

# Vigor2850 Series

**VDSL2** Security Firewall



Your reliable networking solutions partner

# User's Guide

# Vigor2850 Series VDSL2 Security Firewall User's Guide

Version: 1.0 Firmware Version: V3.3.6\_RC6 Date: 08/06/2011



# **Copyright Information**

Copyright Declarations	Copyright 2011 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	<ul> <li>The following trademarks are used in this document:</li> <li>Microsoft is a registered trademark of Microsoft Corp.</li> <li>Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.</li> <li>Apple and Mac OS are registered trademarks of Apple Inc.</li> <li>Other products may be trademarks or registered trademarks of their respective manufacturers.</li> </ul>

# Safety Instructions and Approval

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



### **European Community Declarations**

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, Hukou Township, Hsinchu Industrial Park, Hsinchu County, Taiwan 303Product:Vigor2850 Series Router

DrayTek Corp. declares that Vigor2850 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.

#### **Regulatory Information**

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

Please visit http://www.DrayTek.com/user/AboutRegulatory.php



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.

# Table of Contents



Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor2850 1.2.2 For Vigor2850n 1.2.3 For Vigor2850Vn	4
1.3 Hardware Installation	
1.4 Printer Installation	9



Configuring Basic Settings	15
2.1 Two-Level Management	
2.2 Accessing Web Page	15
2.3 Changing Password	16
2.4 Quick Start Wizard	18
2.4.1 For WAN1 2.4.2 For WAN2 2.4.3 For WAN3	19 23 28
2.5 Service Activation Wizard	29
2.6 Online Status	32
2.6.1 Physical Connection 2.6.2 Virtual WAN	32 33
2.7 Saving Configuration	33
2.8 Registering Vigor Router	34



User Mode Operation	39
3.1 WAN	39
<ul> <li>3.1.1 Basics of Internet Protocol (IP) Network</li></ul>	41 47
3.2 LAN	62
3.2.1 Basics of LAN 3.2.2 General Setup	62 62
3.3 NAT	65
<ul><li>3.3.1 Port Redirection</li><li>3.3.2 DMZ Host</li><li>3.3.3 Open Ports</li></ul>	69



3.4 Applications	. 73
3.4.1 Dynamic DNS 3.4.2 UPnP	. 73 . 75
3.5 Wireless LAN	. 77
<ul> <li>3.5.1 Basic Concepts</li></ul>	. 78 . 81 . 83
3.6 System Maintenance	. 85
3.6.1 System Status.         3.6.2 User Password         3.6.3 Time and Date         3.6.4 Reboot System	. 86 . 87
3.7 Diagnostics	. 88
<ul> <li>3.7.1 DHCP Table</li> <li>3.7.2 Ping Diagnosis</li> <li>3.7.3 Traffic Graph</li> <li>3.7.4 Trace Route</li> </ul>	. 89 . 90



Admin Mode Operation	93
4.1 WAN	93
4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 General Setup 4.1.3 Internet Access	95
4.1.4 Multi-PVCs 4.1.5 Multi-VLAN 4.1.6 Load-Balance Policy	114 119
4.2 LAN	124
<ul> <li>4.2.1 Basics of LAN</li> <li>4.2.2 General Setup</li> <li>4.2.3 Static Route</li> <li>4.2.4 VLAN</li> <li>4.2.5 Bind IP to MAC</li> </ul>	126 131 134
4.3 NAT	138
<ul><li>4.3.1 Port Redirection</li><li>4.3.2 DMZ Host</li><li>4.3.3 Open Ports</li><li>4.3.4 Address Mapping</li></ul>	141 144
4.4 Firewall	147
4.4.1 Basics for Firewall 4.4.2 General Setup 4.4.3 Filter Setup 4.4.4 DoS Defense	149 153
4.5 User Management	164
4.5.1 General Setup 4.5.2 User Profile 4.5.3 User Group	165 166





4.5.4 User Online Status	. 170
4.6 Objects Settings	. 171
4.6.1 IP Object	
4.6.2 IP Group	
4.6.3 Service Type Object	
4.6.4 Service Type Group	
4.6.5 Keyword Object	
4.6.6 Keyword Group	
4.6.7 File Extension Object	. 179
4.7 CSM Profile	. 181
4.7.1 APP Enforcement Profile	
4.7.2 URL Content Filter Profile	
4.7.3 Web Content Filter Profile	. 189
4.8 Bandwidth Management	. 192
4.8.1 Sessions Limit	192
4.8.2 Bandwidth Limit	
4.8.3 Quality of Service	
4.9 Applications	
4.9.1 Dynamic DNS	
4.9.2 Schedule	
4.9.3 RADIUS	
4.9.4 UPnP	
4.9.5 IGMP	
4.9.6 Wake on LAN	
4.10 VPN and Remote Access	
4.10.1 VPN Client Wizard	
4.10.2 VPN Server Wizard	
4.10.3 Remote Access Control	
4.10.4 PPP General Setup	
4.10.5 IPSec General Setup	
4.10.6 IPSec Peer Identity	
4.10.7 Remote Dial-in User	
4.10.8 LAN to LAN	
4.10.9 Connection Management	
4.11 Certificate Management	. 238
4.11.1 Local Certificate	. 238
4.11.2 Trusted CA Certificate	. 240
4.11.3 Certificate Backup	. 241
4.12 VoIP	. 241
4.12.1 DialPlan	. 243
4.12.2 SIP Accounts	
4.12.3 Phone Settings	. 255
4.12.4 Status	. 260
4.13 Wireless LAN	. 261
4.13.1 Basic Concepts	. 261
4.13.2 General Setup	
4.13.3 Security	
4.13.4 Access Control.	
4.13.5 WPS	
4.13.6 WDS	
4.13.7 Advanced Setting	
4.13.8 WMM Configuration	. 276



4.13.9 AP Discovery 4.13.10 Station List	
4.14 USB Application	279
4.14.1 USB General Settings 4.14.2 USB User Management	
4.14.3 File Explorer	283
4.14.4 USB Disk Status	
4.14.5 Syslog Explorer	
4.15 System Maintenance	285
4.15.1 System Status	286
4.15.2 TR-069	
4.15.3 Administrator Password	
4.15.4 User Password	
4.15.5 Configuration Backup	
4.15.6 Syslog/Mail Alert	
4.15.7 Time and Date	
4.15.8 Management	
4.15.9 Reboot System 4.15.10 Firmware Upgrade	
4.15.10 Firmware Opgrade	
4.16 Diagnostics	300
4.16.1 Dial-out Triggering	300
4.16.2 Routing Table	301
4.16.3 ARP Cache Table	
4.16.4 DHCP Table	
4.16.5 NAT Sessions Table	
4.16.6 Ping Diagnosis	
4.16.7 Data Flow Monitor	
4.16.8 Traffic Graph	
4.16.9 Trace Route	
4.16.10 Web Firewall Syslog	308



Application and Examples	311
5.1 How can I get the files from USB storage device connecting to Vigor router?	311
5.2 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	314
5.3 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	322
5.4 QoS Setting Example	326
5.5 Upgrade Firmware for Your Router	331
5.6 Request a certificate from a CA server on Windows CA Server	334
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server	338
5.8 Creating an Account for MyVigor	340
5.8.1 Creating an Account via Vigor Router 5.8.2 Creating an Account via MyVigor Web Site	
5.5.2 Creating an Account via My vigor web Site	544



rouble Shooting .	
-------------------	--

6.1 Checking If the Hardware Status Is OK or Not	349
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	350
6.3 Pinging the Router from Your Computer	352
6.4 Checking If the ISP Settings are OK or Not	353
6.5 Problems for 3G Network Connection	353
6.6 Backing to Factory Default Setting If Necessary	354
6.7 Contacting Your Dealer	355



Vigor2850 series is a VDSL2 router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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

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

In addition, Vigor2850 series supports USB interface for connecting USB printer to share printing function or 3G USB modem for network connection.

Vigor2850 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

## **1.1 Web Configuration Buttons Explanation**

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

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

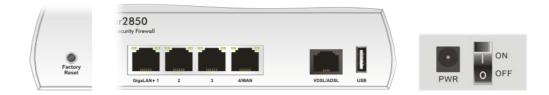
# **1.2 LED Indicators and Connectors**

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

## 1.2.1 For Vigor2850



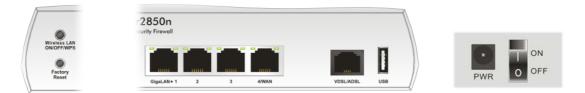
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
WAN2		On	Internet connection is ready.
		Off	Internet connection is not ready.
		Blinking	The data is transmitting.
WCF		On	The Web Content Filter is active. (It is enabled
			from Firewall >> General Setup).
ADSL		On	The router is ready to access Internet through ADSL link.
		Blinking	Slowly: The ADSL connection is ready. Quickly: The connection is training.
VDSL		On	The router is ready to access Internet through VDSL link.
		Blinking	Slowly: The VDSL connection is ready. Quickly: The connection is training.
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 Connec	tor		
	Left LED	On	The port is connected.
GigaLAN 1/2/3	(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.
GigaLAN	Left LED	On	The port is connected.
	(Green)	Off	The port is disconnected.
4/WAN (Giga)		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps.



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

# 1.2.2 For Vigor2850n

	Drey	Vigor28 VDSL2 Security	50n Firewall	
Wireless LAN ONIOFF/WPS ACT WLAN DOS USB ADSL VPN Factory Reset WAN2 VDSL QOS		G	IggLAN + 1 2 3 4/WAN VDSL/ADSL USB	
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.	
WAN2		On	Internet connection is ready.	
		Off	Internet connection is not ready.	
		Blinking	The data is transmitting.	
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.)	
ADSL		On	The router is ready to access Internet through ADSL link.	
		Blinking	Slowly: The ADSL connection is ready. Quickly: The connection is training.	
VDSL		On	The router is ready to access Internet through VDSL link.	
		Blinking	Slowly: The VDSL connection is ready. Quickly: The connection is training.	
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	r			
	Left LED	On	The port is connected.	
GigaLAN 1/2/3	(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.	
	Left LED	On	The port is connected.	
GigaLAN 4/WAN	(Green)	Off	The port is disconnected.	
(Giga)		Blinking	The data is transmitting.	
	Right LED	On	The port is connected with 1000Mbps.	
	(Green)	Off	The port is connected with 10/100Mbps.	



Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS.
01/011/015	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 (1-3)	Connecters for local network devices.
4/WAN	Connecter for local network devices or remote network devices.
VDSL/ADSL	Connecter for accessing the Internet.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

# 1.2.3 For Vigor2850Vn

	DrowTo	Vigor285 VDSL2 Security Fin	0Vn
Vireless LAN ONOFF/WPS ACT WLAN Line USB AD5L Phone1 Factory Reset WAN2 VDSL Phone2	-		
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
ACT (Activity)		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
000		Blinking	The data is transmitting.
WAN2		On	Internet connection is ready.
() / II ( <u>2</u>		Off	Internet connection is not ready.
		Blinking	The data is transmitting.
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.)
ADSL		On	The router is ready to access Internet through ADSL link.
		Blinking	Slowly: The ADSL connection is ready. Quickly: The connection is training.
VDSL		On	The router is ready to access Internet through VDSL link.
		Blinking	Slowly: The VDSL connection is ready. Quickly: The connection is training.
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	(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.
	Left LED	On	The port is connected.
GigaLAN 4/WAN	(Green)	Off	The port is disconnected.
(Giga)		Blinking	The data is transmitting.
	DI LI LED		

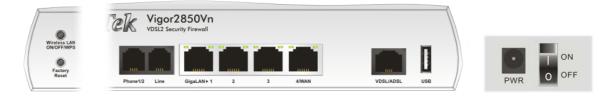


The port is connected with 1000Mbps.

The port is connected with 10/100Mbps.

On Off

Right LED (Green)

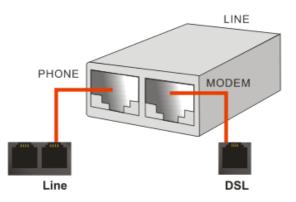


Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device
ON/OFF/WPS	making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on)
	or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default 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 (1-3)	Connecters for local network devices.
4/WAN	Connecter for local network devices or remote network devices.
VDSL/ADSL	Connecter for accessing the Internet.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

## **1.3 Hardware Installation**

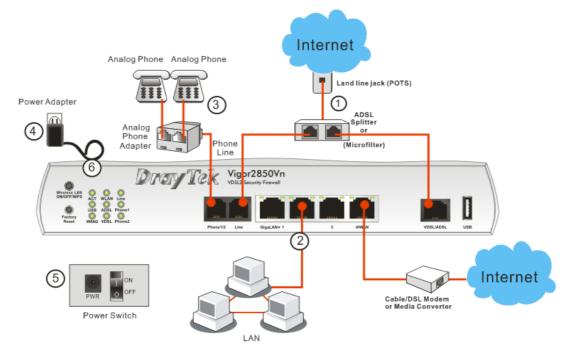
Before starting to configure the router, you have to connect your devices correctly.

1. Connect the XDSL interface to the external XDSL splitter with an XDSL line cable for all models. For Vigor2850Vn, also connect Line interface to external XDSL 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.

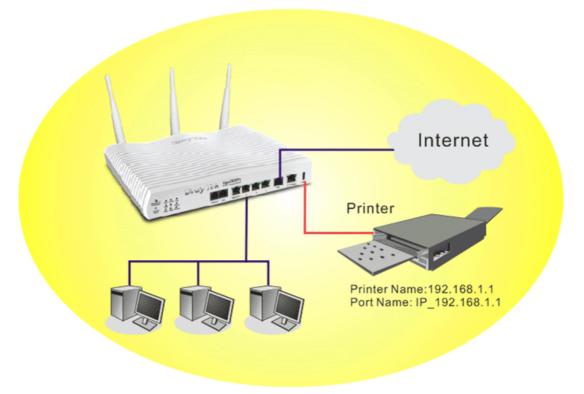
(For the hardware connection, we take "*Vn*" model as an example.)





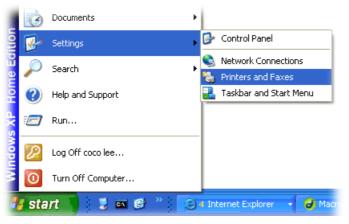
# **1.4 Printer Installation**

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



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

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



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



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

ld Pri	nter Wizard
	I or Network Printer he wizard needs to know which type of printer to set up.
S	elect the option that describes the printer you want to use:
6	DLocal printer attached to this computer
-	Automatically detect and install my Plug and Play printer
6	To set up a network printer that is not attached to a print server,
	Use the "Local printer" option.
	<back next=""> Cancel</back>

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

Select the port you want yo new port.	our printer to use. If the port is not listed, you o	an create a
OUse the following port:	LPT1: (Recommended Printer Port)	1
	use the LPT1: port to communicate with a loca port should look something like this:	al printer.
		al printer.

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

dd Port For which device do you want	to add a port?
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Port Name:	IP_192.168.1.1
	< <u>B</u> ack <u>N</u> ext> Cance

7. Click Standard and choose Generic Network Card.

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

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



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

dd Printer Wizard	
Install Printer Software The manufacturer and	model determine which printer software to use.
	turer and model of your printer. If your printer came with an installation ik. If your printer is not listed, consult your printer documentation for oftware.
Manufacturer AST	Printers
AT&T Brother	Brother HL-1070 BR-Script2
Buil Canon	Brother HL-1070
20	
This driver is digitally sign <u>Tell me why driver signin</u>	
	< <u>B</u> ack <u>N</u> ext > Cancel

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

eneral Sh	aring Ports	Auvanceu	Device Se	sangs	
В	rother HL-1070				
	ollowing port(s).	Document	ts will print to	the first free	
hecked po	at.				
Port	Description		Printer		12
3.250	Standard TC	P/IP Port	Epson Stylu	IS COLOR 1160	
□ IP_1	Standard TCI	P/IP Port			
□ IP_1	Standard TCI	P/IP Port	HP LaserJe	t 1300	
	Standard TCI				
□ IP_1	Standard TCI	P/IP Port			
✓ IP_1	Standard TCI	P/IP Port	Brother HL-	1070	1
PDF	Local Port		PDF995		
Add F	Port	Delete	Port	Configure Port	
Addi		Delete	TOR	<u>c</u> onligate i old	
Enable b	idirectional supp	toot			
Enable n	rinter pooling				

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

ort Name:	IP_192.168.1.1
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Protocol O <u>R</u> aw	(⊙ <u>L</u> PR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	p1
LPR Byte Counting En	abled
SNMP Status Enabled	1
Community Name:	public
SNMP Device Index:	1

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

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

About DrayTek	Products	Support	Partners	Contact Us
ome > Support > FAQ				
FAQ - Basic				FAQ
01. What are the differences among these firmware file form	ats ?			Basic
02. How could I get the telnet command for routers ?				Advanced
03. How can I backup/restore my configuration settings ?				VPN
04. How do I reset/clear the router's password ?				DHCP
05. How to bring back my router to its default value ?				Wireless
06. How do I tell the type of my Vigor Router is AnnexA or A	AnnexB? ( For A	DSL model (	only)	VoIP
07. Ways for firmware upgrade.				QoS
08. Why is SNMP removed in firmware 2.3.6 and above for $arsigma$	igor2200 Serie:	s routers?		ISDN
09. I failed to upgrade Vigor Router's firmware from my Mac I do?	machine const	antly, what s	hould 🕻	Eirewall / IP Filter Printer Server
10. How to upgrade firmware of Vigor Router remotely ?				USB ISDN TA
\Q - Printer Server				
	ws2000/XP	?		
Q - Printer Server . How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo		?		
. How do I configure LPR printing on Windo	ws98/Me ?	?		
. How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo	ws98/Me ? boxes ?		ocument	s through Vigor210
. How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo 3. How do I configure LPR printing on Linux 4. Why there are some strange print-out whe	ws98/Me ? boxes ? en Itry to p	rint my d	ocument	s through Vigor210
. How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo 3. How do I configure LPR printing on Linux 4. Why there are some strange print-out whe 9 / 2300's print server?	ws98/Me? boxes? en Itry to p h Vigor rout	rint my di		s through Vigor210
. How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo 3. How do I configure LPR printing on Linux 4. Why there are some strange print-out whe 9 / 2300's print server? 5. What types of printers are compatible with	ws98/Me? boxes? en Itry to p h <mark>Vigor rout</mark> er Port of V	rint my di		s through Vigor210
. How do I configure LPR printing on Windo 2. How do I configure LPR printing on Windo 3. How do I configure LPR printing on Linux 4. Why there are some strange print-out whe 9 / 2300's print server? 5. What types of printers are compatible with 5. What are the limitations in the USB Printe	ws98/Me? boxes? en Itry top h <mark>Vigor rout</mark> er Port of V outer?	rint my di		s through Vigor210

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

This page is left blank.

#### Vigor2850 Series User's Guide

# **2** Configuring Basic Settings

For using the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

# 2.1 Two-Level Management

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

For user mode operation, do not type any word on the window and click Login for the simple web pages for configuration.

Yet, for admin mode operation, please type "admin/admin" on Username/Password and click Login for full configuration.

# 2.2 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. For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.



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

4. 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.



_	
Off	~
Auto Logout	ard
Off	
1 min	
3 min	
5 min	
10 min	_
Applications	

#### 2.3 Changing Password

No matter user mode operation or admin mode operation, 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" on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.
- 3. Now, the **Main Screen** will appear.

Vigor2850 VDSL2 Security Fir	Series ewall				Dro	<b>y</b> Te
Auto Logout 💌	System Status					
uick Start Wizard Service Activation Wizard Inline Status	Model Name Firmware Version Build Date/Time	: Vigor2850Vn : 3.3.6_RC6 : Jun 1 2011 18:00:07				
/AN			LAN			
AN		MAC Address		Subnet Mask	DHCP Server	DNS
AT	LAN1	00-1D-AA-00-00-00			Yes	8.8.8.8
rewall	LAN2	00-1D-AA-00-00-00			Yes	8.8.8.8
er Management 👘 💼	LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
bjects Setting	LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
SM .	IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8
indwidth Management						
plications 'N and Remote Access			Wireless LAN			
rtificate Management	MAC Address	Frequency	Domain	Firmware Version	n SSID	
IP	00-1D-AA-00-0	0-00 Europe		"2.2.0.7"	DrayT	ek
reless LAN						
B Application			WAN			
stem Maintenance	Link Status	MAC Address	Connectio	n IP Address	Default Ga	teway
agnostics	WAN1 Disconnecte					
	WAN2 Connected	00-1D-AA-00-00-02		172.16.3.102		
	WAN3 Disconnecte	d 00-1D-AA-00-00-03				
inport Area						
			VoIP			
	Port	Profile	Reg.		Out	
and the second	Phone1		No	0/0	)	

Main screen for admin mode operation (full configuration)

Auto Logout 💌	System Status					
Quick Start Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor2850Vn : 3.3.6_RC6 : Jun 1 2011 18:00:07				
WAN			LAN			
NAT		MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
Applications	LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	Yes	8.8.8.8
Vireless LAN	LAN2	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	Yes	8.8.8.8
ystem Maintenance	LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
agnostics	LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
	IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8
			Wireless LAN			
	MAC Address	Frequency	Domain	Firmware Versio	n SSID	
	00-1D-AA-00-0	0-00 Europe		"2.2.0.7"	DrayT	ek
			WAN			
	Link Status	MAC Address	Connectio	n IP Address	Default Ga	teway
	WAN1 Disconnecte		PPPoE			
Logout	WAN2 Connected	00-1D-AA-00-00-02		172.16.3.102		
All Rights Reserved.	WAN3 Disconnecter	d 00-1D-AA-00-00-03				
			VoIP			
	Port	Profile	Reg	. In,	/Out	
	Phone1		No	0/	0	

Main screen for user mode operation (simple configuration)

System Maintenance >> Administrator Password Setup

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

4. Go to System Maintenance page and choose Administrator Password/User Password.

	Old Password	
	New Password	
	Confirm Password	
		OK
		or
ystem Maintenan	ce >> User Password	or
System Maintenan Jser Password	ce >> User Password	or
	ce >> User Password	<i>or</i>
		<i>or</i>

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

6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

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

# 2.4 Quick Start Wizard

**Notice:** Quick Start Wizard for user mode operation is the same as for admin mode operation.

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

Quick Start Wizard

Enter login password		
Please enter an alpha-nume	eric string as your Password (	(Max 23 characters).
Old Password	••••	
New Password	••••	
Confirm Password	••••	
	< Back	Next > Finish Cancel

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

WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL / VDSL
Fallback Mode:	Auto 🔽
Physical Type:	Auto negotiation 👻

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

#### 2.4.1 For WAN1

Quick Start Wizard

WAN1 is specified for ADSL or VDSL connection. If you do not specify **Fallback Mode** first, the router will detect whether the network is built by ADSL or VDSL automatically.

Quick Start Wizard	
WAN Interface	
WAN Interface: Display Name: Physical Mode: Fallback Mode: Physical Type:	WAN1 VDSL ADSL / VDSL Auto VDSL only ADSL only
	< Back Next > Finish Cancel

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

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

#### 2.4.1.1 PPPoE

**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.

If you click PPPoE or PPPoA as the protocol, please manually enter the Username/Password provided by your ISP. Then click **Next**.

#### Quick Start Wizard

Set PPPoE / PPPoA	
WAN 1	
User Name	84005755@hinet.net
Password	•••••
Confirm Password	•••••
	< Back Next > Finish Cancel
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.

Retype the password.

**Confirm Password** 

Click **Next** for viewing summary of such connection.

Quick Start Wizard

WAN Interface: Physical Mode: Fallback Mode: VPI: VCI: Protocol / Encapsulation: Fixed IP: Primary DNS: Secondary DNS:	WAN1 ADSL / VDSL AUTO 0 33 PPPoE / LLC No

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

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

Now, you can enjoy surfing on the Internet.



#### 2.4.1.2 MPoA / Static or Dynamic IP

If you choose MPoA / Static or Dynamic IP as the protocol, please type in the IP address/mask/gateway information originally provided by your ISP. Then click **Next** for next step.

WAN 1	
Protocol	MPoA / Static or Dynamic IP 💌
For ADSL Only:	
Encapsulation	1483 Bridged IP LLC
VPI	0 Auto detect
νсі	33
Fixed IP	⊙Yes ○No(Dynamic IP)
IP Address	172.16.3.102
Subnet Mask	255.255.255.0
Default Gateway	172.16.1.1
Primary DNS	168.95.1.1
Second DNS	

Click **Next** for viewing summary of such connection.

Quick Start Wizard

Quick Start Wizard

WAN Interface:	WAN1
Physical Mode:	ADSL
Fallback Mode:	ADSL only
VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS:	
Secondary DNS:	

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

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

Now, you can enjoy surfing on the Internet.

#### 2.4.2 For WAN2

Quick Start Wizard

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

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

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

Quick Start Wizard

Conne	ect to Internet
	WAN 2
	Select one of the following Internet Access types provided by your ISP.
	PPPoE
	🔘 РРТР
	O L2TP
	🔘 Static IP
	O DHCP
	Sack Next > Finish Cancel

#### 2.4.2.1 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.



If you click PPPoE as the protocol, please manually enter the Username/Password provided by your ISP. Then click **Next**.

Quick Start Wizard

PPPoE Client Mode	
WAN 2	
	e and password provided by your ISP.
User Name	84005657@hinet.net
Password	•••••
Confirm Password	•••••
	< Back Next > Finish Cancel
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.

Click **Next** for viewing summary of such connection.

Quick Start Wizard

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 /igor router.

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

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

Now, you can enjoy surfing on the Internet.

# 2.4.2.2 PPTP/L2TP

If you click PPTP/L2TP, you will get the following page. Please type in all the information originally provided by your ISP.

FP Client Mode		
WAN 2		
Enter the user name, pass <sup>,</sup> your ISP.	vord, WAN IP configuration and L21	TP server IP provided by
User 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		

Click Next for viewing summary of such connection.

Quick Start Wizard

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

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

## Quick Start Wizard Setup OK !!!

Now, you can enjoy surfing on the Internet.

**Dray** Tek

# 2.4.2.3 Static IP

If you click Static IP, you will get the following page. Please type in the IP address information originally provided by your ISP. Then click **Next** for next step.

0	CALLA	10/2
UNICK	Start	Wizard

WAN 2		
Enter the Static IP config	guration provided by your ISP	·
WAN IP	172.16.3.102	
Subnet Mask	255.255.0.0	
Gateway	172.16.1.1	
Primary DNS	168.95.1.1	
Secondary DNS		(optional)

Click **Next** for viewing summary of such connection.

Quick Start Wizard

e confirm your settings:	
WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
2	-

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

## Quick Start Wizard Setup OK !!!

Now, you can enjoy surfing on the Internet.

# 2.4.2.4 DHCP

If you click DHCP, you will get the following page. Simply click **Next** to continue.

Quick Start Wizard

Quick Start Wizard

WAN 2	
enter 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)

Click Next for viewing summary of such connection.

WAN Interface:	WAN2
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
Click <b>Back</b> to modify char settings and restart the V	nges if necessary. Otherwise, click Finish to save the current ligor router.

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

# Quick Start Wizard Setup OK !!!

Now, you can enjoy surfing on the Internet.



# 2.4.3 For WAN3

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

Ouick	Ctart	Wizard
QUICK	Start	vvizaru

WAN Interface: Display Name: Physical Mode: Physical Type:	WAN3 V USB
	< Back Next > Finish Cancel
n, click <b>Next</b> to continue.	
ck Start Wizard ase confirm your settings:	
	WAN3 USB PPP

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 !!!

< Back

Next >

Finish

Cancel

Now, you can enjoy surfing on the Internet.

# 2.5 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 configurator.

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.	riicense 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**.

his product provides 30 days of free trial, p	lease choose the item(s) you want to use.
VCF service:	
Web Content Filter (Commtouch)	License Agreement
	on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can SlobalView WCF package from retailing outlets. Activation Date : 2010-10-27

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

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

confirm your settings	
Sevice Type :	Trial version
Sevice Activated :	Web Content Filter ( Commtouch )
Please click Back to re-s	elect service type you to activate.

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

nection Succeed	led!					
Please check	the followin	ng item(s) to	enable service	es on your rou	ter.	
		Enable V	Web Content F	ilter		

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



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

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

	DrayTek Service	Activation	
Service Name	Start Date	Expire Date	Status
Web Content filter	2010-10-27	2010-11-27	Commtouch
Please check if the licen	se fits with the servic	e provider of your s	signature. To ensur
normal 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**.

This wizard is used for activating - Web Content Filter Please choose the edition you nee	ed.					
	ee trial edition		_			
I FO	ormal edition wit	th license key				
		Nex	t > Fini	sn Ca	ancel	
ice Activation Wizard						
ect the service type that you want to activat	e					
Please choose the item you want to use.						
WCF service:						
<ul> <li>Web Content Filter (Commtouch) Commtouch is the web content filter based purchase DrayTek's prepared Commtouch (</li> </ul>	on Commtouch over SlobalView WCF pac		There is a 30-day tlets.	y trial period. Af	ter trial, you	can
Enter your License key:			Activation Da	te : 2010-11-02	select	

# 2.6 Online Status

Online Status
Physical Connection
Virtual WAN
VII LUAI VVAIN

# 2.6.1 Physical Connection

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

If you select **PPPoE** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

**Online Status** 

LAN Status	Prima	nry DNS: 8.8.8.8	3	Secondary D	<b>IS:</b> 8.8.4.4
IP Address	TX Packets	RX Pac	kets	-	
192.168.1.1	339991	920878	6		
WAN 1 Status					>> <u>Dial PPP</u>
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	69:04:03	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172.16.3.102	172.16.1.1	254391	1926	1525247	1487
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	-
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
ADSL Information	( ADSL Firmware	Version: 2111	302_B)		
ATM Statistics	TX Cells	RX Cells	TX CRC errs	RX C	CRC errs
	0	0	0	0	
ADSL Status Mo	ode State	Up Speed	Down Speed	SNR Margin	Loop Att.
	READY	0	· ·	0	0

Detailed explanation is shown below:

splays the IP address of the primary DNS.
splays the IP address of the secondary DNS.
splays the IP address of the LAN interface.
splays the total transmitted packets at the LAN interface.
splays the total number of received packets at the LAN interface.
splays the physical connection (Ethernet) of this interface.
splays the name set in WAN1/WAN web page.
splays the type of WAN connection (e.g., PPPoE).

Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
<b>RX</b> Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.

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

# 2.6.2 Virtual WAN

Such page displays the virtual WAN connection information.

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

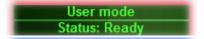
The field of Application will list the purpose of such WAN connection.

### **Online Status**

Virtual WAN				System 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	

# 2.7 Saving Configuration

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



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

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

# 2.8 Registering Vigor Router

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

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

Copyright@, DrayTek Corp. Al	ll Rights Reserved.	<b>Dray</b> Tek
		Login
Password	•••••	
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**.

532			stration entitles you to upgrade firmware d product and receive news about
LO	GIN		
	UserName :	james_fae	]
	Password :	•••••	]
	Auth Code :	txxhdd	t <b>x x h d</b> d
		If you cannot read the word,	d, click here
		Forgotten password?	p Login
-	Don't have a N	yVigor 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> Tek	My	Login
🔒 Home	Search	You
	My Information	
About Us Product My Information VigorACS SI VigorPro	Welcome,james_fae Last Login Time : 2011-03-16 01:45:09 Last Login From : 172.16.2.180 Current Login Time : 2011-03-16 18:20:31 Current Login From : 172.16.3.148 RowNo : 5 V PageNo : V Add	Registe
Product Registration Customer Survey	Your Device List Serial Number / Device Name Model Note Host ID	

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

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

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

Your device has been successfully added to the database.



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

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

Home			Sea	arch GO
	My Information			
About Us Product My Information VigorACS SI VigorPro Customer Survey	Welcome.james_fae Last Login Time : 2011-03-16 0 Last Login From : 172.16.2.180 Current Login Time : 2011-03-1 Current Login From : 172.16.3. Your Device List	6 18:20:31	RowNo : 5 💌 P:	ageNo : 1 💌
customer survey				
	Serial Number / Host ID	Device Name	Model	Note
	<u>2011031609200201</u>	vigor 2850	∨igor2850	-

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

	My Product
About Us Product	Device Information
My Information VigorACS SI VigorPro	Nickname : vigor2850 Serial : 2011031609200201 Model : Vigor2850 Series Rename Transfer Back
Customer Survey	Rename Hansler Dack
	Device's Service Expired License
	Service Provider Action Status Start Date Expired Date
	WCF Commtouch Trial On
	The Commtouch GlobalView Web Filter is provided for Vigor router with only 1-month trial. After trial period, please purchase the official package from your local DrayTek dealer/distributor. BPIM is the web content filter based on service operated in Germany. We recommend only users live in Germany to

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

1	Confirm Messag	e		
About Us				Cancel
Product				
My Information	User Name :	james_fae		
VigorACS SI	Serial :	201103160920020	1	
VigorPro	Model:	Vigor2850		
Customer Survey	Licens	se Number	Service Provider	Status
	PLEASE READ CAREFULLY BI BY DOWNLOAD AGREEING TO NOT AGREE TO	EFORE DOWNLOADING ING, INSTALLING O BE BOUND BY THE O THE TERMS OF TI OR USE THIS SOF	ICENSE AGREEMENT (?LICENSE?) 3 OR OTHERWISE USING THE SOF DR USING THE SOFTWARE, YOU A TERMS OF THIS LICENSE. IF Y HIS LICENSE, YOU ARE NOT AUT IWARE.	RE OU DO HORIZED

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

i Home		Search	60
About Us	Apply For A License Number		
Product			Cancel
My Information VigorACS SI VigorPro Customer Survey	Service Name: WCF STEP 2 Activation Date (MM-DD-YYYY): 03-16-2011	gister	

12 Wait for a moment until the following page appears.

## **DrayTek Service Activation**

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

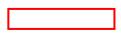
Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

Close

13 Click Close.

This page is left blank.



# **Dray** Tek

# **3** User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation. As for other examples of application, please refer to chapter 5.

- 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. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that "User mode" will be displayed on the bottom left side.

Vigor2850 VDSL2 Security	O Series Firewall				Dra	<b>y</b> Te
Auto Logout 💌	System Status					
Quick Start Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor2850Vn : 3.3.6_RC6 : Jun 1 2011 18:00:07				
VAN			LAN			
IAT		MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
pplications	LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	Yes	8.8.8.8
ireless LAN	LAN2	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	Yes	8.8.8.8
stem Maintenance	LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
agnostics	LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
	IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8
			Nireless LAN			
	MAC Address	Frequency	Domain	Firmware Version	n SSID	
	00-1D-AA-00-0	00-00 Europe		"2.2.0.7"	DrayT	ek
			WAN			
	Link Status	MAC Address	Connectio	n IP Address	Default Ga	teway
	WAN1 Disconnecte		PPPoE			
Logout	WAN2 Connected	00-1D-AA-00-00-02		172.16.3.102		
All Rights Reserved.	WAN3 Disconnecte	d 00-1D-AA-00-00-03				
			VoIP			
	Port	Profile	Reg	. In/	/Out	
	Phone1		No	0/1	0	

# 3.1 WAN

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

# 3.1.1 Basics of Internet Protocol (IP) Network

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



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

# What are Public IP Address and Private IP Address

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

## Get Your Public IP Address from ISP

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

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

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

For 3G mobile communication through Access Point is popular more and more, Vigor2850 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2850, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2850n with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2850n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2850n series.



After connecting into the router, 3G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN3 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting



automatically. The supported 3G USB Modem will be listed on Draytek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.



# 3.1.2 General Setup

WAN<sub>2</sub>

WAN3

V.

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

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

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

WAN >> G	eneral Setup	)				
Load Bala	nce Mode:	Auto Weight	*			
Setup						
Index	Enable	Physical Mode/Type		Line Speed(Kbps) DownLink/UpLink	Active Mode	Backup WAN
WAN1	V	ADSL/-		0/0	Always On	_

Ethernet/Auto negotiation

USB/-

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

0/0

Always On

Always On

Load Balance Mode	This option is available for multiple-WAN for getting end bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the sett <b>According to Line Speed</b> . Otherwise, please choose <b>Aut</b> <b>Weight</b> to let the router reach the best load balance.			
	Load Balance Mode:	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.			
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.			

**Dray** Tek

Line Speed	Display the downstream and upstream rate of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Backup WAN	Display the Backup WAN interface for such WAN when it is disabled.
Note: In default, eac	ch WAN port is enabled.

# WAN1 with ADSL/VDSL

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

#### WAN >> General Setup

Enable:	Yes 🗸
Display Name:	
Physical Mode:	VDSL
Fallback Mode:	Auto 💌
Physical Type:	Auto negotiation 👻
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion (ADSL):	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
VLAN Tag insertion (VDSL):	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On 💌
Backup WAN:	None 💌

Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
Display Name	Type the description for such interface.
Physical Mode	Display the physical mode of such interface. If VDSL is detected, this field will display " <b>VDSL</b> "; if ADSL is detected, it will display " <b>ADSL</b> ".
Fallback Mode	It allows you to specify which physical connection is used. Once the mode is specified, the router will not detect physical mode automatically whenever powering up the router.
Physical type	For such interface, no type can be selected.
Line Speed (Kpbs)	If your choose According to Line Speed as the Load Balance



	<b>Mode</b> in previous page, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.		
VLAN Tag insertion (ADSL)	The settings configured in this field are available for VDSL only.		
	<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.		
VLAN Tag insertion (VDSL)	The settings configured in this field are available for VDSL only.		
	<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>Υ</mark> Always On Backup		
Backup WAN	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 Type (Only for Backup Multiple WAN):		

When any WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be

# WAN2 with Ethernet

WAN2 is fixed with physical mode of Giga Ethernet.

WAN >> General Setup					
WAN 2					
Enable:	Yes 💌				
Display Name:					
Physical Mode:	Ethernet				
Physical Type:	Auto negotiation 💌				
Line Speed(Kbps): DownLink	0				
	0				
UpLink					
VLAN Tag insertion:	Disable 🚩				
Tag value:	0 (0~4095)				
Priority:	0 (0~7)				
Active Mode:	Always On 🔽	Always On 🔽			
Backup WAN:	None 💌				
	ОК С	ancel			
Enable		e the settings for this WAN interface. 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 p negotiation for deter	hysical type for WAN2 or choose <b>Auto</b> mined 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 Balance</b> <b>Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.				
<b>LAN Tag insertion</b>	Enable – Enable the	function of VLAN with tag.			
	The router will add specific VLAN number to all packets on the WAN while sending them out.				
	Please type the tag va sending by WAN1.	lue and specify the priority for the packet			
	Disable – Disable the	e function of VLAN with tag.			
	<b>Tag value</b> – Type the range is form 0 to 409	e value as the VLAN ID number. The 95.			



**Priority** – Type the packet priority number for such VLAN. The range is from 0 to 7.

## Active Mode and Backup WAN/Backup Type

p Active Mode – Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface (Backup WAN).



**Backup WAN/Backup Type** – Determine the role of such WAN interface. It will be changed according to the **Active Mode** specified.

If you choose **Always On** as **Active Mode**, you can choose one of the backup WAN interfaces from the **Backup WAN** drop down list. Later, when such WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.

Active Mode:	Always On 🔽
Backup WAN:	None 💌

If you choose **Backup** as the **Active Mode**, Backup WAN will be changed into **Backup Type**. 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.



When any WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.

# WAN3 with USB

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

WAN	>>	General	Setu	p
		ocherai	2000	μ

Enable:	Yes 🕶			
Display Name:				
Physical Mode:	USB			
Physical Type:	Auto negotiation 👻			
Line Speed(Kbps):	0			
DownLink				
UpLink	0 Always On 🔽 None 👻			
Active Mode:				
Backup WAN:				
	OK Cancel			
Enable	<ul><li>Choose Yes to invoke the settings for this WAN interface.</li><li>Choose No to disable the settings for this WAN interface.</li><li>Type the description for such WAN interface.</li><li>Display the physical mode of such WAN interface.</li><li>In such WAN interface, no type can be selected.</li></ul>			
Display Name				
Physical Mode				
Physical type				
Line Speed	f your choose <b>According to Line Speed</b> as the <b>Load Balance</b> <b>Iode</b> , please type the line speed for downloading and ploading for such WAN interface. The unit is kbps.			
Active Mode and Backup WAN/Backup Type	Active Mode – Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface(Backup WAN).			
	Always On <mark>Υ</mark> Always On Backup			
	<b>Backup WAN/Backup Type</b> – Determine the role of such WAN interface. It will be changed according to the <b>Active</b>			

Mode specified. If you choose Always On as Active Mode, you can choose one of the backup WAN interfaces from the Backup WAN drop down list. Later, when such WAN is disconnected for some reason, the backup WAN will be activated automatically to

	L (0~ )
Active Mode:	Always On 🔽
Backup WAN:	None 🚩

prevent data transmission from connection interrupted.

If you choose **Backup** as the **Active Mode**, Backup WAN will be changed into **Backup Type**. 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 🖌 🖌
Backup Type (Only for Backup Multiple WAN):	⊙ When any WAN disconnect ○ When all WAN disconnect

заскир	. ×			
列 When a	anv.	WAN.	disconn	ect

When any WAN disconnect - Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.

## 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 / VDSL	PPPoE / PPPoA 🛛 🔽 Details Page
WAN2	Ethernet	None Details Page
WAN3	USB	MPoA / Static or Dynamic IP

#### WAN >> Internet Access

Index Display Name	Physical Mode	Access Mode	
WAN1	ADSL / VDSL	PPPoE / PPPoA	Details Page
WAN2	Ethernet	Static or Dynamic IP	Details Page
WAN3	USB	None PPPoE	Details Page
		Static or Dynamic IP PPTP/L2TP	

#### WAN >> Internet Access

PPPoE / PPPo/	A 🔽	Details Page
Static or Dynam	nic IP 💌	Details Page
None	~	Details Page
		None 👻



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/VDSL) /WAN2 (Ethernet) /WAN3 (3G USB Modem) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page according to the access mode that you choose in WAN interface

## **Details Page for PPPoE/PPPoA in WAN1**

PPPoA, included in RFC1483, can be operated in either Logical Link Control-Subnetwork Access Protocol or VC-Mux mode. As a CPE device, Vigor router encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Multiplexer (DSLAM).

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

WAN >> Internet Access

💿 Enable 🔘 Disable	ISP Access Setup
Modem Settings (for ADSL only)         Multi-PVC channel       Channel 1         VPI       0         VCI       33         Encapsulating Type       LLC/SNAP          Protocol       PPPoE          Modulation       Multimode	Username Password Separate Account for ADSL PPP Authentication PAP or CHAP Idle Timeout Idle Timeout IP Address From ISP WAN IP Alias Fixed IP Yes No (Dynamic IP) Fixed IP Address
PPPoE Pass-through  For Wired LAN  For Wireless LAN  WAN Connection Detection  Mode ARP Detect Ping IP TTL:	<ul> <li>Default MAC Address</li> <li>Specify a MAC Address</li> <li>MAC Address: 00 .1D .AA:00 .00 .01</li> </ul>

## Enable/Disable

Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.



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.
	VCI - 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 provided by ISP.If you have already used <b>Quick Start Wizard</b> to set the protocol, then it is not necessary for you to change any settings in this group.
	<b>Modulation</b> – Drop down the list to choose a proper modulation for the router.
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.
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>
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check <b>Always On</b> .
	<b>Username</b> – Type in the username provided by ISP in this field.
	<b>Password</b> – Type in the password provided by ISP in this field.
	<b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.
	<b>Idle Timeout</b> – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the <b>Active on demand</b> option for Active

Mode is selected in **WAN>> General Setup** page.

#### **IP Address From ISP**

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. 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.

ndex	Enable	Aux. WAN IP	Join NAT IP Pool
1.			<b>V</b>
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	

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

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

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

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

# Details Page for MPoA in WAN1

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, 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** mode. The following web page will appear.

WAN >> Internet Access				
WAN 1				
PPPoE / PPPoA		(FC1483/2684)		
🔘 Enable 💿 Disa	able	WAN IP Network Settings WAN IP Alias		
DSL Modem Settings		Obtain an IP address automatically		
Multi-PVC channel	Channel 2 🛛 💌	Router Name Vigor *		
Encapsulation		Domain Name *		
1483	Bridged IP LLC	* : Required for some ISPs     Specify an IP address		
VPI	0	IP Address		
VCI	88	Subnet Mask		
Modulation	Multimode 🛛 👻			
WAN Connection Detection	)n	Gateway IP Address		
Mode	ARP Detect 👻	O Default MAC Address		
Ping IP		O Specify a MAC Address		
TTL:		MAC Address: 00 .50 .7F 00 .00 .01		
RIP Protocol		DNS Server IP Address		
🔲 Enable RIP		Primary IP Address		
Bridge Mode  Enable Bridge Mode		Secondary IP Address		
	OK	Cancel		
Cnable/Disable	this functio	<b>ble</b> for activating this function. If you click <b>Disa</b> on will be closed and all the settings that you adjue will be invalid.		
OSL Modem Settin		DSL parameters required by your ISP. These are ailding DSL connection to your ISP.		
	determined	C <b>channel</b> - The selections displayed here are by the page of <b>Internet Access</b> – <b>Multi PVCs</b> . <b>PVCs Channel</b> means no selection will be chose		
	<b>Encapsula</b> provided by	<b>ting Type</b> - Drop down the list to choose the typy JSP.		
	<b>VPI</b> - Type	e in the value provided by ISP.		
	VCI - Type	e in the value provided by ISP.		
		<b>n</b> – Drop down the list to choose a proper n for the router.		
VAN Connection Detection		Such function allows you to verify whether network connect 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 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.
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	This group allows you to obtain an IP address automatically and allows you type in IP address manually.

**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

	Enable	Ilti-NAT ) Aux. WAN IP	Join NAT IP Pool
1.	<b>V</b>		$\checkmark$
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
		OK Clear All	Close

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically.

Router Name – Type in the router name provided by ISP.

**Domain Name** – Type in the domain name that you have assigned.

**Specify an IP address** – Click this radio button to specify some data.

**IP** Address – Type in the private IP address.

Subnet Mask – Type in the subnet mask.

Gateway IP Address - Type in gateway IP address.

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



address for	your	necessity.
-------------	------	------------

	MAC Address – Type in the MAC address for the router manually.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

# **Details Page for 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

<b>PPP</b> oE	Stat	ic or Dynamic IP	PPTP/L2TP	
🔘 Enab	le 💿 Disab	le	PPP/MP Setup	
			- PPP Authentication	PAP or CHAP 🔽
ISP Access S	etup		Idle Timeout	-1 second(s)
Username			IP Address Assignmer	nt Method (IPCP)
Password			WAN IP Alias	
			— Fixed IP: 🔘 Yes 🧿	) No (Dynamic IP)
WAN Connection Detection		Fixed IP Address		
Mode		ARP Detect 💌		
Ping IP			Oefault MAC Add	ress
TTL:			🔘 Specify a MAC A	ddress
			MAC Address: 00	1D AA 00 00 02

Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	<b>Username</b> – Type in the username provided by ISP in this field.
	<b>Password</b> – Type in the password provided by ISP in this field.
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.
PPP/MP Setup	<b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP. If you want to connect to Internet all the time, you can

**Dray** Tek

#### check Always On.

**Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address AssignmentUsually ISP dynamically assigns IP address to you each time<br/>you connect to it and request. In some case, your ISP provides<br/>service to always assign you the same IP address whenever you<br/>request. In this case, you can fill in this IP address in the Fixed<br/>IP field. Please contact your ISP before you want to use this<br/>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.

🗿 WAN II	🗿 WAN IP Alias - Microsoft Internet Explorer 📃 🗖 🔀				
WAN IP	WAN IP Alias (Multi-NAT)				
Index	Enable	Aux. WAN IP	Join NAT IP Pool		
1.	v	172.16.3.229	V		
2.					
з.					
4.					
5.					
6.					
7.					
8.					
		OK Clear All	Close		

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

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

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

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

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

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

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

WAN 2				
<b>PPP</b> oE	St	tatic or Dynamic IP	РРТР	
💿 Enable	🔘 Disable		WAN IP Network Setting	gs 🛛 WAN IP Alias
Keen MAN Com			🔘 Obtain an IP addres	ss automatically
Keep WAN Conn			Router Name	*
PING to the IP		·	Domain Name	*
PING Interval	0		* : Required for some	e ISPs
	0	minute(s)	Specify an IP addre	SS
WAN Connection	n Detection		IP Address	172.16.3.102
Mode	AR	P Detect 💌	Subnet Mask	255.255.0.0
Ping IP			Gateway IP Address	172.16.1.1
TTL:				
			Oefault MAC Addre	
RIP Protocol Enable RIP			Specify a MAC Add	
			MAC Address: 00 ·	50 .7F 00 .00 .02
			DNS Server IP Address	
			Primary IP Address	
			Secondary IP Address	
nable / Disab	le	this function will	be closed and all the	tion. If you click <b>Disable</b> e settings that you adjuste
		in this page will b	be invalid.	
Keep WAN Connection		because some ISI	Ps will drop connect riods of time. Check	or Dynamic IP environme ions if there is no traffic <b>Enable PING to keep a</b>
			•	ING function, please spective for the spectime of the second seco
		<b>PING Interval</b> - PING operation.	Enter the interval fo	or the system to execute the
VAN Connect Detection	tion		ows you to verify wl gh ARP Detect or Pi	hether network connectio
		Mode – Choose A execute for WAN		<b>Detect</b> for the system to

**Dray** Tek

**Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

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

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

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

🖹 WAN II	P Alias - Mi	crosoft Internet Explorer	
WAN IP	Alias ( Mu	ılti-NAT )	
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

Router Name: Type in the router name provided by ISP.

Domain Name: Type in the domain name that you have assigned.

**Specify an IP address** – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

*Default MAC Address* : Click this radio button to use default MAC address for the router.

*Specify a MAC Address*: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

**RIP** Protocol

Settings

WAN IP Network



**DNS Server IP Address** 

Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

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

# Details Page for PPTP/L2TP in WAN2

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

VAN >> Internet	Access		
WAN 2			
PPPoE	Static or Dynamic IP	PPTP/L2TP	
O Enable Pl	PTP 🔘 Enable L2TP 💿 Disable	PPP Setup	
Server Address		PPP Authentication	PAP or CHAP 💙
Specify Gatewa	y IP Address	Idle Timeout	180 second(s)
	172.16.1.1	IP Address Assignment N WAN IP Alias	lethod (IPCP)
SP Access Setu	p	Fixed IP: O Yes 💿 I	No (Dynamic IP)
Jsername		Fixed IP Address	
Password		WAN IP Network Setting	S
		Obtain an IP addres	s automatically
		Specify an IP addre	SS
		IP Address	172.16.3.102
		Subnet Mask	255.255.0.0
	ОК	Cancel	

PPTP/L2TP Client Mode	<b>Enable PPTP-</b> Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
	<b>Enable L2TP</b> - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.
	<b>Disable</b> – Click this radio button to close the connection through PPTP or L2TP.
	<b>Server Address</b> - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
	<b>Specify Gateway IP Address</b> – Specify the gateway IP address for DHCP server.
ISP Access Setup	<b>Username</b> -Type in the username provided by ISP in this field.
	<b>Password</b> -Type in the password provided by ISP in this field.
PPP Setup	<b>PPP Authentication</b> - Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP.
	<b>Idle Timeout</b> - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	<b>WAN IP Alias</b> - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other

**Dray** Tek

1.     v     172.16.3.229     v       2.     .     .     .       3.     .     .     .       4.     .     .     .       5.     .     .     .       6.     .     .     .       7.     .     .     .       8.     .     .     .		Enable	Aux. WAN IP	Join NAT IP Pool
3.	1.	V	172.16.3.229	V
4.	2.			
5.     .     .     .     .     .       6.     .     .     .     .     .       7.     .     .     .     .     .	з.			
6.	4.			
7.	5.			
	6.			
8.	7.			
	8.			

than the current one you are using.

**Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box.

Fixed IP Address - Type a fixed IP address.

WAN IP Network Settings

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically.

**Specify an IP address** – Click this radio button to specify some data.

**IP** Address – Type the IP address.

Subnet Mask – Type the subnet mask.

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

# **Details Page for 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.

WAN 3							
3G Modem	◯ 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						
WAN Connection Detect	ion						
Mode	ARP Detect 👻						
Ping IP							
TTL:							
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.						
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.						
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.						
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.						
Modem Initial String2	The initial string 1 is shared with APN.						
	In some cases, users may need another initial <i>AT</i> command to restrict 3G band or do any special settings.						
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.						
PPP Username	Type the PPP username (optional).						
PPP Password	Type the PPP password (optional).						
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.						

WAN >> Internet Access



**Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.

**Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

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

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

# 3.1.4 Load-Balance Policy

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

**Note:** Load-Balance Policy is running only when more than one WAN interface is activated.

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Port	Move Up	Move Down
1		any	~	WAN1 🔽								<u>Down</u>
<u>2</u>		any	~	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>3</u>		any	~	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>4</u>		any	~	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>5</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>6</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
Z		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>8</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>9</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>10</u>		any	~	WAN1 🔽							<u>UP</u>	Down

Index	Click the number of index to access into the load-balance policy configuration web page.
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to change the protocol for the WAN interface.
WAN	Use the drop-down menu to change the WAN interface.
Src IP Start	Displays the IP address for the start of the source IP
Src IP End	Displays the IP address for the end of the source IP.
Dest IP Start	Displays the IP address for the start of the destination IP.
Dest IP End	Displays the IP address for the end of the destination IP.

ΟK

WAN >> Load-Balance Policy



Dest Port Start	Displays the IP address for the start of the destination port.
Dest Port End	Displays the IP address for the end of the destination port.
Move UP/Move Down	Use <b>Up</b> or <b>Down</b> link to move the order of the policy.

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

Index: 1		
Enable Protocol Binding WAN Interf Src IP Start Src IP End Dest IP Start Dest IP End Dest Port Start Dest Port Start	ace	any V WAN1 V Auto failover to the other WAN
		OK Cancel
Enable	Check this	box to enable this policy.
Protocol	Use the drew WAN inter	op-down menu to choose a proper protocol for the rface.
	Protocol	any TCP UDP TCP/UDP ICMP IGMP
Binding WAN interface	Choose the binding.	e WAN interface (WAN1 / WAN2 / WAN3) for
	data passir	wer to other WAN – Check this button to lead the ng through other WAN automatically when the VAN interface is failover.
Src IP Start	Type the source IP start for the specified WAN interface.	
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.	
Dest IP Start	Type the d	lestination IP start for the specified WAN interface.
Dest IP End	this field is	lestination IP end for the specified WAN interface. If s blank, it means that all the destination IPs will be ough the WAN interface.
Dest Port Start	Type the d	lestination port start for the destination IP.
Dest Port End	Type the d	lestination port end for the destination IP. If this field

WAN >> Load-Balance Policy



is blank, it means that all the destination ports will be passed through the WAN interface.

# 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

#### 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.

#### 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**.

LAN >> General Setup

General Setup				
Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page

Index	Display all of the LAN items.
Status	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> .
DHCP	LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN.
IP Address	Display the IP address for each LAN item. Such information is set in default and you can not modify it.
Details Page	Click it to access into the setting page. Each LAN will have different LAN configuration page. <b>Each LAN must be configured in different subnet.</b>



# **Details Page for LAN**

Click Details Page to open the following page.

LAN >> General Setup

etwork Configuration		DHCP Server Configuratio	n
or NAT Usage		📀 Enable Server 🔘 Disal	ble Server
IP Address	192.168.1.1	Relay Agent: OEnable (	Disable
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
		IP Pool Counts	50
IP Protocol Control	Disable 💌	Gateway IP Address	192.168.1.1
		DHCP Server IP Address for Relay Agent	
		DNS Server IP Address	
		🔲 Force DNS manual se	tting
		Primary IP Address	
		Secondary IP Address	

OK	
OK	

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> deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	Disable V Disable Enable
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>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.

**Gateway IP Address -** Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

**DHCP Server IP Address for Relay Agent -** Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

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.

**Force DNS manual setting -** 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).

**Primary IP Address -**You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

**Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

The default DNS Server IP address can be found via Online Status:

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 assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

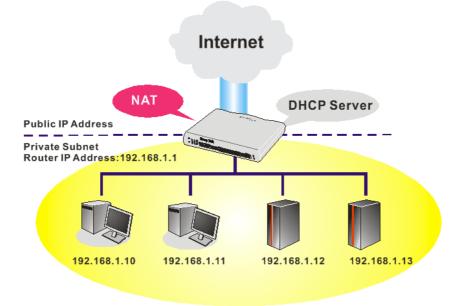
If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

**DNS Server Configuration** 

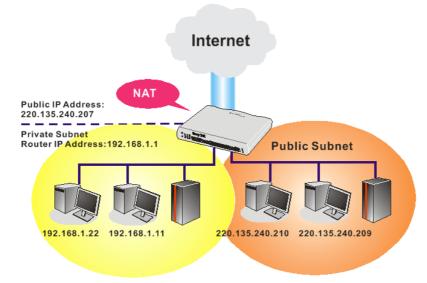


# 3.3 NAT

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.



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.

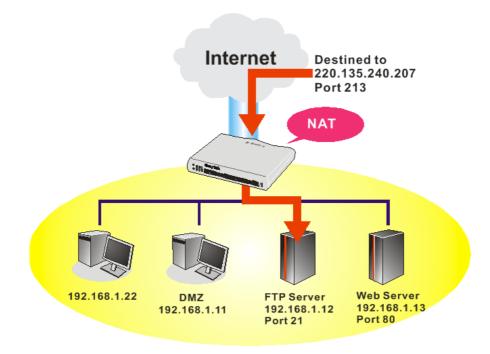
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



#### 3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

	Private IP	Status
		×
		x
		х
		х
		х
		×
		×
		×
		×
		×
>>>		

NAT >> Port Redirection

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

#### NAT >> Port Redirection

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

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

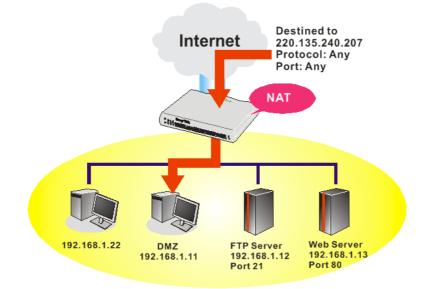
OK	Clear	Cancel

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</b> <b>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.

#### 3.3.2 DMZ Host

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



**Note:** 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
N 1		
None 🗸		
Private IP		Choose PC
MAC Address of the True IP DI	MZ Host 00 . 00 . 00 .00	0.00.00
Note: When a True-IP DMZ h always on.	ost is turned on, it will force the ro	outer's WAN connection to be

DMZ Host for WAN2 and WAN3 is slightly different with WAN1. See the following figure.

DMZ Host Setup					
WAN3					
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	Setu	5
			110.50	- C C C C C	

	WAN1		WAN2	WAN3
WAN 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

OK Clear

**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.

🚰 http://19 📃 🗖 🔀				
	192.168.1.10 192.168.1.18			
	I			

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

	WAN1		WAN2	WAN3
WAN 2 Index	Enable	Aux. WAN IP	Private IP	
1.	<b>V</b>	172.16.3.102	192.168.1.10	Choose PC
2.		172.16.3.200	0.0.0.0	Choose PC

#### 3.3.3 Open Ports

NAT >> 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:

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

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

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **20** port ranges for diverse services.

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

#### Index No. 1

☑ Enable Open Ports							
	Co	mment	P2P				
	W	AN Interface	WAI	V1 🔽			
	Lo	cal Computer	192.	168.1.10	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
з.	💙	0	0	8.	💙	0	0
4.	💙	0	0	9.	💙	0	0
5.	💙	0	0	10.	💙	0	0

Clear

Cancel

ΟK

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Local Computer	Enter the private IP address of the local host or click <b>Choose PC</b> to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be <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.

# 3.4 Applications

Below shows the menu items for Applications.

Ар	olications
►	Dynamic DNS
₽	UPnP

#### 3.4.1 Dynamic DNS

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

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

#### Enable the Function and Add a Dynamic DNS Account

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

Dynamic DNS Setu	p	Set	<u>to Factory Default</u>
🔲 Enable Dynam	ic DNS Setup	View Log	Force Update
Auto-Update inte	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		×

Applications >> Dynamic DNS Setup

OK Clear All

Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
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.	
View Log	Display DDNS log status.	
Force Update	Force the router updates its information to DDNS server.	

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*.

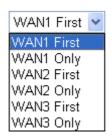
Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Enable Dynamic DNS	Account	
WAN Interface	WAN1 First 💌	
Service Provider	dyndns.org (www.dyndns.org)	~
Service Type	Dynamic 💌	
Domain Name	chronic6853 dyndns.org	dyndns.org 🖌
Login Name	chronic6853	(max. 64 characters)
Password	•••••	(max. 23 characters)
🗹 Wildcards		
🗹 Backup MX		
Mail Extender		

Enable Dynamic DNSCheckAccountcheck

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 InterfaceWAN1/WAN2/WAN3 First - While connecting, the<br/>router will use WAN1/WAN2/WAN3 as the first channel<br/>for such account. If WAN1/WAN2/WAN3 fails, the<br/>router will use another WAN interface instead.<br/>WAN1/WAN2/WAN3 Only - While connecting, the<br/>router will use WAN1/WAN2/WAN3 as the only channel<br/>for such account.



Service ProviderSelect the service provider for the DDNS account.Service TypeSelect a service type (Dynamic, Custom or Static). If you<br/>choose Custom, you can modify the domain that is chosen<br/>in the Domain Name field.Domain NameType in one domain name that you applied previously.<br/>Use the drop down list to choose the desired domain.Login NameType 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 features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

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.

#### 3.4.2 UPnP

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

Applications >> UPnP
UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

**Note:** 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.



# **Enable UPNP Service**

Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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		onnection on Rou	Contraction (CC
Vetwork Tasks         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection           Image: Create a new connection         Image: Create a new connection	hinet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status:		Connected
	Dial-up	Duration:		00:19:06
i) Network Troubleshooter	test Disconnected DrayTek ISDN PPP	Speed:		100.0 Mbps
Other Places  Control Panel My Network Places My Documents	Internet Gateway IP Broadband Connection on Router Enabled	Packets: Sent:	Internet Gateway	My Computer
🚽 My Computer	LAN or High-Speed Internet	Received:	1,115	666
Details (*) Network Connections System Folder	Local Area Connection Enabled Realterk RTL8139/810x Family	Properties	<u>D</u> isable	Close

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

eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
IP Broadband Connection on Router	Services
his connection allows you to connect to the Internet through a hared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>☑ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>☑ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>☑ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>

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.

# **3.5 Wireless LAN**

This function is used for "n" models.

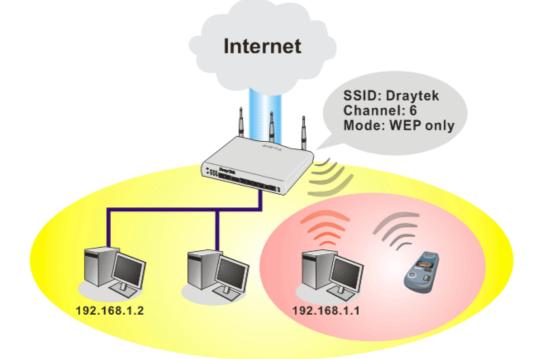
# 3.5.1 Basic Concepts

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.



#### 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.



#### 3.5.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.



#### Wireless LAN >> General Setup

eneral Setting (IEEE 802.11)	
Enable Wireless LAN	
Mode :	Mixed(11b+11g+11n)
SSID:	DrayTek
Channel :	Channel 6, 2437MHz 💌
Packet-OVERDRIVE <sup>TM</sup> Tx Burst Note:	
	also be supported in clients to boost WLAN performance.
Hide SSID	
Long Preamble	
Hide SSID: prevent SSID fro	om being scanned. for some older 802.11b devices only (lowers performance).

OK Cancel

#### **Enable Wireless LAN**

Mode

Check the box to enable wireless function.

At present, the router can connect to 11g Only, 11n Only (2.4 GHz), Mixed (11b+11g), Mixed (11g+11n), Mixed (11a+11n 5 GHz), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

Mix	ed(11b+1	1g+11n)	*
11g	Only		
11n	Only (2.4 ed(11b+1	GHz)	
Mix	ed(11b+1;	1g)	
Mix	ed(11g+1;	1n)	
Mix	ed(11a+1)	1n <sup>´</sup> 5 GHz)	
	ed(11b+1)		

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.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.

Channel:	Channel 6, 2437MHz 🛛 👻
	Auto
	Channel 1, 2412MHz
	Channel 2, 2417MHz
	Channel 3, 2422MHz
	Channel 4, 2427MHz
	Channel 5, 2432MHz
	Channel 6, 2437MHz
	Channel 7, 2442MHz
	Channel 8, 2447MHz
	Channel 9, 2452MHz
	Channel 10, 2457MHz
	Channel 11, 2462MHz
	Channel 12, 2467MHz
	Channel 13, 2472MHz

#### **Packet-OVERDRIVE**

This feature can enhance the performance in data transmission about 40%\* more (by checking **Tx Burs**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**).

Configuration Status Option About		
Configuration Status Option About Configuration Status Option About Configuration Status Auto hide mini status position Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile Group Roeming Ad-hoc WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only Automatically connect to non-preferred networks	Advance Setting Disable Radio Fragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Power Save Mode: Tx Burst :	234 254 802.11b/g/n - 2.4GH 1 Disable Disable
	OK	Cancel
Tx <u>B</u> urst : Diss		*
Disa Enal		

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.

Long Preamble

This option is to define the length of the sync field in an 802.11



packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

#### 3.5.3 Security

Wireless LAN >> Security Settings

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

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.

Mode:		Disable	~
WPA:			
Encryption Mode:		TKIP for WPA/AES for W	/PA2
Pre-Shared Ke	ey(PSK):	******	
Type 8~63 A "cfgs01a2"		r or 64 Hexadecimal digits lea J".	ading by "0x", for example
WEP:			
Encryption Mo	ode:	64-Bit 🗸	
• Key 1 :		******	
○Key 2 :		******	
○Key 3 :		*****	
○Key 4:			
○ Key 4: For 64 bit WEP key		**	
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII chara	acter or 26 He	xadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243".	•
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII chara	acter or 26 He	cadecimal digits leading by "0 exadecimal digits leading by "	•
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII chara	acter or 26 H( - "0x30313233	kadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243".	'0x", for example
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII char. "0123456789abc" or	acter or 26 H( - "0x30313233	xadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243". OK Cancel are several modes provid	'0x", for example
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII char. "0123456789abc" or	acter or 26 He "0x30313233 [ There a	xadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243". OK Cancel are several modes provid	'0x", for example ded for you to choose. Disable
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII char. "0123456789abc" or	acter or 26 He "0x30313233 [ There a	cadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243". OK Cancel are several modes provid	'0x", for example ded for you to choose. Disable
For 64 bit WEP key Type 5 ASCII chara "0x4142333132". For 128 bit WEP key Type 13 ASCII char. "0123456789abc" or	acter or 26 He "0x30313233 [ There a	cadecimal digits leading by "0 exadecimal digits leading by " 343536373839414243". OK Cancel are several modes provid	'0x", for example ded for you to choose. Disable

**WPA/PSK-**Accepts only WPA clients and the encryption key should be entered in PSK.

	<b>WPA2/PSK-</b> Accepts only WPA2 clients and the encryption key should be entered in PSK.		
	<b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.		
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").		
	<b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only.		
	<b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").		
WEP	<b>64-Bit</b> - For 64 bits WEP key, either <b>5</b> ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, 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).		
	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.		
	Encryption Mode: 64-Bit 64-Bit 128-Bit		

#### 3.5.4 Access Control

Wireless LAN >> Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

able Access Control		
Policy	Activate MAC ac	ddress filter 💙
	MAC Address Fi	lter
Index Attribute	MAC Address	Apply SSID
Clien	t's MAC Address :::	
	t's MAC Address ::: ute : s: Isolate the station	

Clear All

ΟK

Enable Access Control	Select to enable the MAC Address access control feature.		
Policy	Select to enable any one of the following policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Isolate WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. Policy : Activate MAC address filter Isolate WLAN from LAN		
MAC Address Filter	Display all MAC addresses that are edited before.		
Client's MAC Address	Manually enter the MAC address of wireless client.		
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.

# 3.5.5 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Station List		
	Status MAC Address	
	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 Access Control :	1
	Client's MAC address	
	Add	
Refresh	Click this button to refresh the status of station l	ist.
٨dd	Click this button to add current typed MAC add	

# 3.6 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, User Password, Time setup and Reboot System.

Below shows the menu items for System Maintenance.

Vigor2850Vn 3.3.6\_RC6 Jun 1 2011 18:00:07

System Maintenance
System Status
User Password
Time and Date
Reboot System

#### 3.6.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System	Status
--------	--------

Model Name	:
Firmware Version	:
Build Date/Time	:

		LAN			
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	Yes	8.8.8.8
LAN2	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	Yes	8.8.8.8
LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8

Wireless LAN				
MAC Address	Frequency Domain	Firmware Version	SSID	
00-1D-AA-00-00-00	Europe	"2.2.0.7"	DrayTek	

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-1D-AA-00-00-01	PPPoE		
WAN2	Connected	00-1D-AA-00-00-02	Static IP	172.16.3.102	172.16.1.1
WAN3	Disconnected	00-1D-AA-00-00-03			

VoIP				
Port	Profile	Reg.	In/Out	
Phone1		No	0/0	
Phone2		No	0/0	

Model Name	Display the model name of the router.	
Firmware Version	Display the firmware version of the router.	
<b>Build Date/Time</b>	Display the date and time of the current firmware build.	
LAN		
LAN1/LAN2/LAN3/LAN4 There are four LAN ports with different IP address offered Vigor router. The MAC address, IP address, Subnet Mask DHCP Server and DNS settings for each LAN port is disp		
<b>IP Routed Subnet</b> Display the general information for the usage of IP rout		
MAC Address	Display the MAC address of the LAN Interface.	
<b>IP Address</b> Display the IP address of the LAN interface.		

Subnet Mask	Display the subnet mask address of the LAN interface.	
<b>DHCP Server</b>	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.	
SSID	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.	

# 3.6.2 User Password

This page allows you to set new password for user operation.

ser Password			 7
	Old Password		
	New Password		
	Confirm Password		
ОК			

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this field.
<b>Confirm Password</b>	Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.



## 3.6.3 Time and Date

It allows you to specify where the time of the router should be inquired from.

System Maintenance >> Time a	nd Date		
Time Information			
Current System Time	2011 Apr 1 Fri 6 : 33 : 27 Inquire Time		
Time Setup			
O Use Browser Time			
💿 Use Internet Time	Client		
Server IP Address	pool.ntp.org		
Time Zone	(GMT) Greenwich Mean Time : Dublin		
Enable Daylight Sav	ring		
Automatically Updat	te Interval 30 min 💌		
Current System Time Use Browser Time	Click <b>Inquire Time</b> to get the current time. Select this option to use the browser time from the remote administrator PC host as router's system time.		
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.		
Time Protocol	Select a time protocol.		
Server IP Address	Type the IP address of the time server.		
Time Zone	Select the time zone where the router is located.		
Enable Daylight Saving	Check the box to activate daylight saving function. Such feature is useful for some areas.		
Automatically Update Interval	Select a time interval for updating from the NTP server.		
Click <b>OK</b> to save these set	tings.		

#### 3.6.4 Reboot System

System Maintenance >> Reboot System

The Web Configurator may be used to restart your router for using current configuration. Click **Reboot System** from **System Maintenance** to open the following page.

ot System	
	Do you want to reboot your router ?
	<ul> <li>Using current configuration</li> </ul>
	Reboot Now

Click **Reboot Now**. The router will take 5 seconds to reboot the system.



**Note:** When the system pops up Reboot System web page after you configure web settings, please click **Reboot Now** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

# 3.7 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.

Diagnostics	
DHCP Table	
🕨 Ping Diagnosis 👘	
Traffic Graph	
Trace Route	

#### 3.7.1 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.

```
DHCP IP Assignment Table | Refresh |

DHCP server: Running

Index IP Address MAC Address Leased Time HOST ID

1 192.168.1.10 00-0E-A6-2A-D5-A1 0:00:11.070 user-6a0e182ce8
```

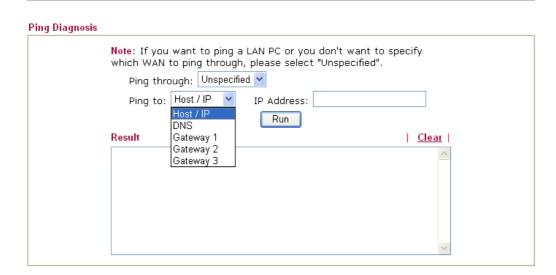
Index	It displays the connection item number.	
IP Address	It displays the IP address assigned by this router for specified PC.	
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.	
Leased Time	It displays the leased time of the specified PC.	
HOST ID	<b>ST ID</b> It displays the host ID name of the specified PC.	
Refresh	Click it to reload the page.	



# 3.7.2 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

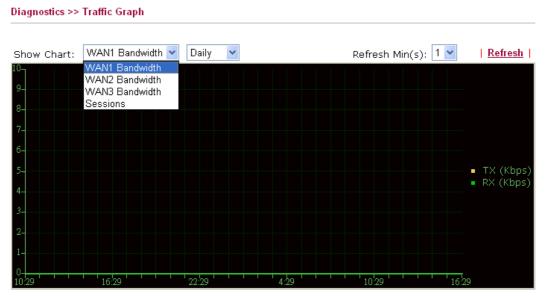
```
Diagnostics >> Ping Diagnosis
```



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 through: Unspecified Unspecified WAN1 WAN2 WAN3		
Ping to	Use the drop down list to choose the destination that you want to ping.		
IP Address	Type in the IP address of the Host/IP 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.		

# 3.7.3 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 following two figures display different charts by daily and weekly.



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

#### 3.7.4 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.

Trace Route			
	Trace through:	Unspecified 💌	
	Protocol:		
	Host / IP Address:		Run
	Result		<u>Clear</u>
			~

Diagnostics >> Trace Route

**Trace through** Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically. Unspecified 🔽 Unspecified WAN1 WAN2 WAN3 **Protocol** Choose the protocol for using by such job ICMP 🔽 **ICMP** UDP It indicates the IP address of the host. Host/IP Address Run Click this button to start route tracing work. Clear Click this link to remove the result on the window.

This page is left blank.

#### Vigor2850 Series User's Guide

# **4** Admin Mode Operation

This chapter will guide users to execute advanced (full) configuration through admin mode operation. As for other examples of application, please refer to chapter 5.

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

Now, the **Main Screen** will appear. Be aware that "Admin mode" will be displayed on the bottom left side.

Vigor2850 VDSL2 Security Fir	Series ewall				Dra	<b>y</b> Te
Auto Logout 💌	System Status					
Quick Start Wizard Service Activation Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor2850Vn : 3.3.6_RC6 : Jun 1 2011 18:00:07				
VAN			LAN			
AN		MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
AT	LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	Yes	8.8.8.8
rewall	LAN2	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	Yes	8.8.8.8
ser Management 👘 📄	LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
bjects Setting	LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
5M	IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8
indwidth Management						
plications			Wireless LAN			
PN and Remote Access	MAC Address	Frequency	Domain	Firmware Versio	n SSID	
ertificate Management	00-1D-AA-00-0		Domain	"2.2.0.7"	DravT	ek
olP ireless LAN						
B Application			WAN			
stem Maintenance	Link Status	MAC Address	Connectio	n IP Address	Default Ga	teway
aqnostics	WAN1 Disconnecte	tente traanezz				condy
agnoonco	WAN2 Connected	00-1D-AA-00-00-02		172.16.3.102	2 172.16.1.1	L
	WAN3 Disconnecte					
pport Area 🛛 💆						
			VoIP			
	Port	Profile	Req	, In	/Out	
	Phone 1		No	0/		

# 4.1 WAN

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

# 4.1.1 Basics of Internet Protocol (IP) Network

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



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

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

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

#### **Get Your Public IP Address from ISP**

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

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

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

For 3G mobile communication through Access Point is popular more and more, Vigor2850 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2850, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2850n with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2850n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2850n series.



After connecting into the router, 3G USB Modem will be regarded as the third WAN port. However, the original WAN1 and WAN2 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN3 also can be used as backup device. Therefore, when WAN1 and WAN2 are not available, the router will use 3.5G for supporting



automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.

WAN

General Setup

Internet Access

Multi-PVCs

Multi-VLAN
Load-Balance Policy

#### 4.1.2 General Setup

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

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

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

WAN >> General Setup

Load Bal Setup	ance Mode	e: Auto Weight			
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode	Backup WAN
WAN1	V	ADSL/-	0/0	Always On	-
WAN2	-	Ethernet/Auto negotiation	0/0	Always On	_
WAN3	V	USB/-	0/0	Always On	-

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

**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 According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance. Auto Weight Load Balance Mode: 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. **Physical Mode / Type** Display the physical mode and physical type of such WAN

	interface.		
Line Speed	Display the downstream and upstream rate of such WAN interface.		
Active Mode	Display whether such WAN interface is Active device or backup device.		
Backup WAN	Display the Backup WAN interface for such WAN when it is disabled.		
Note: In default, each WAN port is enabled.			

#### WAN1 with ADSL/VDSL

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

WAN	>>	General	Setup
-----	----	---------	-------

1	
Enable:	Yes 💌
Display Name:	
Physical Mode:	VDSL
Fallback Mode:	Auto 💌
Physical Type:	Auto negotiation 😪
Line Speed(Kbps):	
DownLink	0
UpLink	0
VLAN Tag insertion (ADSL):	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
VLAN Tag insertion (VDSL):	Disable 💌
Tag value:	0 (0~4095)
Priority:	0 (0~7)
Active Mode:	Always On 💌
Backup WAN:	None 🕶

Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.
Display Name	Type the description for such interface.
Physical Mode	Display the physical mode of such interface. If VDSL is detected, this field will display " <b>VDSL</b> "; if ADSL is detected, it will display " <b>ADSL</b> ".
Fallback Mode	It allows you to specify which physical connection is used. Once the mode is specified, the router will not detect physical mode automatically whenever powering up the router.
Physical type	For such interface, no type can be selected.
Line Speed (Kpbs)	If your choose According to Line Speed as the Load Balance

Cancel



ΟK

	<b>Mode</b> in previous page, please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.		
VLAN Tag insertion (ADSL)	The settings configured in this field are available for VDSL only.		
	<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.		
VLAN Tag insertion (VDSL)	The settings configured in this field are available for VDSL only.		
	<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>Υ</mark> Always On Backup		
Backup WAN	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 Type (Only for Backup Multiple WAN):		

When any WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be

#### WAN2 with Ethernet

WAN2 is fixed with physical mode of Ethernet.

WAN >> General Setup				
WAN 2				
Enable: Display Name: Physical Mode: Physical Type: Line Speed(Kbps): DownLink UpLink VLAN Tag insertion: Tag value: Priority: Active Mode: Backup WAN:	Yes V Ethernet Auto negotiation V O O Disable V (0~4095) O (0~7) Always On V None V			
Enable	OK Cancel Choose <b>Yes</b> to invoke the set Choose <b>No</b> to disable the set	tings for this WAN interface. ings 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 <b>negotiation</b> for determined b	type for WAN2 or choose <b>Auto</b> y the system.		
	Au 10 10 10	uto negotiation Ito negotiation IM half duplex IM full duplex IM half duplex IM full duplex		
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load Balance</b> <b>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 sending by WAN1.	specify the priority for the packet		
	<b>Disable</b> – Disable the function of VLAN with tag.			
	<b>Tag value</b> – Type the value a range is form 0 to 4095.	as the VLAN ID number. The		



**Priority** – Type the packet priority number for such VLAN. The range is from 0 to 7.

Active Mode Choose Always On to make the WAN1 connection being activated always;



**Backup WAN** 

If you choose **Backup** as the **Active Mode**, Backup WAN will be changed into **Backup Type**. 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.

Phonty:	U(U~7)
Active Mode:	Backup 😽
Backup Type (Only for Backup Multiple WAN):	♥ When any WAN disconnect ♥ When all WAN disconnect

When any WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.

#### WAN3 with USB

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

WAN >> General Setup		
WAN 3		
Enable:	Yes 💌	
Display Name:		
Physical Mode:	USB	
Physical Type:	Auto negotiation 🕑	
Line Speed(Kbps):		
DownLink	0	
UpLink	0	
Active Mode:	Always On 💌	
Backup WAN:	None 💌	
Enable	OK Cancel 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 Balance</b> <b>Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.	

**Dray** Tek

Active Mode	Choose <b>Always On</b> to n activated always;	nake the WAN1 connection being
	Always On <mark>.</mark> Alwaγs On Backup	
Backup WAN	be changed into <b>Backup</b> the WAN interface show	as the <b>Active Mode</b> , Backup WAN will <b>D Type</b> . You have to specify which role and play if you want to backup multiple e this setting if you want to backup a
	Phoney:	
	Active Mode:	Backup 💙
	Backup Type (Only for Backup Multiple WAN):	<ul> <li>When any WAN disconnect</li> <li>When all WAN disconnect</li> </ul>

When any WAN disconnect – Such backup WAN will be activated when any master WAN interface disconnects.

When all WAN disconnect – Such backup WAN will be activated only when all master WAN interfaces disconnect.

#### 4.1.3 Internet Access

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

WAN >> Internet Access			
Internet Access			
Index Display Name	Physical Mode	Access Mode	
WAN1	ADSL / VDSL	PPPoE / PPPoA	Details Page
WAN2	Ethernet	None PPPoE / PPPoA	Details Page
WAN3	USB	MPoA / Static or Dynamic IP	Details Page

#### WAN >> Internet Access

Index Display Name	Physical Mode	Access Mode	
WAN1	ADSL / VDSL	PPPoE / PPPoA	Details Page
WAN2	Ethernet	Static or Dynamic IP	Details Page
WAN3	USB	None PPPoE	Details Page
		Static or Dynamic IP PPTP/L2TP	

#### WAN >> Internet Access

Index Display Name	Physical Mode	Access Mode	
WAN1	ADSL / VDSL	PPPoE / PPPoA	Details Page
WAN2	Ethernet	Static or Dynamic IP 👻	Details Page
WAN3	USB	None 💌	Details Page

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/VDSL) /WAN2 (Ethernet) /WAN3 (3G USB Modem) according to the real network connection.
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page according to the access mode that you choose in WAN interface

## 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.

WAN 1		
ΡΡΡοΕ / ΡΡΡοΑ	MPoA / Static or	Dynamic IP
Enable     Dis     Dis     Modem Settings (for ADS     Multi-PVC channel     VPI     VCI Encapsulating Type Protocol	Sable SL only) Channel 1  O  33 LLC/SNAP PPPoE	ISP Access Setup Username Password Separate Account for ADSL PPP Authentication PAP or CHAP Idle Timeout Idle Timeout IP Address From ISP WAN IP Alias Fixed IP Yes No (Dynamic IP)
Modulation PPPoE Pass-through For Wireless LAN For Wireless LAN WAN Connection Detect	Multimode 💌	Fixed IP Address  Default MAC Address  Specify a MAC Address MAC Address: 00 .10 .AA:00 .00 .01
Mode Ping IP TTL:	ARP Detect	Index(1-15) in <u>Schedule</u> Setup: =>,,,,,

Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
Modem Settings (for ADSL only)	Set up the DSL parameters required by your ISP. These settings configured here are specified for ADSL only.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access >> Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	<b>VPI</b> - Type in the value provided by ISP.
	VCI - Type in the value provided by ISP.
	<b>Encapsulating Type</b> - Drop down the list to choose the type provided by ISP.
	<b>Protocol</b> - Drop down the list to choose the one (PPPoE or PPPoA) provided by ISP.
	If you have already used <b>Quick Start Wizard</b> to set the protocol, then it is not necessary for you to change any settings in this group.
	<b>Modulation</b> –Default setting is Multimode. Choose the one that fits the requirement of your router.



	Modulation	T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.	
	-	neck this box, PCs on the same of PPPoE session (different with Internet.
	<b>For Wireless LAN</b> – If you wireless network can use and (different with the Host PC)	
	protocol and check the box(	through, please choose PPPoA es) here. The router will behave like the PPPoE client on the LAN. PPPoA dial-up connection.
WAN Connection Detection	Such function allows you to is alive or not through ARP	verify whether network connection Detect or Ping Detect.
	Mode – Choose ARP Detected execute for WAN detection.	et or <b>Ping Detect</b> for the system to
	<b>Ping IP</b> – If you choose Pin have to type IP address in th	g Detect as detection mode, you is field for pinging.
	<b>TTL (Time to Live)</b> – Disp value is set by telnet comma	lays value for your reference. TTL nd.
ISP Access Setup		ne, password and authentication information provided by your ISP.
	<b>Username</b> – Type in the use field.	ername provided by ISP in this
	<b>Password</b> – Type in the pas	sword provided by ISP in this field.
		ct <b>PAP only</b> or <b>PAP or CHAP</b> for to Internet all the time, you can
	<b>Idle Timeout</b> – Set the time after passing through the tim	out for breaking down the Internet ne without any action.
IP Address From ISP	you connect to it and request service to always assign you request. In this case, you car	signs IP address to you each time t. In some case, your ISP provides the same IP address whenever you fill in this IP address in the Fixed ISP before you want to use this

Modulation

Multimode

\*

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.

<b>@</b> )	🗿 WAN IP Alias - Microsoft Internet Explorer 🛛 🔲 🔀								
v	WAN IP Alias ( Multi-NAT )								
	Index	Enable	Aux. WAN IP	Join NAT IP Pool					
	1.	V	172.16.3.229	V					
	2.								
	з.								
	4.								
	5.								
	6.								
	7.								
	8.								
			OK Clear All	Close					

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

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

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

**Index (1-15) in Schedule Setup -** You can type in four sets of time schedule for your request. 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.

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

#### **Details Page for MPoA 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.

WAN 1			
ΡΡΡοΕ / ΡΡΡοΑ	MPoA / Static or	Dynamic IP	
🔿 Enable 💿 Disable		WAN IP Network Settings	WAN IP Alias
Modem Settings (for ADSL only)		🔘 Obtain an IP address a	utomatically
Multi-PVC channel	Channel 2	Router Name	Vigor *
Encapsulation		Domain Name	*
1483	3 Bridged IP LLC 🛛 🔽	* : Required for some I	BPs
VPI	0	Specify an IP address	
VCI	88	IP Address	
Modulation	Multimode	Subnet Mask	
		Gateway IP Address	
WAN Connection Detection	on		
Mode	ARP Detect 💌	⊙ Default MAC Address	
Ping IP TTL:		Specify a MAC Addres	ss
		MAC Address: 00 .1D	· AA 00 .00 .01
RIP Protocol  Enable RIP		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	
Bridge Mode  Enable Bridge Mode			
	OK	Cancel	
Enable/Disable		c activating this function be closed and all the s	-
	in this page will		settings that you adjust
Modem Settings (for ADSL only)	1 I	parameters required by are specified for ADSL	your ISP. These settin, only.
	determined by th	nnel - The selections d e page of Internet Ac Channel means no sel	cess >>Multi PVCs.
	<b>Encapsulating</b> - provided by ISP.	Drop down the list to	choose the type
	<b>VPI</b> - Type in th	e value provided by IS	P.
	VCI - Type in th	e value provided by IS	P.
		efault setting is Multiment of your router.	ode. Choose the one the

WAN >> Internet Access

	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	-	ou to verify whether network connection 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.			
	•	e Ping Detect as detection mode, you in this field for pinging.		
	<b>TTL (Time to Live)</b> – value is set by telnet co	Displays value for your reference. TTL mmand.		
RIP Protocol	-	otocol is abbreviated as RIP(RFC1058) exchange routing tables information. activating this function.		
Bridge Mode	•	<b>IP</b> as the protocol, you can check this ion. The router will work as a bridge		
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.			
	would like to utilize the WAN IP Alias. You can than the current one you available for WAN1 on and check the Enable be	have multiple public IP addresses and em on the WAN interface, please use n set up to 8 public IP addresses other u are using. Notice that this setting is ly. Type the additional WAN IP address ox. Then click <b>OK</b> to exit the dialog.		
	WAN1 IP Alias (Multi-NAT)			

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v		v
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
		OK Clear All	Close

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically.

Router Name – Type in the router name provided by ISP.

	<b>Domain Name</b> – Type in the domain name that you have assigned.
	<b>Specify an IP address</b> – Click this radio button to specify some data.
	<b>IP</b> Address – Type in the private IP address.
	Subnet Mask – Type in the subnet mask.
	Gateway IP Address – Type in gateway IP address.
	<b>Default MAC Address</b> – Type in MAC address for the router. You can use <b>Default MAC Address</b> or specify another MAC address for your necessity.
	<b>Specify a MAC Address</b> – Type in the MAC address for the router manually.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

# 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

WAN 2			
PPPoE	Static or Dynamic IP	PPTP/L2TP	
🔘 Enab	le 💿 Disable	PPP/MP Setup	
		PPP Authentication	PAP or CHAP
ISP Access S	etup	Idle Timeout	-1 second(s)
Username		IP Address Assignme	nt Method (IPCP)
Password		WAN IP Alias	
Index(1-15)	in <u>Schedule</u> Setup:	Fixed IP: 🔘 Yes 🤇	) No (Dynamic IP)
=>	,,,,,	Fixed IP Address	
WAN Common	den Detenden		
	tion Detection	💿 Default MAC Add	dress
Mode	ARP Detect 🚩	🔵 Specify a MAC A	Address
Ping IP		MAC Address: 00	1D AA 00 00 02
TTL:			
	ОК	Cancel	

Enable/Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	<b>Username</b> – Type in the username provided by ISP in this field.
	<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. <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.
PPP/MP Setup	<b>PPP Authentication</b> – Select <b>PAP only</b> or <b>PAP or CHAP</b> for PPP. If you want to connect to Internet all the time, you can check <b>Always On</b> .
	<b>Idle Timeout</b> – Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method (IPCP)	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 **OK** to exit the dialog.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.102	v
2.	✓	172.16.3.200	✓
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	

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

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

Specify a MAC Address – Type the MAC address for the



#### router manually.

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

#### **Details Page for Static or Dynamic IP in 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.

PPPoE	Static or Dynamic IP	РРТР	
💿 Enable 🛛 Disab	le	WAN IP Network Settings	WAN IP Alias
		🔘 Obtain an IP address	automatically
Keep WAN Connection		Router Name	*
Enable PING to keep alive		Domain Name	*
PING to the IP		* : Required for some I	ISPs
PING Interval	0 minute(s)	Specify an IP address	
WAN Connection Detection		IP Address	172.16.3.102
Mode	ARP Detect 🔽	Subnet Mask	255.255.0.0
Ping IP		Gateway IP Address	<b> </b> 172.16.1.1
TTL:		Default MAC Address	
RIP Protocol		<ul> <li>Specify a MAC Address</li> </ul>	
Enable RIP		MAC Address: 00 50	
		DNS Server IP Address	
		Primary IP Address	168.95.1.1
		Secondary IP Address	
	ОК	Cancel	
Cnable / Disable		be closed and all the s	n. If you click <b>Disable</b> , ettings that you adjusted
Keep WAN Connection	because some ISF	Ps will drop connection iods of time. Check E	Dynamic IP environmer as if there is no traffic nable PING to keep al
		If you enable the PIN the system to PING it	G function, please speci for keeping alive.
	<b>PING Interval</b> - PING operation.	Enter the interval for t	he system to execute th
VAN Connection Such function allo		ows you to verify whet gh ARP Detect or Ping	ther network connectior g Detect.

WAN >> Internet Access



Mode – Choose ARP Detect or Ping Detect for the system to<br/>execute for WAN detection.Ping IP – If you choose Ping Detect as detection mode, you have<br/>to type IP address in this field for pinging.TTL (Time to Live) – Displays value for your reference. TTL<br/>value is set by telnet command.RIP ProtocolRouting Information Protocol is abbreviated as RIP (RFC1058)<br/>specifying how routers exchange routing tables information. Click<br/>Enable RIP for activating this function.WAN IP Network<br/>SettingsThis group allows you to obtain an IP address automatically and<br/>allows you type in IP address manually.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



2. S		172.16.3.102 172.16.3.200	
з. [		).0.0.0	
4.	n la		
	- L	).0.0.0	
5.		).0.0.0	
6.		).0.0.0	
7.		).0.0.0	
8.		).0.0.0	

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

Router Name: Type in the router name provided by ISP.

Domain Name: Type in the domain name that you have assigned.

**Specify an IP address** – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

**Default MAC Address**: Click this radio button to use default MAC address for the router.

**Specify a MAC Address**: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

**DNS Server IP Address** Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for

necessity in the future.

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

### Details Page for PPTP/L2TP in WAN2

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

WAN >> Internet Access			
WAN 2			
PPPoE Static	or Dynamic IP	PPTP/L2TP	
OEnable PPTP OEnat	ole L2TP 💿 Disable	PPP Setup	
Server Address		PPP Authentication	PAP or CHAP 🚩
Specify Gateway IP Address	5	Idle Timeout	-1 second(s)
172.16.1.1		IP Address Assignment WAN IP Alias	t Method (IPCP)
ISP Access Setup		Fixed IP: O Yes O No (Dynamic IP)	
Username		Fixed IP Address	
Password		WAN IP Network Settings	
Index(1-15) in <u>Schedule</u> Se	etup:	🔘 Obtain an IP addr	ess automatically
=>,,,	,	Specify an IP add	ress
		IP Address	172.16.3.102
		Subnet Mask	255.255.0.0
-	OK	Cancel	
		Calleer	
PPTP/L2TP			on to enable a PPTP client n on the WAN interface.
			on to enable a L2TP client n on the WAN interface.
	<b>Disable</b> – Click through PPTP or		close the connection
	Server Address		lress of the PPTP/L2TP ent mode.
	<b>Specify Gatewa</b> address for DHC	<b>y IP Address</b> – Spe P server.	cify the gateway IP
ISP Access Setup	<b>Username</b> -Type in the username provided by ISP in this field.		
	Password -Type in the password provided by ISP in this field.		
	time schedule fo previously in Ap	r your request. All th	ou can type in four sets of he schedules can be set lule web page and you can that web page.
PPP Setup	<b>PPP Authentica</b> PPP.	ntion - Select PAP o	only or PAP or CHAP for
		Set the timeout for bough the time without	reaking down the Internet ut any action.
IP Address Assignment	WAN IP Alias -	If you have multipl	e public IP addresses and



Method(IPCP)

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.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.102	v
2.	✓	172.16.3.200	$\checkmark$
з.		0.0.0	
4.		0.0.0	
5.		0.0.0	
6.		0.0.0.0	
7.		0.0.0	
8.		0.0.0	

**Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box.

Fixed IP Address - Type a fixed IP address.

WAN IP NetworkObtain an IP address automatically – Click this button to<br/>obtain the IP address automatically.

**Specify an IP address** – Click this radio button to specify some data.

**IP** Address – Type the IP address.

Subnet Mask – Type the subnet mask.

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

#### **Details Page for 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.

13		
3G Modem	🔘 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#)
PPP Username		(Optional)
PPP Password		(Optional)
PPP Authentication	PAP or CHAP 🐱	
Index(1-15) in <u>Sched</u>	<u>ule</u> Setup: ,,	
WAN Connection Detec	tion	
Mode	ARP Detect 💌	
Ping IP		
TTL:		

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.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.
Modem Initial String2	The initial string 1 is shared with APN.
	In some cases, user may need another initial AT command to restrict 3G band or do any special settings.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).
Always On	If you want to connect to Internet all the time, you can check <b>Always On</b> .

**Dray** Tek

	<b>Idle Timeout</b> – Set the timeout for breaking down the Internet after passing through the time without any action.
	<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.

#### 4.1.4 Multi-PVCs

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

#### General

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

WAN >> Multi-PVCs

Multi-PV	Cs						
General ATM QoS		F	Port-based Bri	idge			
Channe	I .	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.			0	33	UBR 🔽	PPP0E 🚩	LLC/SNAP 🔽
2.		✓	0	88	UBR 🔽	MPoA 💌	1483 Bridged IP LLC 🛛 👻
з.			1	43	UBR 🔽	PPPoA 🔽	VC MUX
4.			1	44	UBR 🔽	PPPoA 💌	VC MUX 🔽
5.	WAN		1	45	UBR 🔽	PPPoA 🔽	VC MUX
6.	WAN		1	46	UBR 🔽	PPPoA 💌	VC MUX 🗸
7.	WAN		1	47	UBR 🔽	PPPoA 🔽	VC MUX
8.			1	48	UBR 🔽	PPPoA 👻	VC MUX

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



Enable
 Check this box to enable that channel. The channels that you enabled here will be shown in the Multi-PVC channel drop down list on the web page of Internet Access. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of Internet Access.
 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	
nrt∨BR	
rt∨BR	

Protocol

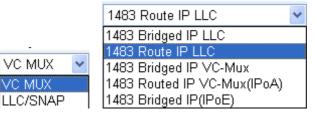
Select a proper protocol for this channel.

# Protocol

PPPoE	*
PPP0A	
PPP <sub>0</sub> E	
MPoA	

Encapsulation

Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.



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

#### WAN >> Multi-PVCs >> PVC Channel 5

DSL Modem Settings				
VPI 1	QoS Type	UBR 💌		
VCI 45	Protocol	PPPoA 💌		
	Encapsulati	on VC MUX 💌		
WAN Connection Detection				
Mode	ARP Detect	~		
Ping IP				
TTL:				
PPPoE/PPPoA Client		MPoA (RFC1483/2684)		
ISP Access Setup		Obtain an IP addres	s automatically	
ISP Name		Router Name	Vigor	
Username		Domain Name		
Password		*: Required for some ISPs		
PPP Authentication PAP or		Specify an IP addre	SS	
Always On		IP Address		
Idle Timeout -1	second(s)	Subnet Mask		
IP Address From ISP		Gateway IP Address		
Fixed IP 🛛 🔿 Yes 💿 No (Dyna	mic IP)	DNS Server IP Address		
Fixed IP Address		Primary IP Address		
		Secondary IP Address		

#### WAN for Router-borne Application

Choose the router service for channel 5, 6 or 7.

**Management** - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR069.

**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.

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

### ATM QoS

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

```
WAN >> Multi-PVCs
```

```
Multi-PVCs
```

General ATM QoS		Port-base	l Bridge	
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

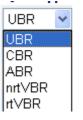
Note: 1.Set 0 means default value.

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

OK	Clear	Cancel

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".

SCRIt represents Sustainable Cell Rate. The value of SCR must<br/>be smaller than PCR.

MBSIt represents Maximum Burst Size. The range of the value is<br/>10 to 50.

#### **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
```

Multi-PVCs								
General	General ATM QoS		ral ATM QoS Port-based Bridge					
Channel	Enable	P1	P2	P3	P4	Service Type	Add Tag	Priority
1.						Normal 😽		0
2.						Normal 💌		0
з.						Normal 🚩		0
4.						Normal 👻	0	0
5.						Normal 🚩		0
6.						Normal 💌	0	0
7.						Normal 😽		0
8.						Normal 🐱	0	0

Note: 1.Channel 1 to 2 are reserved for Nat/Route use.

2.P1 is reserved for Nat/Route use.

OK	Clear	Cancel

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.
It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8.
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> .
<b>Normal</b> – It means that the PVC can accept all packets.
<b>IGMP</b> –It means that such PVC can accept IGMP packets only. Such type just meets a specific environment on some ISPs. Data and IGMP packets will be transmitted and received with different PVC.
To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
To add the packet priority number for such VLAN. The range is from 0 to 7.

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

### 4.1.5 Multi-VLAN

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

#### General

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

WAN >> Multi-VLAN

Gener	al	Bridge		
Channel	Enable		Add Tag	Priority
1.			0	0 😒
2.			0	0 😽
з.			0	0 😽
4.			0	0 🕶
5.		WAN	0	0 🗸
6.		WAN	0	0 🗸
7.		WAN	0	0 🗸
8.			0	0 💙

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

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

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

4. Channel 5 to channel 8 can be used for Router-borne application.

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

OK Clear

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

WAN >> Multi-VLAN >> PVC Channel 5	
WAN for Router-borne Application: Management 💌	
PPPoE/PPPoA Client O Enable O Disable	Static or Dynamic IP O Enable  O Disable
ISP Access Setup	WAN IP Network Settings
ISP Name	Obtain an IP address automatically
Username	Router Name Vigor *
Password	Domain Name *
PPP Authentication PAP or CHAP	*: Required for some ISPs
🗹 Always On	Specify an IP address
Idle Timeout -1 second(s)	IP Address
IP Address From ISP	Subnet Mask
Fixed IP 🔷 Yes 💿 No (Dynamic IP)	Gateway IP Address
Fixed IP Address	DNS Server IP Address
	Primary IP Address
	Secondary IP Address
ОК	Cancel

WAN for Router-borne

#### Application

Choose the router service for channel 5, 6 or 7.

Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this VLAN will be effective for Web

configuration/telnet/TR069. VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this VLAN will be effective for VoIP data transmitting and receiving.

**IPTV** - It can be specified for IPTV only. If you choose IPTV, the configuration for this VLAN will be effective for IPTV data transmitting and receiving.

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

#### Bridge

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

```
WAN >> Multi-VLAN
```

Gener	al	Bridge			
Channel	Enable	P1	P2	P3	P4
1.					
2.					
з.	<b>~</b>				
4.	<b>~</b>				
5.	<b>~</b>				
6.	<b>~</b>				
7.	<b>~</b>				
8.					

Note: P1 is reserved for Nat/Route use.



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.

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.

### 4.1.6 Load-Balance Policy

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

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

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	 Move Up	Move Down
1		any	*	WAN1 🔽							<u>Down</u>
<u>2</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>3</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>4</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>5</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>6</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
Z		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>8</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>9</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>10</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Down</u>

WAN >> Load-Balance Policy

	_
OK	
	OK

Index	Click the number of index to access into the load-balance policy configuration web page.
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to change the protocol for the WAN interface.
WAN	Use the drop-down menu to change the WAN interface.
Src IP Start	Displays the IP address for the start of the source IP.
Src IP End	Displays the IP address for the end of the source IP.
Dest IP Start	Displays the IP address for the start of the destination IP.
Dest IP End	Displays the IP address for the end of the destination IP.
Dest Port Start	Displays the IP address for the start of the destination port.
Dest Port End	Displays the IP address for the end of the destination port.
Move UP/Move Down	Use <b>Up</b> or <b>Down</b> link to move the order of the policy.
	- (h., f.,11,,',, f.,, f', ', 1,, 1, 1,,, 1'

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

# **Dray** Tek

#### WAN >> Load-Balance Policy

	Enable	
F F	Protocol	any 💌
E	Binding WAN Interface	WAN1 👻 🗹 Auto failover to the other WAN
5	Src IP Start	
5	Src IP End	
C	Dest IP Start	
[	Dest IP End	
C	Dest Port Start	
C	Dest Port End	
[	Dest Port End	

Enable

Check this box to enable this policy.

Protocol

Use the drop-down menu to choose a proper protocol for the WAN interface.

Protocol
----------

any	*
any	
TCP	
UDP	
TCP/UDP	
ICMP	
IGMP	

Binding WAN interface	Choose the WAN interface (WAN1/WAN2/WAN3) for binding. <b>Auto failover to other WAN</b> – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is failover.
Src IP Start	Type the source IP start for the specified WAN interface.
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Dest IP Start	Type the destination IP start for the specified WAN interface.
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Dest Port Start	Type the destination port start for the destination IP.
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

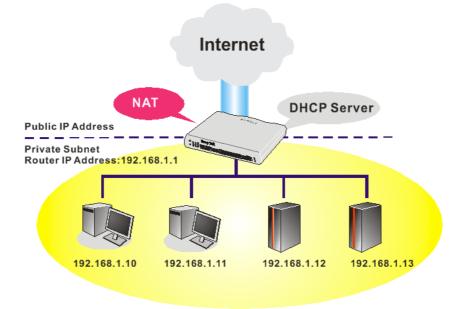
# 4.2 LAN

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



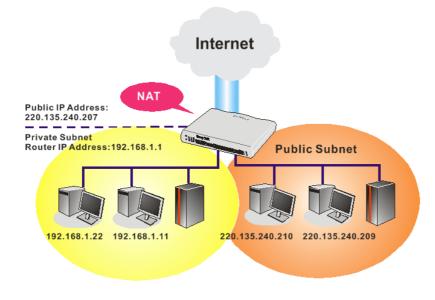
#### 4.2.1 Basics of LAN

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



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





### What is Routing Information Protocol (RIP)

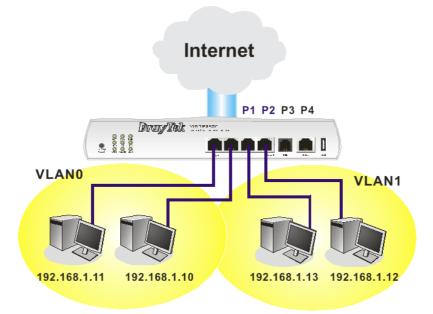
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

#### What is Static Route

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

### What are Virtual LANs and Rate Control

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



**Dray** Tek

## 4.2.2 General Setup

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

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – 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.

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1		Details Page
LAN 2		<b>V</b>	192.168.3.1		Details Page
LAN 3			192.168.5.1		Details Page
LAN 4		<b>V</b>	192.168.7.1		Details Page
IP Routed Subnet		<b>V</b>	192.168.2.1		Details Page
r-LAN Routing					
Subnet	LAN 1	L	AN 2	LAN 3	LAN 4
LAN 1					

LAN 3 LAN 4

LAN >> General Setup

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

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



 $\checkmark$ 

# **Details Page for LAN1**

LAN >> General Setup

LAN 1 Ethernet TCP / IP :	and DHCP Setup				
Network Configuration For NAT Usage			DHCP Server Configuration		
IP Address	192.168.1.1	Relay Agent: OEnable			
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
		IP Pool Counts	50		
RIP Protocol Control	Disable 💌	Gateway IP Address	192.168.1.1		
		DHCP Server IP Address for Relay Agent			
		DNS Server IP Address			
		🔲 Force DNS manual s	Force DNS manual setting		
		Primary IP Address			
		Secondary IP Address			

OK

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)
<b>RIP Protocol Control</b>	<b>Disable -</b> deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	Enable – activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<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>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.
	<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.

**Gateway IP Address -** Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

**DHCP Server IP Address for Relay Agent -** Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

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.

**Force DNS manual setting -** 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).

**Primary IP Address -**You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

**Secondary IP Address -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

The default DNS Server IP address can be found via Online Status:

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 assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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

**DNS Server Configuration** 



## Details Page for LAN2/LAN3/LAN4

LAN >> General Setup

Lan 2 Ethernet TCP / IP and DHCP Setup				
Network Configuration		DHCP Server Configuration		
🔘 Enable 💿 Disable		⊙Enable Server ○Disat	ole Server	
⊙ For NAT Usage	◯ For Routing Usage	Start IP Address	192.168.3.10	
IP Address	192.168.3.1	IP Pool Counts	100	
Subnet Mask	255.255.255.0	Gateway IP Address	192.168.3.1	

OK	_
ON	_

Enable/Disable	Click Enable to enable such configuration.
	Click <b>Disable</b> to disable such configuration.
For NAT Usage	Click this radio button to invoke NAT function.
For Routing Usage	Click this radio button to invoke this function.
IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	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.

# Details Page for IP Routed Subnet

LAN >> General Setup

TCP/IP and DHCP Setup f	or IP Routed Subnet	
Network Configuration		DHCP Server Configuration
🔘 Enable 🛛 💿 Disable		Start IP Address
For Routing Usage		IP Pool Counts 0 (max. 10)
IP Address	192.168.2.1	Use LAN Port P1 P2
Subnet Mask	255.255.255.0	Use MAC Address
RIP Protocol Control	Disable 💌	Index Matched MAC Address given IP Address
		MAC Address :
		Add Delete Edit Cancel
		ок

Enable/Disable	Click <b>Enable</b> to enable such configuration.
	Click <b>Disable</b> to disable such configuration.
For NAT Usage	Click this radio button to invoke NAT function.
For Routing Usage	Click this radio button to invoke this function.
IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
RIP Protocol Control	<b>Disable -</b> deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	<b>Enable</b> – activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address



must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

**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.

**Use LAN Port** – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.

Use MAC Address - Check such box to specify MAC address.

**MAC Address:** Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for  $2^{nd}$  DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in  $2^{nd}$  subnet won't get an IP address belonging to  $1^{st}$  subnet.

**Add** – Type the MAC address in the boxes and click this button to add.

Delete - Click it to delete the selected MAC address.

Edit – Click it to edit the selected MAC address.

**Cancel** – Click it to cancel the job of adding, deleting and editing.

#### 4.2.3 Static Route

Go to LAN to open setting page and choose Static Route.

#### LAN >> Static Route Setup

tatic Route Configuration			Set to Factory Default   View Routing Table		
Index	Destination 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

Index	The number (1 to 10) under Index allows you to open next page to set up static route.
<b>Destination Address</b>	Displays the destination address of the static route.
Status	Displays the status of the static route.
Viewing Routing Table	Displays the routing table for your reference.

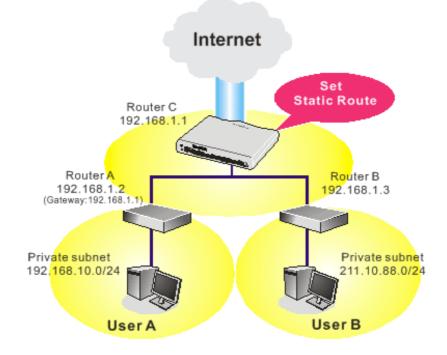
rent Runn	ing Routing Table		Refre
Key: C	- connected, S -	static, R - RIP, * - default, ~ - private	
*	0.0.0/	0.0.0.0 via 172.16.3.1, WAN1	
C~	192.168.1.0/	255.255.255.0 is directly connected, LA	N
С	172.16.3.0/	255.255.255.0 is directly connected, WAN	(1

#### Add Static Routes to Private and Public Networks

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.

× No. 1		
🗹 Enable		
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN1 🔽

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

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 🔽

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

Diagnostics >> View Routing Table

. . . .

. . . .

LAN >> Static Route Setup

Key: C	- connected, S -	static, R - RIP, * - default, ~ -	private	
S~	192.168.10.0/	255.255.255.0 via 192.168.1.2,	LAN	
C~	192.168.1.0/	255.255.255.0 is directly connect	ed, LAN	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3,	LAN	

**Dray** Tek

### 4.2.4 VLAN

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

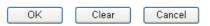
VLAN Config	guration											
🗹 Enable												
		VLAN Tag			L/	AN .			Wirele	ss LAN		
	Enable	VID	Priority	P1	P2	<b>P</b> 3	P4	SSID1	SSID2	SSID3	SSID4	Subnet
VLAN0		0	0 🛩									LAN 1 🔽
VLAN1		0	0 🕶									LAN 1 🔽
VLAN2		0	0 🕶									LAN 1 💌
VLAN3		0	0 🕶									LAN 1 🔽
VLAN4		0	0 🕶									LAN 1 💌
VLAN5		0	0 🕶									LAN 1 🔽
VLAN6		0	0 🕶									LAN 1 💌
VLAN7		0	0 🕶									LAN 1 🔽



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.



#### LAN >> VLAN Configuration

#### VLAN Configuration

🗹 Enable												
	VLAN Tag			LAN			Wireless LAN					
	Enable	VID	Priority	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet
VLAN0		0	0 🛩									LAN 1 🔽
VLAN1		0	0 🕶									LAN 1 🔽
VLAN2		0	0 🕶									LAN 1 💌
VLAN3		0	0 🔽									LAN 1 💌
VLAN4		0	0 🔽									LAN 1 💌
VLAN5		0	0 🔽									LAN 1 🔽
VLAN6		0	0 🕶									LAN 1 💌
VLAN7		0	0 🕶									LAN 1 🔽

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

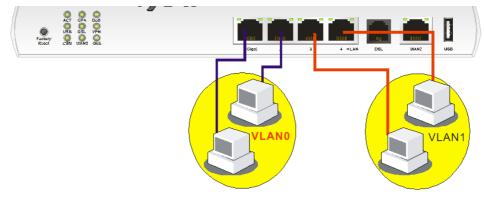


VLAN Tag	<b>Enable</b> – Enable the function of VLAN with tag.
	The router will add specific VLAN number to all packets on the LAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN.
	<b>Disable</b> – Disable the function of VLAN with tag.
	<b>VID</b> – Type the value as the VLAN ID number. The range is form 0 to 4095.
	<b>Priority</b> – Type the packet priority number for such VLAN. The range is from 0 to 7.
LAN	<b>P1</b> – <b>P4</b> – Check the LAN port(s) to be grouped under the selected VLAN.
Wireless LAN	<b>SSID1</b> – <b>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.

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

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

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



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

#### LAN >> VLAN Configuration

#### VLAN Configuration

🗹 Enable												
	VLAN Tag			LAN			Wireless LAN					
	Enable	VID	Priority	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4	Subnet
VLAN0		0	0 🕶									LAN 1 🔽
VLAN1		0	0 🕶									LAN 1 💌
VLAN2		0	0 🕶									LAN 1 💌
VLAN3		0	0 🕶									LAN 1 💌
VLAN4		0	0 🕶									LAN 1 💌
VLAN5		0	0 🔽									LAN 1 💌
VLAN6		0	0 🔽									LAN 1 💌
VLAN7		0	0 🕶									LAN 1 💌

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

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

### 4.2.5 Bind IP to MAC

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

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

LAN >> Bind IP to MAC		
Bind IP to MAC		
○ Enable		
ARP Table   Select All   Sort   Refresh	IP Bind List	Select All   Sort
IP Address Mac Address 192.168.1.10 EO-CB-4E-DA-48-79	Index IP Address	Mac Address
Add and Edit		
IP Address		
Mac Address		
Add	Edit Delete	

Note: IP-MAC binding presets DHCP Allocations.

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

ОК

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

IP Bind List	It displays a list for the IP bind to MAC information.					
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .					
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.					
Delete	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Delete</b> . The selected item will be removed from the <b>IP Bind List</b> .					
<b>Note:</b> Before you select <b>Strict Bind</b> , 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 configurator of the router						
	es can access into internet. And the web configurator of the fouter					

### 4.3 NAT

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

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

The benefit of the NAT includes:

might not be accessed.

- 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.

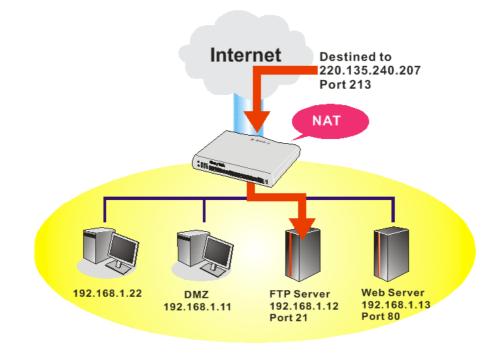
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



### **4.3.1 Port Redirection**

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



The port redirection can only apply to incoming traffic.

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

NAT	>>	Port	Red	irection

Port Redirection	on		Set to F	actory Default
Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				×
<u>4.</u>				×
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				×
<u>9.</u>				×
<u>10.</u>				×
<< <u>1-10</u>   <u>11-2</u>	0 >>			<u>Next</u> >>

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



#### NAT >> Port Redirection

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

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

OK	Clear	Cancel

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</b> <b>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 configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance** >>**Management Setup**. You then



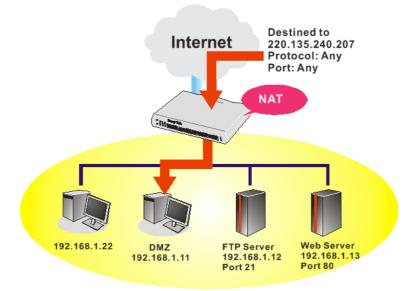
will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

System Maintenance >> Management

Management Access Control		Management Port Setur	Management Port Setup		
<ul> <li>Allow management fro</li> <li>FTP Server</li> <li>HTTP Server</li> </ul>	om the Internet	<ul> <li>User Define Ports</li> <li>Telnet Port</li> <li>HTTP Port</li> </ul>	O Default Ports 23 (Default: 23) 80 (Default: 80)		
<ul> <li>HTTPS Server</li> <li>Telnet Server</li> <li>SSH Server</li> </ul>		HTTPS Port FTP Port SSH Port	443 (Default: 443 21 (Default: 21) 22 (Default: 22)		
Disable PING from the		SNMP Setup	nt		
List IP 1 2	Subnet Mask	Get Community Set Community Manager Host IP	public private		
3		Trap Community Notification Host IP Trap Timeout	public 10 seconds		

### 4.3.2 DMZ Host

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



**Dray** Tek

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 .	
Note: When a True-IP DN always on.	1Z host is turned on, it will	orce the router's WAN connection to be

ОК

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 H	lost Setup
--------	-------	------------

MZ Host Setup		
WAN1	WAN2	WAN3
VAN 2		
Enable	Private IP	1
	0.0.0.0	Choose PC

OK

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

)MZ Host S	Setup			
	WAN1		WAN2	WAN3
WAN 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

**Enable** Check to enable the DMZ Host function.

**Private IP** 

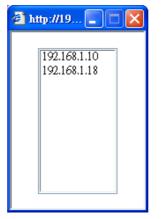
Enter the private IP address of the DMZ host, or click Choose PC

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.



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

	WAN1		WAN2	WAN3
WAN 2 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.102	192.168.1.10	Choose PC
2.		172.16.3.200	0.0.0	Choose PC

OK Clear

## 4.3.3 Open Ports

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

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

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

NAT >> Open Ports

Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				×
<u>4.</u>				×
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				x
<u>9.</u>				х
<u>10.</u>				×
<u>1-10   11-20 &gt;</u>	>			<u>Next</u> >:

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

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

# **Dray** Tek

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

#### Index No. 1

🖌 E	nable Open P	orts					
Comment			P2P				
WAN Interface			WAI	V1 🔽			
Local Computer			192.1	168.1.10	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
з.	💙	0	0	8.	💙	0	0
4.	💙	0	0	9.	💙	0	0
5.	🗸	0	0	10.	🗸	0	0

Clear

Cancel

ΟK

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

### 4.3.4 Address Mapping

This page is used to map specific private IP to specific WAN IP alias.

If you have "a group of IP Addresses" and want to apply to the router, please use WAN IP alias function to record these IPs first. Then, use address mapping function to map specific private IP to specific WAN IP alias.

For example, you have IP addresses ranging from 86.123.123.1 ~ 86.123.123.8. However, your router uses 86.123.123.1, and the rest of the IPs are recorded in WAN IP alias. You want that private IP 192.168.1.10 can use 86.123.123.2 as source IP when it sends packet out to Internet. You can use address mapping function to achieve this demand. Simply type 192.168.1.10 as the Private IP; and type 86.123.123.2 as the WAN IP.



in one map	ping Setup				ory Default
Index	Protocol	Public IP	Private IP	Mask	Status
<u>1.</u>	ALL	172.16.3.102		/32	х
<u>2.</u>	ALL	172.16.3.102		/32	х
<u>3.</u>	ALL	172.16.3.102		/32	х
<u>4.</u>	ALL	172.16.3.102		/32	х
<u>5.</u>	ALL	172.16.3.102		/32	х
<u>6.</u>	ALL	172.16.3.102		/32	х
<u>7.</u>	ALL	172.16.3.102		/32	х
<u>8.</u>	ALL	172.16.3.102		/32	х
<u>9.</u>	ALL	172.16.3.102		/32	х
<u>10.</u>	ALL	172.16.3.102		/32	х

Protocol	Display the protocol used for this address mapping.
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10
Mask	Display the subnet mask selected for this address mapping.
Status	Display the status for the entry, enable or disable.
Clipte the index association	link to open the configuration need

Click the index number link to open the configuration page.

#### NAT >> Address Mapping

Index No. 1				
🔲 Enable				
Protocol:	ALL 💌			
WAN Interface	WAN1 💌			
WAN IP	1-172.16.3.102 💌			
Private IP:				
Subnet Mask:	/32 💌			
	OK Clear Cancel			
Enable	Check to enable this entry.			
Protocol	Specify the transport layer protocol. It could be <b>TCP</b> , <b>UDP</b> , or <b>ALL</b> for selection.			
WAN Interface	Choose the WAN interface for such address mapping profile.			
WAN IP	Select an IP address (the selections provided here are set in <b>IP Alias</b> <b>List</b> of <b>Network</b> >> <b>WAN</b> interface). Local host can use this IP to connect to Internet. If you want to choose any one of the Public IP settings, you must			

	specify some IP addresses in the IP Alias List of the Static/DHCP Configuration page first. If you did not type in any IP address in the IP Alias List, the Public IP setting will be empty in this field. When you click <b>Apply</b> , a message will appear to inform you.
Private IP	Assign an IP address (e.g., 192.168.1.10) or a subnet to be compared with the Public IP address for incoming packets.
Subnet Mask	Select a value of subnet mask for private IP address.

# 4.4 Firewall

# 4.4.1 Basics for Firewall

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

### **Firewall Facilities**

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

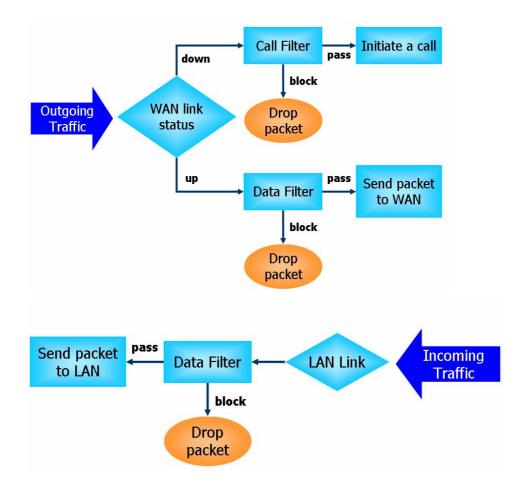
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

### **IP Filters**

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

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

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



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

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

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

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

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

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

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

1. SYN flood attack

9. SYN fragment



UDP flood attack
 ICMP flood attack
 Port Scan attack
 IP options
 Land attack
 Smurf attack
 Trace route

Fraggle attack
 TCP flag scan
 Tear drop attack
 Ping of Death attack
 ICMP fragment
 Unknown protocol

Below shows the menu items for Firewall.

Firewall						
⊳	General Setup					
⊳	Filter Setup					
•	DoS Defense					

### 4.4.2 General Setup

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

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

### **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.

neral Setup		
General Setup	Default Rule	
Call Filter	<ul> <li>Enable</li> </ul>	Start Filter Set Set#1 🔽
Data Filter	O Disable	
Data Filter	<ul> <li>Enable</li> <li>Disable</li> </ul>	Start Filter Set Set#2 💌
	ge incoming fragmented ct Security Firewall	UDP or ICMP packets ( for some games, ex. CS )
		UDP or ICMP packets ( for some games, ex. CS )
	ct Security Firewall	
☑ Enable Stri	ct Security Firewall OK Check Enak start filter se Check Enak	Cancel

# **Dray** Tek

	fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".
Enable Strict Security	Check the box to enable such function.
Firewall	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.

## **Default Rule Page**

Firewall >> General Setup

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.

General Setup	Default Rule		
Actions for defa	ult rule:		
Application		Action/Profile	Syslog
Filter		Pass 🐱	
Sessions Contro	I	67 / 60000	
Quality of Servi	<u>ce</u>	None 🖌	
Load-Balance p	olicy	Auto-Select 💌	
<u>User Manageme</u>	ent	None 🖌	
APP Enforceme	<u>nt</u>	None 💌	
URL Content Fil	ter	None 💌	
Web Content Fi	lter	None 💌	
Advance Settir	ıg	Edit	
	ſ	OK Cancel	

F

the filter rules.

Filter

Pass	*
Pass	
Block	

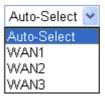
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.		
Quality of Service	Choose one of the QoS rules to be applied as firewall rule.		

For detailed information of setting QoS, please refer to the related section later.

None None Class 1 Class 2 Class 3 Default

**Load-Balance Policy** 

Choose the WAN interface for applying Load-Balance Policy.



**User Management** 

**APP Enforcement** 

Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall rule will be applied to the user/user group/all users specified here.

None	¥
None	
User Object	
[Create New User]	
User Group	
[Create New Group]	
ALL	

**Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.

Select an **APP Enforcement** profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [**Create New**] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the **APP Enforcement** profile selected here. For detailed information, refer to the section of **APP Enforcement** profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

URL Content FilterSelect one of the URL Content Filter profile settings<br/>(created in CSM>> URL Content Filter) for applying with<br/>this router. Please set at least one profile for choosing in<br/>CSM>> URL Content Filter web page first. Or choose<br/>[Create New] from the drop down list in this page to create a<br/>new profile. For troubleshooting needs, you can specify to<br/>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.

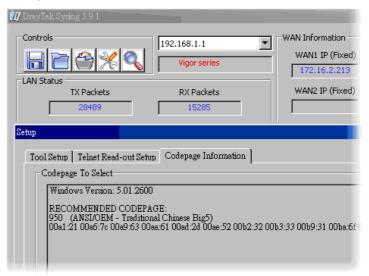
Web Content FilterSelect one of the Web Content Filter profile settings<br/>(created in CSM>> Web Content Filter) for applying with<br/>this router. Please set at least one profile for anti-virus in<br/>CSM>> Web Content Filter web page first. Or choose<br/>[Create New] from the drop down list in this page to create a<br/>new profile. For troubleshooting needs, you can specify to<br/>record information for Web Content Filter by checking the<br/>Log box. It will be sent to Syslog server. Please refer to<br/>section Syslog/Mail Alert for more detailed information.

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

irewall >> General Set	սթ		
Advance Setting			
Codepage	ANSI(1252)-Latin I		*
Window size:	65535		
Session timeout:	1440	Minute	

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

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



Window size – It determines the size of TCP protocol



 $(0\sim65535)$ . The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

**Session timeout** – Setting timeout for sessions can make the best utilization of network resources.

# 4.4.3 Filter Setup

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

Firewall >> Filter Setup	
--------------------------	--

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

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

```
Firewall >> Filter Setup >> Edit Filter Set
```

Filter Set 1 Comments : Default Call Filter Filter Rule Active Move Down Comments Move Up 1 Image: A start of the start of Block NetBios <u>Down</u> 2 UP Down 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 UP Next Filter Set None ΟK Clear Cancel

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

Filter Set 1 Ru	le 1

🗹 Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter:	Pass If No Further Match 💌	
Branch to Other Filter Set:	None 💌	
Sessions Control	0 / 60000	
MAC Bind IP	Non-Strict 💌	
Quality of Service	None 💌	
Load-Balance policy	Auto-Select 💌	
<u>User Management</u>	None 💌	
APP Enforcement:	None 💌	
URL Content Filter:	None 💌	
Web Content Filter:	None 💌	
Advance Setting	Edit	

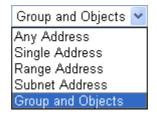
Check to enable the Filter Rule	Check this box to enable the filter rule.		
Comments	Enter filter set comments/description. Maximum length is 14- character long.		
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.		
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.		
	LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN		
	Note: RT means routing domain for 2nd subnet or other LAN.		
Source/Destination IP	Click Edit to access into the following dialog to choose the		



source/destination IP or IP ranges.

🗿 IP Address Edit - Microsoft Internet Explorer	
IP Address Edit	
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	
<u>IP Group</u>	None 💌
or <u>IP Object</u>	None 💌
or IP Object	None 1-RD Department
or IP Object	2-Financial Dept.
ОК	3-HR Department

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



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

Service Type

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

Type Edit - Microsoft Inter	net Explorer
rvice Type Edit	
Service Type	Group and Objects 👻
Protocol	TCP/UDP
Source Port	= 🔽 137 ~ 139
Destination Port	= 🔽 1 ~ 65535
Service Group	None 💌
or <u>Service Object</u>	None 💌
or Service Object	None 1-SIP
or Service Object	2-RTP
ſ	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  User defined Group and Objects
	<b>Protocol -</b> Specify the protocol(s) which this filter rule will apply to.
	Source/Destination Port –
	(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.
	( <i>!=</i> ) – 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.
	Unfragmented - 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	Strict - Make the MAC address and IP address settings

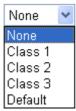


configured in **IP Object** for **Source IP** and **Destination IP** be bound for applying such filter rule.

No-Strict - no limitation.

#### **Quality of Service**

Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.



Load-Balance policy

**User Management** 

Choose the WAN interface for applying Load-Balance Policy.

Such item is available only when **Rule-Based** is selected in User **Management>>General Setup**. The general firewall rule will be applied to the user/user group/all users specified here.

None	*
None	
User Object	
[Create New User]	
User Group	
[Create New Group]	
ALL	

**Note:** When there is no user profile or group profile existed, **Create New User** or **Create New Group** item will appear for you to click to create a new one.

**APP Enforcement**Select an **APP Enforcement** profile for global IM/P2P<br/>application blocking. If there is no profile for you to select,<br/>please choose [**Create New**] from the drop down list in this<br/>page to create a new profile. All the hosts in LAN must follow<br/>the standard configured in the **APP Enforcement** profile<br/>selected here. For detailed information, refer to the section of<br/>**APP Enforcement** profile setup. For troubleshooting needs,<br/>you can specify to record information for IM/P2P by checking<br/>the Log box. It will be sent to Syslog server. Please refer to<br/>section **Syslog/Mail Alert** for more detailed information.

URL Content FilterSelect one of the URL Content Filter profile settings (created<br/>in CSM>> URL Content Filter) for applying with this router.<br/>Please set at least one profile for choosing in CSM>> URL<br/>Content Filter web page first. Or choose [Create New] from<br/>the drop down list in this page to create a new profile. For<br/>troubleshooting needs, you can specify to record information<br/>for URL Content Filter by checking the Log box. It will be<br/>sent to Syslog server. Please refer to section Syslog/Mail Alert<br/>for more detailed information.Web Content FilterSelect one of the Web Content Filter profile settings (created

FilterSelect one of the Web Content Filter profile settings (created<br/>in CSM>> Web Content Filter) for applying with this router.<br/>Please set at least one profile for anti-virus in CSM>> Web



**Content Filter** web page first. Or choose **[Create New]** from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

#### **Advance Setting**

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

ilter Set 1 Rule 1			
Advance Setting Codepage	ANSI(1252)-Latin I		*
Window size:	65535		
Session timeout:	1440	Minute	
DrayTek Banner:			
Strict Security Checkin	g		

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

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

👹 DrayTek Syslog 3.9.1		
	192.168.1.1 Vigor	WAN Information WAN1 IP (Fixed)
LAN Status TX Packets 28489	RX Packets	WAN2 IP (Fixed)
Setup		
Tool Setup   Telnet Read-out Setup Codepage To Select	Codepage Information	_
Windows Version: 5.01.2600 RECOMMENDED CODEPA 950 (ANSI/OEM - Tradition 00a1-21.00a672-008963300a	3E: al Chinese Big5) a.61 00ad.2d 00ae:52 00b2:32 00	h 3:33 በበክዓ:31 በበክa:6f በ

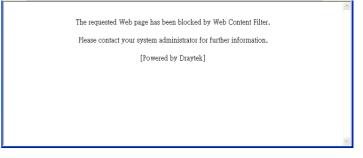
**Window size** – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance



will be. However, if the network is not stable, small value will be proper.

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

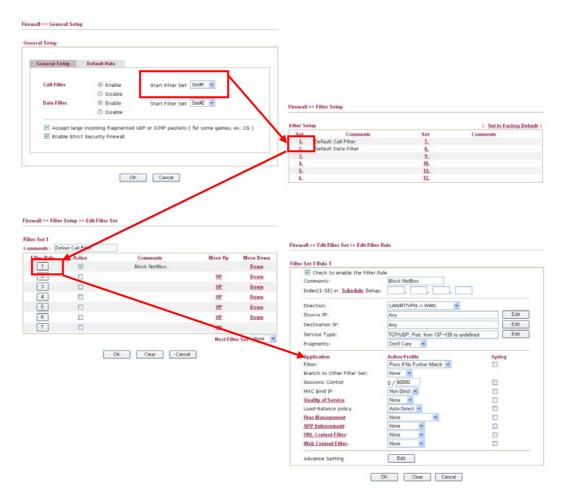
**DrayTek Banner** – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.



**Strict Security Checking** - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.

#### Example

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



# **Dray** Tek

### 4.4.4 DoS Defense

Firewall >> DoS defense Setup

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.

DoS defense Setup				
🗹 Enable DoS Defense 🛛 Select	All			
🔲 Enable SYN flood defense		Threshold	50	packets / sec
		Timeout	10	sec
🗌 Enable UDP flood defense		Threshold	150	packets / sec
		Timeout	10	sec
Enable ICMP flood defense		Threshold	50	packets / sec
		Timeout	10	sec
Enable Port Scan detection		Threshold	150	packets / sec
Enable Port Scan detection           Block IP options		Block TCP flag		
Block Land		Block Tear Drop	_	
Block Smurf		<ul> <li>Block Ping of Death</li> <li>Block ICMP fragment</li> </ul>		
📃 Block trace route				
📃 Block SYN fragment		Block UnknownProtocol		
– Block Fraggle Attack				
nable Dos Defense		ar All Cancel		
nobla Lloc Llotonco	Check the box	to activate the L	os Defe	nse Functionality.
navie Dus Delense				
elect All	Click this butte	on to select all th	e items l	isted below.

Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
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

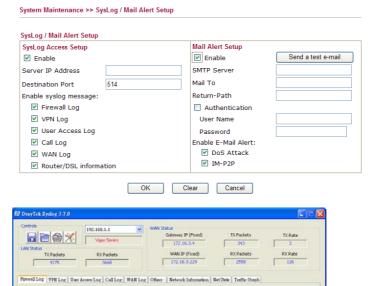
<b>Dray</b> Tek
-----------------

	coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
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



Diagle ICMD Example	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 Unknown Protocol	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.



remonger DoS ryn\_flood Block(10) 192.160.1.115,10605 -> 192.160.1.1,23 PR 6(tcp) lan 20 40 -S 394375 DoS ryn\_flood Block(10) 192.168.1.115 -> 192.168.1.1 PR 1(scmp) lan 20 60 isrmp.08

**Dray** Tek

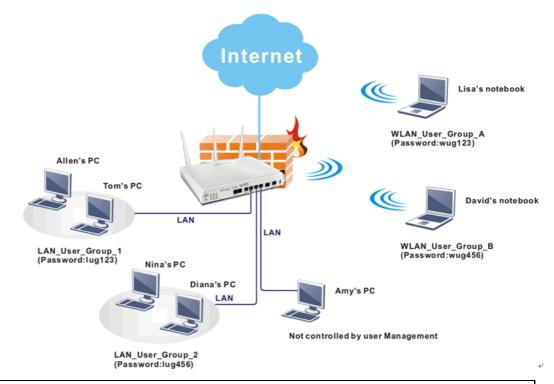
Jan 1 00:00 42 Jan 1 00:00 34

ADS. Status

Vigor

# 4.5 User Management

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



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

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



# 4.5.1 General Setup

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

Mode: Rule	-Based 💌		
Notice :			
	ment will refer to active rules in Da d formulations	ata Filter as whitelist	s and blacklists
	d firewall mode. the above lists will not be requirec	l for authentication.	
The firewall	rules policy will still valid.		
The firewall I 3. Otherwise, a	· · · · · · · · · · · · · · · · · · ·		
The firewall 3. Otherwise, a The firewall	rules policy will still valid. uthentication required for users no rules designated in the user profile'	s policy will still valio	ł.
The firewall 3. Otherwise, a The firewall Welcome Messa	rules policy will still valid. uthentication required for users no rules designated in the user profile ge (Max 255 characters)	s policy will still valio <u>Preview</u>	
The firewall 3. Otherwise, a The firewall Welcome Messa <body stats=":&lt;/td"><td>rules policy will still valid. uthentication required for users no rules designated in the user profile'</td><td>'s policy will still valio <u>Preview</u>  t'&gt;</td><td>ł.</td></body>	rules policy will still valid. uthentication required for users no rules designated in the user profile'	's policy will still valio <u>Preview</u>   t'>	ł.
The firewall 3. Otherwise, a The firewall Welcome Messa <body stats=":&lt;/td"><td>rules policy will still valid. uthentication required for users no rules designated in the user profile' <b>ge</b> (Max 255 characters) L&gt;<script language="javascrip&lt;/td&gt;&lt;td&gt;" policy="" s="" still="" valio<br="" will=""><u>Preview</u>  t'></td><td>ł.</td></tr></tbody></table></script></td></body>	rules policy will still valid. uthentication required for users no rules designated in the user profile' <b>ge</b> (Max 255 characters) L> <script language="javascrip&lt;/td&gt;&lt;td&gt;" policy="" s="" still="" valio<br="" will=""><u>Preview</u>  t'></td><td>ł.</td></tr></tbody></table></script>		

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.

**Rule-Based** –If you choose such mode, the router will apply the filter rules configured in **Firewall>>General Setup** and **Filter Rule** to the users.

### 4.5.2 User Profile

User Management >> User Profile

User Management >> User Profile

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

Profile	Name	Profile	<u>Set to Factory Defau</u> Name
<u>1.</u>	admin	17.	nume
<u>1.</u> 2.	System Reservation	<u>11.</u> <u>18.</u>	
<u>2.</u> <u>3.</u>	LAN_User_Group_1	<u>10.</u> 19.	
<u>4.</u>	WLAN_User_Group_A	<u>20.</u>	
<u>5.</u>	WLAN_User_Group_B	21.	
<u>6.</u>	·····	22.	
<u>7.</u>		23.	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

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.

Enable this account		
User Name	LAN_User_Group_1	
Password		
Confirm Password		
Idle Timeout	10 min(s) 0:Unli	mited
Max User Login	0 0:Unlimited	
External Server Authentication	None 💌	
Log	None 💌	
Pop Browser Tracking Window	$\checkmark$	
Authentication	🗹 Web 🗹 Alert Tool 🗹 Telnet	
Enable Time Quota	0 min(s) Refresh , Ad	d more 0 min
Index(1-15) in <u>Schedule</u> Setup:		

Enable this account	Check this box to enable such user profile.
User Name	Type a name for such user profile (e.g., <i>LAN_User_Group_1</i> , <i>WLAN_User_Group_A</i> , <i>WLAN_User_Group_B</i> , etc). When a

	user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
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.
Confirm Password	Type the password again for confirmation.
Idle Timeout	If the user is idle over the limitation of the timer, the <b>network connection will be stopped for such user.</b> By default, the Idle Timeout is set to 10 minutes.
Max User Login	Such profile can be used by many users. You can set the limitation for the number of users accessing Internet with the conditions of such profile. The default setting is 0 which means no limitation in the number of users.
Policy	It is available only when <b>User-Based</b> mode selected in <b>User</b> <b>Management&gt;&gt;General Setup</b> .

Default	*
Default	
[Create New Policy]	

**Default** – If you choose such item, the filter rules pre-configured in **Firewall** can be adopted for such user profile.

**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.

irewall >> 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	
Fragments:	Don't Care	

For the detailed configuration, simply refer to **Firewall>>Filter Rule**. The firewall filter rules that are not selected in **Firewall>>General>>Default rule** can be available for use in **User Management>>User Profile**.

**External Service** 

The router will authenticate the dial-in user by itself or by



Vigor2850 Series User's Guide

Authentication

external service such as LDAP server or Radius server. If LDAP or Radius is selected here, it is not necessary to configure the password setting above.

Time of login/log out, block/unblock for the user(s) can be sent to and displayed in Syslog. Please choose any one of the log items to take down relational records for the user(s).

None	*
None	
LDAP	
Radius	

None None Login Event All **Pop Browser Tracking** If such function is enabled, a pop up window will be displayed Window on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection. Authentication Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication. Web – If it is selected, the use can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in **User Management >> General Setup**) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router. Alert Tool – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. **Telnet** – If it is selected, the user can use Telnet command to perform the authentication job. **Enable Time Quota** Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet. Refresh – Click this button to recalculate the time quota. Add – Click this box to set the time quota for such profile. Index (1-15) in Schedule You can type in four sets of time schedule for your request.

Log



Setup

All the schedules can be set previously in **Application** >> **Schedule** web page and you can use the number that you have set in that web page.

## 4.5.3 User Group

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

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	Selected User Objects(Max 32 Objects)
1-admin 2-System Reservation 3-LAN_User_Group_1 4-WLAN_User_Group_A 5-WLAN_User_Group_B	>> ((
	OK Clear Cancel
lame	Type a name for this user group.
vailable 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.
elected Keyword	Click button to add the selected user objects in this



Objects

box.

# 4.5.4 User Online Status

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

Current	Time : 10-27 0	6:24:50	Refresh Seconds: 10 💌 Page: 1 💌   Refresh			
Index 1	Active User ↔ admin	IP Address 192.168.1.10	Last Login Time 10-27 03:57:23	Expired Time Unlimited	Idle Time Unlimited	Action Block Logout
			<u> </u>		Т	otal Number : :
			atically.	n 🗸		
ofnoch		Refre	sh Seconds: 1 10 15 30	5 )	anually	
efresh	ı	Refre Click	sh Seconds: 1 10 15 30 this link to refres	h this page ma	anually.	
ndex		Refre Click Displa	sh Seconds: 1 10 15 30 this link to refres	h this page mathematical flow.	·	
		Refre Click Displa Displa can cli	sh Seconds: 1 10 15 30 this link to refres	h this page mathematical flow. the data flow. the connect to V	igor route	
ndex	User	Refre Click Displa Displa can cli setting	sh Seconds: 1 1 15 30 this link to refres by the number of ay the users which ick the link under	h this page ma the data flow. n connect to V the username er.	igor route	
ndex active l P Add	User	Refre Click Displa Displa can cli setting Displa	sh Seconds: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	h this page ma the data flow. n connect to V the username er. of the device.	igor route to open t	he user prof
ndex ctive l P Add ast Lo	User ress	Refre Click Displa Can cli setting Displa time.	sh Seconds: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	h this page ma the data flow. n connect to V the username er. of the device. that such user	igor route to open t connects	he user profi
ndex ctive l P Add ast Lo	User ress ogin Time I Time	Refre Click Displa Displa can cli setting Displa time. Displa user.	sh Seconds: 1 this link to refrest this link to refrest the number of the users which the link under g page for that use the IP address the login time to the login the login to the login time to the login the login to the login the login to the login time to the login to the login time to the login time to the login time to the login to the login the login to the login to the login to the login the logint to the login the l	h this page ma the data flow. the username er. of the device. that such user	vigor route to open t connects ork connec	he user profit to the router ction for the
ndex ctive I P Addr ast Lo xpired	User ress ogin Time I Time	Refre Click Displa Displa can cli setting Displa time. Displa user. Displa	sh Seconds: 1 this link to refrest this link to refrest the number of the users which the link under g page for that use the IP address the login time to the login time to	h this page mathematical flow. h connect to V the username er. of the device. that such user that such user that such user that such user	vigor route to open t connects ork connec uch profile	he user profi to the router ction for the e.
ndex ctive l P Addr ast Lo xpirec dle Tir	User ress ogin Time I Time	Refre Click Displa Displa can cli setting Displa time. Displa user. Displa <b>Block</b>	sh Seconds: 1 this link to refrest this link to refrest this link to refrest the number of the users which ick the link under g page for that use the login time to the login time to the the expired time the idle timeou	h this page mathematical flow. In connect to V the username er. of the device. that such user that such user that such user that setting for such that setting for such the setting for such the set for such the set for such that setting for su	vigor route to open t connects ork connec uch profile	he user profi to the router ction for the e.



# 4.6 Objects Settings

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

Objects Setting	
IP Object	
IP Group	
Service Type Object	
Service Type Group	
Keyword Object	
Keyword Group	
File Extension Object	

# 4.6.1 IP Object

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

Objects Setting >> IP Ob	ject
--------------------------	------

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   65</u>	<u>.96   97-128   129-160   161</u>	<u>192</u> >>	<u>Next</u> >>

**Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Object

Profile Index : 11	
Name:	RD Department
Interface:	Any 🔽
Address Type:	Range Address 💌
Mac Address:	
Start IP Address:	192.168.1.65
End IP Address:	192.168.1.69
Subnet Mask:	0.0.0.0
Invert Selection:	
Name	OK         Clear         Cancel           Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface.
	Any Any LAN/RT/VPN WAN For example, the <b>Direction</b> setting in <b>Edit Filter Rule</b> will

ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page. **Address Type** Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP 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 IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.

ojects Setting >> IP Object			
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>	

## 4.6.2 IP Group

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

Ob	ects	Setting	>>	IP	Group	
~ ~	00.00	Sound			0.040	

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>	

**Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

Ob	iects	Setting	>>	IP	Group
~	10.010	ooung			

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



# 4.6.3 Service Type Object

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

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

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

### **Set to Factory Default** Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Object Setup

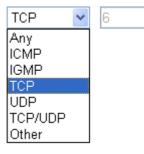
Name	WWW
Protocol	TCP 🖌 6
Source Port	= 🖌 1 ~ 65535
Destination Port	= 💙 80 ~ 80

Name

Protocol

Type a name for this profile.

Specify the protocol(s) which this profile will apply to.



**Source/Destination Port** Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.



(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.

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

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

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

Below is an example of service type objects settings.

Service	e Type	Obj	ject	Profi	es:

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

## 4.6.4 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>	

**Set to Factory Default** Clear all profiles.

Vigor2850 Series User's Guide

Click the number under Index column for settings in detail.

Objects Setting >> Service Type (	Group Setup
Profile Index : 1	
Name:	VolP
Available Service Type	e Objects Selected Service Type Objects
1-SIP 2-RTP	»       «       OK     Clear       Cancel
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.

### 4.6.5 Keyword Object

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

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 Object

**Set to Factory Default** Clear all profiles.



Click the number under Index column for setting in detail.

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
	OK Clear Cancel
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.

### 4.6.6 Keyword Group

Objects Setting >> 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**.

word Group Ta	ole:		Set to Factory Defa
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>	

Set to Factory Default

Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Keyword-1 2-keyword-2	» ((
2	OK Clear Cancel
Name	Type a name for this group.
Available Keyword Dbjects	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 Dbjects	Click button to add the selected Keyword objects in this box.

### 4.6.7 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 >> F	ile 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>	

**Set to Factory Default** Clear all profiles.

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

Profile Index: 1	Pro	ofile Name:					
Categories			Fi	le Extensi	ons		
Image Select All Clear All	.bmp .pct	□.dib □.pcx	□.gif □.pic	.jpeg .jpeg	□.jpg □.png	□.jpg2 □.tif	□.jp2 □.tiff
Video Select All Clear All	🗌 .asf 🗌 .qt	🗌 .avi 🗌 .rm	.mov .wmv	.mpe	.mpeg	.mpg .3gpp2	.mp4
Audio Select All Clear All	🗌 .aac 🗌 .ra	.aiff .ram	🗌 .au 🗌 .vox	.mp3 .wav	□.m4a □.wma	🗌 .m4p	🗌 .ogg
Java Select All Clear All	□.class □.jse	🗌 .jad 🗌 .jsp	□.jar □.jtk	🗌 .jav	🗌 .java	.jcm	🗌 .js
ActiveX Select All Clear All	□ .alx □ .viv	.apb .vrm	.axs	.ocx	.olb	.ole	.tlb
Compression Select All Clear All	.ace .rar	🗌 .arj 🗌 .sit	.bzip2	.bz2	.cab	.gz	.gzip
Executation Select All Clear All	.bas .scr	🗌 .bat	.com	.exe	.inf	.pif	.reg
		ок	Clear	Cancel			

### Profile Name

Type a name for this profile.

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

# 4.7 CSM Profile

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

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

### **APP Enforcement Filter**

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

### **URL Content Filter**

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

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

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

### Web Content Filter

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

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

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





## **4.7.1 APP Enforcement Profile**

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

PP Enforcement P	rofile 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

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 Enf	orcement Profile			
Profile Index : 1	Profile Name:			
IM	P2P	Protocol Misc		
Select All	Clear All			
		Protocol		
DNS	FTP	HTTP	IMAP	IRC IRC
NNTP NNTP	🗌 РОРЗ	SMB	SMTP	SNMP
SSH	SSL/TLS	TELNET	MSSQL	MySQL
Oracle	PostgreSQL	🗌 Sybase	DB2	🔲 Informix
Profile Name	T	OK Cance ype a name for the CS		
Select All	С	lick it to choose all of	the items in thi	s page.
Clear All	U	ncheck all the selected	d boxes.	
		an be applied in the <b>Fi</b> as the standard for th		

Below shows the items which are categorized under **IM**.

CSM >> APP Enforcement Profile

IM	P2P	Protocol	Misc		
Select All	Clear All				
		Advanced	Management		
Activity / A	pplication	MSN	YahooIM	AIM(<=	v5.9) ICQ
Log	lin				
Mess	age				
File Tra	ansfer				
Gan	ne				
Conference(\	/ideo/Voice)				
Other Ac	tivities				
	IM	Application			VoIP
🗌 AIM6/7	🗌 QQ/ТМ	🗌 iChat	🗌 Jabber/G	oogleTalk	
🔲 GoogleChat	🗌 XFire	🗌 GaduGadu	📃 Paltalk		🗌 Skype 🔲 Kubao
🗌 Qnext	POCO/PP365	🗌 AresChat	🗌 AliWW		🔲 Gizmo 🔲 SIP/RTP
□кс	🗌 Lava-Lava	ICU2	🔲 iSpQ		🔲 TelTel 🔲 TeamSpea
UC	🗌 MobileMSN	🔲 BaiduHi			
		/eh IM ( * = mo	re than one addre	<<)	
	eMessenger	WebMSN	meebo*	eBuddy	ILovelM*
<b>—</b>	ICO Java*	ICQ Flash*	goowy*	<u>IMhaha</u>	
🗌 WebIM URLs	IMUnitive*	Wablet*	mabber*	MSN2G	<u>D* KoollM</u>
	MessengerFX*	<u>MessengerAdi</u>	<u>ctos WebYahoolM</u>		

The items categorized under P2P -----

	Profile Name:				
IM	P2P	Protocol	Misc		
Select All	Clear All				
Prot	ocol	-		Applications	
🗌 SoulSee	k	SoulSeek			
🗌 eDonkey	(	eDonkey,	eMule, Sharea	aza	
🗌 FastTrac	ck	KazaA, Be	arShare, iMes	h	
🗌 OpenFT		KCeasy, F	ilePipe		
🗌 Gnutella				hareaza, Foxy, KCea	зѕу
🗌 OpenNap	p _	•	(Nap, WinLop		
BitTorrei	nt	BitTorrent	, BitSpirit, Bit	Comet	
🗌 Winny		Winny, W	inMX, Share		
		Otho	r P2P Applicat	lane	
Xunlei	🗌 Vaga				Clubbox
Ares	n ezPe		PP305	Huntmine	Kuwo
Ares		er	Panuo	Huntmine	LIKUWU
M >> APP Enfo	gorized under I	 Misc	K Can	cel	
	Profile Name:	Misc	K Can	cel	
M >> APP Enfo ofile Index : 1 IM	Profile Name:		K Can	cel	
M >> APP Enfo ofile Index : 1	Profile Name:	Misc		cel	
M >> APP Enfo ofile Index : 1 IM	Profile Name:	Misc Protocol		cel	
M >> APP Enfo ofile Index : 1 IM	Profile Name:	Misc Protocol	Misc	cel	
M >> APP Enfo ofile Index : 1 IM Select All	Profile Name: Profile Name: P2P Clear All	Misc Protocol	Misc Tunneling		VNN
M >> APP Enfo ofile Index : 1 IM Select All	Profile Name: Profile Name: P2P Clear All PGPNet MS TEREE	Misc Protocol	Misc Tunneling ITP Proxy	Tor	

		Streaming		
MMS	RTSP	TVAnts	PPStream	PPTV
📃 FeiDian	UUSee	NSPlayer 🗌	PCAST	TVKoo
🔲 SopCast	🗌 UDLiveX	🗌 TVUPlayer	MySee	🔲 Joost
🔲 FlashVideo	SilverLight	🔲 Slingbox	QVOD 🗌	
		Remote Contro	ol	

	🗌 Radmin	SpyAnywhere ShowMyPC	LogMeIn
🗌 TeamViewer	🔲 Gogrok	🗌 RemoteControlPro 🔲 CrossLoop	🔲 WindowsRDP
pcAnywhere 🗌	🔲 Timbuktu	🗌 WindowsLiveSync 🔲 SharedView	

		web HD		
HTTP Upload	🗌 HiNet SafeBox	MS SkyDrive	🔲 GDoc Uploader	🗌 ADrive
MyOtherDrive	🗌 Mozy	🔲 BoxNet	OfficeLive	

OK Cancel

## 4.7.2 URL Content Filter Profile

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

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

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

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

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

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

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

CSM >> URL Content Filter Profile

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

OK

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

#### CSM >> URL Content Filter Profile

Profile Name:	
Priority:	Both : Pass Vone Vone Vone Vone Vone Vone Vone Vone
1.URL Access	; Control
Enal	ole URL Access Control 💦 Prevent web access from IP address
Actio	on: Group/Object Selections
Pass	Edit
Enal Actio Pass	
	OK Clear Cancel
rofile Name	Type a name for the CSM profile.
riority	It determines the action that this router will apply.
	<b>Both: Pass</b> – The router will let all the packages that match

**Both:** Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.

**Both:Block** –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.

**Either: URL Access Control First** – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.

**Either: Web Feature First** –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

Both : Pass	*
Both : Pass	
Both : Block	
Either : URL Access Control First Either : Web Feature First	
Either : Web Feature First	

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.



### **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. *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 keyword set here, it will be processed with reverse action.

Action:



**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.

192.168.1.1/doc/cfkwgob.htm		
Object/Group Edit		
Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
ОК	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.





### 4.7.3 Web Content Filter Profile

CSM >> 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.

Setup Query Server	auto-selected		Find more	
Setup Test Server	auto-selected		Find more	
Neb Content Filter Profil	e Table:		Set to Factory Defau	
Profile	Name	Profile	Name	
<u>1.</u>	Default	<u>5.</u>		
<u>2.</u>		<u>6.</u>		
<u>3.</u>		<u>7.</u>		
<u>4.</u>		<u>8.</u>		
	· · · ·		Cache : L1 + L2 Cache	
•	) pr> The reque ized with %CL% <br ntact your system &amp;</br 	ested Web page >has been blocked by	from %SIP% to %URL% 7 %RNAME% Web Content	
<body><center> <kody><center> <kody><center> <kody> is categoriFilter.Please cor</kody></center></kody></center></kody></center></body>	) pr> The reque ized with %CL% <br ntact your system &amp;</br 	ested Web page >has been blocked by	from %SIP% to %URL% 7 %RNAME% Web Content	
<body><center> <kody><center> <kody><center> <kody> is categoriFilter.Please cor</kody></center></kody></center></kody></center></body>	) pr> The reque ized with %CL% <br that your system a c&gt;</br 	ested Web page >has been blocked by administrator for fu	from %SIP% to %URL% 7 %RNAME% Web Content	

Setup Test Server It is recommended for you to use the default setting, auto-selected.



Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.
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:	Gi	roup/Object Selections					
Block 💙	Edit						
Action: Block 💙							
Groups	Categories						
Child Protection	Alcohol & Tobacco	Criminal Activity	🗹 Gambling				
Select All	✓ Hate & Intolerance	✓ ✓ Illegal Drug	✓ Nudity				
Clear All	✓ Porn & Sexually	Violence	Weapons				
	School Cheating	Sex Education	✓ Tasteless				
	Child Abuse Images						
Leisure		_	_				
Select All	Entertainment	Games	Sports				
Clear All	Travel	Leisure & Recreation	🗌 Fashion & Beauty				
Business							
Select All	Compromised	Dating & Personals	Education				
Clear All	Finance	Government	 Health & Medicine				
	News	 Non-profits & NGOs	 Personal Sites				
	Politics	 Real Estate	 Religion				
	 Restaurants & Dining		Translators				
	General	Cults	Greeting cards				
	Image Sharing	Network Errors	Parked Domains				
	Private IP Addresses	Uncategorised Sites					

**Black/White List** Enable – Activate white/black list function for such profile. Group/Object Selections - Click Edit to choose the group or object profile as the content of white/black list. **Pass** - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **Block** - **restrict** accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. Action Pass - allow accessing into the corresponding webpage with the categories listed on the box below. Block - 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.

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.



# 4.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bai	ndwidth Management
	Sessions Limit
₽	Bandwidth Limit
₽	Quality of Service

Bandwidth Management >> Sessions Limit

### 4.8.1 Sessions Limit

Log

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.

sions Limit			
🔘 Enable 💿 Disable			
Default Max Sessions: 100			
Limitation List			
Index Start IP	End IP	Max Sessions	
Specific Limitation Start IP: Maximum Sessions:	End IP:		
	Add Edit	Delete	
inistration Message (Max 256	characters)		Default Message
have reached the maximu or more applications to inistrator for further i	m number of permit allow further Inte		
e Schedule			
Index(1-15) in <u>Schedule</u> S	ətup:,	,,	
Note: Action and Idle Timed	ut settings will be ign	ored.	

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

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	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.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
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.
	<b>Default Message</b> – Click this box to display the default message.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
	F
	Click <b>Default Message</b> to display the default message on the screen.

### 4.8.2 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.

	y to 2nd Subnet 💿 Disable	
Default TX Limit: 200	Kbps Default RX Limit: 800 Kbps	
Limitation List		
Index Start IP	End IP TX limit RX limit	Shared
Specific Limitation		
Start IP:	End IP:	
		S
●Each ○Shared ○	TX Limit: Kbps RX Limit: Kbp	
● Each ○ Shared		
● Each ○ Shared ○	Add Edit Delete	
● Each ○ Shared	Add Edit Delete	

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

Enable	Click this button to activate the function of limit bandwidth. <b>Apply to 2<sup>nd</sup> Subnet</b> – Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup.
Disable	Click this button to close the function of limit bandwidth.
Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
Each /Shared	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

Bandwidth Management >> Bandwidth Limit

	RX limit fields.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allow you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
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.

### 4.8.3 Quality of Service

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

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

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

There are two components within Primary configuration of QoS deployment:

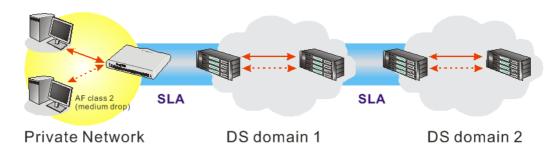
- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

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

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

Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

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



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

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

General Setup   <u>Set to Factory Default</u>										
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	<u>Setu</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
Class Rule Index Name Rule Service Type							ype			
Class	s 1							<u>Edit</u>		
Clas	s 2							<u>Edit</u>	<u>Edit</u>	
Class	s 3							Edit		

Bandwidth Management >> Quality of Service

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.

```
Bandwidth Management >> Quality of Service
```

INT ON	ine Statisti	cs		Refresh Interv	al: 5 ≚ seconds	Refres
Index	Direction	Class Name	Reserved-bandw	idth Ratio Out	bound Throughput (	(Bytes/sec)
1	OUT		25%		0	
2	OUT		25%		0	
З	OUT		25%		0	
4	OUT	Others	25%		0	
		Ot	hers 0	5	10 (Bps)	

### **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 Manage	ement >> Quality of Service	
WAN2 General Set	•	
w	/AN Inbound Bandwidth	10000 Kbps
w	/AN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP B	andwidth Control	Limited_bandwidth Ratio 25 %
Outbound TC	P ACK Prioritize	
	OK Clear	Cancel
Enable the QoS	<b>Control</b> The factory default for	r this setting is checked.
	Please also define which apply to.	ch traffic the QoS Control settings will

**IN-** apply to incoming traffic only.

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

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

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

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

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

General	General Setup   <u>Set to Factory Defa</u>									
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	<u>Setu</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

Class Rule

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

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

Bandwidth	n Manageme	nt >> Quality of Servi	ce		
Class Inde	ex #1				
Name 1	Fest				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
		2	Add Edit Delet	e	
		٢	OK Cancel	]	

For adding a new rule, click **Add** to open the following page. Bandwidth Management >> Quality of Service

Rule Edit	
🗹 ACT	
Local Address	Any Edit
Remote Addres	Any Edit
DiffServ CodeP	t ANY 💌
Service Type	ANY
Note: Please ch	ose/setup the <u>Service Type</u> first.
	OK Cancel
ACT	Check this box to invoke these settings.
Local Address	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.

**Remote Address** Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule.

Edit

### It allows you to edit source address information.

Address Type	Subnet Address 🐱
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0

Address Type – Determine the address type for the source address.

For Single Address, you have to fill in Start IP address.

For **Range Address**, you have to fill in Start IP address and End IP address.

For **Subnet Address**, you have to fill in Start IP address and 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.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Bandwidth Management >> Quality of Service Class Index #1 Game Name DiffServ NO Status Local Address Remote Address Service Type CodePoint 1 () Active IP precedence 2 SYSLOG(UDP:514) Any Any AF Class1 (Low FTP(TCP:20)  $2 \bigcirc$ Active 192.168.1.15 192.168.1.65 Drop) Add Edit Delete

ΟK

Cancel

## Edit the Service Type for Class Rule

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

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

General Setup   <u>Set to Factory Defa</u>								<u>efault</u>		
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	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>

Class Rule

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

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

Bandwidth Management >> Quality of Service

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

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	ТСР 🖌 6
Port Configuratio	n
Туре	💿 Single 🔘 Range
Port Numb	er 0 – 0
	OK Cancel
Service Name	Type in a new service for your request.
Service Type	Choose the type (TCP, UDP or TCP/UDP) for the new service
Port Configuration	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.

**Port Number** – Type in the starting port number and the end

porting number here if you choose Range as the type.

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.

# 4.9 Applications

Below shows the menu items for Applications.

Ар	olications
- 🕨	Dynamic DNS
- 🕨	Schedule
- 🕨	RADIUS
- 🕨	UPnP
- 🕨	IGMP
►	Wake on LAN

# 4.9.1 Dynamic DNS

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

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

### Enable the Function and Add a Dynamic DNS Account

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

Dynamic DNS Set	սթ		Set to	Factory Default
Enable Dynamic DNS Setup			View Log	Force Update
Auto-Update ini	terval 14400	Min(s) (1~14400)		
Accounts:				
Index	WAN	nterface	Domain Name	Active
<u>1.</u>	WAN	I1 First		×
<u>2.</u>	WAN	I1 First		×
<u>3.</u>	WAN	I1 First	,	×
<u> </u>		OK	Clear All	
Enable Dyna Setup	mic DNS	Check this bo	x to enable DDNS function.	
Set to Factory	y Default	Clear all profi	les and recover to factory se	ttings.

Applications >> Dynamic DNS Setup



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.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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

Applications >> D	vnamic DNS S	Setun >> Dv	mamic DNS /	Account Setun
Applications PP D	ynanne bha a	cup Dy	manne bii 5 /	account Setup

Index : 1	
🗹 Enable Dynamic DNS	Account
WAN Interface	WAN1 First 💌
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chronic6853 dyndns.info 🖌
Login Name	chronic6853 (max. 23 characters)
Password	(max. 23 characters)
🔲 Wildcards	
🔲 Backup MX	
Mail Extender	
Enable Dynamic D Account	OKClearCancelNSCheck this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	WAN1/WAN2/WAN3 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3 Only - While connecting, the router will use WAN1/WAN2/WAN3 as the only channel for such account.

WAN1	First	*
WAN1	First	
WAN1		
WAN2		
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 features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

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.

### 4.9.2 Schedule

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

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

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

### Applications >> Schedule

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

#### **Set to Factory Default**

Clear all profiles and recover to factory settings.

IndexClick the number below Index to access into the setting page of<br/>schedule.StatusDisplay 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, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Enable	e Schedule Setup	
	Start Date (yyyy-mm-dd)	2000 🕶 - 1 💌 - 1 💌
	Start Time (hh:mm)	0 💌 : 0 💌
	Duration Time (hh:mm)	0 💌 : 0 💌
	Action	Force On
	Idle Timeout	minute(s).(max. 255, 0 for default)
	How Often	
	Once	
	Weekdays	
	🗌 Sun 🗹 Mon 🗹	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat

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

## 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.

## **4.9.3 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	ons >> RADIUS		
RADIUS Setup			
🗹 Enable			
Server IP Ac	ldress		
Destination	Port 1812		
Shared Secr	et		
Confirm Sha	red Secret		
	OK Clear Cancel		
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.		

## 4.9.4 UPnP

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

Applications >> UPnP

UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

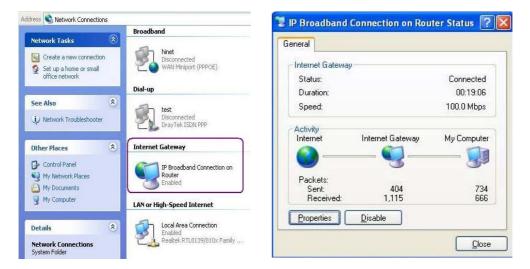
**Note:** If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK	Clear	Cancel

## **Enable UPNP Service**

Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



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



eneral	Services		
Connect to the Internet using:	Select the services running on your network that Internet users can access.		
🧐 IP Broadband Connection on Router	Services		
This connection allows you to connect to the Internet through a shared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>☑ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>☑ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>☑ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>		

The reminder as regards concern about Firewall and UPnP

## Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

## **Security Considerations**

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

# 4.9.5 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.

IGMP  IGMP Proxy WAN1  IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Pro will access any multicast group. But this function take no affect when Bridge Mode is e Enable IGMP Snooping Enable IGMP Snooping, multicast traffic is only forwarded to ports that have member: Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast to	enabled.
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Pro will access any multicast group. But this function take no affect when Bridge Mode is e Enable IGMP Snooping Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members	enabled.
will access any multicast group. But this function take no affect when Bridge Mode is a Enable IGMP Snooping Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members	enabled.
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have member	s of that group.
	s of that group.
	traffic
	and the second
OK Cancel	
	Refrest
Working Multicast Groups	
Index Group ID P1 P2 P3	P4

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.
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.
Refresh	Click this link to renew the working multicast group status.

## 4.9.6 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 LA	4			
	Note: Wake on L can wake up thr		I <u>P to MAC</u> function, only bind	led PCs
	Wake by: IP Address:	MAC Address 💌		
	MAC Address: <b>Result</b>		: Wake Up!	
				<
Wake by		choose Wake by MAC address of	de for you to wake up th MAC Address, you hav the host in MAC Addre IP Address, you have to	e to type the correct ss boxes. If you
		Wake by:	MAC Address V MAC Address IP Address	
IP Address		IP to MAC will	s that have been configu- be shown in this drop d the drop down list that y	own list. Choose the
MAC Addr	ess	Type any one of	the MAC address of the	bound PCs.

Appl	ication	>>	Wake	on	LAN
				· · ·	

Wake Up

Note: Wake on L can wake up thr	.AN cooperate with <u>Bind IP to MAC</u> function, only binded PCs rough IP.
Wake by:	MAC Address 🔽
IP Address:	💙
MAC Address:	: : : : Wake Up!
Result	

Click this button to wake up the selected IP. See the following

figure. The result will be shown on the box.



# 4.10 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN and Remote Access.

VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
IPSec General Setup
IPSec Peer Identity
Remote Dial-in User
LAN to LAN
Connection Management

## 4.10.1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environ	nment				
LAN-to-LAN VPN Client Mode	Selection:	Route Mode	*		
Please choose a LAN-to-LAN I	Profile:	[Index] [	Status] [Nam	e] 🔽	
<b>Note:</b> For a typical LAN-to-LAN If the remote network is the subnet and then selv If in doubt then select R	expecting only a ect NAT mode.			configured to	route
		< Back	Next >	Finish	Cancel
LAN-to-LAN Client Mode Selection	Choose the cl Route Mode/		– If the reme	ote network	only allows
	you to dial in otherwise ple	-	-		node,
	Route Mode			•	



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

[Index] 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	[Status]	[Name] ??? ??? ??? ??? ??? ??? ??? ??? ??? ?	^
2	v	222	
3	x x x	222	
4	x	222	
5	x	222	
16	x	222	
17	x x x x x	222	
8	x	222	
19	x	222	
10	x	222	
11	x	222	
12	x	???	
13	x	???	
14	x x x x x x	???	
15	х	???	
16	x x x x x	???	
17	X	???	
18	x	???	
19	x	???	
20	x	???	
21	x x x x x	???	
22	х	???	
23	х	???	
24	x	???	
25	x	???	
26	x	???	
27	x x x x	???	
28	x	777	
29	X	777	×

When you finish the mode and profile selection, please click Next to open the following page.

```
VPN and Remote Access >> VPN Client Wizard
```

Security ranking (1 is the highest; 5 is the 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>	<ol> <li>PPTP (None Encryption)</li> <li>L2TP</li> <li>IPSec</li> <li>L2TP over IPSec</li> <li>PPTP (Encryption)</li> </ol>
PPTI PPTI IPSe L2TF L2TF	

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	
Iternative 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

VPN Client L2TP Settings	
Profile Name	VPN-1
VPN 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
Username	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0
(	< Back Next > Finish Cancel

• 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 a.g. 5551234, draytek.com or 123.45.67.89)	
E 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	
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

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.



	<ul> <li>WAN1 First</li> <li>WAN1 First</li> <li>WAN1 Only</li> <li>WAN2 First</li> <li>WAN2 Only</li> <li>WAN1 First - While connecting, the router will use</li> <li>WAN1 as the first channel for VPN connection. If</li> <li>WAN1 fails, the router will use another WAN interface instead.</li> <li>WAN1 Only - While connecting, the router will use</li> <li>WAN1 as the only channel for VPN connection.</li> <li>WAN2 First - While connecting, the router will use</li> <li>WAN2 as the first channel for VPN connection. If</li> <li>WAN2 as the first channel for VPN connection. If</li> <li>WAN2 fails, the router will use another WAN interface instead.</li> <li>WAN2 fails, the router will use another WAN interface instead.</li> <li>WAN2 only - While connecting, the router will use</li> <li>WAN2 only - While connecting, the router will use</li> <li>WAN2 as the only channel for VPN connection.</li> </ul>
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. <b>Pre-Shared Key-</b> Specify a key for IKE authentication.
	<b>Confirm Pre-Shared Key-</b> Confirm the pre-shared key.
Digital Signature (X.509)	Click <b>Digital Signature</b> to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local Certificate.</b> Otherwise, the setting you choose here will not be effective.
	<b>Peer ID</b> – Choose the peer ID selection from the drop down list.
	Local ID – Choose Alternative Subject Name First or Subject Name First.
IPSec Security Method	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
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.

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

#### VPN and Remote Access >> VPN Client Wizard

Remote Network Mask:	Digital Signature (X.509) AH-SHA1 192.168.1.6		
	255.255.255.0		
Click <b>Back</b> to modify changes if neces: Ind proceed to the following action:	sary. Otherwise, click <b>Finish</b> to save the current settings		
	● Go to the VPN Connection Management.		
	🔘 Do another VPN Client Wizard setup.		
	🔘 View more detailed configurations.		

	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.

# 4.10.2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

VPN and Remote Access >> VPN S			
VPN Server Mode Selection:		Site to Site VPN (LAN-to-LAN)	
Please choose a LAN-to-LAN F	rofile:	[Index] [Status] [Name]	
Please choose a Dial-in User A	ccounts:	[Index] [Status] [Name]	
Allowed Dial-in Type:		PPTP IPSec L2TP with IPSec Policy None	
		< Back Next > Finish Cancel	
VPN Server Mode Selection	Site to automa Remote maintai be auth Site to Site to	e the direction for the VPN server. Site VPN – To set a LAN-to-LAN profile trically, please choose Site to Site VPN. e Dial-in User –You can manage remote access by ining a table of remote user profile, so that users can enticated to dial-in via VPN connection. Site VPN (LAN-to-LAN) Site VPN (LAN-to-LAN) e Dial-in User (Teleworker)	
Please choose a LAN-to-LAN Profile	(LAN-t	em is available when you choose <b>Site to Site VPN</b> to-LAN) as VPN server mode. There are 32 VPN s for users to set.	

[Index] 1 2 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	[Status]	[Name] ??? ??? ??? ??? ??? ??? ??? ??? ??? ?	^
5	x	222	
2	x x	111	
3	x	222	
4	x x	222	
5	X		
6	x		
12	x x x x x	777	
8	x	277	
19	x	222	
10	X	???	
11	X	???	
12	x x	???	
13	x	???	
14	x	???	
15	x	???	
16	x x	???	
17	х	???	
18	х	???	
19	x	???	
20	x	???	
21	x x x	???	
22	x	222	
23	x	222	
24	x x	222	
25	x	222	
26	×	222	
27	x x	222	
28	x	222	
29	x	222	~
27	A.		

Please choose a Dial-in User Accounts

**Allowed Dial-in Type** 

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.

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).



Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected.

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

Here we take the examples of choosing **Remote-Dial-in User** as the **VPN Server Mode**.



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

VPN and Remote Access >> VPN Server Wizard

PPTP / L2TP / L2TP over IPSec Authenti	cation			
Username		???		
Password				
Peer IP/VPN Client IP				

• When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP** with Policy (Nice to Have/Must), you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting	
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	
IPSec / L2TP over IPSec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🔲 Digital Signature (X.509)	
Peer ID	None 🗸
Peer IP/VPN Client IP	192.168.1.99
Peer ID	
[	< Back Next > Finish Cancel

## • 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			

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 &gt;&gt; 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.



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:	Site to Site VPN (LAN-to-LAN)
Index:	3
Profile Name:	VPN-Ser1
Username:	server1
Allowed Service:	PPTP+IPSec
Peer IP/VPN Client IP:	
Peer ID:	
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0
Click <b>Back</b> to modify changes and proceed to the following a	
	Go to the VPN Connection Management.
	O Do another VPN Server Wizard setup.
	View more detailed configurations.
	< Back Next > Finish Cancel
to to the VPN Connection Ianagement	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.
o another VPN Server Vizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
iew more detailed	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;LAN to LAN</b> for viewing detailed configuration.

## 4.10.3 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup	
	Enable PPTP VPN Service
	Enable IPSec VPN Service
✓	Enable L2TP VPN Service

**Note:** If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

OK	Clear	Cancel



# 4.10.4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

VPN and	Remote	Access	>>	PPP	General	Setur	)

PPP/MP Protocol Dial-In PPP	PAP or CHAP	IP Address Assignment for (When DHCP Disable set)	Dial-In Users
Authentication	PAP of CHAP	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Nutual Authentication	(PAP) 🔘 Yes 💽 No		
Username			
Password			

OK

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.
	Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer.



Assigned IP Range	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.

## 4.10.5 IPSec General Setup

In IPSec General Setup, there are two major parts of configuration.

There are two phases of IPSec.

VPN and Remote Access >> IPSec General Setup

- 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.

IKE Authentication Method	
Pre-Shared Key	•••••
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic	, but will not be encrypted.
High (ESP) 🛛 🗹 DES	SDES AES
Data will be encrypted	and authentic.
	OK Cancel

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



Method

**Pre-Shared Key -**Currently only support Pre-Shared Key authentication.

**Pre-Shared Key-** Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key.

**IPSec Security Method** Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.

**High** - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

## 4.10.6 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

K509 Peer ID Accounts:   Set to Factory Defau					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

## Set to Factory Default

Click it to clear all indexes.

Index

Click the number below Index to access into the setting page of IPSec Peer Identity.

Name Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.



#### VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1	
Profile Name one	
Enable this account	
O Accept Any Peer ID	
• Accept Subject Alternative N	lame
Туре	IP Address 💌
IP	
O Accept Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
	OK Clear Cancel
rofile Name	Type the name of the profile.
ccept 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 Address</b> , <b>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 accep the peer with matching value. The field includes <b>Country (C</b> <b>State (ST), Location (L), Organization (O), Organization</b> <b>Unit (OU), Common Name (CN), and Email (E)</b> .

## 4.10.7 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.

emote Access User Accounts:				Set to Factory Defa	
Index	User	Status	Index	User	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

VPN and Remote Access >> Remote Dial-in User

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.
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	User
----------------	-----------	--------	---------	------

Index No. 1			
User account and Authentication	Username ???		
Enable this account	Password		
Idle Timeout 300 second(s)	Enable Mobile One-Time Passwords(mOTP)		
Allowed Dial-In Type	PIN Code		
PPTP	Secret		
☑ IPSec Tunnel	IKE Authentication Method		
☑ L2TP with IPSec Policy None	Pre-Shared Key		
Specify Remote Node	IKE Pre-Shared Key		
Remote Client IP or Peer ISDN Number	Digital Signature(X.509)		
	None V		
or Peer ID			
Netbios Naming Packet 💿 Pass 🔘 Block	IPSec Security Method		
Multicast via VPN 🛛 🔘 Pass 💿 Block	Medium(AH)		
(for some IGMP,IP-Camera,DHCP Relayetc.)	High(ESP) 🗹 DES 🗹 3DES 🗹 AES		
	Local ID (optional)		
Subnet			
Assign Static IP Address			
0.0.0.0			
ОК	Clear Cancel		

User account and	Enable this account - Check the box to enable this function.
Authentication	<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:
	<b>None -</b> Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
	<b>Nice to Have -</b> Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.
	<b>Must</b> -Specify the IPSec policy to be definitely applied on the L2TP connection.
	<b>Specify Remote Node -</b> You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).

methods in the general settings. **Netbios Naming Packet -Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. Block – When there is conflict occurred between the • hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. Multicast via VPN - Some programs might send multicast packets via VPN connection. **Pass** – Click this button to let multicast packets pass through the router. Block – This is default setting. Click this button to let multicast packets be blocked by the router. Subnet Chose one of the subnet selections for such VPN profile. Assign Static IP Address – Allows you to specify certain IP address as a subnet. 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) - Check this box to make the authentication with mOTP function. **PIN Code** – Type the code for authentication (e.g., 1234). Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6). **IKE Authentication** This group of fields is applicable for IPSec Tunnels and L2TP Method with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity. **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. Medium-Authentication Header (AH) means data will be

Uncheck the checkbox means the connection type you select above will apply the authentication methods and security



authenticated, but not be encrypted. By default, this option is

invoked. You can uncheck it to disable it.

**High-Encapsulating Security Payload** (**ESP**) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

**Local ID** - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

## 4.10.8 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.

LAN-to-LAN Profiles: Set to Factory Defa					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

VPN and Remote Access >> LAN to LAN

## 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.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

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

#### Profile Index : 1

1. Common Settings	
Profile Name ???	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-in
Enable this profile	Always on
VPN Dial-Out Through WAN1 First ♥ Netbios Naming Packet	Idle Timeout 300 second(s)  Enable PING to keep alive  PING to the IP
2. Dial-Out Settings	
Type of Server I am calling      PPTP      IPSec Tunnel      L2TP with IPSec Policy None  Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression On Off IKE Authentication Method Pre-Shared Key Digital Signature(X.509) None IPSec Security Method Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in Schedule Setup: , , , , , ,

Profile Name Enable this profile VPN Dial-Out Through Specify a name for the profile of the LAN-to-LAN connection.

Check here to activate this profile.

Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.

WAN1	First	*
WAN1	First	
WAN1	Only	
WAN2	First	
WAN2	Only	
WAN3	First	
WAN3	Only	

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.

## **Netbios Naming Packet**

Pass – click it to have an inquiry for data transmission between

	the hosts located on both sides of VPN Tunnel while connecting.
	<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.
Multicast via VPN	Some programs might send multicast packets via VPN connection.
	$\mathbf{Pass}$ – 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.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile.
	Both:-initiator/responder
	Dial-Out- initiator only
	Dial-In- responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.
	<b>Idle Timeout:</b> The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
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.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	<b>Enable PING to keep alive</b> is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
Type of Server I am calling	<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.
	<b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.
	<b>L2TP with IPSec Policy -</b> Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:

	<b>None:</b> Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
	<b>Nice to Have:</b> Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.
	<b>Must:</b> Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to <b>Yes</b> to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.
	Pre-Shared Key - Input 1-63 characters as pre-shared key.
	<b>Pre-Shared Key</b> - Input 1-63 characters as pre-shared key. <b>Digital Signature (X.509)</b> - Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> .
IPSec Security Method	Digital Signature (X.509) - Select one predefined Profiles set
IPSec Security Method	<b>Digital Signature (X.509)</b> - Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> . This group of fields is a must for IPSec Tunnels and L2TP with
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES without Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</li> </ul>
IPSec Security Method	<ul> <li>Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access &gt;&gt;IPSec Peer Identity.</li> <li>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</li> </ul>



The window of advance setup is shown as below:

INE advanced settings - Wind http://192.168.1.1/loc/l2IIheDt.htm			
IKE advanced settings			
IKE phase 1 mode	Main mode	O Aggressive mode	
IKE phase 1 proposal	DES_MD5_G1		~
IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5 😒		
IKE phase 1 key lifetime	28800 (900 ~ 8640	00)	
IKE phase 2 key lifetime	3600 (600 ~ 8640	00)	
Perfect Forward Secret	Disable	O 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				
PPTP		Username	???	
🗹 IPSec Tunnel		Password		
L2TP with IPSec Policy None		VJ Compression	💿 On 🔘 Off	
Specify Remote VPN Peer VPN Server IP	Gateway	IKE Authentication Method ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X, 5)		
or Peer ID		Digital Signature(X.509)		
		IPSec Security Method ✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES		
4. TCP/IP Network Settings	;			
My WAN IP	0.0.0.0	RIP Direction	Disable 🔽	
Remote Gateway IP	0.0.0.0		ote network, you have to	
Remote Network IP	0.0.0.0	do	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 WAN supports this )		
	More			
Allowed Dial-In Type		l-in connection with dif	• •	
<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.			user to trigger an IPSec	
	<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:			
	<b>None -</b> Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.			
	<b>Nice to Have</b> - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.			
	<b>Must -</b> Specify the L2TP connection.	e IPSec policy to be def	finitely applied on the	
Specify Remote VPN Gateway	ID (should be the checking the box.	he IP address of the rem same with the ID settin Also, you should furthe curity methods on the rig	er specify the	



	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.
	<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 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. <b>Medium-</b> Authentication Header (AH) means data will be
	authenticated, but not be encrypted. By default, this option is active.
My WAN IP	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),
My WAN IP Remote Gateway IP	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. 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
·	<ul> <li>active.</li> <li>High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</li> <li>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 here. Do not change the default value if you do not select PPTP or L2TP.</li> <li>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 PPTP or L2TP.</li> <li>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 from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed 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</li> </ul>

**Network Mask** 

М	ore	
	UL U	

configuration. You can modify the settings if required.

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 🛛 🚺 🗖	DI
Profile Index :1	-1
Remote Network	
Network IP Netmask 255.255.255 / 32 🖌	
Add Delete Edit	
OK Close	

**RIP Direction**The option specifies the direction of RIP (Routing Information<br/>Protocol) packets. You can enable/disable one of direction here.<br/>Herein, we provide four options: TX/RX Both, TX Only, RX<br/>Only, and Disable.**From first subnet to**<br/>remote network, you<br/>have to doIf the remote network only allows you to dial in with single IP,<br/>please choose NAT, otherwise choose Route.**Change default route to**<br/>this VPN tunnelCheck this box to change the default route with this VPN tunnel.

# 4.10.9 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 Manage	ement				
Dial-out Tool				Refres	h Seconds	5 : 10 🔽 Refresh
			~	Dial		
VPN Connection Status Current Page: 1					Page M	No. GO >>
VPN Type Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-					ata is encr ata isn't er	2 C C C C C C C C C C C C C C C C C C C
Dial	Click this bu	utton to e	xecute di	al out fu	nction.	
Refresh Seconds	Choose the t and 30.	time for r	efresh the	e dial inf	ormation	among 5, 10,

**Refresh** Click this button to refresh the whole connection status.

# 4.11 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.



## 4.11.1 Local Certificate

Certificate Management >> Local Certificate

509 Local Certificate	e configuration		
Name	Subject	Status	Modify
Local			View Delete
GENERATE X509 Local	IMPORT REFRESH		
			<u>~</u>
			~
L			

Generate

Click this button to open Generate Certificate Request window.



Certificate Management >> Local Certificate					
Generate Certificate Request					
Subject Alternative Name					
Туре	IP Address 🔽 💌				
IP					
Subject Name					
Country (C)					
State (ST)					
Location (L)					
Orginization (O)					
Orginization Unit (OU)					
Common Name (CN)					
Email (E)					
Кеу Туре	RSA 💌				
Key Size	1024 Bit 👻				

Generate

Type in all the information that the window requests. Then click **Generate** again.

-	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.

After clicking **Generate**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

Name	Subject	Status	Modify			
Local	/C=TW/O=Draytek/OU=RD/emailA	Requesting	View Delete			
GENERATE	GENERATE IMPORT REFRESH					
X509 Local Certificate Request						
BEGIN CERTIFICATE REQUEST MIIBsjCCARsCAQAwUDELMAKGA1UEBhMCVFcxEDAOH BgNVBASTA1JEMSIWIAYJKoZIhvcNAQkBFhNzZXJ2a MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBqQDPioahu blo1kt9cTdLUDaFk6s8d3wDeQytoV1LBJz2IDF0xj /rGhuVTKd9j6PlcrnkP7du84t23tWBdMD4W5c8Vm2 RZjkRMaHEWpVpwIDAQABoCIwIAYJKoZIhvcNAQkON qAEqMAOGCSqGSIb3DQEBBQUAA4GBAB4304N9nod8r ikisNdZUoUEnKcejeOndc+H83VDA23ACEJpzTPFxc GqeJ9trvYqeZybCrSjRU1PN1Hccfo7ANJ/M/D1EPc j8kJEim0 END CERTIFICATE REOUEST		aWN1QGRyYX1ÖZ u/gFQaYB1ce50 jX6ip7ev187tw SyDjShLhjdxVY MRMwETAPBgNVH rIudBAfTt91ts qklbeZo7a+wE5	WsuY29tMIGf ERSDfWknIdH wTsg41g26Qk PWpNKVIrOT2 REECDAGhwTA o/tYNb2kfEZ 7/+0VhNagBa			

#### X509 Local Certificate Configuration

# 4.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA 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	tificate Information - Windows Intern	net Explorer 📃		
🥖 http	://192.168.1.1/doc/XCaCfVi1.htm		*	
			^	
Certificate Detail Information				
	Certificate Name:	Trusted CA-1		
	Issuer:			
		×		
	Subject:		=	
	Subject Alternative Name:			
	Valid From:			
	Valid To:			
, i	·			
		Close	~	
8				

# 4.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup				
Certificate Backup / Restoration				
Backup				
	Encrypt password:			
	Confirm password:			
	Click Backup to download certificates to your local PC as a file.			
Restoration				
	Select a backup file to restore.			
	Browse.			
	Decrypt password:			
	Click Restore to upload the file.			

# 4.12 VoIP

Note: This function is used for "V" models.

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

#### sip: user:password @ host: port

Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN 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.





# 4.12.1 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 Setup	
DialPlan Configuration	
	Phone Book
	<u>Digit Map</u>
	Call Barring
	Regional
	PSTN Setup
Secure Phone configuration	
	Enable Secure Phone (ZRTP+SRTP)
	☑ Enable SAS Voice Prompt
	OK
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**

VoIP >> DialPlan Setup

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 Vigor2850Vn for setting the phone book.

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
20.				Default	None		None	х

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

Click any index number to display the dial plan setup page.

Phone Book Index No. 1	
Enable	
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
ОК	None ZRTP+SRTP Crear Cancel

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.
	None V None PSTN
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 (PSTN number/ISDN 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.
	<b>Note:</b> 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**

VoIP >> DialPlan Setup

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	OP Number	Min Len	Max Len	Rout	e
1		03	Replace 💌	8863	7	9	PSTN	~
2	<b>~</b>	886	Strip 💌	886	8	10	PSTN	Y
3			None 🗸		0	0	PSTN	~
4			None 🗸		0	0	PSTN	~
5			None 🗸		0	0	PSTN	~
6			None		0	0		

16		None 📉	0	PSTN 📉
17		None 🔽		PSTN 🔽
18		None 🔽		PSTN 🔽
19		None 🔽		PSTN 🔽
20		None 🔽		PSTN 🗸

Note: Min Len and Max Len should be between 0~25.

OK Cancel

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 will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886.	
	<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 VoIP>> Phone Settings.	



# **Call Barring**

Call barring is used to block phone calls coming from the one that is not welcomed.

VoIP >> DialPlan Setup

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>						х
< <u>1-10</u>	<u>11-20</u> >>					Next >

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/URI		
Route		All 💌
Index(1-15) in	Schedule Setup	
Note:Wildcard '?' is supporte	ed.	
	ОК	Cancel
Enable	Click this to e	enable this entry.
Call Direction		e direction for the phone call, IN – incoming call ig call, IN & OUT – both incoming and outgoing

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>3.5.2</b> Schedule 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	ve the caller ID.

0K

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.

Cancel

VoIP >> DialPlan Setup	
Call Barring Block Unknown Domain	
🗹 Enable	
Route	Phone1 Phone2
Index(1-15) in <u>Schedule</u> Setup	
Note: If the domain of the incoming call is diffe be blocked.	rent from the domain found in SIP accounts,the call should

Cancel

ΟK

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	🗌 Phon	ne1 🔲 Phone2		
Index(1-15) in <u>Schedul</u>	le Setup,	,,,,		
Note: The incoming calls by means o	of IP dialing (e.g.#192*1	168*1*1#) should be blocked	1.	
	OK Car	ancel		

# 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 Fa	<u>ctory Default</u>
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	+#			

ОК	Cancel

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 field 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**

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**.

VoIP >> PSTN Setup Default phone number for PSTN relay				
		OK Cancel		

Then, check the Enable box to make the PSTN number available for dial whenever you need.

### 4.12.2 SIP Accounts

VoIP >> 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.

Refresh

Status

**Ring Port** 

G.729A/B Phone1 Phone2

Note: Selection items for Ring Port will differ according to the router you have.

SIP Accounts List					
Index	Profile	Domain/Realm	Proxy	Account Name	Codec
1					G.729A/B
2					G.729A/B
<u>3</u>					G.729A/B
<u>4</u>					G.729A/B
5					G.729A/B

2			G.729A/B	🗌 Phone 1	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	-
NAT Tr	aversal Setting				gistered on Si ter on SIP se	
	STUN Server:					
	External IP:					
	SIP PING Interval:	150 sec				

OK



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. Set Phone, ISDN1-S0 or ISDN-TE as the default ring port for the SIP account. If you choose Phone or ISDN1-S0, the ISDN2-TE selection will be dimmed, vice versa. There are ten internal lines with numbers $(30 - 39)$ offered for <b>ISDN-S0</b> . You can specify any one of them as ring port for specified SIP account. By the way, ISDN-S0 can be used by mapping with MSN numbers.
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.

Profile Name	(11 char max.)
Register via	None 💌 📃 Call without Registration
GIP Port	5060
Domain/Realm	(63 char max.)
roxy	(63 char max.)
Act as outbound pro	xy
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
assword	(63 char max.)
Expiry Time	1 hour 💙 3600 sec
NAT Traversal Support	None 💌
Ring Port	Phone 1 Phone 2
Ring Pattern	1 🕶
Prefer Codec	G.729A/B (8Kbps) 🔽 🗌 Single Codec
Packet Size	20ms 💌
oice Active Detector	Off 🗸

VoIP >> SIP Accounts

Profile Name	Assign a name for this profile for identifying. You can type
	similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose <b>None</b> and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of <b>Call without Registration</b> . Choosing <b>Auto</b> is recommended. The system will select a proper way for your VoIP call.
	None  None Auto WAN1 WAN2 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

**None** – Disable this function.



	your router. Manual – Choose this optio IP address as the NAT trans	f there is STUN server provided for on if you want to specify an external versal support. hat you use supports Nortel solution,
Ring Port	Set Phone 1 and/or Phone 2 SIP account.	as the default ring port(s) for this
Ring Pattern	Choose a ring tone type for	the VoIP phone call.
	Ring Pattern	1 V 1 2 3 4 5 6
Prefer Codec	codec used for each call will before each session, and so a default codec is G.729A/B; maintaining good voice qual If your upstream speed is on	the default for your VoIP calls. The l be negotiated with the peer party may not be your default choice. The it occupies little bandwidth while lity. lly 64Kbps, do not use G.711 codec. t least 256Kbps upstream if you
	Prefer Codec <b>Single Codec</b> – If the box is will be applied.	G.711A (64Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps) G.726_32 (32kbps) G.checked, only the selected Codec
Packet Size	The amount of data containe	ed in a single packet. The default s the data packet will contain 20 ms
	Packet Size	20ms V 10ms 20ms 30ms 40ms 50ms 60ms
Voice Active Detector	not. If not, the router will do	ne voice on both sides is active or o something to save the bandwidth invoke this function; click off to
	Voice Active Detector	Off 💙 Off On



# 4.12.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

VoIP >> Phone Settings
------------------------

Phone List Refresh Seconds: 30 💌 Refresh							Refresh
Index	Port	Call Feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	G.729A/B	User Defined	5/5		InBand
2	Phone2	CW,CT,	G.729A/B	User Defined	5/5		InBand

🔲 Symmetric RTP	
Dynamic RTP Port Start	10050
Dynamic RTP Port End	15000
RTP TOS	IP precedence 5 🛛 💙 10100000

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.
	<b>Codec</b> – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port.
	<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	<b>Symmetric RTP</b> – 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.
	<b>Dynamic RTP Port Start</b> - Specifies the start port for RTP stream. The default value is 10050.

**Dynamic RTP Port End** - Specifies the end port for RTP stream. The default value is 15000.

**RTP TOS** – It decides the level of VoIP package. Use the drop down list to choose any one of them.

Manual	
IP precedence 1	
IP precedence 2	
IP precedence 3	
IP precedence 4	
IP precedence 5	
IP precedence 6	
IP precedence 7	
AF Class1 (Low Drop)	
AF Class1 (Medium Drop)	
AF Class1 (High Drop) 🍈	
AF Class2 (Low Drop)	
AF Class2 (Medium Drop)	
AF Class2 (High Drop)	
AF Class3 (Low Drop)	
AF Class3 (Medium Drop)	
AF Class3 (High Drop)	
AF Class4 (Low Drop)	
AF Class4 (Medium Drop)	
AF Class4 (High Drop)	
EF Class	
Manual	~
L	

RTP TOS

#### **Detailed Settings for Phone Port**

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Phone1		
Call Feature		Default SIP Account
🔲 Hotline		Play dial tone only when account registered
Session Timer	90 sec	
T.38 Fax Function		
Error Correction Mode	REDUNDANCY 🔽	
Call Forwarding	Disable 💌	
SIP URL		
Time Out	30 sec	
🗌 DND(Do Not Disturb) N	Mode	
Index(1-15) in <u>Sche</u>	<u>edule</u> Setup:	
Note: Action and Id be ignored.	lle Timeout settings will	
Index(1-60) in <u>Phon</u>	<u>e Book</u> as Exception List:	
	,,,,,	
CLIR (hide caller ID)		
🗹 Call Waiting		
🗹 Call Transfer		

#### 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.
	Error Correction Mode – choose a mode for error correction.
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
	<b>SIP URL</b> – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. <b>Time Out</b> – Set the time out for the call forwarding. The default setting is 30 sec.
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 the call barring 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.

Tone Settin	igs						
Region User Defined 🛩				Caller ID Type		FSK_ETSI	
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial	tone	350	440	0	0	0	0
Ringin	ig tone	400	450	400	200	400	2000
Busy	tone	400	0	375	375	0	0
Congest	tion tone	0	0	0	0	0	0
Volume Ga	nin			DTMF			
Mic Gain(1	-10)	5		DTMF Mo		InBand	*
Speaker Gain(1-10) 5			Payload T (96 - 127	ype (RFC283)	3) <sub>101</sub>		
MISC							
Dial Tone I	Power Level	(1 - 50) 2	7				
Ring Frequ	ency (10 -	50HZ) 25	5				

#### VoIP >> Phone Settings

#### Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

	-	
Tone Setti	ings	
Region	User Defined 💌	
	User Defined	ow
	UK	<b>(</b> H
Dia	US	0
	Denmark	
Ringi		0
Duc	Germany	0
BUS	Netherlands	0
Conges	Portugal	
-	Sweden	
Volume G	Australia	
Mic Gain(	Slovenia	
	CZECH	
Speaker (	Slovakia	
	Hungary	
MISC	Switzerland	
Dial Tone	France	- 51
	UN CCA	
Ring Freq	China	HZ)
	Taiwan	

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain	<b>Mic Gain (1-10)/Speaker Gain (1-10)</b> - Adjust the volume of microphone and speaker by entering number from 1-10. The larger of the number, the louder the volume is.
MISC	<ul> <li>Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.</li> <li>Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.</li> </ul>
DTMF	<ul> <li>DTMF Mode – There are four DTMF modes for you to choose.</li> <li><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 <i>OutBand</i> - 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.</li> <li><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.</li> </ul>

Advance Settings >> Phone

DTMF mode

InBand	*
InBand	
OutBand ( RFC2833)	
SIP INFO (cisco format)	
SIP INFO (nortel format)	

**Payload Type (rfc2833)** - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

### 4.12.4 Status

From this page, you can find codec, connection and other important call status for each port.

VoIP >> Status

Status								Refres	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	Speake Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5
Log Date (mm=dd=u		Time	m.eel	Duration		n/Out	/Miss	Acc	ount	ID	Peer	ID
(mm-dd-y		(hh:m	ຫ:ສສ)	(hh:mm:s		n/ Ouc	/ 1135	ACC	ounc	10	FEEL	10
00-00-	0	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	-			-				
	0	00:00		00:00:00	-							

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

**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.

It shows current connection status for Phone(s) and ISDN ports.



Port

Status

It shows the VoIP connection status.
IDLE - Indicates that the VoIP function is idle.
HANG\_UP - Indicates that the connection is not established (busy tone).
CONNECTING - Indicates that the user is calling out.
WAIT\_ANS - Indicates that a connection is launched and waiting for remote user's answer.
ALERTING - 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.

# 4.13 Wireless LAN

This function is used for "n" models only.

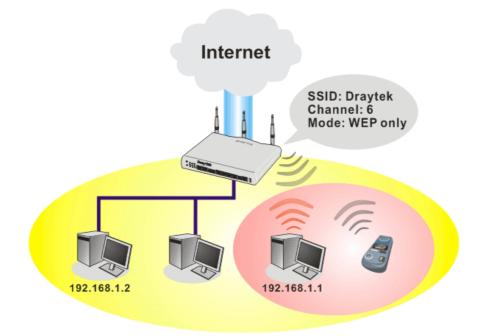
# 4.13.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note**: \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



### **Multiple SSIDs**

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.

### **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.

Wi	reless LAN
- Þ	General Setup
- Þ	Security
- Þ	Access Control
- Þ	WPS
- Þ	WDS
- Þ	Advanced Setting
- Þ	WMM Configuration
- Þ	AP Discovery
⊳	Station List

Wireless LAN >> General Setup

# 4.13.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

ole Wireless I	LAN			
1ode :		Mixed(11b+	11g+11n) 🔽	
ndex(1-15) i	n <u>Schedu</u>	le Setup:, [	,,	
only schedule ther actions		that have the action "Force Dow ed.	vn" are applied to the	WLAN, all
Enable Hid	de SSID	SSID	Isolate Member	Isolate VPN
1		DrayTek		
2				
3				
4				
other. solate VPN:is	olate wire	s clients (stations) with the san eless with remote dial-in and LAM 7000000000000000000000000000000000000	N TO LAN VPN.	s for each
other. solate VPN:is :hannel: Cha	olate wire annel 6, 243 e: necess	eless with remote dial-in and LAM	N to LAN VPN.	
other. solate VPN:is hannel: Cha ong Preambl acket-OVER Tx Burst iote:	annel 6, 243 e: necess DRIVE <sup>TM</sup>	Pless with remote dial-in and LAN	N to LAN VPN. nble: 🔲 es only(lower performa	ance)
other. solate VPN:is hannel: Cha ong Preambl acket-OVER Tx Burst iote:	annel 6, 243 e: necess DRIVE <sup>™</sup> chnology n	eless with remote dial-in and LAN 37MHz  Long Prean ary for some old 802.11 b devic nust also be supported in clients	N to LAN VPN. nble: es only(lower performa s to boost WLAN perfo	ance)
other. solate VPN:is hannel: Cha ong Preambl acket-OVER Tx Burst ote: he same tec	annel 6, 243 e: necess DRIVE <sup>TM</sup>	eless with remote dial-in and LAM IMHz V Long Pream ary for some old 802.11 b devic nust also be supported in clients Upload	N to LAN VPN. nble: 🔲 es only(lower performa	ance) rmance.
other. solate VPN:is hannel: Cha ong Preambl acket-OVER Tx Burst ote: he same tec ate Control	olate wire annel 6, 243 e: necess DRIVE <sup>™</sup> chnology n Enable	Aless with remote dial-in and LAN ATMHZ Long Pream ary for some old 802.11 b devic nust also be supported in clients Upload 30000 kbps	N to LAN VPN. nble: es only(lower performa s to boost WLAN perfo Download	ance) rmance. kbps
other. solate VPN:is hannel: Cha ong Preambl acket-OVER acket-OVER Tx Burst ote: he same tec ate Control SSID 1	colate wire annel 6, 243 e: necess DRIVE <sup>TM</sup> chnology m Enable	Aless with remote dial-in and LAN ATMHZ Long Pream ary for some old 802.11 b devic nust also be supported in clients Upload 30000 kbps	N to LAN VPN. nble: es only(lower performa s to boost WLAN perfo Download 30000	ance) rmance.

Enable Wireless LAN Mode Check the box to enable wireless function.

At present, the router can connect to 11g Only, 11n Only (2.4

GHz), Mixed (11b+11g), Mixed (11g+11n), Mixed (11a+11n 5 GHz), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mixed (11b+11g+11n) mode.

	Mixed(11b+11g+11n)       ✓         11g Only       11n Only (2.4 GHz)         Mixed(11b+11g)       ✓         Mixed(11g+11n)       ✓         Mixed(11a+11n 5 GHz)       ✓         Mixed(11b+11g+11n)       ✓
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.
Isolate	<b>VPN</b> – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.
	<b>Member</b> –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.  Channel: Channel 6, 2437MHz  Channel 1, 2412MHz Channel 3, 2422MHz Channel 3, 2422MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 11, 2462MHz Channel 11, 2467MHz Channel 11, 2472MHz Channel 12, 2477MHz Channel 13, 2472MHz Channel 14, 2472MHz Channel 14, 2472MHz Channel 14, 2472MHz Channel 14,
Long Preamble	This option is to define the length of the sync field in an 802.11

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. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

Packet-OVERDRIVEThis feature can enhance the performance in data transmission<br/>about 40%\* more (by checking **Tx Burst**). It is active only<br/>when both sides of Access Point and Station (in wireless client)<br/>invoke this function at the same time. That is, the wireless client<br/>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**).

	_
Advance Setting Disable Radio Eragmentation Threshold : 2246 RTS Threshold : 2247 Frequency : 802.11b/g/n - 2.4GH ¥ Ad-hoc Channel: 1 ¥ Power Save Mode: Disable ¥ Tx Burst : Disable ¥	
OK Cancel Apply	r
Disable	
	Disable Radio Eragmentation Threshold : 2246 RTS Threshold : 2247 Frequency : 802.11b/g/n - 2.40H ¥ AdJaoc Channel: 1 ¥ Power Save Mode: Disable ¥ Tx Burst : Disable ¥

**Note:** \* means the real transmission rate depends on the environment of the network.

# **Rate Control** It controls the data transmission rate through wireless connection.

**Upload** – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.

**Download** – Type the transmitting rate for data download. Default value is 30,000 kbps.

## 4.13.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

The 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.

```
Wireless LAN >> Security Settings
```

Mode:       Disable         set up RADIUS Server if 802.1x is enabled.         WPA:         Encryption Mode:       TKIP for WPA/AES for WPA2         Pre-Shared Key(PSK):	SSID 1	SSID 2	SSID 3	SSID 4	
WPA:         Encryption Mode:       TKIP for WPA/AES for WPA2         Pre-Shared Key(PSK):		Mode:	[	Disable	~
Pre-Shared Key(PSK):   Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2" or "0x655abcd".   WEP:   Encryption Mode:   6 Key 1 :   6 Key 2 :   6 Key 3 :   6 Key 3 :   7 Key 4 :   Encryption thexadecimal digits leading by "0x", for example "AB312" or "0x4142333132". For 128 bit WEP key Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "AB312" or "0x414233112".	WPA:	Set up <u>RADIUS Se</u>	erver if 802.1>	k is enabled.	
Pre-Shared Key(PSK):         Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2" or "0x655abcd".         WEP:         Encryption Mode:       64-Bit Image: Image	Encry	otion Mode:		TKIP for WPA/AES	for WPA2
"cfgs01a2" or "0x655abcd".         WEP:         Encryption Mode:		Pre-Shared Key(P	SK):	*****	
Encryption Mode:       64-Bit            • Key 1 :       ************************************					igits leading by "Ox", for example
<ul> <li>Key 1:</li> <li>Key 2:</li> <li>Key 3:</li> <li>Key 4:</li> </ul> For 64 bit WEP key Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132". For 128 bit WEP key Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example	WEP:				
Key 1 :		Encryption Mode:	[	64-Bit 💙	
Key 2 :		⊙Key 1 :	[	*****	
Key 3 :		○Кеу 2 :	[	*****	
For 64 bit WEP key Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132". For 128 bit WEP key Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example		○КеуЗ:	[	*****	
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132". <b>For 128 bit WEP key</b> Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example		○Кеу 4 :	[	*****	
	Type "0x414 <b>For 12</b> Type	5 ASCII character 42333132". <b>8 bit WEP key</b> 13 ASCII characte	r or 26 Hexad	- decimal digits lead	ng by "Ox", for example

Mode

There are several modes provided for you to choose.



	Disable	~
	Disable	
1	WEP	
-	WEP/802.1x Only	
	WPA/802.1x Only	
	WPA2/802.1x Only	
	Mixed(WPA+WPA2/802.1x only)	
	WPA/PSK	
	WPA2/PSK	
	Mixed(WPA+WPA2)/PSK	

**Note:** You should also set **RADIUS Server** simultaneously if 802.1x mode is selected.

Disable - Turn off the encryption mechanism.

**WEP**-Accepts only WEP clients and the encryption key should be entered in WEP Key.

**WEP/802.1x Only -** Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

**WPA/802.1x Only-** Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

**WPA2/802.1x Only-** Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

**WPA2/PSK-**Accepts only WPA2 clients and the encryption key should be entered in PSK.

**Mixed (WPA+ WPA2)/PSK -** Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in 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 **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**Type** - Select from Mixed (WPA+WPA2) or WPA2 only. **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as

**Dray** Tek

**WPA** 

WEP

#### 0x4142434445.)

**128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:



All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

### 4.13.4 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.

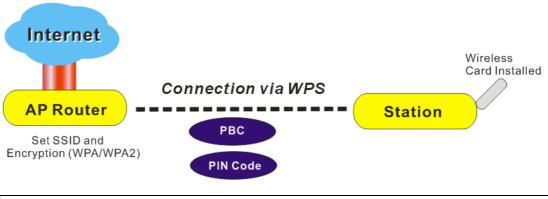
Enable Mac Addres	s Filter 📃 SSID 1 🛛 White List 🛩	🔲 SSID 2 White List 👻
	SSID 3 White List 💙	SSID 4 White List
	MAC Address Filter	
Index Attribut	e MAC Address	Apply SSID
App	Client's MAC Address : : : : : : : : : : : : : : : : : :	: : : : : : : : : : : : : : : : : : :
-	OK Clear A	
Enable Mac Address Filter	identified with SSID 1 to 4 (expressed by MAC address under different wireless LA	Address filter for wireless LAN respectively. All the clients ses) listed in the box can be grouped N. For example, they can be grouped at the same time if you check SSID 1
MAC Address Filter	Display all MAC addresses	that are edited before.

#### Wireless LAN >> Access Control

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.

## 4.13.5 WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

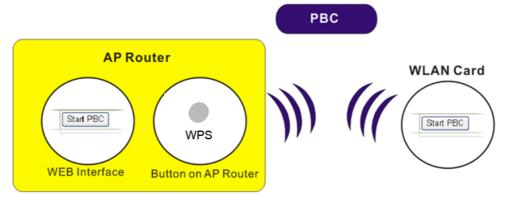


Note: Such function is available for the wireless station with WPS supported.

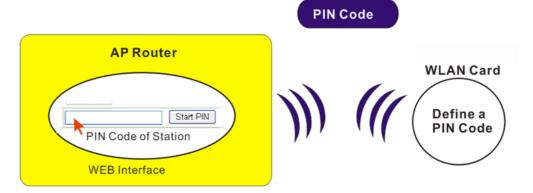
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 2850 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



• If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

#### Below shows **Wireless LAN>>WPS** web page.

Wireless LAN >> WPS (Wi-Fi Protected Setup)

Enable WPS

#### Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	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.

 $\ensuremath{\mathbb{Q}}$  : Waiting for WPS requests from wireless clients.

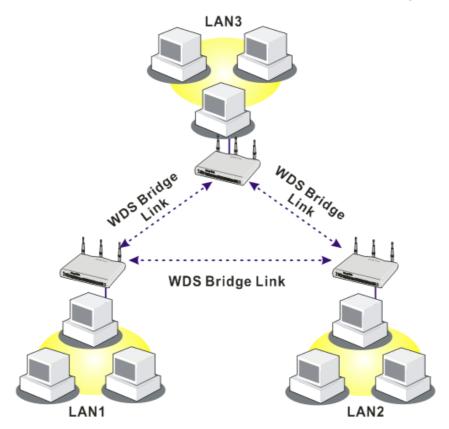
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication 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)

# 4.13.6 WDS

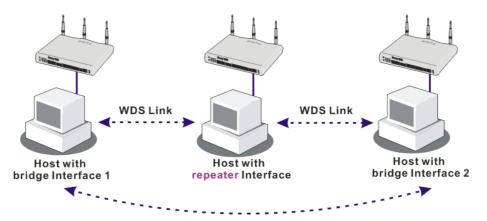
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:



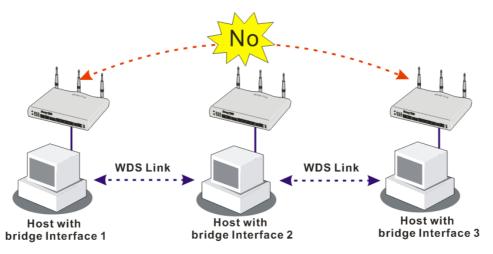
The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.



In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

	Pridao			
Mode: Bridge 💌	Bridge Enable Peer MAC Address			
Security:				
WFP:				
Use the same WEP key set in <u>Security Settings</u> .				
ose the same will key set in <u>security settings</u> .	Note: Disable unused links to get better performance.			
Pre-shared Key:				
Туре:	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.			

Wireless LAN >> WDS Settings

Mode

Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.

	Disable V 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 two types for you to choose. <b>WPA</b> and <b>WPA2</b> are used for WDS devices (e.g., AP700). For example, if you have a wireless AP and a Vigor2850n 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.

# 4.13.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

HT Dhusiaal Mada	
HT Physical Mode Operation Mode	Mixed Mode      Green Field
Channel Bandwidth	
Guard Interval	○ long ⊙ auto
Aggregation MSDU(A-MSDU)	O Disable 💿 Enable
	ОК
Deration Mode	<b>Mixed Mode</b> – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. Howeve the entire wireless transmission will be slowed down if 802.11 or 802.11b wireless client is connected.
	<b>Green Field</b> – to get the highest throughput, please choose suc 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.
Suard Interval	It is to assure the safety of propagation delays and reflections f 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> .

# 4.13.8 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		C Enable	Oisable			
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 Parameters of Station						
	Aifsn	CWMin	С	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	

Wireless LAN >> WMM Configuration



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> Vigor2850 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.

#### 4.13.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List			
	BSSID	Channel	SSID
		Scan	
See <u>St</u>	atistics.		
	uring the scanning ( e router.	process (~5 secor	onds), no station is allowed to connect
Add to	WDS Settings :		
AP's MA	.C address	: :::::::::::::::::::::::::::::::::::::	::::
Add t	to	💿 Bridge	O Repeater

Wireless LAN >> Access Point Discovery

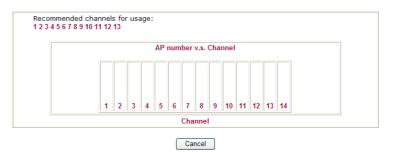
Scan

**Statistics** 

It is used to discover all the connected AP. The results will be shown on the box above this button.

It displays the statistics for the channels used by APs.

#### Wireless LAN >> Site Survey Statistics



Add to

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

#### 4.13.10 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

```
Wireless LAN >> Station List
```

	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 Access Control :	
	Client's MAC address	
	Add	
efresh	Click this button to refresh the status of station list.	

Control.

### 4.14 USB Application

USB storage disk connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the Samba service through Vigor router.



#### 4.14.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB storage disk into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	Default 👻
Samba Service Settings(Network Neighbo	prhood)
C Enable O Disable	
● 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 multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters ,

OK	
----	--

but both cannot contain any of the following: . ; : "  $< > * + = / \setminus |$  ?.

**General Settings** 

**Simultaneous FTP Connections -** This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.

**Default Charset -** At present, Vigor router supports three types of character sets: default, GB2312 and BIG5.

Default	*
Default	
GB2312	
BIG5	

#### 4.14.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.

JSB User Ma	nagement			1.1	Set to Factory Default
Index	Username	Home Folder	Index	Username	Home Folder
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

USB Application >> USB User Management

Click index number to access into configuration page.

USB Application	>> USB	User Management
03D Application	030	user management

FTP/Samba User	🔘 Enable 🛛 💿 Disable
Username	
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	200 200 200 200 200 200 200 200 200 200
Access Rule	
File	🗌 Read 📃 Write 📃 Delete
Directory	🗌 List 📃 Create 📃 Remove

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

ОК	Clear	Cancel
----	-------	--------

FTP/Samba User	<b>Enable</b> – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.
	<b>Disable</b> – Click this button to disable such profile.
Username	Type the username for FTP/Samba users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk.
	<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.
	Note: 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.
<b>Confirm Password</b>	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 $\bowtie$ to open the following dialog to add any new folder which can be specified as the Home Folder.

http://192.168.1.5/doc/ftpuserfolder.htm - Microsoft Internet Explorer	
USB User Management	~
Choose Folder	
Folder Name	
Create New Home Folder	
Folder Name:	
test	
Create	
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) and	
space. Only 11 characters are allowed.	
	V

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.

#### 4.14.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

USB Applicati	on >> File	Explorer				
File Explorer						
↔ ⊙	9	Current Path: /				
		Name		Size	Delete	Rename
Upload		Browse				
Note: The folde	r can not b	e deleted when it is not empty.				
Refres	h	Click this icon t	o refresh files list.			

Kerresh	
<b>(b)</b> Back	Click this icon to return to the upper directory.
🧭 Create	Click this icon to add a new folder.
<b>Current Path</b>	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB diskette can be shared for other user through FTP.

#### 4.14.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. If you want to remove the storage disk from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

USB Application >> USB [	isk Status	
USB Mass Storage Device	Status	
Connection Status: No	Disk Connected	Disconnect USB Disk
Disk Capacity: 0 MB		
Free Capacity: 0 MB	Refresh	
USB Disk Users Connecte	d	Refresh
Index Servic	e IP Address(Port)	Username
Note: If the write protec can be written to	t switch of USB disk is turned on, the USB dis it.	k is in <b>READ-ONLY</b> mode. No data
Connection Status	If there is no USB storage disk c <b>Disk Connected</b> " will be shown	U
Disk Capacity	It displays the total capacity of the	he 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.

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

#### 4.14.5 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

USB	App	lication	>>	Svs	οa	Expl	lorer
030	мрр	rcauon	~~	зуы	iog	LYbi	orei

Web Syslog	USB Syslog	
Enable Web Syslog	yslog Type User 👻 Display Mod	<u>Refresh</u>   <u>Clear</u>   e Stop record when fulls
Time		Message

#### For Web Syslog

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.

Display Mode

There are two modes for you to choose.

Stop record when fulls	*
Stop record when fulls	
Always record the new even	t

**Stop record when fulls** – when the capacity of syslog is full, the system will stop recording.

**Always record the new event** – only the newest events will be recorded by the system.

TimeDisplay the time of the event occurred.

Message Display the information for each event.

#### For USB Syslog

This page displays the syslog recorded on the USB storage disk.

	209.100			
Time	Log Type		Message	
Folder: n/a	File: n/a	Page: n/a	Log Type: n/a	
Web Syste	og	USB Syslog		
Web Suel		HCD Surlag		

Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

#### 4.15 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



#### 4.15.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

#### System Status

lodel Name Firmware Version Build Date/Time	: Vigor2850Vn : 3.3.6_RC6 : Jun 1 2011 18:00:07	,			
		LAN			
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-1D-AA-00-00-00	192.168.1.1	255.255.255.0	Yes	8.8.8.8
LAN2	00-1D-AA-00-00-00	192.168.3.1	255.255.255.0	Yes	8.8.8.8
LAN3	00-1D-AA-00-00-00	192.168.5.1	255.255.255.0	Yes	8.8.8.8
LAN4	00-1D-AA-00-00-00	192.168.7.1	255.255.255.0	Yes	8.8.8.8
IP Routed Subnet	00-1D-AA-00-00-00	192.168.2.1	255.255.255.0	Yes	8.8.8.8
		Wireless LAN			
MAC Address	Frequency	Domain	Firmware Versio	in SSID	
00-1D-AA-00-	00-00 Europe		"2.2.0.7"	DrayT	ek
		WAN			
Link Status	MAC Address	Connectio	on IP Address	Default Ga	teway
WAN1 Disconnecte	ed 00-1D-AA-00-00-01	. PPPoE			
WAN2 Connected	00-1D-AA-00-00-02	Static IP	172.16.3.10	2 172.16.1.1	
WAN3 Disconnecte	ed 00-1D-AA-00-00-03				

		VoIP		
Port	Profile	Reg.	In/Out	
Phone1		No	0/0	
Phone2		No	0/0	

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware built.
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.
SSID	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.

#### 4.15.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

CPE Settings				
ACS Server On	Internet 💌			
ACS Server				
URL				]
Username				
Password				
CPE Client				
🔘 Enable 🛛 💿 Disable				1
URL	http://172.16.3.102:80	69/cwm/CRN.htm		
Port	8069			
Username	vigor			
Password	•••••			
Inform Settings				
O Disable				
💿 Enable				
Interval Time	900	second(s)		
ttings				
<ul> <li>Disable</li> </ul>				
🔘 Enable				
Server IP				
Server Port		3478		
Minimum Keep Alive	Period	60	second(s)	
Maximum Keep Alive	Period	-1	second(s)	
	OK			

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.
	Server Port – 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.

#### 4.15.3 Administrator Password

This page allows you to set new password.

System Maintena	nce >> Administrator Password Setup		
Administrator Pas	sword		
	Old Password	••••	]
	New Password	•••••	]
	Confirm Password	•••••	]
Old Password		•	factory default setting for

**New Password** Type in new password in this field.

**Confirm Password** Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.



#### 4.15.4 User Password

This page allows you to set new password for user operation.

# User Password

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

0K

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this field.

**Confirm Password** Type in the new password again.

When you click **OK**, the login window will appear. Please use the new password to access into the web configurator again.

#### 4.15.5 Configuration Backup

#### **Backup the Configuration**

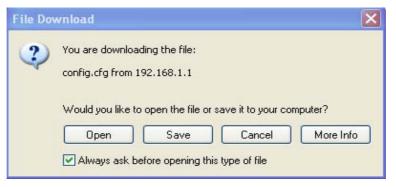
Follow the steps below to backup your configuration.

System Maintenance >> Configuration Backup

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

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.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

Save As		? ×
Save in:	🕝 Desktop 🔹 🕜 🔊 💬 🛄 -	
My Recent Documents Desktop My Documents	My Documents     My Computer     My Network Places     My S-COM Lite     Annex A     mmm     MWSnap300     TeleDanmark     Tools     config     v2k2_232_config_1     V2k6_250_config_1	
My Computer		
	File name: config	Save
My Network	Save as type: Configuration file	Cancel

4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

**Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

#### **Restore Configuration**

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Mainte	System Maintenance >> Configuration Backup Configuration Backup / Restoration					
Configuration						
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.

#### 4.15.6 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

ysLog Access Setup	Mail Alert Setup
Enable	Enable Send a test e-mail
Syslog Save to:	SMTP Server
✓ Syslog Server USB Disk	SMTP Port 25
Router Name	Mail To
Server IP Address	Return-Path
Destination Port 514	Authentication
Enable syslog message:	User Name
✓ Firewall Log	Password
VPN Log	Enable E-Mail Alert:
User Access Log	DoS Attack
🗹 Call Log	✓ IM-P2P
WAN Log	
Router/DSL information	
AlertLog Setup	
Enable	
AlertLog Port 514	

SysLog Access Setup	Enable - Check Enable to activate function of syslog.			
	<b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.			
	Check <b>USB Disk</b> to save the log to the attached USB storage disk.			
Router Name	Display the name for such router configured in <b>System</b> Maintenance>>Management.			
	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.			
Syslog Server IP	The IP address of the Syslog server.			
<b>Destination Port</b>	Assign a port for the Syslog protocol.			
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.			
AlertLog Setup	Check "Enable" to activate function of alert log.			
	Type the port number for alert log. The default setting is 514.			
Mail Alert Setup	Check "Enable" to activate function of mail alert.			
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.			
SMTP Server	The IP address of the SMTP server.			

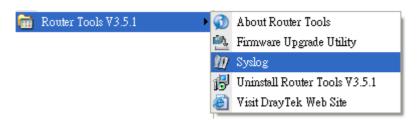


Mail To	Assign a mail address for sending mails out.				
Return-Path	Assign a path for receiving the mail from outside.				
Authentication	Check this box to activate this function while using e-mail application.				
User Name	Type the user name for authentication.				
Password	Type the password for authentication.				
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.				

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.

🏽 DrayTe	ek Syslog	3.6.1							
Controls	6	iets	192.168.1.1 Vigor series RX Packets 1470	•	-wan se F	atus Gateway IF  WAN IP ( 		TX Packets 0 RX Packets 0 0	TX Rate 0 RX Rate 0
Firewall I	Log VPN	Log User Acc	ess Log Call Log	WAN Log	Others	Network	Information Ne	t State	
On Lir	ne Routers			Host N	ame:		vivian		
	Address	Mask	MAC	NIC De	scription:		SiS 900-Based I	PCI Fast Ethernet Adap	oter - Packet S( 🔽
192	2.168.1.1	255.255.2	00-50-7F-54-6	NIC Inf	ormation -				
				MAC A	ddress:	00-1	1-D8-E4-58-CE	Default Geteway:	192.168.1.1
				IP Add	ress:	192.1	68.1.10 🗸	DHCP Server:	192.168.1.1
				Subne	t Mask:	25	5.255.255.0	Lease Obtained:	Mon Jan 22 01:28:23 2007
<		J	>	DNS S	ervers:	168.9	5.1.1	Lease Expires:	Thu Jan 25
	R	efresh						Ecuse Expires.	01:28:23 2007
ADSL St	tatus Mode		State		peed	Do	wn Speed	SNR Margin	Loop Att
Г		— r							

#### 4.15.7 Time and Date

It allows you to specify where the time of the router should be inquired from.

nformation		
Current System Time	2010 Apr 3	2 Fri 9 : 1 : 58 Inquire Time
ietup		
🔘 Use Browser Time		
💿 Use Internet Time C	lient	
Server IP Address		pool.ntp.org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Savir	ig	
Automatically Update	Interval	30 min 🔽

<b>Current System Time</b>	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.				
<b>Time Protocol</b>	Select a time protocol.				
Server IP Address	Type the IP address of the time server.				
Time Zone	Select the time zone where the router is located.				
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.				
Automatically Update Interval	Select a time interval for updating from the NTP server.				
Clipto OV to some these soft	1				

Click **OK** to save these settings.

#### 4.15.8 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

	Management Port Setup				
	🔄 💿 User Define Ports	🔘 Default Ports			
	Telnet Port	23 (Default: 23)			
he Internet	HTTP Port	80 (Default: 80)			
	HTTPS Port	443 (Default: 443			
	FTP Port	21 (Default: 21)			
	SSH Dort				
		22 (Default: 22)			
	SNMP Setup				
ernet	Enable SNMP Agent				
Subnet Mask	Get Community	public			
	Set Community	private			
*	Manager Host IP				
~	-	public			
*					
		10			
	Irap limeout	10 seconds			
	ок				
Type in the route	r name provided by IS	S D			
	· ·				
	-				
		· ·			
the box(es) to spe					
	•				
		nackets from the Intern			
Check the check		packets from the Intern led by default.			
	Type in the route Enable the check from the Internet	Image: Community         Subnet Mask         Image: Host IP         Image:			

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.

Default Ports	Check to use standard port numbers for the Telnet and HTTP			
	servers.			
User Defined Ports	Check to specify user-defined port numbers for the Telnet,			

HTTP and FTP servers.

Enable SNMP AgentCheck it to enable this function.Get CommunitySet the name for getting community by typing a proper<br/>character. The default setting is public.



Set Community	Set community by typing a proper name. The default setting is <b>private.</b>
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP 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	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

#### 4.15.9 Reboot System

The Web Configurator 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 ?
<ul> <li>Using current configuration</li> </ul>
<ul> <li>Using factory default configuration</li> </ul>
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 **Reboot Now**. To reset the router settings to default values, check **Using factory default configuration** and click **Reboot Now**. The router will take 5 seconds to reboot the system.

**Note:** When the system pops up Reboot System web page after you configure web settings, please click **Reboot Now** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.



#### 4.15.10 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

1.3			
Select a firmware file.			
		Browse	
Click Upgrade to upload the file.	Upgrade		

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.3.6_RC6	
Firmware Upgrade Procedures:	
<ol> <li>Click "OK" to start the TFTP server.</li> <li>Open the Firmware Upgrade Utility or other 3-party TFTP client software.</li> <li>Check that the firmware filename is correct.</li> <li>Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.</li> <li>After the upgrade is compelete, the TFTP server will automatically stop running.</li> </ol>	
Do you want to upgrade firmware ?	

Click OK. The following screen will appear. Please execute the firmware upgrade utility first.



For the detailed information about firmware update, please go to Chapter 5.

#### 4.15.11 Activation

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

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

System Maintenance >> Activati	on	Activate via interface : auto-selected 💙
Web-Filter License [Status:Not Activated]		<u>Activate</u>
Authentication Message		
WebFilter, service not ad	tivate 2010-08-16 07:58:36:	
		V
-	alert or syslog, please configure the provider, the configuration of the OK Cancel	ne SysLog/Mail Alert Setup page. 9 function will be reset.
Activate via Interface	Choose WAN interface used Web Content Filter.	l by such device for activating
		auto-selected <mark>&gt;&gt;</mark> auto-selected WAN 1 WAN 2 WAN 3
Activate	The <b>Activate</b> link brings yo www.vigorpro.com to finish the router.	u accessing into the activation of the account and
Authentication Message	As for authentication inform authenticating will be displa reference.	ation of <b>web filter</b> , the process of yed on this field for your



Below shows the successful activation of Web Content Filter:

	<u>Activate</u>
04-27]	
support@draytek.com,	2000-01- 🖄



#### 4.16 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.



#### 4.16.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Trigger** 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

riggered Packet Header	Ret
HEX Format:	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00 00 00 00 00 00 00	
00 00 00 00 00 00 00-00 00 00 00 00 00 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	
Decoded Format:	
0.0.0.0 -> 0.0.0.0	
Pr 0 len 0 (0)	

Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

#### 4.16.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

```
Diagnostics >> View Routing Table
```

```
Current Running Routing Table

Key: C - connected, S - static, R - RIP, * - default, ~ - private

* 0.0.0.0/ 0.0.0.0 via 172.16.3.1, WAN1
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
C 172.16.3.0/ 255.255.255.0 is directly connected, WAN1
```

Refresh

Click it to reload the page.

#### 4.16.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

thernet ARP Cache	Table	<u>Clear</u>   <u>Refresh</u>
IP Address	MAC Address	<u>:</u>
192.168.1.10	00-0E-A6-2A-D5-A1	
172.16.3.112	00-40-CA-6B-56-BA	
172.16.3.132	00-05-5D-E4-ED-86	
172.16.3.20	00-0D-60-6F-83-BC	
172.16.3.121	00-0C-6E-E7-79-99	
172.16.3.141	00-11-2F-C7-39-0B	
172.16.3.133	00-50-7F-23-4D-B1	
172.16.3.179	00-11-2F-4B-15-F2	
172.16.3.21	00-05-5D-A1-2B-FF	
172.16.3.2	00-11-D8-68-0D-AE	
172.16.3.18	00-50-FC-2F-3D-17	
172.16.3.151	00-50-7F-2F-33-FF	
172.16.3.19	00-0D-60-6F-89-CA	

Refresh
Clear

Click it to reload the page. Click it to clear the whole table.

#### 4.16.4 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 s	erver: Running				1
Index 1	IP Address 192.168.1.10	MAC Address OO-OE-A6-2A-D5-A1	Leased Time 0:00:02.630	HOST ID ok-lccgjyiy075u	

Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

#### 4.16.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

```
Diagnostics >> NAT Sessions Table
```

Drivete TD	· Port	#Pseudo Port	Peer IP	· Port	Interfore	
Frivace if	.FOIC	#FSEudo Forc		.FOIC		
.92.168.1.11	2491	52078	24.9.93.189	443	UAN1	
92.168.1.11	2493	52080	207.46.25.2	80	WAN1	
.92.168.1.10	3079	52665	207.46.5.10	80	WAN1	

Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

## 4.16.6 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

Diagnostics >> Pi	ing Diagnosis				
Ping Diagnosis					
			a LAN PC or you n, please select	u don't want to sp t "Unspecified".	ecify
	Ping thro	ough: Unspecifi	ied 🔽		
	Ping to: Result	Host / IP V Host / IP DNS Gateway 1	IP Address:		<u>Clear</u>
		Gateway 2 Gateway 3			~
					V

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 in the IP address of the Host/IP 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.

#### 4.16.7 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.



Click Diagnostics and click Data Flow Monitor to open the web page. You can click IP Address, TX rate, RX rate or Session link for arranging the data display.

Diagnostics >> Data Flow Monitor

#### 🗹 Enable Data Flow Monitor

		Refresh Seconds: 1	10 🚩 Page: 1 🚩	<u>R</u>	efresh
Index	IP Address	<u>TX rate(Kbps)</u>	<u>RX_rate(Kbps)</u> 🗠	Sessions	Action
1	192.168.1.10_CARRIE-0C7CB251	0	0	2	Block
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak	
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.

#### **Enable Data Flow** Monitor

Check this box to enable this function.

**Refresh Seconds** 

Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.



Refresh	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	<b>Block</b> - can prevent specified PC accessing into Internet within 5 minutes.

Page: 1	~	<u>Refresh</u>
Kbps)	Sessions	Action
		<u>Block</u>

**Unblock** – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.

Page	e: 1 💌	<u>Refresh</u>
<u>s)</u>	Sessions	Action
	blocked / 299	<u>Unblock</u>

Current /Peak/Speed

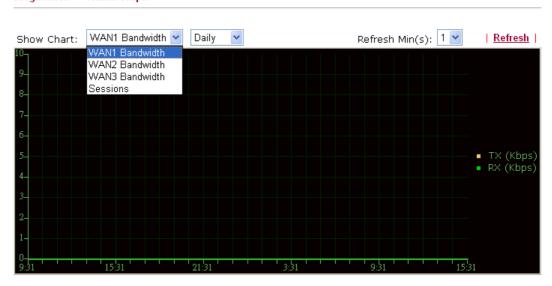
**Current** means current transmission rate and receiving rate for WAN interface.

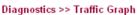
**Peak** means the highest peak value detected by the router in data transmission.

**Speed** means line speed specified in **WAN>>General Setup**. If you do not specify any rate at that page, here will display **Auto** for instead.

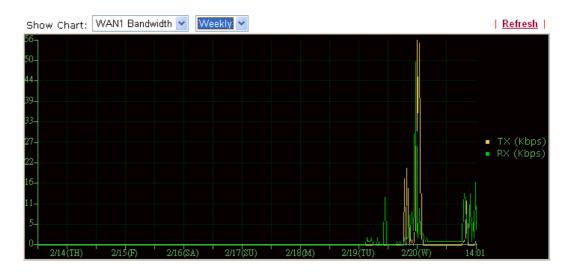
#### 4.16.8 Traffic Graph

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.

#### 4.16.9 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 >> T	race Route		
Trace Route			
	Trace through:	Unspecified 💌	
	Protocol:		
	Host / IP Address:	ICMP UDP	Run
	Result	ODF	<u>Clear</u>

Trace through	Use the drop down list to choose the interface that you want to ping through.
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

#### 4.16.10 Web Firewall Syslog

Such page provides real-time syslog and displays the information on the screen.

#### For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

USB Application >> Syslog Explore	r	
Web Syslog	USB Syslog	
Enable Web Syslog	Syslog Type User 💌 Display Mo	<u>Refresh</u>   <u>Clear</u>   de Stop record when fulls   ❤
Time		Message

Enable Web Syslog Syslog Type	Check this box to enable the function of Web Syslog. Use the drop down list to specify a type of Syslog to be displayed.	
	e User ♥ User ♥ Firewall Call ₩AN VPN All	
	There are two modes for you to choose.	
Display Mode	There are two modes for you to choose.	
Display Mode	Stop record when fulls	
Display Mode	-	
Display Mode	Stop record when fulls	
Display Mode	Stop record when fulls Stop record when fulls Always record the new event Stop record when fulls – when the capacity of syslog is full,	
Time	Stop record when fulls         Stop record when fulls         Always record the new event         Stop record when fulls – when the capacity of syslog is full, the system will stop recording.         Always record the new event – only the newest events will be	



#### For USB Syslog

This page displays the syslog recorded on the USB storage disk.

USB Application >> Syslog Explorer				
Web Syste	og	USB Syslog		
Folder: n/a	File: n/a	Page: n/a	Log Type: n/a	
Time	Log Type		Message	

Time	Display the time of the event occurred.
Log Type	Display the type of the record.
Message	Display the information for each event.

This page is left blank.

#### Vigor2850 Series User's Guide



# 5.1 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SAMBA server or FTP server.

Samba service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

USB Application >> USB Disk Status				
USB Mass Sto	rage Device Status			
	Status: Disk Connect	red	Disconnect USB Disk	
Disk Capacit				
USB Disk Use	ers 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

General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	Default 💌
Samba Service Settings(Network Neig	hborhood)
⊙Enable ↓ Disable	
Access Mode	
💿 LAN Only i 🔘 LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor
<ol> <li>Multi-session ftp download v connection mechanism, such as better performance.</li> </ol>	, 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 be the same as the host name. The workgroup name and the hos

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	20
Access Rule	
File	🗹 Read 🛛 Write 🗌 Delete
Directory	🗹 List 🛛 Create 🗖 Remove
The folder name can only o	contain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( )

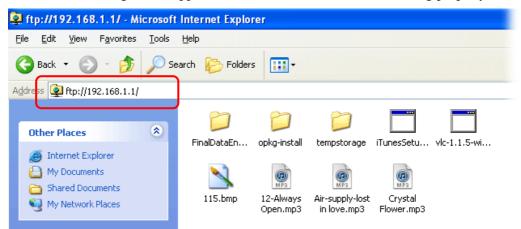
4. Click **OK** to save the configuration.

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	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: User1		
	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 <u>using Web Folders</u> .		
	Log on anonymously		

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



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

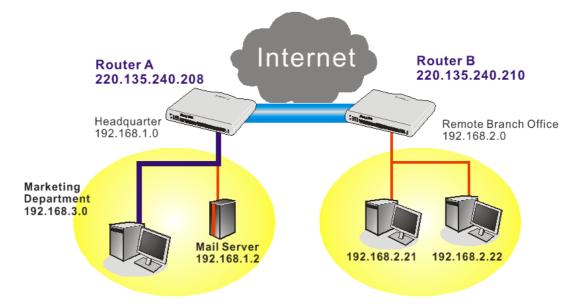
USB Application >> USB Disk Status

USB Mass	Storage Device	Status		
Connection Status: Disk Connected Disconnect USB				SB Disk
Write Protect Status: No				
Disk Capacity: 2009 MB				
Free Capacity: 1610 MB Refresh				
USB Disk	Users Connecte	d		<u>Refresh</u>
Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.10(1963)	user1	Drop

Now, users in LAN of Vigor2710 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application** >>**USB User Management.** 

## 5.2 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:** 

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 Dial-In PPP		IP Address Assignment fo (When DHCP Disable set)	
Authentication	PAP or CHAP \star	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Nutual 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 **IPSec General Setup**, such as the pre-shared key that both parties have known.



VPN IKE/IPSec General Setup			
Dial-in Set up for Remote Dial-in users	s and Dynamic IP Client (LAN to LAN).		
IKE Authentication Method			
Pre-Shared Key	••••		
Confirm Pre-Shared Key	•••••		
IPSec Security Method			
🗹 Medium (AH)			
Data will be authentic, but	t will not be encrypted.		
High (ESP) 🛛 🗹 DES 🔍 3DES 🔍 AES			
Data will be encrypted and	d authentic.		

- 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	Both ○ Dial-Out ○ Dial-in	
	VAN1 First 💙	Idle Timeout Enable PING PING to the IP	300 second(s) to keep alive	

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	Link Type	64k bps 👻
О РРТР	Username	???
IPSec Tunnel	Password	
C L2TP with IPSec Policy None	PPP Authentication	
Dial Number for ISDN or	VJ Compression	💿 On 🔘 Off
Server IP/Host Name for VPN. (such as 5551234, 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.509)	9)
	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	Link Type	64k bps 💙
⊙ РРТР	Username	draytek
O IPSec Tunnel	Password	••••
C L2TP with IPSec Policy None	PPP Authentication	PAP/CHAP 🗸
	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) 220.135.240.210	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509 None IPSec Security Method Medium(AH) High(ESP) DES without Advanced Index(1-15) in <u>Schedule</u>	Authentication

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.505         None         IPSec Security Method         ♥ Medium(AH)         High(ESP)       ♥ DES ♥	) Э) 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		
🗹 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 remote	e 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 to single WAN supports this )	o this VPN tunnel ( Only
Local Network Mask	255.255.255.0		
	More		
	OK (	Clear Cancel	

#### Settings in Router B in the remote 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 D	)ial-In Users
Dial-In PPP PAP or CHAP	(When DHCP Disable set)	
Authentication	Assigned IP range	192.168.2 200
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 **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 Dynamic IP Client (LAN to LAN).			
IKE Authentication Method				
Pre-Shared Key	••••			
Confirm Pre-Shared Key	•••••			
IPSec Security Method				
Medium (AH)				
Data will be authentic, but	will not be encrypted.			
High (ESP) 🕑 DES 🕑 3DES 🗹 AES				
Data will be encrypted and	authentic.			
	OK Cancel			

- 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 Branch 1	Call Direction 💿 Both 🔿 Dial-Out 🔘 Dial-in			
VPN Dial-Out Through WAN1 First V Netbios Naming Packet OPass OBlock	Idle Timeout     300     second(s)       Image: Description of the IP     Image: Description of 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	Link Type	64k bps 😽
О РРТР	Username	???
<ul> <li>IPSec Tunnel</li> </ul>	Password	
O L2TP with IPSec Policy None	PPP Authentication	
Dial Number for ISDN or	VJ Compression	💿 On 🔘 Off
Server IP/Host Name for VPN. (such as 5551234, 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.509	9)
	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.

Type of Server I am calling	Link Type	64k bps 🛛 😪
● РРТР	Username	draytek
O IPSec Tunnel	Password	••••
C L2TP with IPSec Policy None	PPP Authentication	PAP/CHAP 🔽
	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Gerver IP/Host Name for VPN. Such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Meth Pre-Shared Key	od
220.135.240.208	IKE Pre-Shared Key	
	O Digital Signature(X.	509)
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES with	nout Authentication
	Advanced	
	Index(1-15) in <u>Schedu</u>	I <mark>le</mark> 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		
PPTP IPSec Tunnel L2TP with IPSec Policy None	Username Password VJ Compression	??? 
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 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) ♥ DES ♥	-

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

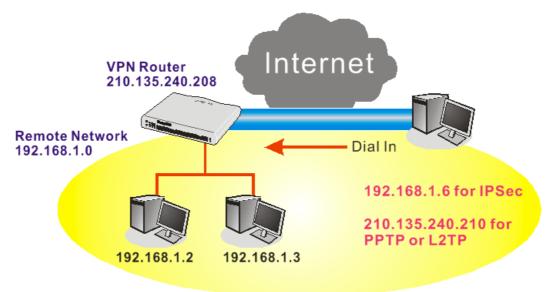
Allowed Dial-In Type		
РРТР	Username	draytek
	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	🗌 Digital Signature(X.509	)
or Peer ID	None 🗸	
	IPSec Security Method	
	Medium(AH)	
		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 single WAN supports this	to this VPN tunnel ( Only )
Local Network Mask	255.255.255.0		/
	More		
	ОК СІ	ear Cancel	

# **5.3 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.

	ion. For more in	connection using fomation, please	to computer in a pre-shared key e read the article
Q240262 in the M	Confi		
	L	gare	
Chan 1 Dial ha ICI			
Step 1. Dial to IS If you have alrea		olic IP, you can si	kip this step.
		olic IP, you can si	kip this step.
If you have alrea	dy gotten a put	olic IP, you can s	
	dy gotten a put	olic IP, you can s	Dial
If you have alrea	dy gotten a put	olic IP, you can si	

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,



iession Name:	Office
PN Server IP/HO	ST Name(such as 123.45.67.89 or draytek.com)
192.168.1.1	
Jser Name :	draytek_user1
Password :	interaction
Type of VPN	
O PPTP	OL2TP
IPSec Tunr	nel OL2TP over IPSec
PPTP Encryption  No encrypt  Require en  Maximum s	tion
	gateway on remote network

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.

My IP :	172.16.3.10	0 🗸
Type of IPSe	c	
O Standard	d IPSec Tunnel	
Remot	e Subnet :	0,0,0,0
Remot	e Subnet Mask :	255 . 255 . 255 . 0
💿 Virture I	P Dray	Tek Virture Interface 🛛 💊
💿 Obt	ain an IP address	automatically (DHCP over IPSec
🔿 Spe	cify an IP address	
IP	Address:	192 . 168 . 1 . 201
Sut	onet Mask:	255 , 255 , 255 , 0
ecurity Met	nod	
	AH) 🤇	• High(ESP)
O Medium(		
	~	DES 😽
O Medium( MD5	thod	DES
O Medium( MD5		DES
Medium( MD5 Authority Me  Pre-shar	ed Key : *****	DES
Medium( MD5 Authority Me  Pre-shar		DES V

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.

	s(such as 123.45.67.89 or draytek.com)
192.168.1.1	
User Name : dray	tek_user1
Password : ****	*
Type of VPN	
• PPTP	OL2TP
O IPSec Tunnel	OL2TP over IPSec
PPTP Encryption	
O No encryption	°,
Require encryption	*
Maximum strength	encryption

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

## 5.4 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

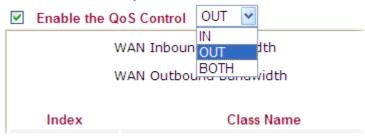
index a	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1 B	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
WAN2 B	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup
WAN3 D	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
lass Rul	le	10000Kbps/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 Mar	nagement >> Quality of Service	
WAN2 General	I Setup e QoS Control BOTH 🔽	
	WAN Inbound Bandwidth	10000 Kbps
	WAN INDOUND BANGWIGHT	10000 Kbps
	WAN Outbound Bandwidth	10000 Kbps
t		Device of the second data Data is
		be smaller than the real bandwidth to ggested to set the bandwidth value for
		cal network speed provided by ISP to
	the QoS performance.	
maximize	the Qob periornance.	

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 Dele	te	
		(	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 C	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	< 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

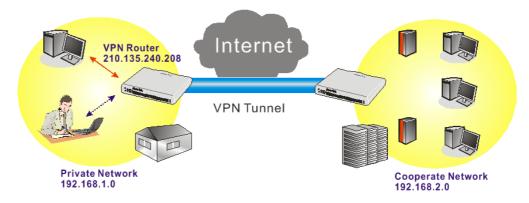
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
WAN2	Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Active	Status	Setur
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%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

Class Rule			
Index	Name	Rule	Service Type
Class 1	E-mail	Edit	
Class 2	HTTPS	Edit	<u>Edit</u>
Class 3		<u>Edit</u>	

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 Status NO Local Address **Remote Address** Service Type CodePoint 1 Empty Delete Add 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**.

## 5.5 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	3					
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	elease 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		KAITEU	eruncation
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 Mod	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 s VigorPro 5510 s		Datashee	t
				VigorPro 5300 s	series	R&TTE C	ertification
Smart VPN Client	2009/05/25	3.6.3	MS-Windows XP	All Module	s		
		( Multi- language )	MS-Vista				
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 se			
				MinorPro 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**

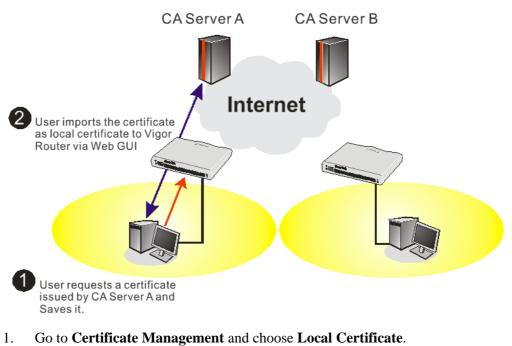
The web page also can guide you to upgrade firmware. Note that this example is running over Windows OS (Operating System).

- 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 >> Firm	ware Upgrade
Web Firmware Upgrade	
Select a firmware file.	Browse. Id the file. Upgrade
TFTP Firmware Upgrade fron	n LAN
Current Firmware Vers	ion: 3.3.6_RC4
Firmware Upgrade Pro	cedures:
3. Check that the 4. Click "Upgrade" (	rt the TFTP server. are Upgrade Utility or other 3-party TFTP client software. firmware filename is correct. on the Firmware Upgrade Utility to start the upgrade. de is compelete, the TFTP server will automatically stop running.
Do you want to upgrad	e firmware ? OK

- 3. Select a firmware file by clicking **Browse**.
- 4. Click **Upgrade** to perform the firmware upgrade.

# **5.6 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.

Senerate 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

Name Subject		Status	Modify
Local /C=TW/O=Draytek/emailAddress		Requesting	View Delete
GENERATE X509 Loc	IMPORT REFRESH		
MIIBqj( Bgkqhk: A4GNAD( 3wDeQy du84t22 oCkwJw hkiG9w uRLq4C I9Fqkj(	GIN CERTIFICATE REQUEST CCARMCAQAwQTELNAkGAIUEBhMCVFcxEDAO: (G9w0BCQEWEXByZXN2QGRyYX10ZW=uY29t): CBIQKBgQDPioahu/gFQaYB1ce50ERSDfWk: coV1LBJz2IDF0xjX6ip7ev187twwTsg41g btWBdHD4W5C8VmSyDjShLhjdxVYPWpNKVI; UKoZIhvcNAQkOMRowCDAWBgNVHREDDAM. DBAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToen LEi6nV4hMRytcx2pEZ6sMarSgRREr86RoO; UN1hip4TCjecSNN2jmQoSWU+Bce8TG+SCB; D0 CERTIFICATE REQUEST	MIGHMAOGCSqGS1 hIdHblo1kt9cTc Z6Qk/rGhuVTKd9 cOT2RZjkRMaHEU ggtkcmF5dGVrLn n1tHQbcwjXvg/t 3JxOI45560xCZ/	ID3DQEBAQUA ALUDaFk6s8d Jj6PlcrnkP7 JpVpwIDAQAB MVbTANBgkq 7NF1zTJiHh /NIGh9VQ911

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	
	rtificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, yo elf to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more e you request.
Select a task: ⊙Retrieve the CA certificate or c	ertificate revocation list
<ul> <li>Request a certificate</li> <li>Check on a pending certificate</li> </ul>	

#### Select Advanced request.

Microsoft Certificate Services vigor	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
User certificate request. User Certificate	
Advanced request	
Next >	

Select Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file

	ificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certi rmine the certificates that you can obtain.	icatio
Submit a certifica	e request to this CA using a form.	
Submit a certifica	e request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.	
	ate for a smart card on behalf of another user using the Smart Card Enrollment Station. collment agent certificate to submit a request for another user.	
	Next	>

Microsoft Certifica	e Services vigor	Home
Submit A Save	Request	
	encoded PKCS #10 certificate request or PKCS #7 re equest field to submit the request to the certification au	enewal request generated by an external application (such as a web thority (CA).
aved Request:		
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUEST MIIBajCCARMCAQAwQTELMAKGAIUEBHMCVFCXEDAO BgkqhkiG9v0BCQEWEXByZXN2QGRYYX10ZWsuY29t A4GMADCB1QKBgQDQYB7m0ZFfFhW9/IEQnG03Xk++ hX4bpB9cUF9d1oACGGiM/tcB0ckkdzdPFVIXcP3 x/G0A7CTV0/fg2pxrcCw1JTjL5jS0/Bn9v50951G v	
ertificate Templa	Browse for a file to insert.	
	Administrator	
Additional Attribut	Administrator Authenticated Session Basic EFS	
Attributes:	EFS Recovery Agent User IPSEC (Offline request) Router (Offline request)	
-	Subordinate Certification Authority Web Server	Submit >

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-----..."

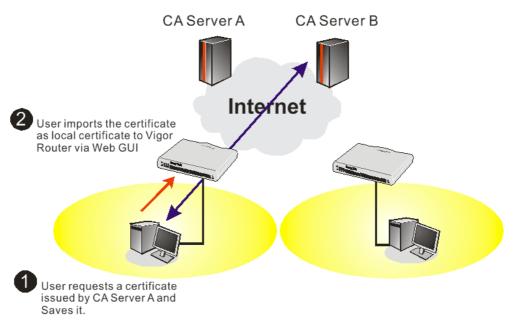
ocal /C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
NERATE IMPORT REFRESH		
X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAKGA1UEBhMCVFcxEDAO BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWk 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg41g du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI oCkwJwJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToeu uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgREr86R00	MIGIMAOGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq t7kFlzTJiHh

Certificate Management >> Local Certificate

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

## 5.7 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	
當案(E) 編輯(E) 檢視(Y) 我的最愛(A) 工具(I) 說明(E)	
3 上-頁 • 🐑 · 🖹 🙆 🏠 🔎 搜尋 🧙 我的最爱 🜒 媒體 🤣 🍰 🛃 • 🍇	
性 (2) ( a) http://172.16.2.179/certary/	
san <sup>24</sup> • 🔽 建築 • 🟒 醒目提示 🛛 🕅 選項 🛛 対鎖快顕視窗 (319) • 🕁 Hotmail	🏜 Messenger [ ใญ 我的 MSN
	Home
Microsoft Cartificate Senices vinor	
Microsoft Certificate Services vigor	
Velcome You use this web site to request a certificate for your web browser, e-mail client, or other secure will be able to securely identify yourself to other people over the web, sign your e-mail message	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 secure will be able to securely identify yourself to other people over the web, sign your e-mail message depending upon the type of certificate you request.	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 secure will be able to securely identify yourself to other people over the web, sign your e-mail message depending upon the type of certificate you request.	program. Once you acquire a certificate, you
Microsoft Certificate Services - vigor         Welcome         You use this web site to request a certificate for your web browser, e-mail client, or other secure will be able to securely identify yourself to other people over the web, sign your e-mail message depending upon the type of certificate you request.         Select a task:	program. Once you acquire a certificate, you

- 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 (II) 🌀 上一頁 🔹 💿 · 🖹 😰 🏠 🔎 搜尋 📩 我的最爱 🜒 媒體 🔗 🔗 - 🌺 🔜 - 🎎 網址 (D) 🕘 http://172.16.2.179/certsrv/certcarc.asp ✓ ● 移至 連結 msn<sup>M</sup> -🖌 🔎 搜尋 🔹 🥒 醒目提示 🛛 🕺 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🚢 Messenger [ 2 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.

## 5.8 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.

## 5.8.1 Creating an Account via Vigor Router

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

CSM >> Web Conte	nt Filter Profile		
Neb-Filter License			Activa
Status: <mark>Not Activa</mark>	ated]		
Setup Query Serve	auto-selected		Find more
Setup Test Server	p Test Server auto-selected 1		Find more
Neb Content Filter	Profile Table:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>	Default	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	

## Or

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

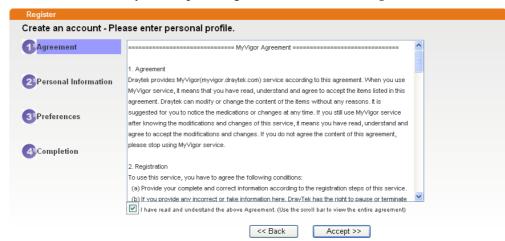
System Maintenance >> Activation	Activate via interface : auto-selected 💙	
Web-Filter License [Status:Not Activated]		<u>Activate</u>
Authentication Message		
Activated Wiz, Authenticate is continuously, connect t OO:O4:55	to the server, 2000	)-01-01

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

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

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

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



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

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
		(3 ~ 20 characters)
Deserved	Password:*	••••
2 Personal		(4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	tion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND

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

Register		
Create an account -	Please enter personal profile.	
	How did you find out about this website?	Internet 🗸
<b>U</b> .g. comon	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.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

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

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site GO
Register Confirm	
	Thank for your register in VigorPro Web Site The Register process is completed
	Close Login

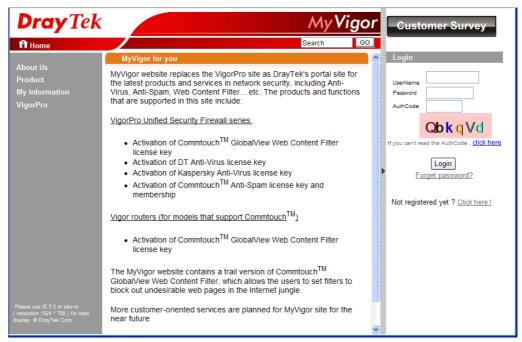
10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

	K	for your purchas	ment to register. istration entitles you to u ed product and receive n cts and services!	
LOGIN				
	UserName :	Mary		
	Password :	••••		
	Auth Code :	T4he1C	T4he1C	
		If you cannot read the wo	rd, <u>oliok here</u>	
		Forgotten password	1 <mark>? Login</mark>	
	Don't have a	MyVigor Account ?	Create an account nov	<u>v</u>
	lf you .	are having difficulty logging in, ( Customer Service : (886)		

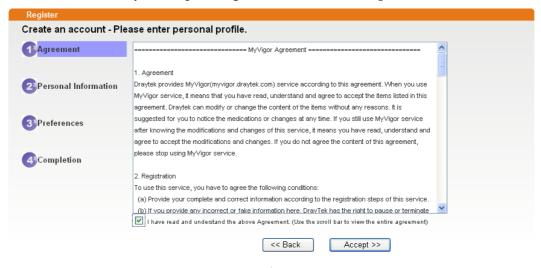
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

## 5.8.2 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.



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
Personal	Password:*	(4~20 characters : Do not set the same as the username.)
Information	Confirm Password:*	(4~20 characters : Do not set the same as the userhame.)
	Personal Informat	ion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND
	Career:*	Supervisor 🗸

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

Register		
Create an account -	Please enter personal profile.	
Agreement	How did you find out about this website?	Internet
<b>U</b> igroomoni	What kind of anti-virus do you use?	AntiVir
2 Personal	I would like to subscribe to the MyVigor e-letter.	V
Information	l would like to receive DrayTek product news.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>

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



6. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

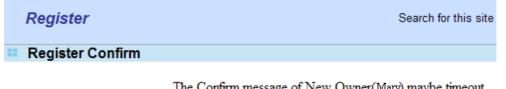
\*\*\*\*\* This is an automated message from myvigor draytek.com.\*\*\*\*\*

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



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

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

	Please take a moment to register. Membership Registration entitles you to upgrade firm for your purchased product and receive news about upcoming products and services!	ware
LOGIN		
UserName :	Mary	
Password :	••••	
Auth Code :	T4he1C	
	If you cannot read the word, <u>click here</u>	
	Forgotten password? Login	
Don't have a N	MyVigor Account ? Create an account now	_
L		

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

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

This page is left blank.

#### Vigor2850 Series User's Guide

# **6** 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.

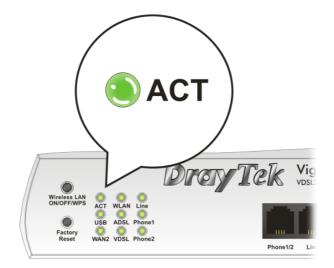
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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.

## 6.1 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.

## 6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

#### For Windows



The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.

eth0	Properties		?
General	Authentication	Advanced	
Connec	et using:		
<b>B</b>	ASUSTeK/Broad	com 440x 10/100 l	Ir <u>C</u> onfigure
This c <u>o</u>	nnection uses th	e following items:	
	Client for Micro File and Printer QoS Packet So Internet Protoc	Sharing for Micros	oft Networks
	nstall	<u>U</u> ninstall	Properties
Tran wide	area network pr	Protocol/Internet F otocol that provide: onnected networks	
-	-	ition area when cor connection has limi	nnected ted or no connectivity
			OK Cancel

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

ieneral	Alternate Configura	tion
this cap		gned automatically if your network supports ou need to ask your network administrator for
<u>o o</u> l	otain an IP address a	utomatically
OU	se the following IP ac	Idress:
IP ad	ddress:	10 AL - 40
Subr	net mask:	10 D1 01
Defa	ult gateway:	
0	otain DNS server add	dress automatically
OU	se the following DNS	server addresses:
Prefe	erred DNS server:	· · · · · · · · · · · ·
Alter	nate DNS server.	
		Advanced

## 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.

and the second second second second		Network	(
how All	Displays So	Network Startup Disk	
		Location: Automatic	
		Show: Built-in Ethernet	
	TCF	P/IP PPPoE AppleTalk Proxies Ethernet	
Co	nfigure IPv4:	Using DHCP	
	IP Address		
		: 255.255.255.0 DHCP Client ID:	ler tease
	Router	(If require	d)
	DNS Servers:		(Optional)
			(Optional)
Sear	ch Domains:		(optional)
		: fe80:0000:0000:0000:020a:95ff:fe8d:72e4	(optional)

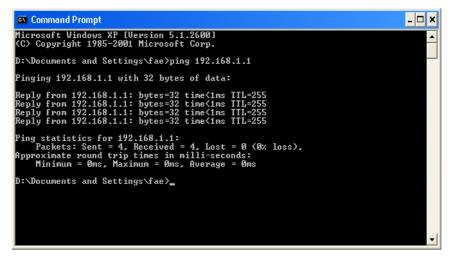
## 6.3 Pinging the Router from Your Computer

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 6.2)

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 Darwi	Jan 3 02:24:18 on ttyp1 n! x\$ ping 192.168.1.1	S
PING 192.168.1.1	. (192.168.1.1): 56 data bytes	
64 bytes from 19	2.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 19	2.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 19	2.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 19	2.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 19 ^C	2.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
192.168.1.1	ping statistics	
5 packets transm	itted, 5 packets received, 0% packet loss wg/max = 0.697/0.723/0.755 ms	

## 6.4 Checking If the ISP Settings are OK or Not

Open **WAN** >> **Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1/WAN2 to review the settings that you configured previously.

WAN >>	Internet Access		
Internet	Access		
Index	Display Name	Physical Mode	Access Mode
WAN1		ADSL	PPPoE / PPPoA 🔽 Details Page
WAN2		Ethernet	Static or Dynamic IP 🛛 🖌 Details Page
WAN3		USB	None   Details Page

## 6.5 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 Vigor2850. 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 Vigor2850.

## 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.



	-5	DrayTek Vigor	Getway IP (Static)	TX Packets	RX Rate
AN Status				0	0
TX Packet	s	RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442		3807		0	0
Wall Log VPN Lo	a Hear Assa	w Log Colling WAN	Log Network Infomation	West State	
Wall Log   VIN Lo	og User Acce	S LOg   Call Log   WAR	Dog Network Infomation	Net State	
Time	Host	Message			~
or 12 09:17:49	Vigor			Invition Out 2 ACCM-1	Oxfl Auther
		WANZ PPPOE <= PIO	tocollUCr(cU21) Confiked 10		
pr 12 09:17:49	Vigor	[3G]Modem status:a1 2	tocol:LCP(c021) ConfReq Id 20 00 00 00 00 02 00 03 00		
		[3G]Modem status:a1 2			
pr 12 09:17:49 pr 12 09:17:49	Vigor	[3G]Modem status:a1 2 WAN2 PPPoE → Pro WAN2 PPPoE <→ V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem response: [3G]Modem status:a1 2	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status al 2 WAN2 PPPoE ⇒> Pro WAN2 PPPoE <= V1 [3G]Modem response: [3G]Modem status al 2 [3G]Modem status al 2	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReg Id T:1 PADS ID-0 CONNECT 3600000 20 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem response: [3G]Modem statusal 2 [3G]Modem statusal 2 [3G]Modem dial ATD	80 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 80 00 00 00 00 02 00 02 00 80 00 00 00 00 02 00 02 00 7999#		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE → Pro WAN2 PPPoE < V:1 [3G]Modem response: [3G]Modem statusal 2 [3G]Modem statusal 2 [3G]Modem dial ATD WAN2 PPPoE → V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 T:1 PADR ID:0		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem response: [3G]Modem statusal 2 [3G]Modem statusal 2 [3G]Modem dial ATD WAN2 PPPoE → V:1 WAN2 PPPoE ← V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 T*99# T:1 PADR ID:0 T:1 PADO ID:0		
pr 12 09:17:49 pr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE ⇒> Pro WAN2 PPPoE ⇒> Pro [3G]Modem response: [3G]Modem statusal 2 [3G]Modem dial ATD WAN2 PPPoE ⇒> V1 WAN2 PPPoE ⇒> V1 [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq 10 T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 T*99# T:1 PADR ID:0 T:1 PADO ID:0 OK	dentifier:0x00 MRU: 15	
hpr 12 09:17:49 hpr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem statusal 2 [3G]Modem statusal 2 [3G]Modem statusal ADD WAN2 PPPoE → V:1 WAN2 PPPoE → V:1 [3G]Modem response: [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 OK 17&FE0V1X1&D2&C1S0=0	dentifier:0x00 MRU: 15	
kpr 12 09:17:49 kpr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE ⇒> Pro WAN2 PPPoE ⇒> Pro [3G]Modem response: [3G]Modem statusal 2 [3G]Modem dial ATD WAN2 PPPoE ⇒> V1 WAN2 PPPoE ⇒> V1 [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 OK 17&FE0V1X1&D2&C1S0=0	dentifier:0x00 MRU: 15	800 ACCM
pr 12 09:17:49 pr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statusal 2 WAN2 PPPoE → Pro WAN2 PPPoE ← V:1 [3G]Modem statusal 2 [3G]Modem statusal 2 [3G]Modem statusal ADD WAN2 PPPoE → V:1 WAN2 PPPoE → V:1 [3G]Modem response: [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReq Id T:1 PADS ID:0 CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 OK 17&FE0V1X1&D2&C1S0=0	dentifier:0x00 MRU: 15	

#### 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 Vigor2850. 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.

## 6.6 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.

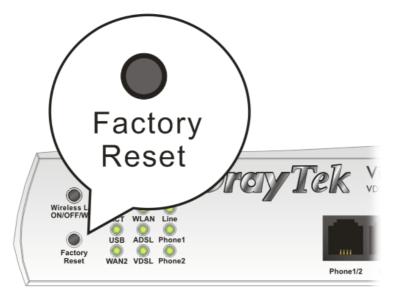
Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.



want to reboot your router ? ng current configuration ng factory default configuration
5 5
g factory default configuration
Data at Nave
Reboot Now
<u>Schedule</u> Setup:,,,,
d Idle Timeout settings will be ignored.

#### **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.

## 6.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@DrayTek.com.

