

### Vigor2920/2920n Dual-WAN Security Router



Your reliable networking solutions partner

### User's Guide

#### **Dray** Tek

### Vigor2920 Series Dual-WAN Security Router User's Guide

Version: 1.0 Firmware Version: V3.3.2 Date: 29/03/2010



#### **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	<ul> <li>The following trademarks are used in this document:</li> <li>Microsoft is a registered trademark of Microsoft Corp.</li> <li>Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.</li> <li>Apple and Mac OS are registered trademarks of Apple Inc.</li> <li>Other products may be trademarks or registered trademarks of their respective manufacturers.</li> </ul>

#### Safety Instructions and Approval

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



#### **European Community Declarations**

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, 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.

#### **Dray** Tek

#### 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	2 4
1.3 Hardware Installation	6
1.4 Printer Installation	7



Configuring Basic Settings	13
2.1 Two-Level Management	13
2.2 Accessing Web Page	13
2.3 Changing Password	14
2.4 Quick Start Wizard	16
2.4.2 PPPoE 2.4.3 PPTP/L2TP 2.4.4 Static IP 2.4.5 DHCP	
2.5 Online Status	22
2.6 Saving Configuration	23



User Mode Operation	25
3.1 Internet Access	25
<ul> <li>3.1.1 Basics of Internet Protocol (IP) Network</li> <li>3.1.2 General Setup</li> <li>3.1.3 Internet Access</li></ul>	27 29
3.2 LAN	38
3.2.1 Basics of LAN 3.2.2 General Setup	38 39
3.3 NAT	42
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	45
3.4 Applications	48
3.4.1 Dynamic DNS 3.4.2 UPnP	49 51
3.5 Wireless LAN	52



3.5.1 Basic Concepts	
3.5.2 General Setup	
<ul> <li>3.5.1 Basic Concepts</li> <li>3.5.2 General Setup</li> <li>3.5.3 Security</li> <li>3.5.4 Access Control</li> </ul>	
3.5.4 Access Control	
3.5.5 Station List	59
3.6 System Maintenance	60
3.6.1 System Status	60
3.6.1 System Status 3.6.2 User Password	61
3.6.3 Time and Date	
3.6.4 Reboot System	
3.7 Diagnostics	63
3.7.1 DHCP Table	63
3.7.2 Traffic Graph	
3.7.3 Ping Diagnosis	
3.7.4 Trace Route	



Admin Mode Operation	67
4.1 Internet Access	
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	
4.2 LAN	80
4.2.1 Basics of LAN	
4.2.2 General Setup	
4.2.3 Static Route	
4.2.4 VLAN	
4.2.5 Bind IP to MAC	
4.3 NAT	
4.3.1 Port Redirection	
4.3.2 DMZ Host	
4.3.3 Open Ports	
4.4 Firewall	
4.4.1 Basics for Firewall	
4.4.2 General Setup	
4.4.3 Filter Setup	
4.4.4 DoS Defense	107
4.5 Objects Settings	
4.5.1 IP Object	
4.5.2 IP Group	
4.5.3 Service Type Object	
4.5.4 Service Type Group	
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	121
4.5.10 Misc Object	
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	
4.7 Bandwidth Management	
4.7.1 Sessions Limit	-
4.7.2 Bandwidth Limit 4.7.3 Quality of Service	
4.8 Applications	
4.8.1 Dynamic DNS	
4.8.2 Schedule 4.8.3 RADIUS	
4.8.4 UPnP	
4.8.5 IGMP	148
4.8.6 Wake on LAN	148
4.9 VPN and Remote Access	150
4.9.1 Remote Access Control	150
4.9.2 PPP General Setup	
4.9.3 IPSec General Setup	
4.9.4 IPSec Peer Identity 4.9.5 Remote Dial-in User	
4.9.5 Remote Dial-in Osei	
4.9.7 Connection Management	
4.10 Certificate Management	166
4.10.1 Local Certificate	
4.10.1 Local Certificate	
4.10.3 Certificate Backup	
4.11 Wireless LAN	169
4.11 Wireless LAN	169 169
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.	169 169 171 174
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.	169 169 171 174 175
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts.</li> <li>4.11.2 General Setup.</li> <li>4.11.3 Security.</li> <li>4.11.4 Access Control.</li> <li>4.11.5 WPS.</li> </ul>	169 169 171 174 175 177
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts.</li> <li>4.11.2 General Setup.</li> <li>4.11.3 Security.</li> <li>4.11.4 Access Control.</li> <li>4.11.5 WPS.</li> <li>4.11.6 WDS.</li> </ul>	169 169 171 174 175 177 179
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration	169 169 171 174 175 177 179 182 183
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery	169 169 171 174 175 177 179 182 183 185
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts</li></ul>	169 169 171 174 175 177 179 182 183 186
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery	169 169 171 174 175 177 179 182 183 186
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts</li></ul>	169 169 171 174 175 177 179 182 183 186 186
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts.</li> <li>4.11.2 General Setup.</li> <li>4.11.3 Security.</li> <li>4.11.3 Security.</li> <li>4.11.4 Access Control.</li> <li>4.11.5 WPS.</li> <li>4.11.6 WDS.</li> <li>4.11.6 WDS.</li> <li>4.11.7 Advanced Setting.</li> <li>4.11.8 WMM Configuration.</li> <li>4.11.9 AP Discovery</li></ul>	169 169 171 174 175 177 179 182 183 186 186 187 188
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts.</li> <li>4.11.2 General Setup.</li> <li>4.11.3 Security.</li> <li>4.11.3 Security.</li> <li>4.11.4 Access Control.</li> <li>4.11.5 WPS.</li> <li>4.11.6 WDS.</li> <li>4.11.6 WDS.</li> <li>4.11.7 Advanced Setting.</li> <li>4.11.8 WMM Configuration.</li> <li>4.11.8 WMM Configuration.</li> <li>4.11.9 AP Discovery.</li> <li>4.11.10 Station List.</li> <li>4.12 System Maintenance.</li> <li>4.12.1 System Status.</li> <li>4.12.2 TR-069.</li> <li>4.12.3 Administrator Password.</li> </ul>	169 169 171 174 175 177 179 182 183 186 186 187 188 189
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.3 Administrator Password.         4.12.4 Configuration Backup	169 169 171 174 175 177 179 182 183 186 186 187 188 189 189 189
<ul> <li>4.11 Wireless LAN.</li> <li>4.11.1 Basic Concepts.</li> <li>4.11.2 General Setup.</li> <li>4.11.3 Security.</li> <li>4.11.3 Security.</li> <li>4.11.4 Access Control.</li> <li>4.11.5 WPS.</li> <li>4.11.6 WDS.</li> <li>4.11.6 WDS.</li> <li>4.11.7 Advanced Setting.</li> <li>4.11.8 WMM Configuration.</li> <li>4.11.8 WMM Configuration.</li> <li>4.11.9 AP Discovery.</li> <li>4.11.10 Station List.</li> <li>4.12 System Maintenance.</li> <li>4.12.1 System Status.</li> <li>4.12.2 TR-069.</li> <li>4.12.3 Administrator Password.</li> </ul>	169 169 171 174 175 177 182 183 185 186 186 188 188 189 189 192
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.3 Administrator Password.         4.12.4 Configuration Backup.         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date         4.12.7 Management.	169 169 171 174 175 177 179 182 183 185 186 186 187 188 189 189 192 193 194
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.2 TR-069.         4.12.4 Configuration Backup.         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date         4.12.7 Management.         4.12.8 Reboot System	169 169 171 174 175 177 179 182 183 185 186 186 186 187 188 189 192 193 194 195
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.2 TR-069.         4.12.3 Administrator Password.         4.12.4 Configuration Backup.         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date.         4.12.7 Management.         4.12.8 Reboot System.         4.12.9 Firmware Upgrade.	169 169 171 174 175 177 179 182 183 185 186 187 188 188 189 189 192 193 195 196
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.2 TR-069.         4.12.4 Configuration Backup.         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date         4.12.7 Management.         4.12.8 Reboot System	169 169 171 174 175 177 179 182 183 185 186 187 188 188 189 189 192 193 195 196
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.2 TR-069.         4.12.3 Administrator Password.         4.12.4 Configuration Backup         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date.         4.12.7 Management.         4.12.8 Reboot System         4.12.9 Firmware Upgrade.         4.13 Diagnostics.         4.13 Dial-out Trigger.	169 169 171 174 175 177 179 182 183 185 186 186 187 188 189 189 192 193 194 195 197 197
4.11 Wireless LAN.         4.11.1 Basic Concepts         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery         4.11.10 Station List         4.12 System Maintenance.         4.12.1 System Status.         4.12.3 Administrator Password.         4.12.4 Configuration Backup         4.12.5 Syslog/Mail Alert         4.12.6 Time and Date         4.12.7 Management         4.12.8 Reboot System         4.13 Diagnostics.         4.13 Dial-out Trigger         4.13.2 Routing Table	169 169 171 174 175 177 179 182 183 185 186 186 187 188 189 189 192 193 194 195 197 197 198
4.11 Wireless LAN.         4.11.1 Basic Concepts.         4.11.2 General Setup.         4.11.3 Security.         4.11.4 Access Control.         4.11.5 WPS.         4.11.6 WDS.         4.11.7 Advanced Setting.         4.11.8 WMM Configuration         4.11.9 AP Discovery.         4.11.10 Station List.         4.12 System Maintenance.         4.12.1 System Status.         4.12.2 TR-069.         4.12.3 Administrator Password.         4.12.4 Configuration Backup         4.12.5 Syslog/Mail Alert.         4.12.6 Time and Date.         4.12.7 Management.         4.12.8 Reboot System         4.12.9 Firmware Upgrade.         4.13 Diagnostics.         4.13 Dial-out Trigger.	169 169 171 174 175 177 179 182 183 186 186 187 188 189 189 192 193 194 197 197 198 198 198 198 198 198 198

4.13.6 Data Flow Monitor	200
4.13.7 Traffic Graph	
4.13.8 Ping Diagnosis	
4.13.9 Trace Route	



Application and Examples	.205
5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	. 205
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	. 213
5.3 QoS Setting Example	. 217
5.4 LAN – Created by Using NAT	. 220
5.5 Upgrade Firmware for Your Router	. 223
5.6 Request a certificate from a CA server on Windows CA Server	. 226
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server	. 230



Trouble Shooting	233
6.1 Checking If the Hardware Status Is OK or Not	233
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	234
6.3 Pinging the Router from Your Computer	236
6.4 Checking If the ISP Settings are OK or Not	237
6.5 Problems for 3G Network Connection	239
6.6 Backing to Factory Default Setting If Necessary	240
6.6 Contacting Your Dealer	241

## 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.
<b>Note:</b> 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 <b>Firewall</b> >> <b>General</b> <b>Setup</b> . (Such profile must be established under <b>CSM</b> menu).	
WCF		On	The Web Content Filter is active. (It is enabled from <b>Firewall &gt;&gt; General Setup</b> ).	
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 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 GigsLAN+1 2 3 4 WAN1 WAN2(Gigs) 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

Reset CSM WAINZ Q	N 55		GigaLAN > 1 2 3 4 WAN1 WAN2(Giga) US
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 <b>Firewall</b> >> <b>Gene</b> <b>Setup</b> . (Such profile must be established und <b>CSM</b> menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink slowly while wireless traffic goes through. If ACT and WLAN LEDs blink quickly and simultaneously when WPS is working, and it 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 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 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.
C' LAN	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	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when LED is on.

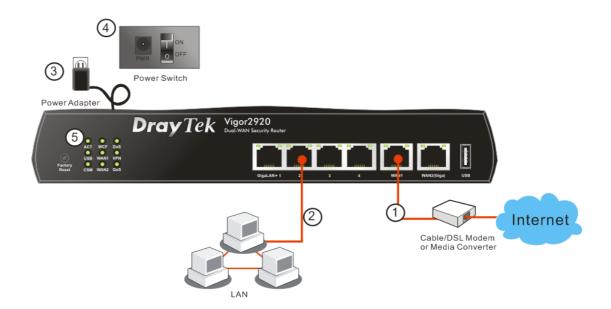
	920 ecurity Router IIIIII GigsLAN + 1 2 3 4 WAN1 WAN2(Gigs) USB
Interface	Description
Wireless LAN ON/OFF/WPS Factory Reset	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection. 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.

#### **1.3 Hardware Installation**

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

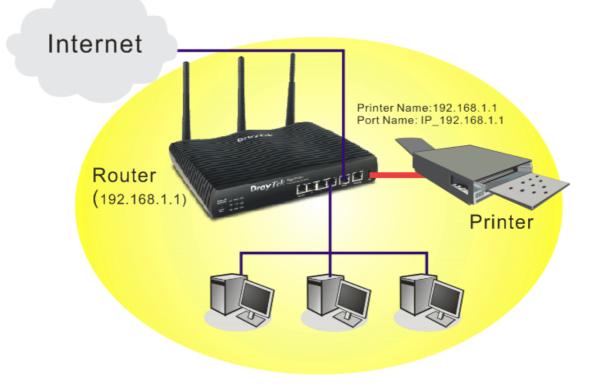
- 1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
- 2. Connect one end of an Ethernet cable (RJ-45) to one of the LAN ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
- 3. Connect one end of 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.)



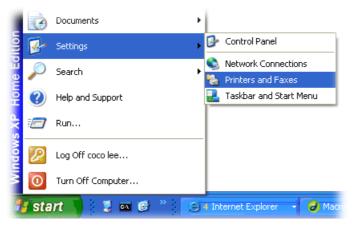
#### **1.4 Printer Installation**

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.

d Printer	Wizard
Loodi oi ii	etwork Printer ard needs to know which type of printer to set up.
Select t	ne option that describes the printer you want to use:
	I printer attached to this computer
	automatically detect and install my Plug and Play printer
( <b>i</b> )	To set up a network printer that is not attached to a print server, use the "Local printer" option.
~	
	< <u>B</u> ack <u>N</u> ext > Cancel

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
O Use 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**.

Add Standard TCP/IP Printer Add Port For which device do you want	
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress: <u>P</u> ort Name:	192.168.1.1 IP_192.168.1.1
Low Hand.	
	( <u>B</u> ack <u>N</u> ext > Cancel

7. Click Standard and choose Generic Network Card.

.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
Custom Settings
( <u>B</u> ack <u>N</u> ext ) Cancel

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



**Dray** Tek

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.

General S	haring Port	s Advanced	d Device Set	tings	
ð	Brother HL-1	070			
checked (	port.		nts will print to t	he first free	
Port	Descrip		Printer		
3.25		TCP/IP Port	Epson Stylus	COLOR 1160	
		TCP/IP Port			
		TCP/IP Port	HP LaserJet	1300	
		TCP/IP Port			
		TCP/IP Port			
		TCP/IP Port		070	
D PDF	Local Po	rt	PDF995	_	1
Add	l Por <u>t</u>	Delete	e Port	<u>C</u> onfigure Port	
	late the set				-
	bidirectional				
Enable	printer poolir	g			

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.

onfigure Standard TCP	/IP Port Monitor
Port Settings	
Port Name:	IP_192.168.1.1
Printer Name or IP Address:	192.168.1.1
Protocol O <u>R</u> aw	<u>⊙ </u> LPR
Raw Settings	
Port Number:	9100
LPR Settings Queue Name:	o1
SNMP Status Enabled	
Community Name:	public
SNMP <u>D</u> evice Index:	
	OK Cancel

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.

FAQ - Basic	FAQ
01. What are the differences among these firmware file formats ?	Basic
02. How could I get the teinet 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 AnnexB? ( For ADSL model only )	VoIP
07. Ways for firmware upgrade.	QoS
08. Whγ is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?	ISDN
	Firewall / IP Filter
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should I do?	Printer Server
10. How to upgrade firmware of Vigor Router remotely ?	USB ISDN TA
	1185

#### FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?

02. How do I configure LPR printing on Windows98/Me ?

03. How do I configure LPR printing on Linux boxes ?

04. Why there are some strange print-out when I try to print my documents through Vigor210 4P / 2300's print server?

05. What types of printers are compatible with Vigor router?

06. What are the limitations in the USB Printer Port of Vigor Router ?

07. What is the printing buffer size of Vigor Router ?

08. How do I configure LPR printing on Mac OSX ?

09. How do I configure LPR printing on My Windows Vista ?

**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

#### **Dray** Tek

# **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
<b>Dray</b> Tek

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



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

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



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

#### 2.3 Changing Password

No matter user mode operation or admin mode operation, please change the password for the original security of the router.

- 1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
- 2. Please type "admin/admin" on Username/Password for admin mode. Otherwise, do not type any word (both username and password are Null for user mode) on the window and click **Login** on the window.
- 3. Now, the **Main Screen** will appear.

ff 🔽	System Status			
uick Start Wizard Iline Status AN N	Model Name Firmware Version Build Date/Time	: Vigor2920 Series : 3.3.2_RC2 : Oct 15 2009 14:26:58		
λT		LAN		WAN 1
rewall ojects Setting SM andwidth Management oplications PN and Remote Access	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-00-00-00 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-00-00-01 : : :
ertificate Management stem Maintenance				WAN 2
All Rights Reserved.			Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-00-00-02 : DHCP Client : 192.168.5.26 : 192.168.5.1

Main screen for admin mode operation (full configuration)

Auto Logout 👻 wick Start Wizard	System Status			
VAN	Model Name Firmware Version Build Date/Time	: Vigor2920 Series : 3.3.2_RC2 : Oct 15 2009 14:26:58		
AT		LAN		WAN 1
pplications ystem Maintenance iagnostics	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-00-00-00 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-00-00-01 : : :
All Rights Reserved.				WAN 2
			Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-00-00-02 : DHCP Client : 192.168.5.26 : 192.168.5.1

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			
л	New Password			
C	Confirm Password			
		OK		
		or		
ystem Maintenance	e >> User Password	or		
	e >> User Password	or		
ser Password	e >> User Password	or		 
ser 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 Dray Tek

#### 2.4 Quick Start Wizard



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

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

#### Quick Start Wizard

login password		
Please enter an alpha-nume	eric string as your Passw	ord (Max 23 characters).
Old Password	••••	
New Password	••••	
Confirm Password	••••	
	< Bac	k Next > Finish Can

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	<ul> <li>PPPoE</li> <li>PPTP</li> <li>L2TP</li> <li>Static IP</li> </ul>	<ul> <li>PPPoE</li> <li>PPTP</li> <li>L2TP</li> <li>Static IP</li> </ul>	<ul> <li>PPPoE</li> <li>PPTP</li> <li>L2TP</li> <li>Static IP</li> </ul>	<ul> <li>PPTP</li> <li>L2TP</li> <li>Static IP</li> </ul>

#### 2.4.2 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 pa	sword provided by your ISP.	
User Name	84005755@hinet.net	
Password	•••••	
Confirm Password	•••••	
	< Back Next > Finish Cancel	

- User Name Assign a specific valid user name provided by the ISP.
- **Password** Assign a valid password provided by the ISP.
- **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.

#### 2.4.3 PPTP/L2TP

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

Quick Start Wizard

WAN 1	
Enter the user name, pass your ISP.	rord, 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 address	
IP Address	172.16.3.229
Subnet Mask	255.255.0.0
PPTP Server	

Click Next for viewing summary of such connection.

Quick Start Wizard

ease confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	РРТР
settings and restart the V	igor router.
	< Back Next > Finish Cance

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 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.

Qu	ick	Start	W	izard	

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP

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

#### 2.4.5 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 igor 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				Sy	stem Uptime: 0:0:
LAN Status	Primary DNS: 168.95.1.1		5.1.1	Secondary DI	NS: 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)	RX Packets	RX Rate(Bps)
192.168.5.30	192.168.5.1	14	60	12	66

Detailed explanation is shown below:

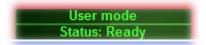
Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
<b>RX</b> Packets	Displays the total number 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

#### **Dray** Tek

## **3** User Mode Operation

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

- 1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
- 2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

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

Auto Logout 💌	System Status			
Quick Start Wizard Online Status WAN AN	Model Name Firmware Version Build Date/Time	: Vigor2920 Series : 3.3.2_RC2 : Oct 15 2009 14:26:58		
IAT		LAN		WAN 1
Applications Mireless LAN System Maintenance Diagnostics Loqout	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-00-00-00 : 192.168.1.1 : 255.255.255.0 : Yes : 168.95.1.1	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-00-00-01 : : :
All Rights Reserved.				WAN 2
			Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-00-00-02 : DHCP Client : 192.168.5.26 : 192.168.5.1

#### **3.1 Internet Access**

**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 **Internet Access** 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.

Note: In default, WAN1 is enabled. WAN2 is optional.			
WAN >> General Setup			
C			
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 on demand:	
🔾 WAN2 Fail		O WAN1 Fail	
WAN2 Upload speed exceed     Kbps		WAN1 Upload spe	eed exceed 0 Kbps
WAN2 Download speed exceed 0 Kbps			
1		1	

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	1.	cal connection is done and fixed through physical connection for WAN2 is done ort (P1) or USB port.	0
	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	
Physical Type	You can chang	ge the physi	ical type for WAN2 or choose Auto	
	-		ed by the system.	
	Physical Type	e:	Auto negotiation 🔽	
	, ,,		Auto negotiation	
			10M half duplex	
			10M full duplex	
			100M half duplex	
			100M full duplex	
Load Balance Mode	If you know th	e practical	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 choos		-		
	demand to make the WAN connection (WAN1/WAN2)			
	activated if it i	s necessary	7.	
	Active Mode:		Active on demand 💙	
			Always On	
			Active on demand	
			lemand, the Idle Timeout will be	
	•		r PPPoE and PPTP access modes in	
			<b>N&gt;&gt;Internet Access</b> . In addition, there but to choose for different purposes.	
			e connection for WAN1 will be	
	activated when			
			<b>ceed XX kbps</b> – It means the	
	-	-	ll be activated when WAN2 Upload	
	•	ertain valu	that you set in this box for $15$	
	seconds.			
		-	exceed XX kbps– It means the	
			Il be activated when WAN2	
	Download spe	ed exceed d	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 Nan	ne 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 in	AN modes that this router supports. WAN1 is the atterface for accessing into the Internet. WAN2 is the interface for accessing into the Internet when WAN ome reason.
Display Name	It shows the nan setup.	ne of the WAN1/WAN2 that entered in general
Physical Mode It shows the physical connection for WAN1 (Ethernet) (Ethernet or 3G USB Modem) according to the real ne connection. Physical Mode Physical Mode		usical connection for $WAN1$ (Ethernet) / $WAN2$
hysical Mode	(Ethernet or 3G connection.	USB Modem) according to the real network
hysical Mode	(Ethernet or 3G connection.	USB Modem) according to the real network

**Dray** Tek

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>	dule Setup:	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	<ul> <li>Default MAC Addre</li> <li>Specify a MAC Address:</li> <li>00 .50 .7F :00 .</li> </ul>	
	OK	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.

🗿 WAN II	? Alias - Mi	crosoft Internet Explorer	
WAN IP	Alias ( Mı	ilti-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           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
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>

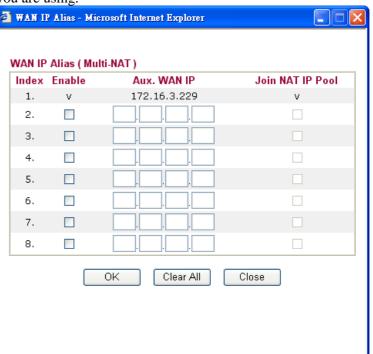
ΟK

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 1			
PPTP/L2TP Client Mode		PPP Setup	
◯ Enable PPTP ◯ E	nable L2TP 💿 Disable	PPP Authentication	PAP or CHAP 🔒
Server Address		Idle Timeout	-1 second(s)
Specify Gateway IP Add	ress	IP Address Assignment M	ethod
		(IPCP) WAN IP Alias	
		Fixed IP: 🔘 Yes 💿 N	lo (Dynamic IP)
ISP Access Setup		Fixed IP Address	
Username		WAN IP Network Settings	
Password		Obtain an IP address	s automatically
Index(1-15) in <u>Schedule</u>	<u>e</u> Setup:	Specify an IP addres	SS
=>,,	,	IP Address	
		Subnet Mask	
MTU	1442 (Max:1460)		
	ОК	Cancel	
ISP Access Setup	Disable – Click this PPTP or L2TP. Server Address - S server if you enable Specify Gateway II for DHCP server. Username -Type in	a DSL modem on the radio button to close to pecify the IP address of PPTP/L2TP client mo <b>P Address</b> – Specify the the username provide the password provided	the connection through of the PPTP/L2TP ode. he gateway IP address d by ISP in this field.
	Index (1-15) in Sch schedule for your re	nedule Setup - You car equest. All the schedule edule web page and yo	n type in four sets of time es can be set previously in u can use the number that
MTU	It means Max Tra 1442.	nsmit Unit for packe	t. The default setting is
PPP Setup	Idle Timeout - Set		r <b>PAP or CHAP</b> for PPP ng down the Internet after on.
IP Address Assignment Method(IPCP)	time you connect to service to always as request. In this case field. Please contact	it and request. In som ssign you the same IP a you can fill in this IP t 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

WAN >> Internet Access



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.

ndex	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.

### 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	Dest Port End
1		any	*	WAN1 💌						
<u>2</u>		any	*	WAN1 🔽						
<u>3</u>		any	*	WAN1 💌						
<u>4</u>		any	*	WAN1 🔽						
<u>5</u>		any	*	WAN1 💌						
<u>6</u>		any	*	WAN1 🔽						
Z		any	*	WAN1 💌						
<u>8</u>		any	*	WAN1 🔽						
<u>9</u>		any	*	WAN1 💌						
<u>10</u>		any	*	WAN1 🔽						
< <u>1-10</u>	<u>11-20</u> >	•>								Next :

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.

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.

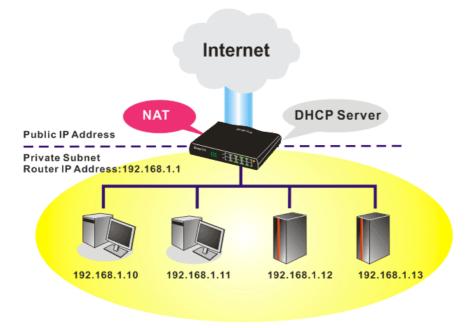
# 3.2 LAN

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.



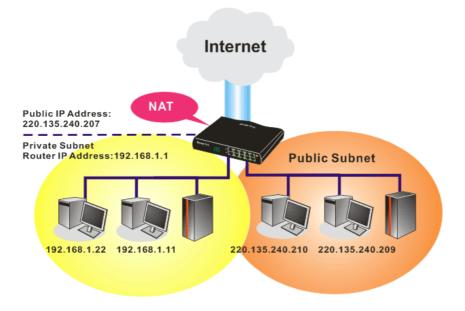
### 3.2.1 Basics of LAN

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 DHCP Setup	
LAN 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 255.255.0	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 255.255.0	DHCP Server IP Address
2nd Subnet DHCP Server	for Relay Agent DNS Server IP Address
	Force DNS manual setting
RIP Protocol Control Disable 🍸	Primary IP Address
	Secondary IP Address

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)

# **Dray** Tek

For IP Routing Usage	Click <b>Enable</b> to invoke this function. The default setting is <b>Disable</b> .
2 <sup>nd</sup> IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)
2 <sup>nd</sup> Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/24)
2 <sup>nd</sup> 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 (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 2<sup>nd</sup> DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2<sup>nd</sup> subnet won't get an IP address belonging to 1<sup>st</sup> 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 - (1<sup>st</sup> subnet/2<sup>nd</sup> 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 DNS Server IP address: 194.109.6.66 to this field.</li> </ul>
	The default DNS Server IP address can be found via Online Status:
	System Optime: 7 1:47:46

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.

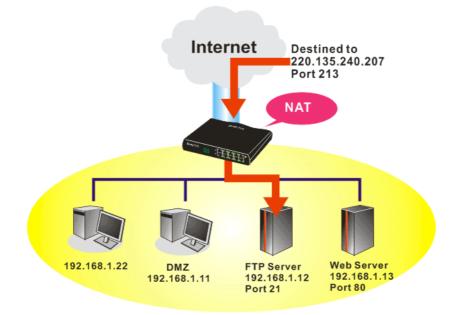
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

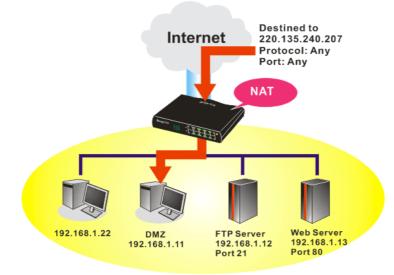
ОК	Clear	Cancel
----	-------	--------

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.

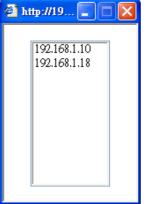
MZ Host S	Setup			
WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229		Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC

**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

# 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>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				х
<u>10.</u>				х

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
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	)				
WAN Interface			WA	N1 💌			
Local Computer 192.168.1.10 Choose 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 🗸
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.

ress 🔕 Network Connections	Contraction of Contraction	📲 IP Broadband Conr	ection on Route	er Status [?]
Vetwork Tasks         Image: Create a new connection           Image: Set up a home or small office network         Image: Create a new connection	Broadband hinet Disconnected WAN Miniport (PPPOE)	General		C
divite official	Dial-up	Status: Duration:		Connected 00:19:06
ee Also 🔹	test Disconnected	Speed:		100.0 Mbps
Other Places         Image: Control Panel           Omega Control Panel         My Network Places	Internet Gateway IP Broadband Connection on Router	<b>O</b>	ernet Gateway - 🥰	My Computer
My Documents My Computer	Enabled	Packets: Sent: Received:	404 1,115	734 666
Details 🛞	Local Area Connection Enabled Realtek RTL8139/810x Family	Properties Dis	able	Close

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



eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
🧐 IP Broadband Connection on Router	Services
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 Wireless LAN

This function is used for "n" models.

### 3.5.1 Basic Concepts

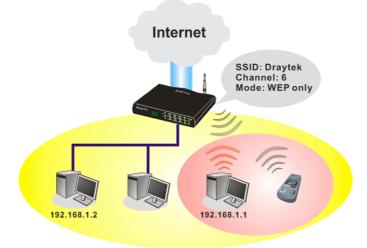
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.



**Note**: \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



### **Security Overview**

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

Wi	reless LAN
₽	General Setup
- 🕨	Security
- Þ	Access Control
₽	Station List

### 3.5.2 General Setup

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

Wireless LAN >> General Setup	

Enable Wireless LAN	
Mode : Mixed(11b+11g+11n) v	
SSID:	DrayTek
Channel :	Channel 6, 2437MHz
Note: The same technology mus	t also be supported in clients to boost WLAN performance.
Hide SSID	
Long Preamble	
Hide SSID: prevent SSID f	rom being scanned. / for some older 802.11b devices only (lowers performance).

Enable Wireless LAN Mode

Check the box to enable wireless function.

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) mode.

Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default

Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the

SSID is "DrayTek". We suggest you to change it.

Mixed(11b+11g+11n) 🎽
11b Only
11g Only
11n Only
Mixed(11b+11g)
Mixed(11g+11n)
Mixed(11b+11g+11n)

SSID

Channel

**Dray** Tek

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	l
	Channel 3, 2422MHz	l
	Channel 4, 2427MHz	l
	Channel 5, 2432MHz	l
	Channel 6, 2437MHz	l
	Channel 7 , 2442MHz	l
	Channel 8, 2447MHz	l
	Channel 9, 2452MHz	l
	Channel 10, 2457MHz	l
	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 <u>s</u> tart up	Disable <u>R</u> adio		
Remember mini status position	Fragmentation Threshold :	2346	
Auto hide mini status	RTS Threshold :	2347	
Set <u>m</u> ini status always on top	Frequency :	802.11b/g/n - 2.4GH 🗙	
Enable IP Setting and Proxy Setting in Profile	Ad-hoc Channel:	1 🗸	
Group Rosming Ad-hoc	Power Save Mode:	Disable 💌	
	Tx Burst :	Disable 🗸	>
WLAN type to connect			
Infrastructure and Ad-hoc network			
O Infrastructure network only			
Ad-hoc network only			
Automatically connect to non-preferred networks			
	OK	Cancel Apply	
		Tippij	
Tx Burst : Dis	able	~	
_	able		
L)15	0.DTC		

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

Enable

### Hide SSID

	see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use <b>Long Preamble</b> if needed to communicate with this kind of devices.

# 3.5.3 Security

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

ity Settings					
Mode:	1	Disable	~		
WPA:					
Encryption Mode:	т	KIP for WPA/AES	for WPA2		
Pre-Shared Key	*(PSK):	*****			
	CII character or 64 r "0x655abcd".	4 Hexadecimal digi	ts leading b	y "0x", for examp	le
WEP:					
Encryption Mod	le:	64-Bit 🗸			
● Key 1 :	*	*****			
<b>Key 2</b> :	*	*****			
<b>○Key 3</b> :	*	****			
		*****			
⊖ Key 4 : For 64 bit WEP key	Ľ	imal digits leading	by "0x" for	evample "AB312"	or
,	er or 10 Hexadeci	cimal digits leading			or
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac	er or 10 Hexadeci	cimal digits leading 86373839414243".			or
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353	cimal digits leading 86373839414243".	) by "0x", fo	r example	
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353	cimal digits leading 6373839414243". Cancel e are several m	) by "0x", fo	r example	
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353 OK There	cimal digits leading 6373839414243". Cancel e are several m	) by "0x", fo	r example ided for you to	
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353 OK There	cimal digits leading 6373839414243". Cancel e are several m	) by "0x", fo	r example ided for you to Disable Disable WEP	
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353 OK There	cimal digits leading 6373839414243". Cancel e are several m	) by "0x", fo	ided for you to Disable WEP WPA/PSK	
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	er or 10 Hexadeci eter or 26 Hexadec 0x3031323334353 OK There	cimal digits leading 6373839414243". Cancel e are several m	) by "0x", fo	r example ided for you to Disable Disable WEP WPA/PSK WPA2/PSK	) choose
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	ter or 10 Hexadeci ox3031323334353 OK There Mode	cimal digits leading 36373839414243". Cancel e are several m e:	odes prov	ided for you to Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WF	o choose PA2)/PSK
For 64 bit WEP key Type 5 ASCII charact "0x4142333132". For 128 bit WEP key Type 13 ASCII charac "0123456789abc" or "	ter or 10 Hexadeci ox3031323334353 OK There Mode	cimal digits leading 6373839414243". Cancel e are several m	odes prov	ided for you to Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WF	o choose PA2)/PSK m.

WPA2/PSK-Accepts only WPA2 clients and the

**Dray** Tek

	encryption key should be entered in PSK. <b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.				
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). <b>Type</b> - Select from Mixed (WPA+WPA2) or WPA2 only. <b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").				
WEP	<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. <b>Four keys</b> can				
	be entered here, but only one key can be selected at a time				

encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

### 3.5.4 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.

Enable Access Con	trol		
·	Policy :	Activate MAC address filter 💌	
	ndex Attribute	MAC Address Filter MAC Address	
	Client's MAC Add		
		: Isolate the station from LAN	
	Add	Delete Edit Cancel	
Enable Access Contr	ol Se	OK Clear All elect to enable the MAC Address access control feature.	
Policy	Ad ad Cl W	elect to enable any one of the following policy. Choose ctivate MAC address filter to type in the MAC dresses for other clients in the network manually. hoose Isolate WLAN from LAN will separate all the LAN stations from LAN based on the MAC Address list policy : Activate MAC address filter Isolate WLAN from LAN	
MAC Address Filter	Di	isplay all MAC addresses that are edited before.	
Client's MAC Addro	ess M	anually enter the MAC address of wireless client.	
Attribute	wi	<b>Isolate the station from LAN -</b> select to isolate the ireless connection of the wireless client of the MAC dress from LAN.	
Add	Ad	dd a new MAC address into the list.	
Delete	De	elete the selected MAC address in the list.	
Edit	Ec	lit the selected MAC address in the list.	
	IntEast the selected MAC address in the list.IncelGive 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.

### 3.5.5 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.

Address
Refresh
ion.
trol.
VPA/PSK authentication.
ects to the router successfully, it may be
In that case, it will still be on the list until the
Add
Click this button to refresh the status of sta
ii v

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

# 3.6 System Maintenance

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

Below shows the menu items for System Maintenance.

System Maintenance	l
System Status	
User Password	
Time and Date	
Reboot System	

### 3.6.1 System Status

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

#### System Status

Model Name	: Vigor 2920 Series
Firmware Version	: 3.3.2_RC2
Build Date/Time	: Sep 2 2009 20:43:53

	LAN		WAN 1
MAC Address	: 00-50-7F-00-00-00	Link Status	: Disconnected
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-00-00-01
1st Subnet Mask	: 255.255.255.0	Connection	: DHCP Client
DHCP Server	: Yes	IP Address	:
DNS	: 168.95.1.1	Default Gateway	:

WAN 2		
Link Status	: Connected	
MAC Address	: 00-50-7F-00-00-02	
Connection	: DHCP Client	
IP Address	: 192.168.5.30	
Default Gateway	: 192.168.5.1	

Wireless LAN		
MAC Address	: 00-50-7F-00-00-00	
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 <sup>st</sup> IP Address	Display the IP address of the LAN interface.
1 <sup>st</sup> 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.

### 3.6.2 User Password

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

System Maintenance >> User Password
User Password
Old Password
New Password
Confirm Password
OK

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

New Password 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.

## 3.6.3 Time and Date

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

System Maintenance >> Time and Date		
Time Information		
Current System Time 2	009 Oct 12 Mon 8 : 18 : 45 Inquire Time	
Time Setup		
O Use Browser Time		
<ul> <li>Use Internet Time Client</li> </ul>		
Server IP Address	pool.ntp.org	
Time Zone	(GMT) Greenwich Mean Time : Dublin	
Enable Daylight Saving		
Automatically Update Inte	erval 30 min 🕶	
Current System Time Use Browser Time	Click <b>Inquire Time</b> to get the current time. Select this option to use the browser time from the remote administrator PC host as router's system time.	
Use Internet Time	Select to inquire time information from Time Server on th Internet using assigned protocol.	
Fime Protocol	Select a time protocol.	
Server IP Address	Type the IP address of the time server.	
Гіте 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.		

## 3.6.4 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 Maintenance >> Reboot System			
Reboot System			
	Do you want to reboot your router ?		
	Osing current configuration		
<u> </u>	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.

## 3.7 Diagnostics

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

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

## 3.7.1 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

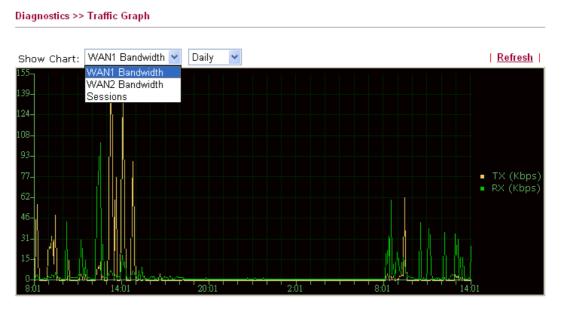
Diagnostics >> View DHCP Assigned IP Addresses

```
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.

## 3.7.2 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.

#### 3.7.3 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

#### **Ping through**

Use the drop down list to choose the WAN interface that you want to ping through or choose **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.

## 3.7.4 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

#### Diagnostics >> Trace Route

Trace Route	
Trace through:	WAN1 💌
Host / IP Address:	Run
Result	Clear
Trace through WAN traceroute to 172 1 Request timed 2 Request timed Trace complete.	2.16.3.229, 30 hops max 4 out. *

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.

This page is left blank.

#### Vigor2920 Series User's Guide

# **4** Admin Mode Operation

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

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

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

Auto Logout 🔽	System Status			
Inline Status	Model Name Firmware Version	: Vigor2920n : 3.3.2		
VAN AN	Build Date/Time	: Dec 11 2009 11:56:23		
IAT		LAN		WAN 1
Firewall Objects Setting CSM Bandwidth Management Applications (PN and Remote Access	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-C9-3B-24 : 192.168.1.1 : 255.255.255.0 : Yes : 4.2.2.1	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-C9-3B-25 : : :
ertificate Management /ireless LAN				WAN 2
System Maintenance Jiagnostics Logout All Rights Reserved.			Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-C9-3B-26 : : :
			Wi	reless LAN
			MAC Address Frequency Domain Firmware Version SSID	: 00-50-7F-C9-3B-24 : Europe : 1.8.1.0 : DrayTek

## **4.1 Internet Access**

**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 **Internet Access** 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, W	AN1 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 on demand:	/ ways on
O WAN2 Fail			
		🔾 WAN1 Fail	
WAN2 Upload spe	eed exceed 0 Kbps	WAN1 Upload spectrum	eed exceed 0 Kbps
WAN2 Download	speed exceed 0 Kbps	WAN1 Download	speed exceed 0 Kbps
1		1	

Enable		settings for this WAN interface. ettings for this WAN interface.
Display Name	Type the description for the	e WAN1/WAN2 interface.
Physical Mode	· • •	onnection is done and fixed through ical connection for WAN2 is done 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.

Interfaces         Interfaces         Interfaces         Interfaces         States         Interfaces         States         Physical Type         You can change the physical type for WAN2 or choose Autonegotiation for determined by the system.         Physical Type:         Auto negotiation         IOM half duplex         100M half duplex         100H half duplex         1		WAN >> Internet Access			
WMR       Externet       Description         Physical Type       You can change the physical type for WAN2 or choose Auto negotiation for determined by the system.         Physical Type:       Auto negotiation Y         Auto negotiation       You Know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance.         Load Balance Mode       If you choose According to Line Speed. Otherwise, please thoose Auto Weigh to let the router reach the best load balance.         Load Balance Mode       If your choose According to Line Speed.         Line Speed       If your choose According to Line Speed         Line Speed       If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is ktps.         Active Mode       Choose Always On to make the WAN connection (WAN1/WAN2) activated if it is necessary.         Active Mode:       Active on demand         Alvarys On Active on demand       Always On Active on demand         Alvays On Active on demand       If you choose Active on demand, the Idle Timeout will be available for you to set for PPPOE and PPTP access modes in the Details Page of WAN>-Internet Access. In addition, there are three selections for you to choose for different purposes.         WAN2 Fail – It means the connection for WAN1 will be       WAN2 Fail – It means the co		Internet Access			
Image       Image <th< th=""><th></th><th></th><th>Physical Mode</th><th>Access Mode</th><th></th></th<>			Physical Mode	Access Mode	
Physical Type       You can change the physical type for WAN2 or choose Auto negotiation for determined by the system.         Physical Type:       Auto negotiation         Auto negotiation       You full duplex         10M half duplex       10M full duplex         10M full duplex       10M full duplex         10A full duplex       10A full duplex					
negotiation for determined by the system.         Physical Type:       Auto negotiation         Auto negotiation       Mathematical Structure         IOM full duplex       IOM full duplex         Iom choose Actoroding to Line Speed       Intersection for		WAN2	3G USB Modem	None	etails Page
Physical Type:       Auto negotiation         Auto negotiation       Nome Not the provided state of the provided state state provided state of the provided state provided state	Physical Type	-		• •	r choose Auto
Auto negotiation 10M half duplex 10M full duplex 100M full duplex 100M full duplex         Load Balance Mode       If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance. Load Balance Mode:         Line Speed       If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.         Active Mode       Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary. Active on demand         Active Mode:       Active on demand         If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be		<b>negotiation</b> fo	r determine	ed by the system.	=
10M half duplex         10M half duplex         100M half duplex         100H half duplex </th <th></th> <th>Physical Typ</th> <th>е:</th> <th>Auto negotiation 🚩</th> <th></th>		Physical Typ	е:	Auto negotiation 🚩	
10M full duplex 100M half duplex 100M full duplexLoad Balance ModeIf you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance. Load Balance Mode:Load Balance Mode:Auto Weigh According to Line SpeedLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary. Active Mode:Active Mode:Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be				Auto negotiation	
100M half duplex 100M full duplexLoad Balance ModeIf you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance. Load Balance Mode:Load Balance Mode:Auto Weigh According to Line SpeedLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand Mode:If you choose Active on demand Always On Active on demandIf you choose Active on demand Mode:If you choose Active on demand Always On Active on demandMathematical Balance Mode:Active on demand Mode:Mathematical Balance Mode:Active on demand Always On Active on demandIf you choose Active on demand the Idle Timeout will be available for you to set for PPOE and PPTP access modes in the Details Page of WAN>-Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be					
100M full duplex         Load Balance Mode       If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance.         Load Balance Mode:       Auto Weigh ▲         Load Balance Mode:       Auto Weigh ▲         Auto Weigh       ▲         According to Line Speed       If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.         Active Mode       Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.         Active Mode:       Active on demand ▲         If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.					
Load Balance ModeIf you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed. Otherwise, please choose Auto Weigh to let the router reach the best load balance. Load Balance Mode:Auto Weigh ImplicationLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be					
please choose the setting of According to Line Speed.         Otherwise, please choose Auto Weigh to let the router reach the best load balance.         Load Balance Mode:       Auto Weigh         Auto Weigh       Auto Weigh         According to Line Speed       If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.         Active Mode       Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.         Active Mode:       Active on demand         Active on demand       If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.         WAN2 Fail – It means the connection for WAN1 will be			. 1		
Otherwise, please choose Auto Weigh to let the router reach the best load balance.Load Balance Mode:Auto Weigh According to Line SpeedLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be	Load Balance Mode				
the best load balance.Load Balance Mode:Auto WeighAuto WeighAuto WeighAccording to Line SpeedIf your choose According to Line Speed as the Load BalanceMode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be					
Auto Weigh According to Line SpeedLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand Malways On Active on demandIf you choose Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be		-		Auto Weigh to let th	le fouter reach
Auto Weigh According to Line SpeedLine SpeedIf your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand Malways On Active on demandIf you choose Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be		Load Balance	e Mode:	Auto Weigh	*
According to Line Speed         Line Speed       If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.         Active Mode       Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.         Active Mode:       Active on demand ✓ Always On Active on demand         If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.         WAN2 Fail − It means the connection for WAN1 will be					
Mode, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.Active ModeChoose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.Active Mode:Active on demand Always On Active on demandIf you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be					peed
<ul> <li>(WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.</li> <li>Active Mode: Active on demand ✓</li> <li>Always On Active on demand</li> <li>If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN&gt;&gt;Internet Access. In addition, there are three selections for you to choose for different purposes.</li> <li>WAN2 Fail – It means the connection for WAN1 will be</li> </ul>	Line Speed	Mode, please	type the lin	e speed for download	ing and
Always On Active on demand If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the <b>Details Page</b> of <b>WAN&gt;&gt;Internet Access</b> . In addition, there are three selections for you to choose for different purposes. <b>WAN2 Fail</b> – It means the connection for WAN1 will be	Active Mode	(WAN1/WAN demand to ma	2) being ac ke the WA	ctivated always; or cho N connection (WAN	oose Active on
Active on demand If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the <b>Details Page</b> of <b>WAN&gt;&gt;Internet Access</b> . In addition, there are three selections for you to choose for different purposes. <b>WAN2 Fail</b> – It means the connection for WAN1 will be		Active Mode:		Active on demand	~
If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the <b>Details Page</b> of <b>WAN&gt;&gt;Internet Access</b> . In addition, there are three selections for you to choose for different purposes. <b>WAN2 Fail</b> – It means the connection for WAN1 will be					
available for you to set for PPPoE and PPTP access modes in the <b>Details Page</b> of <b>WAN&gt;&gt;Internet Access</b> . In addition, there are three selections for you to choose for different purposes. <b>WAN2 Fail</b> – It means the connection for WAN1 will be				Active on demand	
the <b>Details Page</b> of <b>WAN&gt;&gt;Internet Access</b> . In addition, there are three selections for you to choose for different purposes. <b>WAN2 Fail</b> – It means the connection for WAN1 will be					
are three selections for you to choose for different purposes. WAN2 Fail – It means the connection for WAN1 will be					
WAN2 Fail – It means the connection for WAN1 will be					
			•		· ·
activated when wAINZ is failed.					NT WIII be
WAN2 Upload speed exceed XX kbps – It means the					oons the
connection for WAN1 will be activated when WAN2 Upload					
speed exceed certain value that you set in this box for 15					
seconds.		•	, and		
WAN2 Download speed exceed XX kbps– It means the			load speed	exceed XX kbps- It	means the
connection for WAN1 will be activated when WAN2					
Download speed exceed certain value that you set in this box		Download spe	ed exceed o	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 Display Nam	e 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
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 the WAN1/WAN2 that entered in general setup.		
Physical Mode	It shows the physical connection for WAN1 (Ethernet) /WAN2 (Ethernet or 3G USB Modem) according to the real network connection. Physical Mode Physical Mode		
	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 💿 Disable	PPP Authentication PAP or CHAP 😪
ISP Access Setup Username Password Index(1-15) in Schedule Setup: =>,,, WAN Connection Detection Mode ARP Detect  Ping IP TTL: MTU 1442 (Max: 1492)	Idle Timeout -1 second(s) IP Address Assignment Method (IPCP) WAN IP Alias Fixed IP: Yes No (Dynamic IP) Fixed IP Address Default MAC Address Default MAC Address MAC Address: 00 .50 .7F :00 .00 .01

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.

🗿 WAN IP Alias - Microsoft Internet Explorer 📃 🗖 🔀			
WAN II	P 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

**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 <ul> <li>Obtain an IP address automatically</li> </ul>	)
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         Specify an IP address         IP Address	-
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)	Secondary IP Address	
RIP Protocol	<ul> <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>

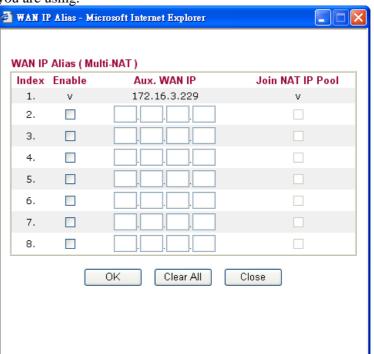
ΟK

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	Obtain an IP address automatically
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 II	WAN IP Alias - Microsoft Internet Explorer		
WAN IP	Alias ( Mu	ılti-NAT )	
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close

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

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End
1		any	*	WAN1 💌						
<u>2</u>		any	*	WAN1 🔽						
<u>3</u>		any	*	WAN1 💌						
<u>4</u>		any	*	WAN1 🔽						
<u>5</u>		any	*	WAN1 💌						
<u>6</u>		any	*	WAN1 🔽						
Z		any	*	WAN1 💌						
<u>8</u>		any	*	WAN1 🔽						
<u>9</u>		any	*	WAN1 💌						
<u>10</u>		any	*	WAN1 🔽						
< <u>1-10</u>	<u>11-20</u> >	•>								Next :

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.

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.

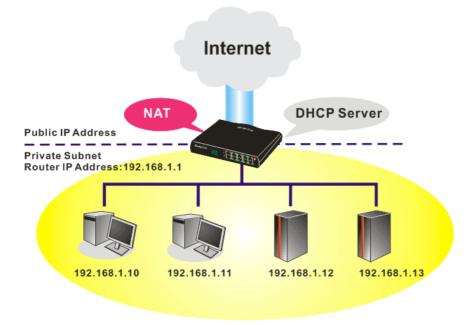
## 4.2 LAN

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.



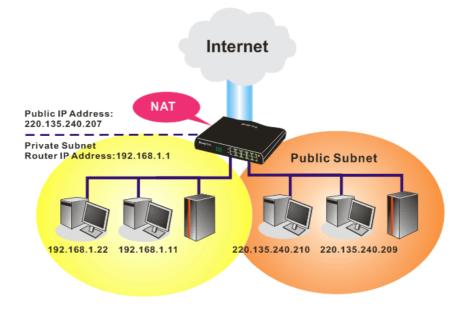
#### 4.2.1 Basics of LAN

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)

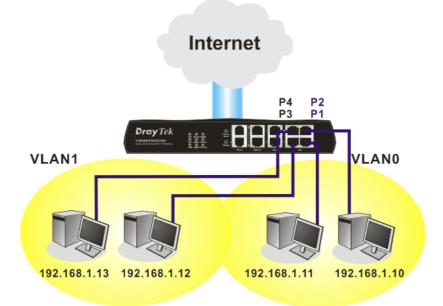
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

#### 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 <sup>nd</sup> IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)				
2 <sup>nd</sup> Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)				
2 <sup>nd</sup> 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 :	
Add Delete Edit Cancel	
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 2<sup>nd</sup> DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2<sup>nd</sup> subnet won't get an IP address belonging to 1<sup>st</sup> 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: 71:47:40
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
		~			~~~~

tatic Route Configuration			Set to Factory Default   View Routing Tab		
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.

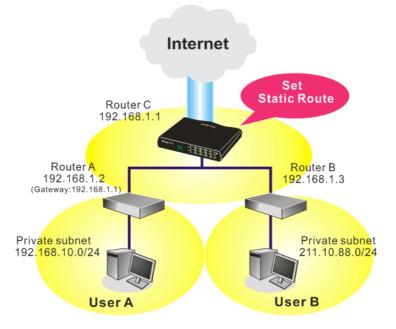
Key: C	- connected, S -	static, R - RIP, * - default, ~ - private	
*	0.0.0/	0.0.0.0 via 172.16.3.1, WAN1	
С~	192.168.1.0/	255.255.255.0 is directly connected,	LAN
С	172.16.3.0/	255.255.255.0 is directly connected, W	AN1

#### 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	AN >> 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.

urrent Runn	ing Routing Table		Re	fresh
Key: C	- connected, S -	static, R - RIP, * - default, ~ - pri	ivate	^
S~	192.168.10.0/	255.255.255.0 via 192.168.1.2, L	IN	
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, LA	NN	

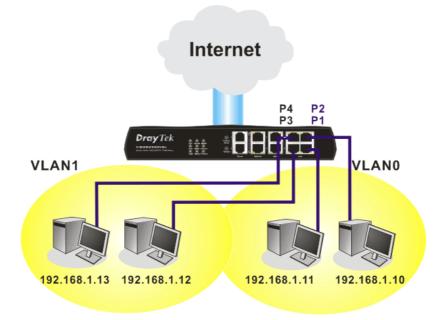
#### 4.2.4 VLAN

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					
	ОК	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           Address         Mac Address	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.
Remove	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Remove</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.

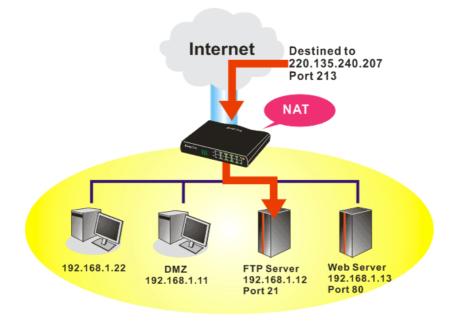
Below shows the menu items for NAT.



#### 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.

OK	Clear	Cancel

Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select <b>Range</b> . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is <b>All</b> which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified <b>Private IP 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



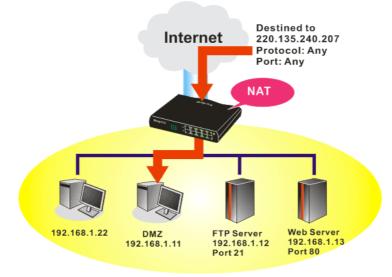
will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

System Maintenance	>> Manag	jement
--------------------	----------	--------

Management Access Control	Management Port Setup			
	💿 User Define Ports 🛛 Default Ports			
<ul> <li>Allow management from the Internet</li> <li>FTP Server</li> <li>HTTP Server</li> <li>HTTPS Server</li> <li>Telnet Server</li> <li>SSH Server</li> </ul>	Telnet Port     23     (Defaulter       HTTP Port     80     (Defaulter       HTTPS Port     443     (Defaulter       FTP Port     21     (Defaulter       SSH Port     22     (Defaulter	:: 80) :: 443] :: 21)		
Disable PING from the Internet           Access List	SNMP Setup Enable SNMP Agent			
List IP Subnet Mask	Get Community public			
	Set Community private     Manager Host IP			
	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

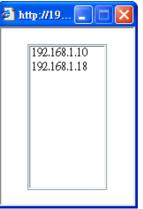
AN 1	
None 🔽	
Private IP	Choose PC
MAC Address of the True IP DM	IZ Host 00 00 00 00 00 00 00 00
	IZ Host 00, 00, 00, 00, 00, 00, 00 ost is turned on, it will force the router's WAN connection to be
Note: When a True-IP DMZ he always on.	
Note: When a True-IP DMZ h	

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	
-----------------------	--

1.		170 16 0 000		
		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>				x
<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.

StatusDisplay the state for the corresponding entry. X or V is to represent<br/>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			P2F	P2P				
WAN Interface				WAN1 V				
	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:

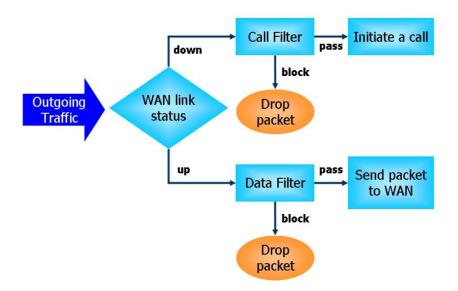
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

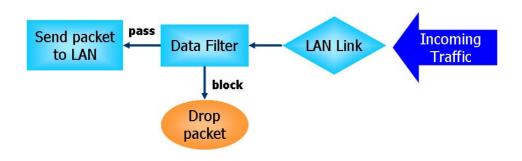
#### **IP Filters**

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.

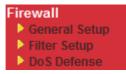
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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 🐱
	🔘 Disable		
Data Filter	Enable	Start Filter	Set Set#2 💌
	🔘 Disable		
Actions for default ru	ile:		
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	comina fraamen	ited UDP or ICMP pac	kets ( for some games, ex.
- Strict Security Cl			
Web-Filter	-		

	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</b> ) for applying with this router. Please

	set at least one profile for choosing in <b>CSM&gt;&gt; URL Content Filter</b> web page first. 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</b> <b>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</b> ) for applying with this router. Please set at least one profile for anti-virus in <b>CSM&gt;&gt; Web Content Filter</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.

http://192.168.1.1/doc/ipfgenady.htm http://192.168.1.1/doc/ipfgenady.htm	n - Windows Internet Explorer		
Firewall >> General Setup			
Advance Setting		)	
Codepage	ANSI(1252)-Latin I	*	
Window size:	65535		
Session timeout:	1440	Minute	
	OK Close		

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

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

📶 DrayTek Syslog 3.9.1		
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 (ANSIADEM - 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 :	Default Call Filter			
Filter Rule	e Active	Comments	Move Up	Move Down
1		Block NetBios		<u>Down</u>
2			<u>UP</u>	<u>Down</u>
3			<u>UP</u>	<u>Down</u>
4			<u>UP</u>	<u>Down</u>
5			<u>UP</u>	<u>Down</u>
6			<u>UP</u>	Down
7			<u>UP</u>	
			Next Filte	r Set 🛛 None 🛛 🛩
		OK Clear Ca	ncel	
Filter Rule		Click a button numbered (1 ~ 7 will open Edit Filter Rule web refer to the following 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.

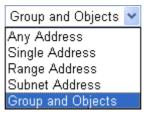
Firewall	>>	Fdit	Filter	Set >>	Fdit	Filter Rule
1 II C WUII		Luit	1 IIICI	361 **	Luit	i niter nuite

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.

Address Type	Group and Objects 💙
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Invert Selection	
<u>IP Group</u>	None 💌
or <u>IP Object</u>	None 💌
or IP Object	None
or IP Object	1-RD Department 2-Financial Dept.
	3-HR Department

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



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

Service Type

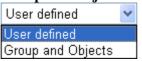
Click **Edit** to access into the following dialog to choose a suitable service type.

Protocol TCP/UDP	
Destination Port	
	5
Service Group None 💌	
or Service Object None 💌	
or Service Object None 1-SIP	
or Service Object <u>2-RTP</u>	

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



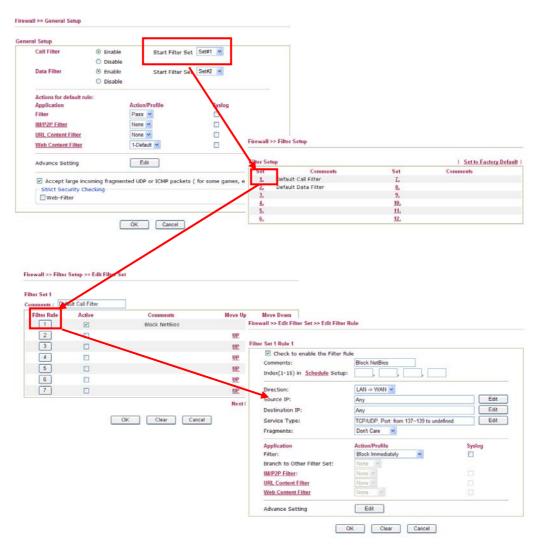
use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



**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. **Branch to other Filter** If the packet matches the filter rule, the next filter rule will branch 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 Web Content Filter profile selected here. For detailed information, refer to the section 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

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

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

Firewall >> DoS defense Setu	ıp			
De Calafanaa Catur				
DoS defense Setup				
Enable SYN flood defense		Threshold	50	packets / sec
		Timeout	10	sec
Enable UDP flood defe	ense	Threshold	150	packets / sec
		Timeout	10	sec
Enable ICMP flood det	fonco	Threshold	50	packets / sec
	ense	Timeout	10	sec
Enable Port Scan det	action	Threshold	150	
Block IP options	sectori	Block TCP flac		packets / sec
Block Land		Block Tear Dro		
Block Smurf	Block Ping of I	•		
Block trace route	Block ICMP fra			
📃 Block SYN fragment		📃 Block Unknowi	- nProtocol	
Block Fraggle Attack				
Enable DoS defer crackers.	nse function to preve	ent the attacks f	irom hackeı	cor
	OK	ar All Cancel	)	
Enable Dos Defense	Check the box to a	activate the DoS	S Defense	Functionality.
Enable SYN flood defense	detecting the Three has exceeded the or randomly discard defined in Timeou packets' attempt to	eshold of the TC defined value, th the subsequent at. The goal for o exhaust the lin reshold and time	P SYN pa ne Vigor r TCP SYN this is pre mited-reso cout value	efense function. Once ackets from the Interne router will start to I packets for a period vent the TCP SYN ource of Vigor router. as are set to 50 packets

- **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 Port Scan attacks the Vigor router by sending lots of packets to



detection	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			
	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

	192.168.1		WAN Sta	Gateway IP (Fixed) 172.16.3.4	Γ	TX Packets 343	TX Rate
TX Packets 4175	RX Pa	ickets 68	Г	WAN IP (Fixed) 172.16.3.229	Γ	RX Packets 2558	RX Rate
vall Log VPN Log Us	er Access Log	Call Log WAN Lo	g Others	Network Information	Net State	Traffic Graph	
an 100:00:42 an 100:00:34	Vigor Vigor	DoS syn_flood B DoS semp_flood I	ock(10s) 19 3lock(10s) 1	2.168.1.115,10605 -> 1 92.168.1.115 -> 192.16	92.168.1. 8.1.1 PR	1,23 PR 6(tep) len (icomp) len 20 60	20 40 -3 394375
i <b>l. Status</b> Mode						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>	
	E   07 120   120 1€0   1€	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

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:	0.0.0.0
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
	For example, the <b>Direction</b> setting in <b>Edit Filter Rule</b> will as you specify IP or IP range for WAN or LAN or any IP address If you choose LAN as the <b>Interface</b> here, and choose LAN as the direction setting in <b>Edit Filter Rule</b> , then all the IP addresses specified with LAN interface will be opened for you to choose in <b>Edit Filter Rule</b> page.
Address Type	<ul> <li>Determine the address type for the IP address.</li> <li>Select Single Address if this object contains one IP address only.</li> <li>Select Range Address if this object contains several IPs with a range.</li> <li>Select Subnet Address if this object contains one subnet for I 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 abo will be applied later while it is chosen.

Below is an example of IP objects settings.

)bjectsSetting >>	> 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.

## 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   33-64   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
C	OK Clear Cancel
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         ICMP       IGMP         IGMP       TCP         UDP       TCP/UDP         Other       0
Source/Destination Port	<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 on 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 (	roup Setup	
Profile Index : 1		
Name:	VoIP	
Available Service Type	Objects Selected Service Type Objects	
1-SIP 2-RTP	With the second seco	
Name	Type a name for this profile.	
Available Service Type Objects	All the available service objects that you have added or <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown this box.	
Selected Service Type Objects	Click >> button to add the selected IP objects in this bo	X.

### 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

ult 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.

Keyword Group Tat	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 ojects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
lected 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	.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.

ofile Index: 1					
ofile Name:					
neck for Disallow:	Select All				
		Advanced	Management		
Activity / Ap	plication	MSN	YahooIM	AIM(<= v5.9)	ICQ
Login	L. C.				
Messa	ge				
File Tran	sfer				
Game					
Video					
Voice	1				
Confere	nce				
Other Acti	ivities				
		M Application			VoIP
AIM6		iChat		er/GoogleTalk	Skype
GoogleChat	XFire	GaduGadu			🗌 Kubao
Qnext	Meetro	POCO/PP3			Gizmo
AliWW	□ KC	Lava-Lav		2	SIP
□iSpQ	UC	MobileMS	N		
	W	eb IM (* = mor	e than one addre	ess)	
WebIM URLs	<u>eMessenger</u> ICQ Java* IMUnitive* MessengerFX*	<u>WebMSN</u> ICQ Flash* Wablet*	<u>meebo*</u> goowy* <u>mabber*</u> tos WebYahoolM	<u>eBuddy</u> <u>IMhaha*</u> <u>MSN2GO*</u>	<u>ILoveIM*</u> getMessenger KooIIM

**Profile Name** 

Type a name for this profile.

120

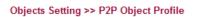


Type a name for such profile and check all the items that not allowed to be used in the host. Finally, click **OK** to save this profile.

### 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

Des Classica de Carto			
Profile Index: 1			
Profile Name:			
Check for Disallow: Select Al			
Protocol		Applications	
SoulSeek	SoulSeek		
eDonkey	eDonkey, eMule	e, Shareaza	
FastTrack	KazaA, BearSha	are, iMesh	
OpenFT	KCeasy, FilePip	e	
Gnutella	BearShare, Lime	ewire, Shareaza, Foxy	
OpenNap	Lopster, XNap,	WinLop	
BitTorrent	BitTorrent, BitS	pirit, BitComet	
Winny	Winny, WinMX,	Share	
	Other P2P	Applications	
Xunlei	🗌 Vagaa	PP365	POCO
Clubbox	Ares	ezPeer	Pando
	ОК С	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.

rofile 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
FeiDian	UUSee	NSPlayer	PCAST	TVKoo
SopCast	UDLiveX	TVUPlayer	MySee	Joost
FlashVideo	SilverLight			
		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.

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.

#### **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.

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

CSM >> IM/P2P Filter Profile

#### **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.

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

CSM >> URL Content Filter Profile

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

OK

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

#### CSM >> URL Content Filter Profile

Profile Name:	
Priority:	Both : Pass V Log: None V
1.URL Access	Control
Enabl	e URL Access Control
Actio	
Pass	Edit
2.Web Feature	•
Enabl	e Restrict Web Feature
Actio	
Pass	Cookie Proxy <u>File Extension Profile:</u> None <u></u>
	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 will be inactive.</li> <li>Either: 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 second Either: Web Feature First –When all 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
Jog	<b>None</b> – There is no log file will be recorded for this profile. <b>Pass</b> – Only the log about Pass will be recorded in Syslog.

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, the more efficiently the Vigor router perform.

Group/Object Edit - Windows Internet Explorer	
http://192.168.1.1/doc/cfkwgob.htm	
Object/Group Edit	
Keyword Object	None 🕶
or Keyword Object	None 💌
or Keyword Object	None 💌
or Keyword Object	None 💌
or Keyword Object	None 🕶
or Keyword Object	None 💌
or Keyword Object	None 💌
or Keyword Object	None 💌
or <u>Keyword Group</u>	None 🕶
or Keyword Group	None 🕶
or Keyword Group	None 💌
<u> </u>	
ОК	Close

#### Web Feature

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

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

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

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

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

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

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

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

CSM >> 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.

etup Query Server	auto-selected		Find more
Setup Test Server	auto-selected		Find more
est a site to verify w	hether it is categorized		
Veb Content Filter Pro	ofile Table:		Set to Factory Defau
/eb Content Filter Pro Profile	ofile Table: Name	Profile	<u>Set to Factory Defat</u> Name
		Profile <u>5.</u>	
Profile	Name		
<u>1.</u>	Name	<u>5.</u>	

Administration Message (Max 255 characters)

<pre>(body&gt;<center> &gt; &gt; <br< th=""></br<></center></pre>
(br>that is categorized with %CL% has been blocked by %RNAME% Web Content
Filter.Please contact your system administrator for further
information.

OK
----

**Setup Query Server** It is recommend for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.

Setup Test Server It is recommend for you to use the default setting, auto-selected. By the way, you can click the link of Test a site to verify whether it is categorized to access into the test server selected.

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



CSM >> Web Content Filter Pro	file
-------------------------------	------

Profile Index: 1 Profile Name: Default			Log: Block 🛩
Black/White List Enable Action: Block	Gr	oup/Object Selections	Edit
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	

Black/White List	<ul> <li>Enable – Check this box to enable the filtering mechanism with the 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>
Action	<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>
Log	<ul> <li>None – There is no log file will be recorded for this profile.</li> <li>Pass – Only the log about Pass will be recorded in Syslog.</li> <li>Block – Only the log about Block will be recorded in Syslog.</li> </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.

Bandwidth Manager	nent
Sessions Limit	
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

🔘 Enab	le 💿 Disable					
Default N	1ax Sessions: 100					
Limitatio	n List					
Index	Start IP	End	IP	Max	Sessions	
Start IP:	imitation		End IP:			
		Add	Edit	elete		
e Schedule						
Index(1-15) ir	n <u>Schedule</u> Setup	:	,,	,		
Note: Action a	and Idle Timeout s	ettings w	ill be ignore	d.		

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 t	to 2nd Subnet 🔘 Disable
Default TX Limit: 200	Kbps Default RX Limit: 800 Kbps
Allow auto adjustm	nent to make the best utilization of available bandwidth.
Limitation List	
Index Start IP	End IP TX limit RX limit Shared
Constilia Limitation	
Specific Limitation	
Start IP:	End IP:
⊙ Each 🔘 Shared	TX Limit: Kbps RX Limit: Kbps Add Edit Delete
chedule	
c <mark>hedule</mark> dex(1-15) in <u>Schedule</u> Se	tup:,,,

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

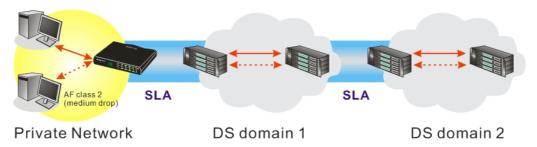


• Scheduling: Based on classification of service level to assign packets to queues and associated service types

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**

Bandwidth Management >> Quality of Service

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.

I Deve devidable	
d Bandwidth	10000 Kbps
Class Name	Reserved_bandwidth Ratio
	25 %
	25%
	25 %
Others	25 <b>%</b>
ıtrol	Limited_bandwidth Ratio 25 %
ze	Online Statistics
<b>OUT</b> -apply to outgoin <b>BOTH-</b> apply to both Check this box and cli	•
For example, if your A	e connecting rate of data input for WAN ADSL supports 1M of downstream and e set 1000kbps for this box. The defaul
	e connecting rate of data output for WA ADSL supports 1M of downstream and e set 256kbps for this box. The default
	Others The factory default for Please also define whi apply to. IN- apply to incoming OUT-apply to outgoin BOTH- apply to outgoin BOTH- apply to both Check this box and cli will see the Online St It allows you to set the For example, if your A 256K upstream, please value is 10000kbps. Ith It allows you to set the

Vigor2920 Series User's Guide



Reserved Bandwidth Ratio	reserv	ed ba	ndwidth	roup index in the to upstream spe tream speed.		
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.					
Outbound TCP ACK Prioritize	The difference in bandwidth between download and up are great in ADSL2+ environment. For the download s might be impacted by the uploading TCP ACK, you ca check this box to push ACK of upload faster to speed to network traffic.				speed can	
Limited_bandwidth Ratio	The rat	• •	ped here is	s reserved for lin	nited bandwidtl	n of UDP
Online Statistics	referen	ice.	online stat ent >> Quality of	istics for quality	of service for y	/our
	WAN1 Onli	ne Statisti	cs	Refresh Inte	rval: 5 💌 seconds	<u>Refresh</u>
			Class Name Re	served-bandwidth Ratio O		ytes/sec)
	1	OUT		25%	0	
	2	OUT OUT		25% 25%	0	
	4	OUT	Others	25%	0	
			Outbo	ound Status		

## 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.

Other

10 (Bps)

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

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setu</u>
Class Ru Inde		N	ame				Rule	Service	Tuno
	0		unic				Edit	Scivice	type
Class	1						Ean		
	-						Edit	Edit	

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



#### Bandwidth Management >> Quality of Service

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 <b>Single Address</b> , you have to fill in Start IP address.				
	For <b>Range Address</b> , you have to fill in Start IP address and				
	End IP address.				
	For <b>Subnet Address</b> , you have to fill in Start IP address and				
	Subnet Mask.				
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with				
	QoS control.				

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

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.

lass In	lex #1				
lame	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

ser 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 Configurat	DN
Туре	💿 Single i 🔘 Range
Port Num	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.

# 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

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

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	6 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.
	(1, 1, 2, 3, 4)

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.

## 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>	×
<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

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	
Weekdays	
🗌 Sun 🔽 Mon 🔽	Tue 🔽 Wed 🔽 Thu 🔽 Fri 🔲 Sat

Clear

Cancel

ΟK

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. How often -Specify how often the schedule will be applied Once -The schedule will be applied just once Weekdays -Specify which days in one week should perform the schedule.

#### Example

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



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

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

## 4.8.3 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 Pc	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.

ress 🔕 Network Connections	Contraction of Contraction	📲 IP Broadband Conr	ection on Route	er Status [?]
Vetwork Tasks         Image: Create a new connection           Image: Set up a home or small office network         Image: Create a new connection	Broadband hinet Disconnected WAN Miniport (PPPOE)	General		C
divite official	Dial-up	Status: Duration:		Connected 00:19:06
ee Also 🔹	test Disconnected	Speed:		100.0 Mbps
Other Places         Image: Control Panel           Omega Control Panel         My Network Places	Internet Gateway IP Broadband Connection on Router	<b>O</b>	ernet Gateway - 🥰	My Computer
My Documents My Computer	Enabled	Packets: Sent: Received:	404 1,115	734 666
Details 🛞	Local Area Connection Enabled Realtek RTL8139/810x Family	Properties Dis	able	Close

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



eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
🧐 IP Broadband Connection on Router	Services
his connection allows you to connect to the Internet through a hared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>☑ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>☑ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>☑ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>
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 P	roxy 🛛 🛛 🗸 🗸					
	to act as a multicast pro y multicast group. But th	·			· · · ·	
Enable IGMP S	nooping					
	nooping, multicast traffic mooping, multicast traffic					
	C	OK Can	cel			
					Refrest	
	t Groups					
Working Multicas	c oroups					

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.
	and the second in a second contract of the second second second

**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	Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the corre MAC address of the host in MAC Address boxes. If you ch Wake by IP Address, you have to choose the correct IP add	
	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
```

Wa	ke	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	
Remote Access Control	
PPP General Setup	
IPSec General Setup	
IPSec Peer Identity	
Remote Dial-in User	
LAN to LAN	
Connection Management	

## 4.9.1 Remote Access Control

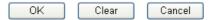
Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

VPN and Remote Access >> PPP General Setup

Remote Access Control Setup	
	Enable PPTP VPN Service
	Enable IPSec VPN Service
	Enable L2TP VPN Service
	Enable ISDN Dial-In

**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.



## 4.9.2 PPP General Setup

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

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

**Dial-In PPP** 

Select this option to force the router to authenticate dial-in

**Dray** Tek

Authentication PAP Only	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) Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. 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 User Name and Password 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.

## 4.9.3 IPSec General Setup

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

There are two phases of IPSec.

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



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

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

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General S Dial-in Set up for Remot		Dynamic IP Client (LAN to LAN).	
IKE Authenticatio		, , ,	
Pre-Shared Key		••••	
Confirm Pre-Shar	ed Key	••••	
IPSec Security M	ethod		
🗹 Medium (AH)			
Data will be a	authentic, but will	not be encrypted.	
High (ESP)	🗹 DES 🛛 🗹 3DES	S 🗹 AES	
Data will be e	encrypted and aut	hentic.	

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

Vigor2920 Series User's Guide



# **4.9.4 IPSec Peer Identity**

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

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

		-			_	
VPN an	d Remote	Access	>>	IPSec	Peer	Identity

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

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 accept the peer with matching value. The field includes <b>Country</b> ( <b>C</b> ), <b>State</b> ( <b>ST</b> ), <b>Location</b> ( <b>L</b> ), <b>Organization</b> ( <b>O</b> ), <b>Organization</b> <b>Unit</b> ( <b>OU</b> ), <b>Common Name</b> ( <b>CN</b> ), and <b>Email</b> ( <b>E</b> ).			

## 4.9.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

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>	???	x

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

Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

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

Index No. 1						
User account and Authentica	tion	Username	???			
Enable this account		Password				
Idle Timeout 3	second(s)					
Allowed Dial-In Type		IKE Authentication Method				
		Pre-Shared Key				
ISDN		IKE Pre-Shared Key				
✓ IPSec Tunnel		Digital Signature(X.50	9)			
L2TP with IPSec Policy	None 🗸	None 🗸				
Specify Remote Node		IPSec Security Method ✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES				
Remote Client IP or Peer IS	DN Number					
or Peer ID		Local ID (optional)				
	• Pass O Block					
5						
	ОК	Clear Cancel				
Enable this account		to enable this function.				
		If the dial-in user is idle				
		outer will drop this conn	ection. By default, the			
	Idle Timeout is	s set to 300 seconds.				
PPTP Allow the rep		ote dial-in user to make				
	6	ernet. You should set the	e User Name and			
	Password of re	mote dial-in user below				
PSec Tunnel		ote dial-in user to make	an IPSec VPN			
	connection thro	ough Internet.				
L2TP			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.				
		Apply the IPSec policy	first, if it is applicable			
		ion. Otherwise, the dial-in VPN connection				
	-	ure L2TP connection.				
	L2TP connecti	the IPSec policy to be d	efinitely applied on the			
Specify Remote Node		ckbox-You can specify				
		remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).				
		<b>heckbox-</b> This means the	e connection type you			
		ill apply the authenticati				
		general settings.	<b>-</b>			
Netbios Naming Packet	<b>Pass</b> – Click it	to have an inquiry for d	ata transmission betwee			
		ed on both sides of VPN				
		there is conflict occurre				
	both sides of V	PN Tunnel in connectin	g, 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.

**Dray** Tek

## 4.9.6 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

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

AN-to-LAN Pr	ofiles:			Set to Fac	tory Default
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	Х	<u>17.</u>	???	Х
<u>2.</u>	???	х	<u>18.</u>	???	х
<u>3.</u>	???	Х	<u>19.</u>	???	Х
<u>4.</u>	???	х	<u>20.</u>	???	х
<u>5.</u>	???	Х	<u>21.</u>	???	Х
<u>6.</u>	???	Х	<u>22.</u>	???	х
<u>7.</u>	???	Х	<u>23.</u>	???	Х
<u>8.</u>	???	х	<u>24.</u>	???	х
<u>9.</u>	???	Х	<u>25.</u>	???	Х
<u>10.</u>	???	х	<u>26.</u>	???	х
<u>11.</u>	???	Х	<u>27.</u>	???	Х
<u>12.</u>	???	х	<u>28.</u>	???	х
<u>13.</u>	???	Х	<u>29.</u>	???	Х
<u>14.</u>	???	х	<u>30.</u>	???	х
<u>15.</u>	???	Х	<u>31.</u>	???	Х
<u>16.</u>	???	Х	<u>32.</u>	???	х

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

???	Call Direction 💿 Both	🔘 Dial-Out 🔘 Dial-in
Enable this profile		
	Idle Timeout	300 second(s)
/AN1 First ⊻	Enable PING to keep a	live
● Pass ○ Block	PING to the IP	
I	Link Type	64k bps 😒
	Username	???
	Password	
	PPP Authentication	PAP/CHAP 🗸
None 🔽	VJ Compression	● On ○ Off
/PN. k.com or 123.45.67.89)	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>	Authentication
		/
	/AN1 First  Pass O Block  vy None	Always on Idle Timeout Enable PING to keep a PING to the IP Link Type Username Password PPP Authentication VJ Compression 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

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

Check here to activate this profile.

**VPN Dial-Out Through** 

**Enable this profile** 

Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.



**WAN1 First** - 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	<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.
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> .
<b>IPSec Security Method</b>	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: 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 MD5 or SHA-1 authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm. 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 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:
	Mby/19216311/ModZTLrbCham     KE advanced settings     KE phase 1 mode @ Main mode @ Aggressive mode     KE phase 2 proposal EES_MD5_G1     KE phase 2 proposal (000 ~ 86400)     KE phase 2 key Metime 5000 (000 ~ 86400)     Perfect Forward Secret @ Disable     Cose  KKE phase 1 mode -Select from Main mode and Aggressive

**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          ISDN         PPTP         IPSec Tunnel         L2TP with IPSec Policy         Specify ISDN CLID or Remote VPN Gateway         Peer ISDN Number or Peer VPN Server IP         or Peer ID		Username ??? Password VJ Compression  On Off 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	
4. TCP/IP Network Setting	S		
My WAN IP Remote Gateway IP Remote Network IP	0.0.0.0 0.0.0.0 0.0.0.0	RIP Direction From first subnet to ren do	Disable 💙 note network, you have to Route 💙
Remote Network Mask	255.255.255.0 More	Change default rout single WAN supports th	te to this VPN tunnel ( Only is )

#### Allowed Dial-In Type

Determine the dial-in connection with different types.

**Dray** Tek

PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	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 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, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.			
Remote Gateway IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.			
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.			
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.			
	Profile Index :1          Remote Network         Netwask         255.255.255 / 32         Add			
	Profile Index :1  Remote Network  Network IP  Netmask  255.255.255.755 / 32			
RIP Direction	Profile Index :1  Remote Network  Network IP  Netmask  255.255.255.732  Add Delete Edit  OK Close			
RIP Direction From first subnet to remote network, you have to do	Profile Index :1         Network IP         Netmask         255.255.255.255.732         Add         Delete         Edit         OK         Close         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			



# 4.9.7 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >>	Connection Manage	ement				
Dial-out Tool				Refres	h Seconds	5 : 10 🗸 Refresh
			*	Dial		
VPN Connection Status Current Page: 1					Page N	No. GO >>
VPN Type Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-					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 tl	he whole	connecti	ion status.

**Dray** Tek

# 4.10 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.



## 4.10.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration					
Name	Subject	Status	Modify		
Local			View Delete		
GENERATE X509 Local	IMPORT REFRESH				
			<u>^</u>		
			~		
L					

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 🔽
Key Size	1024 Bit 😪

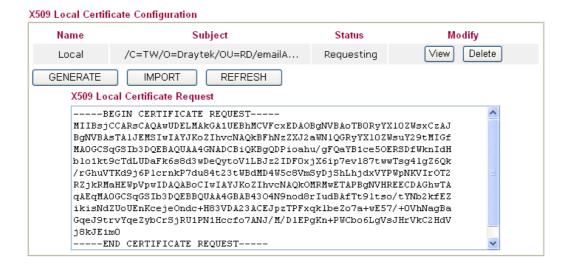
Generate

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:



Certificate Management >> Local Certificate

#### Vigor2920 Series User's Guide

# 4.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

#### X509 Trusted CA Certificate Configuration

 	View Delete
 	View Delete
 	View Delete

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate
Select a trusted CA certificate file.
Browse.,
Click Import to upload the certification.
Import Cancel

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

🖉 Сет	tificate Information - Windows Inter	net Explorer	
🦲 http	://192.168.1.1/doc/XCaCfVi1.htm		<
			^
	Certif	icate Detail Information	
	Certificate Name:	Trusted CA-1	
	Issuer:	<u>^</u>	
	Subject:		Ξ
	Subject Alternative Name:		
	Valid From:		
	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 Mana	agement >> Certificate Backup
Certificate Back	up / Restoration
Backup	Encrypt 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 Wireless LAN

This function is used for "n" models only.

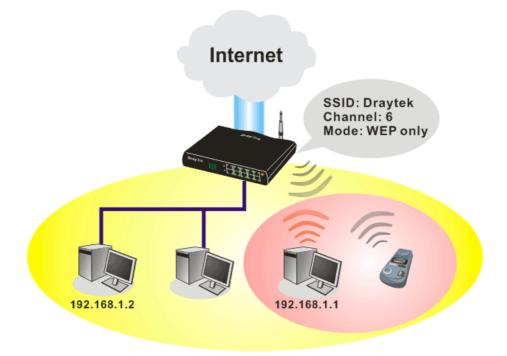
## 4.11.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps\*. Hence, you can finally smoothly enjoy stream music and video.

**Note:** \* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The General Settings will set up the information of this wireless network, including its SSID as identification, located channel etc.



## **Multiple SSIDs**

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.

## **Security Overview**

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/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
- Þ	WPS
- Þ	WDS
⊳	Advanced Setting
⊳	WMM Configuration
⊳	AP Discovery
⊳	Station List

# 4.11.2 General Setup

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

Wireless LAN >> General Setup

ble Wireless	LAN				
Mode :		Mixed(11b+11g	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 <sup>™</sup> 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 <sup>™</sup> 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 <sup>TM</sup> 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 <sup>™</sup> 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 <sup>TM</sup> 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**).

rigor not ouz.trit whereas uso Anapier onniy			
Configuration Status Option About General Setting Auto launch when Windows gtart up Remember mini status position Auto hide mini status Set mini status advays on top Enable IP Setting and Proxy Setting in Profile Group Rosming Ad-hoc WLAN type to connect	Advance Setting Disable Radio Fragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Power Save Mode: Tx Eurst :		46
Infrastructure and Ad-hoc network     Infrastructure network only     Ad-hoc network only     Automatically connect to non-preferred networks		Cancel Ap	oply
Tx <u>B</u> urst : Disab Disab Enab	le		

	<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.
	<ul> <li>Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.</li> <li>Download – Type the transmitting rate for data download. Default value is 30,000 kbps.</li> </ul>

# 4.11.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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(	PSK):	*****
	Type 8~63 ASC: "cfgs01a2" or		r 64 Hexadecimal digits leading by "0x", for example .".
WEP:			
	Encryption Mode	9:	64-Bit 💌
	⊙Key 1 :		****
	○Key 2 :		****
	○Key 3 :		******
For 64	OKey 4 : bit WEP key		****
Type "0x41 <mark>For 12</mark> Type	bit WEP key 5 ASCII characte 42333132". 8 bit WEP key 13 ASCII charact	ter or 26 Hexa	ecimal digits leading by "0x", for example "AB312" or decimal digits leading by "0x", for example 3536373839414243".
Type "0x41 <mark>For 12</mark> Type	bit WEP key 5 ASCII characte 42333132". 8 bit WEP key 13 ASCII charact	er or 26 Hexa x30313233343	lecimal digits leading by "Ox", for example "AB312" or Idecimal digits leading by "Ox", for example
Type "0x41 <mark>For 12</mark> Type	bit WEP key 5 ASCII characte 42333132". 8 bit WEP key 13 ASCII charact	er or 26 Hexa x30313233343	lecimal digits leading by "Ox", for example "AB312" or Idecimal digits leading by "Ox", for example 3536373839414243".
Type "0x41 <b>For 12</b> Type "0123	bit WEP key 5 ASCII characte 42333132". 8 bit WEP key 13 ASCII charact	er or 26 Hexa x30313233343	lecimal digits leading by "0x", for example "AB312" or Idecimal digits leading by "0x", for example 3536373839414243". OK Cancel re are several modes provided for you to choose.

should be entered in WEP Key.

key should be entered in PSK.

WPA/PSK-Accepts only WPA clients and the encryption

WPA2/PSK-Accepts only WPA2 clients and the



	encryption key should be enter <b>Mixed (WPA+ WPA2)/PSK</b> clients simultaneously and the entered in PSK.	- Accepts WPA and WPA2
WPA	The WPA encrypts each fram using the key, which either PS manually in this field below of via 802.1x authentication. Eit such as 012345678(or 64 Hes such as "0x321253abcde"). <b>Type</b> - Select from Mixed (W <b>Pre-Shared Key (PSK)</b> - Eit such as 012345678(or 64 He 0x, such as "0x321253abcde")	SK (Pre-Shared Key) entered or automatically negotiated her <b>8~63</b> ASCII characters, cadecimal digits leading by 0x, /PA+WPA2) or WPA2 only. her <b>8~63</b> ASCII characters, exadecimal digits leading by
WEP	<ul> <li>64-Bit - For 64 bits WEP key such as 12345 (or 10 hexadec such as 0x4142434445.)</li> <li>128-Bit - For 128 bits WEP k characters, such as ABCDEF hexadecimal digits leading by 0x4142434445464748494A4.</li> </ul>	imal digitals leading by 0x, ey, either <b>13</b> ASCII GHIJKLM (or 26 v 0x, such as
	Encryption Mode:	64-Bit 64-Bit 128-Bit
	All wireless devices must sup encryption bit size and have t be entered here, but only one The keys can be entered in AS	port the same WEP he same key. <b>Four keys</b> can key can be selected at a time.

## 4.11.4 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

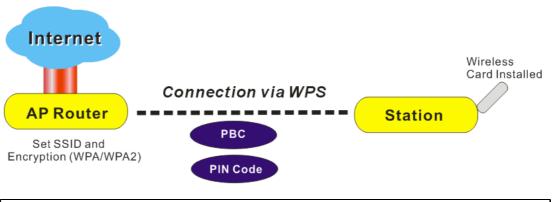
#### Access Control

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.

# 4.11.5 WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

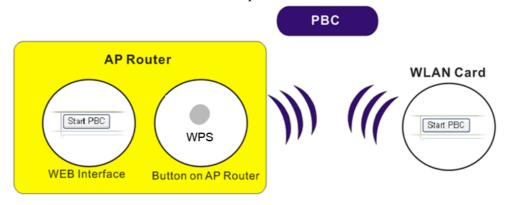


Note: Such function is available for the wireless station with WPS supported.

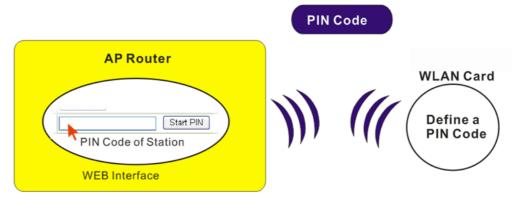
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of 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	't 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.



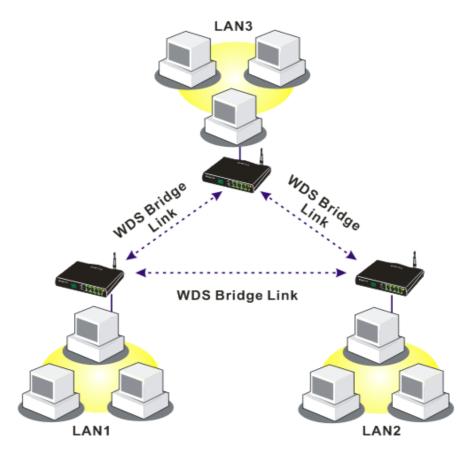
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

# 4.11.6 WDS

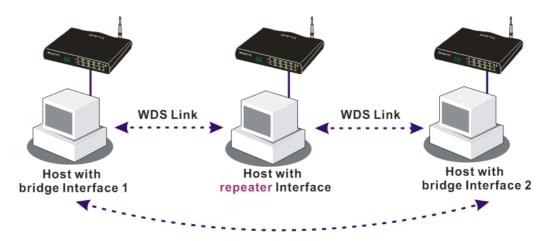
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

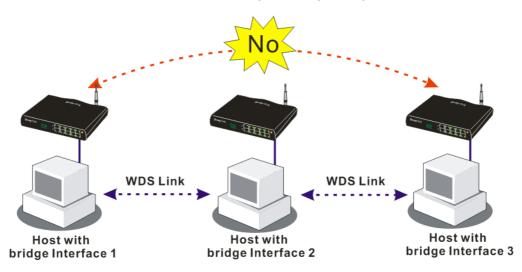


The application for the WDS-Repeater mode is depicted as below:



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

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



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

#### 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 Security	Note: Disable unused links to get better performance.
<u>Settings</u>		performance.
		Repeater
Pre-shared Key:		Enable Peer MAC Addess
Туре : ТКІР		
Key :		
Type 8~63 ASCII character	rs or 64 bevaderimal	
digits leading by "Ox", for ex	ample "cfgs01a2" or	
"0x655abcd".		
		Access Point Function:
		Enable     Oisable
		Status:
		Send "Hello" message to peers.
		Link Status
		Note: The status is valid only when the peer also supports this function.
1		1
	ОК	Cancel
M - J -	Character (ha	<b>Disclusion</b>
Mode		e mode for WDS setting. <b>Disable</b> mode will not 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	<u>×</u>
	Disable	
	Bridge	
	Repeater	
Security	There are t	hree types for security, <b>Disable</b> , <b>WEP</b> and
security		<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	-	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.

# 4.11.7 Advanced Setting

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

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.</li> <li>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>

# 4.11.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC\_BE, AC\_BK, AC\_VI and AC\_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency.

WMM Configura	tion				Set to	Factory Default
WMM Capable		<ul> <li>Enable</li> </ul>	O 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

	ОК
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
APSD Capable	The default setting is <b>Disable</b> .
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data

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

# 4.11.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover 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	WDS Settings :			
AP's MA	.C address	: ::::		
Add t	:0	💽 Bridge	○ Repeater	

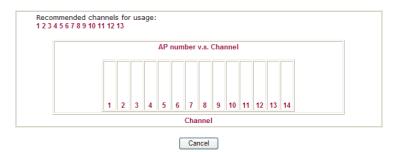
Wireless LAN >> Access Point Discovery

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.

# 4.11.10 Station List

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

Station List	Status MAC Addroce
	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.
	<b>Note</b> : 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
efresh	Click this button to refresh the status of station list.
dd	Click this button to add current typed MAC address

Wireless LAN >> Station List

# Access Control.

# 4.12 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

# 4.12.1 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.

Model Name	: Vigor 2920 Series
Firmware Version	: 3.3.2 RC2
Build Date/Time	: Sep 2 2009 20:43:53

LAN		WAN 1		
MAC Address	: 00-50-7F-00-00-00	Link Status	: Disconnected	
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-00-00-01	
1st Subnet Mask	: 255.255.255.0	Connection	: DHCP Client	
DHCP Server	: Yes	IP Address	:	
DNS	: 168.95.1.1	Default Gateway	:	

Link Status	: Connected
MAC Address	: 00-50-7F-00-00-02
Connection	: DHCP Client
IP Address : 192.168.5.30	
Default Gateway	: 192.168.5.1

WITCHESS LAN				
MAC Address	: 00-50-7F-00-00-00			
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.		
Build Date/TimeDisplay the date and time of the current firmw			
<b>ADSL Firmware Version</b> Display the ADSL firmware version.			
LAN			
MAC Address	Display the MAC address of the LAN Interface.		
1 <sup>st</sup> IP Address	Display the IP address of the LAN interface.		
1 <sup>st</sup> 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.

# 4.12.2 TR-069

System Maintenance >> TR-069 Setting

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 and CPE Settings			
ACS Server On	Internet 💌		
ACS Server			
URL			
Username			
Password			
CPE Client			
○ Enable			
URL	http://192.168.5.30:8069/cwm/CRN.html		
Port	8069		
Username	vigor		
Password			
Periodic Inform Settings			
O Disable			
<ul> <li>Enable</li> </ul>			
Interval Time	900 second(s)		
	OK		
ACS Server On	Choose the interface for the router connecting to ACS server.		
ACS Server	<b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.		
CPE Client	It is not necessary for you to type them. Such information is useful for Auto Configuration Server. <b>Enable/Disable</b> – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.		
Periodic Inform Settings	<b>The default setting is Enable.</b> Please set interval to or schedule time for the router to send notification		

CPE. Or click **Disable** to close the mechanism of notification.

# 4.12.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator P	assword Setup		
Administrator Password			
Old Password	••••		
New Password	•••••	]	
Confirm Password	•••••	]	
	OK		
Old Password	Type in the old password. The factory default setting f password is <b>"admin"</b> .		
New Password	Type in new password in this field.		
Confirm Password	Type in the new passwo	rd again.	

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

# 4.12.4 Configuration Backup

#### **Backup the Configuration**

Follow the steps below to backup your configuration.

System Maintenance >> Configuration Backup

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

Restoration	
	Select a configuration file.
	Browse
	Click Restore to upload the file. Restore
Backup	
	Click Backup to download current running configurations as a file.
	Backup Cancel

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

File Dov	vnload 🗙
?	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  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		~	0 Ø	📂 🛄 •	
My Recent Documents Desktop My Documents	My Documents My Computer My Network Pla RVS-COM Lite Annex A MWSnap300 TeleDanmark Tools config v2k2_232_conl	fia 1				
My Computer	File name:	config			<b>v</b>	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	nance >> Configuration Backup
Configuration	Backup / Restoration
Restoration	
	Select a configuration file. Browse.,
	Click Restore to upload the file. Restore
Backup	
	Click Backup to download current running configurations as a file. Backup Cancel

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

# 4.12.5 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.

System Maintenance >> S	ysLog / Mail Alert Setup
-------------------------	--------------------------

SysLog Access Setup		Mail Alert Setup	
🗹 Enable		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 inform	nation	✓ IM-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.

		192.168.1.1 Vigor series	WAN Statu Ga	is ateway IP (Fixed)	TX Packets	TX Rate
N Status TX Pac		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
ewall Log VPN On Line Routers		ess Log Call Log	WAN Log Others	Network Information Ne	t State	
IP Address	Mask	MAC	NIC Description:	SiS 900-Based F	CI Fast Ethernet Adapt	er - Packet Sc 🗸
192.168.1.1	255.255.2	00-50-7F-54-6	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
			IP Address: Subnet Mask:	192.168.1.10 ¥ 255.255.255.0	DHCP Server: Lease Obtained:	192.168.1.1 Mon Jan 22 01:28:23 2007
	Refresh	>				Mon Jan 22

# 4.12.6 Time and Date

System Maintenance >> Time and Date

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

urrent System Time	2007 O	ct 17 Wed 8 : 3 : 19 Inquire Time
ıp		
) Use Browser Time		
) Use Internet Time Cl	ient	
Time Protocol		NTP (RFC-1305) 🔽
Server IP Address		pool. ntp. org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Savin	g	
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.	

## 4.12.7 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 Setur	)	
Allow management from the Internet		💿 User Define Ports	O Default Ports	
<ul> <li>Allow management from the internet</li> <li>FTP Server</li> <li>HTTP Server</li> <li>HTTPS Server</li> <li>Telnet Server</li> </ul>		Telnet Port	23 (Default: 23)	
		HTTP Port	80 (Default: 80)	
		HTTPS Port	443 (Default: 443)	
		FTP Port	21 (Default: 21)	
SSH Server			22 (Default: 22)	
Disable PING from the Internet				
		SNMP Setup		
Access List List IP Subnet Mask		Enable SNMP Ager		
	*	Get Community	public	
2	~	Set Community	private	
3		Manager Host IP		
		Trap Community	public	
		Notification Host IP		
		Trap Timeout	10 seconds	
			10 seconds	
Allow management from the nternet	login provi	from the Internet. ' ded by the system t	allow system administrat There are several servers to allow you managing th eck the box(es) to specify	e
Disable PING from the Internet			ect all PING packets from the time of time	
Access List	login maxii	from a specific hos mum of three IPs/su IP - Indicate an IP a	he system administrator of st or network defined in t ubnet masks is allowed. address allowed to login	he li



Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
Enable SNMP 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.

## 4.12.8 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.

# 4.12.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is ftp.DrayTek.com.

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.

System Maintena	ance >> Firm	ware Upgrade
-----------------	--------------	--------------

Web Firmware Upgrade
Select a firmware file.
Browse
Click Upgrade to upload the file. Upgrade
TFTP Firmware Upgrade from LAN
Current Firmware Version: 3.3.2_RC1b
Firmware Upgrade Procedures:
1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
<ol> <li>Check that the firmware filename is correct.</li> <li>Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.</li> </ol>
<ol> <li>After the upgrade is compelete, the TFTP server will automatically stop running.</li> </ol>
Do you want to upgrade firmware ? OK

Click OK. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade				
TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.				

For the detailed information about firmware update, please go to Chapter 5.



# 4.13 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 Ta	ble
Data Flow Monito	r
Traffic Graph	
Ping Diagnosis	
Trace Route	

# 4.13.1 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 Triggered Packet Header	<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 C0 A8 01 0A A8 5F 01 01 05 CB 00 35-00 37 E3 91 01 74 01 00	
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.

# 4.13.2 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.

# 4.13.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

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

## 4.13.4 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.

DUICE IE	Assignment Table			<u>Ref</u>	resh
DHCP se Index 1	erver: Running IP Address 192.168.1.10	MAC Address 00-0E-A6-2A-D5-A1	Leased Time 0:00:02.630	HOST ID ok-lccgjyiy075u	
ıdex		It displays	the connection ite	em number.	~
P Addr	ess	It displays specified P		signed by this router	for
	ddress		the MAC address gned IP address f	s for the specified PC for it.	tha
IAC A					
IAC A eased '	Time		the leased time of	f the specified PC.	

4.13.5 NAT Sessions Table

Refresh

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

Diagnostics >> NAT Sessions Table

92.168.1.11 2	:491	52078	24.9.93.18	9 443	 WAN1	
92.168.1.11 2	:493	52080	207.46.25.3	2 80	WAN1	
92.168.1.10 3	8079	52665	207.46.5.1	0 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.

## 4.13.6 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 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>

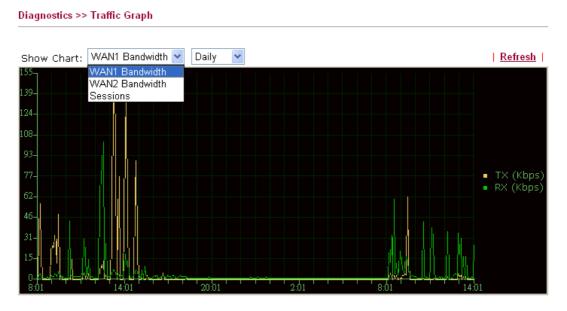
Current /Peak/Speed Current means current transmission rate and receiving rate for WAN1/WAN.

**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.

# 4.13.7 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.

# 4.13.8 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

<b>Note</b> : If you wa which WAN ping			don't want to speci nspecified".	fy
Ping through	n: WAN1	~		
Hos	st / IP 🔽	IP Address:		
	teWay1 teWay2 S		1	<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.

## 4.13.9 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.

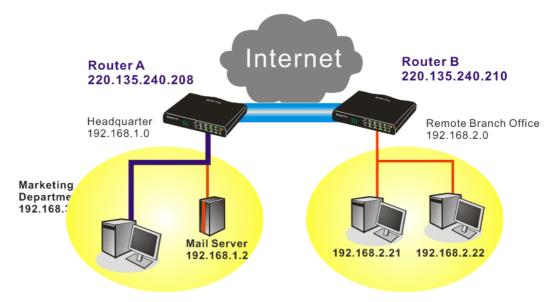
UDP Run
<u>Clear</u>
~

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		
Mutual Authentication	(PAP) 🔘 Yes 💿 No		
Username			
Password			

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set



general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

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    Both Dial-Out 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	
	O Digital Signature(X.509	9)
	None 😪	
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES without	Authentication ¥
	Advanced	
	Index(1-15) in <u>Schedule</u> 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	
	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 Digital Signature(X.509 None IPSec Security Method Medium(AH) High(ESP) DES without Advanced Index(1-15) in <u>Schedule</u>	Authentication

6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP IPSec Tunnel L2TP with IPSec Policy None	Username Password VJ Compression	??? 
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.210 or Peer ID	IKE Authentication Method ♥ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.505 None ♥ IPSec Security Method ♥ Medium(AH) High(ESP) ♥ DES ♥	) Э) 3DES ☑ AES

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings		
Allowed Dial-In Type		
🗹 рртр	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.210	Digital Signature(X.50	9)
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	Clear Cancel

### Settings in Router B in the remote office:

VPN and Remote Access >> PPP General Setup

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

PPP/MP Protocol		IP Address Assignment for 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	
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.

2	D1 -		0		
3.	Dia	l-In	Se	ttir	igs

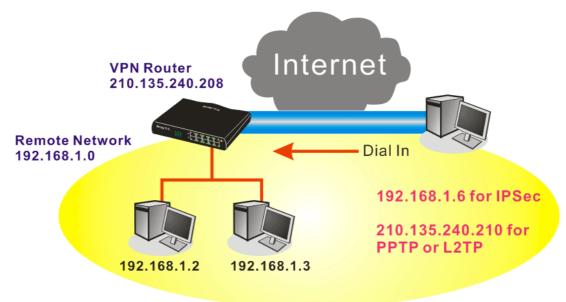
Allowed Dial-In Type		
РРТР	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital Signature(X.509	)
or Peer ID	None 💌	
	IPSec 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	5		
My WAN IP	0.0.0.0	RIP Direction Disa	able 💉
Remote Gateway IP	0.0.0.0	From first subnet to remote ne	etwork, you have to
Remote Network IP	192.168.1.0	Rou	ite 😽
Remote Network Mask	255.255.255.0		
	More	Change default route to the single WAN supports this )	his VPN tunnel ( Only
	ОК С	lear 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      Enable this account	Username ??? Password
Idle Timeout 300 second(s)	IKF Authentication Method
Allowed Dial-In Type	V Pre-Shared Key
РРТР	IKE Pre-Shared Key
<ul> <li>✓ IPSec Tunnel</li> <li>□ L2TP with IPSec Policy None</li> </ul>	Digital Signature(X.509)
Specify Remote Node Remote Client IP or Peer ISDN Number or Peer ID Netbios Naming Packet  Pass  Block	IP Sec Security Method ✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES Local ID (optional)

VPN and Remote Access >> Remote Dial-in User

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

VPN and Remote Access >> Remote Dial-in User

Index No. 1			
User account and Authentication		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.

🍾 Smart VPN Client 3.2.2 (WinXP)	
Step 0. This step will add the ProhibitIpSec registry valu order to configure a L2TP/IPSec connection usin or a L2TP connection. For more infomation, plea Q240262 in the Microsoft Knowledgement Base.	g a pre-shared key se read the article
Step 1. Dial to ISP If you have already gotten a public IP, you can	skip this step.
<b>~</b>	Dial
Step 2. Connect to VPN Server	
×	Connect
Insert Remove	Setup
Status: No connection PPTP	ISP @ VPN @

3. In Step 2. Connect to VPN Server, click Insert button to add a new entry.

If an IPSec-based service is selected as shown below,

Dial To VPN	×	
Session Name:	Office	
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)	
192.168.1.1		
User Name :	draytek_user1	
Password :	*****	
Type of VPN		
○ PPTP	◯ L2TP	
IPSec Tunnel	CL2TP over IPSec	
PPTP Encryption		
Maximum strength encryption		
Use default ga	ateway 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.

IPSec Policy Setti	ng	X
My IP : Type of IPSec —	172.16.3.100	
Standard IPS	ec Tunnel	
Remote Su Remote Su		
Virture IP		ek Virture Interface
💽 Obtain a		utomatically (DHCP over IPSec)
IP Addr		192 . 168 . 1 . 201
Subnet	Mask:	255 . 255 . 255 . 0
Security Method Medium(AH)	•	High(ESP) DES
Authority Method		
Certification	Authority:	Browse
0	ĸ	Cancel

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.



Dial To VPN	X		
Session Name:	office		
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)		
192.168.1.1			
User Name :	draytek_user1		
Password :	*****		
Type of VPN	OL2TP		
O IPSec Tunnel	<u> </u>		
PPTP Encryption -			
🔘 No encryptio	n		
Require encr	Require encryption		
O Maximum stre	O Maximum strength encryption		
🔽 Use default ga	ateway on remote network		
ОК	Cancel		

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

# 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		Test					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

General Setup   Set to Factory D						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

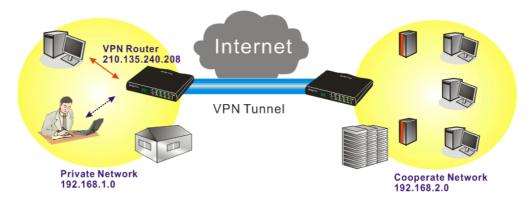
Index	Name	Rule	Service Type
Class 1	E-mail	Edit	
Class 2	HTTPS	Edit	<u>Edit</u>
Class 3		Edit	

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

WAN I	nbound Bandwidth	10000 Kbps
WAN C	outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
Enable UDP Bandw	idth Control	Limited_bandwidth Ratio 25
Outbound TCP AC	< Prioritize	Online Statistic

Bandwidth Management >> Quality of Service

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	
M ACT	

Bandwidth Management >> Quality of Service

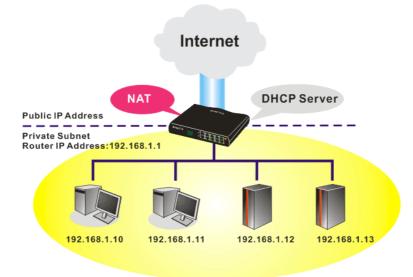
ACT	Hardware Acceleration
Local Address	Any
Remote Address	Any Edit
DiffServ CodePoint	IP precedence 2
Service Type	SYSLOG(UDP:514)
Note: Please choose/setu	p the <u>Service Type</u> first.
	OK Cancel

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.



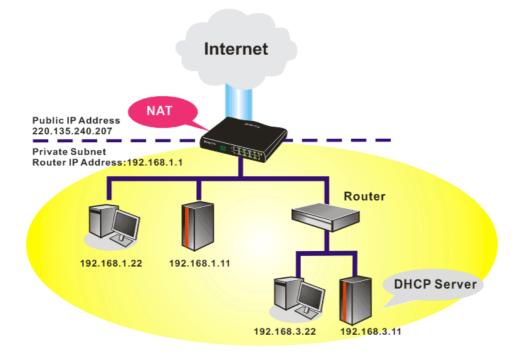


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> Ge	eneral Setup
-----------	--------------

LAN IP Network Configuration			DHCP Server Configuration		
For NAT Usage			💿 Enable Server 🔘 Disab	le Server	
1st IP Address	192.168.1.1		Relay Agent: 🔘 1st Sub	net O 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		
2n	d Subnet DHCP Server	D	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	<u>1</u>
For NAT Usage		◯ Enable Server ⊙ Disat	ole 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 set	tting
		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.

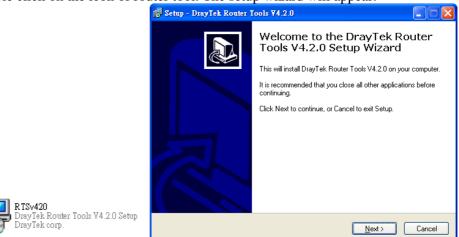
	About DrayTek	Products	Support	Education	Partners	Contact Us
ome > Support > Download	s					
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	elease Date		Firmware	
Vigor120 series	3.2.2.1	2	6/06/2009		Driver	
Vigor2100 series	2.6.2	2	6/02/2008		Utility	
Vigor2104 series	2.5.7.3	1:	3/02/2008		Utility In	troduction
Vigor2110 series	3.3.0	2	5/06/2009		Datashee	
Vigor2200/X/W/E	2.3.11	2	2/09/2004			ertification
Vigor2200Eplus	2.5.7	1	8/02/2009		- KATE U	ennication
Vigor2200USB	2.3.10	1	6/03/2005			

3. Access into **Support** >> **Downloads**. Please find out **Utility** menu and click it.

		About [	DrayTek	Products	Support	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	lindows	All Mod	lules		
Syslog Tools	2009/06/18	4.2.0	MS-Wi	ndows XP	All Mod	lules	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	lules		
		( Multi-	MS	-Vista				
		language)						
Smart Monitor	2009/03/25	2.0	MS-Wi	ndows XP	Vigor2950	) series		
					15			

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.

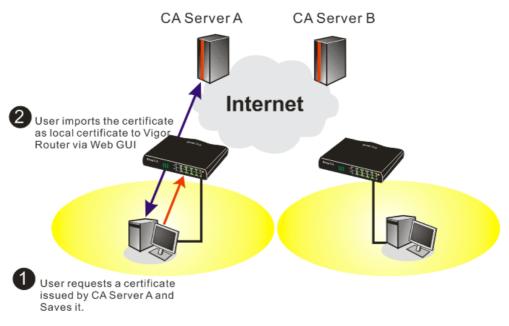
៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69	C:\Documents and Settings\Carrie
Password:	Abort Send

# 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 Cer	tificate		
			~
			$\sim$

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the 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 M	
Key Size	1024 Bit 🛩	

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

lame Subject	Status	Modify
.ocal /C=TW/O=Draytek/emailAddress	Requesting	View Delete
NERATE IMPORT REFRESH X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAKGAIUEBhMCVFcxEDAOI BgkqhkiG9w0BCQEWEXByZXNzQGRYX10ZWauY29tJ A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWkn 3wDeQytoV1LBJz21DF0xjX61p7ev187twwTsg41g; du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI oCkwJwYLKoZIhvcNAQkOMRowGDAWBgNVHREEDzAM; hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToer uRLq4CiEi6nV4hMRytcx2pE26sMarSgRREr86RoOG I9FqkjJNihip4TCjecSNNZjmQoSWU+BceSTG+SCB0 END CERTIFICATE REOUEST	HIGFMAOGCSQCSIb hIdHblo1kt9cTdL 26Qk/rGhuVTKd9j cOT2RZjkRMaHEWp ggtkcmF5dGVrLmN hItHQbcwjXvg/r7 8JxOI45560xC2/N	3DQEBAQUA UDaFk6s8d 6PlcrnkP7 VpwIDAQAB vbTANBgkq kFlzTJiHh 1Gh9VQ9I1

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

Welcome	
	rowser, e-mail client, or other secure program. Once you acquire a certificate, yo the web, sign your e-mail messages, encrypt your e-mail messages, and more
Select a task:	
Retrieve the CA certificate or certificate revocation list	t
<ul> <li>Request a certificate</li> </ul>	
Check on a pending certificate	

### 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 2	,

Select Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file

	e for yourself, another user, or a e the certificates that you can ob	computer using one of the following method ain.	s. Note that the policy of the certification
<ul> <li>Submit a certificate re</li> </ul>	quest to this CA using a form.		
Submit a certificate re	quest using a base64 encoded F	KCS #10 file or a renewal request using a	base64 encoded PKCS #7 file.
	r a smart card on behalf of anoth nt agent certificate to submit a reques	er user using the Smart Card Enrollment S for another user.	ation.
			Next >

Microsoft Certifica	te Services vigor		<u>Home</u>
Submit A Save	dRequest		
		request or PKCS #7 renewal request generated by an external application (such as a v t to the certification authority (CA).	veb
Saved Request:			
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUI MIIBGJCCARRCAQAwGTELMAKGAIUI BgkqhkiG9w0BCQEWEXByZXN2QGR A40NADC5iQKBgQDQYB7wm2FfFhk3 hX4bp89cUF9dloACG6IM/cBOck x/G0A7CTv0/fQ2pxroCulJTJL5js Clowse for a file to insert.	EBhMCVFcxEDAO yTX10ZWsuY29t 9/IeQnG03Xk++ dc2QFFv1Xc93	
Certificate Templa	ite:		
	Administrator 🛛 👻		
Additional Attribut	Administrator Authenticated Session Basic EFS		
Attributes:	EFS Recovery Agent User IPSEC (Offline request)		
	Router (Offline request) Subordinate Certification Authority Web Server	Subn	nit >

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

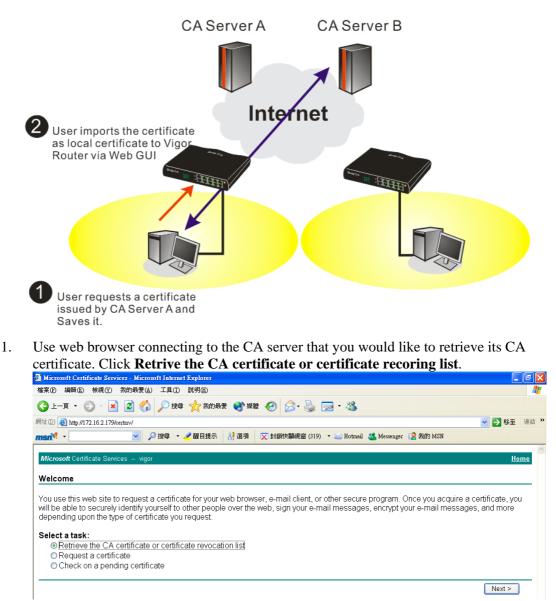
X509 Local Certificate Configuration

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 iG9w0BCQEWEXByZXNzQGRyYX10ZWauY29t CBiQKBgQDPioahu/gFQaYB1ceSOERSDfWk toV1LBJz1DFOxjX6ip7ev187twwTsg41g 3tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKV1 YJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN DBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToe iEi6nV4hMRytcxZpEZ6sMarSgRREx86RoO JNihip4TCjecSNNZjmQoSWU+Bce8TG+SCB ND CERTIFICATE REQUEST	MIGfMAOGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	SIb3DQEBAQUA CdLUDaFk6s8d A9j6PlcrnkP7 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 ③ 上-頁 · ◎ · 図 ② ☆ ♪ 搜尋 ☆ 我的最爱 ④ 媒體 Ø ◎ · ◎ · ◎ · ◎ · ◎ 網址 (D) 🕘 http://172.16.2.179/certsrv/certcarc.asp ✓ → 移至 連結 msn<sup>M</sup> • 🗸 🔎 搜尋 🔹 🥒 醒目提示 🛛 🚶 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🎎 Messenger 12 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] ○DER encoded or ●Base 64 encoded 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.

# 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
Connect using:
ASUSTeK/Broadcom 440x 10/100 Ir
This connection uses the following items:
<ul> <li>Client for Microsoft Networks</li> <li>Elie and Printer Sharing for Microsoft Networks</li> </ul>
Log Cos Packet Scheduler     Scheduler     Torrent Protocol (TCP/IP)
Install Uninstall Properties
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
<ul> <li>✓ Show icon in notification area when connected</li> <li>✓ Notify me when this connection has limited or no connectivity</li> </ul>
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	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
<u>o o</u> t	⊙ <u>O</u> btain an IP address automatically				
-O U <u>s</u>	O Use the following IP address:				
IP ac	dress:				
Subr	net mask:				
<u>D</u> efa	ult gateway:				
00	ptain DNS server address automatically				
- <b>O</b> Us	se the following DNS server addresses:				
Prefe	erred DNS server:				
Alten	nate DNS server:				
	Adyanced				
	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:		

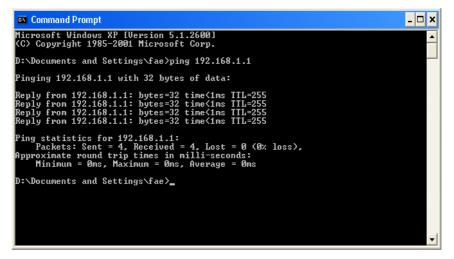
# 6.3 Pinging the Router from Your Computer

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.



000	Terminal — bash — 80x24	
Last login: Sat Jo	an 3 02:24:18 on ttyp1	5
Welcome to Darwin		
Vigor10:~ draytek	\$ ping 192.168.1.1	
PING 192.168.1.1	(192.168.1.1): 56 data bytes	
64 bytes from 192	.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 192	.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 192	.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 192	.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 192	.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
^C		
192.168.1.1 p	ing statistics	
승규는 일양수가 다 있는 것 같아요. 가 가 가지 않는 것?	tted, 5 packets received, 0% packet loss	
	g/max = 0.697/0.723/0.755 ms	
Vigor10:~ drayteks	그 것 그는 장거짓 만 것 것 같아. 것 것 것 같아. 그 것 같아. ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?	

# 6.4 Checking If the ISP Settings are OK or Not

Open **WAN** >> **Internet Access** page and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1/WAN2 to review the settings that you configured previously.

WAN >> Internet Access					
Internet	Access				
Index	Display Name	Physical Mode	Access Mode	3	
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 Disable  ISP Access Setup Username 123 Password	PP Authentication PAP or CHAP  Idle Timeout Idle Timeout If Address Assignment Method (IPCP) WAN IP Alias Fxed IP: ① Yes ④ No (Dynamic IP)
Index(1-15) in <u>Schedule</u> Setup:         =>       ,       ,         WAN Connection Detection         Mode       ARP Detect •         Ping IP	Fixed IP Address © Default MAC Address © Specify a MAC Address MAC Address: 00 .50 .7F :00 .00 .02

## **For Static Users**

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

WAN >> Internet Access

VAN 1		
Static or Dynamic IP (DHCP Client)	WAN IP Network Settings WAN IP Alias	
● Enable	Obtain an IP address automatically	
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	
WAN 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)	Oefault MAC Address	
RIP Protocol	Specify a MAC Address	
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.

			Getway IP (Static)	TX Packets	RX Rate
		DrayTek Vigor2910		0	0
AN Status TX Packets		RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442		3807		0	0
eWall Log 🛛 VPN Log	User Acces	s Log Call Log WA	N Log Network Infomation	Net State	
Time					
	Host	Message			
Apr 12 09:17:49	Vigor	WAN2 PPPoE <== Pi	rotocol:LCP(c021) ConfReq Id	dentifier:0x03 ACCM:	Ox0 Authe:
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor	WAN2 PPPoE <== Pi [3G]Modem status:a1	20 00 00 00 00 02 00 03 00		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor	WAN2 PPPoE <= Pi [3G]Modem status:a1 WAN2 PPPoE => Pi	20 00 00 00 00 02 00 03 00 rotocol:LCP(c021) ConfReq Id		
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	WAN2 PPPoE <= Pr [3G]Modem status:a1 WAN2 PPPoE => Pr WAN2 PPPoE <= V	20 00 00 00 00 00 ú2 00 03 ú0 rotocol:LCP(c021) ConfReq Id :1 T:1 PADS ID:0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem status:a1 WAN2 PPPOE => Pr WAN2 PPPOE <= V [3G]Modem response	20 00 00 00 00 02 00 03 00 rotocol:LCP(c021) ConfReq Id :1 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 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= Pr [3G]Modem status:al WAN2 PPPoE => Pr WAN2 PPPoE <= V [3G]Modem response [3G]Modem status:al	20 00 00 00 00 02 00 03 00 rotocol:LCP(c021) ConfReq Io :1 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	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem status:a1 WAN2 PPPOE => Pr WAN2 PPPOE <= V [3G]Modem response [3G]Modem status:a1 [3G]Modem status:a1	20 00 00 00 00 00 02 00 03 00 rotocol.LCP(c021) ConfReq Io :1 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		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= Pr [3G]Modem status:al WAN2 PPPoE => Pr WAN2 PPPoE <= V [3G]Modem response [3G]Modem status:al [3G]Modem status:al [3G]Modem dial ATI	20 00 00 00 00 00 00 00 00 00 00 rotocolLCP(c021) ConfReq Ic :1 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 00 20 00 20 00 07 *99#		
Lpr 12 09:17:49 Lpr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem status.al WAN2 PPPOE => P [3G]Modem response [3G]Modem status.al [3G]Modem status.al [3G]Modem status.al [3G]Modem dial AT [3G]Modem dial AT [3G]Modem status.al	20 00 00 00 00 00 00 00 00 00 rotocol.LCP(c021) ConfReq Ic :1 T:1 PADS ID:0 :CONNECT 3600000 20 00 00 00 00 02 00 02 00 20 00 00 00 00 00 02 00 02 00 20 00 00 00 00 00 02 00 21 *99# :1 T:1 PADR ID:0		
pr 12 09:17:49 pr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem statusal WAN2 PPPOE => Pr WAN2 PPPOE <= V [3G]Modem response [3G]Modem statusal [3G]Modem dial ATI [3G]Modem dial ATI WAN2 PPPOE => V WAN2 PPPOE <= V	20 00 00 00 00 00 02 00 03 00 rotocol.LCP(c021) ConfReq Ic :1 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 DT*99# :1 T:1 PADR ID:0 :1 T:1 PADO ID:0		
pr 12 09:17:49 pr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= Pr [3G]Modem status:al WAN2 PPPoE => Pr [3G]Modem response [3G]Modem status:al [3G]Modem status:al [3G]Modem dial A TI WAN2 PPPoE => V [3G]Modem response [3G]Modem	20 00 00 00 00 00 00 00 00 00 00 rotocolLCP(c021) ConfReq Id 1 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 DT*99# 1 T:1 PADR ID:0 1 T:1 PADO ID:0 COK	dentifier:0x00 MRU: 1!	
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= Pr [3G]Modem status.al WAN2 PPPoE => Pr [3G]Modem response [3G]Modem status.al [3G]Modem status.al [3G]Modem dial A TI WAN2 PPPoE => V WAN2 PPPoE <= V [3G]Modem response [3G]Modem response	20 00 00 00 00 00 02 00 03 00 rotocolLCP(c021) ConfReq Ic 1 T:1 PADS ID:0 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 20 499# 1 T:1 PADR ID:0 1 T:1 PADR ID:0 2 CK A T&FE0V1X1&D2&C1S0=	dentifier:0x00 MRU: 1!	
http: Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem status.al WAN2 PPPOE => Pr [3G]Modem response [3G]Modem status.al [3G]Modem status.al [3G]Modem status.al [3G]Modem dial A TI WAN2 PPPOE => V WAN2 PPPOE <= V [3G]Modem initialize WAN2 PPPOE => V	20 00 00 00 00 00 02 00 03 00 rotocolLCP(c021) ConfReq Ic 1 T:1 PADS ID:0 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 20 499# 1 T:1 PADR ID:0 1 T:1 PADR ID:0 2 CK A T&FE0V1X1&D2&C1S0=	dentifier:0x00 MRU: 1!	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= Pr [3G]Modem status.al WAN2 PPPoE => Pr [3G]Modem response [3G]Modem status.al [3G]Modem status.al [3G]Modem dial A TI WAN2 PPPoE => V WAN2 PPPoE <= V [3G]Modem response [3G]Modem response	20 00 00 00 00 00 02 00 03 00 rotocolLCP(c021) ConfReq Ic 1 T:1 PADS ID:0 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 20 499# 1 T:1 PADR ID:0 1 T:1 PADR ID:0 2 CK A T&FE0V1X1&D2&C1S0=	dentifier:0x00 MRU: 1!	
pr 12 09:17:49 pr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE <= Pr [3G]Modem status.al WAN2 PPPOE => Pr [3G]Modem response [3G]Modem status.al [3G]Modem status.al [3G]Modem status.al [3G]Modem dial A TI WAN2 PPPOE => V WAN2 PPPOE <= V [3G]Modem initialize WAN2 PPPOE => V	20 00 00 00 00 00 02 00 03 00 rotocolLCP(c021) ConfReq Ic 1 T:1 PADS ID:0 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 20 499# 1 T:1 PADR ID:0 1 T:1 PADR ID:0 2 CK A T&FE0V1X1&D2&C1S0=	dentifier:0x00 MRU: 1!	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.

# 6.6 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.