

# Vigor3200 Series

# **Multi-WAN Security Router**



Your reliable networking solutions partner

# User's Guide

# Vigor3200 Series Multi-WAN Security Router User's Guide

Version: 1.0 Firmware Version: V3.3.6\_RC6 Date: 18/11/2010



# **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 comparent is a source of the neutring of the analysis.</li> </ul>
Warranty	conservation of the environment. 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:Vigor3200 Series Router

DrayTek Corp. declares that Vigor3200 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

#### **Regulatory Information**

Federal Communication Commission Interference Statement

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

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

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

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

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

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



This product is designed for 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.



# Table of Contents



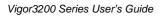
Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor3200 1.2.2 For Vigor3200n	2 4
1.3 Hardware Installation	6
1.4 Printer Installation	7



Configuring Basic Settings	13
2.1 Two-Level Management	13
2.2 Accessing Web Page	13
2.3 Changing Password	
2.4 Quick Start Wizard	
2.4.1 PPPoE 2.4.2 PPTP/L2TP 2.4.3 Static IP 2.4.4 DHCP	
2.5 Service Activation Wizard	
2.6 Online Status	
2.7 Saving Configuration	
2.8 Support Area	



User Mode Operation	29
3.1 WAN	29
<ul> <li>3.1.1 Basics of Internet Protocol (IP) Network</li> <li>3.1.2 General Setup</li></ul>	29 31 35
3.2 LAN	
3.2.1 Basics of LAN 3.2.2 General Setup	47 48
3.3 NAT	51
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	55
3.4 Applications	60





3.4.1 Dynamic DNS 3.4.2 UPnP	
3.5 Wireless LAN	64
<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> <li>3.5.5 Station List</li> </ul>	66 69 71
3.6 USB Application	72
<ul> <li>3.6.1 USB General Settings</li> <li>3.6.2 USB User Management</li> <li>3.6.3 File Explorer</li> <li>3.6.4 USB Disk Status</li> </ul>	
3.7 System Maintenance	
<ul> <li>3.7.1 System Status.</li> <li>3.7.2 User Password</li> <li>3.7.3 Time and Date</li> <li>3.7.4 Reboot System</li></ul>	79 80
3.8 Diagnostics	81
3.8.1 DHCP Table 3.8.2 Traffic Graph 3.8.3 Ping Diagnosis 3.8.4 Trace Route	82 82



Admin Mode Operation	85
4.1 WAN	85
4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 General Setup	
4.1.3 Internet Access 4.1.4 Load-Balance Policy	91
4.2 LAN	103
4.2.1 Basics of LAN 4.2.2 General Setup	
4.2.3 Static Route	112
4.2.4 VLAN 4.2.5 Bind IP to MAC	116
4.2.6 LAN Port Mirror	
4.3 NAT	
4.3.1 Port Redirection 4.3.2 DMZ Host	
4.3.3 Open Ports	125
4.4 Firewall	127
4.4.1 Basics for Firewall	
4.4.2 General Setup 4.4.3 Filter Setup	
4.4.4 DoS Defense	
4.5 User Management	144
4.5.1 General Setup	144



<ul><li>4.5.2 User Profile (Reserved)</li><li>4.5.3 User Group</li><li>3.5.4 User Online Status</li></ul>	
4.6 Objects Settings	
4.6.1 IP Object 4.6.2 IP Group	150
4.6.3 Service Type Object	
4.6.4 Service Type Group	155
4.6.5 Keyword Object	
4.6.6 Keyword Group	
4.6.7 File Extension Object	
4.7 CSM Profile	
4.7.1 APP Enforcement Profile	
4.7.2 URL Content Filter Profile 4.7.3 Web Content Filter Profile	
4.8 Bandwidth Management	
4.8.1 Sessions Limit 4.8.2 Bandwidth Limit	
4.8.3 Quality of Service	
4.9 Applications	
4.9.1 Dynamic DNS 4.9.2 Schedule	
4.9.3 RADIUS	
4.9.4 UPnP	
4.9.5 IGMP	
4.9.6 Wake on LAN	189
4.10 VPN and Remote Access	
4.10.1 VPN Client Wizard	190
4.10.1 VPN Client Wizard 4.10.2 VPN Server Wizard	
4.10.1 VPN Client Wizard 4.10.2 VPN Server Wizard 4.10.3 Remote Access Control	
4.10.1 VPN Client Wizard 4.10.2 VPN Server Wizard	
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 202 203 203 204 204 208 216
<ul> <li>4.10.1 VPN Client Wizard.</li> <li>4.10.2 VPN Server Wizard.</li> <li>4.10.3 Remote Access Control.</li> <li>4.10.4 PPP General Setup.</li> <li>4.10.5 IPSec General Setup.</li> <li>4.10.6 IPSec Peer Identity.</li> <li>4.10.7 Remote Dial-in User</li> <li>4.10.8 LAN to LAN.</li> <li>4.10.9 Connection Management</li> <li>4.11 Certificate Management</li> </ul>	190 196 200 201 202 203 203 204 208 216 217
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 202 203 204 208 216 217 217
<ul> <li>4.10.1 VPN Client Wizard.</li> <li>4.10.2 VPN Server Wizard.</li> <li>4.10.3 Remote Access Control.</li> <li>4.10.4 PPP General Setup.</li> <li>4.10.5 IPSec General Setup.</li> <li>4.10.6 IPSec Peer Identity.</li> <li>4.10.7 Remote Dial-in User</li> <li>4.10.8 LAN to LAN.</li> <li>4.10.9 Connection Management</li> <li>4.11 Certificate Management</li> <li>4.11.1 Local Certificate.</li> </ul>	190 196 200 201 202 203 204 208 216 217 217 217
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 203 203 204 208 216 217 217 217 219 220
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 203 203 204 208 216 217 217 217 219 220 220
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 203 203 204 208 216 217 217 217 219 220 220 220 220 220
<ul> <li>4.10.1 VPN Client Wizard.</li> <li>4.10.2 VPN Server Wizard.</li> <li>4.10.3 Remote Access Control.</li> <li>4.10.4 PPP General Setup</li> <li>4.10.5 IPSec General Setup.</li> <li>4.10.6 IPSec Peer Identity.</li> <li>4.10.7 Remote Dial-in User</li> <li>4.10.8 LAN to LAN.</li> <li>4.10.9 Connection Management</li> <li>4.11 Certificate Management</li> <li>4.11 Certificate Management</li> <li>4.11.2 Trusted CA Certificate</li> <li>4.11.3 Certificate Backup.</li> <li>4.12 Wireless LAN</li> <li>4.12.1 Basic Concepts.</li> <li>4.12.2 General Setup.</li> <li>4.12.3 Security.</li> </ul>	190 196 200 201 202 203 204 208 216 217 217 217 217 217 219 220 220 220 220 220
<ul> <li>4.10.1 VPN Client Wizard.</li> <li>4.10.2 VPN Server Wizard.</li> <li>4.10.3 Remote Access Control.</li> <li>4.10.4 PPP General Setup</li> <li>4.10.5 IPSec General Setup.</li> <li>4.10.6 IPSec Peer Identity.</li> <li>4.10.7 Remote Dial-in User</li> <li>4.10.8 LAN to LAN.</li> <li>4.10.9 Connection Management</li> <li>4.11 Certificate Management</li> <li>4.11.1 Local Certificate</li> <li>4.11.2 Trusted CA Certificate</li> <li>4.11.3 Certificate Backup.</li> <li>4.12 Wireless LAN</li> <li>4.12.1 Basic Concepts.</li> <li>4.12.3 Security.</li> <li>4.12.4 Access Control.</li> </ul>	190 196 200 201 202 203 204 208 216 217 217 217 217 219 220 220 220 220 220 220 220
<ul> <li>4.10.1 VPN Client Wizard.</li> <li>4.10.2 VPN Server Wizard.</li> <li>4.10.3 Remote Access Control.</li> <li>4.10.4 PPP General Setup.</li> <li>4.10.5 IPSec General Setup.</li> <li>4.10.6 IPSec Peer Identity.</li> <li>4.10.7 Remote Dial-in User.</li> <li>4.10.8 LAN to LAN.</li> <li>4.10.9 Connection Management.</li> <li>4.11 Certificate Management.</li> <li>4.11.1 Local Certificate.</li> <li>4.11.2 Trusted CA Certificate</li> <li>4.11.3 Certificate Backup.</li> <li>4.12 Wireless LAN .</li> <li>4.12.4 General Setup.</li> <li>4.12.5 WPS.</li> <li>4.12.6 WDS.</li> </ul>	190 196 200 201 202 203 204 208 216 217 217 217 217 219 220 220 220 220 220 220 220 220 220 22
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 202 203 204 208 216 217 217 217 217 219 220 220 220 220 220 220 220 220 220 22
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 202 203 204 208 216 217 217 217 219 220 220 220 220 220 220 220 220 223 220 223 226 228 229 231 234 235
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190 196 200 201 202 203 204 208 216 217 217 217 219 220 220 220 220 220 220 220 220 221 220 220
<ul> <li>4.10.1 VPN Client Wizard</li></ul>	190         196         200         201         202         203         204         203         204         208         216         217         218         220         220         220         220         220         220         220         220         220         220         220         220         220         221         220         220         220         220         220         220         220         220         220         220         221         220         221         220         221         220         221         220         221         220         221         220         221         220         221         221         2



	4.13.1 USB General Settings	
	4.13.2 USB User Management	
	4.13.3 File Explorer	
	4.13.4 USB Disk Status	242
4.	14 System Maintenance	243
	4.14.1 System Status	244
	4.14.2 TR-069	245
	4.14.3 Administrator Password	246
	4.14.4 User Password	247
	4.14.5 Configuration Backup	247
	4.14.6 Syslog/Mail Alert	
	4.14.7 Time and Date	252
	4.14.8 Management	
	4.14.9 Reboot System	
	4.14.10 Firmware Upgrade	
	4.14.11 Activation	256
4.	15 Diagnostics	257
	4.15.1 Dial-out Trigger	258
	4.15.2 Routing Table	
	4.15.3 ARP Cache Table	259
	4.15.4 DHCP Table	259
	4.15.5 NAT Sessions Table	260
	4.15.6 Data Flow Monitor	260
	4.15.7 Traffic Graph	262
	4.15.8 Ping Diagnosis	263
	4.15.9 Trace Route	264



Application and Examples	265
5.1 How to Configure Multi-Subnet	265
5.2 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	270
5.3 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	278
5.4 QoS Setting Example	283
5.5 Upgrade Firmware for Your Router	287
5.6 Request a certificate from a CA server on Windows CA Server	290
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server	294
5.8 Creating an Account for MyVigor	296
5.8.1 Creating an Account via Vigor Router 5.8.2 Creating an Account via MyVigor Web Site	



Trouble Shooting	303
6.1 Checking If the Hardware Status Is OK or Not	. 303
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	. 304
6.3 Pinging the Router from Your Computer	. 306
6.4 Checking If the ISP Settings are OK or Not	. 307

6.5 Problems for 3G Network Connection	308
6.6 Backing to Factory Default Setting If Necessary	308
6.7 Contacting Your Dealer	309

# 1 Preface

Vigor3200 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/3DES, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to **32** VPN tunnels.

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

Object-based firewall is flexible and allows your network be safe. In addition, Vigor3200 Series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files, or for 3G WAN connection.

Vigor3200 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:

ОК	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.
	ther buttons shown on the web pages, please refer to Chapter 3 and 4 for
detailed explana	411011.

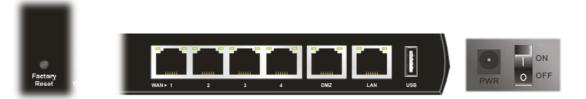
### **1.2 LED Indicators and Connectors**

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

#### 1.2.1 For Vigor3200



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.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while detecting an attack.
VPN		On	The VPN tunnel is active.
WAN1-4		On	The WAN1 ~ WAN4 connection is ready.
		Blinking	It will blink while transmitting data.
CSM		On	The profile(s) of CSM (Content Security
			Management) for IM/P2P, URL/Web Content Filter
			application can be enabled from Firewall
			>>General Setup. (Such profile must be
			established under CSM menu).
LED on Conne	ector		
	Left LED	On	The port is connected.
WAN 1/2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left
			LED is on.
DMZ	Left LED	On	The port is connected.
	(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.
LAN	(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.



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.
WAN1- WAN4	Connecters for remote networked devices.
DMZ	Connecter for local DMZ host.
LAN	Connecter for local network devices.
USB	Connecter for 3G Modem or printer.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

## 1.2.2 For Vigor3200n

	Dray	✓ Tek Vigo	or3200n AN Security Router
Factory	PN CSM AN1 WAN3 AN2 WAN4		
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
< J,		Off	The router is powered off.
USB		On	USB device is connected and ready for use.
		Blinking	The data is transmitting.
WLAN		On	Wireless access point is ready.
		Blinking	Ethernet packets are transmitting over wireless LAN.
		Off	The WLAN function is inactive.
VPN		On	The VPN tunnel is active.
WAN1-4		On	The WAN1 ~ WAN4 connection is ready.
		Blinking	It will blink while transmitting data.
CSM		On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from <b>Firewall</b> >> <b>General Setup</b> . (Such profile must be established under <b>CSM</b> menu).
LED on Conn	ector		· · · · · · · · · · · · · · · · · · ·
	Left LED	On	The port is connected.
WAN 1/2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps when left LED is on.
DMZ	Left LED	On	The port is connected.
	(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.
LAN	(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.





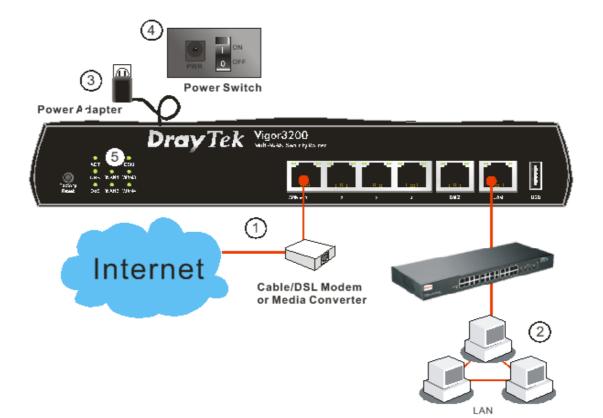
Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device
ON/OFF/WPS	making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN1- WAN4	Connecters for remote networked devices.
DMZ	Connecter for local DMZ host.
LAN	Connecter for local network 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 the LAN port of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer. Or, use a switch to connect Vigor router and computer(s).
- 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.

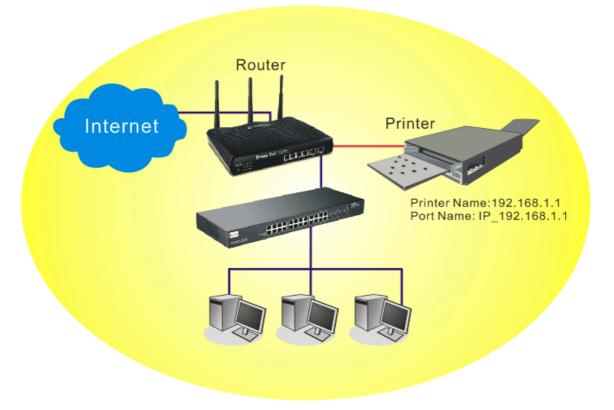
(For the detailed information of LED status, please refer to section 1.1.)



6

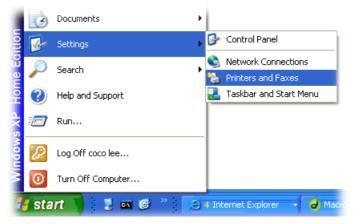
#### **1.4 Printer Installation**

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.



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	can create a
O Use the following port:	LPT1: (Recommended Printer Port)	
Note: Most computers ( The connector for this p	port should look something like this:	

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

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

7. Click Standard and choose Generic Network Card.

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

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



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

The manufacturer an	d model determine which printer software to us	e. 🗳
	cturer and model of your printer. If your printer c sk. If your printer is not listed, consult your print software.	
Manufacturer AST AT&T	Printers Brother HL-1060 BR-Script2 Brother HL-1070 BR-Script2	 
Brother Buil Canon This driver is digitally si	Brother HL-1070 Brother HL-10PS70PS	ate Have Disk
Tell me why driver sign	· · · · · · · · · · · · · · · · · · ·	

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

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

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

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

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

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

ome > Support > FAQ				
FAQ - Basic				FAQ
01. What are the differences among these firmware file formats $? % \left( {{\left[ {{{\rm{T}}} \right]} \right]_{{\rm{T}}}} \right)$				Basic
02. How could I get the telnet command for routers ?				Advanced
03. How can I backup/restore my configuration settings ?				VPN
04. How do I reset/clear the router's password ?				DHCP
05. How to bring back my router to its default value ?				Wireless
06. How do I tell the type of my Vigor Router is AnnexA or Annex	(B? (For AD	OSL model (	only)	  QoS
07. Ways for firmware upgrade.				ISDN
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2	200 Series	routers?		Firewall / IF Filter
09. I failed to upgrade Vigor Router's firmware from my Mac mach I do?	nine constar	ntly, what s	hould	Printer Server
10. How to upgrade firmware of Vigor Router remotely ?				
<b>AQ - Printer Server</b> 1. How do I configure LPR printing on Windows2 2. How do I configure LPR printing on Windows9	techaraterater (	?		
1. How do I configure LPR printing on Windows2 2. How do I configure LPR printing on Windows9	8/Me ?	?		
1. How do I configure LPR printing on Windows2	8/Me ? es ?		ocumen	ts through Vigor210
1. How do I configure LPR printing on Windows2 2. How do I configure LPR printing on Windows9 3. How do I configure LPR printing on Linux boxe 4. Why there are some strange print-out when I t	8/Me ? es ? try to pri	int my de	ocumen	ts through Vigor210
1. How do I configure LPR printing on Windows2 2. How do I configure LPR printing on Windows9 3. How do I configure LPR printing on Linux boxe 4. Why there are some strange print-out when I t 9 / 2300's print server?	8/Me ? es ? try to pri gor route	int my do		ts through Vigor210
1. How do I configure LPR printing on Windows2 2. How do I configure LPR printing on Windows9 3. How do I configure LPR printing on Linux boxe 4. Why there are some strange print-out when I t 9 / 2300's print server? 5. What types of printers are compatible with Vi	8/Me ? es ? try to pri gor route ort of Vie	int my do		ts through Vigor210
<ol> <li>How do I configure LPR printing on Windows2</li> <li>How do I configure LPR printing on Windows9</li> <li>How do I configure LPR printing on Linux boxe</li> <li>Why there are some strange print-out when I to 2 / 2300's print server?</li> <li>What types of printers are compatible with Vistor What are the limitations in the USB Printer Prints</li> </ol>	8/Me? es? try to pri gor route ort of Vie er?	int my do		ts through Vigor210
<ol> <li>How do I configure LPR printing on Windows2</li> <li>How do I configure LPR printing on Windows9</li> <li>How do I configure LPR printing on Linux boxe</li> <li>Why there are some strange print-out when I to 2300's print server?</li> <li>What types of printers are compatible with Vis</li> <li>What are the limitations in the USB Printer Piston</li> <li>What is the printing buffer size of Vigor Route</li> </ol>	8/Me? es? try to pri gor route ort of Vi er? ?	int my do er? gor Rout		ts through Vigor210

This page is left blank.

#### Vigor3200 Series User's Guide

# **2** Configuring Basic Settings

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

### 2.1 Two-Level Management

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

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

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

#### 2.2 Accessing Web Page

1. Make sure your PC connects to the router correctly.

You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section -Trouble Shooting of the guide.

2. Open a web browser on your PC and type http://192.168.1.1. The following window will be open to ask for username and password.

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

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



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

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



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

#### 2.3 Changing Password

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

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

Vigor3200	Series ty Router					<b>Dray</b> Tek
Auto Logout 💌	System Status					
Quick Start Wizard Service Activation Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor3200n : 3.3.6_RC6 : Nov 3 2010 15:47	14			
WAN			LAN			
LAN		MAC Address	IP Address	Subnet Mask	DHCD	Server DNS
NAT	LAN1	00-50-7F-C9-B7-3C	192.168.1.1			168.95.1.1
Firewall	LAN2	00-50-7F-C9-B7-3C	192.168.3.1	255.255.255.0		168.95.1.1
User Management	LAN3	00-50-7F-C9-B7-3C	192.168.5.1	255.255.255.0	Yes	168.95.1.1
Objects Setting	LAN4	00-50-7F-C9-B7-3C	192.168.7.1	255.255.255.0	Yes	168.95.1.1
CSM	DMZ PORT	00-50-7F-C9-B7-3C	192.168.9.1	255.255.255.0	Yes	168.95.1.1
Bandwidth Management	IP Routed Subnet	00-50-7F-C9-B7-3C	192.168.2.1	255.255.255.0	Yes	168.95.1.1
Applications						
VPN and Remote Access			Wireless LAN	4		
Certificate Management Wireless LAN	MAC Address	Frequence	y Domain	Firmware Ve	ersion	SSID
USB Application	00-50-7F-C9-I	B7-3C Europe	·	2.3.2.0		DrayTek
System Maintenance						,
Diagnostics —			WAN			
	Link Status	MAC Address	Connec	tion IP Addre	ss	Default Gateway
Support Area	WAN1 Disconnect	ed 00-50-7F-C9-B7-3	3D			
Application Note	WAN2 Connected	00-50-7F-C9-B7-3	BE Static	IP 172.16.3	8.102	172.16.1.1
FÁQ	WAN3 Disconnect	ed 00-50-7F-C9-B7-3	3F			
Droduct Dogistration	WAN4 Disconnect					
	WAN5 Disconnect	ed 00-50-7F-C9-B7-4	41			

Main screen for admin mode operation (full configuration)

Vigor320 Multi-WAN Sec					D	<b>ray</b> Te
Auto Logout 👻	System Status					
Quick Start Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor3200n 1 : 3.3.6_RC6 : Nov 3 2010 15:47	-14			
WAN	Dunu Duter Time	. 1107 5 2010 13.41				
LAN NAT			LAN			
		MAC Address		Subnet Mask	DHCP Serv	
pplications Vireless I AN	LAN1	00-50-7F-C9-B7-3C		255.255.255.0	Yes	168.95.1.1
SB Application	LAN2	00-50-7F-C9-B7-3C		255.255.255.0	Yes	168.95.1.1
stem Maintenance	LAN3	00-50-7F-C9-B7-3C		255.255.255.0	Yes	168.95.1.1
aqnostics	LAN4	00-50-7F-C9-B7-3C		255.255.255.0	Yes	168.95.1.1
lagnostics	DMZ PORT	00-50-7F-C9-B7-3C		255.255.255.0	Yes	168.95.1.1
	IP Routed Subn	et 00-50-7F-C9-B7-3C	192.168.2.1	255.255.255.0	Yes	168.95.1.1
			Wireless LAN			
	MAC Addres	ss Frequenc	y Domain	Firmware Ve	rsion	SSID
	00-50-7F-0	C9-B7-3C Europe		2.3.2.0		DrayTek
			WAN			
	Link Sta	tus MAC Address	Connect	tion IP Addres	s Defa	ult Gateway
	WAN1 Disconne	ected 00-50-7F-C9-B7-3	3D			
Logout	WAN2 Connect	ed 00-50-7F-C9-B7-	3E Static II	P 172.16.3.	102 172.	16.1.1
	WAN3 Disconne	ected 00-50-7F-C9-B7-3	3F			
All Rights Reserved.	WAN4 Disconne	ected 00-50-7F-C9-B7-	40			
	WAN5 Disconne	ected 00-50-7F-C9-B7-	41			

#### Main screen for user mode operation (simple configuration)

System Maintenance >> Administrator Password Setup

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

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

	Old Password	
	New Password	
	Confirm Password	
		ОК
		or
System Maintenanc	ce >> User Password	or
	ce >> User Password	or
	ce >> User Password	<i>or</i>
System Maintenand Jser Password		<i>or</i>

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



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

#### 2.4 Quick Start Wizard

늰

**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

Please enter an alpha-num	eric string as your Passw	ord (Max 23 characters).	
Old Password	••••		
New Password	••••		
Confirm Password	••••		

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

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

#### Quick Start Wizard

selected for 3G USB modem connection.

WAN 1						
Select one of the	following Interr	net Acces	s types prov	vided by yo	ur ISP.	
	⊙ PP	PoE				
	O PP	тр				
	O L2	TP				
	O St	atic IP				
		ICP				

#### 2.4.1 PPPoE

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

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



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

Quick Start Wizard

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

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

Click Next for viewing summary of such connection.

Quick Start Wizard

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

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

#### 2.4.2 PPTP/L2TP

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

Quic	k Start	Wizard
~~~~		

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

Click Next for viewing summary of such connection.

e confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	РРТР
Click Back to modify char settings and restart the V	nges if necessary. Otherwise, click <b>Finish</b> to save the current rigor router.

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



#### 2.4.3 Static IP

Quick Start Wizard

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

WAN 1	uration probided by your ICD	
WAN IP	uration probided by your ISP. 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.

Quick Start Wizard	ł
--------------------	---

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

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

#### 2.4.4 DHCP

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

Quick Start Wizard

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

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

#### Quick Start Wizard

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
Click <b>Back</b> to modify char settings and restart the V	nges if necessary. Otherwise, click <b>Finish</b> to save the current rigor router.

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

#### 2.5 Service Activation Wizard

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

Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (*MyVigor*) located on <u>http://myvigor.draytek.com</u>. For using Web Content Filter Profile, please refer to later section **Web Content Filter Profile** for detailed information.

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

1. Open Service Activation Wizard.



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

#### Service Activation Wizard

This wizard is used for - Web Content Filter Please choose the edit	-		
<	<ul> <li>Free trial edition</li> <li>Formal edition w</li> </ul>		
		with incense key	

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

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



3. In the following page, you can activate the Web content filter service at the same time or individually. When you finish the selection, please click **Next**.

ect the service type that you want to activate		
his product provides 30 days of free trial, j	please choose the item(s) you want to use.	
/CF service:		
Web Content Filter (Commtouch)	License Agreement	
Commtouch is the web content filter based	on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can	
	GlobalView WCF package from retailing outlets.	
	GlobalView WCF package from retailing outlets. Activation Date : 2010-11-17	

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

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

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

Service Activation Wizard

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

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

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



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

DrayTek Service Activation				
Service Name	Start Date	Expire Date	Status	
Web Content filter	2010-11-17	2010-12-18	Commtouch	
Please check if the lice normal operation for yo				

Later, if you need to extend the license valid time, you can also use the **Service** Activation Wizard again to reach your goal by clicking the radio button of Formal edition with license key and clicking Next.

ervice Activation Wizard	
elect the service type that you want to ac	ctivate
This wizard is used for activating - Web Content Filter Please choose the edition you nee	d.
O Fre	ee trial edition
Equipa	rmal edition with license key
vice Activation Wizard	Next > Finish Cance
ect the service type that you want to activate	
Please choose the item you want to use. WCF service:	•
	<u>ense Agreement</u> mtouch operated in the worldwide. There is a 30-day trial period. After trial, you can ew WCF package from retailing outlets.
Enter your License key:	Activation Date : 2010-12-19 select
□ I have read and accept the above Agreemen	
Note: The activation date is brought out by the	server automatically and cannot be changed.
	< Back Next > Finish Cano

#### 2.6 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**

LAN Status	Prima	ry DNS: 168.95	5.1.1	Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets		-	
192.168.1.1	3220	20499			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet			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					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:07:09	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172,16.3,102	172.16.1.1	1015	81	3366	733
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet			00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 4 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet			00:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 5 Status					
Enable	Line	Name	Mode	Up Time	Signal
Yes	USB			00:00:00	-
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0

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 Packets</b>	Displays the total number of received packets at the LAN interface.	
WAN1~WAN5 Status		
Line	Displays the physical connection (Ethernet) of this interface.	
Name	Displays the name set in WAN web page.	
Mode	Displays the type of WAN connection (e.g., PPPoE).	

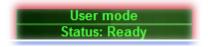


Up Time	Displays the total uptime of the interface.	
IP	Displays the IP address of the WAN interface.	
GW IP	Displays the IP address of the default gateway.	
TX Packets	Displays the total transmitted packets at the WAN interface.	
TX Rate	Displays the speed of transmitted octets at the WAN interface.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

## 2.7 Saving Configuration

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



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

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

#### 2.8 Support Area

When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



Click Support Area>>Application Note, the following web page will be displayed.

<b>Dray</b> Tek	繁體中文 English	Login Search Go
About DrayTek Product	s Support Education	Partners Contact Us
Home > Support > Application Notes		
Application Notes - Latest Application		Application Notes
01. How to use Windows Disk Management to format the USB Disk ?	2009/09/09	Latest Application
02. How to make a call between ATA24 without IP PBX or SIP server	2009/08/25	General
03. Vigor Router to NETGEAR with IPSec tunnel	2009/07/20	Dual WAN
04. SSL VPN Tunnel	2009/07/16	VoIP
05. How to Access the Computers and Shared Files via Samba Protocol?	2009/06/18	Bandwidth Management
06. SSL Web Proxy	2009/06/18	IP Filter/Firewall
07 How to use VNC and RDP via SSL VPN?	2009/06/18	USB
08 Vigor2050 Host to LANI VDN with LDAD Authoritication	2000/06/01	VPN

Click **Support Area>>FAQ**, the following web page will be displayed.



Dray Tek ***	中文 English	Login Search Go
About DrayTek Products Supp	oort Education	Partners Contact Us
ome > Support > FAQ		
FAQ - Latest FAQ		FAQ
01. What types of 3G modem / cellphone are compatible with Vigor router ?	2009/10/01	Latest FAQ
02. How to use PRTG monitors network traffic Vigor Router	2009/09/22	Basic
03. What is Powerline Networking?	2009/09/15	Advanced
04. What are the benefits of networking devices found at home?	2009/09/15	NAT
05. What is the maximum wire length that powerline technology can communicate over?	2009/09/15	VPN
06. Is VigorPlug's powerline technology compatible with other home networking technologies	2009/09/15	DHCP
(including phone line, powerline, and RF)?		Wireless
07. Will Powerline technology interfere with ADSL services?	2009/09/15	VolP
08. How does Powerline networking handle co-interference between two adjacent homes	2009/09/15	QoS

## Click **Support Area>>Product Registration**, the following web page will be displayed.

<b>Dray</b> Tek				English	Login	Search Go
	About DrayTek	Products	Support	Education	Partners	Contact Us
Home > DrayTek Member						
Dray Tek Member Dear Dray Tek new & existing users, For enhancing the users' satisfaction level while u we have designed this membership page. Please product(s). Already a Dray Tek Member – Just sign-in b Want to become a Dray Tek Member – Click Forgot username or password – Click "Forg	complete the membe elow. < "Create Account" an	rship registrati	on and then n	egister your	Sign up Forgot Pa	assword
Benefits for DrayTek Members						
Receiving e-news letters about latest firmwa Software and firmware available online for do Chances to win prizes.		rchased produc	ts.			

Many more henefits only for DrayTek members are coming soon

This page is left blank.

#### Vigor3200 Series User's Guide

# **3** User Mode Operation

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

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

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

Vigor3200 Multi-WAN Secu	O Series Drity Router				Ľ	<b>Dray</b> Tel
Auto Logout 💌	System Status					
Quick Start Wizard Online Status	Model Name Firmware Version Build Date/Time	: Vigor3200n : 3.3.6_RC6 : Nov 3 2010 15:47	:14			
WAN LAN			1.411			
NAT		MAC Address	LAN IP Address	Subnet Mask	DHCP Serv	er DNS
Applications	LAN1	00-50-7F-C9-B7-3C	192.168.1.1		Yes	168.95.1.1
Vireless LAN	LAN1 LAN2	00-50-7F-C9-B7-3C	192.168.3.1			168.95.1.1
ISB Application	LAN3	00-50-7F-C9-B7-3C	192.168.5.1		Yes	168.95.1.1
System Maintenance	LAN4	00-50-7F-C9-B7-3C	192.168.7.1	255.255.255.0	Yes	168.95.1.1
Diagnostics	DMZ PORT	00-50-7F-C9-B7-3C	192.168.9.1		Yes	168.95.1.1
	IP Routed Subnet			255.255.255.0	Yes	168.95.1.1
			Wireless LAN			
	MAC Address	Frequen	cy Domain	Firmware Ve	rsion	SSID
	00-50-7F-C9-		-,	2.3.2.0		DrayTek
			WAN			
	Link Status	MAC Address	Connec	tion IP Addre	ss Defa	ault Gateway
	WAN1 Disconnect	ed 00-50-7F-C9-B7-				
Logout	WAN2 Connected			IP 172.16.3	.102 172.	16.1.1
All Rights Reserved.	WAN3 Disconnect					
Aurogines Reserved.	WAN4 Disconnect					
	WAN5 Disconnect	ed 00-50-7F-C9-B7-	41			

## 3.1 WAN

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

## 3.1.1 Basics of Internet Protocol (IP) Network

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



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

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

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

#### Get Your Public IP Address from ISP

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

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

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

For 3G mobile communication through Access Point is more and more popular, Vigor3200 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3200, it can support HSDPA/UMTS/EDGE/GPRS and the future 3G standard (HSUPA, etc). Vigor3200n 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 the LAN port on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor3200n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor3200n series.



After connecting into the router, 3G USB Modem will be regarded as the fifth WAN port. However, the other Ethernet WAN ports still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN5 also can be used as backup device. Therefore, when other Ethernet WAN port 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 to WAN5 in details.

There are four WAN ports (represented with WAN1, WAN2, WAN3 and WAN4 in web pages) and one USB port (represented with WAN5 in web pages) offered by the router. For this router supports multiple WANs function, it allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation.

This webpage allows you to set general setup for WAN1 to WAN5 respectively.

#### WAN >> General Setup

Load Bal	ance Mode	e: Auto Weight			
Setup					
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode	Backup WAN
WAN1	V	Ethernet/Auto negotiation	10000/10000	Always On	-
WAN2	V	Ethernet/Auto negotiation	10000/10000	Always On	-
WAN3	V	Ethernet/Auto negotiation	10000/10000	Backup	-
WAN4	V	Ethernet/Auto negotiation	10000/10000	Backup	-
WAN5	V	USB/-	2000/384	Always On	-

From the above figure, WAN1 ~ WAN4 connect to Internet through the interface of Ethernet; WAN5 connects to Internet via USB interface. Therefore the configuration for each WAN port will be different slightly. Please click the WAN link under Index to open the web page for detailed configuration.

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

Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
Line Speed	Display the downstream and upstream rate of such WAN interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Backup WAN	Display the Backup WAN interface for such WAN when it is disabled.
Note: In default, each W	AN is enabled.

#### For WAN1 ~ WAN4

WAN >> General Setup

WAN1 ~ WAN4 are fixed with physical mode of Giga Ethernet. Here we take WAN1 as an example.

WAN 1		
Enable:	Yes 🛩	
Display Name:		
Physical Mode:	Ethernet	
Physical Type:	Auto negotiation 💌	
Line Speed(Kbps):		
DownLink	10000	
UpLink	10000	
VLAN Tag insertion:	Disable 💙 (Please configure Internet Ac	cess setting first)
Tag value:	0 (0~4095)	
Priority:	0 (0~7)	
Active Mode:	Always On 😽	
Backup WAN:	None 🗸	
Enable	Choose <b>Yes</b> to invoke the settings f Choose <b>No</b> to disable the settings for	
Display Name	Type the description for such WAN	l interface.
Physical Mode	Display the physical mode of such	WAN interface.
Physical type	You can change the physical type for <b>negotiation</b> for determined by the s	
	Physical Type: Auto neg	gotiation 🔽
	Auto nec	
	10M half	
	10M full	
	100M ha	
	100M ful	i dupiex

Line SpeedIf your choose According to Line Speed as the Load BalanceMode, please type the line speed for downloading and<br/>uploading for such WAN interface. The unit is kbps. The



default setting for down link and up link is 10000Kbps.

**VLAN Tag insertion** Enable – Enable the function of VLAN with tag.

> The router will add specific VLAN number to all packets on the WAN while sending them out.

**Disable** – Disable the function of VLAN with tag.

Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.

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

#### **Active Mode and Backup** WAN/Backup Type

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



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

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

	(U~? (
Active Mode:	Always On 🔽
Backup WAN:	None 💌

If you choose Backup as the Active Mode, Backup WAN will be changed into **Backup Type**. You have to specify which role the WAN interface should play if you want to backup multiple WANs.



Backup		

When any WAN disconnect When all WAN disconnect

When any WAN disconnect -WAN1 will be activated when any master WAN interface disconnects.

When all WAN disconnect -WAN1 will be activated when all master WAN interfaces disconnect.

## For WAN5

To use 3G network connection through 3G USB Modem, please configure WAN5 interface.

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

WAN 5		
Enable:	Yes 🕶	
Display Name:		
Physical Mode:	USB	
Physical Type:	Auto negotiation 👻	
Line Speed(Kbps):		
DownLink	2000	
UpLink	384	
Active Mode:	Always On 🔽	
Backup WAN:	None 💌	
	OK Cancel	
Enable	Choose <b>Yes</b> to invoke the settin Choose <b>No</b> to disable the settin	•
Display Name	Type the description for such W	WAN interface.
Physical Mode	Display the physical mode of s	uch WAN interface.
Physical type	For such WAN interface is fixe is not necessary to specify phys	ed to USB network connection, it sical type.
Line Speed	If your choose <b>According to L</b> <b>Mode</b> , please type the line spee uploading for such WAN interf	
Active Mode and Backup WAN/Backup Type		WAN interface will be active for ted as a backup WAN interface
	Always On <mark>.</mark> Alwaγs On Backup	
	Backup WAN/Backup Type - WAN interface. It will be chan Mode specified.	
	of the backup WAN interfaces down list. Later, when such WA reason, the backup WAN will b	AN is disconnected for some
	ruency.	
	monty.	
	Active Mode: Backup WAN:	Always On 👻
	of the backup WAN interfaces down list. Later, when such WA reason, the backup WAN will b	from the <b>Backup WAN</b> drop AN is disconnected for some be activated automatically to

If you choose **Backup** as the **Active Mode**, Backup WAN will



be changed into **Backup Type**. You have to specify which role the WAN interface should play.

Active Mode:	Backup 🔽
Backup Type (Only for Backup Multiple WAN):	⊙ When any W ○ When all WA

When any WAN disconnect When all WAN disconnect

When any WAN disconnect – WAN1 will be activated when any WAN interface disconnects.

**When all WAN disconnect** – WAN1 will be activated when all the WAN interfaces disconnect.

#### 3.1.3 Internet Access

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3/WAN4/WAN5) for Internet Access. Due to different Physical Mode of WAN interface, the Access Mode for these connections also varies. Refer to the following figures.

WAN >> Internet Access

ndex Display Name	Physical Mode	Access Mode
VAN1	Ethernet	None 💽 Details F
/AN2	Ethernet	Static or Dynamic IP 🛛 🖌 🛛 Details F
/AN3	Ethernet	None PPPoE Details F
/AN4	Ethernet	Static or Dynamic IP Details P PPTP/L2TP Details P
AN5	USB	None 🔽 Details F

#### WAN >> Internet Access

WAN2     Ethernet     Static or Dynamic IP     Details Pa       WAN3     Ethernet     None     Details Pa       WAN4     Ethernet     None     Details Pa       WAN5     USB     None     Details Pa	Index Display Name	Physical Mode	Access Mode		
WAN3     Ethernet     None     Details Pa       WAN4     Ethernet     None     Details Pa       WAN5     USB     None     Details Pa	WAN1	Ethernet	None	*	Details Page
WAN4 Ethernet None Details Pa WAN5 USB None Details Pa	WAN2	Ethernet	Static or Dynamic IP	*	Details Page
WAN5 USB None Details Pa	WAN3	Ethernet	None	*	Details Page
	WAN4	Ethernet	None	*	Details Page
None	VAN5	USB	None	*	Details Page
PPP			None		

Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3/WAN4/WAN5 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1-WAN4 (Ethernet) /WAN5 (3G USB Modem) according to the real network

connection.

Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click <b>Details Page</b> for accessing the page to configure the settings.
Details Page	This button will open different web page according to the access mode that you choose in WAN interface

## Details Page for PPPoE in WAN1 ~ WAN4

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

PPPoE Client Mode		PPP/MP Setup
💽 Enable 🛛 Di:	sable	PPP Authentication PAP or CHAP 🛩
		Idle Timeout 180 second(s)
ISP Access Setup		IP Address Assignment Method
Username		(IPCP) WAN IP Alias
Password		Fixed IP: O Yes O No (Dynamic IP)
WAN Connection Det	ection	Fixed IP Address
Mode	ARP Detect 💌	Operault MAC Address
Ping IP		<ul> <li>Specify a MAC Address</li> </ul>
TTL:		MAC Address:
		00 .50 .7F :C9 .B7 .3D
МТО	1442 (Max: 1492)	

PPPoE Client Mode	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
	<b>Username</b> – Type in the username provided by ISP in this field.
	<b>Password</b> – Type in the password provided by ISP in this field.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	<b>TTL</b> ( <b>Time to Live</b> ) – Displays value for your reference. TTL value is set by telnet command.
PPP/MP Setup	PPP Authentication – Select PAP only or PAP or CHAP for

PPP. If you want to connect to Internet all the time, you can check **Always On**.

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

#### IP Address Assignment Method (IPCP)

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

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

ndex	Enable	Aux. WAN IP	Join NAT IP Pool	
1.				
2.		0.0.0.0		
з.		0.0.0.0		
4.		0.0.0.0		
5.		0.0.0.0		
6.		0.0.0.0		
7.		0.0.0.0		
8.		0.0.0.0		
< <u>1-8   9-16   17-24   25-32</u> >> <u>Next</u> >>				

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

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

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

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

#### Details Page for Static or Dynamic IP in WAN1 ~ WAN4

WAN >> Internet Access

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) <ul> <li>Enable</li> </ul> <li>Keep WAN Connection  <ul> <li>Enable PING to keep alive</li> </ul> </li> <li>PING to the IP</li>		WAN IP Network Settings WAN IP Alias O Obtain an IP address automatically			
		Router Name	Vigor		*
		Domain Name * : Required for	Domain Name * : Required for some ISPs		*
		Specify an IP a	Specify an IP address		
PING Interval	0minute(s)	IP Address		172.16.3.102	
WAN Connection Dete	ection	Subnet Mask		255.255.0.0	
Mode	ARP Detect 💌	Gateway IP Add	ress	172.16.1.1	
Ping IP		DNS Server IP Ad	dress		
TTL:		Primary IP Addre	ess	168.95.1.1	
мти	1442 (Max: 1500)	Secondary IP Ac	ddress		
		Oefault MAC		-	
RIP Protocol			Specify a MAC Address		
Enable RIP		MAC Address:	C9 B7	7.3E	
	OK	Cancel			

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 Enable PING to keep alive box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation. WAN Connection Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Detection Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you



have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command. MTU It means Max Transmit Unit for packet. The default setting is 1442. **RIP** Protocol Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. Usually ISP dynamically assigns IP address to you each time WAN IP Network you connect to it and request. In some case, your ISP provides Settings 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 32 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

	P Alias ( Mu Enable	Aux. WAN IP	Join NAT IP Pool
1.	<b>V</b>		
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
< <u>1.8   9-16   17-24   25-32</u> >> <u>Next</u> >>			

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

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

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

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

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

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

#### Details Page for PPTP/L2TP in WAN1 ~ WAN4

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.

PPTP/L2TP Client Mode		PPP Setup	
© Enable PPTP © Enable L2TP ⊙ Disable Server Address		PPP Authentication	PAP or CHAP 🔽
		Idle Timeout	180 second(s)
Specify Gateway IP Addre	55	IP Address Assignment Me (IPCP) WAN IP Alias	]
ISP Access Setup Username		Fixed IP: OYes ON Fixed IP Address WAN IP Network Settings	o (Dynamic IP)
Password		Obtain an IP address	,
MTU [	1442 (Max: 1460)	<ul> <li>Specify an IP address</li> <li>IP Address</li> </ul>	
		Subnet Mask	
	OK	Cancel	
PTP/L2TP Client Mod		lick this radio button to to a DSL modem on th	
		Click this radio button to the second state of	

WAN >> Internet Access

**Disable** – Click this radio button to close the connection through PPTP or L2TP.

**Server Address** - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.

**Specify Gateway IP Address** – Specify the gateway IP address for DHCP server.

ISP Access SetupUsername -Type in the username provided by ISP in this field.Password -Type in the password provided by ISP in this field.MTUIt means Max Transmit Unit for packet. The default setting is 1442.PPP SetupPPP Authentication - Select PAP only or PAP or CHAP for PPP.

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

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

Index	Enable	Aux. WAN IP	Join NAT IP Pool	
1.	<b>V</b>		$\checkmark$	
2.		0.0.0.0		
з.		0.0.0.0		
4.		0.0.0.0		
5.		0.0.0.0		
6.		0.0.0.0		
7.		0.0.0.0		
8.		0.0.0.0		
<< <u>1-8   9-16   17-24   25-32</u> >> <u>Next</u> >>				

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

Fixed IP Address - Type a fixed IP address.

**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.

WAN IP Network Settings

## **Details Page for PPP in WAN5**

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN5. The following web page will be shown.

WAN >> Internet Access				
WAN 5				
3G Modem	🔿 Enable 💿 Disable			
SIM PIN code				
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)		
APN Name		Apply		
Modem Initial String2	AT			
Modem Dial String	ATDT*99#	(Default:ATDT*99#)		
PPP Username		(Optional)		
PPP Password		(Optional)		
PPP Authentication	PAP or CHAP			
WAN Connection Detec	tion			
Mode ARP Detect 🛩				
Ping IP				
TTL:				
	ОК	Cancel		
nable / Disable IM PIN code	this function will in this page will b	activating this function. If you click <b>Disable</b> , be closed and all the settings that you adjuste e invalid. The SIM card that will be used to access		
Iodem Initial String	Such value is used	d to initialize USB modem. Please use the ou have any question, please contact to your		
PN Name		ss Point Name which is provided and require pe the name and click Apply.		
Iodem Initial String	2 The initial string i	The initial string is shared with APN.		
		ers may need another initial <i>AT</i> command to r do any special settings.		
Iodem Dial String		l to dial through USB mode. Please use the ou have any question, please contact to your		
PP Username	Type the PPP user	rname (optional).		
PP Password	Type the PPP pass	sword (optional).		
<b>PP</b> Authentication	Select PAP only	or <b>PAP or CHAP</b> for PPP.		
VAN Connection Detection	AN Connection Such function allows you to verify whether network connection			

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

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

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

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

## 3.1.4 Load-Balance Policy

WAN >> Load-Balance Policy

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

**Note:** Load-Balance Policy is running only when more than two WAN interfaces are activated.

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

ΟK

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

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

```
WAN >> Load-Balance Policy
```

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

Enable
--------

Check this box to enable this policy.

**Protocol** 

**Dest IP Start** 

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

Protocol	any	~
	any	
	TCP	
	UDP	
	TCP/UDP	
	ICMP	
	IGMP	

**Binding WAN interface** Choose the WAN interface (WAN1 / WAN2 / WAN3 / WAN4 /WAN5) for binding.

> Auto failover to other WAN – 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.

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.



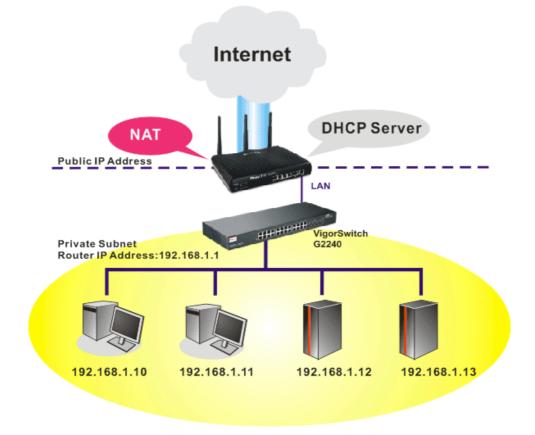
## 3.2 LAN

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.

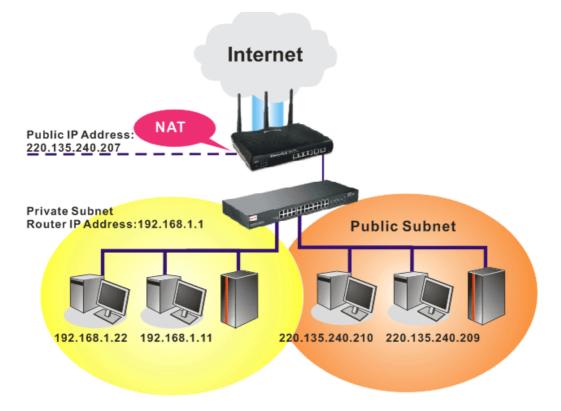


#### 3.2.1 Basics of LAN

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

Index	Display the number of LAN interface.	
Status Basically, LAN1 status is enabled in default.		
DHCP	LAN1 is configured with DHCP in default.	
IP Address	Display the IP address for LAN1. Such information is set in default.	
Details Page	Click it to access into the setting page.	

## **Details Page for LAN1**

#### LAN >> General Setup

LAN 1 Ethernet TCP / IP a	nd DHCP Setup				
Network Configuration For NAT Usage		OHCP Server Configuration O Enable Server O Disable Server			
IP Address 192.168.1.1		Relay Agent: OEnable ODisable			
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
 RIP Protocol Control	Disable 🗸	IP Pool Counts	50		
	Disable	Gateway IP Address	192.168.1.1		
		DHCP Server IP Address for Relay Agent			
		DNS Server IP Address			
		🔲 Force DNS manual se	tting		
		Primary IP Address			
		Secondary IP Address			

OK

IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).		
Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)		
RIP Protocol Control	<b>Disable</b> deactivates the RIP protocol. It will lead to a interruption of the exchange of routing information between routers.		
	RIP Protocol Control Disable 🔽 Disable Enable		
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.		
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.		
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.		
	<b>Relay Agent</b> –Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.		
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.10, the starting IP address must be 192.168.1.11 or greater, but smaller than 192.168.1.254.		
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is		

50 and the maximum is 253.

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

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

**DNS Server IP Address** DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

**Force DNS manual setting -** Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

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

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

System Status			System Uptime: 71:47:46
LAN Status	Primary	DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	347390	214004	

If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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



## 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.

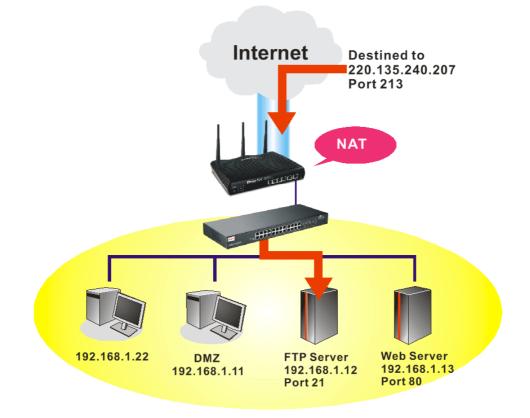
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

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 Redirection

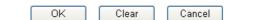
NAT >> Port Redirection

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

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.



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

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

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

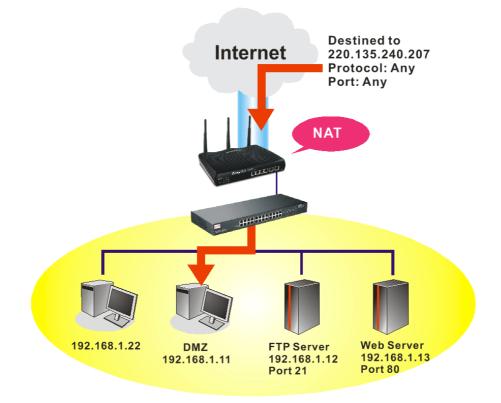
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This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

System Maintenance >> Management

fine Ports 🛛 Default Ports
ort 23 (Default: 23)
rt 80 (Default: 80)
ort 443 (Default: 443)
21 (Default: 21)
22 (Default: 22)
SNMP Agent
unity public
unity private
lost IP
nunity public
n Host IP
out 10 seconds
n

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

WAN1	WAN2	WAN3	WAN4	WAN5
11				
None	<b>~</b>			
Private IP			Choose P	С
MAC Address o	f the True IP DMZ Host	00.00.	00:00.00.00	
Note: When a always on.	True-IP DMZ host is t	urned on, it will force	e the router's WAN co	nnection to be

Enable

NAT >> DMZ Host Setup

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.

Z Host Setup				
WAN1	WAN2	WAN3	WAN4	WAN5
AN 1				
Private IP	~			
Private IP		192.168.1.1	11 Choose	PC
MAC Address	of the True IP DMZ Host	00.00.	00 00 . 00 . 00	
Note: When a always on.	I True-IP DMZ host is t	urned on, it will force	e the router's WAN o	connection to be

DMZ Host for WAN2 ~ WAN5 are slightly different with WAN1. See the following figure.

NAT >> DMZ Host Setup					
DMZ Host Setup					
WAN1	WAN2	WAN3	WAN4	WAN5	
WAN 3					
Enable		Private IP			
		0.0.0		Choose PC	
		ОК			

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2/WAN3/WAN4/WAN5 interface, you will find them in **Aux. WAN IP** for your selection.

DMZ Host Setup WAN1		WAN2	WAN3	WAN4	WAN5
WAN 3					
Index	Enable	Aux. WAN IP	Private IP		
1.		172.16.3.102	0.0.0		Choose PC
2.		172.16.3.200	0.0.0.0		Choose PC
			OK Clear	]	
Inable		Check to e	enable the DMZ H	lost function.	
rivate II		Enter the p PC to sele	private IP address ct one.	of the DMZ ho	st, or click Choose
Choose P	С	as depicted addresses	button and then a d below. The wind of all hosts in you in the list to be th	low consists of r LAN network	a list of private IP
		🕘 http://19	💶 🗖		
			58.1.10 58.1.18		

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.

## 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>				×
<u>10.</u>				×

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface for such NAT profile.
Aux. WAN IP	Display the WAN IP address specified in WAN IP Alias page. It will be hidden if WAN IP Alias page is not configured.
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	W	orts mment AN Interface cal Computer		V1 🔽 168.1.10	Cho	ose PC	
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP 💌	4500	4700	6.	💙	0	0
2.	UDP 🔽	4500	4700	7.	💙	0	0
з.	💙	0	0	8.	💙	0	0
4.	💙	0	0	9.	💙	0	0
5.	💌	0	0	10.	💙	0	0

Clear

Cancel

ΟK

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

## **3.4 Applications**

Below shows the menu items for Applications.

Ар	plications
1	Dynamic DNS
1	UPnP

#### 3.4.1 Dynamic DNS

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

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

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

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

Dynamic DNS Setu	IP	<u>Set</u>	to Factory Default
Enable Dynamic DNS Setup		View Log	Force Update
Auto-Update into	erval 14400 Min(s) (1~14400)	)	
Accounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		×
<u>2.</u>	WAN1 First		×
<u>3.</u>	WAN1 First		×

Applications >> Dynamic DNS Setup

Enable Dynamic DNS Setup	Check this box to enable DDNS function.	
Set to Factory Default	Clear all profiles and recover to factory settings.	
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.	
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).	
WAN Interface	Display the WAN interface used.	
Domain Name	Display the domain name that you set on the setting page of DDNS setup.	



Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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

Index : 1			
Enable Dynamic DNS Account			
WAN Interface	WAN1 First		
Service Provider	dyndns.org (www.dyndns.org)		
Service Type	Dynamic 💌		
Domain Name	chronic6853 dyndns.info 💙		
Login Name	chronic6853 (max. 64 characters)		
Password	••••••••		
🔲 Wildcards			
📃 Backup MX			
Mail Extender			
Enable Dynamic DI Account WAN Interface	<ul> <li>NS 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).</li> <li>WAN1/WAN2/WAN3/WAN4/WAN5 First - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the first channel for such account. If WAN1/WAN2/WAN3 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3/WAN4/WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the only channel for such account.</li> </ul>		
Service Provider	Select the service provider for the DDNS account.		
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.		
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.		
Login Name	Type in the login name that you set for applying domain.		
Password	Type in the password that you set for applying domain.		
Wildcard and Back MX	The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.		

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



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

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

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

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

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

#### 3.4.2 UPnP

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

Applications >> UPnP

UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

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



## Enable UPNP Service

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

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

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

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



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

The reminder as regards concern about Firewall and UPnP

#### Can't work with Firewall Software

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

#### **Security Considerations**

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

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

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

## **3.5 Wireless LAN**

This function is used for "n" models.

#### 3.5.1 Basic Concepts

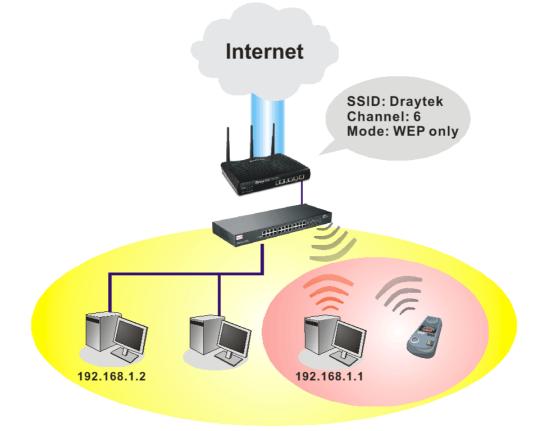
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The 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.

Wireless LAN	
General Setup	
Security	
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
11101000			General	ootup

able Wireless LAN	
Mode :	Mixed(11b+11g+11n) 👻
SSID:	DrayTek
Channel :	Channel 6, 2437MHz
Packet-OVERDRIVE <sup>™</sup>	
Tx Burst	
Note:	
	and the second
The same technology mus	t also be supported in clients to boost WLAN performance.
The same technology mus  Hide SSID	t also be supported in clients to boost WLAN performance.
	t also be supported in clients to boost WLAN performance.
Hide SSID Long Preamble Hide SSID: prevent SSID f	

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) mode.

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

SSID

Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.

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

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

Packet-OVERDRIVEThis feature can enhance the performance in data transmission<br/>about 40% \* more (by checking **Tx Burs**t). It is active only<br/>when both sides of Access Point and Station (in wireless client)<br/>invoke this function at the same time. That is, the wireless<br/>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 Auto launch when Windows gtart up Remember mini status gosition Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile	Advance Setting Disable Radio Fragmentation Threshold : R IS Threshold : Frequency : Ad-hoc Channel:	2346 2347 802.11b/g/n - 2.4GH 🗸 1 👻
Group Roaming Ad-hoc  WLAN type to connect  Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only Ad-hoc network only Automatically connect to non-preferred networks	Power Save Mode: Tx <u>B</u> urst :	Disable V Disable V
	OK	Cancel Apply
Tx <u>B</u> urst : Disal Disal Enab	ole	*

devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

Hide SSID
 Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
 Long Preamble
 This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network

#### 3.5.3 Security

Wireless LAN >> Security Settings

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

Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.

Mode:	Disable 💌
WPA:	
Encryption Mode:	TKIP for WPA/AES for WPA2
Pre-Shared Key(PSK):	****
Type 8~63 ASCII character "cfgs01a2" or "0x655abco	r or 64 Hexadecimal digits leading by "0x", for example 1".
WEP:	
Encryption Mode:	64-Bit 💙
● Key 1 :	****
○Key 2 :	****
○Key 3 :	****
○Key 4 :	****
"0x4142333132". For 128 bit WEP key	adecimal digits leading by "0x", for example "AB312" or

Mode

WPA

There are several modes provided for you to choose.

Cancel

Mode:

OK



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

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

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

**WPA2/PSK-**Accepts only WPA2 clients and the encryption key should be entered in PSK.

**Mixed (WPA+ WPA2)/PSK -** Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered

manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**Type** - Select from Mixed (WPA+WPA2) or WPA2 only.

**Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

**128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

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

Encryption Mode:



WEP

## 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.

Access Control			
Enable Access Control			
Policy	: Activate MAC address filter 💌		
MAC Address Filter Index Attribute MAC Address			
Client's MAC Address : : : : : : : : : : : : : : : : : :			
	Add Delete Edit Cancel		
OK       Clear All         Enable Access Control       Select to enable the MAC Address access control feature.         Policy       Select to enable any one of the following policy. Choose Activate MAC address filter to type in the MAC addresses			
for other clients in the network manually. Choose <b>Isolate</b> <b>WLAN from LAN</b> will separate all the WLAN stations from LAN based on the MAC Address list.			
	Policy : Activate MAC address filter  Activate MAC address filter Isolate WLAN from LAN		
MAC Address Filter	Display all MAC addresses that are edited before.		
Client's MAC Address	Manually enter the MAC address of wireless client.		
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.		
Add	Add a new MAC address into the list.		
Delete	Delete the selected MAC address in the list.		

Wireless LAN >> Access Control



Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

#### 3.5.5 Station List

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

Station List				
	Status	MAC Address	Associated with	
		Refresh		
	Status Codes :	Renear		
	C: Connected, N	lo encryption.		
	E: Connected, V P: Connected, V			
	A: Connected, V	VPA2.		
	B: Blocked by A N: Connecting.	ccess Control.		
		VPA/PSK authentication.		
	Notes Africa a st			
		ation connects to the rout ut notice. In that case, it	will still be on the list until the	
	connection expi	res.		
	Add to <u>Access C</u>	ontrol :		
	Client's MAC add	dress ::::		
		Add		
0 1				
efresh		Click this button to	refresh the status of station list	ι.

# **3.6 USB Application**

USB diskette connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN/WAN can access, write and read data stored in USB diskette with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application**>**USB User Management** on the client software. Then, the client can use the FTP site (USB diskette) or share the Samba service through Vigor router.



Access Control.



#### 3.6.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB diskette with formats of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB diskette is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

USB General Settings	
General Settings	
Simultaneous FTP Connections	s 5 (Maximum 6)
Default Charset	Default 🗸
Samba Service Settings(Networ	k Neighborhood)
⊙ Enable ◯ Disable	
Access Mode	
● LAN Only ● LAN And WAN	1
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor
better performance. 3. A workgroup name mus name can have as many s	uch as FileZilla, you may limit client connections setting to 1 to get st not be the same as the host name. The workgroup name and the host as 15 characters and a host name can have as many as 23 characters , any of the following: . ; : " <> * + = / \   ?.
	OK
General Settings	<b>Simultaneous FTP Connection -</b> This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTI sessions connecting to USB storage diskette at one time.
	<b>Default Charset -</b> At present, Vigor router supports three type of character sets: default, GB2312 and BIG5.
	Default Default GB2312 BIG5
	Default Charset is for English based file name. For Simplified Chinese file/directory names, please choose GB2312; for Traditional Chinese file/directory names, choose BIG5.
Samba Service Settings	Click <b>Enable</b> to invoke samba service via the router.
Access Mode	<b>LAN Only</b> – Users coming from internet cannot connect to the samba server of the router.

LAN And WAN - Both LAN and WAN users can



NetBios Name ServiceFor the NetBios service of USB diskette, you have to specify a<br/>workgroup name and a host name. A workgroup name must not<br/>be the same as the host name. The workgroup name can have as<br/>many as 15 characters and the host name can have as many as<br/>23 characters. Both them cannot contain any of the<br/>following---; : " <> \* + = \| ?.Workgroup Name – Type a name for the workgroup.<br/>Host Name – Type the host name for the router.

#### 3.6.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB diskette must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB diskette first. Otherwise, an error message will appear to warn you.

USB Application >>	USB User	Management
--------------------	----------	------------

USB User Ma	nagement			5	Set to Factory Default
Index	Username	Home Folder	Index	Username	Home Folder
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

Click index number to access into configuration page.

```
USB Application >> USB User Management
```

Profile Index: 1	
FTP/Samba User	🔿 Enable 🛛 💿 Disable
Username	
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	201 201
Access Rule	
File	🗌 Read 📃 Write 🔲 Delete
Directory	List Create Remove
Note: The folder name can only contain the and space.	e following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) /
OK	Clear Cancel

#### FTP/Samba User

**Enable** – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.



	<b>Disable</b> – Click this button to disable such profile.
Username	Type the username for FTP/Samba users for accessing into FTP server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.
	<b>Note:</b> "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
	Note: FTP Passive mode is not supported by Vigor Router.
	Please disable the mode on the FTP client.
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage diskette.
<b>Confirm Password</b>	Type the password again to make confirmation.
Home Folder	It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB diskette. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB diskette. <b>Note:</b> When write protect status for the USB diskette is <b>ON</b> , you cannot type any new folder name in this field. Only "/" can be used in such case.

You can click  $\overleftrightarrow$  to open the following dialog to add any new folder which can be specified as the Home Folder.

🗿 http://192.168.1.5/doc/ftpuserfolder.htm - Microsoft Internet Explorer	
USB User Management	~
	-
Choose Folder	_
Folder Name	
Create New Home Folder	
Folder Name:	
test	
Create	
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) and space. Only 11 characters are allowed.	t
	Y

Access Rule

It determines the authority for such profile. Any user, who uses such profile for accessing into USB diskette, must follow the rule specified here.

**File** – Check the items (Read, Write and Delete) for such profile.

**Directory** –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB diskette into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

#### 3.6.3 File Explorer

File Explorer offers an easy way for users to review and manage the content of USB diskette connected on Vigor router.

USB Application >> File Explorer								
File Exp	lorer							
<del>4)</del>	•	<b>2</b>	Current Path: /					
			Name			Size	Delete	Rename
A 11-1-	-1.521-							
🕇 Upla	ad File							
Select a file:								
Uploa	ad		Diowse.					

Note: The folder can not be deleted when it is not empty.

** Refresh	Click this icon to refresh files list.
<b>†</b> Back	Click this icon to return to the upper directory.
📁 Create	Click this icon to add a new folder.
<b>Current Path</b>	Display current folder.
Upload	Click this button to upload the selected file to the USB diskette. The uploaded file in the USB diskette can be shared for other user through FTP.

#### 3.6.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB diskette) via the Vigor router. If you want to remove the diskette from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB diskette later.

JSB Application >> USB Disk Status				
USB Mass Storage Device Sta	tus			
Connection Status: No Dis	k Connected	Disconnect USB Disk		
Disk Capacity: 0 MB				
Free Capacity: 0 MB <u>Ref</u>	esh			
USB Disk Users Connected		<u>Refresh</u>		
Index Service	IP Address(Port)	Username		

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.



Connection Status	If there is no USB diskette connected to Vigor router, " <b>No Disk Connected</b> " will be shown here.
Disk Capacity	It displays the total capacity of the USB diskette.
Free Capacity	It displays the free space of the USB diskette. Click <b>Refresh</b> at any time to get new status for free capacity.
Index	It displays the number of the client which connecting to FTP server.
IP Address	It displays the IP address of the user's host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB diskette into the Vigor router, the system will start to find out such device within several seconds.

# 3.7 System Maintenance

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

Below shows the menu items for System Maintenance.

System Maintenance	
System Status	
User Password	
Time and Date	
Reboot System	

#### 3.7.1 System Status

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

#### System Status

Model Name Firmware Version Build Date/Time

	vigorszuun	
1	3.3.6_RC6	
1	Nov 3 2010	15:47:14

		LAN			
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-C9-B7-3C	192.168.1.1	255.255.255.0	Yes	168.95.1.1
LAN2	00-50-7F-C9-B7-3C	192.168.3.1	255.255.255.0	Yes	168.95.1.1
LAN3	00-50-7F-C9-B7-3C	192.168.5.1	255.255.255.0	Yes	168.95.1.1
LAN4	00-50-7F-C9-B7-3C	192.168.7.1	255.255.255.0	Yes	168.95.1.1
DMZ PORT	00-50-7F-C9-B7-3C	192.168.9.1	255.255.255.0	Yes	168.95.1.1
IP Routed Subnet	00-50-7F-C9-B7-3C	192.168.2.1	255.255.255.0	Yes	168.95.1.1

	Wireless LA	N	
MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-C9-B7-3C	Europe	2.3.2.0	DrayTek

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-50-7F-C9-B7-3D			
WAN2	Connected	00-50-7F-C9-B7-3E	Static IP	172.16.3.102	172.16.1.1
WAN3	Disconnected	00-50-7F-C9-B7-3F			
WAN4	Disconnected	00-50-7F-C9-B7-40			
WAN5	Disconnected	00-50-7F-C9-B7-41			

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware built.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.
Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
Wireless LAN	



MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
SSID	Display the SSID of the router.
WAN	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.

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

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

## 3.7.3 Time and Date

System Maintenance >> Time and Date

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

```
Time Information
        Current System Time
                                                                     Inquire Time
                                2010 Apr 2 Fri 6 : 7 : 57
 Time Setup
         🔘 Use Browser Time
         Ose Internet Time Client
           Server IP Address
                                           pool.ntp.org
                                           (GMT) Greenwich Mean Time : Dublin
           Time Zone
                                                                              Y
          Enable Daylight Saving
                                           Automatically Update Interval
                                           30 min 🔽
                                        ΟK
                                                   Cancel
Current System Time
                             Click Inquire Time to get the current time.
Use Browser Time
                             Select this option to use the browser time from the remote
                             administrator PC host as router's system time.
Use Internet Time
                             Select to inquire time information from Time Server on the
                             Internet using assigned protocol.
Time Protocol
                             Select a time protocol.
Server IP Address
                             Type the IP address of the time server.
Time Zone
                             Select the time zone where the router is located.
Enable Daylight Saving
                             Check the box to activate daylight saving function. Such feature
                             is useful for some areas.
Automatically Update
                             Select a time interval for updating from the NTP server.
Interval
Click OK to save these settings.
```

#### 3.7.4 Reboot System

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

System Maintenance >> Reboot System		
Reboot System		
	Do you want to reboot your router ?	
	Our State	
<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.

## 3.8 Diagnostics

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

Diagnostics	
DHCP Table	
Traffic Graph	
Ping Diagnosis	
Trace Route	

#### 3.8.1 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

```
DHCP IP Assignment Table
                                                                                                             <u>Refresh</u>
LAN1
               : 192.168.1.1/255.255.255.0, DHCP server: On
           IP Address MAC Address Leased Time
192.168.1.10 E0-CB-4E-DA-48-79 0:00:09.810
Index
                                                                                          HOST ID
                                                                                          carrie-Oc7cb251
1

        192.168.1.255
        00-50-7F-C9-B7-3C
        CONFLICTED IP

        192.168.1.0
        00-50-7F-C9-B7-3C
        CONFLICTED IP

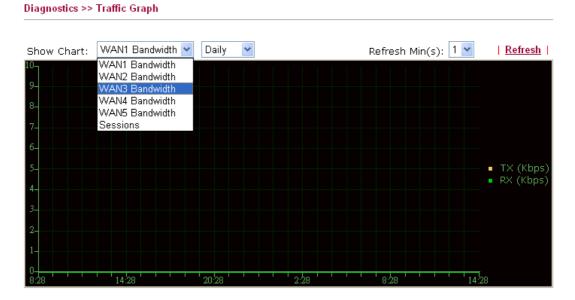
        192.168.1.1
        00-50-7F-C9-B7-3C
        CONFLICTED IP

2
3
4
DMZ Port : 192.168.9.1/255.255.255.0, DHCP server: On
Index IP Address
                                 MAC Address
                                                                                           HOST ID
                                                                   Leased Time
           192.168.9.255 00-50-7F-C9-B7-3C
1
                                                                    CONFLICTED IP
2
           192.168.9.0 00-50-7F-C9-B7-3C
                                                                  CONFLICTED IP
3
           192.168.9.1
                                 00-50-7F-C9-B7-3C
                                                                   CONFLICTED IP
```

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

## 3.8.2 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time. The following two figures display different charts by daily and weekly.



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/WAN4/WAN5 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

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

#### 3.8.3 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

Ping Diagnosis			
which WAN	Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified". Ping through: Unspecified 🛩		
Ping to:	Host / IP 🔽 Host / IP	IP Address:	
Result	DNS Gateway 1 Gateway 2 Gateway 3 Gateway 4 Gateway 5	<u>Clear</u>	
	<u>e alenaj e</u>		

#### **Ping through**

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.



Unspecified	*
Unspecified	
WAN1	
WAN2	
WAN3	
WAN4	
WAN5	

Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

#### 3.8.4 Trace Route

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			
	ace through: otocol:	Unspecified V	
Hos	st / IP Address:		Run
Re	sult		<u>Clear</u>
			~

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Unspecified	*
Unspecified	
WAN1	
WAN2	
WAN3	
WAN4	
WAN5	

Protocol

**Trace through** 

Choose the protocol for using trace route.





Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

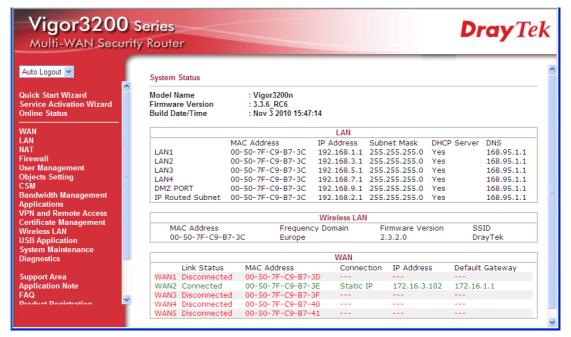
.

# **4** Admin Mode Operation

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

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

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



## 4.1 WAN

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

## 4.1.1 Basics of Internet Protocol (IP) Network

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

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



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

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

#### Get Your Public IP Address from ISP

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

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

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

For 3G mobile communication through Access Point is popular more and more, Vigor3200 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3200, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor3200n 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 the LAN port on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor3200n, and enjoy the powerful firewall, bandwidth management, VPN features of Vigor3200n series.



After connecting into the router, 3G USB Modem will be regarded as the fifth WAN port. However, the other Ethernet WAN ports 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 other Ethernet WAN ports are not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on DrayTek web site. Please visit www.DrayTek.com for more detailed information.

Below shows the menu items for WAN.





WAN >> General Setup

#### 4.1.2 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 to WAN5 in details.

There are four WAN ports (represented with WAN1, WAN2, WAN3 and WAN4 in web pages) and one USB port (represented with WAN5 in web pages) offered by the router. For this router supports multiple WANs function, it allows users to access Internet and combine the bandwidth of the multiple WANs to speed up the transmission through the network. Each WAN port can connect to different ISPs, even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation.

This webpage allows you to set general setup for WAN1 to WAN5 respectively.

Load Bal	ance Mode	e: Auto Weight 💌			
Setup		Physical	Line Speed(Kbps)		
Index	Enable	Mode/Type	DownLink/UpLink	Active Mode	Backup WAN
WAN1	V	Ethernet/Auto negotiation	10000/10000	Always On	-
WAN2	V	Ethernet/Auto negotiation	10000/10000	Always On	-
WAN3	V	Ethernet/Auto negotiation	10000/10000	Backup	-
WAN4	V	Ethernet/Auto negotiation	10000/10000	Backup	-
WAN5	V	USB/-	2000/384	Always On	-

From the above figure, WAN1 ~ WAN4 connect to Internet through the interface of Ethernet; WAN5 connects to Internet via USB interface. Therefore the configuration for each WAN port will be different slightly. Please click the WAN link under Index to open the web page for detailed configuration.

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

Display the downstream and upstream rate of such WAN

**Dray** Tek

Line Speed

	interface.
Active Mode	Display whether such WAN interface is Active device or backup device.
Backup WAN	Display the Backup WAN interface for such WAN when it is disabled.
Note: In default, eac	ch WAN is enabled.

#### For WAN1 ~ WAN4

WAN1 ~ WAN4 are fixed with physical mode of Giga Ethernet. Here we take WAN1 as an example.

WAN >> General Setup

WAN 1			
Enable:	Yes 💌		
Display Name:			
Physical Mode:	Ethernet		
Physical Type:	Auto negotiation 💌		
Line Speed(Kbps):			
DownLink	10000		
UpLink	10000		
VLAN Tag insertion:	Disable 💙 (Please configure Internet Access setting first)		
Tag value:	0 (0~4095)		
Priority:	0 (0~7)		
Active Mode:	Always On 🔽		
Backup WAN:	None 💌		
Enable	Choose <b>Yes</b> to invoke the settings for this WAN interface. Choose <b>No</b> to disable the settings for this WAN interface.		
Display Name	Type the description for such WAN interface.		
Physical Mode	Display the physical mode of such WAN interface.		
Physical type	You can change the physical type for WAN2 or choose <b>Auto negotiation</b> for determined by the system.		
	Physical Type: Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex		

Line SpeedIf your choose According to Line Speed as the Load Balance<br/>Mode, please type the line speed for downloading and<br/>uploading for such WAN interface. The unit is kbps. The<br/>default setting for down link and up link is 10000Kbps.VLAN Tag insertionEnable – Enable the function of VLAN with tag.

100M full duplex

The router will add specific VLAN number to all packets on the

WAN while sending them out.

**Disable** – Disable the function of VLAN with tag.

**Tag value** – Type the value as the VLAN ID number. The range is form 0 to 4095.

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

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



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

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

Active Mode: A	Always On 🔽
Backup WAN: N	Jone 🚩

If you choose **Backup** as the **Active Mode**, Backup WAN will be changed into **Backup Type**. You have to specify which role the WAN interface should play.



When any WAN disconnect – WAN1 will be activated when any WAN interface disconnects.

**When all WAN disconnect** – WAN1 will be activated when all the WAN interfaces disconnect.

# For WAN5

To use 3G network connection through 3G USB Modem, please configure WAN5 interface.

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

WAN 5			
Enable:	Yes 💌		
Display Name:			
Physical Mode:	USB		
Physical Type:	Auto negotiation 👻		
Line Speed(Kbps):			
DownLink	2000		
UpLink	384		
Active Mode:	Always On V		
Backup WAN:			
	OK Cancel		
Enable	Choose <b>Yes</b> to invoke the settings Choose <b>No</b> to disable the settings		
Display Name	Type the description for such WA	N interface.	
Physical Mode	Display the physical mode of such	h WAN interface.	
Physical type	For such WAN interface is fixed to USB network connection, it is not necessary to specify physical type.		
Line Speed	If your choose <b>According to Line Speed</b> as the <b>Load Balance</b> <b>Mode</b> , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.		
Active Mode and Backup WAN/Backup Type	<b>Active Mode</b> – Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface (Backup WAN).		
	Always On <mark>.</mark> Alwaγs On Backup		
	Backup WAN/Backup Type – D WAN interface. It will be change Mode specified.		
	If you choose <b>Always On</b> as <b>Active Mode</b> , you can choose of of the backup WAN interfaces from the <b>Backup WAN</b> drop down list. Later, when such WAN is disconnected for some reason, the backup WAN will be activated automatically to prevent data transmission from connection interrupted.		
		N 17	
	Active Meder	Aluque On M	
	Active Mode:	Always On 🔽	

If you choose **Backup** as the **Active Mode**, Backup WAN will



be changed into Backup Type. You have to specify which role the WAN interface should play.

Active Mode:	Backup 😽
Backup Type (Only for Backup Multiple WAN):	♥ When any WA ♥ When all WAN

AN disconnect N disconnect

When any WAN disconnect - WAN5 will be activated when any WAN interface disconnects.

When all WAN disconnect – WAN5 will be activated when all the WAN interfaces disconnect.

#### **4.1.3 Internet Access**

For the router supports multi-WAN function, the users can set different WAN settings (for WAN1/WAN2/WAN3/WAN4/WAN5) for Internet Access. Due to different Physical Mode of WAN interface, the Access Mode for these connections also varies. Refer to the following figures.

WAN >> Internet Access

dex Display Name	Physical Mode	Access Mode	
AN1	Ethernet	None 🔽 🔽	etails Page
AN2	Ethernet	Static or Dynamic IP 🛛 🖌 🗖	etails Page
ANB	Ethernet	None PPPoE	etails Page
N4	Ethernet	Static or Dynamic IP	etails Page
N5	USB	None 🔽 🗖	tails Page

#### WAN >> Internet Access

Index Display Name	Physical Mode	Access Mode		
WAN1	Ethernet	None	~	Details Page
WAN2	Ethernet	Static or Dynamic IP	~	Details Page
WAN3	Ethernet	None	*	Details Page
WAN4	Ethernet	None	*	Details Page
WAN5	USB	None	~	Details Page
		None		
		IPPP		

Index	Display the WAN interface.
Display Name	It shows the name of the WAN1/WAN2/WAN3/WAN4/WAN5 that entered in general setup.
Physical Mode	It shows the physical connection for WAN1-WAN4 (Ethernet) /WAN5 (3G USB Modem) according to the real network

connection.

Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click <b>Details Page</b> for accessing the page to configure the settings.
Details Page	This button will open different web page according to the access mode that you choose in WAN interface

# Details Page for PPPoE in WAN1 ~ WAN4

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

PPPoE Client Mode		PPP/MP Setup		
🔘 Enable 🛛 💿 Disable		PPP Authentication	PAP or CHAP 🔽	
ISP Access Setup		Idle Timeout	-1 second(s)	
Username		IP Address Assignment M	ethod	
Password		(IPCP) WAN IP Alias Fixed IP: O Yes O No	) (Dynamic ID)	
Index(1-15) in <u>Schedule</u> S =>,,	etup: ,	Fixed IP Address		
		Oefault MAC Addre	SS	
WAN Connection Detection Mode ARP Detect V		Specify a MAC Address		
Mode /	ARP Detect 🚩	MAC Address: 00 .50 .7F :C9 .1	87 · 3D	
TTL:				
МТU [1	442 (Max: 1492)			
PPoE Client Mode		be closed and all the	on. If you click <b>Disable</b> settings that you adjuste	
SP Access Setup		ted username, passwo ding to the informatio	rd and authentication n provided by your ISP	
	<b>Username</b> – Typ field.	e in the username pro	vided by ISP in this	
	Password – Type	e in the password prov	vided by ISP in this field	
	time schedule for previously in <b>Ap</b>	your request. All the	e web page and you can	
/AN Connection etection		ows you to verify whe ough ARP Detect or F	ether network connection Ping Detect.	
	Mode – Choose	ARP Detect or Ping I	Detect for the system to	



execute for WAN detection.

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

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

**PPP/MP SetupPPP Authentication** – Select **PAP only** or **PAP or CHAP** for<br/>PPP. If you want to connect to Internet all the time, you can<br/>check **Always On**.

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

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

**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to **32** public IP addresses other than the current one you are using.

Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

	Enable	Aux. WAN IP	Join NAT IP Pool
1.			
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
< <u>1-8</u>	<u>9-16   17-</u>	<u>24   25-32</u> >>	<u>Next</u> >>

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

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

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

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



#### Details Page for Static or Dynamic IP in WAN1 ~ WAN4

WAN >> Internet Access

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) <ul> <li>Enable</li> <li>Disable</li> </ul>		WAN IP Network Settings WAN IP Alias O Obtain an IP address automatically		
Keep WAN Connection		Router Name Vigo	r *	
Enable PING to keep PING to the IP	eep alive	Domain Name * : Required for som	* ne ISPs	
		Specify an IP address		
PING Interval	0minute(s)	IP Address	172.16.3.102	
WAN Connection Dete	ection	Subnet Mask	255.255.0.0	
Mode	ARP Detect 🐱	Gateway IP Address	172.16.1.1	
Ping IP		DNS Server IP Address		
TTL:		Primary IP Address	168.95.1.1	
МТU	1442 (Max: 1500)	Secondary IP Addre	SS	
		🛑 💿 Default MAC Add	dress	
RIP Protocol		🔘 Specify a MAC A	ddress	
Enable RIP		MAC Address:	.B7 .3E	
	ОК	Cancel		

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 Enable PING to keep alive box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation. WAN Connection Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Detection Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you



have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command. MTU It means Max Transmit Unit for packet. The default setting is 1442. **RIP** Protocol Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. Usually ISP dynamically assigns IP address to you each time WAN IP Network you connect to it and request. In some case, your ISP provides Settings 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 32 public IP addresses other than the current one you are using. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<b>V</b>		
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
< <u>1-8</u>	<u>9-16   17-</u>	2 <u>4</u>   <u>25-32</u> >>	<u>Next</u> >>

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

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

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

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

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

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

## Details Page for PPTP/L2TP in WAN1 ~ WAN4

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

WAN 2				
PPTP/L2TP Client Mode		PPP Setup		
🔵 Enable PPTP 🛛 🔿 E	nable L2TP 💿 Disable	PPP Authentication	PAP or CHAP 🔽	
Server Address		Idle Timeout	-1 second(s)	
Specify Gateway IP Addr	fy Gateway IP Address		IP Address Assignment Method	
172.16.1	1.1	(IPCP) WAN IP Alias		
		- Fixed IP: 🔘 Yes 📀	No (Dynamic IP)	
ISP Access Setup		Fixed IP Address		
Username		WAN IP Network Setting	js	
Password		🔘 Obtain an IP addre	Obtain an IP address automatically	
Index(1-15) in <u>Schedule</u>	Setup:	Specify an IP addre	ess	
=>,,	,	IP Address	172.16.3.102	
MTU	1442 (Max: 1460)	Subnet Mask	255.255.0.0	
	OK	Cancel		
PTP/L2TP Client Mode Enable PPTP establish a tun			on to enable a PPTP client on the WAN interface.	
			on to enable a L2TP clien n on the WAN interface.	
	<b>Disable</b> – Click through PPTP c	this radio button to c or L2TP.	close the connection	
		<b>s</b> - Specify the IP add able PPTP/L2TP clie	ress of the PPTP/L2TP nt mode.	
	<b>Specify Gatew</b> for DHCP serve		cify the gateway IP addre	
SP Access Setup	Username -Typ	pe in the username pr	ovided by ISP in this field	
	Password -Typ	e in the password pro	ovided by ISP in this field	
	time schedule for previously in <b>A</b>	or your request. All th	ou can type in four sets on the schedules can be set alle web page and you can hat web page.	
ITU	It means Max is 1442.	Transmit Unit for p	acket. The default setti	
PP Setup	<b>PPP Authentic</b> PPP.	ration - Select PAP o	nly or PAP or CHAP for	
		Set the timeout for be rough the time withou	reaking down the Internet at any action.	
P Address Assignme Iethod(IPCP)			e public IP addresses and N interface, please use	

#### WAN >> Internet Access



Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.			
2.		0.0.0.0	
з.		0.0.0.0	
4.		0.0.0.0	
5.		0.0.0.0	
6.		0.0.0.0	
7.		0.0.0.0	
8.		0.0.0.0	
< <u>1-8</u>	<u>9-16   17-</u>	<u>24   25-32</u> >>	<u>Next</u> >

WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

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

Fixed IP Address - Type a fixed IP address.

#### WAN IP Network Settings

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

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

IP Address – Type the IP address.

Subnet Mask – Type the subnet mask.

## **Details Page for PPP in WAN5**

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN5. The following web page will be shown.

N 5		
3G Modem	○Enable ⊙Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Initial String2	AT	
Modem Dial String	ATDT*99#	(Default: ATDT * 99#)
PPP Username		(Optional)
PPP Password		(Optional)
PPP Authentication	PAP or CHAP 🔽	
Index(1-15) in <u>Sched</u>	<u>ile</u> Setup:	
=>,	,,	
WAN Connection Detec	tion	
Mode	ARP Detect 💌	
Ping IP		
TTL:		

OK

Cancel

Enable / Disable	Click <b>Enable</b> for activating this function. If you click <b>Disable</b> , this function will be closed and all the settings that you adjusted in this page will be invalid.
SIM PIN code	Type PIN code of the SIM card that will be used to access Internet.
Modem Initial String	Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.
APN Name	APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.
Modem Initial String2	The initial string 1 is shared with APN.
	In some cases, users may need another initial <i>AT</i> command to restrict 3G band or do any special settings.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).
Index (1-15) in Schedule	You can type in four sets of time schedule for your request. All

Setup	the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.	
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.	
	<b>Mode</b> – Choose <b>ARP Detect</b> or <b>Ping Detect</b> for the system to execute for WAN detection.	
	<b>Ping IP</b> – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.	
	<b>TTL</b> ( <b>Time to Live</b> ) – Displays value for your reference. TTL value is set by telnet command.	

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

## 4.1.4 Load-Balance Policy

WAN >> Load-Balance Policy

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

**Note:** Load-Balance Policy is running only when more than two WAN interfaces are activated.

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

ΟK

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

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

```
WAN >> Load-Balance Policy
```

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

Enable

Check this box to enable this policy.

**Protocol** 

**Dest IP Start** 

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

Protocol	any	*
	any	
	ТСР	
	UDP	
	TCP/UDP	
	ICMP	
	IGMP	

**Binding WAN interface** Choose the WAN interface (WAN1 / WAN2 / WAN3 / WAN4 / WAN5) for binding.

> Auto failover to other WAN – 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.

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.



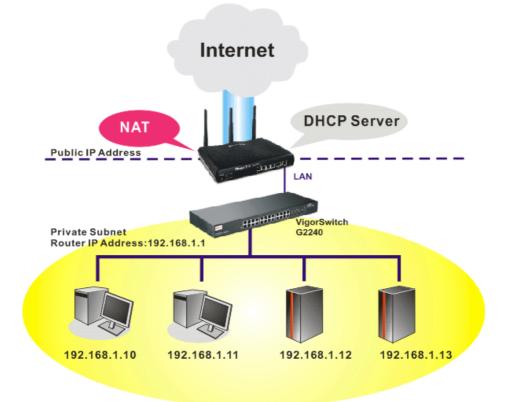
## 4.2 LAN

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.

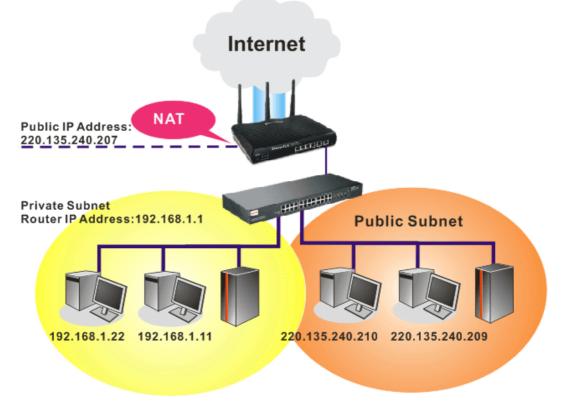
LAN	
🕩 General Set	tup
Static Rout	e
VLAN	
🕨 🕨 Bind IP to N	AC
🕨 🕨 LAN Port M	irror

## 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)

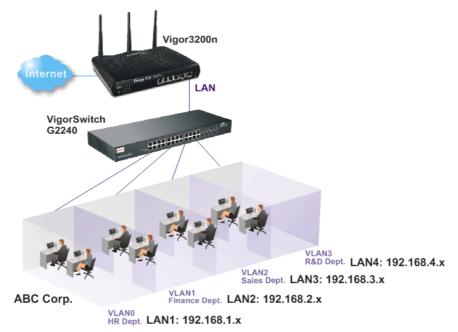
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### 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 port 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. Vigor3200 series provides four LANs, one DMZ and one IP Routed Subnet.

Click LAN to open the LAN settings page and choose General Setup.

There are four subnets provided by the router which allow users to divide groups into different subnets (LAN1 – LAN4). In addition, different subnets can link for each other by configuring Inter-LAN Routing. At present, LAN1 setting is fixed with NAT mode only. LAN2 – LAN4 can be operated under NAT or Route mode. IP Routed Subnet can be operated under Route mode.

#### LAN >> General Setup

General Setup				
Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page
LAN 2		✓	192.168.3.1	Details Page
LAN 3			192.168.5.1	Details Page
LAN 4		<b>~</b>	192.168.7.1	Details Page
DMZ	V	V	192.168.9.1	Details Page
IP Routed Subnet		<b>V</b>	192.168.2.1	Details Page

#### Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1					
LAN 2		<b>V</b>			
LAN 3			<b>V</b>		
LAN 4				<b>V</b>	
DMZ PORT	<b>~</b>			<ul><li>✓</li></ul>	<b>V</b>

ΟK

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

#### General Setup-----Allow to configure settings for each subnet respectively. Index Display all of the LAN items, DMZ and IP Routed Subnet. Status Check the box to enable such LAN configuration. Basically, LAN1 status is enabled in default. LAN2, LAN3, LAN4 and IP Routed Subnet can be observed by checking the box of Status. DHCP Check the box to enable DHCP server for such LAN configuration. LAN1 is configured with DHCP in default. If required, please check the DHCP box for each LAN. **IP Address** Display the IP address of the LAN configuration. Display the IP address for each LAN item. Such information is set in default and you can not modify it. **Details Page** Click it to access into the setting page. Each LAN will have different LAN configuration page. Each LAN must be configured in different subnet. Inter-LAN Routing --- Check the box to allow to link or route two subnets. Subnet Display four LANs and one DMZ PORT available for routing. LAN 1 ~ LAN 4, DMZ Check the box to make the routing among LANs. PORT

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



## LAN 1

LAN1 is the default configuration for basic host connection.

I AN	>>	General	Setup
LOU		ocherui	Setup

LAN 1 Ethernet TCP / IP a	nd DHCP Setup		
LAN 1 Ethernet TCP / IP a Network Configuration For NAT Usage IP Address Subnet Mask RIP Protocol Control	192.168.1.1 255.255.255.0 Disable	DHCP Server Configuration Carbon Enable Server Consel Relay Agent: Enable ( Start IP Address IP Pool Counts Gateway IP Address DHCP Server IP Address for Relay Agent	ole Server
		DNS Server IP Address Force DNS manual se Primary IP Address Secondary IP Address	tting
		OK	

Network Configuration	Set IP address and Subnet Mask for clients connected via LAN1.
	<b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
<b>RIP Protocol Control</b>	<b>Disable</b> deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server -</b> Let you manually assign IP address to every host in the LAN.
	<b>Relay Agent -</b> Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must

be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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

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

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

DNS Server IP Address DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

**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: 71:47:4
LAN Status	Primary	DNS: 194.109.6.66	Secondary DNS: 168.95.1.
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.



## LAN 2, LAN 3, LAN 4

LAN >> General Setup

With the multi-subnet feature offered by Vigor router, LAN2 ~ LAN4 are used for different subnets.

Network Configuration		DHCP Server Configurat	ion
🔘 Enable 🛛 💿 Disable		📀 Enable Server 🔘 Dis	able Server
◯ For NAT Usage	💿 For Routing Usage	Start IP Address	192.168.3.10
IP Address	192.168.3.1	IP Pool Counts	100
Subnet Mask	255.255.255.0	Gateway IP Address	192.168.3.1

Network	<b>Enable</b> – enable the configuration for such LAN.
Configuration	<b>Disable</b> – disable the configuration for such LAN.
For NAT Usage	Click this item to invoke NAT usage.
For Routing Usage	Click this item to invoke Routing usage.
	<b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
	<b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server</b> - Let you manually assign IP address to every host in the LAN.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

## DMZ

DMZ port setting is used for connecting host in DMZ.

LAN >> General Setup

Network Configuration		DHCP Server Configurat	ion
For NAT Usage		💿 Enable Server 🔘 Dis	able Server
IP Address	192.168.9.1	Start IP Address	192.168.9.10
Subnet Mask	255.255.255.0	IP Pool Counts	100
		Gateway IP Address	192.168.9.1

Network Configuration	Set IP address and Subnet Mask for clients connected via DMZ port.
For NAT Usage	<b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.9.1).
	<b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.25.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Enable Server -</b> Let the router assign IP address to every host in the LAN.
	<b>Disable Server</b> – Let you manually assign IP address to every host in the LAN.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.9.10, the starting IP address must be 192.168.9.11 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
	<b>Gateway IP Address -</b> Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.



## **IP Routed Subnet**

Vigor router can serve as a DHCP server to route the request coming from LAN PC.

#### LAN >> General Setup

TCP/IP and DHCP Setup f	or IP Routed Subnet	
Network Configuration		DHCP Server Configuration
🔘 Enable 🛛 💿 Disable		Start IP Address
For Routing Usage		IP Pool Counts 0 (max. 10)
IP Address	192.168.2.1	Use LAN Port P1
Subnet Mask	255.255.255.0	☑ Use MAC Address
RIP Protocol Control	Disable 💌	Index Matched MAC Address given IP Address
		1 00 : 3B : 55 : E7 : 8C : 00
		MAC Address : 00 :38 :55 :E7 :8C :00
		Add Delete Edit Cancel
		OK

Network	<b>Enable</b> – enable the configuration for such LAN.
Configuration	<b>Disable</b> – disable the configuration for such LAN.
	<b>IP Address</b> - Type in private IP address for connecting to a local private network (Default: 192.168.2.1).
	<b>Subnet Mask</b> - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
	<b>RIP Protocol - Disable</b> deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between 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.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	<b>Start IP Address -</b> Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
	<b>IP Pool Counts -</b> Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 0 and the maximum is 10.

**Use LAN Port** – Any PC asked for LAN IP address assigned by the DHCP server will send the request through the LAN port of the router.

**Use MAC Address -** IP Routed Subnet will automatically assign the subnet for incoming DHCP with listed MAC address. Only the PC which matches the MAC address added can ask for LAN IP address assigned by DHCP server.

Add /Delete /Edit- 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 of the DHCP server which can help the router to assign the correct IP address of the correct subnet to the correct host.

## 4.2.3 Static Route

LAN >> Static Route Setup

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

tatic Route	e Configuration		Set	<u>to Factory Default   View R</u>	outing Table
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?

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

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

#### Diagnostics >> View Routing Table

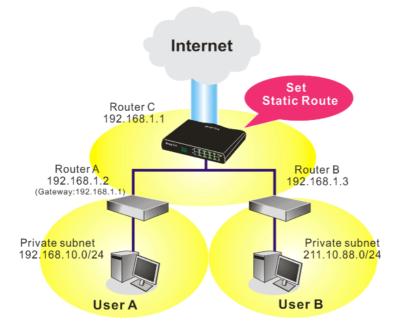
Key: C	- connected, S -	static, R - RIP, * - default, ~ - privat	e
*	0.0.0.0/	0.0.0.0 via 172.16.3.1, WAN1	
С~	192.168.1.0/	255.255.255.0 is directly connected,	LAN
С	172.16.3.0/	255.255.255.0 is directly connected,	WAN1

## Add Static Routes to Private and Public Networks

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

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

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



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

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

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

	Route Setup	 
ndex No. 1		
🗹 Enable		
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN 💌

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.

ex 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 🔽

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

Diagnostics >> View Routing Table

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

## 4.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage subnets by grouping them.

Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

🗹 Enable					
		VLAN Tag			
	Enable	VID	Priority	LAN Port	Subnet
VLAN0		0	0 🕶	$\checkmark$	LAN 1 💌
VLAN1	<b>v</b>	0	1 💌		LAN 1 🔽
VLAN2		0	0 🕶		LAN 1 🔽
VLAN3		0	0 🗸		LAN 1 🔽
VLAN4		0	0 🗸		LAN 1 🔽
VLAN5		0	0 🛰		LAN 1 🔽
VLAN6		0	0 🗸		LAN 1 🔽
VLAN7		0	0 ~		LAN 1 🔽

LAN >> VLAN Configuration

1. Hybrid mode only applied on VLANO to accept both tagged/untagged packets;

2. Tag based VLAN only applied for LAN Port;

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

OK	Clear	Cancel
=		

Enable	Check this box to enable VLAN configuration. The router will add specific VLAN tagging number to all packets on the WAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN port.
VLAN Tag	<b>Enable</b> – Check this box to enable the VID and the Priority. The router will add specific VLAN number to all packets on LAN while sending them out.
VID	Type the value as the VLAN ID number. The range is form 0 to 4095.
Priority	Type the number for such VLAN. The range is from 0 to 7.
LAN Port	Check this box to make the VLAN settings (such as VID, priority, subnet) applying to the LAN port.
Subnet	Choose one of them to make the selected VLAN group mapping to specified subnet only. For example, LAN1 is specified for VLAN0 group. It means that PCs grouped under VLAN0 can get the IP address (es) that specified by the subnet.

## 4.2.5 Bind IP to MAC

LAN >> 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.

Bind IP to MAC 🔘 Enable 💿 Disable 🔘 Strict Bind ARP Table | <u>Select All</u> | <u>Sort</u> | <u>Refresh</u> | IP Bind List Select All Sort IP Address Mac Address Index IP Address Mac Address 192.168.1.10 EO-CB-4E-DA-48-79 Add and Edit IP Address Mac Address Add Edit Delete

Note: IP-MAC binding presets DHCP Allocations.

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

OK

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	<b>IP</b> Address – Type the IP address that will be used for the specified MAC address.
	<b>Mac Address</b> – Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.



Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in <b>Add and Edit</b> to the table of <b>IP Bind List</b> .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in <b>IP Bind List</b> . Simply click and select the one, and click <b>Delete</b> . The selected item will be removed from the <b>IP Bind List</b> .

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

## 4.2.6 LAN Port Mirror

LAN >> LAN Port Mirror

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

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

LAN Port Mirror	
Port Mirror:	
🔘 Enable 💿 Disable	
Mirror port:	
💿 WAN4	
Mirrored port:	
□ P1 □ WAN 1	WAN 2 WAN 3
	OK
Port Mirror	Check <b>Enable</b> to activate this function. Or, check <b>Disable</b> to close this function.
Mirror Port	Select a port to view traffic sent from mirrored ports. At present, only WAN4 will be treated as mirror port.
Mirrored port	Select which ports (LAN port or WAN port) are necessary to be mirrored. P1 represents LAN port.

## 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.

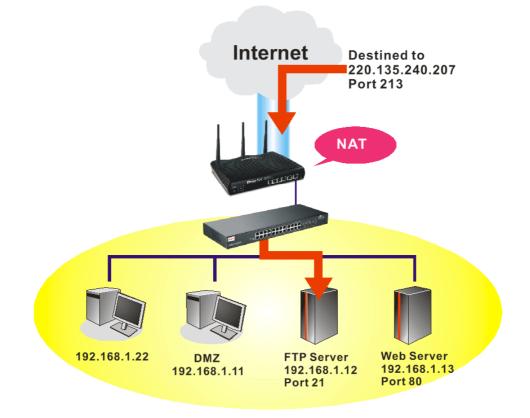
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

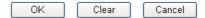
Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				х
<u>4.</u>				×
<u>5.</u>				x
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				×
<u>9.</u>				x
<u>10.</u>				х

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.



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 Interface	Select the WAN interface used for port redirection.
Public Port	Specify which port can be redirected to the specified <b>Private IP</b> <b>and Port</b> of the internal host. If you choose <b>Range</b> as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
Private IP	Specify the private IP address of the internal host providing the

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

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

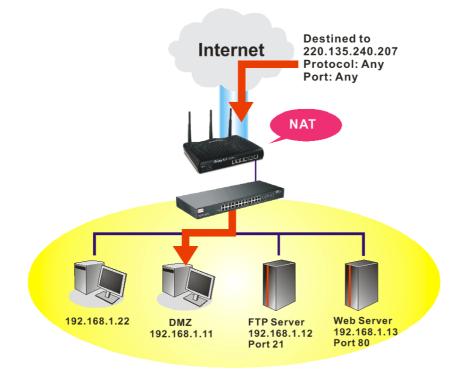
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This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

Management Access Control	Management Port Setup	Management Port Setup			
	O User Define Ports	🔘 Default Ports			
Allow management from the Internet FTP Server	Telnet Port	23 (Default: 23)			
─ HTTP Server	HTTP Port HTTPS Port	80 (Default: 80)			
HTTPS Server	FTP Port	443 (Default: 443 21 (Default: 21)			
SSH Server	SSH Port	22 (Default: 22)			
☑ Disable PING from the Internet	SNMP Setup				
Access List	Enable SNMP Agen	t			
List IP Subnet Mask	Get Community	public			
	Set Community	private			
3	Manager Host IP				
	Trap Community	public			
	Notification Host IP				
	Trap Timeout	10 seconds			

System Maintenance >> Management

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

#### NAT >> DMZ Host Setup

WAN1	WAN2	WAN3	WAN4	WAN5
11				
None	¥			
Private IP			Choose F	20
MAC Address o	f the True IP DMZ Host	00.00.		
Note: When a always on.	True-IP DMZ host is t	urned on, it will force	e the router's WAN co	onnection to be
		OK		

**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.

192.168.1.10 192.168.1.18

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.

Z Host Setup				
WAN1	WAN2	WAN3	WAN4	WAN5
AN 1				
Private IP	~			
Private IP		192.168.1.1	1 Choose	PC
MAC Address o	f the True IP DMZ Host	00.00.	00 00 00 00	
Note: When a always on.	True-IP DMZ host is t	urned on, it will force	e the router's WAN c	onnection to be

DMZ Host for WAN2 ~ WAN5 are slightly different with WAN1. See the following figure.

WAN1	WAN2	WAN3	WAN4	WAN5
4 3				
Enable		Private IP		
		0.0.0		Choose PC

**Dray** Tek

NAT >> DMZ Host Setup

If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode in WAN2/WAN3/WAN4/WAN5 interface, you will find them in **Aux. WAN IP** for your selection.

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

WAN1		WAN2	WAN3	WAN4	WAN5
WAN 3					
Index	Enable	Aux. WAN IP	Private IP		
1.		172.16.3.102	0.0.0	] [	Choose PC
2.		172.16.3.200	0.0.0	] [	Choose PC

0K

Check to enable the DMZ Host function.

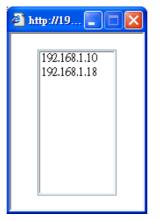
Clear

**Private IP** 

**Choose PC** 

Enter the private IP address of the DMZ host, or click Choose PC to select one.

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.

## 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>				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>				×

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface used by such index.
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	nable Open P	orts					
	Co	mment	P2F	)			
WAN Interface		WA	WAN1 💌				
	Lo	cal Computer	192	.168.1.10	Cho	ose PC	
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP 🔽	4500	4700	6.	💙	0	0
2.	UDP 💌	4500	4700	7.	💙	0	0
з.	¥	0	0	8.	💙	0	0
4.	¥	0	0	9.	💙	0	0
5.	🕶	0	0	10.	💌	0	0

Clear

Cancel

ΟK

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.

## 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:

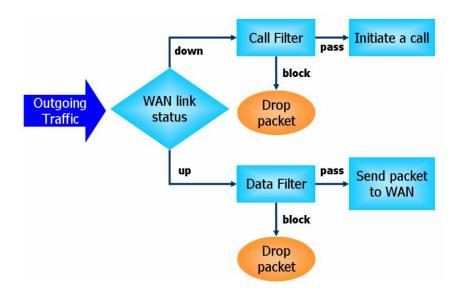
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

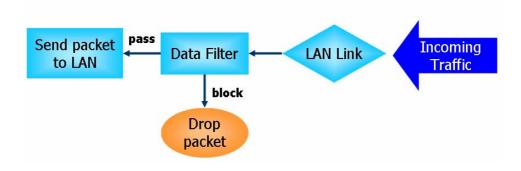
### **IP Filters**

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.

Firewall ▶ General Setup ▶ Filter Setup ▶ DoS Defense



## 4.4.2 General Setup

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

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

### **General Setup Page**

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

Firewall >> General Setup

eneral Setup	Default Rule	
Call Filter	💿 Enable	Start Filter Set Set#1 💌
	🔘 Disable	
Data Filter	📀 Enable	Start Filter Set 🛛 Set#2 🐱
	🔘 Disable	
🗹 Accept lar	ge incoming fragmented	UDP or ICMP packets ( for some games, ex. CS )
🗹 Enable Stri	ct Security Firewall	

Cancel

ΟK

Call Filter	Check <b>Enable</b> to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check <b>Enable</b> to activate the Data Filter function. Assign a start filter set for the Data Filter.
Accept large incoming	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP or ICMP Packets".
Enable Strict Security Firewall	For the sake of security, the router will execute strict security checking for data transmission.
	Such feature is enabled in default. All the packets will be inspected by the web content filter server while transmitting through Vigor router. If the web content filter server does not make any response (pass or block) for the packets, Vigor

router's firewall will block the packets directly for security.

## **Default Rule Page**

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

General Setup Default Ru	le	
Actions for default rule:		
Application	Action/Profile	Syslog
Filter	Pass 💌	
Sessions Control	11 / 120000	
Quality of Service	None 💌	
Load-Balance policy	Auto-Select 🐱	
<u>User Management</u>	None 🖌	
APP Enforcement	None 🔽	
URL Content Filter	None 🖌	
Web Content Filter	1-Default 🔽	
Advance Setting	Edit	

Filter	Select <b>Pass</b> or <b>Block</b> for the packets that do not match with the filter rules.	
	Filter	Pass 💙 Pass Block
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applie For detailed information of setting QoS, related section later. None Class 1 Class 2 Class 3 Default	

Cancel

ΟK

**Load-Balance Policy** Choose the WAN interface for applying Load-Balance Policy.



Auto-Select	*
Auto-Select	
WAN1	
WAN2	
WAN3	
WAN4	
WAN5	

**User Management** Such item is available only when Rule-Based is selected in User Management>>General Setup. The general firewall rule will be applied to the user/user group/all users specified here. None None User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile existed, Create New User or Create New Group item will appear for you to click to create a new one. **APP Enforcement** Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to selelct, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information. **URL Content Filter** Select one of the URL Content Filter profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information. Web Content Filter Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information. **Advance Setting** Click Edit to open the following window. However, it is



strongly recommended to use the default settings here.

Firewall >> General Se	•tup		
- Advance Setting			
Codepage	ANSI(1252)-Latin I		~
Window size:	65535		
Session timeout:	1440	Minute	

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

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

🔟 DrayTek Syslog 3.9.1	and the second	
	192.168.1.1 Vigor series	WAN Information WAN1 IP (Fixed) 172.16.2.213
LAN Status TX Packets 28489	RX Packets	WAN2 IP (Fixed)
Setup		
Tool Setup   Telnet Read-out Setup Codepage To Select	Codepage Information	
Windows Version: 5.01.2600 RECOMMENDED CODEPA 950 (ANSI/OEM - Tradition 00a1:21 00a6:7c 00a9:63 00a	GE:	b3:33 00b9:31 00ba: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.



## 4.4.3 Filter Setup

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

Firewall >> Filter Setup

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

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

### Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1				
Comments : Defa	ult Call Filter			
Filter Rule	Active	Comments	Move Up	Move Down
1		Block NetBios		<u>Down</u>
2			<u>UP</u>	<u>Down</u>
3			<u>UP</u>	<u>Down</u>
4			<u>UP</u>	<u>Down</u>
5			<u>UP</u>	<u>Down</u>
6			<u>UP</u>	<u>Down</u>
7			<u>UP</u>	
-			Next Filte	r Set 🛛 None 🕑
		OK Clear Cancel		
Filter Rule		Click a button numbered $(1 \sim 7)$ to button will open Edit Filter Rule v information, refer to the following	veb page. For	
Active		Enable or disable the filter rule.		
Comment		Enter filter set comments/descripti 23–character long.	ion. Maximu	m length is
Move Up/Dow	n	Use <b>Up</b> or <b>Down</b> link to move the	order of the	filter rules.
Next Filter Set	t	Set the link to the next filter set to filter run. Do not make a loop with		

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Ru	le 1

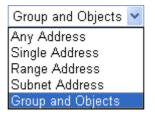
Check to enable the Filter Rul	e	
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter: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

**Check to enable the Filter** Check this box to enable the filter rule. **Rule** 

Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
Direction	Set the direction of packet flow. It is for <b>Data Filter</b> only. For the <b>Call Filter</b> , this setting is not available since <b>Call Filter</b> is only applied to outgoing traffic.
	LAN/RT/VPN -> WAN LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN
	Note: RT means routing domain for 2nd subnet or other LAN.
Source/Destination IP	Click <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	
IP Group	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.

Service Type	Group and Objects 👻
Protocol	
Source Port	= 💙 137 💊 139
Destination Port	= 🔽 1 ~ 65535
Service Group	None 💌
or <u>Service Object</u>	None 💌
or Service Object	None 1-SIP
or Service Object	2-RTP
	OK Close

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.

User defined	~
User defined	
Group and Objects	

**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.</li>Service Group/Object - Use the drop down list to choose the

one that you want.

FragmentsSpecify the action for fragmented packets. And it is used for<br/>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.

Specifies the action to be taken when packets match the rule.

**Block Immediately -** Packets matching the rule will be dropped immediately.

**Pass Immediately -** Packets matching the rule will be passed immediately.

**Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped.

**Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.

**Branch to other Filter Set** If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.

**Sessions Control** The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.

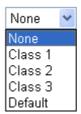
Filter



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

No-Strict - no limitation.

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



**Load-Balance policy** Choose the WAN interface for applying Load-Balance Policy.

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

None	*
None	
User Object	
[Create New User]	
User Group	
[Create New Group	o]
ÄLL	-

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

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

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

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



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

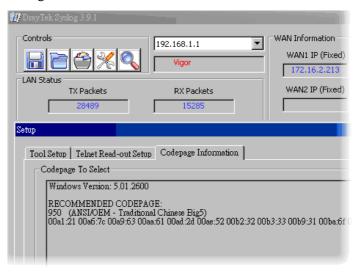
#### **Advance Setting**

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

ilter Set 1 Rule 1			
- Advance Setting Codepage	ANSI(1252)-Latin		*
Window size:	65535		
Session timeout:	1440	Minute	
DrayTek Banner:	<b>~</b>		
Strict Security Checking			
_	OK Close	1	

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

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



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



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

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

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



**Strict Security Checking** - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router if Strict Security Firewall is enabled. If the firewall system does not have any response (pass or block) for these packets, such as no response coming from Anti-Spam server, then the router's firewall will block the packets directly.

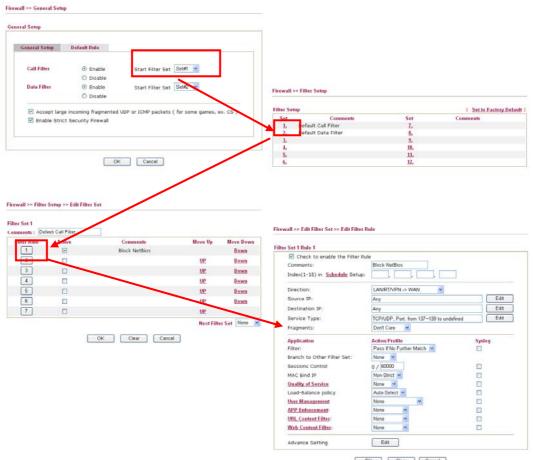
In addition, you can restrict the strict security checking just be done by specified server and conditions such as Anti-Virus, Anti-Spam, In-Sequence and APP Enforcement. Thus, the packets not only must be filtered by general rules by Firewall, but also must be filtered by the items selected in Strict Security Checking. Such work can ensure the data security transferring via network.

*APP Enforcement* – Check this box to execute the critical checking for all the files transferred via IM/P2P.

**Dray** Tek

#### 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.



OK Clear Cancel

### 4.4.4 DoS Defense

Firewall >> DoS defense Setup

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

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

DoS defense Setup				
Enable DoS Defense	t All			
🗌 Enable SYN flood defense		Threshold	50	packets / sec
		Timeout	10	sec
🔲 Enable UDP flood defense		Threshold	150	packets / sec
		Timeout	10	sec
Enable ICMP flood defense		Threshold	50	packets / sec
		Timeout	10	sec
Enable Port Scan detection	1	Threshold	150	packets / sec
Block IP options		🔲 Block TCP fla		] packets / 500
Block Land		<ul> <li>Block Tear Drop</li> <li>Block Ping of Death</li> <li>Block ICMP fragment</li> <li>Block UnknownProtocol</li> </ul>		
🔲 Block Smurf				
🔲 Block trace route				
📃 Block SYN fragment				
📃 Block Fraggle Attack				
				~
nable Dog Defense		ear All Cancel		noo Eurotionality
	Check the box	x to activate the		nse Functionality.
nable Dos Defense elect All	Check the box			2

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

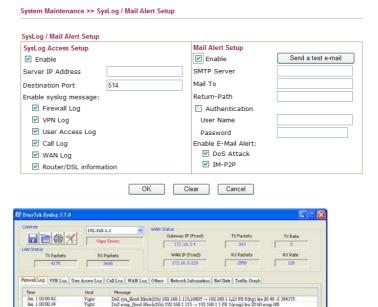
**Dray** Tek

	coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK</i> <i>scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang



	once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.
Warning Messages	We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.



**Dray** Tek

Vigor

ADS. Status

# 4.5 User Management

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

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

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



### 4.5.1 General Setup

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

Mode:	Rule-Based 🚩		
Notice :			
	Management will refer to active rules in Data	a Filter as whitelist	ts and blacklists
	er-based firewall mode. match the above lists will not be required f	or authentication.	
	irewall rules policy will still valid.		
The fi 3. Other	irewall rules policy will still valid. wise, authentication required for users not i	matched the abov	
The fi 3. Other	irewall rules policy will still valid.	matched the abov	
The fi 3. Other The fi	irewall rules policy will still valid. wise, authentication required for users not i	matched the abov policy will still valio	
The fi 3. Other The fi Welcome	irewall rules policy will still valid. wise, authentication required for users not i irewall rules designated in the user profile's	matched the above policy will still valid <u>Preview</u>	d.
The fi 3. Other The fi <b>Welcome</b> <body s<="" td=""><td>irewall rules policy will still valid. wise, authentication required for users not i irewall rules designated in the user profile's e Message (Max 255 characters)</td><td>matched the above policy will still valid <u>Preview</u>  &gt;</td><td>d.</td></body>	irewall rules policy will still valid. wise, authentication required for users not i irewall rules designated in the user profile's e Message (Max 255 characters)	matched the above policy will still valid <u>Preview</u>   >	d.
The fi 3. Other The fi <b>Welcome</b> <body s<="" td=""><td>irewall rules policy will still valid. wise, authentication required for users not i irewall rules designated in the user profile's e Message (Max 255 characters) stats=1&gt;<script <="" language="javascript" td=""><td>matched the above policy will still valid <u>Preview</u>  ></td><td>d.</td></tr></tbody></table></script></td></body>	irewall rules policy will still valid. wise, authentication required for users not i irewall rules designated in the user profile's e Message (Max 255 characters) stats=1> <script <="" language="javascript" td=""><td>matched the above policy will still valid <u>Preview</u>  ></td><td>d.</td></tr></tbody></table></script>		

Mode

There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.

User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.

Rule-Based –If you choose such mode, the router will apply



the filter rules configured in **Firewall>>General Setup** and **Filter Rule** to the users.

## 4.5.2 User Profile (Reserved)

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

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

User Management >> User Profile(Reserved)

To set the user profile, please click any index number link to open the following page. Notice that profile 1 (Admin) and profile 2 (System Reservation) are factory default settings and only few settings for them can be modified.

User Management >> User Profile

rofile Index 3	
Enable this account	<u>User Online Status</u> : <u>Block</u>
User Name	LAN_User_Group_1
Password	
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0: Unlimited
External Server Authentication	Radius 💌
Log	All 💌
Pop Browser Tracking Window	
Authentication	🗹 Web 🗹 Alert Tool 🗹 Telnet
📃 Enable Time Quota	0 min(s) Refresh , Add more 0 m
Index(1-15) in <u>Schedule</u> Setup:	
	OK Clear Cancel

**Dray** Tek

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

**Create New Policy** – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy.

Firewall >> Edit Filter Set >> Edit Filter Rule

Comments:	
Index(1-15) in <u>Schedule</u> Setup:	,,,, _
Direction:	LAN/RT/VPN -> WAN
Source IP:	Any
Destination IP:	Any
Service Type:	Any
Fragments	Don't Care

For the detailed configuration, simply refer to **Firewall>>Filter Rule**. The firewall filter rules that are not

selected in **Firewall>>General>>Default rule** can be available for use in **User Management>>User Profile**.

External ServiceThe router will authenticate the dial-in user by itself or by<br/>external service such as LDAP server or Radius server. If<br/>LDAP or Radius is selected here, it is not necessary to<br/>configure the password setting above.



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

None	~
None	
Login	
Event	
All	

Pop Browser Tracking Window	If such function is enabled, a pop up window will be displayed on the screen with time remaining for connection if Idle Timeout is set. However, the system will update the time periodically to keep the connection always on. Thus, Idle Timeout will not interrupt the network connection.
Authentication	Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.
	Web – If it is selected, the use can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in User Management >> General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.
	<b>Alert Tool</b> – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site.
	<b>Telnet</b> – If it is selected, the user can use Telnet command to perform the authentication job.
Enable Time Quota	Time quota means the total connection time allowed by the router for the user with such profile. Check the box to enable the function of time quota. The first box displays the remaining time of the network connection. The second box allows to type the number of time (unit is minute) which is available for the user (using such profile) to access Internet.

Log

	<b>Refresh</b> – Click this button to recalculate the time quota.
	Add – Click this box to set the time quota for such profile.
Index (1-15) in Schedule 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.

#### 4.5.3 User Group

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

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

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

```
User Management >> User Group
```

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

#### Name

Type a name for this user group.

Available User Objects Y

You can gather user profiles (objects) from **User Profile** page within one user group. All the available user objects that you have created will be shown in this box. Notice that user object, Admin and Dial-In User are factory settings. User defined



profiles will be numbered with 3, 4, 5 and so on.

Selected Keyword	Click button to add the selected user objects in this
Objects	box.

# 3.5.4 User Online Status

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

Current	Time : 08-23 0	7:39:57	Refresh S	econds: 10 🚩	Page: 1 💌	<u>Refresh</u>
Index	<u>Active User</u> ∽	IP Address	Last Login Time	Expired Time	Idle Time	Action
1	<u>admin</u>	192.168.1.10	08-23 06:01:11	Unlimited	Unlimited	<u>Block</u> Logou

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

**Logout** – the user will be logged out forcefully.

# 4.6 Objects Settings

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

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

## 4.6.1 IP Object

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

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

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

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

Click the number under Index column for settings in detail.

#### Objects Setting >> IP Object

Profile	e Index : 1	
	Name:	RD Department
Interface:		Any
	Address Type:	Range Address 💌
	Mac Address:	
	Start IP Address:	192.168.1.89
	End IP Address:	192.168.1.100
	Subnet Mask:	0.0.0.0
	Invert Selection:	
		OK Clear Cancel
Name		Type a name for this profile. Maximum 15 characters are allowed.
Interfa	ace	Choose a proper interface.
		LAN/DMZ/RT/VPN
		For example, the <b>Direction</b> setting in <b>Edit Filter Rule</b> will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the <b>Interface</b> here, and choose LAN as the direction setting in <b>Edit Filter Rule</b> , then all the IP addresses specified with LAN interface will be opened for you to choose in <b>Edit Filter Rule</b> page.
Addre	ess Type	Determine the address type for the IP address. Select <b>Single Address</b> if this object contains one IP address only.
		Select <b>Range Address</b> if this object contains several IPs within a range.
		Select <b>Subnet Address</b> if this object contains one subnet for IP address.
		Select Any Address if this object contains any IP address.
		Select Mac Address if this object contains Mac address.
		Range Address Any Address Single Address Range Address

**Dray** Tek

**MAC Address** 

Start IP Address End IP Address Subnet Address Mac Address

Type the MAC address for Mac Address type.

Type the start IP address for Single Address type.

Type the end IP address if the Range Address type is selected.

Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.

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

# 4.6.2 IP Group

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

#### Objects Setting >> IP Group

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

Ob	iects	Setting	>>	IP	Group
~	10.010	ooung			

Profile Index : 1	
Name:	Administration
Interface:	Any 💌
Available IP Objects	Selected IP Objects
1-RD Department 2-Financial Dept. 3-HR Department	>>> (<)
	OK Clear Cancel
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

## 4.6.3 Service Type Object

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

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

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

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

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Object Setup

Name	WWW
Protocol	ТСР 🖌 6
Source Port	= 🖌 1 ~ 65535
Destination Port	= 💌 80 ~ 80

Name

Protocol

Type a name for this profile.

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

тср 🔽	6
Any	
ICMP	
IGMP	
TCP	
UDP	
TCP/UDP	
Other	

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

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

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

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

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

Below is an example of service type objects settings.

Service T	vpe O	biect	Profiles:
	JP~~~		

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

## 4.6.4 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group	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.

**Dray** Tek

Click the number under Index column for settings in detail.

Objects Setting >> Service Type	Group Setup
Profile Index : 1	
Name:	VoIP
Available Service Typ	e Objects Selected Service Type Objects
1-SIP 2-RTP	
	OK Clear Cancel
Name	Type a name for this profile.
Available Service Type Objects	All the available service objects that you have added on <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

## 4.6.5 Keyword Object

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

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

Objects Setting >> Keyword Object

Set to Factory Default

Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Object Setup

Profile Index : 1	
Name	
Contents	
	Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.
	You can replace a character with %HEX. Example:
	Contents: backdoo%72 virus keep%20out
	Result:
	1. backdoor
	2. virus
	3. keep out
	OK Clear Cancel
Name	Type a name for this profile, e.g., game.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

### 4.6.6 Keyword Group

Objects Setting >> Keyword Group

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

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

Set to Factory Default

Clear all profiles.



Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

Profile Index : 1	
Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Keyword-1 2-keyword-2	» «
	OK Clear Cancel
Name	Type a name for this group.
Available Keyword Objects	You can gather keyword objects from <b>Keyword Object</b> page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.

#### 4.6.7 File Extension Object

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

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.

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

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

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

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

#### **Profile Name**

Type a name for this profile.

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

# 4.7 CSM Profile

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

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

### **APP Enforcement Filter**

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

### **URL Content Filter**

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

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

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

#### Web Content Filter

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

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

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





## **4.7.1 APP Enforcement Profile**

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

CSM >> APP Enforcement Profile

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

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

Click the number under Index column for settings in detail.

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

Below shows the items which are categorized under IM.

Profile Index : 1	Profile Name:					
IM	P2P	Protocol	Misc			
Select All	Clear All					
		Advanced	Management			
Activity / /	Application	MSN	YahooIM	AIM(<=	v5.9)	ICQ
Log	gin					
Mess	age					
File Tr	ansfer					
Gar	ne					
Conference('	/ideo/Voice)					
Other A	otivities					
	IM	Application				VoIP
AIM6/7	🗌 QQ/ТМ	iChat	🗌 Jabber/Go	ogleTalk		
🗌 GoogleChat	🗌 ×Fire	🗌 GaduGadu	🗌 Paltalk	-	🗌 Skyp	ie 🗌 Kubao
Qnext	POCO/PP365	🗌 AresChat	Aliww		Gizmo SIP/RTP	
КС	🗌 Lava-Lava	ICU2	🔲 iSpQ		🗌 TelT	el 🔲 TeamSpeal
UC	🗌 MobileMSN	🔲 BaiduHi				
	W	/eb IM ( * = mo	re than one addre:	5S)		
WebIM URLs	<u>eMessenger</u> ICQ Java* IMUnitive* MessengerFX*	<u>WebMSN</u> I <u>CQ Flash*</u> <u>Wablet*</u> MessengerAdi	<u>meebo*</u> goowy* <u>mabber*</u> ctos WebYahoolM	<u>eBuddy</u> <u>IMhaha*</u> MSN2GC		<u>ILoveIM*</u> getMessenger KoolIM
		OK	Cancel			
ofile Name	;	Type a	name for the	CSM j	profile	е.
lect All		Click it	to choose al	l of the	items	s in this pag
ear All		Unchec	k all the sele	ected bo	oxes.	

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

Below shows the items which are categorized under P2P.

```
CSM >> APP Enforcement Profile
```

IM	P2P	Protocol	Misc		
Select All	Clear All				
Protoc	ol		A	Applications	
📃 SoulSeek		SoulSeek			
🗌 eDonkey		eDonkey, (	eMule, Shareaza		
🔲 FastTrack		KazaA, Bea	arShare, iMesh		
🗌 OpenFT		KCeasy, Fi	lePipe		
🗌 Gnutella		BearShare	Limewire, Share	aza, Foxy, KCeasy	r
🗌 OpenNap		Lopster, X	Nap, WinLop		
BitTorrent		BitTorrent,	BitSpirit, BitCom	iet	
🗌 Winny		Winny, Wi	nMX, Share		
		Other	D2D Ann Bradiana		
			P2P Applications		
🗌 Xunlei	📃 Vaga	a l	PP365	POCO	🗌 Clubbox
🗌 Ares 📃 ezPeer 📃 Pa			Pando	📃 Huntmine	🗌 Kuwo

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

CSM	~~		Enforcement	Drofile
CSIM	>>	APP	Enforcement	Prome

Profile Index : 1	Profile Name:				
IM	P2P	Protocol	Misc		
Select All	Clear All				
			Protocol		
DNS	FTP	[	НТТР	IMAP	IRC 🗌
NNTP	🔲 РОРЗ	[	SMB	SMTP	SNMP
SSH	SSL/TLS	[	TELNET	MSSQL	MySQL
🗌 Oracle	🗌 PostgreSQL	[	Sybase	DB2	🗌 Informix
		Ok	Cancel		

### The items categorized under Misc.

CSM >> APP Enforcement Profile

rofile Index : 1	Profile Name:			
IM	P2P Proto	col Misc		
Select All	Clear All			
		Tunneling		
Socks4/5	PGPNet	HTTP Proxy	🗌 Tor	VNN
SoftEther	MS TEREDO	📃 Wujie/UltraSurf	🗌 Hamachi	🗌 HTTP Tunnel
🗌 Ping Tunnel	TinyVPN	🗌 RealTunnel	🗌 DynaPass	UltraVPN
🗌 FreeU	Skyfire 🗌			
		Streaming		
MMS	RTSP	TVAnts	PPStream	PPTV
🗌 FeiDian	UUSee	NSPlayer	PCAST	🔲 Τ ΥΚοο
SopCast	UDLiveX	🔲 TVUPlayer	🗌 MySee	🗌 Joost
🗌 FlashVideo	🗌 SilverLight	🗌 Slingbox	QVOD	
		Remote Control		
VNC	📃 Radmin	SpyAnywhere	ShowMyPC	LogMeIn
🔲 TeamViewer	📃 Gogrok	🗌 RemoteControlPro	CrossLoop	🔲 WindowsRDP
pcAnywhere	🗌 Timbuktu	UindowsLiveSync 🗌	SharedView	
		Web HD		
HTTP Upload	🗌 HiNet SafeBox	MS SkyDrive	🔲 GDoc Uploader	🗌 ADrive
MyOtherDrive	🗌 Mozy	BoxNet	OfficeLive	
	l	OK Cancel		

## 4.7.2 URL Content Filter Profile

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

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

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

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

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

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

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

CSM >> URL Content Filter Profile

Administration Message (Max 255 characters)

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

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

OK

Vigor3200 Series User's Guide



#### CSM >> URL Content Filter Profile

Profile Name:					
Priority:	Both : Pass	<b>~</b> L	.og:	None 💌	
1.URL Access	Control				
Enal	le URL Access Control	Preve	ent we	eb access from IP address	
Activ		Group/C	Object	Edit	
2.Web Featu	e				
Enal	le Restrict Web Feature				
Pass		e Proxy File Extension Profile: None 💌			
	ОК	Clear	r (	Cancel	
rofile Name	Type a	name for t	the CS	SM profile.	
riority	It deter	mines the a	action	n that this router will apply.	
	with the Feature both co	e condition below pas nfiguratior	ns spe ssing 1 n set i	er will let all the packages that match ecified in URL Access Control and Wel through. When you choose this setting in this page for URL Access Control be inactive.	
				er will block all the packages that matc ecified in URL Access Control and We	

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

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

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

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

None – There is no log file will be recorded for this profile.

**Pass** – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

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



#### **URL Access Control**

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

**Prevent web access from IP address** - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

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

*Block* - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action.

Action:



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



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

#### Web Feature

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

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

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

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

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

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

**File Extension Profile** – Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.



## 4.7.3 Web Content Filter Profile

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

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

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

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

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

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

Profile	Name	Profile	Name
<u>1.</u>	Default	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
dministration Mes	sage (Max 255 characters)	I	Cache : L1 + L2 Cache
or>that is cat	br> <	>has been blocked by	%RNAME% Web Content

CSM >> Web Content Filter Profile

OK	

Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected. By the way, you can click the link of <b>Test a</b> <b>site to verify whether it is categorized</b> to access into the test server selected.
Find more	Click it to open http://myvigor.draytek.com for searching



	another qualified and suitable server.
Test a site to verify whether it is categorized	Click this link to do the verification.
Set to Factory Default	Click this link to retrieve the factory settings.
Cache	<b>None</b> – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.
	L1 – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.
	L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.
T' 1 (	L1+L2 Cache – the router will check the URL with fast processing rate combining the feature of L1 and L2.

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

Profile Index: 1 Profile Name: Default			Log: Block ¥
Black/White List Enable Action: Block V Action: Block V		oup/Object Selections	Edit
Child Protection Select All Clear All	Categories  Chat  Gambling  Sex	<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>	<ul> <li>Entertainment</li> <li>Glamour</li> <li>Lifestyle</li> <li>Photo Searches</li> <li>Streaming Media</li> </ul>	<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	<ul> <li>Education</li> <li>News</li> <li>Usenet News</li> </ul>	Hosting Sites Religion Uncategorised Sites	☐ Kid Sites ☐ Sex Education
OK       Cancel         Black/White List       Enable – Activate white/black list function for such p			

ofile. Group/Object Selections – Click Edit to choose the group or object profile as the content of white/black list. Pass - allow accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **Block** - **restrict** accessing into the corresponding webpage with the characters listed on Group/Object Selections. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. Pass - allow accessing into the corresponding webpage with the categories listed on the box below. Action **Block** - restrict accessing into the corresponding webpage with the categories listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action. Log None – There is no log file will be recorded for this profile.



Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

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



# 4.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management	
Sessions Limit	
Bandwidth Limit	
Quality of Service	

# 4.8.1 Sessions Limit

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

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

#### Bandwidth Management >> Sessions Limit

Sessions Limit	
🔘 Enable 💿 Disable	
Default Max Sessions: 100	
Limitation List	
Index Start IP End IP Max Sessions	
Specific Limitation	
Start IP: End IP:	
Maximum Sessions:	
Add Edit Delete	
Administration Message (Max 250 characters)	
You have reached the maximum number of permitted Internet sessions.Please close	^
one or more applications to allow furthur Internet access.Contact your system administrator for further information.	
Time Schedule	
Index(1-15) in <u>Schedule</u> Setup:,,,,	
Note: Action and Idle Timeout settings will be ignored.	

OK

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

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
Maximum Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
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.
Administration Message	Type the words which will be displayed when reaches the



	maximum number of Internet sessions permitted.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.

# 4.8.2 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.

Bandwidth Management >> Bandwidth Limit

🔵 Ena	ible 🗌 Apply t	o IP Routed Subr	et 💿 Disable		
Default	TX Limit: 200	Kbps Defa	ault RX Limit: 800	Kbps	
		ent to make the	best utilization o	f <u>available b</u>	andwidth.
Limitati	on List				
Index	Start IP	End IP	TX limit	RX limit	Shared
Specific	c Limitation				
		End	тр.		
Start IF	D:	End			
	D:	TX Limit:	Kbps RX Li	mit:	Kbps
Start IF	D:		Kbps RX Li	mit:	Kbps
Start IF	D:	TX Limit:	Kbps RX Li		Kbps
Start IF	D:	TX Limit:	Kbps RX Li	mit:	Kbps
Start IF Eac	D:	TX Limit:	Kbps RX Li	mit:	Kbps

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

ΟK

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



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

# 4.8.3 Quality of Service

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

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

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

There are two components within Primary configuration of QoS deployment:

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

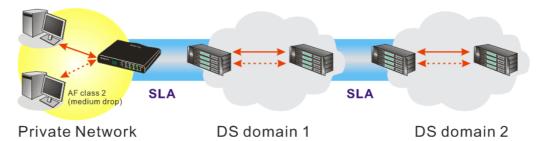
The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the



headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

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

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



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

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

	Setup Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	<u>o Factory Do</u> Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
		10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
lass Ru Inde			Name					Rule	Service T	ype
Class	51							<u>Edit</u>		
Clas:	52							<u>Edit</u>	<u>Edit</u>	
Clas:	53							<u>Edit</u>		

Bandwidth Management >> Quality of Service

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



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

# **General Setup for WAN Interface**

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

	N1 General Enable the	· ·	UT 🗸					
	WAN Inbound		Bandwidth	10000 Kbps				
		WAN Outbound	d Bandwidth	10000 Kbps				
	Index		Class Name	Reserved bandwidth Ratio				
	Class 1			25 96				
	Class 2			25 %				
	Class 3			25 %				
			Others	25 %				
	Enable UD	P Bandwidth Cor	itrol	Limited_bandwidth Ratio 25 %				
	Outbound	TCP ACK Prioriti	28					
			OK Clear	Cancel				
nab	le the Q	oS Control	The factory default for this setting is checked.					
			Please also define which traffic the QoS Control settings will apply to.					
			<b>IN-</b> apply to incoming traffic only.					
			<b>OUT</b> -apply to outgoing traffic only.					
			<b>BOTH-</b> apply to both incoming and outgoing traffic.					
				ick <b>OK</b> , then click <b>Setup</b> link again. Yo <b>tatistics</b> link appearing on this page.				
VAN Inbound andwidth		ıd	It allows you to set the connecting rate of data input for WAN For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.					
VAN Outbound andwidth		ınd	It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.					

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



Reserved Bandwidth Ratio	reserve	d bandwi	<b>e</b> 1	the form of ratio of <b>speed</b> and <b>reserved</b>
Enable UDP Bandwidth Control	field. Th	is is a pro ion traffic	otection of TCP ap	width ratio on the right pplication traffic since UDP g video will exhaust lots of
Outbound TCP ACK Prioritize	great in be impa	ADSL2+ cted by th	environment. For ne uploading TCP	en download and upload are the download speed might ACK, you can check this o speed the network traffic.
Limited_bandwidth Ratio	The rational The r	• •	ere is reserved for	limited bandwidth of UDP
Online Statistics	referenc			ity of service for your
	WAN1 Online	Statistics	Refresh	Interval: 5 💌 seconds 🛛   <u>Refresh</u>
	1 2 3	ection Class Na DUT DUT DUT DUT DUT Other	25% 25% 25%	io Outbound Throughput (Bytes/sec) 0 0 0 0

# Edit the Class Rule for QoS

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

Outbound Status

10 (Bps)

Other

Bandwidth Management >> Quality of Service

Genera	Setup							Set t	o Factory D	<u>efault</u>
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WANЗ	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
lass R Ind			Name					Rule	Service T	уре
Class 1								<u>Edit</u>		
Class 2								<u>Edit</u>	<u>Edit</u>	
Clas	53							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.

3andwidth Management >> Quality of Service								
Class Inc	lex #1							
Name	Test							
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1	Empty	-	-	-	-			
			Add Edit Dele	te				
			OK Cancel					

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

Rule Edit				
	🗹 ACT			
	Local Address	Any		Edit
	Remote Address	Any		Edit
	DiffServ CodePoint	ANY	*	
	Service Type	ANY	~	
	Note: Please choose/setup	the <u>Service Type</u> f	irst.	

OK Cancel

ACT	Check this box to invoke these settings.			
Local Address	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.			
Remote Address	Click the <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			

Start IP Address End IP Address

Subnet Mask

Address Type – Determine the address type for the source address.

0.0.0.0

Close

For **Single Address**, you have to fill in Start IP address.

OK

For **Range Address**, you have to fill in Start IP address and End IP address.

For Subnet Address, you have to fill in Start IP address and



	Subnet Mask.
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.
Service Type	It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

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

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

# Edit the Service Type for Class Rule

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

Genera	Setup							<u>Set t</u>	o Factory De	<u>efault</u>
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WANЗ	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
Class R Ind			Name					Rule	Service T	ype
Clas	s 1							<u>Edit</u>		
Clas	s 2							<u>Edit</u>	<u>Edit</u>	
Class 3							Edit			

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service



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

andwidth 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 Port Configuration					
			TCP 🔽 6		
		on			
	Туре		💿 Single i C Range		
	Port Num	ber	0 - 0		
5	Service Name		Cancel service for your request.		
S	Service Type	Choose the typ	Choose the type (TCP, UDP or TCP/UDP) for the new service		
Port Configuration		0	r <b>Range</b> as the <b>Type</b> . If you select Range, you a the starting port number and the end porting boxes below.		
			- Type in the starting port number and the end er 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.

# 4.9 Applications

Below shows the menu items for Applications.

Applications
Dynamic DNS
Schedule
▶ RADIUS
▶ UPnP
▶ IGMP
Wake on LAN

# 4.9.1 Dynamic DNS

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

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

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

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

Applications >> Dynamic DNS Setup

	p		t to Factory Defaul
📃 Enable Dynam	ic DNS Setup	View Log	Force Update
Auto-Update inte	erval 14400 Min(s) (1~14400)		
Accounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		×
2.	WAN1 First		×
<u> </u>			

OK	Clear All

Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Set to Factory Default	Clear all profiles and recover to factory settings.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).

**Dray** Tek

WAN Interface	Display the WAN interface used.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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

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

Index : 1						
🗹 Enable Dynamic DNS	3 Account					
WAN Interface	WAN1 First 🚩					
Service Provider	dyndns.org (www.dyndns.org)	~				
Service Type	Dynamic 💌					
Domain Name	chronic6853 dyndns.inf	o dyndns.info 💌				
Login Name	chronic6853	(max. 64 characters)				
Password	•••••	(max. 23 characters)				
🔲 Wildcards						
🔲 Backup MX						
Mail Extender						
Enable Dynamic D Account	check the box, y	o enable the current account. If you did ou will see a check mark appeared on the of the previous web page in step 2).				
WAN Interface	connecting, the 1 /WAN4 /WAN5 WAN1/WAN2/ will use another <b>WAN1/WAN2/</b> connecting, the 1	WAN3/WAN4/WAN5 First - While router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN3/WAN4/WAN5 fails, the router WAN interface instead. WAN3/WAN4/WAN5 Only - While router will use WAN1/WAN2/WAN3 as the only channel for such account.				

Select the service provider for the DDNS account.

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.

Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

Type in the login name that you set for applying domain.

Type in the password that you set for applying domain.

**Service Provider** 

Service Type

**Domain Name** 

Login Name

Password



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

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

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

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

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

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

# 4.9.2 Schedule

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

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

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

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

Office Hour: (Force On)

10

.9



Mon - Sun 9:00 am to 6:00
---------------------------

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

# **4.9.3 RADIUS**

Applications >> DADIUS

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.

RADIUS Setup		
🗹 Enable		
Server IP A	ddress	
Destination	Port 1812	
Shared Sec	ret	
Confirm Sha	ired 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 mus be configured to use the same shared secret.	
Confirm Shared Secret	Re-type the Shared Secret for confirmation.	

# 4.9.4 UPnP

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

Applications >> UPnP

UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

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



# **Enable UPNP Service**

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

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

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

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



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

# 4.9.5 IGMP

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

Applications >> IGMP		
IGMP		
will access any multicast Enable IGMP Snooping Enable IGMP Snooping, m	WAN3 multicast proxy for hosts on the LAN side. group. But this function take no affect when ulticast traffic is only forwarded to ports tha ulticast traffic is treated in the same manne	Bridge Mode is enabled. at have members of that group.
	OK Cancel	
		<u>Refresh</u>
Working Multicast Groups	Group ID	P1
	multicast will be executed throug addition, such function is availabl	<b>A</b>
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	It indicates the LAN port used for	the multicast group.
Refresh	Click this link to renew the worki	ng multicast group status.



# 4.9.6 Wake on LAN

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

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

Application	>> Wake on LAN			
Wake on LA	N			
	Note: Wake on LAN cooperate with <u>Bind IP to MAC</u> function, only binded PCs can wake up through IP.			
	Wake by: IP Address: MAC Address: <b>Result</b>	MAC Address 💙	Wake Up!	
Wake by		Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct l address.		
		Wake by:	MAC Address  MAC Address IP Address	
P Address	8	The IP addresses	that have been configured in <b>Firewall</b> >> <b>B</b>	

IP AddressThe IP addresses that have been configured in Firewall>>Bind<br/>IP to MAC will be shown in this drop down list. Choose the<br/>IP address from the drop down list that you want to wake up.MAC AddressType any one of the MAC address of the bound PCs.

	51
Wake Up	Click this button to wake up the selected IP. See the following
	figure. The result will be shown on the box.

Appl	ication	>>	Wake	on	LAN

IP Address:		
MAC Address:	Wake by: MAC Address 💙	
	IP Address:	
Result	MAC Address:	ike Up!
Result	Result	

**Dray** Tek

# 4.10 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
IP Sec General Setup
IP Sec Peer Identity
Remote Dial-in User
LAN to LAN
Connection Management

# 4.10.1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Enviro	nment	
LAN-to-LAN VPN Client Mode	Selection:	Route Mode 💌
Please choose a LAN-to-LAN	Profile:	[Index] [Status] [Name] 🗸
<b>Note:</b> For a typical LAN-to-LA If the remote network is the subnet and then sel If in doubt then select F	expecting only ect NAT mode.	e select Route Mode. / a single client or ip and is not configured to route
		< Back Next > Finish Cancel
LAN-to-LAN Client Mode Selection	Route Mod you to dial	le

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



[Index] 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 22 23 24 25 26 27 28 29	[Status]	[Name] ??? ??? ??? ??? ??? ??? ??? ??? ??? ?	^
2	v	222	
2	x x x	222	
Å	A V	222	
	A V	222	
6	A V	222	
2	<u>.</u>	222	
6	x x x x x x x x x x x x x x	222	
	×	222	
10	×	222	
	×	222	
	×	111	
112	x	111	
13	x	111	
114	x	222	
15	x x	222	
110	X	222	
	x x x	222	
118	x		
119	х	777	
20	х	222	
21	х	222	
22	x	???	
123	х	???	
24	x x x x x	777	
25	x	???	
26	x x x x	???	_
27	x	???	
28	x	???	_
29	x	???	~

When you finish the mode and profile selection, please click Next to open the following page.

```
VPN and Remote Access >> VPN Client Wizard
```

Security ranking (1 is the highest; 5 is the lowest)	Throughput ranking (1 is the highest; 5 is the lowest)
<ol> <li>L2TP over IPSec</li> <li>IPSec</li> <li>PPTP (Encryption)</li> <li>L2TP</li> <li>PPTP (None Encryption)</li> </ol>	<ol> <li>PPTP (None Encryption)</li> <li>L2TP</li> <li>IPSec</li> <li>L2TP over IPSec</li> <li>PPTP (Encryption)</li> </ol>
PTT PTT IPSe L2TP L2TP	-

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

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



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

Profile Name	???
VPN Dial-Out Through	WAN1 First 🗸
Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	•••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0
	< Back Next > Finish Cancel

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

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

rofile Name	???
VPN Dial-Out Through	WAN1 First
Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔿 Digital Signature (X.509)	
Peer ID	None
Local ID	
Iternative Subject Name First	
🔘 Subject Name First	
IPSec Security Method	
💿 Medium (AH)	
🔘 High (ESP)	DES without Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP Settings		
Profile Name	VPN-1	
VPN Dial-Out Through	WAN1 First	
Always on		
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com	
Username	marketing	
Password	•••••	
Remote Network IP	192.168.1.6	
Remote Network Mask	255.255.255.0	
	< Back Next > Finish	Cancel

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

VPN and Remote Access >> VPN Client Wizard

Profile Name	???
VPN Dial-Out Through	WAN1 First
🔲 Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔿 Digital Signature (X.509)	
Peer ID	None
Local ID	
Alternative Subject Name First	
🔘 Subject Name First	
IPSec Security Method	
<ul> <li>Medium (AH)</li> </ul>	
🔘 High (ESP)	DES without Authentication 👻
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

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

VPN and Remote Access >> VPN Client Wizard

Profile Name VPN Dial-Out Through I Always on Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)		???	
		WAN1 First	~
IKE Authentication Method			
💿 Pre-Shared Key			
Confirm Pre-Shared Key			
🔘 Digital Signature (X.509)			
Peer ID		None	~
Local ID			
Alternative Subject N	Name First		
OSubject Name First			
IPSec Security Method			
Medium (AH)     History		DEC millions Anthony	tigation at
🔘 High (ESP)		DES without Authen	ication M
Username		???	
Password			
Remote Network IP		0.0.0.0	
Remote Network Mask	255.255.255.0	255.255.255.0	
rofile Name PN Dial-Out Through	limited to 10 cha		
rofile Name PN Dial-Out Through	limited to 10 cha Use the drop do	such profile. The le	a proper WAN
	limited to 10 cha Use the drop do interface for this only. WAN1 First / W First / WAN5 F use WAN1/WA channel for VPN	such profile. The learacters. wn menu to choose as profile. This setting <b>VAN2 First / WAN</b> <b>'irst</b> - While connec N2/WAN3/WAN4/V I connection. If WA fails, the router will	a proper WAN g is useful for dia <b>3 First / WAN4</b> ting, the router w WAN5 as the firs N1/WAN2/WAN
	limited to 10 cha Use the drop do interface for this only. WAN1 First / W First / WAN5 F use WAN1/WA channel for VPM /WAN4/WAN5 interface instead WAN1 Only / W Only/ WAN5 O	such profile. The learacters. wn menu to choose as profile. This setting VAN2 First / WAN Yirst - While connec N2/WAN3/WAN4/V I connection. If WA fails, the router will WAN2 Only / WAN Only - While connect N2/WAN3/WAN4/V	a proper WAN g is useful for dia <b>3 First / WAN4</b> ting, the router w WAN5 as the firs N1/WAN2/WAN use another WA <b>3 Only / WAN4</b> ing, the router w
	limited to 10 cha Use the drop do interface for this only. WAN1 First / W First / WAN5 F use WAN1/WA channel for VPN /WAN4/WAN5 interface instead WAN1 Only / W Only/ WAN5 O use WAN1/WA channel for VPN	such profile. The learacters. wn menu to choose as profile. This setting VAN2 First / WAN Yirst - While connec N2/WAN3/WAN4/V I connection. If WA fails, the router will WAN2 Only / WAN Only - While connect N2/WAN3/WAN4/V	a proper WAN g is useful for dia <b>3 First / WAN4</b> ting, the router w WAN5 as the firs N1/WAN2/WAN use another WA <b>3 Only / WAN4</b> ing, the router w WAN5 as the onl
PN Dial-Out Through	limited to 10 cha Use the drop do interface for this only. WAN1 First / V First / WAN5 F use WAN1/WA channel for VPN /WAN4/WAN5 interface instead WAN1 Only / V Only/ WAN5 O use WAN1/WA channel for VPN Check to enable IKE Authentica are remote dial-i uses dynamic IP	such profile. The learacters. wn menu to choose as profile. This setting VAN2 First / WAN Yirst - While connec N2/WAN3/WAN4/V I connection. If WA fails, the router will wAN2 Only / WAN Only - While connect N2/WAN3/WAN4/V I connection.	a proper WAN a proper WAN g is useful for dia <b>3 First / WAN4</b> ting, the router w WAN5 as the firs N1/WAN2/WAN use another WA <b>3 Only / WAN4</b> ing, the router w WAN5 as the onl VPN connection ly applies to thos N to LAN) which related VPN
PN Dial-Out Through Iways On	limited to 10 cha Use the drop do interface for this only. WAN1 First / W First / WAN5 F use WAN1/WA channel for VPN /WAN4/WAN5 interface instead WAN1 Only / W Only/ WAN5 O use WAN1/WA channel for VPN Check to enable IKE Authentica are remote dial- uses dynamic IP connections such	such profile. The learacters. wn menu to choose as profile. This setting VAN2 First / WAN First - While connect N2/WAN3/WAN4/W I connection. If WA fails, the router will wan2 Only / WAN only - While connect N2/WAN3/WAN4/W Only - While connect N2/WAN3/WAN4/W only - While connect N2/WAN3/WAN4/W connection. router always keep ation Method usual in user or node (LAN address and IPSec-	a proper WAN g is useful for dia <b>3 First / WAN4</b> ting, the router w WAN5 as the firs N1/WAN2/WAN use another WA <b>3 Only / WAN4</b> ing, the router w WAN5 as the onl VPN connection ly applies to thos N to LAN) which related VPN cc and IPSec tunn

**Digital Signature (X.509)** Click **Digital Signature** to invoke this function. Use the drop down list to choose one of the certificates for using.

	You have to configure one certificate at least previously in <b>Certificate Management</b> >> <b>Local Certificate.</b> Otherwise, the setting you choose here will not be effective.
	<b>Peer ID</b> – Choose one of the ID from the drop down list.
	Local ID – Choose Alternative Subject Name First or Subject Name First.
IPSec Security Method	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High</b> - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

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

Please confirm your settings		
LAN-to-LAN Index:	27	
Profile Name:	test	
VPN Connection Type:	PPTP (None Encryption)	
VPN Dial-Out Through:	WAN1 First	
Always on:	No	
Server IP/Host Name:	192.168.1.87	
Remote Network IP:	172.16.3.99	
Remote Network Mask:	255.255.255.0	
Click <b>Back</b> to modify changes if and proceed to the following a	necessary. Otherwise, click <b>Finish</b> to save the current settings ction:	
	So to the VPN Connection Management.	
	🔘 Do another VPN Client Wizard setup.	
	View more detailed configurations.	
	-	

Go to the VPN Connection Click this radio button to access VPN and Remote

**Dray** Tek

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

# 4.10.2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

hoose VPN Establishment Environmen	t
VPN Server Mode Selection:	Site to Site VPN (LAN-to-LAN)
Please choose a LAN-to-LAN Profile:	[Index] [Status] [Name]
Please choose a Dial-in User Accour	nts: [Index] [Status] [Name]
Allowed Dial-in Type:	PPTP IPSec L2TP with IPSec Policy None
	< Back Next > Finish Cancel
PN Server Mode election	Choose the direction for the VPN server. Site to Site VPN/Remote Dial-in User – To set a LAN-to-LAN profile automatically, please choose

Site VPN. **Remote Dial-in User** –You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection.

Site to Site VPN (LAN-to-LAN)	*
Site to Site VPN (LAN-to-LAN)	
Remote Dial-in User (Teleworker)	

Please choose aThLAN-to-LAN Profile(L

This item is available when you choose **Site to Site VPN** (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.



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

Please choose a Dial-in User Accounts

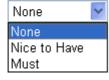
**Allowed Dial-in Type** 

This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.

This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard).

- 🗹 РРТР
- IPSec

☑ L2TP with IPSec Policy



Different Dial-in Type will lead to different configuration page. In addition, adjustable items for each dial-in type will be changed according to the VPN Server Mode (**Site to Site VPN** and **Remote Dial-in User**) selected. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made. Here we take the example of choosing **Remote-Dial-in User** as the **VPN Server Mode**.

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

VPN and Remote Access >> VPN Server Wizard

/PN and Remote Access >> VPN Server Wizard	
VPN Authentication Setting	
PPTP / L2TP / L2TP over IPSec Authentication	
Username	???
Password	
Peer IP/VPN Client IP	
	< Back Next > Finish Cancel

• When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP** with Policy (Nice to Have/Must), you will see the following graphic:

TP / L2TP / L2TP over IPSec Authentication	
ername	server1
ssword	
Sec / L2TP over IPSec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🔲 Digital Signature (X.509)	
Peer ID	None
er IP/VPN Client IP	192.168.1.99
er ID	



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

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting IPSec / L2TP over IPSec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🔲 Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	
Peer ID	
1	
	< Back Next > Finish Cancel

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

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

Please Confirm Your Settings					
VPN Environment:	Site to Site VPN (LAN-to-LAN)				
Index:	3				
Profile Name:	VPN-Ser1				
Username:	server1				
Allowed Service:	PPTP+IPSec				
Peer IP/VPN Client IP:					
Peer ID:					
Remote Network IP:	0.0.0.0				
Remote Network Mask:	255.255.255.0				
Click <b>Back</b> to modify changes and proceed to the following a	<ul> <li>Go to the VPN Connection Management.</li> <li>Do another VPN Server Wizard setup.</li> </ul>				
	View more detailed configurations.				
	< Back Next > Finish Cancel				
Go to the VPN Connection Management	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;Connection Management</b> for viewing VPN Connection status.				
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.				
View more detailed configuration	Click this radio button to access <b>VPN and Remote</b> <b>Access&gt;&gt;LAN to LAN</b> for viewing detailed configuration.				

# 4.10.3 Remote Access Control

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

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup		
	Enable PPTP VPN Service	
	Enable IPSec VPN Service	
✓	Enable L2TP VPN Service	

**Note:** If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

ОК	Clear	Cancel
----	-------	--------

# 4.10.4 PPP General Setup

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

VPN and	Remote	Access	>>	PPP	General	Setur	)

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

OK

Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.
	<b>PAP or CHAP</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE)	<b>Optional MPPE</b> - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.
	Optional MPPE Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit)
	<b>Require MPPE (40/128bits) -</b> Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.
	Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer.

Assigned IP Range	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network.
	For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address.

# 4.10.5 IPSec General Setup

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

There are two phases of IPSec.

VPN and Remote Access >> IPSec General Setup

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

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

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

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

Dial-in Set up for Remote Dial-in users - IKE Authentication Method	
Pre-Shared Key	•••••
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but v	will not be encrypted.
High (ESP) 🛛 🗹 DES 📝 3	DES 🗹 AES
Data will be encrypted and	authentic.
	OK Cancel
<b>IKE Authentication</b> This	s usually applies to those are remote dial-in user or nod

This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and

Method



**Pre-Shared Key -**Currently only support Pre-Shared Key authentication.

**Pre-Shared Key-** Specify a key for IKE authentication **Confirm Pre-Shared Key-** Retype the characters to confirm the pre-shared key.

**IPSec Security Method** Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.

**High** - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

# 4.10.6 IPSec Peer Identity

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

VPN and Remote Access >> IPSec Peer Identity

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>	???	х	<u>32.</u>	???	х

Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPSec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.



#### VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1		
Profile Name one		
Enable this account		
O Accept Any Peer ID		
Occept Subject Alternation	ive 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 the name of the profile.	
Accept Any Peer ID	Click to accept any peer regardless of its identity.	
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be <b>IP Address</b> , <b>Domain</b> , or <b>E-mail Address</b> . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.	
Accept Subject Name	<ul> <li>Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).</li> </ul>	

## 4.10.7 Remote Dial-in User

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

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

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

emote Access User Accounts:					Set to Factory Default	
Index	User	Status	Index	User	Status	
<u>1.</u>	???	Х	<u>17.</u>	???	Х	
<u>2.</u>	???	Х	<u>18.</u>	???	Х	
<u>3.</u>	???	Х	<u>19.</u>	???	Х	
<u>4.</u>	???	Х	<u>20.</u>	???	Х	
<u>5.</u>	???	Х	<u>21.</u>	???	Х	
<u>6.</u>	???	Х	<u>22.</u>	???	Х	
<u>7.</u>	???	Х	<u>23.</u>	???	Х	
<u>8.</u>	???	Х	<u>24.</u>	???	Х	
<u>9.</u>	???	Х	<u>25.</u>	???	Х	
<u>10.</u>	???	Х	<u>26.</u>	???	Х	
<u>11.</u>	???	Х	<u>27.</u>	???	Х	
<u>12.</u>	???	х	<u>28.</u>	???	Х	
<u>13.</u>	???	Х	<u>29.</u>	???	Х	
<u>14.</u>	???	х	<u>30.</u>	???	Х	
<u>15.</u>	???	Х	<u>31.</u>	???	Х	
<u>16.</u>	???	х	<u>32.</u>	???	х	

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.

User account and Author	entication	Username	???	
Enable this accour Idle Timeout	nt 300 second(s)	Password	ne Passwords(mOTP)	
Allowed Dial-In Type		PIN Code		
<ul> <li>✓ PPTP</li> <li>✓ IPSec Tunnel</li> </ul>		Secret		
L2TP with IPSec F		IKE Authentication Method Pre-Shared Key		
Specify Remote No Remote Client IP or Pe		IKE Pre-Shared Key Digital Signature(X.509) None		
or Peer ID				
Netbios Naming Packe Multicast via VPN (for some IGMP,IP-C Subnet	t	IPSec Security Method Medium(AH) High(ESP) Ø DES Ø Local ID (optional)	3DES 🗹 AES	
Assign Static IP A 0.0.0.0	ddress			
	ОК	Clear Cancel		
er account and thentication	Idle Timeout-	count - Check the box the dial-in user is idle outer will drop this control of the dial of	e over the limitation	

VPN and Remote Access >> Remote Dial-in User

Allowed Dial-In Type 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 make an IPSec VPN connection through Internet.

**L2TP with IPSec Policy** - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:

**None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.

**Nice to Have -** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

**Must** -Specify the IPSec policy to be definitely applied on the L2TP connection.



Specify Remote Node	<b>Check the checkbox-</b> You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).
	<b>Uncheck the checkbox-</b> This means the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .
	Netbios Naming Packet
	<b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
	<b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection.
	<b>Pass</b> – Click this button to let multicast packets pass through the router.
	<b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	Chose one of the subnet selections for such VPN profile.
	Assign Static IP Address – Please type a static IP address for the subnet you specified.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Enable Mobile One-Time Passwords (mOTP)	Check this box to make the authentication with mOTP function.
	<b>PIN Code</b> – Type the code for authentication (e.g, 1234).
	<b>Secret</b> – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
	<b>Digital Signature (X.509)</b> – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer</b> <b>Identity.</b>
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check

the Medium, DES, 3DES or AES box as the security method. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.

**High-Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

**Local ID** - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

#### 4.10.8 LAN to LAN

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

The router supports up to 32 VPN tunnels simultaneously. The following figure shows the summary table.

AN-to-LAN Pro	files:			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	Indicate the name of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.



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

#### Profile Index : 1

1. Common Settings			
Profile Name	???	Call Direction 💿 Bo	th 🔘 Dial-Out 🔘 Dial-in
📃 Enable this profile		🔲 Always on	
		Idle Timeout	300 second(s)
VPN Dial-Out Through 🛛	VAN1 First 🔽	📃 Enable PING to keep	p alive
Netbios Naming Packet	💿 Pass i 🔘 Block	PING to the IP	
Multicast via VPN	🔘 Pass 💿 Block		
(for some IGMP,IP-Came	era,DHCP Relayetc.)		
2. Dial-Out Settings			
Type of Server I am calling	g		000
⊙ РРТР		Username	???
🔘 IPSec Tunnel		Password	
🔘 L2TP with IPSec Poli	cy None 💉	PPP Authentication	PAP/CHAP 🔽
Server IP/Host Name for	VDN	VJ Compression	💿 On 🔘 Off
(such as 5551234, drayte			
		IKE Authentication Meth	od
		Pre-Shared Key	
		IKE Pre-Shared Key	
		<ul> <li>Digital Signature(X.</li> </ul>	509)
		None 🗸	
		IPSec Security Method	
		Medium(AH)	
		O High(ESP) DES with	out Authentication 🔛
		Advanced	
		Index(1-15) in <u>Schedu</u>	<u>le</u> Setup:
		,,,,	,

Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
VPN Dial-Out Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.
	WAN1 /WAN2 /WAN3 /WAN4 /WAN5 First - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead. WAN1 /WAN2 /WAN3 /WAN4 /WAN5 Only - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 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.
Multicast via VPN	Some programs might send multicast packets via VPN connection.
	<b>Pass</b> – Click this button to let multicast packets pass through the router.
	<b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile.
	Both:-initiator/responder
	Dial-Out- initiator only
	Dial-In- responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.
	<b>Idle Timeout:</b> The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	<b>Enable PING to keep alive</b> is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
Type of Server I am calling	<b>PPTP</b> - Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
	<b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.
	<b>L2TP with IPSec Policy -</b> Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
	<b>None:</b> Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
	<b>Nice to Have:</b> Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection



	becomes one pure L2TP connection.
	<b>Must:</b> Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to <b>Yes</b> to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.
	Pre-Shared Key - Input 1-63 characters as pre-shared key.
	<b>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 AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High (ESP-Encapsulating Security Payload)-</b> means payload (data) will be encrypted and authenticated. Select from below:
	<b>DES without Authentication</b> -Use DES encryption algorithm and not apply any authentication scheme.
	<b>DES with Authentication-</b> Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
	<b>3DES without Authentication</b> -Use triple DES encryption algorithm and not apply any authentication scheme.
	<b>3DES with Authentication-</b> Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
	<b>AES without Authentication</b> -Use AES encryption algorithm and not apply any authentication scheme.
	<b>AES with Authentication-</b> Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
Advanced	Specify mode, proposal and key life of each IKE phase, Gateway, etc.
	The window of advance setup is shown as below:

KE advanced settings				
IKE phase 1 mode	Main mode		O Aggressive mode	
IKE phase 1 proposal	DES_MD5_G1			~
KE phase 2 proposal	HMAC_SHA1/H	MAC_MD5 💌		
KE phase 1 key lifetime	28800	(900 ~ 86400)		
KE phase 2 key lifetime	3600	(600 ~ 86400)		
Perfect Forward Secret	Oisable		O Enable	
ocal ID				
IKE phase 2 key lifetime Perfect Forward Secret Local ID		(600 ~ 86400)	Ô Enable	

**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 Sottin

3. Dial-In Settings			
Allowed Dial-In Type			
PPTP		Username	???
🗹 IPSec Tunnel		Password	
L2TP with IPSec Pol	icy None 🔽	VJ Compression	💿 On 🔘 Off
Specify Remote VPN Peer VPN Server IP or Peer ID	Gateway	IKE Authentication Method ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509	)
		IPSec Security Method Medium(AH) High(ESP) Ø DES Ø	3DES 🗹 AES
4. TCP/IP Network Setting	s		
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remot	e network, you have to
Remote Network IP	0.0.0.0		Route 💙
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	-	to this VPN tunnel ( Only
Local Network Mask	255.255.255.0	single WAN supports this )	1
	More		
Allowed Dial-In Type	Determine the dia <b>PPTP -</b> Allow the connection throug	Clear Cancel Il-in connection with difference dial-in user to m the Internet. You shou remote dial-in user below	hake a PPTP VPN ld set the User Name
	<b>IPSec Tunnel-</b> A VPN connection	llow the remote dial-in u through Internet.	ser to trigger an IPSec
	make a L2TP VP	c <b>Policy -</b> Allow the remo N connection through the P alone or with IPSec. Se	e Internet. You can
	connection emplo	ply the IPSec policy. Acc yed the L2TP without IP re L2TP connection.	
	during negotiation	pply the IPSec policy firs n. Otherwise, the dial-in V e L2TP connection.	
	Must - Specify th L2TP connection	e IPSec policy to be defi	nitely applied on the
Specify Remote VPN Gateway	ID (should be the checking the box.	he IP address of the remo same with the ID setting Also, you should further curity methods on the right	in dial-in type) by specify the

	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.
	<b>Digital Signature (X.509)</b> –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> .
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. <b>Medium-</b> Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is
	active.
My WAN IP	active. <b>High-</b> Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES),
My WAN IP Remote Gateway IP	active. <b>High-</b> Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP
	<ul> <li>active.</li> <li>High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</li> <li>This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address here. Do not change the default value if you do not select PPTP or L2TP.</li> <li>This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote factor of L2TP.</li> <li>This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do</li> </ul>



**Network Mask** 

м	01	P
V.	U.	L C .

configuration. You can modify the settings if required.

Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

http://192.168.1.1 - LAN-to-LAN Profile - Microsoft Internet Explorer 🛛 🚺 🗖	DI
Profile Index :1	-1
Remote Network	
Network IP Netmask 255.255.255 / 32 🖌	
Add Delete Edit	
OK Close	

**RIP Direction**The option specifies the direction of RIP (Routing Information<br/>Protocol) packets. You can enable/disable one of direction here.<br/>Herein, we provide four options: TX/RX Both, TX Only, RX<br/>Only, and Disable.**From first subnet to**<br/>remote network, you<br/>have to doIf the remote network only allows you to dial in with single IP,<br/>please choose NAT, otherwise choose Route.**Change default route to**<br/>this VPN tunnelCheck this box to change the default route with this VPN tunnel.

### 4.10.9 Connection Management

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

VPN and Remote Access >>	· Connection Manage	ement				
Dial-out Tool				Refres	h Seconds	5 : 10 🗸 Refresh
			~	Dial		
VPN Connection Status Current Page: 1					Page M	No. GO >>
VPN Type Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
					ata is encr ata isn't er	(1)
Dial	Click this bu	itton to e	xecute di	al out fu	nction.	
Refresh Seconds	Choose the t and 30.	time for r	efresh the	e dial inf	ormation	among 5, 10,

**Refresh** Click this button to refresh the whole connection status.

## 4.11 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.

Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup

#### 4.11.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration				
Name Subject		Status	Modify	
Local	Local		View Delete	
GENERATE X509 Local	IMPORT REFRESH Certificate			
			<	

Generate

Click this button to open Generate Certificate Request window.

Certificate Management >> Local C	ertificate
Generate Certificate Request	
Subject Alternative Name	
Туре	IP Address 🔽 🔽
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA 🗸
Key Size	1024 Bit 😽

Generate

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

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

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

Certificate	Management >>	Local	Certificate
-------------	---------------	-------	-------------

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/OU=RD/emailA	Requesting	View Delete
GENERATE IMPORT REFRESH			
B MIIEsj BgNVBA MAOGCS blolkt /rGhuV RZjkRM qAEqMA ikisNd GqeJ9t j8kJEi	cal Certificate Request EGIN CERTIFICATE REQUEST CCARSCAQAWUDELMAKGA1UEBhMCVFcxEDAO STA1JEMSIWIAYJKoZIhvcNAQkBFhNZZXJ2; qGSIb3DQEBAQUAA4GNADCBiQKBgQDPioah 9cTdLUDaFk6s8d3wDeQytoV1LBJz2IDFOx, TKd9j6P1crnkP7du84t23tWBdMD4W5c8Vm aHEWpVpwIDAQABoCIwIAYJKoZIhvcNAQKO OGCSqGSIb3DQEBBQUAA4GBAB43O4N9nod8; ZUoUEnKcejeOndc+H83VDA23ACEJpzTFFx, rvYqeZybCrSjRU1PN1Hccfo7ANJ/M/D1EP4 m0 ND CERTIFICATE REQUEST	aWN1QGRYYX1ÖZ u/gFQaYB1ce5C jX6ip7ev187tw SyDjShLhjdxVY MRMwETAPBgNVH rIudBAfTt91ts qklbe2o7a+wE5	WsuY29tMIGf DERSDfWknIdH wTsg4lg26Qk PWpNKVIrOT2 = IREECDAGhwTA co/tYNb2kfE2 :7/+0VhNagBa

X509 Local Certificate Configuration

## 4.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

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

#### X509 Trusted CA Certificate Configuration

 	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.

🟉 Certificate Inf	tormation - Windows Inte	rnet Explorer	
🙋 http://192.168.1	.1/doc/XCaCfVi1.htm		*
			^
	Cert	ificate Detail Information	-1
Certific	ate Name:	Trusted CA-1	
Issuer:		~	
Subjec	t:		
Subjec	t Alternative Name:		
		<u> </u>	
Valid F	rom:		
Valid T	0:		
·			-
		Close	~
<b>e</b>			.:

### 4.11.3 Certificate Backup

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

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

Certificate Management >> Certificate Backup				
Certificate Backup / Restoration				
Backup	Encrypt password: Confirm password: Click Backup to download certificates to your local PC as a file.			
Restoration	Select a backup file to restore. Browse. Decrypt password: Click Restore to upload the file.			

## 4.12 Wireless LAN

This function is used for "n" models only.

#### 4.12.1 Basic Concepts

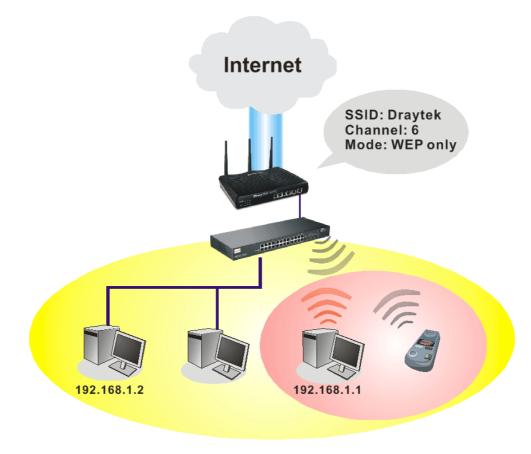
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The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

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

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

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





#### **Multiple SSIDs**

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

#### **Security Overview**

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

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

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

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

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

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



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

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

Below shows the menu items for Wireless LAN.



#### 4.12.2 General Setup

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

l Setting (I	EE 802.11	)						
able Wireles	s LAN							
Mode :				Mixed(11b	o+11g+11n)	~		
Index(1-19	i) in <u>Sche</u>	edule Setup:		,	, ,		,	]
Only scheo other actio		es that have nored.	the action	"Force Do	own" are ap	pliec	l to the W	LAN, all
Enable	Hide SSID		SSID		Isolate L	AN	Isolate Member	Isolate VPN
1		DrayTek			[			
2					[			
3 🔲					[			
4					Γ			
<b>isolate Me</b> for each o <b>isolate LAI</b> PCs on LA	nber:Wire ther. I:Wireless N.	SSID from be eless clients of clients (sta wireless with	(stations) w tions) with <sup>.</sup>	rith the sa the same	SSID canno	ot ac		d
Isolate Mer for each o Isolate LAI PCs on LA Isolate VPI Channel:	nber:Wire ther. I:Wireless N. I:isolate v Channel 6,	eless clients clients (sta wireless with 2437MHz v	(stations) w tions) with <sup>-</sup> remote dial	ith the same -in and L/ Long Prea	SSID canno AN to LAN \ amble: 🔲	ot ac /PN.	ccess wire	
Isolate Mer for each o Isolate LAI PCs on LA Isolate VPI Channel:	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco	eless clients clients (sta wireless with 2437MHz essary for sc	(stations) w tions) with <sup>-</sup> remote dial	ith the same -in and L/ Long Prea	SSID canno AN to LAN \ amble: 🔲	ot ac /PN.	ccess wire	
Isolate Mer for each o Isolate LAI PCs on LA Isolate VPI Channel:	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco	eless clients clients (sta wireless with 2437MHz essary for sc	(stations) w tions) with <sup>-</sup> remote dial	ith the same -in and L/ Long Prea	SSID canno AN to LAN \ amble: 🔲	ot ac /PN.	ccess wire	
Isolate Mei for each o Isolate LAI PCs on LA Isolate VPI Channel: [ Long Pream Packet-OV T x Burs Note:	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup>	eless clients clients (sta wireless with 2437MHz essary for sc	(stations) w tions) with remote dial me old 802.	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	ot ac /PN. wer	performan	ce)
Isolate Mei for each o Isolate LAI PCs on LA Isolate VPI Channel: [ Long Pream Packet-OV T x Burs Note:	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> st	eless clients clients (sta wireless with 2437MHz v essary for sc	(stations) w tions) with remote dial me old 802.	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	ot ac /PN. wer	performan	ce)
Isolate Mei for each o Isolate LAI PCs on LA Isolate VPI Channel: [ Long Prear Packet-OV T x Burs Note: The same	nber:Wire ther. I:Wireless N. I:isolate v I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> St technolog	eless clients clients (sta wireless with 2437MHz v essary for sc	(stations) w tions) with remote dial me old 802.	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	VPN. wer	performan	ce)
Isolate Mei for each o Isolate LAI PCs on LA Isolate VPI Channel: [ Long Prear Packet-OV T x Burs Note: The same	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> st technolog	eless clients clients (sta wireless with 2437MHz essary for sc y must also	(stations) w tions) with remote dial me old 802. be supporte	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	vPN. wer WL	performan	ce)
Isolate Mer for each o Isolate LAI PCs on LA Isolate VPI Channel: 1 Long Prear Packet-OV Tx Burs Note: The same Rate Contr	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> t technolog	eless clients clients (sta wireless with 2437MHz essary for sc y must also able	(stations) w tions) with remote dial me old 802. be supporte	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	VPN. Wer WL	AN performan	nance.
Isolate Mer for each of Isolate LAI PCs on LA Isolate VPI Channel: Channel: Channel: Packet-OV Tx Burs Note: The same Rate Contr SSID 1	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> st technolog	eless clients clients (sta wireless with 2437MHz essary for sc y must also able	(stations) w tions) with remote dial me old 802. be supporte Upload	rith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	WL/	AN performan	 nance.
Isolate Mei for each o Isolate LAI PCs on LA Isolate VPI Channel: [ Long Prear Packet-OV TX Burs Note: The same Rate Contr SSID 1 SSID 2	nber:Wire ther. I:Wireless N. I:isolate v Channel 6, nble: neco ERDRIVE <sup>T</sup> it technolog	eless clients clients (sta wireless with 2437MHz essary for sc y must also able	(stations) w tions) with remote dial me old 802. be supporte Upload 30000	ith the same -in and L/ Long Prea 11 b devi	SSID canno AN to LAN \ amble: ices only(lo	ver WL/ 30 30	AN performan	nance. bps

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.

	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek. We suggest you to change it.
Isolate	LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
	<b>Member</b> –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
	<b>VPN</b> - Check this box to make the wireless clients (stations) with different VPN not accessing for each other.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
	Channel: Channel 6, 2437MHz ✓ 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 802.11<br/>packet. Most modern wireless network uses short preamble with<br/>56 bit sync field instead of long preamble with 128 bit sync<br/>field. However, some original 11b wireless network devices<br/>only support long preamble. Check it to use Long Preamble if<br/>needed to communicate with this kind of devices.

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

**Note:** Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

Configuration Status Option About			
Connect General Setting General Setting Auto launch when Windows gtart up Remember mini status position Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile Group Roaming Ad-hoc WLAN type to connect O Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only	Advance Setting Disable Badio Eragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Power Save Mode: Tx Eurst :	2346 2347 802.11b/g/n - 2.4GH ¥ 1 ¥ Disable ¥ Disable ¥	
Automatically connect to non-preferred networks			
	OK (	Cancel Appl	7
Tx <u>B</u> urst : Disa Disa		*	

**Note:** \* means the real transmission rate depends on the environment of the network.

Rate ControlIt controls the data transmission rate through wireless<br/>connection.

**Upload** – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.

**Download** – Type the transmitting rate for data download. Default value is 30,000 kbps.

#### 4.12.3 Security

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

Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.

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

Wireless LAN >> Security Settings

	Mode:		Disable 💌
	Set up <b>RADIUS S</b>	erver if 802 1	1v is enabled
WPA:	•		
Encry	ption Mode:		TKIP for WPA/AES for WPA2
	Pre-Shared Key(F	PSK):	****
	Type 8~63 ASCII "cfgs01a2" or "		or 64 Hexadecimal digits leading by "Ox", for example".
WEP:	:		
	Encryption Mode:		64-Bit 🗸
			*****
	○Key 2 :		*****
	○Кеу 3 :		*****
	○Key 4 :		******
Type "0x41 For 12 Type	142333132". <mark>28 bit WEP key</mark> 13 ASCII characte	er or 26 Hexa	decimal digits leading by "Ox", for example "AB312" or adecimal digits leading by "Ox", for example 43536373839414243".

Mode

There are several modes provided for you to choose.

Cancel

	Disable 💌
	Disable
1	WEP
-	WEP/802.1x Only
	WPA/802.1x Only
	WPA2/802.1x Only
	Mixed(WPA+WPA2/802.1x only)
	WPA/PSK
	WPA2/PSK
1	Mixed(WPA+WPA2)/PSK

ΟK

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

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

**WEP/802.1x Only -** Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

**WPA/802.1x Only-** Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

**WPA2/802.1x Only-** Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

**WPA2/PSK-**Accepts only WPA2 clients and the encryption key should be entered in PSK.

**Mixed (WPA+ WPA2)/PSK -** Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

> **Type** - Select from Mixed (WPA+WPA2) or WPA2 only. **Pre-Shared Key (PSK)** - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

**64-Bit** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

**128-Bit** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:



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

WPA

WEP

#### 4.12.4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

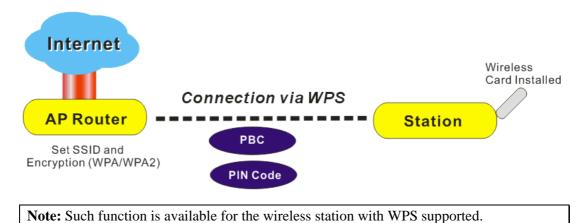
Enable Mac Address Filter	🔲 SSID 1 White List 🗸	🔲 SSID 2 White List 🔽
	SSID 3 White List 🕶	SSID 4 White List 🔽
	MAC Address Filter	
Index Attribute	MAC Address	Apply SSID
- 1	MAC Address : : : :	: :
Client's		
		ID 3 🔲 SSID 4
Apply SSIC		
Apply SSIC	9 : SSID 1 SSID 2 SS 9 : s: Isolate the station from	
Apply SSID Attribute	9 : SSID 1 SSID 2 SS 9 : s: Isolate the station from	
Apply SSID Attribute	9 : SSID 1 SSID 2 SS 9 : s: Isolate the station from	

	under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Attribute Add	connection of the wireless client of the MAC address from
	connection of the wireless client of the MAC address from LAN.
Add	connection of the wireless client of the MAC address from LAN. Add a new MAC address into the list.

ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

#### 4.12.5 WPS

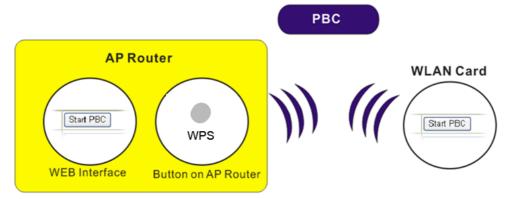
**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



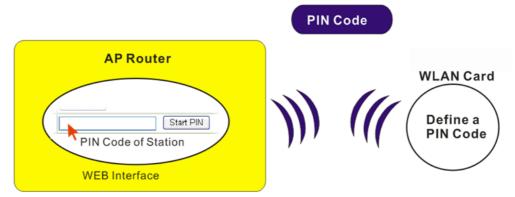
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for 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 3200 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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



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

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

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

Below shows Wireless LAN>>WPS web page.

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

Enable WPS 🖏

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

#### **Device Configure**

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

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

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

😳 : WPS is Disabled.

: WPS is Enabled.

🗘: Waiting for WPS requests from wireless clients.

Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.



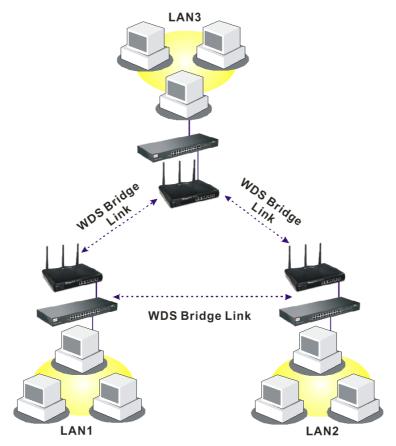
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for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

#### 4.12.6 WDS

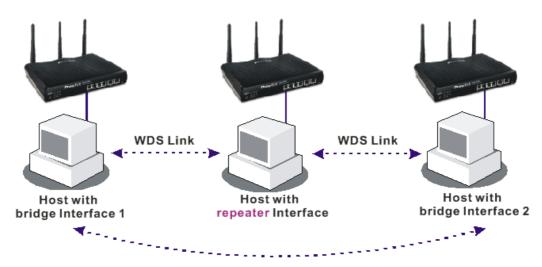
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

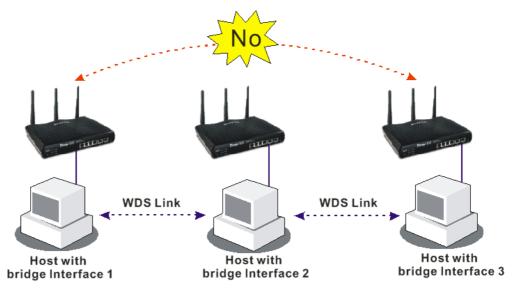


The application for the WDS-Repeater mode is depicted as below:



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

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



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

#### Wireless LAN >> WDS Settings

WDS Settings		Set to Factory Default
		Bridge
Mode: Disabl	e 💙	Enable Peer MAC Address
Security:		
Oisable OWEP	) Pre-shared Key	
WED.		
WEP:		Note: Disable unused links to get better
Use the same WEP ker <u>Settings</u> .	y set in <u>security</u>	performance.
		Repeater
Pre-shared Key:		Enable Peer MAC Addess
Туре : ТКІР		
Кеу : *****	******	
Type 8~63 ASCII characte	ers or 64 hexadecimal	
digits leading by "0x", for e "0x655abcd".	example "cfgs01a2" or	r 🗆 🛄 : 🛄 : 🛄 : 🛄 :
		Access Point Function:
		• Enable
		Status:
		Status.
		Link Status
		Note: The status is valid only when the peer also
		supports this function.
	OK	Cancel
Mode	Choose the r	mode for WDS setting. Disable mode will not
vioue		WDS setting. <b>Bridge</b> mode is designed to fulfill
		application. <b>Repeater</b> mode is for the second on
		application. Repeater mode is for the second on
	Disable 💉	*
	Disable	
	Bridge	
	Repeater	
	Repeater	—
Security	There are thr	nree types for security, <b>Disable</b> , <b>WEP</b> and
	Pre-shared	key. The setting you choose here will make the
	following W	VEP or Pre-shared key field valid or not. Choose
		for the router.
VEP		box to use the same key set in Security Settings
		did not set any key in Security Settings page, th
	check box w	vill be dimmed.
re-shared Key	<b>Type</b> – Ther	ere are three types for you to choose. <b>DrayTek</b>
		be used for all DrayTek wireless routers like
		Vigor2800, Vigor2820, and etc., except for other
		eless routers. <b>WPA</b> and <b>WPA2</b> are used for WDS
		siess routers. WIA and WIA2 are used for WDS
	devices (e.g.	g., AP700). For example, if you have a
	devices (e.g. wireless AP	g., AP700). For example, if you have a and a Vigor2820n wireless router, you can set th
	devices (e.g. wireless AP encryption m	g., AP700). For example, if you have a

	<b>Key</b> - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by " $0x$ ".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check <b>Enable</b> box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check <b>Enable</b> box in the front of the MAC address after typing.
Access Point Function	Click <b>Enable</b> to make this router serving as an access point; click <b>Disable</b> to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

### 4.12.7 Advanced Setting

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

Wireless LAN >> Advanced Setting

HT Physical Mode	
Operation Mode	💿 Mixed Mode 🔘 Green Field
Channel Bandwidth	○ 20 ④ 20/40
Guard Interval	🔘 long 💿 auto
Aggregation MSDU(A-MSDU)	🔘 Disable 💿 Enable
	ОК
Operation Mode	<b>Mixed Mode</b> – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
	<b>Green Field</b> – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	<b>20-</b> the router will use 20Mhz for data transmission and receiving between the AP and the stations.
	<b>20/40</b> – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose <b>auto</b> as guard interval, the AP router will choose short guard interval (increasing the

	wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable.</b>

### 4.12.8 WMM Configuration

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

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

'MM Capable		Enable	🔘 Disable			
PSD Capable		Enable	Oisable			
VMM Paramet	ers of Access Po	pint				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
AC_BK	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
VMM Paramete	ers of Station					
	Aifsn	CWMir	1 C	WMax	Тхор	ACM
AC_BE	3	4	10		0	
AC_BK	7	4	10		0	
AC_VI	2	3	4		94	
AC_VO	2	2	3		47	

Wireless LAN >> WMM Configuration

	OK	
--	----	--

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> Vigor2830 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.
	"Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

#### 4.12.9 AP Discovery

Wireless LAN >> Access Point Discovery

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

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List				
	BSSID	Channel	SSID	
	<u> </u>	Scan		
Con St	atiatian	Scan		
See <u>St</u>		<i>.</i> _		
	uring the scanning p e router.	orocess (~5 secor	nds), no station is allowed to connect	
Add to	WDS Settings :			
AP's MA	C address	::	:: : :	
Add	to	💽 Bridge	○ Repeater	

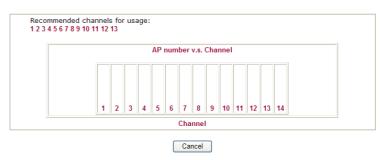
Scan

**Statistics** 

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

It displays the statistics for the channels used by APs.

Wireless LAN >> Site Survey Statistics



Add to

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

#### 4.12.10 Station List

Wireless LAN >> Station List

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

Status	MAC Address	Associated with
1	Refresh	
	Reliesh	
Status Codes : C: Connected, N	lo encryption.	
E: Connected, V P: Connected, V		
A: Connected, V	NPA2.	
B: Blocked by A N: Connecting.	ccess Control.	
F: Fail to pass V	VPA/PSK authentication.	
	ation connects to the rout	
turned off witho connection expi		will still be on the list until the
·		
Add to <u>Access C</u>	ontrol :	
Client's MAC add	tress ::::::	

Refresh

Add

Click this button to refresh the status of station list.

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

## 4.13 USB Application

USB diskette connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN/WAN can access, write and read data stored in USB diskette with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application**>**USB User Management** on the client software. Then, the client can use the FTP site (USB diskette) or share the Samba service through Vigor router.



### 4.13.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB diskette with formats of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB diskette is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

General Settings Simultaneous FTP Connections	5 (Maximum 6)	
Simultaneous FTP Connections	5 (Manimum 6)	
	5 (Maximum 6)	
Default Charset	Default 💌	
Samba Service Settings(Network Neighb	oorhood)	
◯ Enable ③ Disable		
Access Mode		
LAN Only     LAN And WAN		
NetBios Name Service		
Workgroup Name	WORKGROUP	
Host Name	Vigor	

OK

**General Settings** 

**Simultaneous FTP Connection -** This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage diskette at one time.

**Default Charset -** At present, Vigor router supports three types of character sets: default, GB2312 and BIG5.

Default	*
Default	
GB2312	
BIG5	

but both cannot contain any of the following: . ; : " < > \* + = / \ | ?.

Default Charset is for English based file name. For Simplified Chinese file/directory names, please choose GB2312; for Traditional Chinese file/directory names, choose BIG5.

Samba Service Settings	Click <b>Enable</b> to invoke samba service via the router.		
Access Mode	<b>LAN Only</b> – Users coming from internet cannot connect to the samba server of the router.		
	LAN And WAN - Both LAN and WAN users can access samba server of the router.		
NetBios Name Service	For the NetBios service of USB diskette, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as		



many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following---; : "  $<> * + = \setminus |$ ?.

**Workgroup Name** – Type a name for the workgroup.

Host Name – Type the host name for the router.

#### 4.13.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB diskette must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB diskette first. Otherwise, an error message will appear to warn you.

USB Application >> USB User Management

SB User Ma	anagement			2	Set to Factory Default
Index	Username	Home Folder	Index	Username	Home Folder
<u>1.</u>			<u>9.</u>		
<u>2.</u>			<u>10.</u>		
<u>3.</u>			<u>11.</u>		
<u>4.</u>			<u>12.</u>		
<u>5.</u>			<u>13.</u>		
<u>6.</u>			<u>14.</u>		
<u>7.</u>			<u>15.</u>		
<u>8.</u>			<u>16.</u>		

Click index number to access into configuration page.

USB Application >> USB User Management

Profile Index: 1			
FTP/Samba User	🔿 Enable 🛛 Oisable		
Username			
Password	(Maximum 11 Characters)		
Confirm Password			
Home Folder			
Access Rule			
File	🗌 Read 📃 Write 🔲 Delete		
Directory	List Create Remove		
TP/Samba User	OK Clear Cancel Enable – Click this button to activate this profile (account) for		
	FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.		
	<b>Disable</b> – Click this button to disable such profile.		
Jsername	Type the username for FTP/Samba users for accessing into FT server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing		

	into USB storage diskette.
	<b>Note:</b> "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
	Note: FTP Passive mode is not supported by Vigor Router.
	Please disable the mode on the FTP client.
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage diskette.
<b>Confirm Password</b>	Type the password again to make confirmation.
Home Folder	It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB diskette. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB diskette. <b>Note:</b> When write protect status for the USB diskette is <b>ON</b> , you cannot type any new folder name in this field. Only "/" can be used in such case.

You can click  $\overleftrightarrow$  to open the following dialog to add any new folder which can be specified as the Home Folder.

🗟 http://192.168.1.5/doc/ftpnserfolder.htm - Microsoft Internet Explorer	
USB User Management	~
	-
Choose Folder	
Folder Name	
Create New Home Folder	
Folder Name:	
Create	
Create	
Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) and space. Only 11 characters are allowed.	

Access Rule

It determines the authority for such profile. Any user, who uses such profile for accessing into USB diskette, must follow the rule specified here.

**File** – Check the items (Read, Write and Delete) for such profile.

**Directory** –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB diskette into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

#### 4.13.3 File Explorer

File Explorer offers an easy way for users to review and manage the content of USB diskette connected on Vigor router.

USB Application >> File Explorer							
File Exp	plorer						
++	•	9	Current Path: /				
			Name		Size	Delete	Rename
🛉 Սթե	oad File						
Select a	a file:						
Uplo	ad		Browse.				

Note: The folder can not be deleted when it is not empty.

** Refresh	Click this icon to refresh files list.
<b>†</b> Back	Click this icon to return to the upper directory.
🧭 Create	Click this icon to add a new folder.
<b>Current Path</b>	Display current folder.
Upload	Click this button to upload the selected file to the USB diskette. The uploaded file in the USB diskette can be shared for other user through FTP.

#### 4.13.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB diskette) via the Vigor router. If you want to remove the diskette from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB diskette later.

JSB Application >> USB Disk Status	\$	
USB Mass Storage Device Status		
Connection Status: No Disk Con	nected	Disconnect USB Disk
Disk Capacity: 0 MB		
Free Capacity: O MB <u>Refresh</u>		
USB Disk Users Connected		<u>Refresh</u>
Index Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

Connection StatusIf there is no USB diskette connected to Vigor router, "No Disk<br/>Connected" will be shown here.

Disk Capacity	It displays the total capacity of the USB diskette.	
Free Capacity	It displays the free space of the USB diskette. Click <b>Refresh</b> at any time to get new status for free capacity.	
Index	It displays the number of the client which connecting to FTP server.	
IP Address	It displays the IP address of the user's host which connecting to the FTP server.	
Username	It displays the username that user uses to login to the FTP server.	

When you insert USB diskette into the Vigor router, the system will start to find out such device within several seconds.

# 4.14 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
User Password
Configuration Backup
SysLog / Mail Alert
Time and Date
Management
Reboot System
Firmware Upgrade
Activation

# 4.14.1 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.

Aodel Name Firmware Version Build Date/Time	: Vigor3200n : 3.3.6_RC6 : Nov 3 2010 15:47	/:14			
		LAN			
	MAC Address	IP Address	Subnet Mask	DHCP Serve	er DNS
LAN1	00-50-7F-C9-B7-3C	192.168.1.1	255.255.255.0	) Yes	172.16.3.18
LAN2	00-50-7F-C9-B7-3C	192.168.3.1	255.255.255.0	) Yes	172.16.3.18
LAN3	00-50-7F-C9-B7-3C	192.168.5.1	255.255.255.0	) Yes	172.16.3.18
LAN4	00-50-7F-C9-B7-3C	192.168.7.1	255.255.255.0	) Yes	172.16.3.18
DMZ PORT	00-50-7F-C9-B7-3C	192.168.9.1	255.255.255.0	) Yes	172.16.3.18
IP Routed Subnet	00-50-7F-C9-B7-3C	192.168.2.1	255.255.255.0	) Yes	172.16.3.18
		Wireless LA	N		
MAC Address	Frequen	cy Domain	Firmware \	/ersion	SSID
00-50-7F-C9-	B7-3C Europe	-	2.3.2.0		DrayTek
		WAN			
Link Status	MAC Address	Conne	ction IP Addr	ess Defa	ult Gateway
WAN1 Disconnect	ed 00-50-7F-C9-B7-	3D			,
WAN2 Connected	00-50-7F-C9-B7-	3E Static	IP 172.16	.3.102 172.	16.1.1
WAN3 Disconnect	ed 00-50-7F-C9-B7-	3F			
WAN4 Disconnect	ed 00-50-7F-C9-B7-	40			
WAN5 Disconnect	ed 00-50-7F-C9-B7-	41			

Model Name	Display the model name of the router.		
Firmware Version	Display the firmware version of the router.		
<b>Build Date/Time</b>	Display the date and time of the current firmware built.		
LAN			
MAC Address	Display the MAC address of the LAN Interface.		
IP Address	Display the IP address of the LAN interface.		
Subnet Mask	Display the subnet mask address of the LAN interface.		
DHCP Server	Display the current status of DHCP server of the LAN interface.		
DNS	Display the assigned IP address of the primary DNS.		
Wireless LAN			
MAC Address	Display the MAC address of the wireless LAN.		
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.		
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.		
SSID	Display the SSID of the router.		
WAN			
Link Status	Display current connection status.		

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

### 4.14.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

S١	/stem	Maintenance	>>	TR-069	Setting
~		in a new years of the second			ooung

ACS and CPE Settings	
ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client	
🔘 Enable 💿 Disable	
URL	http://172.16.3.102:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	•••••
Periodic Inform Settings	
O Disable	
<ul> <li>Enable</li> </ul>	
Interval Time	900 second(s)
STUN Settings	
O Disable	
Server IP	
Server Port	3478
Minimum Keep Alive P	Period 60 second(s)
Maximum Keep Alive F	
	OK

ACS Server On	Choose the interface for the router connecting to ACS server.	
ACS Server	<b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.	
CPE Client	Such information is useful for Auto Configuration Server. <b>Enable/Disable</b> – Allow/Deny the CPE Client to connect with Auto Configuration Server. <b>Port</b> – Sometimes, port conflict might be occurred. To solve	



	such problem, you might change port number for CPE.
Periodic Inform Settings	The default setting is <b>Enable</b> . Please set interval time or schedule time for the router to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.
STUN Settings	The default is <b>Disable</b> . If you click <b>Enable</b> , please type the relational settings listed below:
	Server IP – Type the IP address of the STUN server.
	Server Port – Type the port number of the STUN server.
	<b>Minimum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	<b>Maximum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

#### 4.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup					
Administrator Password	Administrator Password				
Old	Old Password				
Nev	New Password		]		
Cor	nfirm Password	•••••	]		
OK					
Old Password	• •	Type in the old password. The factory default setting for password is <b>"admin"</b> .			
New Password	Type in new	Type in new password in this field.			
Confirm Passwor	<b>d</b> Type in the	Type in the new password again.			

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



#### 4.14.4 User Password

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

# User Password

Old Password	
New Password	
Confirm Password	

OK

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this field.

Confirm PasswordType in the new password again.

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

#### 4.14.5 Configuration Backup

#### **Backup the Configuration**

Follow the steps below to backup your configuration.

System Maintenance >> Configuration Backup

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

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

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

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

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

Save As						? ×
Save in:	🞯 Desktop		~	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	iystem Maintenance >> Configuration Backup Configuration Backup / Restoration				
Configuration					
Restoration					
	Select a configuration file. Browse.,				
	Click Restore to upload the file. Restore				
Backup					
	Click Backup to download current running configurations as a file. Backup Cancel				

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

# 4.14.6 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

SysLog Access Setup	Mail Alert Setup	
SysLog Access Setup  Syslog Save to:  Syslog Server  USB Disk  Router Name  Server IP Address  Destination Port  Sta  Enable syslog message:  Firewall Log  VPN Log  Call Log  WAN Log  Router/DSL information	Mail Alert Setup  C Enable  SMTP Server  SMTP Port  Mail To  Return-Path  Authentication User Name Password  Enable E-Mail Alert:  DoS Attack  M IM-P2P	Send a test e-mail
AlertLog Setup Enable AlertLog Port 514		

OK Clear Refresh

Enable	Check Enable to activate function of syslog.
Syslog Save to	Check Syslog Server to save the log to Syslog directly.
	Check USB Disk to save the log to the attached USB diskette.
Router Name	Display the name for such router configured in <b>System</b> Maintenance>>Management.
	If there is no name here, simply lick the link to access into <b>System Maintenance&gt;&gt;Management</b> to set the router name.
Server IP Address	The IP address of the Syslog server.
<b>Destination Port</b>	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
AlertLog Setup	Check "Enable" to activate function of alert log.
	Type the port number for alert log. The default setting is 514.
Mail Alert Setup	Check "Enable" to activate function of mail alert.
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.

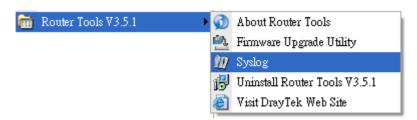


Mail To	Assign a mail address for sending mails out.			
Return-Path	Assign a path for receiving the mail from outside.			
Authentication	Check this box to activate this function while using e-mail application.			
User Name	Type the user name for authentication.			
Password	Type the password for authentication.			
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.			

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

🎒 Дтау	Tek Syslog	3.6.1							
Contro		iets	192.168.1.1 Vigor series RX Packets 1470	•	WAN Sta	itus Gateway IF  WAN IP ( 	<u> </u>	TX Packets 0 RX Packets 0 0	TX Rate 0 RX Rate 0
Firewa	ll Log VPN	Log User Acc	ess Log Call Log	WAN Log	Others	Network I	Information Ne	et State	
On	Line Routers			Host N	ame:		vivian		
	IP Address	Mask	MAC	NIC De	scription:		SiS 900-Based I	PCI Fast Ethernet Adap	ter - Packet St 🐱
1	92.168.1.1	255.255.2	00-50-7F-54-6	NIC Inf	ormation –				
				MAC A	ddress:	00-1	1-D8-E4-58-CE	Default Geteway:	192.168.1.1
				IP Add	ress:	192.1	68.1.10 🔽	DHCP Server:	192.168.1.1
				Subne	t Mask:	25	5.255.255.0	Lease Obtained:	Mon Jan 22 01:28:23 2007
	<i>a</i>	efresh		DNS S	ervers:	168.9	5.1.1	Lease Expires:	Thu Jan 25 01:28:23 2007
ADSL	Status Mode		State	Up S	peed 	Do	wn Speed	SNR Margin	Loop Att

## 4.14.7 Time and Date

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

nformation		
Current System Time	2010 Apr	2 Fri 9 : 1 : 58 Inquire Time
C actives		
Setup		
🔘 Use Browser Time		
💿 Use Internet Time C	lient	
Server IP Address		pool.ntp.org
Time Zone		(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Savir	ig	
Automatically Update	Interval	30 min 🗸

<b>Current System Time</b>	Click <b>Inquire Time</b> to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check this box to enable daylight saving function.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

#### 4.14.8 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.

Router Name		3200	Management Port Setu	p
			📃 💿 User Define Ports	🔘 Default Ports
Management	Access Cont	rol	Telnet Port	23 (Default: 23)
📃 Allow mar	nagement fr	om the Internet	HTTP Port	80 (Default: 80)
🗌 FTP Se	erver		HTTPS Port	443 (Default: 443)
MTTP :	Server		FTP Port	
🗹 HTTPS	Server			(,
<ul><li>Telnet Server</li><li>SSH Server</li></ul>			SSH Port	22 (Default: 22)
			SNMP Setup	SNMP Setup
🗹 Disable PI	NG from the	e Internet	Enable SNMP Age	nt
Access List			Get Community	public
List	IP	Subnet Mask	Set Community	private
1		*	Manager Host IP	
2		~	Trap Community	public
3		*	Notification Host IP	
			Trap Timeout	10 seconds

System Maintenance >	>> Management
----------------------	---------------

Router Name	Type a name as a identification for such router.
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	List IP - Indicate an IP address allowed to login to the router.
	<b>Subnet Mask -</b> Represent a subnet mask allowed to login to the router.
Default Ports	
Default Ports User Defined Ports	router. Check to use standard port numbers for the Telnet and HTTP
	router. Check to use standard port numbers for the Telnet and HTTP servers. Check to specify user-defined port numbers for the Telnet,

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.

#### 4.14.9 Reboot System

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

System Maintenance >> Reboot System Reboot System		
	Osing current configuration	
	O Using factory default configuration	
1	OK	

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.



#### 4.14.10 Firmware Upgrade

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

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

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

System	Maintenance	>>	Firmware	Upgrade
--------	-------------	----	----------	---------

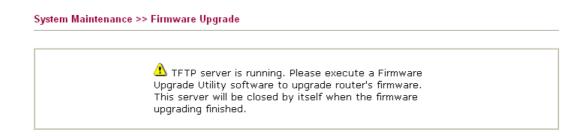
Web	Firmware	U	n a	rad	e

Select a firmware file.				
		Browse		
Click Upgrade to upload the file.	Upgrade			

TFTP Firmware Upgrade from LAN

Curre	Current Firmware Version: 3.3.6_RC6	
Firmv	vare Upgrade Procedures:	
1.	Click "OK" to start the TFTP server.	
2.	Open the Firmware Upgrade Utility or other 3-party TFTP client software.	
З.	Check that the firmware filename is correct.	
4.	Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.	
5.	After the upgrade is compelete, the TFTP server will automatically stop running.	
Do yo	u want to upgrade firmware ? OK	

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



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

#### 4.14.11 Activation

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

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

System Maintenance >> Activati	on Activate via interface : auto-selected 🗸
Web-Filter License [Status:Not Activated]	<u>Activate</u>
Authentication Message	
WebFilter, service not a	ctivate 2010-08-16 07:58:36
	l alert or syslog, please configure the SysLog/Mail Alert Setup page. ce provider, the configuration of the function will be reset.
	OK Cancel
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.
	Activate via interface : auto-selected value auto-selected WAN 1
	WAN 2 WAN 3 WAN 4 WAN 5
Activate	The <b>Activate</b> link brings you accessing into http://myvigor.draytek.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.



Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation	Activate via interface : auto-selected 💙
Web-Filter License	Activate
[Status:Commtouch] [Start Date:2010-07-27 Expire Date:20	10-08-27]
Authentication Message	
Activated Wiz, Activated Wizard query license status 08:47:13	3 Successful, 2010-07-27 🔗
	M
Note: If you want to use email alert or syslog, please configure If you change the service provider, the configuration of t	, , , , , , , ,
OK Cancel	

# 4.15 Diagnostics

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



#### 4.15.1 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
        Refresh

        HEX Format:
        00 50 7F 22 33 44-00 0E A6 2A D5 A1-08 00

        45 00 00 4B 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

        00 01 00 00 00 00 00 00 00-07 67 61 74 65 77 61 79

        09 6D 65 73 73 65 6E 67-65 72 07 68 6F 74 6D 61

        69 6C 03 63 6F 6D 00 00-01 00 01 E6 84 1A 00 00

        Decoded Format:

        192.168.1.10,1483 -> 168.95.1.1,domain

        Pr udp HLen 20 TLen 75
```

**Decoded Format** It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

#### 4.15.2 Routing Table

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

Diagnostics >> View Routing Table

```
Current Running Routing Table Refresh Key: C - connected, S - static, R - RIP, * - default, ~ - private

* 0.0.0.0/ 0.0.00 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.

#### 4.15.3 ARP Cache Table

Diagnostics >> View 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.

thernet ARP Cache	Table	<u>Clear</u>   <u>Refresh</u>
IP Address	MAC Address	2
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

Click it to reload the page.

Clear

Click it to clear the whole table.

#### 4.15.4 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

```
DHCP IP Assignment Table
                                                                           Refresh
          : 192.168.1.1/255.255.255.0, DHCP server: On
LAN1
Index
      IP Address MAC Address
                                        Leased Time
                                                              HOST ID
1
        192.168.1.10
                       EO-CB-4E-DA-48-79
                                              142:37:18.720
                                                              carrie-Oc7cb251
        192.168.1.255 00-50-7F-C9-B7-3C
                                              CONFLICTED IP
2
        192.168.1.0 00-50-7F-C9-B7-3C
                                              CONFLICTED IP
3
4
        192.168.1.1
                      00-50-7F-C9-B7-3C
                                               CONFLICTED IP
DMZ Port : 192.168.9.1/255.255.255.0, DHCP server: On
Index IP Address MAC Address
1 192.168.9.255 00-50-7F-C9-
                                         Leased Time
                                                              HOST ID
                      00-50-7F-C9-B7-3C
                                               CONFLICTED IP
       192.168.9.0
                      00-50-7F-C9-B7-3C
                                              CONFLICTED IP
2
3
        192.168.9.1
                       00-50-7F-C9-B7-3C
                                               CONFLICTED IP
```

Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.

Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

#### 4.15.5 NAT Sessions Table

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

Diagnostics >>	NAT	Sessions	Table

Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface	
.92.168.1.10	1032	34440	216.156.209.25	8888	WAN2	
92.168.1.10	1032	34440	208.91.112.195	8888	WAN2	
92.168.1.10	1032	34440	174.137.33.91	8888	WAN2	
92.168.1.10	1033	34441	208.91.112.195	8888	WAN2	
92.168.1.10	1033	34441	216.156.209.25	8888	WAN2	
92.168.1.10	1034	34442	216.156.209.25	8888	WAN2	
92.168.1.10	1034	34442	208.91.112.195	8888	WAN2	
92.168.1.10	1034	34442	174.137.33.91	8888	WAN2	
92.168.1.10	1057	34465	61.64.70.126	5653	WAN2	
92.168.1.10	1871	35279	207.46.125.36	1863	WAN2	
92.168.1.10	2458	35866	118.168.178.13	34542	WAN2	
92.168.1.10	2460	35868	218.161.51.137	2625	WAN2	
92.168.1.10	2461	35869	115.165.232.72	10465	WAN2	

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.

#### 4.15.6 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	
💿 Enable 🔘 Disable	
Default Max Sessions: 100	
Limitation List	
Index Start IP	End IP

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



#### Diagnostics >> Data Flow Monitor

#### 🗹 Enable Data Flow Monitor

		Refresh Seconds:	10 🚩 Page: 1 🔽	<u>R</u>	efresh
Index	IP Address	<u>TX rate(Kbps)</u>	<u>RX_rate(Kbps)</u> 😪	Sessions	Action
1	192.168.1.10_CARRIE-0C7CB251	9	0	92	<u>Block</u>
			Current / Peak / Speed	Current / Peak	
WAN1		0/0/Auto			
WAN2		9 / 456 / Auto	6 / 1080 / Auto		
WAN3			0 / 0 / Auto		
WAN4		0 / 0 / Auto	0 / 0 / Auto		
WAN5		0 / 0 / Auto	0 / 0 / Auto		
Total		9 / 456 / Auto	6 / 1080 / Auto	54 / 681	

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

3. (Kbps): shared bandwidth + : residual bandwidth used

Current/Peak are average.

#### **Enable Data Flow** Monitor

Check this box to enable this function.

**Refresh Seconds** Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.

Refresh Seconds: 10 🔽



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

Page: 1	*	<u>Refresh</u>
Kbps)	Sessions	Action
		<u>Block</u>

**Unblock** – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.

Page	1 💙	<u>Refresh</u>
s <u>)</u>	Sessions	Action
	blocked / 299	<u>Unblock</u>

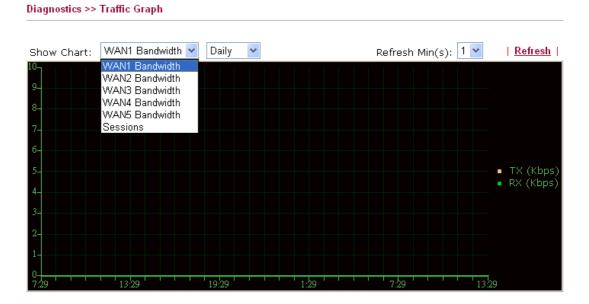
Current /Peak/SpeedCurrent means current transmission rate and receiving rate for<br/>WAN interface.Peak means the highest peak value detected by the router in

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

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

#### 4.15.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.





# Diagnostics >> Traffic Graph Show Chart: WAN1 Bandwidth ♥ 9 0 33 0 27 0 27 0 16 0 16 0 16 0 16 0 16 0 27 2/15(F) 2/14(TH) 2/15(F) 2/14(TH) 2/15(F)

The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2/WAN3/WAN4/WAN5 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.

#### 4.15.8 Ping Diagnosis

Diagnostics >> Ping Diagnosis

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

Ping through: Unspecified V Ping to: Host / IP V IP Address: Host / IP Run DNS Result Gateway 1 Clear   Gateway 2 Gateway 3 Gateway 4 Gateway 5	which WAN to	ping through	, please select "	don't want to specify Unspecified".	
Host / IP     Run       DNS     Gateway 1       Gateway 2     Gateway 3       Gateway 4     Gateway 4	Ping throug	gh: Unspecifie	ed 🔽		
Result     Gateway 1     Clear       Gateway 2     Gateway 3       Gateway 4	H	ost / IP			]
	Result G G G G	ateway 1 ateway 2 ateway 3 ateway 4		<u> </u>	lear
					~

Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose <b>Unspecified</b> to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.

Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

#### 4.15.9 Trace Route

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

Diagnostics >>	Trace Route		
Trace Route			
	Trace through:	Unspecified V	
	Protocol:		
	Host / IP Address:	ICMP Run	
	Result	UDP	
		<u>^</u>	
		~	

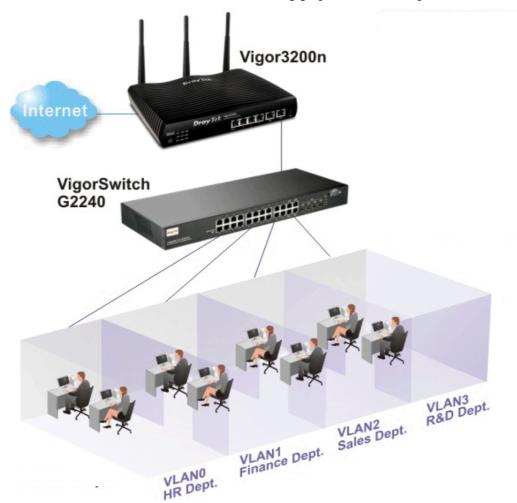
Trace through	Use the drop down list to choose the WAN interface that you want to ping through.
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.



# 5.1 How to Configure Multi-Subnet

By identifying the tagged message, Vigor3200 can divide the LAN Port into several VLAN groups. Such LAN port with tagged information will accept the packets only with VLAN ID number.

For example, Vigor3200 can divide the internal departments of a company into four different groups by using VigorSwitch G2240. Each group uses different network segment and does not connect for each other. VigorSwitch G2240 Trunk Port 23 and Vigor3200 LAN Port are connected with network cable. See the following graphic for an example.



VLAN0 (Human Resource): LAN Port 4 IP: 192.168.1.0/24 VLAN1 (Finance Dept): LAN Port 4 IP: 192.168.3.0/24 VLAN2 (Sales Dept.): LAN Port 4 IP: 192.168.5.0/24 VLAN3 (R&D): LAN Port 4 IP: 192.168.7.0/24



#### **Configuration for Vigor3200**

- 1. In the page of LAN >> VLAN Configuration, check the box of Enable to enable the function of VLAN Configuration.
- 2. Untag VLAN0 and set LAN4 as the Subnet.
- 3. To activate the function of VLAN Tag for VLAN1 setting, check the box of **Enable** and type the value (10) for VID setting. Then check **LAN Port** and set **LAN1** as the **Subnet**.
- 4. To activate the function of VLAN Tag for VLAN2 setting, check the box of **Enable** and type the value (20) for VID setting. Then check **LAN Port** and set **LAN2** as the **Subnet**.
- 5. To activate the function of VLAN Tag for VLAN3 setting, check the box of **Enable** and type the value (30) for VID setting. Then check **LAN Port** and set **LAN3** as the **Subnet**.
- 6. To activate the function of VLAN Tag for VLAN4 setting, check the box of **Enable** and type the value (40) for VID setting. Then check **LAN Port** and set **LAN4** as the **Subnet**.

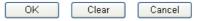
🗹 Enable					
		VLAN Tag			
	Enable	VID	Priority	LAN Port	Subnet
VLAN0		0	0 🛩	<b>V</b>	LAN 4 💌
VLAN1		10	0 💌		LAN 1 🔽
VLAN2		20	0 💌		LAN 2 💌
VLAN3		30	0 💌		LAN 3 🔽
VLAN4		40	0 💌		LAN 4 💌
VLAN5		0	0 🛰		LAN 1 🔽
VLAN6		0	0 🗠		LAN 1 🔽
VLAN7		0	0 🔽		LAN 1 🔽

LAN >> VLAN Configuration

1. Hybrid mode only applied on VLANO to accept both tagged/untagged packets;

2. Tag based VLAN only applied for LAN Port;

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



In the page of LAN >> General Setup, check the Status box of LAN2, LAN3, LAN4 and enable the function of DHCP.

#### LAN >> General Setup

General Setup				
Index	Status	DHCP	IP Address	
LAN 1	V	V	192.168.1.1	Details Page
LAN 2	<b>v</b>		192.168.3.1	Details Page
LAN 3	<b>V</b>		192.168.5.1	Details Page
LAN 4	<b>~</b>	<b>~</b>	192.168.7.1	Details Page
DMZ	V	V	192.168.9.1	Details Page
IP Routed Subnet		<b>V</b>	192.168.2.1	Details Page

After finishing the above configuration, the equipment connecting to Vigor3200 LAN Port can get the corresponding IP address of the network segment.

The equipment connecting to Vigor3200 LAN Port 1 (LAN1) can get the IP address of 192.168.1.0/24.

The equipment connecting to Vigor3200 LAN Port 2 (LAN2) can get the IP address of 192.168.3.0/24.

The equipment connecting to Vigor3200 LAN Port 3 (LAN3) can get the IP address of 192.168.5.0/24.

The equipment connecting to Vigor3200 LAN Port 4 (LAN4) can get the IP address of 192.168.7.0/24.

For the detailed settings of the network segment, open LAN>>General Setup and click **Details Page.** Adjust the settings for your request. Refer to the following figure.

LAN >> General Setup

letwork Configuration		DHCP Server Configuration	n
or NAT Usage		💿 Enable Server 🔘 Disa	ble Server
IP Address	192.168.1.1	Relay Agent: OEnable	🔾 Disable
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
		IP Pool Counts	50
IP Protocol Control	Disable 💌	Gateway IP Address	192.168.1.1
		DHCP Server IP Address for Relay Agent	
		DNS Server IP Address	
		🔲 Force DNS manual se	etting
		Primary IP Address	
		Secondary IP Address	

7. To make any two of VLAN groups linked with each other, just check the boxes of the ones in the field of Inter-LAN Routing in the page of LAN >> General Setup. Refer to the following figure. LAN2 and LAN3 are linked.

IP Routed Subnet		$\checkmark$	192.168.2.1		Details Page		
Inter-LAN Routing		$\frown$					
Subnet	LAN 1	( LAN 2 )	LAN 3	LAN 4	DMZ PORT		
LAN 1							
LAN 2							
LAN 3		→ 🔽	$\checkmark$				
LAN 4				V			
DMZ PORT	<b>~</b>			<ul> <li>Image: A set of the set of the</li></ul>			

#### **Configuration for VigorSwitch G2240**

- 1. Open Vlan>>Tag-based Group.
- 2. Add four VID groups. In this case, we can explanation it with Port 15, 16, 17, 18 and Trunk Port 23.

rt In			P Aware		hips Con			_	Pronacta												
n Mode a-based Group		C TON	VLAN					- Oliv	Tropage		100	F	Port Memi	bers	av – n						100-1
based Group	Del	VID	IGMP-A	P-VLAN	GVRP-P	1 2	3	4 5 1	5 7 8	9 1	0 11	12	13 14	15	16	17	18 1	19 2	0 21	22 7	3 24
ts Lisolation	1.0		Defa	ult		1															
lagement Vian	1	1	Disable	Disable	Disable	1															24
C			3200-	VID10										10							
P		10	Disable	Disable	Disable									15						- 13	3
		-	3200-	VID 20			1	1311212		100	3	12 2		-					14	-	
Р		20		Disable	Disable										16					1	3
		en.	3200-		Lindavit									-							
C Binding					Disable											17				1	3
x		30		Disable	Disable	_			-		_	-		_	-	_	_	_	-	_	_
			3200-														18				3
		_40_	Disable	Disable	Disable	-		an Viel-						-	-		14			_ 1	
oring icast n P Snooping k/Restore ort/Import nostics																					

VLAN Name 3200-VID10, Port Members = 15 × 23 VLAN Name 3200-VID20, Port Members = 16 × 23 VLAN Name 3200-VID30, Port Members = 17 × 23 VLAN Name 3200-VID40, Port Members = 18 × 23

3. Open Vlan>> Ports and set the VID value with role for each Port:

Port 15 VID = 10 Role = Access Port 16 VID = 20 Role = Access Port 17 VID = 30 Role = Access Port 18 VID = 40 Role = Access Port 23 VID = 1 Role = Trunk

Port 23 is set with Trunk in this example and will transfer the packets with VLAN Tag information. That is, packets with VID 10, 20, 30 and 40 will be transferred to Vigor3200 by Port 23 and VID information will be retained.

Dray Tek	Over to	1		<b>H</b>	Ĥ	1Ê.	<b>Å</b>		
		I Con							
VigorSwitch G2240 🔷	5	2		All	×	80	Access 💌	U	UISADIe
System	6	<b>V</b>		All	~	86	Access 💌	0	Disable
Port	7	4		All	*	86	Access ⊻	0	Disable
⊡ Vlan	8	1		All	~	86	Trunk 💌	0	Disable
Vlan Mode Tag-based Group	9	~		All	~	84	Access 💌	0	Disable
Port-based Group	10	~		All	~	84	Access 💌	0	Disable
Ports Port Isolation	11			All	~	84	Access 💌	0	Disable
Management Vian	12	~		All	~	84	Trunk 💌	0	Disable
MAC	13	2		All	~	2611	Trunk 💙	0	Disable
GVRP Gos	14			All	~	2611	Access V	0	Disable
SNMP	1.1.1			1.1.1		-			
⊡ACL	15	~		All	*	10	Access 💙	0	Disable
IP MAC Binding	16	<b>V</b>		All	*	20	Access ⊻	0	Disable
⊡802.1X	17	~		All	*	30	Access 🔀	0	Disable
Trunk	18	~		All	~	40	Access 💌	0	Disable
	19	~		All	~	3700	Access 👻	0	Disable
MSTP     Mirroring	20	<b>v</b>		All	¥	3700	Access 💙	0	Disable
⊡Multicast	21	2		All	~	1	Access 💙	0	Disable
Alarm	22			All	~	1	Access V	0	Disable
DHCP Snooping		100000 C	<u> </u>	A COLORADO			Contraction of the second	1	
■LLDP	23	~		All	~	1	Trunk 💌	0	Disable
Save/Restore  Export/Import	24			All	*	1	Trunk 💌	0	Disable

4. After finishing the above configuration, the equipment connecting to VigorSwitch Port 15, 16, 17 and 18 can get the corresponding IP address(es) of the network segment.

The equipment connecting to VigorSwitch Port 15 can get the IP address of 192.168.1.0/24

The equipment connecting to VigorSwitch Port 16 can get the IP address of 192.168.3.0/24

The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.5.0/24

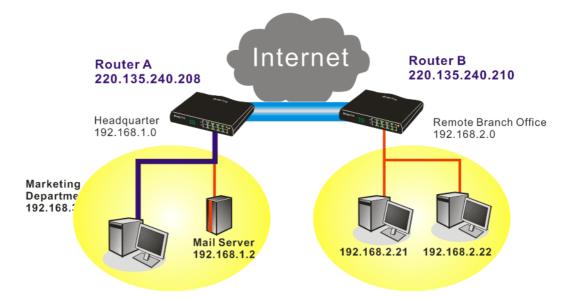
The equipment connecting to VigorSwitch Port 18 can get the IP address of 192.168.7.0/24

5. To make any two of VLAN groups of Tag Based VLAN linked with each other, just check the boxes of the ones in the field of **Inter-LAN Routing** in the page of **LAN** >> **General Setup**. Refer to the following figure. LAN2 and LAN3 are linked.

IP Routed Subnet		$\checkmark$	192.168.2.1		Details Page		
ter-LAN Routing		$\frown$					
Subnet	LAN 1	( LAN 2 )	LAN 3	LAN 4	DMZ PORT		
LAN 1	$\checkmark$						
LAN 2							
LAN 3	<b>—</b>	→ 🔽	$\checkmark$				
LAN 4				<b>V</b>			
DMZ PORT	<b>V</b>		<b>V</b>	<b>V</b>	$\checkmark$		

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

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



#### Settings in Router A in headquarter:

-----

- 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	or 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	<b>*</b>	
Nutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup							
VPN IKE/IPSec General Setup							
Dial-in Set up for Remote Dial-in users	s and Dynamic IP Client (LAN to LAN).						
IKE Authentication Method							
Pre-Shared Key	••••						
Confirm Pre-Shared Key	•••••						
IPSec Security Method							
🗹 Medium (AH)							
Data will be authentic, but	: will not be encrypted.						
High (ESP) 🛛 🔽 DES 📝	3DES 🔽 AES						
Data will be encrypted and	1 authentic.						
	OK Cancel						

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name Branch1 Enable this profile VPN Dial-Out Through WAN1 First V Netbios Naming Packet OPass OBlock Multicast via VPN OPass OBlock (for some IGMP,IP-Camera,DHCP Relayetc.)	Call Direction <ul> <li>Both</li> <li>Dial-Out</li> <li>Dial-in</li> <li>Always on</li> </ul> Idle Timeout <ul> <li>300</li> <li>second(s)</li> <li>Enable PING to keep alive</li> <li>PING to the IP</li> </ul>

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

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

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 👻
О РРТР	Username	???
IPSec Tunnel	Password	
C L2TP with IPSec Policy None	PPP Authentication	
Dial Number for ISDN or	VJ Compression	⊙ On ○ Off
Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Method	
220.135.240.210	Pre-Shared Key	
	IKE Pre-Shared Key	
	O Digital Signature(X.509)	9)
	None 🗸	
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES without	Authentication
	Advanced	
	Index(1-15) in <u>Schedule</u>	Setup:

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

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 💙
⊙ РРТР	Username	draytek
O IPSec Tunnel	Password	••••
C L2TP with IPSec Policy None	PPP Authentication	PAP/CHAP 🗸
	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) 220.135.240.210	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509 None IPSec Security Method Medium(AH) High(ESP) DES without Advanced Index(1-15) in <u>Schedule</u>	Authentication



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

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

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

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

3. Dial-In Settings		
Allowed Dial-In Type		
🗹 РРТР	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.210	Digital Signature(X.509)	
or Peer ID	None 💌	
	IPSec Security Method	
	Medium(AH)	
	High(ESP) 🗹 DES 🗹	3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

4. TCP/IP Network Setting	ıs	
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	
Local Network IP	192.168.1.1	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	
	More	
	OK	Clear Cancel

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

VPN and Remote Access >> PPP General Setup

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

PPP/MP Protocol	IP Address Assignment for	Dial-In Users
Dial-In PPP PAP or CHAP	(When DHCP Disable set) Assigned IP range	192,168,2,200
Dial-In PPP Encryption (MPPE) Optional MPPE	5	
Mutual Authentication (PAP) 🛛 🔿 Yes 💿 No		
Username		
Password		

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup		
VPN IKE/IPSec General Setup		
Dial-in Set up for Remote Dial-in users a	nd Dynamic IP Client (LAN to LAN).	
IKE Authentication Method		
Pre-Shared Key	••••	
Confirm Pre-Shared Key	••••	
IPSec Security Method		
Medium (AH)		
Data will be authentic, but w	/ill not be encrypted.	
High (ESP) 🛛 🔽 DES 🔽 30	DES 🔽 AES	
Data will be encrypted and a	uthentic.	
	OK Cancel	

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name Branch1 Enable this profile VPN Dial-Out Through WAN1 First V Netbios Naming Packet Pass Block Multicast via VPN Pass Block (for some IGMP,IP-Camera,DHCP Relayetc.)	Call Direction   Both Dial-Out Dial-in  Always on  Idle Timeout  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 😽
О РРТР	Username	???
● IPSec Tunnel	Password	
C L2TP with IPSec Policy None	PPP Authentication	
Dial Number for ISDN or	VJ Compression	⊙ On ◯ Off
Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Method	
220.135.240.208	Pre-Shared Key	
	IKE Pre-Shared Key	
	O Digital Signature(X.509	)
	None 🗸	
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES without	Authentication
	Advanced	
	Index(1-15) in <u>Schedule</u> S	Getup:

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

Type of Server I am calling	Link Type	64k bps 💉
• PPTP	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)	IKE Authentication Metho	od
220.135.240.208	IKE Pre-Shared Key	
	O Digital Signature(X.	509)
	IPSec Security Method	
	<ul> <li>Medium(AH)</li> <li>High(ESP) DES with</li> </ul>	out Authentication
	Advanced	
	Index(1-15) in <u>Schedu</u>	le Setup:

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

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

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP IPSec Tunnel L2TP with IPSec Policy None	Username Password VJ Compression	??? 
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID	IKE Authentication Method	9) 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.

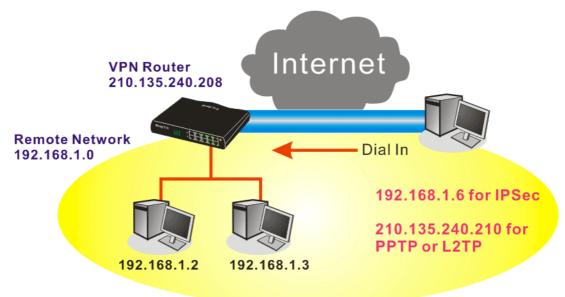
3. Dial-In Settings		
Allowed Dial-In Type		
🕑 рртр	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
<ul> <li>Specify Remote VPN Gateway</li> <li>Peer VPN Server IP</li> </ul>	✓ Pre-Shared Key	
	KE Pre-Shared Key	
220.135.240.208	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 B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings			
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	
Remote Network IP	192.168.1.0		Route 🔽
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	Change default route single WAN supports this	to this VPN tunnel ( Only )
Local Network Mask	255.255.255.0		/
	More		
OK Clear Cancel			

# 5.3 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



#### Settings in VPN Router in the enterprise office:

- 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**.



VPN and Remote Access >> PPP General Setup

PPP/MP Protocol	IP Address Assignment for Dial	In Users
Dial-In PPP PAP or CHAP V	(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.

/PN IKE/IPSec General Setup	
Dial-in Set up for Remote Dial-in use	ers 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, b	ut will not be encrypted.
High (ESP) 🛛 🗹 DES 🛛	☑ 3DES 🔍 AES
Data will be encrypted ar	nd authentic.

- 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.

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

Index No. 1	
User account and Authentication	Username ???
Enable this account	Password
Idle Timeout 300 second(s)	Enable Mobile One-Time Passwords(mOTP)
Allowed Dial-In Type	PIN Code
РРТР	Secret
🗹 IPSec Tunnel	
L2TP with IPSec Policy None	IKE Authentication Method
Specify Remote Node	Pre-Shared Key
Remote Client IP or Peer ISDN Number	IKE Pre-Shared Key
	Digital Signature(X.509)
or Peer ID	None 💌
Netbios Naming Packet 💿 Pass 🔘 Block	IPSec Security Method
Multicast via VPN 🛛 🔘 Pass 💿 Block	Medium(AH)
(for some IGMP,IP-Camera,DHCP Relayetc.)	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
	Local ID (optional)
Subnet	
Assign Static IP Address	
0.0.0.0	
ОК Г	Clear Cancel

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

User account and Authentication	Username ???
Enable this account	Password
Idle Timeout <u>300</u> second(s)	Enable Mobile One-Time Passwords(mOTP)
Allowed Dial-In Type	PIN Code
PPTP	Secret
IPSec Tunnel	IKE Authentication Method
L2TP with IPSec Policy None	Pre-Shared Key
Specify Remote Node	IKE Pre-Shared Key
Remote Client IP or Peer ISDN Number	Digital Signature(X.509)
or Peer ID Netbios Naming Packet 💿 Pass 🔘 Block	IPSec Security Method
Multicast via VPN	Medium(AII)
(for some IGMP,IP-Camera,DHCP Relayetc.)	High(ESP) 🗹 DES 🗹 3DES 🗹 AES
Subnet	Local ID (optional)
LAN 1 💌	
Assign Static IP Address	

#### 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.

Q240262 in the M	tion. For more licrosoft Know	: connectio infomation	n using . , please	to computer in a pre-shared key a read the article
		Ingare		
Step 1. Dial to IS	P			
If you have alread	dy gotten a n	ublic TD vo	u can d	vin this sten
If you have alrea	ady gotten a p	ublic IP, yo	iu can sł	kip this step.
If you have alrea	ady gotten a p	ublic IP, yo	ou can sł	kip this step. Dial
If you have alread			ou can sł	
			iu can sł	

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	X
Session Name:	Office
VPN Server IP/HOS	Name(such as 123.45.67.89 or draytek.com)
192.168.1.1	
User Name :	draytek_user1
Password :	łokołokokał
Type of VPN	
○ PPTP	OL2TP
IPSec Tunne	L2TP over IPSec
PPTP Encryption	
No encryptic	n' :
C Require enci	yption
O Maximum str	ength encryption
🔲 Use default g	ateway on remote network
ОК	Cancel

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



My IP :	172.16.3.10	0 🗸
ype of IPSec		
O Standard	IPSec Tunnel	
Remote	: Subnet :	0 , 0 , 0 , 0
Remote	: Subnet Mask :	255 , 255 , 255 , 0
💿 Virture IP	Dray	Tek Virture Interface 🛛 😽
📀 Obta	in an IP address	automatically (DHCP over IPSec)
🚫 Spec	ify an IP address	
IP A	ddress:	192 , 168 , 1 , 201
Sub	net Mask:	255 , 255 , 255 , 0
ecurity Meth	od	
C Mandiana / 1	4H) 🤇	High(ESP)
O Medium(A	×.	DES 😽
MD5		
MD5	hod	
MD5 Authority Met		
MD5 Authority Met	ed Key : *****	
MD5 Authority Met		Browse

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

Dial To VPN		
Session Name:	office	
VPN Server IP/HC	ST Name(suc	h as 123.45.67.89 or draytek.com)
192.168.1.1		
User Name :	draytek_u	user1
Password :	****	
Type of VPN		
PPTP		OL2TP
O IPSec Tun	nel	OL2TP over IPSec
PPTP Encryption	1.	
🔘 No encryp	tion	
Require er	ncryption	
O Maximum :	strength encr	yption
🔽 Use default	gateway on	remote network
	<	Cancel

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



# 5.4 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 other room.

1. Go to **Bandwidth Management>>Quality of Service.** 

Genera	l Setup							Set t	o Factory De	<u>fault</u>
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WANЗ	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
Class R	ule									
Ind	ex		Name					Rule	Service T	ype
Clas	s 1							<u>Edit</u>		
Clas	s 2							<u>Edit</u>	<u>Edit</u>	
Clas	s 3							Edit		

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 ✓ Enable the QoS Control OUT ✓ WAN Inboun OUT dth WAN Outbound Danewidth

3. Set Inbound/Outbound bandwidth.

10000 Kbps	
10000 Kbps	
ist be smaller than the real languagested to set the bandwid sical network speed provid	dth value for
	ist be smaller than the real lauggested to set the bandwi

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

nail				
Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
Inactive	Any	Any	ANY	undefined
				Status Local Address Remote Address CodePoint

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

Bandwidth Management >> Quality of Service					
WAN1 General Setup					
	I Inbound Bandwidth	10000 Kbps			
WAN Outbound Bandwidth		10000 Kbps			
Index	Class Name	Reserved bandwidth Ratio			
Class 1	E-mail	25 %			
Class 2		25 %			
Class 3		25 %			
	Others	<b>25</b> %			
Enable UDP Band	dwidth Control	Limited_bandwidth Ratio 25 %			
Outbound TCP A	CK Prioritize	Online Statistics			
	OK Clea	r Cancel			

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

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

Vigor3200 Series User's Guide

#### 7. Click **Setup** link for one of the WAN interface.

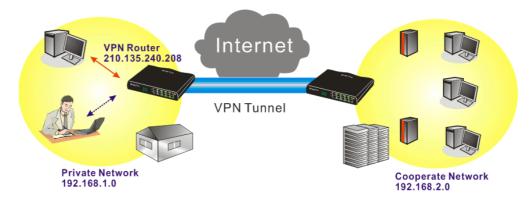
Bandwidth Management >> Quality of Service

Genera	Setup							Set t	o Factory D	efault
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setu</u>
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
Class R Inde			Name					Rule	Service	Гуре
Class	s 1		E-mail					<u>Edit</u>		
Clas	s 2		HTTPS					<u>Edit</u>	<u>Edit</u>	
Class	s 3							Edit		

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

Bandwidth Manag	ement >> Quality of Service	
WAN1 General Se Enable the Q	-	
v	VAN Inbound Bandwidth	10000 Kbps
v	VAN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 % Online Statistics
	OK Clear	Cancel

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



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

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

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

Bandwidth Managemen	t >> Quality	of Service
---------------------	--------------	------------

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

12. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

# 5.5 Upgrade Firmware for Your Router

## **Using Firmware Upgrade Utility**

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Go to www.DrayTek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products	Support	Education	Partners	Contact U
ome > Support > 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		R&TTE C	-
Vigor2200Eplus	2.5.7	1	8/02/2009		- Ralle C	ennication
Vigor2200USB	2.3.10	1	6/03/2005			

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

		About I	DrayTek Produc	ts Support	Education	Partners	Contact Us
ome > Support > Ut	ility						
Utility						Downlo	ads
Tools Name	Release Date	Version	OS	Support I	Model	Firmware	
Router Tools	2009/06/18	4.2.0	MS-Windows	All Mod	ules	Diferen	
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP	All Mod	ules	Driver	
			MS-Vista			Utility	
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Windows XP	VigorPro 10	0 series	Utility In	troduction
Tools		(Multi- language)	MS-Vista	VigorPro 550 VigorPro 551		Datashee	t
				VigorPro 530		R&TTE C	ertification
Smart VPN Client	2009/05/25	3.6.3	MS-Windows XP	All Mod	ules		ortinoadon
		( Multi- language )	MS-Vista				
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950	series		
				VictorPro 551	In series		

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of router tool. The setup wizard will appear.



- 6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 7. From the Start menu, open Programs and choose Router Tools XXX >> Firmware Upgrade Utility.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port	Firmware file:	
69		
Password:	Abort	Send

- 8. Type in your router IP, usually **192.168.1.1**.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

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

10. Click Send.

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

11. Now the firmware update is finished.

#### **Using Web Page**

The web page also can guide you to upgrade firmware. Note that this example is running over Windows OS (Operating System).

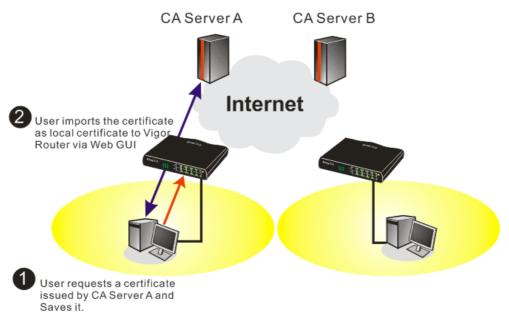
- 1. Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is <u>ftp.DrayTek.com</u>.
- 2. Click System Maintenance>> Firmware Upgrade.

System Maintenance >> Firmware Upgrade	
Web Firmware Upgrade	
Select a firmware file. Browse. Click Upgrade to upload the file. Upgrade	
TFTP Firmware Upgrade from LAN	
Current Firmware Version: 3.3.6_RC5	
Firmware Upgrade Procedures:	
<ol> <li>Click "OK" to start the TFTP server.</li> <li>Open the Firmware Upgrade Utility or other 3-party TFTP client software.</li> <li>Check that the firmware filename is correct.</li> <li>Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.</li> <li>After the upgrade is compelete, the TFTP server will automatically stop running.</li> </ol>	
Do you want to upgrade firmware ? OK	

3. Select a firmware file by clicking **Browse**.

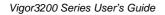
Click **Upgrade** to perform the firmware upgrade.

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



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

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



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

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

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

Name Subject	Status	Modify
Local /C=TW/O=Draytek/emailAddress	Requesting	View Delete
ENERATE IMPORT REFRESH X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARRCAQAwQTELNAkGA1UEBhMCVFcxEDAOB- BgkqhkiG9w0BCQEWEXByZXN2QGRyYX102WauY29tM A4GNADCBiQKBgQDPioahu/gFQaYBice50ERSDfWkn 3wDeQytoV1LBJz21DF0xjX61p7ev187twwTsg41g2 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIr- oCkuJwYJKo2IhvcNAQkOMRowCDAWBgWVHREEDzANg- hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem uRLq4CiEi6nV4hMRytcx2pE256MarSgREte86RoO8- I9FqkjJNihip4TCjecSNN2jmQo5WU+Bce8TG+SCBC' END CERTIFICATE REOUEST	IGfMAOGCSqGSIk IdHblo1kt9cTdI 6Qk/rGhuVTKd9j 0T2RZjkRMaHEWp gtkcmF5dGVrLmM 1tHQbcwjXvg/t Jx0I45560xCZ/M	D3DQEBAQUA ,UDaFk6s8d 16PlcrnkP7 DVpwIDAQAB NvbTANBgkq VsFlzTJiHh N1Gh9VQ9I1

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

Welcome	
	rtificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, yo elf to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more e you request.
Select a task: ⊙Retrieve the CA certificate or c	ertificate revocation list
<ul> <li>Request a certificate</li> <li>Check on a pending certificate</li> </ul>	

#### Select Advanced request.

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

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

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

Microsoft Certifica	te Services vigor	Home
Submit A Save	1 Request	
Jubilit A Save	a intequeat	
	encoded PKCS #10 certificate request or PKCS #7 renewal request generated equest field to submit the request to the certification authority (CA).	by an external application (such as a web
Saved Request:		
Certificate Request	BEGIN CERTIFICATE REQUEST MIIBajiCCARMCAQAwGTELMAKGAIUEBhMCVFcxEDAO BgkqhkiG9w0BCQEWEXByZXNzQGRYYXIQZWuY29t AdGNADCBIQKBg0DQYBTmmZfrfhN9/IeQnG03Xk++ hX4hp89cUF9d1oACCG1M/tcBockdcZdPFFvIXcP3 x/G0A7CTV0/fQzpxrcCulJTjLSjS0/Bn9v509516 ♥	
Certificate Templa	Browse for a file to insert. te:	
	Administrator	
Additional Attribut	Administrator Authenticated Session Basic EFS	
Attributes:	EFS Recovery Agent User IPSEC (Offline request) Router (Offline request)	
	Subordinate Certification Authority Web Server	Submit >

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and

#### you will find the below window showing "-----BEGINE CERTIFICATE-----"...." Certificate Management >> Local Certificate

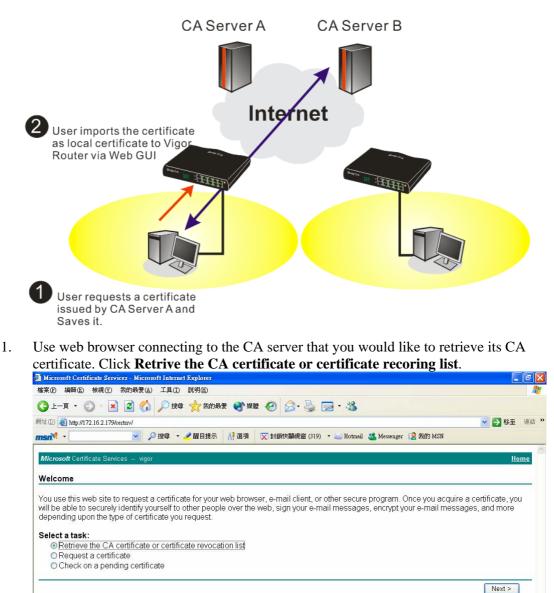
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
GENERATE IMPORT REFRESH X509 Local Certificate Request			
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=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

# 5.7 Request a CA Certificate and Set as Trusted on Windows CA Server



- 2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.
  - 🚰 Microsoft Certificate Services Microsoft Internet Explorer 檔案 (P) 編輯 (E) 檢視 (V) 我的最愛 (A) 工具 (I) 說明 (II) 🌀 上—頁 • 🐑 - 💌 😰 🏠 🔎 搜尋 🧙 我的最爱 🜒 媒體 🤗 🔗 - 🌺 🔜 • 🎎 網址 (D) 🕘 http://172.16.2.179/certsrv/certcarc.asp ✓ ● 移至 連結 msn<sup>M</sup> -🖌 🔎 搜尋 🔹 🥒 醒目提示 🛛 🕺 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔛 Hotmail 🚢 Messenger [ 2 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current (vigor(1)) Previous (vigor) Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

Name	Subject	Status	Modify
rusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
rusted CA-2			View Delete
rusted CA-3			View Delete

4. You may review the detail information of the certificate by clicking **View** button.

	-
Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

Note: Before setting certificate configuration, please go to System Maintenance >> Time and Date to reset current time of the router first.

# 5.8 Creating an Account for MyVigor

The website of MyVigor (a server located on <u>http://myvigor.draytek.com</u>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filter the web pages for protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor first.

### 5.8.1 Creating an Account via Vigor Router

1. Click **System Maintenance>>Activation** to open the following page.

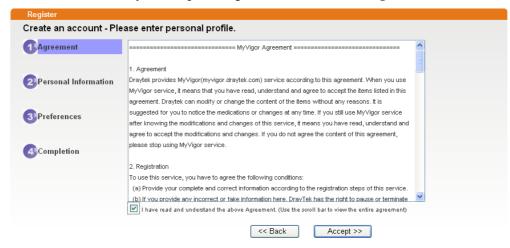
System Maintenance >> Activation	Activate via interface : auto-	: auto-selected 👻	
Web-Filter License [Status:Not Activated]		<u>Activate</u>	
Authentication Message			
Activated Wiz, Authenticate is continuously, co 00:04:55	nnect to the server, 2000-01-0	1	

2. Click the Activate link. A login page for MyVigor web site will pop up automatically.

OGIN			
UserName :			
Password :			
Auth Code :		AYi GXZ	
	If you cannot read the wo	rd, <u>click here</u>	
	Forget password	<sub>?</sub> Login	
Don't have a	MyVigor Account ?	Create an acc	ount now

3. Click the link of **Create an account now**.

4. Check to confirm that you accept the Agreement and click Accept.



5. Type your personal information in this page and then click **Continue**.

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
		(3 ~ 20 characters)
Deserved	Password:*	••••
Personal Information		(4~20 characters : Do not set the same as the username.)
momauvn	Confirm Password:*	••••
	Personal Informat	ion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND
	Career:*	Supervisor

6. Choose proper selection for your computer and click Continue.

Register		
Create an account -	Please enter personal profile.	
	How did you find out about this website?	Internet 🗸
Agreement	What kind of anti-virus do you use?	AntiVir
2 Personal	I would like to subscribe to the MyVigor e-letter.	
Information	l would like to receive DrayTek product news.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server
Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

\*\*\*\*\* This is an automated message from myvigor draytek.com.\*\*\*\*\*

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site	5
Register Confirm		
5	Thank for your register in VigorPro Web Site	
	The Register process is completed	
	Close Login	

- 10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.
  - This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

M		
Mary		
••••		
T4he1C	T4he1C	
lf you cannot read	the word, <u>click here</u>	
Forget pas	sword? Login	
MyVigor Accoun	t? <u>Create an ac</u>	count now
	ging in, contact our customer sei e : (886) 3 597 2727 or	wice.
	T4he1C If you cannot read Forget pas MyVigor Accour	T4he1C T4he1C

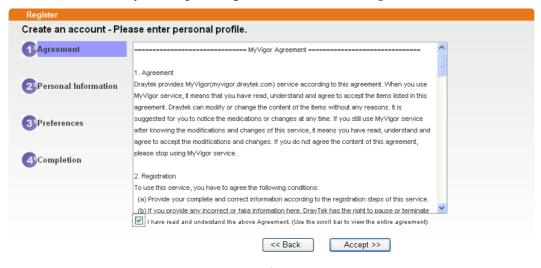
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

### 5.8.2 Creating an Account via MyVigor Web Site

1. Access into <u>http://myvigor.draytek.com</u>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.

<b>Dray</b> Tek	MyVig	or	Customer Survey
ft Home	Search	30	
	MyVigor for you	^	Login
About Us Product My Information VigorPro	MyVigor website replaces the VigorPro site as DrayTek's portal site for the latest products and services in network security, including Anti- Virus, Anti-Spam, Web Content Filter etc. The products and functions that are supported in this site include:		UserName Password AuthCode
	<ul> <li><u>VigorPro Unified Security Firewall series:</u></li> <li>Activation of Commtouch<sup>™</sup> GlobalView Web Content Filter license key</li> <li>Activation of DT Anti-Virus license key</li> </ul>		CbkqVd If you can't read the AuthCode , <u>click here</u> Login
	<ul> <li>Activation of Kaspersky Anti-Virus license key</li> <li>Activation of Commtouch<sup>TM</sup> Anti-Spam license key and membership</li> </ul>		Forget password? Not registered yet ? Click here !
	Vigor routers (for models that support Commtouch <sup>TM</sup> ) <ul> <li>Activation of Commtouch<sup>TM</sup> GlobalView Web Content Filter license key</li> </ul>		
	The MyVigor website contains a trail version of Commtouch <sup>TM</sup> Global/View Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.		
Please use IE 5.0 or above (resolution 1024 * 788) for best display. © DrayTek Corp.	More customer-oriented services are planned for MyVigor site for the near future.	~	

2. Check to confirm that you accept the Agreement and click Accept.



3. Type your personal information in this page and then click Continue.

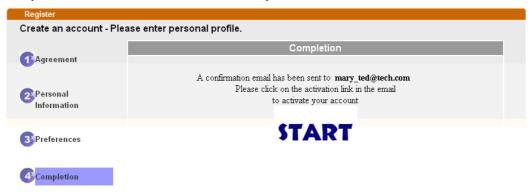
	Account Informati	ion
Agreement	UserName:*	Mary Check Account
	Password:*	(3 ~ 20 characters)
Personal	Password.	( 4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	ion
Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 _
	Country:*	SWITZERLAND
	Career:*	Supervisor

4. Choose proper selection for your computer and click **Continue**.

Register		
Create an account -	Please enter personal profile.	
	How did you find out about this website?	Internet 💌
<b>U</b> .g.comon	What kind of anti-virus do you use?	AntiVir
Personal	I would like to subscribe to the MyVigor e-letter.	
Information	I would like to receive DrayTek product news.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>



5. Now you have created an account successfully. Click START.



6. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

\*\*\*\*\* This is an automated message from myvigor draytek.com.\*\*\*\*\*

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



The Confirm message of New Owner(Mary) maybe timeout Please try again or contact to draytek.com

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN			
UserName :	Mary		
Password :	••••		
Auth Code :	T4he1C	T4he1C	
	If you cannot read the	word, <u>click here</u>	
	Forget passw	ord? Login	
Don't have a	MyVigor Account?	<u>Create an acc</u>	count now
If you a	are having difficulty logging Customer Service : (8	in, contact our customer serv	ice.

email to :webmaster@draytek.com

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

# 6 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

# 6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**1.3 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.



# 6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

#### For Windows



The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.

eth0	Properties		?
General	Authentication	Advanced	
Connec	et using:		
<b>B</b>	ASUSTeK/Broad	com 440x 10/100 l	Ir <u>C</u> onfigure
This c <u>o</u>	nnection uses th	e following items:	
	Client for Micro File and Printer QoS Packet So Internet Protoc	Sharing for Micros	oft Networks
	nstall	<u>U</u> ninstall	Properties
Tran wide	area network pr	Protocol/Internet F otocol that provide: onnected networks	
-	-	ition area when cor connection has limi	nnected ted or no connectivity
			OK Cancel

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

General	Alternate Configuration		
this cap	n get IP settings assigned bability. Otherwise, you nee ropriate IP settings.		
<u>o o</u> t	otain an IP address autom	tically	
OUs	se the following IP address		
∐P ad	ddress:		1. to 3
Sybr	net mask:		er. 80
Defa	ult gateway:	1	a. a.
0	otain DNS server address	utomatically	
OU	se the following DNS serve	r addresses: ——	
Prefe	erred DNS server:		e. e.
Alten	nate DNS server.		
			Advanced
			Cancel

## For Mac OS

- 1. Double click on the current used Mac OS on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

and the second second second second		Network	(
how All	Displays So	Network Startup Disk	
		Location: Automatic	
		Show: Built-in Ethernet	
	TCF	P/IP PPPoE AppleTalk Proxies Ethernet	
Co	nfigure IPv4:	Using DHCP	
	IP Address		
		: 255.255.255.0 DHCP Client ID:	
	Router	(If require	d)
	DNS Servers:		(Optional)
			(Optional)
Sear	ch Domains:		(optional)
		: fe80:0000:0000:0000:020a:95ff:fe8d:72e4	(optional)

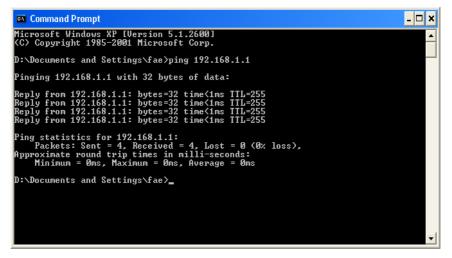
# 6.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 6.2)

Please follow the steps below to ping the router correctly.

#### **For Windows**

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

#### For Mac OS (Terminal)

- 1. Double click on the current used Mac OS 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.



e Contraction Contractica Cont	
Last login: Sat Jan 3 02:24:18 on ttyp1	N
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	
4C	
192.168.1.1 ping statistics	
5 packets transmitted, 5 packets received, 0% packet loss	
round-trip min/avg/max = 0.697/0.723/0.755 ms	
Vigor10:~ draytek\$	

# 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 each WAN interface to review the settings that you configured previously.

WAN >> Internet Access

nternet Access					
Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	None 💌 Details Page		
WAN2		Ethernet	Static or Dynamic IP 💌 Details Page		
WAN3		Ethernet	None		
WAN4		Ethernet	None   Details Page		
WAN5		USB	None		

# 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 Vigor3200. 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 Vigor3200.

#### 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.

		DrayTek Vigor	Getway IP (Static)	TX Packets	RX Rate
AN Status		Dray lek vigor		0	0
TX Packets	;	RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442		3807		0	0
eWall Log VPN Los	g User Acce	ss Log Call Log W	AN Log Network Infomation	Net State	
Time	Host	Message			^
Apr 12 09:17:49	Vigor			American Accesso	0x0 kuthe
10112-09.17.49	V 12OT	WANZ PPPOE <==	Protocol:LCP(c021) ConfReg I	dentiner/0x05 ACCM: (	
	Vigor	[3G]Modem status	al 20 00 00 00 00 02 00 03 00		
Apr 12 09:17:49		[3G]Modem status WAN2 PPPoE>	al 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor	[3G]Modem status: WAN2 PPPoE	al 20 00 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I V: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	Vigor Vigor Vigor Vigor	[3G]Modem status WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I V:1 T:1 PADS ID:0 ase: CONNECT 3600000		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	[3G]Modem status WAN2 PPPoE ==> WAN2 PPPoE <== [3G]Modem respon [3G]Modem status	a1 20 00 00 00 00 00 02 00 03 00 Protocol:LCP(021) ConfReq I V:1 T:1 PADS ID:0 as: CONNECT 3600000 al 20 00 00 00 00 02 00 02 00		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status WAN2 PPPoE	al 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I W:1 T:1 PADS ID:0 nm: CONNECT 3600000 al 20 00 00 00 00 02 00 02 00 al 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	[3G]Modem status WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I V:1 7:1 PADS ID-0 are: CONNECT 3600000 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 TDT*99#		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status: WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(0021) ConfReq I Y:1 7:1 PADS ID:0 as: CONNECT 3600000 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status: WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(0021) ConfReq I V:1 7:1 PADS ID:0 ne: CONNECT 3600000 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0 V:1 7:1 PADR ID:0		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem status WAN2 PPPoE	al 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I V:1 7:1 PADS ID-0 as: CONNECT 3600000 al 20 00 00 00 00 02 00 02 00 al 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0 V:1 7:1 PADO ID:0 as: OK	dentifier:0x00 MRU: 15	
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statu: WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(0021) ConfReq I V:1 7:1 PADS ID:0 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0 V:1 7:1 PADR ID:0 W:1 7:1 PADR ID:0 ate: OK ate: OK	dentifier:0x00 MRU: 15	
Apr 12 09:17:49           Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statu: WAN2 PPPoE	al 20 00 00 00 00 02 00 03 00 Protocol:LCP(c021) ConfReq I V:1 7:1 PADS ID-0 as: CONNECT 3600000 al 20 00 00 00 00 02 00 02 00 al 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0 V:1 7:1 PADO ID:0 as: OK	dentifier:0x00 MRU: 15	500 ACCH
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem statu: WAN2 PPPoE	a1 20 00 00 00 00 02 00 03 00 Protocol:LCP(0021) ConfReq I V:1 7:1 PADS ID:0 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 a1 20 00 00 00 00 02 00 02 00 TDT*99# V:1 7:1 PADR ID:0 V:1 7:1 PADR ID:0 W:1 7:1 PADR ID:0 ate: OK ate: OK	dentifier:0x00 MRU: 15	

#### Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor3200. 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.

Sy	stem	Maintenance	>>	Reboot	S	ystem
----	------	-------------	----	--------	---	-------

Reboot System	
	Do you want to reboot your router ?
	<ul> <li>Using current configuration</li> <li>Using factory default configuration</li> </ul>
	OK

#### Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

# 6.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.

