> IP Object

### IP Object Profiles:

Index	Name	Ind
<u>1.</u>		1
<u>2.</u>		18
3.		10

2. The configuration page will be shown as follows:

#### Objects Setting >> IP Object

Profile Index : 11				
Name:	RD Department			
Interface:	Any 💌			
Address Type:	Range Address 💌			
Mac Address:	00,00,00,00,00,00			
Start IP Address:	192.168.1.65			
End IP Address:	192.168.1.69			
Subnet Mask:	0.0.0.0			
Invert Selection:				
0	K Clear Cancel			

Available settings are explained as follows:

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/RT/VPN or any IP address. If you choose LAN/RT/VPN as the <b>Interface</b> here, and choose LAN/RT/VPN as the direction setting in <b>Edit Filter Rule</b> , then all the IP addresses specified with LAN/RT/VPN interface will be opened for you to choose in <b>Edit Filter Rule</b> page.

Address Type	Determine the address type for the IP address. Select <b>Single Address</b> if this object contains one IP address only. Select <b>Range Address</b> if this object contains several IPs within a range. Select <b>Subnet Address</b> if this object contains one subnet for IP address. Select <b>Any Address</b> if this object contains any IP address. Select <b>Mac Address</b> if this object contains Mac address. Range Address Single Address Single Address Subnet 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.	
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.	
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.	

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

Objects Setting >> IP Object

P 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>	

# 3.7.2 IP Group

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

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

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.

### Objects Setting >> IP Group

#### IP Group Table:

Index	Name	Inc
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		

Objects Setting	>>  [	^o Group	)
-----------------	-------	--------------------	---

Profile Index : 1	
Name:	Administration
Interface:	Any 💙
Available IP Objects	Selected IP Objects
1-RD Department 2-Financial Dept. 3-HR Department	» «
ſ	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.

Objects Setting >> IP Group

P Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>	Administration	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	

# 3.7.3 IPv6 Object

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

Ob	iects	Setting	>>	IPv6	Ob	iect
~					~	

∿6 Object Profiles	s:		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</u> >>			<u>Next</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.

```
Objects Setting >> IPv6 Object
```

IPv6 Object Profiles:	IPv6 0	bject	Profiles:
-----------------------	--------	-------	-----------

Index	Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	

2. The configuration page will be shown as follows:

#### Objects Setting >> IPv6 Object

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

Available settings are explained as follows:

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Address Type	Determine the address type for the IPv6 address. Select <b>Single Address</b> if this object contains one IPv6 address only.	
	Select <b>Range Address</b> if this object contains several IPv6s within a range.	
	Select <b>Subnet Address</b> if this object contains one subnet for IPv6 address.	
	Select <b>Any Address</b> if this object contains any IPv6 address.	
	Select Mac Address if this object contains Mac address.	
	Range Address         Any Address         Single Address         Range Address         Subnet Address         Mac Address	
MAC Address	Type the MAC address of the network card which will be controlled.	
Start IP Address	Type the start IP address for Single Address type.	
End IP Address	Type the end IP address if the Range Address type is selected.	
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.	
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 here, please click **OK** to save the configuration.



# 3.7.4 IPv6 Group

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

IPv6 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.

```
Objects Setting >> IP Group
```

#### IPv6 Group Table:

Index	Name
<u>1.</u>	
2.	

ndex:1		
Name:	v6_group1	
Available IPv6 Objects	Selected IPv6 Objects	
1-v6_ob_1		<u>^</u>
	>>>	
	«	
	<b>~</b>	~

OK Clear Cancel

Available settings are explained as follows:

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

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

Objects Setting >> IP Group

IPv6 Group Ta	able:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>	v6_group1	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
4.		20.	

# 3.7.5 Service Type Object

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

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

Service Type Objec	ct 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>	
< <u>1-32   33-64   6</u>	<u>5-96</u> >>		<u>Next</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.

#### Objects Setting >> Service Type Object

#### Service Type Object Profiles:

Index	Name
<u>1.</u>	
<u>2.</u>	

2. The configuration page will be shown as follows:

```
Dray Tek
```

#### Objects Setting >> Service Type Object Setup

Protocol TCP	Name	WWW
	Protocol	ТСР 🕑 6
Destination Port = 🔽 80 🗸 80	Source Port	= 🖌 1 ~ 65535
	Destination Port	= 💙 80 ~ 80

Available settings are explained as follows:

Item	Description		
Name	Type a name for this profile.		
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         ICMP       IGMP         IGMP       TCP         UDP       TCP/UDP         Other       0		
Source/Destination Port			

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

### Service Type Object Profiles:

Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
<u>3.</u>	
4.	

# 3.7.6 Service Type Group

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

```
Objects Setting >> Service Type Group
```

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

Available settings are explained as follows:

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

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

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

Objects Setting >> Service Type Group

#### Service Type Group Table:

Group	Name
<u>1.</u>	
<u>2.</u>	
3.	

Obiects	Setting	>>	Service	Type	Group	Setup
objects	Setting		0010100		Group	South

Name:	VolP	
Available Service	Type Objects	Selected Service Type Objects
1-SIP 2-RTP		»

Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Available Service Type Objects	All the available service objects that you have added on <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 here, please click **OK** to save the configuration.

ΟK

Objects Setting >> Service Type Group

Service Type Grou	up Table:		Set to Factory Default
Group	Name	Group	Name
<u>1.</u>	VoIP	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	

# 3.7.7 Keyword Object

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

eyword Object Pr	ofiles:		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   6</u>	<u>5-96   97-128   129-160   161</u>	- <u>192   <u>193-200</u> &gt;&gt;</u>	<u>Next</u> >

Objects Setting >> Keyword Object

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.

#### Objects Setting >> Keyword Object

#### Keyword Object Profiles:

-	-
Index	Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	

**Objects Setting >> Keyword Object Setup** 

Profile Index : 1

 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.
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 here, please click **OK** to save the configuration.

Objects Setting >> Keyword Object

Keyword O	bject Profiles:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>	Keyword-1	<u>17.</u>	
<u>2.</u>	Keyword-2	<u>18.</u>	
<u>3.</u>		<u>19.</u>	
4.		20.	

# 3.7.8 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.

eyword Group Tal	ole:		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.

#### Objects Setting >> Keyword Group

#### Keyword Group Table:

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

Objects Setting >> Keyword Group Setup

Name:	night	
vailable Keyword Objects	Selected Keyword Objects(	Max 16 Objects)
1-Кеуword-1 2-Кеуword-2	× «	~
	×	~

Available settings are explained as follows:

Item	Description
Name	Type a name for this group.
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 here, please click **OK** to save the configuration.

Objects Setting >> Keyword Group

le:		Set to Factory Default
Name	Index	Name
night	<u>17.</u>	
	<u>18.</u>	
	<u>19.</u>	
	<u>20.</u>	
	<u>21.</u>	
	<u>22.</u>	
	Name	Name         Index           night         17.           18.         19.           20.         21.

# 3.7.9 File Extension Object

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

Objects	Setting >>	File	Extension Object
---------	------------	------	------------------

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

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.
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.

### Objects Setting >> File Extension Object

#### File Extension Object Profiles:

Profile	Name
<u>1.</u>	
2.	

Objects Setting >> File Extension Object Setup

Profile Index: 1	Pro	ofile Name:					
Categories			Fi	e Extensi	ons		
Image Select All Clear All	.bmp .pct	□.dib □.pcx	.gif	□.jpeg □.pict	🗌 .jpg 🗌 .png	□.jpg2 □.tif	□.jp2 □.tiff
Video Select All Clear All	🗌 .asf 🗌 .qt	.avi .rm	.mov .wmv	.mpe .3gp	.mpeg .3gpp	.mpg .3gpp2	.mp4 .3g2
Audio Select All Clear All	🗌 .aac 🗌 .ra	.aiff	□.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 Select All Clear All	.ace .rar	🗌 .arj 🗌 .sit	.bzip2 .zip	.bz2	.cab	.gz	🗌 .gzip
Executation Select All Clear All	.bas .scr	🗌 .bat	.com	.exe	.inf	.pif	.reg

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile.

- 3. Type a name for such profile and check all the items of file extension that will be processed in the router.
- 4. After finishing all the settings here, please click **OK** to save the configuration.

Objects Setting >> File Extension Object

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

# 3.7.10 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
1.	
<u>2.</u>	
<u>3.</u>	

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

Object Settings >> SMS / Mail Service Object

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile.
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.
Password	Type a password that the sender can use to register to selected SMS provider.
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)

### **Customized SMS Service**

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

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

Object Settings >> SMS / Mail Service Object

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

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

```
Profile Index: 9
```

Profile Name	Custom 1	
Service Provider		
Please contact with your SMS pro	vide to get the exact URL String	
eg:bulksms.vsms.net:5567/eapi/s		
&passworu=###txtPwu###&msis	n=###txtDest###&message=#	##txtMsg###
Weassword=###txtPwd###&msis	In=###txtDest###&message=#	##txtMsg###
•	n=###txtDest###&message=#	##txtMsg###
Username	n=###txtDest###&message=#	##txtMsg###
Username Password		##txtMsg### onds)

Available settings are explained as follows:

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

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

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

### Mail Service Object

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

Object Settings >> SMS / Mail Service Object

SMS 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>				

Each item is explained as follows:

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

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

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

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

### Object Settings >> SMS / Mail Service Object

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1		
Profile Name	Mail_notify	
SMTP Server	192.168.1.98	
SMTP Port	465	
Sender Address	carrie@draytek.com	
Use SSL		
Authentication		
Username	John	
Password		
Sending Interval	0	(seconds)
	OK Clear Ca	ncel

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile.
SMTP Server	Type the IP address of the mail server.
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.
	<b>Password</b> – Type a password for authentication.
Sending Interval	Define the interval for the system to send the SMS out.

**Dray** Tek

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	
<u>1.</u>		Mail_Notify	
<u>2.</u>			
<u>3.</u>			
4.			

## 3.7.11 Notification Object

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

You can set an object with different monitoring situation.

Object Settings >> Notification Object

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

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

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

Object Settings >> Notification Object

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

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.
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
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

# **Dray** Tek

# 3.8 CSM Profile

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

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

### **APP Enforcement Filter**

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

### **URL Content Filter**

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

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

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

### Web Content Filter

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

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

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





### 3.8.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/OTHERS 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.

APP Enford	ement Profile 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 Enforcement Profile						
Profile Index : 1	Profile Name:					
IM	P2P	PROTOCOL	OTHERS			
Select All	Clear All		Support List		Action : Block	
			Protocol			
DNS	■ FTP	(	■ HTTP	IMAP	IRC 🗆	
NNTP	POP3	(	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.
Select All Click it to choose all of the items in this page.	
Clear All	Uncheck all the selected boxes.
Support List	Display the all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.
Action	<ul> <li>Block – Block all the packets passing with the settings configured in this page.</li> <li>Pass – Pass all the packets with the settings configured in this page.</li> </ul>

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.

The items categorized under P2P -----

#### CSM >> APP Enforcement Profile

rofile Index : 1 Pro	file Name:				
IM	P2P	PROTOCOL	OTHERS		
Select All Clea	ar All			Suppor	<u>t List</u>
Protoc	ol			Applications	
SoulSeek		SoulSeek			
🗆 eDonkey		eDonkey, eMi	ule, Shareaza		
FastTrack		KazaA, BearShare, iMesh			
OpenFT		KCeasy, FilePipe			
🗆 Gnutella		BearShare, Limewire, Shareaza, Foxy, KCeasy			
OpenNap		Lopster, XNap	o, WinLop		
BitTorrent		BitTorrent, Bit	Spirit, BitComet		
		Othe	r P2P Applications		
🗆 Xunlei	🗆 Vagaa		PP365	■ POCO	🗆 Clubbox
Ares	■ezPeer		Pando	Huntmine	■Kuwo

OK Cancel

# Below shows the items which are categorized under IM.

rofile Index : 1	Profile Name:				
IM	P2P	PROTOCOL	OTHERS		
Select All [ (	Clear All			<u>Support Li</u>	<u>st</u>
			ed Management		
	/ Application	MSN	YahooIM	AIM(<= v5.	
	Login				
	essage Transfer		0		
	Game	0	0		
	e(Video/Voice)	0		0	
	r Activities		0		
		IM Application			VoIP
AIM6/7 GoogleChat Qnext KC UC LINE	QQ/TM XFire POCO/PP3 Lava-Lava MobileMSN	ICU2	■ Jabber/Gi ■ Paltalk ■ AliWW ■ iSpQ ■ Fetion		Skype Kubao Gizmo SIP/RTP TelTel TeamSpe RaidCall
		Web IM ( * = m	ore than one address)	1	
■ WebIM URLs	e <u>Messenger</u> ICQ Java* IMUnitive* MessengerFX*	WebMSN me ICQ Flash* go	ebo* eBuddy owy* IMhaha* ibber* MSN2GO	<u>ILovell</u> getMe	ssenger
		OK	Cancel		
he items cat	egorized unde	er OTHERS			
SM >> APP Enfor	0				

Socks4/5	PGPNet	HTTP Proxy Reply	Tor	■ VNN
SoftEther	MS TEREDO	Skyfire	🗆 Hamachi	🗆 HTTP Tunnel
🗆 Ping Tunnel	TinyVPN	RealTunnel	🗆 DynaPass	🗆 UltraVPN
🗆 FreeU	Wujie/UltraSurf	🗆 Hotspot Shield		

<ul> <li>MMS</li> <li>FeiDian</li> <li>SopCast</li> <li>FlashVideo</li> </ul>	RTSP UUSee UDLiveX SilverLight	<ul> <li>TVAnts</li> <li>NSPlayer</li> <li>TVUPlayer</li> <li>Slingbox</li> </ul>	PPStream PCAST MySee QVOD	■ PPTV ■ TVKoo ■ Joost		
Remote Control						

	Remote Control		
Radmin	SpyAnywhere	ShowMyPC	■LogMeIn
Gogrok	🗏 RemoteControlPro	CrossLoop	WindowsRDP
Timbuktu	WindowsLiveSync	SharedView	
	Web HD		
HiNet SafeBox	MS SkyDrive	🗆 GDoc Uploader	ADrive
Mozy	🗏 BoxNet	OfficeLive	■DropBox
	Gogrok Timbuktu HiNet SafeBox	Radmin SpyAnywhere Gogrok RemoteControlPro Timbuktu WindowsLiveSync Web HD HiNet SafeBox MS SkyDrive	Radmin SpyAnywhere ShowMyPC Gogrok RemoteControlPro CrossLoop Timbuktu WindowsLiveSync SharedView Web HD HiNet SafeBox MS SkyDrive GDoc Uploader

OK Cancel

## 3.8.2 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.

RL Content Filter F	Profile Table:		Set to Factory Def
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

CSM >> URL Content Filter Profile

Administration Message (Max 255 characters)

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

OK

Each item is explained as follows:

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

0

Default Message

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.

CSM >> URL Content Filter Profile	CSM >>	URL	Content	Filter	Profile
-----------------------------------	--------	-----	---------	--------	---------

Profile Name:		
Priority:	Both : Pass	Log: None V
1.URL Access	Control	
Enat	ble URL Access Control	Prevent web access from IP address
Actio	on:	Group/Object Selections
Pass	~	Edit
2.Web Featu	re	
Enal	ble Restrict Web Feature	
Actio	on:	
Pass	Cookie Pro	xy File Extension Profile: None 🕶

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile.
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, bot configuration set in this page for URL Access Control and Web Feature will be inactive.
	<b>Either: URL Access Control First</b> – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one the router will process the packages with the conditions set below for URL first, then Web feature second.
	<b>Either: Web Feature First</b> –When all the packages matching with the conditions specified in URL Access

	Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second. Both : Pass Both : Pass Both : Block Either : URL Access Control First 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 All
URL Access Control	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. Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before. 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. Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action. 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. 🥖 Group/Object Edit - Windows Internet Explorer 🕖 http://192.168.1.1/doc/cfkw.gob.htm Object/Group Edit Keyword Object None N None 🗸 or Keyword Object 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 🗸 OK Close Web Feature Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed. Action - This setting is available only when Either: URL Access Control First or Either: Web Feature Firs is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below. Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below. **Block** - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. **Proxy** - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. **Upload** – Check the box to block the file upload by way of web page. File Extension Profile – Choose one of the profiles that you configured in Object Setting>> File Extension Objects previously for passing or blocking the file downloading.

File Extension Profile:	None 🏻	*
	None	
	1-default	

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

### 3.8.3 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

#### Web-Filter License

[Status:Not Activated]

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

#### Web Content Filter Profile Table: Set to Factory Default Profile Name Profile Name Default <u>1.</u> <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 💌 <br><bn>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter. Please contact your system administrator for further information.</center></body>

#### Legend:

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
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> .

Activate

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.

#### CSM >> Web Content Filter Profile

Profile Index: 1 Profile Name: Default			Log: Block 💙
Black/White List			
Enable Action: Block 💌	Gr	oup/Object Selections	Edit
Action: Block 🛩 Groups	Categories		
Child Protection Select All Clear All	<ul> <li>✓ Alcohol &amp; Tobacco</li> <li>✓ Hate &amp; Intolerance</li> <li>✓ Porn &amp; Sexually</li> <li>✓ School Cheating</li> <li>✓ Child Abuse Images</li> </ul>	<ul> <li>✓ Criminal Activity</li> <li>✓ Illegal Drug</li> <li>✓ Violence</li> <li>✓ Sex Education</li> </ul>	<ul> <li>✓ Gambling</li> <li>✓ Nudity</li> <li>✓ Weapons</li> <li>✓ Tasteless</li> </ul>
Leisure Select All Clear All Business	Entertainment     Travel	Games	☐ Sports ☐ Fashion & Beauty
Select All Clear All	Compromised Finance News Politics Restaurants & Dining General Image Sharing Private IP Addresses	Dating & Personals Government Non-profits & NGOs Real Estate Shopping Cults Network Errors Uncategorised Sites	Education Health & Medicine Personal Sites Religion Translators Greeting cards Parked Domains

Item	Description	
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.	
	<b>Block</b> - <b>restrict</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.	
Action	<b>Pass</b> - allow accessing into the corresponding webpage with the categories listed on the box below.	
	<b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.	

	If the web pages do not match with the specified feature set here, it will be processed with reverse action.
Log	None – There is no log file will be recorded for this profile.         Pass – Only the log about Pass will be recorded in Syslog.         Block – Only the log about Block will be recorded in Syslog.         All – All the actions (Pass and Block) will be recorded in Syslog.         Block 💌         None         Pass         Block All

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

## 3.8.4 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 💌
Enable Block Page	🗹 Enable
Administration Message (Max 255 character:	s) Default Message ted Web page br> from %SIP% tha
	locked by %RNAME% DNS Filter.Please contact
egend: %SIP% - Source IP , %URL% - URL &CL% - Category , %RNAME% - Router M	Name
0	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.



	<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> </ul>
	All – All the actions (Pass and Block) will be recorded in Syslog.
	Block V 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.
Enable Block Page	Check the box to enable such function.

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

# 3.8.5 APPE Support List

This page offers the software versions for each applications managed by APP Enforcement Profiles by Vigor router. Click the IM/P2P/PROTOCOL/OTHERS tab to open the information page for different APP type.

SM >> APPE Support List This charts lists out the APP Enforcement supported by Vigor routers. Last update on 2014-03-11					
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 ot 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 tir	os are blocked, Voic ne. In ICQ5 or forme be blocked separat	er versions, Videos
	ICU2	8.0.6			
	Jabber Protocol/Google Talk				
	KC	2008			
IM	LINE	4.0.1	To block LINE f (v4.0.1).	or PC (3.5.1.36) and	l mobile phone
	Lava-Lava	2007			
	MSN	2011			
	MobileMSN				

# 3.9 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management
Sessions Limit
Bandwidth Limit
Ouality of Service
Applications

## 3.9.1 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	100		
Limitation List			
Index Start IP	End IP	Max Sessions	
Specific Limitation			
Start IP:	End IP:		
Maximum Sessions:	Add Ed	t Delete	
ninistration Message (Max 2	56 characters)		Default Message
a have reached the maxi	imum number of perm to allow further I	itted Internet sessions nternet access.Conta	.Please close
ne Schedule Index(1-15) in <u>Schedule</u>	e Setup:,,	,,	

Bandwidth Management >> Sessions Limit

To activate the function of limit session, simply click Enable and set the default session limit.



Item	Description
Session Limit	<ul><li>Enable - Click this button to activate the function of limit session.</li><li>Disable - Click this button to close the function of limit</li></ul>
	session. <b>Default Max Session -</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	<ul> <li>Start IP- Defines the start IP address for limit session.</li> <li>End IP - Defines the end IP address for limit session.</li> <li>Maximum Sessions - Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.</li> </ul>
	<ul> <li>Add - Adds the specific session limitation onto the list above.</li> <li>Edit - Allows you to edit the settings for the selected limitation.</li> <li>Delete - Remove the selected settings existing on the limitation list.</li> </ul>
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted. Click <b>Default Message</b> to display the default message on the screen.
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.

Available settings are explained as follows:

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

## 3.9.2 Bandwidth Limit

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

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

Enable IP	Routed Subnet 💿 Disable
Default TX Limit:	2000 Kbps 💌 Default RX Limit: 8000 Kbps 💌
🔲 Allow auto ad	ljustment to make the best utilization of <mark>available bandwidth</mark> .
Limitation List	
Index Start IP	End IP
Specific Limitation	
Start IP:	End IP:
Each Share	
TX Limit:	Kbps 💟 RX Limit: Kbps 💙
	Add Update Delete
🗆 Smart Bandwidt	
For any LAN IP ( 1000	Not in Limitation List, whose session number exceeds
TX Limit : 200	Kbps 🔽 RX Limit : 800 Kbps 🔽
: For TX/RX, a setting o	f "O" means unlimited bandwidth.
Schedule	
Index(1-15) in <u>Schedul</u>	<u>e</u> Setup:,,,
Note: Action and Idle Ti	meout settings will be ignored.

Bandwidth Management >> Bandwidth Limit

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

ΟK

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



	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	Start IP - 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>Update -</b> Allow you to edit the settings for the selected limitation.
	<b>Delete -</b> Remove the selected settings existing on the limitation list.
Smart Bandwidth Limit	Check this box to have the bandwidth limit determined by the system automatically.
	<b>TX limit -</b> Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
	<b>RX limit -</b> Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Time Schedule	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.

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

# 3.9.3 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?

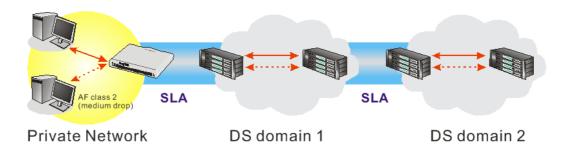
There are two components within Primary configuration of QoS deployment:

- 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.

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setur
WAN2	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	<u>Setu</u>
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
Class			нттр					Edit	<u>Edit</u>	
Class			VoIP					<u>Edit</u>		
Class	s 3		Mail					Edit		
		First Priority for VolP SIP/R ort: 5060 (Default: 5060								

Bandwidth Management >> Quality of Service

Item	Description
General Setup	<b>Index</b> – Display the WAN interface number that you can edit.
	Status - Display the current QoS status of this WAN.
	<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.

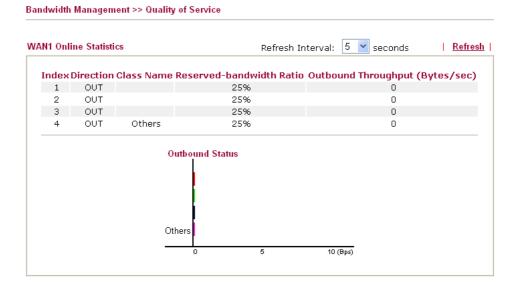
Item	Description
Enable the First Priority for VoIP SIP/RTP	When this feature is enabled, the VoIP SIP/RTP packets will be sent with highest priority.
	<b>SIP UDP Port</b> - Set a port number used for SIP.

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

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

## **Online Statistics**

Display an online statistics for quality of service for your reference.



## **General Setup for WAN Interface**

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.



#### Bandwidth Management >> Quality of Service

WAN1 General Setup							
Enable the QoS (	Control OUT 💌						
Index	Class Name	Reserved_bandwidth Ratio					
Class 1		25 %					
Class 2		25 %					
Class 3		25 %					
	Others	25 %					
🔲 Enable VDP Ba	Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %						
🔲 Outbound TCP	ACK Prioritize						
Materil Defeue emela	lo OoC, you should tost the real ha	ndwidth first. OnC may not work properly if					

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

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

OK Clear Cancel

Available settings are explained as follows:

Item	Description		
Enable the QoS Control	<ul> <li>The factory default for this setting is checked.</li> <li>Please also define which traffic the QoS Control settings will apply to.</li> <li>IN- apply to incoming traffic only.</li> <li>OUT- apply to outgoing traffic only.</li> <li>BOTH- apply to both incoming and outgoing traffic.</li> <li>Check this box and click OK, then click Setup link again.</li> <li>You will see the Online Statistics link appearing on this page.</li> </ul>		
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN2/WAN3. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.		
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN2/WAN3. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.		
	<b>Note:</b> 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.		
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.

## 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.

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setu
WAN2	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
Clas	c 1		VoIP					Edit		
Clas			HTTP					Edit	Edit	
Clas			Mail					Edit	2011	
Club										

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

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

lass Inde	ex #1							
Name [	VolP		🗹 Ta	g packets as: AF C	lass1 (High Drop) 🛛 📘			
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1 🔿	Active	Any	Any	ANY	ANY			
	Add Edit Delete							
			OK Cancel					

Item	Description	
Name	Display the name of such class.	
Tag packets as	Check the box to tag the packets with the header selected in the drop down list for this class.	
NO	Display the number of the rules defined for such rule.	
Status	Display if such rule is enabled (Active) or not.	
Local Address	Display the local IP address (on LAN) for the rule.	
<b>Remote Address</b>	Display the remote IP address (on LAN/WAN) for the rule.	
<b>DiffServ CodePoint</b> Display the levels of the data for processing with Q control.		
Service Type	Display the service type of the data for processing with QoS control	

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
Note: Please choose/set	tup the <u>Service Type</u> first.

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.

Edit	It allows you to edit source address information.  The provide the the the the the the the the the th				
	Address Type Subnet Address  Start IP Address 0.0.0.0 End IP Address 0.0.0.0 Subnet Mask 0.0.0.0 OK Close				
	Address Type – Determine the address type for the source address.				
	For <b>Single Address</b> , you have to fill in Start IP address.				
	For <b>Range Address</b> , you have to fill in Start IP address and End IP address.				
	For <b>Subnet Address</b> , you have to fill in Start IP address and Subnet Mask.				
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.				
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.				

- 4. After finishing all the settings here, please click **OK** to save the configuration.
- 5. By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Bandwidth Management >> Quality of Service

Iame VolP 🗹 Tag packets as: AF Class1 (High Drop) 🔻					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Active	Any	Any	ANY	ANY
2 🔿	Active	192.168.1.96	172.16.3.228	AF Class1 (Medium Drop)	SNMP-TRAPS (TCP/UDP:162)
Add Edit Delete					

## Edit the Service Type for Class Rule

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



#### Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setu
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

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

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

Jser Defined Service Type						
NO	Name	Protocol	Port			
1	Empty	-	-			
Add Edit Delete						
		Cancel				

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

Bandwidth Management >>	Quality of Service
-------------------------	--------------------

Service Type Edit	
Service Name	
Service Type	TCP 6
Port Configuration	
Туре	💿 Single 🛛 Range
Port Number	0 – 0
OK	Cancel

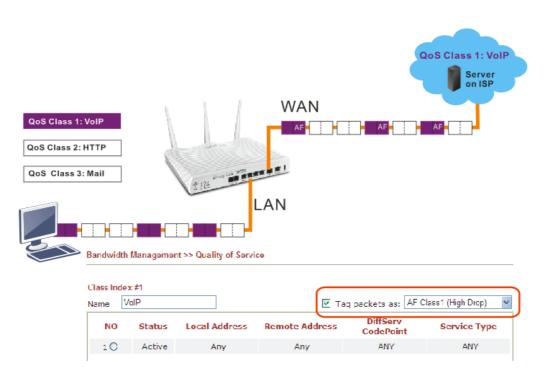
Item	Description
Service Name	Type in a new service for your request.
Service Type	Choose the type (TCP, UDP or TCP/UDP or other) for the new service.
Port Configuration	<b>Type</b> - Click <b>Single</b> or <b>Range</b> as the <b>Type</b> . If you select Range, you have to type in the starting port number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

4. 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 the 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.



# 3.10 Applications

Below shows the menu items for Applications.

bandwidth Management
Applications
Dynamic DNS
LAN DNS
Schedule
▶ RADIUS
Active Directory /LDAP
▶ UPnP
▶ IGMP
Wake on LAN
SMS/Mail Alert Service

## 3.10.1 Dynamic DNS

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

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

## Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

)ynamic DNS Setup	1	<u> </u>	<u>et to Factory Default</u>
📃 Enable Dynar	nic DNS Setup	View Lo	g Force Update
Auto-Update int	erval 14400 Min(s) (1~14400)		
Accounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		×
<u>2.</u>	WAN1 First		×
<u>3.</u>	WAN1 First		×
<u>4.</u>	WAN1 First		×
<u>5.</u>	WAN1 First		×
<u>6.</u>	WAN1 First		х

OK Clear All

Available settings are explained as follows:

Item	Description
Enable Dynamic	Check this box to enable DDNS function.

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

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS** Account, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 1	
🗹 Enable Dynamic DNS	3 Account
WAN Interface	WAN1 First 💌
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chronic6653 . dyndns.org
Login Name	chronic6653 (max. 64 characters)
Password	(max. 23 characters)
🔲 Wildcards	
🔲 Backup MX	
Mail Extender	
Determine Real WAN IP	
	Internet IP OK Clear Cancel

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	<ul> <li>WAN1/WAN2/WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead.</li> <li>WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account.</li> </ul>



	WAN1 First V WAN1 Only WAN2 First WAN2 Only WAN3 First WAN3 Only
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine Real WAN IP	<ul> <li>If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP.</li> <li>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.</li> <li>There are two methods offered for you to choose:</li> <li>WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.</li> <li>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.</li> </ul>

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**

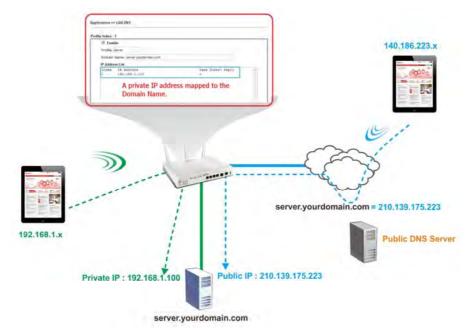
In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

## **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.

## 3.10.2 LAN DNS

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address (es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor2830 series will respond the specified private IP address.



Open **Application>>LAN DNS** to get the following page:

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>		

Applications >> LAN DNS

OK

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable	Check the box to enable such profile.

Index	Click the number below Index to access into the setting page of schedule.
Profile	Display the name of the profile.
Domain Name	Display the domain name for certain service (e.g., FTP, Mail or Web server) used by such profile.

To add a new LAN DNS profile,

Applications >> LAN DNS

Click any index, for example Index No.1. 1.

🗹 Enable		
Profile: Change		
Domain Name:		
P Address List		
Index IP Address	Same Subnet Reply	~

OK Clear

Γ

Item	Description	
Enable	Check the box to enable such profile.	
Profile	Type a name for such profile.	
Domain Name	Type a domain name (e.g., FTP, Mail or Web server) for such profile.	
IP Address List	<ul> <li>Add – Click it to open the following dialog. You have to give an IP address representing the host.</li> <li>Indified IP Address - Google Chrome IP 22.168.1.1/doc/andnshost.htm <ul> <li>Host's IP Address</li> <li>172.16.3.56</li> <li>Only responds to the DNS request when the sender is in the same subnet.</li> </ul> </li> <li>Only responds Disable it to apply this profile to all of the LAN subnets. Or enable it to apply such profile to the PCs on the same subnet.</li> <li>Delete – Click it to remove the existed IP address displayed on the IP Address List.</li> </ul>	

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

```
Note: For the detailed information about LAN DNS application, refer to DrayTek website, http://www.draytek.com.tw/index.php?option=com_k2&view=item&id=5242&Itemid=293 &lang=en.
```

## 3.10.3 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

Index	Status	Index	Status
Index	Status	index	Status
<u>1.</u>	×	<u>9.</u>	×
<u>2.</u>	×	<u>10.</u>	×
<u>3.</u>	х	<u>11.</u>	×
<u>4.</u>	×	<u>12.</u>	×
<u>5.</u>	×	<u>13.</u>	×
<u>6.</u>	×	<u>14.</u>	×
<u>7.</u>	Х	<u>15.</u>	×
<u>8.</u>	×		

#### 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, for example Index No.1.

Applications >> Schedule			
Schedule:   Set to Factory Defa			Set to Factory Default
Index	Status	Index	Status
<u>1.</u>	x	<u>9.</u>	×
<u>2.</u>	x	<u>10.</u>	x
<u>3.</u>	х	<u>11.</u>	х
<u>4.</u>	х	<u>12.</u>	х
<u>5.</u>	х	<u>13.</u>	х
<u>6.</u>	x	<u>14.</u>	×
<u>7.</u>	X	<u>15.</u>	х
<u>8.</u>	×		

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

2. The detailed settings of the call schedule with index 1 are shown below.

Index No. 1	
🔽 Enable Schedule Setup	
Start Date (yyyy-mm-dd)	2000 🗸 - 1 🔽 - 1 🔽
Start Time (hh:mm)	
Duration Time (hh:mm)	
Action	Force On
Idle Timeout	minute(s).(max. 255, 0 for default)
How Often	
O Once	
💿 Weekdays	
📃 Sun 🗹 Mon 🗹 T	'ue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat
ОК	Clear Cancel

Applications >> Schedule

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.	
	<b>Force On -</b> Force the connection to be always on.	
	Force Down -Force the connection to be always down.	
	<b>Enable Dial-On-Demand -</b> Specify the connection to be dial-on-demand and the value of idle timeout should be specified in <b>Idle Timeout</b> field.	
	<b>Disable Dial-On-Demand -</b> Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.	
Idle Timeout	Specify the duration (or period) for the schedule.	
	How often -Specify how often the schedule will be applied Once -The schedule will be applied just once	
	<b>Weekdays</b> -Specify which days in one week should perform the schedule.	

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

## Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).



- 1. Make sure the PPPoE connection and **Time Setup** is working properly.
- 2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- 3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.



## **3.10.4 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	
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.	
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.	
Confirm Shared Secret	Re-type the Shared Secret for confirmation.	

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

# 3.10.5 Active Directory/LDAP

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

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

## **General Setup**

Applications >> Active Directory /LDAP

This page allows you to enable the function and specify general settings for LDAP server.

General Setup	Active Directory / LDAP Profiles	
Enable Bind Type		Simple Mode
Server Addr		
Destination		389
Use SSL		
Regular DN		
Regular Pas	sword	
		OK Cancel
		n of the LDAP profiles, they will be listed in the page

Item	Description
Enable	Check to enable such function.
Bind Type	There are three types of bind type supported.         Simple Mode         Simple Mode         Anonymous         Regular Mode         Simple Mode – Just simply do the bind authentication without any search action.         Anonymous – Perform a search action first with Anonymous account then do the bind authentication.



	<ul> <li>Regular Mode– Mostly it is the same with anonymous mode.</li> <li>The different is that, the server will firstly check if you have the search authority.</li> <li>For the regular mode, you'll need to type in the Regular DN and Regular Password.</li> </ul>
Server Address	Enter the IP address of LDAP server.
<b>Destination Port</b>	Type a port number as the destination port for LDAP server.
Use SSL	Check the box to use the port number specified for SSL.
Regular DN	Type this setting if <b>Regular Mode</b> is selected as <b>Bind Type.</b>
Regular Password	Specify a password if <b>Regular Mode</b> is selected as <b>Bind</b> <b>Type.</b>

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

## **Profiles**

You can configure eight AD/LDAP profiles. These profiles would be used with User Management for different purposes in management.

Applications 53	Activo	Directory	A DAD
Applications >>	ACTIVE	Directory	LUAP

ieneral Setup	Active Directory / LDAP Profiles	
Index	Name	Distinguished Name
<u>1.</u>		
<u>2.</u>		
<u>3.</u> <u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		
f VPN and Rem	iote Access >> <u>PPP Ge</u> , check the boxes un	n of the LDAP profiles, they will be listed in the page neral <u>Setup</u> . If you want to use the profiles for VPN der PPTP LDAP Profiles in <b>VPN and Remote Access &gt;&gt;</b>

Click any index number link to open the following page.

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 1		
Name	vpn	
Common Name Identifier	uid	
Base Distinguished Name	ou=People,dc=ms,dc=draytek,dc=com	
Additional Filter	gidNumber=500	
Note: Please type in your additional fi For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)	ilter for BaseDN search request.	
Group Distinguished Name	cn=vpn,ou=Group,dc=ms,dc=draytek,dc=c	<u>,</u>
	OK Cancel	

Available settings are explained as follows:

Item	Description
Name	Type a name for such profile. The length of the use name is limited to 19 characters.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is "cn".
Base Distinguished Name / Group Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server. Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the subtron to list all the account information on the AD/LDAP Server to assist you finish the setup.
Additional Filter	This is an optional setting.

After finished the above settings, click **OK** to save and exit this page. A new profile will be created.

For detailed information about LDAP application, refer to section 4.14 How to Implement the AD/LDAP Authentication for User Management?

## 3.10.6 UPnP

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

Applications >> UPnP

UPnP	
Enable UPnP Service	Default WAN 💽
Enable Connection control Service Enable Connection Status Service	Default WAN WAN1 WAN2
	WAN3

**Note:** If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK	Clear	Cancel

Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the <b>Connection Control</b> <b>Service</b> or <b>Connection Status Service</b> .
Default WAN	It is used to specify the WAN interface for applying such function. The default setting is WAN1.

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	on month offerings
Network Tasks (Received a new connection Set up a home or small office network	binet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status:	Connected
iee Also	test Disconnected DrayTek ISDN PPP	Duration: Speed: Activity Internet Internet Gal	00:19:06 100.0 Mbps teway My Compute
Control Panel     Result       My. Network Places     My Documents	Internet Gateway IP Broadband Connection on Router Enabled	Packets: Sent: 404	<b>}</b> + 734
My Computer	LAN or High-Speed Internet	Received: 1,11!	5 666 ) 

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.

eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access
Section on Router	(Services
	<ul> <li>Imple</li> <li< td=""></li<></ul>
his connection allows you to connect to the Internet through a hared connection on another computer.	msnmsgr (192.168.29.11:8789) 63231 TCP
Settings	Add Edit Detere

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.

# 3.10.7 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications >>	GMP					
IGMP						
Enable IGMP	Proxy	WAN1 🔽				
	is to act as a mi any multicast gro					
Enable IGMP Enable IGM	<b>Snooping</b> ^D Snooping, mul [:]	ticast traffic i	s only forward	ed to ports tha	at have membe	ers of that
group. Disable IGM	P snooping, mul	ticast traffic i	is treated in th	ie same manne	er as broadcas	t traffic.
			OK Can	cel		
						Refresh
Working Multi	cast 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.

## 3.10.8 Wake on LAN

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

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

Application >>	Wake on LAN	
Wake on LAN		
	ote: Wake on LAN cooperate with <u>Bind IP to MAC</u> function, only binded PCs an wake up through IP.	
	Vake by: MAC Address 💌	
N	IAC Address:	
F	esult	

Item	Description	
Wake by	Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.         Wake by:       MAC Address \vee MAC Address IP Address         MAC Address       IP Address	
IP Address	The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.	
MAC Address	Type any one of the MAC address of the bound PCs.	
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.	



#### Application >> Wake on LAN

Wake by: MAC Address  IP Address:  MAC Address:  Wake Up! Result	IP Address: V MAC Address: ::::::::::::::::::::::::::::::::::	Note: Wake on can wake up th	LAN cooperate with Bind IP to MAC function, only binded PCs rough IP.
MAC Address:	MAC Address: ::::::::::::::::::::::::::::::::::	Wake by:	MAC Address
	Result	IP Address:	😒
Result		MAC Address:	Wake Up!
	Send command to client done	Result	

## 3.10.9 SMS/Mail Alert Service

The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user's mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to **10** SMS profiles which will be sent out according to different conditions.

## **SMS Provider**

This page allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent.

SMS Provider	Mail Server		2	Set to Factory Default
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - Line_down 💌		1 - ??? 💌	
2 🗹	1 - Line_down 💌		1 - ??? 💌	
3	1 - Line down 2 - ???		1 - ??? 💙	
4	3 - ???		1 - ??? 💙	
5	5 - ??? 6 - ???		1 - ??? 💙	
6	7 - ??? 8 - ???		1 - ??? 🛰	
7	9 - Custome 1 10 - Custome 2		1 - ??? 💌	
8	1 - Line_down		1 - ??? 🛰	
9	1 - Line_down 💟		1 - ??? 💙	
10 🗌	1 - Line_down 😽		1 - ??? 🛰	

Application >> SMS / Mail Alert Service

OK Cancel

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.



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>9</u>	et to Factory Default
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - Mail_Notify 💙		1 - ??? 💙	
2 🗹	1 - Mail_Notify 💙		1 - ??? 💌	
3 🗌	1 - Mail Notify 2 - ???		1 - ??? 💙	
4	3 - ??? 4 - ???		1 - ??? 💙	
5 🗌	5 - ???		1 - ??? 💙	
6	7 - ??? 8 - ???		1 - ??? 💙	
7 🗌	9 - ???		1 - ??? 💌	
8	1 - Mail_Notify V		1 - ??? 💙	
9	1 - Mail_Notify 💙		1 - ??? 💌	
10	1 - Mail_Notify 💙		1 - ??? 💙	

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.	

Cancel

Schedule	Type the schedule number that the notification will be sent out.
	You can click the <b>Schedule</b> (1-15) link to define the schedule.

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

# 3.11 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.



# 3.11.1 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.

Access Control Setur	1
Image: A start of the start	Enable PPTP VPN Service
$\checkmark$	Enable IPSec VPN Service
$\checkmark$	Enable L2TP VPN Service
<b>~</b>	Enable SSL VPN Service

**Note**: To allow VPN pass-through to a separate VPN server on the LAN, disable any services above that use the same protocol and ensure that NAT <u>Open Ports</u> or <u>Port Redirection</u> is also configured.

OK	Clear	Cancel	1
	oroar	Cancer	

# 3.11.2 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

VPN and Remote Access >> Remote Access Control Setup

PPP General Setup		
PPP/MP Protocol		LDAP Server Profiles for PPP Authentication
Dial-In PPP Authentication	РАР/СНАР/МЗ-СНАР/МЗ-СНАРv2 🗸	rd1
Dial-In PPP Encryption(MPPE)	Optional MPPE	Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for
Mutual Authentica	tion (PAP) 🛛 🔍 Yes 💿 No	PPP Authentication!!
Username		
Password		
IP Address Assignme	ent for Dial-In Users	
(When DHCP Disable	set)	
Assigned IP start	LAN 1 192.168.1.200	
	LAN 2 192.168.2.200	
	LAN 3 192.168.3.200	
	LAN 4 192.168.4.200	

OK

Item	Description
Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.
	<b>PAP or CHAP</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE)	<b>Optional MPPE</b> - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user



	does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.	
	Optional MPPE Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit)	
	<b>Require MPPE (40/128bits) -</b> Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. <b>Maximum MPPE -</b> This option indicates that the router	
	will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.	
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer.	
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 LAN.	
LDAP Server Profiles for PPP Authentication	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.	
	However, if there is no profile listed, simply click the link of <b>PPTP LDAP Profile</b> to create/add some new LDAP profiles you want.	
	For detailed information about LDAP application, refer to section 4.14 How to Implement the AD/LDAP Authentication for User Management?	

**Dray** Tek

## 3.11.3 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 IKE/IPSec General Setup Dial-in Set up for Remote Dial-in users and I	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 n	ot be encrypted.
High (ESP)	▼ AES entic.
	OK Cancel

VPN and Remote Access >> IPSec General Setup

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.
	<b>Pre-Shared Key -</b> Currently only support Pre-Shared Key authentication.
	Pre-Shared Key- Specify a key for IKE authentication



	<b>Confirm Pre-Shared Key-</b> Retype the characters to confirm the pre-shared key.
<b>IPSec Security Method</b>	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High</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.

# 3.11.4 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	ccounts:			Set to Fac	tory 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	<u>26.</u>	???	Х
<u>11.</u>	???	Х	<u>27.</u>	???	Х
<u>12.</u>	???	х	<u>28.</u>	???	х
<u>13.</u>	???	Х	<u>29.</u>	???	Х
<u>14.</u>	???	х	<u>30.</u>	???	х
<u>15.</u>	???	Х	<u>31.</u>	???	Х
<u>16.</u>	???	х	<u>32.</u>	???	х



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 Name	one	
🗹 Enable this	account	
O Accept Any	Peer ID	
Accept Subj	ect Alternative Name	
Туре		IP Address 👻
IP		
OAccept Subj	ect Name	
Country (C)		
State (ST)		
Location (L)		
Orginization (	(0)	
Orginization (	Jnit (OU)	
Common Nam	ne (CN)	
Email (E)		

Item	Description
Profile Name	Type the name of the 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 Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

### 3.11.5 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.

Index	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>	???		
<u>16.</u>	???			<u>32.</u>	???		

#### VPN and Remote Access >> Remote Dial-in User

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 enable the selected profile.			
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.			



Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> Remote Dial-in Use
---------------------------------------------

Index No. 1	
User account and Authentication  ✓ Enable this account  Idle Timeout 300 second(s)  Allowed Dial-In Type  ✓ PPTP ✓ IPsec Tunnel ✓ L2TP with IPsec Policy None ✓	Username ??? Password(Max 19 char) Enable Mobile One-Time Passwords(mOTP) PIN Code Secret KE Authentication Method Pre-Shared Key KE Pre-Shared Key
✓ SSL Tunnel         Specify Remote Node         Remote Client IP         or Peer ID         Netbios Naming Packet          Netbios Naming Packet          Pass          Block         (for some IGMP,IP-Camera,DHCP Relayetc.)	Digital Signature(X.509)   None   IPsec Security Method   ✓ Medium(AH)   High(ESP)   ✓ DES   JDES   AES   Local ID (optional)
Subnet LAN 1  Assign Static IP Address 0.0.0 OK C	

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.				

Item	Description
	<b>SSL Tunnel</b> – Allow the remote dial-in user to make an SSL VPN connection through Internet.
	<b>Specify Remote Node -</b> Check the checkbox to specify the IP address of the remote dial-in user, or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the
	connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .
	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.
Subnet	Chose one of the subnet selections for such VPN profile.
	LAN 1 LAN 1 LAN 2 LAN 3 LAN 4
	Assign Static IP Address – Please type a static IP address for the subnet you specified.
	<b>User Name</b> - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for username is 16 characters.
	<b>Password</b> - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 16 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).
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.
	<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



Item	Description
	pre-shared key. <b>Digital Signature (X.509)</b> – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer</b> <b>Identity.</b>
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. <b>Medium-Authentication Header</b> (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.
	<b>High-Encapsulating Security Payload (ESP)</b> means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
	<b>Local ID (optional)-</b> Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

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

## 3.11.6 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 according to the item (All/Trunk) selected for **View**.

LAN-to	LAN Profiles					Set to	Factory Default
View:	⊙ All O Trunk						
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>	???		
<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>	???		
			OK	Can	cel		

VPN and Remote Access >> LAN to LAN

[XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism] [XXXXXX:This Dial-out profile does not join for VPN TRUNK]

#### The following shows profiles joined into VPN Backup mechanism.

#### VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:			
View: 🔿 All 🛛 💿 Trunk			
Name	Activate	Members	Status

[XXXXXX:This Dial-out profile has already joined for VPN Backup Mechanism]

Item	Description
View	All – Click it to display the LAN to LAN profiles. <b>Trunk</b> – Click it to display the Trunk profiles.
Set to Factory Default	Click to clear all indexes.

Name	Indicate the name of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.
Active	Check the box to enable the selected profile.
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.

Profile Index : 1 1. Common Settings	
Profile Name ???	Call Direction 🛛 📀 Both 🔿 Dial-Out 🔿 Dial-in
Enable this profile	Always on
	Idle Timeout 300 second(s)
VPN Dial-Out Through WAN1 First 🛛 👻	Enable PING to keep alive
Netbios Naming Packet	PING to the IP
Multicast via VPN OPass 💿 Block	
(for some IGMP,IP-Camera,DHCP Relayetc.)	
2. Dial-Out Settings	
Type of Server I am calling	Username ???
	Password(Max 15 char)
O IPsec Tunnel	PPP Authentication
C L2TP with IPsec Policy None	PAP Only
Server IP/Host Name for VPN.	VJ Compression 💿 On 🔘 Off
(such as draytek.com or 123.45.67.89)	IKE Authentication Method
	Pre-Shared Key
	IKE Pre-Shared Key
	O Digital Signature(X.509)
	Peer ID None V
	Local ID
	• Alternative Subject Name First
	🔘 Subject Name First
	Local Certificate None 😪
	IPsec Security Method
	Medium(AH)
	O High(ESP) DES without Authentication 💟
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:

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.	
	<b>VPN Dial-Out Through -</b> Use the drop down menu to choose a proper WAN interface for this profile. This setting	

is useful for dial-out only.
VPN Dial-Out Through
WAN1 First
WAN1 First WAN1 Only
WAN2 First
WAN2 Only
WAN1 only: Only establish VPN if WAN2 down
WAN2 only: Only establish VPN if WAN1 down WAN3 First
WAN3 Only
O IPsec Tunnel
• WAN1 /WAN2 /WAN3 First - While connecting, the
router will use WAN1 /WAN2 /WAN3 as the first
channel for VPN connection. If WAN1 fails, the
router will use another WAN interface instead.
• WAN1 /WAN2 /WAN3 Only - While connecting, the
router will use WAN1 /WAN2 /WAN3 as the only channel for VPN connection.
<ul> <li>WAN1 only: Only establish VPN if WAN2 down-</li> </ul>
While connecting, the router will use WAN2 for VPN
connection. If WAN2 fails, the router will use backup
WAN1 interface instead.
• WAN2 only: Only establish VPN if WAN1 down -
While connecting, the router will use WAN1 for VPN
connection. If WAN1 fails, the router will use backup
WAN2 interface instead.
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.
<ul> <li>Block – When there is conflict occurred between the</li> </ul>
hosts on both sides of VPN Tunnel in connecting,
such function can block data transmission of Netbios
Naming Packet inside the tunnel.
Multicast via VPN - Some programs might send multicast
packets via VPN connection.
• <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.
Both:-initiator/responder
• <b>Dial-Out</b> - initiator only
• <b>Dial-In-</b> responder only.
Always On-Check to enable router always keep VPN connection.
Idle Timeout: The default value is 300 seconds. If the
connection has been idled over the value, the router will
drop the connection.



	<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> <li>Enable PING to keep alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).</li> <li>PING to the IP - Enter the IP address of the remote host</li> </ul>
	that located at the other-end of the VPN tunnel.
<b>Dial-Out Settings</b>	<b>Type of Server I am calling:</b> <b>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.
	<ul><li><b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.</li><li><b>L2TP with IPSec Policy -</b> Build a L2TP VPN connection</li></ul>
	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 maximum length for username is 49 characters.
	<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 15 characters.
	<b>PPP Authentication -</b> This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP/MS-CHAP/MS-CHAPv2 is the most common selection due to wild compatibility.
	<b>VJ compression -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ

com	pression is used for TCP/IP protocol header pression. Normally set to <b>Yes</b> to improve bandwidth
IKE	zation. 2 <b>Authentication Method -</b> This group of fields is icable for IPSec Tunnels and L2TP with IPSec Policy.
•	<b>Pre-Shared Key</b> - Input 1-63 characters as pre-shared key.
•	<b>Digital Signature (X.509)</b> - Click Digital Signature to invoke this function and select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> as <b>Peer ID</b> .
	Local ID – Specify which one will be inspected first.
	<ul> <li>Alternative Subject Name First – The alternative subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
	<ul> <li>Subject Name First – The subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
	<b>Local Certificate</b> – Select one of the profiles set in <b>Certificate Management&gt;&gt;Local Certificate</b> .
	ec Security Method - This group of fields is a must for ec 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.
•	<b>High (ESP-Encapsulating Security Payload)-</b> 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>vanced</b> - Specify mode, proposal and key life of each phase, Gateway, etc.
	window of advance setup is shown as below:



RE advanced settings				
DKE phase 1 mode	Main mod	e	O Appressive mode	
IKE phase 1 proposal				-
IKE phase 2 proposal				
DKE phase I key Metme	28800	(900 ~ 86400)		
DE phase 2 key lifetone	3600	(600 - 86400)		
Perfect Forward Secret	() Disable		C Enable	
Local ID				

**IKE phase 1 mode -**Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

- **IKE phase 1 proposal-**To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
- **IKE phase 2 proposal-**To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
- **IKE phase 1 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
- **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.
- **Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

**Local ID-**In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

#### 3. Dial-In Settings

Allowed Dial-In Type		Username	222
		1	
☑ PPTP ☑ IPsec Tunnel		Password(Max 11 char)	
L2TP with IPsec Policy None		VJ Compression	💿 On 🔘 Off
L2 IP with IPsec Policy None		IKE Authentication Method	
Specify Remote VPN (	Catoway	Pre-Shared Key	
Peer VPN Server IP	Galeway		
		IKE Pre-Shared Key	
		Digital Signature(X.50	19)
or Peer ID		None 🔽	
		Local ID	
		Alternative Subje	
		OSubject Name Firs	st
		IPsec Security Method	
		Medium(AH)	
		High(ESP) 🛛 🗹 DES 🗹	3DES 🗹 AES
4. GRE over IPsec Settings		•	
🔲 Enable IPsec Dial-Out	function GRE over IPsec		
Logical Traffic My GRE IP		Peer GRE IP	
5. TCP/IP Network Settings			
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remo	te network, you have to
Remote Network IP	0.0.0.0	do	Route 🗸
			Roule
Remote Network Mask	255.255.255.0	Change default route	to this VPN tunnel ( Only
Local Network IP	192.168.1.1	single WAN supports this	
Local Network Mask	255.255.255.0		
	More		
L		1	
	ОК С	lear Cancel	

Item	Description	
Allowed Dial-In Type	Determine the dial-in connection with different types. <b>PPTP -</b> Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.	
	<b>IPSec Tunnel-</b> Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.	
	<b>L2TP with IPSec Policy -</b> Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:	
	• None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.	
	• Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.	
	• <b>Must</b> - Specify the IPSec policy to be definitely applied	



	on the L2TP connection.
	<b>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 L2TP with or without IPSec policy above. The maximum length for both username is 11 characters.
	<ul> <li>Password - This field is applicable when you select PPTP of L2TP with or without IPSec policy above. The maximum length for both username is 11 characters.</li> <li>VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when y select PPTP or L2TP with or without IPSec policy above.</li> </ul>
	<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 onl 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 invot this function and type in the required characters (1-63) as the pre-shared key. <b>Digital Signature (X.509)</b> –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> .
	Local ID – Specify which one will be inspected first.
	• Alternative Subject Name First – The alternative subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
	• Subject Name First – The subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
	<b>IPSec Security Method</b> - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specific the remote node.
	• <b>Medium-</b> Authentication Header (AH) means data wil be authenticated, but not be encrypted. By default, this option is active.
	<ul> <li>High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. Yo may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</li> </ul>
<b>GRE over IPSec</b>	Enable IPSec Dial-Out function GRE over IPSec: Check
Settings	this box to verify data and transmit data in encryption with

	<ul> <li>GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.</li> <li>Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.</li> <li>My GRE IP: Type the virtual IP for router itself for verified by peer.</li> <li>Peer GRE IP: Type the virtual IP of peer host for verified by router.</li> </ul>
TCP/IP Network Settings	<b>My WAN IP</b> - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, 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.
	<b>Remote Gateway IP</b> - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the 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.
	<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> Add a static route to direct all traffic destined to Local Network IP Address/Local Network Mask through the VPN connection.
	<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.



🚰 http://192.168.1.1 - LAN-to-LAN Profile - Microsoft Internet Explorer 💽 🗖 🔀
Profile Index :1
Remote Network
Network IP
Netmask
255.255.255.255 / 32 💌
Add Delete Edit
· · · · · · · · · · · · · · · · · · ·
<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.
<b>From first subnet to remote network, you have to 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. Note that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

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

## 3.11.7 VPN TRUNK Management

VPN trunk includes some features - VPN Backup, GRE over IPSec, and Binding tunnel policy.

#### Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- > VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, and L2TP over IPSec (depends on hardware specification)
- > The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network
- Mail Alert support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Syslog support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

**VPN TRUNK-VPN Backup** mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

VPN and Remote Access >> VPN TRUNK Management

0

Note:	[Active	(NO] The	LAN-to-LAN Profile is disabled o	r under Dial-In(Call Direction) at p	resent.
No.	Status	Name	Memberl (Active) Type	Member2(Active)Type	~
	anced				~

#### General Setup

Status	●Enable ○Disable
Profile Name	
Member1	Please select a LAN-to-LAN Dial-Out profile.
Member2	Please select a LAN-to-LAN Dial-Out profile.
Active Mode	Sackup

Add Update Delete

Item	Description		
Backup Profile List	<b>Set to Factory Default -</b> Click to clear all VPN TRUNK-VPN Backup mechanism profile.		
	<b>No</b> – The order of VPN TRUNK-VPN Backup mechanism profile.		
	<b>Status</b> - "v" means such profile is enabled; "x" means such profile is disabled.		
	<b>Name -</b> Display the name of VPN TRUNK-VPN Backup mechanism profile.		
	<b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.		
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.		
	<b>Type -</b> Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.		
	<b>Member2</b> - Display the dial-out profile selected from the Member2 drop down list below.		
	Advanced – This button is available only when LAN to LAN profile (or more) is created.		
	http://192.168.1.1 - VPN Backup Advance Settings - Microsoft Internet Explorer VPN Backup Advance Settings   Profile Name: Backup1   ERD Mode: ③ Normal   © Resume (Member 1 first)   Detail Information:   Environment Recovers Detection (ERD) Status: Normal Mode   OK Close		
	Detailed information for this dialog, see later section - Advanced Backup.		
General Setup	Status- After choosing one of the profile listed above, please click Enable to activate this profile. If you clickDisable, the selected or current used VPNTRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.		
	<b>Profile Name</b> - Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields.		
	Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >> LAN-to-LAN) for you to choose for grouping under certain VPN TRUNK-VPN Backup mechanism profile.		
	• No - Index number of LAN-to-LAN dial-out profile.		

<ul> <li>Name - Profile name of LAN-to-LAN dial-out profile.</li> <li>Connection Type - Connection type of LAN-to-LAN</li> </ul>
dial-out profile.
• VPN ServerIP (Private Network) - VPN Server IP of LAN-to-LAN dial-out profiles.
Active Mode - Display available mode for you to choose.
Add - Add and save new profile to the backup profile list.
<b>Update -</b> Click this button to save the changes to the <b>Status</b> (Enable or Disable), profile name, member1 or member2.
<b>Delete -</b> Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

### Time for activating VPN TRUNK – VPN Backup mechanism profile

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

# **Dray** Tek

#### How can you set a VPN TRUNK-VPN Backup mechanism profile?

- First of all, go to VPN and Remote Access>>LAN-to-LAN. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup mechanism profile management well.
- 2. Access into VPN and Remote Access>>VPN TRUNK Management.
- 3. Set one group of VPN TRUNK VPN Backup mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.

Status	C Enable C Disable
Profile Name	071023
Member1	Please choose the combination that you want.
Member2	Please choose the combination that you want.
Attribute Mode	Please choose the combination that you want       No. (Name) <connection-type>       1     To-A PlaceIPSec       2     To-B Site IPSec       192.168.2.25(20.20.20.0)</connection-type>

4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

Index	Name	Status
<u>1.</u>	To-A Place	V
<u>2.</u>	To-B Site	V
<u>3.</u>	To-C place	V
<u>4.</u>	To-D Site	V
5	222	~

VPN and Remote Access >> LAN to LAN

### How can you set a GRE over IPSec profile?

- 1. Please go to LAN to LAN to set a profile with IPSec.
- 2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

		Callback Budget	0 minute(s)
4. GRE over IPSec Setting	s		
Enable IPSec Dial-Out function GRE over IPSec			
🗖 Logical Traffic	My GRE IP 192.168.50.200	Peer GRE IP	192.168.50.100
5. TCP/IP Network Settings			
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	From first subnet to n do	emote network, you have to
Remote Network IP	Remote Network IP 192.168.10.0		Route 💌
Remote Network Mask	255.255.255.0		·



3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.

		Callback Budget	minute(s)	
4. GRE over IPSec Setting	3			
Enable IPSec Dial-Out function GRE over IPSec				
🗖 Logical Traffic	My GRE IP 192.168.50.100	Peer GRE IP 192	2.168.50.200	
5. TCP/IP Network Settings	3			
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both	
Remote Gateway IP	0.0.0.0	From first subnet to ren do	note network, you have to	
Remote Network IP	192.168.1.0		Route 💌	
Remote Network Mask	255.255.255.0		·	
	More	Change default route single WAN supports this	to this VPN tunnel ( Only )	
	OK CI	ear Cancel		

### **Advanced Backup**

After setting profiles for backup, you can choose any one of them and click **Advanced** for more detailed configuration.

ø	http://192.168.1.1 - V	'PN Backup Advance Settings - Microsoft Internet Explorer	
			^
,	/PN Backup Advanc	e Settings	
	Profile Name:	Backup1	
	ERD Mode:	💿 Normal	
		🔘 Resume (Member 1 first)	
	Detail Informa	tion:	
	Environment	Recovers Detection(ERD) Status: Normal Mode	<u>~</u>
		OK Close	
	r.		~
<			>

Item	Description		
Profile Name	List the backup profile name.		
ERD Mode	ERD means "Environment Recovers Detection".		
	<b>Normal</b> – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.		
	<b>Resume</b> – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.		
Detail Information	This field will display detailed information for Environment Recovers Detection.		



# 3.11.8 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management								
Dial-out T	ool				Refres	sh Seco	nds : 10	✓ Refresh
General Mode:		General Mode:			~	Dial		
Backup Mode:					*	Dial		
VPN Conn	ection Stat	us						
Current Pa	age: 1					Pag	je No.	Go >>
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
-					oxxxxxx : D oxxxxxx : D			

Item	Description
Dial-out Tool	General Mode - This filed displays the profile configured
	in LAN-to-LAN (with Index number and VPN Server IP
	address). The VPN connection built by General Mode does
	not support VPN backup function.
	Refresh Seconds :
	General Mode: (Alfa ) 192.168.0.26
	Backup Mode: (Alfa.) 192.168.0.26 Dial
	Bentley ) 192.168.0.27
	Audi ) 192.168.0.28 BMW ) 192.168.0.29
	Buick ) 192.168.0.30
	1 Cadillac ) 192.168.0.31 Page No.
	Chrysler ) 192.168.0.32
	Type Remote Citroen ) 192.168.0.33 Rx Rx Daihatsu ) 192.168.0.34 Pkts Rate
	Ferrari ) 192.168.0.35 : Data is er
	(Fiat) 192.168.0.36 🚽 : Data isn't
	Backup Mode - This filed displays the profile name saved
	in VPN TRUNK Management (with Index number and
	VPN Server IP address). The VPN connection built by
	Backup Mode supports VPN backup function.
	General Mode: (Alfa ) 192.168.0.26   Dial
	Backup Mode: (VpnBackup) 192.168.2.103  Dial
	(VpnBackup ) 192.168.2.103
	(VpnBackup) 192.168.2.203
	<b>Dial -</b> Click this button to execute dial out function.
	Refresh Seconds - 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.
	suuus.

# 3.12 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.



### 3.12.1 Local Certificate

Certificate Management >> Local Certificate

Subject	Status	Modify
 		View Delete
 		View Delete
 		View Delete

REFRESH

GENERATE MPORT

Available settings are explained as follows:

Item	Description		
Generate	Click this button to open <b>Generate Certificate Request</b> window.		
	Type in all the information that the window requests. Then click <b>Generate</b> again.		
Import	Click this button to import a saved file as the certification information.		
Refresh	Click this button to refresh the information listed below.		
View	Click this button to view the detailed settings for certificate request.		
Delete	Click this button to delete selected name with certification information.		

#### GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different



certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Certificate Management >> Local Certificate

Generate Certificate Signing Reques	đ
Certificate Name	
Subject Alternative Name	
Туре	IP Address 🛛 🐱
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA 🔽
Key Size	1024 Bit 💌

Generate

**Note:** Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
local	/C=TW/O=DrayTek/OU=RD/CN=192	Requesting	View Delete
			View Delete
			View Delete

GENERATE IMPORT REFRESH

**Dray** Tek

#### **IMPORT**

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Certificate Management >> Local Certificate
Import X509 Local Certificate
Upload Local Certificate Select a local certificate file.
Certificate file: Select
Click Import to upload the local certificate.
Import Cancel
Upload PKCS12 Certificate
Select a PKCS12 file.
PKCS12 file: Select
Password:
Click Import to upload the PKCS12 file.
Import Cancel
Upload Certificate and Private Key
Select a certificate file and a matchable Private Key.
Certificate file: Select
Key file: Select
Password:
Click Import to upload the local certificate and private key.
Import Cancel

n is generated by on, the Status of been imported successfully. to view the certificate.
been imported successfully.
Status
5/ OK
IMPORT REFRESH
e extensions are sually
ate keys and
50



	certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

#### REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.

🌀 Certi	ficate Signing Request Informat	ion - Google Chrome	- 0	x
192				Q
		Certificate Signing Request Information		
	Certificate Name :	local		
	Issuer :			
	Subject :	C=TW, O=DrayTek, OU=RD, CN=192.168.1.56, emailAddress=press@drayt	ek.com	
	Subject Alternative Name :			
	Valid From :			
	Valid To :			
	PEM Format Content :	BEGIN CERTIFICATE REQUEST MIIBpTCCAQ4CAQAwZTELMAkGALUEBMACYFCxEDAOBgNVBAoTBORYYX1UZWsxCzAJ BgNVBAsTAIJENRUWEWYDYQQDEwuxOTIUMTY4LjEUNTYxIDAeBgkqhkiG9w0BCQEW EXByZXN2QGRYYX10ZWsuY29tMI6fMAOGCSqGS1b3DQEBAQUAA4GNADCB1QKBgQCm 8SR1BR75Tcfq+ToA92JkvspQZsBqZm0xksQ/6q0mtNQ05/91N9VFm4N/Cs+V16e5 aklEwduHnJT91bVFVU/x54AaqKWC2baRobULp5tACeDHscTiHQmHYWUnFTDpxf0 z1RIYjuzi5dcp61reUB32LBWkxKy3rvHcPkKQ92QQIDAQABoAAwDQYJKoZIhvcN AQEFBQADgYEAc0+QYR34rj0tcXywxUIR/YRA676aUxJpeCs90AMQ40RguTx1orD YM01U170gsQ4m5UvbgwuWyMmxHrsM4KL4XftpKPWHff5AveCXWAOdcRlyT3vsWr 3zuyy4hCaV2i7ffn2tcLd2HBrLVpZsoP/CXn0UAsxCq9JQ9df+3TuxI= END CERTIFICATE REQUEST	a	
		Close		

**Note:** You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

**Dray** Tek

# 3.12.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Managemen	t >>	Trusted	CА	Certificate
-----------------------	------	---------	----	-------------

#### X509 Trusted CA Certificate Configuration

 	View Delete
 	View Delete
 	View Delete

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate
Select a trusted CA certificate file.
Browse.
Click Import to upload the certification.
Import Cancel

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

Cer 🧭	🖉 Certificate Information - Windows Internet Explorer 🛛 🔲 🗖 🔀				
🦲 http	://192.168.1.1/doc/XCaCfVi1.htm		<		
			^		
	Certif	icate Detail Information			
	Certificate Name:	Trusted CA-1			
	Issuer:	< ×			
	Subject:				
	Subject Alternative Name:				
	Valid From:				
	Valid To:				
		Close	~		
۲					

## 3.12.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup					
Certificate Back	up / Restoration				
Backup					
	Encrypt password:				
	Confirm password:				
	Click Backup to download certificates to your local PC as a file.				
Restoration					
	Select a backup file to restore.				
	Select				
	Decrypt password:				
	Click Restore to upload the file.				

# 3.13 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.

Registrar draytel.com Proxy a.com (sip: alice@draytel.com)

If you both register to the same SIP Registrar, then it will be illustrated as below:

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.





# 3.13.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

VoIP >> DialPlan Set	>
DialPlan Configurati	I
	Phone Book
	<u>Digit Map</u>
	<u>Call Barring</u>
	<u>Regional</u>
	PSTN Setup
Secure Phone config	ration
	Finable Secure Phone (7PTP+SPTP)

Enable SAS Voice Prompt
Enable Secure Phone (ZRTP+SRTP)

OK

Available settings are explained as follows:

Item	Description
Enable Secure Phone	It allows users to have encrypted RTP stream with the peer side using the same protocol (ZRTP+SRTP). Check this box to have secure call.
Enable SAS Voice Prompt	If it is enabled, SAS prompt will be heard for both ends every time. If it is disabled, no SAS prompt will be heard any more.

### **Application for Secure Phone**

Enable SAS Voice Prompt, for ex: if vigor router A calls vigor router B with checking **Enable Secure Phone** and **Enable SAS Voice Prompt**, then:

- 1. After the connection established, vigor router A will send SAS voice prompt to A and vigor router B will send the SAS voice prompt to B.
- 2. Then the RTP traffic is secured until the call ends.
- 3. If vigor router A wants to call vigor router B again next time, both A and B will not hear any voice prompt again even checking **Enable SAS Voice Prompt** on web UI. It means only the first call between them will have voice prompt.

Enable SAS Voice Prompt, for ex: if vigor router A calls vigor router B with checking **Enable Secure Phone** but not **Enable SAS Voice Prompt**, then:

- 1. After the connection established, vigor router A will **NOT** send SAS voice prompt to vigor router A and vigor router B will NOT send the SAS voice prompt to vigor router B.
- 2. Even no voice prompt, but the RTP traffic is still secured until the call ends.

**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.



#### 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.

hone Bo	ok							
Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Secure Phone	Status
<u>1.</u>				Default	None		None	х
<u>2.</u>				Default	None		None	х
<u>3.</u>				Default	None		None	х
<u>4.</u>				Default	None		None	х
<u>5.</u>				Default	None		None	х
<u>6.</u>				Default	None		None	х
<u>15.</u>				Default	None		None	х
<u>16.</u>				Default	None		None	х
<u>17.</u>				Default	None		None	х
<u>18.</u>				Default	None		None	х
<u>19.</u>				Default	None		None	х
<u>20.</u>				Default	None		None	х

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

VoIP >> DialPlan Setup

Click any index number to display the dial plan setup page.

Enable	ndex No. 1	
	Phone Number	1
	Display Name	Polly
	SIP URL	1112 @ fwd.pulver.com
	Dial Out Account	Default 💌
	Loop through	None 💌
	Backup Phone Number	
	Secure Phone	None 💌

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.
Secure Phone	<b>ZRTP+SRTP</b> - It allows users to have encrypted RTP stream with the peer side using the same protocol (ZRTP+SRTP). Check this box to have secure call.

**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	Mode	9	OP Number	Min Len	Max Len	Rout	е		Move Down
1		03	Replace	~	8863	7	8	PSTN	~		<u>Down</u>
2	<b>~</b>	886	Strip	*	886	9	10	PSTN	*	<u>UP</u>	<u>Down</u>
3			None	$\mathbf{v}$		0	0	PSTN	~	<u>UP</u>	<u>Down</u>
4			None	×		0	0	PSTN	×	<u>UP</u>	<u>Down</u>
5			None	~		0	0	PSTN	~	<u>UP</u>	<u>Down</u>
18			None	~		0	0	PSTN	~	<u>UP</u>	<u>Down</u>
۱9			None	v		0	0	PSTN	$\sim$	<u>UP</u>	<u>Down</u>
20			None	$\mathbf{v}$		0	0	PSTN	$\mathbf{v}$	<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.
	<b>Add</b> - 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 deleted by the prefix number for calling out through specific VoIP interface. Take the above picture (Pro Table Setup web page) as an example, the OP number 886 will be deleted completely for the prefix number with 886.	
	<b>Replace</b> - 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.	

# **Call Barring**

VoIP >> DialPlan Setup

Call barring is used to block phone calls coming from the one that is not welcomed.

Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Schedule	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

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.	
ОК	Cancel

Available settings are explained as follows:

Item	Description	
Enable	Check it to enable this entry.	
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.	
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	
🗹 Enable	
Route	🗌 Phone1 🔲 Phone2
Index(1-15) in <u>Schedule</u> Setup	
Note:Block the incoming calls which do not ha	ave 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 >> Dia	hIPIan Setup	
Call Barrin	ıg Block Unknown Domain	
🗹 Enable	9	
	Route	Phone1 Phone2
	Index(1-15) in <u>Schedule</u> Setup	
Note:If the be blocked	2	from the domain found in SIP accounts,the call should
	ОК	Cancel

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	
🗹 Enable	
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.

Cancel

ΟK

## 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		I	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 +#		
	OK	Cancel	

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 typed in this field to call back to that one.
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.	

### **PSTN Setup**

VoIP >> 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. Please type the number in the field of **phone number for PSTN relay**.

 umber for PSTN relay Enable	phone number for PSTN relay

Then, check the **Enable** box to make the PSTN number available for dial whenever you need.



## 3.13.2 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.

SIP Acc	ounts Lis	st						Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring	j Port	Status
1					G.729A/B	Phone1	Phone2	-
2					G.729A/B	Phone1	Phone2	-
<u>3</u>					G.729A/B	Phone1	Phone2	-
<u>4</u>					G.729A/B	Phone1	Phone2	-
<u>5</u>					G.729A/B	Phone1	Phone2	-
<u>6</u>					G.729A/B	Phone1	Phone2	-
Z					G.729A/B	Phone1	Phone2	-
<u>8</u>					G.729A/B	Phone1	Phone2	-
<u>9</u>					G.729A/B	Phone1	Phone2	-
<u>10</u>					G.729A/B	Phone1	Phone2	-
<u>11</u>					G.729A/B	Phone1	Phone2	-
<u>12</u>					G.729A/B	Phone1	Phone2	-

VoIP >> SIP Accounts

R: success registered on SIP server -: fail to register on SIP server

NAT Traversal Setting	
STUN Server:	
External IP:	
SIP PING Interval:	150 sec

ΟK

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.		
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 **None** 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 **Call without Registration**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call.

None	*
None	
Auto	
WAN1	
WAN2	
WAN3	
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		



	None – 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 Disable Always Busy No Answer Busy or No Answer 1		
	<ul> <li>SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.</li> <li>Time Out – Set the time out for the call forwarding. The default setting is 30 sec.</li> </ul>		
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.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps) iLBC_15 (15.20kbps) iLBC_13 (13.20kbps) Single Codec – If the box is checked, Codec will be applied.	only the selected
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. Packet Size	
	10ms <mark>20ms</mark> 30ms 40ms 50ms 60ms	
Voice Active Detector	This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.	
	Voice Active Detector Off 🕶 Off On	

# 3.13.3 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 🛛 10100000

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	<ul> <li>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 remote router to the private IP of local router), you can check this box to solve this problem.</li> <li>Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050.</li> <li>Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000.</li> <li>RTP TOS – It decides the level of VoIP package. Use the drop down list to choose any one of them.</li> </ul>							
	ManualIP precedence 1IP precedence 2IP precedence 3IP precedence 4IP precedence 5IP precedence 6IP precedence 7AF Class1 (Low Drop)AF Class1 (Medium Drop)AF Class2 (Low Drop)AF Class2 (Low Drop)AF Class2 (Low Drop)AF Class3 (Medium Drop)AF Class4 (Low Drop)AF Class4 (Medium Drop)AF Class4 (High Drop)AF Class4 (High Drop)							
	EF Class Manual							

## **Detailed Settings for Phone Port**

VoIP >> Phone Settings

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

Phone1	
Call Feature	Default SIP Account
Hotline	Play dial tone only when account registered
Session Timer 90 sec	
T.38 Fax Function	
Error Correction Mode REDUNDANCY 💌	
DND(Do Not Disturb) Mode	
Index(1-15) in <u>Schedule</u> Setup:	
Note: Action and Idle Timeout settings will be ignored.	
Index(1-60) in Phone Book as Exception List:	
CLIR (hide caller ID)	
Call Waiting	
Call Transfer	
ОК Са	ncel Advanced

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.
	<b>Index (1-15) in Schedule -</b> Enter the index of schedule profiles to control when the phone will ring and when will not according to the preconfigured schedules. Refer to section <b>Application</b> >> <b>Schedule</b> for detailed configuration.
	<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.
	<b>Play dial tone only when account registered -</b> 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

Tone Set	tings							
Region	User Defined	*		Ca	ller 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)	
Di	al tone	350	440	0	0	0	0	
Ring	jing tone	400	450	400	200	400	2000	
Bu	sy tone	400	0	375	375	0	0	
Conge	stion tone	400	0	400	350	225	525	
Volume	Gain			DTMF				
Mic Gain	(1-10)	5		DTMF Mode		OutBand (RFC2833)		
Speaker	Gain(1-10)	5	Payload Type (RFC28 (96 - 127)			³⁾ 101		
MISC		_						
Dial Tone	e Power Level	(1 - 50) 2	7					
Ring Free	quency (10 -	50HZ) 2	5					
Call Wait (1 - 30)	ting Tone Pow	ver Level 1	3					

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

	•		<b>ned</b> and fill out the tone, ringing tone, busy tone,
	congestion tone		
	Advance Se	ettings >> Pho	one
	Tone Sett	_	
	Region	User Defined	
		User Defined UK	.ow (⊩
	Dia	US Denmark	0
	Ringi		0
		Germany Netherlands	0
	Conges	Dortugal	
		Sweden	
	Volume G	Clouonia	
	Mic Gain(	Czech	
	Speaker (	Hungary	
	MISC	Switzerland	
	Dial Tone	France UK CCA	- 51
	Ring Freq	China	HZ)
		Taiwan	
		or you to use t	eld for your necessity. It is he default settings for VoIP
Volume Gain	of microphone	and speaker by	<b>in</b> ( <b>1-10</b> ) - Adjust the volume entering number from 1- 10. louder the volume is.
MISC	loudness of the	dial tone. The	s setting is used to adjust the smaller the number is, the commended for you to use the
		e ring tone. It i	g is used to drive the is recommended for you to use
	adjust the loudr	ness of the call ouder the tone	<b>evel</b> - This setting is used to waiting tone. The smaller the is. It is recommended for you
DTMF	DTMF Mode - choose.	- There are fou	r DTMF modes for you to
	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.

# 3.13.4 Status

From this page, you can find codec, connection and other important call status for each port.

```
VoIP >> Status
```

Status								Refresł	n Seco	nds:	10 💌	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	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5

Date (mm-dd-yyyy)		Time	Time Duration In/Out		Account ID	Peer ID
		(hh:mm:ss) (hh:mm				
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. xxxxxxxx : VoIP isn't encrypted.

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.

	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.	
	ACTIVE-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	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.	

# **3.14 Wireless LAN**

This function is used for "n" models only.

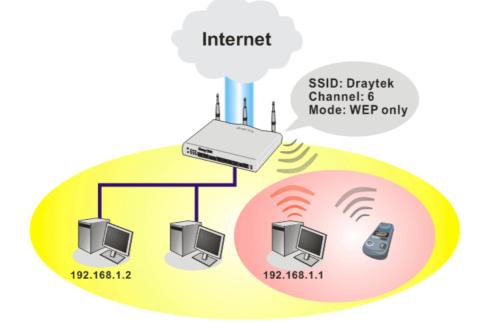
### 3.14.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

**Note**: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



### **Multiple SSIDs**

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.



### **Security Overview**

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

**Manage Wireless Stations - Station List** will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.





## 3.14.2 General Setup

Wireless LAN >> General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Mode :	ss LAN	Mixed(11b+11q+11n)		
Channel:		Channel 6, 2437MHz 🛛 👻		
Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1		DrayTek		
2		DrayTek_Guest		
3				
4				
to the san The isolat	ne SSID fror e VPN config	Aember configuration will forbi n connecting to each other. guration will isolate the wirele: ents will not be able to access	ss traffic from VPN co	nnections
Associateo Note:	d <u>Schedule</u> F	· .	)own" are applied to	]

OK Cancel

	channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.	
	Channel: Channel 6, 2437MHz ✓ Auto Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 12, 2467MHz	
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. The default SSID is "DrayTek". We suggest you to change it.	
Isolate	<ul> <li>VPN – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</li> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> </ul>	
Schedule	(stations) with the same SSID not accessing for each other. 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.	

### 3.14.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

The default security mode is **Mixed (WPA+WPA2)/PSK.** Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WPA and WEP.

Wirel	ess	$\Delta N >$	> Sec	uritv	Setting	ıs
	033		. 300	unity	Security	,

SSID 1	SSID 2	SSID 3	SSID 4
Mode:			Mixed(WPA+WPA2)/PSK
<u>WPA</u>			
	Encryption Mod	e:	TKIP for WPA/AES for WPA2
	Pre-Shared Key	(PSK):	*****
	Type 8~63 ASC example "cfgs0		64 Hexadecimal digits leading by "0x", for 55abcd".
<u>WEP</u>			
	Encryption Mod	e:	64-Bit 💉
	⊛ Key 1 :		****
	Key 2 :		****
	● Кеу З:		*****
	🔍 Key 4 :		*****
Note:			
Please	e configure the <b>F</b>	ADIUS Server if	802.1x is used.
			ease insert 5 ASCII characters or 10 xamples are "AB312" or "0x4142333132".
	28 bit WEP key c lecimal digits lea		please insert 13 ASCII characters or 26



Item	Description
Item Mode	Description         There are several modes provided for you to choose.         Disable         UWEP         WEP/802.1x Only         WPA/802.1x Only         WPA/802.1x Only         WPA/802.1x Only         WPA/802.1x Only         WPA/PSK         WPA/PSK         WPA2/PSK         Mixed(WPA+WPA2)/PSK         Note: You should also set RADIUS Server simultaneously if 802.1x mode is selected.
	<b>Disable</b> - Turn off the encryption mechanism. <b>WEP-</b> Accepts only WEP clients and the encryption key should be entered in WEP Key.
	<b>WEP/802.1x Only -</b> Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>WPA/802.1x Only-</b> Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>WPA2/802.1x Only-</b> Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>Mixed (WPA+WPA2/802.1x only) -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
	<b>WPA/PSK-</b> Accepts only WPA clients and the encryption key should be entered in PSK.
	<b>WPA2/PSK-</b> Accepts only WPA2 clients and the encryption key should be entered in PSK.
	<b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
	<b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only. <b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").



WEP	<b>64-Bit</b> - For 64 bits WEP key, either <b>5</b> ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, 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  $\mathbf{O}\mathbf{K}$  to save the configuration.

## 3.14.4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Enable Mac Address Filter	SSID 1 White List 🗸	🔲 SSID 2 White List 💌
	SSID 3 White List	SSID 4 White List
	MAC Address Filter	
Index Attribute	MAC Address	Apply SSID
Client's M.	AC Address :::	
	AC Address : : : : : : : : : : : : : : : : : :	
Apply SSID :		

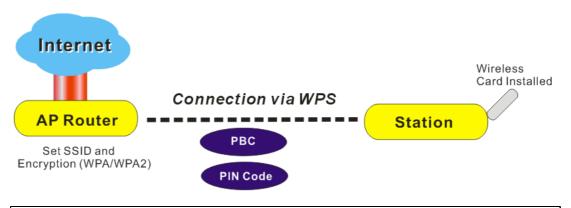
Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 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.

### 3.14.5 WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

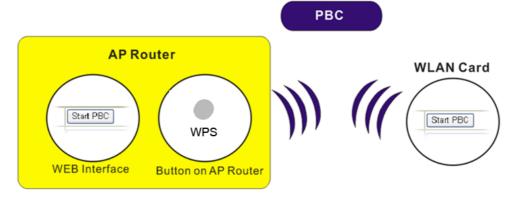


Note: Such function is available for the wireless station with WPS supported.

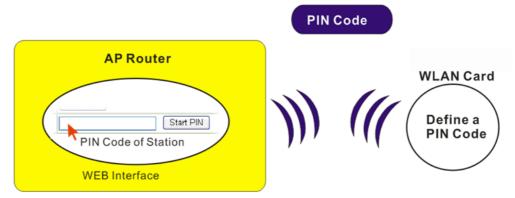
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 2830 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.

Microsof	t Internet Explorer 🛛 🔀
⚠	WPS only supports in WPA/WPA2-PSK Mode.
	ОК

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	Disable	

#### **Device Configure**

Configure via Push Button	Start PBC		
Configure via Client PinCode	Start PIN		

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

😳 : WPS is Enabled.

🗘 : Waiting for WPS requests from wireless clients.

### Available settings are explained as follows:

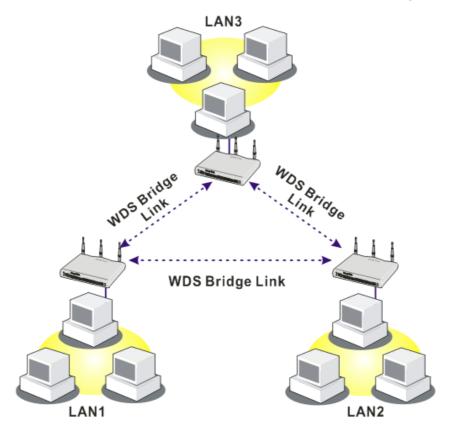
Item	Description		
Enable WPS	Check this box to enable WPS setting.		
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.		
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.		
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.		
Configure via Push Button	Click <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)		

### 3.14.6 WDS

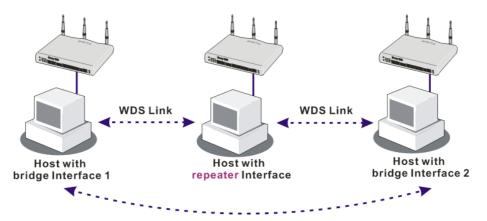
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:



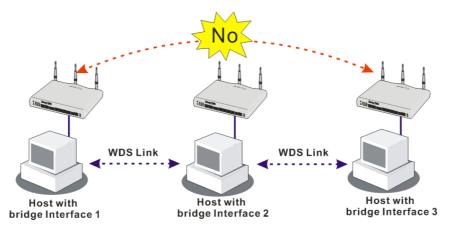
The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.



In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click WDS from Wireless LAN menu. The following page will be shown.

WDS Settings	Set to Factory Default			
Mode: Bridge 💌	Bridge Enable Peer MAC Address			
Security:				
Disable O WEP O Pre-shared Key				
WEP:				
Use the same WEP key set in <u>Security Settings</u> .	Note: Disable unused links to get better performance.			
Pre-shared Key:	·			
Type:	Repeater			
○ WPA	Enable Peer MAC Addess			
Key : *********				
Note: WPA and WPA2 are not compitable with				
DrayTek WPA.				
Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2" or				
"0x655abcd".	Access Point Function:			
	Status:			
	Send "Hello" message to peers.			
	Link Status			
	Note: The status is valid only when the peer also supports this function.			
ОК	Cancel			

Wireless LAN >> WDS Settings

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. <b>Disable</b> mode will not

	invoke any WDS setting. <b>Bridge</b> mode is designed to fulfill the first type of application. <b>Repeater</b> mode is for the second one. Disable Disable Bridge Repeater		
Security	There are three types for security, <b>Disable</b> , <b>WEP</b> and <b>Pre-shared key</b> . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.		
WEP	Check this box to use the same key set in <b>Security Settings</b> page. If you did not set any key in <b>Security Settings</b> page, this check box will be dimmed.		
Pre-shared Key	<b>Type</b> – There are some types for you to choose. <b>WPA</b> and <b>WPA2</b> are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router. <b>Key</b> - Type 8 ~ 63 ASCII characters or 64 hexadecimal 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.		



# 3.14.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN >> Advanced Setting

💿 Mixed Mode 🔘 Green Field
0 20 💿 20/40
🔘 long 💿 auto
🔿 Disable 💿 Enable
💿 Disable 🔘 Enable
💿 Disable 🔘 Enable

OK

Item	Description		
Operation Mode	Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected. Green Field – to get the highest throughput, please choose		
	such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.		
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	<ul> <li>This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Click Enable to use Long Preamble if needed to communicate with this kind of devices.</li> </ul>		
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.

**Note:** Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

- General Setting	Advance Setting		
Auto launch when Windows start up	Disable Radio		
Remember mini status position	Fragmentation Threshold :	2340	
🔲 Auto <u>h</u> ide mini status	RTS Threshold :	234	
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH 💙 1 💙 Disable 💙	
Enable IP Setting and Proxy Setting in Profile	Ad-hoc Channel:		
Group Roaming Ad-hoc	Power Save Mode:		
	Tx Burst :	Disable	
Infrastructure and Ad-hoc network     Infrastructurg network only     Ad-hoc network only     Ad-hoc network only			
		Cancel App	
	OK		

## 3.14.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE, AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.

WMM Configura	ation				Set to	Factory Default
WMM Capable		💿 Enable 🔘 Disable				
APSD Capable		🔘 Enable 💿 Disable				
WMM Paramet	ers of Access Po	pint				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
AC_BK	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
WMM Paramet	ers of Station					
	Aifsn	CWMin	C	WMax	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	
2						

Wireless LAN >> WMM Configuration

OK

Item	Description		
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.		
APSD Capable	The default setting is <b>Disable</b> .		
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.		
CWMin/CWMax	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO		

	categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.		
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.		
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> Vigor2920 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.		
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.		

## 3.14.9 AP Discovery

Wireless LAN >> Access Point 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			
				-		
l						
Scan						
See <u>Statistics</u> .						
<b>Note:</b> During the scanning process (~5 seconds), no station is allowed to connect with the router.						
Add to <u>WDS Settings</u> :						
AP's MA	C address	: ::::				
Add t	Add to 💿 Bridge 💿 Repeater					



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

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics
	Recommended channels for usage: 1 2 3 4 5 6 7 8 9 10 11 12 13
	AP number v.s. Channel
	1 2 3 4 5 6 7 8 9 10 11 12 13 14
	Channel
	Cancel
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click Add to. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

## 3.14.10 Station List

Wireless LAN >> Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Status MAC Address
Refresh
Status Codes :
C: Connected, No encryption. E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control. N: Connecting.
F: Fail to pass 802.1X or WPA/PSK authentication.
Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the
connection expires.
Add to <u>Access Control</u> :
Client's MAC address

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.	



# 3.14.11 Bandwidth Management

It controls the bandwidth limit for all the wireless clients accessing into Internet through such router.

#### Wireless LAN >> Bandwidth Management

SSID 1	SSID 2	SSID 3	SSID 4	
SSID:		Dra	ay⊤ek	
Enable		<ul> <li></li> </ul>		
Bandwid	th Limit Type	A	uto Adjustment 🔽	
Total Up	oload Limit(Kbps	) 30	000	
Total Do	ownload Limit(Kb	ops) 30	000	

Note: 1.Download: Traffic going to any station.Upload: Traffic being sent from a wireless station. 2.Allow auto adjustment could make the best utilization of available bandwidth.

OK ]	Cancel

Available settings are explained as follows:

Item	Description	
Enable	Click this button to enable such function.	
Bandwidth Limit Type	There are two types to be specifiy.          Auto Adjustment         Auto Adjustment         Per Station Limit	
Auto Adjustment	If you choose <b>Auto Adjustment</b> , the router will assign the required bandwidth for each wireless station according to the real usage.	
	<b>Total Upload Limit</b> –Default value is 30,000 kbps. All the wireless stations share the bandwidth for uploading without exceeding the valued typed here.	
	<b>Total Download Limit -</b> Default value is 30,000 kbps. All the wireless stations share the bandwidth for downloading without exceeding the valued typed here.	
Per Station Limit	If you choose <b>Per Station Limit</b> , the router will offer the bandwidth for each wireless station based on the values configured here.	
	<b>Upload Limit</b> –Default value is 30,000 kbps. Each wireless station can have the bandwidth for uploading without exceeding the values typed here.	
	<b>Download Limit -</b> Default value is 30,000 kbps. Each wireless station can have the bandwidth for uploading without exceeding the values typed here.	

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



# 3.15 SSL VPN

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

There are two benefits that SSL VPN provides:

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

SSL VPN
General Setup
SSL Web Proxy
SSL Application
User Account
User Group
Online User Status

### 3.15.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

```
Web Access Control >> General Setup
```

```
SSL VPN General Setup
```

· · · · · ·	
Port	443 (Default: 443)
Server Certificate	self-signed 💌
Encryption Key Algorithm	
○High - AES(128 bits) a	nd 3DES
💿 Default - RC4(128 bits	)
◯Low - DES	

Note: The settings will act on all SSL applications.

OK Cancel

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in <b>System</b> <b>Maintenance&gt;&gt;Management</b> . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose <b>Self-signed</b> to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.



Encryption Key	Choose the encryption level for the data connection in SSL
Algorithm	VPN server.

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

# 3.15.2 SSL Web Proxy

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

SSL Web Pi	oxy Servers Profiles:	I	Set to Factory Default
Index	Name	URL	Active
<u>1.</u>			×
<u>2.</u>			×
<u>3.</u>			x
<u>4.</u>			×
<u>5.</u>			x
<u>6.</u>			x
<u>7.</u>			x
<u>8.</u>			x
<u>9.</u>			x
<u>10.</u>			×

Each item is explained as follows:

Item	Description
Name	Display the name of the profile that you create.
URL	Display the URL.
Active	Display current status (active or inactive) of such profile.

Click number link under Index filed to set detailed configuration.

```
Web Access Control >> SSL Web Proxy
```

Profile Index : 1

Name		
URL		
Host IP Address		
Access Method	SSL	

**Note:** URL format must be entered as http://ip:port/directory or http://Domain_name/directory where Domain_name is a FQDN.

OK	Clear	Cancel
----	-------	--------

Item	Description
Name	Type name of the profile. The length of the name is limited to 15 characters.



URL	Type the address (function variation or IP address) or path of the proxy server.
Host IP Address	If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.
Access Method	There are three modes for you to choose.
	<b>Disable</b> – the profile will be inactive. If you choose <b>Disable</b> , all the web proxy profile appeared under VPN remote dial-in web page will disappear.
	<b>Secured Port Redirection</b> – such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute "Connect" manually in SSL Client Portal page.
	<b>SSL</b> – if you choose such selection, web proxy over SSL will be applied for VPN.

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

# 3.15.3 SSL Application

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

SSL Applicati	ons Profiles:		<u>S</u>	et to Factory Default
Index	Name	Host Address	Service	Active
<u>1.</u>				х
<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>				×

Web Access Control >> SSL Application

Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP or SAMBA path.
Service	Display the type of the service selected, e.g., VNC/RDP/SAMBA.
Active	Display current status (active or inactive) of the selected profile.



To create a new SSL application profile:

1. Click number link under Index filed to set detailed configuration.

### Web Access Control >> SSL Application

### **SSL Applications Profiles:**

Index	Name	F
<u>1.</u>		
<u>2.</u>		
3.		

2. The following page will appear.

Web Access Control >> SSL Application

Profile Index : 1	
Enable Application Service	
Application Name	VNC_1
Application	Virtual Network Computing (VNC)
IP Address	Please Select Virtual Network Computing (VNC)
Port	Remote Desktop Protocol (RDP) Samba Application
Idle Timeout	0 second(s)
Scaling	100% 💌

Clear

Cancel

Available settings are explained as follows:

ΟK

Item	Description	
Enable Application Server	Check the box to enable such profile.	
Application Name	Type a name for such application. The length of the name is limited to 23 characters.	
Application		

	remote PC through Samba service.
IP Address	If you choose VNC or RDP, you have to type the IP address for this protocol.
Port	If you choose VNC or RDP, you have to specify the port used for this protocol. The default setting is 5900.
Idle Timeout	If you choose VNC, you have to specify the time for disconnecting the SSL VPN tunnel.
Scaling	If you choose VNC, you have to choose the percentage (100%, 80%, 60%) for such application.
Screen Size	If you choose RDP, you have to choose the screen size for such application.
Samba Path	If you choose Samba, you have to specify the path of the Samba service.

- 3. Enter the required information.
- 4. After finished the above settings, click **OK** to save the configuration.

Web Access Control >> SSL Application

SSL Applicati	ons Profiles:		<u> </u>	et to Factory Default
Index	Name	Host Address	Service	Active
<u>1.</u>	VNC_1	192.168.1.54:5900	VNC	v
<u>2.</u>				×
<u>3.</u>				x
<u>4.</u>				×
5				

## 3.15.4 User Account

With SSL VPN, Vigor2830 series let teleworkers have convenient and simple remote access to central site VPN. The teleworkers do not need to install any VPN software manually. From regular web browser, you can establish VPN connection back to your main office even in a guest network or web cafe. The SSL technology is the same as the encryption that you use for secure web sites such as your online bank. The SSL VPN can be operated in either full tunnel mode or proxy mode. Now, Vigor2830 series allows up to 10 simultaneous incoming users.

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into **VPN and Remote Access>>Remote Dial-in user**.

Remote Ac	ccess User A	ccounts:				Set t	<u>o Factory Default</u>
Index	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>	???		
12.	???			<u>28.</u>	???		
<u>13.</u>	???			<u>29.</u>	???		
14.	???			<u>30.</u>	???		
<u>15.</u>	???			<u>31.</u>	???		
<u>16.</u>	???			<u>32.</u>	???		

Web Access Control >> Remote Dial-in User

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

OK Cancel

Click each index to edit one remote user profile.

#### Web Access Control >> Remote Dial-in User

Index No. 1	
User account and Authentication  Enable this account Idle Timeout  Allowed Dial-In Type	Username ??? Password(Max 19 char) Enable Mobile One-Time Passwords(mOTP) PIN Code Secret
<ul> <li>PPTP</li> <li>IPsec Tunnel</li> <li>L2TP with IPsec Policy None</li> <li>SSL Tunnel</li> <li>Specify Remote Node Remote Client IP</li> <li>or Peer ID</li> <li>Netbios Naming Packet          <ul> <li>Pass</li> <li>Block</li> <li>Multicast via VPN</li> <li>Pass</li> <li>Block</li> <li>(for some IGMP, IP-Camera, DHCP Relayetc.)</li> </ul> </li> </ul>	IKE Authentication Method         ✓ Pre-Shared Key         IKE Pre-Shared Key         Digital Signature(X.509)         None         IPsec Security Method         ✓ Medium(AH)         High(ESP)       ✓ DES ✓ 3DES ✓ AES         Local ID (optional)
LAN 1 V Assign Static IP Address	ear Cancel

Item	Description	
User account and Authentication	<b>Enable this account</b> - Check the box to enable this function. <b>Idle Timeout-</b> If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.	
Allowed Dial-In Type	<b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.	
	<b>IPSec Tunnel</b> - Allow the remote dial-in user to make an IPSec VPN connection through Internet.	
	<b>L2TP with IPSec Policy</b> - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:	
	• None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.	
	• Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.	
	• <b>Must</b> -Specify the IPSec policy to be definitely applied on the L2TP connection.	
	<b>SSL Tunnel -</b> It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g.,	



Item	Description		
	PPTP/L2TP/IPSec)		
	If you check this box, the function of SSL Tunnel for this account will be activated immediately.		
	<ul> <li>Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</li> </ul>		
	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.		
Subnet	Chose one of the subnet selections for such VPN profile.          Subnet         LAN 1         LAN 2         LAN 3         LAN 4    Assign Static IP Address – Please type a static IP address for the subnet you specified.		
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.		
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.		
Enable Mobile One-Time Passwords (mOTP)	<ul> <li>Check this box to make the authentication with mOTP function.</li> <li>PIN Code – Type the code for authentication (e.g, 1234).</li> <li>Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</li> </ul>		
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.		

Item	Description
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
	<b>Digital Signature (X.509)</b> – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer</b> <b>Identity.</b>
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. <b>Medium-Authentication Header</b> (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.
	<b>High-Encapsulating Security Payload (ESP)</b> means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
	<b>Local ID</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.

# **Dray**Tek

## 3.15.5 User Group

There are 10 user group profiles which can be created for authentication by LDAP server. Such profiles will be used by applications such as User Management, VPN and etc.

Web	Arross	Control >>	Hear	Group
web	ALLESS	Control >>	Usei	oroup

SSL User Group Profiles:		Set to Factory Default
Index	Name	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>		×

Each item is explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
Index	Display the number of the client which connecting to FTP server.
Name	Display the name of the group profile.

Click any index number link to open the following page for detailed configuration.

ndex No. 1		
Enable		
iroup Name		
Access Authority		
SSL Web Proxy	SSL Application	
Authentication Methods		
🔲 Local User DataBase		
Available User Accounts	Selected User Acco	unts
RADIUS	>>> <	
LDAP / Active Directory rd1 shrd		

Web Access Control >> User Group



Item	Description		
Item	Description		
Enable	Check this box to enable such profile.		
Group Name	Type a name for such profile. The length of the name is limited to 23 characters.		
Access Authority	Specify the authority for such profile.		
	At present, Vigor router allows you to create SSL Web Proxy and SSL Application profiles used for SSL VPN. The available profiles will be displayed here for you to select. Access Authority SSL Web Proxy SSL Web Proxy SSL_WP_1 Game_APP		
Authentication Methods	It can determine the authentication method used for such profile.		
	Local User DataBase – The system will do the authentication by using the user defined account profiles (in VPN and Remote Access>>Remote Dial-In User). The enabled profiles will be listed in the Available User Account on the left box. To add a profile into a group, simply choose the one from the left box and click the >> button. It will be displayed in the Selected User Account on the right box. For detailed information about configuring the profile setting, refer to Objects Setting>>IP Group.		
	<ul> <li>RADIUS – The RADIUS server will do the authentication by using the username and password</li> <li>LDAP / Active Directory - If it is checked, the LDAP / AD</li> </ul>		
	server will do the authentication by using the username, password, information stated on the selected profiles.		
	If the above three options are enabled, the system will do the authentication based on them in sequence.		

Available settings are explained as follows:

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

# 3.15.6 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into **DrayTek SSL VPN portal** interface.

Provide SSL VPN	Home	SSL Web Proxy SSL Tunnel	[ <u>loqout</u>
INFO	Main Page:		
mike , (172.17.1.42) Welcome to DrayTek SSL VPN!		You have successfully logged in! You are given the following privileges: <u>SSL Web Proxy</u> <u>SSL Tunnel</u>	
Timeout after 5 minutes. ( <u>Reset</u> )			

Next, users can open SSL VPN>> Online Status to view logging status of SSL VPN.

Web Access Control >> Online User Status

			Refresh Seconds : 10 🔽 refresh
Active User	Host IP	Time out(seconds)	Action
Kate	192.168.30.14	299	Drop

Item	Description
Active User	Display current user who visit SSL VPN server.
Host IP	Display the IP address for the host.
Time out	Display the time remaining for logging out.
Action	You can click <b>Drop</b> to drop certain login user from the router's SSL Portal UI.

# 3.16 USB Application

USB storage disk connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the Samba service through Vigor router.

USB Application
USB General Settings
USB User Management
File Explorer
USB Device Status
Modem Support List
System Maintenance

## 3.16.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English 💌
Samba Service Settings(Network Neigh	borhood)
<ul> <li>Enable</li> <li>Disable</li> <li>Access Mode</li> </ul>	
LAN Only LAN And WAN NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor
2. Multi-session ftp download v	, only English long file name is supported. vill be banned by Router FTP server. If your ftp client have multi- s FileZilla, you may limit client connections setting to 1 to get

3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; : " < > * + =  $/ \setminus |$ ?.



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. English English Chinese(Simple) Chinese(Traditional) German				
Samba Service Settings	Click <b>Enable</b> to invoke samba service via the router.				
Access Mode	<ul> <li>LAN Only – Users coming from internet cannot connect to the samba server of the router.</li> <li>LAN And WAN - Both LAN and WAN users can access samba server of the router.</li> </ul>				
NetBios Name Service	For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following; : " $<> * + = \setminus  $ ?.				
	Workgroup Name – Type a name for the workgroup.				
	Host Name – Type the host name for the router.				

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

### 3.16.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

USB User Management Set to Fa							
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>				

USB Application >> USB User Management

**Dray** Tek

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	
Access Rule	
File	🗌 Read 📃 Write 🔛 Delete
Directory	List Create Remove
lote: The folder name can only co and space.	ntain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) /

UK	Clear	Cancel
ON	Clear	Cancer

Item	Description
FTP/Samba User	<ul> <li>Enable – 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.</li> <li>Disable – Click this button to disable such profile.</li> </ul>
Username	Type the username for FTP/Samba users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk.
	<b>Note:</b> "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
	<b>Note:</b> FTP Passive mode is not supported by Vigor Router. Please disable the mode on the FTP client.
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.
	<b>Note:</b> When write protect status for the USB storage disk is <b>ON</b> , you cannot type any new folder name in this field. Only "/" can be used in such case.



You can click  $\overleftrightarrow{}$  to open the following dialog to add any new folder which can be specified as the Home Folder. 92.168.1.574 USB User Management ase Falder Folder Name ale New Hamu Fuld Folder Name: Cenata ote: The fo A-Z a-z 0-9 \$ % '-__@ ~ ' ( ( ) and der name can only contain the Only 11 characters are allower **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.

# 3.16.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB App	USB Application >> File Explorer							
File Exp	lorer							
<del>4)</del>	•	<b>9</b>	Current Path: /					
			Name		Size	Delete	Rename	
Uplo     Select a     Uploa	file: .d		Browse.					

note	me	rolder	can	nocibe	ueleteu	when	IC 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.

# 3.16.4 USB Device Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. In addition, the status of the USB modem or USB printer connecting to Vigor router can be checked from such page. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

#### USB Application >> USB Device Status

Disk	Modem	Printer	Refresh
JSB Mass Stor	age Device Status		
Connection ! Connected	Status: No Disk		Disconnect USB Disk
Disk Capacit	y: 0 MB		
Free Capacit	ty: O MB <u>Refresh</u>		
USB Disk Use	rs 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.

# 3.16.5 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 >> Modern Support List

The following compatibility tests listed above Vigor router models with USB modems / mobiles. If it is confirmed as the latest and still does not work, please contact support@draytek.com

3.5G L	TE	WiMAX		
Brand		Module		Status
AnyDATA	ADU-510/	۹.		Y
D-Link	DWM156			Y
Huawei	Huawei E	150		Y
Huawei	Huawei E	153		Y
Huawei	Huawei E	1550		Y
Huawei	Huawei E	Jawei E160E Y		Y
Huawei	Huawei E	łuawei E171 Y		Y
Huawei	Huawei E	Huawei E173 Y		Y
Huawei	Huawei E	łuawei E1750C Y		Y
Huawei	Huawei E	łuawei E1756C Y		Y
Huawei	Huawei E	Huawei E176c Y		Y
Huawei	Huawei E	Huawei E188 Y		Υ
Huawei	Huawei E	Huawei E220 Y		Y
Huawei	Huawei E	Huawei EC306 Y		Y
Huawei	Huawei K4511 Y		Y	

# 3.17 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Admin Password, User Password, Login Page Greeting, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, Firmware Upgrade and Activation.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
▶ TR-069
Admin Setting
User Password
Login Page Greeting
Configuration Backup
SysLog / Mail Alert
Time and Date
▶ SNMP
Management
Reboot System
Firmware Upgrade
Activation

# 3.17.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System S	Status						
Model Na Firmwar Build Da	e Version	: Vigor2830Vn : 3.6.7_db : Mar 24 2014 15:47:	36				
			LAN				
		MAC Address	IP Address	Subi	net Mask	DHCP Server	DNS
LAN1		00-50-7F-6A-FB-18	192.168.1.1	255.	.255.255.0	ON	8.8.8.8
LAN2		00-50-7F-6A-FB-18	192.168.2.1	255.	.255.255.0	ON	8.8.8.8
LAN3		00-50-7F-6A-FB-18	192.168.3.1	255.	.255.255.0	ON	8.8.8.8
LAN4		00-50-7F-6A-FB-18	192.168.4.1	255.	.255.255.0	ON	8.8.8.8
IP Rout	ed Subnet	00-50-7F-6A-FB-18	192.168.0.1	255.	.255.255.0	ON	8.8.8.8
			Marine Labl				
	.C Address		Wireless LAN	<b></b> ;			
		Frequency	Domain		ware Versior .0.7"		-1.
	-50-7F-6A-FB	-18 FCC		~2.2	.0.7	DrayT	ек
			WAN				
	Link Status	MAC Address	Conne	ction	IP Address	Default Gat	eway
WAN1	Disconnected	00-50-7F-6A-FB-1	9 PPPoE				,
WAN2	Disconnected	00-50-7F-6A-FB-1	A				
WAN3	Disconnected	00-50-7F-6A-FB-1	В				
			IPv6				
Δ	ddress			cope	Internet Ar	cess Mode	
		F:FE6A:FB18/64		nk			
			V-10				
Daut		Duefile	VoIP		T	0+	
Port		Profile		eg.		Out	
Phone1			No		0/0		
Phone2	:		No	J	0/0	J	

#### 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.

Wireless LAN	MAC Address
	- Display the MAC address of the wireless LAN.
	Frequency Domain
	- It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
	Firmware Version
	- It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
	<b>SSID</b> - Display the SSID of the router.
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.
VoIP	Profile
	- Display the VoIP profile for the phone port.
	In/Out
	- Display the number of incoming /outgoing phone call.

# **Dray** Tek

# 3.17.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

ystem Maintenance >> TR-069 Settin	ng
CS and CPE Settings	
ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client CPE Client Disable	
URL	http://172.16.3.102:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	•••••
eriodic Inform Settings	
O Disable	
📀 Enable	
Interval Time	900 second(s)
TUN Settings	
<ul> <li>Disable</li> </ul>	
<ul> <li>Enable</li> </ul>	
Server IP	
Server Port	3478
Minimum Keep Alive F	Period 60 second(s)
Maximum Keep Alive	
	ОК

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
CPE Client	Such information is useful for Auto Configuration Server. <b>Enable/Disable</b> – Allow/Deny the CPE Client to connect with Auto Configuration Server.
	<b>Port</b> – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.

Periodic Inform Settings	The default setting is <b>Enable</b> . Please set interval time or schedule time for the router to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.
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.

# 3.17.3 Admin Setting

This page allows you to set new password.

(Max. 23 characters allowed)
(Max. 23 characters allowed)

Note:Passwor	d can conta	in only a-z	A-Z 0-9	,;;·"	< > *	° + = \	?@#	$^{()}$
--------------	-------------	-------------	---------	-------	-------	---------	-----	---------

Administrator Local User	
Local User	
Local User List	
Index User Name	
	V
Specific User	
User Name:	
Password: Confirm Password:	
Add Edit Delete	
🗹 Enable 'Admin' Login From Wan	
Administrator LDAP Setting	
Enable LDAP/AD login for Admin users	
🗹 Enable 'Admin' Login From Wan	
LDAP Server Profiles	
LDAP Profile Setup	

Note: Please select 'Admin' from group select box on login UI.

OK

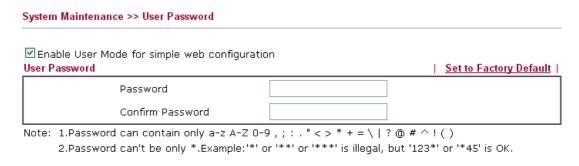
Available settings are explained as follows:

Item	Description	
Administrator Password	Old Password - Type in the old password. The factory default setting for password is "admin". New Password -Type in new password in this field. The	
	length of the password is limited to 23 characters.	
	<b>Confirm Password</b> -Type in the new password again.	
Administrator Local User	The administrator can login web user interface of Vigor router to modify all of the settings to fit the requirements. This feature allows other user in LAN who can access into the web user interface with the same privilege of the administrator.	
	<b>Local User</b> – Check the box to enable the local user configuration.	
	<b>Local User List</b> – It displays the username of the local user.	
	User Name – Give a user name for the local user.	
	<b>Password</b> – Type the password for the local user.	
	<b>Confirm Password</b> – Type the password again for confirmation.	
	Add – After typing the user name and password above, simply click it to create a new local user. The new one will be shown on the Local User List immediately.	
	<b>Edit</b> – If the username listed on the box above is not satisfied, simply click the username and modify it on the field of User Name. Later, click <b>Edit</b> to update the information.	
	<b>Delete</b> – If the local user listed on the box above is not satisfied, simply click the username and click <b>Delete</b> to remove it.	
	<b>Enable Admin Login From Wan</b> – The default setting is enabled. It can ensure any user accessing into web user interface of Vigor router through <b>Internet</b> by username/password of "admin/admin".	
Administrator LDAP Setting	<b>Enable LDAP/AD login for Admin users</b> – If it is enabled, any user can access into the web user interface of Vigor router through the LDAP server authentication.	
	<b>LDAP Server Profiles</b> – Available profiles will be displayed here under the link of LDAP Profile Setup.	
	<b>LDAP Profile Setup</b> – It allows you to create a new LDAF profile.	

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

## 3.17.4 User Password

This page allows you to set new password for user operation.



OK

Available settings are explained as follows:

Item	Description
Enable User Mode for simple web configuration	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Password	Type in new password in this field.
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.
- 2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

System Maintenance >> User Password	d	
Enable User Mode for simple web	configuration	
User Password		Set to Factory Default
Password	••••	]
Confirm Password	••••	
Note:Password can contain only a-z	A-Z 0-9 , ; : " < > * + = \   ? @	# ^ ! ( )
	OK	

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password			
Active Configuration			
Password	. No No No No No		

4. Log out Vigor router Web user interface.



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**.

6. The main screen with User Mode will be shown as follows.

uto Logout 💌 🛛 🛛 🥵	System Status					
zards line Status	Model Name Firmware Version Build Date/Time	: Vigor2830Vn : 3.6.7_db : Mar 24 2014 15:47::	36			
AN N			LAN			
ad-Balance/Route Policy T plications	LAN1 LAN2	MAC Address 00-50-7F-6A-FB-18 00-50-7F-6A-FB-18	IP Address 192.168.1.1 192.168.2.1		DHCP Server ON ON	DNS 8.8.8.8 8.8.8.8
reless LAN stem Maintenance ignostics	LAN3 LAN4 IP Routed Subnet	00-50-7F-6A-FB-18 00-50-7F-6A-FB-18 00-50-7F-6A-FB-18	192.168.3.1 192.168.4.1 192.168.0.1	255.255.255.0 255.255.255.0 255.255.255.0	ON ON ON	8.8.8.8 8.8.8.8 8.8.8.8
ternal Devices			Wireless LAN			
	MAC Address 00-50-7F-6A-FE	Frequency		Firmware Versio "2.2.0.7"	n SSID DrayT	ek
			WAN			
	Link Status WAN1 Disconnecte WAN2 Disconnecte			tion IP Address	Default Gat	eway
	WAN3 Disconnecte					
Logout			IPv6			
All Rights Reserved.	Address	F:FE6A:FB18/64	Sci Lin		ccess Mode	

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 and can be configured as same as in Admin Mode.

# **Dray** Tek

# 3.17.5 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 background message and the heading on the Login window if you have such requirement.

Enable		
Login Page Title	Router Login	(31 char max.)
Welcome Message a	nd Bulletin (Max 511 characters)	Preview Set to Factory Default
message is displa with your own mes in HTML so lists	pr=red>Welcome Messagesyed in the Login page of the sage. <ol><li>The welcor such as this one can be crea font or img can be used</li>&lt;</ol>	e router. Replace this text me message can be written ated <li>Other markup</li>
		2

OK Cancel

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.

Login for Test
Username Password
Login Copyright©, DrayTek Corp. All Rights Reserved. DrayTek Vigor:
This is an example of Bulletin feature of Vigor Routers
- 1. John, please pay your rent
- 2. Mary, please collect your electricity bill in the mailbox
- 3. Josh, could't manage to reach you but your parents were looking for you urgently

# 3.17.6 Configuration Backup

## **Backup the Configuration**

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup				
Configuration	Backup / Restoration			
Restoration				
	Select a configuration file.			
	Browse			
	Click Restore to upload the file.			
	Restore			
Backup				
	Click Backup to download current running configurations as a file.			
	Backup Cancel			

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Do	wnload 🛛 🕹
2	You are downloading the file:
4	config.cfg from 192.168.1.1
	And a data was the same the file of any internet same to 7
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	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.

iave As					?
Save in:	🞯 Desktop		~	0 # 10	<del>.</del>
My Recent Documents Desktop My Documents	My Documen My Computer My Network I RVS-COM Litr Annex A mmm MWSnap300 TeleDanmark Tools Config V2k2_232_cc V2k6_250_cc	Places ∋			
	File name:	config		~	Save
My Network	Save as type:	Configuration file		~	Cancel

4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

### **Restore Configuration**

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.
	Browse
	Click Restore to upload the file.
	Restore
Backup	
	Click Backup to download current running configurations as a file.
	Backup Cancel

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

# 3.17.7 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web user interface of the router or borrow debug equipments.

Svs	tem Maintenanc	e >>	SvsLog	/ Mail	Alert Set	up
	contraintention	<b>U</b>				

SysLog / Mail Alert Setup		
SysLog Access Setup	Mail Alert Setup	
<ul> <li>✓ Enable</li> <li>Syslog Save to:</li> <li>✓ Syslog Server</li> <li>USB Disk</li> <li>Router Name</li> <li>Server IP Address</li> <li>Destination Port</li> <li>514</li> <li>Mail Syslog</li> <li>Enable</li> <li>Enable syslog message:</li> <li>✓ Firewall Log</li> <li>✓ VPN Log</li> <li>✓ User Access Log</li> <li>✓ Call Log</li> <li>✓ Call Log</li> <li>✓ WAN Log</li> <li>✓ Router/DSL information</li> <li>AlertLog Port</li> <li>514</li> </ul>	<ul> <li>Enable</li> <li>SMTP Server</li> <li>SMTP Port</li> <li>Mail To</li> <li>Return-Path</li> <li>Use SSL</li> <li>Authentication</li> <li>Username</li> <li>Password</li> <li>Enable E-Mail Alert:</li> <li>Ø DOS Attack</li> <li>Ø IM-P2P</li> <li>Ø VPN LOG</li> </ul>	Send a test e-mail

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



Item	Description
SysLog Access Setup	<b>Enable</b> - Check <b>Enable</b> to activate function of syslog.
	<b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.
	Check <b>USB Disk</b> to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in <b>System</b> <b>Maintenance&gt;&gt;Management.</b>
	If there is no name here, simply lick the link to access into <b>System Maintenance&gt;&gt;Management</b> to set the router name.
	Server IP Address - The IP address of the Syslog server.
	<b>Destination Port -</b> Assign a port for the Syslog protocol.
	<b>Mail Syslog</b> – Check the box to recode the mail event on Syslog.
	<b>Enable syslog message -</b> Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to



	Syslog.
AlertLog Setup	Check "Enable" to activate function of alert log.
	<b>AlertLog Port</b> - Type the port number for alert log. The default setting is 514.
Mail Alert Setup	Check "Enable" 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.
	SMTP Server - The IP address 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>Authentication -</b> 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.

🎒 DrayTek S	yslog 4.5.3						للالك
Dr	<b>ay</b> Tek					Syslog U	tility
Log Filter	▰▦₽≍ᅇ	17	2.16.3.130	• •	WAN Inform	TX Rate	RX Rate
Keyword	Misc						IP I
Apply to:	Tool Setup Telnet Read-out Set	up Codepage Information Recov	ry Netwo	ork Information	Net State		
Firewall	Host Name	carrie-0c7cb251					
	NIC Description	Atheros AR8121/AR8113/AR8114	CI-E Ether	net Controller - Pa	acket Schedul 🔽		
System	NIC Information	· ·		On Line Routers		1	
	MAC Address	E0-CB-4E-DA-48-79		IP Address	Mask	MAC	
	IP Address	192.168.1.10	<b>~</b>	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	Ĩ				
	Lease Expires	Fri Aug 30 00:04:10 2013				Refresh	
					ОК	Cancel	
<							>

# 3.17.8 Time and Date

System Maintenance >> Time and Date

It allows you to specify where the time of the router should be inquired from.

Current System Time	2013 Oct 31 Thu 8 : 53 : 10 Inquire 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 Int	erval 30 min 💙

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. Auto Auto IPv6 First	
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.

#### 3.17.9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

Vications >> SNMP		
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>	
Set Community	Set community by typing a proper name. The default setting is <b>private.</b>	
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>	
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.	
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. No Auth MD5 SHA	
Auth Password	Type a password for authentication.	
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. No Priv DES AES	
Privacy Password	Type a password for privacy.	

### 3.17.10 Management

This page allows you to manage the settings for Internet Access Control, Access List from the 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 Setup	
Router Name	Management Port Setu	p
	💿 User Define Ports	🔘 Default Ports
Default:Disable Auto-Logout	Telnet Port	23 (Default: 23)
Internet Access Control	HTTP Port	80 (Default: 80)
Allow management from the Internet	HTTPS Port	443 (Default: 443)
FTP Server	FTP Port	21 (Default: 21)
HTTP Server	TR069 Port	8069 (Default: 8069)
HTTPS Server	TRU69 Port	
🗹 Telnet Server	SSH Port	22 (Default: 22)
🗹 TR069 Server		
SSH Server	External Device Control	
☑ Disable PING from the Internet	No respond to Exte	rnal Device
LAN Access Control		
🗹 Allow management from LAN		
FTP Server		
HTTP Server		
HTTPS Server		
🗹 Telnet Server		
SSH Server		
Apply To Subnet		
🗹 LAN2 🗹 LAN3 🗹 LAN4		
☑ IP Routed Subnet		
Access List from the Internet		
List IP Subnet Mask		
1		
2		
3		

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

OK	
----	--

Item	Description
Router Name	Type in the router name provided by ISP.
Default: Disable Auto-Logout	The web user interface will not log out if it is enabled.
Internet Access Control	Allow management from the Internet - Enable the



	<ul> <li>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><b>Disable PING from the Internet -</b> Check the checkbox to reject all PING packets from the Internet. For security issue,</li> </ul>
	this function is enabled by default.
LAN Access Control	Allow management from LAN - Enable the checkbox to allow system administrators to access from LAN. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	<b>Apply To</b> – Choose the subnet(s) for the administrator to access.
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	<b>User Defined Ports -</b> Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
	<b>Default Ports -</b> Check to use standard port numbers for the Telnet and HTTP servers.
External Device Control	<b>No respond to External Device</b> – Check the box to make Vigor2830 not being detected by other router and not being displayed as an external device.

#### For IPv6

System Maintenance >> Management

IP	∿4 Management Setup	IPv6 Management Setup	
Mana	agement Access Control		
Allo	w management from the Intern	et	
	] Telnet Server ( Port : 23)		
	HTTP Server ( Port : 80)		
	Enable PING from the Internet		
Acces	ss List		
List	IPv6 Address / Prefix Length		
1.		/ 128	
2.		/ 128	
з.		/ 128	
Note	: Telnt / Http server port is the	e same as IPv4.	
		ОК	

Item	Description
Management Access Control	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.

#### 3.17.11 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System** Maintenance to open the following page.

System Maintenance >> Reboot System
Reboot System
Do you want to reboot your router ?
Osing current configuration
O Using factory default configuration
Reboot Now Auto Reboot Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,,,
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 **OK**. To reset the router settings to default values, check **Using** factory default configuration and click **OK**. 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 **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.



### 3.17.12 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is ftp.DrayTek.com.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file. Select Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.6.7_db

Firmware Upgrade Procedures:

- 1. Click "OK" to start the TFTP server.
- 2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
- 3. Check that the firmware filename is correct.
- 4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
- 5. After the upgrade is compelete, the TFTP server will automatically stop running.

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

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.



#### 3.17.13 Activation

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

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.



OK Cancel

Available settings are explained as follows:

Item	Description	
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.	
	Activate via interface : auto-selected value auto-selected WAN 1 WAN 2 WAN 3	
Activate	The <b>Activate</b> link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.	
Authentication Message	As for authentication information of <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.	

Below shows the successful activation of Web Content Filter:

Activate 27]
ssful, 2010-07-27 📩



## 3.18 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.

System Maintenance
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

### 3.18.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

```
Diagnostics >> Dial-out Triggering
```

Dial-out Trigger	ed Packet Header	<u>Refresh</u>
	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	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	Decoded Format:	
	0.0.0.0 -> 0.0.0.0	
	Pr 0 len 0 (0)	

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

## 3.18.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
C~ 192.168.1.0/ 255.255.255.0	via 172.16.1.1 WAN2	
		~

or

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing	j Table			Refres	<u>sh</u>
Destination	Interface	-	Metric	Next	Нор	^
FE80::/64	LAN	U	256			
FF00::/8	LAN	U	256			
						~
<					>	

Item	Description
Refresh	Click it to reload the page.

#### 3.18.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

IP Address	MAC Address	Netbios Name	Interface	
172.16.3.166 192.168.1.1	00-26-6C-E4-6C-02 00-50-7F-CF-46-D8		WAN2 LAN1	
192.168.1.10	E0-CB-4E-DA-48-79	CARRIE-0C7CB251	LAN1 LAN1	
52.100.1.10	20 02 12 DA 10 /5	SARRE 00/05201		

Diagnostics >> View ARP Cache Table

Available settings are explained as follows:

Item	Description
Clear	Click it to clear the whole table.
Refresh	Click it to reload the page.

#### 3.18.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Diagnostics >> View IPv6 Neighbour Table

IPv6 Address	Mac Address	Interface	State	~
FF02::2	33-33-00-00-00-02	LAN	CONNECTED	
FF02::1:3	33-33-00-01-00-03	LAN	CONNECTED	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	STALE	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	CONNECTED	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	STALE	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	STALE	
FF02::1	33-33-00-00-00-01	LAN	CONNECTED	
FF02::1	00-00-00-00-00-00	USB2	CONNECTED	
FF02::1:2	00-00-00-00-00	USB2	CONNECTED	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	STALE	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	CONNECTED	
FE80::213:CEFF:FE0A:673C	00-13-ce-0a-67-3c	LAN	STALE	
FF02::1:FFB0:B00C	33-33-ff-b0-b0-0c	LAN	CONNECTED	
FE80::90:1A00:242:AD52	00-00-00-00-00	USB2	CONNECTED	
FF02::16	33-33-00-00-00-16	LAN	CONNECTED	~



Item	Description
Refresh	Click it to reload the page.

## 3.18.5 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

Diagnostics >> View DHCP Assigned IP Addresses

	DHCP IP Assignmen	it Table	DHCP	v6 IP Assignment Tab	le	IE	efresh
LAN1	: 192.168.1	.1/255.255.2	55.0, DHCP	server: On			~
Index	IP Address	MAC Addres	3	Leased Time	HOST	ID	
1	192.168.1.10	E0-CB-4E-D	A-48-79	10:10:54.970	carrie	e-0c7cb251	
2	192.168.1.1	00-1D-AA-0	0-00-00				
							~

or

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 Le	ased Time
		Y
<		>

Each item is explained as follows:

Item	Description
Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.



Leased Time	It displays the leased time of the specified PC.	
HOST ID	It displays the host ID name of the specified PC.	
Refresh	Click it to reload the page.	

## 3.18.6 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

```
Diagnostics >> NAT Sessions Table
```

#### NAT Active Sessions Table

Active Sessions	s Table					<u>Refr</u>
Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface	
	2491	52078	24.9.93.189	443	UAN1	
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.

## 3.18.7 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

Diagnostics >> Ping Diagnosis

Ping Diagnosis	
● IPV4 ○ IPV6	
Note: If you want to ping a ping through, please selec	a LAN PC or you don't want to specify which WAN to t "Unspecified".
Ping through: Unspecif	ied 💌
Ping to: Host / IP 💌	IP Address:
Host / IP DNS	Run
Result Gateway 1 Gateway 2	<u>Clear</u>
Gateway 3	
	×

#### or

Diagnostics >> Ping Diagnosis

Ping Diagnosis	
OIPV4 ⊙IPV6	
Ping IPv6 Address:	
Run	
Result	<u>Clear</u>
	~

Item	Description
IPV4 /IPV6	Choose the interface for such function.
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose <b>Unspecified</b> to be determined by the router automatically.



Ping to	Use the drop down list to choose the destination that you want to ping.	
IP Address	Type the IP address of the Host/IP that you want to ping.	
Ping IPv6 Address	Type the IPv6 address that you want to ping.	
Run	Click this button to start the ping work. The result will be displayed on the screen.	
Clear	Click this link to remove the result on the window.	

#### 3.18.8 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.

Limit	Session
-------	---------

💿 Enab	le 🔘 Disable	
Default N	Aax Sessions: 100	
Limitatio	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.

		Refresh Seconds: 1	10 💌 Page: 1 💌	<u>B</u>	efresh
Index	IP Address	TX rate(Kbps)	<u>RX_rate(Kbps)</u> 🛩	Sessions	Action
1	192.168.1.10_CARRIE-0C7CB251		0	2	Block
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak	c
WAN1		0 / 0 / Auto	0 / 0 / Auto		
WAN2	172.16.3.102	1 / 334 / Auto	7 / 788 / Auto		
WAN3		0 / 0 / Auto	0 / 0 / Auto		
Total		1 / 334 / Auto	7 / 788 / Auto	56 / 260	

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

3. (Kbps): shared bandwidth

+ : residual bandwidth used Current/Peak are average.



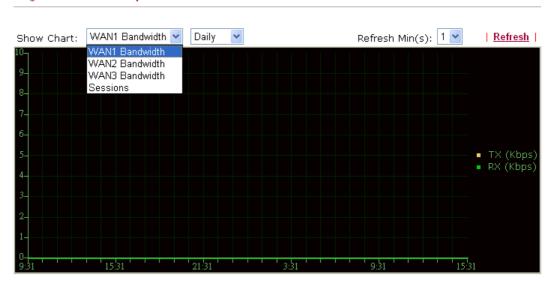
Available settings are explained as follows:
----------------------------------------------

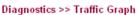
Item	Description			
Enable Data Flow Monitor	Check this box to enable this function.			
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.			
	10 15 30			
Refresh	Click this link to refresh this page manually.			
Index	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.			
Action	Session web page.         Block - can prevent specified PC accessing into Internet within 5 minutes.         Page: 1 <   Refresh           Kbps)       Sessions         Action         Imblock - the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.         Page: 1 <   Refresh           Sessions       Action         Imblock - the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.         Page: 1 <   Refresh           Sessions       Action         Imblock - the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.			
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>			



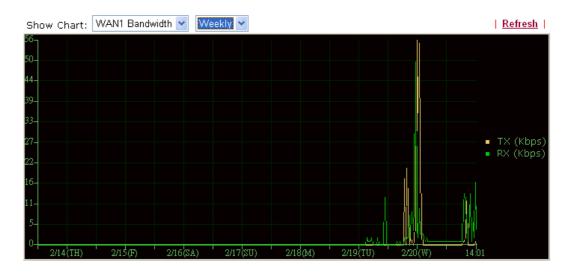
## 3.18.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1/WAN2/WAN3 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.









The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

#### 3.18.10 Trace Route

_ .

Click Diagnostics and click Trace Route to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click Run. The result of route trace will be shown on the screen.

Diagnostics >> Trace Route		
Trace Route		
● IPV4 ○ IPV6		
Trace through: Protocol:	Unspecified V	
Host / IP Address:		
Result	Run	<u>Clear</u>
		<u>~</u>
		×

or



Trace Route

Trace Host / IP Address:		
	Run	
Result	<u>Clea</u>	u I
		~

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 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.	

## 3.18.11 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

### For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

Web Syslog	USB Syslog	
Enable Web Syslog		<u>Export   Refresh   Clear</u>
Linable Web Syslog		
	Syslog Type 🛛 🕙 Display Mode	Stop record when fulls

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 Viewall Call WAN VPN All		
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.

USB Application >> Syslog Explorer

Web Syslog		USB Syslog		
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.

#### 3.18.12 IPv6 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

Diagnostics >> TSPC	C Status	
---------------------	----------	--

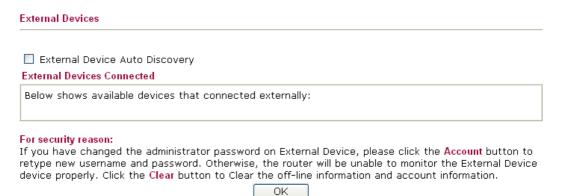
WAN1	WAN2	WAN3	Refresh
TSPC Enabled			
TSPC Connectio	n Status		
Local Endpoint	v4 Address :	1.169.155.138	
Local Endpoint	v6 Address :	2001:05c0:1400:000b:0000:0000:0000:b527	
Router DNS na	ime :	vigor2850.broker.freenet6.net	
Remote Endpo	int v4 Address :	81.171.72.11	
Remote Endpo	int v6 Address :	2001:05c0:1400:000b:0000:0000:0000:b526	
Tspc Prefix :		2001:05c0:1513:5900:0000:0000:0000:0000	
Tspc Prefixlen	:	56	
Tunnel Broker	:	amsterdam.freenet6.net	
Tunnel Status		Connected	

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

## **3.19 External Devices**

This page allows you to enable or disable the function of detecting external devices.



Item	Description
External Device Auto	Check this box to detect the external device automatically
Discovery	and display on this page.



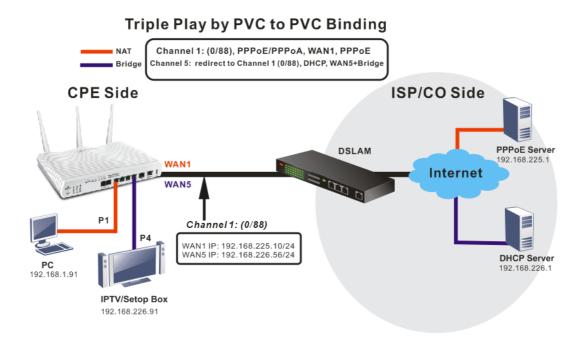
This page is left blank.

#### Vigor2830 Series User's Guide



# 4.1 How to Configure Multiple Services with PVC to PVC Binding

The router supports a new feature that single PVC can offer more than one service. The following illustration shows how to bind the functions of NAT and Bridge processed with one PVC.



From the above figure, Setop Box and DHCP server can reach for each other through WAN5 with Bridge mode; LAN PC in P1 beneath Vigor router can reach to PPPoE Server through WAN1 with NAT. Both NAT and Bridge are built through the same Channel 1.

Follow the steps listed below to configure the settings:

- 1. Log into the web user interface of Vigor router.
- 2. Open WAN>>Internet Access. Only PPPoE and MPoA 1483 Bridge can support PVC to PVC Binding feature, you have to choose PPPoE/PPoA as the Access Mode for WAN1.

nternet	Access				
Index	Display Name	Physical Mode	Access Mode		
WAN1		ADSL	PPPoE / PPPoA	*	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.

WAN >> Internet Access



3. Click the **Details Page** of WAN1 to display the following page. Check **Enable** and set **Channel 1** as **Multi-PVC channel**; set 0 and 88 for VPI and VCI; type the username (e.g., pppoeuser) and the password.

WAN >> Internet Access				
WAN 1		MPoA (RF	C1483/2684) SP Access Setup	IPv6
Enable     Di     Di     DSL Modern Settings	sable		Jsername	pppoeuser
Multi-PVC channel VPI VCI	Channel 1 0 33	~	eassword PPP Authentication Idle Timeout	PAP or CHAP V -1 second(s)
Encapsulating Type Protocol Modulation	LLC/SNAP V PPPoE V Multimode	~	IP Address From ISP Fixed IP O Yes Fixed IP Address	No (Dynamic IP)
PPPoE Pass-through			<ul> <li>Default MAC Add</li> <li>Specify a MAC Add</li> </ul>	

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

WAN >> Multi-PVCs

5. Open WAN>>Multi-PVCs. Click the General tab to check the box of Enable for the 5th WAN.

General	ATM Q	lo S	Port-based Bridge		PVC to PVC Binding/Add Tag		
hannel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation	
1.		0	88	UBR 💌	PPPoE 💌	LLC/SNAP	
2.		0	65	UBR 🗸	MPoA 🗸	1483 Bridged IP LLC	
з.		1	43	UBR 🖌	PPPoA 🛩	VC MUX	
4.		1	44	UBR 🗸	PPPoA 🗸	VC MUX 🗸	
5. <u>WA</u>	<u>N</u>	1	45	UBR 🖌	MPoA 💌	1483 Bridged IP LLC	
6. <u>WA</u>	N	1	46	UBR 🗸	PPPoA 🗸	VC MUX 🗸	
7. <u>WA</u>	N 🗌	1	47	UBR 🖌	PPPoA 🗸	VC MUX 🗸	
8.		1	48	UBR 🗸	PPPoA 🗸	VC MUX 😪	

Clear

Cancel

Note: Only 5th WAN to 7th WAN can be used for PVC to PVC Binding.

OK

6. Click the link of the 5th WAN to configure the settings. Choose **IPTV** as the **WAN for Router-borne Application**; check **Enable.** In the **DSL Modem Setup**, choose **MPoA** as the **Protocol**; and select **1483 Bridged IP LLC** as **Encapsulation**.

NAN for Router-borne Ap	plication:	
DSL Modem Settings VPI 1 VCI 45	QoS Type UBR Protocol MPoA Encapsulation 1483 Brid	
WAN Connection Detecti Mode Ping IP	ARP Detect	
TTL: PPPoE/PPPoA Client SP Access Setup		MPoA (RFC1483/2684) Obtain an IP address automatically

WAN >> Multi-PVCs >> PVC Channel 5

In this case, we want to redirect PVC channel 5 to PVC channel 1, we have to choose **1** as **PVC Binding.** Check the box of **Add Tag** and type **405** as the tag number.

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

WAN >> Multi-PVCs

8. The PVC Binding and the Tag setting can also be seen in WAN>>Multi-PVCs>>PVC to PVC Binding/Add Tag page.

eneral	ATM QoS	Port-based Bridge	PVC to PVC Bir	nding/Add Tag
Channe	el la	PVC Binding	Add Tag	Priority
1.		Disable 🗸	0	0
2.		Disable 😪	0	0
з.		Disable 🛩	0	0
4.		Disable 😽	0	0
5.		1 💌	✓ 405	0
6.		Disable 👻	0	0
7.		Disable 💌	0	0
8.		Disable 💌	0	0

OK	Clear	Cancel
----	-------	--------

Note: Channel 1 and Channel 2 are reserved for WAN1 service.

9. Click the tab of **Port-based Bridge**. Check the box of **Enable** for the 5th WAN. Check the box of P4. All of the traffic coming from LAN Port 4 will be directed to channel 5 first and then to channel 1.

eneral	ATM QoS P	ort-based E	Bridge		PVC to P	VC Binding/Add Tag
Channel	Enable	P1	P2	P3	P4	Service Type
1.						Normal 😽
2.						Normal 😪
3.						Normal 💌
4.						Normal 💌
5.					<b>V</b>	Normal 💌
6.						Normal 💌
7.						Normal 💌
8.						Normal 💌

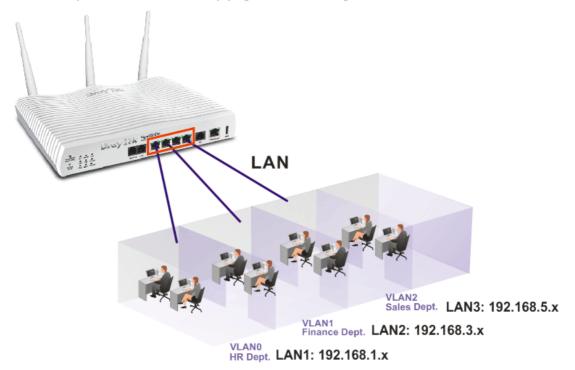
- 10. Click **OK** to save the settings.
- 11. Now, all the data from P1 transmitted to the remote PPPoE server via WAN1 and the data from P4 (IPTV) transmitted to the remote DHCP Server via WAN 5 are all processed by **Channel 1**.

# 4.2 How to Configure Multi-Subnet in Vigor2830

There are two types of VLAN. One is Port Based VLAN; the other is Tag Based VLAN. Refer to the following sections for learning the usage of VLAN.

#### I. Port Based VLAN

Vigor2830 can divide the physical LAN ports into several groups. For example, it can divide the internal departments of a company into three different groups. Each group uses different network segment. See the following graphic for an example.



Group 0 (VLAN0)(Human Resource): LAN Port 1 IP: 192.168.1.0/24 Group 1 (VLAN1)(Finance Dept): LAN Port 2 IP: 192.168.3.0/24 Group 2 (VLAN2)(Sales Dept.): LAN Port 3 \ Port 4 IP: 192.168.5.0/24

#### **Configuration:**

- 1. In the page of LAN >> VLAN Configuration, check the box of Enable to enable the function of VLAN Configuration.
- 2. For VLAN0 setting, check **P1** and set **LAN1** as the **Subnet**.
- 3. For VLAN1 setting, check P2 and set LAN2 as the Subnet.
- 4. For VLAN2 setting, check **P3** and **P4**, and set **LAN3** as the **Subnet**.



#### LAN >> VLAN Configuration

VLAN	Configuration
	Sonnganation

LAN >> General Setup

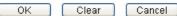
🗹 Enat	hle											
		IJ	AN			Wirele	ss LAN				VLAN Tag	I
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAN0	<b>~</b>								LAN 1 🔽		0	0 🗸
VLAN1		<b>~</b>							LAN 2 🔽		0	0 🗸
VLAN2			<b>V</b>	<b>V</b>					LAN 3 🔽		0	0 🔽
VLAN3									LAN 1 💌		0	0 🗸
VLAN4									LAN 1 🔽		0	0 🗸
VLAN5									LAN 1 💌		0	0 🔽
VLAN6									LAN 1 🔽		0	0 🗸
VLAN7									LAN 1 💌		0	0 🗸

Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;

2. The checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;

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



5. In the page of LAN >> General Setup, check the Status box of LAN2 and LAN3 and enable the function of DHCP.

General Setup					
Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	<ul> <li>Image: A start of the start of</li></ul>	<b>~</b>	192.168.3.1	Details Page	
LAN 3	<ul> <li>Image: A set of the set of the</li></ul>	<b>V</b>	192.168.5.1	Details Page	
LAN 4		<b>~</b>	192.168.7.1	Details Page	
IP Routed Subnet		V	192.168.0.1	Details Page	

Advanced You can configure DHCP options here.

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

After finishing the above configuration, the equipment connecting to Vigor2830 LAN Port can get the corresponding IP address of the network segment.

The equipment connecting to Vigor2830 LAN Port 1 (LAN1) can get the IP address of 192.168.1.0/24

The equipment connecting to Vigor2830 LAN Port 2 (LAN2) can get the IP address of 192.168.3.0/24

The equipment connecting to Vigor2830 LAN Port 3 and Port 4 (LAN3) can get the IP address of 192.168.5.0/24

For the detailed settings of the network segment, open LAN>>General Setup and click **Details Page.** Adjust the settings for your request. Refer to the following figure.



#### LAN >> General Setup

LAN 1 Ethernet TCP / IP a	nd DHCP Setup	LAN 1 IPv6 Setup		
Network Configuration		DHCP Server Configurati	on	
For NAT Usage		💿 Enable Server 🔘 Dis	able Server	
IP Address	192.168.1.1	Enable Relay Agent		
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
·		IP Pool Counts	200	]
RIP Protocol Control	Disable 🚩	Gateway IP Address	192.168.1.1	]
Note: Disable LAN & Enab same subnet.	le LAN shouldn't be in the	Lease Time	86400	(s)
		Retrieve IPs from ina	active clients periodica	ally
		DNS Server IP Address		_
		Primary IP Address		
		Secondary IP Address		]

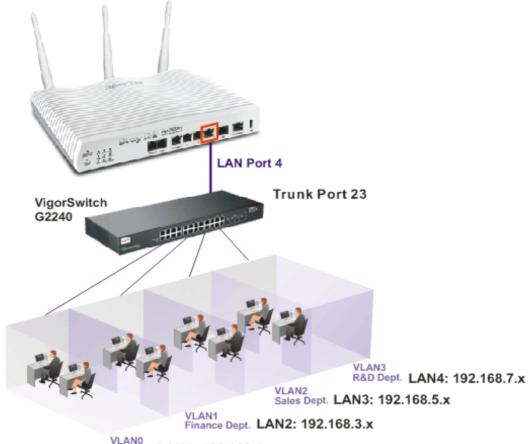
- ОК
- 6. To make any two of VLAN groups linked with each other, just check the boxes of the ones in the field of Inter-LAN Routing in the page of LAN >> General Setup. Refer to the following figure. LAN2 and LAN3 are linked.

Inter-LAN Routing				
Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	V			
LAN 2		V 🗹		
LAN 3		→ 🔽	¥	
LAN 4				1

#### II. Tag Based VLAN

By identifying the tagged message, Vigor2830 can divide the LAN Port into several VLAN groups. Such LAN port with tagged information will accept the packets only with VLAN ID number.

For example, Vigor2830 can divide the internal departments of a company into four different groups by using VigorSwitch 2240. Each group uses different network segment and does not link for each other. VigorSwitch 2240 Trunk Port 23 and Vigor2830 LAN Port 4 are connected with network cable. See the following graphic for an example.



VLAN0 HR Dept. LAN1: 192.168.1.x

Group 0 (VLAN0)( Human Resource): LAN Port 4 IP: 192.168.1.0/24 Group 1 (VLAN1)( Finance Dept): LAN Port 4 IP: 192.168.3.0/24 Group 2 (VLAN2)( Sales Dept.): LAN Port 4 IP: 192.168.5.0/24 Group 3 (VLAN3)(R&D): LAN Port 4 IP: 192.168.7.0/24

#### **Configuration for Vigor2830:**

- 1. In the page of LAN >> VLAN Configuration, check the box of Enable to enable the function of VLAN Configuration.
- 2. To activate the function of VLAN Tag for VLAN0 setting, check the box of **Enable** and type the value (7) for VID setting. Then check **P4** and set **LAN1** as the **Subnet**.
- 3. To activate the function of VLAN Tag for VLAN1 setting, check the box of **Enable** and type the value (8) for VID setting. Then check **P4** and set **LAN2** as the **Subnet**.
- 4. To activate the function of VLAN Tag for VLAN2 setting, check the box of **Enable** and type the value (9) for VID setting. Then check **P4** and set **LAN3** as the **Subnet**.



5. To activate the function of VLAN Tag for VLAN3 setting, check the box of **Enable** and type the value (10) for VID setting. Then check **P4** and set **LAN4** as the **Subnet**.

🗹 Enat	le	L	AN			Wirele	ss LAN				VLAN Tag	9
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
/LAN0				<b>V</b>	✓	✓	✓	<b>V</b>	LAN 1 🔽	<ul><li>✓</li></ul>	7	0 🗸
VLAN1				<b>~</b>					LAN 2 🔽	<b>~</b>	8	0 🗸
VLAN2				<b>V</b>					LAN 3 🔽	<b>~</b>	9	0 🗸
VLAN3				<b>~</b>					LAN 4 💌	<b>~</b>	10	0 🗸
VLAN4									LAN 1 💌		0	0 🗸
VLAN5									LAN 1 💌		0	0 🗸
VLAN6									LAN 1 💌		0	0 🗸
VLAN7									LAN 1 🔽		0	0 🗸

LAN >> VLAN Configuration

Permit untagged device in P1 to access router

1. Tag based VLAN only applied for LAN Ports;

LAN >> General Setup

2. The checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;

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

OK	Clear	Cancel

6. In the page of LAN >> General Setup, check the Status box of LAN2, LAN3 and LAN4 and enable the function of DHCP.

General Setup					
Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	✓	<b>~</b>	192.168.3.1	Details Page	
LAN 3	<b>V</b>		192.168.5.1	Details Page	
LAN 4	<b>~</b>	<b>~</b>	192.168.7.1	Details Page	
IP Routed Subnet			192.168.0.1	Details Page	

Advanced You can configure DHCP options here.

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

For the detailed settings of the network segment, open LAN>>General Setup and click **Details Page.** Adjust the settings for your request. Refer to the following figure.

#### LAN >> General Setup

LAN 1 Ethernet TCP / IP	and DHCP Setup	LAN 1 IPv6 Setup	
Network Configuration		DHCP Server Configuration	
For NAT Usage		📃 💽 Enable Server 🔘 Disable Server	
IP Address	192.168.1.1	🔲 Enable Relay Agent	
Subnet Mask	255.255.255.0	Start IP Address 192.168.1.10	
		IP Pool Counts 200	
RIP Protocol Control	Disable ⊻	Gateway IP Address 192.168.1.1	
		Lease Time 86400 (s	s)
		🔲 Retrieve IPs from inactive clients periodica	ally
		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	
L			

#### **Configuration for VigorSwitch 2240:**

- 1. Open Vlan>>Tag-based Group.
- 2. Add four VID groups. In this case, we can explanation it with Port 15, 16, 17, 18 and Trunk Port 23.

porSwitch G2240 System Port /lan					Private VL	1 1 1				opagati													
lan Mode ag-based Group	IGINP	A. IGIV	VLAN		Private VD		GVR	-P. G	RP PI	opagau	on		P	ort Me	mber	15							
orf-based Group	Del	VID	IGMP-A	P-VLAN	GVRP-P	1	2 3	4 5	6	7 8	9 1	10 11	12	13 1	4 1	15 10	5 17	18	19	20 2	1 2	2 23	2
orts			Defa	ault																			
ort Isolation lanagement Vlan		1	Disable	Disable	Disable	1																	2
MAC			2830-	VID7													-					-	-
SVRP		7	Disable	Disable	Disable											15						23	
QoS			2830-	VID8									1				-	-					
INMP		8	Disable	Disable	Disable											16						23	
NCL .		¥	2830-		Disable											-							-
P MAC Binding	-	0			Disable												17					23	
102.1X		9	Disable	Disable	Disable		_			_	_	_		_	_	_	1				_	_	_
frunk STP			2830-1															18				23	
ISTP		<u>10</u>	Disable	Disable	Disable																		
Airroring	1.1																						
Aulticast																							
larm																							

VLAN Name 2830-VID7, Port Members =  $15 \cdot 23$ VLAN Name 2830-VID8, Port Members =  $16 \cdot 23$ VLAN Name 2830-VID9, Port Members =  $17 \cdot 23$ VLAN Name 2830-VID10, Port Members =  $18 \cdot 23$ 

3. Open Vlan>> Ports and set the VID value with role for each Port:

Port 15 VID = 7 Role = Access Port 16 VID = 8 Role = Access Port 17 VID = 9 Role = Access Port 18 VID = 10 Role = Access Port 23 VID = 1 Role = Trunk

Port 23 is set with Trunk in this example and will transfer the packets with VLAN Tag information. That is, packets with VID 7, 8, 9 and 10 will be transferred to Vigor2830 by Port 23 and VID information will be retained.



DrayTek Auto Logout OFF 🕑	Dyay 20		I E	Ħ	H			
VigorSwitch G2240	5	~	All	1	80	Access M	U	UISADIE
System	6		All	~	86	Access 💌	0	Disable
⊡ Port	7	~	All	*	86	Access 💙	0	Disable
⊡Vlan	8		All	*	86	Trunk 💌	0	Disable
Vlan Mode Tag-based Group	9		All	~	84	Access 🗸	0	Disable
Port-based Group	10		All	~	84	Access ¥	0	Disable
Ports Port Isolation	11		All	~	84	Access ¥	0	Disable
Management Vlan	12		All	*	84	Trunk V	0	Disable
			-				-	
GVRP	13	~	All	*	2611	Trunk 💌	0	Disable
⊡QoS	14		All	~	2611	Access \star	0	Disable
SNMP	15	~	All	~	7	Access 🗙	0	Disable
ACL IP MAC Binding	16	2	All	~	8	Access 💙	0	Disable
B02.1X	17		All	~	9	Access 🗸	0	Disable
Trunk	18		All	~	10	Access ¥	0	Disable
⊡ STP	19		All	~	3700	Access ¥	0	Disable
■MSTP			1.00	1000	Land			
Mirroring	20		All	*	3700	Access 💙	0	Disable
■Multicast	21	~	All	~	1	Access 🚩	0	Disable
Alarm     DHCP Snooping	22		All	~	1	Access 💙	0	Disable
	23	~	All	~	1	Trunk 💌	0	Disable
Save/Restore Export/Import	24	2	All	*	1	Trunk 💌	0	Disable

4. After finishing the above configuration, the equipment connecting to VigorSwitch Port 15, 16, 17 and 18 can get the corresponding IP address(es) of the network segment.

The equipment connecting to VigorSwitch Port 15 can get the IP address of 192.168.1.0/24

The equipment connecting to VigorSwitch Port 16 can get the IP address of 192.168.3.0/24

The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.5.0/24

The equipment connecting to VigorSwitch Port 18 can get the IP address of 192.168.7.0/24

5. To make any two of VLAN groups of Tag Based VLAN linked with each other, just check the boxes of the ones in the field of **Inter-LAN Routing** in the page of **LAN** >> **General Setup**. Refer to the following figure. LAN2 and LAN3 are linked.

ter-LAN Routing Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	$\checkmark$			
LAN 2				
LAN 3	—	→ 🔽	<b>V</b>	
LAN 4				<b>V</b>

# 4.3 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Router?

There are three methods to get files from USB devices connecting to router.

- File Explorer Under Administration operation, the administer can control the files on USB storage device through USB Application>>File Explorer.
- FTP Use common FTP utility.
- Samba Invoke Samba service and use <u>\\192.168.1.1</u> to access into the USB storage device.

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** Below shows the example of getting files from FTP:

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

USB Application >> USB Disk Status					
USB Mass Storage Device Status					
Connection Status: Disk Conn Write Protect Status: NO	ected	Disconnect USB Disk			
Disk Capacity: 2009 MB					
USB Disk Users Connected		<u>Refresh</u>			
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. Then, please open **USB Application >> USB General Settings** to enable Samba service.

USB Application >> USB General Settings

USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	Default 💌
Samba Service Settings(Network Neighbo	rhood)
💿 Enable 🔘 Disable	
Access Mode	
⊙ LAN Only ○ LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor

Note: 1. If Charset is set to "default", 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.

3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: .; : " <> * + = / \ | ?.



3. Setup a user account for the FTP service by using **USB Application** >>**USB User Management.** Click **Enable** to enable FTP/Samba User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

FTP/Samba User	💿 Enable 🔵 🔘 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 o	ontain the following characters: A-Z a-z O-9 \$ % ' @ ~ ` ! ( )

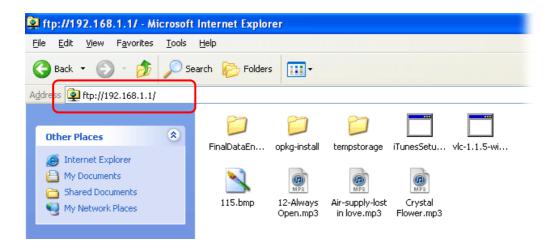
4. Click **OK** to save the configuration.

USB Application >> USB User Management

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

Log On a	As 🔀				
۲	Either the server does not allow anonymous logins or the e-mail address was not accepted.				
	FTP server: 192.168.1.1				
	User name:				
	Password:				
	After you log on, you can add this server to your Favorites and return to it easily.				
⚠	FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.				
	Learn more about using Web Folders.				
	Log on anonymously				
	Log On Cancel				

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



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

USB Application >> USB Disk Status

USB Mass Sto	rage Device Status			
Connection	Status: Disk Conne	Disconnect US	SB Disk	
Write Protec	t Status: No			
Disk Capacit	y: 2009 MB			
Free Capacit	ty: 0 MB – <mark>Refresh</mark>			
USB Disk Use	ers Connected			<u>Refresh</u>
Index	Service	IP Address(Port)	Usernam	e
1.	FTP	192.168.1.10(1963)	user1	Drop

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

Now, users in LAN of Vigor2830 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application** >>**USB User Management.** 



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

Follow the steps listed below:

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index	Profile	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	

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.

ect Settings >> SMS / Mail Service Object				
rofile Index: 1				
Profile Name	Local number			
Service Provider	kotsms.com.tw (TW)			
Username	abc5026			
Password	•••			
Quota	10			
Sending Interval	3 (seconds)			
	OK Clear			
	Cancel			

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

Set to Factor	Mail Server	SMS Provider
e SMS Provider	Profile	Index
kotsms.com.tw (TW)	Local	<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>
	Cust	<u>9.</u>
	Cust	<u>10.</u>

Object Settings >> SMS / Mail Service Object

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

Object Settings >> Notification Object

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>		

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.

Category     Status       WAN     Disconnected     Reconnected       VPN Tunnel     Disconnected     Reconnected			WAN_Notify	e	rofile Name
		Status		ategory	Ca
VPN Tunnel Disconnected Reconnected	nnecte	Recon	Disconnected		NAN
	nnecte	Recon	Disconnected	il 🗌 🖸	/PN Tunnel

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

Object Settings >> Notifica	ition Object	
		Set to Factory Default
Index	Profile Name	Settings
<u>1.</u>	WAN_Notify	WAN
<u>Z.</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).

Application >> SMS / Mail Alert Service

SMS Provide	er Mail Server		<u>S</u>	et to Factory Default
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 💟		1 - WAN_Notify 💟	
		ОК		

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.

Cancel

Configure the settings as the following figure. Choose one of the SMS profiles. In this example, the profile "For warning" is selected. Then, click OK to save the settings.
 WAN >> General Setup

Enable:	Yes 🕶
Display Name:	
Physical Mode:	Ethernet
Physical Type:	Auto negotiation 💌
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion :	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Send Mail Alert if line drops out	or warning
Active Mode:	Backup 👻
	WAN 1 WAN 2 WAN 3
Backup Type (Only if acting as backup for multiple WAN):	When any of selected WAN disconnect     ○ When all of selected WAN disconnect

When such WAN (e.g., WAN2 in this example) disconnects due to some reason, the system will use other WAN for connection instead and send SMS to notify the user (destination number #123456789). However, if there is no available WAN for connection, the system will send SMS to inform the user after reconnecting WAN2 successfully.

## 4.5 Web Portal Log-In Application for Wireless Client

With the increase of hotspot deployed via Wi-Fi technology in the world, we may easily get Internet connection with the served wireless connection facility provided by the campus, chain store, the coffee shop, the airport, department store, municipal...etc.. Such hotspot deployment contributes to seamless Internet connection which enables the remote workers or wireless users to get onto the cyber space anywhere at anytime.

In contrast to the real wireless user's advantage earn from hotspot, the Wi-Fi connection providers may also earn placement marketing advantage via Vigor2830n as offering wireless connection service at its hotspot. With the smart, easy configuration of WLAN on Vigor2830n, the free riders of Wi-Fi connection at hotspot would be automatically directed to dedicated web site. In a department store with Vigor2830n deployed, the mobile users will be directed to its own company web site or dedicated special promotion program web page as firstly get wireless connection to the Internet. The Internet surfers would have a glance at least on the dedicated web site and related contents.

# **Direct Marketing via Web Portal Log-in**



## **Wireless General Setup**

- 1. From Vigor router web configuration page, select **Wireless LAN>>General Setup**.
- 2. Check **Enable Wireless LAN** and set the SSID. Then click **OK** to save the settings.

Vigor2830 ADSL2 + Security I	Series Firewall					Dray
Off 💌 📭6	Wireless LA	(N >> (	General Setup			
Wizards Online Status	General Se	tting (	IEEE 802.11)			
WAN	🗹 Enable		ess LAN			
LAN	MO	ue:		Mixed(11b+11g+11n) 🛛 👻		
_oad-Balance/Route Policy	Cha	annel:		Channel 6, 2437MHz 🛛 🖌		
irewall	_					
Jser Management		Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
Dbjects Setting CSM	1			DrayTek		
Bandwidth Management Applications	2			DrayTek_Guest		
/PN and Remote Access Certificate Management	3					
/oIP Wireless LAN	4					

## Wireless Portal Log-in Setting

1. Open LAN>>Web Portal Setup.

LAN >> Web Portal Setup

2. Click **Redirect to URL** and type the URL in the field below. User's first HTTP request will be redirected to the URL defined here. (Here we take <u>www.draytek.com</u> for an example.)

ODisable	
ORL Redirect	www.draytek.com
	e.g. http://www.draytek.com Note : If the User Management application is enabled, it will override the Web Portal settings seen here.
⊘Message	<hl><font color="red">Vigor</font></hl> <h2> - Reliable connectivity</h2> <h2> - Robust firewall protection<h2> - Multi-site secure communication</h2></h2>
Applied Interfaces	(Max 255 characters)
	LAN1 LAN2 LAN3 LAN4
	SSID1 SSID2 SSID3 SSID4

3. Click **OK** to save the settings. Note that do not choose **Redirect to URL** for this page if you have already enabled the user-based mode under **User Management**. For such case, choosing **Show the message** will be accepted.

**Note:** This feature is useful for restaurant, hotel, shopping store and so on. Wireless clients will be redirected to the specified web sites when they open the browser through the wireless environment set by the restaurant, hotel, shopping store, and so on. It can gain the result of advertisement effectively.

4. Use a Notebook or mobile device supporting Wireless function to connect Vigor2830 via Wireless LAN.

General Support	
Connection	
Status:	Connected
Network:	Vigor2830 web portal log-in
Duration:	00:03:38
Speed:	54.0 Mbps
Signal Strength:	Öllse
Activity	4
	Sent — Preceived
Packets:	744   5
Properties	Disable View Wireless Networks

- 5. Try to open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
- 6. The first connection session will be redirected to DrayTek Website (specified in step 2) automatically.



However, if open another new tab again in the same browser, the browser will open default page based on the default setting.



## 4.6 How to Customize Your Login Page

Login page can be customized to fit the request of the administrator.

1. Open User Management>>General Setup. Set User-Based as the Mode and click OK to save teh settings.

Vigor2830 ADSL2+ Security F	Series Dray
Off 💌 1166	User Management >> General Setup
Wizards Online Status	General Setup
WAN LAN Load-Balance/Route Policy NAT	Mode: Rule-Based Display IP Rule-Based User-Based cking window: Off
Firewall Jser Management Security Security User Profile User Group User Online Status Dbjects Setting CSM Bandwidth Management Applications //PN and Remote Access Certificate Management /oIP	<ul> <li>Web Authentication: HTTPS </li> <li>Notice :         <ol> <li>User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode.</li> <li>Users match the above lists will not be required for authentication. The firewall rules policy will still valid.</li> <li>Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.</li> </ol> </li> <li>Landing Page (Max 255 characters) Preview Set to Factory Default</li> </ul>
Nireless LAN SL VPN SB Application ystem Maintenance iagnostics xternal Devices	<pre><body stats="1"><script language="javascript"> window.location='http://www.draytek.com'</script></body></pre>
Admin mode	OK Clear Cancel

2. Open **User Management>>User Profile** to create a new user profle.

User Management >> User Profile

ser Profile Table			Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>	admin	<u>17.</u>	
<u>2.</u>	Dial-In User	<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>	

3. Click any link (e.g., #3) to access into the following page. Type a User Name and a Password. Then, click **OK**.

Enable this account		
Username	carrie	
Password	•••••	
Confirm Password	•••••	
Idle Timeout	10	min(s) 0:Unlimited
Max User Login	0	0:Unlimited
External Server Authentication	None 💌	
Log	None 💌	
Pop Browser Tracking Window	<ul> <li>Image: A start of the start of</li></ul>	
Authentication	🗹 Web 🗹 Alert To	ool 🗹 Telnet
Landing Page		
Index(1-15) in <u>Schedule</u> Setup:	, , , ,	
🔲 Enable Time Quota o min.	(+)-)0	min.
📃 Enable Data Quota 0 🛛 🕅 MB 🔽	+ - 0	мв
Reset quota to default when schedu	ling time expired	
Enable Default Time Quota	0 min. D	efault Data Quota 🛛 🛛 MB

4. Open **System Maintenance>>Login Page Greeting**. Check the box to enable this function. Type a brief description (e.g., *Just for Carrie*) in the field of **Login Page Title** which will be shown on the heading of the login dialog. Next, click **OK**.

System Maintenance >> Login Page Greeting

User Management >>User Profile

Enable		
Login Page Title	Just for Carrie	(31 char max.)
Welcome Message a	and Bulletin (Max 511 characters)	Preview   Set to Factory Default
message is displ with your own me in HTML so lists	Lor=red>Welcome MessageLayed in the Login page of th essage. <ol><li>The welco s such as this one can be cre font or img can be used</li></ol>	e router. Replace this text me message can be written ated <li>Other markup</li>
		2

5. Open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.

Cancel

OK

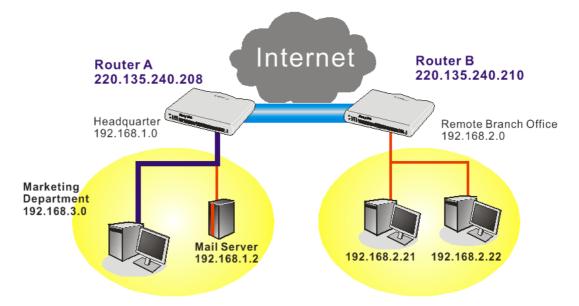
6. Try to access into the web user interface (e.g., 192.168.1.1) of Vigor router. Please note *"Just for Carrie"* is displayed as a heading on the login dialog box.

2 http://192.168.1.5/weblogin.htm	
Just for Carrie Username Password Login	X
Copyright©, DrayTek Corp. All Rights Reserved. DrayTek 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>	

7. After typing the username and password (defined in **User Management>>User Profile**), click **Login**. You can access into Internet or access into the **Landing Page** if configured in **User Management>>General Setup**.

# 4.7 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



**Settings in Router A in headquarter:** 

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then,

For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup			
PPP/MP Protocol			LDAP Server Profiles for PPP Authentication
Dial-In PPP Authentication	PAP/CHAP/	MS-CHAP/MS-CHAPv2 🔽	PPTP LDAP Profile Note: Please select 'PAP Only' in 'Dial-In PPP
Dial-In PPP Encryption(MPPE)	Optional Mi	PPE 🔽	Authentication', if you want to use AD/LDAP for PPP Authentication!!
Mutual Authentica	tion (PAP)	🔘 Yes 💿 No	
Username			
Password			
IP Address Assignme (When DHCP Disable		n Users	
Assigned IP start	LAN 1	192.168.1.200	
	LAN 2	192.168.3.200	
	LAN 3	192.168.5.200	
	LAN 4	192.168.7.200	
		ОК	

VPN and Remote Access >> PPP General Setup

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



VPN and Remote Access >> IPsec General Setup				
VPN IKE/IPsec General Setup				
Dial-in Set up for Remote Dial-in users and	d Dynamic IP Client (LAN to LAN).			
IKE Authentication Method				
Certificate for Dial-in	None 🔽			
Pre-Shared Key				
Pre-Shared Key				
Confirm Pre-Shared Key				
IPsec Security Method				
Medium (AH)				
Data will be authentic, but will r	not be encrypted.			
High (ESP) 🗹 DES 🗹 3DES	AES			
Data will be encrypted and auth	hentic.			
	OK Cancel			

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN					
Profile Index : 1 1. Common Settings					
Profile Name	Branch 1	Call Direction     Always on     Idle Timeout	Both O Dial-Out O Dial-in           300         second(s)		
		Enable PING PING to the IP			

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

2. Dial-Out Settings	
Type of Server I am calling	Username ???
O PPTP	Password(Max 15 char)
💿 IPsec Tunnel	PPP Authentication
🔘 🔘 L2TP with IPsec Policy 🛛 None 🔤	PAP/CHAP/MS-CHAP/MS-CHAPv2 🔽
	VJ Compression 💿 On 🔾 Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method
220.135.240.210	O Pre-Shared Key
	IKE Pre-Shared Key
	O Digital Signature(X.509)
	Peer ID None 🔽
	Local ID
	Alternative Subject Name First
	🔘 Subject Name First
	Local Certificate None 💽
	IPsec Security Method
	Medium(AH)
	O High(ESP) DES without Authentication 🛛
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:
	, , , , , , , , , , , , , , , , , , ,

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings		
Type of Server I am calling	Username	draytek
● PPTP	Password(Max 15 char)	
🛛 🔘 IPsec Tunnel	PPP Authentication	
🔘 🔘 L2TP with IPsec Policy 🛛 None 🔤	PAP/CHAP/MS-CHAP/MS-CH	IAPv2 🔽
Converting (Legt Marrie for VDM	VJ Compression	💿 On 🔘 Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method	
220.135.240.210	Pre-Shared Key	
	[IKE Pre-Shared Key]	
	O Digital Signature(X.50	9)
	Peer ID	None 🔽
	Local ID	
	Alternative Subject	t Name First
	🔷 Subject Name First	
	Local Certificate	None 🗸
	IPsec Security Method	
	Medium(AH)	
	O High(ESP) DES withou	t Authentication 🛛 🔽
	Advanced	
	Index(1-15) in <u>Schedule</u> S	ietup:



6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP IPSec Tunnel L2TP with IPSec Policy None	Username Password VJ Compression	??? 
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.210 or Peer ID	IKE Authentication Method         Pre-Shared Key         IKE Pre-Shared Key         Digital Signature(X.509)         None         IPSec Security Method         Medium(AH)         High(ESP)         IMES         Image: Security Method         Image: Security Method	

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings		
Allowed Dial-In Type		
🗹 РРТР	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.210	🗌 Digital Signature(X.509	)
or Peer ID	None 😪	
	IPSec Security Method	
	Medium(AH)	
	High(ESP) 🗹 DES 🗹	3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

4. TCP/IP Network Setting	S		
My WAN IP	0.0.0.0	RIP Direction	Disable 🖌
Remote Gateway IP	0.0.0.0	From first subnet to remo do	te network, you have to
Remote Network IP	192.168.2.0		Route 💌
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	Change default route single WAN supports this	to this VPN tunnel ( Only )
Local Network Mask	255.255.255.0	single ward supports this	,
	More		
	OK (	Clear Cancel	

### Settings in Router B in the remote office:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup				
PPP/MP Protocol Dial-In PPP Authentication	PAP/CHAP/	MS-CHAP/MS-CHAPv	2 💌	LDAP Server Profiles for PPP Authentication <u>PPTP LDAP Profile</u> Note: Please select 'PAP Only' in 'Dial-In PPP
Dial-In PPP Encryption(MPPE)	Optional MF	PE 💌		Authentication', if you want to use AD/LDAP for PPP Authentication!!
Mutual Authentica	tion (PAP)	🔘 Yes 💿 No		
Username				
Password				
IP Address Assignme (When DHCP Disable		Users		
Assigned IP start	LAN 1	192.168.2.200		
	LAN 2	192.168.3.200		
	LAN 3	192.168.5.200		
	LAN 4	192.168.7.200		

OK

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

#### VPN and Remote Access >> IPsec General Setup

VPN IKE/IPsec General Setup Dial-in Set up for Remote Dial-in users an	id Dynamic IP Client (LAN to LAN).			
IKE Authentication Method				
Certificate for Dial-in	None 💌			
Pre-Shared Key				
Pre-Shared Key				
Confirm Pre-Shared Key				
IPsec Security Method				
Medium (AH)				
Data will be authentic, but will	not be encrypted.			
High (ESP) IDES I 3DES AES Data will be encrypted and authentic.				
	OK Cancel			

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Acce	ss >> LAN to LAN	
Profile Index : 1 1. Common Settings		
Profile Name	Branch 1	Call Direction ③ Both 〇 Dial-Out 〇 Dial-in Always on Idle Timeout 300 second(s)
Multicast via VPN	ah WAN1 First	Enable PING to keep alive PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

#### 2. Dial-Out Settings

Type of Server I am calling	Username ???			
О РРТР	Password(Max 15 char)			
💿 IPsec Tunnel	PPP Authentication			
🔘 L2TP with IPsec Policy 🛛 None 🔤	PAP/CHAP/MS-CHAP/MS-CHAPv2 😒			
	VJ Compression 💿 On 🔿 Off			
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)				
220.135.240.208				
220.100.240.200	Pre-Shared Key			
	IKE Pre-Shared Key			
	🔘 Digital Signature(X.509)			
	Peer ID None 😪			
	Local ID			
	Alternative Subject Name First			
	OSubject Name First			
	Local Certificate None 🗸			
	IPsec Security Method			
	Medium(AH)			
	O High(ESP) DES without Authentication			
	Advanced			
	Index(1-15) in <u>Schedule</u> Setup:			

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings				
Type of Server I am calling	Username	draytek		
● PPTP	Password(Max 15 char)	•••••		
🛛 🔿 IPsec Tunnel	PPP Authentication			
🛛 🔿 L2TP with IPsec Policy 🛛 None 🔤	PAP/CHAP/MS-CHAP/MS-CHAPv2 🔽			
L	VJ Compression	💿 On 🔘 Off		
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method			
220.135.240.208	Pre-Shared Key			
	IKE Pre-Shared Key			
	O Digital Signature(X.50	Digital Signature(X.509)		
	Peer ID	None 🔽		
	Local ID			
	Alternative Subject	t Name First		
	Subject Name Firs	t		
	Local Certificate	None 🗸		
	IPsec Security Method			
	Medium(AH)			
	O High(ESP) DES without Authentication			
	Advanced			
	Index(1-15) in Schedule	Setup:		

6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



3. Dial-In Settings		
Allowed Dial-In Type	Username	???
П РРТР	Password(Max 11 char)	
🗹 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	
220.135.240.208	🔲 Digital Signature(X.50	)9)
or Peer ID	None 🗸	
	Local ID	
	💿 Alternative Subject	ct Name First
	OSubject Name Firs	st
	IPsec Security Method	
	Medium(AH)	
	High(ESP) 🛛 🗹 DES 🗹	3DES 🗹 AES

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

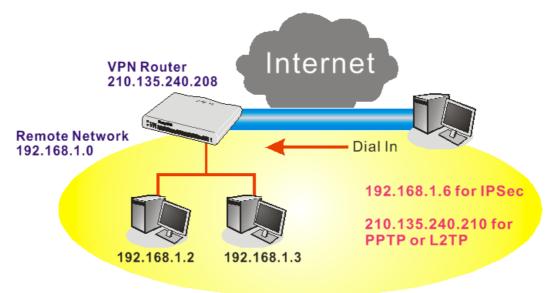
3. Dial-In Settings			
Allowed Dial-In Type	Username	draytek	
🗹 РРТР	Password(Max 11 char)		
🔲 IPsec Tunnel	VJ Compression	💿 On 🔘 Off	
🔲 🔲 L2TP with IPsec Policy 🛛 None 🔤			
	IKE Authentication Method		
Specify Remote VPN Gateway	🗹 Pre-Shared Key		
Peer VPN Server IP	[IKE Pre-Shared Key]		
220.135.240.208	Digital Signature(X.509)		
or Peer ID	None 💌		
	Local ID		
	💿 Alternative Subje	ct Name First	
	OSubject Name Fir	st	
	IPsec Security Method		
	🗹 Medium(AH)		
	High(ESP) 🛛 🗹 DES 🗹	3DES 🗹 AES	

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings	;		
My WAN IP	0.0.0.0	RIP Direction	Disable 🖌
Remote Gateway IP	0.0.0.0	From first subnet to remo do	te network, you have to
Remote Network IP	192.168.1.0		Route 💌
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	Change default route	to this VPN tunnel ( Only )
Local Network Mask	255.255.255.0	single way supports this	,
	More		
	ОК С	lear Cancel	

# 4.8 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



### Settings in VPN Router in the enterprise office:

VPN and Remote Access >> PPP General Setup

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP/MP Protocol	IP Address Assignment for	Dial-In Users
Dial-In PPP PAP or CHAP	(When DHCP Disable set)	
Authentication	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE) Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.



VPN a	nnd F	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, bu	it will not be encrypted.
High (ESP) 🛛 🗹 DES 🛛	3DES 🔽 AES
Data will be encrypted ar	d authentic.
	OK Cancel

- 3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
- 4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

Username ???
IKE Authentication Method
Pre-Shared Key
IKE Pre-Shared Key
Digital Signature(X.509)
IPSec Security Method
High(ESP) 🗹 DES 🗹 3DES 🗹 AES
Local ID (optional)

VPN and Remote Access >> Remote Dial-in User

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

VPN and Remote Access >> Remote Dial-in User

Index No. 1	
User account and Authentication  Enable this account	Username ???
Idle Timeout 300 second(s)	
Allowed Dial-In Type	IKE Authentication Method Pre-Shared Key
РРТР	IKE Pre-Shared Key
IPSec Tunnel	Digital Signature(X.509)
L2TP with IPSec Policy None	None V
Specify Remote Node	
Remote Client IP or Peer ISDN Number	IPSec Security Method
	Medium(AH)
or Peer ID	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
Netbios Naming Packet   Pass  Block	Local ID (optional)
ОК С	ear Cancel

#### Settings in the remote host:

- 1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.DrayTek.com download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

🖕 Smart VPN Client 3.2.2 (WinXP)	
Step 0. This step will add the ProhibitIpSec registry valu order to configure a L2TP/IPSec connection usin or a L2TP connection. For more infomation, plea Q240262 in the Microsoft Knowledgement Base.	ig a pre-shared key ise read the article
Configure Step 1. Dial to ISP If you have already gotten a public IP, you can	skip this step.
×	Dial
Step 2. Connect to VPN Server	
×	Connect
Insert Remove	Setup
Status: No connection PPTP	ISP @ VPN @

3. In Step 2. Connect to VPN Server, click Insert button to add a new entry.

If an IPSec-based service is selected as shown below,



Dial To VPN	×				
Session Name:	Office				
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)				
192.168.1.1					
User Name :	draytek_user1				
Password :	*****				
Type of VPN					
○ PPTP	◯ L2TP				
IPSec Tunnel	CL2TP over IPSec				
PPTP Encryption     No encryption					
	Require encryption     Maximum strength encryption				
🔲 Use default ga	ateway on remote network				
ок	Cancel				

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.

IPSec Policy Setti	ng		×		
My IP : Type of IPSec	172.16.3.100	) <b>v</b>			
◯ Standard IPS		0.0.0.0			
Remote Su Remote Su	bnet : bnet Mask :	255 . 255 . 255 . 0			
💽 Virture IP	DrayT	ek Virture Interface 🛛 🗸			
	n IP address a an IP address	utomatically (DHCP over IPSec)			
IP Address: 192 . 168 . 1 . 201 Subnet Mask: 255 . 255 . 255 . 0					
-Security Method -					
Medium(AH)	·	)High(ESP) DES			
Authority Method					
Certification	Authority:	Browse			
	ĸ	Cancel			

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

Dial To VPN	×			
Session Name:	office			
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)			
192.168.1.1				
User Name :	draytek_user1			
Password :	****			
Type of VPN				
PPTP	OL2TP			
O IPSec Tunnel O L2TP over IPSec				
PPTP Encryption O No encryption				
	ength encryption ateway on remote network			
ОК	Cancel			

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

## 4.9 QoS Setting Example

Class 3

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 VPN 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

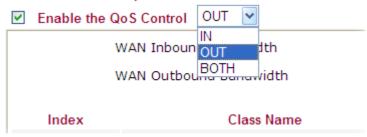
WAN1 Ena WAN2 Ena		Kbps/Kbps	Outbound					Control		
WAN2 Ena			outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
	nable 1	.0000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN3 Disa	sable 1	.0000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
Class Rule		0000kbps/10000kbps	Name	25%	25%	25%	25%	Rule	Status Service T	

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**.

<u>Edit</u>

## Bandwidth Management >> Quality of Service

## WAN2 General Setup



3. Set Inbound/Outbound bandwidth.

Bandwidth Ma	anagement >> Quality of Service	
WAN2 Genera	al Setup he QoS Control BOTH 🗸	
	WAN Inbound Bandwidth	10000 Kbps
	WAN Inbound bandwiden	10000 Kbps
	WAN Outbound Bandwidth	10000 Kbps
1		Descendent for a statistic Dest.
		be smaller than the real bandwidth to ggested to set the bandwidth value for
		cal network speed provided by ISP to
	the QoS performance.	
шахниге	ane Quo 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.

Bandwidth Management >> Quality of Service

Class Inde Name	e <b>x #1</b> E-mail					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1 ()	Inactive	Any	Any	ANY	undefined	
Add Edit Delete						
		(	OK Cancel			

5. For this index, the user will set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP.

Enable the QoS Co	ntrol BOTH 🛩	
WAN I	nbound Bandwidth	10000 Kbps
WAN Outbound Bandwidth		10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Bandw	idth Control	Limited_bandwidth Ratio 25 %
Outbound TCP AC	K Prioritize	

Bandwidth Management >> Quality of Service

Return to previous page. Enter the Name of Index Class 2 by clicking Edit link. In this index, the user will set reserved bandwidth for HTTPS. And click OK.
 Bandwidth Management >> Quality of Service

ass Inde	x #2				
ame H	ITTPS				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 💿	Active	Any	Any	ANY	ANY
		4	Add Edit Delet	e	
			OK Cancel		

## 7. Click **Setup** link for WAN2.

Bandwidth Management >> Quality of Service

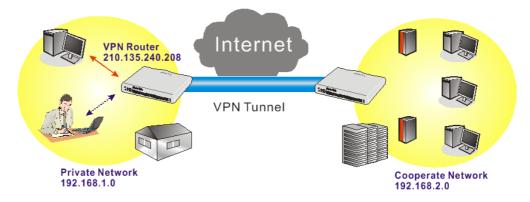
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
WAN2	Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Active	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

Class Rule			
Index	Name	Rule	Service Type
Class 1	E-mail	Edit	
Class 2	HTTPS	Edit	<u>Edit</u>
Class 3		Edit	

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

VAN2 General Setup		
Enable the QoS C	ontrol BOTH 💌	
WAN	Inbound Bandwidth	10000 Kbps
WAN	Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
Enable UDP Band Outbound TCP A		Limited_bandwidth Ratio 25

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



10. Click **Edit** to open a new window.

Bandwidth Management >> Quality of Service

Class Index #3 VPN Name DiffServ NO Status Local Address **Remote Address** Service Type CodePoint 1 Empty Add Delete Edit OK Cancel

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

le Edit				
ACT				
Local Addre	SS	Any		Edit
Remote Add	lress	Any		Edit
DiffServ Co	dePoint	IP precedence 4	*	
Service Typ	e	SYSLOG(UDP:514)	*	
Note: Please	e choose/setu	p the <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**.

## 4.10 Upgrade Firmware for Your Router

## **Using Firmware Upgrade Utility**

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Go to www.DrayTek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products	Support	Education	Partners	Contact U
ome > Support > Downloads						
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	lease Date		Firmware	
Vigor120 series	3.2.2.1	2	6/06/2009		Driver	
Vigor2100 series	2.6.2	2	6/02/2008		Utility	
Vigor2104 series	2.5.7.3	1	3/02/2008			troduction
Vigor2110 series	3.3.0	2	5/06/2009		Datashee	
Vigor2200/X/W/E	2.3.11	2	2/09/2004			ertification
Vigor2200Eplus	2.5.7	1	8/02/2009		KATTEU	ennication
Vigor2200USB	2.3.10	1	6/03/2005			

3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.

		About	DrayTek Products	Support E	ducation	Partners	Contact Us
ome > Support > Ut	ility						
Utility						Downlo	ads
Tools Name	Release Date	Version	OS	Support Mo	del	Firmware	
Router Tools	2009/06/18	4.2.0	MS-Windows	All Module	s	Deixer	
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP	All Module	s	Driver	
, , ,			MS-Vista			Utility	
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Windows XP	VigorPro 100 s	series	Utility In	troduction
Tools		(Multi- language)	MS-Vista	VigorPro 5500 VigorPro 5510		Datasheet	t
		lunguuge /		VigorPro 5300		R&TTE C	artification
Smart VPN Client	2009/05/25	3.6.3	MS-Windows XP	All Module	s		Sitting at the
		( Multi- language )	MS-Vista				
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 se	ries		
				VinorPro 5510			

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of router tool. The setup wizard will appear.



- 6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 7. From the Start menu, open Programs and choose Router Tools XXX >> Firmware Upgrade Utility.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port	Firmware file:	
69		
Password:	Abort	Send

- 8. Type in your router IP, usually **192.168.1.1**.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send

10. Click Send.

🛍 Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send
Sending	

11. Now the firmware update is finished.

## Using Web Page

The web page also can guide you to upgrade firmware. Note that this example is running over Windows OS (Operating System).

- 1. 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 <u>ftp.DrayTek.com</u>.
- 2. Click System Maintenance>> Firmware Upgrade.

System Maintenance >> Firmware Upgrade

 Web Firmware Upgrade

 Select a firmware file.

 選擇檔案

 未選擇檔案

 Click Upgrade to upload the file.

 Upgrade

 TFTP Firmware Upgrade from LAN

 Current Firmware Version: 3.6.6.1_db_RC1

 Firmware Upgrade Procedures:

 1. Click "OK" to start the TFTP server.

 2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.

 3. Check that the firmware filename is correct.

 4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.

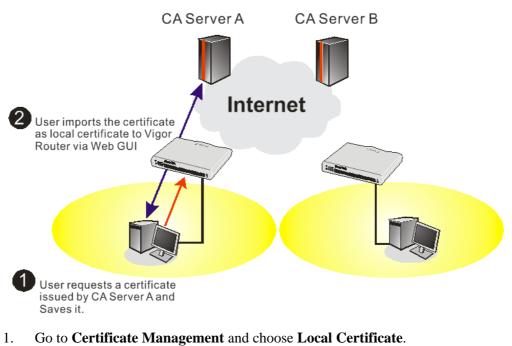
 5. After the upgrade is compelete, the TFTP server will automatically stop running.

 Do you want to upgrade firmware ?

- 3. Select a firmware file by clicking **Browse**.
- 4. Click **Upgrade** to perform the firmware upgrade.



# 4.11 Request a certificate from a CA server on Windows CA Server



Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local			View Delete
GENERATE IN	PORT REFRESH		
X509 Local Certifi	cate		
			~
			~

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.

Generate Certificate Request		
Subject Alternative Name		
Туре	Domain Name 💙	
Domain Name	draytek.com	
Subject Name		
Country (C)	TW	
State (ST)		
Location (L)		]
Orginization (O)	Draytek	
Orginization Unit (OU)		
Common Name (CN)		
Email (E)	press@draytek.com	]
Кеу Туре	RSA 💌	
Key Size	1024 Bit 🗸	

3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use. Certificate Management >> Local Certificate

lame Subject	Status	Modify
.ocal /C=TW/O=Draytek/emailAddress	Requesting	View Delete
NERATE IMPORT REFRESH X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAKGAIUEBhMCVFcxEDAOI BgkqhkiG9w0BCQEWEXByZXNzQGRYX10ZWauYZ9tI A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWkn 3wDeQytoV1LBJz21DF0xjX61p7ev187twwTsg41g; du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI oCkwJwYLKoZIhvcNAQkOMRowGDAWBgNVHREEDzAM; hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToer uRLq4CiEi6nV4hMRytcx2pE26sMarSgREER86RoOG I9FqkjJNihip4TCjecSNNZjmQoSWU+BceSTG+SCB0 END CERTIFICATE REOUEST	HIGFMAOGCSQCSIb hIdHblo1kt9cTdL 26Qk/rGhuVTKd9j cOT2RZjkRMaHEWp ggtkcmF5dGVrLmN hItHQbcwjXvg/r7 8JxOI45560xC2/N	3DQEBAQUA UDaFk6s8d 6PlcrnkP7 VpwIDAQAB vbTANBgkq kFlzTJiHh 1Gh9VQ9I1

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

Welcome		
	ificate for your web browser, e-mail client, or other s f to other people over the web, sign your e-mail mes you request.	
Select a task:		
Retrieve the CA certificate or ce	rtificate revocation list	
<ul> <li>Request a certificate</li> </ul>		
Check on a pending certificate		

## Select Advanced request.

Microsoft Certificate Services vigor	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request:	
Next	>

Select Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file

You can request a certificate for yourself, another user, or a computer using o authority (CA) will determine the certificates that you can obtain	one of the following methods. Note that the policy of the certification
Submit a certificate request to this CA using a form.	
Submit a certificate request using a base64 encoded PKCS #10 file or a	a renewal request using a base64 encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user using the You must have an enrollment agent certificate to submit a request for another user.	Smart Card Enrollment Station.
	Next >

<b>Microsoft</b> Certifica	te Services vigor	Hon
Submit A Save	d Request	
		request or PKCS #7 renewal request generated by an external application (such as a web t to the certification authority (CA).
Saved Request:		
Certificate Request	BEGIN CERTIFICATE REQUI MIIBejCCARMCAQAwGTELMAKGAlUI BgkqhkiGywBCCDEWEXPyZNX2QGR A4GNADCB1QKBgQDQYB7wm2FfFhNS hX4bpB9cUF9dloACGG1M/cEBOck X/GDA7CTvO/fQ2xroCuJJTjLSJS <	EBhRCVFcxEDAO YYX102WsuY29t 9/IeQnG03Xk++ dc2dFFVIXcP3
	<u>Browse</u> for a file to insert.	
Certificate Templa	ate:	
	Administrator 🗸	
	Administrator Authenticated Session Basic EFS	
Attributes:	EFS Recovery Agent User IPSEC (Offline request)	
	Router (Offline request)	
	Subordinate Certification Authority Web Server	Submit >
	Aven Selvel	

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

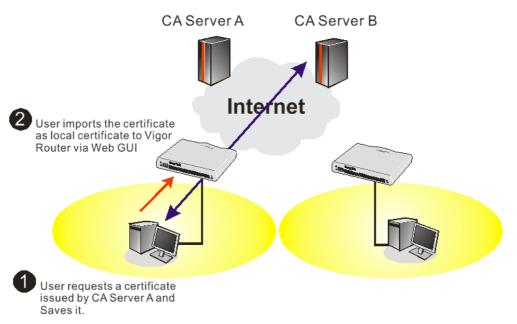
5. Back to Vigor router, go to Local Certificate. Click IMPORT button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing "-----BEGINE CERTIFICATE-----...." Certificate Management >> Local Certificate

ame Subject	Status	Modify
ocal /C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
NERATE IMPORT REFRESH X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDA BgkqhkiG9w0BCQEWEXByZXN2QGRyYX10ZWsuY29 A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfW 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg41 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKV oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzA hkiG9w0BAQUFAA0BqQAuSBRUGt4W1hH9N6/HwTo	tMIGfMADGCSqGS knIdHblo1kt9cTd gZ6Qk/rGhuVTKd IrOT2RZjkRMaHE NggtkcmF5dGVrLa	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq

6. You may review the detail information of the certificate by clicking View button.

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

# 4.12 Request a CA Certificate and Set as Trusted on Windows CA Server



1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
檔案(图 編輯(四) 檢視(四) 我的最愛(4) 工具(四) 說明(四)	
🌀 上一頁 • 🌍 - 🛃 🖻 🚮 🔎 搜尋 📩 我的最爱 🐠 媒體 🙆 🍰 🛃 • 🎿	
總址① @ http://172.16.2.179/certax/	✓ → 移至 連結 、
misa 🔧 🔪 搜尋 🔸 🗾 翻目提示 📊 選項  🔀 封錮快顯親窗 (319) 🔹 🔐 Hotma	1 🍊 Messenger [ 提的 MSN
	(band)
Microsoft Certificate Services - wgor	<u>Home</u>
Microsoft Certificate Services - vigor. Welcome	nome
	re program. Once you acquire a certificate, you
Welcome You use this web site to request a certificate for your web browser, e-mail client, or other secu will be able to securely identify yourself to other people over the web, sign your e-mail messag	e program. Once you acquire a certificate, you

Vigor2830 Series User's Guide

- 2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded**, and **Download CA certificate** to save the .cer. file.
  - Microsoft Certificate Services Microsoft Internet Explorer 檔案(P) 編輯(E) 檢視(V) 我的最愛(A) 工具(I) 說明(H) 🌀 上一頁 • 🜍 - 🛃 🛃 🍰 🔎 搜尋 📩 我的最爱 🜒 媒體 🙆 🍰 💆 😒 🍛 🖌 🔁 移至 網址(D) 截 http://172.16.2.179/certsrv/certcarc.asp 連結 msn^{*} * 💉 🔎 搜尋 • 🛃 醒目提示 / 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔜 Hotmail 👅 Messenger 👔 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current (vigor(1)) Previous [vigor] Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

Name	Subject	Status	Modify
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

4. You may review the detail information of the certificate by clicking **View** button.

Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

**Note**: Before setting certificate configuration, please go to **System Maintenance** >> **Time and Date** to reset current time of the router first.

# 4.13 Creating 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.

#### 4.13.1 Creating an Account via Vigor Router

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

Veb-Filter License Status:Not Activated]				
Setup Test Server	auto-selected	auto-selected		
Neb Content Filter	Profile Table:		Set to Factory Defau	
Veb Content Filter Profile	Profile Table: Name	Profile	<u>Set to Factory Defau</u> Name	
		Profile <u>5.</u>		
Profile	Name			
<u>1.</u>	Name	<u>5.</u>		

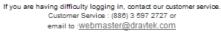
#### Or

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

System Maintenance >> Activation	Activate via interface	: auto-selected 💙
Web-Filter License [Status:Not Activated]		<u>Activate</u>
Authentication Message		
Activated Wiz, Authenticate is continuously, connect t OO:O4:55	to the server, 2000	)-01-01

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

	ole for MyVigor memb of the members of My		
LOGIN			
UserName :			
Password :			
Auth Code :		AYi GXZ	
	If you cannot read the v	vord, <u>click here</u>	
	<u>Forget passwo</u>	_{rd?} Login	
Don't have a	MyVigor Account?	Create an acc	ount now



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

Create an account - Ple	ease enter personal profile.		
1 Agreement	======================================		
	1. Agreement		
2 Personal Information	Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use		
	MyVigor service, it means that you have read, understand and agree to accept the items listed in this		
	agreement. Draytek can modify or change the content of the items without any reasons. It is		
3 Preferences	suggested for you to notice the medications or changes at any time. If you still use MyVigor service		
	after knowing the modifications and changes of this service, it means you have read, understand and		
	agree to accept the modifications and changes. If you do not agree the content of this agreement,		
	please stop using MyVigor service.		
4 Completion			
	2. Registration		
	To use this service, you have to agree the following conditions:		
	(a) Provide your complete and correct information according to the registration steps of this service.		
	(b) If you provide any incorrect or fake information here. DrayTek has the right to pause or terminate		
	🗹 I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)		

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	
3 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 - F	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	I would like to subscribe to the MyVigor e-letter.	
Information	l would like to receive DrayTek product news.	V
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
-		
Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

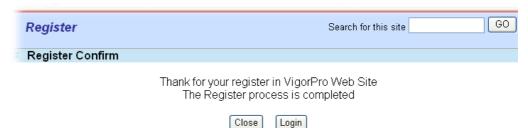
***** This is an automated message from myvigor.draytek.com.*****

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



- 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**.
  - This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

M		
Mary		
••••		
T4he1C	T4he1C	
lf you cannot read	the word, <u>click here</u>	
Forget pas	sword? Login	
MyVigor Accoun	t? <u>Create an ac</u>	count now
	ging in, contact our customer sei e : (886) 3 597 2727 or	wice.
	T4he1C If you cannot read Forget pas MyVigor Accour	T4he1C T4he1C

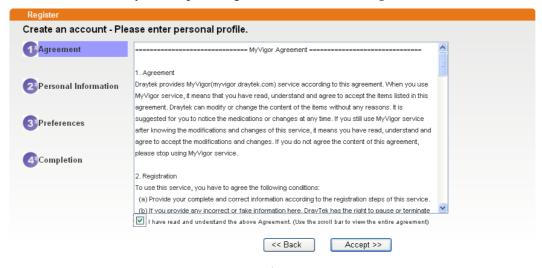
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

#### 4.13.2 Creating 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.

<b>Dray</b> Tek	MyVig	or		Customer Survey
ft Home	Search	30		
AL (1)	MyVigor for you	^		Login
About Us Product My Information VigorPro	MyVigor website replaces the VigorPro site as DrayTek's portal site for the latest products and services in network security, including Anti- Virus, Anti-Spam, Web Content Filter etc. The products and functions that are supported in this site include:			UserName Password AuthCode
	VigorPro Unified Security Firewall series:			<b>Qb</b> k q Vd
	<ul> <li>Activation of CommtouchTM GlobalView Web Content Filter license key</li> <li>Activation of DT Anti-Virus license key</li> <li>Activation of Kaspersky Anti-Virus license key</li> <li>Activation of CommtouchTM Anti-Spam license key and</li> </ul>		•	f you can't read the AuthCode , <u>click here</u> Login Forget password?
	membership <u>Vigor routers (for models that support Commtouch</u> TM )			Not registered yet ? <u>Click here !</u>
	- Activation of Commtouch TM GlobalView Web Content Filter license key			
	The MyVigor website contains a trail version of Commtouch TM GlobalView Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.			
Please use IE 5.0 or above (resolution 1024 * 788 ) for best display. ⊜ DrayTek Corp.	More customer-oriented services are planned for MyVigor site for the near future.	~	•	

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



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

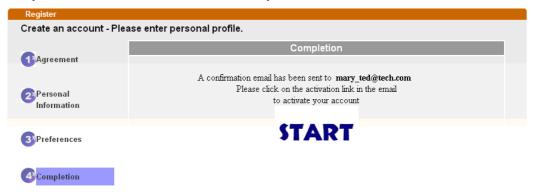
	Account Informati	ion
Agreement	UserName:*	Mary Check Account
	Password:*	(3 ~ 20 characters)
Personal	Password.	(4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	
	Personal Informat	tion
3 Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	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	I would like to subscribe to the MyVigor e-letter.	
Information	I would like to receive DrayTek product news.	V
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
Completion		< Back Continue >>



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>.

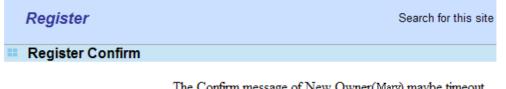
***** This is an automated message from myvigor draytek.com.*****

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.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN			
UserName :	Mary		
Password :	••••		
Auth Code :	T4he1C	T4he1C	
	If you cannot read the	word, <u>click here</u>	
	Forget passw	ord? Login	
Don't have a	MyVigor Account ?	<u>Create an acc</u>	ount now
lf you a	are having difficulty logging Customer Service : (;	in, contact our customer serv 386) 3 597 2727 or	ice.

email to :webmaster@draytek.com

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

# 4.14 How to Implement the LDAP/AD Authentication for User Management?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 3200 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

- 1. Access into the web user interface of the Vigor router.
- 2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings.

<ul> <li>✓ Enable</li> <li>Bind Type</li> <li>Regular Mode ▼</li> <li>Server Address</li> <li>172.16.2.8</li> <li>Destination Port</li> <li>389</li> <li>Use SSL</li> <li>Regular DN</li> <li>uid=vpntest,ou=vpnuser,dc=ms,dc=dr</li> </ul>	Seneral Setup Active Directory / LDAP Profiles	
	Bind Type Server Address Destination Port	172.16.2.8
Regular Password OK Cancel	Regular Password	

Applications >> Active Directory /LDAP

There are three types of bind type supported:

- **Simple Mode** Just simply do the bind authentication without any search action.
- Anonymous Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode** Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
- 3. Create LDAP server profiles. Click the **Active Directory** /LDAP tab to open the profile web page and click any one of the index number link.

If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.



Applications >> Active Directory /LDAP>>Server Profiles

ex No. 1		
Name	rd1	
Common Name Identifier	uid	
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com	9
Additional Filter	cn=rd1,ou=group,dc=ms,dc=draytek,d	
Note: Please type in your addition. For example, 1) For OpenLDAP: (gidNumber=50( 2) For AD: (msNPAllowDialin=TRUE)	))	
Group Distinguished Name	OK Cancel	2

#### and

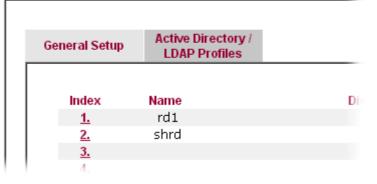
Applications >> Active Directory /LDAP>>Server Profiles

dex No. 2		
Name	shrd	
Common Name Identifier	uid	
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com	9
Additional Filter	cn=shrd,ou=group,dc=ms,dc=draytek,	
Note: Please type in your addition. For example, 1) For OpenLDAP: (gidNumber=50( 2) For AD: (msNPAllowDialin=TRUE)	))	
Group Distinguished Name	OK Cancel	
2		

4. Click **OK** to save the settings above.

Applications >> Active Directory /LDAP

Active Directory /LDAP



5. Open User Management>>General Setup. Select User-Based as the Mode option.

User Management >> General Setup

Mode: User-Based 💌				
Web Authentication: H	TTPS 🔽			
Notice :		- in Data Filter -		
<ol> <li>User Management will n in user-based firewall m</li> </ol>		s in Data Filter a:	s whitel	ists and placklists
2. Users match the above		quired for authe	nticatio	n.
The firewall rules policy 3. Otherwise, authentication		ers not matched	the ab	ove lists.
The firewall rules desigr				
Landing Page (Max 255 cha	racters)	P	review	Set to Factory Default
<body stats="l"><script 1a<="" td=""><th></th><th>-</th><th></th><th></th></tr><tr><td>window.location='http://</td><th></th><th></th><th></th><th></th></tr></tbody></table></script></body>				

6. Then open **User Management>>User Profile.** Click index 3 to create a new user profile.

User Profile 1	Fable
Profile	Name
1.	admin
<u>2.</u>	Dial-In User
<u>3.</u>	

User Management >> User Profile

User Management >>User Profile

7. Check **Enable this account;** choose **LDAP** as **External Server Authentication**; and check the user profile you want.

Index 3	
Enable this account	
Username	
Password	
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	LDAP 💌
☑ rd1	🖉 shrd
Log	None 💌
Pop Browser Tracking Window	
Authentication	🖉 Web 🕜 Alert Tool 🖉 Telnet
Landing Page	
Index(1-15) in <u>Schedule</u> Setup:	, , , , , , , , , , , , , , , , , , ,
Enable Time Quota 0 min.	(+) - 0 min.
🔲 Enable Data Quota 🛛 🛛 🕅 🖪	✓ + - 0 MB
Reset quota to default when sched	luling time expired
📃 Enable 🛛 Default Time Quota	0 min. Default Data Quota 0 MB

8. After finished above configurations, click OK to save the settings. Now, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.



# 4.15 How to Implement the LDAP/AD Authentication for VPN?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 3200 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

- 1. Access into the web user interface of the Vigor router.
- 2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings.

General Setup	Active Directory / LDAP Profiles	
Enable Bind Type Server Addres Destination Po Use SSL	-	Regular Mode 💌 172.16.2.8 389
Regular DN Regular Passv	vord	uid=vpntest,ou=vpnuser,dc=ms,dc=dr •••• Cancel
of VPN and Remote A	Access >> <u>PPP General</u>	the LDAP profiles, they will be listed in the page <u>Setup</u> . If you want to use the profiles for VPN PTP LDAP Profiles in <b>VPN and Remote Access &gt;&gt;</b>

Applications >> Active Directory /LDAP

There are three types of bind type supported:

- Simple Mode Just simply do the bind authentication without any search action.
- Anonymous Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode** Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
- 3. Create LDAP server profiles. Click the **Active Directory** /**LDAP** tab to open the profile web page and click any one of the index number link.

If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.



Applications >> Active Directory /LDAP>>Server Profiles

ex No. 1		
Name	rd1	
Common Name Identifier	uid	
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com	9
Additional Filter	cn=rd1,ou=group,dc=ms,dc=draytek,d	
Note: Please type in your addition For example, 1) For OpenLDAP: (gidNumber=50 2) For AD: (msNPAllowDialin=TRUE		
Group Distinguished Name	OK Cancel	2

#### and

Applications >> Active Directory /LDAP>>Server Profiles

Name	shrd	
Common Name Identifier	uid	
Base Distinguished Name	ou=people,dc=ms,dc=draytek,dc=com	9
Additional Filter	cn=shrd,ou=group,dc=ms,dc=draytek,	
Noto, Diobeo tupo in your odd	litional filter for BaseDN search request.	
For example, 1) For OpenLDAP: (aidNumber		

- 4. Click **OK** to save the settings above.
- 5. Open User Management>>General Setup. Select User-Based as the Mode option.

User Management >> General Setup

Web Authentication:	
Notice :	
1. User Management will refer to active rules i	in Data Filter as whitelists and blacklists
in user-based firewall mode.	
5. I the sub-sector to the sector to the sub-sector to the sector to the	
	uired for authentication.
The firewall rules policy will still valid. 3. Otherwise, authentication required for user	rs not matched the above lists.
The firewall rules policy will still valid.	rs not matched the above lists.
The firewall rules policy will still valid. 3. Otherwise, authentication required for user The firewall rules designated in the user pr	rs not matched the above lists.
The firewall rules policy will still valid. 3. Otherwise, authentication required for user The firewall rules designated in the user pr Landing Page (Max 255 characters)	rs not matched the above lists. ofile's policy will still valid. <u>Preview  Set to Factory Default</u>
The firewall rules policy will still valid. 3. Otherwise, authentication required for user The firewall rules designated in the user pr Landing Page (Max 255 characters) <body stats="1"><script language="javascrip&lt;/td&gt;&lt;td&gt;rs not matched the above lists.&lt;br&gt;ofile" policy="" s="" still="" valid.<br="" will=""><u>Preview</u>  <u>Set to Factory Default</u> it'></td></tr><tr><td>3. Otherwise, authentication required for user</td><td>rs not matched the above lists. ofile's policy will still valid. <u>Preview</u>  <u>Set to Factory Defat</u> tt'></td></tr></tbody></table></script></body>	

6. Then open VPN and Remote Access>>PPP General Setup to check the profile(s) that will be authenticated with LDAP server. Choose PAP Only as Dial-In PPP Authentication.

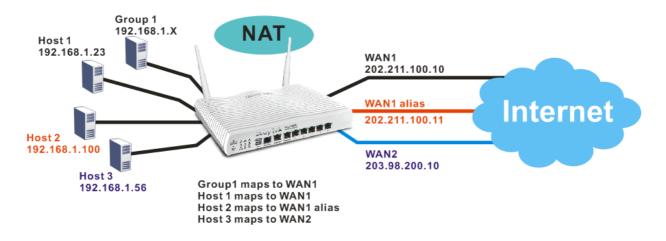
PPP General Setu	р			
PPP/MP Protocol		_		LPAP Server Profiles for PPP Authentication
Dial-In PPP Authentication	PAP Only		*	✓ rd1 ✓ shrd
Dial-In PPP Encryption(MPPE)	Optional MP	PE		Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for
Mutual Authentica	ition (PAP)	🔘 Yes 💽 No		PPP Authentication!!
Username				
Password				
IP Address Assignme (When DHCP Disable		n Users		
Assigned IP start	LAN 1	192.168.1.200		
	LAN 2	192.168.2.200		
	LAN 3	192.168.3.200		
	LAN 4	192.168.4.200		
			ОK	

VPN and Remote Access >> PPP General Setup

7. After finished above configurations, click OK to save the settings. Now, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.

# 4.16 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 Vigor2830.
- 2. Open WAN>>Internet Access. For WAN1, choose MPoA/Static or Dynamic IP as the Access Mode.

WAN >> Internet Access

nternet Index	 Physical Mode	Access Mode		
WAN1	ADSL	MPoA (RFC1483/2684)	*	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.

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 / PPPoA	MPoA (RFC	1483/2684)	IPv6
🔍 Enable 🛛 🖲 Disab	le	WAN IP Network Settin	gs WAN IP Alias
DSL Modem Settings		🔍 Obtain an IP addres	s automatically
-	Channel 2 🗸 🗸	Router Name	Vigor
Encapsulation		Domain Name	
	ðridged IP LLC 🛛 👻	* : Required for sor DHCP Client Identifier for	
VPI 8	}	🔲 Enable	
VCI E	38	Username	
Modulation	Multimode 🛛 🔽	Password	
	(	Specify an IP addres	ss
WAN Connection Detection		IP Address	202.211.100.10
	ARP Detect 🔽	Subnet Mask	255.255.255.0
Ping IP		Gateway IP Addres	s
TTL:			
RIP Protocol		Default MAC Addr	
Enable RIP		<ul> <li>Specify a MAC Ad</li> <li>MAC Address: 00</li> </ul>	
Bridge Mode		DNS Server IP Address	
🔲 Enable Bridge Mode		Drimary ID Address	0000

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.

/AN1 II Index	P Alias ( Mu Enable	Aux. WAN IP	Join NAT IP Pool
1.			
2.	V	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	

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

.oad-Ba	lance/Re	oute Policy										0
.oad-Ba	oad-Balance/Route Policy   Set to Fac											
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start		Move Up	Move Down
1		Any	WAN1									<u>Down</u>
<u>2</u>		Any	WAN1								UP	<u>Down</u>
<u>3</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>4</u>		Any	WAN1								UP	Down
<u>5</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>6</u>		Any	WAN1								UP	Down
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								UP	Down
< <u>1-10</u>	11-20	21-30	<u> 31-40   41-5</u>	<u>50</u> >>							ļ	Next >>

Wizard Mode: most frequently used settings in three pages

- Advance Mode: all settings in one page
- 5. Click Index number 1 and 2 to configure the details. After finished the settings, click **OK** to save the settings respectively.

OK

Load-Balance/Route Policy	
---------------------------	--

h

🗹 Enable	
Criteria	
Protocol	Any 💌
Source IP	Any
	Src IP Start Src IP End
	192.168.1.16 ~ 192.168.1.31
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
Interface Address	1 💙
Gateway IP	Default Gateway
*	Specific Gateway
More Options	
Auto Failover to the Othe	r WAN
Packet Forwarding to WAN	Force NAT
via	Force Routing

#### And

Load-Balance/Route Policy

Load-Balance/Route Policy

✓ Enable Criteria	
Protocol	Any 🗸
Source IP	Any
	Src IP Start Src IP End
	192.168.1.100 ~ 192.168.1.100
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
Interface Address	2-202.211.100.11 🔽
Gateway IP	Default Gateway
	Specific Gateway
More Options	
Auto Failover to the Othe	er WAN
Packet Forwarding to WAN	Force NAT
via	Force Routing

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

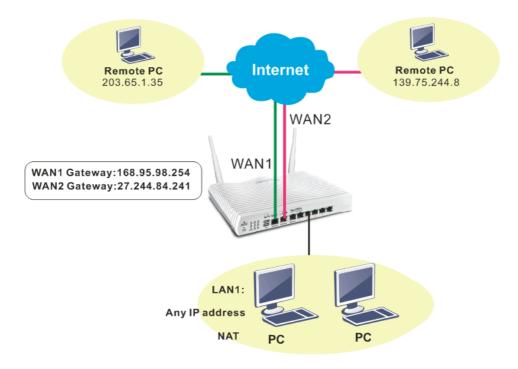
ndex E	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	10	Dest Port Start	FUIL		Move Dow
1		Any	WAN1		192.168.1.16	192.168.1.31	Any	Any	Any	Any		Dow
<u>2</u>		Any	WAN1	202.211.100.11	192.168.1.100	192.168.1.100	Any	Any	Any	Any	UP	Dow
<u>3</u>		Any	WAN1								<u>UP</u>	Dow
<u>4</u>		Any	WAN1								<u>UP</u>	Dow
<u>5</u>		Any	WAN1								<u>UP</u>	Dow
<u>6</u>		Any	WAN1								<u>UP</u>	Dow
<u>7</u>		Any	WAN1								<u>UP</u>	Dow
<u>8</u>		Any	WAN1								<u>UP</u>	Dow
<u>9</u>		Any	WAN1								<u>UP</u>	Dow
<u>10</u>		Any	WAN1								<u>UP</u>	Dow
< 1-10	11-20	21-30	31-40   41-5	<u>50</u> >>							1	lext :

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

0

# 4.17 How to setup Load Balance for Packets?

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



1. Access into web user interface of Vigor2830 series. Open Load-Balance/Route Policy.



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

Load-Bala	ance/Rout	te Policy
-----------	-----------	-----------

ndex	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Port	Move Up	Move Dowr
1		Any	WAN1									Down
2		Any	WAN1								<u>UP</u>	Down
<u>3</u>		Any	WAN1								<u>UP</u>	Down
<u>4</u>		Any	WAN1								<u>UP</u>	Down
<u>5</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>6</u>		Any	WAN1								<u>UP</u>	Down
<u>7</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>8</u>		Any	WAN1								<u>UP</u>	Down
<u>9</u>		Any	WAN1								<u>UP</u>	<u>Down</u>
<u>10</u>		Any	WAN1								UP	Down

• Wizard Mode: most frequently used settings in three pages

Advance Mode: all settings in one page

Load-Balance/Route Policy

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

OK )

✓ Enable Criteria	
Protocol	Any 🗸
Source IP	Any
	Src IP Start Src IP End
	~
Destination IP	Any
	Dest IP Start Dest IP End
	203.65.1.35 ~ 203.65.1.35
Destination Port	Any     Dest Port Start Dest Port End
Send to if Criteria Matched	
Interface	WAN1
Interface Address	1
Gateway IP	Default Gateway
	Specific Gateway
More Options	
Auto Failover to the Other Auto Failover to the Other Auto Failover to the Other Automatication and the Automat	ner WAN
Packet Forwarding to WAN	Force NAT
via	Force Routing

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

0

.oad-Ba	bad-Balance/Route Policy Set to Factor												
Index	Enable	Protocol	Interface	Interface Address	Src IP Start	IP	Dest IP Start	Dest I	P End	Dest Port Start		Move Up	Move Dowi
1		Any	WAN1		Any	Any	203.65.1.35	203.65	5.1.35	Any	Any		Dowr
<u>2</u>		Any	WAN1									UP	Dow
3		Any	WAN1									<u>UP</u>	Dowr
<u>4</u>		Any	WAN1									UP	Dowr
<u>5</u>		Any	WAN1									UP	Dowr
<u>6</u>		Any	WAN1									UP	Dowr
7		Any	WAN1									<u>UP</u>	Dowr
8		Any	WAN1									UP	Dowr
<u>9</u>		Any	WAN1									<u>UP</u>	Dowr
<u>10</u>		Any	WAN1									UP	Dowr

Wizard Mode: most frequently used settings in three pages

Advance Mode: all settings in one page

OK	
----	--

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

# 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

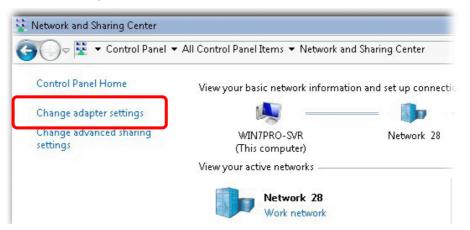


The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

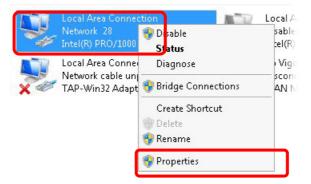
1. Open All Programs>>Getting Started>>Control Panel. Click Network and Sharing Center.



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	tion Properties	2
Networking Sharing		
Connect using:		
🔮 Intel(R) PRO/1	000 MT Network Conne	ection
		Configure
This connection uses	the following items:	
🗹 🛃 Client for Mic		
Privacyware		
🛛 🗹 💂 QoS Packet		100 IV
	er Sharing for Microsoft	
	acol Version 6 (TCP/IP)	
	ocol Version 4 (TCP/IP)	
	opology Discovery Map	
Link-Layer T	opology Discovery Resp	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 automat	ically	ו			
🖯 Use the following IP address:-		,			
IP address:			9	÷.	
Subnet mask:		12	2		
Default gateway:					
Obtain DNS server address au	tomatio	ally			
🔿 Use the following DNS server a	address	ses:			
Preferred DNS server:		15		11 - A	
Alternate DNS server:	Γ	2	1		
Validate settings upon exit				Adv	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.

0 0	Network	e
5how All Displays	Sound Network Startup Disk	
	Location: Automatic	
	CP/IP PPPoE AppleTalk Proxies Ethernet	
Configure IP	v4: Using DHCP	
IP Addre	ss: 192.168.1.10 (Renew DHC	P Lease
Subnet Ma Rout	(If required)	
DNS Serve	irs:	(Optional)
Search Domai	ns:	(Optional)
IPv6 Addre	ss: fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	?
Click the lock	to prevent further changes.	Apply Now



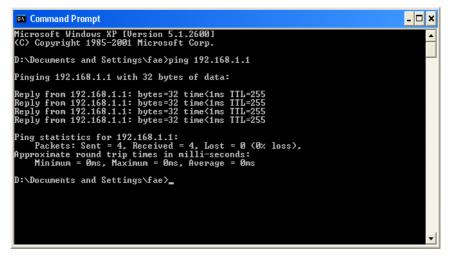
# **5.3 Pinging the Router from Your Computer**

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

#### For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

#### For MacOs (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	
Welcome to Darwin! Vigor18:~ draytek\$ p PING 192.168.1.1 (19 64 bytes from 192.16 64 bytes from 192.16 64 bytes from 192.16 64 bytes from 192.16	3 02:24:18 on ttyp1 ing 192.168.1.1 2.168.1.1): 56 data bytes 8.1.1: icmp_seq=0 ttl=255 time=0.755 ms 8.1.1: icmp_seq=1 ttl=255 time=0.697 ms 8.1.1: icmp_seq=2 ttl=255 time=0.716 ms 8.1.1: icmp_seq=3 ttl=255 time=0.731 ms 8.1.1: icmp_seq=4 ttl=255 time=0.72 ms	2
In the second	statistics d, 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/WAN2 to review the settings that you configured previously.

WAN >>	Internet Access		
nternet	Access		
Index	Display Name	Physical Mode	Access Mode
WAN1		ADSL	PPPoE / PPPoA 💙 Details Page
WAN2		Ethernet	Static or Dynamic IP 🛛 🖌 Details Page
WAN3		USB	None 🔽 Details Page

# 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 Vigor2830. 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 Vigor2830.

#### 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.



Image:	g Utility
System Time         Router Time         Host         Message           2013-08-27 15:11:09         Aug 27 07:10:53         Vigor-router         statistic: Session Usage: 123 (5 min average)           2013-08-27 15:11:09         Aug 27 07:10:53         Vigor-router         statistic: Session Usage: 123 (5 min average)           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/Host Controller Driver: OTG           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/IndopintAddress=02 (m), Attributes=02 (Bulk)           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/Interface Class           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/Interface Classes           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/Interface Classes           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB/Interface Classes           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor	Gateway IP
2013-08-27 15:11:09         Aug 27 07:10:53         Vigor-router         statistic:         Session Usage: 123 (5 min average)           2013-08-27 15:11:09         Aug 27 07:10:53         Vigor-router         statistic:         Session Usage: 123 (5 min average)           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         IUSB[Phost Controller Driver: OTG           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=82 (m), Attributes=02 (Bulk)           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=82 (m), Attributes=02 (Bulk)           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Interface Class:Subclass:Protocol = [08:06:50]           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Interface Class:Subclass:Protocol = [08:06:50]           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Pretrieac Class:Subclass:Protocol = [00:00:00]           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Periolutical (Class:Protocol = [00:00:00]           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Periolutical (Class:Protocol = [00:00:00]           2013-08-27 15:11:00         Aug 27 07:09:51         Vigor-router         [USB]Product:[2] PMS         [USB]Product:[2	
2013-08-27 15:11:09         Aug 27 07:10:53         Vigor-router         statistic: WAN1: Tx 81 Kbps, Rx 12 Kbps (\$ min average)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Host Controller Driver: OTG           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=02 (m), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=01 (out), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Mass Storage device class           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface Class:Subclass:Protocol = [08:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Per-interface classes           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]Pervice Class: Subclass:Protocol = [00:00:00]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Podurict[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Podurict[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router	
2013-08-27 15:11:09         Aug 27 07:10:53         Vijor-router         statistic: WAN1: Tx 81 Kbps, Åx 12 Kbps (Š min average)           2013-08-27 15:10:07         Aug 27 07:09:51         Vijor-router         [USB]Host Controller Driver: OTG           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]EndpointAddress=01 (out), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]EndpointAddress=01 (out), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]Interface class: Subclass: Wrotocol =         [08:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]Interface class: Subclass: Wrotocol =         [08:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]Interface classes         [USB]Interface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]SerialNumber:[3] ED96E018         [US0:00]         [US1]           2013-08-27 15:10:06         Aug 27 07:09:51         Vijor-router         [USB]BerialNumber:[3] ED96E018         [US2]         [US2]         [US3] Storage         [US3] Storage         [US3]         [US3]         [US3]         [US3]         [US3]         [US3]         [US3]         [US3]         [US3]	
2013-08-27 15:10:07         Aug 27 07:09:51         Vigor-router         [USB]Fhost Controller Driver: OTG           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=82 (in), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=82 (in), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]EndpointAddress=82 (in), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]IndpointAddress=82 (in), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface: class: SubClass: Protocol = [08:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface: dasses           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]SerialNumber:[3] ED96E018           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Product:[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Product:[2] Mass Storage           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         [USB]EndpointAddress=01 (out), Attributes=02 (Bulk)           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface (Lass: Subclass: Protocol = [06:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface (Lass: Subclass: Protocol = [06:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface (Lass: Subclass: Protocol = [06:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Er-interface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Ereinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Ereinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Ereinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Manufacturer: [1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Manufacture: [1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Ush new device: Vendor ID [058F], Product ID: [6387]           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]Mass Storage device class           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface class:SubClass:Protocol = [08:06:50]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface class:SubClass:Protocol = [00:00:00]           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]Device Class:SubClass:Protocol = [00:00:00]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Derinterface: [3] ED96E018           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Derinter[3] ED96E018           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Maunfacturer: [1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb _set_configuration: configuration=1	
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         Wigor-router         [USB]Interface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Interface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Perinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Vanufacturer:[1] Generic           2013-08-27 15:10:06         Au	
2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Interface: 0           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Device Class:SubClass:Protocol = [00:00:00]           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]Device Class:SubClass:Protocol = [00:00:00]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Droduct:[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Maunfacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Ush new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ush new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ush gene device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ush gene device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ush gene device: Vendor ID [058F], Product ID: [6387]	
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]Derinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Derinterface classes           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Product[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Vanufacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb new device: Nondor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb _set_configuration: configuration=1	
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         Wigor-router         [USB]SerialNumber:[3] E096018           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Product:[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Manufacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Manufacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Ush new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ush_sew device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ush_sew device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ush_set_configuration: configuration=1	
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         Wigor-router         [USB]Product:[2] Mass Storage           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Vanufacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ub new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ub new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ub new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wigor-router         [USB]ub set_configuration: configuration=1	
2013-08-27         15:10:06         Aug 27         07:09:51         Vigor-router         [USB]Product:[2] Mass Storage           2013-08-27         15:10:06         Aug 27         07:09:51         Vigor-router         [USB]Manufacturer:[1] Generic           2013-08-27         15:10:06         Aug 27         07:09:51         Vigor-router         [USB]Ush new device: Vendor ID [058F], Product ID: [6387]           2013-08-27         15:10:06         Aug 27         07:09:51         Vigor-router         [USB]ush new device: Vendor ID [058F], Product ID: [6387]           2013-08-27         15:10:06         Aug 27         07:09:51         Vigor-router         [USB]ush_set_configuration: configuration=1	
2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Manufacturer:[1] Generic           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ub new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]ub_sceconfiguration: configuration=1	
2013-08-27 15:10:06         Aug 27 07:09:51         Wgor-router         [USB]Usb new device: Vendor ID [058F], Product ID: [6387]           2013-08-27 15:10:06         Aug 27 07:09:51         Wgor-router         [USB]unun of interfaces=1           2013-08-27 15:10:06         Aug 27 07:09:51         Wgor-router         [USB]usb_set_configuration: configuration=1	
2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]num of interfaces=1           2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]usb_set_configuration: configuration=1	
2013-08-27 15:10:06 Aug 27 07:09:51 Vigor-router USBjusb_set_configuration: configuration=1	
2013-08-27 15:10:06         Aug 27 07:09:51         Vigor-router         [USB]Usb Device Connected at Port 0	

#### Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2830. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

# 5.6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.



**Warning:** After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

#### Software Reset

You can reset the router to factory default via Web page. Such function is available in **Admin Mode** only.

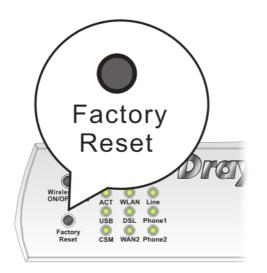
Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

Reboot System	
	Do you want to reboot your router ?
	O Using current configuration
	<ul> <li>Using factory default configuration</li> </ul>
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

#### **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 your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

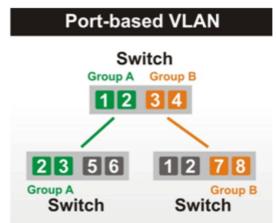


# Appendix I: VLAN Applications on Vigor Router

Virtual Local Area Network is so-called VLAN. It offers the logical grouping technique to separate the physical ports of Ethernet switches, thus we can management our local network easier, more flexible and secure. For instance, you're a networking administrator in your company and you're planning to isolate the visitors' traffics from your private network for security considerations because you cannot ensure that visitors' computer is clean. Or you want to separate your private network into several parts by divisions because there are too many computers in the same network segment and it results in the local traffics heavily. VLAN helps you to solve these situations, and DrayTek's products support bellow two popular types:

#### Port-based

It uses a matrix table of the physical ports to define the traffics how to exchange between each port, and the traffics will be isolated from the ports are not being ticked in the same line. It is the easiest way to setup an isolate network, but not a flexible way to maintain a growing network. Because the idea of port-based VLAN is grouping by physical ports, but the difficulty is how to handle the traffics between two or more Ethernet switches. Thus, VLAN is suitable for some circumstances, for example, the rental apartment, SOHO office...and so on. These clients may need two or three isolated networks only and setup a network in a simple way.

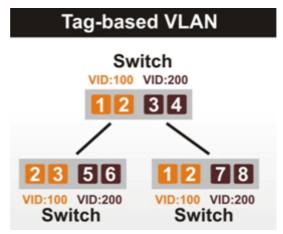


#### Tag-based

The idea of tag-based VLAN is to identify a virtual LAN with a specific ID, therefore, VLAN ID introduced by tag-based VLAN. Through VLAN ID, ports with different VID (VLAN ID) will be identified as in different LANs, so the traffics also will be isolated from each of VLANs. Many administrators who manage an enterprise network or even the internet service providers (ISP) adopt Tag-based VLAN popularly because it is convenient to maintenance and management a distributed network. Setting a large-scale network is easy by giving each of them with different VID and isolating the traffics at the same time. Besides the VLAN ID, there is another feature, **Trunk**, introduced. While the role of a port on an Ethernet switch is setup as a Trunk port, it means the VLAN ID will be kept while forwarding the packets between switches. By this feature, VLANs are able to distribute over two or more Ethernet



switches easily, moreover design a large and secured network is possible through Trunk port. When VLAN is being enabled on Vigor routers, the LAN ports are being turned into Trunk mode automatically. Therefore, a VLAN supported switch, like VigorSwitch G2260/P2261, or VigorSwitch G1240, is needed.



Vigor routers ^[Note] support Tag-based feature both on LAN and WAN interfaces. The next we'll demonstrate our web design and how to configure the settings by introducing the functionalities of Vigor router.

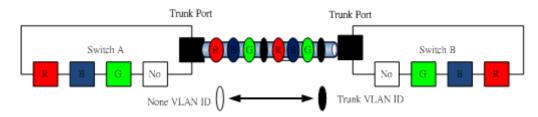
#### [Note]

Broadband router: Vigor2920/Vigor3200/Vigor2925/Vigo2960/Vigor3900

Modem router: Vigor2850/Vigor2860

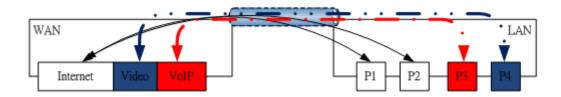
#### VLAN Packets on Vigor routers

Trunk mode of LAN



Trunk Port can carry the packets with VID but replace the Non-VID packet as the VID of Trunk port while forwarding the packets to another switch.

#### Bridge mode of WAN



P1 and P2 are doing NAT flow to access to the internet, but P3 and P4 will forward the packets between WAN and LAN ports directly.

#### Web User Interface

So far, there are two kinds of open system on Vigor router. One is DrayOS, which is DrayTek owned, and another is Linux-like which customized by DrayTek from OpenWRT. Here



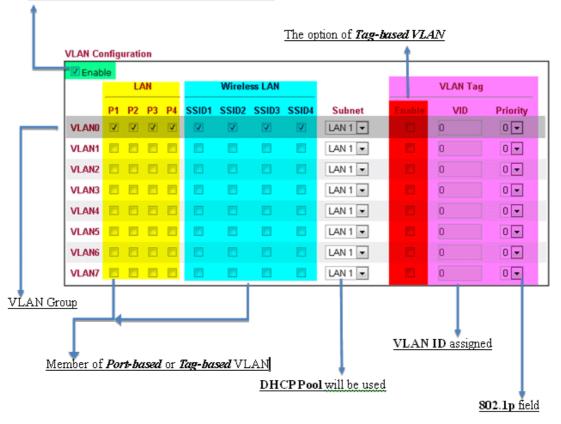
DrayOS system is going to be introduced to you because it is the most stable and superfast booting system in DrayTek products. If the UI style of yours is different from the following. It may not DrayOS system with new web style or maybe the Linux-like model.

#### WAN

Multi-VLA	N	L	1		
mana-v CPa	General		1		
Channel	Enable	WAN Type	VLAN Tag	Post-based Bridge	
<u> </u>	Yes	Ethernet(WAN1)	None		
2	Yes	Ethernet(WAN2)	None		
3.	No	Ethernet(WAN1)	None	Enable P1 P2 P3 P	P4 🗌 P8
4.	No	Ethernet(WAN1)	None	Enable P1 P2 P3 F	P4 🗌 P9
5.WAN5	No	Ethernet(WAN1)	None	Enable P1 P2 P3 F	P4 🗌 P!
6.WAN6	No	Ethernet(WAN1)	None	Enable P1 P2 P3 F	P4 🗌 P
Z.WAN7	No	Ethernet(WAN1)	None	Enable P1 P2 P3 F	P4 🗌 P
<u>8.</u>	No	Ethernet(WAN1)	None	Enable P1 P2 P3 P	P4 🗌 P
Prior	rog.	0			
nbers	rity: 1.Tag value .Only one of pen Port-bas fical Member 1	e must be set betw channel can be unta sed Bridge Connection ers P3 P4 P5	gged (equal to		
ibers	rity: 1.Tag valu .Only one of pen Port-bas ical Member 1	e must be set betw channel can be unta sed Bridge Connection ars P3 P4 P5 reved for NAT use,a	igged (equal to for this Channel ind cannot be c	0) at a time.	
nbers	rity: 1.Tag valu .Only one of pen Port-bas ical Member 1 P2 3 3.P1 is res pen WAN Int	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a erface for this Channe	igged (equal to for this Channel ind cannot be c	0) at a time.	
ibers Prior Note: 2 bers Phys Phys Note: 0 Phys Note: 0 WAN	rity: 1.Tag valu .Only one of pen Port-bas cical Member 1 P2 3 3.P1 is res pen WAN Int for Router-b	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a erface for this Channe	agged (equal to for this Channel and cannot be c	0) at a time.	
ng &	rity: 1.Tag valu .Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-base Setup: Sta	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a borne Application: Ma atic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time.	
bers Prior Note: 2 Dop Physic Physic Note: Note: Note: WAN WAN	rity: 1.Tag valu .Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-base Setup: Sta ccess Setup	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a borne Application: Ma atic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time. configured for bridge mode. WAN IP Network Settings	lly
ng & ISP A	rity: 1.Tag valu .Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-base Setup: Sta ccess Setup Name	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a borne Application: Ma atic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time.	lly
ng & Usen	rity: 1.Tag valu .Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-base Setup: Sta- ccess Setup Name name	e must be set betwichannel can be unta sed Bridge Connection ars P3 P4 P5 erved for NAT use, a borne Application: Ma atic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time. configured for bridge mode. WAN IP Network Settings Obtain an IP address automatical	lly
ng & Usen Pass	rity: 1.Tag valu Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-b Setup: Sta- ccess Setup Name name word	e must be set betwichannel can be unta sed Bridge Connection ers     P3     P4     P5 erved for NAT use, a terface for this Channel borne Application: Ma attic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time. configured for bridge mode. WAN IP Network Settings Obtain an IP address automatical Router Name <u>Vigor</u>	lly
bers bers prior Phys P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P P Note: P P Note: P P Note: P P P P P P P P P P P P P	rity: 1.Tag valu Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-b Setup: Sta ccess Setup Jame name word Authentical	e must be set betwichannel can be unta sed Bridge Connection ers     P3     P4     P5 erved for NAT use, a terface for this Channel borne Application: Ma attic or Dynamic IP	agged (equal to for this Channel and cannot be c anagement v	0) at a time. configured for bridge mode. WAN IP Network Settings Obtain an IP address automatical Router Name Vigor Domain Name Vigor	lly
Ders Ders Ders Ders Ders Ders Ders Ders	rity: 1.Tag valu Only one of pen Port-bas- cical Member 1 P2 [ 3.P1 is res- pen WAN Int for Router-b Setup: Sta ccess Setup Jame name word Authenticat ways On	or PAP or CH	agged (equal to for this Channel and cannot be c anagement AP	O) at a time.      Monthead for bridge mode.      WAN IP Network Settings     Obtain an IP address automatical     Router Name     Vigor     Domain Name     *: Required for some ISPs	lly
bers bers ing & WAN Usen Pass PP Val Idle	rity: 1.Tag valu Only one of pen Port-bas- ical Member 1 P2 [ 3.P1 is resonant pen WAN Inter- for Router-b Setup: State ccess Setup Name name word Authenticat ways On Timeout	0       •         e must be set betwichannel can be untained can be untained by the set betwichannel can be untained by the set of t	agged (equal to for this Channel and cannot be c anagement v	WAN IP Network Settings Obtain an IP address automatical Router Name *: Required for some ISPs Specify an IP address	lly
bers bers bers bers bers p Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Not	rity: 1.Tag valu Only one of pen Port-bas- ical Member 1 P2 [ 3.P1 is resonant pen WAN Inter- for Router-b Setup: Stand Ccess Setup Jame name word Authenticat ways On Timeout dress From	0       •         e must be set betwichannel can be untained can be untained by the set betwichannel can be untained by the set of t	agged (equal to for this Channel and cannot be c anagement AP second(s)	O) at a time.	lly
ers Prior Note: P Phys P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note: P Note:	rity: 1.Tag valu Only one of pen Port-bas- ical Member 1 P2 [ 3.P1 is resonant pen WAN Inter- for Router-b Setup: Stand Ccess Setup Jame name word Authenticat ways On Timeout dress From	O     O     e must be set betwichannel can be untained can be untained by the set betwichannel can be untained by the set of th	agged (equal to for this Channel and cannot be c anagement • AP • second(s) t IP)	0) at a time.         configured for bridge mode.         WAN IP Network Settings         Obtain an IP address automatical         Router Name       Vigor         Domain Name         *: Required for some ISPs         Specify an IP address         IP Address         Subnet Mask	lly
g & Usen Pass PA Base PA Base PA Base PP Pass PP A Base PP P C A I C P C C C C C C C C C C C C C C C C C	rity: 1.Tag valu Only one of pen Port-bas- cal Member 1 P2 [ 3.P1 is result or Router-bas- Setup: Star- basen WAN Inter- for Router-base- Setup: Star- basen WAN Inter- for Router-base- Setup: Star- basen WAN Inter- for Router-base- Setup: Star- Setup: Star- star- star- star- top of the setup of	O     O     e must be set betwichannel can be untained can be untained by the set betwichannel can be untained by the set of th	agged (equal to for this Channel and cannot be c anagement • AP • second(s) t IP)	O) at a time.      MAN IP Network Settings     Obtain an IP address automatical     Router Name     Yigor     Domain Name     *: Required for some ISPs     Specify an IP address     IP Address     Subnet Mask     Gateway IP Address	lly

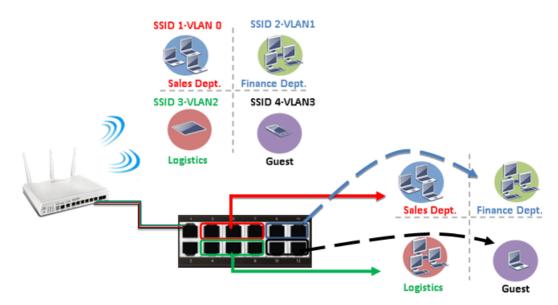
#### LAN

Enable Port-based VLAN by checking the option



#### **VLAN** applications on Vigor router

• Multi Subnet (VLAN of LAN)



#### Port-based mode

	_	U	NN .			Wirele	ss LAN			VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSI03	SSID4	Subnet	Enable	VID	Priority	
VLANO	V		8	8	V			23	LAN 1 💌		0	0 -	
VLAN1	8	V	۵		8	7			LAN 2 💌		0	0 💌	
VLAN2			7				1		LAN 3 📼		0	0 💌	
VLAN3				V				V	LAN 4 💌	1	0	0 💌	
VLAN4									LAN 1 💌		0	0 💌	
VLAN5									LAN 1 💌		0	0 💌	
VLAN6									LAN 1 💌		0	0 💌	
VLAN7	23	83	23	23	13	12	10	23	LAN 1 💌		0	0 .	

#### Tag-based mode

	LAN					Wirele	ss LAN			VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority	
VLAND									LAN 1 💌		10	0.	
VLAN1		V				V			LAN 2 💌	1	20	0 💌	
VLAN2			$\overline{\mathbf{v}}$				V	8	LAN 3 💌	V	30	0 💌	
VLAN3				7				V	LAN 4 💌	V	40	0 💌	
VLAN4									LAN 1 💌		0	0 💌	
VLAN5									LAN 1 💌		0	0 💌	
VLAN6									LAN 1 💌		0	0 💌	
VLAN7	23	83	83	23			13	23	LAN 1 💌		0	0 -	

By above settings, there are four private networks will be created and computers attached with each of LAN ports or SSIDs which are able to obtain a private IP address from each DHCP servers (LAN1/LAN2/LAN3/LAN4). However, the traffics of the LAN port or SSID that are NOT being grouped in the same VLAN are unable to forward to each other. The benefit of Port-based is able to extend the wired ports by installing a cheaper dumb switch as many as you need, but Tag-based offers you a flexible and well-managed network. The networks are isolated, secured and reduce the broadcasting storm effectively in each of networks with VLAN.

- SSID 1-VLAN 0 SSID 2-VLAN 0 Sales Dept. SSID 3-VLAN0 Logistics SSID 4-VLAN1 Couest Cuest SSID 4-VLAN1 Couest Cuest SSID 4-VLAN1 Couest Cuest
- Guest Network

#### Port-based mode

2 Enab	LAN			Wireless LAN						VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority	
VLANO				V					LAN 1 💌		0	0 💌	
VLAN1								V	LAN 2 💌	1	0	0 💌	
VLAN2									LAN 1 💌		0	0 💌	
VLAN3									LAN 1 💌	1	0	0 💌	
VLAN4									LAN 1 💌		0	0 💌	
VLAN5									LAN 1 💌		0	0 💌	
VLAN6									LAN 1 💌		0	0 💌	
VLAN7	23	23	23	23	23	23	23	13	LAN 1 💌	<b>F</b>	0	0 💌	

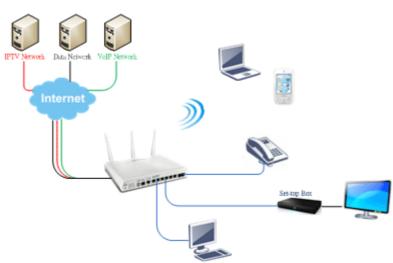
#### Tag-based mode

V Enable												
	_	LAN			Wireless LAN				VLAN Tag			
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet	Enable	VID	Priority
VLAND	63		$[\overline{e}]$		1	V	1		LAN 1 💌	8	0	0 💌
VLAN1	V	۲						V	LAN 2 💌	V	10	0 💌
VLAN2									LAN 1 💌		0	0 💌
VLAN3									LAN 1 💌		0	0 💌
VLAN4									LAN 1 💌		0	0 💌
VLAN5									LAN 1 💌		0	0 💌
VLAN6									LAN 1 💌		0	0 💌
VLAN7									LAN 1 💌		0	0 💌

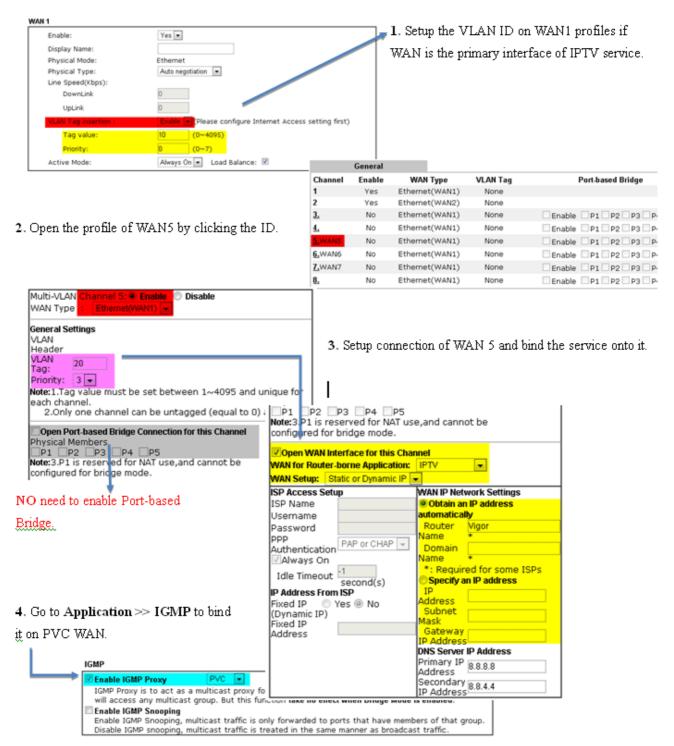
To deploy a guest network, which serves your guests the internet accessibility, but the traffics have to be isolated from your private network due to the security considerations, it can be done by above settings. However, a switch support VLAN function is need if VLAN Tag enabled.

#### • Triple Play (Multi-WAN)

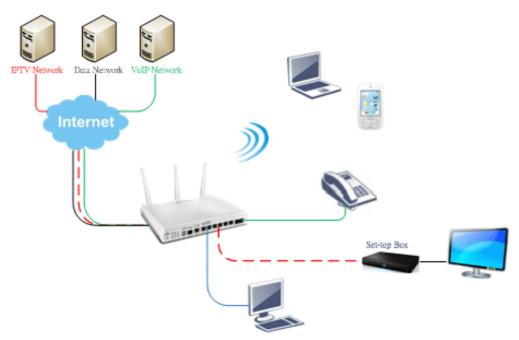
NAT mode with VLAN



Following settings, the set-top box (STB) is able to attach with any LAN port. Video streaming which your ISP provided will be played on your monitor.



#### Bridge mode with VLAN



	General			
Channel	Enable	WAN Type	VLAN Tag	Port-based Bridge
1	Yes	Ethernet(WAN1)	None	
2	Yes	Ethernet(WAN2)	None	
3.	No	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
<u>4.</u>	No	Ethernet(WAN1)	None	Enable P1 P2 P3 P4 P5
5.WAN5	No	mat		n n
6.WAN6	No	Multi-VLAN Channel	3: 🤨 Enable 🛛	🗇 Disable
LWAN7	No	WAN Type : Ethe	rnet(WAN1) 💌	
8.	No			
		VLAN Header VLAN Tag: 10 Priority: 4		
		-		een 1~4095 and unique for each channel. agged (equal to 0) at a time.
		Bridge mode		
		Enable Physical Members P1 P2 P3 Note:3 P1 is recentled		ind cannot be configured for bridge mode.

Set-top box (STB) or the other kinds of media devices are able to attach with Port4 or Port5 of LAN. Those devices that attached with Port4 or Port5 are able to access the services network directly which your ISP provided.



# **Appendix II: Release Note**

#### Firmware Version: 3.6.7

#### **New Features**

• None.

#### Improvement

- Improved: Support Huawei E303D, Vodafone K4201, SpinCom GPRS Modem.
- Improved: Support NS/ANY/SOA type for DNS cache.
- Improved: IPv6 firewall allows incoming packets transferred to certain ports.

If the firmware of the router is upgraded from 3.6.6(or before) to 3.6.7 firmware, .all and .rst will have different effects for the incoming packets.

1) .all --> keep routing settings in 3.6.6(or before), (both IPv4 and IPv6)

2) .rst --> block routing packets from WAN in default, (both IPv4 and IPv6)

- Improved: Add some TR-069 parameters for setting WAN >> WAN mode: Backup or Always On, LAN >> DHCP relay enable/disable, DHCP relay IP address and Device hostname, LAN >> Bind IP to MAC, VPN >> Create Phase2 SA for each subnet.(IPSec), VPN >> Netbios Naming Packets Pass/Block, Firewall >> IPv6 Group/IPv6 Object, SNMP, and Diagnostics >> Ping Diagnosis.
- Improved: Support to block Tor tunnel ver. 0.2.3.25, hotspot shield with ver.3.19, telnet protocol by using "putty" or "pietty", and LINE app in 3.5.1.36 (for PC) version and in 4.1.1 version (for mobile) for APP Enforcement.
- Improved: Support block page for DNS filter.
- Improved: Add SSL VPN setting in VPN Server Wizard.
- Improved: Add Wizards menu.
- Improved: Route policy supports VPN LAN to LAN traffics.
- Improved: Add an option to force the user clicking on a button to proceed the operation under the option URL Redirect on LAN>>Web Portal Setup.
- Improved: Add VALN tag for WAN IPv6 packets if WAN VLAN tag is enabled.
- Corrected: Some DHCP relay issues
- Corrected: Some SSH memory leakage issues.
- Corrected: Load Balance/Route Policy didn't work with WAN5 in PPP mode.
- Corrected: Load Balance/Route Policy cleaned all sessions when the dropped down WAN reconnected.
- Corrected: DDNS could not work when updating to freedns.afraid.org
- Corrected: Could not add DHPC option 66/15.
- Corrected: Router showed wrong Syslog messages when a VPN LAN to LAN tunnel dropped.



- Corrected: Router dropped all DNS packets with unknown type.
- Corrected: Daylight Saving didn't work with time zone Brasilia (GMT -03:00).
- Corrected: SSH didn't work with Macintosh, while it can work on Windows and Linux.
- Corrected: VigorACS SI couldn't show Network information when DNS Filter was enabled for Vigor2830.
- Corrected: Some error on External Device Status page.
- Corrected: Remove Mhaha, getMessenger, IMUnitive, Wablet from WebIM on CSM>>APP Enforcement Profile.