

Vigor2920/2920n Dual-WAN Security Router



Your reliable networking solutions partner

User's Guide

Vigor2920 Series Dual-WAN Security Router User's Guide

Version: 1.1 Firmware Version: V3.3.3_RC2 Date: 26/04/2010



Copyright Information

Copyright Declarations	Copyright 2010 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.
• • • • • •	

Safety Instructions and Approval

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



European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303Product:Vigor2920 Series Router

DrayTek Corp. declares that Vigor2920 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 2.4GHz 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 Vigor2920 1.2.2 For Vigor2920n 1.2.3 For Vigor2920Vn	4
1.3 Hardware Installation	
1.4 Printer Installation	9



Configuring Basic Settings	15
2.1 Two-Level Management	15
2.2 Accessing Web Page	15
2.3 Changing Password	16
2.4 Quick Start Wizard	18
2.4.1 PPPoE 2.4.2 PPTP/L2TP 2.4.3 Static IP 2.4.4 DHCP	
2.5 Online Status	24
2.6 Saving Configuration	25



User Mode Operation	27
3.1 WAN	27
3.1.1 Basics of Internet Protocol (IP) Network3.1.2 General Setup3.1.3 Internet Access	29
3.1.4 Load-Balance Policy	
3.2 LAN	40
3.2.1 Basics of LAN 3.2.2 General Setup	40 41
3.3 NAT	44
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	47
3.4 Applications	50
3.4.1 Dynamic DNS 3.4.2 UPnP	51 53



3.5 VolP	54
 3.5.1 DialPlan 3.5.2 SIP Accounts 3.5.3 Phone Settings 3.5.4 Status 	65 68
3.6 Wireless LAN	
 3.6.1 Basic Concepts 3.6.2 General Setup 3.6.3 Security 3.6.4 Access Control 3.6.5 Station List 	77 79 81
3.7 System Maintenance	83
 3.7.1 System Status. 3.7.2 User Password 3.7.3 Time and Date 3.7.4 Reboot System 	84 85
3.8 Diagnostics	86
3.8.1 DHCP Table 3.8.2 Traffic Graph 3.8.3 Ping Diagnosis 3.8.4 Trace Route	87 87
	00



Admin Mode Operation	89
4.1 WAN	89
 4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 General Setup 4.1.3 Internet Access 4.1.4 Load-Balance Policy 	91 93
4.2 LAN	102
 4.2.1 Basics of LAN	104 107 110
4.3 NAT	112
4.3.1 Port Redirection 4.3.2 DMZ Host 4.3.3 Open Ports	115
4.4 Firewall	119
 4.4.1 Basics for Firewall 4.4.2 General Setup 4.4.3 Filter Setup 4.4.4 DoS Defense 	121 123
4.5 Objects Settings	132
 4.5.1 IP Object 4.5.2 IP Group 4.5.3 Service Type Object 4.5.4 Service Type Group 	134 136





 4.5.5 Keyword Object 4.5.6 Keyword Group 4.5.7 File Extension Object 4.5.8 IM Object 4.5.9 P2P Object 4.5.10 Misc Object 	139 140 142 143
4.6 CSM Profile	
4.6.1 IM/P2P Filter Profile 4.6.2 URL Content Filter Profile 4.6.3 Web Content Filter Profile	148
4.7 Bandwidth Management	154
4.7.1 Sessions Limit 4.7.2 Bandwidth Limit 4.7.3 Quality of Service	155
4.8 Applications	163
4.8.1 Dynamic DNS 4.8.2 Schedule	165 167 168 170
4.9 VPN and Remote Access	
 4.9.1 VPN Client Wizard	178 182 182 184 186 187
4.9.9 Connection Management	
4.10 Certificate Management	
4.10.1 Ebcar Certificate 4.10.2 Trusted CA Certificate 4.10.3 Certificate Backup	201
4.11 VoIP	202
 4.11.1 DialPlan 4.11.2 SIP Accounts 4.11.3 Phone Settings 4.11.4 Status 	213 216
4.12 Wireless LAN	223
 4.12.1 Basic Concepts	225 228 229 231 233 236 237 239
4.12.10 Station List 4.13 System Maintenance	



4.13.1 System Status	
4.13.2 TR-069	
4.13.3 Administrator Password	
4.13.4 User Password	
4.13.5 Configuration Backup	
4.13.6 Syslog/Mail Alert	
4.13.7 Time and Date	
4.13.8 Management	
4.13.9 Reboot System	
4.13.10 Firmware Upgrade	
4.14 Diagnostics	
4.14.1 Dial-out Trigger	
4.14.2 Routing Table	
4.14.3 ARP Cache Table	
4.14.4 DHCP Table	
4.14.5 NAT Sessions Table	
4.14.6 Data Flow Monitor	
4.14.7 Traffic Graph	
4.14.8 Ping Diagnosis	
4.14.9 Trace Route	



Application and Examples	261
5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	261
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	269
5.3 QoS Setting Example	273
5.4 LAN – Created by Using NAT	276
5.5 Upgrade Firmware for Your Router	279
5.6 Request a certificate from a CA server on Windows CA Server	282
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server	286



Trouble Shooting	289
6.1 Checking If the Hardware Status Is OK or Not	289
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	290
6.3 Pinging the Router from Your Computer	292
6.4 Checking If the ISP Settings are OK or Not	293
6.5 Problems for 3G Network Connection	295
6.6 Backing to Factory Default Setting If Necessary	296
6.7 Contacting Your Dealer	297



1 Preface

Vigor2920 series is a broadband 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/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 2 VPN tunnels.

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

Object-based firewall is flexible and allows your network be safe. In addition, Vigor2920 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files.

Vigor2920 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.
Note: For the ot explanation.	ther buttons shown on the web pages, please refer to Chapter 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 Vigor2920



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application is enabled from Firewall >> General Setup . (Such profile must be established under CSM menu).
WCF		On	The Web Content Filter is active. (It is enabled
			from Firewall >> General Setup).
WAN1/2		On	The WAN1 or WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while an attack is detected.
VPN QoS		On	The VPN tunnel is active.
		On	The QoS function is active.
LED on Conned	ctor		
	Left LED	On	The port is connected.
WAN 1	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps when left LED is on.
	Left LED	On	The port is connected.
WAN 2 (Giga)	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.
	Left LED	On	The port is connected.
GigaLAN	(Green)	Off	The port is disconnected.
1/2/3/4		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.



	2920 I Security Router GigaLAN+1 2 3 4 WAN1 WAN2(Giga) USB
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
GigaLAN (1-4)	Connecters for local networked devices.
WAN1/WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for 3G Modem or printer.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.2 For Vigor2920n

USB WAN1 VP Factory Reset CSM WAN2 Q	S) N S S		
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normal
		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Conten application is enabled from Firewall >> Gene Setup . (Such profile must be established under CSM menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink slowly while wireless traffic goes through. If ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and it return to normal condition after two minutes. need to setup WPS within 2 minutes.)
WAN1/2		On	The WAN1 or WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while an attack is detected.
VPN		On	The VPN tunnel is active.
QoS		On	The QoS function is active.
LED on Connec	ctor		
	Left LED	On	The port is connected.
WAN 1	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps when left is on.
	Left LED	On	The port is connected.
WAN 2 (Giga)	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when LED is on.
Circl AN	Left LED	On	The port is connected.
GigaLAN 1/2/3/4	(Green)	Off	The port is disconnected.
1/2/3/4		Blinking	The data is transmitting.
	Right LED (Green)	On Off	The port is connected with 1000Mbps.The port is connected with 10/100Mbps wher



	920 ecurity Router GigsLAN+1 2 3 4 WAN1 WAN2(Gigs) USB
Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
GigaLAN (1-4)	Connecters for local networked devices.
WAN1/WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for 3G Modem or printer.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.3 For Vigor2920Vn

			Dray Tek	Vigor2	2920Vn Security Router				
Wireless LAN ON/OFF/WPS		WLAN Line				 	 -	-	
Factory Reset	۰	WAN1 Phone1		m		 			

LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
-		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from Firewall >> General Setup . (Such profile must be established under CSM menu).
WLAN	WLAN		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.)
WAN1/2		On	The WAN1 or WAN2 connection is ready.
			It will blink while transmitting data.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off.
		Off	There is no PSTN phone call.
Phone 1/2		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
		Blinking	A phone call comes.
LED on Conne	ctor		
	Left LED	On	The port is connected.
WAN 1/	(Green)	Off	The port is disconnected.
WAN2 (Giga)		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.
	Left LED	On	The port is connected.
GigaLAN	(Green)	Off	The port is disconnected.
1/2/3/4		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.



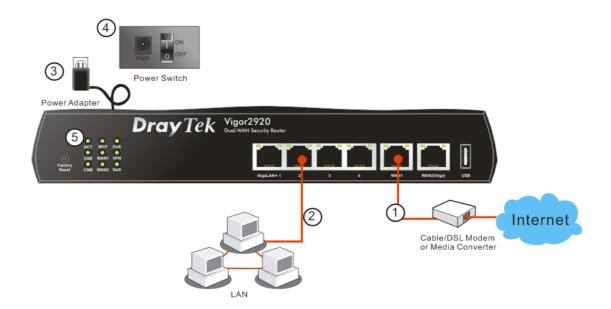
Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device
ON/OFF/WPS	making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on)
	or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking).
	Press the hole and keep for more than 5 seconds. When you see the ACT LED
	begins to blink rapidly than usual, release the button. Then the router will
	restart with the factory default configuration.
Phone 1/2	Connecter for analog phone(s).
Line	Connector for PSTN life line.
GigaLAN (1-4)	Connecters for local networked devices.
WAN1/WAN2(Giga)	Connecters for remote networked devices.
USB	Connecter for Mobile HDD, 3G 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.

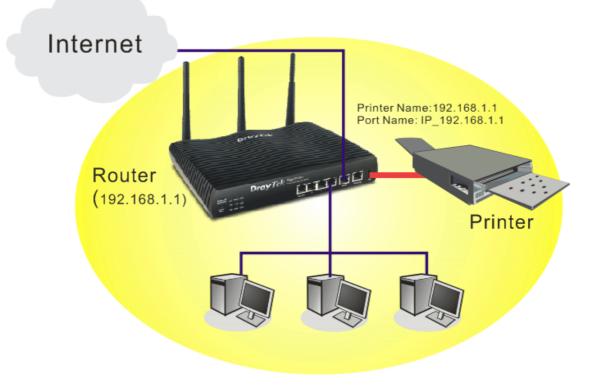
- 1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
- 2. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
- 4. Power on the device by pressing down the power switch on the rear panel.
- 5. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

(For the detailed information of LED status, please refer to section 1.1.)



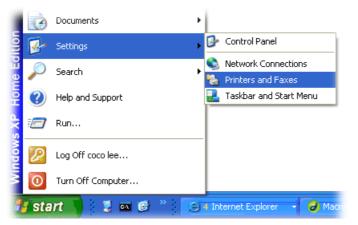
1.4 Printer Installation

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 wan	t 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

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	e model determine which printer software to use.	B
	•	
	turer and model of your printer. If your printer came with sk. If your printer is not listed, consult your printer docum oftware.	
Manufacturer	Printers	2
AST AT&T	Brother HL-1060 BR-Script2 Brother HL-1070 BR-Script2	-
Brother	Brother HL-1070	
Canon	Biother HL-TUPS7DPS	
💱 This driver is digitally sig		<u>H</u> ave Disk
Tell me why driver signir	ig is important	
	< Back Next >	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 UPR name.

ort Name:	IP_192.168.1.1
rinter Name or IP <u>A</u> ddress:	192.168.1.1
Protocol O <u>R</u> aw	<u>⊙ </u> LPR
Raw Settings	
Port Number:	9100
LPR Settings	_
Queue Name:	51
LPR Byte Counting En	abled
SNMP Status Enabled	
Community Name:	public
SNMP Device Index:	

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 forma	ıts ?			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	nnexB? (For A	DSL model o	nly)	VoIP
07. Ways for firmware upgrade.				QoS
08. Why is SNMP removed in firmware 2.3.6 and above for V	igor2200 Serie:	s routers?		ISDN
09. I failed to upgrade Vigor Router's firmware from my Mac I do?	machine const:	antly, what sl	nould 🤇	Eirewall / IP Filter Printer Servet
10. How to upgrade firmware of Vigor Router remotely ?				USB ISDN TA
AQ - Printer Server				IISB .
	vs2000/XP	?		8211
AQ - Printer Server		?		8211
AQ - Printer Server I. How do I configure LPR printing on Window	vs98/Me ?	?		8211
AQ - Printer Server 1. How do I configure LPR printing on Window 2. How do I configure LPR printing on Window	ws98/Me ? ioxes ?		ocuments	
AQ - Printer Server 1. How do I configure LPR printing on Window 2. How do I configure LPR printing on Window 3. How do I configure LPR printing on Linux H 4. Why there are some strange print-out whe	ws98/Me ? boxes ? n I try to p	rint my de	ocuments	
AQ - Printer Server 1. How do I configure LPR printing on Window 2. How do I configure LPR printing on Window 3. How do I configure LPR printing on Linux B 4. Why there are some strange print-out whe P / 2300's print server?	ws98/Me ? poxes ? n I try to p i Vigor rout	rint my da		
AQ - Printer Server 1. How do I configure LPR printing on Window 2. How do I configure LPR printing on Window 3. How do I configure LPR printing on Linux B 4. Why there are some strange print-out whe b / 2300's print server? 5. What types of printers are compatible with	vs98/Me? poxes? n I try to p v <mark>Vigor rout</mark> r Port of V	rint my da		
AQ - Printer Server 1. How do I configure LPR printing on Window 2. How do I configure LPR printing on Window 3. How do I configure LPR printing on Linux H 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 Printer	vs98/Me ? poxes ? n I try to p v Vigor rout r Port of V puter ?	rint my da		

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

This page is left blank.

Vigor2920 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.
 - 8

Notice: 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.

Login
Dray 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.

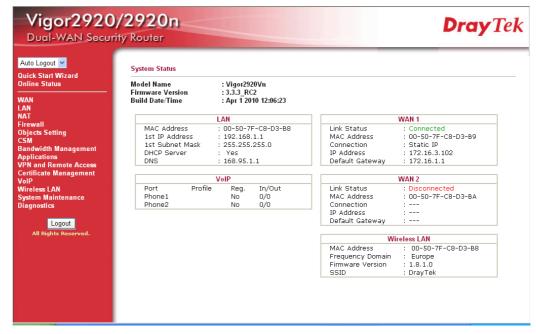


_	
Off	~
Auto Logout	ard
Off	
1 min	
3 min	
5 min	
10 min	_
Applications	

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.



Main screen for admin mode operation (full configuration)

Auto Logout 👻	System Status			
Quick Start Wizard Online Status	Model Name	: Vigor2920Vn		
WAN LAN	Firmware Version Build Date/Time	: 3.3.3_RC2 : Apr 1 2010 12:06:23		
NAT		LAN		WAN 1
Applications VolP Wireless LAN System Maintenance Diagnostics	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-C8-D3-B8 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-C8-D3-B9 : Static IP : 172.16.3.102 : 172.16.1.1
Logout		VoIP		WAN 2
All Rights Reserved.	Port Profile Phone1 Phone2	Reg. In/Out No 0/0 No 0/0	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-C8-D3-BA : : :
			Wi	reless LAN
			MAC Address Frequency Domain Firmware Version SSID	: 00-50-7F-C8-D3-B8 : Europe : 1.8.1.0 : DrayTek

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			
		ОК	(
		or		
System Maintenan	ce >> User Password	or		
	ce >> User Password	or		
	ce >> User Password	or		
ystem Maintenand Jser Password		or		

- 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	
Copyright©, DrayTek Corp. All Rights Reserved.	Login DrayTek

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

nter login password		
Please enter an alpha-nume	eric string as your Password	d (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. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.

Quick Start Wizard

Quick Start Wizard

WAN Interface:	WAN1 🕶
Display Name:	
Physical Mode:	Ethernet 💙
Physical Type:	Auto negotiation
	Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex

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

e followin	g Internet Acc	ess types pro	vided by you	r ISP.	
	PPPoE				
	О РРТР				
	L2TP				
	🔘 Static IP				
	O DHCP				
	e followin	 PPPoE PPTP L2TP Static IP 	 PPPoE PPTP L2TP Static IP 	 PPPoE PPTP L2TP Static IP 	 PPTP L2TP Static IP

2.4.1 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 your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown:

Quick Start Wizard

PPPoE Client Mode	
WAN 1	
Enter the user name and passwo	rd provided by your ISP.
User Name	84005755@hinet.net
Password	•••••
Confirm Password	•••••
	<pre>< Back Next > Finish Cancel</pre>

- 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:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
	nges if necessary. Otherwise, click Finish to save the current rigor router.
settings and restart the V	

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

2.4.2 PPTP/L2TP

Click **PPTP/L2TP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quic	k Star	t Wizard
~~~~		

WAN 1 Enter the user name, pass your ISP.	word, WAN IP configuration and PPTP server IP provided by	
User Name		
Password		
Confirm Password		
WAN IP Configuration		
🔘 Obtain an IP address	automatically	
💿 Specify an IP addres		
IP Address	172.16.3.102	
Subnet Mask	255.255.0.0	
Gateway	172.16.1.1	
Primary DNS		
Second DNS		
PPTP Server		

Click Next for viewing summary of such connection.

se confirm your settings:			
WAN Interface:	WAN1		
Physical Mode:	Ethernet		
Physical Type:	Auto negotiation		
Internet Access:	РРТР		
Internet Access: PPTP Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router.			

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



#### 2.4.3 Static IP

Quick Start Wizard

Click **Static IP** as the protocol. Type in all the information that your ISP provides for this protocol.

WAN 1		
-	uration probided by your ISP.	
WAN IP	172.16.3.229	
Subnet Mask	255.255.255.0	
Gateway	172.16.3.1	
Primary DNS	168.95.1.1	
Secondary DNS		(optional)

After finishing the settings in this page, click **Next** to see the following page.

Out	ick	Start	Wizard	
Qu	IC N	Jun	vvizaru	

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
settings and restart the V	nges if necessary. Otherwise, click Finish to save the current

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

### 2.4.4 DHCP

Click **DHCP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

WAN 1	
If your ISP requenter it in.	uire you to enter a specific host name or specific MAC address, please
0	
Host Name	(optional)
MAC	00 -50 -7F -00 -00 -01 (optional)

After finishing the settings in this page, click **Next** to see the following page.

#### Quick Start Wizard

WAN Interface:	WAN1
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 <b>Finish</b> to save the current rigor router.

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

## 2.5 Online Status

The online status shows the system status, WAN status, and other status related to this router within one page. 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 for DHCP**

Online Status

System Status					stem Uptime: 0:0:
LAN Status	Prima	ry DNS: 168.95	5.1.1	Secondary DI	<b>IS:</b> 168.95.1.1
IP Address	TX Packets	RX Pac	kets		
192.168.1.1	382	297			
WAN 1 Status					>> <u>Renev</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX Packets</b>	RX Rate(Bps)
		0	0	0	0
WAN 2 Status					>> <u>Releas</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:00:21	
IP	GW IP	TX Packets	TX Rate(Bps)	<b>RX Packets</b>	RX Rate(Bps)
192.168.5.30	192.168.5.1	14	60	12	66

Detailed explanation is shown below:

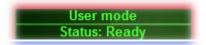
Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
<b>RX</b> Packets	Displays the total number of received packets at the LAN interface.
WAN Status	
Line	Displays the physical connection (Ethernet) of this interface.
Name	Displays the name set in WAN1/WAN web page.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
<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 Saving Configuration

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



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

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

This page is left blank.

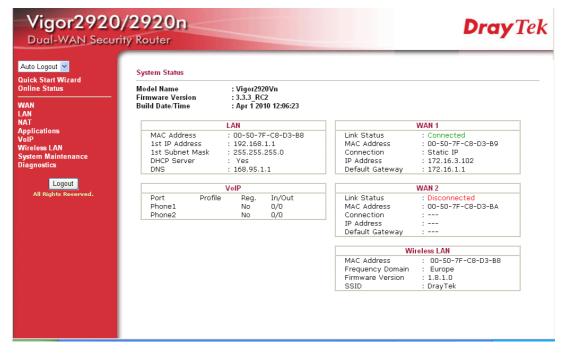
#### Vigor2920 Series User's Guide

# **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.



# 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**

F For 3G mobile communication through Access Point is popular more and more, Vigor2920 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2920, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2920n 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 Vigor2920n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2920n series.



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

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

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port (WAN1- through WAN port/WAN2- through LAN1 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

WAN >> General Setup				
	WAN2			
es 💙	Enable:	Yes 🕶		
	Display Name:			
hernet	Physical Mode:	Ethernet 🗸		
uto negotiation ⊻	Physical Type:	Auto negotiation 💌		
uto Weight 🛛 👻	Load Balance Mode:	Auto Weight		
ownLink 0	Line Speed(Kbps):	DownLink 0		
DLink 0		UpLink 0		
lways On 🛛 👻		Always On		
	O WAN1 Fail			
WAN2 Upload speed exceed     Kbps		ed exceed 0 Kbps		
WAN2 Download speed exceed 0 Kbps				
:   	nernet uto negotiation v uto Weight v wnLink 0 Link 0 ways On v exceed 0 Kbps	Enable: Enable: Display Name: Physical Mode: Physical Type: Load Balance Mode: Link 0 ways On • Enable: Display Name: Physical Type: Load Balance Mode: Line Speed(Kbps): Active Mode: Active on demand: • WAN1 Fail • WAN1 Upload spe		

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 the WAN1/WAN2 interface.		
Physical Mode	For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port.		
	Physical Mode:	Ethernet 💌	
		Ethernet	

0K

**Dray** Tek

3G USB Modem

To use 3G network connection through 3G USB Modem, choose **3G USB Modem** as the physical mode in **WAN2**. Next, go to **WAN>> Internet Access**. 3G USB Modem is available for WAN2. You can choose **PPP** as the access mode and click Details Page for further configuration.

	WAN >> Internet Access		
	Internet Access		
	Index Display Name	Physical Mode	Access Mode
	WAN1	Ethernet	Static or Dynamic IP V Details Page
	WAN2	3G USB Modem	None Details Page
			PPP
Physical Type	-		ical type for WAN2 or choose Auto
	<b>negotiation</b> fo	r determine	ed by the system.
	Physical Typ	e:	Auto negotiation 🚩
			Auto negotiation
			10M half duplex
			10M full duplex 100M half duplex
			100M full duplex
Lood Dolonoo Modo	If 1		i
Load Balance Mode	Load Balance Mode If you know the practical bandwidth for your WA please choose the setting of According to Line Sp		
			Auto Weigh to let the router reach
	the best load b		
	Load Balance	e Mode:	Auto Weigh 🔽
			Auto Weigh
			According to Line Speed
Line Speed	Mode, please t	type the lin	<b>g to Line Speed</b> as the <b>Load Balance</b> le speed for downloading and 1/WAN2. The unit is kbps.
Active Mode	Choose Always On to make the WAN connection		
	(WAN1/WAN2) being activated always; or choose <b>Act demand</b> to make the WAN connection (WAN1/WAN2 activated if it is necessary.		-
	Active Mode:		Active on demand 🚩
			Always On
	TC 1		Active on demand
	If you choose Active on demand, the Idle Timeout		
			or PPPoE and PPTP access modes in <b>N&gt;&gt;Internet Access</b> . In addition, there
			bu to choose for different purposes.
		•	ne connection for WAN1 will be
	activated when	n WAN2 is	failed.
	-	-	ceed XX kbps – It means the
			ll be activated when WAN2 Upload
	-	ertain valu	that you set in this box for 15
	seconds.	lood mood	avoad VV khng. It maans the
		-	exceed XX kbps– It means the Il be activated when WAN2
			certain value that you set in this box
	Download spo		certain value that you set in this box



for 15 seconds.

**WAN1 Fail** – It means the connection for WAN2 will be activated when WAN1 is failed.

WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.

**WAN1 Download speed exceed XX kbps**– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.

# 3.1.3 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different Physical Mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.

WAN >> Internet Access

Index D	Display Name	Physical Mode	Access Mode
WAN1		Ethernet	Static or Dynamic IP 💌 🗌 Details Page
WAN2		3G USB Modem	None 🔽 Details Page
			None PPP

#### WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode
WAN1		Ethernet	Static or Dynamic IP 💌 🛛 Details Page
WAN2		Ethernet	None 💽 Details Page
			None PPPoE Static or Dynamic IP PPTP/L2TP
ndex		default WAN optional WA	VAN modes that this router supports. WAN1 is the interface for accessing into the Internet. WAN2 is the I interface for accessing into the Internet when WAN some reason.
Display	y Name	It shows the name of the WAN1/WAN2 that entered in general setup.	
Physical Mode			hysical connection for WAN1 (Ethernet) /WAN2 G USB Modem) according to the real network ode Physical Mode
		r ny stodri	
		Etherne	t Ethernet
		3G USB Ma	dem Ethernet

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.

Static or Dynamic IP 💌
None
PPPoE
Static or Dynamic IP
PPTP/L2TP

There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP/L2TP.

**Details Page** This button will open different web page according to the access mode that you choose in WAN1 or WAN2.

## **Details Page for PPPoE**

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

WAN 2		
PPPoE Client Mode		PPP/MP Setup
🔵 Enable 🛛 💿 Dis	sable	PPP Authentication PAP or CHAP 🐱
		Idle Timeout -1 second(s)
ISP Access Setup		IP Address Assignment Method
Username		(IPCP) WAN IP Alias
Password		Fixed IP: O Yes O No (Dynamic IP)
WAN Connection Det	ection	Fixed IP Address
Mode	ARP Detect 💌	Default MAC Address
Ping IP		<ul> <li>Specify a MAC Address</li> </ul>
TTL:		MAC Address:
		00 .50 .7F :C8 .D3 .BA
мти	1442 (Max: 1492)	

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	<ul> <li>Enter your allocated username, password and authentication parameters according to the information provided by your ISP.</li> <li>Username – Type in the username provided by ISP in this field.</li> <li>Password – Type in the password provided by ISP in this field.</li> <li>Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.</li> </ul>
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



	<ul> <li>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>
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
PPP/MP Setup	<ul> <li>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</li> <li>If you want to connect to Internet all the time, you can check</li> <li>Always On.</li> <li>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</li> </ul>
IP Address Assignment Method (IPCP)	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please

**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.

contact your ISP before you want to use this function.

🕘 WAN II	P Alias - M	icrosoft Internet Explorer	
WAN IP	Alias ( M	ulti-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**

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 choose Static or Dynamic IP mode from Internet Access menu. The following web page will be shown.

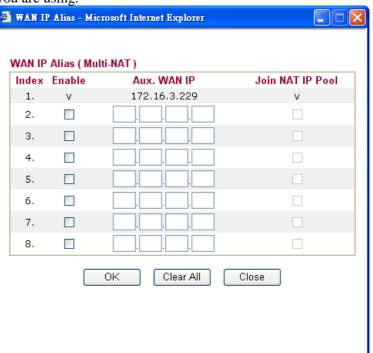
Static or Dynamic IP (DHCP Client)	WAN IP Network Settings WAN IP Alias
⊙ Enable ○ Disable	Obtain an IP address automatically
Keep WAN Connection	Router Name
Enable PING to keep alive	Domain Name
PING to the IP	* : Required for some ISPs
PING Interval 0 minute(s)	Specify an IP address
PING Interval 0 minute(s)	IP Address
WAN Connection Detection	Subnet Mask
Mode ARP Detect 🛩	Gateway IP Address
Ping IP	DNS Server IP Address
TTL:	Primary IP Address
	Secondary IP Address
MTU 1442 (Max:150	0)
	<ul> <li>Default MAC Address</li> </ul>
RIP Protocol	Specify a MAC Address
Enable RIP	MAC Address:

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



MTU	It means Max Transmit Unit for packet. The default setting is 1442.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.
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

**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.



**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**<br/>AddressType in the primary IP address for the router if you want to use<br/>Static IP mode. If necessary, type in secondary IP address for<br/>necessity in the future.

# **Details Page for PPTP/L2TP**

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.

WAN 2			
PPTP/L2TP Client Mode		PPP Setup	
🔾 Enable PPTP 📿	Enable L2TP 💿 Disable	PPP Authentication	PAP or CHAP 🔽
Server Address		Idle Timeout	-1 second(s)
Specify Gateway IP Ad	dress	IP Address Assignment M	lethod
		(IPCP) WAN IP Alias	
		Fixed IP: 🔘 Yes 💽 I	No (Dynamic IP)
ISP Access Setup		Fixed IP Address	
Username		WAN IP Network Setting	s
Password	rd 📀 Obtain an IP address automatic		is automatically
		💿 Specify an IP addre	SS
MTU	1442 (Max: 1460)	IP Address	
		Subnet Mask	
	OK	Cancel	
vlode SP Access Setup MTU	<ul> <li>Enable L2TP - Clic establish a tunnel to</li> <li>Disable – Click this PPTP or L2TP.</li> <li>Server Address - Sp server if you enable</li> <li>Specify Gateway IP for DHCP server.</li> <li>Username -Type in</li> <li>Password -Type in to</li> </ul>	a DSL modem on the radio button to close to pecify the IP address of PPTP/L2TP client mo <b>Address</b> – Specify the the username provided	enable a L2TP client to WAN interface. the connection through of the PPTP/L2TP ide. he gateway IP address d by ISP in this field.
PPP Setup	<b>PPP Authentication</b> <b>Idle Timeout</b> - Set t	n - Select PAP only of	r <b>PAP or CHAP</b> for PPP ng down the Internet after
P Address Assignment Method(IPCP)	time you connect to service to always ass request. In this case, field. Please contact	it and request. In some sign you the same IP a you can fill in this IP your ISP before you	ns IP address to you each e case, your ISP provides address whenever you address in the Fixed IP want to use this function. a fixed IP address in the
	like to utilize them o	on the WAN interface,	lic IP addresses and woul please use WAN IP Alia her than the current one

#### WAN >> Internet Access



2)	WAN II	Alias - M	icrosoft Internet Explorer	
١	NAN IP	Alias ( Mu	ulti-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

you are using. Notice that this setting is available for WAN1 only.

Fixed IP Address - Type a fixed IP address.

WAN IP NetworkObtain an IP address automatically – Click this button to obtain<br/>the IP address automatically.SettingsSpecify an IP address – Click this radio button to specify some data.<br/>IP Address – Type the IP address.<br/>Subnet Mask – Type the subnet mask.

# 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 WAN1 or WAN2 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 both WAN1 and WAN2 are activated.

#### WAN >> Load-Balance Policy

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>	<u>Down</u>
<< <u>1-10</u>	<u>11-20</u> :	•>									1	Next >:

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

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

#### WAN >> Load-Balance Policy

Enable	
Protocol	any 💌
Binding WAN Interface	WAN1 🗹 🗹 Auto failover to the other WAN
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
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



Binding WAN interface	Choose the WAN interface (WAN1 or WAN2) 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.

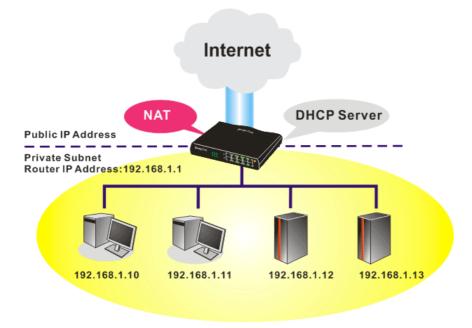
# 3.2 LAN

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



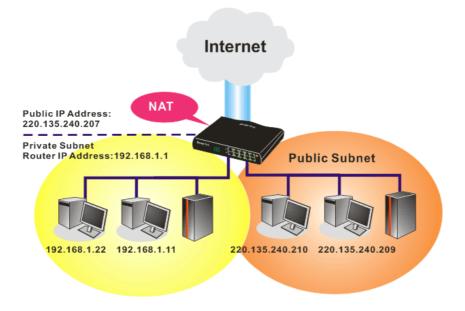
# 3.2.1 Basics of LAN

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



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





# 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

Ethernet TCP / IP and DHC	P Setup			
LAN IP Network Configurat	tion		DHCP Server Configuration	1
For NAT Usage			💿 Enable Server 🔘 Disab	le Server
1st IP Address	192.168.1.1		Relay Agent: 🔘 1st Sub	onet 🔾 2nd Subnet
1st Subnet Mask	255.255.255.0		Start IP Address	192.168.1.10
For IP Routing Usage 🔘	Enable 💿 Disable		IP Pool Counts	50
2nd IP Address	192.168.2.1		Gateway IP Address	192.168.1.1
2nd Subnet Mask	255.255.255.0		DHCP Server IP Address	
2n	d Subnet DHCP Server		for Relay Agent DNS Server IP Address	
			📃 Force DNS manual s	etting
RIP Protocol Control	Disable 🚩		Primary IP Address	
			Secondary IP Address	
		0	ĸ	

1st IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
1st Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)



For IP Routing Usage	Click <b>Enable</b> to invoke this function. The default setting is <b>Disable</b> .
2 nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)
2 nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/24)
2 nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd

You can configure the router to serve as a DHCP server for the 2nd subnet.

IP Pool Co	ddress unts O (max. :	10)
ndex	Matched MAC Address	given IP Address
AC Addre	955 : :::::::::::::::::::::::::::::::::	
	Add Delete Edit	t Cancel

**Start IP Address:** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

**IP Pool Counts:** Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

**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 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

**RIP Protocol Control Disable** deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

RIP Protocol Control

Disable 🖌 🖌
Disable
1st Subnet
2nd Subnet

**1st Subnet -** Select the router to change the RIP information of the 1st subnet with neighboring routers.



	<b>2nd Subnet -</b> Select the router to change the RIP information of the 2nd subnet with neighboring routers.
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.
	<ul> <li>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.</li> <li>Enable Server - Let the router assign IP address to every host in the LAN.</li> <li>Disable Server - Let you manually assign IP address to every host in the LAN.</li> <li>Relay Agent - (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</li> </ul>
	<ul> <li>Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ul>
DNS Server Configuration	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	<ul> <li>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).</li> <li>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.</li> <li>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 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.</li> </ul>
	The default DNS Server IP address can be found via Online Status:
	System untime: / 1/4/46

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.

There are two common scenarios of LAN settings that stated in Chapter 5. For the configuration examples, please refer to that chapter to get more information for your necessity.

# 3.3 NAT

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

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

The benefit of the NAT includes:

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

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.

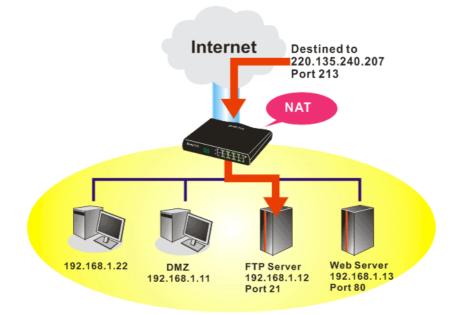
Below shows the menu items for NAT.





# 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.

NAT >> Port Redirection

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.

Index	Service Name	Public Port	Private IP	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
< 1-10   11-2	0 >>			Next:

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

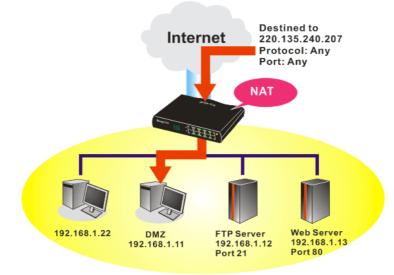
ОК	Clear	Cancel
----	-------	--------

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 and</b> <b>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.



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	Setu	p

VAN 1	
None 💌	
Private IP	Choose PC
MAC Address of the True IP DM	NZ Host 00 00 00 00 00 00
	IZ Host         OO         OO <t< th=""></t<>
Note: When a True-IP DMZ h	
Note: When a True-IP DMZ he always on.	

**Dray** Tek

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

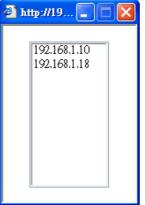
MZ Host S	Setup			
NAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229		Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC

**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.

NAT >> DMZ Host Setup

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229	192.168.1.10	Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC
			OK Clear	



# 3.3.3 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>				х
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				×
<u>7.</u>				х
<u>8.</u>				×
<u>9.</u>				×
<u>10.</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.

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

#### Index No. 1

🗹 E	Enable Open P	orts						
Comment		P2F	P2P					
WAN Interface			WA	WAN1 💌				
Local 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 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.
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.

Applications

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.

Applications >> Dynamic DNS Setup

Enable Dynam	ic DNS Setup	View Log	Force Update
uto-Update inte			
ccounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		x
<u>3.</u>	WAN1 First		х

OK Clear All

**Set to Factory Default** Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
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

Index : 1	
🗹 Enable Dynamic DNS	5 Account
WAN Interface	WAN1 First 💌
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chronic6853 , dyndns.info v
Login Name	chronic6853 (max. 23 characters)
Password	••••••••• (max. 23 characters)
🔲 Wildcards	
🔲 Backup MX	
Mail Extender	
	OK Clear Cancel

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

4. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

#### 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.

- 1000	Broadband	🐮 IP Broadband Connection	on Router Status
Intervent Tasks     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create 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
0	Dial-up	Duration:	00:19:06
ee Also 🔹	test Disconnected DrayTek ISDN PPP	Speed:	100.0 Mbps
ther Places (*)	Internet Gateway	Activity Internet Internet Ga	teway My Computer
My Documents My Computer	LAN or High-Speed Internet	Sent: 404 Received: 1,115	
etails 🛞	Local Area Connection Enabled	Properties Disable	)
Network Connections	Realtek RTL8139/810x Family		

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.

# **3.5 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



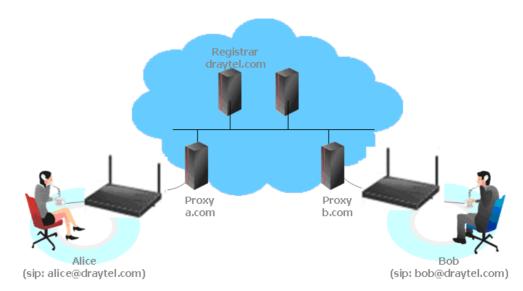
very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN 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.



If you both register to the same SIP Registrar, then it will be illustrated as below:

The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar.

## Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



Our Vigor V models firstly apply efficient codecs designed to make the best use of



available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



# 3.5.1 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
	<u>Regional</u>
	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

# **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:

time. If it is disabled, no SAS prompt will be heard any more.

- 1. After the connection established, vigor router A will send SAS voice prompt to A and vigor router B will send the SAS voice prompt to B.
- 2. Then the RTP traffic is secured until the call ends.
- 3. If vigor router A wants to call vigor router B again next time, both A and B will not hear any voice prompt again even checking **Enable SAS Voice Prompt** on web UI. It means only the first call between them will have voice prompt.

Enable SAS Voice Prompt, for ex: if vigor router A calls vigor router B with checking **Enable Secure Phone** but not **Enable SAS Voice Prompt**, then:

1. After the connection established, vigor router A will **NOT** send SAS voice prompt to vigor router A and vigor router B will **NOT** send the SAS voice prompt to vigor router B.



2. Even no voice prompt, but the RTP traffic is still secured until the call ends.

**Note:** If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

## Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2820V for setting the phone book.

```
VoIP >> DialPlan Setup
```

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
<u>1.</u>				Default	None		×
<u>2.</u>				Default	None		×
<u>3.</u>				Default	None		х
<u>4.</u>				Default	None		х
<u>5.</u>				Default	None		×
<u>6.</u>				Default	None		×
<u>19.</u>				Default	None		×
<u>20.</u>				Default	None		х
< <u>1-20</u>	21-40   41-6	0 >>					<u>Next</u> >

Click any index number to display the dial plan setup page.

VoIP >> DialPlan Setup	
------------------------	--

Phone Book	Index No. 1			
	Phone Number	1		
	Display Name	Polly		
	SIP URL	1112	@ fwd.pulver.com	
	Dial Out Account	Default 🚩		
	Loop through	None 💌		
	Backup Phone Number			
	OK	Clear	Cancel	
nable	Click the click	his to enable th	is entry.	

Phone Number	The speed-dial number of this index. This can be any number you choose, using digits <b>0-9</b> and <b>*</b> .
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	At AccountChoose one of the SIP accounts for this profile to dial out. It useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.			
Loop through	Choose PSTN to enable loop through function.			
Backup Phone Number	When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch,			

phone setting.

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

# **Dray** Tek

# **Digit Map**

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

#	Enable	Prefix Number	Mode	e	OP Number	Min Len	Max Len	Route
1		03	Replace	*	8863	7	9	PSTN 🔽
2	<b>~</b>	886	Strip	*	886	8	10	PSTN 🔽
з			None	~		0	0	PSTN 🔽
4			None	$\vee$		0	0	PSTN 🔽
5			None	~		0	0	PSTN 🔽
6			None	~		0	0	PSTN 🗸
16			None	Y		0	0	PSTN M
17			None	~		0	0	PSTN 🔽
18			None	~		0	0	PSTN 🗸
19			None	Y		0	0	PSTN 🔽
20			None	~		0	0	PSTN 🗸

Note: Min Len and Max Len should be between 0~25.

OK	Cancel
U.V.	Cancer

Enable Prefix Number	Check this box to invoke this setting. The phone number set here is used to add, strip, or replace the OP number.
Mode	<ul> <li>None - No action.</li> <li>Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.</li> <li>Strip - 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.</li> <li>Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 386 will be deleted completely for 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 "03111111" will be changed to "8863111111" and sent to SIP server. Mode</li> </ul>
	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.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in <b>VoIP&gt;&gt; Phone Settings</b> .

# **Call Barring**

Call barring is used to block phone calls coming from the one that is not welcomed.

VolP	>>	DialE	lan	Setup	
0.01	~~	Dian	T G H	Setup	

Call Barrin	g Setup		<u>S</u>	et to Factor	<u>y Default</u>
Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	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   1</u>	1-20 >>				<u>Next</u> >>

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u>

Click any index number to display the dial plan setup page.

VoIP >> DialPlan Setup	
Call Barring Index No. 1	
🗹 Enable	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Route	
	OK Cancel

Enable	Click this to enable this entry.			
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.			
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number			
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.			
Route	All means all the phone calls will be blocked with such mechanism.			

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 Ano	ymous			
🗹 Enable				
Route	Phone1 Phone2			
Note:Block the incomin	g calls which do not have the caller ID.			
	OK Cancel			

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup							
Call Barring Block Unknown Domain							
🗹 Enable	!						
	Route	Phone1	Phone2				
Note: If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked.							

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 Addı	ess						
🗹 Enable							
Route	Phone1 Phone2						
Note: The incoming calls by means of IP dialing (e.g.#192*168*1*1#) should be blocked.							
	OK Cancel						

# Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

#### VoIP >> DialPlan Setup

🗹 Enable Regional			1	Set to Fac	tory Default
Last Call Return [Miss]:	*69				
Last Call Return [In]:	*12		Last Call Return [Out]:	*14	
Call Forward [All] [Act]:	*72	+number+#	Call Forward [Deact]:	*73	+#
Call Forward [Busy] [Act]:	*90	+number+#	Call Forward [No Ans] [Act]:	*92	+number+#
Do Not Disturb [Act]:	*78	+#	Do Not Disturb [Deact]:	*79	+#
Hide caller ID [Act]:	*67	+#	Hide caller ID [Deact]:	*68	+#
Call Waiting [Act]:	*56	+#	Call Waiting [Deact]:	*57	+#
Block Anonymous [Act]:	*77	+#	Block Anonymous [Deact]:	*87	+#
Block Unknow Domain [Act]:	*40	+#	Block Unknow Domain [Deact]:	*04	+#
Block IP Calls [Act]:	*50	+#	Block IP Calls [Deact]:	*05	+#
Block Last Calls [Act]:	*60	+#			

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.

Cancel



ΟK

Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

# **PSTN Setup**

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**.

VolP	>>	PST	NS	etuj	p
------	----	-----	----	------	---

Enab	ole	phone number for PSTN relay
	l	
	l	
	l	

Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

# 3.5.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name** 

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Note: Selection items for **Ring Port** will differ according to the router you have.

SIP Acco	unts List					(	Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring	g Port	Status
1					Phone1	Phone2	-
2					Phone1	Phone2	-
<u>3</u>					Phone1	Phone2	-
4					Phone1	Phone2	-
<u>5</u>					Phone1	Phone2	-
<u>6</u>					Phone1	Phone2	-
7					Phone1	Phone2	-
<u>8</u>					Phone1	Phone2	-
<u>9</u>					Phone1	Phone2	-
<u>10</u>					Phone1	Phone2	-
<u>11</u>					Phone1	Phone2	-
<u>12</u>					Phone1	Phone2	-

#### VoIP >> SIP Accounts

R: success registered on SIP server -: fail to register on SIP server

#### NAT Traversal Setting

STUN Server:			
External IP:			]
SIP PING Interval:	150	sec	

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 @.
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. $\mathbf{R}$ 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.

#### VoIP >> SIP Accounts

Profile Name	(11 char ma	эх.)
Register via	None 💌 🗌 Call without Reg	gistration
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
Act as outbound pro	xy	
Display Name	(23 char ma	ах.)
Account Number/Name		(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 💌 3600 sec	
NAT Traversal Support	None 💌	
Ring Port	Phone 1 Phone 2	
Ring Pattern	1 💌	

**Profile Name** 

**Register via** 

Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.

If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **Call without Registration**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call.

None	*	
None		
Auto		
WAN1		
WAN2		F
LANAVPN		L

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				
	<ul> <li>None – Disable this function.</li> <li>Stun – Choose this option if there is Stun server provided for your router.</li> <li>Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.</li> <li>Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.</li> </ul>				
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.				
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern  1 2 3 4 5 6				

# 3.5.3 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.

VolP	>>	Pho	ne	Sett	inas
				360	myə

Phone List Refresh Seconds: 30 🗸 Refres							
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	<ul> <li>Port – there are two phone ports provided here for you to configure. Phone1/Phone2 allow you to set general settings for PSTN phones.</li> <li>Call Feature – A brief description for call feature will be shown in this field for your reference.</li> <li>Codec – The default Codec setting for each port will be shown in this field to change it for each phone port.</li> <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> <li>Default SIP Account – "draytel_1" is the default SIP account. You can click the number below the Index field to change of Phone Index.</li> <li>DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.</li> </ul>
RTP	<ul> <li>Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.</li> <li>Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050.</li> <li>Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000.</li> <li>RTP TOS – It decides the level of VoIP package. Use the drop</li> </ul>



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 💌

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		Codecs	
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽
Session Timer	90 sec		🔲 Single Codec
Call Forwarding Disable		Packet Size	20ms 💌
		Voice Active Detector	Off 🛩
Time Out	30 sec		
DND(Do Not Disturb)	500	Default SIP Account	<b>*</b>
	mode <u>ne Book</u> as Exception List:	Play dial tone only	when account registered
CLIR (hide caller ID)			
Call Transfer			
lotline		to enable it. Type in	the SIP URL in the field f
		tically when you pic	
ession Timer		field, if there is no re	n. In the limited time that sponse, the connecting cal
Call Forwarding	forwarding fun be forwarded i the incoming c the local system	action. Always means nto SIP URL without alls will be forwarde n is busy. No Answe ceive any response, th	noose. <b>Disable</b> is to close of s all the incoming calls wi t any reason. <b>Busy</b> means d into SIP URL only when er means if the incoming ney will be forwarded to the
	abc@iptel.org)	as the site for call for et the time out for the	e.g., aaa@draytel.org or orwarded. e call forwarding. The

DND (Do Not Disturb) 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.



		- Enter the index of phone book IPlan – Phone Book for detailed		
CLIR (hide caller ID)	Check this box to hide the ca phone set.	ller ID on the display panel of the		
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		function. Click hook flash to /hen the phone call connection The other two sides can		
Prefer Codec	codec used for each call will before each session, and so m default codec is G.729A/B; it maintaining good voice quali If your upstream speed is onl It is better for you to have at would like to use G.711.	y 64Kbps, do not use G.711 codec. least 256Kbps upstream if you		
	Prefer Codec	G.711A (64Kbps) G.711MU (64Kbps)		

G.711A (64Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps)

**Single Codec** – If the box is checked, only the selected Codec will be applied.

**Packet Size**-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size

20ms	*
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

**Voice Active Detector -** This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



**Default SIP Account** 

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

**Play dial tone only when account registered -** Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Settings						
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
<b>Ringing tone</b>	400	450	400	200	400	2000
Busy tone	400	0	375	375	0	0
Congestion tone 0		0	0	0	0	0
Volume Gain			DTMF			
Mic Gain(1-10)	5		DTMF Mo	de	InBand	~
Speaker Gain(1-10)			Payload T (96 - 127	Гуре (RFC283 ')	3) 101	
MISC						
Dial Tone Power Level (1 - 50)		7				
Ring Frequency (10 - 50HZ)		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.

	ione Sem	ngs	
	Region	User Defined 🚩	
		User Defined	owi
		UK	(H:
	Dia	US Denmark	i0
	Ringi		0
		Germany	0
		Netherlands Portugal	
		Sweden	
	V VIUITO O	Australia	
	Mic Gain(	Slovenia Czech	
		Slovakia	
		Hungary	
		Switzerland France	
	Dial Tone ^L	France Power Lever (.	<b>1</b> - 50
	recommended	l for you to use t	eld for your necessity. It is he default settings for VoIP
	communicatio		
Volume Gain		· •	(1-10) - Adjust the volume of
	-		ntering number from 1- 10. The er the volume is.
MISC	-		
MISC	loudness of th	ne dial tone. The	s setting is used to adjust the smaller the number is, the louder nded for you to use the default
	<b>Ring Freque</b>		g is used to drive the frequency of led for you to use the default
	setting.		
DTMF	setting.		r DTMF modes for you to choose.
DTMF	setting. DTMF Mode	e – There are fou	r DTMF modes for you to choose. n the Vigor will send the DTMF
DTMF	setting. DTMF Mode InBand - Cho tone as audio	e – There are fou pose this one the directly when yo	n the Vigor will send the DTMF ou press the keypad on the phone
DTMF	setting. DTMF Mode InBand - Cho tone as audio OutBand - Ch	e – There are fou pose this one the directly when yo hoose this one th	n the Vigor will send the DTMF ou press the keypad on the phone then the Vigor will capture the
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cl keypad numb	e – There are fou pose this one the directly when yo hoose this one th er you pressed a	n the Vigor will send the DTMF ou press the keypad on the phone
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cl keypad numb then send to th according to t	e – There are fou bose this one the directly when yo hoose this one th er you pressed a he other side; the he digital form i	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Ch keypad numb then send to th according to the useful when the	e – There are fou bose this one the directly when yo hoose this one th er you pressed a he other side; the che digital form i he network traff	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cho keypad numb then send to the according to the useful when the can remain the	e – There are fou oose this one the directly when yo hoose this one th er you pressed a he other side; the he digital form i he network traffi e accuracy of D'	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still TMF tone.
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Che tone as audio <i>OutBand</i> - Cl keypad numb then send to th according to t useful when th can remain th <i>SIP INFO</i> - C	e – There are four bose this one the directly when you hoose this one the er you pressed a he other side; the he digital form i he network traffi e accuracy of D' choose this one the	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cl keypad numb then send to th according to th useful when th can remain th <i>SIP INFO</i> - C DTMF tone a	e – There are four oose this one the directly when yo hoose this one the er you pressed a he other side; the he digital form i he network traffi e accuracy of D' choose this one th	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still TMF tone. hen the Vigor will capture the o SIP form. Then it will be sent to
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cl keypad numb then send to th according to th useful when th can remain th <i>SIP INFO</i> - C DTMF tone a	e – There are fou oose this one the directly when yo hoose this one th er you pressed a he other side; the digital form i he network traffi e accuracy of D' choose this one th nd transfer it int d with SIP mess	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still TMF tone. hen the Vigor will capture the o SIP form. Then it will be sent to age.
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cho keypad numb then send to the according to the useful when the can remain the <i>SIP INFO</i> -CO DTMF tone a the remote en	e – There are fou bose this one the directly when yo hoose this one the er you pressed a the other side; the che digital form i he network traffi e accuracy of D' Choose this one the nd transfer it int d with SIP mess	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still TMF tone. hen the Vigor will capture the o SIP form. Then it will be sent to age. nBand
DTMF	setting. <b>DTMF Mode</b> <i>InBand</i> - Cho tone as audio <i>OutBand</i> - Cho keypad numb then send to the according to the useful when the can remain the <i>SIP INFO</i> -CO DTMF tone a the remote en	e – There are fou oose this one the directly when yo hoose this one the er you pressed a he other side; the he digital form i he network traffi e accuracy of D' choose this one the nd transfer it int d with SIP mess	n the Vigor will send the DTMF ou press the keypad on the phone een the Vigor will capture the nd transform it to digital form e receiver will generate the tone t receive. This function is very ic congestion occurs and it still TMF tone. hen the Vigor will capture the o SIP form. Then it will be sent to age.

**Payload Type (rfc2833)** - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

# 3.5.4 Status

From this page, you can find codec, connection and other important call status for each port.

V.ID		CARANNE
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		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		Time		Duration	I	n/Out	/Miss	Acc	ount	ID	Peer	ID
(mm-dd-y	ууу)	(hh:mn	n:ss)	(hh:mm:s	s)							
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	0	00:00:	00	00:00:00	-			-				
00-00-	0	00:00:	:00	00:00:00	-			-				
00-00-	Ο	00:00:	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.

Refresh Seconds : 10 V 5 10 30

	30
Port	It shows current connection status for Phone(s) and ISDN ports.
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.	

# **3.6 Wireless LAN**

This function is used for "n" models.

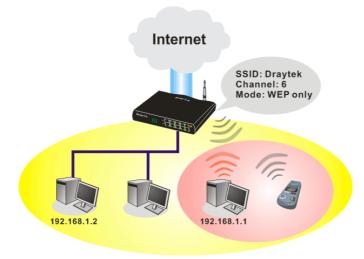
# 3.6.1 Basic Concepts

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.





# 3.6.2 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 Set	tup
General Setting (IEEE 802.11	1)
Enable Wireless LAN	
Mode :	Mixed(11b+11g+11n) 💌
SSID:	DrayTek
Channel :	Channel 6, 2437MHz
Packet-OVERDRIVE ^T	гм
Tx Burst	
Note:	
The same technolog	gy must also be supported in clients to boost WLAN performance.
Hide SSID	
Long Preamble	
	SSID from being scanned. cessary for some older 802.11b devices only (lowers performance).
	OK Cancel
nable Wireless LAN	Check the box to enable wireless function.
ſode	At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11b+11g+11n) Mixed(11b+11g+11n)
SID	Means the identification of the wireless LAN. SSID can b any text numbers or various special characters. The defaul SSID is "DrayTek". We suggest you to change it.
Channel Means the channel of frequency of the wireless L default channel is 6. You may switch channel if the selected channel is under serious interference. If y no idea of choosing the frequency, please select A 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 Burst**). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

**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**).

Vigor N61 802.11n Wireless USB Adapter	Utility	×
Configuration Status Option About		
General Setting	Advance Setting	
🗹 Auto launch when Windows start up	Disable <u>R</u> adio	
Remember mini status position	Fragmentation Threshold :	2346
🔲 Auto <u>h</u> ide mini status	R TS Threshold :	2347
Set <u>m</u> ini status always on top	Frequency :	302.11b/g/n - 2.4GH 💌
Enable IP Setting and Proxy Setting in Prof	le Ad-hoc Channel:	· · · · · · · · · · · · · · · · · · ·
Group Roaming Ad-hoc	Power Save Mode:	Disable 🗸
	Tx <u>B</u> urst :	Disable
WLAN type to connect		
Infrastructure and Ad-hoc <u>n</u> etwork		
<ul> <li>Infrastructure network only</li> </ul>		
O Ad-hoc network only		
Automatically connect to non-preferred net	wor <u>k</u> s	
	ОК	Cancel Apply
Tx <u>B</u> urst :	Disable 💊	*
	Disable	
	Enable	

#### 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<br/>enabled. You can hide it for your necessity.Long PreambleThis option is to define the length of the sync field in an<br/>802.11 packet. Most modern wireless network uses short<br/>preamble with 56 bit sync field instead of long preamble<br/>with 128 bit sync field. However, some original 11b<br/>wireless network devices only support long preamble.<br/>Check it to use Long Preamble if needed to communicate<br/>with this kind of devices.

# 3.6.3 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.

Mode:	Disable 💙
WPA:	
Encryption Mode:	TKIP for WPA/AES for WPA2
Pre-Shared Key(PSK):	*****
Type 8~63 ASCII charac "cfgs01a2" or "0x655al	ter or 64 Hexadecimal digits leading by "0x", for example bcd".
WEP:	
Encryption Mode:	64-Bit 😒
● Key 1 :	****
○Key 2 :	****
○Key 3 :	****
○Key 4 :	****
"0x4142333132". For 128 bit WEP key	Hexadecimal digits leading by "0x", for example "AB312" or Hexadecimal digits leading by "0x", for example

Mode

There are several modes provided for you to choose.

Mode:

•	
Disable	*
Disable	
WEP	
WPA/PSK	
WPA2/PSK	
Mixed(WPA+WPA2)/PSK	

**Disable** - Turn off the encryption mechanism.

**WEP-**Accepts only WEP clients and the encryption key should be entered in WEP Key.

**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.
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	<ul> <li>64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)</li> <li>128-Bit - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).</li> </ul>
	Encryption Mode: 64-Bit 64-Bit 128-Bit
	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.

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.

# 3.6.4 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.

Access Control	trol		
·	Policy :	Activate MAC address filter	
1	Index Attribute	MAC Address Filter MAC Address	
	Client's MAC Add	Iress : : : : : : : : : : : : : : : : : :	
	Add	Delete Edit Cancel	
Enable Access Conti Policy	Se A ac C W	elect to enable the MAC Address access control feature. elect to enable any one of the following policy. Choose <b>ctivate MAC address filter</b> to type in the MAC ddresses for other clients in the network manually. hoose <b>Isolate WLAN from LAN</b> will separate all the /LAN stations from LAN based on the MAC Address list Policy : Activate MAC address filter Solicy : Activate MAC address filter Isolate WLAN from LAN	
MAC Address Filter	D	isplay all MAC addresses that are edited before.	
Client's MAC Addr	ess M	anually enter the MAC address of wireless client.	
Attribute	W	<b>Isolate the station from LAN -</b> select to isolate the ireless connection of the wireless client of the MAC ddress from LAN.	
Add	А	Add a new MAC address into the list.	
Delete	D	elete the selected MAC address in the list.	
Edit	E	dit the selected MAC address in the list.	
Cancel	G	ive up the access control set up.	

Wireless LAN >> Access Control



Click it to save the access control list.

**Clear All** Clean all entries in the MAC address list.

# 3.6.5 Station List

OK

**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	N >> Station List	
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 <u>Access Control</u> :	
	Client's MAC address	
	Add	
Refresh	Click this button to refresh the status of station l	ist.
dd	Click this button to add current typed MAC add	ress ir

Access Control.

Vigor2920 Series User's Guide

# 3.7 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.

System Maintenance	
System Status	
User Password	
Time and Date	
Reboot System	

# 3.7.1 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 : Vigor2920Vn Firmware Version : 3.3.3_RC2 Build Date/Time : Apr 1 2010 12:06:23				
	LAN			WAN 1
MAC Address	: 00-50-7F	-C8-D3-B8	Link Status	: Connected
1st IP Address	: 192.168.1	1.1	MAC Address	: 00-50-7F-C8-D3-B9
1st Subnet Mask : 255,255,255,0		255.0	Connection	: Static IP
DHCP Server	: Yes		IP Address	: 172.16.3.102
DNS	: 168.95.1	.1	Default Gateway	: 172.16.1.1
	VoIP			WAN 2
Port Pro	file Req.	In/Out	Link Status	: Disconnected
Phone1	No	0/0	MAC Address	: 00-50-7F-C8-D3-BA
Phone2	No	0/0	Connection	:
			IP Address	:
			Default Gateway	:

Wi	reless LAN
MAC Address	: 00-50-7F-C8-D3-B8
Frequency Domain	: Europe
Firmware Version	: 1.8.1.0
SSID	: DrayTek

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	
MAC Address	Display the MAC address of the LAN Interface.
1 st IP Address	Display the IP address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN	
Link Status	Display current connection status.

MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
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.

# 3.7.2 User Password

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

S١	vstem	Maint	enance	>>	User	Password
-	300111	manne	chance		0301	1 03311010

Old Passwo	ord	
New Passw	vord	
Confirm Pa	ssword	

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.

# 3.7.3 Time and Date

System Maintenance >> Time and Date

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

Current System Time 20	10 Apr 2 Fri 6 : 7 : 57 Inquire Time
Time Setup	
🔘 Use Browser Time	
💿 Use Internet Time Client	
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin 🛛 💌
Enable Daylight Saving	
Automatically Update Inter	val 30 min 🛩
	OK Cancel
Current System Time	Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time 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 settings.	

# 3.7.4 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.

System Mainten	ance >> Reboot System
Reboot System	
	Do you want to reboot your router ?
	Osing current configuration
	ОК

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



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

# 3.8 Diagnostics

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

Dia	gnostics
⊳	DHCP Table
- Þ	Traffic Graph
- Þ	Ping Diagnosis
⊳	Trace Route

# 3.8.1 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.

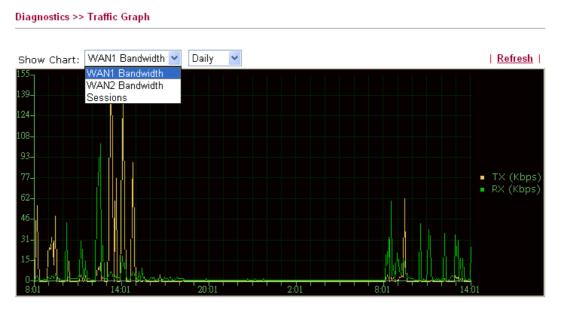
Diagnostics >> View DHCP Assigned IP Addresses

```
DHCP IP Assignment Table | Refresh |
DHCP server: Running
Index IF 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	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

# 3.8.2 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 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 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.

# 3.8.3 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

Ping Diagnosis				
which WAN p	want to ping ping through, j ugh: WAN1	a LAN PC or you please select "U	u don't want to specify Inspecified".	,
Ping to:	Host / IP 💌 Host / IP	IP Address:		
Result	GateWay1 GateWay2 DNS		<u> </u>	<u>Clear</u>
				~

**Ping 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. Ping through: Unspecified Unspecified WAN1 WAN2
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.

# 3.8.4 Trace Route

Diagnostics >> 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.

ace Route		
	Trace through:	WAN1 💌
	Host / IP Address:	
	Result	

Host / IP Address:		Run
Result		<u>Clear</u>
Trace through WAN1. traceroute to 172.16. 1 Request timed out 2 Request timed out Trace complete.	. *	

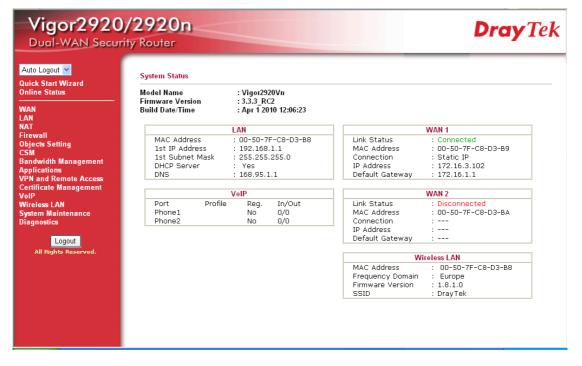
Trace through	Use the drop down list to choose the WAN interface that you want to ping through or choose <b>Unspecified</b> to be determined by the router automatically.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

# **4** 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.



# 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, Vigor2920 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2920, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2920n 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 Vigor2920n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor2920n series.



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



# 4.1.2 General Setup

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

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port (WAN1- through WAN port/WAN2- through LAN1 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

Note: In default, WAN1 is enabled. WAN2 is optional.			
WAN >> General Setup			
General Setup			
WAN1		WAN2	
Enable:	Yes 🛩	Enable:	Yes 💌
Display Name:		Display Name:	
Physical Mode:	Ethernet	Physical Mode:	Ethernet 💌
Physical Type:	Auto negotiation 👻	Physical Type:	Auto negotiation
Load Balance Mode:	Auto Weight 🛛 👻	Load Balance Mode:	Auto Weight
Line Speed(Kbps):	DownLink 0	Line Speed(Kbps):	DownLink 0
	UpLink 0		UpLink 0
Active Mode:	Always On	Active Mode:	Always On
Active on demand:		Active mode. Active on demand:	Always On
🔾 WAN2 Fail		O WAN1 Fail	
WAN2 Upload speed exceed     Kbps		WAN1 Upload sp	eed exceed 0 Kbps
WAN2 Download	speed exceed 0 Kbps		
		WANT DOWINDad	speed exceed o Kups

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 the WAN1/WAN2 interface.		
Physical Mode	For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port.		
	Physical Mode:	Ethernet 💌	
		Ethernet	

OK

**Dray** Tek

3G USB Modem

To use 3G network connection through 3G USB Modem, choose **3G USB Modem** as the physical mode in **WAN2**. Next, go to **WAN>> Internet Access**. 3G USB Modem is available for WAN2. You can choose **PPP** as the access mode and click Details Page for further configuration.

	WAN >> Internet Access				
	Internet Access				
	Index Display Name	Physical Mode	Access Mode		
	WAN1	Ethernet	Static or Dynamic IP V Details Page		
	WAN2	3G USB Modem	None Details Page None PPP		
Physical Type	You can chang	ge the physi	ical type for WAN2 or choose Auto		
	-		ed by the system.		
	Physical Type:		Auto negotiation 🔽		
			Auto negotiation		
			10M half duplex		
			10M full duplex		
			100M half duplex		
			100M full duplex		
Load Balance Mode			bandwidth for your WAN interface,		
			of According to Line Speed.		
	-		Auto Weigh to let the router reach		
	the best load b	alance.			
	Load Balance	e Mode:	Auto Weigh 🛛 👻		
			Auto Weigh		
			According to Line Speed		
Line Speed	Mode, please t	type the lin	<b>g to Line Speed</b> as the <b>Load Balance</b> e speed for downloading and 1/WAN2. The unit is kbps.		
Active Mode	Choose Always On to make the WAN connection				
	(WAN1/WAN2) being activated always; or choose Active on				
	<b>demand</b> to make the WAN connection (WAN1/WAN2 activated if it is necessary.				
	Active Mode:		Active on demand 🐱		
			Always On		
			Active on demand		
			lemand, the Idle Timeout will be		
			r PPPoE and PPTP access modes in		
		0	N>>Internet Access. In addition, there		
		•	bu to choose for different purposes. The connection for WAN1 will be		
	activated when				
			ceed XX kbps – It means the		
	-	-	ll be activated when WAN2 Upload		
			that you set in this box for $15$		
	seconds.				
		-	exceed XX kbps– It means the		
			ll be activated when WAN2		
	Download speed exceed certain value that you set in this box				



for 15 seconds.

**WAN1 Fail** – It means the connection for WAN2 will be activated when WAN1 is failed.

WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.

**WAN1 Download speed exceed XX kbps**– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.

# 4.1.3 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different Physical Mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.

WAN >> Internet Access

Index Displa	iy Name – Physi	ical Mode	A	ccess Mode	
WAN1	Et	hernet	Static or D	ynamic IP 💌	Details Page
WAN2	3G U9	3B Modem	None	~	Details Page
			None PPP		

#### WAN >> Internet Access

Index	Display Name	Physical Mode	Access Mode
VAN1		Ethernet	Static or Dynamic IP 🔽 🛛 Details
WAN2		Ethernet	None 🔽 Details
			None PPPoE Static or Dynamic IP PPTP/L2TP

Index	It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.			
Display Name	It shows the name of setup.	f the WAN1/WAN2	that entered in general	
Physical Mode	· ·	ll connection for WA B Modem) according Physical Mode	N1 (Ethernet) /WAN2 to the real network	
	Ethernet	Ethernet		
	3G USB Modem	Ethernet		

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.

Static or Dynamic IP 💌
None
PPPoE
Static or Dynamic IP
PPTP/L2TP

There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP/L2TP.

**Details Page** This button will open different web page according to the access mode that you choose in WAN1 or WAN2.

## **Details Page for PPPoE**

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

WAN	>>	Internet	Access

WAN 1			
PPPoE Client Mode		PPP/MP Setup	
🔘 Enable 🛛 💿 Dis	able	PPP Authentication	PAP or CHAP
ISP Access Setup Username Password Index(1-15) in <u>Sche</u> => ,		Idle Timeout IP Address Assignment M (IPCP) WAN IP Alias Fixed IP: O Yes O N Fixed IP Address	
WAN Connection Dete Mode Ping IP TTL: MTU	ARP Detect  ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect ARP Detect	<ul> <li>Default MAC Addre</li> <li>Specify a MAC Address:</li> <li>00.50.7F:00.</li> </ul>	
	ОК	Cancel	

Enable/Disable
 Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.
 ISP Access Setup
 Enter your allocated username, password and authentication parameters according to the information provided by your ISP. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.



WAN Connection Detection	<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>
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
PPP/MP Setup	<ul> <li>PPP Authentication – Select PAP only or PAP or CHAP for PPP.</li> <li>If you want to connect to Internet all the time, you can check</li> <li>Always On.</li> <li>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</li> </ul>
IP Address Assignment Method (IPCP)	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

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

<b>@)</b> w.	AN II	Alias - Mi	crosoft Internet Explorer	
WA	N IP	Alias ( Mu	ilti-NAT )	
In	dex	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**

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 choose **Static or Dynamic IP** mode from **Internet Access** menu. The following web page will be shown.

Static or Dynamic IP (DHCP Client)	WAN IP Network Settings         WAN IP Alias           Obtain an IP address automatically	
Keep WAN Connection         Enable PING to keep alive         PING to the IP         PING Interval         0         minute(s)	Router Name         Domain Name         * : Required for some ISPs         O Specify an IP address         IP Address	3 3
WAN Connection Detection Mode ARP Detect  Ping IP TTL:	Subnet Mask Gateway IP Address DNS Server IP Address Primary IP Address	
MTU 1442 (Max: 1500) RIP Protocol Enable RIP	<ul> <li>Secondary IP Address</li> <li>Default MAC Address</li> <li>Specify a MAC Address</li> <li>MAC Address:</li> <li>00 .50 .7F :00 .00 .01</li> </ul>	

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

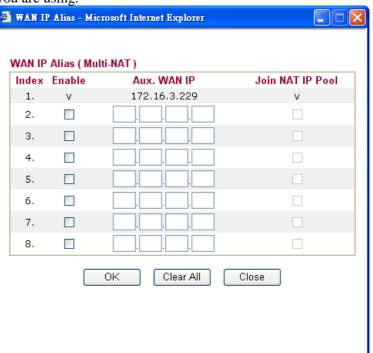
ΟK

Cancel



MTU	It means Max Transmit Unit for packet. The default setting is 1442.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click <b>Enable RIP</b> for activating this function.
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

**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.



**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**Type in the primary IP address for the router if you want to use**AddressStatic IP** mode. If necessary, type in secondary IP address for<br/>necessity in the future.

# **Details Page for PPTP/L2TP**



To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **PPTP/L2TP** from **Internet Access** menu. The following web page will be shown.

WAN >> Internet Access

WAN 1	
PPTP/L2TP Client Mode	PPP Setup
○ Enable PPTP ○ Enable L2TP ④ Disable	PPP Authentication PAP or CHAP 🗸
Server Address	Idle Timeout -1 second(s)
Specify Gateway IP Address	IP Address Assignment Method (IPCP) WAN IP Alias
	Fixed IP: 🔿 Yes 💿 No (Dynamic IP)
ISP Access Setup	Fixed IP Address
Username	WAN IP Network Settings
Password	<ul> <li>Obtain an IP address automatically</li> </ul>
Index(1-15) in <u>Schedule</u> Setup:	Specify an IP address
=>,,,	IP Address
MTU 1442 (Max:1460)	Subnet Mask
ОК	Cancel

PPTP/L2TP Client Mode	<ul> <li>Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.</li> <li>Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.</li> <li>Disable – Click this radio button to close the connection through PPTP or L2TP.</li> <li>Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.</li> <li>Specify Gateway IP Address – Specify the gateway IP address for DHCP server.</li> </ul>
ISP Access Setup	Username -Type in the username provided by ISP in this field. Password -Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
PPP Setup	<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>Fixed IP</b> - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click <b>Yes</b> to use this function and type in a fixed IP address in the box.



**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.

🖥 WAN IP Alias - Microsoft Internet Explorer 🛛 🔲 🔀							
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 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.

### 4.1.4 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 WAN1 or WAN2 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 both WAN1 and WAN2 are activated.

#### WAN >> Load-Balance Policy

```
Load-Balance Policy
```

Index	Enable	Protoco	l	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port End	Move	Move Dowr
1		any	~	WAN1 💌							<u>Dowr</u>
<u>2</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Dowr</u>
<u>3</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Dowr</u>
<u>4</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Dowr</u>
<u>5</u>		any	~	WAN1 💌						<u>UP</u>	<u>Dowr</u>
<u>6</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Dowr</u>
Z		any	~	WAN1 💌						<u>UP</u>	<u>Dowr</u>
<u>8</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Dowr</u>
<u>9</u>		any	~	WAN1 🔽						<u>UP</u>	Dowr
<u>10</u>		any	*	WAN1 🔽						<u>UP</u>	<u>Down</u>
<< <u>1-10</u>	<u>11-20</u> :	>>								ļ	Next >
					_						

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

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

#### WAN >> Load-Balance Policy

Src I	col ng WAN Interface P Start	any  WAN1  Auto failover to the other WAN
Src I	-	WAN1 👻 🗹 Auto failover to the other WAN
	P Start	
	Juli	
Src I	P End	
Dest	IP Start	
Dest	IP End	
Dest	Port Start	
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 or WAN2) 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.

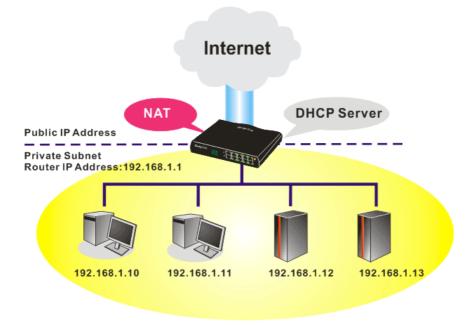
## 4.2 LAN

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.



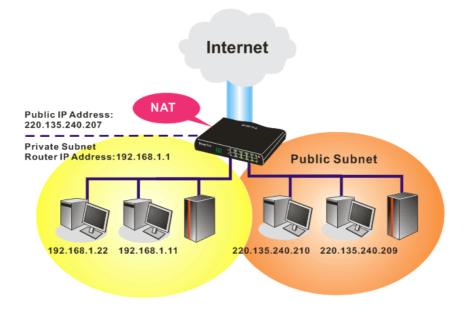
### 4.2.1 Basics of LAN

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)

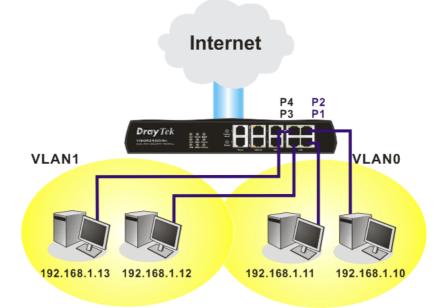
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### 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.





## 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.

LAN >> General Setup			
Ethernet TCP / IP and DHC	P Setup		
LAN IP Network Configura	tion	DHCP Server Configuratio	n
For NAT Usage		💿 Enable Server 🔘 Disa	ble Server
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Su	bnet 🔾 2nd Subnet
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	
2r	nd Subnet DHCP Server	for Relay Agent	
		DNS Server IP Address	
RIP Protocol Control	Disable 🗸	Force DNS manual s	setting
KIP PIOLOCOI CUITITOI		Primary IP Address	
		Secondary IP Address	

OK

1st IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).		
1st Subnet Mask	Type in an address code that determines the size of the network. Default: 255.255.255.0/24)		
For IP Routing Usage	Click <b>Enable</b> to invoke this function. The default setting is <b>Disable</b> .		
2 nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)		
2 nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)		
2 nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd subnet.		

http://192.168.1.1 - Router Web Configurator - Microsoft Internet Explorer	
2nd DHCP Server	
Start IP Address	
IP Pool Counts 0 (max. 10)	
Index Matched MAC Address given IP Address	
MAC Address : : : : : : : : : : : : : : : : : :	
OK Clear All Close	

Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

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 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

**RIP Protocol Control** Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

**RIP Protocol Control** 

Disable	*
Disable	
1st Subnet	
2nd Subnet	

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.

2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP stands for Dynamic Host Configuration Protocol. The **DHCP Server** 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.

Configuration

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

**Enable Server -** Let the router assign IP address to every host in the LAN.

**Disable Server** – Let you manually assign IP address to every host in the LAN.

**Relay Agent** –  $(1^{st} subnet/2^{nd} subnet)$  Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

**Start IP Address -** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

**IP Pool Counts -** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

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

**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**



There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that chapter to get more information for your necessity.

### 4.2.3 Static Route

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

LAN	>>	Stat	ic F	Route	Setup
		~			~~~~

Static 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.

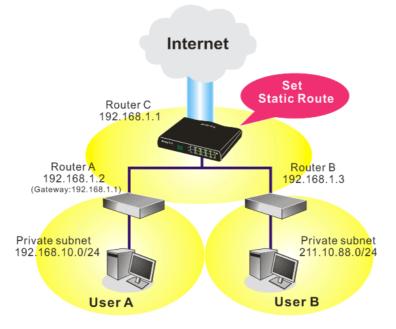
Key: (	C - connected, S -	static, R - RIP, * - default, ~ - priva	te
*	0.0.0/	0.0.0.0 via 172.16.3.1, WAN1	
С~	192.168.1.0/	255.255.255.0 is directly connected,	LAN
С	172.16.3.0/	255.255.255.0 is directly connected,	WAN1

### 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.

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.



LAN >> Static	Route Setup		
Index No. 1			
🗹 Enable			
	Destination IP Address		211.100.88.0
	Subnet Mask		255.255.255.0
	Gateway IP Address		192.168.1.3
	Network Interface		LAN 💌
1	(	OK	Cancel

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

rrent Runn	ing Routing Table		<u>Refresh</u>
Key: C	- connected, S -	static, R - RIP, * - default, ~ - private	1
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 connected, LAN	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3, LAN	

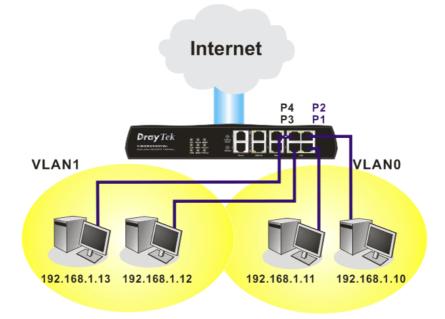
### 4.2.4 VLAN

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.

LAN >> VLAN Configuration						
VLAN Configuration						
Enable						
	P1	P2	P3	P4		
VLAN0						
VLAN1						
VLAN2						
VLAN3						
	OK	Clear	Cancel			

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.

VLAN Configuration					
🗹 Enable					
	P1	P2	P3	P4	
VLAN0					
VLAN1			<b>~</b>		
VLAN2					
VLAN3					

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.

42

LAN >> Bind IP to MAC

Bind IP to MA	c		
	AC binding presets DHCP Allocatio		
	u select Strict Bind, unspecified L	AN clients cannot access.	the Internet.
● Enable	🔿 Disable 🛛 Strict Bind		
ARP Table	<u>Select All</u>   <u>Sort</u>   <u>Refresh</u>	IP Bind List	<u>Select All</u>   <u>Sort</u>
IP         Address           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           192.168.1.         192.168.1.           Mad and Edit         IP           Add and Edit         IP	10 00-0E-A6-2A-D5-A1 219 00-50-7F-33-F8-0B 92 00-13-D4-1B-B3-3D 218 00-0B-CD-55-CB-45 11 00-0D-0B-A7-86-F3 100 00-08-A1-36-97-5D 222 00-18-F3-C0-42-2C 10 00-E0-18-F9-53-D5 4 00-85-A0-01-01-00 ♥	Index IP Address	Mac Address
	Add	Edit Delete	
		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.
Add and Edit	<ul> <li>IP Address – Type the IP address that will be used for the specified MAC address.</li> <li>Mac Address – Type the MAC address that is used to bind with the assigned IP address.</li> </ul>
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
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> .

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

### 4.3 NAT

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

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

The benefit of the NAT includes:

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

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.

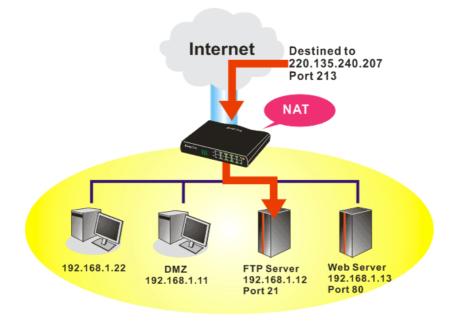
Below shows the menu items for NAT.



### 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	Redi	irection
		1 010	NO G	n e eu on

Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				×
<u>2.</u>				x
<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>				×

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.

ОК	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 and</b> <b>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



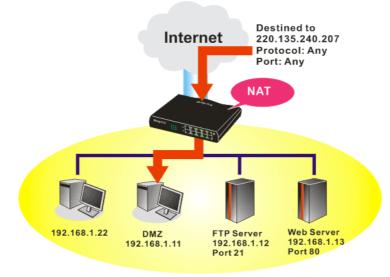
will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

System Maintenance >> Management

Management Acces	s Control	Management Port Setu	p
		💿 User Define Ports	🔘 Default Ports
-	ent from the Internet	Telnet Port	23 (Default: 23)
FTP Server		HTTP Port	80 (Default: 80)
HTTP Serve		HTTPS Port	443 (Default: 443)
HITPS Serv Telnet Servi		FTP Port	21 (Default: 21)
SSH Server		SSH Port	22 (Default: 22)
🗹 Disable PING fr	om the Internet	SNMP Setup	
Access List		📃 Enable SNMP Age	nt
List IP	Subnet Mask	Get Community	public
1		Set Community	private
2		Manager Host IP	
3			ablia
		Trap Community	public
		Notification Host IP	
		Trap Timeout	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.



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

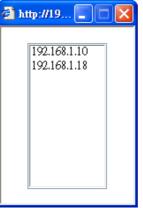
VAN 1	
None 💌	
Private IP	Choose PC
	AZ Host
MAC Address of the True IP D	AZ Host 00 00 00 00 00 00 00 00
	lost is turned on, it will force the router's WAN connection to be
Note: When a True-IP DMZ h	
Note: When a True-IP DMZ h always on.	

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

NAT >> DMZ	Host Setup
------------	------------

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229		Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				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. NAT >> DMZ Host Setup

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229	192.168.1.10	Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC

### 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>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				×
<u>10.</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. Specify the name for the defined network service.

Comment

## **Local IP Address** Display the private IP address of the local host offering the service.

Status Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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

🗹 E	nable Open P	orts						
	Comment			P2P				
	WAN Interface			WAN1 💌				
	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

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

<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.
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.



## 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:

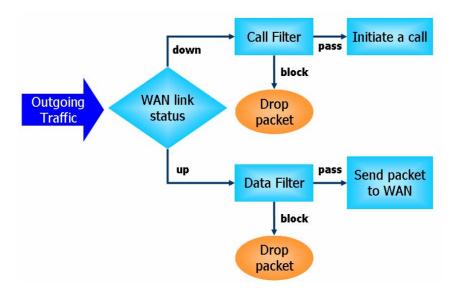
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

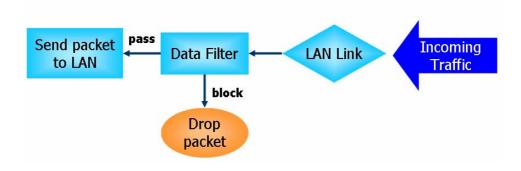
### **IP Filters**

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.

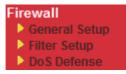
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

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

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

Below shows the menu items for Firewall.



### 4.4.2 General Setup

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

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

Call Filter	Enable	Start Filter	Set Set#1 V
	O Disable	otarernitor	
Data Filter	Enable	Start Filter	Set Set#2 💙
	🔘 Disable		
Actions for default ru	le:		
Application		Action/Profile	Syslog
Filter		Pass 💌	
IM/P2P Filter		None 💌	
URL Content Filter		None 🛩	
Web Content Filter		1-Default 💌	
Advance Setting		Edit	
Accept large inc	omina fraamen	ited UDP or ICMP pack	ets ( for some games, ex. CS
- Strict Security Ch		, cou obri or romin puor	
Web-Filter	5		

	Cancel
Call Filter	Check <b>Enable</b> to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check <b>Enable</b> to activate the Data Filter function. Assign a start filter set for the Data Filter.
Filter	Select <b>Pass</b> or <b>Block</b> for the packets that do not match with the filter rules.       Pass      Pass      Block
IM/P2P Filter	Select a CSM profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
URL Content Filter	Select one of the <b>URL Content Filter</b> profile settings (created in <b>CSM&gt;&gt; URL Content Filter Profile</b> ) for applying with this router.



	Please set at least one profile for choosing in <b>CSM&gt;&gt; URL Content</b> <b>Filter Profile</b> web page first. For troubleshooting needs, you can specify to record information for <b>URL Content Filter</b> by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
Web Content Filter	Select one of the <b>Web Content Filter</b> profile settings (created in <b>CSM&gt;&gt; Web Content Filter Profile</b> ) for applying with this router. Please set at least one profile for anti-virus in <b>CSM&gt;&gt; Web Content</b> <b>Filter Profile</b> web page first. For troubleshooting needs, you can specify to record information for <b>Web Content Filter</b> by checking the Log box. It will be sent to Syslog server. Please refer to section <b>Syslog/Mail Alert</b> for more detailed information.
Syslog	For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on DrayTek Syslog window.
Advance Setting	Click Edit to open the following window. However, it is strongly

recommended to use the default settings here.

Advance Setting		
Codepage	ANSI(1252)-Latin I	*
Window size:	65535	
Session timeout:	1440 Minute	
[	OK	

**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		
Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Controls Contre	192.168.1.1           Vigor           RX Packets           15285	WAN Information WAN1 IP (Fixed) 172.16.2.213 WAN2 IP (Fixed)
Setup		
Tool Setup   Telnet Read-out Setur	p Codepage Information	
Windows Version: 5.01.2600 RECOMMENDED CODEPA 950 (ANSI/OEM - Tradition 00a1-21.00a6:7c.00a9:63.00a	GE:	163:33 0069:31 006a:6f (

**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.

Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".

### 4.4.3 Filter Setup

Firewall >> Filter Setup

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

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1				
Comments : Defa	ault Call Filter			
Filter Rule	Active	Comments	Move Up	Move Down
1	<b>~</b>	Block NetBios		<u>Down</u>
2			<u>UP</u>	<u>Down</u>
3			<u>UP</u>	<u>Down</u>
4			<u>UP</u>	<u>Down</u>
5			<u>UP</u>	<u>Down</u>
6			<u>UP</u>	<u>Down</u>
7			<u>UP</u>	
			Next Filte	er Set 🛛 None 💌
		OK Clear Cancel		
Filter Rule		lick a button numbered (1 ~ 7) to ed ill open Edit Filter Rule web page.		

	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.

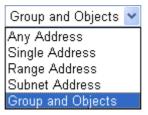
Firewall >> Edit Filter Set >> Edit Filte
-------------------------------------------

Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN -> 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:	Block Immediately	
Branch to Other Filter Set:	None 🗸	
IM/P2P Filter:	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 (LAN->WAN/WAN->LAN). It is for <b>Data Filter</b> only. For the <b>Call Filter</b> , this setting is not available since <b>Call Filter</b> is only applied to outgoing traffic.
Source/Destination IP	Click <b>Edit</b> to access into the following dialog to choose the source/destination IP or IP ranges.

IP Addı	ress 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	
	IP Group	None 💌
	or <u>IP Object</u>	None 🔽
	or IP Object	None 1-RD Department
	or IP Object	2-Financial Dept.
		3-HR Department
	OK	Close

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

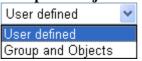
Click **Edit** to access into the following dialog to choose a suitable service type.

evurce Port = 137 ~139 estination Port = 1 ~65535 ervice Group None		
estination Port = 1 ~ 65535	Protocol	
ervice Group	Source Port	= 🖌 137 🖌 139
	Destination Port	= 🗸 1 ~ 65535
	Service Group	None 💌
	or <u>Service Object</u>	None 💌
Service Object None 1-SIP	or Service Object	
Service Object 2-RTP	or Service Object	
	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



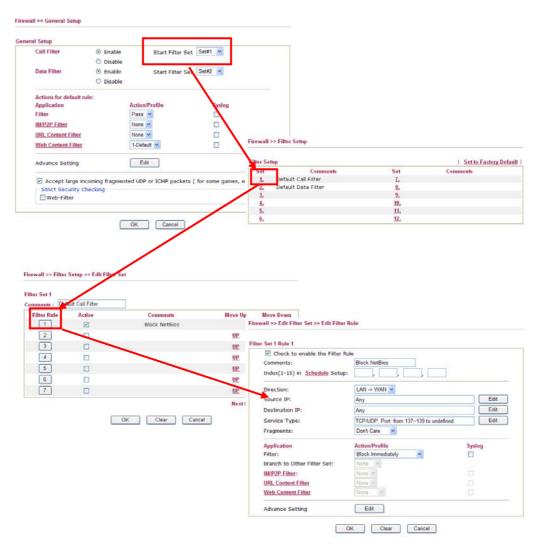
use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



**Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -**(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. (!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) – the port number greater than this value is available. (<) – the port number less than this value is available for this profile. Service Group/Object - Use the drop down list to choose the one that you want. **Fragments** Specify the action for fragmented packets. And it is used for Data Filter only. Don't care - No action will be taken towards fragmented packets. **Unfragmented** - Apply the rule to unfragmented packets. Fragmented - Apply the rule to fragmented packets. Too Short - Apply the rule only to packets that are too short to contain a complete header. Filter Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. **Pass Immediately** - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through. If the packet matches the filter rule, the next filter rule will branch **Branch to other Filter** Set 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. IM/P2P Filter / All the packets/connections within the range configured in the **URL Content Filter /** above conditions must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section Web Content Filter of CSM profile setup. For troubleshooting needs you can specify the filter log and/or CSM SysLog log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on DrayTek Syslog window.

### 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.



### 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.

Enable DoS Defense			
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
Block IP options	🔲 Block TCP flag	scan	
Block Land	🔲 Block Tear Dro	р	
Block Smurf	🔲 Block Ping of D	eath	
🔲 Block trace route	🔲 Block ICMP fra	gment	
Block SYN fragment	📃 Block Unknown	Protocol	
📃 Block Fraggle Attack			
Enable DoS defense function to preve crackers.	ent the attacks f	rom hacker	or 🔨

Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
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 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 scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.



Block Unknown	Check the box to activate the Block Unknown Protocol function.
Protocol	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.

SysLog / Mail Alert Setup Mail Alert Setup SysLog Access Setup Send a test e-mail Enable 🗹 Enable Server IP Address SMTP Server Mail To Destination Port 514 Enable syslog message: Return-Path Firewall Log Authentication VPN Log User Name User Access Log Password Call Log Enable E-Mail Alert: WAN Log DoS Attack M-P2P Router/DSL information OK Clear Cancel

ntrols N Status TX Packets 4175	RXP	.1  Series ackets 568	WAN Stat	us ateway IP (Fixed) 172.16.3.4 WAN IP (Fixed) 172.16.3.229	TX Packets 343 RX Packets 2558	TX Rate 3 RX Rate 126
wall Log VPN Log User			ζ Others	Network Information	Net State Traffic Graph	
līme Jan 100:00:42 Jan 100:00:34	Host Vigor Vigor	Message DoS syn_flood Bl DoS iemp_flood E	ock(10s) 192 lock(10s) 19	168.1.115,10605 -> 19: 2.168.1.115 -> 192.168	2.168 1 1,23 PR 6(kp) len 2 1 1 PR 1(icmp) len 20 60 ic	0 40 -8 3943751 mp 0/8
						د
K J Mode	State	Up S	peed	Down Speed	SNR Margin	Loop Att

System Maintenance >> SysLog / Mail Alert Setup

## 4.5 Objects Settings

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

Objects Setting
IP Object
IP Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
IM Object
P2P Object
Misc Object
Milde Object

### 4.5.1 IP Object

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

Objects Setting >> IP Object	
------------------------------	--

5 In march		
Name	Index	Name
	<u>17.</u>	
	<u>18.</u>	
	<u>19.</u>	
	<u>20.</u>	
	<u>21.</u>	
	<u>22.</u>	
	<u>23.</u>	
	<u>24.</u>	
	<u>25.</u>	
	<u>26.</u>	
	<u>27.</u>	
	<u>28.</u>	
	<u>29.</u>	
	<u>30.</u>	
	<u>31.</u>	
	<u>32.</u>	
	6   07 120   120 160   16	18.         19.         20.         21.         22.         23.         24.         25.         26.         27.         28.         29.         30.         31.

#### Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

#### Objects Setting >> IP Object

Nine: - :	<b>BD</b> Department		
Name:	RD Department		
Interface:	Any 🕶		
Address Type:	Range Address 💙		
Start IP Address:	192.168.1.64		
End IP Address:	192.168.1.75		
Subnet Mask:	0.0.0		
Invert Selection:			
	OK Clear Cancel		
Name	Type a name for this profile. Maximum 15 characters are allowed.		
Interface	Choose a proper interface (WAN, LAN or Any).		
	Interface: Any Any LAN WAN		
	<ul> <li>For example, the <b>Direction</b> setting in <b>Edit Filter Rule</b> will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the <b>Interface</b> here, and choose LAN as the direction setting in <b>Edit Filter Rule</b>, then all the IP addresses specified with LAN interface will be opened for you to choose in <b>Edit Filter Rule</b> page.</li> </ul>		
Address Type	<ul> <li>Determine the address type for the IP address.</li> <li>Select Single Address if this object contains one IP address only.</li> <li>Select Range Address if this object contains several IPs within a range.</li> <li>Select Subnet Address if this object contains one subnet for II address.</li> <li>Select Any Address if this object contains any IP address.</li> </ul>		
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.

Objects Setting >> IP Object			
P Object Profiles	:		
Index	Name	Index	
<u>1.</u>	RD Department	<u>17.</u>	
<u>2.</u>	Financial Dept.	<u>18.</u>	
<u>3.</u>	HR Department	<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	

## 4.5.2 IP Group

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

Objects Setting >> IP Group

IP Group Table:			Set to Factory Default
Index	Name	Index	Name
<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 >> IP Group

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

**Dray** Tek

# 4.5.3 Service Type Object

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

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

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

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

Click the number under Index column for settings in detail.

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

Profile Index : 1	
Name	WWW
Protocol	TCP 💽 6
Source Port	= 🖌 1 ~ 65535
Destination Port	= 🖌 80 ~ 80
(	OK Clear Cancel
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to. TCP  Any ICMP IGMP TCP UDP TCP/UDP Other
Source/Destination Port	<ul> <li>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</li> <li>(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a</li> </ul>



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 Type Object Profiles:

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

## 4.5.4 Service Type Group

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

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

Service Type Group	o 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.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type G	roup Setup	
Profile Index : 1		
Name:	VoIP	
Available Service Type	Objects Selected	I Service Type Objects
1-SIP 2-RTP	OK Clear	Cancel
Name	Type a name for this pr	ofile.
Available Service Type Objects	All the available service	e objects that you have added on vice Type Object will be shown in
Selected Service Type Objects	Click >> button to add	the selected IP objects in this box.

## 4.5.5 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

It 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

## 4.5.6 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**.

passed/blocked based on the configuration on Firewall settings.

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

Objects Setting >> Keyword Group

**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			
	») ((		
	OK Clear Cancel		
me	Type a name for this group.		
ailable Keyword jects	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.		
ected Keyword Objects	Click button to add the selected Keyword objects in this box.		

## 4.5.7 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.

Profile 1 with name of "default" is the default profile, some files with the file extensions specified in this profile will be ignored and not be scanned by Vigor router.

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.

Objects Setting >> File Extension Object

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

## 4.5.8 IM Object

Objects Setting >> IM Object Profile

This page allows you to set 32 profiles for Instant Messenger. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

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

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

Click the number under Profile column for configuration in details. There are several types of Instant Messenger (IM) provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **IM Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Profile Index: 1					
rofile Name:		_			
Check for Disallow:	Select All				
neck for Disanow:		Advanced	Management		
Activity / Ap	plication	MSN	YahooIM	AIM(<= v5.9)	ICQ
Logir					
Messa					
File Trar	-				
Gam					
Vide					
Voice	e				
Confere	nce			_	
Other Act	ivities				
	]	M Application			VoIP
AIM6	□ QQ	iChat	🗌 Jabb	er/GoogleTalk	Skype
GoogleChat	XFire	🗌 GaduGadu	u 🗌 Palta	alk	Kubao
Qnext	Meetro	POCO/PP3	365 Ares	Chat	Gizmo
AliWW	КС	Lava-Lav	a 🗌 ICU2	2	SIP
□iSpQ	UC	MobileMS	N		L SIP
	w	eb IM ( * = mor	e than one addre	ess)	
WebIM URLs	<u>eMessenger</u> ICQ Java* IMUnitive* MessengerFX*	<u>WebMSN</u> ICQ Flash* <u>Wablet*</u> MessengerAdic	<u>meebo*</u> g <u>oowy*</u> <u>mabber*</u> tos WebYahoolM	<u>eBuddy</u> <u>IMhaha*</u> <u>MSN2GO*</u>	<u>ILoveIM*</u> getMessenger KooIIM
		ок С	lear Cance		

**Profile Name** 

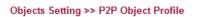
Type a name for this profile.

Type a name for such profile and check all the items that not allowed to be used in the host. Finally, click **OK** to save this profile.

## 4.5.9 P2P Object

This page allows you to set 32 profiles for peer-to-peer application. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

P2P Profile Ta	able:		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>	



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

Click the number under Profile column for configuration in details. There are several items for P2P protocols provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **P2P Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

#### Objects Setting >> P2P Object Profile

Profile Index: 1					
Profile Name:					
Check for Disallow: Select A	I				
Protocol		Applications			
SoulSeek	SoulSeek				
eDonkey	eDonkey, eMule	, Shareaza			
FastTrack	KazaA, BearSha	re, iMesh			
OpenFT	KCeasy, FilePipe				
Gnutella	BearShare, Limewire, Shareaza, Foxy				
OpenNap	Lopster, XNap, WinLop				
BitTorrent	BitTorrent, BitSpirit, BitComet				
Winny	Winny, WinMX,	Share			
	Other P2P	Applications			
Xunlei	🗌 Vagaa	PP365	POCO		
Clubbox	Ares	ezPeer	Pando		
	ОК С	lear Cancel			

#### **Profile Name**

Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

## 4.5.10 Misc Object

This page allows you to set 32 profiles for miscellaneous applications. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

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

Objects Setting >> Misc Object Profile

#### Set to Factory Default

Clear all profiles.

Click the number under Profile column for configuration in details. Applications for tunneling and streaming are listed in the page for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **Misc Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Profile Index: 1				
Profile Name:				
Check for Disallow:	Select All			
		Tunneling		
Socks4/5	PGPNet	HTTP Proxy	Tor	
SoftEther	MS TEREDO	Wujie/UltraSurf	Hamachi	HTTP Tunnel
Ping Tunnel	TinyVPN	RealTunnel	DynaPass	
		Streaming		
MMS	RTSP	TVAnts	PPStream	PPlive
EeiDian	UUSee	NSPlayer	PCAST	TVKoo
SopCast	UDLiveX	TVUPlayer	MySee	Joost
🗌 FlashVideo	SilverLight	Slingbox	QVOD	
		Remote Control		
	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	
	ОК	Clear	Cancel	

Objects Setting >> Misc Object Profile

#### **Profile Name**

Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

# 4.6 CSM Profile

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

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

### **IM/P2P 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.





## 4.6.1 IM/P2P Filter Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. CSM profile can be used in Filter Setup page.

CSM >> IM/P2P Filter Profile

IM/P2P Filte	er Profile Table:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

#### **Set to Factory Default**

Clear all profiles.

Click the number under Index column for settings in detail.

CSM >>	IM/P2P	Filter	Profile
--------	--------	--------	---------

Profile Index: 1		
Profile Name:		
	IM Object	None 💌
	P2P Object	None 💌
	Protocol Object	None 💌
	Misc Object	None 💌
-		OK Cancel

#### **Profile Name**

Type a name for the CSM profile.

Each profile can contain three objects settings, IM Object, P2P Object and Misc Object. Such profile can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.



## 4.6.2 URL Content Filter Profile

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

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

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

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

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

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

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)

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

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

OK



#### CSM >> URL Content Filter Profile

Profile Name:	
Priority:	Both : Pass V Log: None V
1.URL Access	Control
Enabl	le URL Access Control
Action	
Pass	Edit
2.Web Feature	3
Enabl	le Restrict Web Feature
Actio	
Pass	Cookie Proxy <u>File Extension Profile</u> : None
	OK Clear Cancel
Profile Name	Type the name for such profile.
	<ul> <li>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.</li> <li>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 below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</li> <li>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 specified in URL Access Control and Web Feature below, such function can determine the packages matching 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 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 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.</li> </ul>
	Both : Pass Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First

All – All the actions (Pass and Block) will be recorded in Syslog.



URL Access ControlEnable URL Access Control - Check the box to activate URL<br/>Access Control. Note that the priority for URL Access Control is<br/>higher than Restrict Web Feature. If the web content match the<br/>setting set in URL Access Control, the router will execute the action<br/>specified in this field and ignore the action specified under Restrict<br/>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.





**Group/Object Selections** – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.



🤗 Group/Object Edit - Windows Internet Explorer	
🙋 http://192.168.1.1/doc/cfkw.gob.htm	✓
Object/Group Edit	
Keyword Object	None 💙
or Keyword Object	None 💌
or Keyword Object	None 🛩
or Keyword Object	None 🛩
or Keyword Object	None 💙
or <u>Keyword Group</u>	None 💙
or Keyword Group	None 🛩
or Keyword Group	None 🛩
or Keyword Group	None 💙
or Keyword Group	None 🛩
OK	Close

#### Web Feature

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

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

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

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

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

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

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

File Extension Profile – Choose one of the profiles that you configured in Object Setting>> File Extension Objects previously

for passing or blocking the file downloading.

File Extension Profile: None



## 4.6.3 Web Content Filter Profile

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.

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

/eb Content Filter	Profile Table:		Set to Factory Defaul
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>	

CSM >> Web Content Filter Profile

ΟK

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

Profile Index: 1 Profile Name: Default			Log: Block 🛩				
Black/White List Enable Action: Block	Group/Object Selections						
Action: Block V Groups C	ategories						
Child Protection Select All Clear All	<ul> <li>✓ Chat</li> <li>✓ Gambling</li> <li>✓ Sex</li> </ul>	<ul> <li>✓ Criminal</li> <li>✓ Hacking</li> <li>✓ Violence</li> </ul>	<ul> <li>✓ Drugs/Alcohol</li> <li>✓ Hate Speech</li> <li>✓ Weapons</li> </ul>				
Leisure Select All Clear All	<ul> <li>Advertisements</li> <li>Games</li> <li>Hobbies</li> <li>Personals</li> <li>Sports</li> </ul>	Entertainment Glamour Lifestyle Photo Searches Streaming Media	<ul> <li>Food</li> <li>Health</li> <li>Motor Vehicles</li> <li>Shopping</li> <li>Travel</li> </ul>				
Business Select All Clear All	Computing/Internet Politics Remote Proxies	☐ Finance ☐ Real Estate ☐ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail				
Others Select All Clear All	Education  News Usenet News	Hosting Sites Religion Uncategorised Sites	☐ Kid Sites ☐ Sex Education				
	ОК	Cancel					

<b>Enable</b> – Check this box to enable the filtering mechanism with the
<ul> <li>condition of black/white list. Click Edit to open the keyword object /group selection window and choose the one you want to use. Then, choose the action for such selection.</li> <li>Action, Pass – A webpage which content matches with the keyword object /group selection listed in this field is allowed to be passed through the router.</li> <li>Action, Block - A webpage which content matches with the keyword object /group selection listed in this field is blocked through the router.</li> </ul>
<ul> <li>Pass - allow accessing into the corresponding webpage with the categories listed on the box below.</li> <li>Block - restrict accessing into the corresponding webpage with the categories listed on the box below.</li> <li>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</li> </ul>
<ul> <li>None – There is no log file will be recorded for this profile.</li> <li>Pass – Only the log about Pass will be recorded in Syslog.</li> <li>Block – Only the log about Block will be recorded in Syslog.</li> </ul>

All – All the actions (Pass and Block) will be recorded in Syslog.



## 4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Ban	dwidth Management
	Sessions Limit
- Þ. (	Bandwidth Limit
- 🕨 (	Quality of Service

#### 4.7.1 Sessions Limit

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

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

Bandwidth Management >> Sessions Limit

Sessions Limit	t
0	Enable 💿 Disable
De	fault Max Sessions: 100
Lin	nitation List
Īr	ndex Start IP End IP Max Sessions
Sta	ecific Limitation art IP: End IP:
	Add Edit Delete
	-15) in <u>Schedule</u> Setup:,,,,
Note: A	ction and Idle Timeout settings will be ignored.
	OK

To activate the function of limit session, simply click **Enable** and set the default session limit.EnableClick this button to activate the function of limit session.DisableClick 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.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Remove	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.

### 4.7.2 Bandwidth Limit

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

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

💿 Enable 📃 Apply	to 2nd Subnet 🔘 Disable
Default TX Limit: 200	Kbps Default RX Limit: 800 Kbps
Allow auto adjustn	nent to make the best utilization of available bandwidth.
Limitation List	
Index Start IP	End IP TX limit RX limit Shared
Specific Limitation	
Start IP:	TX Limit: Kbps RX Limit: Kbps
€ Each ○ Shared	Add Edit Delete
Each O Shared	
	Add Edit Delete

Bandwidth Management >> Bandwidth Limit



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 2nd 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.
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	Allows 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.

## 4.7.3 Quality of Service

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

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

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

There are two components within Primary configuration of QoS deployment:

• Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.

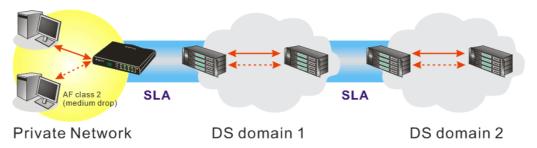


• Scheduling: Based on classification of service level to assign packets to queues and associated service types

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

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

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



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

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

Index Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1 Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2 Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
Class Rule Index	N	ame				Rule	Service	Туре
Class 1						<u>Edit</u>		
Class 2						<u>Edit</u>	<u>Edit</u>	

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.

## **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.

WAN Inbound Ba	andwidth	10000 Kbps
WAN Outbound	Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Bandwidth Cont	rol	Limited_bandwidth Ratio 25 %
Outbound TCP ACK Prioritize	9	Online Statistics
nable the QoS Control	Please also define whi apply to.	Cancel this setting is checked. ch traffic the QoS Control settings will
nable the QoS Control	The factory default for Please also define whi apply to. <b>IN-</b> apply to incoming <b>OUT-</b> apply to outgoin <b>BOTH-</b> apply to both Check this box and cli	this setting is checked. ch traffic the QoS Control settings will traffic only.
nable the QoS Control /AN Inbound Bandwidth	The factory default for Please also define white apply to. <b>IN-</b> apply to incoming <b>OUT-</b> apply to outgoin <b>BOTH-</b> apply to both Check this box and cli will see the <b>Online Sta</b> It allows you to set the For example, if your A	this setting is checked. ch traffic the QoS Control settings will traffic only. g traffic only. incoming and outgoing traffic. ck <b>OK</b> , then click <b>Setup</b> link again. Yo

Bandwidth Management >> Quality of Service



Reserved Bandwidth Ratio	reserv	ed ba	andwidth	group index in th to upstream sp stream speed.		
Enable UDP Bandwidth Control	field. 7	This is pplica	s a protec ation traff	e limited bandwi tion of TCP app ic such as strear	lication traffic si	ince
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 ra applica	• •	•	s reserved for lin	mited bandwidth	n of UDP
Online Statistics	referer	nce.	online stat	istics for quality	of service for y	vour
	WAN1 Onli	ne Statisti	cs	Refresh Int	erval: 5 💌 seconds	<u>Refresh</u>
	Index Direction Class Name Reserved-bandwidth Ratio Outbound Throughput (Bytes/sec)					
	2	OUT		25%	0	
	3	OUT		25%	0	
	4	OUT	Others	25%	0	

#### 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.

Others

10 (Bps)

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

Index S	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1 D	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2 D	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
Class Rul Index	-	N	ame				Rule	Service	
	×	N	ame						
	<b>x</b> 1	N	ame				Rule		Туре

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



#### Bandwidth Management >> Quality of Service

lass Inc	lex #1				
lame	Test				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
Add Edit Delete					

For adding a new rule, click **Add** to open the following page. Bandwidth Management >> Quality of Service

🗹 ACT		
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	*
Service Type	ANY	~
Note: Please choose,	setup the <u>Service Typ</u>	<u>e</u> first.

Cancel

OK

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 <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.
Edit	It allows you to edit source address information.
	🗿 http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer
	Address Type Subnet Address 🖌
	Start IP Address 0.0.0.0
	End IP Address 0.0.0.0
	Subnet Mask 0.0.0.0
	OK Close
	Address Type – Determine the address type for the source
	address.
	For 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 <b>Subnet Address</b> , you have to fill in Start IP address and
	Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.



# Service Type It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Class Inc	lex #1				
Jame	Game				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 🔿	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)
2 🔿	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)
Add Edit Delete					

#### 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

Bandwidth Management >> Quality of Service

General	Setup								
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<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 Se	lser 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	TCP 🔽 6
Port Configurati	n
Туре	💿 Single 🛛 Range
Port Num	er 0 - 0
Service Name	OK Cancel 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. <b>Port Number</b> – 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 40 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.

# **Dray** Tek

# 4.8 Applications

Below shows the menu items for Applications.

Appli	ications
🕑 🕨 D	ynamic DNS
🔸 🕨 S	chedule
🔸 🕨 R	ADIUS
🕩 U	PnP
🔹 🕨 IG	MP
🔹 🕨 M	lake on LAN

## 4.8.1 Dynamic DNS

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

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

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

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

Applications >> Dynamic DNS Setup

Enable Dynamic DNS Setup		View Log	Force Update
Auto-Update inte	erval 1440 Min(s)		
ccounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		x
<u>3.</u>	WAN1 First		x

**Set to Factory Default** Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Auto-Update IntervalType the time interval for auto update information about<br/>dynamic DNS server.IndexClick the number below Index to access into the setting<br/>page of DDNS setup to set account(s).

**Dray** Tek

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.

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

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

Index : 1	
🗹 Enable Dynamic DNS	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	
	OK Clear Cancel

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	Select the WAN interface order to apply settings here.
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.
Clipt OV by the to get	mate the settings. Very will see mere setting has here some

8. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

#### Disable the Function and Clear all Dynamic DNS Accounts

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

#### **Delete a Dynamic DNS Account**



In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

## 4.8.2 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.

dule:			Set to Factory Defau
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	х
<u>2.</u>	х	<u>10.</u>	х
<u>3.</u>	х	<u>11.</u>	х
<u>4.</u>	×	<u>12.</u>	х
<u>5.</u>	X	<u>13.</u>	х
<u>6.</u>	×	<u>14.</u>	х
<u>7.</u>	х	<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.	
Index	Click the number below Index to access into the setting page of schedule.	
Status	Display if this schedule setting is active or inactive.	

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

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.

#### Applications >> Schedule

ndex No. 1	
🗹 Enable Schedule Setup	
Start Date (yyyy-mm-dd)	2000 🕶 1 💌 1 💌
Start Time (hh:mm)	0 💌 : 0 💌
Duration Time (hh:mm)	0 💌 : 0 💌
Action	Force On
Idle Timeout	minute(s).(max. 255, 0 for default)
How Often	
O Once	
<ul> <li>Weekdays</li> </ul>	
🗌 Sun 🗹 Mon 🗹	] Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat

	OK Clear Cancel	
Enable Schedule Setup	Check to enable the schedule.	
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.	
Start Time (hh:mm)	Specify the starting time of the schedule.	
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.	
Action	<ul> <li>Specify which action Call Schedule should apply during the period of the schedule.</li> <li>Force On -Force the connection to be always on.</li> <li>Force Down -Force the connection to be always down.</li> <li>Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field.</li> <li>Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.</li> </ul>	
Idle Timeout	Specify the duration (or period) for the schedule. <b>How often -</b> Specify how often the schedule will be applied <b>Once -</b> The schedule will be applied just once <b>Weekdays -</b> Specify which days in one week should perform the schedule.	
Б		

#### Example

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



Make sure the PPPoE connection and **Time Setup** is working properly. 1.

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

## 4.8.3 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	
RADIUS Setup	
🗹 Enable	
Server IP Add	ress
Destination Po	ort 1812
Shared Secret	t
Confirm Share	d 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.

## 4.8.4 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.



### **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.

- 1000	Broadband	🐮 IP Broadband Connection	on Router Status
Intervent Tasks     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create a new connection       Image: Create a new connection     Image: Create 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 Minipart (PPPOE)	General Internet Gateway Status:	Connected
0	Dial-up	Duration:	00:19:06
ee Also 🔹	test Disconnected DrayTek ISDN PPP	Speed:	100.0 Mbps
ther Places (*)	Internet Gateway	Activity Internet Internet Ga	teway My Computer
My Documents My Computer	LAN or High-Speed Internet	Sent: 404 Received: 1,115	
etails 🛞	Local Area Connection Enabled	Properties Disable	)
Network Connections	Realtek RTL8139/810x Family		

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>
Settings	Add Edit Delete

The reminder as regards concern about Firewall and UPnP

#### Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

#### **Security Considerations**

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

## 4.8.5 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.

Applications >> IGMP						
IGMP						
Enable IGMP I	Proxy WAN1 🗸					
	to act as a multicast prop y multicast group. But thi					
Enable IGMP	Snooping					
	Snooping, multicast traffic snooping, multicast traffic					
		OK Can	cel			
					<u>Refresh</u>	
Working Multica	st Groups					
Index	Group ID	P1	P2	P3		

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.

If you check Enable IGMP Proxy, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.

### 4.8.6 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** 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

Note: Wake on L can wake up thr	AN cooperate with <u>Bind IP to MAC</u> function, only binded PCs ough IP.
Wake by:	MAC Address 💌
IP Address:	😵
MAC Address:	Wake Up!
Result	
	<u>^</u>

Wake by	choose Wake by MAC MAC address of the ho	you to wake up the binded IP. If you Address, you have to type the correct ost in MAC Address boxes. If you choose you have to choose the correct IP address.
	Wake by:	MAC Address MAC Address IP Address
IP Address	IP to MAC will be sho	ave been configured in <b>Firewall&gt;&gt;Bind</b> own in this drop down list. Choose the IP down list that you want to wake up.
MAC Address	Type any one of the M	AC address of the bound PCs.
Wake Up	Click this button to wa figure. The result will	ke up the selected IP. See the following be shown on the box.

```
Application >> Wake on LAN
```

Wake	on	LAN	

Wake by:	MAC Address 💌
IP Address:	😒
MAC Address:	Wake Up!
Result	

# **4.9 VPN and Remote Access**

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN and Remote Access.

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

# 4.9.1 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 Environment** LAN-to-LAN VPN Client Mode Selection: Route Mode 🔽 Please choose a LAN-to-LAN Profile: [Index] [Status] [Name] 🗸 Note: For a typical LAN-to-LAN tunnel, please select Route Mode. If the remote network is expecting only a single client or ip and is not configured to route the subnet and then select NAT mode. If in doubt then select Route Mode Cancel Next > LAN-to-LAN Client Mode Choose the client mode. Selection Route Mode/NAT Mode - If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.



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

Vigor2920 Series User's Guide



[Index] 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 22 22 24 25 26 27 28 29	[Status]	[Name] ??? ??? ??? ??? ??? ??? ??? ??? ??? ?	^
2	л У	222	
2	A	222	
3		222	
14 F	x	222	
5	x	222	
	x	222	
16	x	222	
8	X		
19	х		
110	х	777	
111	х	277	
12	х	222	
13	x	???	
14	X	???	
15	х	???	
16	х	???	
17	х	???	
18	х	???	
19	x	???	
20	x	???	
21	х	???	
22	х	???	
23	х	???	
24	х	???	
25	х	???	
26	x	???	_
27	x	???	
28	x x x x x x x x x x x x x x	???	
29	x	???	*

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>
PTT PTT IPSe L2TP L2TP	-

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:



#### 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)	draytek.com
Username	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0
	< Back Next > Finish Cancel

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

VPN and Remote Access >> VPN Client Wizard

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
🗌 Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔘 Digital Signature (X.509)	None 🗸
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), you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

ofile Name	VPN-1
PN Dial-Out Through	WAN1 First 🗸
] Always on	
erver IP/Host Name for VPN .g. draytek.com or 123.45.67.89)	
E Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔿 Digital Signature (X.509)	None 🗸
Sec Security Method	
💿 Medium (AH)	
🔿 High (ESP)	DES without Authentication 💌
ername	???
ssword	
mote Network IP	0.0.0.0
mote Network Mask	255.255.255.0

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

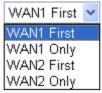
#### VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Must) Settings

Profile Name	???	
VPN Dial-Out Through	WAN1 First	
Always on		
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)		
IKE Authentication Method		
💿 Pre-Shared Key		
Confirm Pre-Shared Key		
🔘 Digital Signature (X.509)	None	
IPSec Security Method Medium (AH)		
🔘 High (ESP)	DES without Authentication 💉	
Username	???	
Password		
Remote Network IP	0.0.0.0	
Remote Network Mask	255.255.255.0	
	<pre>&lt; Back Next &gt; Finish Cancel</pre>	

# **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.



WAN1 First - While connecting, the router will use
WAN1 as the first channel for VPN connection. If WAN1
fails, the router will use another WAN interface instead.
WAN1 Only - While connecting, the router will use
WAN1 as the only channel for VPN connection.
WAN2 First - While connecting, the router will use
WAN2 as the first channel for VPN connection. If WAN2
fails, the router will use another WAN interface instead.
WAN2 as the first channel for VPN connection. If WAN2
fails, the router will use another WAN interface instead.
WAN2 Only - While connecting, the router will use
WAN2 as the only channel for VPN connection.

#### Check to enable router always keep VPN connection.

Pre-Shared KeyIKE Authentication Method usually applies to those are<br/>remote dial-in user or node (LAN to LAN) which uses<br/>dynamic IP address and IPSec-related VPN connections<br/>such as L2TP over IPSec and IPSec tunnel.<br/>Pre-Shared Key- Specify a key for IKE authentication<br/>Confirm Pre-Shared Key-Confirm the pre-shared key.

# **Digital Signature (X.509)** Click **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

**Always On** 

	<b>Certificate Management &gt;&gt; Local Certificate.</b> Otherwise, the setting you choose here will not be effective.
IPSec Security Method	<ul> <li>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is 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> </ul>
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

o to the VPN Connection Tanagement	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.			
	< Back Next > Finish Cancel			
	<ul> <li>View more detailed configurations.</li> </ul>			
	O Do another VPN Client Wizard setup.			
	⊙ Go to the VPN Connection Management.			
Click <b>Back</b> to modify changes if ne and proceed to the following actio	ecessary. Otherwise, click <b>Finish</b> to save the current settings on:			
Remote Network Mask: 255.255.255.0				
Remote Network IP:	192.168.1.6			
IPSec Security Method:	draytek.com Digital Signature (X.509) AH-SHA1			
IKE Authentication Method:				
Server IP/Host Name:				
Always on:	No			
VPN Connection Type: L2TP over IPSec (Must) VPN Connection Through: WAN1 First				
VPN Connection Type:	L2TP over IPSec (Must)			
Profile Name:	3 VPN-1			

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.

# 4.9.2 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	ierver Wizard	
Choose VPN Establishment Enviro	nment	
VPN Server Mode Selection:		Site to Site VPN (LAN-to-LAN)
Please choose a LAN-to-LAN P	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 S LAN-to- Site VPI Remote maintain be authe Site to Site to	the direction for the VPN server. Site VPN/Remote Dial-in User – To set a -LAN profile automatically, please choose Site to N. Dial-in User –You can manage remote access by hing a table of remote user profile, so that users can enticated to dial-in via VPN connection. Site VPN (LAN-to-LAN) Dial-in User (Teleworker)
Please choose a LAN-to-LAN Profile	(LAN-to	n is available when you choose <b>Site to Site VPN</b> o-LAN) as VPN server mode. There are 32 VPN 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] x	[Name] ??? ??? ??? ??? ??? ??? ??? ??? ??? ?	^
2	x	222	
3	X	222	
4	¥	222	
5	x x	222	
Ğ	x	222	
2	x	222	
8	x x	222	
9	x	222	
10	x x	222	
11	x	???	
12	x	???	
13	x x	???	
14	x	???	
15	x	???	
16	x	???	
17	x	???	
18	х	???	
19	x	???	
20	х	???	
21	x	???	
22	х	???	
23	x	???	
24	x x	???	
25	х	??? ??? ??? ???? ???? ???? ???????????	
26	х	???	
27	х	???	
28	X	???	-
29	X	???	$\mathbf{\mathbf{v}}$

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.

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

• 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

Profile Name	VPN-Ser1
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)	None
Peer IP/VPN Client IP	192.168.1.99
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0
	< Back Next > Finish Cancel

• When you check **PPTP/L2TP** (two types) or **PPTP** or **L2TP with Policy** (**None**), you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

Profile Name	VPN-Ser1	
PPTP / L2TP / L2TP over IPSec Authentic	ation	
Username	server1	
Password	•••••	
Peer IP/VPN Client IP		
Site to Site Information	-	
Remote Network IP	0.0.00	
Remote Network Mask	255.255.255.0	

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

#### VPN and Remote Access >> VPN Server Wizard

rofile Name	VPN-Ser1
PSec / L2TP over IPSec Authentication	
🗹 Pre-Shared Key	•••••
Confirm Pre-Shared Key	•••••
🗌 Digital Signature (X.509)	None 🗸
Peer IP/VPN Client IP	172.16.1.50
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

< Back

Next >

Cancel

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



#### VPN and Remote Access >> VPN Server Wizard

			a
Please	Confirm	Your	Settings

	<ul> <li>Do another VPN Server Wizard setup.</li> <li>View more detailed configurations.</li> <li>&lt; Back Next &gt; Finish Canc</li> </ul>
	-
	🔘 Do another VPN Server Wizard setup.
	O to the VPN Connection Management.
Click <b>Back</b> to modify changes and proceed to the following	if necessary. Otherwise, click <b>Finish</b> to save the current settings action:
Remote Network Mask:	255.255.255.0
Peer IP/VPN Client IP: Peer ID: Remote Network IP:	0.0.0.0
Allowed Service:	PPTP+IPSec
Username:	server1
	VPN-Ser1
Profile Name:	3
Index: Profile Name:	

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.

## 4.9.3 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.

PN and Remote Access >> Remote Access Control Setup			
emote Acces	s Control Setu	p	
	<b>~</b>	Enable PPTP VPN Service	
	<b>~</b>	Enable IPSec VPN Service	
	<b>~</b>	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.



# 4.9.4 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

VPN and	Remote	Access	>>	PPP	General	Setup
---------	--------	--------	----	-----	---------	-------

PPP/MP Protocol Dial-In PPP	IP Address Assignment for (When DHCP Disable set)	Dial-In Users
Authentication PAP or CHAP V	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE) Optional MPPE	✓	L
Mutual Authentication (PAP) 🛛 🔿 Yes 💿 No		
Username		
Password		

Dial-In PPP Authentication PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	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 Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Maximum MPPE(128 bit) 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.
Start IP Address	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.

# 4.9.5 IPSec General Setup

In IPSec General Setup, there are two major parts of configuration.

There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

IKE Authentication Method		
Pre-Shared Key	•••••	
Confirm Pre-Shared Key	•••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, I	out will not be encrypted.	
High (ESP) 🛛 🗹 DES	🗹 3DES 🛛 🗹 AES	
Data will be encrypted a	and authentic.	

0K

VPN and Remote Access >> IPSec General Setup

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

Cancel



<b>IPSec Security Method</b>	<ul> <li>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is 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> </ul>
	Triple DES (3DES), and AES.

# 4.9.6 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.

La da se	Nama	C	In days	News	Ctature
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
16.	???	х	32.	???	x

		-			_	
VPN and	l Remote	Access	>>	IPSec	Peer	Identity

Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to acce

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			
Occept Subject Alternative Name			
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		
Profile Name	Type in .		
Accept Any Peer ID	Click to accept any peer regardless of its identity.		
Accept Subject Alternative Name	<ul> <li>Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address, Domain, or E-mail Address. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.</li> </ul>		
Accept Subject Name	Click to check the specific fields of digital signature to acce the peer with matching value. The field includes <b>Country</b> ( <b>State</b> (ST), <b>Location</b> (L), <b>Organization</b> (O), <b>Organization</b> <b>Unit</b> (OU), <b>Common Name</b> (CN), and <b>Email</b> (E).		

# 4.9.7 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.

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 ??? 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.

User account and Authentication	Username ???	
Enable this account	Password	
(dle Timeout 300 second(s)		
	IKE Authentication Method	
Allowed Dial-In Type	🕑 Pre-Shared Key	
PPTP	IKE Pre-Shared Key	
🗹 IPSec Tunnel	Digital Signature(X.509)	
🗹 L2TP with IPSec Policy None 💌	None 💌	
Specify Remote Node		
Remote Client IP or Peer ISDN Number	IPSec Security Method	
	Medium(AH)	
pr Peer ID	High(ESP) 🗹 DES 🗹 3DES 🗹 AES	
Netbios Naming Packet 💿 Pass 🔘 Block	Local ID (optional)	

Enable this account	Check the box to enable this function. <b>Idle Timeout-</b> If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
РРТР	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below
IPSec Tunnel	Allow the remote dial-in user to make an IPSec VPN connection through Internet.
L2TP	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.
Specify Remote Node	Check the checkbox-You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). Uncheck the checkbox-This means the connection type you select above will apply the authentication methods and security methods in the general settings.
Netbios Naming Packet	<b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can

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

# 4.9.8 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 2 VPN tunnels simultaneously and provides up to **32** profiles. The following figure shows the summary table.

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>	???	x
<u>7.</u>	???	Х	<u>23.</u>	???	x
<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>	???	x	<u>32.</u>	???	x

VPN and Remote Access >> LAN to LAN

Set to Factory Default

Click to clear all indexes.

Name

Status

Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.

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

**Profile Name** 

1. Common Settings		
Profile Name     ???       Enable this profile       VPN Dial-Out Through     WAN1 First ▼       Netbios Naming Packet     ● Pass     ● Block	Call Direction <ul> <li>Both</li> <li>Dial-Out</li> <li>Dial-in</li> <li>Always on</li> </ul> Idle Timeout <ul> <li>300</li> <li>second(s)</li> </ul> Enable PING to keep alive PING to the IP	
2. Dial-Out Settings		
Type of Server I am calling <ul> <li>PPTP</li> <li>IPSec Tunnel</li> <li>L2TP with IPSec Policy None</li> </ul>	Username ??? Password PAP/CHAP V VJ Compression Off	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication Method            • Pre-Shared Key          IKE 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:         ,         ,	

Specify a name for the profile of the LAN-to-LAN connection.

**Enable this profile** Check here to activate this profile.

**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.

WAN1	First	*
WAN1	First	
WAN1		
WAN2	First	
WAN2		

**WAN1 First** - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.

**WAN1 Only** - While connecting, the router will use WAN1 as the only channel for VPN connection.

**WAN2 First** - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead.

**WAN2 Only** - While connecting, the router will use WAN2 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.	
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. <b>Both</b> :-initiator/responder <b>Dial-Out</b> - initiator only <b>Dial-In</b> - responder only.	
Always On or Idle Timeout	<ul><li>Always On-Check to enable router always keep VPN connection.</li><li>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</li></ul>	
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).	
РРТР	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.	
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.	
L2TP with	<ul> <li>Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:</li> <li>None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</li> <li>Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.</li> <li>Must: Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul>	
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. <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	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.			
Medium	Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.			
Advanced	<ul> <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 apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and not apply any 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 algorithm.</li> <li>AES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> </ul>			
	The window of advance setup is shown as below:			
	(g) http://192.108.1.14bod/278-PU.htm			
	IKE advanced settings IKE phase 1 mode ○ Main mode ○ Aggressive mode IKE phase 2 proposal DES_MO5_G1 VE phase 2 proposal IKE phase 2 key lifetime 2000 (000 ~ 86400) IKE phase 2 key lifetime 3000 (000 ~ 86400) Ferfect Forward Secret ① Disable ○ Enable Local ID			
	OK Close			

**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 Po	licy None 💌	VJ Compression	💿 On 🔘 Off
Specify Remote VPN Gateway Peer VPN Server IP 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)	3DES 🗹 AES
4. TCP/IP Network Setting	s		
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		Rodie .
	More	Change default route single WAN supports this	e to this VPN tunnel ( Only ; )
OKClearCancelAllowed Dial-In TypeDetermine the dial-in connection with different types.			

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.

# **Dray** Tek

РРТР

IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	<ul> <li>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:</li> <li>None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</li> <li>Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.</li> <li>Must - Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul>
Specify Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
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</b> <b>Identity</b> .
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. <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.
My WAN IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0,



Remote Gateway IP	which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
<b>RIP Direction</b>	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose <b>NAT</b> , otherwise choose <b>Route</b> .
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel.

# **4.9.9 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	۰. GO >>
VPN Type Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
<u>.</u>					ata is encr ata isn't er	(1)
Dial	Click this	button to	execute	dial out f	unction.	
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.					
Refresh	Click this button to refresh the whole connection status.					

# 4.10 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.



# 4.10.1 Local Certificate

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local			View Delete
GENERATE X509 Local Cert	IMPORT REFRESH		
			~

Generate

Click this button to open Generate Certificate Request window.

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 V
Key Size	1024 Bit 😒

Generate

Type in all the information that the window requests. Then click **Generate** again.

Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.

Certificate Management >> Local Certificate

After clicking **Generate**, the generated information will be displayed on the window below:

Name Subject Sta		Modify
ocal /C=TW/O=Draytek/OU=RD/emailA	Requesting	View Delete
GENERATE IMPORT REFRESH		
X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBsjCCARsCAQAwUDELMAKGA1UEBhMCVFcxEDAO BgNVBASTA1JEMSIwIAYJKoZIhvcNAQkBFhNzZXJ2 MAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPioah blo1kt9cTdLUDaFk6s8d3wDeQytoV1LBJz2IDF0x /rGhuVTKd9j6PlcrnkP7du84t23tWBdMD4W5c8Vm RZjkRMaHEWpVpwIDAQABoCIwIAYJKoZIhvcNAQkO qAEqMAOGCSqGSIb3DQEBBQUAA4GBAB43O4N9nod8 ikisNdZUoUEnKcejeOndc+H83VDA23ACEJpzTPFx GgeJ9trVYgeZvbCrSjRU1PN1Hccfo7ANJ/M/D1EP	aWN1QGRyYX10Z u/gFQaYB1ce5OJ jX6ip7ev187tw SyDjShLhjdxVYJ MRMwETAPBgNVHJ rIudBAfTt91ts( qklbeZo7a+wE5'	WsuY29tMIGf ERSDfWknIdH øTsg4lgZ6Qk PWpNKVIrOT2 ≡ REECDAGhwTA b/tYNb2kfEZ 7/+0VhNagBa

#### Certificate Management >> Local Certificate

### X509 Local Certificate Configuration

# 4.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate	Management	>> Trusted	CA	Certificate
-------------	------------	------------	----	-------------

#### X509 Trusted CA Certificate Configuration

	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.

🏉 Certifi	icate Information - Windows Intern	net Explorer	
🥭 http://1	92.168.1.1/doc/XCaCfVi1.htm		*
			^
	Certifi	cate Detail Information	
(	Certificate Name:	Trusted CA-1	
1	Issuer:		
5	Subject:		
9	Subject Alternative Name:		
1	Valid From:		
· ا	Valid To:		
		Close	~
ē			

# 4.10.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup			
Certificate Backup / Restoration			
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.		

# 4.11 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.

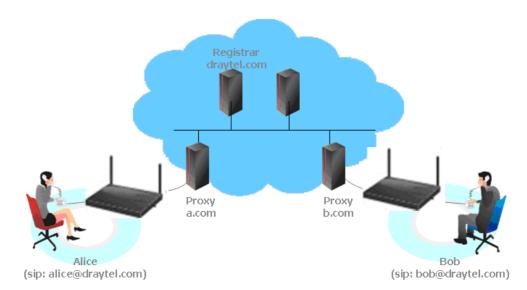
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ $\mu$ -law, G.723, G.726 and G.729 A & B. Each codec uses a 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.



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.



# 4.11.1 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
	<u>Regional</u>
	PSTN Setup
Secure Phone configuration	✓ Enable Secure Phone (ZRTP+SRTP)
	✓ Enable SAS Voice Prompt
	OK
nable Secure Phone	It allows users to have encrypted RTP stream with the peer sinusing the same protocol (ZRTP+SRTP). Check this box to have

**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.

secure call.

# **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:

- 4. 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.
- 5. Then the RTP traffic is secured until the call ends.
- 6. 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:

- 3. 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.
- 4. Even no voice prompt, but the RTP traffic is still secured until the call ends.

**Note:** If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

# Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries



in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2820V for setting the phone book.

```
VoIP >> DialPlan Setup
```

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
<u>1.</u>				Default	None		х
<u>2.</u>				Default	None		х
<u>3.</u>				Default	None		х
<u>4.</u>				Default	None		х
<u>5.</u>				Default	None		х
<u>6.</u>				Default	None		×
<u>19.</u>				Default	None		×
<u>20.</u>				Default	None		х
< <u>1-20</u>	<u>)   21-40   41-6</u>	0 >>					Next >

VoIP >> DialPlan Setup

Click any index number to display the dial plan setup page.

Phone Book Ind	IEX NO. 1						
	Phone Number	1					
	Display Name	Poll	y	$\overline{}$			
	SIP URL	111:	2	@ fwd.pulver.com			
	Dial Out Account	Def	Default 💌				
	Loop through	Nor	ne 💌				
	Backup Phone Nu	mber		]			
hable		Click this to	enable this e	ntry.			
Cnable		Click this to	enable this e	ntry.			
		-	peed-dial number of this index. This can be any numbe noose, using digits <b>0-9</b> and *.				
Display Name	:	The Caller-ID that you want to be displayed on your fr screen. This let your friend can easily know who's call without memorizing lots of SIP URL Address.					
IP URL		Enter your friend's SIP Address.					
Dial Out Acco	Choose one of the SIP accounts for this profile useful for both sides (caller and callee) that reg different SIP Registrar servers. If caller and ca the same SIP server, sometimes, the VoIP phot connection may not succeed. By using the spec account, the successful connection can be assu			er and callee) that registered to rvers. If caller and callee do not use etimes, the VoIP phone call eed. By using the specified dial out			

Loop through

Choose PSTN to enable loop through function.



**Backup Phone Number** When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number/ISDN number) for this VoIP phone setting.

## **Digit Map**

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

#	Enable Prefix Number		Mode		OP Number	Min Len	Max Len	Route	
1	<ul><li>✓</li></ul>	03	Replace	e 🗸	8863	7	9	PSTN 🔽	
2	<b>~</b>	886	Strip	*	886	8	10	PSTN 🔽	
3			None	~		0	0	PSTN 🔽	
4			None	~		0	0	PSTN 🔽	
5			None	~		0	0	PSTN 🔽	
6			None	~		0	0	PSTN 🗸	
16			None	Y		0	0	PSTN M	
17			None	~		0	0	PSTN 🔽	
18			None	$\sim$		0	0	PSTN 🔽	
.9			None	$\sim$		0	0	PSTN 🔽	
20			None	~		0	0	PSTN 🗸	

VoIP >> DialPlan Setup

Note: Min Len and Max Len should be between 0~25.

OK	Cancel

Enable	Check this box to invoke this setting.				
Prefix Number	The phone number set here is used to add, strip, or replace the OP number.				
Mode	<b>None</b> - 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.				



Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886.
Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "8863111111" and sent to SIP server.

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.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in <b>VoIP&gt;&gt; Phone Settings</b> .

### **Call Barring**

Call barring is used to block phone calls coming from the one that is not welcomed.

### VoIP >> DialPlan Setup

Call Barrin	ig Setup		<u>S</u>	et to Factor	<u>y Default</u>
Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Status
<u>1.</u>					x
<u>2.</u>					×
<u>3.</u>					×
<u>4.</u>					×
<u>5.</u>					х
<u>6.</u>					х
<u>7.</u>					х
<u>8.</u>					×
<u>9.</u>					х
<u>10.</u>					×
<< <u>1-10</u>   ]	<u>11-20</u> >>				<u>Next</u> >>

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u>

VoIP >> DialPlan Setup

Click any index number to display the dial plan setup page.

Call Barring Index No. 1	
🗹 Enable	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Route	All 💌
Index(1-15) in	Schedule Setup,,,,
	OK Cancel
Enable	Click this to enable this entry.
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number
Specific URI/URL or	This field will be changed based on the type you selected for

Specific Number	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 Schedule</b> for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.

VoIP >> Dia	IPIan Setup	
Call Barrin	g Block Anonymous	
🗹 Enable		
	Route	Phone1 Phone2
	Index(1-15) in <u>Schedule</u> Setup	
Note:Block	the incoming calls which do not have t	he caller ID.
	ОК	Cancel

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

VoIP >> Dia	hIPIan Setup	
Call Barrir	ıg Block Unknown Domain	
🗹 Enable	9	
	Route	Phone1 Phone2
	Index(1-15) in <u>Schedule</u> Setup	
Note:If the be blocked	2	t from the domain found in SIP accounts,the call should
	OK	Cancel

For **Block IP Address** – this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup	
Call Barring Block IP Address	
🗹 Enable	
Route	🗌 Phone1 🔲 Phone2
Index(1-15) in <u>Schedule</u> Setup	, , , , , , , , , , , , , , , , , , ,
Note: The incoming calls by means of IP dialing	(e.g.#192*168*1*1#) should be blocked.

ΟK

### Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

Cancel

#### VoIP >> DialPlan Setup 🗹 Enable Regional Set to Factory Default *69 Last Call Return [Miss]: *12 *14 Last Call Return [In]: Last Call Return [Out]: *72 *73 Call Forward [All] [Act]: +number+# Call Forward [Deact]: +# Call Forward [Busy] [Act]: *90 +number+# Call Forward [No Ans] [Act]: *92 +number+# *78 *79 Do Not Disturb [Act]: Do Not Disturb [Deact]: +# +# Hide caller ID [Act]: *67 Hide caller ID [Deact]: +# *68 +# Call Waiting [Act]: *56 +# Call Waiting [Deact]: *57 +# *77 Block Anonymous [Act]: Block Anonymous [Deact]: *87 +# +# Block Unknow Domain Block Unknow Domain [Act]: *40 +# *04 +# [Deact]: *50 Block IP Calls [Deact]: *05 Block IP Calls [Act]: +# +# Block Last Calls [Act]: *60 +# ΟK 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 filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

## **PSTN Setup**

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**.

VolP	>>	PST	NS	etuj	p
------	----	-----	----	------	---

Enab	ole	phone number for PSTN relay
	l	
	l	

Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

# 4.11.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy**, and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name** 

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Note: Selection items for **Ring Port** will differ according to the router you have.

SIP Acco	unts List					(	Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring	g Port	Status
1					Phone 1	Phone2	-
2					Phone1	Phone2	-
<u>3</u>					Phone1	Phone2	-
4					Phone1	Phone2	-
<u>5</u>					Phone1	Phone2	-
<u>6</u>					Phone1	Phone2	-
Z					Phone1	Phone2	-
<u>8</u>					Phone1	Phone2	-
<u>9</u>					Phone1	Phone2	-
<u>10</u>					Phone1	Phone2	-
<u>11</u>					Phone1	Phone2	-
<u>12</u>					Phone1	Phone2	-

### VoIP >> SIP Accounts

R: success registered on SIP server -: fail to register on SIP server

### NAT Traversal Setting

STUN Server:			
External IP:			]
SIP PING Interval:	150	sec	

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 @.
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. $\mathbf{R}$ 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.

### VoIP >> SIP Accounts

Profile Name	(11 char ma	іх.)
Register via	None 🔽 🔲 Call without Reg	jistration
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
📃 Act as outbound pro	xy	
Display Name	(23 char ma	эх.)
Account Number/Name		(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 💌 3600 sec	
NAT Traversal Support	None 💌	
Ring Port	Phone 1 Phone 2	
Ring Pattern	1 💌	

**Profile Name** 

**Register via** 

Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.

If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **Call without Registration**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call.

None	*	
None		
Auto		
WAN1		
WAN2		F
LANAVPN		L

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
	<ul> <li>None – Disable this function.</li> <li>Stun – Choose this option if there is Stun server provided for your router.</li> <li>Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.</li> <li>Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.</li> </ul>
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern  1 2 3 4 5 6

# 4.11.3 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	>>	Ph	one	Sett	inas
				~ ~ ~ ~ ~	

Phone List Refresh Seconds: 30 V 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 V 10100000

Phone List	<ul> <li>Port – there are two phone ports provided here for you to configure. Phone1/Phone2 allow you to set general settings for PSTN phones.</li> <li>Call Feature – A brief description for call feature will be shown in this field for your reference.</li> <li>Codec – The default Codec setting for each port will be shown in this field to change it for each phone port.</li> <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> <li>Default SIP Account – "draytel_1" is the default SIP account. You can click the number below the Index field to change of Phone Index.</li> <li>DTMF Relay – Display DTMF mode that configured in the advanced in the advanced settings page of Phone Index.</li> </ul>
RTP	<ul> <li>Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.</li> <li>Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050.</li> <li>Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000.</li> <li>RTP TOS – It decides the level of VoIP package. Use the drop</li> </ul>



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 💌

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		Codecs				
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽			
Session Timer	90 sec		🔲 Single Codec			
 Call Forwarding	Disable 🗸	Packet Size	20ms 💌			
SIP URL		Voice Active Detector	Off 🛩			
Time Out	30 sec					
DND(Do Not Disturb)	500	Default SIP Account	<b>*</b>			
	mode <u>ne Book</u> as Exception List:	Play dial tone only	when account registered			
CLIR (hide caller ID)						
Call Transfer						
lotline		to enable it. Type in	the SIP URL in the field f			
		tically when you pic				
ession Timer		field, if there is no re	n. In the limited time that sponse, the connecting cal			
Call Forwarding	forwarding fun be forwarded i the incoming c the local system	action. Always means nto SIP URL without alls will be forwarde n is busy. No Answe ceive any response, th	noose. <b>Disable</b> is to close of s all the incoming calls wi t any reason. <b>Busy</b> means d into SIP URL only when er means if the incoming ney will be forwarded to the			
	abc@iptel.org)	as the site for call for et the time out for the	e.g., aaa@draytel.org or orwarded. e call forwarding. The			

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 (1-60) 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 ca phone set.	ller ID on the display panel of the		
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.			
Prefer Codec	Select one of five codecs as the default for your VoIP call codec used for each call will be negotiated with the peer p before each session, and so may not be your default choic default codec is G.729A/B; it occupies little bandwidth w maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 It is better for you to have at least 256Kbps upstream if yo would like to use G.711.			
	Prefer Codec	G.711A (64Kbps) G.711MU (64Kbps)		

G.711A (64Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps)

**Single Codec** – If the box is checked, only the selected Codec will be applied.

**Packet Size**-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size

20ms	*
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

**Voice Active Detector -** This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



**Default SIP Account** 

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

**Play dial tone only when account registered -** Check this box to invoke the function.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Settin	igs						
Region I	User Defined	*		Ca	ller ID Type	FSK_ETSI	*
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
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 Type (RFC2833) (96 - 127)			
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.

	ione Settings	
	Region User Define	d 💌
	User Define	ow
		(H
	Dia Denmark	ю
	Ringi Italy	0
	Germany Bus Netherlands	ю
	Conges Curadan	
	Sweden	
	Volume GAustralia Slovenia	
	Mic Gain(Czech	
	Speaker (Slovakia	
	Hungary MISC Switzerland	
	Dial Tone France	सर्ग - 50
		h field for your necessity. It is use the default settings for VoIP
Volume Gain	Mic Gain (1-10)/Speake	<b>r Gain (1-10)</b> - Adjust the volume of
		by entering number from 1- 10. The
	larger of the number, the	louder the volume is.
MISC	loudness of the dial tone.	• This setting is used to adjust the The smaller the number is, the louder nmended for you to use the default
	setting. <b>Ring Frequency</b> - This s	etting is used to drive the frequency of nended for you to use the default
DTMF	setting. <b>Ring Frequency</b> - This so the ring tone. It is recommon setting.	
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommon setting. <b>DTMF Mode</b> – There are <i>InBand</i> - Choose this one	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommon setting. <b>DTMF Mode</b> – There are <i>InBand</i> - Choose this one tone as audio directly who	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommon setting. <b>DTMF Mode</b> – There are <i>InBand</i> - Choose this one tone as audio directly whe <i>OutBand</i> - Choose this one	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations for the recommendation of the recommenda	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommenda	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the led and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommenda	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations for the ring tone. It is recommendation of the ring tone. It is recommendation of the recommendation of th	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommenda	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the it into SIP form. Then it will be sent to
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommendation of the remote setting. <b>DTMF Mode</b> – There are <b>InBand</b> - Choose this one to the setting of the digital for the setting of the setting to the digital for useful when the network of the remote remain the accuracy of <b>SIP INFO</b> - Choose this of DTMF tone and transfer if the remote end with SIP remote setting to the set of the remote end with SIP remote setting to the set of the remote set of the remote setting to the set of the remote set of the remote set of the se	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the it into SIP form. Then it will be sent to message.
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommenda	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the it into SIP form. Then it will be sent to message.
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommendation of the remote setting. <b>DTMF Mode</b> – There are <b>InBand</b> - Choose this one to the setting of the digital for the setting of the setting to the digital for useful when the network of the remote remain the accuracy of <b>SIP INFO</b> - Choose this of DTMF tone and transfer if the remote end with SIP remote setting to the set of the remote end with SIP remote setting to the set of the remote set of the remote setting to the set of the remote set of the remote set of the se	nended for you to use the default e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the it into SIP form. Then it will be sent to message.
DTMF	setting. <b>Ring Frequency</b> - This setting tone. It is recommendations and the recommendation of the recommendation of the remote setting. <b>DTMF Mode</b> – There are <b>InBand</b> - Choose this one to the setting of the digital for the setting of the setting to the digital for useful when the network of the remote remain the accuracy of <b>SIP INFO</b> - Choose this of DTMF tone and transfer if the remote end with SIP remote setting to the set of the remote end with SIP remote setting to the set of the remote set of the remote setting to the set of the remote set of the remote set of the se	e four DTMF modes for you to choose. e then the Vigor will send the DTMF en you press the keypad on the phone ne then the Vigor will capture the ed and transform it to digital form e; the receiver will generate the tone orm it receive. This function is very traffic congestion occurs and it still of DTMF tone. one then the Vigor will capture the it into SIP form. Then it will be sent to nessage.

**Payload Type (rfc2833)** - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

# 4.11.4 Status

From this page, you can find codec, connection and other important call status for each port.

VolP	>>	Status	
		otutuo	

Status								Refres	n Seco	nds:	10 🚩	Refresh
Port	Status	Codec I	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out 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		Time		Duration	I	n/Out	/Miss	Acc	ount	ID	Peer	ID
(mm-dd-y	уууу)	(hh:mm	:ss)	(hh:mm:s	з)							
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	-			-				
00-00-	0	00:00:0	00	00:00:00	_			_				

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

<b>Refresh Seconds</b>	Specify the interval of refresh time to obtain the latest VoIP
	calling information. The information will update immediately
	when the Refresh button is clicked.

Refresh Seconds : 10 ¥ 5 10 30

	30
Port	It shows current connection status for Phone(s) and ISDN ports.
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.

# 4.12 Wireless LAN

This function is used for "n" models only.

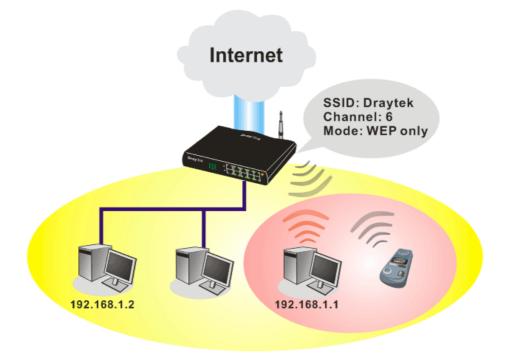
### 4.12.1 Basic Concepts

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
₽	Security
₽	Access Control
₽	WPS
- Þ	WDS
⊳	Advanced Setting
⊳	WMM Configuration
⊳	AP Discovery
⊳	Station List

## 4.12.2 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

ble Wireless	LAN		
Mode :		Mixed(11b+11g	+11n) 🔽
ndex(1-15)	in <u>Schedule</u> Se	tup:,	,,
	le profiles that h s are ignored.	nave the action "Force Down"	are applied to the WLAN, all
Enable H	Hide SSID	SSID	Isolate LAN Member
1		DrayTek	
2			
3			
4			
Isolate Meml other. Isolate LAN:\ LAN.	ber:Wireless clie	m being scanned. nts (stations) with the same s (stations) with the same SSID : Long Preamble	cannot access wired PCs on
Isolate Memi other. Isolate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVEF T X Burst	ber:Wireless clien Wireless clients annel 6, 2437MHz le: necessary fo	nts (stations) with the same s (stations) with the same SSID	cannot access wired PCs on
solate Meml other. Isolate LAN:V AN. Channel: Ch .ong Preamb Packet-OVER T X Burst lote:	Wireless clients Mineless clients annel 6, 2437MHz le: necessary fo	nts (stations) with the same s (stations) with the same SSID : Long Preamble	cannot access wired PCs on : poly(lower performance)
Isolate Memi other. Isolate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVEF T X Burst Note:	ber:Wireless clients Wireless clients annel 6, 2437MHz le: necessary fo RDRIVE [™] chnology must a	nts (stations) with the same s (stations) with the same SSID Long Preamble or some old 802.11 b devices of also be supported in clients to	cannot access wired PCs on :  Donly(lower performance) boost WLAN performance.
solate Meml other. solate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVER Tx Burst Jote: The same te Rate Control	ber:Wireless clients Wireless clients annel 6, 2437MHz le: necessary fo RDRIVE [™] chnology must a Enable	Ints (stations) with the same s (stations) with the same SSID Long Preamble or some old 802.11 b devices of also be supported in clients to Upload	boost WLAN performance.
Isolate Meml other. Isolate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVEF Tx Burst Iote: The same te Rate Control SSID 1	Der:Wireless clients Wireless clients annel 6, 2437MHz le: necessary fo RDRIVE TM chnology must a Enable	Ints (stations) with the same s (stations) with the same SSID Long Preamble or some old 802.11 b devices of also be supported in clients to Upload 30000 kbps	boost WLAN performance.
Isolate Meml other. Isolate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVEF Tx Burst Note: The same te Rate Control SSID 1 SSID 2	ber:Wireless clients Wireless clients annel 6, 2437MHz le: necessary fo RDRIVE [™] chnology must a Enable	nts (stations) with the same s (stations) with the same SSID . V Long Preamble or some old 802.11 b devices of also be supported in clients to Upload 30000 kbps 30000 kbps	boost WLAN performance.
Isolate Meml other. Isolate LAN:\ LAN. Channel: Ch .ong Preamb Packet-OVEF Tx Burst Iote: The same te Rate Control SSID 1	Der:Wireless clients Wireless clients annel 6, 2437MHz le: necessary fo RDRIVE TM chnology must a Enable	Ints (stations) with the same s (stations) with the same SSID Long Preamble or some old 802.11 b devices of also be supported in clients to Upload 30000 kbps	boost WLAN performance.

Enable Wireless LAN

Check the box to enable wireless function.

Mode	At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11b+11g) Mixed(11b+11g) Mixed(11b+11g+11n) Note: You should also set <b>RADIUS Server</b> simultaneously if 11g Only, 11b Only or 11n Only mode is selected.
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	<ul> <li>LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.</li> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> </ul>
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

Long PreambleThis option is to define the length of the sync field in an<br/>802.11 packet. Most modern wireless network uses short<br/>preamble with 56 bit sync field instead of long preamble<br/>with 128 bit sync field. However, some original 11b<br/>wireless network devices only support long preamble.<br/>Check it to use Long Preamble if needed to communicate<br/>with this kind of devices.

# Packet-OVERDRIVEThis feature can enhance the performance in data<br/>transmission about 40%* more (by checking **Tx Burst**). It<br/>is active only when both sides of Access Point and Station<br/>(in wireless client) invoke this function at the same time.<br/>That is, the wireless client must support this feature and<br/>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**).

vigor not suz.iin wheless use Adapter Uthity			
Auto Holz, I.H. Wheless OSB Adapter Only       Configuration       Status       Option       Auto launch when Windows start up       Remember mini status gosition       Auto hide mini status       Set mini status always on top       Enable IP Setting and Proxy Setting in Profile       Group Roaming       Ad-hoc	Advance Setting Disable Redio Fragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Power Save Mode: Tx Burst :	Disable	47
WLAN type to connect  Infrastructure and Ad-loc getwork Infrastructure network only Ad-loc network only Ad-toc network only Automatically connect to non-preferred networks	Tx Burst :		♥ 
Tx Burst : Disab Disab Brad	ole	*	
131000	200		

	<b>Note:</b> * means the real transmission rate depends on the environment of the network.
Rate Control	It controls the data transmission rate through wireless connection.
	<b>Upload</b> – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps. <b>Download</b> – Type the transmitting rate for data download. Default value is 30,000 kbps.

### 4.12.3 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.

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

SSID 1	SSID 2	SSID 3	SSID 4
	Mode:		Disable 💌
WPA:	:		
	Pre-Shared Key(I	PSK):	*****
	Type 8~63 ASCI "cfgs01a2" or "		r 64 Hexadecimal digits leading by "Ox", for example .".
WEP:			
	Encryption Mode	:	64-Bit 💙
	⊙Key 1 :		*****
	○Key 2 :		*****
	○Кеу 3 :		****
	OKey 4 :	10	
Type "0x41 <b>For 1</b> : Type	4 bit WEP key 5 ASCII character 142333132". 28 bit WEP key 13 ASCII characte	er or 26 Hexad	ecimal digits leading by "Ox", for example "AB312" or decimal digits leading by "Ox", for example 3536373839414243".
Type "0x41 <b>For 1</b> : Type	4 bit WEP key 5 ASCII character 142333132". 28 bit WEP key 13 ASCII characte	er or 26 Hexad <30313233343	ecimal digits leading by "Ox", for example "AB312" or decimal digits leading by "Ox", for example
Type "0x41 <b>For 1</b> : Type	4 bit WEP key 5 ASCII character 142333132". 28 bit WEP key 13 ASCII characte	er or 26 Hexad <30313233343	ecimal digits leading by "Ox", for example "AB312" or decimal digits leading by "Ox", for example 3536373839414243". OK Cancel
Type "0x41 <b>For 1</b> : Type "0123	4 bit WEP key 5 ASCII character 142333132". 28 bit WEP key 13 ASCII characte	er or 26 Hexad <30313233343	ecimal digits leading by "0x", for example "AB312" or decimal digits leading by "0x", for example 3536373839414243". OK Cancel re are several modes provided for you to choose.



	encryption key should be entered <b>Mixed (WPA+ WPA2)/PSK -</b> clients simultaneously and the entered in PSK.	Accepts WPA and WPA2
WPA	The WPA encrypts each frame using the key, which either PSI manually in this field below or via 802.1x authentication. Eithe such as 012345678(or 64 Hexa such as "0x321253abcde"). <b>Type</b> - Select from Mixed (WF <b>Pre-Shared Key (PSK)</b> - Eithe such as 012345678(or 64 Hex 0x, such as "0x321253abcde")	K (Pre-Shared Key) entered automatically negotiated er <b>8~63</b> ASCII characters, decimal digits leading by 0x, PA+WPA2) or WPA2 only. er <b>8~63</b> ASCII characters, adecimal digits leading by
WEP	<ul> <li>64-Bit - For 64 bits WEP key, or such as 12345 (or 10 hexadecir such as 0x4142434445.)</li> <li>128-Bit - For 128 bits WEP key characters, such as ABCDEFG hexadecimal digits leading by 0 0x4142434445464748494A4B</li> </ul>	nal digitals leading by 0x, y, either <b>13</b> ASCII HIJKLM (or 26 Dx, such as
	Encryption Mode:	64-Bit 64-Bit 128-Bit
	All wireless devices must supp encryption bit size and have the be entered here, but only one key The keys can be entered in ASC	ort the same WEP e same key. <b>Four keys</b> can ey can be selected at a time.

### 4.12.4 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.

the key you wish to use.

### Wireless LAN >> Access Control

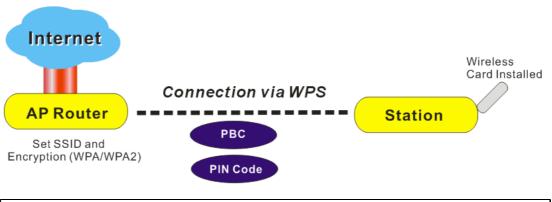
### Access Control

Enable Mac Address Filter
SSID 1 SSID 2 SSID 3 SSID 4
MAC Address Filter
Index Attribute MAC Address
Client's MAC Address : : : : : : : : : : : : : : : : : :
Attribute :
s: Isolate the station from LAN
Add Delete Edit Cancel
OK Clear All
OK Clear All

Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
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.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

## 4.12.5 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.

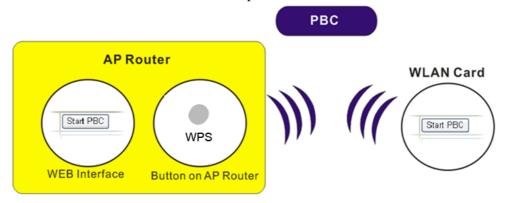


Note: Such function is available for the wireless station with WPS supported.

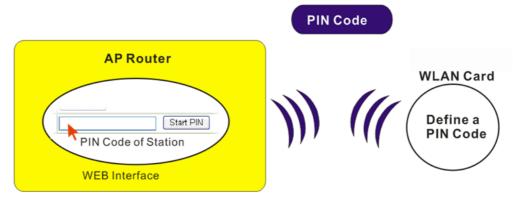
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for 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 2920 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



• If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.

Microsof	ft Internet Explorer 🛛 🔀
♪	WPS only supports in WPA/WPA2-PSK Mode.
	OK

Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Below shows Wireless LAN>>WPS web page.

```
Wireless LAN >> WPS (Wi-Fi Protected Setup)
```

Enable WPS 🗘

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

### **Device Configure**

Configure via Push Button	Start PBC	
Configure via Client PinCode	Start PIN	

Status: The Authentication Mode is NOT WPA/WPA2 PSK !!

Note: WPS can help your wireless client automatically connect to the Access point.

: WPS is Disabled.

WPS is Enabled.

♀: Waiting for WPS requests from wireless clients.

Enable WPSCheck this box to enable WPS setting.WPS StatusDisplay related system information for WPS. If the<br/>wireless security (encryption) function of the router is<br/>properly configured, you can see 'Configured' message<br/>here.



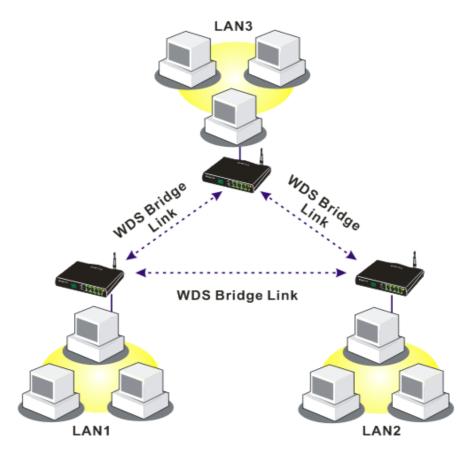
SSID Authentication Mode	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication would	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The 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)

### 4.12.6 WDS

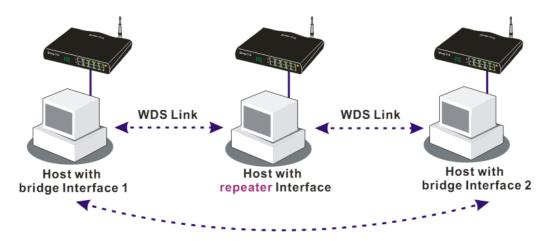
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

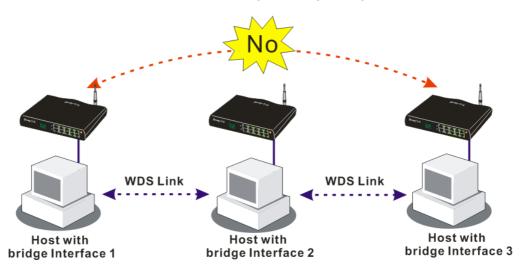


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

### Wireless LAN >> WDS Settings

WDS Settings		Set to Factory Default
		Bridge
Mode: Disable	• •	Enable Peer MAC Address
Security:		
	Pre-shared Key	
WEP:		
Use the same WEP key	set in <u>Security</u>	Note: Disable unused links to get better
<u>Settings</u>		performance.
		Repeater
Pre-shared Key:		Enable Peer MAC Addess
Туре : ТКІР		
Кеу :		
Type 8~63 ASCII character	rs or 64 bevadecimal	
digits leading by "Ox", for ex	ample "cfgs01a2" or	
"0x655abcd".		
		Access Point Function:
		Enable     Disable
		Status:
		Send "Hello" message to peers.
		Link Status
		Note: The status is valid only when the peer also
		supports this function.
		·
	ОК	Cancel
Mode	Choose the	e mode for WDS setting. <b>Disable</b> mode will not
vioue		WDS setting. <b>Bridge</b> mode is designed to fulfill the
	•	f application. <b>Repeater</b> mode is for the second one.
		application. Repeater mode is for the second one.
	Disable	×
	Disable	
	Bridge	
	Repeater	
Security	There are t	hree types for security, <b>Disable</b> , <b>WEP</b> and
		<b>d key</b> . The setting you choose here will make the
		WEP or Pre-shared key field valid or not. Choose one
		s for the router.
WEP		box to use the same key set in <b>Security Settings</b>
		u did not set any key in <b>Security Settings</b> page, this
	check box	will be dimmed.
Pre-shared Key	Type 8 ~ 6	3 ASCII characters or 64 hexadecimal digits leading
·	by "0x".	
Bridge	If you about	as Bridge as the connecting mode places type in the
Bridge	-	ose Bridge as the connecting mode, please type in the
	-	address in these fields. Four peer MAC addresses are
		be entered in this page at one time. Yet please
		unused link to get better performance. If you want to
		peer MAC address, remember to check <b>Enable</b> box
	in the front	t 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.

# 4.12.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN >> Advanced Setting

HT Physical Mode	
Operation Mode	⊙ Mixed Mode ○ Green Field
Channel Bandwidth	○ 20 ④ 20/40
Guard Interval	🔘 long 💿 auto
Aggregation MSDU(A-MSDU)	🔘 Disable 💿 Enable

OK

Operation Mode	<ul> <li>Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.</li> <li>Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.</li> </ul>
Channel Bandwidth	<ul> <li>20- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</li> <li>20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</li> </ul>
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose <b>auto</b> as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable.</b>

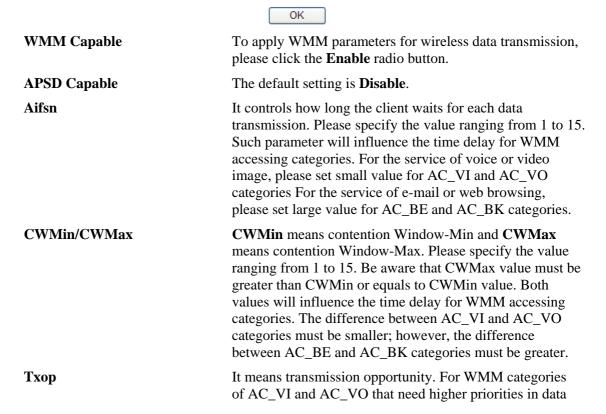
## 4.12.8 WMM Configuration

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	tion				Set to	Factory Default
WMM Capable	pable 💿 Enable 🔘 Disable					
APSD Capable		🔘 Enable	Oisable			
WMM Paramet	ers of Access Po	int				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
AC_BK	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
WMM Paramet	ers of Station					
	Aifsn	CWMir	1 <b>C</b>	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



	transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked.
	<b>Note:</b> Vigor2920 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

## 4.12.9 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	
	1	Scan		
See <u>Sta</u>	atistics.			
	uring the scanning   e router.	process (~5 secor	nds), no station is allowed t	o connect
Add to <u>WDS Settings</u> :				
AP's MA	.C address	: ::::		
Add t	:0	💽 Bridge	○ Repeater	

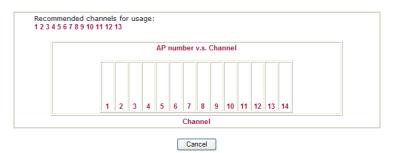
Wireless LAN >> Access Point Discovery

Scan

It is used to discover all the connected AP. The results will be shown on the box above this button.

**Statistics** 

It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics



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.

### 4.12.10 Station List

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

Station List	Status MAC Address	
	Status MAC Address  Refresh  Status Codes :  C: Connected, No encryption.  E: Connected, WEP.  P: Connected, WPA.  A: Connected, WPA.  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	
Refresh	Click this button to refresh the status of station list	t.
Add	Click this button to add current typed MAC addres	SS

Wireless LAN >> Station List

Click this button to add current typed MAC address into **Access Control**.

# 4.13 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.

System Maintenance
System Status
TR-069
Administrator Password
Configuration Backup
SysLog / Mail Alert
Time and Date
Management
Reboot System
Firmware Upgrade

### 4.13.1 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

Aodel Name Firmware Version Build Date/Time	: Vigor2920Vn : 3.3.3_RC2 : Apr 1 2010 12:06:23		
	LAN		WAN 1
MAC Address	: 00-50-7F-C8-D3-B8	Link Status	: Connected
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-C8-D3-B9
1st Subnet Mask	: 255.255.255.0	Connection	: Static IP
DHCP Server	: Yes	IP Address	: 172.16.3.102
DNS	: 168.95.1.1	Default Gateway	: 172.16.1.1
	VoIP		WAN 2
Port Profil	e Reg. In/Out	Link Status	Disconnected
Phone1	No 0/0	MAC Address	: 00-50-7F-C8-D3-BA
Phone2	No 0/0	Connection	:
		IP Address	:
		Default Gateway	:
		N	/ireless LAN
		MAC Address	: 00-50-7F-C8-D3-B8

Frequency Domain Firmware Version

SSID

: Europe : 1.8.1.0 : DrayTek

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
Bunu Date/Thile	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
1 st IP Address	Display the IP address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
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.

### 4.13.2 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.

ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client	
🔘 Enable 🛛 💿 Disable	
URL	http://172.16.3.102:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	•••••
<ul> <li>Disable</li> <li>Enable</li> <li>Interval Time</li> </ul>	000
-	900 second(s)
<ul> <li>Enable</li> <li>Interval Time</li> </ul>	900 second(s)
<ul> <li>Enable</li> <li>Interval Time</li> </ul>	900 second(s)
<ul> <li>Enable Interval Time</li> <li>ttings</li> </ul>	900 second(s)
<ul> <li>Enable Interval Time</li> <li>ttings</li> <li>Disable</li> </ul>	
<ul> <li>Enable Interval Time</li> <li>Disable</li> <li>Enable</li> </ul>	900 second(s)
<ul> <li>Enable Interval Time</li> <li>Disable</li> <li>Enable Server IP</li> </ul>	3478
<ul> <li>Enable Interval Time</li> <li>Disable</li> <li>Enable Server IP Server Port</li> </ul>	3478 60 second(s)

ACS Server URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.



CPE Client	Such information is useful for Auto Configuration Server. Enable/Disable – 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:
	Server IP – Type the IP address of the STUN server.
	<b>Server Port</b> – Type the port number of the STUN server.
	Minimum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

# 4.13.3 Administrator Password

This page allows you to set new password. System Maintenance >> Administrator Password Setup

Old Password	••••	
New Password	•••••	
Confirm Password	•••••	

Old PasswordType in the old password. The factory default setting for<br/>password is "admin".New PasswordType in new password in this field.Confirm PasswordType 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.

# 4.13.4 User Password

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



User Password		
	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.

**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.

# 4.13.5 Configuration Backup

### **Backup the Configuration**

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Mainte	ystem 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			

#### Vigor2920 Series User's Guide

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Dov	wnload	×
?	You are downloading the file: config.cfg from 192.168.1.1 Would you like to open the file or save it to your computer? Open Save Cancel More Info I Always ask before opening this type of file	)

3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

Save As						? 🗙
Save in:	🞯 Desktop		~	GØ	📂 🛄	•
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Pl. RVS-COM Lite Annex A MWSnap300 TeleDanmark Tools config vzk2_232_con vzk6_250_con	aces				
	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	ystem 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.

# 4.13.6 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.

SysLog Access Setup	Mail Alert Setup	
Inable	Enable Send a test e-	mail
Server IP Address	SMTP Server	
Destination Port 514	Mail To	
Enable syslog message:	Return-Path	
Firewall Log	Authentication	
VPN Log	User Name	
User Access Log	Password	
Call Log	Enable E-Mail Alert:	
✓ WAN Log	DoS Attack	
Router/DSL information	M-P2P	

Clear

Cancel

OK

Enable (Syslog Access)	Check "Enable" to activate function of syslog.
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.
Enable (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.

rewall Log VPN Log User Access Log Call Log WAN Log Others Network Information Net State  On Line Routers  IP Address Mask MAC  192.168.1.1 255.255.2 00-50-7F-54-6  NIC Description: SIS 900-Based PCI Fast Ethernet Adapter - Packet S( ▼  NIC Information  MAC Address: 00-11-D8-E4-58-CE Default Geteway: 192.168.1.1  IP Address: 192.168.1.10 ♥ DHCP Server: 192.168.1.1  Subnet Mask: 255.255.25.0 Lease Obtained: 01:28:23 2007  NIS Servers: 168.95.1.1 Lease Expires: Thu Jan 25 01:28:23 2007	ontrols	kets	192.168.1.1 Vigor series RX Packets 1470		JS ateway IP (Fixed)  WAN IP (Fixed)	TX Packets 0 RX Packets 0	TX Rate 0 RX Rate 0
NLC Information           MAC Address:         00-11-D8-E4-58-CE         Default Geteway:         192.168.1.1           IP Address:         192.168.1.10         DHCP Server:         192.168.1.1           Subnet Mask:         255.255.255.0         Lease Obtained:         Mon Jan 22 01:28:23 2007           DNS Servers:         168.95.1.1         Lease Expires:         Thu Jan 25 01:20:2007	On Line Routers	Mask	MAC	Host Name:	vivian		er - Packet St 💙
DNS Servers: 168.95.1.1 Lease Expires: Thu Jan 25	192.168.1.1	255.255.2	00-50-7F-54-6	MAC Address: IP Address:	192.168.1.10	DHCP Server:	192.168.1.1 Mon Jan 22
			>	DNS Servers:	168.95.1.1	Lease Expires:	Thu Jan 25

# 4.13.7 Time and Date

System Maintenance >> Time and Date

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

Current System Time	2010 Apr 3	2 Fri 9 : 1 : 58
Setup		
🔘 Use Browser Time		
💿 Use Internet Time Cli	ent	
Server IP Address		pool.ntp.org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Saving	3	
Automatically Update	Interval	30 min 🔽

**Current System Time** 

Click **Inquire Time** to get the current time.

Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time 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.
Automatically Update Interval	Select a time interval for updating from the NTP server.
Click <b>OK</b> to save these settings.	

### 4.13.8 Management

System Maintenance >> Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

Management Access Control	Management Port Setu	р	
	👓 User Define Ports	🔘 Default I	Ports
Allow management from the Internet	Telnet Port	23	(Default: 23)
FTP Server	HTTP Port	80	(Default: 80)
HTTP Server	HTTPS Port	443	(Default: 443)
HTTPS Server	FTP Port	21	(Default: 21)
<ul> <li>Telnet Server</li> <li>SSH Server</li> </ul>	SSH Port	22	7
Disable PING from the Internet		22	(Default: 22)
	SNMP Setup		
Access List	📃 Enable SNMP Age	nt	
.ist IP Subnet Mask	Get Community	public	
	Set Community	private	
2	Manager Host IP		
3	✓		
	Trap Community	public	
	Notification Host IP		
	Trap Timeout	10	seconds
llow management from the nternet	Enable the checkbox to login from the Internet. provided by the system router from Internet. Ch	There are to allow y	several serve ou managing
isable PING from the Internet	Check the checkbox to rej Internet. For security issue		1
ccess List	You could specify that login from a specific ho maximum of three IPs/s List IP - Indicate an IP router.	ost or netw subnet mas	ork defined in sks is allowed

to

Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
<b>User Defined Ports</b>	Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is <b>public.</b>
Set Community	Set community by typing a proper name. The default setting is <b>private.</b>
Manager Host IP	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.

### 4.13.9 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> <li>Using factory default configuration</li> </ul>
	ОК

If you want to reboot the router using the current configuration, check **Using current** configuration and click **OK**. To reset the router settings to default values, check **Using** factory default configuration and click **OK**. The router will take 5 seconds to reboot the system.

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



# 4.13.10 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.

S	vstem	Maint	enance	>>	Firmware	Up	arade
	yatem	manne	enance		1 IIII W GI C	υp:	graac

Select a firmware file.	
	Browse

TFTP Firmware Upgrade from LAN

Curi	rent Firmware Version: 3.3.3_RC2
Firn	nware Upgrade Procedures:
- 2 3 4	<ul> <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> </ul>
Doy	you want to upgrade firmware ? OK

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.

# 4.14 Diagnostics

Diagnostic Tools provide a useful way to view or diagnose the status of your Vigor router.

Below shows the menu items for Diagnostics.

Diagnostics	
Dial-out Trigger	
Routing Table	
ARP Cache Table	
DHCP Table	
NAT Sessions Table	e
Data Flow Monitor	
Traffic Graph	
Ping Diagnosis	
Trace Route	

# 4.14.1 Dial-out Trigger

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 Trigger

Dial-out Triggere	d Packet Header	I.	<u>Refresh</u>
	HEX Format:		
	00 50 7F 22 33 44-00 0E A6 2A D5 A1-08 00		
	45 00 00 48 BE 54 00 00-7F 11 12 3B CO A8 01 0A A8 5F 01 01 05 CB 00 35-00 37 E3 91 01 74 01 00 00 01 00 00 00 00 00 00-07 67 61 74 65 77 61 79 09 6D 65 73 73 65 6E 67-65 72 07 68 6F 74 6D 61 69 6C 03 63 6F 6D 00 00-01 00 01 E6 84 1A 00 00		
	Decoded Format:		
	192.168.1.10,1483 -> 168.95.1.1,domain Pr udp HLen 20 TLen 75		

**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.

# 4.14.2 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.

# 4.14.3 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

nernet ARP Cache	Table	<u>Clear</u>   <u>Refresh</u>
IP Address	MAC Address	
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.

### 4.14.4 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.

	Assignment Table			<u>Re</u>	<u>fresh</u>
DHCP se Index	erver: Running IP Address	MAC Address	Leased Time	HOST ID	^
1	192.168.1.10	00-0E-16-21-D5-11	0:00:02.630	ok-lccgjyiy075u	
					8
ndex		It displays	the connection ite	em number.	
P Addı	ress	It displays specified P		signed by this router	for
IAC A	ddress		the MAC address gned IP address f	for the specified PC for it.	C tha
eased	Time	It displays	the leased time of	f the specified PC.	
IOST I	(D)	T 1 1	the loss ( ID as a set	of the specified PC.	

4.14.5 NAT Sessions Table

Refresh

Click **Diagnostics** and click **NAT Sessions Table** to open the list page.

Diagnostics >> NAT Sessions Table

Active Sessions	a Table					<u>Refre</u>
Private IP	:Port #P	seudo Port	Peer IP	:Port	Interface	
192.168.1.11	2491	 52078	24.9.93.189	443	UAN1	
192.168.1.11	2493	52080	207.46.25.2	80	WAN1	
192.168.1.10	3079	52665	207.46.5.10	80	WAN1	

Click it to reload the page.

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.

### 4.14.6 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Limit Session		
💿 Enab	le 🔘 Disable	
Default M	Max Sessions: 100	
Limitatio	n List	
Index	Start IP	End IP

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

🗌 Enab	le Data Flow Mon	itor	Refresh Seconds: 10 💌 P	age: 1 💌 🛛	<u>Refresh</u>
Index	IP Address	<u>TX rate(Kbps)</u>	<u>RX_rate(Kbps)</u> 🛩	Sessions	Action
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak	
WAN1	172.16.3.229	1 / 1655 / Auto	1 / 852 / Auto		
WAN2		0 / 0 / Auto	0 / 0 / Auto		
Total		1 / 1655 / Auto	1 / 852 / Auto	6 / 44	

Diagnostics >> Data Flow Monitor

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 C 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.

15 30



Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	Block - can prevent specified PC accessing into Internet within 5

**Block** - can prevent specified PC accessing into Internet within 5 minutes.

Page: 1	*	<u>Refresh</u>
K <u>bps)</u>	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	: 1 🕶	<u>Refresh</u>
<u>s)</u>	Sessions	Action
	blocked / 299	<u>Unblock</u>

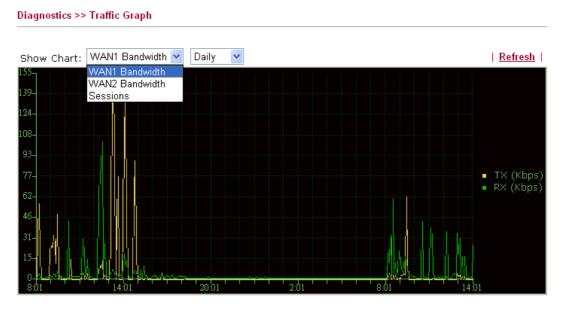
Current /Peak/Speed Current means current transmission rate and receiving rate for WAN1/WAN.

**Peak** means the highest peak value detected by the router in data transmission.

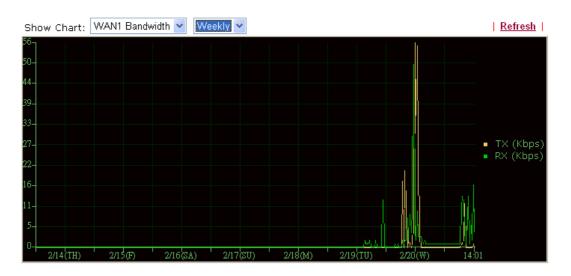
**Speed** means line speed specified in **WAN>>General**. If you do not specify any rate at that page, here will display **Auto** for instead.

# 4.14.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



Diagnostics >> Traffic Graph



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

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

# 4.14.8 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

Ping Diagnosis			
which WA		a LAN PC or you don't want to specify olease select "Unspecified". ~	
Ping ti		IP Address:	
Result	GateWay1 GateWay2 DNS	<u>Clear</u>	
		~	

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.

### 4.14.9 Trace Route

Diagnostics >> 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.

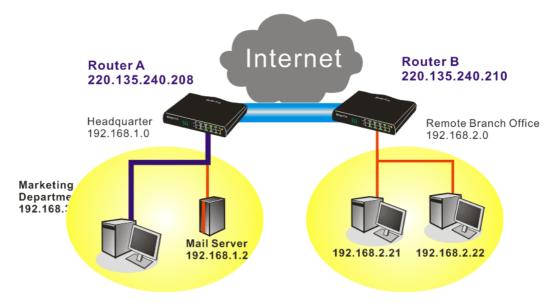
Trace through:	Unspecified 🛩
Protocol:	
Host / IP Address:	ICMP Run
Result	<u> </u>
	<u>^</u>

Protocol	Use the drop down list to choose the interface 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.



# 5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



### Settings in Router A in headquarter:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then,

For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup				
PPP/MP Protocol		IP Address Assignment for D	ial-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			
Autual 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.

s and Dynamic IP Client (LAN to LAN).
••••
••••
t will not be encrypted.
3DES 🗹 AES
d authentic.
t

- 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 ③ Both 〇 Dial-Out 〇 Dial-in Always on
VPN Dial-Out Through WAN1 First V Netbios Naming Packet  Pass OBlock	Idle Timeout     300     second(s)       Enable PING to keep alive       PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 👻
○ РРТР	Username	???
③ 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	
	<ul> <li>Digital Signature(X.509)</li> </ul>	
	None 😪	
	IPSec Security Method	
	Medium(AH)	
	○ High(ESP) DES without Authentication ♥	
	Advanced	
	Index(1-15) in <u>Schedule</u> S	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> S	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 ♥	) 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 network, you have to do
Remote Network IP	192.168.2.0	Route 🖌
Remote Network Mask	255.255.255.0	
	More	$\hfill\square$ Change default route to this VPN tunnel ( Only single WAN supports this )
	ОК С	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 Di	al-In Users
Dial-In PPP	PAP or CHAP	(When DHCP Disable set)	
Authentication		Assigned IP range	192.168.2 200
vial-In PPP Encryption MPPE)	Optional MPPE		
1utual Authentication (	(PAP) 🔘 Yes 💽 No		
Jsername			
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.

eral Setup
s and Dynamic IP Client (LAN to LAN).
••••
••••
t will not be encrypted.
3DES 🗹 AES
d authentic.
5 t



- 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 ③ Both 〇 Dial-Out 〇 Dial-in Always on
VPN Dial-Out Through WAN1 First V Netbios Naming Packet  Pass OBlock	Idle Timeout     300     second(s)       Enable PING to keep alive       PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 😽
○ рртр	Username	???
IPSec Tunnel	Password	
C L2TP with IPSec Policy None	PPP Authentication	PAP/CHAP 🐱
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.50	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) 220.135.240.208	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50) None IPSec Security Method Medium(AH) High(ESP) DES without Advanced Index(1-15) in <u>Schedule</u> , , , ,	t Authentication

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	) 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.

_		 	
-	Dial	Settings	
э.	Dia	 Setunus	

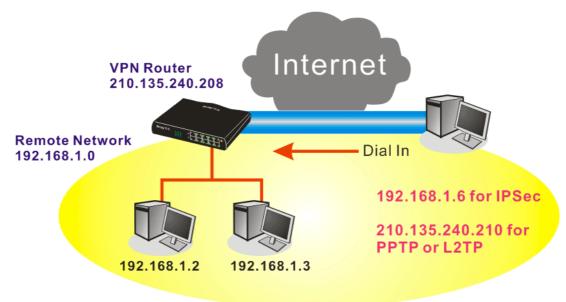
Allowed Dial-In Type		
✓ РРТР	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital Signature(X.509	)
or Peer ID	None 💌	
	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 B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Setting	S		
My WAN IP	0.0.0.0	RIP Direction	Disable 🎽
Remote Gateway IP	0.0.0.0	From first subnet to remo	te network, you have to
Remote Network IP	192.168.1.0		Route 😽
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	to this VPN tunnel ( Only )
	ОК С	Cancel	

# 5.2 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:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup		
PPP/MP Protocol	IP Address Assignment fo	r 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	id 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.

User account and Authentication	Username ???
Enable this account	Password
Idle Timeout 300 second(s)	
Allowed Dial-In Type	IKE Authentication Method
anowed Diai-in Type	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)
	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
or Peer ID	Local ID (optional)
Netbios Naming Packet 💿 Pass 🔘 Block	

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		Username Password	???
Idle Timeout 300	second(s)		LI
Allowed Dial-In Type		IKE Authentication Method	
✓ РРТР		IKE Pre-Shared Key	
IPSec Tunnel		Digital Signature(X.50	9)
L2TP with IPSec Policy None	*	None 🗸	
Specify Remote Node Remote Client IP or Peer ISDN Num	nber	IPSec Security Method	
or Peer ID Netbios Naming Packet ③ Pass	O Block		3DES 🗹 AES
[	ок Сі	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.

or a L2TP connection Q240262 in the Micr	L2TP/IPSec conne . For more infoma	ction using ition, please	
	Configure		
Step 1. Dial to ISP			
Step 1. Dial to ISP If you have already	, gotten a public IF	', you can sł	kip this step.
	' gotten a public If	', you can sł	ip this step. Dial
If you have already		r, you can sł	
		r, you can sł	Dial
If you have already		r, you can sl	

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.

	Setting	
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 II	P Dray	Tek Virture Interface 🛛 💊
💿 Obta	ain an IP address	automatically (DHCP over IPSec
🔘 Spe	cify an IP address	
IP a	Address:	192 , 168 , 1 , 201
Sub	onet Mask:	255 , 255 , 255 , 0
	nod	
Security Meth		High(ESP)
Security Meth	AH) 🤇	Sauduren. V
	AH) (	DES
O Medium(	~	
O Medium(	thod	
Medium( MD5 Authority Me	thod ed Key : *****	
MD5 Authority Me Pre-shar	thod	

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.

# 5.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or 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	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setu</u>
Class Rule Index Name							Rule	Service	Гуре
TUQ						Edit			
Clas	51	Т	est				Luit		
		Т	est				Edit	<u>Edit</u>	

2. Click **Setup** link of WAN. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.

#### WAN1 General Setup

<b>~</b>	Enable the QoS Control	OUT	۷	
	WAN Inboun	IN OUT		jth
	WAN Outbou	BOTH		vidth

3. Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

#### WAN1 General Setup

<b>~</b>	Enable the QoS Control BOTH 💌
	WAN Inbound Bandwidth
	WAN Outbound Bandwidth

10000	Kbps
10000	Kbps

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

4. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1.

Bandwidth Management >> Quality of Service

Class Inc	lex #1					
Name	E-mail					
NO	Status	Local Addres	ss Re	mote Address	DiffServ CodePoint	Service Type
1 ()	Inactive	Any		Any	ANY	undefined
Add Edit Delete						
OK Cancel						

5. For this index, the user will set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP.

Enable the QoS Cor	trol BOTH 🛩	
WAN In	bound Bandwidth	10000 Kbps
WAN O	utbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Bandwi	dth Control	Limited_bandwidth Ratio 25 %
Outbound TCP ACK	Prioritize	Online Statistic

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

ne H	ITTPS				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 💿	Active	Any	Any	ANY	ANY
Add Edit Delete					

### 7. Click **Setup** link for WAN.

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

General	Setup						1.1	Set to Factory I	Default
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>

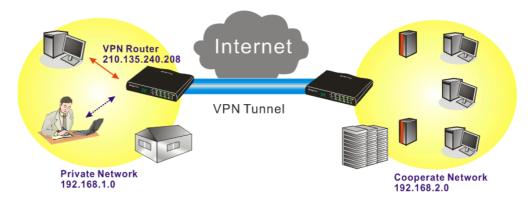
**Class Rule** 

Index	Name	Rule	Service Type
Class 1	E-mail	Edit	
Class 2	HTTPS	Edit	Edit
Class 3		Edit	

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

WAN1 General So		
	WAN Inbound Bandwidth WAN Outbound Bandwidth	10000         Kbps           10000         Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
Enable UDP E	Bandwidth Control	Limited_bandwidth Ratio 25 %
Outbound TC	CP ACK Prioritize	Online Statistics
	OK Clear	Cancel

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.



Click Edit to open a new window.
 Bandwidth Management >> Quality of Service

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

11. Click Edit to open the following window. Check the ACT box, first.

Rule Edit			

Bandwidth Management >> Quality of Service

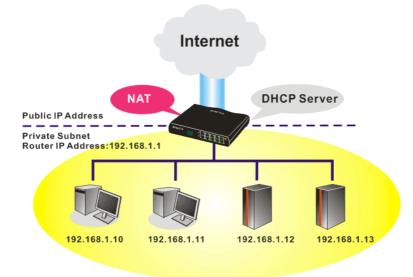
ACT	Hardware Acceleration				
Local Address	Any Edit				
Remote Address	Any				
DiffServ CodePoint	IP precedence 2				
Service Type	SYSLOG(UDP:514)				
Note: Please choose/se	Note: Please choose/setup the Service Type first.				

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**.

# 5.4 LAN - Created by Using NAT

An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



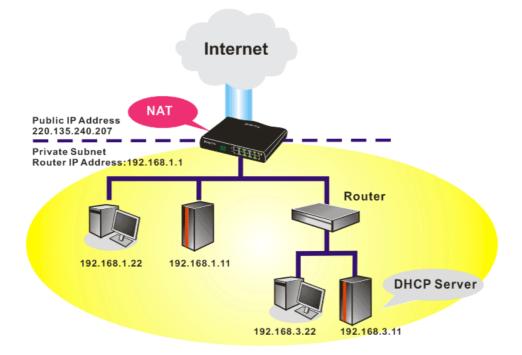


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >>	General	Setup
--------	---------	-------

AN IP Network Configuration			DHCP Server Configuration		
For NAT Usage			⊙Enable Server ○Disable Server		
1st IP Address 192.168.1.1			Relay Agent: 🔘 1st Subnet 🗌 2nd Subnet		
1st Subnet Mask	255.255.255.0		Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable		IP Pool Counts	50	
2nd IP Address	192.168.2.1		Gateway IP Address	192.168.1.1	
2nd Subnet Mask	255.255.255.0	ľ	DHCP Server IP Address		
2nd Subnet DHCP Server			for Relay Agent DNS Server IP Address		
			🔲 Force DNS manual s	etting	
RIP Protocol Control Disable 💌			Primary IP Address		
			Secondary IP Address		

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

#### LAN >> General Setup

Ethernet TCP / IP and DHCI	P Setup			
LAN IP Network Configurat	tion	DHCP Server Configuration		
For NAT Usage		○ Enable Server		
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Subr	et 🔾 2nd Subnet	
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50	
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.3.1	
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address		
2	nd Subnet DHCP Server	for Relay Agent		
		DNS Server IP Address		
RIP Protocol Control Disable 👻		Force DNS manual setting		
		Primary IP Address		
		Secondary IP Address		
		ок		

# 5.5 Upgrade Firmware for Your Router

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 Us
ome > Support > Download	s					
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		R&TTE C	-
Vigor2200Eplus	2.5.7	1	8/02/2009		- Kalle U	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	Education	Partners	Contact U
ome > Support > Ut	ility							
Utility							Downlo	ads
Tools Name	Release Date	Version		os	Support	Model	Firmware	
Router Tools	2009/06/18	4.2.0	MS-V	Vindows	All Mod	ules		
Syslog Tools	2009/06/18	4.2.0	MS-Wi	ndows XP	All Mod	ules	Driver	
-)			MS	-Vista			Utility	
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Wi	ndows XP	VigorPro 10	0 series	Utility In	troduction
Tools		( Multi- language )	MS	-Vista	VigorPro 55 VigorPro 55		Datashee	t
					VigorPro 53	00 series	R&TTE C	ertification
Smart VPN Client	2009/05/25	3.6.3	MS-Wi	ndows XP	All Mod	ules		
		( Multi-	MS	-Vista				
		language)						
Smart Monitor	2009/03/25	2.0	MS-Wi	ndows XP	Vigor2950	series		

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.

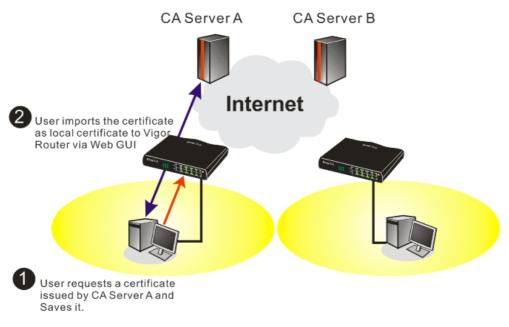
៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send

# 10. Click Send.

៉ Firmware Upgrade	Utility 3.5.1			
Time Out(Sec.) 5	Router IP:			
Port	Firmware file:			
69 Password:	C:\Documents and Settings\Carrie			
Abort Send				
Sending				

11. Now the firmware update is finished.

# 5.6 Request a certificate from a CA server on Windows CA Server



1. Go to Certificate Management and choose Local Certificate. Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		
X509 Local Co	ertificate		
			~
			~

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.

Generate Certificate Request		
Subject Alternative Name		
Туре	Domain Name 👻	
Domain Name	draytek.com	
Subject Name		
Country (C)	TW	
State (ST)		
Location (L)		
Orginization (O)	Draytek	
Orginization Unit (OU)		
Common Name (CN)		
Email (E)	press@draytek.com	
Кеу Туре	RSA 🔽	
Key Size	1024 Bit 🗸	

3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use. Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local /C=TW/O=Draytek/emailAddress		Requesting	View Delete
GENERATE IMPORT REFRESH X509 Local Certificate Request			
MIIBqj( Bgkqhk: A4GNAD( 3wDeQy du84t22 oCkwJw hkiG9w uRLq4C I9Fqkj(	GIN CERTIFICATE REQUEST CCARMCAQAwQTELNAkGAIUEBhMCVFcxEDAO: (G9w0BCQEWEXByZXN2QGRyYX10ZW=uY29t): CBIQKBgQDPioahu/gFQaYB1ce50ERSDfWk: coV1LBJz2IDF0xjX6ip7ev187twwTsg41g btWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI; 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		
vill be able to securely id-	equest a certificate for your web browser, e-mail client, or other secure program. Once you acquire a ce entify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, of certificate you request.	
Select a task:	tificate or certificate revocation list	
<ul> <li>Request a certificat</li> </ul>		
Check on a pending		

#### Select Advanced request.

Microsoft Certificate Services vigor	Home
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request.	
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

	ate for yourself, another user, or a computer using ne the certificates that you can obtain.	one of the following methods. Note that the policy of the certificatio
O Submit a certificate r	equest to this CA using a form.	
<ul> <li>Submit a certificate r</li> </ul>	equest using a base64 encoded PKCS #10 file or	a renewal request using a base64 encoded PKCS #7 file.
	for a smart card on behalf of another user using th nent agent certificate to submit a request for another user.	e Smart Card Enrollment Station.
		Next >

Microsoft Certifica	e Services vigor	Home
Submit A Save	Request	
Sublinit A Save	IRequest	
	encoded PKCS #10 certificate request or PKCS #7 renewal request generate equest field to submit the request to the certification authority (CA).	d by an external application (such as a web
Saved Request:		
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUEST MIIBaj(CARHCAQAwGTELMAKCAIUEBHKUVTCXEDAO BydychkiG900BCCEWEXByZXNQGQRYVIOZWaUY29; A4GNADCB1QKBgQDQVB7mmZFfFhM9/IcQmG03Xk++ hX4bp89cUF9dIoACGG1M/tcB0ckdcZdPFvIXcP3 X/GOA7CTvO/fQzpxrcCwIJJ]LSJS0/Bn9v509516v	
Certificate Templa	<u>Browse</u> for a file to insert. <b>te:</b>	
	Administrator V	
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-----"...." Certificate Management >> Local Certificate

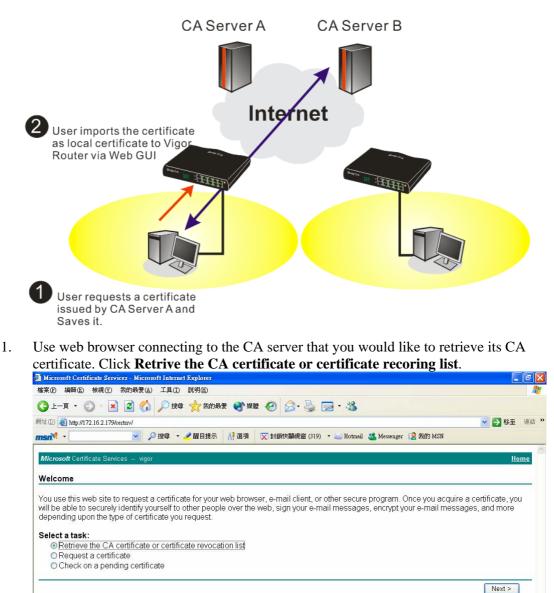
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
GENERATE X509 Lo	IMPORT REFRESH		
MIIBqj Bgkqhk A4GNAD 3wDeQy du84t2 oCkwJw hkiG9w uRLq4C I9Fqkj	EGIN CERTIFICATE REQUEST CCARMCAQAwQTELMAKGA1UEBhMCVFcxEDAO iG9w0BCQEWEXByZXNzQGRYYX10ZWsuY29t CBiQKBgQDPioahu/gFQaYB1ce50ERSDfWk toV1LBJz2IDF0xjX6ip7ev187twwTsg41g 3tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI YJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN DBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToe iEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO JNihip4TCjecSNNZjmQo5WU+Bce8TG+SCB ND CERTIFICATE REQUEST	MIGfMAOGCSqGS nIdHbloltkt9cT Z6Qk/rGhuVTKc rOT2RZjkRMaHF ggtkcmF5dGVrI m1tHQbcwjXvg/ 8JxOI45560xCZ	SIb3DQEBAQUA CdLUDaFk6s8d 19j6PlcrnkP7 CWpVpwIDAQAB mNvbTANBgkq 't7kFlzTJiHh 2/N1Gh9VQ9I1

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=TVWO=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



- 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—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^M -🖌 🔎 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.

This page is left blank.

#### Vigor2920 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**.

Internet	Protocol (TCP/IP) Properties
General	Alternate Configuration
this cap	n get IP settings assigned automatically if your network supports ability. Otherwise, you need to ask your network administrator for ropriate IP settings.
<u>ی ()</u>	otain an IP address automatically
	e the following IP address:
IP ad	idress:
Subr	iet mask:
Defa	ult gateway:
00	atain DNS server address automatically
-OU:	e the following DNS server addresses:
Prefe	erred DNS server.
≜lten	nate DNS server.
	Advanced
	OK Cancel

#### For MacOs

- 1. Double click on the current used MacOs 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.

		Network	
how All	Displays Sou	Network Startup Disk	
	Lo	ocation: Automatic	
		Show: Built-in Ethernet	
	TCP/	(IP PPPoE AppleTalk Proxies Ethernet	)
60	nfigure IPv4:	Using DHCP	, 
	· ·		
	IP Address:	192.168.1.10 Renew I	OHCP Lease
5	Subnet Mask:		
	Router:	(If requir	red)
	DNS Servers:		(Optional)
Sear	ch Domains:		(Optional)
Jean		fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Pv6 Address:		

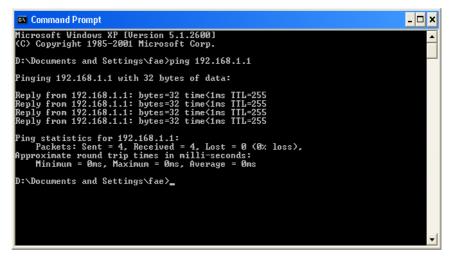
# 6.3 Pinging the Router from Your Computer

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.



	Terminal — bash — 80x24	
Last login: Sat	Jan 3 02:24:18 on ttyp1	
Welcome to Darwi	n!	
Vigor10:~ drayte	k\$ ping 192.168.1.1	
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	2.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
vC		
192.168.1.1	ping statistics	
5 packets transm	itted, 5 packets received, 0% packet loss	
round_trip min/a	va/max = 0.697/0.723/0.755 ms	
Vigor10:~ drayte	k\$ I	

# 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				
WAN1		Ethernet	None 💌	Details Page
WAN2		Ethernet	None PPPoE	Details Page
			Static or Dynamic IP PPTP/L2TP	

#### For PPPoE Users

WAN >> Internet Access

- 1. Check if the **Enable** option is selected.
- 2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

PPPoE Client Mode	PPP/MP Setup
Enable Oisable  ISP Access Setup Username 123 Password	PP Authentication PAP or CHAP v Idle Timeout -1 second(s) IF Address Assignment Method (IPCP) WAN IP Alias Fxed IP: O Yes O No (Dynamic IP)
Index(1-15) in Schedule Setup:         =>       ,       ,         WAN Connection Detection         Mode       ARP Detect 💌         Ping IP	Fixed IP Address



#### **For Static Users**

1. Check if the **Enable** option for Broadband Access is selected.

WAN >> Internet Access

Static or Dynamic IP (DHCP Client)	WAN IP Network Settings	WAN IP Alias
● Enable	Obtain an IP address au	tomatically
Keep WAN Connection	Router Name	*
Enable PING to keep alive	* : Required for some ISPs	
PING to the IP	Specify an IP address	
PING Interval 0 minute(s)	IP Address	172.16.3.229
	- Subnet Mask	255.255.0.0
VAN Connection Detection	Gateway IP Address	172.16.3.4
Mode ARP Detect 💙	DNS Server IP Address	
Ping IP	Primary IP Address	
TTL:	Secondary IP Address	
MTU 1442 (Max: 1500)	Default MAC Address	
RIP Protocol	Specify a MAC Addre	SS
Enable RIP	MAC Address: 00 .50 .7F :00 .00	.01

- 2. Check if **WAN IP Network Settings** is set appropriately.
- 3. Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

#### For PPTP Users

WAN >> Internet Access

1. Check if the **Enable** option for **PPTP** Link is selected.

PPTP/L2TP Client Mode	PPP Setup
● Enable PPTP ○ Enable L2TP ○ Disable	PPP Authentication PAP or CHAP 🗸
Server Address 10.0.0.138	Idle Timeout -1 second(s)
Specify Gateway IP Address	IP Address Assignment Method (IPCP) WAN IP Alias
	Fixed IP: 🔘 Yes 💿 No (Dynamic IP)
ISP Access Setup	Fixed IP Address
Username	WAN IP Network Settings
Password	O Obtain an IP address automatically
Index(1-15) in <u>Schedule</u> Setup:	<ul> <li>Specify an IP address</li> </ul>
=>,,,	IP Address 10.0.0.150
	Subnet Mask 255.0.0.0
MTU 1442 (Max:1460)	

- 2. Check if **PPTP Server, Username,** and **Password** are set correctly (must identify with the values from your ISP).
- 3. Check if **WAN IP Network Settings** are set properly. If you select **Specify an IP address**, you have to type in the values of **IP Address** and **Subnet Mask** manually. Be sure the values that you type identify with the values from your ISP.

#### 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 Vigor2920. 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 Vigor2920.

#### 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.

	1 32 .	192.168.1.1	Getway IP (Static)	TX Packets	RX Rate
		DrayTek Vigor2910		0	0
AN Status TX Packets	c	RX Packets	WAN IP (Static)	RX Packets	, TX Rate
6442		3807		0	0
1 0442		3007	1	1 0	1 0
			•		
Wall Log VPN Lo	g User Acce	ss Log Call Log WAN	Log Network Infomation	Net State	
Time	Host	Message			
Apr 12 09:17:49					
	Vigor		tocol:LCP(c021) ConfReq Id	entimer:0x03 ACCM: (	JXO A GUIE.
Apr 12 09:17:49	Vigor	[3G]Modem status:a1 2	20 00 00 00 00 02 00 03 00		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE => Pro	20 00 00 00 00 00 02 00 03 00 tocol:LCP(c021) ConfReg Ide		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor 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	Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE => Pro WAN2 PPPoE <= V:1 [3G]Modem response:	20 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 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 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE => Pro WAN2 PPPoE <= V1 [3G]Modem response: [3G]Modem status:a1 2 [3G]Modem status:a1 2	20 00 00 00 00 02 00 03 00 tocol.LCP(e021) ConfReg Id: T1 PADS ID:0 CONNECT 3600000 20 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	Vigor Vigor Vigor 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 [3G]Modem status:a1 2 [3G]Modem dial ATD	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 P99#		
Apr 12 09:17:49           Apr 12 09:17:49	Vigor Vigor Vigor 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 [3G]Modem status:a1 2 [3G]Modem dial ATD WAN2 PPPoE => V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 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 status:a1 2 WAN2 PPPoE => Pro WAN2 PPPoE <= V:1 [3G]Modem status:a1 2 [3G]Modem status:a1 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		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE => Pro WAN2 PPPoE => Pro [3G]Modem response: [3G]Modem status:a1 2 [3G]Modem dial ATD WAN2 PPPoE => V:1 WAN2 PPPoE => V:1 [3G]Modem response:	20 00 00 00 00 00 02 00 03 00 tocol:LCP(021) ConfReq Id. T:I 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:I PADR ID-0 T:I PADC ID-0 CK	entifier:0x00 MRU: 15	
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE ⇒> Pro WAN2 PPPoE <=> V:1 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem response: [3G]Modem response: [3G]Modem initialize A	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 CK 17&FE0V1X1&D2&C1S0=0	entifier:0x00 MRU: 15	
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor 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 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem response: [3G]Modem response: [3G]Modem response: [3G]Modem status:a2 WAN2 PPPoE => V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 CK 17&FE0V1X1&D2&C1S0=0	entifier:0x00 MRU: 15	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status:a1 2 WAN2 PPPoE ⇒> Pro WAN2 PPPoE <=> V:1 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem response: [3G]Modem response: [3G]Modem initialize A	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 CK 17&FE0V1X1&D2&C1S0=0	entifier:0x00 MRU: 15	
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor 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 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem status:a1 2 [3G]Modem response: [3G]Modem response: [3G]Modem response: [3G]Modem status:a2 WAN2 PPPoE => V:1	20 00 00 00 00 00 02 00 03 00 tocol:LCP(6021) 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 20 00 00 00 00 02 00 02 00 7:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0 CK 17&FE0V1X1&D2&C1S0=0	entifier:0x00 MRU: 15	500 ACCM

#### 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 Vigor2920. 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 **OK**. After few seconds, the router will return all the settings to the factory settings.



Reboot System		
	Do you want to reboot your router ?	
	<ul> <li>Using current configuration</li> <li>Using factory default configuration</li> </ul>	
1	ОК	

#### **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.