

Vigor3200 Series

Multi-WAN Security Router



Your reliable networking solutions partner

User's Guide

Vigor3200 Series Multi-WAN Security Router User's Guide

Version: 1.6 Firmware Version: V3.6.3 (For future update, please visit DrayTek web site) Date: 26/02/2013



Copyright Information

Copyright Declarations	Copyright 2013 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.	
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers. 	
Safety Instruction	s and Approval	
Safety Instructions	 Read the quick start guide thoroughly before you set up the router. The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router 	

- yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

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 RegisteredWeb registration is preferred. You can register your Vigor router via
http://www.DrayTek.com.

Firmware & ToolsDue 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



Warranty

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/SupportDLRTTECE.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



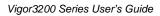
Introduction	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor3200 1.2.2 For Vigor3200n	2 4
1.3 Hardware Installation	6
1.4 Printer Installation	7



Basic Settings	13
2.1 Accessing Web Page	13
2.2 Changing Password	14
2.3 Quick Start Wizard	15
2.3.1 For WAN1 – WAN4 2.3.2 For WAN5	17 24
2.4 Service Activation Wizard	26
2.5 Wireless Wizard	29
2.6 Online Status	32
2.7 Saving Configuration	34
2.8 Support Area	34
2.9 Registering Vigor Router	35



Tutorials and Applications	39
3.1 How to establish OpenVPN - host to LAN tunnels(authenticated without CA) via SmartVPI Client?	
3.2 How to establish OpenVPN - host to LAN tunnels(authenticated with CA) via SmartVPN Client?	43
3.3 How to Implement the AD/LDAP Authentication for User Management?	62
3.4 How to implement the AD/LDAP authentication for SSL Application?	65
3.5 How to Configure Multi-Subnet	73
3.6 How to Customize Your Login Page	78
3.7 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	80
3.8 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	89
3.9 QoS Setting Example	94





3.10 Upgrade Firmware for Your Router	. 98
3.11 Request a certificate from a CA server on Windows CA Server	101
3.12 Request a CA Certificate and Set as Trusted on Windows CA Server	105
3.13 Creating an Account for MyVigor	107
3.13.1 Creating an Account via Vigor Router 3.13.2 Creating an Account via MyVigor Web Site	
3.14 How can I get the files from USB storage device connecting to Vigor router?	.114
3.15 VPN Trunk Load-Balance between Vigor 3200 and Other Vigor Router	.117



Web Configuration	129
4.1 WAN	129
4.1.1 Basics of Internet Protocol (IP) Network	129
4.1.2 General Setup	
4.1.3 Internet Access	
4.1.4 Load-Balance Policy	150
4.2 LAN	152
4.2.1 Basics of LAN	153
4.2.2 General Setup	
4.2.3 Static Route	
4.2.4 VLAN	
4.2.5 Bind IP to MAC	
4.2.6 LAN Port Mirror	
4.2.7 Web Portal Setup	
4.3 NAT	174
4.3.1 Port Redirection	175
4.3.2 DMZ Host	178
4.3.3 Open Ports	181
4.3.4 Address Mapping	
4.3.5 Port Triggering	185
4.4 Firewall	188
4.4.1 Basics for Firewall	188
4.4.2 General Setup	190
4.4.3 Filter Setup	194
4.4.4 DoS Defense	202
4.5 User Management	205
4.5.1 General Setup	
4.5.2 User Profile (Reserved)	207
4.5.3 User Group	
4.5.4 User Online Status	212
4.6 Objects Settings	213
4.6.1 IP Object	213
4.6.2 IP Group	
4.6.3 IPv6 Object	
4.6.4 IPv6 Group	
4.6.5 Service Type Object	
4.6.6 Service Type Group	
4.6.7 Keyword Object	226



4.6.8 Keyword Group	
4.6.9 File Extension Object	
4.6.10 SMS/Mail Service Object	
4.6.11 Notification Object	
4.7 CSM Profile	239
4.7.1 APP Enforcement Profile	240
4.7.2 URL Content Filter Profile	
4.7.3 Web Content Filter Profile	
1.9 Dendwidth Management	252
4.8 Bandwidth Management	
4.8.1 Sessions Limit	
4.8.2 Bandwidth Limit	
4.8.3 Quality of Service	257
4.9 Applications	266
4.9.1 Dynamic DNS	266
4.9.2 Schedule	
4.9.3 RADIUS	272
4.9.4 LDAP / Active Directory	
4.9.5 UPnP	
4.9.6 IGMP	
4.9.7 Wake on LAN 4.9.8 SMS/Mail Alert Service	
4.10 VPN and Remote Access	281
4.10.1 VPN Client Wizard	281
4.10.2 VPN Server Wizard	
4.10.3 Remote Access Control	
4.10.4 PPP General Setup	
4.10.5 IPSec General Setup	
4.10.6 IPSec Peer Identity	
4.10.7 OpenVPN General Setup 4.10.8 Remote Dial-in User	
4.10.9 LAN to LAN	
4.10.10 VPN TRUNK Management	
4.10.11 Connection Management	
4.11 Certificate Management	324
-	
4.11.1 Local Certificate	
4.11.2 Trusted CA Certificate 4.11.3 Certificate Backup	
4.12 Wireless LAN	329
4.12.1 Basic Concepts	329
4.12.2 General Setup	
4.12.3 Security	
4.12.4 Access Control	
4.12.5 WPS	
4.12.6 WDS 4.12.7 Advanced Setting	
4.12.7 Advanced Setting	
4.12.9 AP Discovery	
4.12.10 Station List	
4.13 SSL VPN	
4.13.1 General Setup	
4.13.2 SSL Web Proxy	
4.13.3 SSL Application 4.13.4 User Account	
4. 13.4 USEI ACCUUII	554



4.13.5 User Group 4.13.6 Online User Status	
4.14 USB Application	361
4.14.1 USB General Settings	361
4.14.2 USB User Management	362
4.14.3 File Explorer	365
4.14.4 USB Disk Status	365
4.14.5 Syslog Explorer	366
4.15 System Maintenance	368
4.15.1 System Status	368
4.15.2 TR-069	
4.15.3 Administrator Password	
4.15.4 User Password	
4.15.5 Login Page Greeting	
4.15.6 Configuration Backup	
4.15.7 Syslog/Mail Alert	
4.15.8 Time and Date	
4.15.9 SNMP	381
4.15.10 Management	383
4.15.11 Reboot System	
4.15.12 Firmware Upgrade	
4.15.13 Activation	387
4.16 Diagnostics	388
4.16.1 Dial-out Triggering	389
4.16.2 Routing Table	
4.16.3 ARP Cache Table	
4.16.4 IPv6 Neighbour Table	391
4.16.5 DHCP Table	392
4.16.6 NAT Sessions Table	393
4.16.7 Data Flow Monitor	394
4.16.8 Traffic Graph	396
4.16.9 Ping Diagnosis	
4.16.10 Trace Route	
4.16.11 TSPC Status	399
4.17 External Devices	400



Trouble Shooting	401
5.1 Checking If the Hardware Status Is OK or Not	401
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	402
5.3 Pinging the Router from Your Computer	404
5.4 Checking If the ISP Settings are OK or Not	405
5.5 Problems for 3G Network Connection	406
5.6 Backing to Factory Default Setting If Necessary	407
5.7 Contacting Your Dealer	408



Vigor3200 Series, a broadband router, 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 easily. 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, USB storage device for sharing files, or for 3G WAN.

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:

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

detailed explanation.

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	SB Connecter for 3G Modem or printer.		
PWRConnecter for a power adapter.			
ON/OFF	Power Switch.		

1.2.2 For Vigor3200n

DrayTek Vigor3200n Wireless LAN Multi-WAN Security Router				
USB W/	PN CSM ANI WAN3 AN2 WAN4			
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.	
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 Firewall >> General Setup . (Such profile must be established under CSM 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.	



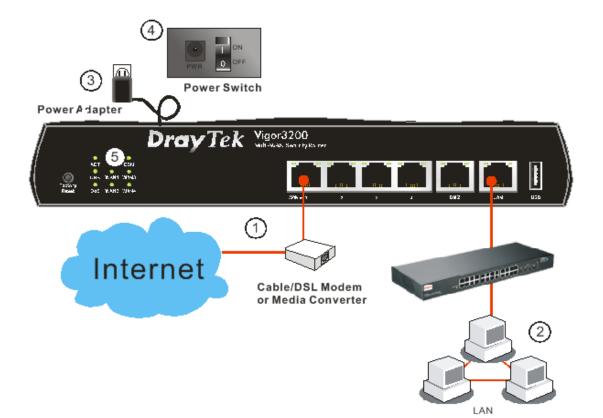
Interface	Description
Wireless LAN	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device
ON/OFF/WPS	making network connection through WPS.
	Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default 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.

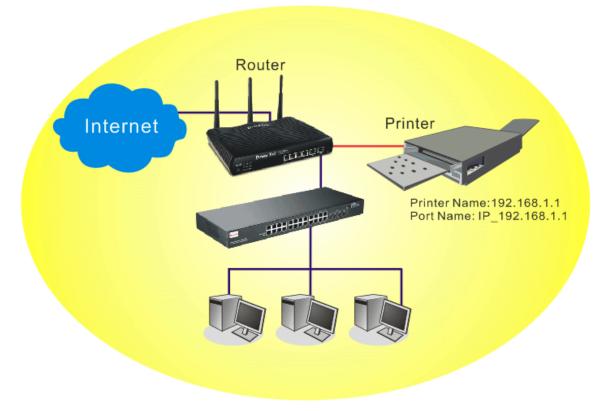
(For the detailed information of LED status, please refer to section 1.1.)





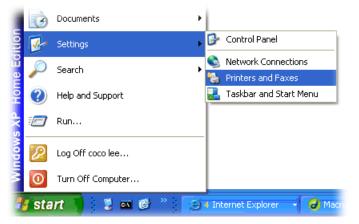
1.4 Printer Installation

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**.

Use the following port LPT1: [Recommended Printer Port]	Select the port you want yo new port.	our printer to use. If the port is not listed, you	can create a
	Use the following port:	LPT1: (Recommended Printer Port)	*

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	t to add a port?
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Port Name:	IP_192.168.1.1
	<pre>< Back Next > Cancel</pre>

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 property 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 O Standard Genetic Network Card O Eustom Sgttings
	(<u>B</u> ack <u>N</u> ext) Cancel

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**.

Id Printer Wizard Install Printer Software The manufacturer and mo	del determine which printer software to use.	L
	r and model of your printer. If your printer came with I your printer is not listed, consult your printer docum vare,	
Manufacturer AST AT&T	Printers Printers Brother HL-1060 BR-Script2	[
Brother Built Canon	Brother HL-1070 BR-Script2 Brother HL-1070 Brother HL-1070 Brother HL-1070 Brother HL-1070 Brother HL-1070 Brother HL-1070 Brother HL-1070	6
This driver is digitally signed <u>Tell me why driver signing is</u>		<u>H</u> ave Disk

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.

ieneral Sha	ring Ports Advancer	d Device Settings	
Br	other HL-1070		
			_
Print to the for checked por		nts will print to the first free	
Port	Description	Printer	-
3.250	Standard TCP/IP Port	Epson Stylus COLOR 1160	
□ IP_1	Standard TCP/IP Port		
□ IP_1	Standard TCP/IP Port	HP LaserJet 1300	
□ IP_1	Standard TCP/IP Port		
	Standard TCP/IP Port		
	Standard TCP/IP Port		
PDF	Local Port	PDF995	N
Add P	or <u>t</u> <u>D</u> elete	e Port <u>C</u> onfigure Port.	
			_
	directional support		
Enable pri	nter 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.

Dray Tek	MyVigor Register E-newsletter DrayTek.HQ Media Center Global (English) 🔽 Log
About DrayTek Prod	ducts Supports Solutions Multi-Media Demo Contact Us Q Search	
FAQ / Application	You are here: Home + Supports + FAQ / Application Notes + Printer Server	
Latest FAO/Application		3
USB		
Printer Server		
3G/4G Internet Connection	What types of printers are compatible with Viscor routs	ang link
Connection hen, click the V	Vhat types of printers are compatible with Vigor route You are here: Home + Supports + FAQ / Application Notes + Printer Server	e r ? link. ₪
Connection hen, click the V AQ / Application Latest FAQ/Application	You are here: Home + Supports + FAQ / Application Notes + Printer Server	er? link. ₪
Connection hen, click the W AQ / Application Latest FAQ/Application Basic		er? link. S
Connection hen, click the V AQ / Application Latest FAQ/Application Basic Firmware Upgrade	You are here: Home + Supports + FAQ / Application Notes + Printer Server	er? link. ₪ 2012/01/12
Connection hen, click the W AQ / Application Latest FAQ/Application Basic	You are here: Home + Supports + FAQ / Application Notes + Printer Server Printer Server	8
Connection hen, click the W AQ / Application Latest FAQ/Application Basic Firmware Upgrade //AN	You are here: Home > Supports > FAQ / Application Notes > Printer Server Printer Server What types of printers are compatible with Vigor router?	2012/01/12

This page is left blank.

Vigor3200 Series User's Guide



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

This chapter explains how to setup a password for accessing into the web user interface of Vigor router and how to adjust settings for accessing Internet successfully.

2.1 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.

opyright©, DrayTek Corp	All Rights Reserved.	Dray Tek
		Login
Group	💌	
Password	••••	
Username	admin	

3. Please type "admin/admin" on Username/Password and click **Login**. For the option of Group, it is used to access into SSL VPN portal. Just keep it in default. For the detailed information about the Group application of SSL VPN portal, refer to Chapter 3.



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		Tre
Off		
1 min		
3 min		
5 min		
10 min		
Applications		

2.2 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 s Multi-WAN Security		Dray Tek
Quick Start Wizard Service Activation Wizard Wireless Wizard	System Status Model Name : Vigor3200n Firmware Version : 3.6.3 Build Date/Time : Jan 15 2013 15:04:20	
Online Status		
	LAN	
WAN	MAC Address IP Address Subnet Mask DHCP Server DM LAN1 00-50-7F-CE-46-FC 192,168,1,1 255,255,255,0 Yes 16	VS i8.95.1.1
LAN		8.95.1.1 8.95.1.1
NAT		8.95.1.1
Firewall		8.95.1.1
User Management		8.95.1.1
Objects Setting	IP Routed Subnet 00-50-7F-CE-46-FC 192.168.0.1 255.255.255.0 Yes 16	68.95.1.1
CSM		
Bandwidth Management	Wireless LAN	
Applications	MAC Address Frequency Domain Firmware Version SSID	
VPN and Remote Access	00-50-7F-CE-46-FC Europe 2.3.2.0 DrayT	ek
Certificate Management		
Wireless LAN	WAN	
SSL VPN	Link Status MAC Address Connection IP Address Default Ga	teway
USB Application	WAN1 Disconnected 00-50-7F-CE-46-FD WAN2 Connected 00-50-7F-CE-46-FE Static IP 172.16.3.130 172.16.1.1	
System Maintenance	WAN2 Connected 00-50-7F-CE-46-FE Static IP 172.16.3.130 172.16.1.1 WAN3 Disconnected 00-50-7F-CE-46-FE	·
Diagnostics	WANS Disconnected 00-50-7F-CE-46-00	
External Devices	WAN5 Disconnected 00-50-7F-CE-46-01	
Comment Area		
Support Area Application Note	IPv6	
FAQ	Address Scope Internet Access Mode	
Product Registration	LAN FE80::250:7FFF:FECE:46FC/64 Link	
Status: Ready		~

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**.

System Maintenance >> Administrator Password Setu	p
Administrator Password	
Old Password	
New Password	
Confirm Password	
Note:Password can contain only a-z A-Z 0-9 , ; :	$" < > * + = \ ? @ # ^ ! ()$
	OK

Enter the login password on the field of **Old Password**. Type **New Password** and confirm the password. Then click **OK** to continue.

5. Now, the password has been changed. Next time, use the new password to access the Web user interface for this router.





2.3 Quick Start Wizard



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

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

Quick Start Wizard

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

On the next page as shown below, please select the WAN interface that you use. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.

Quick Start Wizard

Interface	
WAN Interface:	WAN5 💌
Display Name:	WAN1 WAN2
Physical Mode:	WANZ WAN3
Physical Type:	WAN4 liation V
	WAN3
	< Back Next > Finish Can

Note: There are five WAN selections available for you to choose. In which, WAN5 is selected for 3G USB modem connection. Refer to the following for detailed information.



2.3.1 For WAN1 - WAN4

Choose WAN1/WAN2/WAN3/WAN4 and click **Next**. 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.

2.3.1.1 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.

1. Choose WAN1/WAN2/WAN3/WAN4 as the WAN Interface and click the Next button. The following page will be open for you to specify Internet Access Type.

Quick Start Wizard

Connect to Internet	
WAN 1	
Select one of the following Internet Access	types provided by your ISP.
PPPoE	
О РРТР	
O L2TP	
Static IP	
O DHCP	
·	
	< Back Next > Finish Cancel

2. Click **PPPoE** as the Internet Access Type. Then click **Next** to open the following page.

Quick Start Wizard

PPP ₀ E	Client	Mode	
TITUL	Circin	moue	

Quick Start Wizard

		Password
		Passworu Confirm Password
	••••••	Commin Password

Available settings are explained as follows:

Item	Description	
User Name	Assign a specific valid user name provided by the ISP.	
Password	Assign a valid password provided by the ISP.	
Confirm Password	Retype the password.	
Back	Click it to return to previous setting page.	
Next	Click it to get into the next setting page.	
Cancel	Click it to give up the quick start wizard.	

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

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
settings and restart the V	gor router.

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

Quick Start Wizard Setup OK !!!

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

2.3.1.2 PPTP/L2TP

1. Choose **WAN1/WAN2/WAN3/WAN4** as the WAN Interface and click the **Next** button. The following page will be open for you to specify Internet Access Type.

nnect to Internet				
WAN 1				
Select one of th	e following Internet Acco	ess types provid	ded by your ISP.	
	O PPPoE			
	• РРТР			
	O L2TP			
	Static IP			
	O DHCP			

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

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

Available settings are explained as follows:



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

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

Quick Start Wizard

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

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

Quick Start Wizard Setup OK !!!

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

2.3.1.3 Static IP

1. Choose WAN1/WAN2/WAN3/WAN4 as the WAN Interface and click the Next button. The following page will be open for you to specify Internet Access Type.

ect to Internet				
WAN 1				
Select one of the f	ollowing Internet Acc	cess types prov	ided by your ISP.	
	O PPPoE			
	○ РРТР			
	O L2TP			
	Static IP			
	O DHCP			

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

Quick Start Wizard

WAN 1		
Enter the Static IP config	juration probided by your ISP.	
WAN IP	172.16.3.229	
Subnet Mask	255.255.255.0	
Gateway	172.16.3.1	
Primary DNS	168.95.1.1	
Secondary DNS		(optional)

Available settings are explained as follows:

Item	Description
WAN IP	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the IP address of gateway.
Primary DNS	Type in the primary IP address for the router.
Secondary DNS	Type in secondary IP address for necessity in the future.

Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

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

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

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

Quick Start Wizard Setup OK !!!

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

2.3.1.4 DHCP

Quick Start Wizard

1. Choose WAN1/WAN2/WAN3/WAN4 as the WAN Interface and click the Next button. The following page will be open for you to specify Internet Access Type.

ect to Internet		
WAN 1	leving Internet Access to reactive details and to be	
Select one of the i	lowing Internet Access types provided by your ISP.	
	O PPPoE	
	О РРТР	
	O L2TP	
	Static IP	
	O DHCP	

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

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

Available settings are explained as follows:

Item	Description
Host Name	Type the name of the host.
MAC	Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to enter the MAC address.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.

Cancel	Click it to give up the quick start wizard.
--------	---

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

Quick Start Wizard

ease confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
settings and restart the V	igur router.

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

Quick Start Wizard Setup OK !!!

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

Quick Start Wizard

2.3.2 For WAN5

To use 3G USB modem for network connection, please choose WAN5.

1. Choose **WAN5** as the WAN Interface and click the **Next** button.

 WAN Interface:
 WANS ▼

 Display Name:
 Display Name:

 Physical Mode:
 USB

 Physical Type:
 Auto negotiation ▼

2. Then, click **Next** to continue.

ase confirm your settings:	
WAN Interface:	WAN5
Physical Mode:	USB
Physical Type:	Auto negotiation
Internet Access:	РРР
Click Back to modify char settings and restart the V	nges if necessary. Otherwise, click Finish to save the current /igor router.

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

Quick Start Wizard Setup OK !!!

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

2.4 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 user interface.

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

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

1. Open Service Activation Wizard.



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

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

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

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



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

his product provides 30 days of free trial, p	lease choose the item(s) you want to use.
VCF service:	
Web Content Filter (Commtouch)	License Agreement
	on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can SlobalView WCF package from retailing outlets.
	Activation Date : 2010-11-17
I have read and accept the above Agr	eement. (Please check this box).

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

Please	e confirm your settings			
	Sevice Type : Sevice Activated :	Trial version Web Content Filter (Commtouch)		
	Please click <mark>Back</mark> to re-se	lect 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		
	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 licer normal operation for you		signature again is r			

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 a	activate
This wizard is used for activating - Web Content Filter	
Please choose the edition you ne	ed.
O F	ree trial edition
	formal edition with license key
\subset	
rvice Activation Wizard	Next > Finish Cancel
lect the service type that you want to activate	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Please choose the item you want to use.	
WCF service:	
	. <mark>icense Agreement</mark> ommtouch operated in the worldwide. There is a 30-day trial period. After trial, you can
purchase DrayTek's prepared Commtouch Global	Iview WCF package from retailing outlets.
Enter your License key:	Activation Date : 2010-12-19 select
I have read and accept the above Agreeme	ent. (Please check this hox).
Note: The activation date is brought out by th	ne server automatically and cannot be changed.
	Seck Next > Finish Cancel

2.5 Wireless Wizard

The wireless wizard allows you to configure settings specified for a host AP (for home use or internal use for a company) and specified for a guest AP (for any wireless clients accessing into Internet).

Follow the steps listed below:

1. Open Wireless Wizard.



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

P Configuration	
Name:	DrayTek
Mode:	Mixed(11b+11g+11n) V
Channel:	Channel 6, 2437MHz 🗸
Password:	
Note:The host A	P configured here will be used for home or internal company use.

Available settings are explained as follows:

Item	Description
Name	Type the SSID name of this router. (SSID1) The default name is defined with DratTek.
Mode	At present, the router can connect to 11n Only, 11g Only, Mixed (11b+11g), Mixed (11a+11n), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.
Password	The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
	Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

3. After typing the required information, click **Next**. The settings in the page limit the wireless station (guest) accessing into Internet but not being allowed to share the LAN network and VPN connection.

💿 Enable 🛛 🔿 🛛	visable
Name:	carrie
Password:	carrie 12345
Rate Control:	✓ Enable Upload 25000 kbps Download 25000 kbps
	ured guest AP will not be able to access the LAN network,VPN communicate with wireless devices connecting to the router's other

Available settings are explained as follows:

Wireless Wizard

Item	Description
Enable/Disable	Click it to enable or disable settings in this page.
Name	Type the SSID name of this router. (SSID2)
Password	 The wireless mode offered by this wizard is WPA2/PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as



	"0x321253abcde").
Rate Control	It controls the data transmission rate through wireless connection.
	Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.
	Download – Type the transmitting rate for data download. Default value is 30,000 kbps.
Next	Click it to get into the next setting page.
Cancel	Exit the wireless wizard without saving any changes.

- 4. After typing the required information, click Next.
- 5. The following page will display the configuration summary for wireless setting.

Basic Wireless Settings			
Mode:11n Only (2.4 GHz)			
Channel:Channel 6, 2437MHz			
Host AP Configurations			
Name:DrayTek			
Password:12345678			
Guest AP Configurations			
Status:Enabled			
Name:carrie			
Password:carrie12345			
Rate Control:Enabled			

6. Click **Finish t**o complete the wireless settings configuration.

Wireless Wizard

Wireless Wizard

Wireless Wizard Setup OK!

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.

For IPv4 Protocol

Online Status

Physical Connection	n			System Up	time: 4days 23:29:1
	IPv4		IPv6		
LAN Status	Prima	ry DNS: 168.95	DNS: 168.95.1.1		NS: 8.8.4.4
IP Address	TX Packets	RX Pac	kets		
192.168.1.5	2208065	980968			
WAN 1 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 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	94:17:37	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172.16.3.103	172.16.3.1	923456	7576	1431311	798
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

For IPv6 Protocol

Online Status

Physical Connect	ion			System Uptime: 4days 23:32:21
	IPv4		IPv6	
LAN Status				
IP Address				
FE80::250:7FF	F:FE00:0/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes	
1865	1699	145470	239741	
WAN IPv6 Status				
Enable	Mode	Up Time		
No	Offline			
IP			Gat	teway IP



Detailed explanation is shown below:

Item	Description	
LAN Status	Primary DNS	
	- Displays the IP address of the primary DNS.	
	Secondary DNS	
	- Displays the IP address of the secondary DNS.	
	IP Address	
	- Displays the IP address of the LAN interface.	
	TX Packets	
	- Displays the total transmitted packets at the LAN interface.	
	RX Packets	
	- Displays the total number of received packets at the LAN interface.	
WAN 1 Status ~ WAN 5	Line	
Status	- Displays the physical connection of this interface.	
	Name	
	- Displays the name set in WAN1/WAN web page.	
	Mode	
	- Displays the type of WAN connection (e.g., PPPoE).	
	Up Time	
	- Displays the total uptime of the interface.	
	IP	
	- Displays the IP address of the WAN interface.	
	GW IP	
	- Displays the IP address of the default gateway.	
	TX Packets	
	- Displays the total transmitted packets at the WAN interface.	
	TX Rate	
	- Displays the speed of transmitted octets at the WAN interface.	
	RX Packets	
	- Displays the total number of received packets at the WAN interface.	
	RX Rate	
	- Displays the speed of received octets at the WAN interface.	

Detailed explanation (for IPv6) is shown below:

Item	Description
LAN Status	IP Address - Displays the IPv6 address of the LAN interface
	TX Packets -Displays the total transmitted packets at the LAN interface.
	RX Packets -Displays the total received packets at the LAN

Item	Description
	interface.
	TX Bytes - Displays the total transmitted octets at the LAN interface.
	RX Bytes - Displays the total received octets at the LAN interface.
WAN IPv6 Status	Enable – No in red means such interface is available but not enabled. Yes in green means such interface is enabled. No in red means such interface is not available.
	Mode - Displays the type of WAN connection (e.g., TSPC).
	Up Time - Displays the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	Gateway IP - Displays the IP address of the default gateway.

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

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 / FAQ, the following web page will be displayed.

Dray Tek	MyVigor Register E-newsletter DrayTek.HQ Media Center Global (English)	V Log in
About DrayTek Products	s Supports Solutions Multi-Media Demo Contact Us	ch
FAQ / Application Basic Firmware Upgrade	You are here: Home > Supports > FAQ / Application Notes Latest FAQ / Application Notes	8
WAN	1. Host to LAN VPN : IPsec	2013/01/11
IPv6	2. Host to LAN VPN : L2TP over IPSec	2013/01/11
Triple-Play Dual WAN	3. How to Create a Host to LAN PPTP/L2TP VPN?	2013/01/09
		2010/01/00
LAN	4. Wake on LAN Application : Wake your LAN Computer Remotely via tool	2013/01/09

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

		on entitles you to up	grade firmware for your upcoming products and
LOGIN			
UserName :	james_fae		
Password :	•••••		
Auth Code :	txxhdd	t xxhd d	
lf y	ou cannot read the word	, <u>click here</u>	
	Forgotten password?	Login	
Don't have a	MyVigor Account ?	<u>Create an account n</u>	<u>ow</u>
Become the MyVigo	r member, you can red	ceive the e-newslei	ter update.

2.9 Registering Vigor Router

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

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

Password	••••	1
Group	💌	
		_
	Login	

2. Click **Support Area>>Production Registration** from the home page.



3. A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.

	Please take a moment to register. Membership Registration entitles you to upgrade firmware for yo purchased product and receive news about upcoming products a services!	
LOGIN		
UserName :	james_fae	
Password :	******	
Auth Code :	txxhdd t txxhdd	
lf y	you cannot read the word, <u>click here</u>	
	Forgotten password? Login	
Don't have a	a MyVigor Account ? Create an account now	
Become the MyVigo	or member, you can receive the e-newsletter update.	

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

Dray Tek				M		
🚹 Home				Search		
D About Us	My Information Welcome,james					
Product	Last Login Time :					
My Information		Last Login From : 123.110.144.220 Current Login Time : 2011-08-24 23:01:15				
🦕 VigorACS SI	Current Login Fro	m : 114.37.142.1 RowNo : 5 💌		Add		
🗘 Vigor Series	Your Device List	RUWINU . S	rayeno. ·			
🌣 Management						
S Product	Serial Number / Host ID	Device Name	Model	Note		
Registration	<u>104001703857</u>	Vigor2710	Vigor2710	-		
🍐 Customer Survey	<u>200807100001</u>	VigorPro5300	VigorPro5300	-		
	200911030001	ryan	VigorPro5300	_		

Note: Below the field of Your Device List, all the Vigor routers that you have registered to MyVigor website will be displayed in sequence.



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

Dray Tek				My V	/igor
Home .				Search	GO
D About Us	My Product		Search for t	his site	60
My Information VigorACS SI Vigor Series	Serial number : Nickname : *	20110822143203 vigor3200	101		
Management	Registration Date :	08-24-2011]		
 Product Registration Customer Survey 	Usage : Product Rating : No. of Employees : Supplier : Date of Purchase : Internet Connection : *			2	
	Cable	🗆 ADSL	🗆 VDSL	🗌 Fiber	
Convictite @BravTek Com				Cancel	mit

6. When the following page appears, your router information has been added to the database. Click **OK** to leave this web page and return to **My Information** web page.

Your device has been successfully added to the database.

- OK
- 6. Take a look at the page of **My Information**, the new added Vigor router is listed under **Your Device List**.

Dray Tek			٨	AyVigo
i Home			Sea	arch G
About Us Product My Information VigorACS SI Vigor Series	Last Login From : 123.110.14 Current Login Time : 2011-08	Welcome,drayteklae Last Login Time : 2011-08-24 09:39:13 Last Login From : 123.110.144.220 Current Login Time : 2011-08-24 23:01:15 Current Login From : 114.37.142.184		
Management	Serial Number / Host ID	Device Name	Model	Note
Customer Survey	20100707144801	Vigor3300V	Vigor3300	
	20100708105301	Vigor2820	Vigor2820	
	20101005104801	Vigor2710vn	Vigor2710	
	2010121707335201	Vigor2380	Vigor2830	
	<u>2011082214320301</u>	Vigor 3200	Vigor3200	•

This page is left blank.

Vigor3200 Series User's Guide

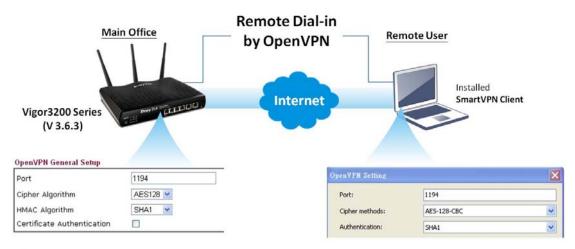


3.1 How to establish OpenVPN - host to LAN tunnels(authenticated without CA) via SmartVPN Client?

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. OpenVPN uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows remote users to authenticate for each other using a pre-shared secret key, certificate, or username/password. When OpenVPN is used in a multi-client server configuration, it allows the server to release an authentication certificate for every client via signature and Certificate authority.

Below shows an illustration for successful OpenVPN tunnel established between Vigor router (Main Office) and notebook (Remote User). The OpenVPN settings for both ends shall be the same. Otherwise, the VPN connection is unable to establish successfully.



Note:

The OpenVPN choice supported by Vigor3200 Series can work with Windows, Linux and Mac OS. For the Windows-based PC, users can use SmartVPN client to simplify settings in the client devices.

Note: Before configuring settings for OpenVPN, you should install **SmartVPN Client 4.1.0.1** on your PC and latest firmware version on your Vigor router.

Settings for Router (Main Office)

- 1. Access into the web user interface of Vigor router.
- 2. Open VPN and Remote Access >> OpenVPN General Setup to configure the OpenVPN setting with disabled Certificate Authentication. Click OK to save the settings.

/PN and Remote Access >> OpenVPN General Setup					
OpenVPN General Setup					
Port	1194				
Cipher Algorithm	AES128 💌				
HMAC Algorithm	SHA1 🔽				
Certificate Authentication					
	support UDP protocol and TUN device interface currently. So please setup tions on the client side.				

3. Open VPN and Remote Access >> Remote Dial-in User to create a profiles for Dial-in User. Set the Username (e.g., jos) and Password (e.g., jos) for OpenVPN. Click OK to save the settings.

OK

VPN and Remote Access >> Remote Dial-in User

Index No. 1	
User account and Authentication	Username
🗹 Enable this account	
Idle Timeout 300 secon	nd(s) Password(Max 19 char)
	Enable Mobile One-Time Passwords(mOTP)
Allowed Dial-In Type	PIN Code
🗖 РРТР	Secret
🔲 🗖 IPsec Tunnel	
L2TP with IPsec Policy None	KE Authentication Method
SSL Tunnel	🗹 Pre-Shared Key
🗹 OpenVPN Tunnel	IKE Pre-Shared Key
Specify Remote Node	Digital Signature(X.509)
Remote Client IP	None 💌
	IPsec Security Method
or Peer ID	Medium(AH)

Settings for PC (Remote User)

1. Execute **SmartVPN Client.** Click **Insert** to create a new dial-in VPN profile (e.g., Profile 6).

Dray Te	2k Smart VPN Client
Shee O. Enable/Alley	v IPSec NAT-Traversal and L2TP
This step will add the AssumeUDPEncapsul computer. For more i	Prohibit/Dserversion of the and the lationContextOnSendRule registry value to infomation, please read the article Q240262 Microsoft Knowledgement Base.
Step 1. Dial to ISP	
	gotten a public IP, you can skip this step.
	gotten a public IP, you can skip this step.
If you have already	gotten a public IP, you can skip this step.

Type a name (e.g., Profile 6) as the Profile Name and an IP address (e.g., 200.200.200.200) as VPN Server IP. Set jos/jos as the User Name/Password. Click OpenVPN as the type of VPN and click OK to display the OpenVPN Setting dialog.

Dial To VPN Profile Name : Profile 6			
Auto re-dial after disconnect. Redial attempts :	3		
Redial interval :	30 seconds		Contra
Auto run when system start up.			×
VPN Server IP/HOST Name(such as	123.45.67.8 Port:	1194	
200.200.200.200	Cipher methods:	AES-128-CBC	*
User Name : jos	Authentication:	SHA1	~
Password : ***	Certificate Authenticati	ion	
Enable mobile One Time Passv	rord (mOTP) CA cert:	Browse.	
Configure Sec	ret for mOTP Client cert:	Browse.	
Type of VPN	Client key:	Browse.	
	CL2TP Fallback to SSL Tunnel		
	OpenVPN Port:	443	
PPTP Encryption	OK	Cancel	
No encryption			
Require encryption			
Maximum strength encrypti	xn		
Authentication method	PAD 🖌		
Use default gateway on rem	ote network More		
OK	Cancel		

3. Configure the Port number, Cipher methods and Authentication as the settings defined above. Then click **OK**.



Checking the VPN Connection Status

Now both ends (router and remote PC) are configured well.

- 1. Access into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>Connection Management** to check the VPN connection status. From the following figure, we can know that the remote user can access the Vigor router's LAN successfully by using the username/password (jos/jos).

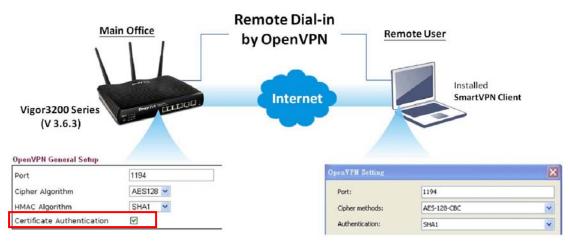
VPN and Remote Access >> Connection Management

Dial-out Tool	Refresh Seconds : 10 💌 Refresh
General Mode:	Dial
Backup Mode:	Dial
Load Balance Mode:	✓ Dial

1 OpenVPN 188.188.188 192.168.1.11/32 14 52 20 52 D:0:31 al User Database AES-SHA1 Auth via WAN1 192.168.1.11/32 14 52 20 52 D:0:31 as CAWINDOWSkystem32/cmd.exe - ping 192.168.1.1 -t - - × ringing 192.168.1.1 with 32 bytes of data: - × deply from 192.168.1.1: bytes=32 time<1ms TL=255 Steply from 192.168.1.1: bytes=32 time<1ms TL=255 keply from 192.168.1.1: bytes=32 time<1ms TL=255 Steply from 192.168.1.1: bytes=32 time<1ms TL=255 keply from 192.168.1.1: bytes=32 time<1ms TL=255 Steply from 192.168.1.1: bytes=32 time<1ms TL=255 keply from 192.168.1.1: bytes=32 time<1ms TL=255 Steply from 192.168.1.1: bytes=32 time<1ms TL=255	VPN	Туре	Remote IP	Virtual Network	Tx Pkts I	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	1 (jos) al User Databa:	OpenVPN se AES-SHA1 Auth	188.188.188.188 via WAN1	192.168.1.11/32	14	52	20	52	0:0:31	D
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	ex C:\WINDOW:	S\system32\cmd_exe	- ping 192.168.1.1	-t					. 🗆 🗙	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	Pinging 192.1	68 1 1 with 32	butes of dat							
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	2	CONTER ATOM SE	byces of uac	.a.=						
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255 Reply from 192.168.1.1: bytes=32 time<1ms TTL=255										
leply from 192.168.1.1: bytes=32 time<1ms TTL=255	Reply from 19	2.168.1.1: byt	es=32 time<1m	ns TTL=255						
지수는 것이 수 있는 것이 가지 않는 것이 같아요. 이 가지 않는 것이 없는 것이 같이 있는 것이 같이 있는 것이 같이 있는 것이 같이 있는 것이 것이 않는 것이 같이 같이 않는 것이 같이 같이 같이 않는 것이 같이 같이 않는 것이 같이 없는 것이 같이 없는 것이 같이 없다. 않는 것이 같이 없는 것이 않이 않는 것이 없는 것이 않이 않이 않는 것이 않는 것이 없는 것이 없는 것이 없는 것이 없는 것이 없는 것이 않이	Reply from 19 Reply from 19	92.168.1.1: byt 92.168.1.1: byt	es=32 time<1m es=32 time<1m	ns TTL=255 ns TTL=255						
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	Reply from 19 Reply from 19 Reply from 19	92.168.1.1: byt 92.168.1.1: byt 92.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m	ns TTL=255 ns TTL=255 ns TTL=255						
	Reply from 19 Reply from 19 Reply from 19 Reply from 19	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m	ns TTL=255 ns TTL=255 ns TTL=255 ns TTL=255 ns TTL=255						
	Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from <u>19</u>	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m	as TTL=255 as TTL=255 as TTL=255 as TTL=255 as TTL=255 as TTL=255						
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255	Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m	AS TTL=255 AS TTL=255 AS TTL=255 AS TTL=255 AS TTL=255 AS TTL=255 AS TTL=255 AS TTL=255						

3.2 How to establish OpenVPN - host to LAN tunnels(authenticated with CA) via SmartVPN Client?

Below shows an illustration for successful OpenVPN tunnel established between Vigor router (Main Office) and notebook (Remote User) via certificate authentication. The OpenVPN settings for both ends shall be the same. Otherwise, the VPN connection is unable to establish successfully.



Note:

The OpenVPN choice supported by Vigor3200 Series can work with Windows, Linux and Mac OS. For the Windows-based PC, users can use SmartVPN client to simplify settings in the client devices.

Note: Before configuring settings for OpenVPN, you should install **SmartVPN Client 4.1.0.1** on your PC and install the latest firmware version with XCA on your Vigor router (served as a CA server).

XCA is a freeware for the CA Server. This section guides you to create CA (Certificate Authentication) for Vigor users.

All the jobs you have to configure include:

- Configuring the Time and Date.
- Generating a local certificate and trusted CA certificate.
- Generating a trusted CA certificate, private certificate and private key for PC
- Configuring OpenVPN.
- Configuring SmartVPN Client (Remote User)
- Checking the VPN Connection Status

Configuring the Time and Date for Router (Main Office)

- 1. Access into the web user interface of Vigor router.
- 2. Open **System Maintenance>>Time and Date**. Click **User Internet Time** and set the time zone for the router located. Remember to click **Inquire Time** and click **OK** to save the settings.

_

Generating a local certificate and trusted CA certificate (Main Office)

1. Open **Certificate Management >> Local Certificate** to a generate certificate signing request. Click **GENERATE**.

9 Local Certificate C	onfiguration		
Name	Subject	Status	Modify
			View Delete
			View Delete
			View Delete

2. Type related information in the **Subject Alternative Name** and **Subject Name** sections.

Certificate Management >> Local Certificate

Certificate Name	Draytek_CA
Subject Alternative Name	
Туре	Domain Name 💌
Domain Name	draytek.com
Subject Name	
Country (C)	TW
State (ST)	
Location (L)	
Organization (O)	
Organization Unit (OU)	draytek
Common Name (CN)	vigor
Email (E)	
Кеу Туре	RSA V
Key Size	1024 Bit 💌

3. After clicking **Generate**, the new generated CA will be shown as follows:

Certificate Management >> Local Certificate

Name	cate Configuration Subject	Status	Modify
Draytek_CA	/C=TW/OU=draytek/CN=vigor	Requesting	View Delete
			View Delete
			View Delete

4. Run XCA and create a new XCA database first by clicking File>>NewDatabase. Later,

🖌 X Certificate and Key management
<u>File Import Token H</u> elp
Private Keys Certificate signing requests Certificates Templates Revocation lists
Internal name Type Size Use Passw New Key
Export
Import
Import PFX (PKCS#12)
Show Details
Delete
Database:C:/Documents and Settings/USER/My Documents/ca-1.xdb

5. Click the **Certificate** tab and click **New Certificate**.

🖋 X Certificate and Key management		
<u>File Import T</u> oken <u>H</u> elp		
Private Keys Certificate signing requests	Certificates Templates Revocation lists	
Internal name 🔶 commonName 🤇	CA Serial <u>N</u> ew Certificate	
	<u>Export</u>	
	Import	
	Chow Dataila	

6. Choose **Create a self signed Certificate with the serial** in the signing section. Click **Apply All** to apply the CA Template.

🖋 X Certificate and Key management	? 🛛
Create x509 Certificate	(a) Protocol (c)
Source Subject Extensions Key usage N	etscape Advanced
Signing request	
Sign this Certificate signing request	~
Copy extensions from the request	Show request
Modify subject of the request	
Signing Create a self signed certificate with the serial Use this Certificate for signing 	
Signature algorithm	SHA 1
- Template for the new certificate	
[default] CA	
	Apply extensions Apply subject Apply all
	OK Cancel

7. Click the **Subject** tab. Type distinguishable or preferred names as **Internal name**, countryName, commonName and emailAddress respectively. Then, click Generate a new key.

🖋 X Certificate and k	Key management			? 🛛
Create x509 0	Certificate			A Residence - Star
Source Subject	Extensions Key usage	Netscape Advanced		
-Distinguished name -		•		
Internal name	Dray CA test	organizationName		
countryName	ΤW	organizationalUnitName		
stateOrProvinceNam	e	commonName	jos	
localityName		emailAddress	jos@draytek.(com
Т	уре	Content		Add
				Delete
Private key				
		🔽 🗌 Used	keys too <u>G</u> er	nerate a new key
			OK	Cancel

8. Choose **RSA** as **Keytype** and choose **1024 bit** as **Keysize** for this certificate. Click **Create** and wait for a moment.

🝼 X Certif	icate and Key ı	nanagement	? 🛛
New ke	ey		
Please give a Key prope		key and select the desired keysi	ze
Name	Dray CA test		
Keytype	RSA		~
Keysize	1024 bit		~
		•	
			Create Cancel

9. Click OK.



- 10. Now we have generated a Trusted CA Certificate well. Return to the web user interface of Vigor router.
- 11. Open Certificate Management >> Local Certificate. Click View.

Certificate Manager	nent >> Local Certificate		
X509 Local Certifica	ate Configuration		
Name	Subject	Status	Modify
Draytek_CA	/C=TW/OU=draytek/CN=vigor	Requesting	View Delete
			View Delete
			View Delete
	GENERATE IMPORT	REFRESH	

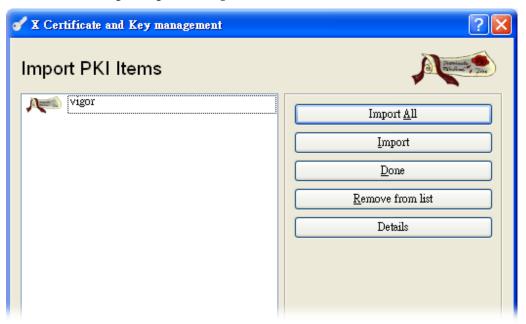
12. Copy the content of **X509 Local Certificate Request** for pasting to the XCA.

Certificate Signing Request Information Certificate Name : Draytek_CA Issuer : Subject : C=TW, OU=draytek, CN=vigor Subject Alternative Name : DNS:draytek.com Valid From : Valid To : PEM Format Content : BEGIN CERTIFICATE REQUEST MIIBmDCCAQECAQ&LaELMAKGAIUEBhMCVFCxEDA0BgNVBAsTB2RYX102WsxDjAM BgNVBAMTBX2p229yMIGfMA0GCSqGSIb3DQEBAQUAAGNADCBiQKBqQDEQeEvaKXI taVHe0j12VLegphjV4LEdFFW3SUG2g0XkQTw13mLeHNA7fM9twKSA41xek0S41xek0x 9ktv/tKJwWCSQ5YgCJfnVTA5E0mZYsYC2Yute+DL2uP6HpMJxJ/dQ4Tkq0r2KFFP 1zy801TqVUdzFDf3V8JTsvmqxfFWKG7mxW1DAQABoCkwJwJJK0ZIhvcNAQk0MRow GDAWBgNVREEDzANgtkcmF3d6VrLmNvbTANBgkqhkiG9w0BAQUFAA0BgQASmfA2 cqvLaB_XhDct3aCXnH98L0e2130U1ct372y01WBLsw1TqkEEm3NBmCewrqCCuISj 102Ccck6NrexQ0WTcp2ItvIJo6t3N4dwRNR0rCBb7wsKYBJNO2nh410XU+/9d/1 E0Hf718nkSwY0BVH001KvyrDCCRImGrV/0Q59A== END CERTIFICATE REQUEST	:// 192.168.1.5 /doc/XLoCfVi1.htm		
Issuer : Subject : C=TW, OU=draytek, CN=vigor Subject Alternative Name : DNS:draytek.com Valid From : Valid To : PEM Format Content :BEGIN CERTIFICATE REQUEST MI IBmDCCAQECAQAwLxELMAkGA1UEBhMCVFcxEDAOBgNVBAsTB2RyYX102WaxDjAM BgNVBAMTBXZp229yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBqQDEQeEvaKX1 taV+HeJ12VzLegphJV4LEdrFW385UGzgOXkQTw13mLzHNA7fM9twK3CA41xek0Sq 9ktv/tKJwKCSQSYgCJfnVTASEOmZYaYCZYute+DLZuP6HpMJxJ/dQ4Tkq0r2KFfP 1zy8o1TqVUd2FDf3V8JTswmayfPWKS7mXw1DAQABoCkwJwJKJC2IhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBJXibCt3aCXnH)8L0e2130U1ct372yo1WBLswITqkeEm3NBmCewrqCCuISj 102Ccck6NrexQ0JWTcp2ltvIJo653M4cWRGCBb7wsKYBJN0Znh410XU+/9d/1		Certificate Signing Request Information	
Subject : C=TW, OU=draytek, CN=vigor Subject Alternative Name : DNS:draytek.com Valid From : Valid To : PEM Format Content :BEGIN CERTIFICATE REQUEST MIIBmDCCAQECAQAWLEELMAkGAIUEBhMCVFcxEDAOBgNVBAsTB2RyYX102WsxDjAM BgNVBAMTBX2p229yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBgQDEQeEvaKX1 taV+HeJ12VzLegphjV4LEdrFW385UG2g0XkgTw13mLzHNA7fM9twKSCA41xek0Sq 9ktv/tKJwKCSQ5YgCJfnVTA5E0m2YsYC2Yute+DLZuP6HpMJxJ/dQ4Tkq0r2KFfP 1zy801rqVUd2FDf3V8JTswmaffPWKG7mXw1DAQABoCkwJwJJK02IhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBJXibCt3aCXnHj8L0e2130U1ct372yo1WBLswITqkeEm3NBmCewrqCCuISj 102Ccck6NrexQ0JWTcp2ltv1Jo6t3N4cWRGCBb7wsKYBJN02nh410XU+/9d/1	Certificate Name :	Draytek_CA	
Subject Alternative Name : DNS:draytek.com Valid From : Valid To : PEM Format Content : BEGIN CERTIFICATE REQUEST MIIBmDCCAQECAQAWLEELMAkGAIUEBhMCVFcxEDAOBgNVBAsTB2RyYX102WaxDjAM BgNVBAMTBXZp229yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBgQDEQeEvaKX1 taV+HeJ12VzLegghJV4LEd1FW385UGzg0XkQTw13mLzHNA7fM9twK3cA41xek0Sq 9ktv/tkJwKCSQ5YgCJfnVTA5E0mZYsYCZYute+DLZuP6HpMJxJ/dQ4Tkq0r2KFfP 1zy8o1TqVUd2FDf3V8JTswmqxfPWKG7mxW1DAQABoCkwJwYJKoZIhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAA0BgQASmfA2 cqvLaBJXibCt3aCXnHJ8L0e2130Ulct372y01WBLswITqkeEm3NBmCewrqCCuISj DO2ccck6NrexQ0WTpO2LvIJo6c13McGWRCBb7wsKYBJNOZnh410XU+/9d/1	Issuer :		
Valid From : Valid To : PEM Format Content : MIIBmDCCAQECAQ&L2ELMAkGA1UEBhMCVFczEDAOBgNVBAsTB2RyYX102WsxDjAM BgNVBAMTBXZp229yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBgQDEQeEvaKX1 taV+HeJ12VzLegphjV4LEdrFW385UG2gOXkQTw13mLzHNA7fM9twKScA41xek0Sq 9ktv/tKJwWCSQ5YgCJfnVTA5EOmZYsYCZYute+DLZuP6HpMJxJ/dQ4Tkq0r2KFfP 1zy8o1TqVUd2FDf3V8JTswmqxfPWKG7mXw1DAQABoCkwJwYJKoZ1hvcNAQkOMRow GDANBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBjXibCt3aCXnHj8L0e2130U1ct372y01WBLswITqkeEm3NBmCewrqCCuISj 10zCcck6NrexQ0JWTpC2LtvIJo613M4CWRGCBb7wsKYBJN0Znh410XU+/9d/1 E0Hf718nk5wYoBVH0U1KvyrDCCR1mGrV/0Q59A==	Subject :	C=TW, OU=draytek, CN=vigor	
Valid To: PEM Format Content: PEM Format Content: Unid To: PEM Format Content: PEM For	Subject Alternative Name :	DNS:draytek.com	
PEM Format Content : BEGIN CERTIFICATE REQUEST MI IBmDCCAQECAQAWLEELMAkGAIUEBhMCVFcxEDAOBgNVBAsTB2RyYX102WsxDjAM BgNVBAMTBXZp229yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDEQeEvaKX1 taV+HeJ12VzLegphjV4LEdrFW385UGzgOXkQTw13mLzHNA7fM9twKScA41xek0Sq 9ktv/tKJwKCSQ5YgCJfnVTA5EOmZYsYCZYute+DLZuP6HpMJxJ/dQ4Tkq0r2KFFP 1zy801TqVUd2FDf3V8JTswmqxfFWKG7mXwIDAQABoCkwJwJKJC2IhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBJXibCt3aCXnH)8L0e2130U1ct372yo1WBLswITqkeEm3NBmCewrqCCuISj 10zCcckNrexQ0JWTcp2ltvIJ06c3N4cWKGCBb7wsKYBJN0Znh410XU+/9d/1 E0Hf718nk5wYoBVH001KvyrDCCR1mGrV/0Q59A==	Valid From :		
MIIBmDCCAQECAQ&WLzELMAkGAIUEBhMCVFcxEDAOBgNVBAsTB2RyYX102WsxDjAM BgNVBAMTBXZpZ29yMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDEQeEvaKX1 taV+HeJ12VzLegghJV4LEdrW38SUGzgOXkQTw13mLzHNA7fM9twKScA41xek0Sq 9ktv/tKJwWCSQSYgCJfnVTA5EOmZYsYCZYute+DLZuP6HpMJxJ/dQ4Tkq0r2KFfP 1zy8o1TqVUd2FDf3V&JTswmqxfPWKG7mXw1DAQABoCkwJwYJKCZIhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBJXibCt3aCXnHj8L0e2130U1ct372yo1WBLswITqkeEm3NBmCewrqCCuISj 10zCcck6NrexQ0JWTcD2ItvIJo6t3N4cWx8KGCBb7wsKYBJN0Znh410XU+/9d/1 E0Hf718nk5wYoBVH001KvyrDCCR1mGrV/0Q59A==	Valid To :		
	PEM Format Content :	MIIBmDCCAQECAQAwLzELMAkGAIUEBhMCVFcxEDAOBgNVBAsTB2RyYX102WsxDjAM BgNVBAMTBX2p229yMIGEMAOGCSqGSIb3DQEBAQUAAGNADCB1QKBqQDEQEEvaKXI taV+HeJ12VzLegphjV4LEdrFW385UGzg0XkQTw13mLzHNA7fM9twKSCA41xekOSq 9ttv/tKJwWCSQ5YgcJfnVTA5EOmZysYC2Yute+DL2UP6HpMJxJ/dQ4Tkq0r2KFFP 1zy801TqVUdzFDf3V8JTswmqxfPWKG7mXwIDAQABoCkwJwYJKoZIhvcNAQkOMRow GDAWBgNVHREEDzANggtkcmF5dGVLLmNvbTANBgkqhkiG9w0BAQUFAAOBgQASmfA2 cqvLaBjXibCt3aCXnHj8L0e213oU1ct372y01WBLswITqkeEm3NBmCewrqCCuISj 102ccck6NrexQ0JWTcp2ltv1Jo6t3N4cWRNGrCBD7wsKYBJN02hh410XU+/9d/1 E0Hf718nk5wY0BVH0U1KvyrDCCR1mGrV/0 <u>Q59A==</u>	<

13. Return to XCA. Click **Certificate signing requests** and click the right mouse button to display the drop down selection. Choose **Paste PEM data**.

🖋 X Certificate and Key management	
<u>F</u> ile I <u>m</u> port <u>T</u> oken <u>H</u> elp	
Private Keys Certificate signing requests Certificates Tem	uplates Revocation lists
Internal name 🔶 commonName Signed	New Request
	Export
	Import
New Request	Show Details
Import Paste PEM data	Delete
Columns	Framineata DYnoboob Fina
Database:C:/Documents and Settings/USER/My Documents/ca-1.xdb	

14. From the following dialog, click Import All.



15. Click **Certificate signing requests**. Choose the Certificate and choose the **Sign** option from the drop down menu with right click the mouse button.

🝼 X Certificate and Key man	gement
<u>File Import T</u> oken <u>H</u> elp	
Private Keys Certificate sign	ng requests Certificates Templates Revocation lists
Internal name 🔶 comr New vigor vigor	NonName Signed Unhandled New Request
	Import
	Extract public Key Rename
	Show Details
	Sign Export • Delete
	Delete Paste PEM data Columns •
Database:C:/Documents and Setting	/USER/My Documents/ca-1.xdb

16. The follwoing dialgo will appear. From the **Source tab**, click **Use this Certificate for signing** and choose **DrayCA Test** from the drop down list. Click **OK**.

🖌 X Certificate and Key management	? 🛛
Create x509 Certificate	a) comments from
Source Extensions Key usage Netscape	Advanced
Signing request	
✓ Sign this Certificate signing request	vigor
Copy extensions from the request	Show request
Modify subject of the request	
Signing	
O Create a self signed certificate with the serial	1
O Use this Certificate for signing	DrayCA Test
Signature algorithm	SHA 1
- Template for the new certificate	
[default] CA	▼
	Apply extensions Apply subject Apply all
	OK Cancel

17. The certificate has be created and signed successfully. Click **OK**.

rivate Keys	Certifi	cate signing requests	Certificates	Templates	Revocation lists
Internal nam		commonName	Signed		New Request
Net vigo	r v	/igor	V Signed		Export
					Import
		🖋 X Certific	ate and Key n	nanagement	Show Details
			cessfully created		/igor' Delete
		i) Suc			
			OK		

18. Click the **Certificates** tab and click **Export** to export the selected local certificate and trusted CA certificate to Vigor router respectively.

Private Keys Certificate signing requests	Certificates	Templates Revocation lists
Internal name <u>commonNam</u>	e CA 🖌 Yes	<u>N</u> ew Certificate
Vigor Vigor	·	Export
		Import
		Show Details
		Delete

19. Choose **PEM with Certificate chain** as the **Export Format** and click **OK**.

Certifika	ate export 🥂	inate Sant
Please enter	the filename for the certificate.	
Filename 🤇	:/Program Files/xca/wigor.crt	
DER is a bi	ary format of the Certificate	
PEM is a ba	æ64 encoded Certificate	
	n official Certificate exchange format an encrypted official Key-Certificate exchange format	
	nat PEM with Certificate chain	_

20. Return to web user interface of Vigor router. Open **Certificate Management>>Trusted CA Certificate**. Click **IMPORT**.

Certificate Management >> Trusted CA Certificate

Name	Subject	Status	Modify
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

21. Locat the certificate file (e.g., DraytekCA_test) and click Import.

Certificate Management >	>> Trusted CA Certificate		
Import X509 Trusted CA (Certificate		
	Select a trusted CA certifica Click Import to upload the ce	瀏覽	
選擇要上傳的檔	 案		? 🔀
查詢():	🚱 桌面	🗾 🔇 🕸 📂 🖽-	
我最近的文件	名稱 Selvigor Selvigor DraytekCA_test	大小類型 2 KB 安全性憑證 1 KB 安全性憑證 2 KVD Minute Word 文/4	修改 へ 2013/ 2013/

22. The trusted CA certificate has been uploaded to rotuer successfully.

Certificate Management >> Trusted CA Certificate

Name	Subject		Status	Modify	
rusted CA-1	I CA-1 /C=TW/CN=jos/emailAddress=jo OK Vjew Delete			View Delete	
rusted CA-2	ted CA-2 View Delete			View Delete	
usted CA-3 View Dele			View Delete		
Certificate Info	ormation - Windows Interne	t Explorer			
) http://192.168.1.5	5/doc/XCaCfVi1.htm				2
	Certi	ficate Detail Info	ormation		
Certifica	ate Name:	Trusted CA-1			
Certifica Issuer:	ate Name:			ss=jos@drayte	
		/C=TW/CN=jc k.com	s/emailAddres	ss=jos@drayte ^ v ss=jos@drayte ^ v	
Issuer: Subject		/C=TW/CN=jc k.com /C=TW/CN=jc	s/emailAddres	×	
Issuer: Subject	:: : Alternative Name:	/C=TW/CN=jc k.com /C=TW/CN=jc	s/emailAddres	×	
Issuer: Subject Subject	:: : Alternative Name: om:	/C=TW/CN=jc k.com /C=TW/CN=jc k.com	s/emailAddres	×	
Issuer: Subject Subject Valid Fr	:: : Alternative Name: om:	/C=TW/CN=jc k.com /C=TW/CN=jc k.com	s/emailAddres s/emailAddres	×	

23. Open Certificate Management>>Local Certificate. Click IMPORT.

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Draytek_CA	/C=TW/OU=draytek/CN=vigor	Requesting	View Delete
			View Delete
			View Delete

24. Locat the certificate file (e.g., vigor) and click **Import**.

Import X509 Local Certificate		
Upload Local Certificate		
Select a local certificate file.		
Certificate file:	瀏覽	
Click Import to upload the local	certificate.	
Upload Pl 選擇要上傳的檔案		
Upload Pt 選擇要上傳的檔案 查詢①: 🗁 xxa	· G 🕈 🖻 📰 •	
	✓ 3 3 10 111 大小 類型	修改 🔨
查詢(1): 🗁 xxa		修改 A 2013/
查詢(): 📄 xxa	大小類型	and the second s
	大小 類型 2 KB 安全性憑證	2013/

25. The local certificate has been uploaded to rotuer successfully.

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
vigor	/C=TW/OU=draytek/CN=vigor	ОК	View Delete
			View Delete

Generating a private certificate and private key for PC (Main Office)

- 1. Run XCA.
- 2. Click the **Certificate** tab and click **New Certificate**.

🖋 X Certificate and Key management		
<u>File Import Token H</u> elp		
Private Keys Certificate signing requests	Certificates Templates Revocation lists	
Internal name 🔶 commonName	CA Serial <u>N</u> ew Certificate	
	Export	
	Import	
	Show Detaile	

3. Click **Use this Certificate for signing**. Then click the **Subject** tab.

🖋 X Certificate and Key management	?X
Create x509 Certificate	Commission State
Source Subject Extensions Key usage 1	Netscape Advanced
Signing request	
Sign this Certificate signing request	vigor 💙
Copy extensions from the request	Show request
Modify subject of the request	
Signing	
Create a gelf signed certificate with the serial	
O Use this Certificate for signing	DraytekCA test
Signature algorithm	SHA 1
Template for the new certificate	
[default] CA	
	Apply extensions Apply subject Apply all
	OK Cancel

4. Click the **Subject** tab. Type distinguishable or preferred names as **Internal name**, **countryName**, and **commonName** respectively. Then, click **Generate a new key**.

X Certificate and Key management				
Create x509 Ce	rtificate		Comments of the second	
Source Subject E	xtensions Key usage	Netscape Advanced		
Distinguished name —				
Internal name j	jos	organizationName		
countryName	TW	organizationalUnitName		
stateOrProvinceName		commonName	jos	
localityName		emailAddress		
Туре	,	Content	Add Delete	
Private key		💌 🗌 Used	keys too Generate a new key OK Cancel	

5. Choose **RSA** as **Keytype** and choose **1024 bit** as **Keysize** for this certificate. Click **Create** and wait for a moment.

🝼 X Certif	icate and Key 1	nanagement	? 🗙
New ke	ey		
_		key and select the desired keysize	
-Key prope	erties		
Name	jos		
Keytype	RSA		~
Keysize	1024 bit		~
		•	
		Create	Cancel

6. Click OK.



- 7. Now we have generated a Trusted CA Certificate well. Return to the web user interface of Vigor router.
- 8. Click the **Certificates** tab and click **Export** to export the selected local certificate and trusted CA certificate to Vigor router respectively.

🖋 X Certificate and Key management	
<u>File Import Token H</u> elp	
Private Keys Certificate signing requests Certificates Templa	tes Revocation lists
Internal name CA	<u>N</u> ew Certificate
jos jos	<u>E</u> xport
Vigor Vigor	Import
	Show Details
	Delete

9. Choose **PEM with Certificate chain** as the **Export Format** and click **OK**.

🖌 X Certificate	and Key management	? 🔀
Certifikate	export	a manual 200
Please enter the	filename for the certificate.	
Filename C:/D	ocuments and Settings/USER/桌面\jos.crt	
PEM is a base64 PKCS#7 is an o PKCS#12 is an	format of the Certificate encoded Certificate fficial Certificate exchange format encrypted official Key-Certificate exchange format PEM with Certificate chain	✓
		OK Cancel

10. Click **Private Keys** and select the one you want for exporting to Vigor router. Click **Export**.

🝼 X Certific	ate and Key manager	nent		
<u>F</u> ile I <u>m</u> port	<u>T</u> oken <u>H</u> elp			
Private Keys	Certificate signing r	equests Certif	icates Temp	lates Revocation lists
Internal		Size U 1024 bit	Jse Pa 1 Comr	New Key
CE D	raytekCA test RSA	1024 bit	1 Comr	Export
				Import
				Import PFX (PKCS#12)
				Show Details
				Delete
<				BUILDE STREET
Database:C:/Do	ocuments and Settings/US	ER/My Document	ts/ca-1.xdb	

11. Choose **PEM** as the **Export Format** and click **OK**.

🖋 X Certificate and Key management	? 🛛
Key export	
Please enter the filename for the key. Filename C:/Documents and Settings/USER/桌面\jos.key	
DER is a binary format of the key without encryption PEM is a base64 encoded key with optional encryption PKCS#8 is an encrypted official Key-exchange format Export Format PEM	
When exporting the private key it should be encrypted.	
 Export as PKCS#8 Encrypt the Key with a password 	
	OK Cancel

Configuring OpenVPN (Main Office)

VPN and Remote Access >> OpenVPN General Setup

Return to web user interface of Vigor router. Open VPN and Remote Access >> 1. OpenVPN General Setup. Configure the settings as shown below.

OpenVPN General Setup	
Port	1194
Cipher Algorithm	AES128 V
HMAC Algorithm	SHA1 🔽
Certificate Authentication	

Note: OpenVPN on vigor only support UDP protocol and TUN device interface currently. So please setup corresponding configurations on the client side.

OK

2. Open VPN and Remote Access >> Remote Dial-in User to create a profiles for Dial-in User. Click any index number link to create a new one.

VPN and	Remote Access >>	Remote Dia	II-in User	
Remote	Access User Accour	nts:		
View:	💿 All 🛛 Online	O Offline		
Index	User	Active	Status	Index
<u>1.</u>	???			<u>17.</u>
<u>2.</u>	???			<u>18.</u>

4. Check the box of **Enable this account**. Set the Username (e.g., jos) and Password (e.g., jos) for OpenVPN. Click **OK** to save the settings.

Index No. 1	
User account and Authentication	Username
Enable this account	Password(May 19 char)
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
SSL Tunnel	Pre-Shared Key
🗹 OpenVPN Tunnel	IKE Pre-Shared Key
Specify Remote Node	Digital Signature(X.509)
Remote Client IP	None 🔽
or Peer ID	IPsec Security Method
or Peer ID	Medium(AH)

VPN and Remote Access >> Remote Dial-in User

5. Open **SSL VPN>>General Setup**. Choose **vigor** which defined in the **Local Certificate** page for OpenVPN user. Click **OK** to save the settings.

SL VPN >> General Setup					
SSL VPN General Setup	L VPN General Setup				
Port	443 (Default: 443)				
Server Certificate	self-signed 💙				
Encryption Key Algorithm	self-signed vigor				
🔘 High - AES(128 bits) ;					
💿 Default - RC4(128 bit	5)				
O Low - DES					

Cancel

Note: The settings will act on all SSL applications.

OK

Configuring SmartVPN Client (Remote User)

1. Execute **SmartVPN Client.** Click **Insert** to create a new dial-in VPN profile (e.g., Profile 6).

White share will ended	llow IPSec NAT			
This step will add AssumeUDPEncap computer. For mo	sulationConte	xtOnSendR	ule regist	ry value to
and Q818043 in t				
		figure		
		ingure		
Step 1. Dial to IS If you have alread		iblic IP. you	i can skin	this step.
a you have alloc	a) gotton a p		- curr ship	cias scopi
			~	Dial
			~	Dial
Step 2. Connect	to VPN Server		•	Dial
Step 2. Connect	to VPN Server		•	Dial

Type a name (e.g., Profile 6) as the **Profile Name** and an IP address (e.g., 200.200.200.200) as VPN Server IP. Set jos/jos as the User Name/Password. Click **OpenVPN** as the type of VPN and click **OK** to display the **OpenVPN Setting** dialog.

Dial To VPN				
Profile Name :	Profile 6			
Auto re-dial after d				
Redial attempts		0		
Redial interval :		0 seconds		(1991)
Auto run when sys		Open¥PN Setting		×
VPN Server IP/HOST N	lame(such as 123.45.67.8	Port:	1194	
200.200.200.3	200	Cipher methods:	AES-128-CBC	~
User Name : j	os	Authentication:	SHA1	~
Password :	**	Certificate Authentication		
Enable mobile On	e Time Password (mOTP)	CA cert:	Draytek_CA_test.crt	Browse
C	onfigure Secret for mOTP	Client cert:	jos.crt	Browse
Type of VPN	OL2TP	Client key:	jos.key	Browse
O IPSec Tunnel	OL2TP over	Fallback to SSL Tunnel		
SSL VPN Tunne		Port:	443	
PPTP Encryption	a O opanin	ОК	Cancel	
No encryption				
O Require encryp	stion			
O Maximum stren	ngth encryption			
Authentication me	thod AP	·		
Use default gate	eway on remote network	More		
ОК	Cance			
	Cance	<u> </u>		

3. Configure the Port number, Cipher methods and Authentication as the settings defined above. Check the box of **Certificate Authentication**. Then click **OK**.



Checking the VPN Connection Status

Now both ends (router and remote PC) are configured well.

- 1. Access into the web user interface of Vigor router.
- 2. Open **VPN and Remote Access>>Connection Management** to check the VPN connection status. From the following figure, we can know that the remote user can access the Vigor router's LAN successfully by using the username/password (jos/jos).

VPN and Remote Access >> Connection Management

Dial-out Tool	Refresh Seconds : 10 💌 Refresh
General Mode:	Dial
Backup Mode:	Dial
Load Balance Mode:	✓ Dial

VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (jos) al User Databa	OpenVPN se AES-SHA1 Auth	188.188.188.188 via WAN1	192.168.1.11/32	14	52	20	52	0:0:31	0
C:\WINDOW	S\system32\cmd_exe	- ping 192.168.1.1					-	. 🗆 🗙	
		the second s							
	168.1.1 with 32								
Reply from 19	92.168.1.1: byt	es=32 time<1m	s TTL=255						
Reply from 19 Reply from 19	92.168.1.1: byt 92.168.1.1: byt	es=32 time<1m es=32 time<1m	as TTL=255 as TTL=255						
Reply from 19 Reply from 19 Reply from 19	92.168.1.1: byt 92.168.1.1: byt 92.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m	os TTL=255 os TTL=255 os TTL=255						
Reply from 19 Reply from 19 Reply from 19 Reply from 19	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m	es TTL=255 es TTL=255 es TTL=255 es TTL=255					-	
Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	:es=32 time<1m :es=32 time<1m :es=32 time<1m :es=32 time<1m :es=32 time<1m	as TTL=255 as TTL=255 as TTL=255 as TTL=255 as TTL=255 as TTL=255						
Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from <u>19</u>	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	ses=32 time<1m ses=32 time<1m ses=32 time<1m ses=32 time<1m ses=32 time<1m ses=32 time<1m	s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255						
Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19 Reply from 19	22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt 22.168.1.1: byt	es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m es=32 time<1m	as TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255 s TTL=255						

3.3 How to Implement the AD/LDAP Authentication for User Management?

For simplifying the configuration of LDAP authentication for User Access Management, we implement "Group" feature.

There is no need to pre-configure user profile for each user on Vigor router anymore. We only need to configure the Groups DN, then the Vigor router (e.g., Vigor 3200 series) can pass the authentication to LDAP server with the pre-defined Group path.

Below shows the configuration steps:

Applications >> Active Directory /LDAP

- 1. Access into the web user interface of the Vigor router.
- 2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings.

General Setup	Active Directory / LDAP Profiles	
🗹 Enable		
Bind Type		Regular Mode 💌
Server IP Ac	dress	172.16.2.8
Destination I	Port	389
Regular DN		uid=vpntest,ou=vpnusers,dc=ms,dc=drayte
Regular Pass	word	1234
		OK Cancel

There are three types of bind type supported:

- Simple Mode Just simply do the bind authentication without any search action.
- Anonymous Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode** Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.
- 3. Create LDAP server profiles. Click the **Active Directory /LDAP** tab to open the profile web page and click any one of the index number link.

If we have two groups "**RD1**" and "**SHRD**" on LDAP server, we can configure two LDAP server profiles with different Group Distinguished Name.



Applications >> Active Directory /LDAP>>Server Profiles

« No. 1		
Name	rd1	
Common Name Identifier	uid	
Base Distinguished Name	ou=People,dc=ms,dc=draytek,dc=com	2
Group Distinguished Name	cn=rd1,ou=Group,dc=ms,dc=draytek,dc=c	
	OK Cancel	



Name	shrd	
Common Name Identifier	uid	
Base Distinguished Name	ou=People,dc=ms,dc=draytek,dc=com	
Group Distinguished Name	cn=shrd,ou=Group,dc=ms,dc=draytek,dc=	9

- 4. Click **OK** to save the settings above.
- 5. Open User Management>>General Setup. Select User-Based as the Mode option.

User Management >> General Setup

ral Setup		
Mode: User-Based 💌		
Web Authentication:		
Notice :		
1. User Management will refer to active rules in Data	Filter as whitelist	ts and blacklists
in user-based firewall mode.		
Users match the above lists will not be required fo The framely rules policy will still would	r authentication.	
The firewall rules policy will still valid. 3. Otherwise, authentication required for users not m	atched the abov	o liste
The firewall rules designated in the user profile's p		
J		
Landing Page (Max 255 characters)	Preview	Set to Factory Default
<body stats="1"><script language="javascript"></td><th>></th><td>1</td></tr><tr><td>window.location='http://www.draytek.com'</so</td><th>cript></body></th><td></td></tr><tr><td></td><th></th><td></td></tr><tr><td></td><th></th><td></td></tr><tr><td></td><th></th><td></td></tr><tr><td></td><th></th><td>2</td></tr></tbody></table></script></body>		

6. Then open **VPN and Remote Access>>PPP General Setup** to **check** the profile(s) that will be authenticated with LDAP server.

PPP General Setup PPP/MP Protocol			LDAP Server F	Profiles for PPP Authentication
Dial-In PPP Authentication	PA	P or CHAP 🔽		rd1 shrd
Dial-In PPP Encry (MPPE)	ption Opt	ional MPPE		sind
Mutual Authentic	ation (PAP) 🔘 Yes 💽 No		
Username				
Password				
P Address Assignme When DHCP Disable		n Users		
Assigned IP start	LAN 1	192.168.1.200		
	LAN 2	192.168.2.200		
	LAN 3	192.168.3.200		
	LAN 4	192,168,4,200		

7. After above configurations, users belong to either "rd1" or "shrd" group can access Internet after inputting their credentials on LDAP server.

VPN and Remote Access >> PPP General Setup

3.4 How to implement the AD/LDAP authentication for SSL Application?

Below shows the configuration steps:

Applications >> Active Directory /LDAP

- 1. Access into the web user interface of the Vigor router.
- 2. Open **Applications>>Active Directory /LDAP** to get the following page for configuring LDAP related settings. Click the **General Setup** tab and enable the AD/LDAP service.

	Set to Factory Defa
General Setup Active Directory / LDAP Profiles	
🗷 Enable	
Bind Type	Regular Mode 👻
Server IP Address	172.16.2.8
Destination Port	636
Use SSL	
Regular DN	uid=vpntest, ou=Vpnusers, dc=ms, dc=dray
Regular Password	1234
	OK Cancel

There are three types of bind type supported:

- **Simple Mode** Just simply do the bind authentication without any search action.
- **Anonymous** Perform a search action first with Anonymous account then do the bind authentication.
- **Regular Mode** Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority.

For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.

3. Click the Active Directory /LDAP tab to open the profile web page.

Applications >> Active Directory /LDAP

Active Directory /LDAP)		Set to Factory Default
General Setup	Active Directory / LDAP Profiles		
Index	Name	Distinguished Name	
<u>1.</u>			
<u>Ž.</u>	,		
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			

4. Click any one of the index number link to configure the proper **Base Distinguished Name** and **Group Distinguished Name**.

Applications >> Active Directory /LDAP>>Server Profiles

Name	RD1
Common Name Identifier	uid
Base Distinguished Name	ou=Vpnusers, dc=ms, dc=draytek, dc=com
Group Distinguished Name	cn=vpn, ou=Group, dc=ms, dc=draytek, dc=c
	OK Cancel

Suppose that there are several departments in your company, e.g., RD1 and RD2. Here, create a profile for RD1 first.

Sometimes, you may forget the Distinguished Name since it's too long. Then you may click the solution to list all the account information on the AD/LDAP Server to assist you finish the setup.

AD/LDAP Server 172.16 Query List Tree Menu	
	dc=ms,dc=draytek,dc=com
	cn=Manager
	• ou=Hostlist
	Sou=Group
	······································
	Sou=People
	Sou=Filters
	sambaDomainName=MS.DRAYTEK.COM
	• Ou=Hosts
	ou=Vpnusers
	SambaDomainName=TS
AD/LDAP Distingui	shed Name
	ОК

Mozilla Firefox		
] 172.17.1.137/doc/ldap_query.htm		17
D/LDAP Server 172.16.2.8:636 uery List Tree Menu	dc=ms, dc=draytek, dc=com ou=Vpnusers uid=tyrone_yeh uid=ichena uid=lacky_Lee uid=lacky_Lee uid=rank_wang uid=frank_wang uid=dena uid=grchang uid=dni uid=dni uid=stephen uid=Harry uid=loseph uid=stephen uid=loseph uid=dri uid=lastephen uid=loseph uid=lastephen uid=loseph uid=lastephen uid=lastephen <t< th=""><th></th></t<>	
AD/LDAP Distinguished Name	ou=Vpnusers,dc=ms,dc=draytek,dc=com	
	ОК	

Press the 🔯 button on this page to keep searching its sub-tree.

In addition, \square means this item is an organization; \square means this item is an account.

5. Press certain item, its **Base Distinguished Name (BDN)** will be shown automatically in the AD/LDAP Distinguished Name field box. Then, press **OK** to save the profile and return to the previous page.

Applications >> Active Directory /LDAP

ve Directory /LDAF)	Set to Factory Defa
General Setup	Active Directory / LDAP Profiles	
Index	Name	Distinguished Name
<u>1.</u>	RD1	cn=vpn1,ou=Group,dc=ms,dc=draytek,dc=com
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		

6. After finishing the AD/LDAP configuration, go to **VPN and Remote Access** >> **PPP General Setup**. Check the box of LDAP that you've enabled in **Application** >> **Active Directory** / **LDAP**.

PPP General Setup			
PPP/MP Protocol			LDAP Server Profiles for PPP Authentication
Dial-In PPP Authentication	PAP Only	•	LDAP
Dial-In PPP Encryption(MPPE)	Optional	MPPE -	
Mutual Authenticati	on (PAP)	🔘 Yes 🔍 No	
Username			
Password			
IP Address Assignmen (When DHCP Disable		n Users	
Assigned IP start	LAN 1	192.168.1.200	
	LAN 2	192.168.2.200	
	LAN 3	192.168.3.200	
	LAN 4	192.168.4.200	
	LANT	102.100.4.200	

VPN and Remote Access >> PPP General Setup

Note: Group Distinguished Name is not a MUST required option for the AD/LDAP configuration. However, you may need, sometimes, to separate certain accounts' authority with it. For example, the **Base Distinguished** Name (BDN) is "ou=people,dc=ms,dc=draytek,dc=com". There is a lot of accounts information. But, only several of them you may prefer to grant the authority of VPN dial-up. For such case, you will have to use this Group Distinguished Name feature separate those accounts.

OK

- 7. Click **OK** to save the configuration.
- 8. Configure the AD/LDAP profiles for different departments (supposed that there several departments in your company, e.g., RD1/RD2).

Applications >> Active Directory /LDAP

ve Directory /LDAP		Set to Factory Default
General Setup	Active Directory / LDAP Profiles	
Index	Name	Distinguished Name
<u>1.</u>	RD1	cn=vpn1,ou=Group,dc=ms,dc=draytek,dc=com
<u>2.</u>	RD2	cn=vpn2,ou=Group,dc=ms,dc=draytek,dc=com
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		
	General Setup Index 1. 2. 3. 4. 5. 6. 7.	General Setup Active Directory / LDAP Profiles Index Name 1. RD1 2. RD2 3. - 4. - 5. - 6. - 7. -

9. Setup two applications profiles (named PC1 and PC2) for SSL VPN.

SSL VPN >> SSL Application

Index	Name	Host Address	Service	Active
<u>1.</u>	PC1	192.168.1.10:5900	VNC	v
<u>2.</u>	PC2	192.168.1.11:3389	RDP	v
<u>3.</u>				х
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				x
<u>9.</u>				x
<u>10.</u>				x

10. Setup two SSL Web Proxy Servers profiles (named google and baidu) for SSL VPN.

SSL Web F	Proxy Servers Profile	95:	Set to Factory Default
Index	Name	URL	Active
<u>1.</u>	google	http://www.google.com	v
<u>2.</u>	baidu	http://baidu.com	v
<u>3.</u>			x
<u>4.</u>			x
<u>5.</u>			x
<u>6.</u>			x
<u>7.</u>			x
<u>8.</u>			x
<u>9.</u>			x
<u>10.</u>			x

SSL VPN >> SSL Web Proxy

SSL VPN >> User Group

11. Go to **SSL VPN** >>**User Group** to setup two separate groups (named with g1 and g2) with different authorities and different authentication methods.

ser Group Profiles:		Set to Factory Defaul
Index	Name	Status
<u>1.</u>	g1	v
<u>2.</u>	g2	v
<u>3.</u>		x
<u>4.</u>		x
<u>5.</u>		x
<u>6.</u>		x
<u>7.</u>		x
<u>8.</u>		x
<u>9.</u>		x
<u>10.</u>		x

Different departments should have separated access authorities. For example, RD1 can only access Google web site and connect to PC1 via VNC; while RD2 can only access Baidu web site and connect to PC2 via RDP. Therefore,

Set the user group profile (named g1) for RD1 department:



SSL VPN >> User Group	
Index No. 1 Enable Group Name g1	
Access Authority	
SSL Web Proxy	SSL Application
🗹 google	PC1
🗖 baidu	PC2

Authentication Methods

Available User Accounts	Se	elected User Accounts	
3-frank 4-ada 5-mike 6-monica 7-pete		-test -caesar	
RADIUS			
LDAP / Actice Directory			
RD1			
RD2			

Set the user group profile (named g2) for RD2 department:

SSL VPN >> User Group		
Index No. 2 Enable Group Name g2 Access Authority		
SSL Web Proxy	SSL Application	
☐ google ☑ baidu	□ PC1 ▼ PC2	
Authentication Methods		
✓ Local User DataBase Available User Accounts 1-test 2-caesar 5-mike 6-monica 7-pete	Selected User Accounts 3-frank 4-ada	×
RADIUS LDAP / Actice Directory RD1 RD2		
ОК	Clear Cancel	

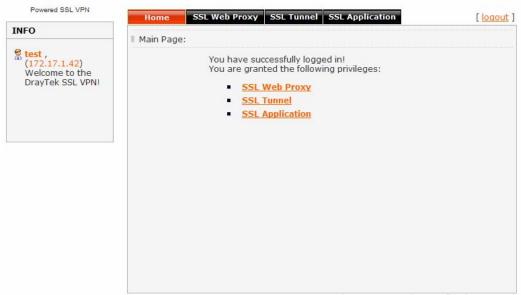
- 12. Once you've finished the configuration on Vigor router, try to login SSL portal with <u>https://<IPAddress>/</u>.
- 13. Please type in the user name and password, and select the group that the account belongs to (In this case, the username is *Caesar* and the group it belongs to is gI).

Username Password	
Group	g1 🔻
	Login

You may also leave this Group option blank. The router will look through all the group profiles to check which one your account belongs to. (It might take a few seconds.)

If the authentication is successful, SSL portal web interface with the applications related to such user account will be displayed on the screen.





Copyright © 2008, DrayTek Corp. All Rights Reserved.

Dray Tek

INFO

Powered SSL VPN Home SSL Web Proxy SSL Tunnel SSL Application [logout] Access methods for SSL Web Proxy: SSL Web Proxy "Green" means the profile is ready for access. "Black" means the profile needs to be activated first. I. SSL google

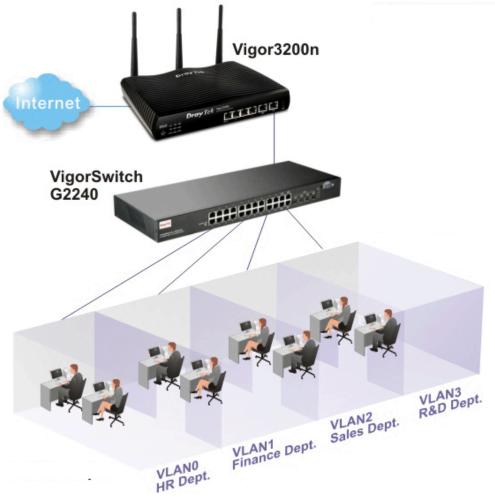
Copyright © 2008, DrayTek Corp. All Rights Reserved.



3.5 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 IP: 192.168.1.0/24 VLAN1 (Finance Dept): LAN Port IP: 192.168.2.0/24 VLAN2 (Sales Dept.): LAN Port IP: 192.168.3.0/24 VLAN3 (R&D): LAN Port IP: 192.168.4.0/24

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				Wirele	ss LAN		
	Enable	VID	Priority	LAN Port	SSID1	S SID2	S SID3	SSID4	Subnet
VLAN0		0	0 🗸	V					LAN 4 💌
VLAN1	~	10	0 🗸						LAN 1 🔽
VLAN2	~	20	0 🗸						LAN 2 🗸
VLAN3	~	30	0 🗸						LAN 3 🗸
VLAN4	V	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 checked Wireless LAN SSID will not has VLAN tagging function but regarded as joining VLAN group;

4. 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		✓	192.168.2.1	Details Page
LAN 3			192.168.3.1	Details Page
LAN 4		✓	192.168.4.1	Details Page
DMZ	V	V	192.168.5.1	Details Page
IP Routed Subnet		\checkmark	192.168.0.1	Details Page

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

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 (LAN1) can get the IP address of 192.168.1.0/24.

The equipment connecting to Vigor3200 LAN Port (LAN2) can get the IP address of 192.168.2.0/24.

The equipment connecting to Vigor3200 LAN Port (LAN3) can get the IP address of 192.168.3.0/24.

The equipment connecting to Vigor3200 LAN Port (LAN4) can get the IP address of 192.168.4.0/24.

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.

Network Configuration		DHCP Server Configuratio	n				
For 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 Disable IP Pool Counts 50 Gateway IP Address 192.168.1.1 DHCP Server IP Address 192.168.1.1						
RIP Protocol Control		IP Pool Counts	50				
	Disable 🔽	Gateway IP Address	192.168.1.1				
		DNS Server IP Address					
		🔲 Force DNS manual se	tting				
		Primary IP Address					
		Secondary IP Address					

OK

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		V	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				×	
DMZ PORT		V	V	~	

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.

rSwitch G2240 🔷 🔿 stem rt n					hips Conf				< >>											
Mode	IGMP-/	A: IGM	VLAN I		Private VLAN	(SVRP-P	GVRP	Propagati	n		ort Me	mhores							_
based Group	Det	VID	IGMP A		CUPP-D	1 2	34	5 6	78	9 10	11 12		4 15	16	17	10	19 20	21 2		24
			Defa											10			1.1.0			10.040
elation ement Vian		1	Disable		Disable	1														24
erreens vian			3200-1			_					_	_	-		_	_	_			
		10	Disable	Disable	Disable								15						23	
	-	-	3200-1				100	100		CORRECT ON CONTRACT	5 3		17			-	12.12	12	1000	
• ·		20	Disable	Disable	Disable									16					23	
and the second second	-	ey.	3200-1		Lindavie											-				
C Binding		30	Disable		Disable										17				23	
x		29	3200-1		LAsable	-	-				-	-	1	-	_	-			-	
*				Disable	Disable											18			23	
		40	Uisable	Disable	URSable	_		1 Million				-		1	_	1				
ring																				
cast																				
1																				
P Snooping																				
Restore																				
ort/import																				

VLAN Name 3200-VID10, Port Members = $15 \cdot 23$ VLAN Name 3200-VID20, Port Members = $16 \cdot 23$ VLAN Name 3200-VID30, Port Members = $17 \cdot 23$ VLAN Name 3200-VID40, Port Members = $18 \cdot 23$

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	Dray Tel		TYYYY	1	r'r'	1010	<u> </u>		
Auto Logout OFF 🔗	Windowski Million			ĘĻ,	Ľ,				
VigorSwitch G2240	5	2		All	Y	80	Access M	U	
System	6	V		All	~	86	Access 💌	0	Disable
⊡ Port	7	~		All	*	86	Access 💌	0	Disable
⊡Vlan	8			All	~	86	Trunk 💌	0	Disable
Vlan Mode Tag-based Group	9			All	Y	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 GVRP	14			All	~	2611	Access 💙	0	Disable
SNMP	15	2		All	*	10	Access ¥	0	Disable
• ACL	16			All	- Contraction	20			Disable
IP MAC Binding	1				*		Access 💌	0	
⊞802.1X	17			All	~	30	Access 💌	0	Disable
Trunk	18			All	*	40	Access \star	0	Disable
STP MSTP	19			All	~	3700	Access 🎽	0	Disable
Mirroring	20			All	Y	3700	Access 💌	0	Disable
Multicast	21			All	Y	1	Access 🗸	0	Disable
●Alarm	22			All	~	1	Access 💙	0	Disable
DHCP Snooping	23			All	~	1	Trunk V	0	Disable
	97.25			12.22	No. Con	-			
Save/Restore Export/Import	24			All	Y	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 192.168.2.0/24

The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.3.0/24

The equipment connecting to VigorSwitch Port 18 can get the IP address of 192.168.4.0/24



3.6 How to Customize Your Login Page

Login page can be customized to fit the request of the administrator.

1. Open User Management>>General Setup. Set User-Based as the Mode and click OK to save teh settings.

Auto Logout 💌	User Management >> General Setup
Quick Start Wizard Service Activation Wizard Online Status	General Setup
WAN LAN NAT Firewall User Management User Management User Frotile > User Frotile > User Group > User Group > User Colline Status Objects Setting CSM	 Mode: User-Based Notice : User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode. Users match the above lists will not be required for authentication. The firewall rules policy will still valid. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.
Bandwidth Management Applications	Landing Page (Max 255 characters) Preview Set to Factory Default
VPN and Remote Access Certificate Management VoIP Wireless LAN USB Application System Maintenance	<pre><body stats="1"><script language="javascript"> window.location='http://www.yahoo.com'</script></body> </pre>
Diagnostics External Devices	OK Clear Cancel

2. Open User Management>>User Profile to create a new user profle.

User Management >> User Profile

User Profile Tab	le		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>	admin	<u>17.</u>	
<u>2.</u>	System Reservation	<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>	
9.		25.	

3. Click any link (e.g., #3) to access into the following page. Type a User Name and a Password. Then, click **OK**.

Profile Index 3	
Enable this account	
User Name	carrie
Password	•••••
Confirm Password	•••••
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None 💌
Log	None 💌
Pop Browser Tracking Window	
Authentication	🗹 Web 🗹 Alert Tool 🗹 Telnet
Landing Page	

User Management >>User Profile(Reserved)

4. Open **System Maintenance>>Login Page Greeting**. Check the box to enable this function. Type a brief description (e.g., *Just for Carrie*) in the field of **Login Description** which will be shown on the heading of the login dialog. Next, click **OK**.

🗹 Enable					
Login Page Title	Just for Carrie		(31 char max.)		
Welcome Message	and Bulletin (Max	511 character	s) <u>Preview</u>	Set to Factory Def	ault
	or=red>Vigor <th></th> <th>onerodile oo bru</th> <th>york worldn (yp</th> <th></th>		onerodile oo bru	york worldn (yp	
	ome Message and E or=red>Welcome N		>		>

System Maintenance >> Login Page Greeting

Note that do not type URL redirect link in Bulletin box.

- 5. Open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
- 6. Try to access into the web user interface (e.g., 192.168.1.1) of Vigor router. Please note *"Just for Carrie"* is displayed as a heading on the login dialog box.

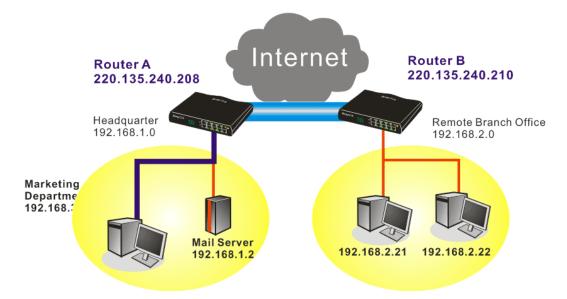
🖉 Yigor Login Page - Windows Internet Explorer	×
http://192.168.1.1/weblogin.htm	
Just for Carrie Username Password Group Login Login Copyright@, DrayTek Corp. All Rights Reserved.	
Welcome Message This welcome message is displayed in the Login page of the router. Replace this text with your own message.	
 The welcome message can be written in HTML so lists such as this one can be created Other markup tags such as p, font or img can be used 	

7. After typing the username and password (defined in User Management>>User Profile), click Login. You can access into Internet or access into the Landing Page if configured in User Management>>General Setup.



3.7 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

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



Settings in Router A in headquarter:

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

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

PPP General Setup	
PPP/MP Protocol	IP Address Assignment for Dial-In Users
Dial-In PPP PAP or CHAP	(When DHCP Disable set)
Authentication	Assigned IP range 192.168.1.20
Dial-In PPP Encryption (MPPE) Optional MPPE	
Mutual Authentication (PAP) 🛛 🔿 Yes 💿 No	
Username	
Password	

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN IKE/IPSec General Setup	
Dial-in Set up for Remote Dial-in user:	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, bu	t will not be encrypted.
High (ESP) 🛛 🗹 DES 🔽	3DES 🔽 AES
Data will be encrypted and	d authentic.

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name Branch1	Call Direction ③ Both 〇 Dial-Out 〇 Dial-in
VPN Dial-Out Through WAN1 First V Netbios Naming Packet O Pass O Block Multicast via VPN O Pass O Block (for some IGMP,IP-Camera,DHCP Relayetc.)	Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP

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

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

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 👻
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> 9	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	••••
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 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.509 None IPSec Security Method Medium(AH) High(ESP) DES) 3DES ☑ AES

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

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	9)
or Peer ID	None 😪	
	IPSec Security Method	
	Medium(AH)	
	High(ESP) 🗹 DES 🔽	3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

4. TCP/IP Network Setting	IS		
My WAN IP	0.0.0.0	RIP Direction	Disable 🖌
Remote Gateway IP	0.0.0.0	From first subnet to remo	te network, you have to
Remote Network IP	192.168.2.0		Route 💌
Remote Network Mask	255.255.255.0		
Local Network IP	192.168.1.1	Change default route single WAN supports this	to this VPN tunnel (Only)
Local Network Mask	255.255.255.0		,
	More		
	ОК	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 V	(When DHCP Disable set)	
Authentication	Assigned IP range	192.168.2 200
Dial-In PPP Encryption (MPPE) Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec Genera	al Setup
VPN IKE/IPSec General Setup	
Dial-in Set up for Remote Dial-in users a	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 v	will not be encrypted.
High (ESP) 🔽 DES 💌 3	DES 🔽 AES
Data will be encrypted and a	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 O Pass O Block Multicast via VPN O Pass O Block (for some IGMP,IP-Camera,DHCP Relayetc.)	Call Direction Both Dial-Out Dial-in Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP

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

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

2. Dial-Out Settings

Type of Server I am calling	Link Type	64k bps 😽
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	Setup:

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

Type of Server I am calling	Link Type	64k bps 💉
• РРТР	Username	draytek
O IPSec Tunnel	Password	••••
C L2TP with IPSec Policy None	PPP Authentication	
	VJ Compression	💿 On 🔘 Off
ial Number for ISDN or erver IP/Host Name for VPN.	IKE Authentication Meth	od
such as 5551234, draytek.com or 123.45.67.89)	Pre-Shared Key	
220.135.240.208	IKE Pre-Shared Key	
	 Digital Signature(X. 	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:
		,

Vigor3200 Series User's Guide

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

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

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP IPSec Tunnel L2TP with IPSec Policy None	Username Password VJ Compression	???
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID	IKE Authentication Method ♥ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.505 None ♥ IPSec Security Method ♥ Medium(AH) High(ESP) ♥ DES ♥	

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

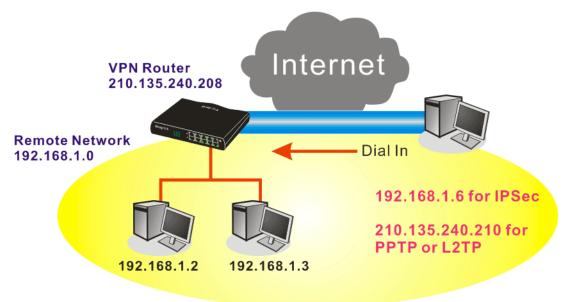
3. Dial-In Settings		
Allowed Dial-In Type		
✓ РРТР	Username	draytek
🔲 IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
	IKE Authentication Method	
 Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID 	Pre-Shared Key KE Pre-Shared Key Digital Signature(X.509 None))
	IPSec Security Method ✓ Medium(AH) High(ESP) ✓ DES ✓	3DES 🗹 AES

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Setting	\$			
My WAN IP	0.0.0.0	RIP Direction	Disable 💌	
Remote Gateway IP	0.0.0.0	From first subnet to remo	te network, you have to	
Remote Network IP	192.168.1.0		Route 🔽	
Remote Network Mask	255.255.255.0			
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				

3.8 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

- 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			Address Assignme	sers
Dial-In PPP Authentication			ien DHCP Disable igned IP range	.168.1.200
Dial-In PPP Encryption (MPPE) Optional	MPPE	~	5 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 **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.



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

VPN and Remote Access >> Remote Dial-in User

VPN IKE/IPSec General Setup

Dial-in Set up	for Remote	Dial-in users	and Dynamic	IP Client ((LAN to LAN).
----------------	------------	---------------	-------------	-------------	---------------

IKE Authentication Method		
Pre-Shared Key		
Confirm Pre-Shared Key	••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, b	ut will not be encrypted.	
High (ESP) 🛛 🗹 DES 🛛	🗹 3DES 🛛 AES	
Data will be encrypted a	nd authentic.	
	OK Cancel	

- 3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
- 4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

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

User account and Authentication Enable this account	Username ???
Idle Timeout 300 second(s)	Password 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 Remote Client IP or Peer ISDN Number or Peer ID	IKE Pre-Shared Key Digital Signature(X.509) None
Netbios Naming Packet 💿 Pass 🔘 Block	IPSec Security Method
Multicast via VPN O Pass O Block (for some IGMP,IP-Camera,DHCP Relayetc.)	 ✓ Medium(AH) High(ESP) ✓ DES ✓ 3DES ✓ AES
Subnet	
Assign Static IP Address	

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

VPN and Remote Access >> Remote Dial-in User

Index No. 1		
User account and Authentication	Username ???	
🔲 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	-
	🗹 Pre-Shared Key	
Specify Remote Node	IKE Pre-Shared Key	
Remote Client IP or Peer ISDN Number	Digital Signature(X.509)	
	None 🗸	
or Peer ID		_
Netbios Naming Packet 💿 Pass 🔘 Block	IPSec Security Method	
Multicast via VPN 🔷 Pass 📀 Bluck	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		
OK	Clear Cancel	

Settings in the remote host:

- 1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.DrayTek.com download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0**. **Configure** button. Reboot the host.

🔽 Smart YPN Client 3.2.2 (WinXP)
Step 0. This step will add the ProhibitIpSec registry value to computer in order to configure a L2TP/IPSec connection using a pre-shared key or a L2TP connection. For more infomation, please read the article Q240262 in the Microsoft Knowledgement Base.
Configure
Step 1. Dial to ISP If you have already gotten a public IP, you can skip this step.
Dial
Step 2. Connect to VPN Server
Connect
Insert Remove Setup
Status: No connection PPTP ISP @ VPN @

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

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

Dial To VPN					
Session Name:	Office				
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)				
192.168.1.1					
User Name : draytek_user1					
Password :	yokokokokok				
Type of VPN					
○ РРТР	O L2TP				
⊙ IPSec Tunne	OL2TP over IPSec				
PPTP Encryption					
No encryptio					
	Require encryption				
O Maximum strength 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.

IPSec Policy Setti	ng	
My IP : Type of IPSec —	172.16.3.100	0 💌
🔘 Standard IPS	iec Tunnel	
Remote Su	bnet :	0,0,0,0
Remote Su	bnet Mask :	255 . 255 . 255 . 0
💿 Virture IP	Dray1	Tek Virture Interface 🛛 🗸
	n IP address a an IP address	automatically (DHCP over IPSec)
IP Addr	ess:	192 . 168 . 1 . 201
Subnet	Mask:	255 . 255 . 255 . 0
Security Method Medium(AH)	0	High(ESP)
MD5	~	DES 💌
Authority Method		
Pre-shared K	ey: *****	
 Certification 	Authority:	
		Browse
0	ĸ	Cancel

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



then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

Dial To VPN					
Session Name:	office				
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)				
192.168.1.1					
User Name :	draytek_user1				
Password :	****				
Type of VPN					
PPTP	O L2TP				
O IPSec Tunnel	OL2TP over IPSec				
PPTP Encryption					
O No encryption					
Require encr					
O Maximum strength encryption					
Use default ga	ateway on remote network				
ОК	Cancel				

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

3.9 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>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	<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	<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 ith

- WAN Outbound BOTH
- 3. Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service		
WAN1 General Setup		
Enable the QoS Control BOTH 💌		_
WAN Inbound Bandwidth	10000 Kbps	
WAN Outbound Bandwidth	10000 Kbps	
	ust be smaller than the real bandwidth t suggested to set the bandwidth value for	
inbound/outbound as 80% - 85% of ph	ysical network speed provided by ISP to	0
maximize the QoS performance.		

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

iss ma	ex#1				
me	E-mail				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ()	Inactive	Any	Any	ANY	undefined
		1	Add Edit Delete	9	

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

WAN1 General Setup		
Enable the QoS (Control BOTH 🛩	
WAN	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	25 %
Enable UDP Band	lwidth Control	Limited_bandwidth Ratio 25 9
Outbound TCP A	CK Prioritize	Online Statistic

Return to previous page. Enter the Name of Index Class 2 by clicking Edit link. In this index, the user will set reserved bandwidth for HTTPS. And click OK.
 Bandwidth Management >> Quality of Service

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

7. Click **Setup** link for one of the WAN interface.

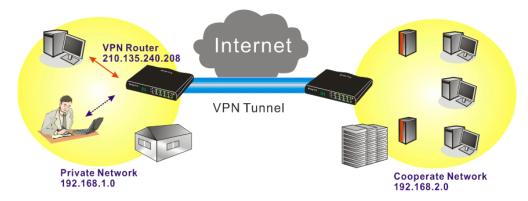
Bandwidth Management >> Quality of Service

General Setup <u>Set to Factory Defa</u>									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	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
Class R Ind			Name					Rule	Service	Гуре
Class	s 1		E-mail					<u>Edit</u>		
Class	s 2		HTTPS					<u>Edit</u>	<u>Edit</u>	
Clas	s 3							Edit		

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

Bandwidth Managem	ent >> Quality of Service	
WAN1 General Setu Enable the QoS		
WAI	N Inbound Bandwidth	10000 Kbps
WAI	N Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
Enable UDP Ban	dwidth Control	Limited_bandwidth Ratio 25 %
Outbound TCP	ACK Prioritize	Online Statistics
2	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

ne \	/PN			D!//0	
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.

ACT	Hardware Acceleration
Local Address	Any
Remote Address	Any
DiffServ CodePoint	IP precedence 2
Service Type	SYSLOG(UDP:514)
Note: Please choose/set	tup 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**.

3.10 Upgrade Firmware for Your Router

Using Firmware Upgrade Utility

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Go to www.DrayTek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products	Support	Education	Partners	Contact U
ome > Support > Download	S					
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	elease Date		Firmware	
Vigor120 series	3.2.2.1	26/06/2009			Driver	
Vigor2100 series	2.6.2	26/02/2008			Utility	
Vigor2104 series	2.5.7.3	13/02/2008			Utility Introduction	
Vigor2110 series	3.3.0	25/06/2009			Datasheet	
Vigor2200/X/W/E	2.3.11	22/09/2004			R&TTE Certification	
Vigor2200Eplus	2.5.7	18/02/2009				
Vigor2200USB	2.3.10	1	6/03/2005			

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

	About I	DrayTek Prod	ucts	Support	Education	Partners	Contact Us
ility							
						Downlo	ads
Release Date	Version	OS	DS Support Model		Model	Firmware	
2009/06/18	4.2.0	MS-Windows		All Mod	ules	Diana	
2009/06/18	4.2.0		(P	All Mod	ules		
2009/06/03	1.1.0		(P	VigorPro 10	0 series		troduction
	(Multi- language)	MS-Vista	2		Datasheet		
				VigorPro 53	00 series	R&TTE C	ertification
2009/05/25	3.6.3	MS-Windows)	(P	All Mod	ules		
	(Multi- language)	MS-Vista					
2009/03/25	2.0	MS-Windows)	(P	-			
	Release Date 2009/06/18 2009/06/18 2009/06/03 2009/05/25	Version 2009/06/18 4.2.0 2009/06/18 4.2.0 2009/06/03 1.1.0 (Multi- language) (Multi- language)	Iity OS Release Date Version OS 2009/06/18 4.2.0 MS-Windows 2 2009/06/18 4.2.0 MS-Windows 2 2009/06/03 1.1.0 MS-Windows 2 (Multi- language) MS-Vista MS-Vista 2009/05/25 3.6.3 MS-Windows 2 (Multi- language) MS-Vista MS-Vista	Release Date Version OS 2009/06/18 4.2.0 MS-Windows 2009/06/18 4.2.0 MS-Windows XP 2009/06/03 1.1.0 MS-Vista 2009/06/03 1.1.0 MS-Vindows XP (Multi- language) MS-Vista 2009/05/25 3.6.3 MS-Windows XP Multi- language) MS-Vista	Iity OS Support I 2009/06/18 4.2.0 MS-Windows All Mod 2009/06/18 4.2.0 MS-Windows XP All Mod 2009/06/18 4.2.0 MS-Windows XP All Mod 2009/06/18 4.2.0 MS-Windows XP All Mod 2009/06/18 1.1.0 MS-Windows XP VigorPro 100 (Multi- language) MS-Vista VigorPro 550 2009/05/25 3.6.3 MS-Windows XP All Mod (Multi- language) MS-Vista All Mod 2009/05/25 3.6.3 MS-Vista All Mod (Multi- language) MS-Vista Vigor250	Release Date Version OS Support Model 2009/06/18 4.2.0 MS-Windows All Modules 2009/06/18 4.2.0 MS-Windows XP All Modules 2009/06/03 1.1.0 MS-Windows XP VigorPro 100 series (Multi- language) MS-Vista VigorPro 5500 series 2009/05/25 3.6.3 MS-Windows XP All Modules	Iity Downlo Release Date Version OS Support Model 2009/06/18 4.2.0 MS-Windows All Modules 2009/06/18 4.2.0 MS-Windows XP All Modules 2009/06/18 4.2.0 MS-Vista Driver 2009/06/18 4.2.0 MS-Vindows XP All Modules 2009/06/03 1.1.0 MS-Vindows XP VigorPro 100 series (Multi- MS-Vista VigorPro 5510 series Utility In 2009/05/25 3.6.3 MS-Vindows XP All Modules (Multi- MS-Vista Balashee (Multi- MS-Vista Image P 2009/05/25 3.6.3 MS-Vindows XP All Modules (Multi- MS-Vista Image P 2009/05/25 2.0 MS-Windows XP Vigor2950 series

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the icon of router tool. The setup wizard will appear.



- 6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 7. From the Start menu, open Programs and choose Router Tools XXX >> Firmware Upgrade Utility.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port	Firmware file:	
69		
Password:	Abort	Send

- 8. Type in your router IP, usually **192.168.1.1**.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

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

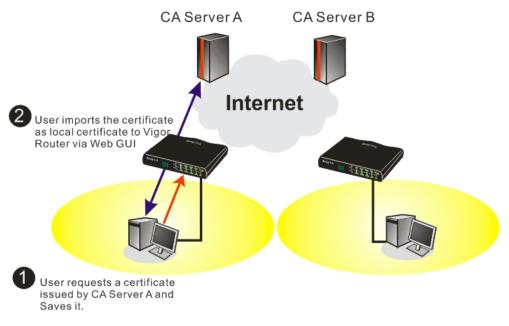
- 1. Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.DrayTek.com (or local DrayTek's web site) and FTP site is <u>ftp.DrayTek.com</u>.
- 2. Click System Maintenance>> Firmware Upgrade.

System Maintenance >> Firmware Upgrade	
Web Firmware Upgrade	
Select a firmware file. Click Upgrade to upload the file.	Browse
TFTP Firmware Upgrade from LAN	
Current Firmware Version: 3.3.6_RC5	
Firmware Upgrade Procedures:	
 Click "OK" to start the TFTP server. Open the Firmware Upgrade Utility or other 3 Check that the firmware filename is correct. Click "Upgrade" on the Firmware Upgrade Utili After the upgrade is compelete, the TFTP server. 	ty to start the upgrade.
Do you want to upgrade firmware ? OK	

3. Select a firmware file by clicking **Browse**.

Click **Upgrade** to perform the firmware upgrade.

3.11 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 C	Certificate		
			<u>^</u>
			~

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

Certificate Management >> Local Certificate

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 🗸	
	Generate	

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

IMPORT REFRESH X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDA0BgNVBAoTB0RYX102WsxIDAe BgkqhkiG9w0BCQEWEXByZXN2QGRYYX102WsuY29tMIGfMA0GCSqGSIb3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWknIdHblo1kt9cTdLUDaFk6s8d 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg4lg26Qk/rGhuVTKd9j6PlcrnkP7 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2R2jKRMaHEWpVpwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kF1zTJiHh uRq4C1E16nV4hMRytcx2pE26sMarSgREr86R003UX0145560xC2/N1Gh9VQ911 l9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	Name	Subject	Status	Modify
X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAKGA1UEBhMCVFcxEDAOBgNVBAoTBORyYX102WsxIDAe BgkqhkiG9w0BCQEWEXByZXNzQGRyYX102WsuY29tMIGfMAOGCSqGSIb3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDEWknIdHblo1kt9cTdLUDaFk6s8d 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg4lg26Qk/rGhuVTKd9j6PlcrnkP7 du84t23tWBdM04W5c8VmSyDjShLhjdxVYPWpNKVIr0T2R2jkRMaHEWpVpwIDAQAB oCkwJwYJKo2IhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmf5dGVrLmNvbTANBgkq hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem1tHQbcvjXvg/t7kFlzTJiHh uRLq4C1E16nV4hMRytcxZpEZ6sMarSgREr86Ro08Jx0145560xC2/N1Gh9VQ9I1 I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	Local	/C=TW/O=Draytek/emailAddress	Requesting	View Delete
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTBORyYX10ZWsxIDAe BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWknIdHblo1kt9cTdLUDaFk6s8d 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg41g26Qk/rGhuVTKd9j6PlcrnkP7 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9M6/HwToem1tHQbcwjXvg/t7kFlzTjiHh uRLq4CiEi6nV4hMRytcx2pE26sMarSgREr86Ro08JxOI45560xC2/N1Gh9VQ911 I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	ENERATE X509 Lo			
END CERTIFICATE REQUESI	MIIBqj Bgkqhk A4GNAD 3wDeQy du84t2 oCkwJw hkiG9w uRLq4C I9Fqkj	CCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO iG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t CBiQKBgQDPioahu/gFQaYB1ceSOERSDfWk coV1LBJz2IDF0xjX6ip7ev187twwTsg41g 3tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI YJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN DBAQUFAAOBgQAuSBRUCt4W1hH9N6/HwToe iEi6nV4hMRytcxZpEZ6SMarSgRREr86RoO	MIGfMAOGCSqGS nIdHblo1kt9cT 26Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq t7kFlzTJ1Hh /NIGh9VQ9I1

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**.

'ou use this web site to re	quest a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, yo
vill be able to securely ide lepending upon the type (ntify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more of certificate you request.
Select a task:	
Retrieve the CA cert	ificate or certificate revocation list
Request a certificate	3
OCheck on a pending	certificate

Select Advanced request.

Microsoft Certificate Services vigor	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate	
Advanced request	
Next 2	,

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

	cate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certific ine the certificates that you can obtain.
O Submit a certificate	request to this CA using a form.
Submit a certificate	request 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 the Smart Card Enrollment Station. ment agent certificate to submit a request for another user.
	Next>

Microsoft Certificat	te Services vigor		Home
Submit A Saved	d Request		
		equest or PKCS #7 renewal request generated by an external application (such as a web to the certification authority (CA).)
Saved Request:			
Base64 Encoded Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUE MIIBegicCARECAQAwGTELMAKGAIUE BydghkiGydDGCGEVEXP3ZN2CGRA A4GNADCBIQKBgQDQYB7wmZFfFhM hX4bp89cUF9dloACGGIN/ccBOck X/OBA7CTVO/f02pxrcCW1JTJLSjS CINCTVO/f02pxrcCW1JTJLSjS	EBHCVFcxEDAO YX102WsuY29t /I2QnG03Xk++ /I2QhFFvIXcP3	
ertificate Templa	ite:		
	Administrator 🗸		
Additional Attribut	Administrator Authenticated Session Basic EFS EFS Recovery Agent		
Attributes:	User IPSEC (Offline request) Router (Offline request)	× >	
	Subordinate Certification Authority Web Server	Submit >	>

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and

you will find the below window showing "-----BEGINE CERTIFICATE-----"...." Certificate Management >> Local Certificate

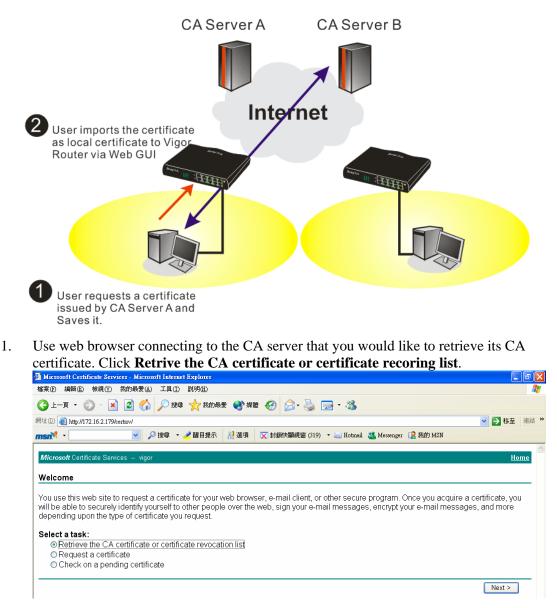
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
GENERATE X509 Lo	IMPORT REFRESH		
MIIBqj Bgkqhk A4GNAD 3wDeQy du84t2 oCkwJw hkiG9w uRLq4C I9Fqkj	EGIN CERTIFICATE REQUEST CCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO iG9w0BCQEWEXByZXNzQGRyYX10ZWauY29t CBiQKBgQDPioahu/gFQaYB1ceSOERSDfWk toV1LBJz1DFOxjX6ip7ev187twwTsg41g 3tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKV1 YJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN DBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToe iEi6nV4hMRytcxZpEZ6sMarSgRREx86RoO JNihip4TCjecSNNZjmQoSWU+Bce8TG+SCB ND CERTIFICATE REQUEST	MIGfMAOGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	SIb3DQEBAQUA CdLUDaFk6s8d A9j6PlcrnkP7 CWpVpwIDAQAB mNvbTANBgkq 't7kFlzTJiHh 2/N1Gh9VQ9I1

6. You may review the detail information of the certificate by clicking **View** button.

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TVWO=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

3.12 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 🌀 上一頁 🔹 💿 · 😰 🟠 🔎 搜尋 🧙 我的最爱 🜒 媒體 🚱 🔗 - 🌺 🔜 • 🆄 網址 (1) 🍓 http://172.16.2.179/certsrv/certcarc.asp msnM -🗸 🔎 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] ○DER encoded or ●Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

Name	Subject	Status	Modify
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

4. You may review the detail information of the certificate by clicking **View** button.

Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

Note: Before setting certificate configuration, please go to **System Maintenance** >> **Time and Date** to reset current time of the router first.

3.13 Creating an Account for MyVigor

The website of MyVigor (a server located on <u>http://myvigor.draytek.com</u>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filter the web pages for protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor first.

3.13.1 Creating an Account via Vigor Router

1. Click **System Maintenance>>Activation** to open the following page.

System Maintenance >> Activation	Activate via interface :	auto-selected 💌
Neb-Filter License 'Status:Not Activated]	Γ	<u>Activate</u>
Authentication Message Activated Wiz, Authenticate is continuously, con	meet to the server, 2000-0	1-01
00:04:55		

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	12 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
1 Agreement	UserName:*	Mary Check Account
	o contraintor,	(3 ~ 20 characters)
Demonst	Password:*	••••
Personal Information		(4 ~ 20 characters : Do not set the same as the username.)
mormation	Confirm Password:*	
	Personal Informat	tion
3 Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	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	I would like to receive DrayTek product news.	V			
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server			
4 Completion		<< Back Continue >>			

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

***** This is an automated message from myvigor draytek.com.*****

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site GO
Register Confirm	
	Thank for your register in VigorPro Web Site The Register process is completed
	Close Login

- 10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.
 - 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
	lf you cannot read t	he word, <u>click here</u>
	Forget pass	sword? Login
Don't have a	MyVigor Account	? Create an account now
If you a	Customer Service	ing in, contact our customer service. : (888) 3 597 2727 or aster@draytek.com

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.

3.13.2 Creating an Account via MyVigor Web Site

1. Access into <u>http://myvigor.draytek.com</u>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.

Dray Tek	MyVig	or		Customer Survey
ft Home	Search	30	Ī	
AL (1)	MyVigor for you		•	Login
About Us Product My Information VigorPro	MyVigor website replaces the VigorPro site as DrayTek's portal site for the latest products and services in network security, including Anti- Virus, Anti-Spam, Web Content Filter etc. The products and functions that are supported in this site include:			UserName Password AuthCode
	VigorPro Unified Security Firewall series:			QbkqVd
	 Activation of CommtouchTM GlobalView Web Content Filter license key Activation of DT Anti-Virus license key Activation of Kaspersky Anti-Virus license key Activation of CommtouchTM Anti-Spam license key and 			If you can't read the AuthCode , <u>click here</u> Login Forget password?
	membership <u>Vigor routers (for models that support Commtouch</u> TM)			Not registered yet ? Click here !
	 Activation of Commtouch[™] GlobalView Web Content Filter license key 			
	The MyVigor website contains a trail version of Commtouch TM GlobalView Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.			
Please use IE 5.0 or above (resolution 1024 * 788) for best display. ☺ DrayTek Corp.	More customer-oriented services are planned for MyVigor site for the near future.	~	•	

2. Check to confirm that you accept the Agreement and click Accept.



3. Type your personal information in this page and then click Continue.

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
	Deenwarkt	(3 ~ 20 characters)
Personal	Password:*	(4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	ion
3 Preferences	First Name:*	Mary
	Last Name:*	Ted
4 Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND
	Career:*	Supervisor 🗸

4. Choose proper selection for your computer and click **Continue**.

Register		
Create an account -	Please enter personal profile.	
Agreement	How did you find out about this website?	Internet
U . groomont	What kind of anti-virus do you use?	AntiVir
2 Personal	I would like to subscribe to the MyVigor e-letter.	V
Information	l would like to receive DrayTek product news.	V
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	
	lf you cannot read the	word, <u>click here</u>	
	Forget passw	vord? Login	
Don't have a	MyVigor Account ?	Create an acc	ount now
		g in, contact our customer serv	

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.

3.14 How can I get the files from USB storage device connecting to Vigor router?

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** If it is necessary for you to delete, copy files on the device or write, paste files to the devcie, it must be done through SAMBA server or FTP server.

Samba service is based on the original USB FTP service. You will need to setup USB FTP first. We would like to give brief instructions on USB FTP setup here.

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

USB Applicati			
USB Mass Sto	rage Device Status		
Write Protec	Status: Disk Connect ct Status: No	ed	Disconnect USB Disk
Disk Capacit Free Capacit	,	<u>1</u>	
USB Disk Use	ers Connected		<u>Refresh</u>
Index	Service	IP Address(Port)	Username

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

2. Then, please open **USB Application >> USB General Settings** to enable Samba service.

USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	Default 💌
Samba Service Settings(Network Neigh	borhood)
Workgroup Name	WORKGROUP
Host Name	Vigor

USB Application >> USB General Settings

Note: 1. If Charset is set to "default", only English long file name is supported.

2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multiconnection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.

3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; : " <> * + = / \ | ?.



3. Setup a user account for the FTP service by using **USB Application** >>**USB User Management.** Click **Enable** to enable FTP/Samba User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

FTP/Samba User	💿 Enable 🔘 Disable
Username	user1
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	/ 🧭
Access Rule	
File	🛛 🖉 Write 🗌 Delete
Directory	☑ List □ Create □ Remove
The folder name can only (contain the following characters: A-Z a-z O-9 % ' @ ~ ` ! ()
and space.	

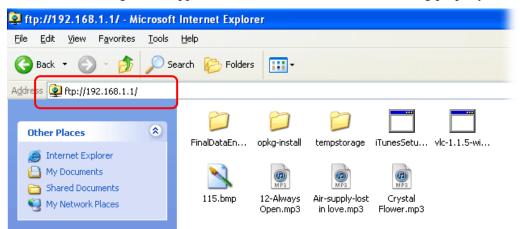
USB Application >> USB User Management

Click **OK** to save the configuration.

4. Make sure the FTP service is running properly. Please open a browser and type <u>ftp://192.168.1.1</u>. Use the account "**user1**" to login.

Log On	As 🔀
۴	Either the server does not allow anonymous logins or the e-mail address was not accepted.
	FTP server: 192.168.1.1
	User name:
	Password:
	After you log on, you can add this server to your Favorites and return to it easily.
Æ	FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.
	Learn more about <u>using Web Folders</u> .
	Log on anonymously

5. When the following screen appears, it means the FTP service is running properly.



6. Return to **USB Application** >> **USB Disk Status**. The information for FTP server will be shown as below.

USB Application >> USB Disk Status

Connection Status: Disk Connected Disconnect USB Disk						
Write Prot	ect Status: No					
Disk Capac	ity: 2009 MB					
Free Capa	city: 1664 MB <u>R</u>	<u>efresh</u>				
USB Disk U	sers Connected		1	<u>Refresh</u>		
Index	Service	IP Address(Port)	Username			
Index 1.	Service FTP	IP Address(Port) 192.168.1.11(3343)	Username user1	Drop		

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

 Now, users in LAN of Vigor3200 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in USB Application >>USB User Management.

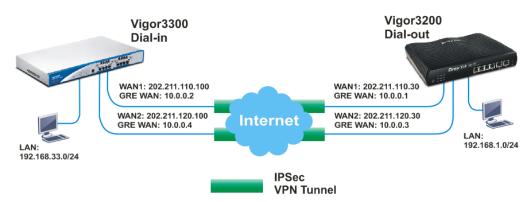
Vigor3200 Series User's Guide

3.15 VPN Trunk Load-Balance between Vigor 3200 and Other Vigor Router

This section will discuss how to build VPN Trunk with load-balance between Vigor3200 and other router (e.g., Vigor3300).

Scenario 1: One-pair VPN Trunk

The purpose is to setup a VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24).



At present, Vigor3200 just supports one VPN trunk group with two members for the same VPN network pair. In this case, the VPN trunk is built for 192.168.1.0/24 <-> 192.168.33.0/24. In other word, although Vigor3200 supports 4 WAN connections, it just allows you to use 2 VPN connections over two WAN ports for one VPN trunk group between the networks 192.168.1.0/24 and 192.168.33.0/24.

Note:

- You can still setup two VPN trunk groups over 4 WAN connections between the networks 192.168.1.0/24 and 192.168.33.0/24. But the VPN traffic can just pass through one VPN trunk group.
- You can create arbitrary number of VPN trunk groups between Vigor3200 and Vigor3300 for different VPN network pairs. For example, suppose there is another network (192.168.10.0/24) behind Vigor3300. You may create a VPN trunk group over WAN1 and WAN2 connections for 192.168.1.0/24 <-> 192.168.33.0/24, and the other VPN trunk group over WAN3 and WAN4 for 192.168.1.0/24 <-> 192.168.1.0/24 <-> 192.168.1.0/24. Please refer to the Scenario 2 described in this document later.

Vigor3200 as a VPN client (dial out site),

LAN: 192.168.1.0/24 WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2) WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4)

Vigor3300 as a VPN server (dial in site),

LAN: 192.168.33.0/24 WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1) WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3)



Settings for Vigor 3200:

1. Open VPN and Remote Access>>>LAN to LAN. Choose Index number 1 for configuring a VPN LAN to LAN profile.

VPN and Remote Access >> LAN to LAN

AN-to-LAN Profiles: Set to Factory Defat					
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	×	<u>17.</u>	???	×
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	×

2. In the following page, please configure the settings as the following figure.

VPN and Remote Access >> LAN to LAN

Profile Index : 1 1. Common Settings	
	Call Direction C Both © Dial-Out © Dial-in
Profile Name wani only	Call Direction O Both O Dial-Out O Dial-in
💌 Enable this profile	Idle Timeout -1 second(s)
VPN Dial-Out Through WAN1 Only -	Enable PING to keep alive
Netbios Naming Packet Pass Delock	PING to the IP
Multicast via VPN O Pass O Block	
(for some IGMP, IP-Camera, DHCP Relayetc.)	
2. Dial-Out Settings	1
Type of Server I am calling	Username ???
O PPTP	Password
IPSec Tunnel	PPP Authentication PAP/CHAP
C L2TP with IPSec Policy None	VJ Compression © On © Off
Server IP/Host Name for VPN.	IKE Authentication Method
(such as draytek.com or 123.45.67.89)	Pre-Shared Key
202. 211. 110. 100	IKE Pre-Shared Key
	O Digital Signature(X.509)
	Peer ID None
	Local ID
	Alternative Subject Name First
	C Subject Name First
	Local Certificate None 💌
	IPSec Security Method
	C Medium(AH)
	High(ESP) DES without Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:
3. Dial-In Settings	
Allowed Dial-In Type	Username
🕅 РРТР	Password
IPSec Tunnel	VJ Compression @ On @ Off
L2TP with IPSec Policy None	IKE Authentication Method
Specify Remote VPN Gateway	🖾 Pre-Shared Key
Peer VPN Server IP	IKE Pre-Shared Key
	Digital Signature(X.509)
or Peer ID	None 💌
	Local ID
	C Alternative Subject Name First
	O Subject Name First
	IPSec Security Method
	Medium(AH)
	High(ESP) 🕅 DES 🕅 3DES 🕅 AES
4. Gre over IPSec Settings	
☑ Enable IPSec Dial-Out function GRE over IPSec	
Logical Traffic My GRE IP 10.0.0.1	Peer GRE IP 10.0.0.2
5. TCP/IP Network Settings	
My WAN IP 0.0.0.0	RIP Direction Disable
Remote Gateway IP 0.0.0.0	From first subnet to remote network, you have to
Remote Network IP 192.168.33.0	do
Remote Network IP 192. 168. 33. 0 Remote Network Mask 255. 255. 255. 0	
	do Route 💌
Remote Network Mask 255. 255. 255. 0	do

3. Click **OK** to save the configuration and return to previous page. Choose Index number **2** for configuring another VPN LAN to LAN profile.

VPN and Remote Access >> LAN to LAN					
AN-to-LAN Profiles: Set to Factory Default					
Index	Name	Status	Index	Name	Status
<u>1.</u>	wan1 only	×	<u>17.</u>	???	×
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	×

4. In this page, please configure the settings as the following figure.

/PN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name wan2 only	Call Direction C Both O Dial-Out C Dial-in
Enable this profile	Always on
	Idle Timeout
VPN Dial-Out Through WAN2 Only 💌	Enable PING to keep alive
Netbios Naming Packet 💿 Pass 🔿 Block	PING to the IP
Multicast via VPN C Pass 💿 Block	
(for some IGMP, IP-Camera, DHCP Relayetc.)	
2. Dial-Out Settings	
Type of Server I am calling	Username ???
Орртр	Password
IPSec Tunnel	PPP Authentication PAP/CHAP
C L2TP with IPSec Policy None	VJ Compression © On © Off
Common ID Allock Monte Fee LIDM	IKE Authentication Method
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	Pre-Shared Key
202. 211. 120. 100	IKE Pre-Shared Key
	C Digital Signature(X.509)
	Peer ID None
	Local ID
	C Alternative Subject Name First
	C Subject Name First
	Local Certificate None 💌
	IPSec Security Method
	C Medium(AH) G High(ESP) DES without Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:
3. Dial-In Settings	
Allowed Dial-In Type	Username
	Password
	VJ Compression © On © Off
L2TP with IPSec Policy None	IKE Authentication Method
Creatify Remote VRN Category	Pre-Shared Key
Specify Remote VPN Gateway Peer VPN Server IP	IKE Pre-Shared Key
	Digital Signature(X.509)
or Peer ID	None 💌
	Local ID
	C Alternative Subject Name First
	O Subject Name First
	IPSec Security Method
	Medium(AH) High(ESP) M DES M 3DES M AES
4. Gre over IPSec Settings	Medium(AH)
4. Gre over IPSec Settings ☞ Enable IPSec Dial-Out function <u>GRE over IPSec</u>	I Medium(AH) High(ESP) I DES I 3DES I AES
	I Medium(AH) High(ESP) I DES I 3DES I AES
Enable IPSec Dial-Out function GRE over IPSec Logical Traffic My GRE IP 10.0.0.3	Medium(AH) High(ESP) MEDES ME3DES MEAES
 ✓ Enable IPSec Dial-Out function GRE over IPSec □ Logical Traffic My GRE IP 10.0.0.3 	Medium(AH) High(ESP) MEDES ME3DES MEAES
Enable IPSec Dial-Out function <u>GRE over IPSec</u> Logical Traffic My GRE P 10.0.0.3 5. TCP/IP Network Settings	Medium(AH) High(ESP) DES 3DES AES Peer GRE IP[10.0.0.4] RIP Direction Disable From first subnet to remote network, you have to
Image: Production Content France Logical Traffic My GRE Image: Production Content Production Image: Product Traffic Production Image: Product Traffic Production Image: Product Traffic Production Image: Product Traffic Product Traffic Image: Product Traffic Product Traffic <	Medium(AH) High(ESP) DES 3DES AES Peer GRE IP 10.0.0.4 RIP Direction Disable From first subnet to remote network, you have to do
Image: Project Dial-Out function GRE over IPSec Logical Traffic My GRE P 10.0.0.3 5. TCP/IP Network Settings My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 192.168.33.0	Medium(AH) High(ESP) DES Peer GRE IP IO RIP Direction Pisable From first subnet to remote network, you have to
Image IPSec Dial-Out function GRE over IPSec Logical Traffic My GRE P 10.0.0.3 5. TCP/IP Network Settings My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 192.168.33.0 Remote Network Mask 255.255.0	Image: Medium(AH) High(ESP) Image: DES Image: 3DES Image: AES Peer GRE IP 10.0.0.4 Image: AES RIP Direction Disable Image: AES From first subnet to remote network, you have to do Image: AES Image: AES Route Image: AES Image: AES Image: AES
Image: Project Dial-Out function GRE over IPSec Logical Traffic My GRE P 10.0.0.3 5. TCP/IP Network Settings My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 192.168.33.0	Image: Medium(AH) High(ESP) Image: Des Image: Base image:

- 5. Click **OK** to save the configuration.
- 6. Open **VPN and Remote Access>>VPN TRUNK Management**. Add these VPN profiles to the VPN Trunk and set **Load Balance** as the **Attribute Mode**.

L	Load Balance Profile List Set to Factory Defa					
Γ	Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at pre			er Dial-In(Call Direction) at present.		
	No.	Status	Name	Member1(Active)Type	Member2(Active)Type	-
	1	v	wan1wan2	1(YES)IPSec	2 (YES) IPSec	
1						
						-
	Adva	anced	wan1wan2 💌			

General Setup

Status Profile Name	C Enable C Disable	
Member1	Please select a LAN-to-LAN Dial-Out profile.	•
Member2	Please select a LAN-to-LAN Dial-Out profile.	•
Active Mode	C Backup 💿 Load Balance	
	Add Edit Delete	

7. Click Advanced for specifying Load Balance Algorithm.

Profile Name: Trunk1		
.oad Balance Algorithm:	Round Robin	
	C Weighted Round	Robin
	Auto Weight	
		to Speed Ratio (Member1:Member2): 50:50 💌
	C Fastest	
/PN Load Balance - Binding	g Tunnel Policy	
	⊙ Create O Afte	er insert
Funnel Bind Table Index:	(1~400)	
Active:	In-active/Delete 💌	
Binding Dial Out Index:	1 💌	
Binding Src IP Start:	0.0.0.0	End: 0.0.0.0
Binding Dest IP Start:	0.0.0.0	End: 0.0.0.0
Binding Dest Port Start:	1	End: 65535
Binding Fragmented:	NO 💌	Binding Protocol: ANY 🗾 🛛
	OK	Close
tail Information		
VPN Load Balance Prof:	ile nemer Terrilet 1	
Algorithm: Round Robin	SABL sentences on a success of the	

8. When the VPN trunk is successfully connected, you may check the connection status by viewing the page of **VPN and Remote Access>>Connection Management**. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.

)ial-out Tool					Refr	esh S	econds :	10 💌 F	lefresh
	Gen	eral Mode:			-] Di	.al		
	Back	up Mode:			•]Di	ial		
	Load Balan	ice Mode: (wai	n1wan2) 202.2	11.11	0.100 💌	Di	ial		
		(war	1wan2) 202.2	11.110	0.100				
/PN Connect Current Page		· · ·	11wan2) 202.2 11wan2) 202.2				Page No.	Go	>>
		· · ·	· · ·	11.120 Tx		Rx Pkts	Rx	UnTime	>>
Current Page	: 1 Type IPSec Tunnel	(war	11wan2) 202.2 Virtual Network	11.120 Tx Pkts	0.100 Tx		Rx	UnTime	Drop

VPN and Remote Access >> Connection Management

xxxxxxxx : Data isn't encrypted.

Settings for Vigor3300:

1. Open VPN>>IPSec>>VPN Trunk>>Policy Table. Choose Index 1 and click Edit.

#		Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	۲							
2	0							
3	0							
4	\circ							
5	0							
6	0							
7	0							
8	0							
9	0							
10	0							

2. In this page, please configure the settings as the following figure.

VPN - IPSec - V	PN Trunk - Policy Table - Edit
Default	Advanced
Basic	
Profile Status :	Enable 💌
Name :	wan1
Authentication :	Preshared Key
Preshared Key :	
Security Protocol :	ESP -
NAT Traversal :	Enable
Local Gateway	
WAN Interface :	WAN1 -
Local Certificate :	V
Security Gateway :	default
Local GRE IP :	10. 0. 0. 2
Next hop :	default
Remote Gateway	
Remote ID :	
Security Gateway :	0.0.0.0 ('0.0.0.0' for dynamic client)
Remote GRE IP :	10. 0. 0. 1

- 3. Click **Apply** to save the configuration and return to previous page. Choose Index **2** for configuring another VPN Trunk policy.
- 4. In this page, please configure the settings as the following figure.

VPN - IPSec - V	PN Trunk - Policy Table - Edit
Default	Advanced
Basic	
Profile Status :	Enable 💌
Name :	wan2
Authentication :	Preshared Key 💌
Preshared Key :	
Security Protocol :	ESP 💌
NAT Traversal :	Enable
Local Gateway	
WAN Interface :	WAN2 💌
Local Certificate :	
Security Gateway :	default
Local GRE IP :	10. 0. 0. 4
Next hop :	default
Remote Gateway	
Remote ID :	
Security Gateway :	0.0.0.0 ('0.0.0.0' for dynamic client)
Remote GRE IP :	10. 0. 0. 3

- 5. Click **Apply** to save the configuration.
- 6. Open **VPN>>VPN Trunk>>Group Table** to group these two VPN policies.

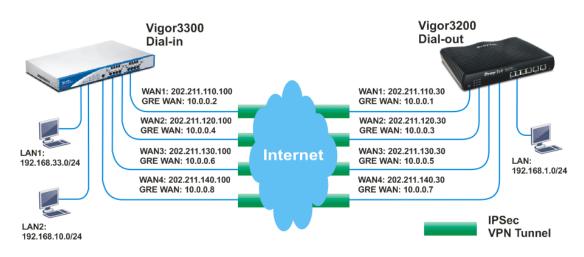
¥	Profile Status	Name	Local Subnet	Remote Subnet
	۲			
2	0			
	0			
	0			
	0			
	0			
	0			
	0			
	0			
0	0			

7. Choose Index 1 and click **Edit**. Add these two VPN profiles (wan1 and wan2) to a VPN Trunk.

VPN - VPN Trur	nk - Group Table - Edit
1	
Profile Status :	O Disable 💿 Enable
Name :	192.168.33.0
Local Subnet :	192.168.33.0 / 24
Remote Subnet :	192.168.1.0 / 24
Tunnel 1 :	wan1 Veight: 50
Tunnel 2 :	wan2 Veight: 50
Tunnel 3 :	Veight:
Tunnel 4 :	VVeight :
Backup	
Active	Master Slave
	•

Now, one-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.

Scenario 2: Two-pair VPN Trunk



Vigor3200 as VPN client (dial out site)

LAN: 192.168.1.0/24

WAN 1 IP: 202.211.110.30 (My GRE IP, 10.0.0.1, Peer GRE IP, 10.0.0.2) WAN 2 IP: 202.211.120.30 (My GRE IP, 10.0.0.3, Peer GRE IP, 10.0.0.4) WAN 3 IP: 202.211.130.30 (My GRE IP, 10.0.0.5, Peer GRE IP, 10.0.0.6) WAN 4 IP: 202.211.140.30 (My GRE IP, 10.0.0.7, Peer GRE IP, 10.0.0.8)

Vigor3300 as VPN server (dial in site),

LAN1: 192.168.33.0/24 LAN2: 192.168.10.0/24 WAN 1 IP: 202.211.110.100 (Local GRE IP, 10.0.0.2, Remote GRE IP, 10.0.0.1) WAN 2 IP: 202.211.120.100 (Local GRE IP, 10.0.0.4, Remote GRE IP, 10.0.0.3) WAN 3 IP: 202.211.130.100 (Local GRE IP, 10.0.0.6, Remote GRE IP, 10.0.0.5) WAN 4 IP: 202.211.140.100 (Local GRE IP, 10.0.0.8, Remote GRE IP, 10.0.0.7)

Settings for Vigor 3200:

- 1. Open VPN and Remote Access>>>LAN to LAN.
- 2. Create LAN to LAN profile 1-4. Setting configuration is the same as Scenario 1. The differences are, Remote Network IP of Profile 1 and Profile 2 must be 192.168.33.0/24 and Remote Network IP of Profile 3 and Profile 4 must be 192.168.10.0/24.

AN-to-LAN Pr	ofiles:			Set to Fa	<u>ctory Default</u>
Index	Name	Status	Index	Name	Status
<u>1.</u>	wan1 only	V	<u>17.</u>	???	Х
<u>2.</u>	wan2 only	V	<u>18.</u>	???	Х
<u>3.</u>	wan3 only	V	<u>19.</u>	???	Х
<u>4.</u>	wan4 only	V	<u>20.</u>	???	Х
<u>5.</u>	???	×	<u>21.</u>	???	Х
<u>6.</u>	???	×	<u>22.</u>	???	×
<u>7.</u>	???	×	<u>23.</u>	???	Х
<u>8.</u>	???	×	<u>24.</u>	???	×
<u>9.</u>	???	×	<u>25.</u>	???	Х
<u>10.</u>	???	Х	<u>26.</u>	???	×
<u>11.</u>	???	Х	<u>27.</u>	???	Х
<u>12.</u>	???	Х	<u>28.</u>	???	×
<u>13.</u>	???	×	<u>29.</u>	???	Х

3. Open VPN and Remote Access>>VPN TRUNK Management. Add these VPN profiles to the VPN Trunk and set Load Balance as the Attribute Mode. Setting configuration is the same as Scenario 1. Profile 1 and Profile 2 are one pair; Profile 3 and Profile 4 are the other pair.

lote: [Ac	tive:NO] The LA	N-to-LAN Profile is disabled or u	nder Dial-In(Call Direction) at presen	
No. Sta	tus Name	Member1(Active)Type	Member2(Active)Type	
1 v	wan1wan2	1(YES)IPSec	2(YES)IPSec	
2 v	wan3wan4	3(YES)IPSec	4(YES)IPSec	

General Setup

Status	© Enable C Disable	
Profile Name		
Member1	Please select a LAN-to-LAN Dial-Out profile.	
Member2	Please select a LAN-to-LAN Dial-Out profile.	
Active Mode	☉ Backup C Load Balance	
	Add Edit Delete	

4. When the VPN trunk is successfully connected, you may check the connection status by viewing the page of VPN and Remote Access>>Connection Management. Transferred packets (Tx Pkts) will keep increasing through both tunnels when outgoing packets sent to the remote VPN network.

Dial-out Tool Refresh Seconds : 10 💌 Refresh • General Mode: Dial • Backup Mode: Dial Load Balance Mode: (wan1wan2) 202.211.110.100 -Dial (wan1wan2) 202.211.110.100 **VPN Connection Status** (wan1wan2) 202.211.120.100 (wan3wan4) 202.211.130.100 \rightarrow Go Current Page: 1 Page No. (wan3wan4) 202.211.140.100 Rx Rx VPN Remote IP UpTime Type Network Pkts Rate(Bps) Pkts Rate(Bps) 202.211.110.100 192.168.33.0/24 3393 IPSec Tunnel DES-No Auth 1 (wan1 only) 1:53:18 Drop 24 6800 60 IPSec Tunnel 202.211.120.100 192.168.33.0/24 3753 2:2:30 Drop 39 137 3 (wan2 only) DES-No Auth via WAN2 IPSec Tunnel DES-No Auth 202.211.130.100 via WAN3 192.168.10.0/24 3630 39 7213 60 2:2:28 Drop (wan3 only) IPSec Tunnel DES-No Auth 202.211.140.100 192.168.10.0/24 3583 4 (wan4 only) 0 0 2:2:19 Drop 24 xxxxxxxx : Data is encrypted.

VPN and Remote Access >> Connection Management

xxxxxxxx : Data isn't encrypted.

Settings for Vigor3300:

1. Open Advanced>>LAN VLAN. Choose the tab of 802.1Q VLAN. Configure the settings as the following figure.

C Disa	ble C Po	irt Base VLAN	€ 802.1Q VLA	N											
Port E	Base VLA	N 802.	1Q VLAN												
Group															
Index	Active	Name	VLAN ID		Mer	nber				Fram	e Tag	Operation			
				P1	P2	P3	P4	P1		P2		P3		P4	
1	~	VLAN5	20	◄			Г	Untagged	•	Tagged	•	Tagged	•	Tagged	Ţ
2	◄	VLAN6	21		•		Γ	Tagged	•	Untagged	-	Tagged	•	Tagged	-
3	◄	VLAN7	22			◄	Γ	Tagged	•	Tagged	•	Untagged	•	Tagged	Ŧ
4	\checkmark	VLAN8	8	Γ	Г		V	Tagged	-	Tagged	~	Tagged	~	Untagged	-
🔽 Ena	ble mana	gement port fo	r P4												
🗆 Ena	ble packe	t forwarding be	etween VLANs												
Port Se	etting														
		P1		P2		P3		P4							
Port	VLAN ID	20	2	l		22	_	8							

2. Next, open Network>>LAN. Set two LAN subnet: LAN1 192.168.33.0/24 and LAN2 192.168.10.0/24.

LAN IP/DHCP	LAN2 IP/DHCP	LAN3 IP/DHCP	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
P Configuration						
• Address :	192.168.33	. 1				
ubnet Mask :	255.255.25	5.0				
HCP Server						
tatus :	Enable	C Disable C Rela	ay Agent			
tart IP :	192.168.33	. 10				
nd IP :	192.168.33	. 254				
rimary DNS :						
econdary DNS :						
ease Time (Min) :	1440					
ateway IP(Optional) :						
				n T.L. 04007 0000		TIR. 194
Network - LAN					ID Doution	
LAN IP/DHCP	LAN2 IP/DHCP	LAN3 IP/DHCP	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
	LAN2 IP/DHCP 192. 168. 1	•	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
LAN IP/DHCP		D. 1	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
LAN IP/DHCP	192.168.1	D. 1	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
LAN IP/DHCP	192. 168. 1 255. 255. 2	0. 1	LAN4 IP/DHCP	DHCP Relay Agent	IP Routing	
LAN IP/DHCP	192. 168. 1 255. 255. 2	0. 1 55. 0		DHCP Relay Agent	IP Routing	
LAN IP/DHCP IP Configuration IP Address : Subnet Mask : DHCP Server Status :	192. 168. 1 255. 255. 2 C Enable	0. 1 © Disable C Rei 0. 10		DHCP Relay Agent	IP Routing	
LAN IP/DHCP IP Configuration IP Address : Subnet Mask : DHCP Server Status : Start IP :	192. 168. 1 255. 255. 2 C Enable 192. 168. 1	0. 1 © Disable C Rei 0. 10		DHCP Relay Agent	IP Routing	
LAN IP/DHCP IP Configuration IP Address : Subnet Mask : DHCP Server Status : Start IP : End IP :	192. 168. 1 255. 255. 2 C Enable 192. 168. 1	0. 1 © Disable C Rei 0. 10		DHCP Relay Agent	IP Routing	
LAN IP/DHCP	192. 168. 1 255. 255. 2 C Enable 192. 168. 1	0. 1 © Disable C Rei 0. 10		DHCP Relay Agent	IP Routing	

- 3. Click Apply.
- 4. Open **VPN>>IPSec>>VPN Trunk>>Policy Table** to create VPN Trunk policy. The way

Apply Cancel

to configure the setting is the same as Scenario 1.

#		Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	œ	wan1	10.0.0.2	0.0.0.0	10.0.0.1	WAN1	enable	up
2	0	wan2	10.0.0.4	0.0.0.0	10.0.0.3	WAN2	enable	up
3	0	wan3	10.0.0.6	0.0.0.0	10.0.0.5	WAN3	enable	up
4	0	wan4	10.0.0.8	0.0.0.0	10.0.0.7	WAN4	enable	up
5	0							
6	0							
7	0							
8	0							
9	0							
10	0							

5. Open **VPN>>VPN Trunk>>Group Table** to group these VPN policies. Group two VPN policies as the following figure and then click **Apply**. The way to configure the setting is the same as Scenario 1.

#	Profile Status	Name	Local Subnet	Remote Subnet	
1 (Enable 	192.168.33.0	192.168.33.0/24	192.168.1.0/24	
2 (O Enable	192.168.10.1	192.168.10.0/24	192.168.1.0/24	
3 (0				
4	0				
5 (0				
6	0				
7	0				
8 (0				
9	0				
10 (0				

Now, two-pair VPN trunk between Vigor3200 (192.168.1.0/24) and Vigor3300 (192.168.33.0/24) has be established.

This page is left blank.

.



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.

ulti-WAN Securit		Dray
Start Wizard Activation Wizard s Wizard Status	System Status Model Name : Vigor 3200n Firmware Version : 3.6.3 Build Date/Time : Jan 15 2013 15:04:20	
	LAN	
	LAN1 00-50-7F-CE-46-FC 192.168.1.1 255.255.255.0 Y	HCP Server DNS es 168.95.1.1
	LAN2 00-50-7F-CE-46-FC 192.168.2.1 255.255.255.0 Y	
II	LAN3 00-50-7F-CE-46-FC 192.168.3.1 255.255.255.0 Y LAN4 00-50-7F-CE-46-FC 192.168.4.1 255.255.255.0 Y	
anagement	DMZ PORT 00-50-7F-CE-46-FC 192.168.4.1 255.255.255.0 Y	
Setting	IP Routed Subnet 00-50-7F-CE-46-FC 192.168.0.1 255.255.255.0 Y	
E.		
dth Management	Wireless LAN	
tions d Remote Access	MAC Address Frequency Domain Firmware Versi	
a Remote Access	00-50-7F-CE-46-FC Europe 2.3.2.0	DrayTek
s LAN	WAN	
N	Link Status MAC Address Connection IP Address	Default Gateway
plication	WAN1 Disconnected 00-50-7F-CE-46-FD	
Maintenance	WAN2 Connected 00-50-7F-CE-46-FE Static IP 172.16.3.1	30 172.16.1.1
tics	WAN3 Disconnected 00-50-7F-CE-46-FF	
I Devices	WAN4 Disconnected 00-50-7F-CE-46-00 WAN5 Disconnected 00-50-7F-CE-46-01	
	WANG DISCONNECCED 00-30-77-CE-40-01	
Area	IPv6	
ion Note		Access Mode
Registration 💌	LAN FE80::250:7FFF:FECE:46FC/64 Link	

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.



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.

WAN >> General Setup

Load Balai	nce Mode:	Auto Weight		
Setup				
Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
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

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

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.

Available settings are explained as follows:

Item	Description
Load Balance Mode	This option is available for multiple-WAN for getting enough bandwidth for each WAN port. If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed . Otherwise, please choose Auto Weigh to let the router reach the best load balance.

	Load Balance Mode: Auto Weight Auto Weight According to Line Speed
Index	Click the WAN interface link under Index to access into the WAN configuration page.
Enable	V means such WAN interface is enabled and ready to be used.
Physical Mode / Type	Display the physical mode and physical type of such WAN interface.
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.
	Always On - Display that such WAN interface is active.
	Backup WAN - Display the Backup WAN interface for such WAN when it is disabled.

Note: In default, each WAN is enabled.

For WAN1 ~ WAN4 (Ethernet)

WAN >> General Setup

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

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:	Backup 🔽 Load Balance: 🗹
	WAN 1 WAN 2 WAN 3 WAN 4 WAN 5
Backup Type (Only if acting as backup for multiple WAN):	 When any of selected WAN disconnect When all of selected WAN disconnect

Available settings are explained as follows:



Item	Description		
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No 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 Auto negotiation for determined by the system.		
	Physical Type: Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex		
Line Speed	If your choose According to Line Speed as the Load Balance Mode, please type the line speed for downloading and 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 		
Active Mode	from 0 to 7. Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface (Backup). Always On Υ Always On		
	Backup 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, such interface will be used for access into Internet all the time. If you choose Backup as the Active Mode, you have to specify which WAN interface will be selected to backup multiple WANs. However, ignore this setting if you want to backup a single WAN. Backup WAN 1 WAN 2 WAN 3 WAN 4 WAN 5 When any of selected WAN disconnect When all of selected 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.
Load Balance	Check this box to enable auto load balance function for such WAN interface. When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.

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

For WAN5 (USB)

WAN >> General Setup

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

Enable:	Yes 🕶
Display Name:	
Physical Mode:	USB
Physical Type:	Auto negotiation 🐱
Line Speed(Kbps):	
DownLink	2000
UpLink	384
Active Mode:	Backup 🖌 Load Balance: 🗹
	WAN 1 WAN 2 WAN 3 WAN 4 WAN 5
Backup Type	• When any of selected WAN disconnect
(Only if acting as backup for multiple WAN):	When all of selected WAN disconnect

Available settings are explained as follows:

Item	Description
Enable	Choose Yes to invoke the settings for this WAN interface. Choose No 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	For such WAN interface is fixed to USB network connection, it is not necessary to specify physical type.
Line Speed	If your choose According to Line Speed as the Load Balance Mode , please type the line speed for downloading and uploading for such WAN interface. The unit is kbps.
Active Mode	Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface (Backup).



	Always On Always On Backup 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, such interface will be used for access into Internet all the time.
	If you choose Backup as the Active Mode , you have to specify which WAN interface will be selected to backup multiple WANs. However, ignore this setting if you want to backup a single WAN. Backup WAN 1 WAN 2 WAN 3 WAN 5
	 When any of selected WAN disconnect When all of selected 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.
Load Balance	Check this box to enable auto load balance function for such WAN interface.
	When the data traffic is large, the WAN interface with the function enabled will balance the data transmission automatically among all of the WAN interfaces in connection status.

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

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

Internet	Access				
Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	None	*	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page IPv6
WAN3		Ethernet	None PPPoE		Details Page IPv6
WAN4		Ethernet	Static or Dynamic IP PPTP/L2TP		Details Page IPv6
WAN5		USB	None	*	Details Page IPv6

Note : Only one WAN can support IPv6.

Dray Tek

WAN >> Internet Access

Internet	Access				
Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	None	~	Details Page IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page IPv6
WAN3		Ethernet	None	*	Details Page IPv6
WAN4		Ethernet	None	*	Details Page IPv6
WAN5		USB	None	~	Details Page IPv6
Note : Or	nly one WAN can	support IPv6.	None 3G/4G USB Modem(PPP mode)		

Each item is explained as follows:

Item	Description
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 Details Page for accessing the page to configure the settings.
Details Page	This button will open different web page according to the access mode that you choose in WAN interface
IPv6	This button will open different web page (based on Physical Mode) to setup IPv6 Internet Access Mode for WAN interface.
	If IPv6 service is active on this WAN interface, the color of "IPv6" will become green.

Dray Tek

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 1		
PPPoE Client Mode	PPP/MP Setup	
🔘 Enable 💿 Disable	PPP Authentication	PAP or CHAP 🔽
ISP Access Setup Username Password Index(1-15) in Schedule Setup: =>,,, WAN Connection Detection Mode Ping IP TTL:	Idle Timeout IP Address Assignment Me (IPCP) WAN IP Alias Fixed IP: Yes No Fixed IP Address O Default MAC Address O Specify a MAC Address: O .50 .7F 00 .00	(Dynamic IP)
MTU 1442 (Max: 1492) PPPoE Pass-through For Wired LAN For Wireless LAN		

WAN >> Internet Access

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

Item	Description
	 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.
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.
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 8 public IP addresses other than the current one you are using.

ltem	Descrip	tion		
	🧷 WANII	P Alias - W	indows Internet Explorer	
	http://19	2.168.1.5/doc	Avipalias.htm	
	WAN1 I	P Alias (M	ulti-NAT)	
	Index	Enable	Aux. WAN IP	Join NAT IP Pool
	1.	V		
	2.		0.0.0	
	3.		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</u> <u>17</u>	-24 25-32 >>	<u>Next</u> >>
			OK Clear All	Close
			Yes to use this funct box of Fixed IP Add	ion and type in a fixed Iress .
	Address	s or spec	ddress – You can us ify another MAC add ddress for the router.	ress by typing on the
	Specify router m		Address – Type the	MAC address for the

Details Page for Static or Dynamic IP in WAN1 ~ WAN4

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.

WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client) The second s		WAN IP Network Settings WAN IP Alias			
Keep WAN Connection Enable PING to keep alive PING to the IP PING Interval		C Obtain an IP a Router Name Domain Name * : Required fo Specify an IP IP Address	VIGOR r some I	SPs	*
WAN Connection Detection Mode Ping IP TTL:	ARP Detect	Subnet Mask Gateway IP Adı DNS Server IP A Primary IP Addr	ddress ress	255.255.0.0 172.16.1.1 168.95.1.1	
MTU RIP Protocol Enable RIP Bridge Mode Enable Bridge Mode	1442 (Max: 1500)	 Secondary IP A Default MAC Specify a M MAC Address: 00 .50 .7F 	C Addres 1AC Addr	-]
	ОК	Cancel			

Item	Description
Static or Dynamic IP	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
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 Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.
	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.



Item	Description				
MTU	It means Max Tr setting is 1442.	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.				
Bridge Mode	-		nction, the router will ilable only for WAN1.		
WAN IP Network Settings	This group allows you to obtain an IP address automatical and allows you type in IP address manually.				
	WAN IP Alias - If you have multiple public IP address would like to utilize them on the WAN interface, please WAN IP Alias. You can set up to 8 public IP addresses than the current one you are using.				
	🖉 WAN1IP Alias - Wir	ndows Internet Explorer			
	D http://192.168.1.5/doc/	wipalias.htm			
	WAN1 IP Alias (Mu Index Enable	Ilti-NAT) Aux. WAN IP	Join NAT IP Pool		
	1. 🗸				
	2.	0.0.0.0			
	3.	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			
	<< <u>1-8</u> <u>9-16</u> <u>17-3</u>	<u>24 25-32</u> >>	<u>Next</u> >>		
		OK Clear All	Close		
	obtain the IP addr Dynamic IP mod	ress automatically if le.	-		
	<i>Router Name</i> : Type in the router name provided by ISP.				
	 <i>Domain Name:</i> 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	e the IP address.			
	Subnet Mask: Type the subnet mask.				
	Gateway IP Addr	ess: Type the gatew	ay IP address.		
	Default MAC Ad	dross. Click this radi	o button to use default		

Item	Description
	MAC address for the router.
	<i>Specify a MAC Address</i> : 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

WAN >> Internet Access

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 M	ode	PPP Setup	
	O Enable L2TP O Disable	PPP Authentication	PAP or CHAP
		PPP Authentication	
Server Address		Idle Timeout	-1 second(s)
Specify Gateway IF) Address	IP Address Assignment	Method
17	72.16.1.1	(IPCP) WAN IP Alias	3
		— Fixed IP: 🔘 Yes 💿	No (Dynamic IP)
ISP Access Setup		Fixed IP Address	
Username		WAN IP Network Settin	gs
Password		🔘 Obtain an IP addre	ess automatically
Index(1-15) in <u>Sch</u>	edule Setup:	💿 Specify an IP addr	ess
=>,	,,	IP Address	172.16.3.102
		 Subnet Mask	255.255.0.0
MTU	1442 (Max: 1460)		

Item	Description
PPTP/L2TP Client Mode	Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
	 Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface. 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 Setup	Username -Type in the username provided by ISP in this field.



Item	Descript	lion		
	Passwor	·d -Type	in the password pro	ovided by ISP in this fie
	time scho previous	edule for ly in Ap	r your request. All th	ou can type in four sets ne schedules can be set le web page and you ca hat web page.
MTU	It means 1442.	Max Tr	ansmit Unit for pack	xet. The default setting
PPP Setup	PPP Aut PPP.	thentica	ntion - Select PAP of	nly or PAP or CHAP f
			Set the timeout for br ough the time withou	reaking down the Intern at any action.
	wheneve address i you wan and type WAN IF	er you re in the Fin t to use t in a fixe P Alias -	quest. In this case, y xed IP field. Please of this function. Click Y ed IP address in the l If you have multiple	contact your ISP before Yes to use this function
	WAN IP than the	Alias. N current (P Alias - W	You can set up to 8 p one you are using. indows Internet Explorer	public IP addresses othe
	WAN IP than the	Alias. S	You can set up to 8 p one you are using. indows Internet Explorer	
	WAN IP than the	Alias. N current (P Alias - W	You can set up to 8 p one you are using. indows Internet Explorer Avipalias.htm	
	WAN IP than the	P Alias. N current of P Alias - W 2.168.1.5/doc	You can set up to 8 p one you are using. indows Internet Explorer Avipalias.htm	
	WAN IP than the WANII WAN1 IF Index 1.	P Alias. N current of P Alias - W 2.168.1.5/doc P Alias (M	You can set up to 8 p one you are using. indows Internet Explorer //vipalias.htm ulti-NAT) Aux. WAN IP	oublic IP addresses othe
	WAN IP than the WANII WAN1 IF Index 1. 2.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer Wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0	Join NAT IP Pool
	WAN IP than the WANII WAN1 IF Index 1. 2. 3.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer //wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0.0	Join NAT IP Pool
	WAN IP than the WAN1IF WAN1 IF Index 1. 2. 3. 4.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer ///ipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0 0.0.0	Join NAT IP Pool
	WAN IP than the WANII WAN1 IF Index 1. 2. 3. 4. 5.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0	Join NAT IP Pool
	WAN IP than the WANII WAN1 IF Index 1. 2. 3. 4. 5. 6.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer /wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	Join NAT IP Pool
	WAN IP than the WAN1IF Index 1. 2. 3. 4. 5. 6. 7.	P Alias. Y current of P Alias - W 2.168.1.5/doo P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer /wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0 0.0.0 0.0.0	Join NAT IP Pool
	WAN IP than the WAN1IF WAN1 IF Index 1. 2. 3. 4. 5. 6. 7. 8.	P Alias. No. current of P Alias - W. 2.168.1.5/doc P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer /wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	Join NAT IP Pool
	WAN IP than the WAN1IF WAN1 IF Index 1. 2. 3. 4. 5. 6. 7. 8.	P Alias. No. current of P Alias - W. 2.168.1.5/doc P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer ///ipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	Join NAT IP Pool
	WAN IP than the WAN1IF WAN1 IF Index 1. 2. 3. 4. 5. 6. 7. 8.	P Alias. No. current of P Alias - W. 2.168.1.5/doc P Alias (M Enable	You can set up to 8 p one you are using. indows Internet Explorer /wipalias.htm ulti-NAT) Aux. WAN IP 0.0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0	Join NAT IP Pool

Item	Description
	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 3G/4G USB Modem (PPP mode) 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

AN 5	
3G/4G USB Modem(PPP mode)	○ Enable ④ Disable
SIM PIN code	
Modem Initial String	AT&FE0V1X1&D2&C1S0=0
Hoden Inda String	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	Apply
Modem Initial String2	AT
Modem Dial String	ATDT*99#
	(Default:ATDT*99#, CDMA:ATDT#777, TD- SCDMA:ATDT*98*1#)
PPP Username	(Optional)
PPP Password	(Optional)
PPP Authentication	PAP or CHAP
Index(1-15) in <u>Schedule</u> Setup:	
=>,,,	
WAN Connection Detection	
Mode	ARP Detect 💌
Ping IP	
TTL:	

Item	Description
3G/4G USB Modem (PPP mode)	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you



Item	Description
	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 Setup	Set the PCs on LAN to work at certain time interval only. You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.
	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.
Default	Click it to reset to the factory default setting for 3G connection.

Details Page for IPv6 – Offline in WAN1/WAN2/WAN3/WAN4

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

1 IPv6	
Internet Access Mode	
Connection Type	Offline 🗸

Details Page for IPv6 – PPP in WAN1/WAN2/WAN3/WAN4

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

No need to type any other information for PPP mode.

W	N >> Internet Access		
w	AN 1 IPv6		
Г	Internet Access Mode		
	Connection Type	PPP 💌	
	Note : IPv4 WAN setting should be	PPPoE client.	
		OK Cancel	

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

Online Status

Physical Connect	ion			System Uptime: 0:0:30
	IPv4		IPv6	
LAN Status				
IP Address				
	00:200:21D:AAFF:F FF:FE7A:3E58/64 (L	E7A:3E58/64 (Global) ink)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
7	8	618	672	
WAN2 IPv6 Status	5			
Enable	Mode	Up Time		
Yes	PPP	0:00:11		
IP			Gateway IP	
	00:200:21D:AAFF:F F:FE7A:3E5A/128 (L		FE80::90:1A00:242:AD52	
DNS IP				
2001:B000:16 2001:B000:16				
TX Packets	RX Packets	TX Bytes	RX Bytes	
7	4	544	616	

Note: At present, the **IPv6 prefix** can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

Details Page for IPv6 – TSPC in WAN1/WAN2/WAN3/WAN4/WAN5

Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (<u>http://gogonet.gogo6.com/page/freenet6-account</u>) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

Internet Access Mode	
Connection Type	TSPC 💌
TSPC Configuration	
Username	
Password	
Confirm Password	
Tunnel Broker	

Cancel

0K

Available settings are explained as follows:

WAN >> Internet Access

Item	Description
Username	Type the name obtained from the broker.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.

Details Page for IPv6 – AICCU in WAN1/WAN2/WAN3/WAN4/WAN5

WAN >> Internet Access

PPPoE	Static or Dyna	amic IP		PPTP	IPv6
Internet Access Mode					
Connection Type		AICCU	*		
AICCU Configuration					
Always On					
Username					
Password					
Confirm Password					
Tunnel Broker	tic.sixxs.net				
Subnet Prefix				1	

Note : If "Always On" is not enabled, AICCU connection would only retry three times.

OK Cancel

Item	Description
Always On	Check this box to keep the network connection always.
Username	Type the name obtained from the broker. Please apply new account at <u>http://www.sixxs.net/</u> . It is suggested for you to apply another username and password.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address getting from service provider

Details Page for IPv6 – DHCPv6 Client in WAN1/WAN2/WAN3/WAN4

DHCPv6 client mode would use DHCPv6 protocol to obtain IPv6 address from server.

Pv6	
ternet Access Mode	
onnection Type	DHCPv6 Client 💌
ICPv6 Client Configuration	
Identity Association 💿	Prefix Delegation 🔘 Non-temporary Address
(AID (Identity Association ID)	2644712601

Available settings are explained as follows:

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

Details Page for IPv6 – Static IPv6 in WAN1/WAN2/WAN3/WAN4

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

WAN >> Internet Access

Static IPv6
/ Prefix Length / Add Delete

Dray Tek

Available settings are explained as follows:

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

4.1.4 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in 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.

WAN >> Load-Balance Policy

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Port	Move Up	Move Down
1		any	*	WAN1 💌								<u>Down</u>
<u>2</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>3</u>		any	*	WAN1 💌							<u>UP</u>	<u>Down</u>
<u>4</u>		any	*	WAN1 🔽							<u>UP</u>	Down
<u>5</u>		any	*	WAN1 💌							<u>UP</u>	<u>Down</u>
<u>6</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
Z		any	*	WAN1 💌							<u>UP</u>	<u>Down</u>
<u>8</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>9</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
<u>10</u>		any	*	WAN1 🔽							<u>UP</u>	<u>Down</u>
< <u>1-10</u>	<u>11-20</u>	<u>21-30</u>	<u>31-32</u>	>>							l	<u>lext</u> >:

Each item is explained as follows:

Item	Description
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 Up or Down link to move the order of the policy.

Click any Index number link to access into the following page for configuring load-balance policy.

WAN >> Load-Balance Policy

Index: 1	
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	
1	
	OK Cancel

Each item is explained as follows:

Item	Description		
Enable	Check this box to enable this policy.		
Protocol	Use the drop-down menu to choose a proper protocol for the WAN interface.		
	Protocol any any TCP UDP TCP/UDP ICMP IGMP		
Binding WAN interface	Choose the WAN interface (WAN1 / WAN2 / WAN3 / 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.
Dest IP Start	Type the destination IP start for the specified WAN interface.
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Dest Port Start	Type the destination port start for the destination IP.
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

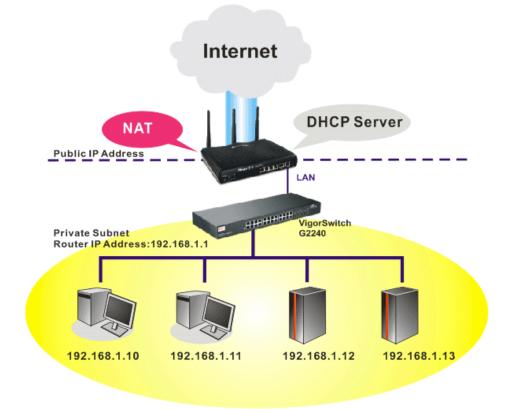
4.2 LAN

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



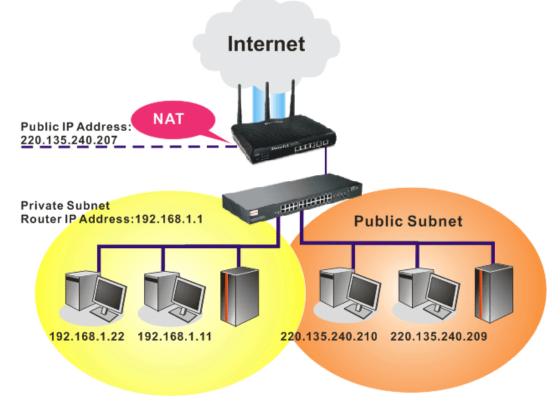
4.2.1 Basics of LAN

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



Dray Tek

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)

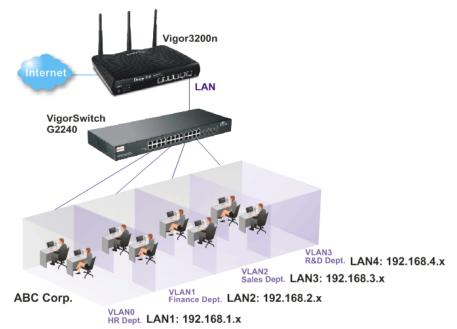
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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	192.168.1.5	Details Page IPv6
LAN 2		V	192.168.2.1	Details Page
LAN 3			192.168.3.1	Details Page
LAN 4		V	192.168.4.1	Details Page
DMZ	V	V	192.168.5.1	Details Page
IP Routed Subnet		\checkmark	192.168.0.1	Details Page

Advanced You can configure DHCP options here.

Force router to use "DNS server IP address" settings specified in IAN1

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	V				
LAN 2		1			
LAN 3			V		
LAN 4				V	
DMZ PORT		V	~	~	V

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

	OK		
ОК	Cancel	Default	

Each item is explained as follows:

Item	Description
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.
	IPv6 – Click it to access into the settings page of IPv6.
Advanced	DHCP packets can be processed by adding option number



	and data information when such function is enabled.
	DHCP Options Status
	Option Number:
	Enable/Disable – Enable/Disable the function of DHCP Option. Each DHCP option is composed by an option number with data. For example,
	Option number:100
	Data: abcd
	When such function is enabled, the specified values for DHCP option will be seen in DHCP reply packets.
	Option Number – Type a number for such function.
	DataType – Choose the type (ASCII or Hex) for the data to be stored.
	Data – Type the content of the data to be processed by the function of DHCP option.
Force router to use "DNS server IP address" settings as specified in	Force Vigor router to use DNS servers configured in LAN1/LAN2/LAN3/LAN4 instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Inter-LAN Routing	LAN 1 ~ LAN 4, DMZ PORT - Check the box to make the routing among LANs.

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

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

Details Page for LAN 1

LAN1 is the default configuration for basic host connection.

LAN >> General Setup

LAN 1 Ethernet TCP / IP	and DHCP Setup	LAN 1 IPv6 Setup		
Network Configuration		DHCP Server Configu	ration	
For NAT Usage			Disable Server	
IP Address	192.168.1.5	Enable Relay Ager	nt	
Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
		IP Pool Counts	150	
RIP Protocol Control	Disable 💌	Gateway IP Address	192.168.1.5	
		Lease Time	259200	(s)
		DNS Server IP Addres	S	
		Primary IP Address		
		Secondary IP Addres	s	
OK				

Item	Description
Network Configuration	IP Address - Type in 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 - Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default) Enable can activate the RIP protocol.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server - Let you manually assign IP address to every host in the LAN.
	Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
	Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.



Item	Description		
	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.		
	Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.		
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 usua more than one DNS Server. If your ISP does not provide it, t router will automatically apply default DNS Server IP addrest 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 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.		

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



Details Page for LAN 2, LAN 3, LAN 4

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

nd DHCP Setup		
	DHCP Server Configurat	tion
	💿 Enable Server 🔘 Dis	sable Server
💿 For Routing Usage	Start IP Address	192.168.3.10
192.168.3.1	IP Pool Counts	100
255.255.255.0	Gateway IP Address	192.168.3.1
	• For Routing Usage	 DHCP Server Configuration Enable Server O District Start IP Address 192.168.3.1 IP Pool Counts

ΟK

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



gateway.

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

Details Page for DMZ

DMZ port setting is used for connecting host in DMZ.

MZ Ethernet TCP / IP a	and DHCP Setup		
letwork Configuration		DHCP Server Configura	ation
⊙ For NA⊤ Usage	For Routing Usage	⊙Enable Server ○D	isable Server
IP Address	192.168.5.1	Enable Relay Agent	:
Subnet Mask	255.255.255.0	Start IP Address	192.168.5.10
		IP Pool Counts	100
		Gateway IP Address	192.168.5.1
		Lease Time	259200 (s)
		DNS Server IP Address	
		Primary IP Address	
		Secondary IP Address	

Item	Description
Network Configuration	Set IP address and Subnet Mask for clients connected via DMZ port.
	For NAT Usage - Click this item to invoke NAT usage.
	For Routing Usage - Click this item to invoke Routing usage.
	IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.9.1).
	Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server – Let you manually assign IP address to

	every host in the LAN.
	Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.9.10, the starting IP address must be 192.168.9.11 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.
	Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.
DNS Server IP Address	Type in the primary IP address for the router if you want to use Static IP mode. If necessary, type in secondary IP address for necessity in the future.

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

Dray Tek

IP Routed Subnet

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

LAN >> General Setup

Network Configuration		DHCP Server Configuration
● Enable ● Disable For Routing Usage IP Address Subnet Mask	192.168.0.1 255.255.255.0	Start IP Address IP Pool Counts 0 Lease Time Use LAN Port P1
RIP Protocol Control	Disable 💌	Use MAC Address Index Matched MAC Address given IP Address
		MAC Address : : : : : : : : : : : : : : : : : :

Item	Description
Network Configuration	Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.
	IP Address - Type in IP address for connecting to a local private network (Default: 192.168.0.1).
	Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/24)
	RIP Protocol Control –
	Disable - Deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)
	Enable – Trigger the router to exchange the entire routing table with the other nodes in the same subnet by sending/receiving RIP packets.
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.
	Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than

192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 10.
Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.
Use LAN Port – Specify an IP for IP Route Subnet. If it is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of P1 and P2.
Use MAC Address - Check such box to specify MAC address.
MAC Address: Enter the MAC Address of the host one by one and click Add to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2 nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2 nd subnet won't get an IP address belonging to 1 st subnet.
Add – Type the MAC address in the boxes and click this button to add.
Delete – Click it to delete the selected MAC address.
Edit – Click it to edit the selected MAC address.
Cancel – Click it to cancel the job of adding, deleting and editing.

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

4.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4

LAN >> Static Route Setup

IPv4	IPv6		1 3	Set to Factory Default	View Routing Table
Index	Destination Address	Status	Index	Destination Addres	s 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

Each item is explained as follows:

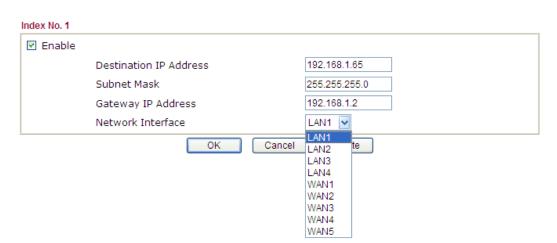
Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.



Viewing Routing Table	Displays the routing table for your reference.		
	Current Running Routing Table <u>Refresh</u>		
	<pre>Key: C - connected, S - static, R - RIP, * - default, ~ - private * 0.0.0.0/ 0.0.0.0 via 172.16.3.1, VAN1 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</pre>		
Index	The number (1 to 10) under Index allows you to open next page to set up static route.		
Destination Address	Displays the destination address of the static route.		
Status	Displays the status of the static route.		

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

LAN >> Static Route Setup



Item	Description
Enable	Click it to enable this profile.
Destination IP Address	Type an IP address as the destination of such static route.
Subnet Mask	Type the subnet mask for such static route.
Network Interface	Use the drop down list to specify an interface for such static route.

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

Static Route for IPv6

LAN >> Static Route Setup

Click the IPv6 tab to open the following page. You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:

IPv4	IPv6		Set to	Factory Default View IPv6	Routing Table
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	::85.170.85.16/0	х	<u>11.</u>	::/0	х
<u>2.</u>	::/0	x	<u>12.</u>	::/0	х
<u>3.</u>	::/0	x	<u>13.</u>	::/0	х
<u>4.</u>	::/0	х	<u>14.</u>	::/0	х
<u>5.</u>	::/0	х	<u>15.</u>	::/0	х
<u>6.</u>	::/0	x	<u>16.</u>	::/0	х
<u>7.</u>	::/0	x	<u>17.</u>	::/0	х
<u>8.</u>	::/0	x	<u>18.</u>	::/0	x
<u>9.</u>	::/0	х	<u>19.</u>	::/0	х
<u>10.</u>	::/0	х	<u>20.</u>	::/0	x
< 1 - 20 21 -	40 >>				Next >>

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

Each item is explained as follows:

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

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

LAN >> Static Route Setup

🗹 Enable		
Destination IPv6 Address / Prefix Len	::85.170.85.16	/ 0
Gateway IPv6 Address		
Network Interface	LAN 🗸	

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.

Dray Tek

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

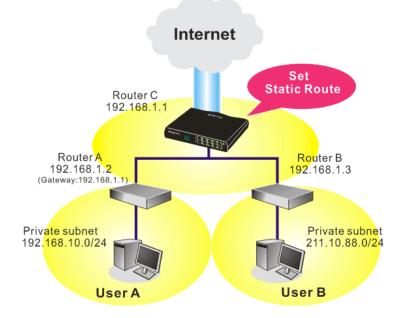
After finishing all the settings here, please click **OK** to save the configuration.

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

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

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

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



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



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

2. Click the LAN>> Static Route and click on the Index number 1. 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.

LAN >> Static 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	LAN1 💌		
	ОК	Cancel Delete		

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

ndex No. 2		
🗹 Enable		
	Destination IP Address	211.100.88.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.3
	Network Interface	LAN1 🔽

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

Diagnostics >> View Routing Table

LAN >> Static Route Setup

Curr	ent Runr	ning Routing Table			<u>Refresh</u>
	Key: C	C - connected, S -	static, R - RIP, * - default, ~ -	private	^
	ສ~ C~ ສ~	192.168.1.0/	255.255.255.0 via 192.168.1.2, 255.255.255.0 is directly connect 255.255.255.0 via 192.168.1.3,	ed, 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				Wirele	ss LAN		
	Enable	VID	Priority	LAN Port	SSID1	S SID2	S SID3	SSID4	Subnet
VLAN0		0	0 🗸	V					LAN 1 🗸
VLAN1		0	0 🗸						LAN 1 🔽
VLAN2		0	0 🗸						LAN 1 💌
VLAN3		0	0 🗸						LAN 1 🔽
VLAN4		0	0 🗸						LAN 1 💌
VLAN5		0	0 🗸						LAN 1 🔽
VLAN6		0	0 🗸						LAN 1 💌
VLAN7		0	0 🗸						LAN 1 🗸

Enable management port for P1

LAN >> VLAN Configuration

1. Hybrid mode only applied on VLAN0 to accept both tagged/untagged packets;

2. Tag based VLAN only applied for LAN Port;

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

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



Item	Description
VLAN Tag	 Enable – Check the box to enable the function of VLAN with tag. The router will add specific VLAN number to all packets on the LAN while sending them out.
	Please type the tag value and specify the priority for the packets sending by LAN.
	VID – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority 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.
Wireless LAN	SSID1 – SSID4 – Check the SSID box (es) for the wireless clients to be grouped under the selected VLAN.
Subnet	Choose one of them to make the selected VLAN mapping to the specified subnet only. For example, LAN1 is specified for VLAN0. It means that PCs grouped under VLAN0 can get the IP address (es) that specified by the subnet.

Enable management port for P1	It can help users to communicate with the router still even though configuring wrong VLAN tag setting. For Vigor router has one LAN physical port only, it is recommended to enable the management port (LAN 1) to ensure the data transmission is unimpeded.
----------------------------------	---

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

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

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 192.168.1.10 EO-CB-4E-DA-48-79 192.168.1.12 D8-B3-77-12-AF-9A Add and Edit IP Address Mac Address ::::::::::::::::::::::::::::::::::::	Index IP Address	Mac Address
Comment		Show Comment
Add	Edit Delete	

Note: IP-MAC binding presets DHCP Allocations.

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

OK

Item	Description
Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.

Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.		
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.		
Select All	Click this link to select all the items in the ARP table.		
Sort	Reorder the table based on the IP address.		
Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.		
Add and Edit	 IP Address - Type the IP address that will be used for the specified MAC address. Mac Address - Type the MAC address that is used to bind with the assigned IP address. Comment - Type a brief description for such list. Show Comment - Check this box to display the comment on IP Bind List box. 		
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 Add and Edit to the table of IP Bind List .		
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 IP Bind List . Simply click and select the one, and click Delete . The selected item will be removed from the IP Bind List .		

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

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

4.2.6 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 >> LAN Port Mirror

LAN Port Mi	irror		
Port Mirror	:		
🔘 Enable	📀 Disable		
Mirror port	:		
💿 WAN4			
Mirrored po	ort:		
P 1	WAN 1	🗌 WAN 2	WAN 3

ΟK

Available settings are explained as follows:

Item	Description		
Port Mirror	Check Enable to activate this function. Or, check Disable 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. When Port Mirror is enabled, the Mirror Port (WAN4) will be disabled.		
Mirrored port	Select which ports (LAN port or WAN port) are necessary to be mirrored. P1 represents LAN port.		

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

4.2.7 Web Portal Setup

This page allows you to configure a profile with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router. No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal.

LAN >> Web Portal Setup

Profile	Status	Interface	
<u>1.</u>	Disable	None	Preview
<u>2.</u>	Disable	None	Preview
<u>3.</u>	Disable	None	Preview
4.	Disable	None	Preview

Each item is explained as follows:

Item	Description	
Profile	Display the number link which allows you to configure the profile.	



Status	Display the content (Disable, URL Redirect or Message) of the profile.		
Interface	Display the applied interfaced of the profile.		
Preview Open a preview window according to the configured			

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

LAN >> Web Portal Setup

Profile Index: 1	
O Disable	
OURL Redirect	http://
	e.g. http://www.draytek.com Note : If the User Management application is enabled, it will override the Web Portal settings seen here.
O Message	<h1>Vigor</h1> <h2> - Reliable connectivity</h2> <h2> - Robust firewall protection</h2> <h2> - Multi-site secure communication</h2>
	(Max 255 characters)
Applied Interfaces	(
	LAN1 LAN2 LAN3 LAN4
	SSID1 SSID2 SSID3 SSID4

Cancel

0K

Available settings are explained as follows:

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

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

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.

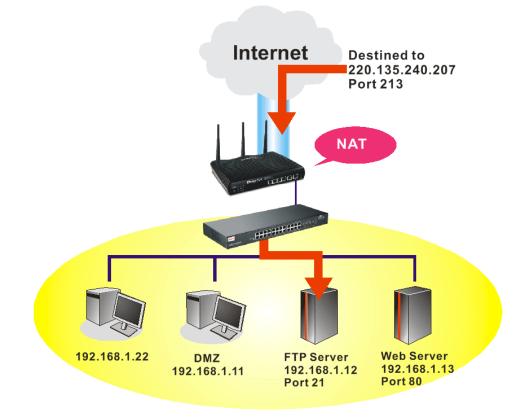
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Port Red	irection				Set to Fact	ory Default
Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
<u>1.</u>		All				х
<u>2.</u>		All				х
<u>3.</u>		All				х
<u>4.</u>		All				х
<u>5.</u>		All				х
<u>6.</u>		All				х
<u>7.</u>		All				х
<u>8.</u>		All				х
<u>9.</u>		All				х
<u>10.</u>		All				х
<< 1-10	11-20 21-30 31-4	0 >>				Next >>

Each item is explained as follows:

Item	Description			
Index	Display the number of the profile.			
Service Name	Display the description of the specific network service.			
WAN Interface	Display the WAN IP address used by the profile.			
Protocol	Display the transport layer protocol (TCP or UDP).			
Public Port	Display the port number which will be redirected to the specified Private IP and Port of the internal host.			
Private IP	Display the IP address of the internal host providing the service.			
Status	Display if the profile is enabled (v) or not (x).			

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

Index No. 1	
Enable	
Mode	Single 🐱
Service Name	
Protocol	💌
WAN Interface	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.



NAT >> Port Redirection

Item	Description
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . 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 Private IP and Port of the internal host. If you choose Range 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 Range 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.

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

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

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

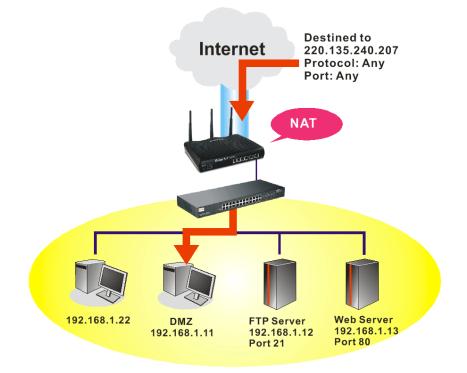
Aanagement Setup				
Management Access Control	Management Port Setup)		
	 User Define Ports 	🔘 Default Ports		
Allow management from the Internet	Telnet Port	23 (Default: 23)		
FTP Server	HTTP Port	80 (Default: 80)		
HTTP Server		· · · · ·		
HTTPS Server	HTTPS Port	443 (Default: 443)		
🗹 Telnet Server	FTP Port	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		

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
N 1				
None 💊	•			
Private IP			Choose	PC
MAC Address of	the True IP DMZ Host	00.00.	00 00 00 00	
Note: When a ⁻ always on.	Frue-IP DMZ host is t	urned on, it will force	e the router's WAN o	connection to be

ΟK

Vigor3200 Series User's Guide

Available settings are explained as follows:

Item	Description
WAN 1 None	Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.
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. The private IP address in the list to be the DMZ host. The 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. National Host Setup DEX Host Setup DEX Host Setup

Dray Tek

Active True IP selection is available for WAN1 only. 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	1	
		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.

NAT >> DM.	Z Host Setup				
OMZ Host S	ietup				
WA	N1	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

Item	Description
Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



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

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:

ΝΔΤ	>>	0	nen	Ports	
INA I	~~	~	ben.	1 0115	

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>				×

Each item is explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	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 Inactive or Active state.

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

Comment		P2P				
WAN Interface		WAN	WAN1 💌			
	Local Computer	192.1	68.1.10	Cho	ose PC	
Protoco	l Start Port	End Port		Protocol	Start Port	End Port
1. TCP 🗸	4500	4700	6.	💙	0	0
2. UDP 🔽	4500	4700	7.	💙	0	0
3 🚩	0	0	8.	💙	0	0
4 🍟	0	0	9.	💙	0	0
5 🗸	0	0	10.	💙	0	0

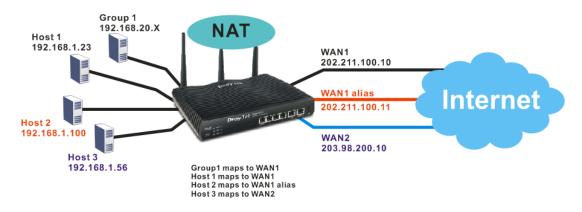
Available settings are explained as follows:

Item	Description
Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Local Computer	Enter the private IP address of the local host or click Choose PC 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 TCP , UDP , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

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

4.3.4 Address Mapping

Address Mapping is used to map a specified private IP or a range of private IPs of NAT subnet into a specified WAN IP (or WAN IP alias IP). Refer to the following figure.



Suppose the WAN settings for a router are configured as follows:

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11 WAN2: 203.98.200.10

Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host1 to always map to 202.211.100.10 (WAN1); Host2 to always map to 202.211.100.11 (WAN1 alias); Host3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

	ping Setup			Set to Factory Def		
Index	Protocol	Public IP	Private IP	Mask	Status	
<u>1.</u>	ALL			/32	х	
<u>2.</u>	ALL			/32	х	
<u>3.</u>	ALL			/32	х	
<u>4.</u>	ALL			/32	х	
<u>5.</u>	ALL			/32	х	
<u>6.</u>	ALL			/32	х	
<u>7.</u>	ALL			/32	х	
<u>8.</u>	ALL			/32	×	
<u>9.</u>	ALL			/32	×	
<u>10.</u>	ALL			/32	х	

NAT >> Address Mapping

Available settings are explained as follows:

Item	Description
Index	Indicate the relative number for the particular entry that you want to configure You should click the appropriate index

Dray Tek

	number to edit or clear the corresponding entry.	
Protocol	Display the protocol used for this address mapping.	
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.	
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10.	
Mask	Display the subnet mask selected for this address mapping.	
Status	Display the status for the entry, enable or disable.	

Click the index number link to open the configuration page.

NAT >>	> Address	Mapping

Index No. 1	
🕑 Enable	
Protocol:	ALL 💌
WAN Interface	WAN2 🔽
WAN IP	1-172.16.3.130 🔽
Private IP:	
Subnet Mask:	/32 🗸
	OK Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or ALL for selection.
WAN Interface	Choose the WAN interface for such address mapping profile.
WAN IP	This is the source IP of a packet captured on the WAN side and sent by a NAT host specified in the Private IP field. The drop down menu contains WAN interface IPs and WAN IP alias IPs.
Private IP	This is the source IP of a NAT host which wishes to send packets to the WAN side and have source address as configured in the WAN IP field.
Subnet Mask	Select a value of subnet mask for private IP address.

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



4.3.5 Port Triggering

Port Triggering is a variation of open ports function.

The key difference between "open port" and "port triggering" is:

- Once the OK button is clicked and the configuration has taken effect, "open port" keeps the ports opened forever.
- Once the OK button is clicked and the configuration has taken effect, "port triggering" will only attempt to open the ports once the triggering conditions are met.
- The duration that these ports are opened depends on the type of protocol used. The "default" durations are shown below and these duration values can be modified via telnet commands.

TCP: 86400 sec.

UDP: 180 sec.

IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.

NAT >> Port Triggering

Port Trig	ggering				Set to Factory	Default
Index	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Status
<u>1.</u>						х
<u>2.</u>						х
<u>3.</u>						х
<u>4.</u>						х
<u>5.</u>						х
<u>6.</u>						х
<u>7.</u>						х
<u>8.</u>						х
<u>9.</u>						х
<u>10.</u>						х
<< <u>1-10</u>	<u>11-20</u> >>					<u>Next</u> >>

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

Available settings are explained as follows:

Click the index number link to open the configuration page.



_ Enable	3	
	Service	User Defined 💙
	Comment	
	Triggering Protocol	💌
	Triggering Port	
	Incoming Protocol	💌
	Incoming Port	
	Note: The Triggering Port and Incoming Port 123-456,777-789 (legal),123-456,789 (leg	

Item	Description	
Enable	Check to enable this entry.	
Service	Choose the predefined service to apply for such trigger profile. User Defined User Defined Real Player QuickTime WMP IRC AIM Talk ICQ PalTalk BitTorrent	
Comment	Type the text to memorize the application of this rule.	
Triggering Protocol	Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile.	
Triggering Port	Type the port or port range for such trigger profile.	
Incoming Protocol	When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.	

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

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

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:

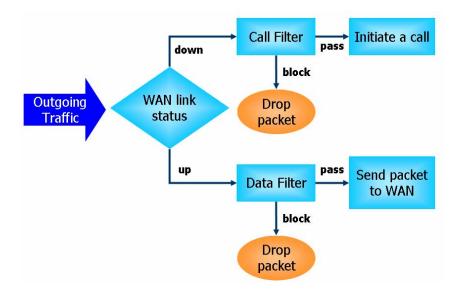
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

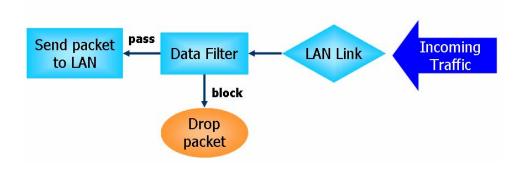
Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **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.



Dray Tek



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

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

Item	Description	
Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.	
Data Filter	Check Enable 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 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, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not make any response (pass or block) for these packets, then the router's firewall will block the packets directly.

Default Rule Page

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

Firewall >> General Setup)		
General Setup			
General Setup	Default Rule		
Actions for def Application	ault rule:	Action/Profile	S
Filter		Pass 💌	[
Sessions Cont	rol	30 / 120000	[
Quality of Servi	ice	None 🗸	[
Load-Balance	policy	Auto-Select 🐱	[

Syslog User Management None * None APP Enforcement ¥ None ~ URL Content Filter Web Content Filter None ¥ Advance Setting Edit 0K Cancel

Item	Description	Description	
Filter	Select Pass or Block for the packet filter rules.	Select Pass or Block for the packets that do not match with the filter rules.	
	Filter	Pass 💌 Pass Block	
Sessions Control	51	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related		



Item	Description	
	section later. None Class 1 Class 2 Class 3 Default	
Load-Balance Policy	Choose the WAN interface for applying Load-Balance Policy. Auto-Select WAN1 WAN2 WAN3 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 User Object [Create New User] User Group [Create New Group] ALL Note: When there is no user profile or group profile	
APP Enforcement	existed, Create New User or Create New Group item will appear for you to click to create a new one.Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.	
URL Content 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	



Item	Description		
	 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 Setup Advance Setting Codepage ANSI(1252)-Latin 1 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. 		
	Image: Controls 192.168.1.1 Image: Controls 172.16.2.213 Image: Controls 172.16.2.213 Image: Controls 172.16.2.213 WAN Information WAN IP (Fixed) Image: Controls 172.16.2.213 Wand IP (Fixed) 172.16.2.213 Setup Codepage Information Codepage To Select Windows Version: 5.01.2600 RECOMMENDED CODEPAGE: 950 (ANSI/OEM - Traditional Chinese Big5) Obal: 21 Oba6:7c Oba9:63 Obaa:61 Obad:20 Obae:52 Obb2:32 Obb3:33 Obb9:31 Obba:61		
	 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 		

Item	Description	
	best utilization of network resources.	

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

4.4.3 Filter Setup

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

Firewal	>>	Filter	Setup
---------	----	--------	-------

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1						
Comments : Def	ault 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		

Item	Description
Filter Rule	Click a button numbered $(1 \sim 7)$ to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23–character long.
Move Up/Down	Use Up or Down link to move the order of the filter rules.



Next Filter Set	Set the link to the next filter set to be executed after the current
	filter run. Do not make a loop with many filter sets.

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Check to enable the Filter Rule	DL L N D	
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:	, , , , , , , , , , , , , , , , , , ,	
Clear sessions when schedule ON:	Enable	
Direction:	LAN/DMZ/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:	Block Immediately	
Branch to Other Filter Set:	None 😽	
Sessions Control	0 / 120000	
MAC Bind IP	Non-Strict 🗸	
Quality of Service	None 🗸	
Load-Balance policy	Auto-Select V	
<u>User Management</u>	None 🗸	
APP Enforcement:	None 🗸	
URL Content Filter:	None 🗸	
Web Content Filter:	None	
Advance Setting	Edit	

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

Item	Description			
	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.			
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.			
	IP Address Edit - Windows Internet Explorer Intp://192.168.1.5/doc/spfspedt.htm			
	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			
	IP Group None 🖌			
	or IP Groupt None 💙			
	or IP Object None V			
	or IP Object None 🛩			
	or IPv6 Object None 🗸			
	or IPv6 Object None 🗸			
	or IPv6 Object None 🔽			
	OK Close			
	To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and Objects as the Address Type.			
	Group and Objects 🐱			
	Any Address			
	Single Address			
	Range Address			
	Subnet Address			
	Group and Objects			
	From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to above			
	want to apply. Or use the IP Object drop down list to choose the object that you want			
	the object that you want.			
Service Type	Click Edit to access into the following dialog to choose a suitable service type.			

Item	Description			
	3 Service Type Edit - Microsoft Internet Explorer			
	Service Type Edit			
	Service Type Group and Objects			
	Protocol TCP/UDP			
	Source Port = 137 ~139 Destination Port = 1 ~65635			
	Service Group None V			
	or Service Object None or Service Object None			
	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, it			
	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			
	Group and Objects Protocol Specify the protocol(c) which this filter rule will			
	Protocol - Specify the protocol(s) which this filter rule will apply to.			
	Source/Destination Port –			
	(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.			
	(!=) – when the first and last value are the same, it indicates			
	all the ports except the port defined here; when the first			
	and last values are different, it indicates that all the ports			
	except the range defined here are available for this service type.			
	(>) – the port number greater than this value is available.			
	(<) – the port number less than this value is available for this			
	profile.			
	Service Group/Object - Use the drop down list to choose the one that you want.			
Fragments	Specify the action for fragmented packets. And it is used for Data Filter only.			
	<i>Don't care</i> -No action will be taken towards fragmented packets.			
	<i>Unfragmented</i> - Apply the rule to unfragmented packets.			
	<i>Fragmented</i> - Apply the rule to fragmented packets.			
	<i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.			
Filter	Specifies the action to be taken when packets match the rule.			
	Block Immediately - Packets matching the rule will be			
	dropped immediately.			

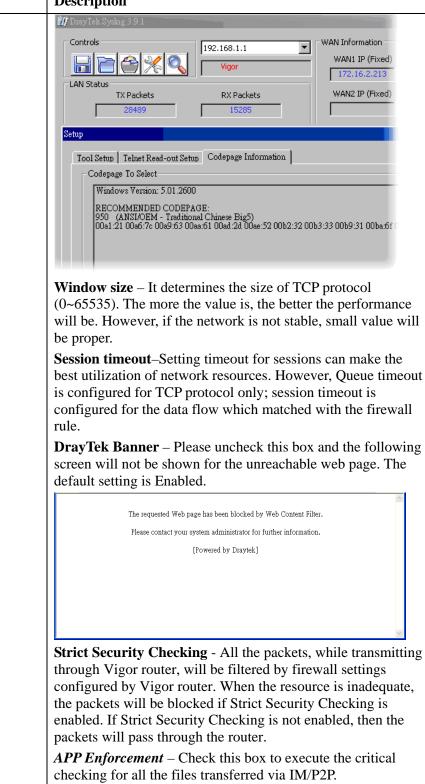
Item	Description	
	Pass Immediately - Packets matching the rule will be passed immediately.	
	Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.	
	Pass If No Further Match - A packet matching the rule, and that does not match further rules, 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.	
MAC Bind IP	 Strict – Make the MAC address and IP address settings configured in IP Object for Source IP and Destination IP be bound for applying such filter rule. No-Strict - no limitation. 	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default	
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 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 select, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of	



Item	Description		
	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 Aler 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 Aler for more detailed information. 		
Advance Setting	Click Edit to open the following window. However, it is		
	strongly recommended to use the default settings here.		
	http://192.168.1.1/doc/ipfedrady.htm - Microsoft Internet Explorer		
	Electronilli de Elda Eldas Contes Elda Eldas Dada		
	Firewall >> Edit Filter Set >> Edit Filter Rule		
	Firewall >> Edit Filter Set >> Edit Filter Rule Filter Set 1 Rule 1 Advance Setting		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I		
	Filter Set 1 Rule 1		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: E5535		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Strict Security Checking		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Compage in the second seco		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Strict Security Checking		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Compage in the second seco		
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Vindow size: E5535 Session timeout: 1440 Minute DrayTek Banner: Strict Security Checking APP Enforcement OK Close		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: 65535 Session timeout: 1440 DrayTek Banner: Strict Security Checking APP Enforcement OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: Esssion timeout: 1440 DrayTek Banner: Strict Security Checking APP Enforcement OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Strict Security Checking APP Enforcement Image: OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Strict Security Checking Strict Security Checking Image: APP Enforcement Image: OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: Bession timeout: It440 DrayTek Banner: Strict Security Checking APP Enforcement OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage		
	Filter Set 1 Rule 1 Advance Setting Codepage Window size: Session timeout: 1440 DrayTek Banner: Vindow Strict Security Checking APP Enforcement OK Close Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do		

Itom	
nem	

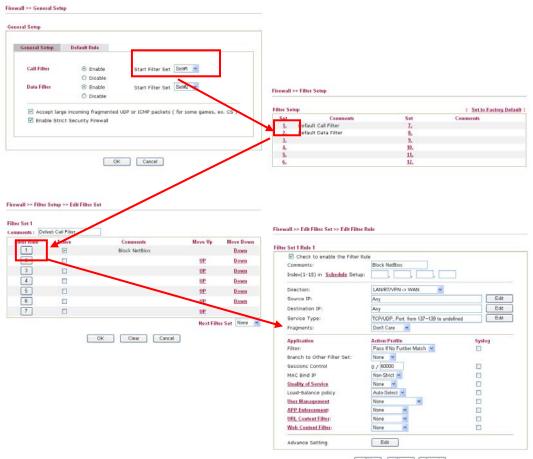
Description



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

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.

Enable SYN flood defense Enable UDP flood defense Enable ICMP flood defense	Threshold Timeout Threshold Timeout	50 packets / sec 10 sec 150 packets / sec	
	Threshold	150 packets / sec	
		packets / sec	
Enable ICMD flood defense	Timeout		
Enable ICMP flood defense		10 sec	
	Threshold	50 packets / sec	
	Timeout	10 sec	
Enable Port Scan detection	Threshold	150 packets / sec	
Block IP options	🗌 Block TCP fla	ag scan	
Block Land	🗌 Block Tear Drop		
Block Smurf	Block Ping of Death		
Block trace route	Block ICMP fragment		
Block SYN fragment	📃 Block Unassi	gned Numbers	
Block Fraggle Attack			

Item	Description
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Select All	Click this button to select all the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per



Item	Description
	second and 10 seconds, respectively. That means, when 150 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet.
	The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.
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. That means, when 150 packets per second received, they will be regarded as "attack event".
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	 Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the

Description		
Internet might be dropped.		
Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .		
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.		
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.		
Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.		
Check the box to activate the 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.		
We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected. System Maintenance >> SysLog / Mail Alert Setup SysLog / Mail Alert Setup SysLog / Mail Alert Setup SysLog / Mail Alert Setup SysLog / Mail Alert Setup Server IP Address Destination Port Firewall Log VPN Log Server Subscription Call Log Seture / Call Log Wan Log Seture / De Sattack Seture / Seture		

Item	Description
	Controls VMM 52-004 TX Packets TX Satur LAN 52-004 Vagor Series Vagor Series Vagor Series Vagor Series LAN 52-004 TX Packets BX Packets Status Status Status 4175 5664 172-16-3-229 2959 126 Phrevil Log: VYB Log: User Accem Log: Coll Log: WAN Log: Others Network Information: Rel Table Traffic Graph.
	Time Hook Message Jan 1 00:00:42 Tigge Dol 5 yrg, flood Block(10) 192 160 1.115,10565 -> 192 160 1.1.22 PR 6(bg) inn 20:40 - 2.794775 Jan 1 00:00:34 Tigger Dol mmg_Thood Block(10) 192 160 1.115 -> 192
	K AGS Salue (b) Sealer

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

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.



Dray Tek

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.

neral Setup				
Mode:	Rule-Based	v		
Web Aut Notice :	thentication:	HTTPS V		
1. User I in use 2. Users The fi 3. Other	er-based firewa match the ab rewall rules po wise, authent	ove lists will not be required licy will still valid. ication required for users no	for authentication. t matched the above lists	
	Page (Max 255	esignated in the user profile characters)		to Factory Default
-	-	ot language='javascript'> p://www.draytek.com' <th>ipt></th> <td></td>	ipt>	

Available settings are explained as follows:

Item	Description
Mode	There are two modes offered here for you to choose. Each mode will bring different filtering effect to the users involved.
	User-Based - If you choose such mode, the router will apply the filter rules configured in User Management>>User Profile to the users.
	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.
Web Authentication	Choose HTTP or HTTPS as the protocol used by users to log into the web page.
	HTTPS
Landing Page	Type the information to be displayed on the first web page when the LAN user accessing into Internet via such router.

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

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>	Dial-In User	<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

User Management >> User Profile(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 (Dial-In User) are factory default settings and only few settings for them can be modified.

User Management >>User Profile(Reserved)

Profile Index 3	
Enable this account	
User Name	LAN_User_Group1
Password	
Confirm Password	
Idle Timeout	10 min(s) 0:Unlimited
Max User Login	0 0:Unlimited
External Server Authentication	None 💙
Log	None 💌
Pop Browser Tracking Window	\checkmark
Authentication	🗹 Web 🗹 Alert Tool 🗹 Telnet
Landing Page	

Index(1-15) in <u>Schedule</u> Setup:	
Enable Time Quota 0 mir	n. + - 0 min.
Enable Data Quota 0	
Reset quota to default when sche	

Clear

Cancel

Refresh

Available settings are explained as follows:

OK

Item	Description
Enable this account	Check this box to enable such user profile.
User Name	Type a name for such user profile (e.g., <i>LAN_User_Group_1</i> , <i>WLAN_User_Group_A</i> , <i>WLAN_User_Group_B</i> , etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the User Name specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router. However the accessing operation will be restricted with the conditions configured in this user profile.
Password	Type a password for such profile (e.g., <i>lug123</i> , <i>wug123</i> , <i>wug456</i> , etc). When a user tries to access Internet through this router, an authentication step must be performed first. The user has to type the password specified here to pass the authentication. When the user passes the authentication, he/she can access Internet via this router with the limitation configured in this user profile.
Confirm Password	Type the password again for confirmation.
Idle Timeout	If the user is idle over the limitation of the timer, the network connection will be stopped for such user. 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.



Item	Description		
Policy	It is available only when User-Based mode selected in User Management>>General Setup .		
	Default Default [Create New Policy]		
	 Default – If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile. Create New Policy – If you choose such item, the following page will be popped up for you to define another filter rule as a new policy. 		
	Filter Set 1 Rule 2 Comments: Index(1-15) in Schedule Setup:		
	Direction: LAN/RT/VPN -> WAN Source IP: Any Destination IP: Any Service Type: Any		
	For the detailed configuration, simply refer to Firewall>>Filter Rule . The firewall filter rules that are not selected in Firewall>>General>>Default rule can be available for use in User Management>>User Profile .		
External Service Authentication	The router will authenticate the dial-in user by itself or by external service such as LDAP server or Radius server. If LDAP or Radius is selected here, it is not necessary to configure the password setting above.		
	None None LDAP Radius		
Log	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.		

Item	Description	
Authentication	Any user (from LAN side or WLAN side) tries to connect to Internet via Vigor router must be authenticated by the router first. There are three ways offered by the router for the user to choose for authentication.	
	Web – If it is selected, the use can type the URL of the router from any browser. Then, a login window will be popped up and ask the user to type the user name and password for authentication. If succeed, a Welcome Message (configured in User Management >> General Setup) will be displayed. After authentication, the destination URL (if requested by the user) will be guided automatically by the router.	
	Alert Tool – If it is selected, the user can open Alert Tool and type the user name and password for authentication. A window with remaining time of connection for such user will be displayed. Next, the user can access Internet through any browser on Windows. Note that Alert Tool can be downloaded from DrayTek web site. Telnet – If it is selected, the user can use Telnet command to	
	perform the authentication job.	
Landing Page	When a user tries to access into the web user interface of Vigor3200 series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in User Management>>General Setup . Check this box to enable such function.	
Index (1-15) in Schedule Setup	 You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page. 	
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. Then, type the number of time (unit is minute) which is available for the user (using such profile) to access Internet in the value box. The unit is minutes. - Click this box to set and increase the time quota for such profile.	
	- Click this box to decrease the time quota for such profile.	
Enable Data Quota	Data Quota means the total amount for data transmission allowed for the user. The unit is MB.	
	 Click this box to set and increase the data quota for such profile. Click this box to decrease the data quota for such profile. 	
Reset quota to default when scheduling time expired	Set default time quota and data quota for such profile. When the scheduling time is up, the router will use the default quota settings automatically.	



Item	Description
	Enable – Check it to use the default setting for time quota and data quota.
	Default Time Quota – Type the value for the time manually.
	Default Data Quota – Type the value for the data manually.

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

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.

ame:	
ailable User Objects	Selected User Objects(Max 32 Objects
1-admin 2-Dial-In User	
	>>
	~

Available settings are explained as follows:

Item	Description
Name	Type a name for this user group.
Available User Objects	You can gather user profiles (objects) from User Profile page

Item	Description	
	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 User Objects	Click button to add the selected user objects in this box.	

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

4.5.4 User Online Status

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

Current Time : 08-23 07:39:57			Refresh S	econds: 10 💌 i	Page: 1 💌	<u>Refresh</u>
Index	Active User 🗸	IP Address	Last Login Time			
1	<u>admin</u>	192.168.1.10	08-23 06:01:11	Unlimited	Unlimited	<u>Block Logout</u>
					T	otal Number : 1

User Management >> User Online Status

Available settings are explained as follows:

Item	Description	
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.	
	Refresh Seconds: 10 🛩 10 15 30	
Refresh	Click this link to refresh this page manually.	
Index	Display the number of the data flow.	
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	



Item	Description	
	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 Inter Unblock – 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).

Obje	cts Setting
📄 🕨 II	P Object
📄 🕨 II	P Group
📄 🕨 II	Pv6 Object
📄 🕨 II	Pv6 Group
🕨 🕨 S	ervice Type Object
🕨 🕨 S	ervice Type Group
🕨 🕨 к	eyword Object
🕨 🕨 к	eyword Group
E F	ile Extension Object
🕨 Þ s	MS/Mail Service Object
	otification Object

4.6.1 IP Object

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

Objects Setting	>>	P Obj	ect
-----------------	----	-------	-----

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>	

 $<<\underline{1.32} | \underline{33.64} | \underline{65.96} | \underline{97.128} | \underline{129.160} | \underline{161.192} >>$

<u>Next</u> >>

Dray Tek

Available settings are explained as follows:

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

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

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

Objects Setting >> IP Object

IP Object Profiles:

Index	Name	Ind
<u>1.</u>		17
<u>2.</u>		<u>18</u>
3.		10

2. The configuration page will be shown as follows:

Objects Setting >> IP Object

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

Available settings are explained as follows:

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Interface	allowed. Choose a proper interface. LAN/DMZ/RT/VPN Any LAN/DMZ/RT/VPN WAN For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in Edit Filter Rule , then all the IP	



Item	Description		
	addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page.		
Address Type	Determine the address type for the IP address. Select Single Address if this object contains one IP address only.		
	Select Range Address if this object contains several IPs within a range.		
	Select Subnet Address if this object contains one subnet for IP address.		
	Select Any Address if this object contains any IP address.		
	Select Mac Address if this object contains Mac address.		
	Range Address Any Address Single Address Range Address Subnet Address Mac Address		
MAC Address	Type the MAC address of the network card which will be controlled.		
Start IP Address	Type the start IP address for Single Address type.		
End IP Address	Type the end IP address if the Range Address type is selected.		
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.		
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.		

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

Objects Setting >> IP Object

IP 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>

Dray Tek

4.6.2 IP Group

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

Objects Se	etting >>	IP	Group
-------------------	-----------	----	-------

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

Available settings are explained as follows:

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

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

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

Objects Setting >> IP Group

IP Group Table:

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

Obi	iects	Setting	>>	IP	Group
~~~	0.000	ooung			o. o. p

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

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

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

Objects Setting >> IP Group

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

## 4.6.3 IPv6 Object

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

Ob	iects	Setting	>>	IPv6	Ob	iect
00	ecis	Setting	~~	11 00	00	jeu

/6 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>	

Available settings are explained as follows:

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

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

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

### Objects Setting >> IPv6 Object

### IPv6 Object Profiles:

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

Objects Setting >> IPv6 Object

Name:	
Address Type:	Subnet Address 💌
Mac Address:	00:00:00:00:00
Start IP Address:	
End IP Address:	
Prefix Len:	
Invert Selection:	

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	Determine the address type for the IPv6 address. Select <b>Single Address</b> if this object contains one IPv6 address only.
	Select <b>Range Address</b> if this object contains several IPv6s within a range.
	Select <b>Subnet Address</b> if this object contains one subnet for IPv6 address.
	Select <b>Any Address</b> if this object contains any IPv6 address.
	Select Mac Address if this object contains Mac address.
	Range Address Any Address Single Address Range Address Subnet Address Mac Address
MAC Address	Type the MAC address of the network card which will be controlled.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.

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



## 4.6.4 IPv6 Group

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

Objects Setting >> IP Grou	ip
----------------------------	----

IPv6 Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Available settings are explained as follows:

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

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

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

Objects Setting >> IP Group

### IPv6 Group Table:

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

Name:	v6_group1	
Available IPv6 Objects	Selected IPv6 Object	cts
1-v6_ob_1		
	>>	
	~~ )	

Objects Setting >> IP∨6 Group

OK Clear Cancel

Available settings are explained as follows:

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

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

Objects Setting >> IP Group

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

## 4.6.5 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
	Name		Hame
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

<< <u>1-32</u> | <u>33-64</u> | <u>65-96</u> >>

<u>Next</u> >>

Available settings are explained as follows:

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

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

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

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

### Service Type Object Profiles:

Index	Name	
1.		
2.		

Objects Setting >> Service Type Object Setup

Name	www.
Protocol	TCP 6
Source Port	= 💙 1 👡 65535
Destination Port	= 🖌 80 ~ 80

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         IGMP       1         TCP       UDP         TCP/UDP       0
Source/Destination Port	<ul> <li>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</li> <li>(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.</li> <li>(!=) – when the first and last value are the same, it indicates a lalt 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.</li> <li>(&gt;) – the port number greater than this value is available.</li> <li>(&lt;) – the port number less than this value is available for this profile.</li> </ul>

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

Service Typ	be Object Profiles:
Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
<u>3.</u>	
4.	

## Service Type Object Profiles:

## 4.6.6 Service Type Group

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

Objects Setting >> Service Type Group

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

Available settings are explained as follows:

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

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

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

### **Objects Setting >> Service Type Group**

### Service Type Group Table:

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

Objects Setting >> Service Type Group Setup

Name:	VolP			
vailable Service	Type Objects	Sel	ected Service Type Objects	
-SIP -RTP				
		<u> </u>		
		_ << ]		

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Available Service Type Objects	All the available service objects that you have added on <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

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

Objects Setting >> Service Type Group

Service Type Group	Table:		Set to Factory Default
Group	Name	Group	Name
<u>1.</u>	VoIP	<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
4			

## 4.6.7 Keyword Object

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

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

Objects Setting >> Keyword Object

Available settings are explained as follows:

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

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

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

#### Objects Setting >> Keyword Object

#### **Keyword Object Profiles:**

Index	Name	
1.		
2.		
3.		

Objects Setting >>	Keyword Object Setup
--------------------	----------------------

lame	
Contents	
	Limit of Contents: Max 3 Words and 63 Characters.
	Each word should be separated by a single space.
	You can replace a character with %HEX.
	Example: Contents: backdoo%72 virus keep%20out
	Result:
	1. backdoor
	2. virus
	3. keep out

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile, e.g., game.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

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

Objects Setting >> Keyword Object

Keyword Object P	rofiles:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>	Keyword-1	<u>17.</u>	
<u>2.</u>	Keyword-2	<u>18.</u>	
<u>3.</u>		<u>19.</u>	
1		20	

## 4.6.8 Keyword Group

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

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

Objects Setting >> Keyword Group

Available settings are explained as follows:

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

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

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

### Objects Setting >> Keyword Group

### Keyword Group Table:

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

file Index : 1	
Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Object
1-Keyword-1 2-keyword-2	
2.46399010.2	· · · · · · · · · · · · · · · · · · ·

Available settings are explained as follows:

Item	Description	
Name	Type a name for this group.	
Available Keyword Objects	You can gather keyword objects from <b>Keyword Object</b> page within one keyword group. All the available Keyword objects that you have created will be shown in this box.	
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.	

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

Objects Setting >> Keyword Group

eyword Group Tab	le:		Set to Factory Default
Index	Name	Index	Name
<u>1.</u>	night	<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>	

**Dray** Tek

### 4.6.9 File Extension Object

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

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.

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

Objects Setting >> File Extension Object

#### Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all of the settings and return to factory default settings.	
Index	Display the profile number that you can configure.	
Name	Display the name of the object profile.	

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

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

#### Objects Setting >> File Extension Object

#### File Extension Object Profiles:

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

Objects Setting >> File Extension Object Setup

Profile Index: 1	Pro	ofile Name:					
Categories			Fi	e Extensio	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	.mov .wmv	.mpe .3gp	.mpeg	.mpg .3gpp2	.mp4
Audio Select All Clear All	🗌 .aac 🗌 .ra	.aiff .ram	□.au □.vox	.mp3 .wav	.m4a .wma	□.m4p	🗆 .ogg
Java Select All Clear All	□.class □.jse	🗌 .jad 🗌 .jsp	🗌 .jar 🗌 .jtk	🗌 .jav	🗌 .java	.jcm	🗌 .js
ActiveX Select All Clear All	□ .alx □ .viv	.apb .vrm	.axs	.ocx	.olb	.ole	.tlb
Compression Select All Clear All	.ace .rar	🗌 .arj 🗌 .sit	.bzip2	.bz2	.cab	.gz	.gzip
Executation Select All Clear All	.bas .scr	.bat	.com	.exe	.inf	.pif	.reg
		ок	Clear	Cancel			

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile.

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

Objects Setting >> File Extension Object

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

**Dray** Tek

## 4.6.10 SMS/Mail Service Object

### **SMS Service Object**

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

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

Object Settings >> SMS / Mail Service Object

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Index	Display the profile number that you can configure.
Profile Name	Display the name for such SMS profile.
SMS Provider	Display the service provider which offers SMS service.

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

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

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

SMS Provider	Mail Server
Index	Profile Name
1.	
<u>2.</u>	
<u>3.</u>	

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

Object Settings >> SMS / Mail Service Object

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such SMS profile.
Service Provider	Use the drop down list to specify the service provider which offers SMS service.
Username	Type a user name that the sender can use to register to selected SMS provider.
Password	Type a password that the sender can use to register to selected SMS provider.
Quota	Type the number of the credit that you purchase from the service provider chosen above. Note that one credit equals to one SMS text message on the standard route.
Sending Interval	To avoid quota being exhausted soon, type time interval for sending the SMS.

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider
<u>1.</u>	Line_down	kotsms.com.tw (TW)
<u>2.</u>		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)

### **Customized SMS Service**

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

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

Object Settings >> SMS / Mail Service Object

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

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

```
Profile Index: 9
```

Profile Name	Custom 1	
Service Provider		
Please contact with your SMS p	provide to get the ex	act URL String
eq:bulksms.vsms.net:5567/eapi	/submission/send_sm	ns/2/2 0?username=###tytliser###
&password=###txtPwd###&ms		
&password=###txtPwd###&ms		
&password=###txtPwd###&ms Username		
&password=###txtPwd###&ms Username Password	sisdn=###txtDest##	

Available settings are explained as follows:

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

Username	Type a user name that the sender can use to register to selected SMS provider.
Password	Type a password that the sender can use to register to selected SMS provider.
Quota	Type the number (e.g., 5, 10, etc.) of the SMS text message allowed to be sent out by this profile. When WAN interface disconnects frequently, the text message will be sent for several time (e.g., 5, 10, etc.) within the time interval. Once the quota ran out, no SMS will be sent out.
	<b>Note</b> : The number of the credit can be purchased from the service provider chosen above. One credit equals to one SMS text message on the standard route.
Sending Interval	Type the shortest time interval for the system to send SMS.

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

### **Mail Service Object**

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

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

SMS Provi	der Mail Server	Set to Factory Default
Index		Profile Name
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		
<u>9.</u>		
<u>10.</u>		

Each item is explained as follows:

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

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

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

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

Object Settings >> SMS / Mail Service Object

2. The configuration page will be shown as follows:

Profile Name	Mail_Notify
SMTP Server	192.168.1.98
SMTP Port	25
Sender Address	carrie@draytek.com
Authentication	
Username	John
Password	12345
Sending Interval	60 (seconds)

Object Settings >> SMS / Mail Service Object

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such mail service profile.
SMTP Server	Type the IP address of the mail server.
SMTP Port	Type the port number for SMTP server.
Sender Address	Type the e-mail address of the sender.
Authentication	The mail server must be authenticated with the correct username and password to have the right of sending message out. Check the box to enable the function. Username – Type a name for authentication. Password – Type a password for authentication.
Sending Interval	Define the interval for the system to send the SMS out.

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

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server		Set to Factory Default
Index		Profile Name	
<u>1.</u>		Mail_Notify	
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			

## 4.6.11 Notification Object

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

You can set an object with different monitoring situation.

Object Settings >> Notification Object

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

Each item is explained as follows:

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

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

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

Object Settings >> Notification Object

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

**Dray** Tek

Object Settings >> Notification Object

rofile Name	Notify_attack		
Category		Status	
WAN	🗹 Disconnected	Reconnected	
VPN Tunnel	🗹 Disconnected	Reconnected	

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such notification profile.
Category	Display the types that will be monitored.
Status	Display the status for the category. You can check the box you want to be monitored.

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

Object Settings >> Notification Object

		Set to Factory Default
Index	Profile Name	Settings
<u>1.</u>	Notify_attack	WAN
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

# 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

PP Enforcement Profile Table:			Set to Factory Defaul		
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>			

#### Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the 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 / Ap	oplication	MSN	YahooIM	AIM(<=	v5.9)	ICQ
Logi	n					
Messa	ige					
File Tra	nsfer					
Gam	e					
Conference(Video/Voice)						
Other Activities						
	IM	Application				VoIP
🔲 AIM6/7	🔲 QQ/TM	🔲 iChat	🗌 Jabber/G	oogleTalk		
🔲 GoogleChat	🗌 XFire	🔲 GaduGadu	📃 Paltalk			🗌 Kubao
🗌 Qnext	POCO/PP365	🗌 AresChat	Aliww		🗌 Gizmo	SIP/RTP
КС	🗌 Lava-Lava	🗌 ICU2	🗌 iSpQ		🗌 TelTel	🔲 TeamSpeal
UC	🗌 MobileMSN	🔲 BaiduHi				
	W	/eb IM ( * = mo	re than one addre	ess)		
	eMessenger	WebMSN	meebo*	eBuddy		_ovelM*
	ICQ Java*	ICQ Flash*	goowy*	<u>IMhaha</u>		etMessenger
WebIM URLs	IMUnitive*	Wablet*	mabber*	MSN2G	<u>)* k</u>	oollM
	MessengerFX*	<u>MessengerAdi</u>	<u>ctos WebYahoolM</u>			

Available settings are explained as follows:

Item	Description		
Profile Name	Type a name for the CSM profile.		
Select All	Click it to choose all of the items in this page.		
Clear All	Uncheck all the selected boxes.		

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

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.

rofile Index : 1	Profile Name:				
IM	P2P	Protocol	Misc		
Select All	Clear All	]			
Protoc	ol		Δ	pplications	
🗌 SoulSeek		SoulSeek			
🗌 eDonkey		eDonkey, e	Mule, Shareaza		
🗌 FastTrack		KazaA, Bea	arShare, iMesh		
🗌 OpenFT		KCeasy, FilePipe			
🔲 Gnutella		BearShare, Limewire, Shareaza, Foxy, KCeasy			
🔲 OpenNap		Lopster, XNap, WinLop			
🔲 Bit Torrent		BitTorrent, BitSpirit, BitComet			
🗌 Winny		Winny, WinMX, Share			
		Other	P2P Applications		
🗌 Xunlei	📃 Vaga	ia [	PP365	POCO	🗌 Clubbox
🗌 Ares 🗌 ezPeer 📃 Pando 📃 Huntmine 📃 Kuwo					

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

CSM >> A	PP En	forcement	Profile
----------	-------	-----------	---------

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

# The items categorized under Misc.

SM >> APP Enforce	ment Profile			
rofile Index : 1 P	rofile Name:			
IM	P2P Proto	col Misc		
Select All	Clear All			
		Tunneling		
Socks4/5	PGPNet	HTTP Proxy	🗌 Tor	VNN VNN
SoftEther	MS TEREDO	🗌 Wujie/UltraSurf	🗌 Hamachi	HTTP Tunnel
🗌 Ping Tunnel	Tiny VPN	🗌 RealTunnel	🗌 DynaPass	🗌 UltraVPN
FreeU	Skyfire 🗌			
		Streaming		
Пммя	RTSP	TVAnts	PPStream	<b>PPTV</b>
EeiDian		NSPlayer		
SopCast		TVUPlayer	MySee	Joost
FlashVideo	SilverLight	Slingbox		
		Remote Control		
VNC	🔲 Radmin	🔲 SpyAnywhere	ShowMyPC ShowMyPC	📃 LogMeIn
🗌 TeamViewer	🔲 Gogrok	🔲 RemoteControlPro	CrossLoop	🗌 WindowsRDP
pcAnywhere	🗌 Timbuktu	WindowsLiveSync	SharedView	
		Web HD		
HTTP Upload	🗌 HiNet SafeBox	MS SkyDrive	GDoc Uploader	🗌 ADrive
MyOtherDrive	🗖 Mozy	BoxNet	OfficeLive	
	(	OK Cancel		

# 4.7.2 URL Content Filter Profile

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

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

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

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

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

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

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

ОK	

Fach	item	is	exp	lained	28	fol	lows.
Lach	num	19	CAP	lanicu	as	101	10 10 5.

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

Default Message	You can type the message manually for your necessity or
	click this button to get the default message which will be
	displayed on the field of Administration Message.

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

#### CSM >> URL Content Filter Profile

Profile Name:		
Priority:	Both : Pass	V Log: None V
1.URL Access	Control	
Enab	le URL Access Control	Prevent web access from IP address
Actio	on:	Group/Object Selections
Pass	~	Edit
2.Web Featur	e	
Enab	le Restrict Web Feature	
Actio	on:	
Pass	🗠 🗌 Cookie 🗌 Proxy	File Extension Profile: None 👻

Item	Description	
Profile Name	Type a name for the CSM profile.	
Priority	It determines the action that this router will apply.	
	<b>Both: Pass</b> – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.	
	<b>Both: Block</b> –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.	
	<b>Either: URL Access Control First</b> – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determin the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.	
	<b>Either: Web Feature First</b> –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determin the priority for the actions executed. For this one, the router	

Item	Description			
	will process the packages with the conditions set below for web feature first, then URL second.			
	Both : Pass 🔽			
	Both : Block Either : URL Access Control First Either : Web Feature First			
Log	None – There is no log file will be recorded for this profile.			
0	<b>Pass</b> – Only the log about Pass will be recorded in Syslog.			
	Block – Only the log about Block will be recorded in Syslog			
	All – All the actions (Pass and Block) will be recorded in Syslog.			
	None V None Pass Block All			
URL Access Control	Enable URL Access Control - Check the box to activate			
	URL Access Control. Note that the priority for URL Access			
	<b>Control</b> is higher than <b>Restrict Web Feature</b> . 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.			
	<b>Prevent web access from IP address</b> - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.			
	Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. <i>Pass</i> - Allow accessing into the corresponding webpage with the keywords listed on the box below.			
	<ul><li>Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.</li><li>If the web pages do not match with the keyword set here, it</li></ul>			
	will be processed with reverse action.			
	Block V			
	Pass Block			
	Group/Object Selections – The Vigor router provides			
	several frames for users to define keywords and each frame			
	supports multiple keywords. The keyword could be a noun, a			
	partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon			
	In addition, the maximal length of each frame is 32-character			
	long. After specifying keywords, the Vigor router will			



Item	Description			
	string matched to any user-	nest to the website whose URL defined keyword. It should be lified the blocking keyword list i gor router performs.		
	🏉 Group/Object Edit - Windows Internet Explorer			
	C http://192.168.1.1/doc/efkwgob.htm	V		
	Object/Group Edit			
	Keyword Object or Keyword Object	None V		
	or Keyword Object	None 👻		
	or Keyword Object	None 💌		
	or Keyword Object	None 💙		
	or Keyword Object or Keyword Object	None V		
	or Keyword Object	None 🗸		
	or Keyword Group	None 💌		
	or Keyword Group or Keyword Group	None V		
	or Keyword Group	None V		
	or Keyword Group	None 💌		
	or Keyword Group	None 🗸		
	or Keyword Group or Keyword Group	None V		
	ОК	Close		
Web Feature	Enable Restrict Web Feat	ture - Check this box to make th		
	keyword being blocked or passed.			
	Access Control First or Ei selected. Pass allows access webpage with the keyword Pass - Allow accessing into the keywords listed on the	the corresponding webpage with box below.		
	with the keywords listed or	into the corresponding webpage the box below. tch with the specified feature set		
	here, it will be processed with reverse action.			
	-	filter out the cookie transmission		
	<b>Proxy</b> - Check the box to recontrol efficiently the limit	eject any proxy transmission. To ed-bandwidth usage, it will be of locking mechanism that filters of oading from web pages.		
		block the file upload by way of		
		hoose one of the profiles that yo ng>> File Extension Objects		

Item	Description
	File Extension Profile: None None 1-default

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

## 4.7.3 Web Content Filter Profile

CSM >> Web Content Filter Profile

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

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

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

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

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

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

Setup Query Server			
Setup duery Server	auto-selected		Find more
Setup Test Server	auto-selected		Find more
Web Content Filter Profile	Fable:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>	Default	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
Administration Message	(Max 255 characters)	Default Mess	age Cache : L1 + L2 Cache 🛩
that is categorize	ed with %CL% has b act your system admini	een blocked b	-
111011001011.() 0010011	() DOULY		2

#### Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize

Item	Description
	searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Set to Factory Default	Click this link to retrieve the factory settings.
Default Message	You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of <b>Administration Message</b> .
Cache	<b>None</b> – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.
	L1 – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.
	L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.
	<b>L1+L2 Cache</b> – the router will check the URL with fast processing rate combining the feature of L1 and L2.

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



CSM >> Web Content Filter Profile	CSM >>	Web	Content	Filter	Profil
-----------------------------------	--------	-----	---------	--------	--------

Profile Index: 1			
Profile Name: Default			Log: Block 🚩
Black/White List			
🗌 Enable			
Action:	Gi	roup/Object Selections	
Block 💙			Edit
Action: Block 🗸			
Groups	Categories		
Child Protection	Alcohol & Tobacco	Coincipal Activity	Combline .
Select All	✓ Alconol & Tobacco ✓ Hate & Intolerance	Criminal Activity	Gambling
Clear All		☑ Illegal Drug ☑ Violence	✓ Nudity
Clear All	Porn & Sexually	Sex Education	✓ Weapons ✓ Tasteless
	School Cheating	Sex Education	I asteless
	🗹 Child Abuse Images		
Leisure	Entertainment	Games	Sports
Select All	Travel	Leisure & Recreation	Fashion & Beauty
Clear All			<u> </u>
Business			
Select All	Compromised	🗌 Dating & Personals	Education
Clear All	Einance	🗌 Government	🗌 Health & Medicine
	News	🗌 Non-profits & NGOs	Personal Sites
	Politics	🗌 Real Estate	🗌 Religion
	🗌 Restaurants & Dining	🔲 Shopping	Translators
	🗌 General	Cults	Greeting cards
	🗌 Image Sharing	Network Errors	Parked Domains
	🔲 Private IP Addresses	Uncategorised Sites	
	OK	Cancel	

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

Item	Description
	<b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.
	If the web pages do not match with the specified feature set here, it will be processed with reverse action.
Log	None – There is no log file will be recorded for this profile.         Pass – Only the log about Pass will be recorded in Syslog.         Block – Only the log about Block will be recorded in Syslog.         All – All the actions (Pass and Block) will be recorded in Syslog.         Block ▼         None         Pass         Block

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

# 4.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Ban	dwidth Management
	Sessions Limit
1 Þ.	Bandwidth Limit
- Þ.	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.

🔘 Enable	⊙ Disable				
Default Ma	x Sessions: 10	)			
Limitation L	ist				
Index S	tart IP	End IP	Max	Sessions	
Specific Lin Start IP:		End IP:			
Maximum S	essions:	Add Ed	it Delete	]	
inistration Me	<mark>ssage</mark> (Max 256	i characters)			Default Messa
	<u> </u>				
e Schedule					
	) in <u>Schedule</u> 9	Satura			
		out settings will be			

Bandwidth Management >> Sessions Limit

Available settings are explained as follows:

Item	Description
Enable	Click this button to activate the function of limit session.

Item	Description
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.
Delete	Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
Default Message	Click this button to apply the default message offered by the router.
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.

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

## 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.

	to TD Douted Cubrot	Disable	
	to IP Routed Subnet		
Default TX Limit: 2000		fault RX Limit: 8000	Kbps 🗡
Allow auto adjustn	ent to make the bes	t utilization of <u>available</u>	<u>bandwidth</u> .
Limitation List			
Index Start IP	End IP	TX limit RX limi	t Shared
1			
Conselling Lington days			
Specific Limitation			-
Start IP:	End IP:		
💿 Each 🛛 🔘 Shared			
TX Limit:	Kbps 🔽 RX Limit:	Kbps 🗸	
	Add Update	Delete	
Smart Bandwidth Lir	nit		
For any LAN IP Not in	Limitation List, whos	e session number exce	eds 1000
TX Limit : 200	Kbps 💌 RX Limit :		
TX/RX, a setting of "0"	means unlimited ban	dwidth.	
dule			
x(1-15) in <u>Schedule</u> Se	tup:,	,,	
Action and Idle Times	ut settings will be igr	ored	

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

	Allow auto adjustment Check this box to make the best utilization of available bandwidth.			
Limitation List	Display a list of specific limitations that you set on this web page.			
Specific Limitation	Start IP - Define the start IP address for limit bandwidth.			
	End IP - Define the end IP address for limit bandwidth.			
	<ul> <li>Each /Shared - Select Each 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 Shared 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.</li> <li>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.</li> </ul>			
	<b>RX limit -</b> Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.			
	Add - Add the specific speed limitation onto the list above.			
	<b>Update -</b> Allow you to edit the settings for the selected limitation.			
	<b>Delete -</b> Remove the selected settings existing on the limitation list.			
Time Schedule	Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application >> Schedule web page and you can use the number that you have set in that web page.			

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

# 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?

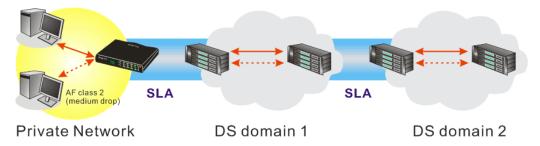
There are two components within Primary configuration of QoS deployment:

- 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.

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN4	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setu
WAN5	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status	Setur

Bandwidth Management >> Quality of Service

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

Enable the First Priority for VoIP SIP/RTP:				
SIP UDP Port: 5060 (Default:5060)				
	ОК			

Item	Description
General Setup	<b>Index</b> – Display the WAN interface number that you can edit.
	<b>Status</b> – Display if the WAN interface is available for such function or not.
	<b>Bandwidth</b> – Display the inbound and outbound bandwidth setting for the WAN interface.
	<b>Direction</b> – Display which direction that such function will influence.
	<b>Class 1/Class2/Class 3/Others</b> – Display the bandwidth percentage for each class.
	<b>UDP Bandwidth Control</b> – Display the UDP bandwidth control is enabled or not.
	<b>Online Statistics</b> – Display an online statistics for quality of service for your reference
	<b>Setup</b> – Allow to configure general QoS setting for WAN interface.
Class Rule	<b>Index</b> – Display the class number that you can edit.
	<b>Name</b> – Display the name of the class.
	Rule - Allow to configure detailed settings for the selected



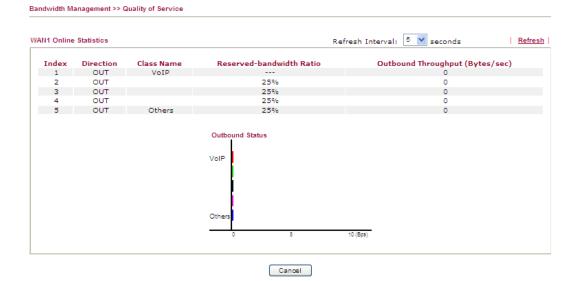
Item	Description
	Class. Service Type - Allow to configure detailed settings for the service type.
Enable the First Priority for VoIP SIP/RTP	When this feature is enabled, the VoIP SIP/UDP packets will be sent with highest priority. SIP UDP Port - Set a port number used for SIP.

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

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

## **Online Statistics**

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.



#### **General Setup for WAN Interface**

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

Bandwidth Managem	Bandwidth Management >> Quality of Service							
WAN1 General Setup								
Enable the QoS		40000						
VVAN	I Inbound Bandwidth	10000 Kbps						
WAN	I Outbound Bandwidth	10000 Kbps						
Index	Class Name	Reserved_bandwidth Ratio						
Class 1		25 %						
Class 2		25 96						
Class 3		25 %						
	Others	25 %						
🔲 Enable UDP Band	dwidth Control	Limited_bandwidth Ratio 25 %						
🔲 Outbound TCP A	CK Prioritize							
	OK Clear	Cancel						

Item	Description
Enable the QoS Control	<ul> <li>The factory default for this setting is checked.</li> <li>Please also define which traffic the QoS Control settings will apply to.</li> <li>IN- apply to incoming traffic only.</li> <li>OUT- apply to outgoing traffic only.</li> <li>BOTH- apply to both incoming and outgoing traffic.</li> </ul>
	Check this box and click <b>OK</b> , then click <b>Setup</b> link again. You will see the <b>Online Statistics</b> link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
	<b>Note:</b> The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.



Item	Description
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of <b>reserved bandwidth to upstream speed</b> and <b>reserved bandwidth to downstream speed</b> .
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

#### Edit the Class Rule for QoS

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

Bandwidth Management >> Quality of Service

sellera	Setup							serr	o Factory De	eraun
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	Setu
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setu

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

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

	dex #1		_		Default
lame	Test		🗹 Ta	ig packets as:	Default
NO	Status	Local Address	Remote Address	DiffServ CodePoint	service Type
1	Empty	-	-	-	-
		4	Add Edit Delet	е	

Bandwidth Management >> Quality of Service

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

ACT		
Ethernet Type	⊙ IPv4 ○ IPv6	
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoi	ANY 🖌	
Service Type	Predefined 🗸	
Note: Please cho	ose/setup the <u>Service Type</u> first.	

Bandwidth Management >> Quality of Service

Item	Description		
ACT	Check this box to invoke these settings.		
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.		
Local Address	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.		
Remote Address	Click the <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.		
Edit	It allows you to edit source address information.		
	Address Type – Determine the address type for the source address. For Single Address, you have to fill in Start IP address and End IP 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.		



Item	Description	
	Those types are predefined in factory. Simply choose the one that you want for using by current QoS.	
	that you want for using by current QoS.	

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

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.

ne T	est		Tag packets as: Default				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type		
1 💿	Active	Any	Any	ANY	ANY		
2 🔿	Active	192.168.1.25	Any	IP precedence 1	SMTP(TCP:25)		
		-	Add Edit Delet	te			

## Edit the Service Type for Class Rule

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

Bandwidth	Management >>	Quality of	Service

senera	Setup							Sett	o Factory De	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	<u>Setup</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	<u>Setup</u>
WANЗ	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	Setu

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

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

Bandwidth Management >> Quality of Service

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

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

Bandwidth Management >> Quality of Service

Service Name	
Service Type	TCP 6
Port Configuration	
Туре	💿 Single i 🔘 Range
Port Number	0 - 0

Available settings are explained as follows:

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

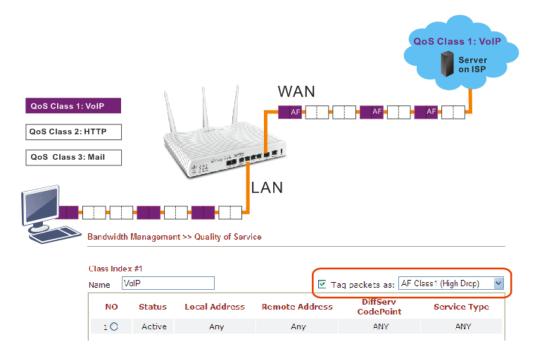
4. After finishing all the settings here, please click **OK** to save the configuration.

By the way, you can set up to 10 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

#### **Retag the Packets for Identification**

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all of them will be tagged with certain header and that will be easily to be identified by server on ISP.

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



# 4.9 Applications

Below shows the menu items for Applications.

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

## 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

Oynamic DNS Setu	p	<u>S</u>	et to Factory Default
📃 Enable Dynam	ic DNS Setup	View Log	Force Update
Auto-Update interval 14400 Min(s) (1~14400)			
Accounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		×
<u>3.</u>	WAN1 First		×

OK Clear All

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



Item	Description	
Enable Dynamic DNS Setup	Check this box to enable DDNS function.	
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.	
View Log	Display DDNS log status.	
Force Update	Force the router updates its information to DDNS server.	
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).	
WAN Interface	Display the WAN interface used.	
Domain Name	Display the domain name that you set on the setting page of DDNS setup.	
Active	Display if this account is active or inactive.	

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

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

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

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	WAN1/WAN2/WAN3/WAN4/WAN5 First - While connecting, the router will use WAN1/WAN2/WAN3 as the first channel for such account. If WAN1/WAN2/WAN3/WAN4/WAN5 fails, the router will use another WAN interface instead. WAN1/WAN2/WAN3/WAN4/WAN5 Only - While

Item	Description	
	connecting, the router will use WAN1/WAN2/WAN3 WAN4/WAN5 as the only channel for such account. WAN1 First WAN1 First WAN2 Only WAN2 First WAN3 Only WAN3 First WAN4 Only WAN5 First WAN5 Only	
Service Provider	Select the service provider for the DDNS account.	
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.	
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.	
Login Name	Type in the login name that you set for applying domain.	
Password	Type in the password that you set for applying domain.	
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.	
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.	
Determine Real WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: <b>WAN IP</b> - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. <b>Internet IP</b> – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.	

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.

chedule:			Set to Factory Default
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	х
<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>	×	<u>14.</u>	×
<u>7.</u>	х	<u>15.</u>	×
<u>8.</u>	×		

#### Applications >> Schedule

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

Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all profiles and recover to factory settings.	
Index	Click the number below Index to access into the setting page of schedule.	
Status	Display if this schedule setting is active or inactive.	

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

To add a schedule:

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

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

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

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

Enable	Schedule Setup	
	Start Date (yyyy-mm-dd) 20	00 🕶 1 💌 1 💌
	Start Time (hh:mm) 0	• : 0 •
	Duration Time (hh:mm)	💌 : O 💌
	Action Fo	rce On 💌
	Idle Timeout	minute(s).(max. 255, 0 for default)
	How Often	
	Once	
	💿 Weekdays	
	🗌 Sun 🗹 Mon 🗹 Tue	🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat

Applications >> Schedule

Item	Description	
Enable Schedule Setup	Check to enable the schedule.	
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.	
Start Time (hh:mm)	Specify the starting time of the schedule.	
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.	
Action	Specify which action Call Schedule should apply during the period of the schedule.	
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.	

Item	Description		
	<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. <b>How often -</b> Specify how often the schedule will be applied <b>Once -</b> The schedule will be applied just once		
	<b>Weekdays -</b> Specify which days in one week should perform the schedule.		

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

#### Example

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



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

## **4.9.3 RADIUS**

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Applications >> RADIUS	
RADIUS Setup	
🗹 Enable	
Server IP Address	
Destination Port	1812
Shared Secret	
Confirm Shared Secret	
ОК	Clear Cancel

Available settings are explained as follows:

Item	Description
Enable	Check to enable RADIUS client feature.
Server IP Address	Enter the IP address of RADIUS server
<b>Destination Port</b> The UDP port number that the RADIUS server is using default value is 1812, based on RFC 2138.	
Shared SecretThe RADIUS server and client share a secret that is authenticate the messages sent between them. Both be configured to use the same shared secret.	
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

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

# 4.9.4 LDAP / Active Directory

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

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

### **General Setup**

Applications >> Active Directory /LDAP

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

General Setup	Active Directory / LDAP Profiles			
Enable				
Bind Type			Simple Mode 🗸	
Server IP A	ddress			
Destination	Port		389	
Use SSL				
Regular DN				
Regular Pas	sword			
	(	OK	Cancel	

Item	Description	
Enable	Check to enable such function.	
Bind Type	There are three types of bind type supported.          Simple Mode         Simple Mode         Anonymous         Regular Mode	
	<b>Simple Mode</b> – Just simply do the bind authentication without any search action.	
	<b>Anonymous</b> – Perform a search action first with Anonymous account then do the bind authentication.	
	Regular Mode– Mostly it is the same with anonymous mode.	

	The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the <b>Regular DN</b> and <b>Regular Password</b> .	
Server IP Address	Enter the IP address of LDAP server.	
<b>Destination Port</b>	Type a port number as the destination port for LDAP server.	
Use SSL	Check it to enable LDAP over SSL (LDAPS), which is a common method of securing LDAP communication.	
Regular DN	Type this setting if <b>Regular Mode</b> is selected as <b>Bind Type.</b>	
Regular Password	Specify a password if <b>Regular Mode</b> is selected as <b>Bind Type.</b>	

## **Active Directory/LDAP Profiles**

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

Applications >> Active Directory /LDAP

General Setup	Active Directory / LDAP Profiles	
Index	Name	Distinguished Name
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		
<u>5.</u>		
<u>6.</u>		
<u>7.</u>		
<u>8.</u>		

Click any index number link to open the following page.

Applications >> Active Directory /LDAP>>Server Profiles

c=ms, dc=draytek, dc=com
ıp, dc=ms, dc=draytek, dc=c
ncel

Available settings are explained as follows:

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

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

**Note:** You can refer to "3.3 How to Implement the AD/LDAP Authentication for User Management?" and "3.4 How to implement the AD_LDAP authentication for SSL Application" for detailed information.

#### 4.9.5 UPnP

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

Applications >> UPnP

UPnP	
Enable UPnP Service	Default WAN 💌
Enable Connection control Service	Default WAN WAN1
Enable Connection Status Service	WAN2
Note: If you intend running UPnP service inside your LAN, you should allow control, as well as the appropriate UPnP settings.	WAN3 WAN4 WAN5 WAN5
OK Clear Ca	ncel

Available settings are explained as follows:

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

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.

dress 🔕 Network Connections		🦉 IP Broadband Connection on	Router Status 🔽
	Broadband		
Network Tasks         (2)           Create a new connection         (2)           Set up a home or small office network         (2)	hinet Disconnected WAN Miniport (PPPOE) Dial-up	General	Connected
0	C. C	Duration:	00:19:06
See Also	test Disconnected DrayTek ISDN PPP	Speed:	100.0 Mbps
Other Places 🛞	Internet Gateway	Activity Internet Internet Gatew	ay My Computer
Control Panel My Network Places My Documents	IP Broadband Connection on Router Enabled	Packets: Sent: 404	734
My Computer	LAN or High-Speed Internet	Received: 1,115	666
Details	Local Area Connection Enabled	Properties Disable	
Network Connections System Folder	Realtek RTL8139/810× 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.
This connection allows you to connect to the Internet through a shared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>☑ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>☑ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>☑ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>

The reminder as regards concern about Firewall and UPnP

#### Can't work with Firewall Software

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

#### **Security Considerations**

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



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

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

### 4.9.6 IGMP

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

Applications >> IGMP

IGMP			
Enable IGMP Proxy	WAN1 🗸		
	a multicast proxy for hosts on the LAN side. Enable t group. But this function take no affect when Bridge		
Enable IGMP Snooping			
	nulticast traffic is only forwarded to ports that have nulticast traffic is treated in the same manner as br		
Disable IGMP shooping, i	nulucast tranic is treated in the same manner as br	oaucast trainc.	
OK Cancel			
		<u>Refresh</u>	
Working Multicast Groups			
Index	Group ID	P1	

Item	Description	
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.           WAN1           WAN1           WAN2           WAN3           WAN4	
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 working multicast group status.	

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

# 4.9.7 Wake on LAN

Application >> 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.

<b>Note</b> : Wake on can wake up t	LAN cooperate with <u>Bind IP to MAC</u> function,only binded PCs hrough IP.
Wake by:	MAC Address 🔽
IP Address:	💙
MAC Address:	Wake Up!
Result	

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



## 4.9.8 SMS/Mail Alert Service

The function of Short Message Service is that Vigor router sends a message to user's mobile through specified service provider to assist the user knowing the real-time abnormal situations.

Vigor router allows you to set up to 8 SMS profiles which will be sent out according to different conditions.

### **SMS** Provider

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

SMS Provider	Mail Server		I	Set to Factory Defau
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - ??? 💌		1 - ??? 💌	
2	1 - ??? 2 - ???		1 - ??? 💌	
3	3 - ???		1 - ??? 💙	
4	5 - ??? 6 - ???		1 - ??? 💙	
5	7 - ??? 8 - ???		1 - ??? 🗸	
6	9 - Custom 1 10 - Custom 2		1 - ??? 💙	
7	1 - ???		1 - ??? 🛰	
8	1 - ???		1 - ??? 💙	
9	1 - ???		1 - ??? 💙	
10 🗆	1 - ???		1 - ??? 💙	

Application >> SMS / Mail Alert Service

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Check the box to enable such profile.
SMS Provider	Use the drop down list to choose SMS service provider. You can click <b>SMS Provider</b> link to define the SMS server.
Recipient	Type the name of the one who will receive the SMS.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the SMS.
Schedule (1-15)	Type the schedule number that the SMS will be sent out. You can click the <b>Schedule(1-15)</b> link to define the schedule.

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



### **Mail Server**

This page allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent.

SMS Provider	Mail Server		<u> </u>	Set to Factory Defa
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)
1 🗹	1 - Mail_Notify 💌		1 - ??? 💌	
2 🗹	1 - Mail_Notify 💌		1 - ??? 💌	
3 🗌	1 - Mail Notify 2 - ???		1 - ??? 🗸	
4	3 - ??? 4 - ???		1 - ??? 💙	
5 🗌	5 - ???		1 - ??? 💙	
6	7 - ???		1 - ??? 💙	
7	9 - ???		1 - ??? 💙	
8	1 - Mail_Notify 💙		1 - ??? 💙	
9	1 - Mail_Notify 😪		1 - ??? 💙	
10 🔲	1 - Mail_Notify 🔽		1 - ??? 🛰	

Cancel

OK

Application >> SMS / Mail Alert Service

Available settings are explained as follows:

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Check the box to enable such profile.
Mail Service	Use the drop down list to choose mail service provider. You can click <b>Mail Service</b> link to define the mail server.
Recipient	Type the e-mail address of the one who will receive the notification message.
Notify Profile	Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. You can click the <b>Notify Profile</b> link to define the content of the mail message.
Schedule	<ul><li>Type the schedule number that the notification will be sent out.</li><li>You can click the Schedule(1-15) link to define the schedule.</li></ul>

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

# 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.

- sep princiali orna
VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
IPsec General Setup
IPsec Peer Identity
OpenVPN General Setup
Remote Dial-in User
LAN to LAN
VPN TRUNK Management
Connection Management
Certificate Management

VPN and Remote Access >> VPN Client Wizard

## 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.

1. Open VPN and Remote Access>>VPN Client Wizard. The following page will appear.

AN-to-LAN VPN Client Mode Selection:	Route Mode 💙
Please choose a LAN-to-LAN Profile:	[Index] [Status] [Name] 🖌
	y a single client or ip and is not configured to route
the subnet and then select NAT mode	y a single client or ip and is not configured to route

Item	Description
LAN-to-LAN Client	Choose the client mode.
Mode Selection	<b>Route Mode/NAT Mode</b> – If the remote network only allows



		gle IP, please choose this mode,	
	otherwise please choos	se Route Mode.	
	Route Mode 🔽		
	Route Mode		
	NAT Mode		
Please choose a	There are 32 VPN prof	files for users to set.	
LAN-to-LAN Profile	[Index] [Status]		
	1 x	???	
	1 x 2 x	222	
	3 x	???	
	4 x	???	
	5 x	???	
	5 x 6 x 7 x	??? ???	
	7 x  8 x	????	
	9 x	222	
	10 x	222	
	11 x	???	
	12 x	???	
	13 x	???	
	14 x	???	
	15 x 16 x	??? ???	
	17 x	???	
	18 x	222	
	19 x	???	
	20 x	???	
	21 x	???	
	22 x 23 x	???	
		??? ???	
	24 x 25 x	????	
	26 x	222	
	27 x	222	
	28 x	???	
	29 x	??? 💌	
			_

2. When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

ecurity ranking (1 is the highest; 5 is the lowest)	Throughput ranking (1 is the highest; 5 is the lowes
<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>
PPT PPT IPSe L2TF L2TF	

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

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

	???
/PN Dial-Out Through	WAN1 First
Always on	
erver 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

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

VPN and Remote Access >> VPN Client Wizard

Client IPSec Settings	
Profile Name	???
VPN Dial-Out Through	WAN1 First
🔲 Always on	
Server IP/Host Name for VPN	
(e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
💿 Pre-Shared Key	
Confirm Pre-Shared Key	
🔿 Digital Signature (X.509)	
Peer ID	None
Local ID	
Iternative Subject Name First	
🔘 Subject Name First	
IPSec Security Method	
Medium (AH)	
O 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	
<ul> <li>Digital Signature (X.509)</li> </ul>	
Peer ID	None
Local ID	
Alternative Subject Name First	
🔘 Subject Name First	
IPSec Security Method	
💿 Medium (AH)	
🔿 High (ESP)	DES without Authentication 💌
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

• 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	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	
Medium (AH)	
🔘 High (ESP)	DES without Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

Item	Description	
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.	
VPN Dial-Out Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only. WAN1 First WAN1 First WAN1 Only WAN2 First WAN2 Only WAN2 Only: Backup WAN2 WAN2 Only: Backup WAN1 WAN3 First WAN3 Only WAN4 First WAN3 Only WAN4 First WAN5 First WAN5 Only WAN5 First - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the first channel for VPN connection. If WAN1/WAN2/WAN3 /WAN4/WAN5 fails, the router will use another WAN interface instead.	

	<ul> <li>WAN1 Only / WAN2 Only / WAN3 Only / WAN4 Only/ WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the only channel for VPN connection.</li> <li>WAN1 Only: Backup WAN2/WAN2 Only: Backup WAN1 - While connecting, the router will use WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 fails, the router will use backup WAN2/backup WAN1 interface instead.</li> </ul>	
Always On	Check to enable router always keep VPN connection.	
Server IP/Host Name for VPN	Type the IP address of the server or type the host name for such VPN profile.	
Pre-Shared Key	<ul> <li>IKE Authentication Method usually applies to those are remote dial-in user or node (LAN to LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.</li> <li>Pre-Shared Key- Specify a key for IKE authentication.</li> <li>Confirm Pre-Shared Key-Confirm the pre-shared key.</li> </ul>	
Digital Signature		
Digital Signature (X.509)	Click <b>Digital Signature</b> to invoke this function. <b>Peer ID</b> – Choose the peer ID selection from the drop down list. <b>Local ID</b> – Choose <b>Alternative Subject Name First</b> or <b>Subject Name First</b> .	
	Local Certificate – Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in Certificate Management >> Local Certificate. Otherwise, the setting you choose here will not be effective.	
IPSec Security Method	<ul> <li>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</li> <li>High - Encapsulating Security Payload (ESP) means payload</li> </ul>	
	(data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.	
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.	
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.	
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.	
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.	



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

27
test
PPTP (None Encryption)
WAN1 First
No
192.168.1.87
172.16.3.99
255.255.255.0
necessary. Otherwise, click <b>Finish</b> to save the current settings
💿 Go to the VPN Connection Management.
🔘 Do another VPN Client Wizard setup.
View more detailed configurations.
-

Available settings are explained as follows:

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

Choose VPN Establishment Environment	
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 Accounts:	[Index] [Status] [Name]
Allowed Dial-in Type:	
	PPTP
	IPSec
	L2TP with IPSec Policy None

Item	Description
VPN Server Mode Selection	Choose the direction for the VPN server. <b>Site to Site VPN</b> – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN. <b>Remote Dial-in User</b> –You can manage remote access by
	maintaining a table of remote user profile, so that users can be authenticated to dial-in via VPN connection. Site to Site VPN (LAN-to-LAN) Site to Site VPN (LAN-to-LAN) Remote Dial-in User (Teleworker)
Please choose a LAN-to-LAN Profile	This item is available when you choose <b>Site to Site VPN</b> (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.



Item	Description		
	[Index] [Status] [Name]         1       x         2       x         3       x         4       x         5       x         6       x         7       x         8       x         9       x         10       x         11       x         12       x         13       x         14       x         17       x         18       x         19       x         20       x         21       x         23       x         26       x         27       x         28       x         29       x		
Please choose a Dial-in User Accounts	This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.		
Allowed Dial-in Type	This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are several types provided here (similar to VPN Client Wizard). PPTP IPSec L2TP with IPSec Policy None None Nice to Have Must		
	Different Dial-in Type will lead to different configuration page.		

- 1. Here we take the example of choosing **Remote-Dial-in User** as the **VPN Server Mode**.
- 2. Choose a dial-in user account number.
- 3. Check the Allowed Dial-in Type for the VPN server profile.
- 4. After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection (dial-in type) you made.
- When you check **PPTP**, you will see the following graphic:

N Authentication Setting	
PPTP / L2TP / L2TP over IPSec Autho	entication
Username	???
Password	
Peer IP/VPN Client IP	

• When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP** with Policy (Nice to Have/Must), you will see the following graphic:

VPN and Remote	Access >>	VPN Server	Wizard
----------------	-----------	------------	--------

VPN Authentication Setting	
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	•••
Authentication Type	Local User Database 🛛 👻
IPSec / L2TP over IPSec Authentication	
🗹 Pre-Shared Key	
Confirm Pre-Shared Key	
🔲 Digital Signature (X.509)	
Peer ID	None
Peer IP/VPN Client IP	1.1.1.1
Peer ID	
	<pre>&lt; Back Next &gt; Finish Cancel</pre>

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

VPN and Remote Access >> VPN Server Wizard

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

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Authentication Type	Choose a proper authentication type for VPN connection. Local User Database Radius LDAP
Pre-Shared Key	For IPSec/L2TP IPSec authentication, you have to type a pre-shared key.
Confirm Pre-Shared Key	Type the pre-shared key again for confirmation.
Digital Signature (X.509)	Check the box of Digital Signature to invoke this function. Use the drop down list to choose one of the certificates for using. You have to configure one certificate at least previously in <b>Certificate Management &gt;&gt; Local 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

Item	Description
	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.

5. After finishing the configuration, please click **Next.** The confirmation page will be shown as follows.

VPN and Remote Access >> VPN Server Wizard

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
	ssary. Otherwise, click <mark>Finish</mark> to save the current settings
and proceed to the following action:	
	● Go to the VPN Connection Management.
	-
	O Do another VPN Server Wizard setup.
	View more detailed configurations.
	< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Go to the VPN Connection Management	Click this radio button to access <b>VPN and Remote</b> 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> Access>>LAN to LAN for viewing detailed configuration.

6. 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.

# 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 (e.g., PPTP VPN, IPSec VPN, L2TP VPN, SSL VPN, OpenVPN, etc.) of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

Remote Access Control Setup		
	<b>V</b>	Enable PPTP VPN Service
	<b>~</b>	Enable IPSec VPN Service
	<b>~</b>	Enable L2TP VPN Service
	<b>~</b>	Enable SSL VPN Service
	<b>~</b>	Enable OpenVPN Service

above to allow pass-through, as well as the appropriate NAT settings.

ОК	Clear	Cancel
----	-------	--------

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

## 4.10.4 PPP General Setup

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

PPP General Setup			
PPP/MP Protocol			LDAP Server Profiles for PPP Authentication
Dial-In PPP Authentication	PA	P or CHAP 👻	PPTP LDAP Profile
Dial-In PPP Encry (MPPE)	ption Opt	tional MPPE	
Mutual Authentic	ation (PAP	) 🔘 Yes 💽 No	
Username			
Password			
P Address Assignme When DHCP Disable		n Users	
ssigned IP start	LAN 1	192.168.1.200	
	LAN 2	192.168.2.200	
	LAN 3	192.168.3.200	
	LAN 4	192.168.4.200	

Item	Description
Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.
	<b>PAP or CHAP</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol

Item	Description
	first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE Optional MPPE	Optional MPPE - This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.
	<b>Maximum MPPE (128 bit)-</b> This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the <b>User Name</b> and <b>Password</b> of the mutual authentication peer.
Assigned IP Start	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. You can configure up to four start IP addresses for LAN1 ~ LAN4.
LDAP Server Profiles for PPP Authentication	Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.
	However, if there is no profile listed, simply click the link of <b>PPTP LDAP Profile</b> to create/add some new LDAP profiles you want.
	For the detailed information of LDAP application, refer to section 3.3 and 3.4.

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



# 4.10.5 IPSec General Setup

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

There are two phases of IPSec.

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

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

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

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

Dial-in Set up for Remote Dial-in users a	nd Dynamic IP Client (LAN to LAN).
IKE Authentication Method	
Certificate for Dial-in	None 💌
Pre-Shared Key	
Pre-Shared Key	
Confirm Pre-Shared Key	
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but w	/ill not be encrypted.
High (ESP) 🛛 🗹 DES 🔽 30	DES 🔽 AES
Data will be encrypted and a	uthentic.

____

VPN and Remote Access >> IPSec General Setup

Available settings are explained as follows:

Item	Description	
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and	
	IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel. There are two methods offered by Vigor router for you to authenticate the incoming data coming from remote	

Item	Description
	dial-in user, Certificate (X.509) and Pre-Shared Key.
	<b>Certificate for Dial-in</b> – Choose one of the local certificates from the drop down list.
	Pre-Shared Key- Specify a key for IKE authentication.
	<b>Confirm Pre-Shared Key-</b> Retype the characters to confirm the pre-shared key.
	Note: Any packets from the remote dial-in user which does not match the rule defined in VPN and Remote Access>>Remote Dial-In User will be applied with the method specified here.
<b>IPSec Security Method</b>	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High (ESP)</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.

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

# **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.

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

VPN and Remote Access >> IPSec Peer Identity

Each item will be explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.

Item	Description
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

ess
ess
ess
ess 🔽
ess 🔽
]

Available settings are explained as follows:

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

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



# 4.10.7 OpenVPN General Setup

OpenVPN is a comprehensive SSL VPN software that combines OpenVPN server functions, enterprise management mechanism, simplified OpenVPN Connect User Interface and OpenVPN Client software package. It can work on Windows, Linux OS, and Macintosh operating system.

OpenVPN Access Server offers a wide range of configurations for remote access to private cloud network resources and/or internal network.

Note: Vigor3200 will support up to 10 simultaneous dial-in OpenVPN tunnels.

In general, there are two advantages of OpenVPN:

- OpenVPN can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-clients to connect to a single OpenVPN Server process over a single TCP or UDP port.

VPN and Remote Access >> OpenVPN General Setup

OpenVPN General Setup	
Port	1194
Cipher Algorithm	AES128 V
HMAC Algorithm	SHA1 🗸
Certificate Authentication	
Note: OpenVPN on vigor only su	port UDP protocol and TUN device interface currently. So please setup

Note: OpenVPN on vigor only support UDP protocol and TUN device interface currently. So please setup corresponding configurations on the client side.

### OK

Item	Description		
Port	Usually, the default UDP port number for OpenVPN is 1194.		
Cipher Algorithm	Two encryptions are supported, AES128 and AES256. AES128 AES128 AES256 NONE		
HMAC Algorithm	The HMAC algorithm only supports SHA1/SHA256. SHA1 SHA256 NONE		
Certificate Authentication	If certificate authentication is required for OpenVPN, simply check the box to apply the trusted CA certificate and local certificate for OpenVPN tunnel. Certificate authentication can offer more secure VPN tunnel between the client and the router.		



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

### 4.10.8 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 **64** 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.

Remote View:	Access User Acc					Set to	Factory Default Search
Index	User	Active	Status	Index	User	Active	Status
<u>1.</u>	???			<u>17.</u>	???		
<u>2.</u>	???			<u>18.</u>	???		
<u>3.</u>	???			<u>19.</u>	???		
<u>4.</u>	???			<u>20.</u>	???		
<u>5.</u>	???			<u>21.</u>	???		
<u>6.</u>	???			<u>22.</u>	???		
<u>7.</u>	???			<u>23.</u>	???		
<u>8.</u>	???			<u>24.</u>	???		
<u>9.</u>	???			<u>25.</u>	???		
<u>10.</u>	???			<u>26.</u>	???		
<u>11.</u>	???			<u>27.</u>	???		
<u>12.</u>	???			<u>28.</u>	???		
<u>13.</u>	???			<u>29.</u>	???		
<u>14.</u>	???			<u>30.</u>	???		
<u>15.</u>	???			<u>31.</u>	???		
<u>16.</u>	???			<u>32.</u>	???		
<< <u>1-32</u>	33-64 >>		ОК	Cancel			<u>Next</u> >>

VPN and Remote Access >> Remote Dial-in User

Each item will be explained as follows:

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

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

VPN and Remote Ad	ccess >> Remote	Dial-in User
-------------------	-----------------	--------------

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

Item	Description	
User account and	<b>Enable this account</b> - Check the box to enable this function.	
Authentication	<b>Idle Timeout-</b> If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.	
Allowed Dial-In Type	<b>PPTP</b> - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.	
	<b>IPSec Tunnel</b> - Allow the remote dial-in user to make an IPSec VPN connection through Internet.	
	<b>L2TP with IPSec Policy</b> - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:	
	• 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	



Item	Description			
	connection becomes one pure L2TP connection.			
	• <b>Must</b> -Specify the IPSec policy to be definitely applied on the L2TP connection.			
	<b>SSL Tunnel -</b> It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)			
	If you check this box, the function of SSL Tunnel for this account will be activated immediately.			
	<b>OpenVPN Tunnel -</b> Allow the remote dial-in user to make an OpenVPN connection through Internet.			
	<b>Specify Remote Node -</b> Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .			
	Netbios Naming Packet			
	• <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.			
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.			
	<b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.			
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.			
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.			
Subnet	Chose one of the subnet selections for such VPN profile.			
	<b>Assign Static IP Address</b> – Please type a static IP address for the subnet you specified.			
User Name	This field is applicable when you select PPTP or L2TP with o 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).			



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

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

# 4.10.9 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 **64** VPN tunnels simultaneously. The following figure shows the summary table.

View: 💿	All Online	Offline	O Trunk				Search
Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	???			<u>17.</u>	???		
<u>2.</u>	???			<u>18.</u>	???		
<u>3.</u>	???			<u>19.</u>	???		
<u>4.</u>	???			<u>20.</u>	???		
<u>5.</u>	???			<u>21.</u>	???		
<u>6.</u>	???			<u>22.</u>	???		
<u>7.</u>	???			<u>23.</u>	???		
<u>8.</u>	???			<u>24.</u>	???		
<u>9.</u>	???			<u>25.</u>	???		
<u>10.</u>	???			<u>26.</u>	???		
<u>11.</u>	???			<u>27.</u>	???		
<u>12.</u>	???			<u>28.</u>	???		
<u>13.</u>	???			<u>29.</u>	???		
<u>14.</u>	???			<u>30.</u>	???		
<u>15.</u>	???			<u>31.</u>	???		
<u>16.</u>	???			<u>32.</u>	???		
<< <u>1-32</u>	<u>33-64</u> >>						<u>Next</u> >:

VPN and Remote Access >> LAN to LAN

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

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

LAN-to-LAN Profiles:			
View: OAII OOnline O	Offline Trunk		Search
Name	Activate	Members	Status
<u>RD1213</u>	<ul> <li>Image: A start of the start of</li></ul>	Sandy	Offline
		Marketing	Offline
	0	K Cancel	

### Each item will be explained as follows:

VPN and Remote Access >> LAN to LAN

Item	Description	
Set to Factory Default	Click to clear all indexes.	
View	All – Click it to show all of profiles.	

Item	Description		
	<b>Online/Offline</b> – Click it to show the active/inactive profiles		
	<b>Trunk -</b> Click it to show the profile which VPN tunnel is up.		
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.		
Active	Check the box to enable the selected profile.		
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.		

To edit each profile:

VPN and Remote Access >> LAN to LAN

1. Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

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



Item	Description		
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 First WAN1 Only WAN2 First WAN2 Only WAN2 Only WAN2 Only: Backup WAN2 WAN2 Only: Backup WAN1 WAN3 First WAN3 Only WAN4 First WAN4 Only WAN5 First WAN5 Only WAN5 First WAN5 Only WAN5 First WAN5 Only WAN5 A first - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the first channel for VPN connection. If		
	<ul> <li>/WAN4 /WAN5 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.</li> <li>WAN1 /WAN2 /WAN3 /WAN4 /WAN5 Only - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the only channel for VPN connection.</li> <li>WAN1 Only: Backup WAN2/WAN2 Only: Backup WAN1</li> </ul>		
	- While connecting, the router will use WAN1/WAN2 as the only channel for VPN connection. If WAN1/WAN2 fails, the router will use backup WAN2/backup WAN1 interface instead.		
Netbios Naming Packet	<b>Pass</b> – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.		
	<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. <b>Both</b> :-initiator/responder		

Item	Description
	Dial-Out- initiator only
	Dial-In- responder only.
Always On or Idle Timeout	<ul> <li>Always On-Check to enable router always keep VPN connection.</li> <li>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop</li> </ul>
Enable PING to keep alive	the connection. 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	<ul> <li>PPTP - 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.</li> <li>IPSec Tunnel - Build an IPSec VPN connection to the server through Internet.</li> <li>L2TP with IPSec Policy - Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:</li> <li>None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</li> <li>Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.</li> <li>Must: Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul>
User Name	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common



Item	Description		
	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> – Check the box of Digital Signature to invoke this function. Then, specify the following items for authentication with digital signature.		
	• <b>Peer ID</b> - Select one of the predefined Profiles set in <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity.</b>		
	• Local ID – Specify a local ID (Alternative Subject Name First or Subject Name First) 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.		
	Local Certificate – Select one of the profiles set in Certificate Management>>Local Certificate.		
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.		
	<b>Medium AH (Authentication Header)</b> 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:		

Item	Description
	IKE advanced settings IFE phase 1 mode IKE phase 1 mode IKE phase 1 proposal IKE phase 2 proposal IKE phase 2 proposal IKE phase 2 proposal IKE phase 1 key lifetime 28900 (900 ~ 86400) IKE phase 1 key lifetime 3600 (600 - 66400) Perfect Forward Secret O Enable Local ID IKE th you select *Auto* in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_MOS_GHAA_G1, 20ES_MOS_G2, 20ES_MOS_C2, 20ES_MOS_KAES12e_MOS_(C2/G5), AES22e_SHA_(C2/G5),
	<b>IKE phase 1 mode -</b> Select from <b>Main</b> mode and <b>Aggressive</b> mode. The ultimate outcome is to exchange security proposals
	to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPSec session. However, the <b>Aggressive</b> mode is faster. The default value in Vigor router is Main mode.
	<b>IKE phase 1 proposal-</b> 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 <b>Main</b> mode. We suggest you select the combination that covers the most schemes.
	<b>IKE phase 2 proposal-</b> 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.
	<b>IKE phase 1 key lifetime-</b> 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.
	<b>IKE phase 2 key lifetime-</b> 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.
	<b>Perfect Forward Secret (PFS)-</b> The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.
	<b>Local ID-</b> In <b>Aggressive</b> mode, Local ID is on behalf of the IF address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

2	D:-		C - 441-	
э.	Dia	I-IN	Settir	IOS

Allowed Dial-In Type		Username	
PPTP     IPsec Tunnel		Password(Max 11 char)     VJ Compression     Image: On Complexity of the second s	
L2TP with IPsec Policy None Specify Remote VPN Gateway Peer VPN Server IP or Peer ID		IKE Authentication Method ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None ✓ Local ID ● Alternative Subject Name First ● Subject Name First IPsec Security Method ✓ Medium(AH)	
4. GRE over IPsec Settings		High(ESP) 🗹 DES 🗹 3DES 🗹 AES	
Enable IPsec Dial-Out			
Logical Traffic	My GRE IP	Peer GRE IP	
5. TCP/IP Network Settings			
My WAN IP Remote Gateway IP Remote Network IP	0.0.0.0	RIP Direction Disable V From first subnet to remote network, you have to do Route V	
Remote Network Mask Local Network IP Local Network Mask	255.255.255.0 192.168.1.5 255.255.255.0 More	□ Change default route to this VPN tunnel ( Only single WAN supports this )	

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

Item	Description
	address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
	<b>User Name -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
	<b>Password</b> (Max 11 char) - This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
	<b>VJ Compression -</b> 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> .
	Local ID – Specify which one will be inspected first.
	<ul> <li>Alternative Subject Name First – The alternative subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> </ul>
	• Subject Name First – The subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. <b>Medium-</b> Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High-</b> Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
GRE over IPSec Settings	<b>Enable IPSec Dial-Out function GRE over IPSec</b> : Check this box to verify data and transmit data in encryption with GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.



Item	Description
	Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacke can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.
	<b>My GRE IP</b> : Type the virtual IP for router itself for verified by peer.
	<b>Peer GRE IP</b> : Type the virtual IP of peer host for verified by router.
TCP/IP Network Settings	My WAN IP - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The defaul value is 0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	<b>Remote Gateway IP</b> - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	<b>Remote Network IP/ Remote Network Mask -</b> Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
	<b>Local Network IP / Local Network Mask -</b> Add a static route to direct all traffic destined to Local Network IP Address/Loca Network Mask through the VPN connection.
	<b>More -</b> Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

Item	Description	
	🔄 http://192.168.1.1 - LAN-to-LAN Profile - Microsoft Internet Explorer 🔲 🔲 🗙	
	Profile Index :1	
	Remote Network	
	Network IP	
	255.255.255.255 / 32 💌	
	Add Delete Edit	
	OK Close	
	<b>2</b>	
	<b>RIP Direction -</b> The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.	
	<b>From first subnet to remote network, you have to do -</b> If the remote network only allows you to dial in with single IP, please choose <b>NAT</b> , otherwise choose <b>Route</b> .	
	<b>Change default route to this VPN tunnel -</b> Check this box to change the default route with this VPN tunnel. Note that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.	

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

## 4.10.10 VPN TRUNK Management

VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPSec, and Binding tunnel policy.

### Features of VPN TRUNK – VPN Backup Mechanism

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

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- > The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network



- Mail Alert support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Syslog support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

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

# Features of VPN TRUNK – VPN Load Balance Mechanism

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism to let the administrator manage the network more flexibly.

- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and GRE over IPSec
- > The web page is simple to understand and easy to configure
- The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably

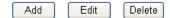
#### VPN and Remote Access >> VPN TRUNK Management

Member2(Active)Type

o. Status Name	Member1(Active)Type	Member2 (Active) Type
Advanced 🔽 🗸 🗸		

#### General Setup

Status	⊙ Enable 🔿 Disable	
Profile Name		
Member1	Please select a LAN-to-LAN Dial-Out profile.	~
Member2	Please select a LAN-to-LAN Dial-Out profile.	*
Active Mode	⊙Backup ○Load Balance	



Item	Description
Backup Profile List	<b>Set to Factory Default -</b> Click to clear all VPN TRUNK-VPN Backup mechanism profile.
	<b>No</b> – The order of VPN TRUNK-VPN Backup mechanism profile.
	<b>Status (on Backup Profile field)</b> - "v" means such profile is enabled; "x" means such profile is disabled.
	<b>Name (on Backup Profile field) -</b> Display the name of VPN TRUNK-VPN Backup mechanism profile.
	<b>Member1 (on Backup Profile field) -</b> Display the dial-out profile selected from the Member1 drop down list below.
	Active (on Backup Profile field) - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.



	<ul> <li>Type (on Backup Profile field) - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.</li> <li>Member2 (on Backup Profile field) - Display the dial-out profile selected from the Member2 drop down list below.</li> <li>Advanced – This button is available only when LAN to LAN profile (or more) is created.</li> </ul>	
	Introvingendation for this dialog, see later section - Advanced Load Balance and Backup.	
Load Balance Profile List	<ul> <li>Set to Factory Default - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.</li> <li>No - The order of VPN TRUNK-VPN Load Balance mechanism profile.</li> </ul>	
	<b>Status</b> - "v" means such profile is enabled; "x" means such profile is disabled.	
	<b>Name -</b> Display the name of VPN TRUNK-VPN Load Balance mechanism profile.	
	<b>Member1</b> - Display the dial-out profile selected from the Member1 drop down list below.	
	Active - "Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.	
	<b>Type -</b> Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.	
	<b>Member2</b> - Display the dial-out profile selected from the Member2 drop down list below.	
	Advanced – This button is only available when there is one or more profiles created in this page.	

	🗟 http://192.168.1.1 - YPN Load Balance Advance Settings - Microsoft Internet Explorer
	VPN Load Balance Advance Settings
	Profile Name: Balance1 Load Balance Algorithm: © Round Robin
	<ul> <li>○ Weighted Round Robin</li> <li>⊙ Auto Weighted</li> <li>○ According to Speed Ratio (Member1:Member2); 50:50 ▼</li> </ul>
	VPN Load Balance Policy © Edit O Insert after
	Tunnel Bind Table Index: (1~128) Active: Active V
	Binding Dial Out Profile:         1 •         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5         5<
	Dest IP Start:         D0.00         End:         255.255.255           Dest IP Start:         1         End:         66535
	Protocol: TCP/UDP V 255
	OK Close
	Detail Information
	[VPN Load Balance Profile name: Balance1] [Algorithm: Round Robin]
	Detailed information for this dialog, see later section - Advanced Load Balance and Backup.
General Setup	<b>Status</b> - After choosing one of the profile listed above, please
General Setup	click <b>Enable</b> to activate this profile. If you click <b>Disable</b> , the
	selected or current used VPN TRUNK-Backup/Load Balance
	mechanism profile will not have any effect for VPN tunnel.
	<b>Profile Name</b> - Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN.
	The saved VPN profiles in LAN-to-LAN will be shown on
	Member1 and Member2 fields.
	Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >>
	LAN-to-LAN) for you to choose for grouping under certain
	VPN TRUNK-VPN Backup/Load Balance mechanism profile.
	<i>No</i> - Index number of LAN-to-LAN dial-out profile.
	Name - Profile name of LAN-to-LAN dial-out profile.
	<i>Connection Type</i> - Connection type of LAN-to-LAN dial-out profile.
	<i>VPN ServerIP (Private Network)</i> - VPN Server IP of LAN-to-LAN dial-out profiles.
	Active Mode - Display available mode for you to choose.
	Choose <b>Backup</b> or <b>Load Balance</b> for your router.
Add	Add and save new profile to the backup profile list. The
	corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile
	will be locked. The profiles in LAN-to-LAN will be displayed
	in red. VPN TRUNK – VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed
	in blue.



Update	Click this button to save the changes to the <b>Status</b> (Enable or Disable), profile name, member1 or member2.
Delete	Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

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

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

#### Time for activating VPN TRUNK – VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

# Time for activating VPN TRUNK – Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

# How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

- First of all, go to VPN and Remote Access>>LAN-to-LAN. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup /Load Balance mechanism profile management well.
- 2. Access into VPN and Remote Access>>VPN TRUNK Management.
- 3. Set one group of VPN TRUNK VPN Backup/Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.

Status	€ Enable ⊂ Disable
Profile Name	071023
Member1	Please choose the combination that you want.
Member2	Please choose the combination that you want.
Attribute Mode	Please choose the combination that you want.       No. (Name)     (Connection-Type)       1     To-A PlaceIPSec       2     To-B Site IPSec       192.168.2.26(20.20.21.0)

4. Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red



to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup/Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

VPN and Remote Access >> LAN to LAN

#### LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	To-A Place	V
<u>2.</u>	To-B Site	V
<u>3.</u>	To-C place	V
<u>4.</u>	To-D Site	V
5	222	×

#### How can you set a GRE over IPSec profile?

- 1. Please go to LAN to LAN to set a profile with IPSec.
- 2. If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

		Callback Budget	0 minute(s)
4. GRE over IPSec Setting	5	-	
🗖 Enable IPSec Dial-Out	t function GRE over IPSec		
🗆 Logical Traffic	My GRE IP 192.168.50.200	Peer GRE IP 19	32.168.50.100
5. TCP/IP Network Settings	3		
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	From first subnet to read	mote network, you have to
Remote Network IP	192.168.10.0		Route 💌
Remote Network Mask	255.255.255.0		

3. Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.

		Callback Budget	<pre>0 minute(s)</pre>
4. GRE over IPSec Setting	S		
🗹 Enable IPSec Dial-Ou	t function GRE over IPSec		
🗖 Logical Traffic	My GRE IP 192.168.50.100	Peer GRE IP 192	2.168.50.200
5. TCP/IP Network Settings	\$		
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	From first subnet to rem	note network, you have to
Remote Network IP	192.168.1.0		Route 💌
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	to this VPN tunnel ( Only )
	ок сі	ear Cancel	

## Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

#### Advanced Load Balance

🖹 http://192.168.1.1 - ¥PN Load I	Balance Advance Settings	- Microsoft Internet E	xplorer	
				^
VPN Load Balance Advance S	ettings			
Profile Name:	Balance1			
Load Balance Algorithm:	💿 Round Robin			
	OWeighted Round			
	💽 Auto Weigł			50.50
	According	to Speed Ratio (Me	ember1:Member2):	50:50 🚩
VPN Load Balance Policy				
	💿 Edit 🛛 🔿 Insert	after		
Tunnel Bind Table Index:	(1~128)			
Active:	Active 🔽			
Binding Dial Out Profile:	1 🕶			
Src IP Start:	0.0.0	End:	255.255.255.255	
Dest IP Start:	0.0.0.0	End:	255.255.255.255	
Dest Port Start:	1	End:	65535	
Protocol:	TCP/UDP 🖌 255			
	OK	Close		
Detail Information				
[VPN Load Balance Prof [Algorithm: Round Robi		]		<u>^</u>
[XIGOLICIAN: KOUNG KODI				
				_
				=
<				>

Item	Description	
Profile Name	List the load balance profile name.	
Load Balance Algorithm	<b>Round Robin</b> – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.	
	Weighted Round Robin –Such method can reach the balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. Auto Weighted can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. According to Speed Ratio allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).	

VPN Load Balance	Below shows the algorithm for Load Balance.
Policy	<b>Edit</b> – Click this radio button for assign a blank table for configuring Binding Tunnel.
	After insert – Click this radio button to adding a new binding tunnel table.
	<b>Tunnel Bind Table Index</b> - 128 Binding tunnel tables are provided by this device. Specify the number of the tunnel for such Load Balance profile.
	Active – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.
	<b>Binding Dial Out Index</b> – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.
	<b>Scr IP Start /End</b> – Specify source IP addresses as starting point and ending point.
	<b>Dest IP Start/End</b> – Specify destination IP addresses as starting point and ending point.
	<b>Dest Port Start /End</b> – Specify destination service port as starting point and ending point.
	<b>Protocol</b> – <b>Any</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.
	<b>TCP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. <b>UDP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such binding tunnel table can be established. <b>TCP/UPD</b> means when the source II destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. <b>ICMP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. <b>ICMP</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. IGMP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. <b>Other</b> means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with differer TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.



<b>Detail Information</b>	This field will display detailed information for Binding Tunnel		
	Policy. Below shows a successful binding tunnel policy for		
	load balance:		
	VPN Load Balance - Binding Tunnel Policy		
	Create C After insert     Tunnel Bind Table Index: (1~400)		
	Tunnel Bind Table Index:     (1~400)       Active:     In-active/Delete •		
	Binding Dial Out Index:		
	Binding Src IP Start: 0.0.0.0 End: 0.0.0.0		
	Binding Dest IP Start: 0.0.0.0 End: 0.0.0.0		
	Binding Dest Port Start: 1 End: 65535		
	Binding Fragmented: NO 💌 Binding Protocol: ANY 🔽 🛛		
	Finish setting up!		
	OK Close		
	Detail Information		
	[VPN Load Balance Profile name: VpnLB1 ]		
	[Algorithm: Fastest ]		
	No.1> Tunnel Bind Table Idnex :2		
	Binding Dial Out Index = 1		
	Binding protocol = TCP Protocol 6 Binding Src IP = 192.168.10.24 ~ 192.168.10.24		
	Binding Dst IP = 192.168.1.20 ~ 192.168.1.20 Binding Dst Port = 20 ~ 21		
	Binding Fragmented = NO		
	Note : To configure a successful binding tunnel, you have		
	to:		
	Type Binding Src IP range (Start and End) and Binding Des IP		
	range (Start and End). Choose TCP/UDP, IGMP/ICMP or		
	Other as Binding Protocol.		

#### Advanced Backup

🗿 http://192.168.1.1 - YP	N Backup Advance Settings - Microsoft Internet Explorer	
		^
VPN Backup Advance	Settings	
Profile Name:	Backup1	
ERD Mode:	<ul> <li>Normal</li> </ul>	
	◯Resume (Member 1 first)	
Detail Informati	on:	
Environment	Recovers Detection(ERD) Status: Normal Mode	<u>^</u>
		~
	OK Close	
		~
<		>

Item	Description
Profile Name	List the backup profile name.
ERD Mode	ERD means "Environment Recovers Detection".
	<b>Normal</b> – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.
	<b>Resume</b> – when VPN connection breaks down or disconnects,

Item	Description
	Member 1 will be the top priority for the system to do VPN connection.
Detail Information	This field will display detailed information for Environment Recovers Detection.

#### 4.10.11 Connection Management

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

VPN and Remote Access >> Connection Management

					XXXXXX : Da XXXXXX : Da			.d
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
Current Pa	age: 1					Pag	je No.	Go >>
VPN Conn	ection Status							
	Load Ba	alance Mode:			*	Dial		
	В	ackup Mode:			~	Dial		
	G	ieneral Mode:			*	Dial		
Dial-out T	bol				Refres	h Seco	nds : 10	<ul> <li>Refresh</li> </ul>

Item	Description
Dial-out Tool	General Mode - This filed displays the profile configured in LAN to LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.
	General Mode:Backup Mode:Alfa ) 192.168.0.26Backup Mode:DialLoad Balance Mode:Bentley ) 192.168.0.27Audi ) 192.168.0.28DialBMW ) 192.168.0.29Buick ) 192.168.0.30Cadillac ) 192.168.0.30Cadillac ) 192.168.0.32Citroen ) 192.168.0.32Page No.Citroen ) 192.168.0.35Rx RxFiat ) 192.168.0.36I Data is erBackup Mode - This filed displays the profile name saved inVPN TRUNK Management (with Index number and VPNServer IP address). The VPN connection built by BackupMode supports VPN backup function.

	General Mode: (Alfa ) 192.168.0.26 🔽 Dial
	Backup Mode: (VpnBackup) 192.168.2.103 💌 Dial
	Load Balance Mode: (VpnBackup) 192.168.2.103 (VpnBackup) 192.168.2.203
	<b>Dial</b> - Click this button to execute dial out function.
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.
Refresh	Click this button to refresh the whole connection status.
VPN Connection Status	Display current connected VPN status.
	<b>VPN</b> – Display the name of the VPN profile.
	<b>Type</b> – Display the VPN connection mode such as PPTP or IPSec.
	<b>Remote IP</b> – Display the IP address of remote peer.
	<b>Virtual Network</b> – Display the remote network IP address with subnet address.
	<b>Tx Pkts</b> – Display the transmission packets passing through such VPN channel.
	<b>Tx Rate</b> – Display the transmission rate for data through such VPN tunnel.
	<b>Rx Pkts</b> – Display the receiving packets passing through such VPN channel.
	<b>Rx Rate</b> – Display the receiving rate for data through such VPN tunnel.

# 4.11 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.



#### 4.11.1 Local Certificate

Certificate Management >> Local Certificate

#### X509 Local Certificate Configuration

View         Delete             View         Delete             View         Delete	Name	Subject	Status	Modify
				View Delete
View Delete				View Delete
				View Delete

Description Item Generate Click this button to open Generate Certificate Request window. Import Click this button to import a saved file as the certification information. Refresh Click this button to refresh the information listed below. View Click this button to view the detailed settings for certificate request. Click this button to delete selected name with certification Delete information.

Available settings are explained as follows:

#### GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different



certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Certificate Name	
Subject Alternative Name	
Туре	IP Address 👻
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA V
Key Size	1024 Bit 🗸

Certificate Management >> Local Certificate

Generate

**Note:** Please be noted that "Common Name" must be configured with rotuer's WAN IP or domain name.

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

Certificate	Management >>	Local	Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Modify
server	/C=TW/ST=Hsinchu/L=Hsinchu/O	Requesting	View Delete
			View Delete
			View Delete
	GENERATE	REFRES	H

#### **IMPORT**

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.



#### Certificate Management >> Local Certificate

mport X509 Local Certificate
Upload Local Certificate
Select a local certificate file.
Certificate file: Browse.,
Click Import to upload the local certificate.
Import Cancel
Upload PKCS12 Certificate
Select a PKCS12 file.
PKCS12 file: Browse.
Password:
Click Import to upload the PKCS12 file.
Import Cancel
Upload Certificate and Private Key
Select a certificate file and a matchable Private Key.
Certificate file: Browse.
Key file: Browse.,
Password:
Click Import to upload the local certificate and private key.
Import Cancel

Item	Description				
Upload Local Certificate	It allows users to import the certificate which is generated by vigor router and signed by CA server. If you have done well in certificate generation, the Status of				
	the certificate will be shown as " <b>OK</b> ".				
	Import X509 Local Certificate Congratulation! Local Certificate has been imported successfully. Please click Back to view the certificate.				
	X509 Local Certificate Configuration				
	Name Subject Status Modify				
	draytekdemo /O=Draytek/OU=Draytek Sales/ OK View Delete				
	View Delete View Delete				
	GENERATE IMPORT REFRESH				
Upload PKCS12 Certificate	It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.				
	<b>Note:</b> PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.				
Upload Certificate and Private Key	It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.				



#### REFRESH

Click this button to refresh the information listed below.

#### View

Click this button to view the detailed settings for certificate request.

p://192.168.1.1 - Certificate S	igning Request Information - Microsoft Internet Explorer	
	Certificate Signing Request Information	
Certificate Name :	server	
Issuer :		
Subject :	C=TW, ST=Hsinchu, L=Hsinchu, O=Draytek, OU=MKT, CN=DT, emailAddress=support@draytek.com	
Subject Alternative Name	:	
Valid From :		
Valid To :		
PEM Format Content :	BEGIN CERTIFICATE REQUEST MIIBwzCCAŚwCAQAwgYIXCZAJBGMVBATTAIRXMRAwDgYDVQQIEwdIc2luY2h1MRAw DgYDVQQHEwdIc2luY2h1MRAwDgYDVQQKEwdEcmF5dGVrMQwwCgYDVQQLEwNNS1Qy CzAJBGMVBAMTAkRUMSIWIAYJKOZIhvcNAQkBFhNzdXBwb3J0QGRyYX10ZWsuY29t MIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCb06gdDL7KUjwGouC9HYPwq1Iz Ra/uaSCXJjhmJ+Vokmk8FRYkU28PTuWtavvPKH61M2cHDLRUJhQMXMA6bIuVsn3u k+2rW0Mp2IFpbnd7YgmQIBUx261Q1IK7vU/YmVYXIQR/CMhdpsgMOrGiK2N9sGVr u2/T+QqY2K7GaQw6fQIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEABIINMnczHBdd X07+ktPJaRyo2VKo9YTYQxJxuNrbVaJhvTx9NqHCyAi/DLMWSIQYJPs5Tz94Ddcr yC1rbh+206IsxcUzK7OGjMB9Y01ubchHRYRAxi2RTNQY0ICRscVJMExxAjpnXWNE IaNe0IwGZ/12/+BhlnYXzFQ8u2IIsXY= END CERTIFICATE REQUEST	( ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
	Close	
	by the certificate request information from above window or and enter the page of certificate request, copy the inform	

**Note:** You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

# 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

	Subject	Status	Modify
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

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

Certificate Management >> Trusted CA Certificate

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

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

Cer	rtificate Information - Windows In	ternet Explorer	×
🦲 http	p:// <b>192.168.1.1</b> /doc/XCaCfVi1.htm		
			^
	Certi	ficate Detail Information	
	Certificate Name:	Trusted CA-1	
	Issuer:	/C=TW/CN=jos/emailAddress=jos@draytek	
	Subject:	/C=TW/CN=jos/emailAddress=jos@draytek	
	Subject Alternative Name:		
	Valid From:	Jan 18 07:04:00 2013 GMT	
	Valid To:	Jan 18 07:04:00 2023 GMT	
		Close	~

# 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 Mana	Certificate Management >> Certificate Backup				
Certificate Back	kup / 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

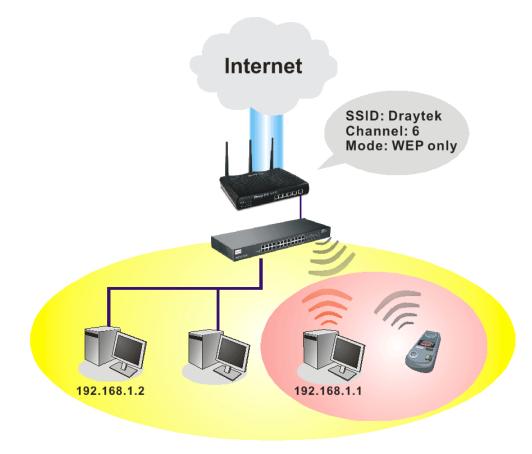
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The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

**Dray** Tek



#### **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 (IEE							
able Wireless	LAN		r				
Mode :				Mixed(11b+1	1g+11n) 🚩		
Index(1-15)	in <u>Schedu</u>	<u>ule</u> Setup:	[	,,	,		
Only schedu other action			he action	"Force Down	n" are appli	ed to the	e WLAN, all
Enable H	ide SSID		SSID		Isolate	e Membe	r Isolate VPN
1		DrayTek					
2							
3 🔲							
4					_		
Isolate Mem other. Isolate VPN: Channel: Ch	isolate win nannel 6, 24	eless with re 37MHz 💌	emote dial-	-in and LAN Long Preaml	to LAN VPr	J.	
Isolate Memi other. Isolate VPN:: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note:	isolate win nannel 6, 24 nle: necess RDRIVE [™]	eless with re 37MHz 💌 sary for som	emote dial I e old 802.	-in and LAN Long Preaml 11 b device	to LAN VPI ble: 🗌 is only(lowe	۱. r perforr	nance)
Isolate Memi other. Isolate VPN: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note: The same te	isolate win nannel 6, 24 nle: necess RDRIVE TM chnology n	eless with re 37MHz 💌 sary for som	emote dial I e old 802.	-in and LAN Long Preaml 11 b device	to LAN VPI ble: 🗌 is only(lowe	۱. r perforr	nance)
Isolate Memi other. Isolate VPN:: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note:	isolate win nannel 6, 24 nle: necess RDRIVE TM chnology n	eless with re 37MHz 💌 sary for som must also be	emote dial l e old 802. e supporte	-in and LAN Long Preaml 11 b device	to LAN VPP ble: s only(lowe to boost W	J. Pr perforr LAN perf	nance) formance.
Isolate Memi other. Isolate VPN: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note: The same te	isolate win nannel 6, 24 nle: necess RDRIVE TM chnology n	eless with re 37MHz 💌 sary for som must also be	emote dial I e old 802.	-in and LAN Long Preaml 11 b device	to LAN VPP ble: so only(lowe to boost W	۱. r perforr	nance) formance.
Isolate Memi other. Isolate VPN: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note: The same te Rate Control	isolate win nannel 6, 24 nle: necess RDRI∨E TM chnology n Enabl	eless with re 37MHz 💌 sary for som must also be	emote dial e old 802. e supporte	-in and LAN Long Preaml 11 b device d in clients	to LAN VPP ble: s only(lowe to boost W	J. Ir perforr LAN perf	nance) formance.
Isolate Memi other. Isolate VPN: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note: The same te Rate Control SSID 1	isolate win nannel 6, 24 nle: necess RDRI∨E TM chnology n Enabl	eless with re 37MHz 💌 sary for som must also be	emote dial- l e old 802. e supporte Upload	-in and LAN Long Pream 11 b device d in clients	to LAN VPP ble: is only(lowe to boost W	r perforr LAN perf Downloa	formance.
Isolate Memi other. Isolate VPN: Channel: Cr Long Preamb Packet-OVEI Tx Burst Note: The same te Rate Control SSID 1 SSID 2	isolate win nannel 6, 24 nle: necess RDRI∨E TM chnology n Enabl	eless with re 37MHz 💌 sary for som must also be	emote dial- e old 802. e supporte Upload 30000	-in and LAN Long Pream 11 b device d in clients kbps kbps	to LAN VPP ble: so only(lowe to boost W	I. r perforr LAN perf Downloar 30000	nance) formance. d kbps kbps

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, the router can connect to 11n Only, 11g Only, Mixed (11b+11g), Mixed (11a+11n), Mixed (11g+11n), and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

# **Dray** Tek

	Mixed(11b+11g+11n) 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11a+11n) Mixed(11b+11g+11n)
	In which, 802.11b/g operates on 2.4G band, 802.11a operates on 5G band, and 802.11n operates on either 2.4G or 5G band.
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this field is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.
Isolate	<ul> <li>VPN – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</li> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> </ul>
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 6, 2437MHz Channel 8, 2447MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 12, 2467MHz Channel 13, 2472MHz

Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use <b>Long Preamble</b> if needed to communicate with this kind of devices.				
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40% * more (by checking <b>Tx Burs</b> t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.				
	<b>Note:</b> 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 <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b> ).				
	Vigor N61 802.11n Wireless USB Adapter Utility         Configuration       Status       Option       About         General Setting       Advance Setting       Disable Radio         Auto launch when Windows gtart up       Disable Radio       Disable Radio         Remember mini status position       Atvo hyde mini status       2346         Auto hyde mini status       Configuration Threshold :       2347         Set mini status always on top       Bradbe IP Setting and Proxy Setting in Profile       Prequency :       802.11b/g/n - 2.4GH V         Ad-hoc       Ad-hoc       Tx Eurst :       Disable       Tx Eurst :         WILAN type to connect       only       Ad-hoc metwork only       Via Automatically connect to non-preferred networks       Via Automatically connect to non-preferred networks				
	OK Cancel Apply				
	Tx Burst : Disable Disable Enable				
	<b>Note:</b> * means the real transmission rate depends on the environment of the network.				
Rate Control	<ul> <li>It controls the data transmission rate through wireless connection.</li> <li>Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.</li> <li>Download – Type the transmitting rate for data download. Default value is 30,000 kbps.</li> </ul>				

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



### 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.

The default security mode is **Mixed (WPA+WPA2)/PSK.** Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



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

```
Wireless LAN >> Security Settings
```

SSID 1	SSID 2	SSID 3	SSID 4	
	Mode:	[	Disable	~
Set up <u>RADIUS Server</u> if 802.1			is enabled.	
WPA:				
Encry	otion Mode:	Т	KIP for WPA/AES	for WPA2
	Pre-Shared Key(F	יSK):	*****	
	Type 8~63 ASCII "cfgs01a2" or "			ligits leading by "0x", for example
WEP:				
	Encryption Mode:		64-Bit 🔽	
	⊙Key 1 :	Э		
	○Key 2 :	Э		
	○КеуЗ:	Ч	*****	
	○Кеу 4:	4	*****	
Type : "0x414 <b>For 12</b> Type :	42333132". 8 bit WEP key	er or 26 Hexad	ecimal digits lead	ng by "Ox", for example "AB312" or ing by "Ox", for example ".

ОК	Cancel
----	--------



Item	Description
Item Mode	There are several modes provided for you to choose.         Disable         WEP         WEP/802.1x Only         WPA2/802.1x mode is selected.         Disable - Turn off the encryption mechanism.         WEP-Accepts only WEP clients and the encryption key shoul 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.         WPA2/802.1x 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.         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.         WPA2/80X-Accepts only WPA2 clients and the encryption key should be entered
	key should be entered in PSK. <b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
WPA	<ul> <li>The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").</li> <li>Type - Select from Mixed (WPA+WPA2) or WPA2 only.</li> </ul>
	<b>Pre-Shared Key (PSK)</b> - Either <b>8~63</b> ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such



Item	Description
	as "0x321253abcde").
WEP	<b>64-Bit</b> - For 64 bits WEP key, either <b>5</b> ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
	<b>128-Bit</b> - For 128 bits WEP key, either <b>13</b> ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).
	Encryption Mode: 64-Bit 64-Bit 128-Bit
	All wireless devices must support the same WEP encryption bit size and have the same key. <b>Four keys</b> can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

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

#### 4.12.4 Access Control

Wireless LAN >> Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Enable Mac Address Filter	🔲 SSID 1   White List 🚩	SSID 2 White List 🔽
	SSID 3 White List 💌	SSID 4 White List 💙
	MAC Address Filter	
Index Attribute	MAC Address	Apply SSID
Client's M	AC Address : : : : : : : : : : : : : : : : : :	
	AC Address : : : : : : : : : : : : : : : : : :	
Apply SSID :		

**Dray** Tek

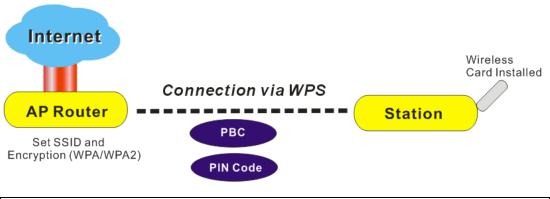
Available settings are explained as follows:

Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

### 4.12.5 WPS

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



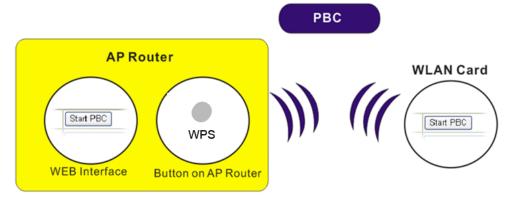
Note: Such function is available for the wireless station with WPS supported.

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

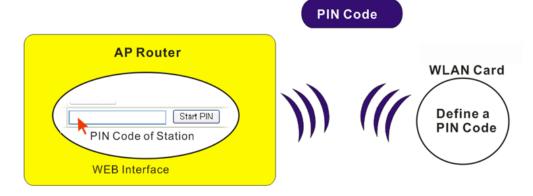


There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 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.
	ОК

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

#### Below shows Wireless LAN>>WPS web page:

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

Enable WPS

#### Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

#### **Device Configure**

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

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

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

2: WPS is Disabled.

WPS is Enabled.

Q: Waiting for WPS requests from wireless clients.

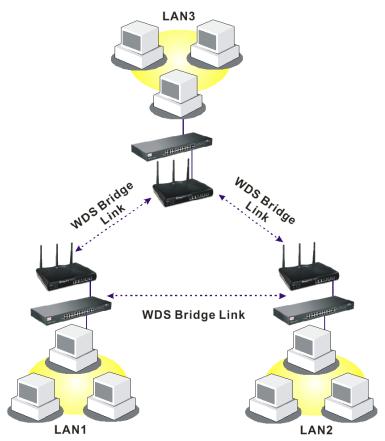
Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

## 4.12.6 WDS

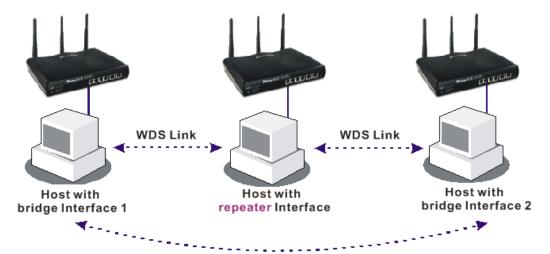
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:



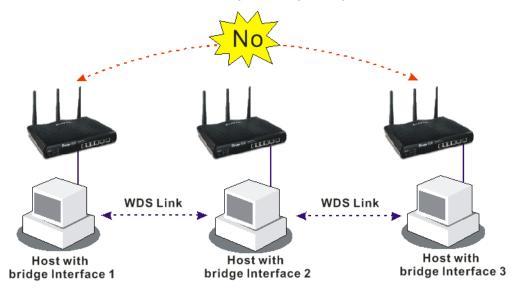
The application for the WDS-Repeater mode is depicted as below:



**Dray** Tek

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.

# **Dray** Tek

#### Wireless LAN >> WDS Settings

VDS Settings	Set to Factory Default
	Bridge
Mode: Bridge 🔽	Enable Peer MAC Address
Security:	
NEP:	
Use the same WEP key set in <u>Security Settings</u> .	<b>Note</b> : Disable unused links to get better performance.
Pre-shared Key:	Repeater
Туре:	Enable Peer MAC Addess
● DrayTek WPA ○ WPA ○ WPA2	
Кеу :	
Type 8∼63 ASCII characters or 64 hexadecimal	
digits leading by "Ox", for example "cfgsO1a2" or 'Ox655abcd".	
	Access Point Function:
	💿 Enable 🔿 Disable
	Status:
	Send "Hello" message to peers.
	Link Status
	Note: The status is valid only when the peer also supports this function.

Item	Description
Mode	Choose the mode for WDS setting. <b>Disable</b> mode will not invoke any WDS setting. <b>Bridge</b> mode is designed to fulfill the first type of application. <b>Repeater</b> mode is for the second one. Disable Bridge Repeater
Security	There are three types for security, <b>Disable</b> , <b>WEP</b> and <b>Pre-shared key</b> . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in <b>Security Settings</b> page. If you did not set any key in <b>Security Settings</b> page, this check box will be dimmed.
Pre-shared Key	Type – There are some types for you to choose. WPA and WPA2 are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router.

Item	Description
	<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.

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

# 4.12.7 Advanced Setting

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

Wireless LAN >>	Advanced Setting
-----------------	------------------

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

OK

Item	Description
Operation Mode	<ul> <li>Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards.</li> <li>However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.</li> </ul>
	<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.



Item	Description
	<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>

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

## 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.

IM Configura	ation				Set to	Factory Defau
WMM Capable 💿 Enable 🔘 Disable						
APSD Capable 🔘 Enable 💿 Disable						
MM Paramet	ters 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		
MM Paramet	ters of Station					
	Aifsn	СММІ	n 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



Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.

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

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

# 4.12.9 AP Discovery

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

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List				
	BSSID	Channel	SSID	
	1	Scan		
See <u>St</u>				
	uring the scanning p e router.	rocess (~5 secor	nds), no station is allowed to connec	t
Add to	WDS Settings :			
AP's MA	C address	: :::::		
Add t	to	💿 Bridge	🔿 Repeater	

Wireless LAN >> Access Point Discovery

Item	Description	
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.	
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics	
	Recommended channels for usage: 1 2 3 4 5 6 7 8 9 10 11 12 13	
	AP number v.s. Channel	
	1 2 3 4 5 6 7 8 9 10 11 12 13 14	
	Channel	
	Cancel	
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click <b>Add to</b> . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.	

# 4.12.10 Station List

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

Status	MAC Address	Associated with
1	Refresh	
Status Codes :		J
C: Connected, M E: Connected, V		
P: Connected, V	WPA.	
A: Connected, V B: Blocked by A		
N: Connecting.	NPA/PSK authentication.	
		ter successfully, it may be will still be on the list until the
connection expi	res.	
Add to <u>Access C</u>	ontrol :	
Client's MAC add	dress :::::	

Wireless LAN >> Station List

Item	Description	
Refresh	Click this button to refresh the status of station list.	
Add	Click this button to add current typed MAC address into Access Control.	

# 4.13 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

There are two benefits that SSL VPN provides:

- It is not necessary for users to preinstall VPN client software for executing SSL VPN connection.
- There are less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.

SSL VPN
General Setup
SSL Web Proxy
SSL Application
User Account
User Group
Online User Status
USB Application

### 4.13.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

```
SSL VPN General Setup
```

Port	443 (Default: 443)
Server Certificate	self-signed 💌
Encryption Key Algorithm	
○High - AES(128 bits) a	nd 3DES
💿 Default - RC4(128 bits	)
🔿 Low - DES	

Note: The settings will act on all SSL applications.

OK Cancel

Available settings are explained as follows:

Item	Description
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in <b>System</b> <b>Maintenance&gt;&gt;Management</b> . In general, the default setting is 443.
Server Certificate	When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose <b>Self-signed</b> to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.
Encryption Key Algorithm	Choose the encryption level for the data connection in SSL VPN server.

# **Dray** Tek

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

# 4.13.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.

SL Web Proxy Servers Profiles:			Set to Factory Default	
Index	Name	URL	Active	
<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>			×	

SSL VPN >> SSL Web Proxy

Available settings are explained as follows:

Item	Description
Name	Display the name of the profile that you create.
URL	Display the URL.
Active	Display current status (active or inactive) of such profile.

Click number link under Index filed to set detailed configuration.

#### SSL VPN >> SSL Web Proxy

	file Index : 1	
Host IP Address	me	
	L	
Access Method Secured Port Redirection	st IP Address	
	cess Method	Secured Port Redirection 🐱
Note:     URL format must be entered as http       Secured Port Redirection       SSL   OK Clear Cancel	e: URL format must be entered as http main_name is a FQDN.	Secured Port Redirection SSL ://Domain_name/directory where

Item	Description
Name	Type name of the profile.
URL	Type the address (function variation or IP address) or path of the proxy server.
Host IP Address	If you type function variation as URL, you have to type corresponding IP address in this filed. Such field must match with URL setting.

Access Method	There are three modes for you to choose
	<b>Disable</b> – the profile will be inactive. If you choose <b>Disable</b> , all the web proxy profile appeared under VPN remote dial-in web page will disappear.
	<b>Secured Port Redirection</b> – such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute "Connect" manually in SSL Client Portal page.
	<b>SSL</b> – if you choose such selection, web proxy over SSL will be applied for VPN.

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

## 4.13.3 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) /SAMBA, to any remote user with access to Internet and a web browser.

SSL	VPN	>>	SSL	Ар	pli	cat	ion
~~~			~~~			~ ~ ~ ~	

SSL Applicati	ons Profiles:		Ι.	Set to Factory Default
Index	Name	Host Address	Service	Active
<u>1.</u>				х
<u>2.</u>				х
<u>3.</u>				x
<u>4.</u>				x
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				×
<u>9.</u>				×
<u>10.</u>				×

Each item is explained as follows:

Item	Description
Name	Display the application name of the profile that you create.
Host Address	Display the IP address for VNC/RDP or SAMBA path.
Service	Display the type of the service selected, e.g., VNC/RDP/SAMBA.
Active	Display current status (active or inactive) of the selected profile.

Click number link under Index filed to make detailed configuration.

SSL	VPN >>	SSL An	plication
002		OOLAP	phoadon

Profile Index : 1		
Enable Application Service		
Application Name	For menu	
Application	Samba Application	~
Samba Path	\\172.16.3.17\Carrie	

Note: Samba Path format must be entered as \\ip\directory or \\Computer Name\directory.

OK	Clear	Cancel

Available settings are explained as follows:

Item	Description
Enable Application Service	Check this box to enable this application.
Application Name	Type the profile name for the application.
Application	Use the drop down list to choose an application applied to

this profile.		
Please Select	~	
Please Select Virtual Network Computing (VNC) Remote Desktop Protocol (RDP) Samba Application		
Different application type will lead Refer to the following:	d di	fferent web pages.

• Virtual Network Computing – Choose this item for accessing and controlling a remote PC through VNC protocol.

Profile Index : 1	
Enable Application Service	
Application Name	For menu
Application	Virtual Network Computing (VNC)
IP Address	
Port	5900
Idle Timeout	0 second(s)
Scaling	100% 😽

IP Address - Type the IP address for this protocol.

SSL VPN >> SSL Application

Port - Specify the port used for this protocol. The default setting is 5900. **Idle Timeout** – Specify a period time setting for disconnecting the VPN. **Scaling -** Chose the percentage (100%, 80%, 60) for such application.

• **Remote Desktop Protocol** - Choose this item for accessing and controlling a remote PC through RDP protocol.

Profile Index : 1	
Enable Application Servic	2
Application Name	For menu
Application	Remote Desktop Protocol (RDP)
IP Address	
Port	3389
Screen Size	Fullscreen 💌
	Fullscreen 1920*1440 1920*1200 1920*1200 1600*1200 1440*900

IP Address - Type the IP address for this protocol.**Port -** Specify the port used for this protocol.

Screen Size - Chose the screen size for such application.

• Samba Application - Any remote user can upload/download/delete certain files on a local samba server through web browser with this application

Enable Application Service	
Application Name	
Application	Samba Application
Samba Path	
	Samba Application
ote: Samba Path format must	be entered as \\ip\directory or \\Computer Name\directory.
	OK Clear Cancel

4.13.4 User Account

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item is similar to **VPN and Remote Access>>Remote Dial-in user**.

iew:	⊙All ◯Onli	ine Offline					Search
ndex	User	Active	Status	Index	User	Active	Status
<u>1.</u>	222			<u>17.</u>	272		
2.	???			<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>	???		

SSL VPN >> Remote Dial-in User

Click each index to edit one remote user profile.

SSL VPN >> Remote Dial-in User

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

Available settings are explained as follows:

Item	Description		
User account and	Enable this account - Check the box to enable this function.		
Authentication	Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.		
Allowed Dial-In Type	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.		
	SSL Tunnel - It allows the remote dial-in user to make an SSL		

Item	Description	
	VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)	
	If you check this box, the function of SSL Tunnel for this account will be activated immediately.	
	OpenVPN Tunnel - Allow the remote dial-in user to make an OpenVPN connection through Internet.	
	Specify Remote Node - Check the checkbox to specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings .	
	Netbios Naming Packet	
	• Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.	
	• Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.	
	Multicast via VPN - Some programs might send multicast packets via VPN connection.	
	• Pass – Click this button to let multicast packets pass	
	 block – This is default setting. Click this button to let multicast packets be blocked by the router. 	
Subnet	Chose one of the subnet selections for such VPN profile.	
	LAN 1 LAN 2 LAN 3 LAN 4 DMZ	
	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 o without IPSec policy above.	
Enable Mobile One-Time Passwords (mOTP)	Check this box to make the authentication with mOTP function.	
	PIN Code – Type the code for authentication (e.g, 1234). Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).	
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the	



Item	Description		
	remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.		
	Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.		
Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predex Profiles set in the VPN and Remote Access >>IPSec Identity.			
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium-Authentication Header (AH) means data will be 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.		

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

4.13.5 User Group

There are 10 user group profiles which can be created for authentication by LDAP server. Such profiles will be used by applications such as User Management, VPN and etc.

SSL VPN >> User Group

User Group Profiles:		Set to Factory Default
Index	Name	Status
<u>1.</u>		x
<u>2.</u>		x
<u>3.</u>		x
<u>4.</u>		×
<u>5.</u>		x
<u>6.</u>		x
<u>7.</u>		x
<u>8.</u>		x
<u>9.</u>		x
<u>10.</u>		x

Each item is explained as follows:

SSL VPN >> User Group

Item	Description	
Index Display the number of the client which connecting server.		
Name	Display the name of the group profile.	

Click any index number link to open the following page for detailed configuration.

ndex No. 1	
Enable	
iroup Name SSL_group1	
Access Authority	
SSL Web Proxy	SSL Application
Web_Test	🗌 For menu
Authentication Methods	
🗌 Local User DataBase	
Available User Accounts	Selected User Accounts
	>>
	**
RADIUS	
LDAP / Active Directory	

Item	Description		
Enable	Check this box to enable such profile.		
Group Name	Type a name for such profile.		
Access Authority	Specify the authority for such profile. At present, Vigor router allows you to create SSL Web Proxy and SSL Application profiles used for SSL VPN. The available profiles will be displayed here for you to select.		
	SSL Web Proxy SSL Application Web_Test For menu		
Authentication Methods	It can determine the authentication method used for such profile. Local User DataBase – The system will do the authentication by using the user defined account profiles (in VPN and Remote Access>>Remote Dial-In User). The enabled profiles will be listed in the Available User Account on the left box. To add a profile into a group, simply choose the one from the left box and click the >> button. It will be displayed in the Selected User Account on the right box. For detailed information about configuring the profile setting, refer to Objects Setting>>IP Group. RADIUS – The RADIUS server will do the authentication by using the username and password LDAP / Active Directory - If it is checked, the LDAP / AD server will do the authentication by using the username, password, information stated on the selected profiles. If the above three options are enabled, the system will do the authentication based on them in sequence.		

Available settings are explained as follows:

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

4.13.6 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into Draytek SSL VPN portal interface.

Dray Tek					
Provide SSL VPN	Home	SSL Web Proxy	SSL Tunnel		[<u>loqout</u>]
INFO	Main Page:				
mike , (172.17.1.42) Welcome to DrayTek SSL VPN! Timeout after 5 minutes. (<u>Reset</u>)	Main Page:	You have successfu You are given the fu <u>SSL Web P</u> <u>SSL Tunnel</u>	ollowing privileges: <u>roxy</u>		
			Copyright © 201	06, DrayTek Corp. All I	Rights Reserved.

Next, users can open SSL VPN>> Online Status to view logging status of SSL VPN.

			Refresh Seconds : 10 💌 refresh
Active User	Host IP	Time out(seconds)	Action
caesar	172.17.1.42	292	Drop

Each item is explained as follows:

SSL VPN >> Online Status

Item	Description	
Active User	Display current user who visit SSL VPN server.	
Host IP	Display the IP address for the host.	
Time out	Display the time remaining for logging out.	
Action	You can click Drop to drop certain login user from the router's SSL Portal UI.	

4.14 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.



4.14.1 USB General Settings

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

USB Application >> USB General Setti	ngs
USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English 💌
Samba Service Settings(Network Nei	ghborhood)
◯ Enable	
Access Mode	
● LAN Only ○ LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor

2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters, but both cannot contain any of the following: .; : " < > * + = / \ | ?.



Available settings are explained as follows:

Item	Description
General Settings	Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.
	Default Charset - At present, Vigor router supports several

Item	Description			
	types of character sets. 5 (Maximum 6) English Image: Chinese(Simple) Chinese(Simple) Chinese(Traditional) German German			
Samba Service Settings	Click Enable to invoke samba service via the router.			
Access Mode	 LAN Only – 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 storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following; : " $<> * + = \setminus $?.			
	Workgroup Name – Type a name for the workgroup.			
	Host Name – Type the host name for the router.			

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

4.14.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB 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.

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>		
8.			16.		

USB Application >> USB User Management

Each item is explained as follows:

Item	Description
Index	Display the number link of the profile.

Username	Display the name that FTP/Samba users will use for accessing into FTP/Samba server.
Home Folder	Display the home folder of this entry.

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
Access Rule	
File	🗌 Read 🔛 Write 🔛 Delete
Directory	List Create Remove
Note: The folder name can only co and space.	ontain the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! () /

Clear

Cancel

Available settings are explained as follows:

ОK

Item	Description			
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. Disable – Click this button to disable such profile. 			
Username	Type the username for FTP/Samba users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage disk.			
	 Note: "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 that mode on the FTP client. 			
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk.			
Confirm Password	Type the password again to make confirmation.			
Home FolderIt determines the folder for the client to access into The user can enter a directory name in this field. The clicking OK, the router will create the specific/new the USB storage disk. In addition, if the user types he/she can access into all of the disk folders and filled.				

Item	Description
	 storage disk. Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. Only "/" can be used in such case. You can click <i>in the specified as the following dialog to add any new folder which can be specified as the Home Folder.</i>
	http://192.168.1.5/doe/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-2 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 storage disk, must follow the rule specified here. File – Check the items (Read, Write and Delete) for such profile. Directory –Check the items (List, Create and Remove) for such profile.

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

4.14.3 File Explorer

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

USB App	lication	ı >> File E	xplorer				
File Exp	lorer						
4)	•	9	Current Path: /				
			Name		Size	Delete	Rename
↓ Up Io Select a Uploa	file: d		Browse.				

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

Item	Description
** Refresh	Click this icon to refresh files list.
✤ Back	Click this icon to return to the upper directory.
😂 Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB storage disk can be shared for other user through FTP.

Available settings are explained as follows:

4.14.4 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.

USB Application >> USB Disk Status					
USB Mass Stor	age Device Status				
Connection S	Status: No Disk Conn	ected	Disconnect USB Disk		
Disk Capacity	/: 0 MB				
Free Capacit	y: 0 MB <u>Refresh</u>				
USB Disk Use	rs Connected		Refresh		
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.



Each item is explained as follows:

Item	Description
Connection Status	If there is no USB storage disk connected to Vigor router, " No Disk Connected " will be shown here.
Disk Capacity	Display the total capacity of the USB storage disk.
Free Capacity	Display the free space of the USB storage disk. Click Refresh at any time to get new status for free capacity.
Index	Display the number of the client which connecting to FTP server.
IP Address	Display the IP address of the user's host which connecting to the FTP server.
Username	Display 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.

4.14.5 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

```
USB Application >> Syslog Explorer

      Web Syslog
      USB Syslog

      Enable Web Syslog
      I Refresh | Clear |

      Syslog Type
      User

      Time
      Message
```

For Web Syslog

Available parameters are explained as follows:

Item	Description
Enable Web Syslog	Check this box to enable the function of Web Syslog.
Syslog Type	Use the drop down list to specify a type of Syslog to be displayed. User User Firewall Call WAN VPN All
Display Mode	There are two modes for you to choose.

Item	Description
	Stop record when fulls
	Stop record when fulls Always record the new event
	 Stop record when fulls – when the capacity of syslog is full, the system will stop recording. Always record the new event – only the newest events will be recorded by the system.
Time	Display the time of the event occurred.
Message	Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.

```
USB Application >> Syslog Explorer
```

Time	Log Type	Mess	
Folder: n/a	File: n/a	Page: n/a Log	g Type: n/a
v	Veb Syslog	USB Syslog	
V	Vah Svelag	IISB Suelog	

Each item is explained as follows:

Item	Description	
Time	Display the time of the event occurred.	
Log Type	Display the type of the record.	
Message	Display the information for each event.	

4.15 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
TR-069
Administrator Password
User Password
Login Page Greeting
Configuration Backup
SysLog / Mail Alert
Time and Date
SNMP
Management
Reboot System
Firmware Upgrade
Activation
Diagnostics

4.15.1 System Status

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

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

Address

Model Name Firmware Version Build Date/Time	: Vigor3200n : 3.6.3 : Jan 15 2013 15:0	04:20				
		LAN				
	MAC Address	IP Address	Subnet Ma	ask DHCP	Server DNS	
LAN1	00-50-7F-00-00-00	192.168.1.5	255.255.2	55.0 Yes	168	.95.1.1
LAN2	00-50-7F-00-00-00	192.168.2.1	255.255.2	55.0 Yes	168	.95.1.1
LAN3	00-50-7F-00-00-00	192.168.3.1	255.255.2	55.0 Yes	168	.95.1.1
LAN4	00-50-7F-00-00-00	192.168.4.1	255.255.2	55.0 Yes	168	.95.1.1
DMZ PORT	00-50-7F-00-00-00	192.168.5.1	255.255.2	55.0 Yes	168	.95.1.1
IP Routed Subnet	00-50-7F-00-00-00	192.168.0.1	255.255.2	55.0 Yes	168	.95.1.1
		Wireless LA	N			
MAC Address	Frequen	cy Domain	Firmwa	re Version	SSID	
00-50-7F-00-00-00 Europe		2.3.2.0		DrayTek		
	· · · · ·					
		WAN				
Link Status	MAC Address	Connec	ction IP A	ddress	Default Gate	way
WAN1 Disconnect	ed 00-50-7F-00-00-	-01				
WAN2 Connected	00-50-7F-00-00-	-02 Static	IP 172	.16.3.103	172.16.3.1	
WAN3 Disconnect	ed 00-50-7F-00-00-	-03				
WAN4 Disconnect	ed 00-50-7F-00-00-	-04				
WAN5 Disconnect	ed 00-50-7F-00-00-	-05				
		IPv6				

Scope

Internet Access Mode

Each	item	is	expla	ained	as	follows:	
Lach	nem	19	CAPIC	anicu	as	10110 w 5.	

Item	Description	
Model Name	Display the model name of the router.	
Firmware Version	Display the firmware version of the router.	
Build Date/Time	Display the date and time of the current firmware build.	
LAN	MAC Address	
	- Display the MAC address of the LAN Interface.	
	IP Address	
	- Display the IP address of the LAN interface.	
	Subnet Mask	
	- Display the subnet mask address of the LAN interface.	
	DHCP Server	
	- Display the current status of DHCP server of the LAN interface	
	DNS	
	- Display the assigned IP address of the primary DNS.	
Wireless LAN	MAC Address	
	- Display the MAC address of the wireless LAN.	
	Frequency Domain	
	- It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireles 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.	
IPv6	Address - Display the IPv6 address for LAN.	
	Scope - Display the scope of IPv6 address. For example, IPv6 Link Local could only be used for direct IPv6 link. It can't be used for IPv6 internet.	
	Internet Access Mode – Display the connection mode chosen for accessing into Internet.	

4.15.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

stem Maintenance >> TR-069 Se	rtting
CS and CPE Settings	
ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client 〇 Enable	ole
URL	http://172.16.3.102:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	•••••
eriodic Inform Settings	
O Disable	
💿 Enable	
Interval Time	900 second(s)
FUN Settings	
 Disable 	
Enable	
Server IP	
Server Port	3478
Minimum Keep Aliv	/e Period 60 second(s)
Maximum Keep Ali	
·	OK

Available parameters are explained as follows:

Item	Description	
ACS Server On	Choose the interface for the router connecting to ACS server.	
ACS Server	URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.	
CPE Client	Such information is useful for Auto Configuration Server. Enable/Disable – Allow/Deny the CPE Client to connect with Auto Configuration Server.	
	Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.	
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the router to send notification to CPE. Or	



Item	Description
	click Disable to close the mechanism of notification.
STUN Settings	The default is Disable . If you click Enable , 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.
	Minimum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

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

4.15.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password			
Old Password			
New Password			
Confirm Password			
Note:Password can contain only a-z A-Z 0-9 , ; : "	< > * + = \ ? @ # ^ ! ()		

ОК

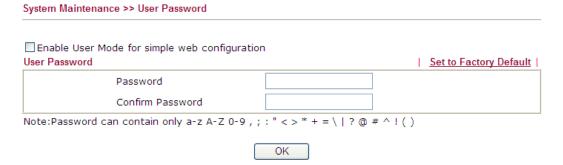
Available parameters are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is "admin" .
New Password Type in new password in this field.	
Confirm Password	Type in the new password again.

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

4.15.4 User Password

Sometimes, you may want to access into User Mode to configure the web settings for some reason. Vigor router allows you to set new user password to login into the WUI to fit your request. Simply open **System Maintenance>>User Password**.



Available parameters are explained as follows:

Item	Description
Enable User Mode for simple web configuration	Check this box to enable user mode operation. If you do not check this box, you cannot access into the user mode operation even if you enter user password in login page.
Password	Type in new password in this field.
Confirm Password	Type in the new password again.

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

Below shows an example for accessing into User Operation with User Password.

- 1. Open System Maintenance>>User Password.
- 2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

Enable User Mode	for simple web config	uration		
User Password				Set to Factory Default
P	assword	••••		
С	onfirm Password	••••		
Note:Password can	contain only a-z A-Z ()-9 , ; : " <> * + = \ ?	@ # ^ ! ()	

3. The following screen will appear. Simply click **OK**.

System Maintenance >> User Password		
Active Configuration		
Password	****	

4. Log out Vigor router Web user interface.



5. The following window will be open to ask for username and password. Type the new user password in the filed of **Password** and click **Login**.

Username	
Password	
Group	💌

6. The main screen with User Mode will be shown as follows.

Vigor3200 s Multi-WAN Security	v Router	Dray Tek
Auto Logout 💌 📭 6	System Status	~
Quick Start Wizard Online Status	Model Name : Vigor 3200n Firmware Version : 3.6.3_RC4 Build Date/Time : Jan 15 2013 15:04:20	
WAN	LAN	
VAN LAN NAT Applications Wireless LAN System Maintenance Diagnostics External Devices	LAN2 00-50-7F-CE-46-FC 192.168.2.1 255.255.255.0 Yes 168. LAN3 00-50-7F-CE-46-FC 192.168.3.1 255.255.255.0 Yes 168. LAN4 00-50-7F-CE-46-FC 192.168.4.1 255.255.255.0 Yes 168. DM2 D0-50-7F-CE-46-FC 192.168.5.1 255.255.255.0 Yes 168. DM2 D0-50-7F-CE-46-FC 192.168.5.1 255.255.255.0 Yes 168. DM2 D0-50-7F-CE-46-FC 192.168.5.1 255.255.255.0 Yes 168.	95.1.1 95.1.1 95.1.1 95.1.1 95.1.1 95.1.1 95.1.1
	Wireless LAN	
	MAC Address Frequency Domain Firmware Version SSID 00-50-7F-CE-46-FC Europe 2.3.2.0 DrayTek	
	WAN	
	Link Status MAC Address Connection IP Address Default Gate WAN1 Disconnected 00-50-7F-CE-46-FD 172.16.3.130 172.16.1.1 WAN3 Disconnected 00-50-7F-CE-46-FF WAN3 Disconnected 00-50-7F-CE-46-FF WAN4 Disconnected 00-50-7F-CE-46-FF WAN5 Disconnected 00-50-7F-CE-46-FF	way
	IPv6	
Logout All Rights Reserved.	Address Scope Internet Access Mode LAN FE80::250:7FFF:FECE:46FC/64 Link	

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

Setting in User Mode can be configured as same as in Admin Mode



4.15.5 Login Page Greeting

When you want to access into the web user interface of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify background message and the heading on the Login window if you have such requirement.

Enable			
Login Page Title	Router Login	(31 char max.)	
Welcome Message	and Bulletin (Max 511 chara	cters) <u>Preview</u> <u>Set to Factory Def</u>	<u>ault</u>
with your own m	essage. The	of the router. Replace this tex welcome message can be written be created Other markup	
tags such as p,	font or img can be used		2

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
Preview Click it to display the preview of the login window b on the settings on this web page.	
Set to Factory Default	Click to return to the factory default setting.

🔗 Vigor Login Page - Windows Internet Explorer	
🔊 http://192.168.1.1/weblogin.htm	
Just for Car Username Password Group Copyright®, DrayTek Corp. All Rights Reserve Welcome Message This welcome message is displayed in the Login page of the 1. The welcome message can be written in HTML so lis 2. Other markup tags such as p, font or img can be used	Login DrayTek

Below shows an example of login customization with the information typed in Login Description and Bulletin.

4.15.6 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

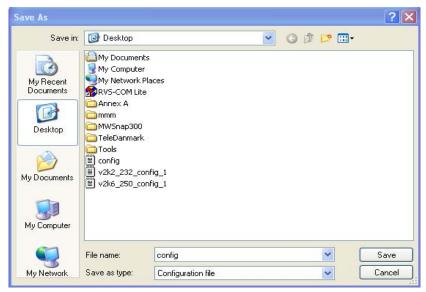
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup		
Configuration	Backup / Restoration	
Restoration		
	Select a configuration file.	
	Browse	
	Click Restore to upload the file.	
	Restore	
Backup		
	Click Backup to download current running configurations as a file.	
	Backup Cancel	

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

File Dov	vnload 🗙
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer? Open Save Cancel More Info Image: 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.



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

System Maintenance >> Configuration Backup

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

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

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

4.15.7 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web user interface of the router or borrow debug equipments.

SysLog Access Setup		Mail Alert Setup	
 Enable Syslog Save to: Syslog Server USB Disk Router Name 		Enable SMTP Server SMTP Port Mail To	Send a test e-mail
Server IP Address Destination Port Mail Syslog Enable syslog message:	514 Enable ation 514	Return-Path Authentication User Name Password Enable E-Mail Alert: Ø DOS Attack M-P2P Ø VPN LOG	

System Maintenance >> SysLog / Mail Alert Setup

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to". 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.

OK Clear

Available parameters are explained as follows:

Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog.
	Syslog Save to – Check Syslog Server to save the log to Syslog server.
	Check USB Disk to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in System Maintenance>>Management.
	If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.
Server IP Address	The IP address of the Syslog server.
Destination Port	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.



Item	Description
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.

🛅 Router Tools V3.5.1	🕨 🕥 About Router Tools	
	🐴 Firmware Upgrade Utility	
	😰 Syslog	
	😼 Uninstall Router Tools V3.5.1	
	🕘 Visit DrayTek Web Site	

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.

Dray Tek

itrols	١ 🔏	192.168.1.1 Vigor series	WAN Stati	ateway IP (Fixed)	TX Packets	TX Rate
TX Pac		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
wall Log VPN On Line Routers		ess Log Call Log	WAN Log Others Host Name:	Network Information Ne	t State	
IP Address 192.168.1.1	Mask 255.255.2	MAC 00-50-7F-54-6	NIC Description:		PCI Fast Ethernet Adapt	er - Packet St 💙
			MAC Address: IP Address:	00-11-D8-E4-58-CE	Default Geteway: DHCP Server:	192.168.1.1 192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Mon Jan 22 01:28:23 2007
	Refresh		DNS Servers:	168.95.1.1	Lease Expires:	Thu Jan 25 01:28:23 2007

4.15.8 Time and Date

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

System Maintenance >> Time and Date

Current System Time	2013 Jan 24 Thu 7 : 11 : 22 Inquire Time
Setup	
🔘 Use Browser Time	
💿 Use Internet Time	
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin 🗸
Enable Daylight Saving	
Automatically Update I	nterval 30 min 🗸

Available parameters are explained as follows:

Item	Description
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.



Item	Description
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

Applications >> SNMP

4.15.9 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the encryption method (support AES and DES) and authentication method (support MD5 and SHA) for the management needs.

✓ Enable SNMP Agent	
Get Community	public
Set Community	private
Manager Host IP(IPv4)	
Manager Host IP(IPv6)	
Trap Community	public
Notification Host IP(IPv4)	
Notification Host IP(IPv6)	
Trap Timeout	10
Enable SNMPV3 Agent	
USM User	
Auth Algorithm	No Auth 💌
Auth Password	
Privacy Algorithm	No Priv 💌
Privacy Password	

Available settings are explained as follows:

Item	Description
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public.
Set Community	Set community by typing a proper name. The default setting is private.
Manager Host IP (IPv4)	Set one host as the manager to execute SNMP function. Please type in IPv4 address to specify certain host.
Manager Host IP (IPv6)	Set one host as the manager to execute SNMP function. Please type in IPv6 address to specify certain host.

Trap Community	Set trap community by typing a proper name. The default setting is public.	
Notification Host IP (IPv4)	Set the IPv4 address of the host that will receive the trap community.	
Notification Host IP (IPv6)	Set the IPv6 address of the host that will receive the trap community.	
Trap Timeout	The default setting is 10 seconds.	
Enable SNMPV3 Agent	Check it to enable this function.	
USM User	USM means user-based security mode. Type a username which will be used for authentication.	
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm. No Auth No Auth MD5 SHA	
Auth Password	Type a password for authentication.	
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. No Priv V DES AES	
Privacy Password	Type a password for privacy.	

Click **OK** to save these settings.

4.15.10 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.

The management pages for IPv4 and IPv6 protocols are different.

For IPv4

System Maintenance >> Management

IPv4 Managemen	t Setup I	Pv6 Management Setup	
Router Name		Management Port Setup	Default Ports
Management Access Contr	ol	Telnet Port	23 (Default: 23)
Allow management from the second s	om the Internet	HTTP Port	80 (Default: 80)
FTP Server HTTP Server		HTTPS Port	443 (Default: 443)
HTTP Server HTTPS Server		FTP Port	21 (Default: 21)
✓ Telnet Server		SSH Port	22 (Default: 22)
SSH Server			
Disable PING from the	Internet		
Access List			
List IP	Subnet Mask		
1	*		
2	~		
3	~		
		Ж	

Available parameters are explained as follows:

Item	Description	
Router Name	Type a name as an identification for such router.	
Management Access Control	 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. Subnet Mask - Represent a subnet mask allowed to login to the router. 	

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

For IPv6

System Maintenance >> Management

Mana	agement Access Control	
	ow management from the Intern	et
	Telnet Server (Port : 23)	
	HTTP Server (Port : 80)	
	Enable PING from the Internet	
	ss List	
List	IPv6 Address / Prefix Length	
1.		/ 128
2.		/ 128
з.		/ 128
	: Telnt / Http server port is the	same as IPv4

Available settings are explained as follows:

Item	Description
Management Access Control	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	Enable PING from the Internet - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
	IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.

Click **OK** to save these settings.

4.15.11 Reboot System

The Web user interface may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System
Reboot System
Do you want to reboot your router ?
Osing current configuration
O Using factory default configuration
Reboot Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,,
Index(1-15) in <u>Schedule</u> Setup:,,, _,

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

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

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

4.15.12 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade
Web Firmware Upgrade
Select a firmware file. Browse
Click Upgrade to upload the file. Upgrade
TFTP Firmware Upgrade from LAN
Current Firmware Version: 3.6.3
Firmware Upgrade Procedures:
 Click "OK" to start the TFTP server. Open the Firmware Upgrade Utility or other 3-party TFTP client software. Check that the firmware filename is correct. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade. After the upgrade is compelete, the TFTP server will automatically stop running.

0K

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

System Maintenance >> Firmware Upgrade

Do you want to upgrade firmware ?

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

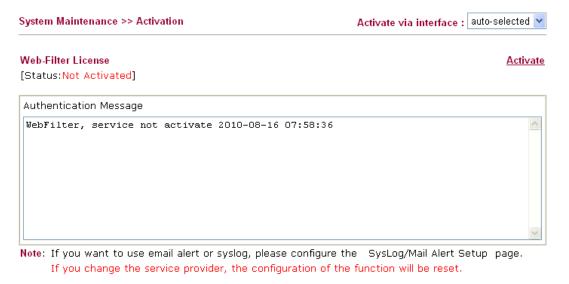


4.15.13 Activation

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

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

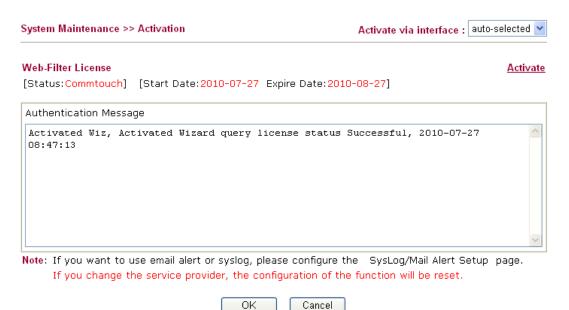


OK Cancel

Available parameters are explained as follows:

Item	Description			
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter.			
	Activate via interface : auto-selected via auto-selected via WAN 1 WAN 2 WAN 3 WAN 4 WAN 5			
Activate	The Activate 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 web filter , the process of authenticating will be displayed on this field for your reference.			

Below shows the successful activation of Web Content Filter:



4.16 Diagnostics

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



4.16.1 Dial-out Triggering

Click **Diagnostics** and click **Dial-out Triggering** to open the web page. The internet connection (e.g., PPPoE) is triggered by a package sending from the source IP address.

```
Diagnostics >> Dial-out Triggering
```

Dial-out i	Friggered Packet Header	Refresh
	HEX Format:	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00-00 00 00 00 00 0	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00 00-00 00 00 00 00 0	
	Decoded Format:	
	0.0.0.0 -> 0.0.0.0 Pr 0 len 0 (0)	

Item	Description
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

4.16.2 Routing Table

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

```
Diagnostics >> View Routing Table
```

C	urrent Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
Кеу: С * С~	- connected, S - static, R 0.0.0.0/ 0.0.0.0 192.168.1.0/ 255.255.255.	- RIP, * - default, ~ - private via 172.16.1.1 WAN1 0 directly connected LAN1 directly connected WAN1	

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
Destination FE80::/64	Interface Flags Metric LAN U 256	Next Hop 📥
FF00::/8	LAN U 256	
		~
<		>

Item	Description		
Refresh	Click it to reload the page.		

4.16.3 ARP Cache Table

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

hernet ARP Cache Table		<u>Clear</u> <u>Refresh</u>
IP Address	MAC Address	
192.168.1.10	00-0E-A6-2A-D5-A1	
172.16.3.112	00-40-CA-6B-56-BA	
172.16.3.132	00-05-5D-E4-ED-86	
172.16.3.20	00-0D-60-6F-83-BC	
172.16.3.121	00-0C-6E-E7-79-99	
172.16.3.141	00-11-2F-C7-39-0B	
72.16.3.133	00-50-7F-23-4D-B1	
72.16.3.179	00-11-2F-4B-15-F2	
72.16.3.21	00-05-5D-A1-2B-FF	
.72.16.3.2	00-11-D8-68-0D-AE	
.72.16.3.18	00-50-FC-2F-3D-17	
72.16.3.151	00-50-7F-2F-33-FF	
172.16.3.19	00-0D-60-6F-89-CA	

Each item is explained as follows:

Diagnostics >> View ARP Cache Table

Item	Description		
Clear	Click it to clear the whole table.		
Refresh	Click it to reload the page.		

4.16.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc. Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

Diagnostics >> View IPv6 Neighbour Table

IPv6 Address	Mac Address	Interface	State	^
FF02::2	33-33-00-00-00-02	LAN	CONNECTED	
FF02::1:3	33-33-00-01-00-03	LAN	CONNECTED	
FE80::3D5E:E74:8751:A44B	e8-9d-87-87-69-2f	LAN	STALE	
FF02::1:FF51:A44B	33-33-ff-51-a4-4b	LAN	CONNECTED	
FE80::250:7FFF:FEC9:1E79	00-50-7f-c9-1e-79	LAN	STALE	
FE80::250:7FFF:FEC8:4305	00-50-7f-c8-43-05	LAN	STALE	
FF02::1	33-33-00-00-00-01	LAN	CONNECTED	
FF02::1	00-00-00-00-00	USB2	CONNECTED	
FF02::1:2	00-00-00-00-00	USB2	CONNECTED	
FE80::9D5C:CA86:5428:3CA7	00-26-2d-fe-63-4f	LAN	STALE	
FF02::1:FF0A:673C	33-33-ff-0a-67-3c	LAN	CONNECTED	
FE80::213:CEFF:FE0A:673C	00-13-ce-0a-67-3c	LAN	STALE	-
FF02::1:FFB0:B00C	33-33-ff-b0-b0-0c	LAN	CONNECTED	
FE80::90:1A00:242:AD52	00-00-00-00-00	USB2	CONNECTED	
FF02::16	33-33-00-00-00-16	LAN	CONNECTED	~
<			3	

Each item is explained as follows:

Item	Description		
Refresh	Click it to reload the page.		

4.16.5 DHCP Table

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

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

	DHCP IP Assignmen	t Table	DHCPv6	IP Assign	nment Tabl	е		Refresh
LAN1	: 192.168.1.1	/255.255.255.	0, DHCP server	: On				~
Index	IP Address	MAC Address		Leased	Time	HOST	ID	
1	192.168.1.10	E0-CB-4E-DA	-48-7966:48:43		carrie	-0c7cb2	51	
2	192.168.1.11	CC-F3-A5-02	-9F-0649:42:04					
	android_b4636b5	5c154acb4 a`` İ	Êß					
3	192.168.1.12	7C-61-93-18	-EA-DF 68:02:44					
	android_807f1d0	bfff92630 ôP	" <u>}</u>					
4	192.168.1.13	A0-F4-50-10	-94-BD71:56:12		Androi	d_35896	8044568596	
5	192.168.1.14	68-09-27-BE	-CF-2270:35:08		Vivian	-iPhone		
6	192.168.1.15	F0-DC-E2-42	-24-C7 67:58:32		Hua-iP	hone		
7	192.168.1.24	70-DE-E2-E5	-EF-8050:07:04		iPad			
8	192.168.1.133	00-0E-2E-44	-68-A851:01:02		ubuntu	kyeh		
9	192.168.1.1	00-50-7F-CE	-46-FC					
DMZ Por	t : 192.168.5.1	/255.255.255.	0, DHCP server	: On				
Index	IP Address	MAC Address		Leased	Time	HOST	ID	
1	192.168.5.1	00-50-7F-CE	-46-FC					~

Diagnostics >> View DHCP Assigned IP Addresses

Diagnostics >> View DHCP Assigned IP Addresses

	DHCP II	^o Assignme	nt Table	DHCPv6 IP Assi	ignment Table	L 1	Refresh
1		r binding Address	client:	MAC	Address Le	ased Time	~
1							~

Available settings are explained as follows:

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

4.16.6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active 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	

Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

4.16.7 Data Flow Monitor

Diagnostics >> Data Flow Monitor

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



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

		Refresh Sec	onds: 10 🔽 Page	e: 1 🚩		Refr	esh
Index	IP Address	TX rate(Kbps)	RX rate(Kbps) 😪	Sessions	Action	APP Q	oS
1	192.168.1.10_CARRIE- 0C7CB251	0	0	55	Block	None	~
2	192.168.1.13			22	Block	None	~
						None	
						Class 1	
						Class 2 Class 3	
						Default	
					L		_
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak			
WAN1		0 / 0 / Auto	0 / 0 / Auto	0			
WAN2	172.16.3.130	2 / 1091 / Auto	200 / 6293 / Auto	74			
WAN3		0 / 0 / Auto	0 / 0 / Auto	0			
WAN4		0 / 0 / Auto	0 / 0 / Auto	0			
WAN5		0 / 0 / Auto	0 / 0 / Auto	0			
Total		2 / 1091 / Auto	200 / 6293 / Auto	74 / 344			

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.

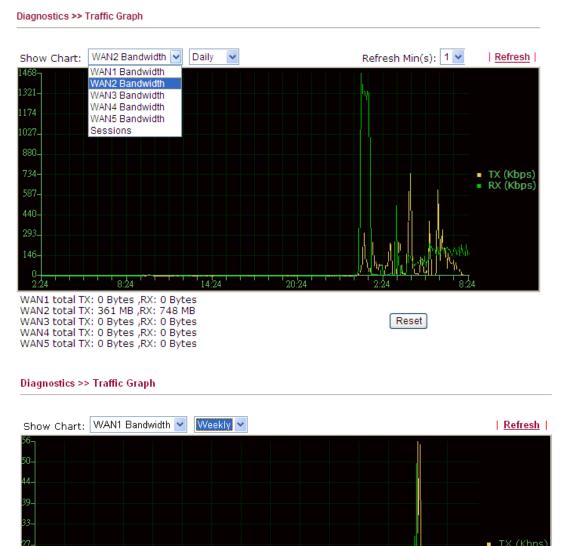
Item	Description
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system



Item	Description			
	automatically.			
	Refresh Seconds: 10 🕶 10 15 30			
Refresh	Click this link to refresh this page manually.			
Index	Display the number of the data flow.			
IP Address	Display the IP address of the monitored device.			
TX rate (kbps)	Display the transmission speed of the monitored device.			
RX rate (kbps)	Display the receiving speed of the monitored device.			
Sessions	Display the session number that you specified in Limit Session web page.			
Action	Block - can prevent specified PC accessing into Internet within 5 minutes. Page: 1 Image: 1 Refresh Kbps) Sessions Action Block Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.			
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host)			
Current /Peak/Speed	 Current means current transmission rate and receiving rate for WAN interface. Peak means the highest peak value detected by the router in data transmission. Speed means line speed specified in WAN>>General Setup. If you do not specify any rate at that page, here will display Auto for instead. 			

4.16.8 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.



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.

2/18(M)

2/20/W

14 N

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

2/14⁽TH)

2/15(F)



2/17(SU)

2/16(SA)

4.16.9 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis			
⊙ IPV4 ◯ IP	V6		
		LAN PC or you don't want to specif t "Unspecified".	y which WAN to
Ping throu	ugh: Unspecifie	ed 🔽	
Ping to: H	Host / IP 🛛 🖌	IP Address:	
	Host / IP DNS	Run	
	Sateway 1		<u>Clear</u>
	Gateway 2 — Gateway 3		<u>~</u>
	Gateway 4 Gateway 5		
			~

Diagnostics >> Ping Diagnosis

Ping Diagnosis	
Ping IPv6 Address:	
Run	
Result	<u>Clear</u>
	~
	~
	2

Item	Description	
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically.	
Ping to	Use the drop down list to choose the destination that you want to ping.	
IP Address	Type in the IP address of the Host/IP that you want to ping.	
Run	Click this button to start the ping work. The result will be displayed on the screen.	

Clear	Click this link to remove the result on the window.
-------	---

4.16.10 Trace Route

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

Diagnostics >> Trace Route

Frace Route		
⊙ IPV4 ○ IPV6		
Trace through:	Unspecified 💌	
Protocol:	Unspecified WAN1	
Host / IP Address:	WAN2 WAN3	
Result	WAN4 Run WAN5	<u>Clear</u>
		\sim

Diagnostics >> Trace Route

Trace Route	
Trace Host / IP Address:	
Run	
Result	<u>Clear</u>
	~
	<u>~</u>

Item	Description
Trace through	Use the drop down list to choose the WAN interface that you want to ping through.



	Unspecified Unspecified WAN1 WAN2 WAN3 WAN4 WAN5		
Protocol	Use the drop down list to choose the protocol that you want to ping through.		
Host/IP Address	It indicates the IP address of the host.		
Run	Click this button to start route tracing work.		
Clear	Click this link to remove the result on the window.		

4.16.11 TSPC Status

IPv6 TSPC status web page could help you to diagnose the connection status of TSPC.

If TSPC has configured properly, the router will display the following page when the user connects to tunnel broker successfully.

```
Diagnostics >> IPv6 TSPC Status
```

WAN1	WAN2	WAN3	WAN4	WAN5	Refresh								
TSPC Ena	bled												
TSPC Con	nection Status												
Local En	dpoint v4 Addre	ess :	1.169.155.138										
Local En	dpoint v6 Addre	ess :	2001:05c0:	1400:000b:00	00:0000:0000:b527								
Router DNS name :			vigor2850.broker.freenet6.net										
Remote Endpoint v4 Address : Remote Endpoint v6 Address : Tspc Prefix :			81.171.72.11 2001:05c0:1400:000b:0000:0000:0000:b526 2001:05c0:1513:5900:0000:0000:0000:0000										
								Tspc Pre	efixlen :		56		
								Tunnel E	Broker :		amsterdam.	freenet6.net	
Tunnel S	Status :		Connected										

Available settings are explained as follows:

Item	Description		
Refresh	Click this link to refresh this page manually.		

4.17 External Devices

Vigor router can be used to connect with many types of external devices. In order to control or manage the external devices conveniently, open **External Devices** to make detailed configuration.

External Devices

External Device Auto Discovery
External Devices Connected
Below shows available devices that connected externally:

For security reason:
If you have changed the administrator password on External Device, please click the Account button to
retype new username and password. Otherwise, the router will be unable to monitor the External Device
device properly. Click the Clear button to Clear the off-line information and account information.

OK

From this web page, check the box of External Device Auto Discovery. Later, all the

From this web page, check the box of **External Device Auto Discovery**. Later, all the available devices will be displayed in this page with icons and corresponding information. You can change the device name if required or remove the information for off-line device whenever you want.

When you finished the configuration, click **OK** to save it.

Note: Only DrayTek products can be detected by this function.



This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**1.3 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to "**1.3 Hardware Installation**" to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

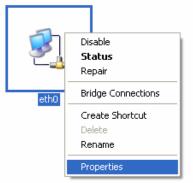


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.DrayTek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.



2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.

🕹 eth0 Properties 🛛 🔹 💽 🔀
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 lr
This connection uses the following items:
Elient for Microsoft Networks Elient for Microsoft Networks Elie and Printer Sharing for Microsoft Networks Elient Sharing for Microso
Leg QoS Packet Scheduler Internet Protocol (TCP/IP)
Install Uninstall Properties
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 ✓ Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity
OK Cancel

4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Internet Protocol (TCP/IP) Prope	erties 🛛 🛛 🔀
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
Obtain an IP address automatica	lly
Use the following IP address: —	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	· · · ·
Obtain DNS server address auto	matically
OUse the following DNS server ad	dresses:
Preferred DNS server:	
Alternate DNS server:	
	Ad <u>v</u> anced
	OK 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.

			Network				
how All	Displays Sou	Network Star	tup Disk				
	Lo	ocation: Autom	atic		:		
		Show: Built-i	n Etherne	!	•		
	TCP/	IP PPPoE A	ppleTalk	Proxies	Ethern	et	
Cor	nfigure IPv4:	Using DHCP			•		
	IP Address:	192.168.1.10			Ren	ew DHC	P Lease
Si	ubnet Mask:	255.255.255.0	D	HCP Client I			
	Router:	192.168.1.1			(11.1	equired)	
C	ONS Servers:						(Optional)
Searc	ch Domains:						(Optional)
IP	v6 Address:	fe80:0000:0000	:0000:02	Da:95ff:fe8d	d:72e4		
		Configure IPv6					(?)

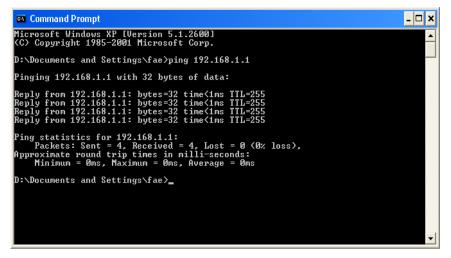
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

Please follow the steps below to ping the router correctly.

For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

For 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.



000	Terminal — bash — 80x24	
Welcome to Darwin Vigor10:~ draytek PING 192.168.1.1	\$ ping 192.168.1.1 (192.168.1.1): 56 data bytes	8
64 bytes from 192 64 bytes from 192 64 bytes from 192	.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms .168.1.1: icmp_seq=1 ttl=255 time=0.697 ms .168.1.1: icmp_seq=2 ttl=255 time=0.716 ms .168.1.1: icmp_seq=3 ttl=255 time=0.731 ms .168.1.1: icmp_seq=4 ttl=255 time=0.72 ms	
192.168.1.1 p 5 packets transmi	ing statistics tted, 5 packets received, 0% packet loss g/max = 0.697/0.723/0.755 ms \$ ∎	

5.4 Checking If the ISP Settings are OK or Not

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

WAN >> Internet Access

ndex	Display Name	Physical Mode	Access Mode			
WAN1		Ethernet	None	*	Details Page	IPv6
WAN2		Ethernet	Static or Dynamic IP	*	Details Page	IPv6
WAN3		Ethernet	None PPPoE		Details Page	IPv6
WAN4		Ethernet	Static or Dynamic IP PPTP/L2TP		Details Page	IPv6
WAN5		USB	None	~	Details Page	IPv6

Note : Only one WAN can support IPv6.

5.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your 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.

/ = > _	- *	192.168.1.1 Vigor	Getway IP (Static)	TX Packets	RX Rate
AN Status TX Packets 6442		RX Packets 3807	WAN IP (Static)	RX Packets	TX Rate
e Wall Log VPN Log	User Acce	ss Log Call Log WAN L	og Network Infomation	Net State	
Time	Host	Message			~
Apr 12 09:17:49	Vigor		col:LCP(c021) ConfReq Ide 00 00 00 00 02 00 03 00	entifier:0x03 ACCM:	0x0 Authe:
Apr 12 09:17:49	Vigor		00 00 00 00 02 00 03 00		
		MAN2 PPPoF Proto	cold CP(c021) ConfPer Ide	antifiar 0x00 MRII-19	SOD ACCN
	Vigor		col:LCP(c021) ConfReq Ide I 1 PADS ID-0	entifier:0x00 MRU: 15	500 ACCM
Apr 12 09:17:49	Vigor Vigor Vigor	WAN2 PPPoE -> Proto WAN2 PPPoE -> V:1 1 [3G]Modem response: C	I:1 PADS ID:0	entifier:0x00 MRU: 15	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor	WAN2 PPPoE <= V:1 1 [3G]Modem response: C [3G]Modem status:a1 20	T 1 PADS ID 0 ONNECT 3600000 00 00 00 00 02 00 02 00	entifier:0x00 MRU: 15	SOD ACCM
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	WAN2 PPPoE <= V:1 1 [3G]Modem response: C [3G]Modem status:a1 20 [3G]Modem status:a1 20	T:1 PADS ID:0 CONNECT 3600000 00 00 00 00 02 00 02 00 00 00 00 00 02 00 02 00	entifier:0x00 MRU: 15	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE - V:1 [3G]Modem response: C [3G]Modem status:a1 20 [3G]Modem status:a1 20 [3G]Modem dial ATDT*	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 02 00 02 00 00 00 00 00 02 00 02 00 99#	entifier:0x00 MRU: 15	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE - V:1 1 [3G]Modem response: C [3G]Modem status:a1 20 [3G]Modem status:a1 20 [3G]Modem dial ATDT* WAN2 PPPoE - V:1 1	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 02 00 02 00 00 00 00 00 00 02 00 02 00 99% T:1 PADR ID:0	entifier:0x00 MRU: 15	SOD ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE ← V:1 [3G]Modem response: C [3G]Modem statusal 20 [3G]Modem statusal 20 [3G]Modem dial ATDT ⁴ WAN2 PPPoE → V:1 WAN2 PPPoE → V:1	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 00 02 00 02 00 00 00 00 00 00 02 00 02 00 99# T:1 PADR ID:0 T:1 PADR ID:0 T:1 PADR ID:0	entifier:0x00 MRU: 15	SOD ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= V:1 1 [3G]Modem response: C [3G]Modem status:al 20 [3G]Modem dial ATDT4 WAN2 PPPoE => V:1 1 WAN2 PPPoE <= V:1 1 [3G]Modem response: O [3G]Modem initialize A1	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 02 00 02 00 999# T:1 PADR ID:0 T:1 PADC ID:0 K K G&FE0V1X1&D2&C1S0=0		SOD ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= V:1 [3G]Modem response: C [3G]Modem status: al 20 [3G]Modem dial A TD 1 WAN2 PPPoE => V:1 1 WAN2 PPPoE <= V:1 [3G]Modem response: O	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 02 00 02 00 999# T:1 PADR ID:0 T:1 PADC ID:0 K K G&FE0V1X1&D2&C1S0=0		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE <= V:1 1 [3G]Modem response: C [3G]Modem status:al 20 [3G]Modem dial ATDT4 WAN2 PPPoE => V:1 1 WAN2 PPPoE <= V:1 1 [3G]Modem response: O [3G]Modem initialize A1	T:1 PADS ID:0 ONNECT 3600000 00 00 00 00 02 00 02 00 999# T:1 PADR ID:0 T:1 PADC ID:0 K K G&FE0V1X1&D2&C1S0=0		500 ACCM

Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by 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.



5.6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

2

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.

Software Reset

You can reset the router to factory default via Web page. Such function is available in Admin Mode only.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System				
Reboot System				
Do you want to reboot your router ?				
Osing current configuration				
O Using factory default configuration				
Reboot Now Auto Reboot Time Schedule				
Index(1-15) in <u>Schedule</u> Setup:,,,,,,, Note: Action and Idle Timeout settings will be ignored.				
OK Cancel				

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.



5.7 Contacting 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.