

DrayTek

Vigor3200 Series

Multi-WAN Security Router



Your reliable networking solutions partner

User's Guide

V2.0

Vigor3200 Series Multi-WAN Security Router User's Guide

Version: 2.0

Firmware Version: V3.6.8.5

(For future update, please visit DrayTek web site)

Date: July 19, 2016

Copyright Information

Copyright Declarations

© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the quick start guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

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

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

<http://www.DrayTek.com>

European Community Declarations

Manufacturer: DrayTek Corp.

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

Product: 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

1

Introduction	1
1.1 Web Configuration Buttons Explanation	2
1.2 LED Indicators and Connectors	3
1.2.1 For Vigor3200	3
1.2.2 For Vigor3200n	5
1.3 Hardware Installation	7
1.4 Printer Installation	8
1.5 Accessing Web Page	14
1.6 Changing Password	15
1.7 Online Status	16
1.8 Saving Configuration	19
1.9 Support Area	19

2

Quick Setup	21
2.1 Quick Start Wizard	21
2.1.1 For WAN1 – WAN4	23
2.1.2 For WAN5	30
2.2 Service Activation Wizard	33
2.3 VPN Client Wizard	36
2.4 VPN Server Wizard	43
2.5 Wireless Wizard	48
2.6 Registering Vigor Router	51

3

Tutorials and Applications	55
3.1 How to Implement the AD/LDAP Authentication for User Management?	55
3.2 How to implement the AD/LDAP authentication for SSL Application?	58
3.3 How to Configure Multi-Subnet	66
3.4 How to Customize Your Login Page	71
3.5 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	73
3.6 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	82
3.7 QoS Setting Example	87
3.8 Request a certificate from a CA server on Windows CA Server	91

3.9 Request a CA Certificate and Set as Trusted on Windows CA Server	95
3.10 Creating an Account for MyVigor	97
3.10.1 Creating an Account via Vigor Router	97
3.10.2 Creating an Account via MyVigor Web Site.....	100
3.11 How can I get the files from USB storage device connecting to Vigor router?	104
3.12 VPN Trunk Load-Balance between Vigor 3200 and Other Vigor Router	107
3.13 How to implement RADIUS authentication for User Management?	118

4

Web Configuration 131

4.1 WAN	131
4.1.1 Basics of Internet Protocol (IP) Network.....	131
4.1.2 General Setup.....	133
4.1.3 Internet Access	137
4.2 LAN	153
4.2.1 Basics of LAN	154
4.2.2 General Setup.....	156
4.2.3 Static Route	167
4.2.4 VLAN.....	172
4.2.5 Bind IP to MAC	173
4.2.6 LAN Port Mirror.....	174
4.2.7 Web Portal Setup.....	175
4.3 Load-Balance /Route Policy.....	177
4.4 NAT	183
4.4.1 Port Redirection	184
4.4.2 DMZ Host.....	187
4.4.3 Open Ports.....	190
4.4.4 Port Triggering	192
4.5 Firewall.....	195
4.5.1 Basics for Firewall.....	195
4.5.2 General Setup.....	197
4.5.3 Filter Setup	201
4.5.4 DoS Defense	209
4.6 User Management.....	212
4.6.1 General Setup.....	213
4.6.2 User Profile (Reserved)	214
4.6.3 User Group	218
4.6.4 User Online Status.....	219
4.7 Objects Settings	220
4.7.1 IP Object	220
4.7.2 IP Group	223
4.7.3 IPv6 Object	225
4.7.4 IPv6 Group.....	227
4.7.5 Service Type Object	229
4.7.6 Service Type Group.....	231
4.7.7 Keyword Object	233
4.7.8 Keyword Group.....	235
4.7.9 File Extension Object.....	237

4.7.10 SMS/Mail Service Object.....	239
4.7.11 Notification Object.....	244
4.8 CSM Profile.....	246
4.8.1 APP Enforcement Profile.....	247
4.8.2 URL Content Filter Profile.....	250
4.8.3 Web Content Filter Profile.....	255
4.8.4 DNS Filter.....	258
4.8.5 APPE Support List.....	260
4.9 Bandwidth Management.....	261
4.9.1 Sessions Limit.....	261
4.9.2 Bandwidth Limit.....	263
4.9.3 Quality of Service.....	265
4.10 Applications.....	274
4.10.1 Dynamic DNS.....	274
4.10.2 LAN DNS.....	277
4.10.3 Schedule.....	279
4.10.4 RADIUS.....	282
4.10.5 LDAP / Active Directory.....	283
4.10.6 UPnP.....	285
4.10.7 IGMP.....	287
4.10.8 Wake on LAN.....	288
4.10.9 SMS/Mail Alert Service.....	289
4.11 VPN and Remote Access.....	291
4.11.1 Remote Access Control.....	292
4.11.2 PPP General Setup.....	292
4.11.3 IPSec General Setup.....	294
4.11.4 IPSec Peer Identity.....	295
4.11.5 Remote Dial-in User.....	298
4.11.6 LAN to LAN.....	302
4.11.7 VPN TRUNK Management.....	311
4.11.8 Connection Management.....	321
4.12 Certificate Management.....	323
4.12.1 Local Certificate.....	323
4.12.2 Trusted CA Certificate.....	327
4.12.3 Certificate Backup.....	328
4.13 Wireless LAN.....	328
4.13.1 Basic Concepts.....	328
4.13.2 General Setup.....	331
4.13.3 Security.....	334
4.13.4 Access Control.....	336
4.13.5 WPS.....	337
4.13.6 WDS.....	340
4.13.7 Advanced Setting.....	343
4.13.8 WMM Configuration.....	343
4.13.9 AP Discovery.....	346
4.13.10 Station List.....	347
4.14 SSL VPN.....	348
4.14.1 General Setup.....	348
4.14.2 SSL Web Proxy.....	349
4.14.3 SSL Application.....	351
4.14.4 User Account.....	353
4.14.5 User Group.....	357
4.14.6 Online User Status.....	359

4.15 USB Application	360
4.15.1 USB General Settings.....	360
4.15.2 USB User Management.....	361
4.15.3 File Explorer.....	364
4.15.4 USB Disk Status	364
4.15.5 Modem Support List.....	365
4.16 System Maintenance.....	366
4.16.1 System Status.....	366
4.16.2 TR-069.....	368
4.16.3 Administrator Password.....	369
4.16.4 User Password	370
4.16.5 Login Page Greeting.....	372
4.16.6 Configuration Backup	375
4.16.7 Syslog/Mail Alert	377
4.16.8 Time and Date	379
4.16.9 SNMP.....	381
4.16.10 Management.....	383
4.16.11 Reboot System	386
4.16.12 Firmware Upgrade	387
4.16.13 Activation	388
4.17 Diagnostics.....	389
4.17.1 Dial-out Triggering	390
4.17.2 Routing Table	391
4.17.3 ARP Cache Table	392
4.17.4 IPv6 Neighbour Table.....	392
4.17.5 DHCP Table.....	393
4.17.6 NAT Sessions Table	394
4.17.7 DNS Cache Table.....	395
4.17.8 Data Flow Monitor.....	396
4.17.9 Traffic Graph.....	398
4.17.10 Ping Diagnosis.....	399
4.17.11 Trace Route	400
4.17.12 Syslog Explorer.....	401
4.17.13 IPv6 TSPC Status.....	403
4.18 External Devices	404

5

Trouble Shooting.....405

5.1 Checking If the Hardware Status Is OK or Not.....	405
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	406
5.3 Pinging the Router from Your Computer	409
5.4 Checking If the ISP Settings are OK or Not.....	410
5.5 Problems for 3G Network Connection	411
5.6 Backing to Factory Default Setting If Necessary	412
5.7 Contacting DrayTek.....	413

1

Introduction

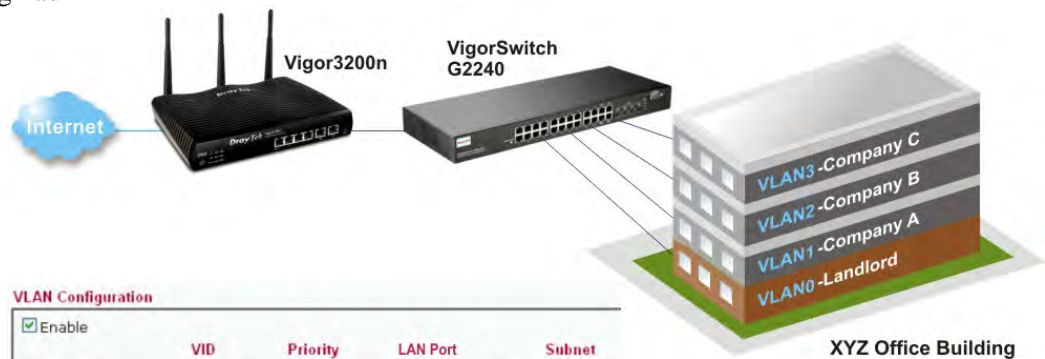
Vigor3200 Series, a broadband router, integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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



VLAN Configuration

Enable

	VID	Priority	LAN Port	Subnet
VLAN0	Landlord	4	Tagged/Untagged	LAN 1
VLAN1	A	1	<input checked="" type="checkbox"/>	LAN 2
VLAN2	B	2	<input checked="" type="checkbox"/>	LAN 3
VLAN3	C	3	<input checked="" type="checkbox"/>	LAN 4


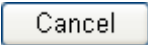
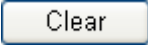
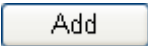


Multiple Subnet

LAN1: 192.168.5.x
LAN2: 192.168.6.x
LAN3: 192.168.7.x
LAN4: 192.168.8.x

mode.

1.1 Web Configuration Buttons Explanation

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

	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the settings for the selected item.
	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.

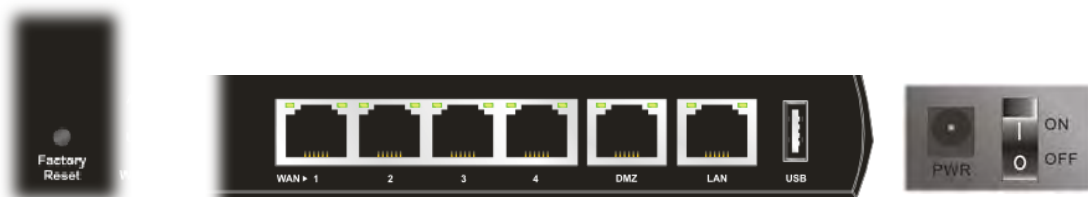
1.2.1 For Vigor3200



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).

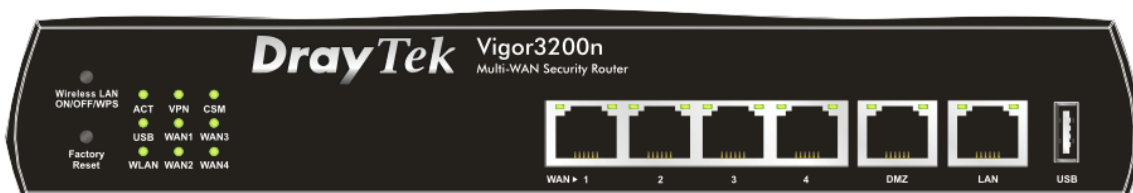
LED on Connector

WAN 1/2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
LAN	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		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	Connector for local DMZ host.
LAN	Connector for local network devices.
USB	Connector for 3G Modem or printer.
PWR	Connector for a power adapter.
ON/OFF	Power Switch.

1.2.2 For Vigor3200n



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 Connector

WAN 1/2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
		Blinking	The data is transmitting.
DMZ	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
		Blinking	The data is transmitting.
LAN	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps when left LED is on.
		Blinking	The data is transmitting.



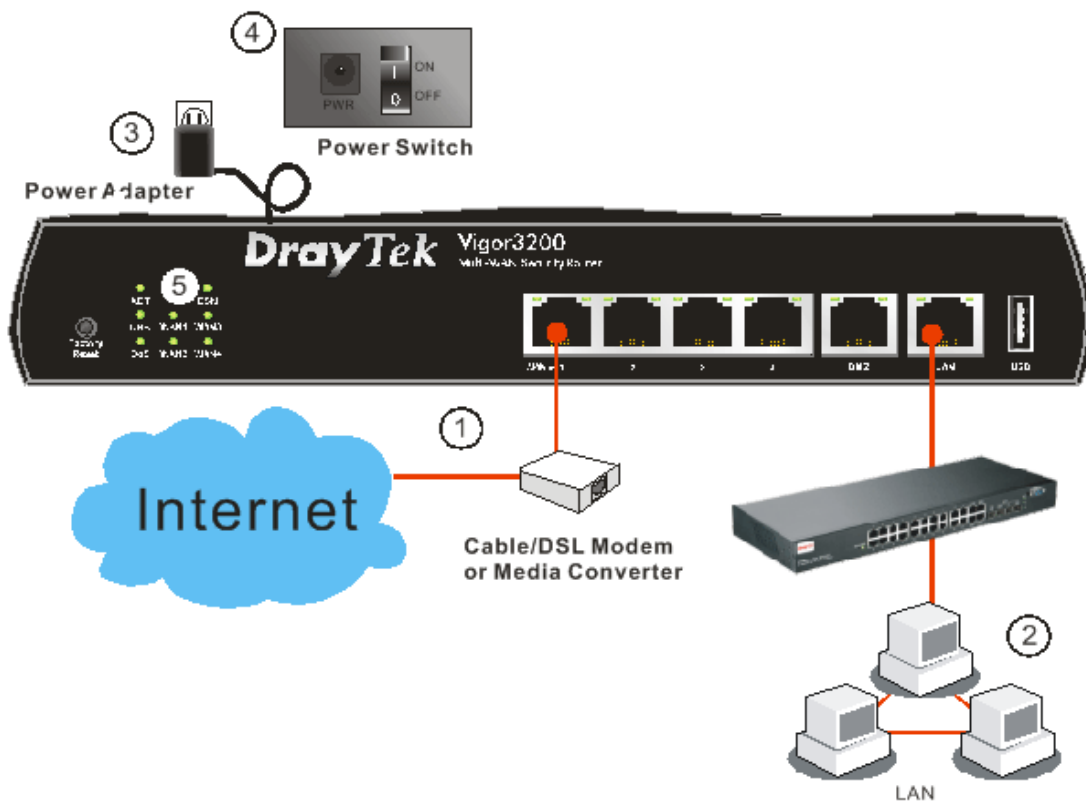
Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button once to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button twice to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
WAN1- WAN4	Connecters for remote networked devices.
DMZ	Connector for local DMZ host.
LAN	Connector for local network devices.
USB	Connector for 3G Modem or printer.
PWR	Connector 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.

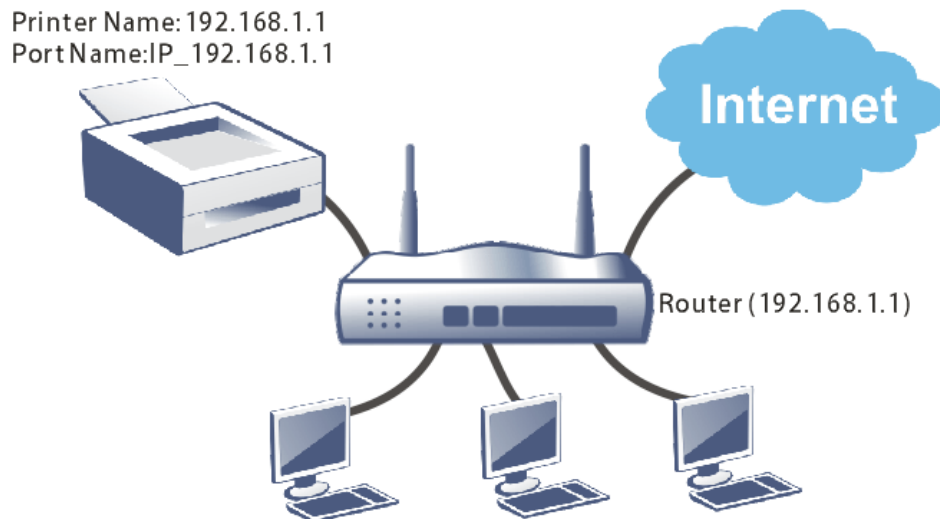
1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one end of an Ethernet cable (RJ-45) to the LAN port of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer. Or, use a switch to connect Vigor router 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.)



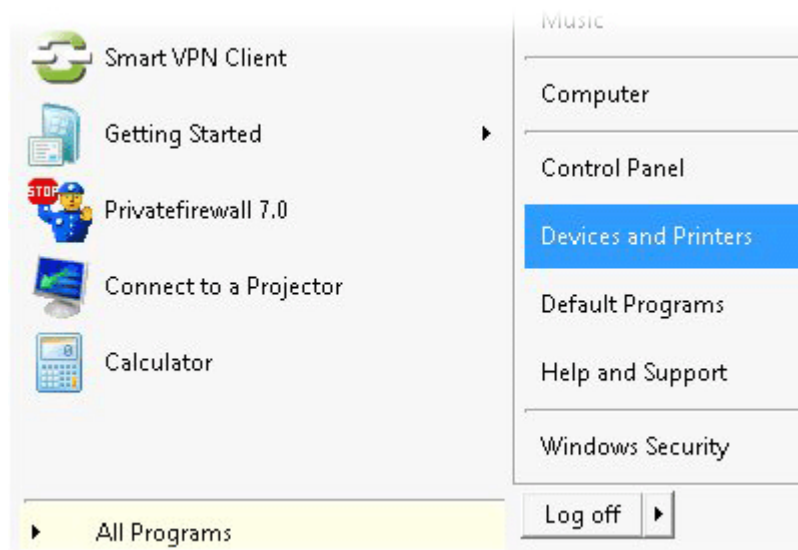
1.4 Printer Installation

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 7. For other Windows system, please visit www.DrayTek.com.

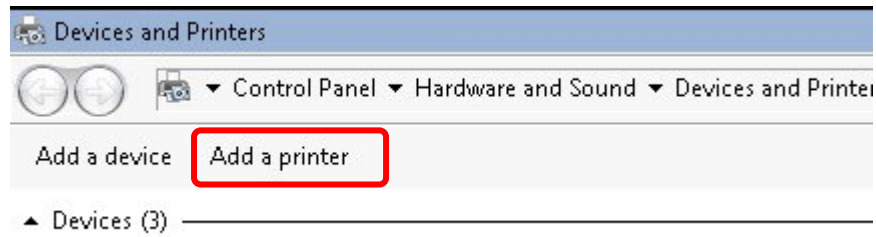


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

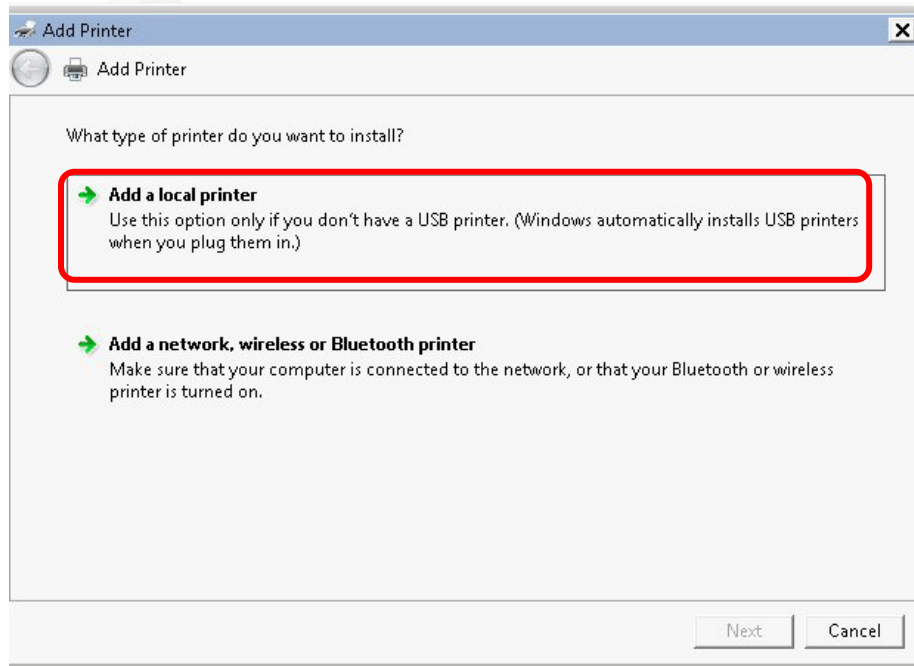
1. Connect the printer with the router through USB/parallel port.
2. Open **All Programs>>Getting Started>>Devices and Printers**.



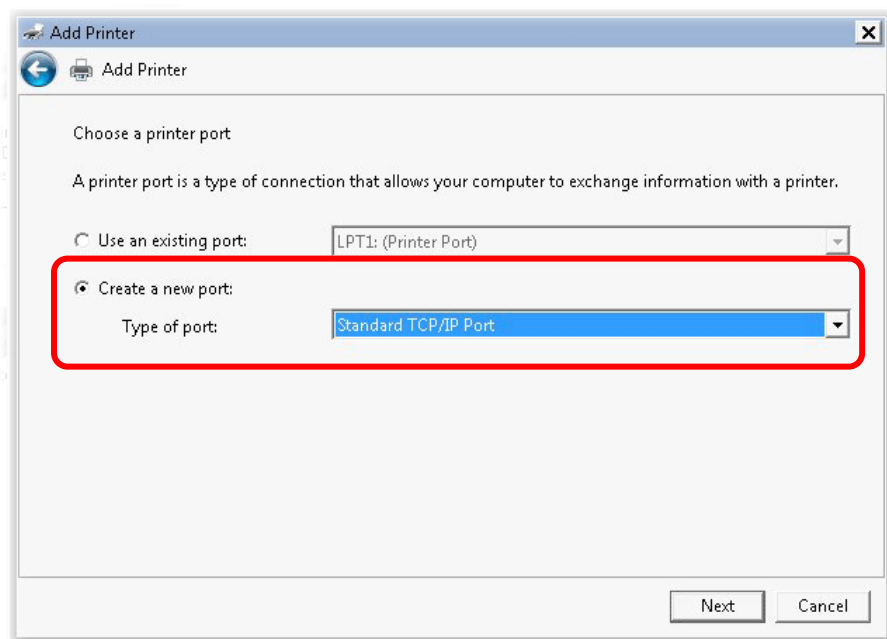
3. Click **Add a printer**.



4. A dialog will appear. Click **Add a local printer** and click **Next**.



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



6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Hostname or IP Address** and type **192.168.1.1** as the **Port name**. Then, click **Next**.

The screenshot shows the 'Add Printer' dialog box with the following fields and values:

- Device type: TCP/IP Device
- Hostname or IP address: 192.168.1.1
- Port name: 192.168.1.1

A red rectangular box highlights the 'Hostname or IP address' and 'Port name' fields. At the bottom right, there are 'Next' and 'Cancel' buttons.

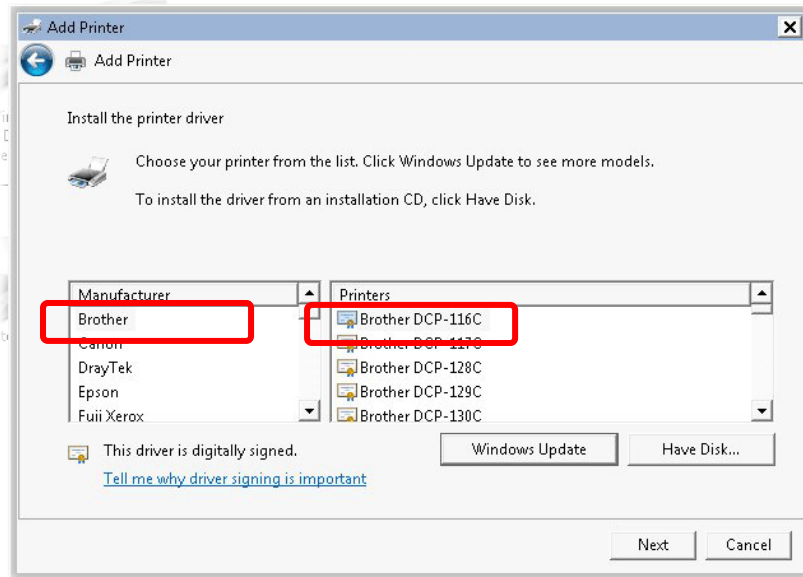
7. Click **Standard** and choose **Generic Network Card**.

The screenshot shows the 'Add Printer' dialog box with the following information:

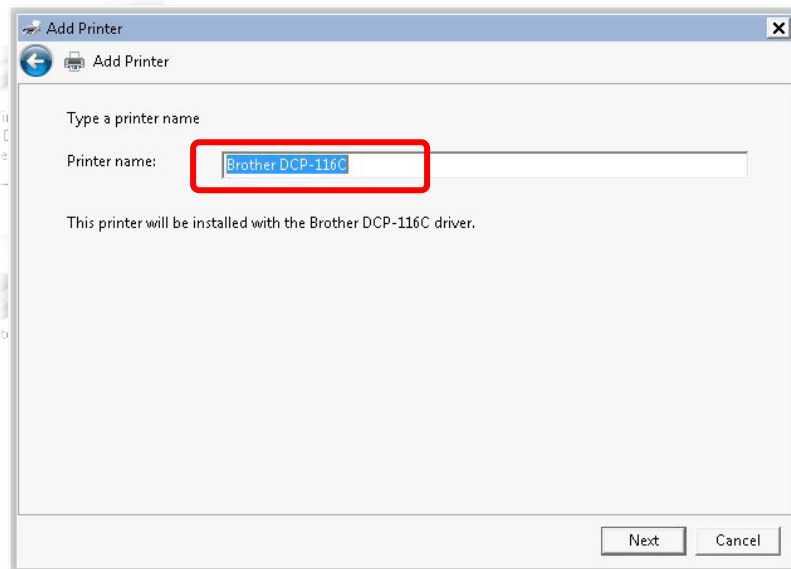
- Additional port information required
- The device is not found on the network. Be sure that:
 1. The device is turned on.
 2. The network is connected.
 3. The device is properly configured.
 4. The address on the previous page is correct.
- If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
- Device Type:
 - Standard: Generic Network Card
 - Custom: Settings...

A red rectangular box highlights the 'Standard' radio button and the 'Generic Network Card' dropdown menu. At the bottom right, there are 'Next' and 'Cancel' buttons.

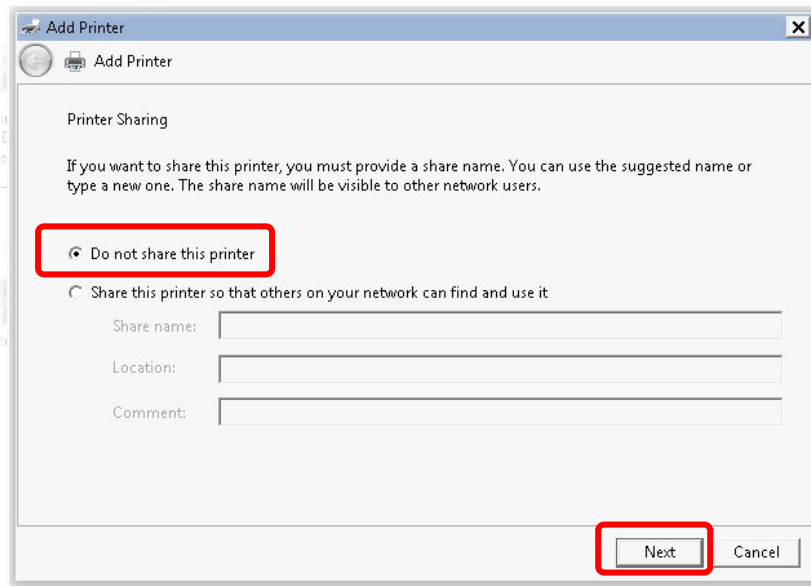
- Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



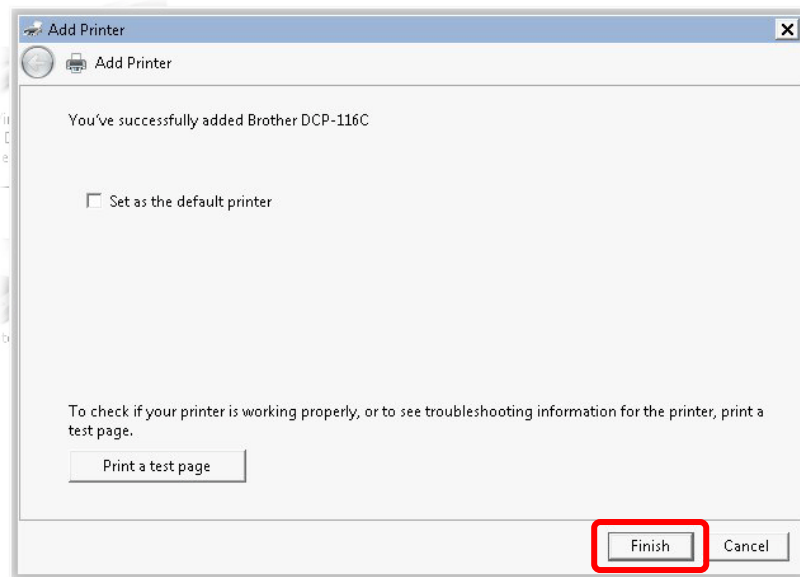
- Type a name for the chosen printer. Click **Next**.



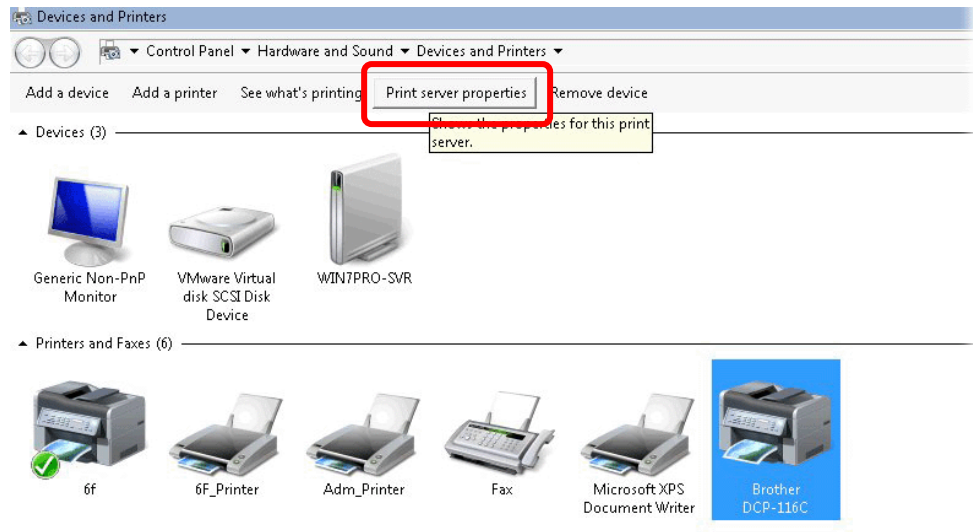
10. Choose **Do not share this printer** and click **Next**.



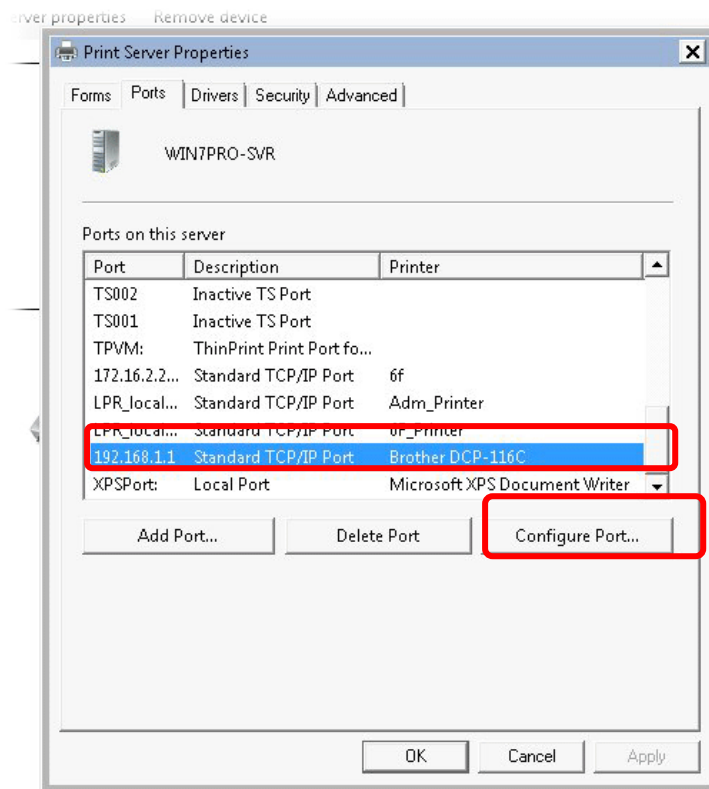
11. Then, in the following dialog, click **Finish**.



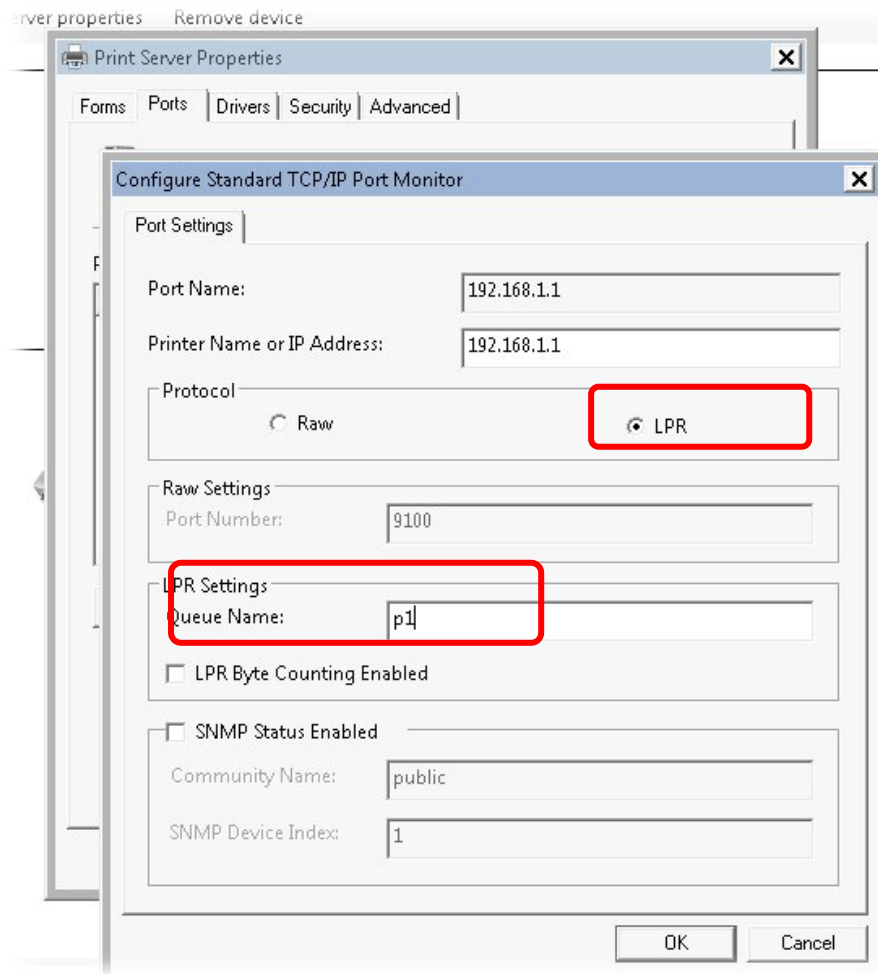
12. The new printer has been added and displayed under **Printers and Faxes**. Click the new printer icon and click **Printer server properties**.



13. Edit the property of the new printer you have added by clicking **Configure Port**.



14. 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.



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

Note 1: Some printers with the fax/scanning or other additional functions are not supported.

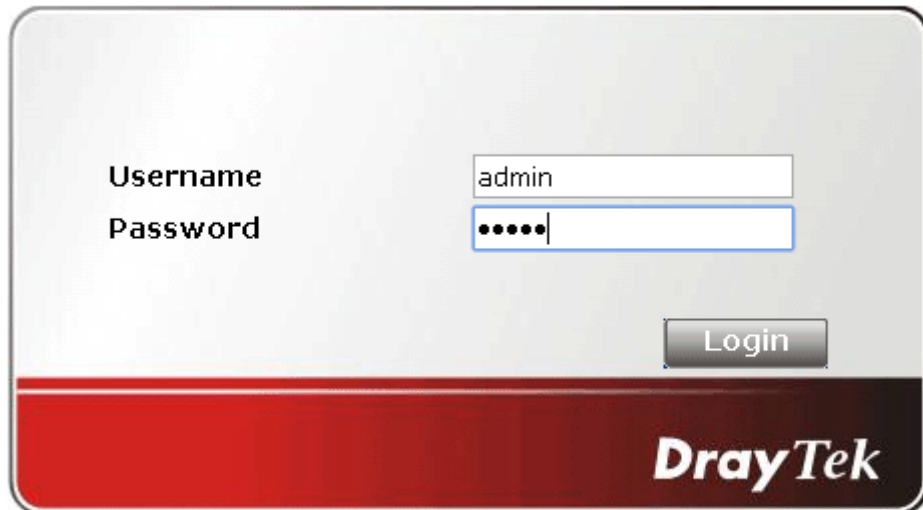
Note 2: Vigor router supports printing request from computers via the LAN port but not WAN port.

1.5 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.



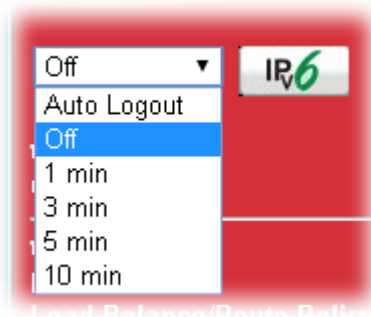
Copyright © 2016 DrayTek Corp. All Rights Reserved.

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.

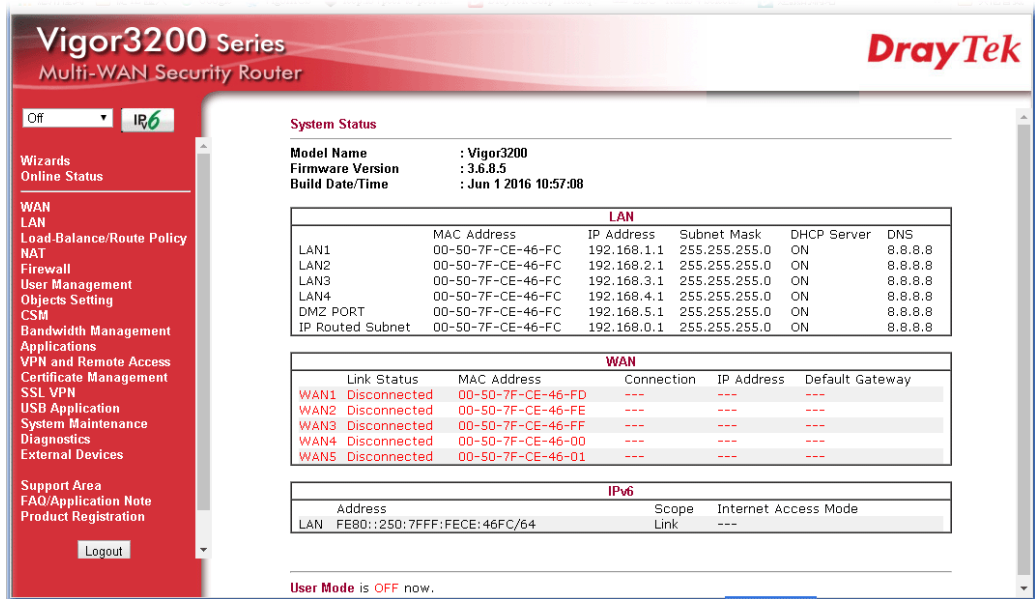
4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



1.6 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.



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

- Go to **System Maintenance** page and choose **Administrator Password**.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="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.

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

Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
Group	<input type="text" value="---"/> ▼
<input type="button" value="Login"/>	
Copyright©, DrayTek Corp. All Rights Reserved. DrayTek	

1.7 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						System Uptime: 4days 23:29:14
IPv4			IPv6			
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 8.8.4.4		
IP Address	TX Packets	RX Packets				
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 Connection				System Uptime: 4days 23:32:21
IPv4		IPv6		
LAN Status				
IP Address				
FE80::250:7FFF: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	Gateway IP			
---	---			

Detailed explanation is shown below:

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

Detailed explanation (for IPv6) is shown below:

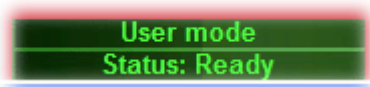
Item	Description
LAN Status	<p>IP Address- Displays the IPv6 address of the LAN interface..</p> <p>TX Packets-Displays the total transmitted packets at the LAN interface.</p> <p>RX Packets-Displays the total received packets at the LAN interface.</p> <p>TX Bytes - Displays the total transmitted octets at the LAN</p>

Item	Description
	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.

1.8 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.

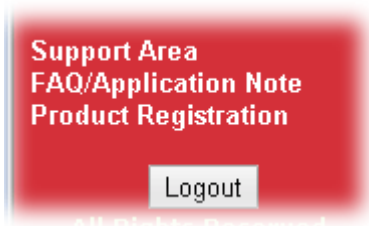


Ready indicates the system is ready for you to input settings.

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

1.9 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.

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

2

Quick Setup

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 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 **Wizards>>Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

Quick Start Wizard

Enter login password

Please enter an alpha-numeric string as your **Password** (Max 23 characters).

Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="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

WAN Interface

WAN Interface:	WAN5
Display Name:	
Physical Mode:	
Physical Type:	Auto negotiation

< Back Next > Finish Cancel

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.

2.1.1 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.

2.1.1.1 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
- PPTP
- L2TP
- Static IP
- DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

PPPoE Client Mode

WAN 1
Enter the user name and password provided by your ISP.

Service Name (Optional)	<input type="text"/>
Username	<input type="text" value="84005755@hinet.net"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

Available settings are explained as follows:

Item	Description
Service Name (Optional)	Enter the description of the specific network service.
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.

Quick Start Wizard

Please confirm your settings:

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

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

- Now, you can enjoy surfing on the Internet.

2.1.1.2 PPTP/L2TP

- 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
 PPTP
 L2TP
 Static IP
 DHCP

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

Quick Start Wizard

PPTP Client Mode

WAN 1
Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.

Username

Password

Confirm Password

WAN IP Configuration

Obtain an IP address automatically
 Specify an IP address

IP Address

Subnet Mask

Gateway

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	<p>Obtain an IP address automatically – the router will get an IP address automatically from DHCP server.</p> <p>Specify an IP address – you have to type relational settings manually.</p> <p>IP Address - Type the IP address.</p> <p>Subnet Mask –Type the subnet mask.</p> <p>Gateway – Type the IP address of the gateway.</p>
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.

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

Quick Start Wizard

Please confirm your settings:

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

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

- Now, you can enjoy surfing on the Internet.

2.1.1.3 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.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 L2TP
 Static IP
 DHCP

< Back Next > Finish Cancel

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

Quick Start Wizard

Static IP Client Mode

WAN 1
Enter the Static IP configuration provided by your ISP.

WAN IP
Subnet Mask
Gateway
Primary DNS
Secondary DNS (optional)

< Back Next > Finish Cancel

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.

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

Quick Start Wizard

Please confirm your settings:

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

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

- Now, you can enjoy surfing on the Internet.

2.1.1.4 DHCP

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
 PPTP
 L2TP
 Static IP
 DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 1
If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name (optional)
MAC (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.
---------------	---

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

Quick Start Wizard

Please confirm your settings:

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

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

- Now, you can enjoy surfing on the Internet.

2.1.2 For WAN5

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

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

Quick Start Wizard

WAN Interface

WAN Interface:	<input type="text" value="WAN5"/>
Display Name:	<input type="text"/>
Physical Mode:	USB

- Then, click **Next** for getting the following page.

Quick Start Wizard

Connect to Internet

WAN 5

Internet Access : 3G/4G USB Modem(PPP mode) ▼
3G/4G USB Modem(PPP mode)

3G/4G USB Modem(PPP mode)

SIM PIN code

Modem Initial String
(Default: AT&FE0V1X1&D2&C1S0=0)

APN Name

Available settings are explained as follows:

Item	Description
Internet Access	Choose one of the selections as the protocol of accessing the internet.
3G/4G USB Modem (PPP mode)	<p>SIM Pin code –Type PIN code of the SIM card that will be used to access Internet. The maximum length of the pin code you can set is 15 characters.</p> <p>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. The maximum length of the string you can set is 47 characters.</p> <p>APN Name – APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.</p>

- Then, click **Next** for viewing summary of such connection.

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN5
Physical Mode:	USB
Internet Access:	PPP

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back

Next >

Finish

Cancel

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

Quick Start Wizard Setup OK !!!

- Now, you can enjoy surfing on the Internet.

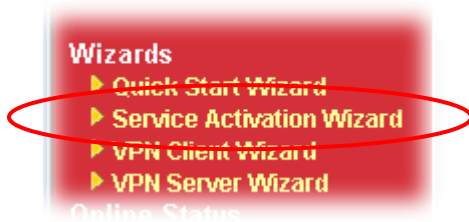
2.2 Service Activation Wizard

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 <http://myvigor.draytek.com>. 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 **Wizards>>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 license 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**.

Service Activation Wizard

Select the service type that you want to activate

This product provides 30 days of free trial, please choose the item(s) you want to use.

WCF service:

Web Content Filter (Commtouch) [License Agreement](#)

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

Activation Date :

I have read and accept the above Agreement. (Please check this box).

Note: The activation date is brought out by the server automatically and cannot be changed.

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

Service Activation Wizard

Please confirm your settings

Service Type : Trial version

Service Activated : Web Content Filter (Commtouch)

Please click **Back** to re-select service type you to activate.

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

Service Activation Wizard

Connection Succeeded!

Please check the following item(s) to enable services on your router.

Enable Web Content Filter

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**.

- 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.

Service Activation Wizard

Server Enabled!

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	2010-11-17	2010-12-18	Commtouch

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

Copyright © DrayTek Corp. All Rights Reserved.

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**.

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 license key

Service Activation Wizard

Select the service type that you want to activate

Please choose the item you want to use.

WCF service:

Web Content Filter (Commtouch) [License Agreement](#)
Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.

Enter your License key: Activation Date : [select](#)

I have read and accept the above Agreement. (Please check this box).

Note: The activation date is brought out by the server automatically and cannot be changed.

2.3 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.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environment

LAN-to-LAN VPN Client Mode Selection:

Please choose a LAN-to-LAN Profile:

Note: For a typical LAN-to-LAN tunnel, please select Route Mode.
 If the remote network is expecting only a single client or ip and is not configured to route the subnet and then select NAT mode.
 If in doubt then select Route Mode

Available settings are explained as follows:

Item	Description
LAN-to-LAN Client Mode Selection	Choose the client mode. Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode. <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> Route Mode ▾ Route Mode NAT Mode </div>
Please choose a LAN-to-LAN Profile	There are 32 VPN profiles for users to set.

[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	???
15	x	???
16	x	???
17	x	???
18	x	???
19	x	???
20	x	???
21	x	???
22	x	???
23	x	???
24	x	???
25	x	???
26	x	???
27	x	???
28	x	???
29	x	???

- When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

VPN Connection Setting

Security ranking (1 is the highest; 5 is the lowest)	Throughput ranking (1 is the highest; 5 is the lowest)
1. L2TP over IPSec	1. PPTP (None Encryption)
2. IPSec	2. L2TP
3. PPTP (Encryption)	3. IPSec
4. L2TP	4. L2TP over IPSec
5. PPTP (None Encryption)	5. PPTP (Encryption)

Select VPN Type:

- PPTP (None Encryption)
- PPTP (Encryption)
- IPSec
- L2TP
- L2TP over IPSec (Nice to Have)
- L2TP over IPSec (Must)

< Back Next > Finish Cancel

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

- When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP None Encryption Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	●●●●●●●●
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

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

VPN and Remote Access >> VPN Client Wizard

VPN Client IPSec Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- 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
<input type="checkbox"/> 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

VPN Client L2TP over IPSec (Nice to Have) Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

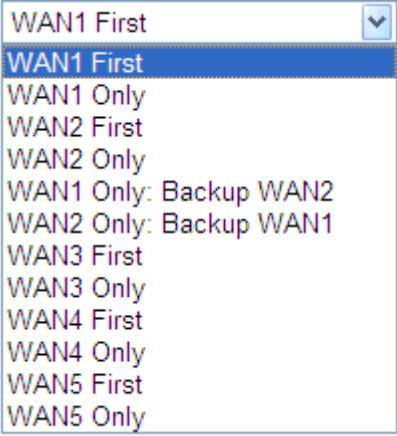
- When you choose **L2TP over IPSec (Must)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Must) Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. draytek.com or 123.45.67.89)	
IKE Authentication Method	
<input checked="" type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	DES without Authentication
<input type="radio"/> High (ESP)	
Username	???
Password	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for such profile. The length of the file is limited to 10 characters.
VPN Dial-Out Through	<p>Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.</p>  <p>WAN1 First / WAN2 First / WAN3 First / WAN4 First / 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.</p>

	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key- Confirm the pre-shared key.</p>
Digital Signature (X.509)	<p>Click Digital Signature to invoke this function.</p> <p>Peer ID – Choose the peer ID selection from the drop down list.</p> <p>Local ID – Choose Alternative Subject Name First or Subject Name First.</p> <p>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.</p>
IPSec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>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.</p>
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

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

VPN and Remote Access >> VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index: 27
 Profile Name: test
 VPN Connection Type: PPTP (None Encryption)
 VPN Dial-Out Through: WAN1 First
 Always on: No
 Server IP/Host Name: 192.168.1.87
 Remote Network IP: 172.16.3.99
 Remote Network Mask: 255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Client 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 VPN and Remote 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 VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

2.4 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

[VPN and Remote Access >> VPN Server Wizard](#)

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 ▾

< Back
Next >
Finish
Cancel

Available settings are explained as follows:

Item	Description
VPN Server Mode Selection	<p>Choose the direction for the VPN server.</p> <p>Site to Site VPN – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> <p>Site to Site VPN (LAN-to-LAN) ▾</p> <p style="background-color: #e0e0e0;">Site to Site VPN (LAN-to-LAN)</p> <p>Remote Dial-in User (Teleworker)</p> </div>
Please choose a LAN-to-LAN Profile	<p>This item is available when you choose Site to Site VPN (LAN-to-LAN) as VPN server mode. There are 32 VPN profiles for users to set.</p>

Item	Description																																																																																										
	<table border="1"> <thead> <tr> <th data-bbox="679 248 783 271">[Index]</th> <th data-bbox="783 248 895 271">[Status]</th> <th data-bbox="895 248 1054 271">[Name]</th> </tr> </thead> <tbody> <tr><td>1</td><td>x</td><td>???</td></tr> <tr><td>2</td><td>x</td><td>???</td></tr> <tr style="background-color: #0000FF; color: white;"><td>3</td><td>x</td><td>???</td></tr> <tr><td>4</td><td>x</td><td>???</td></tr> <tr><td>5</td><td>x</td><td>???</td></tr> <tr><td>6</td><td>x</td><td>???</td></tr> <tr><td>7</td><td>x</td><td>???</td></tr> <tr><td>8</td><td>x</td><td>???</td></tr> <tr><td>9</td><td>x</td><td>???</td></tr> <tr><td>10</td><td>x</td><td>???</td></tr> <tr><td>11</td><td>x</td><td>???</td></tr> <tr><td>12</td><td>x</td><td>???</td></tr> <tr><td>13</td><td>x</td><td>???</td></tr> <tr><td>14</td><td>x</td><td>???</td></tr> <tr><td>15</td><td>x</td><td>???</td></tr> <tr><td>16</td><td>x</td><td>???</td></tr> <tr><td>17</td><td>x</td><td>???</td></tr> <tr><td>18</td><td>x</td><td>???</td></tr> <tr><td>19</td><td>x</td><td>???</td></tr> <tr><td>20</td><td>x</td><td>???</td></tr> <tr><td>21</td><td>x</td><td>???</td></tr> <tr><td>22</td><td>x</td><td>???</td></tr> <tr><td>23</td><td>x</td><td>???</td></tr> <tr><td>24</td><td>x</td><td>???</td></tr> <tr><td>25</td><td>x</td><td>???</td></tr> <tr><td>26</td><td>x</td><td>???</td></tr> <tr><td>27</td><td>x</td><td>???</td></tr> <tr><td>28</td><td>x</td><td>???</td></tr> <tr><td>29</td><td>x</td><td>???</td></tr> </tbody> </table>	[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	???	15	x	???	16	x	???	17	x	???	18	x	???	19	x	???	20	x	???	21	x	???	22	x	???	23	x	???	24	x	???	25	x	???	26	x	???	27	x	???	28	x	???	29	x	???
[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	???																																																																																									
15	x	???																																																																																									
16	x	???																																																																																									
17	x	???																																																																																									
18	x	???																																																																																									
19	x	???																																																																																									
20	x	???																																																																																									
21	x	???																																																																																									
22	x	???																																																																																									
23	x	???																																																																																									
24	x	???																																																																																									
25	x	???																																																																																									
26	x	???																																																																																									
27	x	???																																																																																									
28	x	???																																																																																									
29	x	???																																																																																									
<p>Please choose a Dial-in User Accounts</p>	<p>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.</p>																																																																																										
<p>Allowed Dial-in Type</p>	<p>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).</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> L2TP with IPsec Policy <div style="border: 1px solid black; padding: 2px; display: inline-block;"> None ▼ None Nice to Have Must </div> <p>Different Dial-in Type will lead to different configuration page.</p>																																																																																										

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:

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

PPTP / L2TP / L2TP over IPSec Authentication

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

Password

Authentication Type

IPSec / L2TP over IPSec Authentication

Pre-Shared Key

 Confirm Pre-Shared Key

Digital Signature (X.509)

 Peer ID

Peer IP/VPN Client IP

Peer ID

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

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

IPSec / L2TP over IPSec Authentication

Pre-Shared Key

Confirm Pre-Shared Key

Digital Signature (X.509)

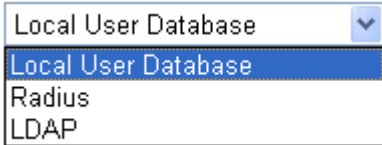
Peer ID

Peer IP/VPN Client IP

Peer ID

< Back Next > Finish Cancel

Available settings are explained as follows:

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. 
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 Certificate Management >> Local Certificate . 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

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Server 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 VPN and Remote 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 VPN and Remote 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.

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 **Wizards>>Wireless Wizard**.

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

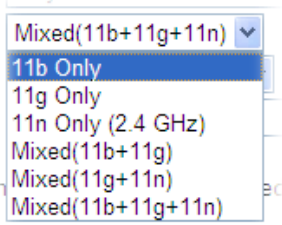
Wireless Wizard

Host AP Configuration

Name:	<input type="text" value="DrayTek"/>
Mode:	<input type="button" value="Mixed(11b+11g+11n)"/>
Channel:	<input type="button" value="Channel 6, 2437MHz"/>
Password:	<input type="text"/>

Note:The host AP 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.

- 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.

Wireless Wizard

Guest AP Configuration

Enable
 Disable

Name:

Password:

Rate Control: Enable Upload kbps Download kbps

Note:The configured guest AP will not be able to access the LAN network,VPN connections, or communicate with wireless devices connecting to the router's other APs.This AP interface shall be used for Internet access only.

Available settings are explained as follows:

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.

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

Wireless Wizard

Configuration Summary

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

5. Click **Finish** to complete the wireless settings configuration.

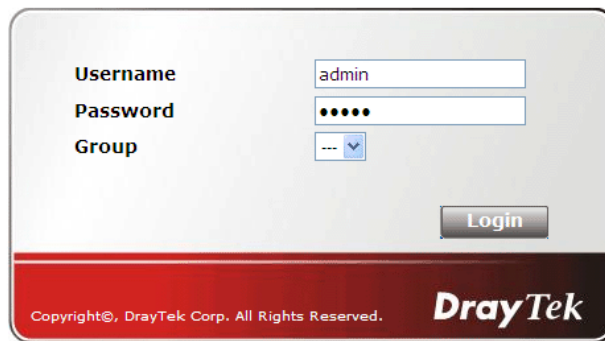
Wireless Wizard

Wireless Wizard Setup OK!

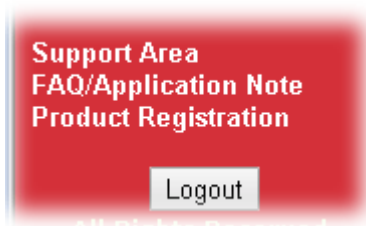
2.6 Registering Vigor Router

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.

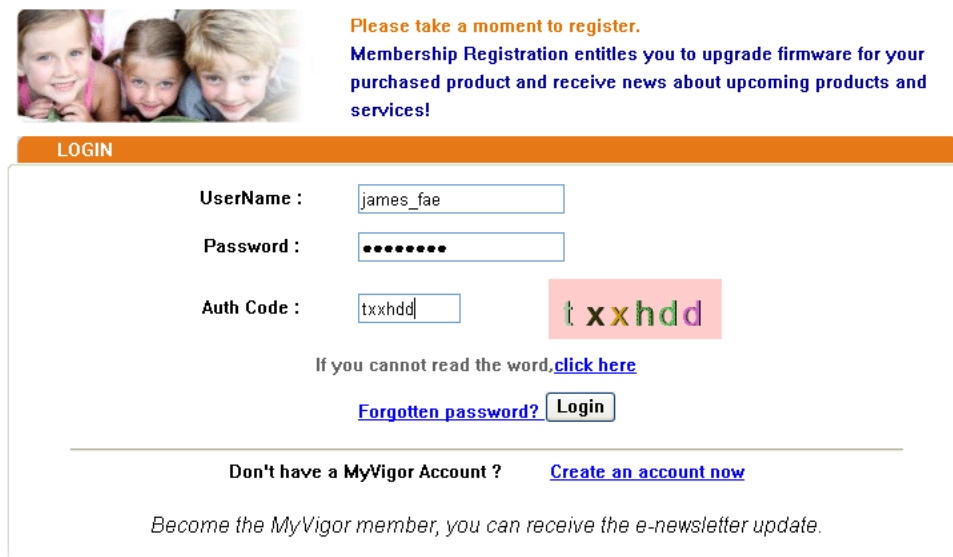
1. Please login the web configuration interface of Vigor router by typing “**admin/admin**” as User Name / Password.



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**.



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

The screenshot shows the DrayTek MyVigor website. The top navigation bar includes the DrayTek logo and a search field. A left sidebar contains menu items: Home, About Us, Product, My Information, VigorACS SI, Vigor Series, Management, Product Registration (highlighted with a red box), and Customer Survey. The main content area is titled 'My Information' and displays user details for 'james_fae', including last and current login times and IP addresses. Below this is a 'Your Device List' section with a table and pagination controls (RowNo: 5, PageNo: 1, and an Add button highlighted with a red box).

My Information

Welcome, **james_fae**
 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

RowNo : 5 PageNo : 1 **Add**

Your Device List

Serial Number / Host ID	Device Name	Model	Note
104001703857	Vigor2710	Vigor2710	-
200807100001	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.

- 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**.

DrayTek MyVigor

Home Search GO

My Product Search for this site GO

Registration Device

Serial number : 2011082214320301

Nickname : * vigor3200

Registration Date : 08-24-2011

Usage : - Select -

Product Rating : - Select - [Your opinion so far]

No. of Employees : - Select - [In total within your company]

Supplier : [] [Where you bought it from]

Date of Purchase : [] [mm-dd-yyyy]

Internet Connection : *

Cable ADSL VDSL Fiber

3G WIMAX LTE

Cancel Submit

- 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

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

DrayTek MyVigor

Home Search GO

My Information

Welcome, draytekfac

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

RowNo : 5 PageNo : 2

Your Device List

Serial Number / Host ID	Device Name	Model	Note
20100707144801	Vigor3300V	Vigor3300	-
20100708105301	Vigor2820	Vigor2820	-
20101005104801	Vigor2710vn	Vigor2710	-
2010121707335201	Vigor2380	Vigor2830	-
2011082214320301	Vigor3200	Vigor3200	-

This page is left blank.

3

Tutorials and Applications

3.1 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:

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.

[Applications >> Active Directory /LDAP](#)

Active Directory /LDAP | [Set to Factory Default](#)

General Setup | **Active Directory / LDAP Profiles**

Enable

Bind Type: Regular Mode

Server IP Address: 172.16.2.8

Destination Port: 389

Regular DN: uid=vpntest,ou=vpnusers,dc=ms,dc=drayte

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. 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

Index No. 1

Name	<input type="text" value="rd1"/>	
Common Name Identifier	<input type="text" value="uid"/>	
Base Distinguished Name	<input type="text" value="ou=People,dc=ms,dc=draytek,dc=com"/>	
Group Distinguished Name	<input type="text" value="cn=rd1,ou=Group,dc=ms,dc=draytek,dc=c"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

Applications >> Active Directory /LDAP>>Server Profiles

Index No. 2

Name	<input type="text" value="shrd"/>	
Common Name Identifier	<input type="text" value="uid"/>	
Base Distinguished Name	<input type="text" value="ou=People,dc=ms,dc=draytek,dc=com"/>	
Group Distinguished Name	<input "="" type="text" value="cn=shrd,ou=Group,dc=ms,dc=draytek,dc="/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

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

General Setup

Mode:	<input type="button" value="User-Based"/>
Web Authentication:	<input type="button" value="HTTPS"/>
Notice :	
<ol style="list-style-type: none"> 1. User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode. 2. Users match the above lists will not be required for authentication. The firewall rules policy will still valid. 3. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid. 	
Landing Page (Max 255 characters)	Preview Set to Factory Default
<pre><body stats=1><script language='javascript'> window.location='http://www.draytek.com'</script></body></pre>	

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

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption (MPPE): Optional MPPE

Mutual Authentication (PAP): Yes No

Username:

Password:

IP Address Assignment for Dial-In Users (When DHCP Disable set)

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

LDAP Server Profiles for PPP Authentication

<input checked="" type="checkbox"/>	rd1
<input checked="" type="checkbox"/>	shrd

OK

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

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

Below shows the configuration steps:

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.

[Applications >> Active Directory /LDAP](#)

Active Directory /LDAP | [Set to Factory Default](#)

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

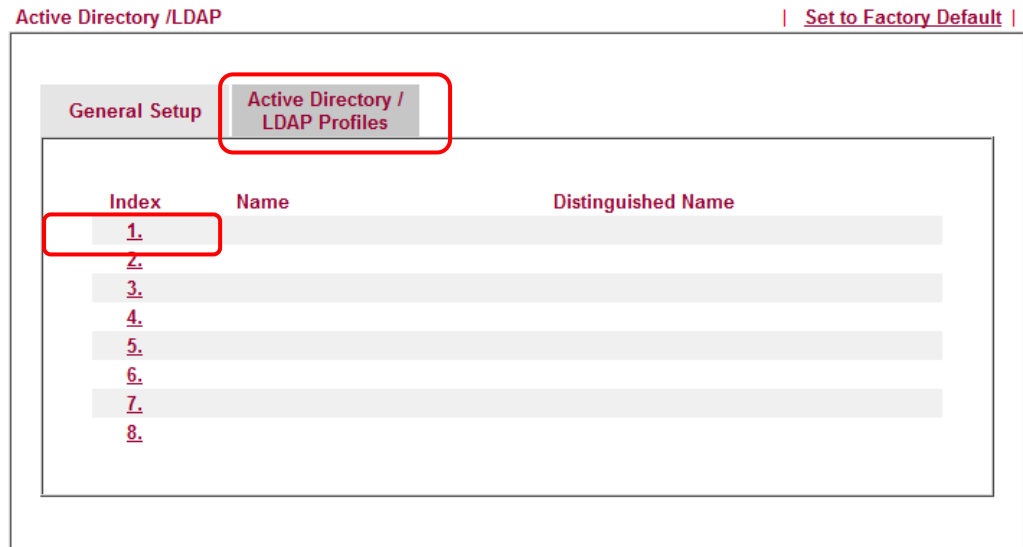
There are three types of bind type supported:

- **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**.

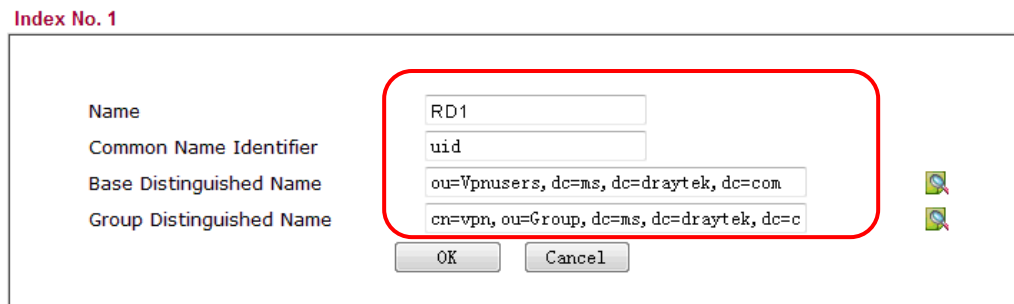
- Click the **Active Directory /LDAP** tab to open the profile web page.

Applications >> Active Directory /LDAP




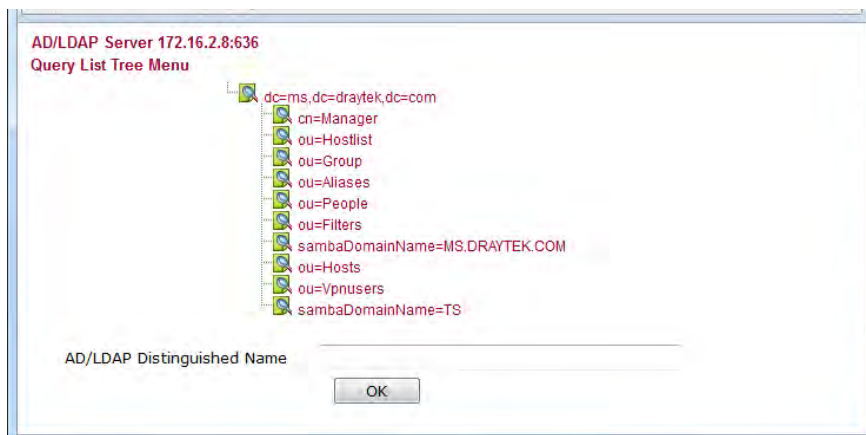
- Click any one of the index number link to configure the proper **Base Distinguished Name** and **Group Distinguished Name**.


Applications >> Active Directory /LDAP>> Server Profiles

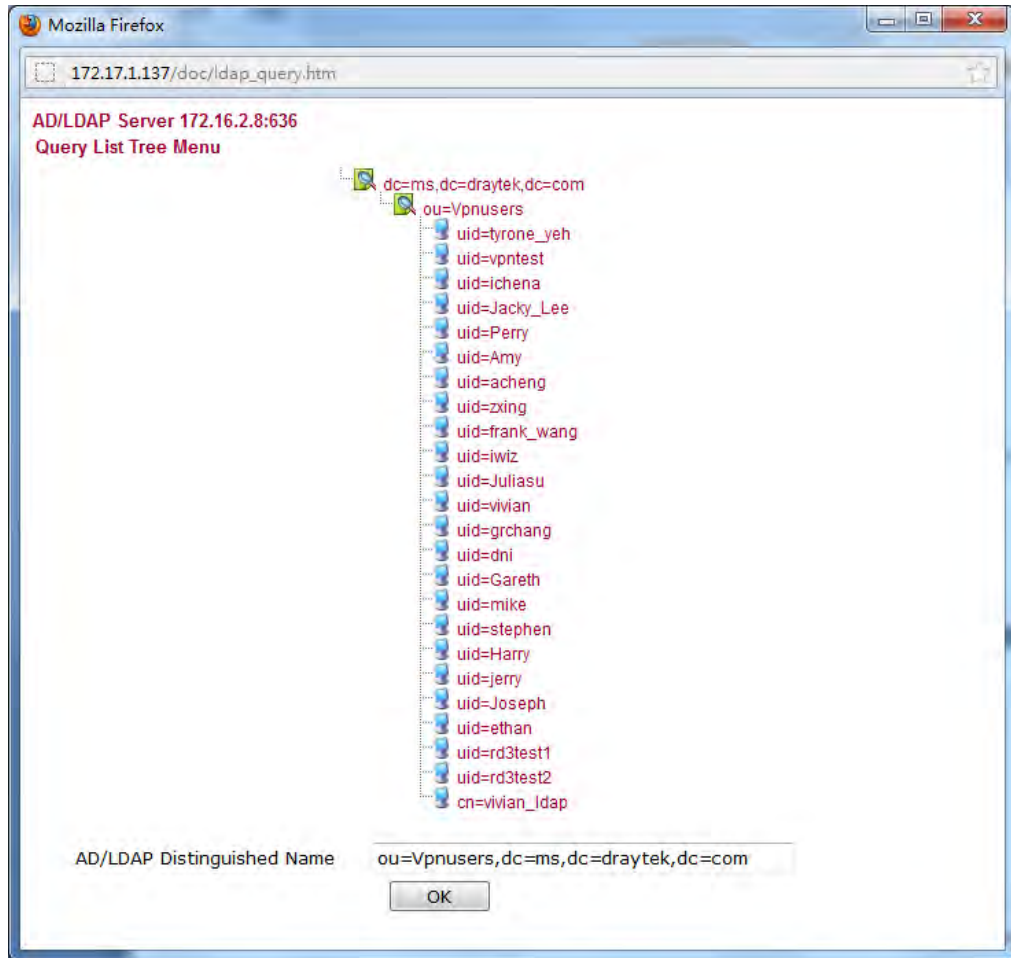




Suppose that there are several departments in your company, e.g., RD1 and RD2. Here, create a profile for RD1 first.

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



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



In addition,  means this item is an organization;  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](#)

Active Directory /LDAP [Set to Factory Default](#)

General Setup | **Active Directory / LDAP Profiles**

Index	Name	Distinguished Name
1.	RD1	cn=vpn1,ou=Group,dc=ms,dc=draytek,dc=com
2.		
3.		
4.		
5.		
6.		
7.		
8.		

- 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**.

[VPN and Remote Access >> PPP General Setup](#)

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: PAP Only</p> <p>Dial-In PPP Encryption(MPPE): Optional MPPE</p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <p>Assigned IP start</p> <table border="1"> <tr><td>LAN 1</td><td>192.168.1.200</td></tr> <tr><td>LAN 2</td><td>192.168.2.200</td></tr> <tr><td>LAN 3</td><td>192.168.3.200</td></tr> <tr><td>LAN 4</td><td>192.168.4.200</td></tr> </table>	LAN 1	192.168.1.200	LAN 2	192.168.2.200	LAN 3	192.168.3.200	LAN 4	192.168.4.200	<p>LDAP Server Profiles for PPP Authentication</p> <p><input checked="" type="checkbox"/> LDAP</p>
LAN 1	192.168.1.200								
LAN 2	192.168.2.200								
LAN 3	192.168.3.200								
LAN 4	192.168.4.200								

OK

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.

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

[Applications >> Active Directory /LDAP](#)

Active Directory /LDAP [Set to Factory Default](#)

General Setup	Active Directory / LDAP Profiles
---------------	---

Index	Name	Distinguished Name
1.	RD1	cn=vpn1,ou=Group,dc=ms,dc=draytek,dc=com
2.	RD2	cn=vpn2,ou=Group,dc=ms,dc=draytek,dc=com
3.		
4.		
5.		
6.		
7.		
8.		

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

SSL VPN >> SSL Application

SSL Applications Profiles: [Set to Factory Default](#)

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

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

SSL VPN >> SSL Web Proxy

SSL Web Proxy Servers Profiles: [Set to Factory Default](#)

Index	Name	URL	Active
1.	google	http://www.google.com	v
2.	baidu	http://baidu.com	v
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

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

SSL VPN >> User Group

SSL User Group Profiles: [Set to Factory Default](#)

Index	Name	Status
1.	g1	v
2.	g2	v
3.		x
4.		x
5.		x
6.		x
7.		x
8.		x
9.		x
10.		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

Access Authority

<input checked="" type="checkbox"/> SSL Web Proxy	<input checked="" type="checkbox"/> SSL Application
<input checked="" type="checkbox"/> google	<input checked="" type="checkbox"/> PC1
<input type="checkbox"/> baidu	<input type="checkbox"/> PC2

Authentication Methods

<input checked="" type="checkbox"/> Local User DataBase	
Available User Accounts	Selected User Accounts
3-frank 4-ada 5-mike 6-monica 7-pete	1-test 2-caesar
<input type="button" value=">>"/> <input type="button" value="<<"/>	
<input checked="" type="checkbox"/> RADIUS	
<input checked="" type="checkbox"/> LDAP / Actice Directory	
<input checked="" type="checkbox"/> RD1	
<input type="checkbox"/> RD2	

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

SSL VPN >> User Group

Index No. 2

Enable

Group Name

Access Authority

<input checked="" type="checkbox"/> SSL Web Proxy	<input checked="" type="checkbox"/> SSL Application
<input type="checkbox"/> google	<input type="checkbox"/> PC1
<input checked="" type="checkbox"/> baidu	<input checked="" type="checkbox"/> PC2

Authentication Methods

<input checked="" type="checkbox"/> Local User DataBase	
Available User Accounts	Selected User Accounts
1-test 2-caesar 5-mike 6-monica 7-pete	3-frank 4-ada
<input type="button" value=">>"/> <input type="button" value="<<"/>	
<input checked="" type="checkbox"/> RADIUS	
<input checked="" type="checkbox"/> LDAP / Actice Directory	
<input type="checkbox"/> RD1	
<input checked="" type="checkbox"/> RD2	

12. Once you've finished the configuration on Vigor router, try to login SSL portal with <https://<IPAddress>/> .
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 *g1*).

Username: caesar
Password: ●●●●●●
Group: g1

Login

Copyright©, DrayTek Corp. All Rights Reserved. **DrayTek**

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.

DrayTek
Powered SSL VPN

Home | **SSL Web Proxy** | SSL Tunnel | SSL Application [[logout](#)]

INFO

test (172.17.1.42)
Welcome to the DrayTek SSL VPN!

Main Page:

You have successfully logged in!
You are granted the following privileges:

- [SSL Web Proxy](#)
- [SSL Tunnel](#)
- [SSL Application](#)

Copyright © 2008, DrayTek Corp. All Rights Reserved.

INFO

- **SSL Web Proxy**
 - "Green" means the profile is ready for access.
 - "Black" means the profile needs to be activated first.

Home **SSL Web Proxy** SSL Tunnel SSL Application [[logout](#)]

Access methods for SSL Web Proxy:

I. SSL

- [google](#)

Copyright © 2008, DrayTek Corp. All Rights Reserved.

INFO

- **SSL Application**
 - Click "Connect" to establish an SSL Application!

Home SSL Web Proxy SSL Tunnel **SSL Application** [[logout](#)]

Use SSL Application:

I. VNC

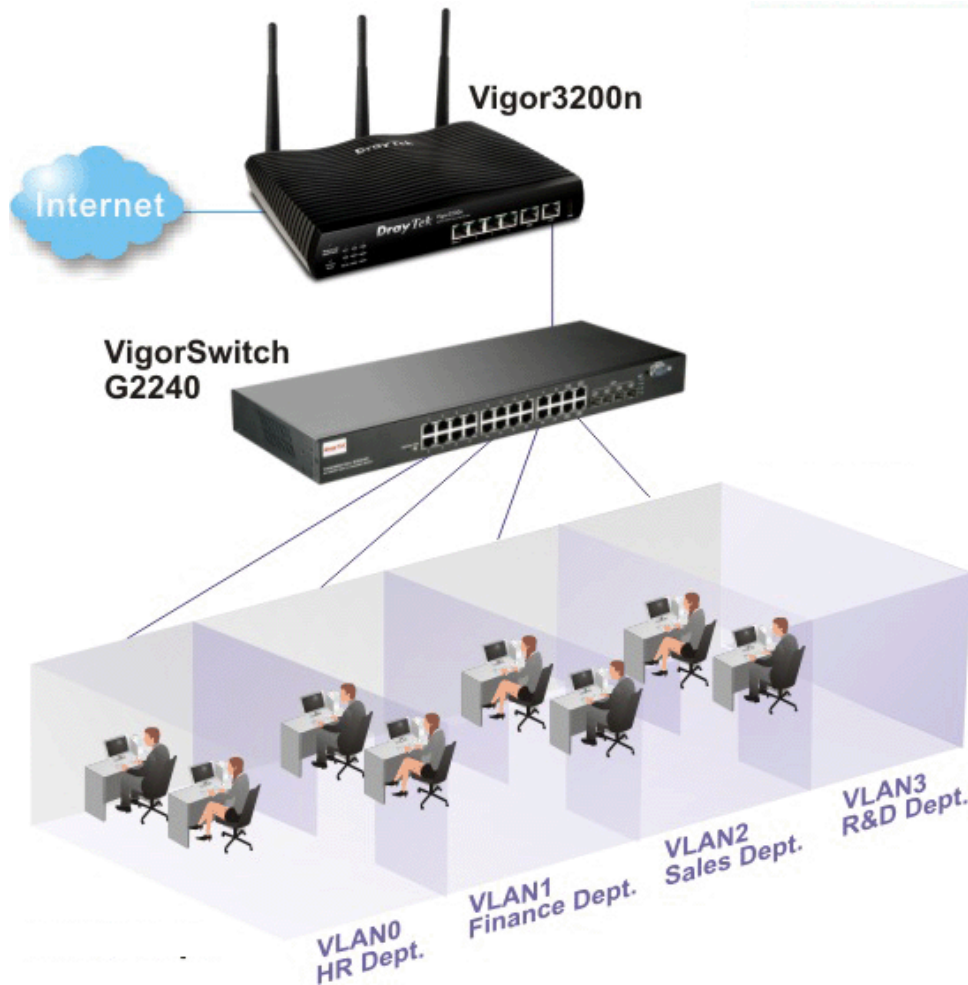
- PC1 192.168.1.10:5900, 100% [Connect](#)

Copyright © 2008, DrayTek Corp. All Rights Reserved.

3.3 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**.

LAN >> VLAN Configuration

VLAN Configuration

Enable

	VLAN Tag			Wireless LAN					Subnet
	Enable	VID	Priority	LAN Port	SSID1	SSID2	SSID3	SSID4	
VLAN0	<input type="checkbox"/>	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 4
VLAN1	<input checked="" type="checkbox"/>	10	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1
VLAN2	<input checked="" type="checkbox"/>	20	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 2
VLAN3	<input checked="" type="checkbox"/>	30	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3
VLAN4	<input checked="" type="checkbox"/>	40	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 4
VLAN5	<input type="checkbox"/>	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1
VLAN6	<input type="checkbox"/>	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1
VLAN7	<input type="checkbox"/>	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1

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.

OK Clear Cancel

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page
LAN 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page
LAN 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page
DMZ	V	V	192.168.5.1	Details Page
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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.

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration		DHCP Server Configuration	
For NAT Usage		<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
IP Address	<input type="text" value="192.168.1.1"/>	Relay Agent: <input type="radio"/> Enable <input type="radio"/> Disable	
Subnet Mask	<input type="text" value="255.255.255.0"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
RIP Protocol Control	<input type="text" value="Disable"/> ▼	IP Pool Counts	<input type="text" value="50"/>
		Gateway IP Address	<input type="text" value="192.168.1.1"/>
		DHCP Server IP Address for Relay Agent	<input type="text"/>
		DNS Server IP Address	
		<input type="checkbox"/> Force DNS manual setting	
		Primary IP Address	<input type="text"/>
		Secondary IP Address	<input type="text"/>

OK

- 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.

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ PORT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Configuration for VigorSwitch G2240

- Open **Vlan>>Tag-based Group**.
- Add four VID groups. In this case, we can explain it with Port 15, 16, 17, 18 and Trunk Port 23.

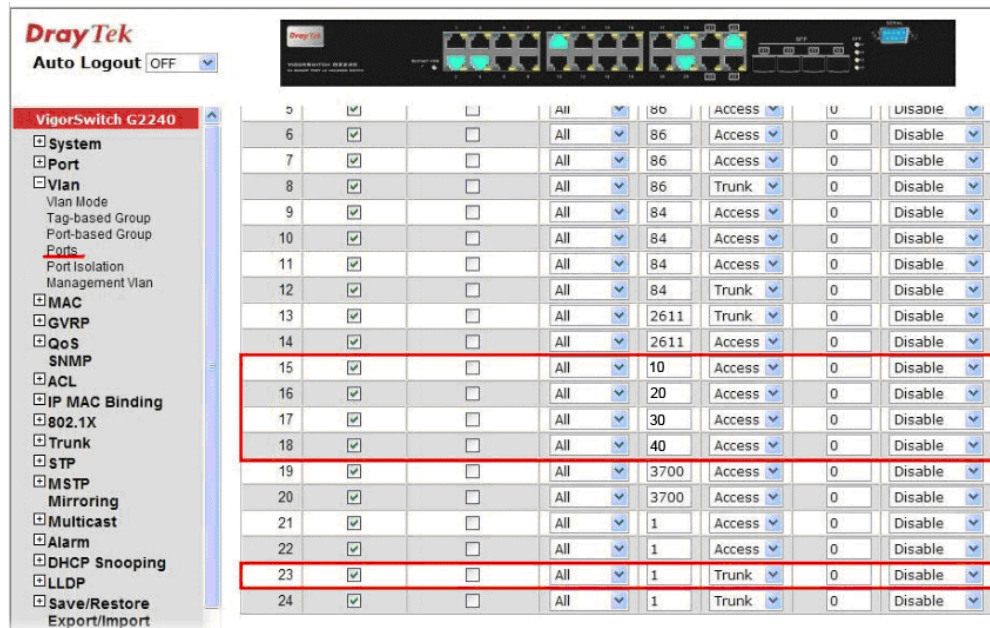
Def	VID	IGMP-A	P-VLAN	GVRP-P	Port Members																							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24					
1	10	Disable	Disable	Disable											15								23					
	20	Disable	Disable	Disable											16								23					
	30	Disable	Disable	Disable												17							23					
	40	Disable	Disable	Disable													18						23					

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

- 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.



- 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

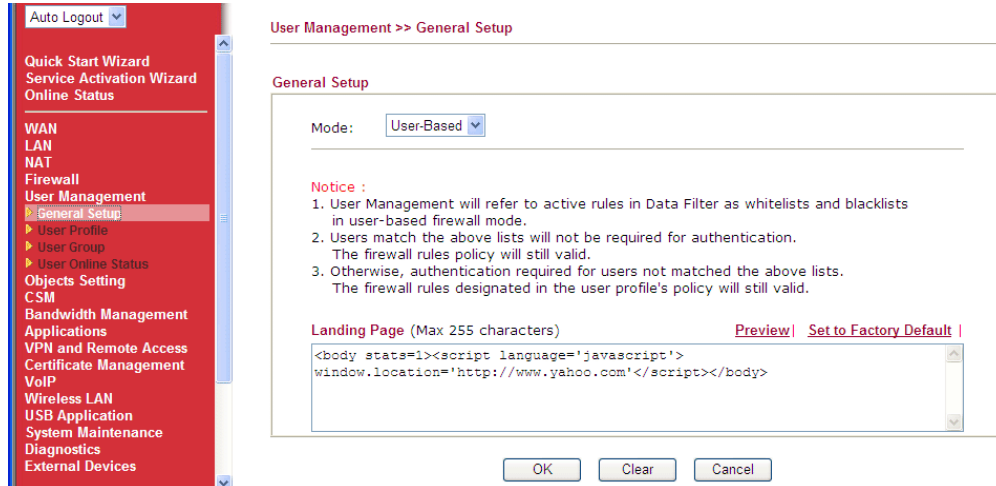
The equipment connecting to VigorSwitch Port 17 can get the IP address of 192.168.3.0/24

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

3.4 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 the settings.



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

User Management >> User Profile

User Profile Table				Set to Factory Default
Profile	Name	Profile	Name	
1.	admin	17.		
2.	System Reservation	18.		
3.		19.		
4.		20.		
5.		21.		
6.		22.		
7.		23.		
8.		24.		
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**.

User Management >>User Profile(Reserved)

Profile Index 3

Enable this account

User Name:

Password:

Confirm Password:

Idle Timeout: min(s) 0:Unlimited

Max User Login: 0:Unlimited

External Server Authentication:

Log:

Pop Browser Tracking Window:

Authentication: Web Alert Tool Telnet

Landing Page:

- 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**.

System Maintenance >> Login Page Greeting

Login Page Greeting

Enable

Login Page Title (31 char max.)

Welcome Message and Bulletin (Max 511 characters) [Preview](#) [Set to Factory Default](#)

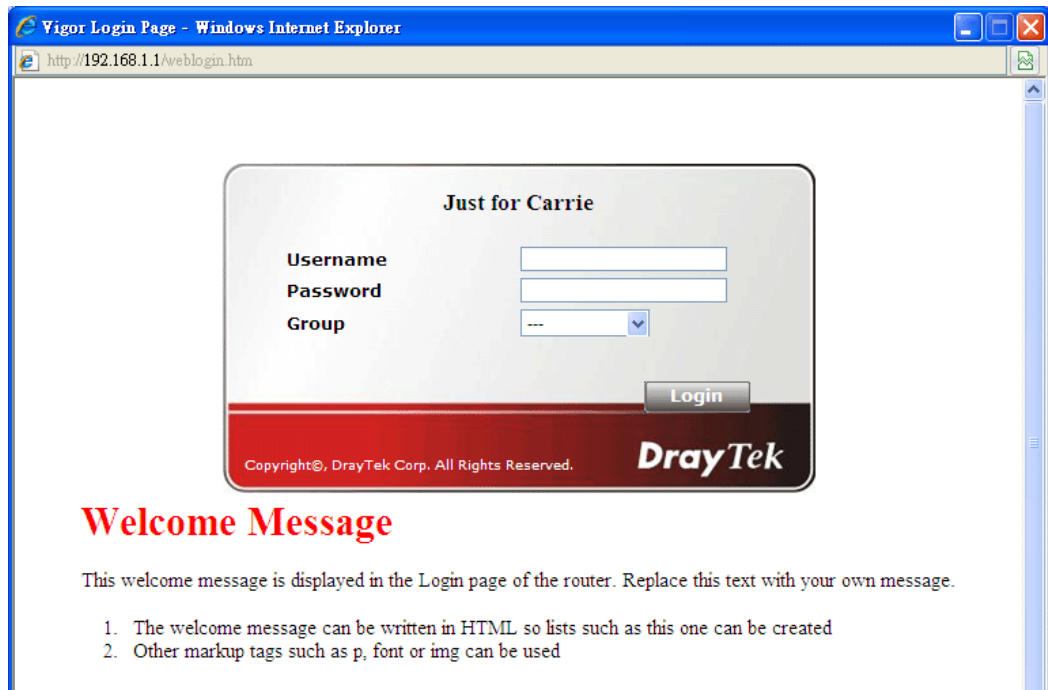
```
<h1><b><font color=red>Vigor</font></b></h1><p>Welcome to Draytek world. </p>
```

Examples of Welcome Message and Bulletin:

```
<h1><b><font color=red>Welcome Message</font></b></h1>
<p>Message</p>
```

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

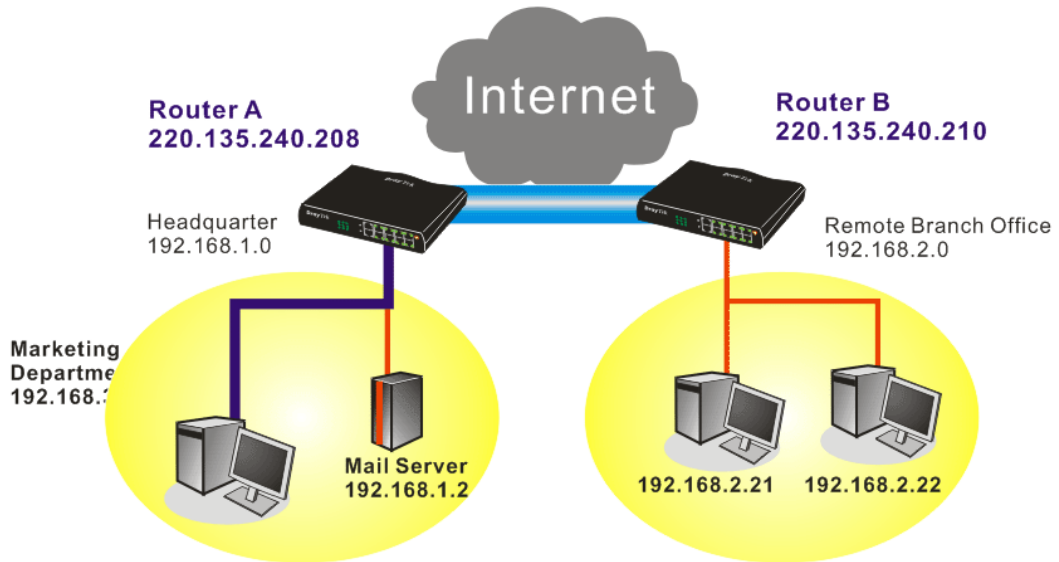
- Open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
- Try to access into the web user interface (e.g., 192.168.1.1) of Vigor router. Please note “*Just for Carrie*” is displayed as a heading on the login dialog box.



- 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**.

3.5 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**.

VPN and Remote Access >> PPP General Setup

PPP General Setup	
PPP/MP Protocol	
Dial-In PPP Authentication	PAP or CHAP
Dial-In PPP Encryption (MPPE)	Optional MPPE
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	<input type="text"/>
Password	<input type="text"/>
IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Assigned IP range	192.168.1.200

OK

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method	
Pre-Shared Key	<input type="password" value="•••••"/>
Confirm Pre-Shared Key	<input type="password" value="•••••"/>
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.
<input type="button" value="OK"/> <input type="button" value="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 <input type="text" value="Branch1"/>	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input type="text" value="WAN1 First"/>	Idle Timeout <input type="text" value="300"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP <input type="text"/>
<small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	

2. Dial Out Settings

- 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

<p>Type of Server I am calling</p> <p><input type="radio"/> PPTP</p> <p><input checked="" type="radio"/> IPSec Tunnel</p> <p><input type="radio"/> L2TP with IPSec Policy None</p> <p>Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)</p> <p><input type="text" value="220.135.240.210"/></p>	<p>Link Type 64k bps</p> <p>Username <input data-bbox="1189 510 1417 539" type="text" value="???"/></p> <p>Password <input data-bbox="1189 551 1417 580" type="text"/></p> <p>PPP Authentication PAP/CHAP</p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>IKE Authentication Method</p> <p><input checked="" type="radio"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1189 757 1417 786" type="text"/></p> <p><input type="radio"/> Digital Signature(X.509)</p> <p>None</p> <p>IPSec Security Method</p> <p><input checked="" type="radio"/> Medium(AH)</p> <p><input type="radio"/> High(ESP) DES without Authentication</p> <p><input type="button" value="Advanced"/></p> <p>Index(1-15) in Schedule Setup:</p> <p><input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p>
---	---

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

<p>Type of Server I am calling</p> <p><input checked="" type="radio"/> PPTP</p> <p><input type="radio"/> IPSec Tunnel</p> <p><input type="radio"/> L2TP with IPSec Policy None</p> <p>Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)</p> <p><input type="text" value="220.135.240.210"/></p>	<p>Link Type 64k bps</p> <p>Username <input data-bbox="1189 1413 1417 1442" type="text" value="draytek"/></p> <p>Password <input data-bbox="1189 1453 1417 1482" type="text" value="●●●●"/></p> <p>PPP Authentication PAP/CHAP</p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>IKE Authentication Method</p> <p><input checked="" type="radio"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1189 1655 1417 1684" type="text"/></p> <p><input type="radio"/> Digital Signature(X.509)</p> <p>None</p> <p>IPSec Security Method</p> <p><input checked="" type="radio"/> Medium(AH)</p> <p><input type="radio"/> High(ESP) DES without Authentication</p> <p><input type="button" value="Advanced"/></p> <p>Index(1-15) in Schedule Setup:</p> <p><input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p>
---	--

- 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

<p>Allowed Dial-In Type</p> <p><input type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPSec Tunnel</p> <p><input type="checkbox"/> L2TP with IPSec Policy None</p>	<p>Username <input data-bbox="1182 495 1414 524" type="text" value="???"/></p> <p>Password <input data-bbox="1182 539 1398 568" type="password"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><input checked="" type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP</p> <p><input data-bbox="400 752 628 781" type="text" value="220.135.240.210"/></p> <p>or Peer ID <input data-bbox="504 792 735 822" type="text"/></p>	<p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1182 707 1398 736" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p>
	<p>IPSec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>

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

<p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input type="checkbox"/> IPSec Tunnel</p> <p><input type="checkbox"/> L2TP with IPSec Policy None</p>	<p>Username <input data-bbox="1182 1167 1414 1196" type="text" value="draytek"/></p> <p>Password <input data-bbox="1182 1211 1398 1240" type="password" value="*****"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><input checked="" type="checkbox"/> Specify Remote VPN Gateway</p> <p>Peer VPN Server IP</p> <p><input data-bbox="400 1424 628 1453" type="text" value="220.135.240.210"/></p> <p>or Peer ID <input data-bbox="504 1464 735 1494" type="text"/></p>	<p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input data-bbox="1182 1379 1398 1408" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p>None</p>
	<p>IPSec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>

- 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.

Settings in Router B in the remote office:

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

VPN and Remote Access >> PPP General Setup

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method
Pre-Shared Key: [Masked]
Confirm Pre-Shared Key: [Masked]

IPSec Security Method
 Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

OK Cancel

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: Branch1
 Enable this profile

VPN Dial-Out Through: WAN1 First
Netbios Naming Packet: Pass Block
Multicast via VPN: Pass Block
(for some IGMP, IP-Camera, DHCP Relay..etc.)

Call Direction: Both Dial-Out Dial-in
 Always on
Idle Timeout: 300 second(s)
 Enable PING to keep alive
PING to the IP: [Empty]

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 <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

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 <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Link Type 64k bps Username draytek Password ●●●● PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

- 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 <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None		Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> 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 <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None		Username <input type="text" value="draytek"/> Password <input type="text" value="●●●●●●"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

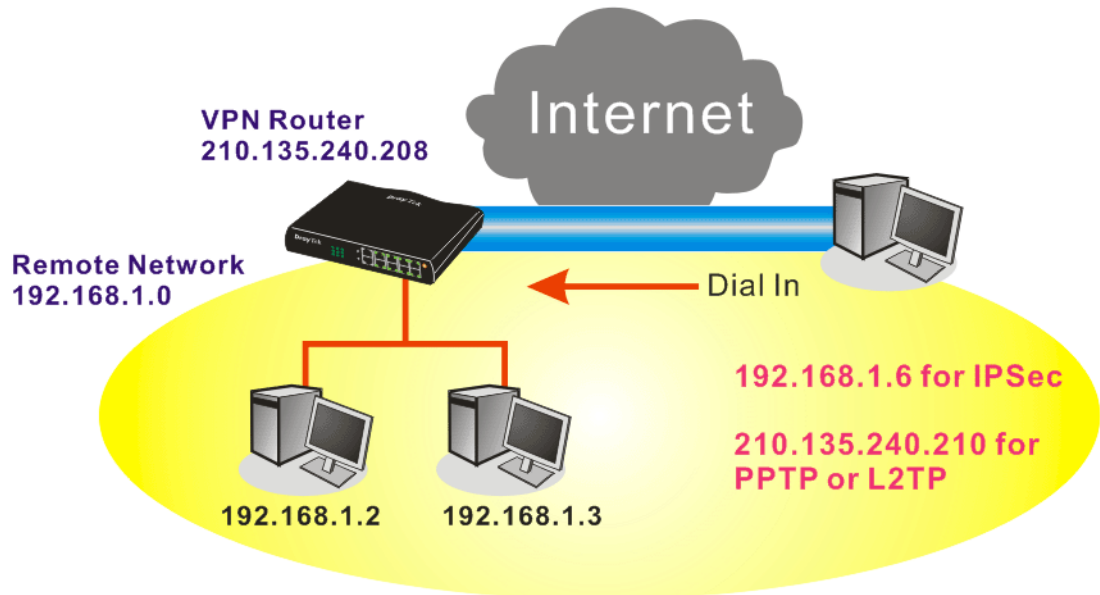
7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	<input type="text" value="Disable"/>
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	
Remote Network IP	<input type="text" value="192.168.1.0"/>	<input type="text" value="Route"/>	
Remote Network Mask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	
Local Network IP	<input type="text" value="192.168.1.1"/>		
Local Network Mask	<input type="text" value="255.255.255.0"/>		
<input type="button" value="More"/>			

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

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



Settings in VPN Router in the enterprise office:

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

VPN and Remote Access >> PPP General Setup

PPP General Setup	
PPP/MP Protocol	
Dial-In PPP Authentication	PAP or CHAP
Dial-In PPP Encryption (MPPE)	Optional MPPE
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	<input type="text"/>
Password	<input type="text"/>
IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Assigned IP range	192.168.1.200

OK

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 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	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and 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.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout 300 second(s)	Username ??? Password <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code Secret IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None
Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None <input type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number or Peer ID Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) Subnet LAN 1 <input type="checkbox"/> Assign Static IP Address 0.0.0.0

OK Clear Cancel

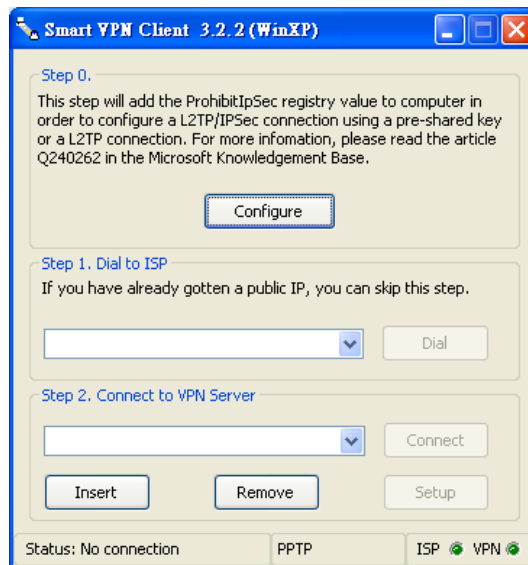
If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

Index No. 1

<p>User account and Authentication</p> <input type="checkbox"/> Enable this account Idle Timeout: <input type="text" value="300"/> second(s)		Username: <input type="text" value="???"/> Password: <input type="password"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code: <input type="text"/> Secret: <input type="password"/>
<p>Allowed Dial-In Type</p> <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy: <input type="text" value="None"/> <input type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number: <input type="text"/> or Peer ID: <input type="text"/> Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP, IP-Camera, DHCP Relay..etc.)		<p>IKE Authentication Method</p> <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key: <input type="password"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/>
<p>Subnet</p> <input type="text" value="LAN 1"/> <input type="checkbox"/> Assign Static IP Address <input type="text" value="0.0.0.0"/>		<p>IPSec Security Method</p> <input checked="" type="checkbox"/> Medium(All) High(ESP): <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional): <input type="text"/>

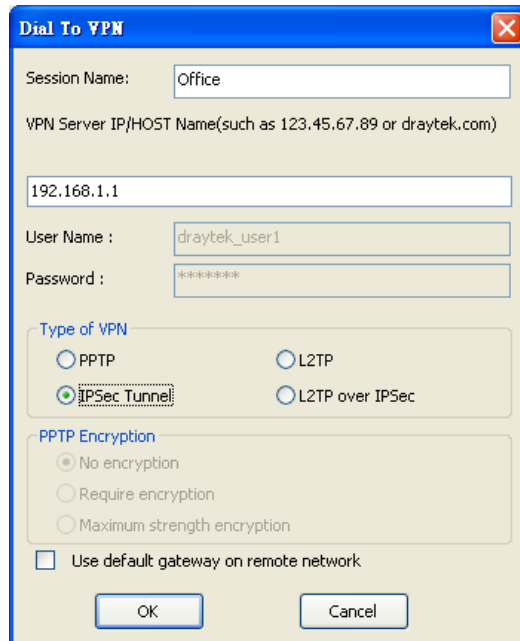
Settings in the remote host:

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.



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

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



Dial To VPN

Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

PPTP L2TP

IPSec Tunnel L2TP over IPSec

PPTP Encryption

No encryption

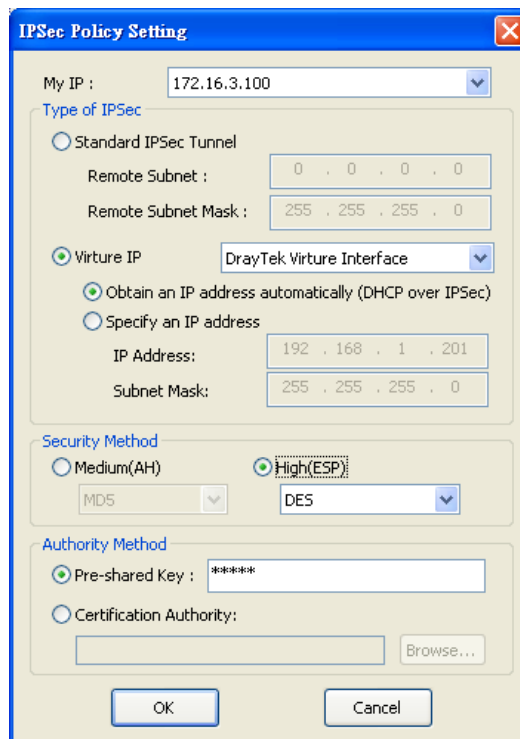
Require encryption

Maximum strength encryption

Use default gateway on remote network

OK 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 Setting

My IP : 172.16.3.100

Type of IPSec

Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

Virture IP DrayTek Virture Interface

Obtain an IP address automatically (DHCP over IPSec)

Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

Medium(AH) High(ESP)

MD5 DE5

Authority Method

Pre-shared Key : *****

Certification Authority: Browse...

OK 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 L2TP

IPsec Tunnel L2TP over IPsec

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Use default gateway on remote network

OK Cancel

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

3.7 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**.

Bandwidth Management >> Quality of Service

General Setup | [Set to Factory Default](#)

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	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 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 Inbound Bandwidth In

WAN Outbound Bandwidth Out

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

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

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

[Bandwidth Management >> Quality of Service](#)

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Inactive	Any	Any	ANY	undefined

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

[Bandwidth Management >> Quality of Service](#)

WAN1 General Setup

Enable the QoS Control

WAN Inbound Bandwidth Kbps
 WAN Outbound Bandwidth Kbps

Index	Class Name	Reserved bandwidth Ratio
Class 1	E-mail	<input type="text" value="25"/> %
Class 2		<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
Others		<input type="text" value="25"/> %

Enable UDP Bandwidth Control
 Outbound TCP ACK Prioritize

Limited_bandwidth Ratio %
[Online Statistics](#)

- 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](#)

Class Index #2

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Active	Any	Any	ANY	ANY

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

Bandwidth Management >> Quality of Service

General Setup

[Set to Factory Default](#)

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 Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

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

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

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control BOTH

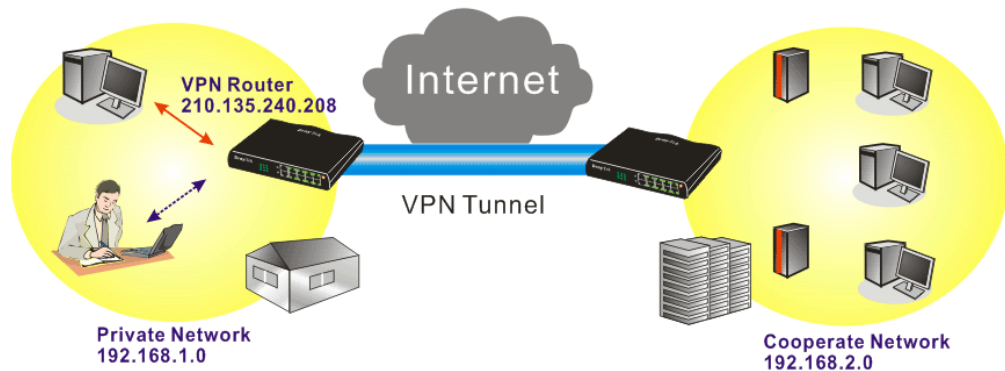
WAN Inbound Bandwidth	<input type="text" value="10000"/>	Kbps	
WAN Outbound Bandwidth	<input type="text" value="10000"/>	Kbps	

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	<input type="text" value="25"/> %
Class 2	HTTPS	<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %

Outbound TCP ACK Prioritize [Online Statistics](#)

- 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

Class Index #3

Name

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

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

Bandwidth Management >> Quality of Service

Rule Edit

ACT
 Hardware Acceleration

Local Address

Remote Address

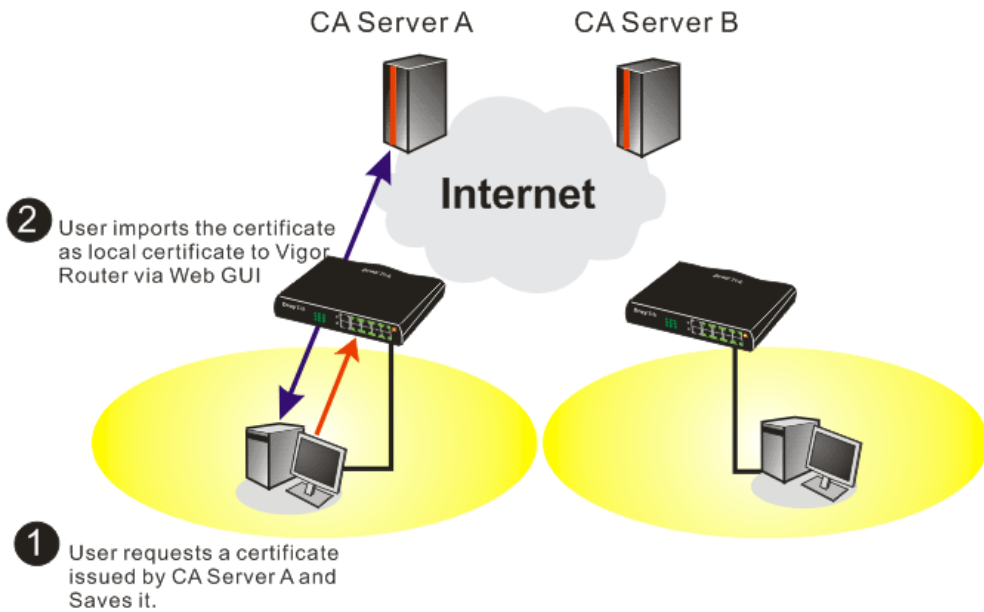
DiffServ CodePoint

Service Type

Note: Please choose/setup the **Service Type** first.

- 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**.

3.8 Request a certificate from a CA server on Windows CA Server



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

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>

X509 Local Certificate

- 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

Type: Domain Name (dropdown)
 Domain Name: draytek.com

Subject Name

Country (C): TW
 State (ST):
 Location (L):
 Organization (O): Draytek
 Organization Unit (OU):
 Common Name (CN):
 Email (E): press@draytek.com

Key Type: RSA (dropdown)
 Key Size: 1024 Bit (dropdown)

- Copy and save the X509 Local Certificate Request as a text file and save it for later use.

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Requesting	<input type="button" value="View"/> <input type="button" value="Delete"/>

X509 Local Certificate Request

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCQAwwQTELMakGA1UEBhMCFVcxEDA0BgNVBAoTB0RyYX10ZWsxIDAe
BgkqhkiG9wOBCQEWEXByZXRyYX10ZWsxY29tMIGfMA0GCSqGSIb3DQEBAAQMA4GNADCBiQKBgQDPioahu/gfQaYB1ce5OERSDFWknIdHb1o1kt9cTdlUDaFk6s8d
3wDeQytoV1LBjz2IDFOXjX6ip7ev187twwTsg4lgZ6Qk/rGhuVTkd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdXVYPpNKVlrOT2RZjkRMaHEWpVpIDAQAB
oCkwJwYJKoZIHveNAQkOMRowGDANBgNVHREEDzANGgtkcmF5dGVrLmNvbTANBgkq
hk1G9wOBAQUFAA0BgQAuSBRUGt4WlhH9N6/HwToem1tHQbcwjXvg/t7kf1zTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRRER86Ro08JxOI45560xCZ/N1Gh9VQ9I1
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejq/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
  
```

- 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**.

Microsoft Certificate Services -- vigor Home

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Select **Advanced request**.

Microsoft Certificate Services -- vigor Home

Choose Request Type

Please select the type of request you would like to make:

User certificate request

Advanced request

[Next >](#)

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

Microsoft Certificate Services -- vigor Home

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

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.

Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

[Next >](#)

Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.

Microsoft Certificate Services -- vigor Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARNCQAwwQTELHAKGA1UEBhMCVFcxEEDAO
BgkqhkiG9w0BCQEWEYBzZXNzQGRyYX10ZM5uY29t
A4GNADCB1QKBgQDQYB7mmZFfFhN9/ IeQnG03Xk++
hX4bp89cUF9d1oACGG1M/tcBockdcZdPFFvIXcP3
x/G0A7CTv0/fQzpxroCw1JTjLSjS0/Bn9v50951G
-----
```

[Browse](#) for a file to insert.

Certificate Template:

Administrator

Additional Attributes:

- Authenticated Session
- Basic EFS
- EFS Recovery Agent
- User
- IPSEC (Offline request)
- Router (Offline request)**
- Subordinate Certification Authority
- Web Server

[Submit >](#)

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

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

you will find the below window showing “-----BEGIN CERTIFICATE-----.....”
Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
Local	/C=TW/O=Draytek/emailAddress...	Not Valid Yet	<input type="button" value="View"/>	<input type="button" value="Delete"/>

X509 Local Certificate Request

```

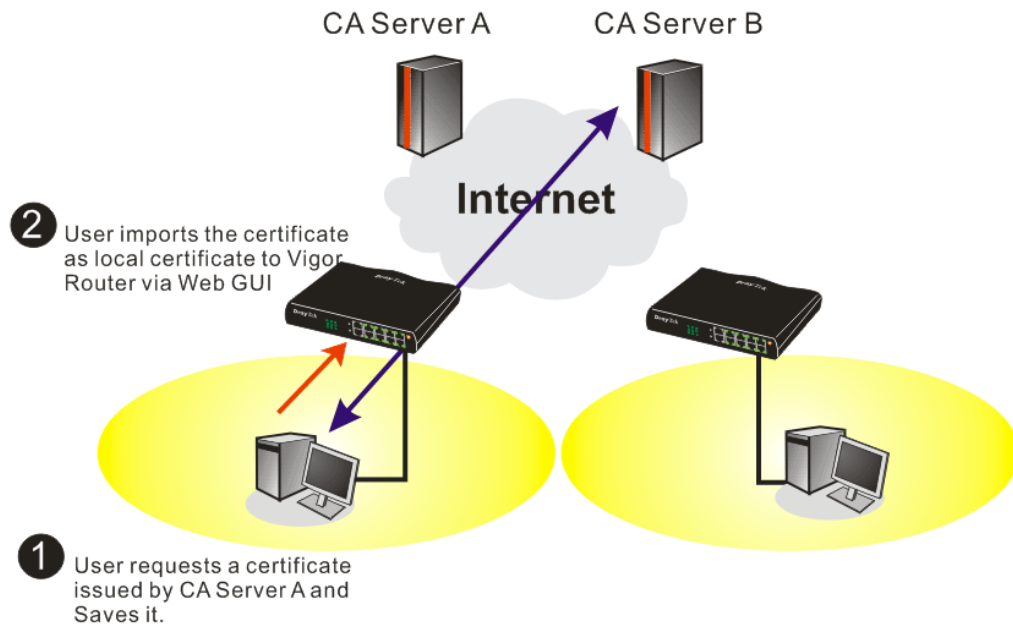
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCQAwwQTElMAkGA1UEBhMCVFcxEDAoBgNVBAoTBORyYX10ZWsxIDAe
BgkqhkiG9wOBCQEWEYyZXRyYX10ZWsuY29tMIGfMAOGCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSdfWknIdHb1o1kt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdXVYPWpNKVTrOT2RZjkRmaHEWpVpWIDAQAB
oCkwJwYJKoZlIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLnNvbTANBgkq
hkiG9wOBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiE16nV4hMRytcxZpEZ6sMarSgRREr86RoO8JxOI45560xCZ/N1Gh9VQ9I1
I9FqkjJNihp4TCjecSNMZjmQo5WU+Bce8TG+SCBCyejqqu/fo/AJQFajB7Gvii==
-----END CERTIFICATE REQUEST-----

```

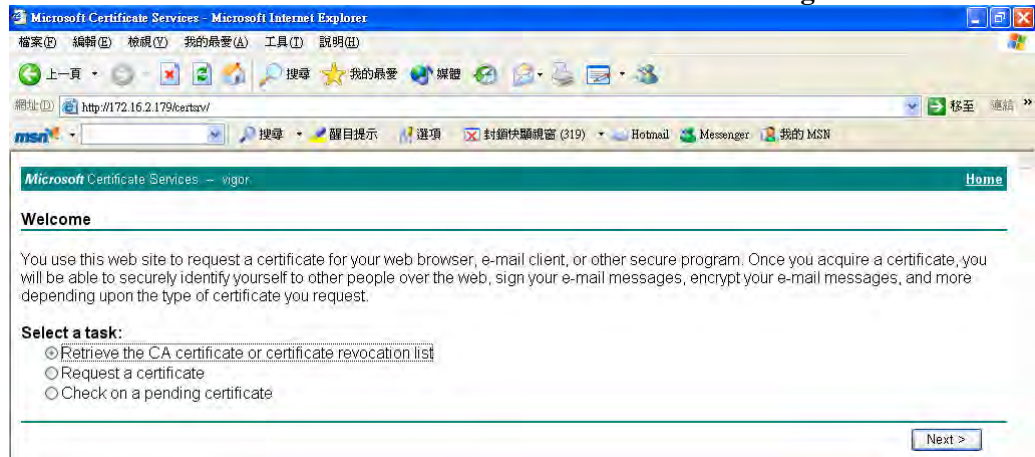
6. You may review the detail information of the certificate by clicking **View** button.

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

3.9 Request a CA Certificate and Set as Trusted on Windows CA Server



1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrieve the CA certificate or certificate recoring list**.



- In **Choose file to download**, click **CA Certificate Current** and **Base 64 encoded**, and **Download CA certificate** to save the .cer. file.



- 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

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify	
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

- 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

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

3.10 Creating an Account for MyVigor

The website of MyVigor (a server located on <http://myvigor.draytek.com>) 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.

3.10.1 Creating an Account via Vigor Router

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

System Maintenance >> Activation Activate via interface : auto-selected

Web-Filter License
[Status:Not Activated] **Activate**

Authentication Message
Activated Wiz, Authenticate is continuously, connect to the server, 2000-01-01 00:04:55


2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.

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 :

Password :

Auth Code : 

If you cannot read the word, [click here](#)

[Forget password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to :webmaster@draytek.com

3. Click the link of **Create an account now**.

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

MyVigor Agreement

1. Agreement

Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the medications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration

To use this service, you have to agree the following conditions:

(a) Provide your complete and correct information according to the registration steps of this service.

(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your account.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

<< Back Accept >>

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

Register

Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:* Mary Check Account

(3 ~ 20 characters)

Password:* ●●●●

(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:* ●●●●

Personal Information

First Name:* Mary

Last Name:* Ted

Company Name: Tech Ltd.

Email Address:* mary_ted@tech.com

Tel: 0 -

Country:* SWITZERLAND

Career:* Supervisor

Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

<< Back Continue >>

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

<< Back Continue >>

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

Register
Create an account - Please enter personal profile.

1 Agreement
2 Personal Information
3 Preferences
4 Completion

Completion

A confirmation email has been sent to **mary_ted@tech.com**
Please click on the activation link in the email
to activate your account

START

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

***** 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 :

Password :

Auth Code : **T4he1C**

If you cannot read the word, [click here](#)

[Forget password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to :webmaster@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.

3.10.2 Creating an Account via MyVigor Web Site

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

DrayTek MyVigor Customer Survey

Home Search GO

MyVigor for you

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:

VigorPro Unified Security Firewall series:

- Activation of Commtouch™ GlobalView Web Content Filter license key
- Activation of DT Anti-Virus license key
- Activation of Kaspersky Anti-Virus license key
- Activation of Commtouch™ Anti-Spam license key and membership

Vigor routers (for models that support Commtouch™)

- Activation of Commtouch™ GlobalView Web Content Filter license key

The MyVigor website contains a trail version of Commtouch™ GlobalView Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.

More customer-oriented services are planned for MyVigor site for the near future.

Please use IE 5.0 or above (resolution 1024 * 768) for best display. © DrayTek Corp.

Login

UserName

Password

AuthCode

If you can't read the AuthCode, [click here](#)

[Forget password?](#)

Not registered yet ? [Click here!](#)

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

MyVigor Agreement

1. Agreement

Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the medications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration

To use this service, you have to agree the following conditions:

(a) Provide your complete and correct information according to the registration steps of this service.

(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your account.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

<< Back Accept >>

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

Register

Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:* Mary Check Account

(3 ~ 20 characters)

Password:* Password

(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:* Password

Personal Information

First Name:* Mary

Last Name:* Ted

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

<< Back Continue >>

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

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

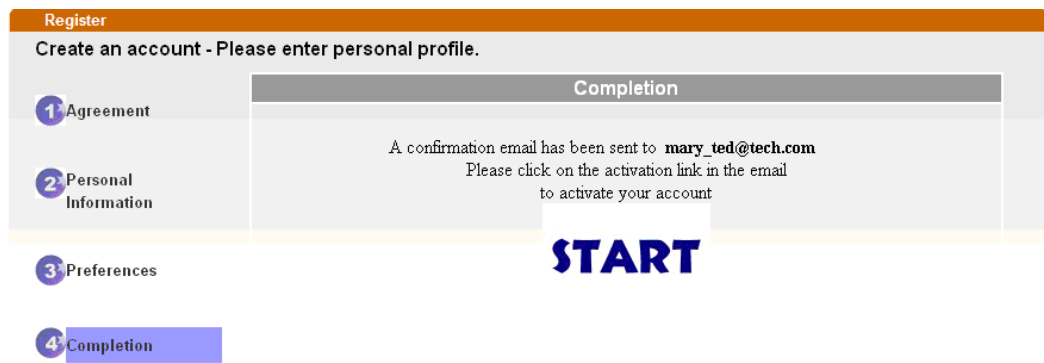
I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

<< 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 myvigor.draytek.com**.

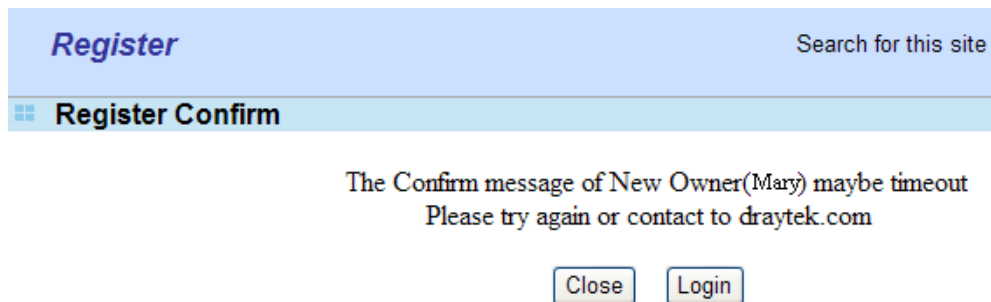
***** This is an automated message from myvigor.draytek.com.*****

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**.



- 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 :

Password :

Auth Code : **T4he1C**

If you cannot read the word, [click here](#)

[Forget password?](#)

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.
Customer Service : (886) 3 597 2727 or
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.

3.11 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 Application>>File Explorer**. If it is necessary for you to delete, copy files on the device or write, paste files to the device, it must be done through SAMBA server or FTP server.

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

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

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status:	Disk Connected	Disconnect USB Disk	
Write Protect Status:	No		
Disk Capacity:	2009 MB		
Free Capacity:	1664 MB	Refresh	
USB Disk Users 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.

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

USB Application >> USB General Settings

USB General Settings

General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	Default
Samba Service Settings(Network Neighborhood)	
<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Access Mode	
<input checked="" type="radio"/> LAN Only	<input type="radio"/> LAN And WAN
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor

- Note:**
1. If Charset is set to "default", only English long file name is supported.
 2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
 3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . ; " < > * + = / \ | ?.

OK

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.

USB Application >> USB User Management

Profile Index: 1

FTP/Samba User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="user1"/>
Password	<input type="password"/> (Maximum 11 Characters)
Confirm Password	<input type="password"/>
Home Folder	<input type="text" value="/"/>
Access Rule	
File	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input checked="" type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

OK Clear Cancel

Click **OK** to save the configuration.

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

Log On As

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.

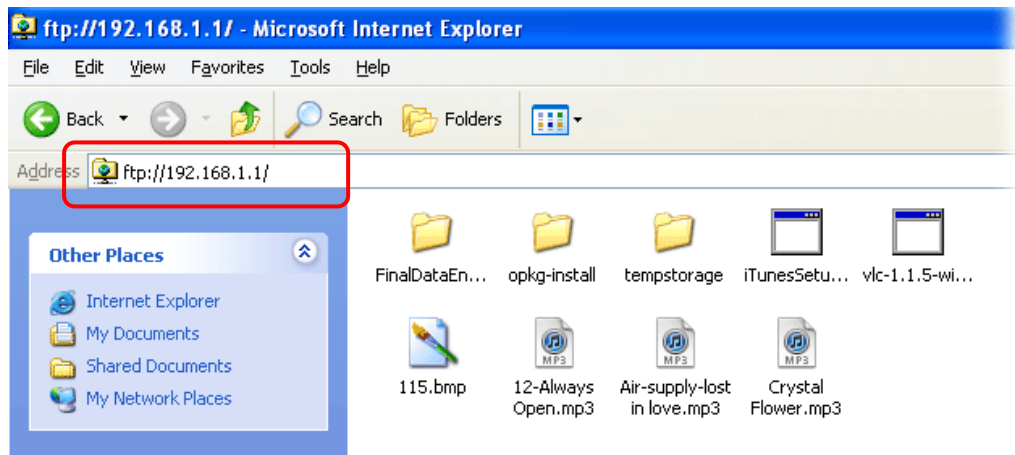
FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

Learn more about [using Web Folders](#).

Log on anonymously Save password

Log On Cancel

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



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

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: Disk Connected
 Write Protect Status: No
 Disk Capacity: 2009 MB
 Free Capacity: 1664 MB [Refresh](#)

USB Disk Users Connected | [Refresh](#) |

Index	Service	IP Address(Port)	Username	
1.	FTP	192.168.1.11(3343)	user1	<input type="button" value="Drop"/>
2.	FTP	192.168.1.11(3344)	user1	<input type="button" value="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.

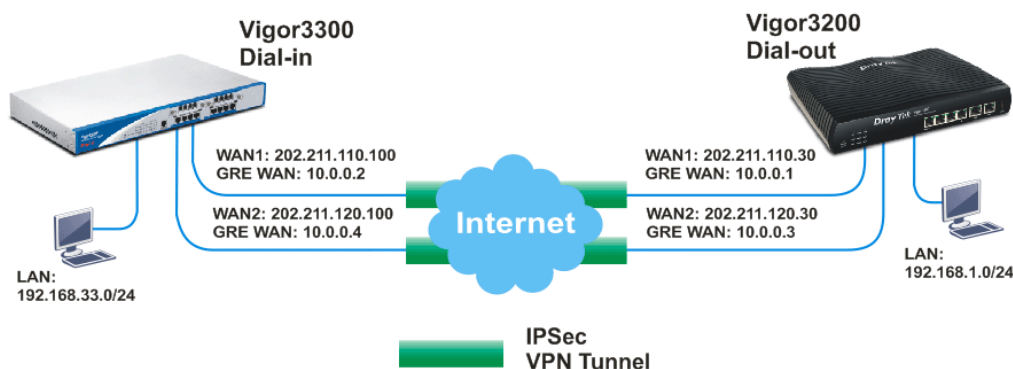
- Now, users in LAN of Vigor3200 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management**.

3.12 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 <-> 192.168.10.0/24. 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

LAN-to-LAN Profiles:

[Set to Factory Default](#)

Index	Name	Status	Index	Name	Status
<u>1.</u>	???	X	<u>17.</u>	???	X
<u>2.</u>	???	X	<u>18.</u>	???	X
<u>3.</u>	???	X	<u>19.</u>	???	X

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

Profile Name: wan1 only

Enable this profile

VPN Dial-Out Through: WAN Only

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

Call Direction: Both Dial-Out Dial-in

Always on

Idle Timeout: 1 second(s)

Enable PING to keep alive

PING to the IP: _____

2. Dial-Out Settings

Type of Server I am calling:

PPTP

IPsec Tunnel

L2TP with IPsec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

202.211.110.100

Username: ???

Password: _____

PPP Authentication: PAP/CHAP

VJ Compression: On Off

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

Local Certificate: None

IPsec Security Method:

Medium(AH)

High(ESP) DES without Authentication

Advanced

Index(1-15) in Schedule Setup:

3. Dial-In Settings

Allowed Dial-In Type:

PPTP

IPsec Tunnel

L2TP with IPsec Policy: None

Specify Remote VPN Gateway

Peer VPN Server IP: _____

or Peer ID: _____

Username: _____

Password: _____

VJ Compression: On Off

IKE Authentication Method:

Pre-Shared Key

IKE Pre-Shared Key: _____

Digital Signature(X.509)

Local ID: None

Alternative Subject Name First

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

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.33.0

Remote Network Mask: 255.255.255.0

Local Network IP: 192.168.1.1

Local Network Mask: 255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do:

Route

Change default route to this VPN tunnel (Only single WAN supports this)

- 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

LAN-to-LAN Profiles: [Set to Factory Default](#)

Index	Name	Status	Index	Name	Status
<u>1.</u>	wan1 only	X	<u>17.</u>	???	X
<u>2.</u>	???	X	<u>18.</u>	???	X
<u>3.</u>	???	X	<u>19.</u>	???	X

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: wan2 only

Enable this profile

VPN Dial-Out Through: WAN2 Only

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP, IP-Camera, DHCP Relay...etc.)

Call Direction: Dial-Out Dial-in

Always on

Idle Timeout: -1 second(s)

Enable PING to keep alive

PING to the IP: _____

2. Dial-Out Settings

Type of Server I am calling

PPTP

IPsec Tunnel

L2TP with IPsec Policy [None]

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

202.211.120.100

Username: ???

Password: _____

PPP Authentication: PAP/CHAP

VJ Compression: On Off

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: [REDACTED]

Digital Signature(X.509)

Peer ID: [None]

Local ID: _____

Alternative Subject Name First

Subject Name First

Local Certificate: [None]

IPsec Security Method

Medium(AH)

High(ESP) | DES without Authentication

Advanced

Index(1-15) in **Schedule** Setup:
[] [] [] [] [] [] [] [] [] [] [] [] [] [] []

3. Dial-In Settings

Allowed Dial-In Type

pPTP

IPsec Tunnel

L2TP with IPsec Policy [None]

Specify Remote VPN Gateway

Peer VPN Server IP: _____

or Peer ID: _____

Username: _____

Password: _____

VJ Compression: On Off

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: _____

Digital Signature(X.509)

[None]

Local ID: _____

Alternative Subject Name First

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: 10.0.0.3

Peer GRE IP: 10.0.0.4

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: 255.255.255.0

Local Network IP: 192.168.1.1

Local Network Mask: 255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do _____

[Route]

Change default route to this VPN tunnel (Only single WAN supports this)

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

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1 (Active) Type	Member2 (Active) Type
1	v	wan1wan2	1 (YES) IPSec	2 (YES) IPSec

Advanced wan1wan2 ▾

General Setup

Status **Enable** Disable

Profile Name

Member1

Member2

Active Mode Backup **Load Balance**

- Click **Advanced** for specifying **Load Balance Algorithm**.

VPN Load Balance Advance Settings

Profile Name: Trunk1

Load Balance Algorithm: Round Robin
 Weighted Round Robin
 Auto Weighted
 According to Speed Ratio (Member1:Member2):
 Fastest

VPN Load Balance - Binding Tunnel Policy

Create After insert

Tunnel Bind Table Index: (1~400)

Active:

Binding Dial Out Index:

Binding Src IP Start: End:

Binding Dest IP Start: End:

Binding Dest Port Start: End:

Binding Fragmented: Binding Protocol:

Detail Information

[VPN Load Balance Profile name: Trunk1]
 [Algorithm: Round Robin]

- 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.

VPN and Remote Access >> Connection Management

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

(wan1wan2) 202.211.120.100

VPN Connection Status Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	1983	42	3971	60	1:6:10	Drop
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	2334	18	137	3	1:15:22	Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

Settings for Vigor3300:

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

VPN - IPSec - VPN Trunk - Policy Table

#	Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1							<input checked="" type="radio"/>
2							<input type="radio"/>
3							<input type="radio"/>
4							<input type="radio"/>
5							<input type="radio"/>
6							<input type="radio"/>
7							<input type="radio"/>
8							<input type="radio"/>
9							<input type="radio"/>
10							<input type="radio"/>

Refresh Edit Delete Delete All

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

VPN - IPSec - VPN Trunk - Policy Table - Edit

Default | Advanced

Basic

Profile Status :

Name :

Authentication :

Preshared Key :

Security Protocol :

NAT Traversal :

Local Gateway

WAN Interface :

Local Certificate :

Security Gateway :

Local GRE IP :

Next hop :

Remote Gateway

Remote ID :

Security Gateway : ('0.0.0.0' for dynamic client)

Remote GRE IP :

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 - VPN Trunk - Policy Table - Edit

Default | Advanced

Basic

Profile Status :

Name :

Authentication :

Preshared Key :

Security Protocol :

NAT Traversal :

Local Gateway

WAN Interface :

Local Certificate :

Security Gateway :

Local GRE IP :

Next hop :

Remote Gateway

Remote ID :

Security Gateway : ('0.0.0.0' for dynamic client)

Remote GRE IP :

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

VPN - VPN Trunk - Group Table

#	Profile Status	Name	Local Subnet	Remote Subnet
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

1

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

VPN - VPN Trunk - Group Table - Edit

1

Profile Status : Disable Enable

Name :

Local Subnet : /

Remote Subnet : /

Tunnel 1 : Weight :

Tunnel 2 : Weight :

Tunnel 3 : Weight :

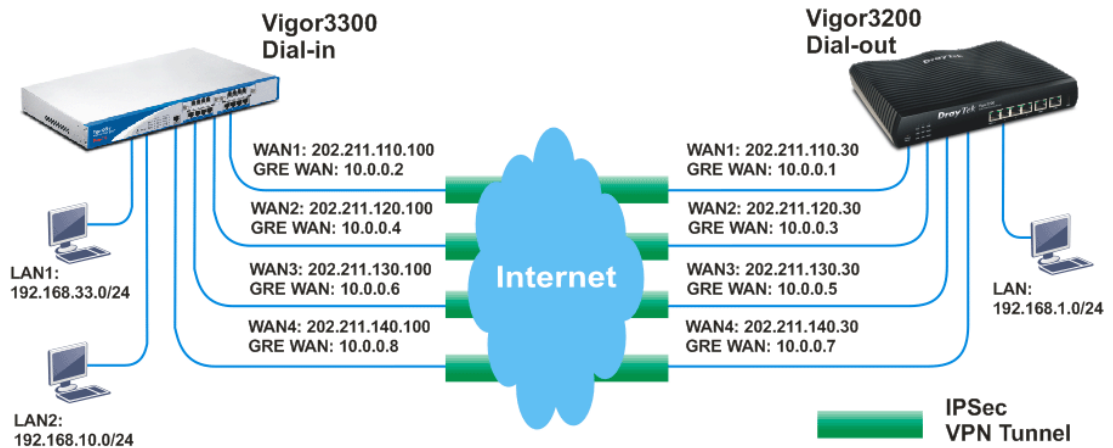
Tunnel 4 : Weight :

Backup

Active	Master	Slave
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

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.

LAN-to-LAN Profiles:			Set to Factory Default		
Index	Name	Status	Index	Name	Status
<u>1.</u>	wan1 only	√	<u>17.</u>	???	×
<u>2.</u>	wan2 only	√	<u>18.</u>	???	×
<u>3.</u>	wan3 only	√	<u>19.</u>	???	×
<u>4.</u>	wan4 only	√	<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>	???	×

- 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.

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	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

Advanced | wan1wan2 ▾

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

Add | Edit | Delete

- 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.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds: 10 ▾ Refresh

General Mode: ▾ Dial

Backup Mode: ▾ Dial

Load Balance Mode: (wan1wan2) 202.211.110.100 ▾ Dial

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Network	Pkts	Rate(Bps)	Rx Pkts	Rx Rate(Bps)	UpTime	
1 (wan1 only)	IPSec Tunnel DES-No Auth	202.211.110.100 via WAN1	192.168.33.0/24	3393	24	6800	60	1:53:18	Drop
2 (wan2 only)	IPSec Tunnel DES-No Auth	202.211.120.100 via WAN2	192.168.33.0/24	3753	39	137	3	2:2:30	Drop
3 (wan3 only)	IPSec Tunnel DES-No Auth	202.211.130.100 via WAN3	192.168.10.0/24	3630	39	7213	60	2:2:28	Drop
4 (wan4 only)	IPSec Tunnel DES-No Auth	202.211.140.100 via WAN4	192.168.10.0/24	3583	24	0	0	2:2:19	Drop

xxxxxxx : Data is encrypted.
xxxxxxx : 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.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN **802.1Q VLAN**

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	22	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Enable management port for P4
 Enable packet forwarding between VLANs

Port Setting

	P1	P2	P3	P4
Port VLAN ID	20	21	22	8

Apply Reset Cancel

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

Network - LAN

LAN IP/DHCP
 LAN2 IP/DHCP
 LAN3 IP/DHCP
 LAN4 IP/DHCP
 DHCP Relay Agent
 IP Routing

IP Configuration

IP Address : 192.168.33.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : Enable Disable Relay Agent

Start IP : 192.168.33.10

End IP : 192.168.33.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

Apply Cancel

Network - LAN

LAN IP/DHCP
 LAN2 IP/DHCP
 LAN3 IP/DHCP
 LAN4 IP/DHCP
 DHCP Relay Agent
 IP Routing

IP Configuration

IP Address : 192.168.10.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : Enable Disable Relay Agent

Start IP : 192.168.10.10

End IP : 192.168.10.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

Apply Cancel

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

to configure the setting is the same as Scenario 1.

VPN - IPSec - VPN Trunk - Policy Table

#	Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1	<input checked="" type="radio"/> wan1	10.0.0.2	0.0.0.0	10.0.0.1	WAN1	enable	up
2	<input type="radio"/> wan2	10.0.0.4	0.0.0.0	10.0.0.3	WAN2	enable	up
3	<input type="radio"/> wan3	10.0.0.6	0.0.0.0	10.0.0.5	WAN3	enable	up
4	<input type="radio"/> wan4	10.0.0.8	0.0.0.0	10.0.0.7	WAN4	enable	up
5	<input type="radio"/>						
6	<input type="radio"/>						
7	<input type="radio"/>						
8	<input type="radio"/>						
9	<input type="radio"/>						
10	<input type="radio"/>						

1

DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

- 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.

VPN - VPN Trunk - Group Table

#	Profile Status	Name	Local Subnet	Remote Subnet
1	<input checked="" type="radio"/> Enable	192.168.33.0	192.168.33.0/24	192.168.1.0/24
2	<input type="radio"/> Enable	192.168.10.1	192.168.10.0/24	192.168.1.0/24
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

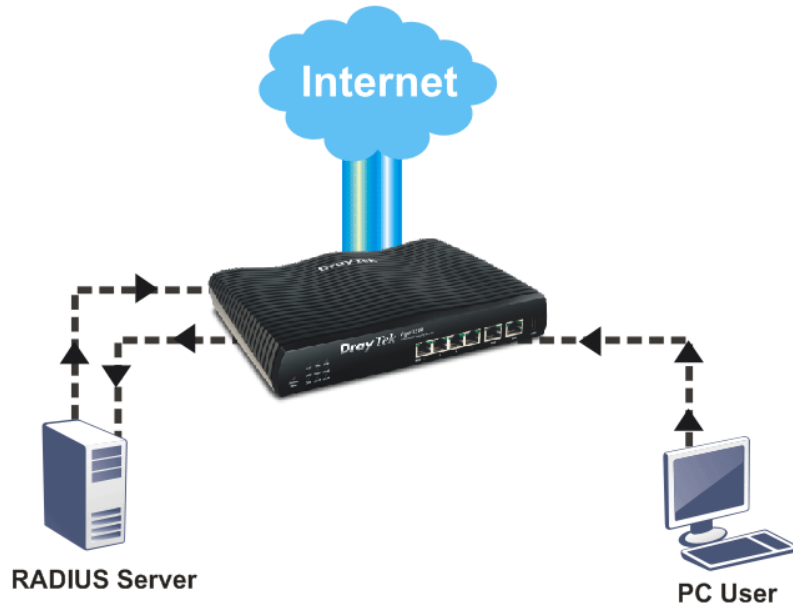
1

DrayTek Corp. © 1997 - 2009 All rights reserved. DrayTek Enterprise Network Solutions.

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

3.13 How to implement RADIUS authentication for User Management?

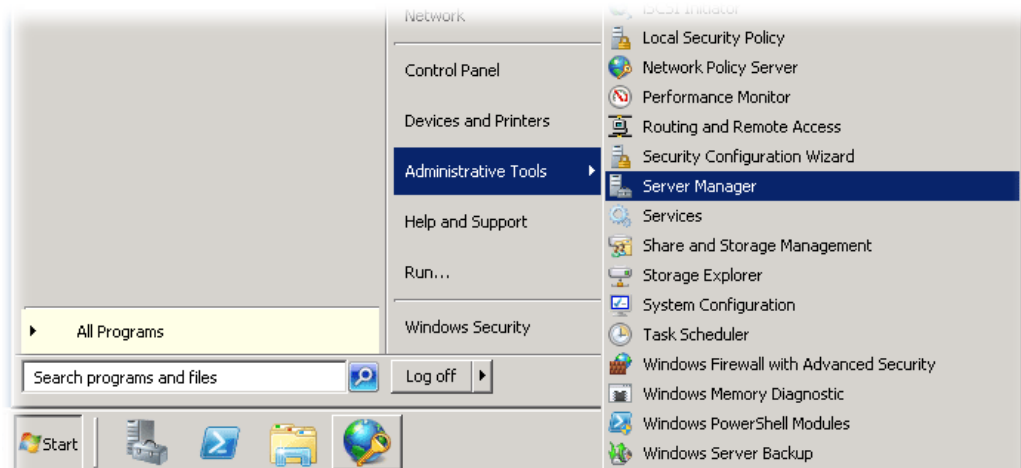
We will take Windows2008 R2 as the RADIUS server for this case.



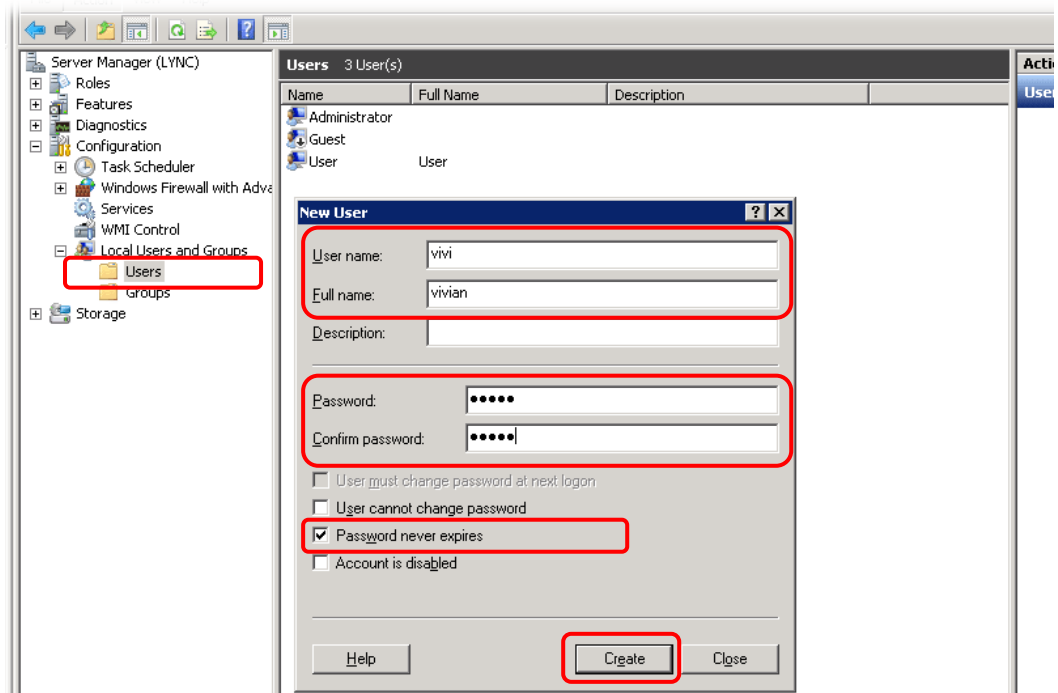
This page is left blank.

Settings on RADIUS server:

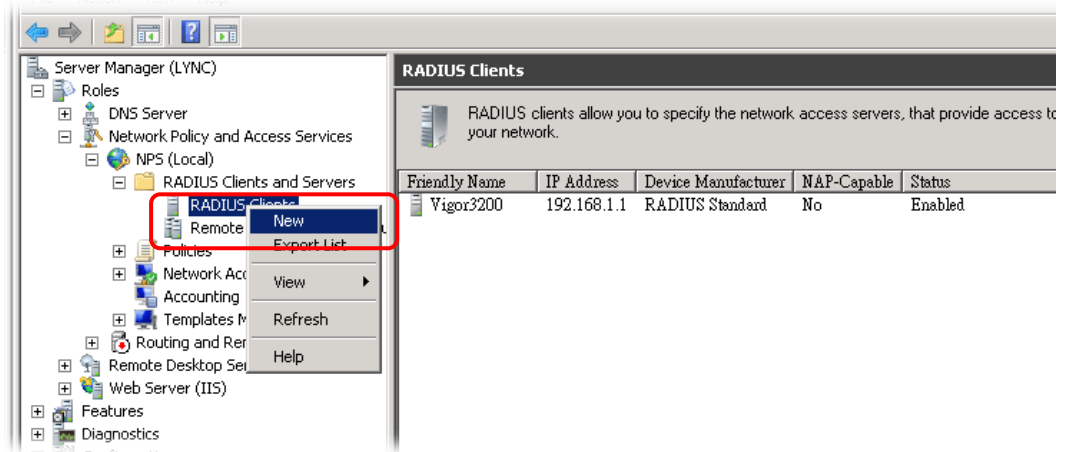
1. Click **Start** and open **Server Manager**.



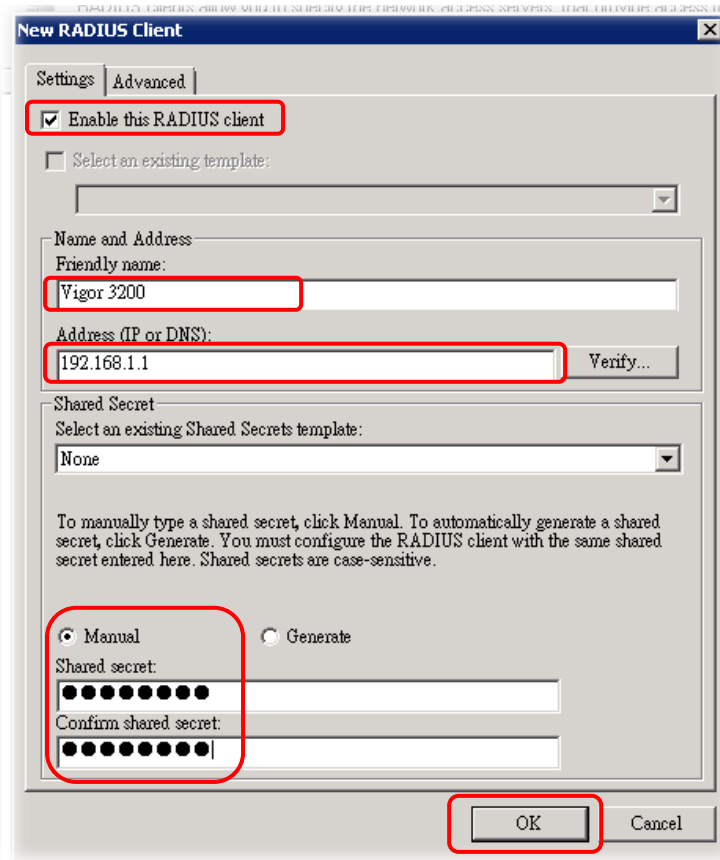
2. Create a user account and password (e.g., vivi in this case) by clicking **Local Users and Groups>>Users.**)



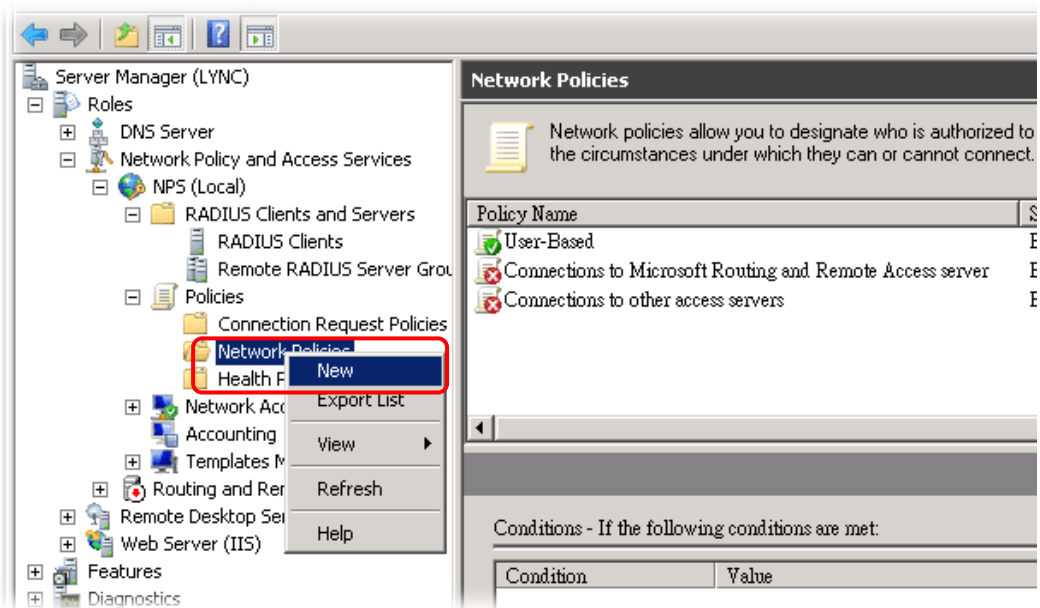
3. Locate **RADIUS Client** and right click the mouse button to select **New**.



4. Type the related information (for Friendly name, Address (IP or DNS), shared secret and so on) for the client. Keep the value of the shared secret in mind. At last, click **OK** to save the settings.



5. Open **NPS>>Policy>>Network Policy**. Right click the mouse button on the **Network Policy** to select **New**.



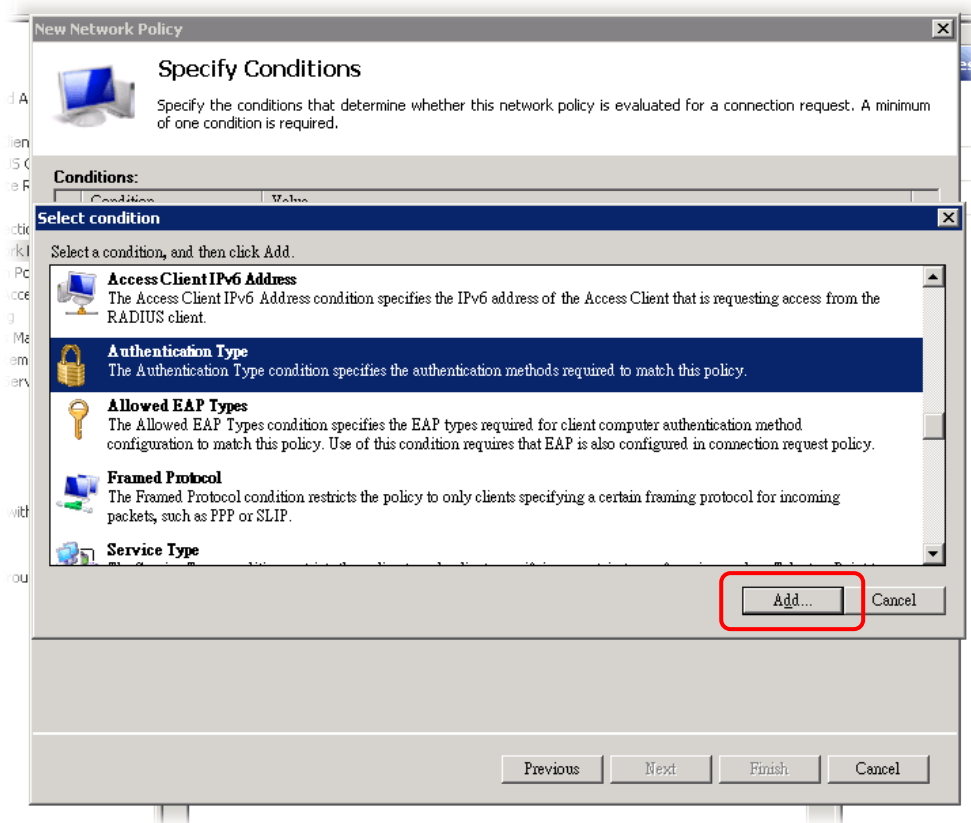
6. A pop-up window will appear as follows. Please type the name of the policy (e.g., **User-Based** in this case) and click **Next**.

The screenshot shows a dialog box titled "New Network Policy" with the subtitle "Specify Network Policy Name and Connection Type". The main text reads: "You can specify a name for your network policy and the type of connections to which the policy is applied." Below this, there is a text input field labeled "Policy name:" containing the text "User-Based". Underneath is a section for "Network connection method" with instructions: "Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified." There are two radio buttons: "Type of network access server:" (selected) and "Vendor specific:". The "Type of network access server:" has a dropdown menu showing "Unspecified". The "Vendor specific:" has a text input field with "10". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel". The "Next" button is highlighted with a red box.

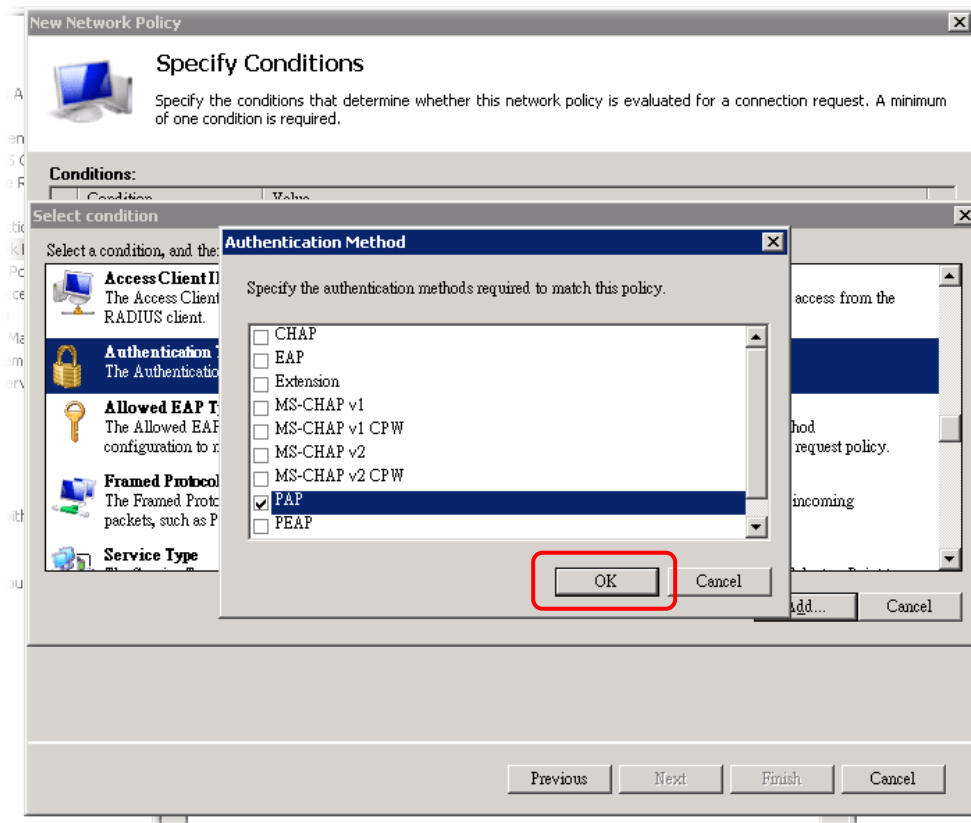
7. In the following page, simply click **Add**.

The screenshot shows a dialog box titled "New Network Policy" with the subtitle "Specify Conditions". The main text reads: "Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required." Below this is a table with two columns: "Condition" and "Value". The table is currently empty. Below the table is a text input field labeled "Condition description:". At the bottom right, there are three buttons: "Add...", "Edit...", and "Remove". The "Add..." button is highlighted with a red box. At the very bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

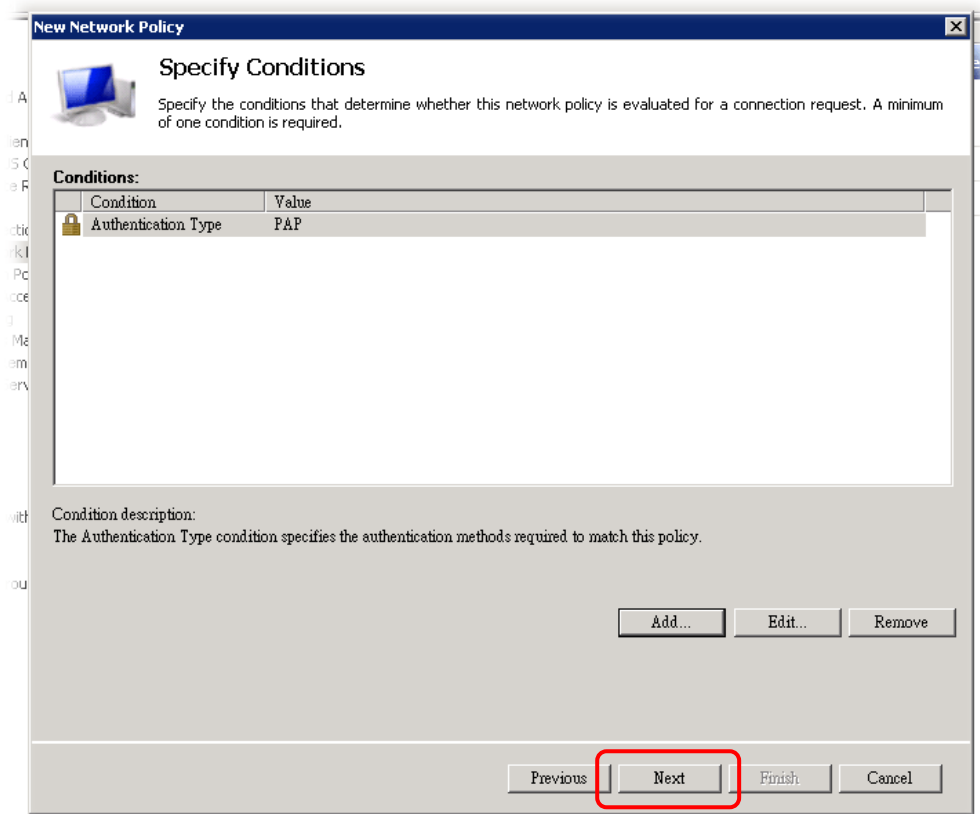
8. Choose **Authentication Type** and click **Add** for next step.



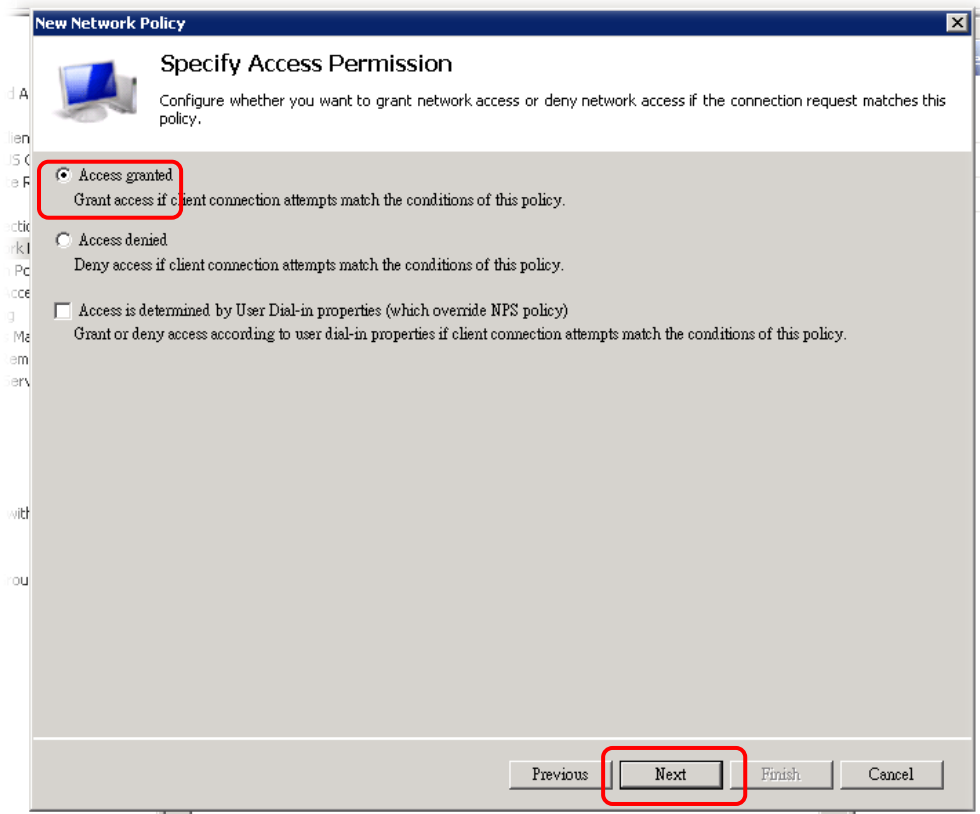
9. In the following dialog, check the box of **PAP**. Then, click **OK**.
User Management of Vigor router can only supports PAP authentication. Therefore, configure the RADIUS server to accept PAP authentication.



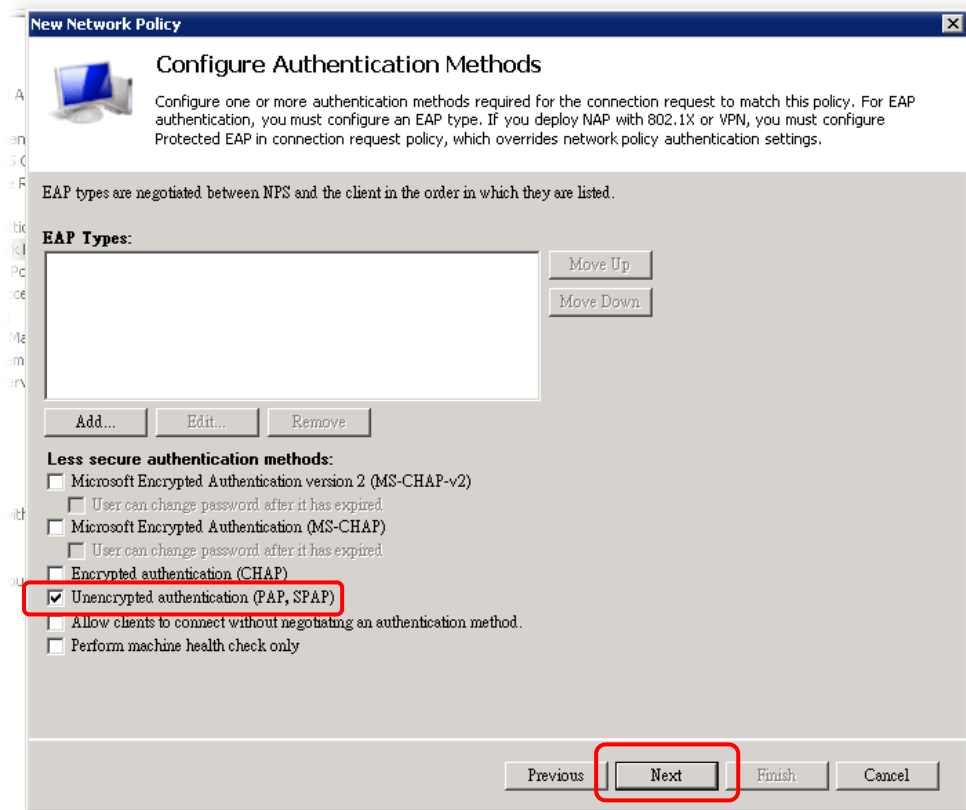
10. In the following dialog, click **Next**.



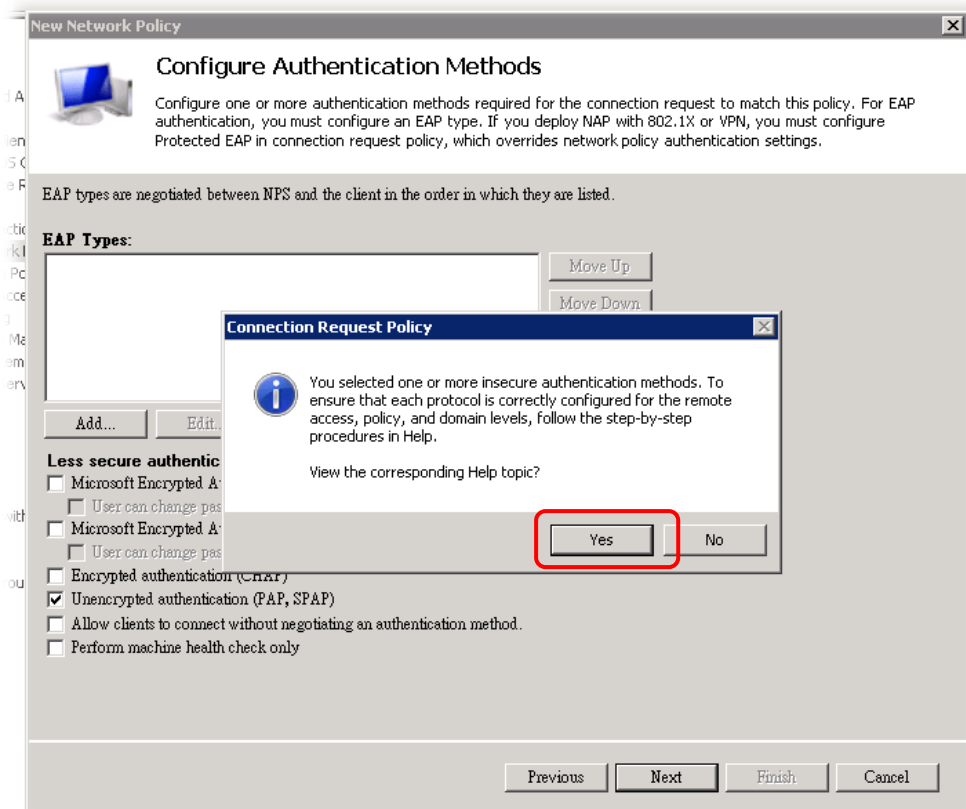
11. Choose **Access granted** and click **Next**.



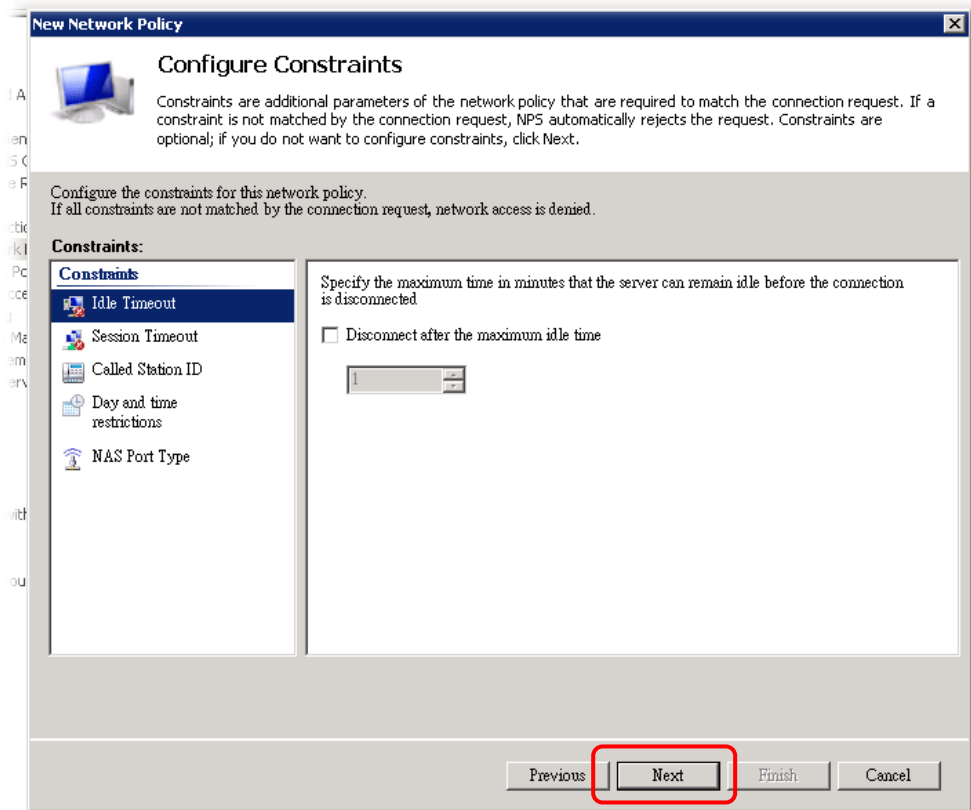
12. Check the box of Unencrypted authentication (PAP, SPAP) and click Next.



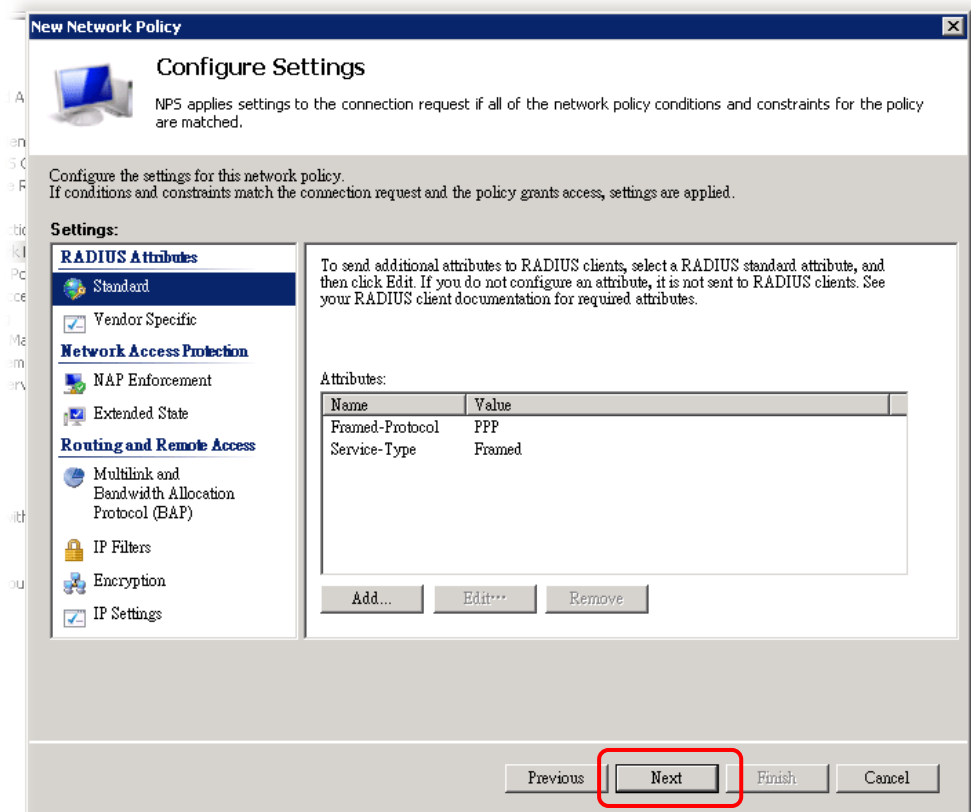
13. When the following dialog appears, simply click No.



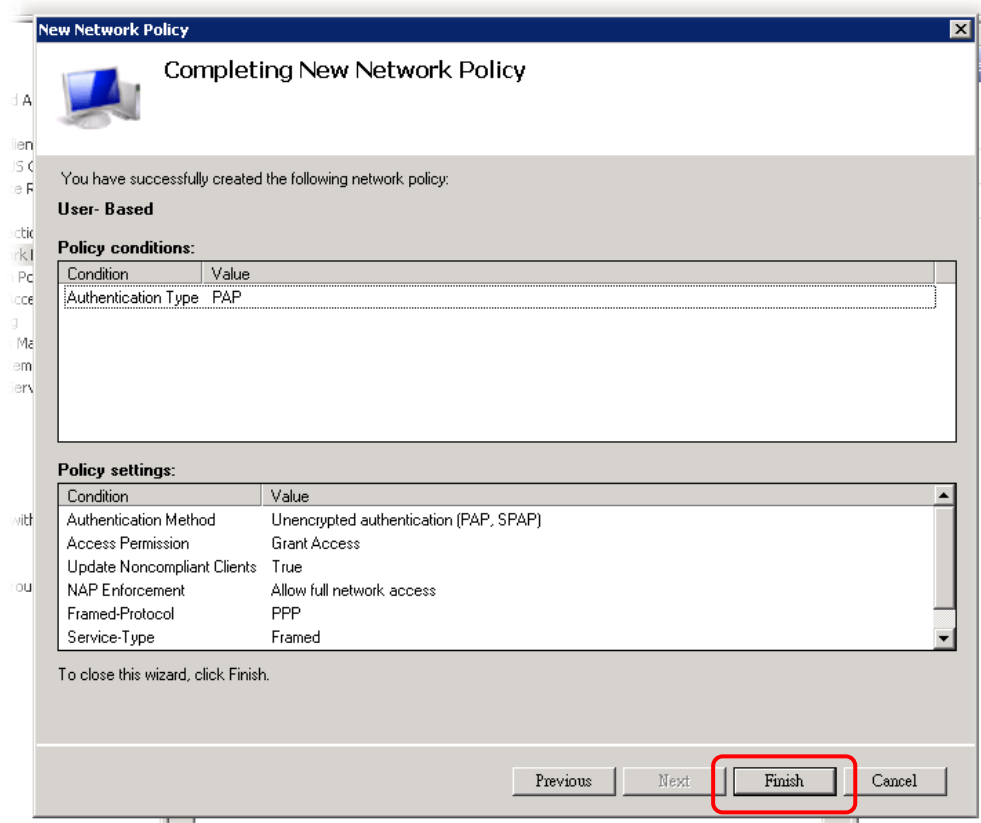
14. In the following window, just click **Next**.



15. Then, click **Next**.



- Now, the network policy (named with User-Based) has been created. Click **Finish**.



Settings on Vigor3200:

- Access into the web configurator of Vigor3200.
- Open **Application**>>**RADIUS**. Configure RADIUS server IP and Shared Secret. The value for Shared Secret should be the same as the settings configured in Step 4 described above for **Settings on RADIUS server**.

Applications >> RADIUS

RADIUS Setup

<input checked="" type="checkbox"/> Enable	
Server IP Address	192.168.1.199
Destination Port	1812
Shared Secret
Confirm Shared Secret	

- Click **OK** to save the settings.

- Open **User Management>>User Profile (Reserved)** and click Index #3 to create a user profile.

User Management >> User Profile(Reserved)

User Profile Table | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.	admin	17.	
2.	Dial-In User	18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	

- Check the box of **Enable this account** and type a user name for such profile. Choose **Radius** as **External Server Authentication** and click **OK** to save the settings.

User Management >>User Profile(Reserved)

Profile Index 3

Enable this account

User Name:


Password:

Confirm Password:

Idle Timeout: min(s) 0:Unlimited

Max User Login: 0:Unlimited

Policy:

External Server Authentication: 

Log:

Pop Browser Tracking Window:

Authentication: Web Alert Tool Telnet

Landing Page:

Index(1-15) in [Schedule Setup](#): , , ,

The selection of items could be created as rules and which not set to active.

6. Open **User Management>>General Setup** and specify **User-Based** as the **Mode** setting. Click **OK**.

User Management >> General Setup

General Setup

Mode:

Notice :

1. User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode.
2. Users match the above lists will not be required for authentication. The firewall rules policy will still valid.
3. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.

Landing Page (Max 255 characters) [Preview](#) | [Set to Factory Default](#) |

```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

7. Any user who wants to access into the Internet shall be authenticated by the RADIUS authentication mechanism. Vigor router will redirect the HTTP connection to the login page as the picture shown below.

The screenshot shows a login interface with a light gray background and a red footer. It contains three input fields: 'Username' with the text 'vivi', 'Password' with four dots, and 'Group' with a dropdown arrow. A 'Login' button is positioned to the right of the input fields. The footer contains the text 'Copyright©, DrayTek Corp. All Rights Reserved.' and the 'DrayTek' logo.

8. If the access is granted, the following screen will appear.



This page is left blank.

4

Web Configuration

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.

Vigor3200 Series
Multi-WAN Security Router

DrayTek

Off IPv6

Online Status

WAN
LAN
Load-Balance/Route Policy
NAT
Firewall
User Management
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
SSL VPN
USB Application
System Maintenance
Diagnostics
External Devices
Support Area
FAQ/Application Note
Product Registration

Logout
All Rights Reserved.

System Status

Model Name : Vigor3200
Firmware Version : 3.6.8.5
Build Date/Time : Jun 1 2016 10:57:08

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-CE-46-FC	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-50-7F-CE-46-FC	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-50-7F-CE-46-FC	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-50-7F-CE-46-FC	192.168.4.1	255.255.255.0	ON	8.8.8.8
DMZ PORT	00-50-7F-CE-46-FC	192.168.5.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-50-7F-CE-46-FC	192.168.0.1	255.255.255.0	ON	8.8.8.8

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-50-7F-CE-46-FD	---	---	---
WAN2	Disconnected	00-50-7F-CE-46-FE	---	---	---
WAN3	Disconnected	00-50-7F-CE-46-FF	---	---	---
WAN4	Disconnected	00-50-7F-CE-46-00	---	---	---
WAN5	Disconnected	00-50-7F-CE-46-01	---	---	---

IPv6			
	Address	Scope	Internet Access Mode
LAN	FE80::250:7FFF:FECE:46FC/64	Link	---

User Mode is OFF now.

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 Balance Mode:

Index	Enable	Physical Mode/Type	Line Speed(Kbps) DownLink/UpLink	Active Mode
WAN1	<input checked="" type="checkbox"/>	Ethernet/Auto negotiation	10000 / 10000	Always On
WAN2	<input checked="" type="checkbox"/>	Ethernet/Auto negotiation	10000 / 10000	Always On
WAN3	<input checked="" type="checkbox"/>	Ethernet/Auto negotiation	10000 / 10000	Backup
WAN4	<input checked="" type="checkbox"/>	Ethernet/Auto negotiation	10000 / 10000	Backup
WAN5	<input checked="" type="checkbox"/>	USB/-	2000 / 384	Always On

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

OK

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	<p>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.</p> <p>Load Balance Mode: <input type="text" value="Auto Weight"/></p> <p>IP Based - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.</p> <p>Session Based- All of the WAN interfaces will be used (as</p>

	<p>out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP.</p> <p>If you have no strong demand about speed test result, keep default settings as IP based.</p>
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(Kbps) DownLink/UpLink	Display the downstream and upstream rate of such WAN interface.
Active Mode	<p>Display whether such WAN interface is Active device or backup device.</p> <p>Always On - Display that such WAN interface is active.</p> <p>Backup WAN - Display the Backup WAN interface for such WAN when it is disabled.</p>

Note: In default, each WAN is enabled.

For WAN1 ~ WAN4 (Ethernet)

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


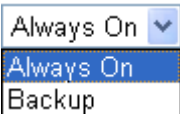
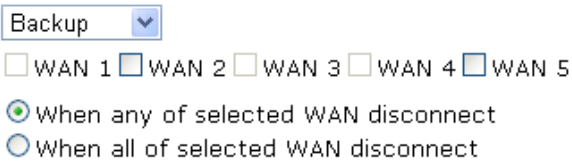
WAN >> General Setup

WAN 1

Enable:	Yes ▾
Display Name:	<input type="text"/>
Physical Mode:	Ethernet
Physical Type:	Auto negotiation ▾
Line Speed(Kbps):	
DownLink	<input type="text" value="10000"/>
UpLink	<input type="text" value="10000"/>
VLAN Tag insertion :	Disable ▾ (Please configure Internet Access setting first)
Tag value:	<input type="text" value="0"/> (0~4095)
Priority:	<input type="text" value="0"/> (0~7)
Active Mode:	Backup ▾ Load Balance: <input checked="" type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5
Backup Type (Only if acting as backup for multiple WAN):	<input checked="" type="radio"/> When any of selected WAN disconnect <input type="radio"/> When all of selected WAN disconnect

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

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	<p>You can change the physical type for WAN2 or choose Auto negotiation for determined by the system.</p> <p>Physical Type: </p>
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	<p>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.</p> <p>Disable – Disable the function of VLAN with tag.</p> <p>Tag value – Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority – Type the number for such VLAN. The range is from 0 to 7.</p>
Active Mode	<p>Determine the WAN interface will be active for always (Always On) or be treated as a backup WAN interface (Backup).</p> <p></p> <p>Backup Type - Determine the role of such WAN interface. It will be changed according to the Active Mode specified.</p> <p>If you choose Always On as Active Mode, such interface will be used for access into Internet all the time.</p> <p>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.</p> <p></p>

	<p>When any of selected WAN disconnect – WAN1 will be activated when any WAN interface disconnects.</p> <p>When all of selected WAN disconnect – WAN1 will be activated when all the WAN interfaces disconnect.</p>
Load Balance	<p>Check this box to enable auto load balance function for such WAN interface.</p> <p>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.</p>

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

For WAN5 (USB)

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

WAN >> General Setup

WAN 5

Enable:	<input type="button" value="Yes"/>
Display Name:	<input type="text"/>
Physical Mode:	USB
Physical Type:	<input type="button" value="Auto negotiation"/>
Line Speed(Kbps):	
DownLink	<input type="text" value="2000"/>
UpLink	<input type="text" value="384"/>
Active Mode:	<input type="button" value="Backup"/> Load Balance: <input checked="" type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5
Backup Type (Only if acting as backup for multiple WAN):	<input checked="" type="radio"/> When any of selected WAN disconnect <input type="radio"/> 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).

	<div data-bbox="699 203 879 309"> <input type="button" value="Always On"/> <ul style="list-style-type: none"> <input type="button" value="Always On"/> <input type="button" value="Backup"/> </div> <p>Backup Type - Determine the role of such WAN interface. It will be changed according to the Active Mode specified.</p> <p>If you choose Always On as Active Mode, such interface will be used for access into Internet all the time.</p> <p>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.</p> <div data-bbox="710 629 1326 792"> <input type="button" value="Backup"/> <ul style="list-style-type: none"> <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5 <input checked="" type="radio"/> When any of selected WAN disconnect <input type="radio"/> When all of selected WAN disconnect </div> <hr/> <p>When any of selected WAN disconnect – WAN1 will be activated when any WAN interface disconnects.</p> <p>When all of selected WAN disconnect – WAN1 will be activated when all the WAN interfaces disconnect.</p>
<p>Load Balance</p>	<p>Check this box to enable auto load balance function for such WAN interface.</p> <p>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.</p>

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	<input type="button" value="Details Page"/>	<input type="button" value="IPv6"/>
WAN2		Ethernet	None	<input type="button" value="Details Page"/>	<input type="button" value="IPv6"/>
WAN3		Ethernet	None	<input type="button" value="Details Page"/>	<input type="button" value="IPv6"/>
WAN4		Ethernet	None	<input type="button" value="Details Page"/>	<input type="button" value="IPv6"/>
WAN5		USB	Static or Dynamic IP	<input type="button" value="Details Page"/>	<input type="button" value="IPv6"/>

Note : Only one WAN port can be configured to support IPv6.

You can configure DHCP client options here.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	None	Details Page	IPv6
WAN2		Ethernet	None	Details Page	IPv6
WAN3		Ethernet	None	Details Page	IPv6
WAN4		Ethernet	None	Details Page	IPv6
WAN5		USB	None	Details Page	IPv6

Note : Only one WAN port can be configured to

- None
- 3G/4G USB Modem(PPP mode)

Advanced You can configure DHCP client options here.

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.

Details Page for PPPoE in WAN1 ~ WAN4

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

WAN >> Internet Access

WAN 1

<p>PPPoE Client Mode <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>ISP Access Setup Service Name (Optional) <input type="text"/> Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <p>WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input type="text"/> TTL: <input type="text"/></p> <p>MTU <input type="text" value="1442"/> (Max:1492)</p> <p>PPPoE Pass-through <input type="checkbox"/> For Wired LAN</p>	<p>PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/></p> <p><input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="CE"/> <input type="text" value="46"/> <input type="text" value="FD"/></p>
--	--

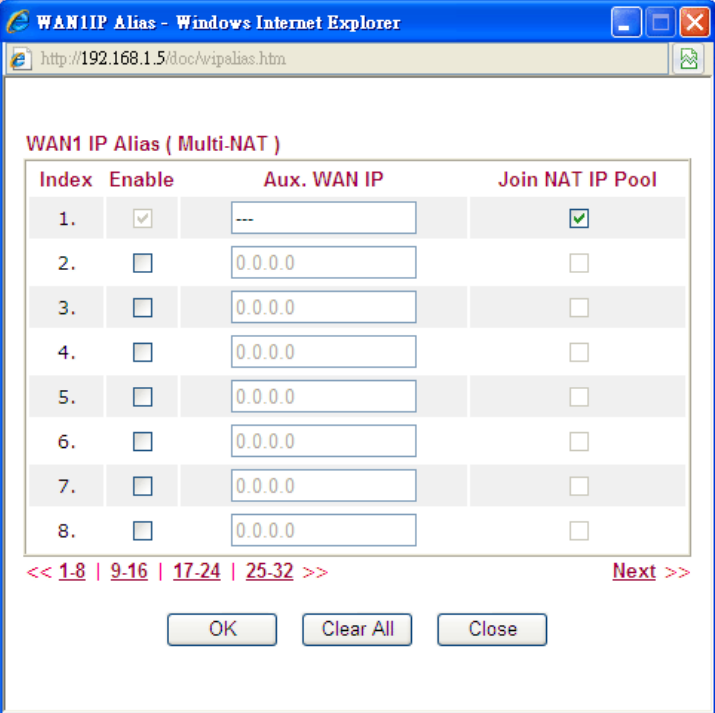
Note: (Optional) Required for some ISPs. Leave blank if in doubt because the connection request might be denied if "Service Name" is incorrect.

OK Cancel

Available settings are explained as follows:

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. Service Name (Optional) - Enter the description of the specific network service. 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
	<p>have to type IP address in this field for ping.</p> <p>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</p>
MTU	<p>It means Max Transmit Unit for packet. The default setting is 1442.</p>
PPPoE Pass-through	<p>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.</p> <p>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.</p> <p>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.</p>
PPP/MP Setup	<p>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.</p> <p>Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method (IPCP)	<p>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.</p> <p>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.</p>

Item	Description
	 <p>Fixed IP – Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.</p> <p>Default MAC Address – You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.</p> <p>Specify a MAC Address – Type the MAC address for the router manually.</p>

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

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

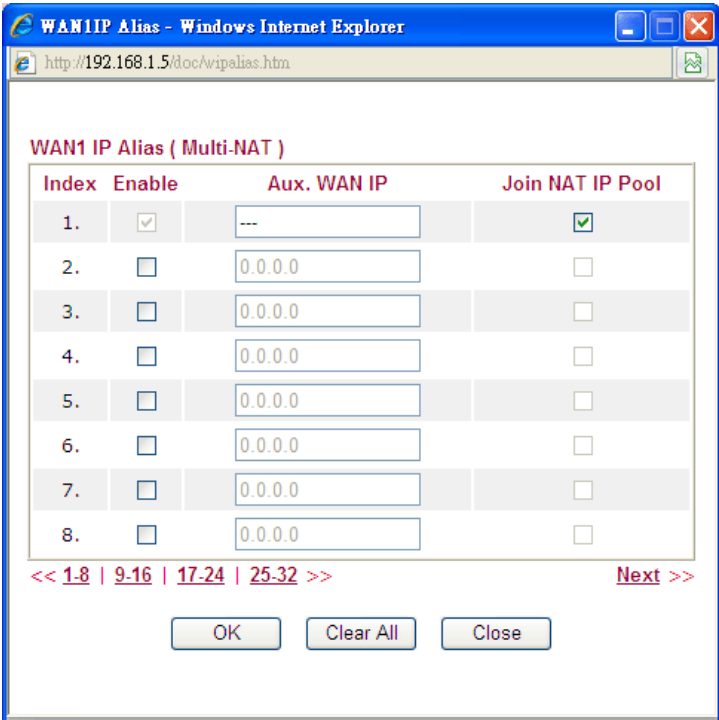
WAN 1

<p>Static or Dynamic IP (DHCP Client) <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/> PING Interval: <input type="text"/> minute(s)</p> <p>WAN Connection Detection Mode: <input type="text" value="ARP Detect"/> Ping IP: <input type="text"/> TTL: <input type="text"/></p> <p>MTU <input type="text" value="1442"/> (Max:1500)</p> <p>RIP Protocol <input type="checkbox"/> Enable RIP</p> <p>Bridge Mode <input type="checkbox"/> Enable Bridge Mode</p>	<p>WAN IP Network Settings <input type="button" value="WAN IP Alias"/></p> <p><input type="radio"/> Obtain an IP address automatically</p> <p>Router Name: <input type="text" value="Vigor"/> *</p> <p>Domain Name: <input type="text"/> *</p> <p><input type="checkbox"/> DHCP Client Identifier *</p> <p>Username: <input type="text"/> Password: <input type="text"/></p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Gateway IP Address: <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address: <input type="text" value="8.8.8.8"/> Secondary IP Address: <input type="text" value="8.8.4.4"/></p> <p><input type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="CE"/> <input type="text" value="46"/> <input type="text" value="FD"/></p>
--	---

*: Required for some ISPs

Available settings are explained as follows:

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.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.

Item	Description
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	If you check this box to invoke the function, the router will work as a bridge. Such function is available only for WAN1.
WAN IP Network Settings	<p>This group allows you to obtain an IP address automatically and allows you type in IP address manually.</p> <p>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.</p>  <p>Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use Dynamic IP mode.</p> <ul style="list-style-type: none"> ● Router Name: Type in the router name provided by ISP. ● Domain Name: Type in the domain name that you have assigned. <p>DHCP Client Identifier for some ISP</p> <ul style="list-style-type: none"> ● Enable: Check the box to specify username and password as the DHCP client identifier for some ISP. ● Username: Type a name as username. The maximum length of the user name you can set is 63 characters. ● Password: Type a password. The maximum length of the password you can set is 62 characters. <p>Specify an IP address – Click this radio button to specify some data if you want to use Static IP mode.</p>

Item	Description
	<ul style="list-style-type: none"> ● IP Address: Type the IP address. ● Subnet Mask: Type the subnet mask. ● Gateway IP Address: Type the gateway IP address. <p>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.</p> <ul style="list-style-type: none"> ● Default MAC Address: Click this radio button to use default MAC address for the router. ● Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a MAC Address and enter the MAC address in the MAC Address field.

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

Details Page for PPTP/L2TP in WAN1 ~ WAN4

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

WAN >> Internet Access

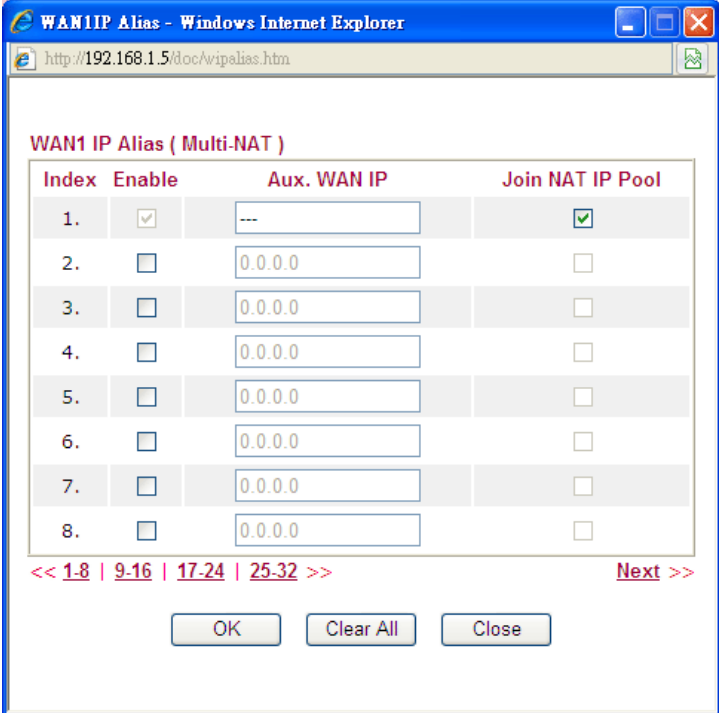
WAN 2

<p>PPTP/L2TP Client Mode</p> <p> <input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable </p> <p>Server Address <input type="text"/></p> <p>Specify Gateway IP Address <input type="text" value="172.16.1.1"/></p>	<p>PPP Setup</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address Assignment Method (IPCP) <input type="text" value="WAN IP Alias"/></p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p> <p>WAN IP Network Settings</p> <p> <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address </p> <p>IP Address <input type="text" value="172.16.3.102"/></p> <p>Subnet Mask <input type="text" value="255.255.0.0"/></p>
<p>ISP Access Setup</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p>	<p>MTU <input type="text" value="1442"/> (Max: 1460)</p>

Available settings are explained as follows:

Item	Description
PPTP/L2TP Client Mode	<p>Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.</p> <p>Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.</p> <p>Disable – Click this radio button to close the connection</p>

Item	Description
	<p>through PPTP or L2TP.</p> <p>Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.</p> <p>Specify Gateway IP Address – Specify the gateway IP address for DHCP server.</p>
ISP Access Setup	<p>Username -Type in the username provided by ISP in this field.</p> <p>Password -Type in the password provided by ISP in this field.</p> <p>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.</p>
MTU	<p>It means Max Transmit Unit for packet. The default setting is 1442.</p>
PPP Setup	<p>PPP Authentication - Select PAP only or PAP or CHAP for PPP.</p> <p>Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.</p>
IP Address Assignment Method(IPCP)	<p>Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.</p> <p>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.</p>

Item	Description
	 <p>Fixed IP - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click Yes to use this function and type in a fixed IP address in the box.</p> <p>Fixed IP Address -Type a fixed IP address.</p>
<p>WAN IP Network Settings</p>	<p>Obtain an IP address automatically – Click this button to obtain the IP address automatically.</p> <p>Specify an IP address – Click this radio button to specify some data.</p> <p>IP Address – Type the IP address.</p> <p>Subnet Mask – Type the subnet mask.</p>

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

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 5

| [Modem Support List](#) |

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

Available settings are explained as follows:

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 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 AT command to restrict 3G band or do any special settings.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
Service Name	Enter the description of the specific network service.
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

Item	Description
	web page.
WAN Connection Detection	<p>Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.</p> <p>Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.</p> <p>Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.</p> <p>TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.</p>
Default	Click it to reset to the factory default setting for 3G connection.

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

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

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

WAN >> Internet Access

WAN 1 IPv6

Internet Access Mode	
Connection Type	Offline <input type="button" value="v"/>

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.

WAN >> Internet Access

WAN 1 IPv6

Internet Access Mode	
Connection Type	PPP <input type="button" value="v"/>
Note : IPv4 WAN setting should be PPPoE client.	

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

Online Status

Physical Connection		System Uptime: 0:0:30	
IPv4	IPv6		
LAN Status			
IP Address			
2001:B010:7300:200:21D:AAFF:FE7A:3E58/64 (Global)			
FE80::21D:AAFF:FE7A:3E58/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
7	8	618	672
WAN2 IPv6 Status			
Enable	Mode	Up Time	
Yes	PPP	0:00:11	
IP		Gateway IP	
2001:B010:7300:200:21D:AAFF:FE7A:3E5A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AAFF:FE7A:3E5A/128 (Link)			
DNS IP			
2001:B000:168::1			
2001:B000:168::2			
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 (<http://gogonet.gogo6.com/page/freenet6-account>) 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.

WAN >> Internet Access

WAN 1 IPv6

Internet Access Mode

Connection Type

TSPC Configuration

Username

Password

Confirm Password

Tunnel Broker

Available settings are explained as follows:

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



WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type		AICCU ▼	
AICCU Configuration			
<input type="checkbox"/> Always On			
Username		<input type="text"/>	
Password		<input type="text"/>	
Confirm Password		<input type="text"/>	
Tunnel Broker		tic.sixxs.net	
Subnet Prefix		<input type="text"/> / <input type="text"/>	
<p>Note: If "Always On" is not enabled, AICCU connection would only retry three times.</p>			
OK		Cancel	

Available settings are explained as follows:

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 http://www.sixxs.net/ . 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.

WAN >> Internet Access



WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6
Internet Access Mode			
Connection Type		DHCPv6 Client	
DHCPv6 Client Configuration			
Identity Association		<input checked="" type="radio"/> Prefix Delegation <input type="radio"/> Non-temporary Address	
IAID (Identity Association ID)		4139321753	
OK		Cancel	

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



WAN 1

PPPoE	Static or Dynamic IP	PPTP	IPv6						
Internet Access Mode									
Connection Type		Static IPv6							
Static IPv6 Address Configuration									
IPv6 Address		/ Prefix Length							
<input type="text"/> / <input type="text"/>		<input type="button" value="Add"/> <input type="button" value="Delete"/>							
Current IPv6 Address Table									
Index		Scope							
<table border="1"> <thead> <tr> <th>Index</th> <th>IPv6 Address/Prefix Length</th> <th>Scope</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>				Index	IPv6 Address/Prefix Length	Scope			
Index	IPv6 Address/Prefix Length	Scope							
Static IPv6 Gateway configuration									
IPv6 Gateway Address		::							
<input type="text"/>		<input type="text"/>							
OK		Cancel							

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.

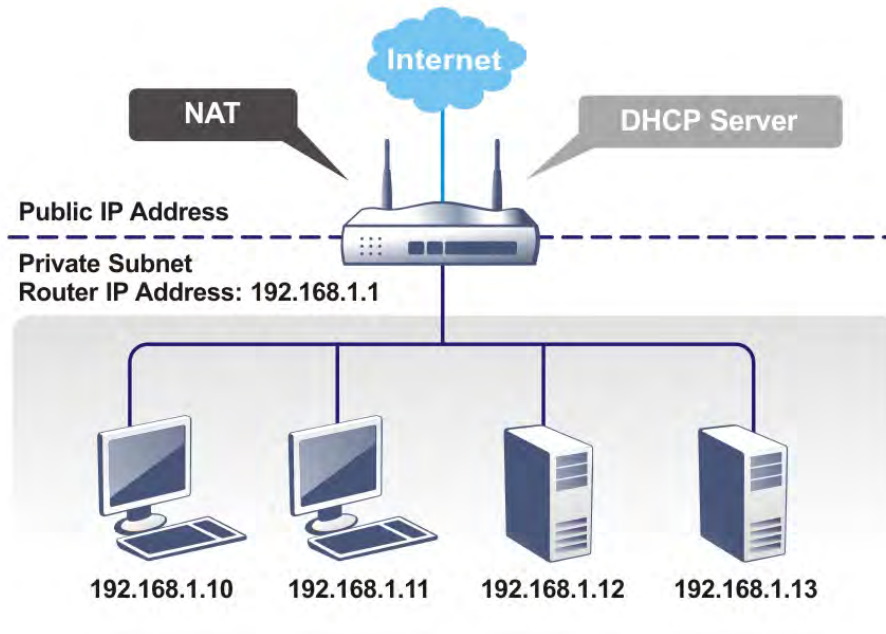
4.2 LAN

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.

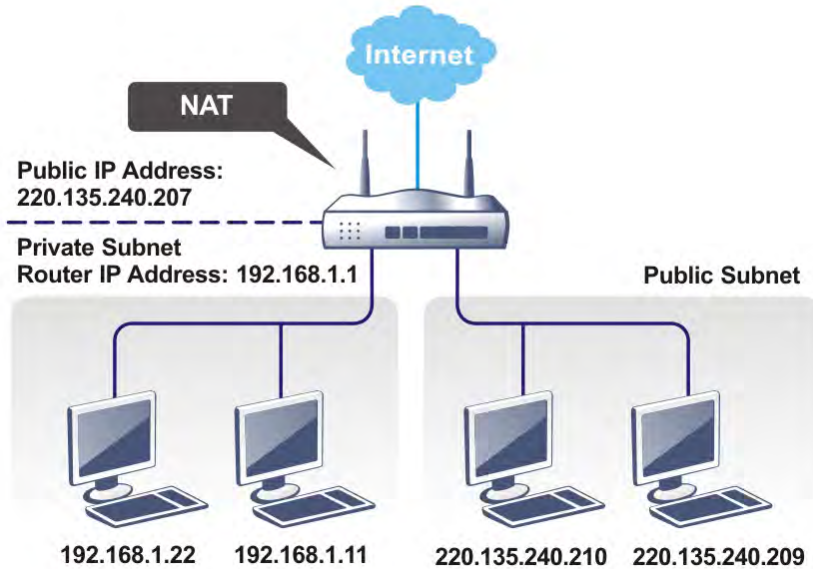
- WAN
- LAN
 - ▶ General Setup
 - ▶ Static Route
 - ▶ VLAN
 - ▶ Bind IP to MAC
 - ▶ LAN Port Mirror
 - ▶ Web Portal Setup
- NAT

4.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

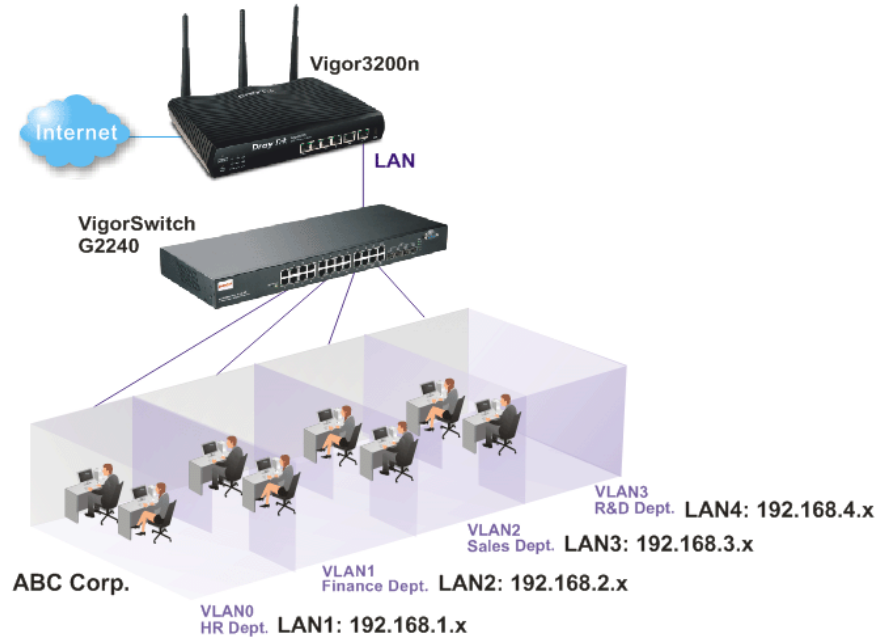
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



4.2.2 General Setup

This page provides you the general settings for LAN. Vigor3200 series provides four LANs, one DMZ and one IP Routed Subnet.

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

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

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.5	Details Page	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	Details Page	
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	
DMZ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	Details Page	
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	Details Page	

[Advanced](#) You can configure DHCP options here.

Force router to use "DNS server IP address" settings specified in [LAN1](#)

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	DMZ PORT
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ PORT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

[OK](#)

[OK](#) [Cancel](#) [Default](#)

Each item is explained as follows:

Item	Description
General Setup-----	<p>Allow to configure settings for each subnet respectively.</p> <p>Index - Display all of the LAN items, DMZ and IP Routed Subnet.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>IPv6 – Click it to access into the settings page of IPv6.</p>
Advanced	DHCP packets can be processed by adding option number

and data information when such function is enabled.

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
<p>Network Configuration</p> <p>For NAT Usage</p> <p>IP Address <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <hr/> <p>RIP Protocol Control <input type="text" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p><input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server</p> <p><input type="checkbox"/> Enable Relay Agent</p> <p>Start IP Address <input type="text" value="192.168.1.10"/></p> <p>IP Pool Counts <input type="text" value="200"/></p> <p>Gateway IP Address <input type="text" value="192.168.1.1"/></p> <p>Lease Time <input type="text" value="86400"/> (s)</p> <p><input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>IP Address - Type in IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>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.</p>
DHCP Server Configuration	<p>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.</p> <p>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.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>Enable Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.</p> <ul style="list-style-type: none"> ● DHCP Server IP Address – It is available when Enable Relay Agent is checked. 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.

Item	Description																
	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.</p> <p>Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).</p>																
<p>DNS Server IP Address</p>	<p>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.</p> <p>Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.</p> <p>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.</p> <p>The default DNS Server IP address can be found via Online Status:</p> <table border="1" data-bbox="678 1854 1441 1951"> <tr> <td colspan="2">System Status</td> <td colspan="2">System Uptime: 71:47</td> </tr> <tr> <td>LAN Status</td> <td>Primary DNS: 194.109.6.66</td> <td colspan="2">Secondary DNS: 168.95.1.1</td> </tr> <tr> <td>IP Address</td> <td>TX Packets</td> <td colspan="2">RX Packets</td> </tr> <tr> <td>192.168.1.1</td> <td>347390</td> <td colspan="2">214004</td> </tr> </table> <p>If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users</p>	System Status		System Uptime: 71:47		LAN Status	Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1		IP Address	TX Packets	RX Packets		192.168.1.1	347390	214004	
System Status		System Uptime: 71:47															
LAN Status	Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1															
IP Address	TX Packets	RX Packets															
192.168.1.1	347390	214004															

Item	Description
	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 **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.

[LAN >> General Setup](#)

Lan 3 Ethernet TCP / IP and DHCP Setup

<p>Network Configuration</p> <p> <input type="radio"/> Enable <input checked="" type="radio"/> Disable <input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage </p> <p>IP Address: <input type="text" value="192.168.3.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p>	<p>DHCP Server Configuration</p> <p> <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server <input type="checkbox"/> Enable Relay Agent </p> <p>Start IP Address: <input type="text" value="192.168.3.10"/></p> <p>IP Pool Counts: <input type="text" value="100"/></p> <p>Gateway IP Address: <input type="text" value="192.168.3.1"/></p> <p>Lease Time: <input type="text" value="259200"/> (s)</p> <p><input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically.</p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address: <input type="text"/></p> <p>Secondary IP Address: <input type="text"/></p>
---	---

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Click Enable to enable such configuration.</p> <p>Click Disable to disable such configuration.</p> <p>For NAT Usage - Click this item to invoke NAT usage.</p> <p>For Routing Usage - Click this item to invoke Routing usage.</p> <p>IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.1.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p>
DHCP Server Configuration	<p>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.</p> <p>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.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>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</p>

must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

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

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

Lease Time - Enter the time to determine how long the IP address assigned by DHCP server can be used.

Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).

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.

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

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

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

Online Status

Physical Connection		System Uptime: 22:22:45	
IPv4		IPv6	
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	
IP Address	TX Packets	RX Packets	
192.168.1.1	0	41533	

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 **OK** to save the configuration.

Details Page for DMZ

DMZ port setting is used for connecting host in DMZ.

[LAN >> General Setup](#)

DMZ Ethernet TCP / IP and DHCP Setup

Network Configuration <input checked="" type="radio"/> For NAT Usage <input type="radio"/> For Routing Usage IP Address: <input type="text" value="192.168.5.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>		DHCP Server Configuration <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server <input type="checkbox"/> Enable Relay Agent Start IP Address: <input type="text" value="192.168.5.10"/> IP Pool Counts: <input type="text" value="100"/> Gateway IP Address: <input type="text" value="192.168.5.1"/> Lease Time: <input type="text" value="259200"/> (s) <input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically.	
		DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/>	

OK

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Set IP address and Subnet Mask for clients connected via DMZ port.</p> <p>For NAT Usage - Click this item to invoke NAT usage.</p> <p>For Routing Usage - Click this item to invoke Routing usage.</p> <p>IP Address - Type in private IP address for connecting to a local private network (Default: 192.168.9.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p>
DHCP Server Configuration	<p>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.</p> <p>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.</p> <p>Enable Server - Let the router assign IP address to every host in the LAN.</p> <p>Disable Server - Let you manually assign IP address to every host in the LAN.</p> <p>Enable Relay Agent - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP</p>

	<p>request to.</p> <ul style="list-style-type: none"> ● DHCP Server IP Address – It is available when Enable Relay Agent is checked. 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. <p>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.</p> <p>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.</p> <p>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.</p> <p>Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.</p> <p>Clear DHCP lease for inactive clients periodically - Whenever a DHCP client requests an IP address from the LAN DHCP server, the server will give out an IP to this client for a certain amount of time (e.g., 1 day). However, even if this client only uses the IP for say 5 minutes, the server still "reserves" 1 day for that client. Because a DHCP server only has a limited number of IPs to lease to its DHCP clients, soon enough all the IPs will be used out and then no one will be able to get any IPs from this server anymore. Therefore, this feature is used to get the IP back from inactive clients (i.e. doesn't use the IP but the server still reserves the IP for him).</p>
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.

IP Routed Subnet

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

LAN >> General Setup

TCP/IP and DHCP Setup for IP Routed Subnet

<p>Network Configuration</p> <p><input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>For Routing Usage</p> <p>IP Address <input type="text" value="192.168.0.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <hr/> <p>RIP Protocol Control <input type="text" value="Disable"/></p>	<p>DHCP Server Configuration</p> <p>Start IP Address <input type="text"/></p> <p>IP Pool Counts <input type="text" value="0"/> (max. 10)</p> <p>Lease Time <input type="text" value="259200"/></p> <p><input type="checkbox"/> Use LAN Port <input checked="" type="checkbox"/> P1</p> <p><input checked="" type="checkbox"/> Use MAC Address</p> <hr/> <table border="1"> <thead> <tr> <th>Index</th> <th>Matched MAC Address</th> <th>given IP Address</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="height: 60px;"></td> </tr> </tbody> </table> <p>MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/></p> <p><input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/></p>	Index	Matched MAC Address	given IP Address			
Index	Matched MAC Address	given IP Address					

Available settings are explained as follows:

Item	Description
Network Configuration	<p>Enable/Disable - Click Enable to enable such configuration; click Disable to disable such configuration.</p> <p>IP Address - Type in IP address for connecting to a local private network (Default: 192.168.0.1).</p> <p>Subnet Mask - Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)</p> <p>RIP Protocol Control –</p> <p>Disable - Deactivate the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)</p> <p>Enable – Trigger the router to exchange the entire routing table with the other nodes in the same subnet by sending/receiving RIP packets.</p>
DHCP Server Configuration	<p>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.</p> <p>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</p>

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

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

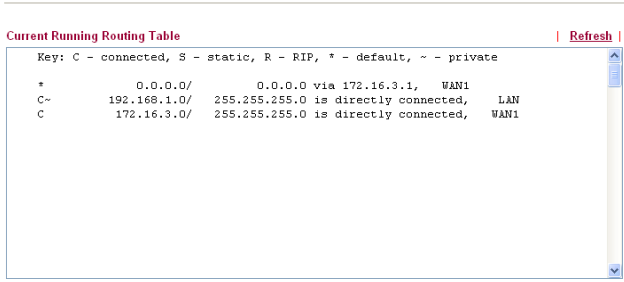
LAN >> Static Route Setup

IPv4			IPv6			Set to Factory Default	View Routing Table
Index	Destination Address	Status	Index	Destination Address	Status		
1.	???	?	6.	???	?		
2.	???	?	7.	???	?		
3.	???	?	8.	???	?		
4.	???	?	9.	???	?		
5.	???	?	10.	???	?		

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	<p>Displays the routing table for your reference.</p> <p>Diagnostics >> View Routing Table</p> 
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](#)

Index No. 1

Enable

Destination IP Address:

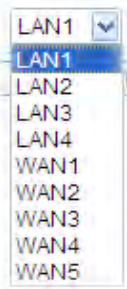
Subnet Mask:

Gateway IP Address:

Network Interface:

Available settings are explained as follows:

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

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:

LAN >> Static Route Setup

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

Index No. 1

Enable

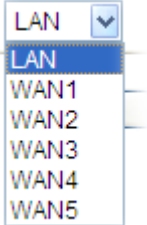
Destination IPv6 Address / Prefix Len: /

Gateway IPv6 Address:

Network Interface:

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.

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. 

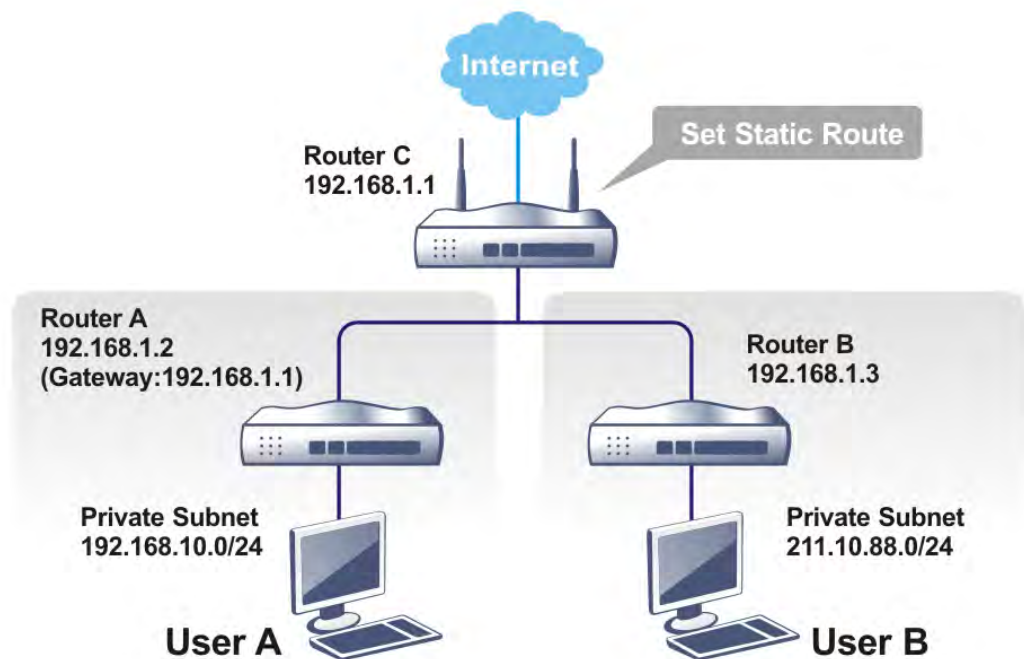
After finishing all the settings here, please click **OK** to save the configuration.

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.

- 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

Index 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

OK Cancel Delete

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

LAN >> Static Route Setup

Index No. 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

OK Cancel Delete

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

Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

Key: C - connected, S - static, R - RIP, * - default, ~ - private

S~	192.168.10.0/	255.255.255.0	via 192.168.1.2,	LAN
C~	192.168.1.0/	255.255.255.0	is directly connected,	LAN
S~	211.100.88.0/	255.255.255.0	via 192.168.1.3,	LAN

4.2.4 VLAN

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

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

LAN >> VLAN Configuration

VLAN Configuration

Enable

	VLAN Tag				Wireless LAN				Subnet
	Enable	VID	Priority	LAN Port	SSID1	SSID2	SSID3	SSID4	
VLAN0	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN1	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN2	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN3	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN4	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN5	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN6	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>
VLAN7	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="LAN 1"/>

Enable management port for P1

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.

OK Clear Cancel

Available settings are explained as follows:

Item	Description
VLAN Tag	<p>Enable – Check the box to enable the function of VLAN with tag.</p> <p>The router will add specific VLAN number to all packets on the LAN while sending them out.</p> <p>Please type the tag value and specify the priority for the packets sending by LAN.</p> <p>VID – Type the value as the VLAN ID number. The range is form 0 to 4095.</p> <p>Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.</p>
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

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

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

[LAN >> Bind IP to MAC](#)

Bind IP to MAC

Enable
 Disable
 Strict Bind

ARP Table	IP Bind List
Select All Sort Refresh	Select All Sort
IP Address Mac Address	Index IP Address Mac Address
192.168.1.5 00-05-5D-E4-D8-EE	

Add or Update

IP Address:

Mac Address:

Comment:

Show Comment

Note: IP-MAC binding presets DHCP Allocations.
If you select Strict Bind, unspecified LAN clients cannot access the Internet.

Available settings are explained as follows:

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 or Update	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 or Update to the table of IP Bind List .
Update	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 Mirror

Port Mirror:
 Enable Disable
Mirror port:
 WAN4
Mirrored port:
 P1 WAN 1 WAN 2 WAN 3

Note :The selected mirror port will only serve debug purposes and should not be used as a part of the LAN.

OK

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

Web Portal Table:

Profile	Status	Interface	
1.	Disable	None	<input type="button" value="Preview"/>
2.	Disable	None	<input type="button" value="Preview"/>
3.	Disable	None	<input type="button" value="Preview"/>
4.	Disable	None	<input type="button" value="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 settings.

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

LAN >> Web Portal Setup

Profile Index: 1

Disable
 URL Redirect
 Message

http://

Force the user to click on the button to proceed
e.g. http://www.draytek.com
Note: If the User Management application is enabled, it will override the Web Portal settings seen here.

```
<h1><font color="red">Vigor</font></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

Available settings are explained as follows:

Item	Description
Disable	Click this button to close this function.
URL Redirect	<p>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.</p> <p>Force the user to click on the button to proceed - Check the box to force the user click the button (with the word defined on Button box) to proceed the operation.</p>
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	<p>Check the box(es) representing different interfaces to be applied by such profile.</p> <p>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.</p>

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

4.3 Load-Balance /Route 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.

Load-Balance/Route Policy



Load-Balance/Route Policy

[Set to Factory Default](#)

Index	Enable	Protocol	Interface	Interface Address	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input type="checkbox"/>	Any	WAN1	---								Down
2	<input type="checkbox"/>	Any	WAN1	---							UP	Down
3	<input type="checkbox"/>	Any	WAN1	---							UP	Down
4	<input type="checkbox"/>	Any	WAN1	---							UP	Down
5	<input type="checkbox"/>	Any	WAN1	---							UP	Down
6	<input type="checkbox"/>	Any	WAN1	---							UP	Down
7	<input type="checkbox"/>	Any	WAN1	---							UP	Down
8	<input type="checkbox"/>	Any	WAN1	---							UP	Down
9	<input type="checkbox"/>	Any	WAN1	---							UP	Down
10	<input type="checkbox"/>	Any	WAN1	---							UP	Down

<< [1-10](#) | [11-20](#) | [21-30](#) | [31-40](#) | [41-50](#) >>

[Next >>](#)

- Wizard Mode: most frequently used settings in three pages
- Advance Mode: all settings in one page

OK

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.
Interface	Display the interface to send packets to once the policy is matched.
Interface Address	Display the WAN IP or WAN IP alias address which is used as source IP of the outgoing packets.
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.
Wizard Mode	Allows to configure frequently used settings of route policy via three setting pages
Advance Mode	Allows to configure detailed settings of route policy.

To use **Wizard Mode**, simple do the following steps:

1. Click the **Wizard Mode** radio button.
2. Click **Index 1**. The setting page will appear as follows:

Load-Balance/Route Policy

Index: 1 Criteria

Load-Balance/Route Policy applies to packets that meet the following criteria

Source IP

Any
 Src IP Start Src IP End
 ~

Destination IP

Any
 Dest IP Start Dest IP End
 ~

Available settings are explained as follows:

Item	Description
Source IP	<p>Any – Any IP can be treated as the source IP.</p> <p>Src IP Start - Type the source IP start for the specified WAN interface.</p> <p>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.</p>
Destination IP	<p>Any – Any IP can be treated as the destination IP.</p> <p>Dest IP Start- Type the destination IP start for the specified WAN interface.</p> <p>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.</p>

3. Click **Next** to get the following page.

Load-Balance/Route Policy

Index: 1 Interface

Load-Balance/Route Policy directs the packets to the interface below

Interface

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Interface	Use the drop down list to choose an interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.

- After specifying the interface, click **Next** to get the following page.

Load-Balance/Route Policy

Index: 1 NAT or Routing

Based on the settings in the previous pages, we guess you want to have: Force NAT

The current setting is:

Force NAT

Force Routing

< Back Next > Finish Cancel

Available settings are explained as follows:

Item	Description
Force NAT /Force Routing	It determines which mechanism that the router will use to forward the packet to WAN.

- After choosing the mechanism, click **Next** to get the summary page for reference.

Load-Balance/Route Policy

Index: 1 Configuration Summary

Criteria

Source IP Any

Destination IP 192.168.1.6 ~ 192.168.1.65

Interface

WAN1

More options

Force NAT

< Back Next > Finish Cancel

- If there is no error, click **Finish** to complete wizard setting.



Index	Enable	Comment	Protocol	Interface	Priority	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input checked="" type="checkbox"/>		Any	WAN1 IP Alias 2	200	Any	Any	192.168.1.6	192.168.1.66	Any	Any		Down
2	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
3	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down
4	<input type="checkbox"/>		Any	WAN1	200	Any	Any	Any	Any	Any	Any	UP	Down

To use **Advance Mode**, do the following steps:

1. Click the **Advance Mode** radio button.
2. Click **Index 2** to access into the following page.

Load-Balance/Route Policy

Index: 1

Enable

Criteria

Protocol Any ▾

Source IP
 Any
 Src IP Start Src IP End
 ~

Destination IP
 Any
 Dest IP Start Dest IP End
 ~

Destination Port
 Any
 Dest Port Start Dest Port End
 ~

Send to if Criteria Matched

Interface WAN1 ▾

Gateway IP
 Default Gateway
 Specific Gateway

More Options

Auto failover to other WAN

Packet Forwarding to WAN via
 Force NAT
 Force Routing

Available settings are 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.
Source IP	<p>Any – Any IP can be treated as the source IP.</p> <p>Src IP Start - Type the source IP start for the specified WAN interface.</p> <p>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.</p>
Destination IP	<p>Any – Any IP can be treated as the destination IP.</p> <p>Dest IP Start- Type the destination IP start for the specified WAN interface.</p> <p>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.</p>
Destination Port	<p>Any – Any port number can be treated as the destination port.</p> <p>Dest Port Start - Type the destination port start for the destination IP.</p> <p>Dest Port End - Type the destination port end for the</p>

	destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.
Send to if criteria matched	<p>Interface – Use the drop down list to choose a WAN or LAN interface or VPN profile. Packets match with the above criteria will be transferred to the interface chosen here.</p> <p>Gateway IP – Specific gateway is used only when you want to forward the packets to the desired gateway. Usually, Default Gateway is selected in default.</p>
More options	<p>Auto failover to other WAN – Check this button to lead the data passing through specific interface (WAN/LAN/VPN/Route Policy) automatically when the selected interface (defined in Send via if criteria matched) is down.</p> <p>Packet Forwarding to WAN via – When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose Force NAT or Force Routing.</p>

3. When you finish the configuration, please click **OK** to save and exit this page.

4.4 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.

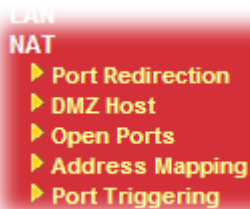
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize 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.

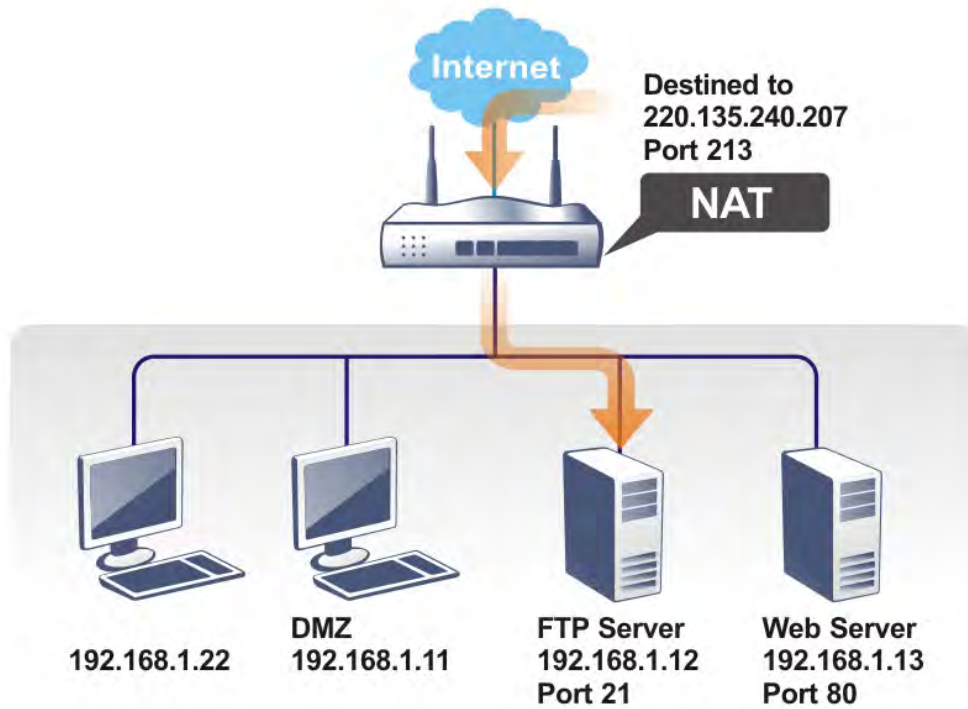
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



4.4.1 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 40 port-mapping entries for the internal hosts.

[NAT >> Port Redirection](#)

Port Redirection						Set to Factory Default
Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
1.		All				x
2.		All				x
3.		All				x
4.		All				x
5.		All				x
6.		All				x
7.		All				x
8.		All				x
9.		All				x
10.		All				x

[<< 1-10 | 11-20 | 21-30 | 31-40 >>](#)

[Next >>](#)

Note: The port number values set in this page might be invalid due to the same values configured for Management Port Setup in [System Maintenance>>Management](#) and [SSL VPN](#).

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.

NAT >> Port Redirection

Index No. 1

<input type="checkbox"/> Enable	
Mode	Single ▾
Service Name	<input type="text"/>
Protocol	--- ▾
WAN Interface	ALL ▾
Public Port	<input type="text" value="0"/>
Private IP	<input type="text"/>
Private Port	<input type="text" value="0"/>

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

OK Clear Cancel

Available settings are explained as follows:

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.

[System Maintenance >> Management](#)

Management Setup

Management Access Control

Allow management from the Internet

FTP Server

HTTP Server

HTTPS Server

Telnet Server

SSH Server

Disable PING from the Internet

Access List

List IP Subnet Mask

Management Port Setup

User Define Ports Default Ports

Telnet Port (Default: 23)

HTTP Port (Default: 80)

HTTPS Port (Default: 443)

FTP Port (Default: 21)

SSH Port (Default: 22)

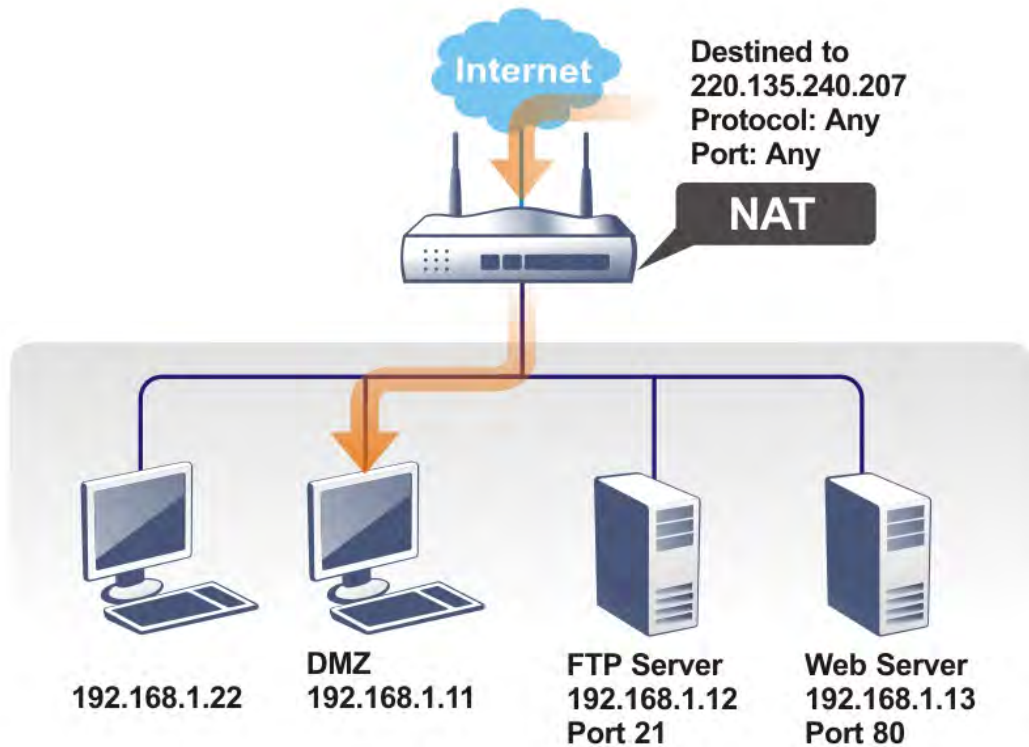
SNMP Setup

Enable SNMP Agent

Get Community

4.4.2 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.


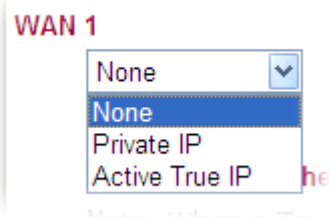
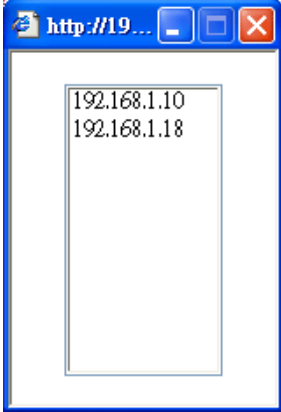
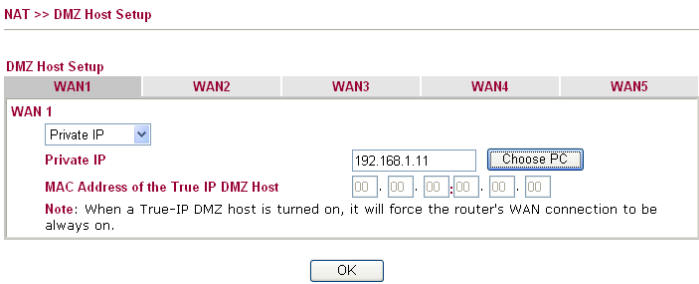
Click **DMZ Host** to open the following page. You can set different DMZ host for each WAN interface. Click the WAN tab to switch into the configuration page for that WAN.

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

WAN1	WAN2	WAN3	WAN4	WAN5
<p>WAN 1</p> <p>None <input type="button" value="v"/></p> <p>Private IP <input type="text"/> <input type="button" value="Choose PC"/></p> <p>MAC Address of the True IP DMZ Host <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/></p> <p>Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.</p>				

Available settings are explained as follows:

Item	Description
<p>WAN 1</p> 	<p>Choose Private IP or Active True IP first. Active True IP selection is available for WAN1 only.</p> 
<p>Private IP</p>	<p>Enter the private IP address of the DMZ host, or click Choose PC to select one.</p>
<p>Choose PC</p>	<p>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.</p>  <p>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.</p> 

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		
<input checked="" type="checkbox"/>		0.0.0.0		Choose PC

OK

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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1	WAN2	WAN3	WAN4	WAN5
WAN 3				
Index	Enable	Aux. WAN IP	Private IP	
1.	<input type="checkbox"/>	172.16.3.102	0.0.0.0	Choose PC
2.	<input type="checkbox"/>	172.16.3.200	0.0.0.0	Choose PC

OK Clear

Available settings are explained as follows:

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.
	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.

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

4.4.3 Open Ports

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

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

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

NAT >> Open Ports

Open Ports Setup						Set to Factory Default
Index	Comment	WAN Interface	Aux. WAN IP	Local IP Address	Status	
1.					X	
2.					X	
3.					X	
4.					X	
5.					X	
6.					X	
7.					X	
8.					X	
9.					X	
10.					X	

<< [1-10](#) | [11-20](#) | [21-30](#) | [31-40](#) >>

[Next](#) >>

Note: The port number values set in this page might be invalid due to the same values configured for Management Port Setup in [System Maintenance>>Management](#) and [SSL VPN](#).

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.
Aux. WAN IP	Display the IP alias setting used by such index. If no IP alias setting exists, such field will not appear.
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.

Index No. 1

<input checked="" type="checkbox"/> Enable Open Ports							
Comment		<input type="text" value="P2P"/>					
WAN Interface		<input type="text" value="WAN1"/>					
Local Computer		<input type="text" value="192.168.1.10"/>	<input type="button" value="Choose PC"/>				
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	6.	-----	0	0
2.	UDP	4500	4700	7.	-----	0	0
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.

4.4.4 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 Triggering						Set to Factory Default
Index	Comment	Triggering Protocol	Triggering Port	Incoming Protocol	Incoming Port	Status
1.						x
2.						x
3.						x
4.						x
5.						x
6.						x
7.						x
8.						x
9.						x
10.						x

[<< 1-10](#) | [11-20 >>](#)

[Next >>](#)

Available settings are explained as follows:

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.

Click the index number link to open the configuration page.

No. 1

Enable

Service User Defined ▾

Comment

Triggering Protocol --- ▾

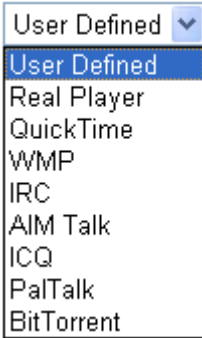

Triggering Port


Incoming Protocol --- ▾

Incoming Port

Note: The Triggering Port and Incoming Port should be input like this :
 123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).

Available settings are explained as follows:

Item	Description
Enable	Check to enable this entry.
Service	Choose the predefined service to apply for such trigger profile. 
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.

	
Incoming Port	Type the port or port range for the incoming packets.

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

4.5 Firewall

4.5.1 Basics for Firewall

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

Firewall Facilities

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

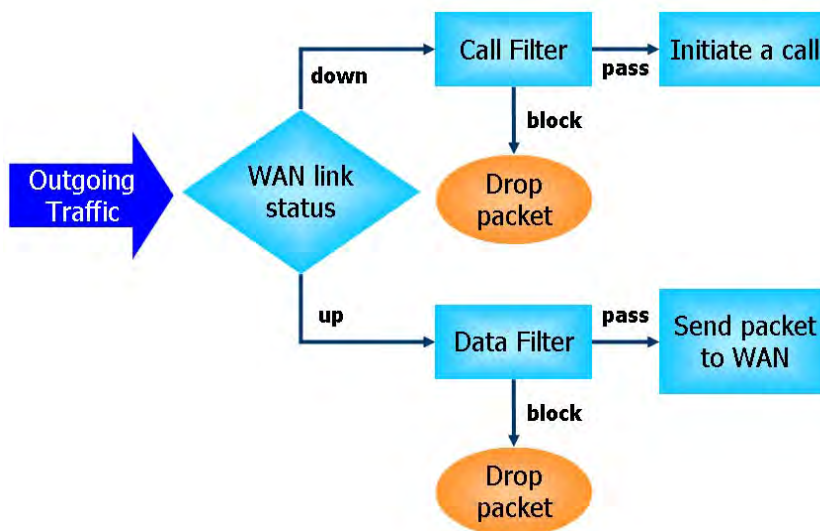
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

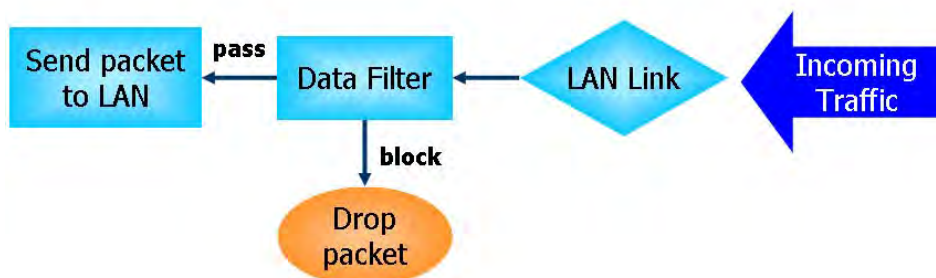
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

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

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

- | | |
|----------------------|--------------------------|
| 1. SYN flood attack | 9. SYN fragment |
| 2. UDP flood attack | 10. Fraggle attack |
| 3. ICMP flood attack | 11. TCP flag scan |
| 4. Port Scan attack | 12. Tear drop attack |
| 5. IP options | 13. Ping of Death attack |
| 6. Land attack | 14. ICMP fragment |
| 7. Smurf attack | 15. Unknown protocol |
| 8. Trace route | |

Below shows the menu items for Firewall.



4.5.2 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

General Setup

General Setup
Default Rule

Call Filter Enable Start Filter Set:

Disable

Data Filter Enable Start Filter Set:

Disable

Accept large incoming fragmented UDP or ICMP packets (used in some games and streaming)

Enable Strict Security Firewall

Block routing packet from WAN

IPv4 IPv6

Note: The packets will be filtered by the following firewall functions sequentially:

1. Data Filter Sets and Rules
2. Block routing packets from WAN
3. Default Rule

Available settings are explained as follows:

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 ”.

<p>Enable Strict Security Firewall</p>	<p>For the sake of security, the router will execute strict security checking for data transmission.</p> <p>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.</p>
<p>Block routing packet from WAN</p>	<p>Usually, IPv6 network sessions/traffic from WAN to LAN will be accepted by IPv6 firewall in default.</p> <p>IPv6 - To prevent remote client accessing into the PCs on LAN, check the box to make the packets (routed from WAN to LAN) via IPv6 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.</p> <p>IPv4 - To prevent remote client accessing into the PCs on LAN, check the box to make the incoming packets via IPv4 being blocked by such router. It is effective only for the packets routed but not for packets translated by NAT.</p>

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

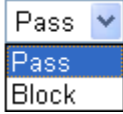
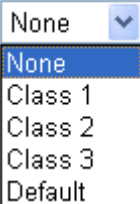
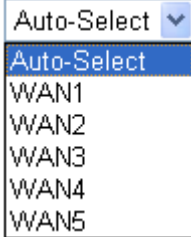
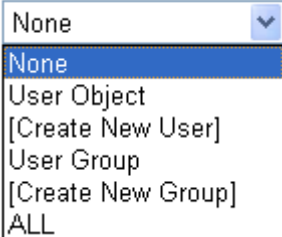
General Setup
Default Rule

Actions for default rule:	Action/Profile	Syslog
Application		
Filter	Pass <input type="button" value="v"/>	<input type="checkbox"/>
Sessions Control	30 / <input type="text" value="120000"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
Load-Balance policy	Auto-Select <input type="button" value="v"/>	<input type="checkbox"/>
User Management	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>

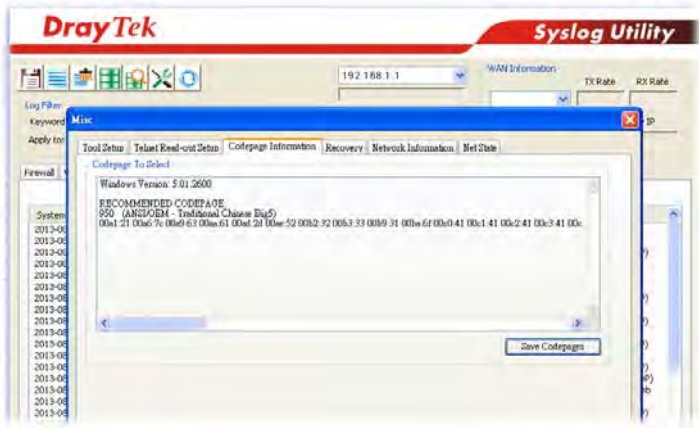
Advance Setting

Available settings are explained as follows:

Item	Description
------	-------------

Item	Description
Filter	<p>Select Pass or Block for the packets that do not match with the filter rules.</p> <p>Filter </p>
Sessions Control	<p>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.</p>
Quality of Service	<p>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.</p> 
Load-Balance Policy	<p>Choose the WAN interface for applying Load-Balance Policy.</p> 
User Management	<p>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.</p>  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>
APP Enforcement	<p>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</p>

Item	Description
	section Syslog/Mail Alert for more detailed information.
URL Content Filter	<p>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.</p>
Web Content Filter	<p>Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.</p>
Advance Setting	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p> <p>Firewall >> General Setup</p> <hr/> <div data-bbox="692 1093 1382 1223" style="border: 1px solid gray; padding: 5px;"> <p>Advance Setting</p> <p>Codepage: <input type="text" value="ANSI(1252)-Latin I"/></p> <p>Window size: <input type="text" value="65535"/></p> <p>Session timeout: <input type="text" value="1440"/> Minute</p> </div> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </p> <p>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.</p>

Item	Description
	 <p>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.</p> <p>Session timeout – Setting timeout for sessions can make the best utilization of network resources.</p>

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

4.5.3 Filter Setup

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

Firewall >> Filter Setup

Filter Setup		Set to Factory Default	
Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

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.

Filter Set 1

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios		Down
<input type="button" value="2"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="3"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="4"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="5"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="6"/>	<input type="checkbox"/>		UP	Down
<input type="button" value="7"/>	<input type="checkbox"/>		UP	

Next Filter Set

Available settings are explained as follows:

Item	Description
Filter Rule	Click a button numbered (1 ~ 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.

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments:

Index(1-15) in [Schedule](#) Setup: , , ,

Clear sessions when schedule ON: Enable

Direction:

Source IP:

Destination IP:

Service Type:

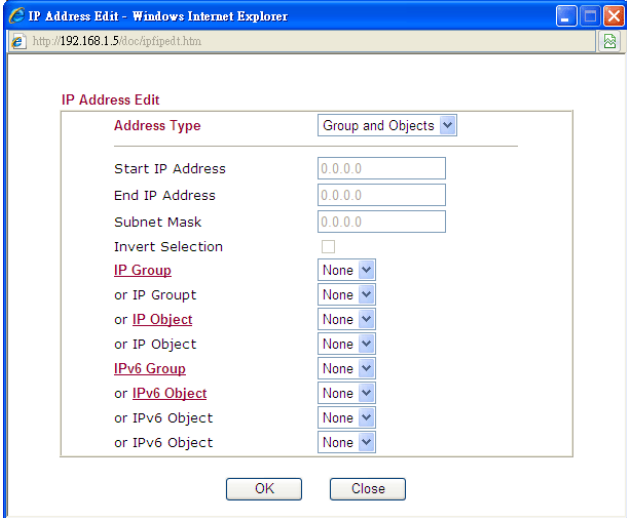
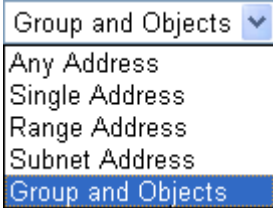
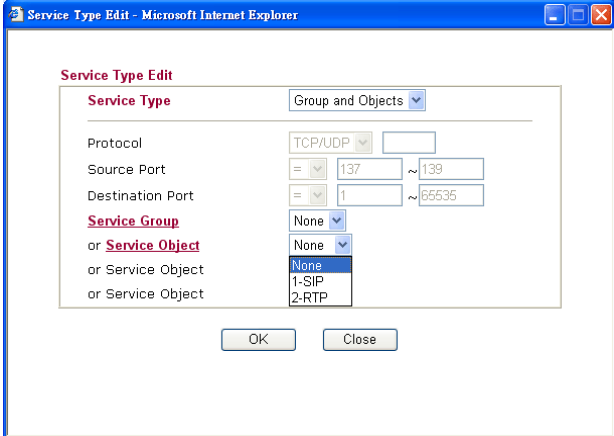
Fragments:

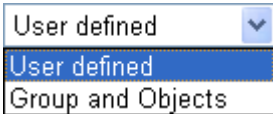
Application	Action/Profile	Syslog
Filter:	<input type="text" value="Block Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	0 / <input type="text" value="120000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
User Management	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement:	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter:	<input type="text" value="None"/>	<input type="checkbox"/>
Web Content Filter:	<input type="text" value="None"/>	<input type="checkbox"/>

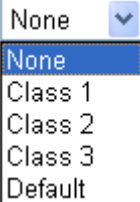
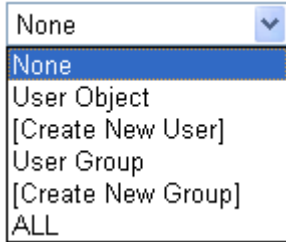
Advance Setting

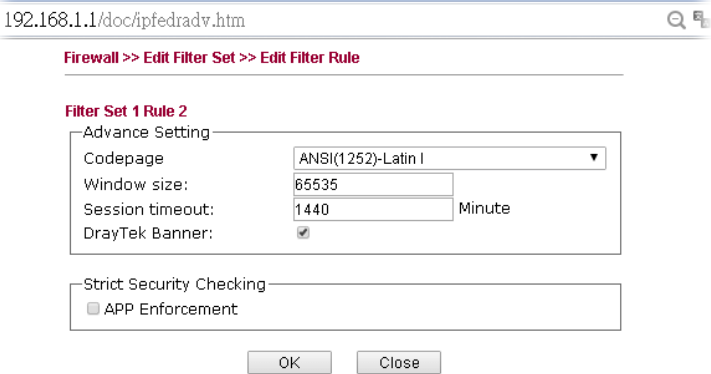
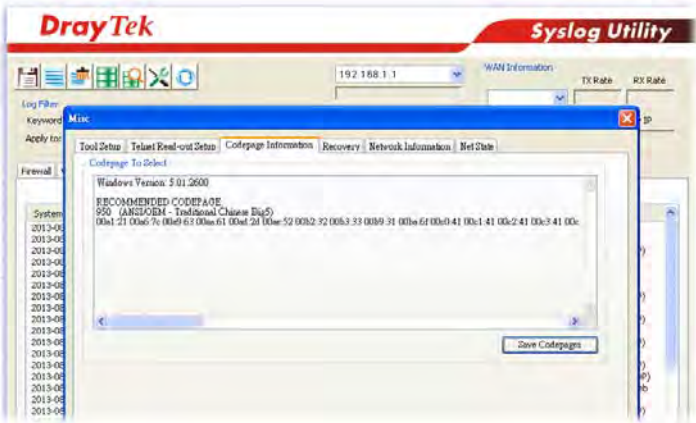
Available settings are explained as follows:

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 default setting of this field is blank and the function will always work.
Clear sessions when schedule ON	Check this box to clear all the sessions when the schedule is configured and specified above.
Direction	<p>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.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <input type="text" value="LAN/RT/VPN -> WAN"/> <ul style="list-style-type: none"> LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN </div> <p>Note: RT means routing domain for 2nd subnet.</p>

Item	Description
<p>Source/Destination IP</p>	<p>Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.</p>  <p>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.</p>  <p>From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want.</p>
<p>Service Type</p>	<p>Click Edit to access into the following dialog to choose a suitable service type.</p>  <p>To set the service type manually, please choose User defined as the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose Group and Objects as the Service</p>

Item	Description
	<p>Type.</p>  <p>Protocol - Specify the protocol(s) which this filter rule will apply to.</p> <p>Source/Destination Port –</p> <p>(=) – 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.</p> <p>(! =) – 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.</p> <p>(>) – the port number greater than this value is available.</p> <p>(<) – the port number less than this value is available for this profile.</p> <p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
Fragments	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p><i>Don't care</i> -No action will be taken towards fragmented packets.</p> <p><i>Unfragmented</i> -Apply the rule to unfragmented packets.</p> <p><i>Fragmented</i> - Apply the rule to fragmented packets.</p> <p><i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.</p>
Filter	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p>
Branch to other Filter Set	<p>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.</p>
Sessions Control	<p>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.</p>
MAC Bind IP	<p>Strict – Make the MAC address and IP address settings</p>

Item	Description
	<p>configured in IP Object for Source IP and Destination IP be bound for applying such filter rule.</p> <p>No-Strict - no limitation.</p>
<p>Quality of Service</p>	<p>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.</p> 
<p>Load-Balance policy</p>	<p>Choose the WAN interface for applying Load-Balance Policy.</p>
<p>User Management</p>	<p>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.</p>  <p>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.</p>
<p>APP Enforcement</p>	<p>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.</p>
<p>URL Content Filter</p>	<p>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.</p>
<p>Web Content Filter</p>	<p>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</p>

Item	Description
	<p>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.</p>
<p>Advance Setting</p>	<p>Click Edit to open the following window. However, it is strongly recommended to use the default settings here.</p>  <p>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.</p>  <p>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.</p> <p>Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is</p>

Item	Description
	<p>configured for the data flow which matched with the firewall rule.</p> <p>DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.</p> <div data-bbox="678 430 1385 723" style="border: 1px solid blue; padding: 10px; text-align: center;"> <p>The requested Web page has been blocked by Web Content Filter.</p> <p>Please contact your system administrator for further information.</p> <p>[Powered by Draytek]</p> </div> <p>Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.</p> <p>APP Enforcement – Check this box to execute the critical checking for all the files transferred via IM/P2P.</p>

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.

4.5.4 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

Enable DoS Defense

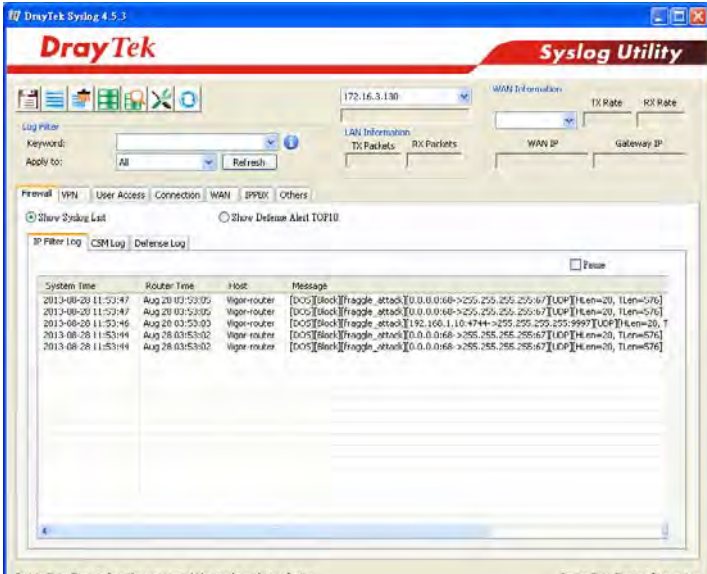
<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="2000"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="250"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="2000"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unassigned Numbers		
<input type="checkbox"/> Block Fraggle Attack			

Available settings are explained as follows:

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	<p>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.</p> <p>By default, the threshold and timeout values are set to 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.</p>

Item	Description
Enable UDP flood defense	<p>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.</p> <p>The default setting for threshold and timeout are 2000 packets per second and 10 seconds, respectively. That means, when 2000 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable ICMP flood defense	<p>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.</p> <p>The default setting for threshold and timeout are 250 packets per second and 10 seconds, respectively. That means, when 250 packets per second received, they will be regarded as “attack event” and the session will be paused for 10 seconds.</p>
Enable PortScan detection	<p>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.</p> <p>By default, the Vigor router sets the threshold as 2000 packets per second. That means, when 2000 packets per second received, they will be regarded as “attack event”.</p>
Block IP options	<p>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 messages...etc. An eavesdropper outside might learn the details of your private networks.</p>
Block Land	<p>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.</p>
Block Smurf	<p>Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.</p>
Block trace router	<p>Check the box to enforce the Vigor router not to forward any trace route packets.</p>
Block SYN fragment	<p>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.</p>

Item	Description
Block Fraggle Attack	<p>Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked.</p> <p>Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.</p>
Block TCP flag scan	<p>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>.</p>
Block Tear Drop	<p>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.</p>
Block Ping of Death	<p>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.</p>
Block ICMP Fragment	<p>Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.</p>
Block Unassigned Numbers	<p>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.</p>
Warning Messages	<p>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.</p> <p>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.</p>

Item	Description
	<p data-bbox="691 248 1002 271">System Maintenance >> SysLog / Mail Alert Setup</p> <div data-bbox="691 302 1380 627"> <p>SysLog / Mail Alert Setup</p> <p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Server IP Address: <input type="text"/></p> <p>Destination Port: <input type="text" value="514"/></p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server: <input type="text"/></p> <p>Mail To: <input type="text"/></p> <p>Return-Path: <input type="text"/></p> <p><input type="checkbox"/> Authentication</p> <p>User Name: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input type="button" value="OK"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/></p> </div>  <p data-bbox="691 1216 991 1229">System Time: Time tag from the computer which runs the syslog application</p> <p data-bbox="1236 1216 1374 1229">Router Time: Time tag from router</p>

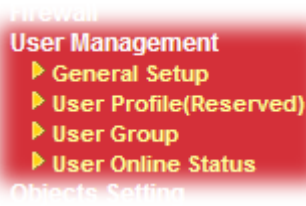
After finishing all the settings here, please click **OK** to save the configuration.

4.6 User Management

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

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

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



4.6.1 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.

User Management >> General Setup

General Setup

Mode:

Web Authentication:


Notice :

1. User Management will refer to active rules in Data Filter as whitelists and blacklists in user-based firewall mode.
2. Users match the above lists will not be required for authentication. The firewall rules policy will still valid.
3. Otherwise, authentication required for users not matched the above lists. The firewall rules designated in the user profile's policy will still valid.

Landing Page (Max 255 characters) [Preview](#) | [Set to Factory Default](#) |

```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

Available settings are explained as follows:

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

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

4.6.2 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)**.

User Management >> User Profile(Reserved)

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> [Next](#) >>

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

Username

Password

Confirm Password

Idle Timeout min(s) 0:Unlimited

Max User Login 0:Unlimited

External Server Authentication

Log

Pop Browser Tracking Window

Authentication Web Alert Tool Telnet

Landing Page

Index(1-15) in **Schedule** Setup: , , ,

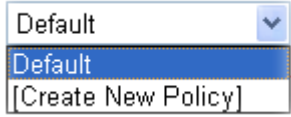
Enable Time Quota 0 min. 0 min.

Enable Data Quota 0 MB 0 MB

Reset quota to default when scheduling time expired

Enable Default Time Quota 0 min. Default Data Quota 0 MB

Available settings are explained as follows:

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.
Policy	<p>It is available only when User-Based mode selected in User Management>>General Setup.</p>  <p>Default – If you choose such item, the filter rules pre-configured in Firewall can be adopted for such user profile.</p> <p>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.</p>

Item	Description
	<p>Firewall >> Edit Filter Set >> Edit Filter Rule</p> <hr/> <p>Filter Set 1 Rule 2</p> <div data-bbox="715 376 1380 638"> <p>Comments: <input type="text"/></p> <p>Index(1-15) in Schedule Setup: <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <hr/> <p>Direction: <input type="text" value="LAN/RT/VPN -> WAN"/></p> <p>Source IP: <input type="text" value="Any"/></p> <p>Destination IP: <input type="text" value="Any"/></p> <p>Service Type: <input type="text" value="Any"/></p> <p>Fragments: <input type="text" value="Don't Care"/></p> </div> <p>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.</p>
<p>External Service Authentication</p>	<p>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.</p> <div data-bbox="683 943 817 1086"> <p><input type="text" value="None"/></p> <ul style="list-style-type: none"> <input type="text" value="None"/> <input type="text" value="LDAP"/> <input type="text" value="Radius"/> </div>
<p>Log</p>	<p>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).</p> <div data-bbox="683 1211 801 1391"> <p><input type="text" value="None"/></p> <ul style="list-style-type: none"> <input type="text" value="None"/> <input type="text" value="Login"/> <input type="text" value="Event"/> <input type="text" value="All"/> </div>
<p>Pop Browser Tracking Window</p>	<p>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.</p>
<p>Authentication</p>	<p>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.</p> <p>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.</p> <p>Alert Tool – If it is selected, the user can open Alert Tool and</p>

Item	Description
	<p>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.</p> <p>Telnet – If it is selected, the user can use Telnet command to perform the authentication job.</p>
Landing Page	<p>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.</p> <p>Check this box to enable such function.</p>
Index (1-15) in Schedule Setup	<p>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.</p>
Enable Time Quota	<p>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.</p> <p><input type="checkbox"/> + – Click this box to set and increase the time quota for such profile.</p> <p><input type="checkbox"/> - – Click this box to decrease the time quota for such profile.</p>
Enable Data Quota	<p>Data Quota means the total amount for data transmission allowed for the user. The unit is MB.</p> <p><input type="checkbox"/> + – Click this box to set and increase the data quota for such profile.</p> <p><input type="checkbox"/> - – Click this box to decrease the data quota for such profile.</p>
Reset quota to default when scheduling time expired	<p>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.</p> <p>Enable – Check it to use the default setting for time quota and data quota.</p> <p>Default Time Quota – Type the value for the time manually.</p> <p>Default Data Quota – Type the value for the data manually.</p>

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

4.6.3 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
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

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

User Management >> User Group

Profile Index : 1

Name:

Available User Objects

1-admin
2-Dial-In User

Selected User Objects(Max 32 Objects)

(Empty)

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 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 <input type="button" value="»"/> button to add the selected user objects in this box.

4.7 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).



4.7.1 IP Object

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

Objects Setting >> IP Object

IP Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >> [Next](#) >>

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 >> IP Object

IP Object Profiles:

Index	Name	Ind
1.		1
2.		1
3.		1

2. The configuration page will be shown as follows:

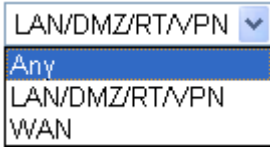
Objects Setting >> IP Object

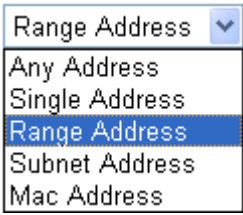
Profile Index : 11

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:	<input type="checkbox"/>

OK Clear Cancel

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	<p>Choose a proper interface.</p>  <p>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 addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page.</p>
Address Type	<p>Determine the address type for the IP address.</p> <p>Select Single Address if this object contains one IP address only.</p> <p>Select Range Address if this object contains several IPs within a range.</p> <p>Select Subnet Address if this object contains one subnet for IP address.</p>

Item	Description
	Select Any Address if this object contains any IP address. Select Mac Address if this object contains 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.

- 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>

4.7.2 IP Group

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

[Objects Setting >> IP Group](#)

IP Group Table: [Set to Factory Default](#)

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

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
1.		1
2.		1
3.		1

- The configuration page will be shown as follows:

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface:

Available IP Objects

1-RD Department
2-Financial Dept.
3-HR Department

>>
<<

Selected IP Objects

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.

- 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>	

4.7.3 IPv6 Object

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

[Objects Setting >> IPv6 Object](#)

IPv6 Object Profiles: [Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) >> [Next](#) >>

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
1.	
2.	
3.	

- The configuration page will be shown as follows:

Objects Setting >> IPv6 Object

Profile Index : 1

Name:	<input type="text"/>
Address Type:	Subnet Address <input type="button" value="v"/>
Mac Address:	<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/>
Start IP Address:	<input type="text"/>
End IP Address:	<input type="text"/>
Prefix Len:	<input type="text"/>
Invert Selection:	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Address Type	<p>Determine the address type for the IPv6 address.</p> <p>Select Single Address if this object contains one IPv6 address only.</p> <p>Select Range Address if this object contains several IPv6s within a range.</p> <p>Select Subnet Address if this object contains one subnet for IPv6 address.</p> <p>Select Any Address if this object contains any IPv6 address.</p> <p>Select Mac Address if this object contains Mac address.</p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Range Address <input type="button" value="v"/> Any Address Single Address Range Address Subnet Address Mac Address </div>
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.

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

4.7.4 IPv6 Group

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

[Objects Setting >> IP Group](#)

IPv6 Group Table: [Set to Factory Default](#)

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

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
1.	
2.	

- The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Profile Index : 1

Name:

Available IPv6 Objects

1-v6_ob_1

>>

<<

Selected IPv6 Objects

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.

- 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
1.	v6_group1	17.	
2.		18.	
3.		19.	
4.		20.	

4.7.5 Service Type Object

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

[Objects Setting >> Service Type Object](#)

Service Type Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) >> [Next](#) >>

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.	

- The configuration page will be shown as follows:

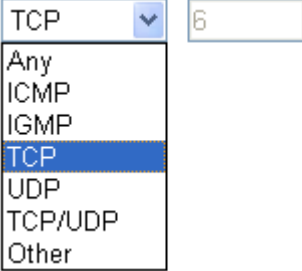
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	<input type="text" value="WWW"/>		
Protocol	TCP	6	
Source Port	=	1	~ 65535
Destination Port	=	80	~ 80

OK Clear Cancel

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. 
Source/Destination Port	<p>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.</p> <p>(=) – 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.</p> <p>(!=) – 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.</p> <p>(>) – the port number greater than this value is available.</p> <p>(<) – the port number less than this value is available for this profile.</p>

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

Service Type Object Profiles:

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

4.7.6 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
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

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.	
2.	
3.	

- The configuration page will be shown as follows:

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name:

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

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 Objects Setting>>Service Type Object will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

- 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>	

4.7.7 Keyword Object

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

[Objects Setting >> Keyword Object](#)

Keyword Object Profiles: [Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> [Next](#) >>

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.	

2. The configuration page will be shown as follows:

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	<input type="text"/>
Contents	<input type="text"/>

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 Profiles: [Set to Factory Default](#)

Index	Name	Index	Name
1.	Keyword-1	17.	
2.	Keyword-2	18.	
3.		19.	

4.7.8 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**.

[Objects Setting >> Keyword Group](#)

Keyword Group Table: | [Set to Factory Default](#) |

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

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
1.	
2.	
3.	
4.	

- The configuration page will be shown as follows:

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects

1-Keyword-1
2-keyword-2

Selected Keyword Objects(Max 16 Objects)

Available settings are explained as follows:

Item	Description
Name	Type a name for this group.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click <input type="button" value="»"/> button to add the selected Keyword objects in this box.

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

Objects Setting >> Keyword Group

Keyword Group Table: | [Set to Factory Default](#) |

Index	Name	Index	Name
1.	night	17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	

4.7.9 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.

[Objects Setting >> File Extension Object](#)

File Extension Object Profiles: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

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
1.	
2.	

- The configuration page will be shown as follows:

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrml
Compression <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .ace <input type="checkbox"/> .arj <input type="checkbox"/> .bzip2 <input type="checkbox"/> .bz2 <input type="checkbox"/> .cab <input type="checkbox"/> .gz <input type="checkbox"/> .gzip <input type="checkbox"/> .rar <input type="checkbox"/> .sit <input type="checkbox"/> .zip
Execution <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bas <input type="checkbox"/> .bat <input type="checkbox"/> .com <input type="checkbox"/> .exe <input type="checkbox"/> .inf <input type="checkbox"/> .pif <input type="checkbox"/> .reg <input type="checkbox"/> .scr

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile.

- Type a name for such profile and check all the items of file extension that will be processed in the router.
- After finishing all the settings here, please click **OK** to save the configuration.

Objects Setting >> File Extension Object

File Extension Object Profiles: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.	game	5.	
2.		6.	
3.		7.	
4.		8.	

4.7.10 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**.

[Object Settings >> SMS / Mail Service Object](#)

SMS Provider		Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider	
1.		kotsms.com.tw (TW)	
2.		kotsms.com.tw (TW)	
3.		kotsms.com.tw (TW)	
4.		kotsms.com.tw (TW)	
5.		kotsms.com.tw (TW)	
6.		kotsms.com.tw (TW)	
7.		kotsms.com.tw (TW)	
8.		kotsms.com.tw (TW)	
9.	Custom 1		
10.	Custom 2		

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.		
2.		
3.		

- The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text" value="Line_down"/>
Service Provider	<input type="text" value="kotsms.com.tw (TW)"/>
Username	<input type="text" value="line1"/>
Password	<input type="password" value="****"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

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.

- 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
1.	Line_down	kotsms.com.tw (TW)
2.		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.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server	Set to Factory Default
Index	Profile Name	SMS Provider
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

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	<input type="text" value="Custom 1"/>
Service Provider	<input type="text"/>
<div style="border: 1px solid black; height: 40px; width: 100%;"></div>	
<p>Please contact with your SMS provide to get the exact URL String eg: bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username=###txtUser###&password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###</p>	
Username	<input type="text"/>
Password	<input type="text"/>
Quota	<input type="text" value="10"/>
Sending Interval	<input type="text" value="3"/> (seconds)

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. Note: 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 Provider		Mail Server		Set to Factory Default	
Index		Profile Name			
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

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.

Object Settings >> SMS / Mail Service Object

SMS Provider	Mail Server
Index	Prf
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

2. The configuration page will be shown as follows:

Object Settings >> SMS / Mail Service Object

Profile Index: 1

Profile Name	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Port	<input type="text" value="0"/>
Sender Address	<input type="text"/>
<input type="checkbox"/> Use SSL	
<input type="checkbox"/> Authentication	
Username	<input type="text"/>
Password	<input type="text"/>
Sending Interval	<input type="text" value="0"/> (seconds)

OK Clear Cancel

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.
Use SSL	Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.
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.

- 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			
1.		Mail_Notify			
2.					
3.					
4.					

4.7.11 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		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

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:

- 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
1.	
2.	
3.	
4.	

- The configuration page will be shown as follows:

Object Settings >> Notification Object

Profile Index: 1

Profile Name	Notify_attack	
Category	Status	
WAN	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> Reconnected
VPN Tunnel	<input checked="" type="checkbox"/> Disconnected	<input checked="" type="checkbox"/> 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.

- 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>		

4.8 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 misuse 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.

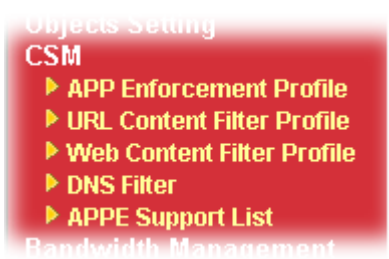
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from 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.
--



4.8.1 APP Enforcement Profile

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

CSM >> APP Enforcement Profile

APP Enforcement Profile Table:

[Set to Factory Default](#)

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

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**.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	PROTOCOL	OTHERS
Select All	Clear All	Support List	
Advanced Management			
Activity / Application	MSN	YahooIM	AIM(<= v5.9) ICQ
Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Message	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File Transfer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Game	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conference(Video/Voice)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IM Application			VoIP
<input type="checkbox"/> AIM6/7	<input type="checkbox"/> QQ/TM	<input type="checkbox"/> iMessge	<input type="checkbox"/> Jabber/GoogleTalk
<input type="checkbox"/> GoogleChat	<input type="checkbox"/> XFire	<input type="checkbox"/> GaduGadu	<input type="checkbox"/> Paltalk
<input type="checkbox"/> Qnext	<input type="checkbox"/> POCO/PP365	<input type="checkbox"/> AresChat	<input type="checkbox"/> AliWW
<input type="checkbox"/> KC	<input type="checkbox"/> Lava-Lava	<input type="checkbox"/> ICU2	<input type="checkbox"/> iSpQ
<input type="checkbox"/> UC	<input type="checkbox"/> MobileMSN	<input type="checkbox"/> BaiduHi	<input type="checkbox"/> Fetion
<input type="checkbox"/> LINE			
Web IM (* = more than one address)			
<input type="checkbox"/> WebIM URLs	eMessenger	WebMSN	meebo*
	ICQ Flash*	mabber*	MSN2GO*
			eBuddy
			MessengerFX*
			iLoveIM*
			ICQ Java*
			MessengerAdictos
			WebYahooIM

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**.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM	P2P	PROTOCOL	OTHERS
Select All	Clear All	Support List	
Protocol		Applications	
<input type="checkbox"/> SoulSeek		SoulSeek	
<input type="checkbox"/> eDonkey		eDonkey, eMule, Shareaza	
<input type="checkbox"/> FastTrack		KazaA, BearShare, iMesh	
<input type="checkbox"/> OpenFT		KCeasy, FilePipe	
<input type="checkbox"/> Gnutella		BearShare, Limewire, Shareaza, Foxy, KCeasy	
<input type="checkbox"/> OpenNap		Lopster, XNap, WinLop	
<input type="checkbox"/> BitTorrent		BitTorrent, BitSpirit, BitComet	
Other P2P Applications			
<input type="checkbox"/> Xunlei	<input type="checkbox"/> Vagaa	<input type="checkbox"/> PP365	<input type="checkbox"/> POCO
<input type="checkbox"/> Ares	<input type="checkbox"/> ezPeer	<input type="checkbox"/> Pando	<input type="checkbox"/> Huntmine
<input type="checkbox"/> Spotify			<input type="checkbox"/> Clubbox
			<input type="checkbox"/> Kuwo

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

Profile Index : 1 Profile Name:

IM		P2P		PROTOCOL	OTHERS	
Select All	Clear All	Support List				Action : <input type="text" value="Block"/>
Protocol						
<input type="checkbox"/> DNS	<input type="checkbox"/> FTP	<input type="checkbox"/> HTTP	<input type="checkbox"/> IMAP	<input type="checkbox"/> IRC		
<input type="checkbox"/> NNTP	<input type="checkbox"/> POP3	<input type="checkbox"/> SMB	<input type="checkbox"/> SMTP	<input type="checkbox"/> SNMP		
<input type="checkbox"/> SSH	<input type="checkbox"/> SSL/TLS	<input type="checkbox"/> TELNET	<input type="checkbox"/> MSSQL	<input type="checkbox"/> MySQL		
<input type="checkbox"/> Oracle	<input type="checkbox"/> PostgreSQL	<input type="checkbox"/> Sybase	<input type="checkbox"/> DB2	<input type="checkbox"/> Informix		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

The items categorized under **Others**.

CSM >> APP Enforcement Profile

Profile Index : 1 Profile Name:

IM		P2P		PROTOCOL	OTHERS
Select All	Clear All	Support List			
Tunneling					
<input type="checkbox"/> Socks4/5	<input type="checkbox"/> PGPNet	<input type="checkbox"/> HTTP Proxy Reply	<input type="checkbox"/> Tor	<input type="checkbox"/> VNN	
<input type="checkbox"/> SoftEther	<input type="checkbox"/> MS TEREDO	<input type="checkbox"/> Skyfire	<input type="checkbox"/> Hamachi	<input type="checkbox"/> HTTP Tunnel	
<input type="checkbox"/> Ping Tunnel	<input type="checkbox"/> TinyVPN	<input type="checkbox"/> RealTunnel	<input type="checkbox"/> DynaPass	<input type="checkbox"/> UltraVPN	
<input type="checkbox"/> FreeU	<input type="checkbox"/> Wujie/UltraSurf	<input type="checkbox"/> Hotspot Shield			
Streaming					
<input type="checkbox"/> MMS	<input type="checkbox"/> RTSP	<input type="checkbox"/> TVAnts	<input type="checkbox"/> PPStream	<input type="checkbox"/> PPTV	
<input type="checkbox"/> FeiDian	<input type="checkbox"/> UUSee	<input type="checkbox"/> NSPlayer	<input type="checkbox"/> PCAST	<input type="checkbox"/> TVKoo	
<input type="checkbox"/> SopCast	<input type="checkbox"/> UDLiveX	<input type="checkbox"/> TVUPlayer	<input type="checkbox"/> MySee	<input type="checkbox"/> Joost	
<input type="checkbox"/> FlashVideo	<input type="checkbox"/> SilverLight	<input type="checkbox"/> Slingbox	<input type="checkbox"/> QVOD		
Remote Control					
<input type="checkbox"/> VNC	<input type="checkbox"/> Radmin	<input type="checkbox"/> SpyAnywhere	<input type="checkbox"/> ShowMyPC	<input type="checkbox"/> LogMeIn	
<input type="checkbox"/> TeamViewer	<input type="checkbox"/> Gogrok	<input type="checkbox"/> RemoteControlPro	<input type="checkbox"/> CrossLoop	<input type="checkbox"/> WindowsRDP	
<input type="checkbox"/> pcAnywhere	<input type="checkbox"/> Timbuktu	<input type="checkbox"/> WindowsLiveSync	<input type="checkbox"/> SharedView		
Web HD					
<input type="checkbox"/> HTTP Upload	<input type="checkbox"/> HiNet SafeBox	<input type="checkbox"/> MS SkyDrive	<input type="checkbox"/> GDoc Uploader	<input type="checkbox"/> ADrive	
<input type="checkbox"/> MyOtherDrive	<input type="checkbox"/> Mozy	<input type="checkbox"/> BoxNet	<input type="checkbox"/> OfficeLive	<input type="checkbox"/> DropBox	
<input type="checkbox"/> Google Service	<input type="checkbox"/> iCloud				

4.8.2 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.

CSM >> URL Content Filter Profile

URL Content Filter Profile Table: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters)

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

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 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 Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

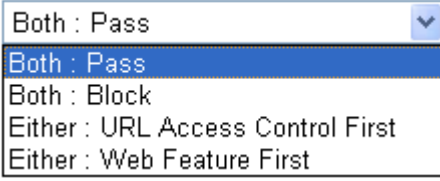
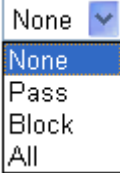

2.Web Feature

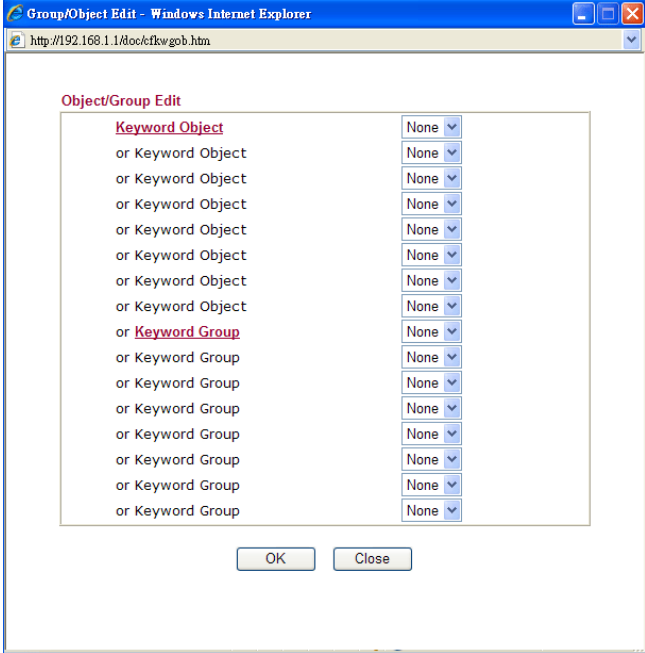
Enable Restrict Web Feature


Action: Cookie Proxy **File Extension Profile:**

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for the CSM profile.
Priority	<p>It determines the action that this router will apply.</p> <p>Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Both: Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.</p> <p>Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.</p> <p>Either: Web Feature First –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router</p>

Item	Description
	<p>will process the packages with the conditions set below for web feature first, then URL second.</p> 
Log	<p>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.</p> 
URL Access Control	<p>Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for URL Access Control is higher than Restrict Web Feature. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.</p> <p>Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p> <p>Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below. Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the keyword set here, it will be processed with reverse action.</p> <p>Action:</p>  <p>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</p>

Item	Description
	<p>decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.</p> 
<p>Web Feature</p>	<p>Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.</p> <p>Action - This setting is available only when Either: URL Access Control First or Either: Web Feature Firs is selected. Pass allows accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.</p> <p>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</p> <p>Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.</p> <p>Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.</p> <p>Upload – Check the box to block the file upload by way of web page.</p> <p>File Extension Profile – Choose one of the profiles that you configured in Object Setting>> File Extension Objects previously for passing or blocking the file downloading.</p>

Item	Description
	<p data-bbox="691 259 975 293"><u>File Extension Profile:</u></p> <div data-bbox="983 248 1134 360"><p data-bbox="983 248 1134 286">None </p><p data-bbox="983 286 1134 324">None</p><p data-bbox="983 324 1134 360">1-default</p></div>

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

4.8.3 Web Content Filter Profile

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

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

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.

CSM >> Web Content Filter Profile

Web-Filter License [Activate](#)
 [Status:Not Activated]

Setup Query Server	<input type="text" value="auto-selected"/>	Find more
Setup Test Server	<input type="text" value="auto-selected"/>	Find more

Web Content Filter Profile Table: [Set to Factory Default](#)

Profile	Name	Profile	Name
1.	Default	5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters) Cache :

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%
<br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content
Filter.<p>Please contact your system administrator for further
information.</center></body>
```

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 Administration Message .
Cache	<p>None – 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.</p> <p>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 in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.</p> <p>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.</p> <p>L1+L2 Cache – the router will check the URL with fast processing rate combining the feature of L1 and L2.</p>

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

Profile Index: 1

Profile Name:

Log:

Black/White List

Enable

Action:

Action:

Groups

Child Protection

Leisure

Business

Categories

Alcohol & Tobacco Criminal Activity Gambling

Hate & Intolerance Illegal Drug Nudity

Porn & Sexually Violence Weapons

School Cheating Sex Education Tasteless

Child Abuse Images

Entertainment Games Sports

Travel Leisure & Recreation Fashion & Beauty

Compromised Dating & Personals Education

Finance Government Health & Medicine

News Non-profits & NGOs Personal Sites

Politics Real Estate Religion

Restaurants & Dining Shopping Translators

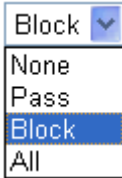
General Cults Greeting cards

Image Sharing Network Errors Parked Domains

Private IP Addresses Uncategorized Sites

Available settings are explained as follows:

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

Item	Description
	<p>Block - restrict accessing into the corresponding webpage with the categories listed on the box below.</p> <p>If the web pages do not match with the specified feature set here, it will be processed with reverse action.</p>
Log	<p>None – There is no log file will be recorded for this profile.</p> <p>Pass – Only the log about Pass will be recorded in Syslog.</p> <p>Block – Only the log about Block will be recorded in Syslog.</p> <p>All – All the actions (Pass and Block) will be recorded in Syslog.</p> 

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

4.8.4 DNS Filter

The DNS Filter monitors DNS queries on UDP port 53 and will pass the DNS query information to the WCF to help with categorizing HTTPS URL's.

DNS can be specified in **LAN>>General Setup** by using the server (e.g., 168.95.1.1) on router or external DNS server (e.g., 8.8.8.8). If the router server is used, **DNS Filter General Setting** will be applied to DNS query from clients on LAN. However, if the external DNS server is used, **DNS Filter Profile** will be applied to DNS query coming from clients on LAN.

Note: For DNS filter must use the WCF service profile to filter the packets, therefore WCF license must be activated first. Otherwise, DNS filter does not have any effect on packets.

DNS Filter

DNS Filter	<input type="checkbox"/> Enable
Syslog	None ▾
Service	None ▾
Enable Block Page	<input checked="" type="checkbox"/> Enable

Administration Message (Max 255 characters)

Default Message

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% DNS Filter.<p>Please contact your system administrator for further information.</center></body>
```

Legend:

%SIP% - Source IP , %URL% - URL
%CL% - Category , %RNAME% - Router Name

OK Cancel

Available settings are explained as follows:

Item	Description
DNS Filter	<p>DNS Filter - Check Enable to enable such feature.</p> <p>Syslog - The filtering result can be recorded according to the setting selected for Syslog.</p> <ul style="list-style-type: none"> ● 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. <p>Service- Set the filtering conditions.</p> <p>Enable Block Page - If such function is enabled, when DNS packets are blocked by DNS filter, a web page containing the description listed on Administration Message will be shown on the screen.</p>
Administration Message	Type the words or sentences which will be displayed when a web page is blocked by Vigor router.

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

4.8.5 APPE Support List

Such page lists all the information (name, version and note) about IM, P2P, Protocol and others applications that Vigor router supports for APPE function.

CSM >> APPE Support List

This charts lists out the APP Enforcement supported by Vigor routers.
Last update on 2014-07-21

IM	P2P	PROTOCOL	OTHERS
APP Type	APP Name	Version	Note
	AIM	5.9	
	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.
	AliWW	2008	
	Ares	2.0.9	
	BaiduHi	37378	
	Fetion	2010	
	GaduGadu Protocol		
	Google Chat		
	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or former versions, Videos and Voices can be blocked separately.
	ICU2	8.0.6	
	Jabber		

4.9 Bandwidth Management

Below shows the menu items for Bandwidth Management.



4.9.1 Sessions Limit

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

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

Bandwidth Management >> Sessions Limit

Sessions Limit

Enable
 Disable

Default Max Sessions:

Limitation List

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Administration Message (Max 256 characters)

Time Schedule

Index(1-15) in **Schedule** Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

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 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.

4.9.2 Bandwidth Limit

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

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

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

Enable Apply to IP Routed Subnet **Disable**
 Allow auto adjustment to make better use of the available bandwidth.

Default TX Limit:
 Default RX Limit:

Limitation List

Index	Start IP	End IP	TX limit	RX limit	Shared

Specific Limitation

Start IP: End IP:
 Each Shared
 TX Limit:
 RX Limit:

Smart Bandwidth Limit

For any LAN IP Not in Limitation List, whose session number exceeds

TX Limit :
 RX Limit :

Note:

- For TX/RX Limit, a setting of "0" means unlimited bandwidth.
- Available bandwidth is calculated according to the maximum bandwidth detected or the Line Speed defined in WAN >> [General Setup](#) when in "According to Line Speed" Load Balance mode.

Time Schedule

Index(1-15) in [Schedule](#) Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

Available settings are explained as follows:

Item	Description
Bandwidth Limit	<p>Enable - Click this button to activate the function of limit bandwidth.</p> <p>Apply to IP Routed Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN>>General Setup.</p> <p>Disable - Click this button to close the function of limit bandwidth.</p> <p>Allow auto adjustment...- Check this box to make the best utilization of available bandwidth.</p> <p>Default TX limit - Define the default speed of the upstream for each computer in LAN.</p> <p>Default RX limit - Define the default speed of the</p>

	downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Specific Limitation	<p>Start IP - Define the start IP address for limit bandwidth.</p> <p>End IP - Define the end IP address for limit bandwidth.</p> <p>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.</p> <p>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.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p> <p>Add - Add the specific speed limitation onto the list above.</p> <p>Update - Allow you to edit the settings for the selected limitation.</p> <p>Delete - Remove the selected settings existing on the limitation list.</p>
Smart Bandwidth Limit	<p>Check this box to have the bandwidth limit determined by the system automatically.</p> <p>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.</p> <p>RX limit - Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.</p>
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.

4.9.3 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?

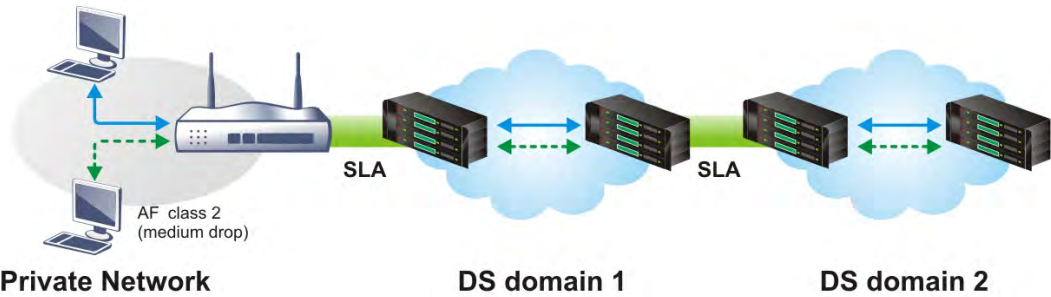
There are two components within Primary configuration of QoS deployment:

- **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.

[Bandwidth Management >> Quality of Service](#)

General Setup | [Set to Factory Default](#) |

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 Setup
WAN2	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN3	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN5	Disable	100000Kbps/100000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

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: (Default: 5060)

Available settings are explained as follows:

Item	Description
General Setup	<p>Index - Display the WAN interface number that you can edit.</p> <p>Status - Display if the WAN interface is available for such function or not.</p> <p>Bandwidth - Display the inbound and outbound bandwidth setting for the WAN interface.</p> <p>Direction - Display which direction that such function will influence.</p> <p>Class 1/Class2/Class 3/Others - Display the bandwidth percentage for each class.</p> <p>UDP Bandwidth Control - Display the UDP bandwidth</p>

Item	Description
	control is enabled or not. Online Statistics – Display an online statistics for quality of service for your reference Setup – Allow to configure general QoS setting for WAN interface.
Class Rule	Index – Display the class number that you can edit. Name – Display the name of the class. Rule – Allow to configure detailed settings for the selected 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.

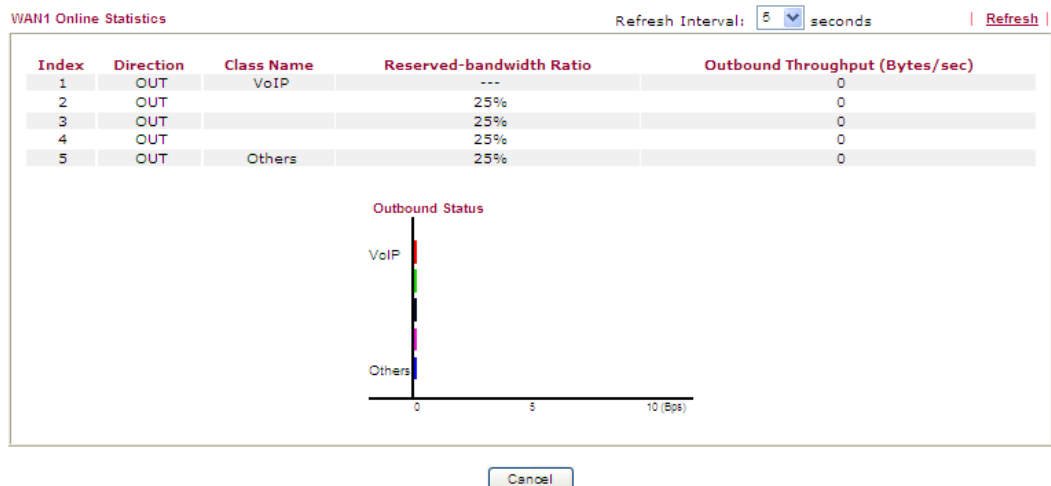
This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN interface. As to class rule, simply click the **Edit** link to access into next for configuration.

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.

Bandwidth Management >> Quality of Service



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 Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth	100	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps
WAN Outbound Bandwidth	100	<input type="radio"/> Kbps	<input checked="" type="radio"/> Mbps
Index	Class Name	Reserved_bandwidth Ratio	
Class 1		25	%
Class 2		25	%
Class 3		25	%
	Others	25	%
<input type="checkbox"/> Enable UDP Bandwidth Control		Limited_bandwidth Ratio 25 %	
<input type="checkbox"/> Outbound TCP ACK Prioritize			

Note: 1. Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.

2. You can do speed test by <http://speedtest.net> or contact with your ISP for speed test program.

Available settings are explained as follows:

Item	Description
Enable the QoS Control	<p>The factory default for this setting is checked.</p> <p>Please also define which traffic the QoS Control settings will apply to.</p> <p>IN- apply to incoming traffic only.</p> <p>OUT- apply to outgoing traffic only.</p> <p>BOTH- apply to both incoming and outgoing traffic.</p> <p>Check this box and click OK, then click Setup link again. You will see the Online Statistics link appearing on this page.</p>
WAN Inbound Bandwidth	<p>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.</p>
WAN Outbound Bandwidth	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.</p> </div>
Reserved Bandwidth	<p>It is reserved for the group index in the form of ratio of</p>

Item	Description
Ratio	reserved bandwidth to upstream speed and reserved bandwidth to downstream speed.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

Edit the Class Rule for QoS

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

Bandwidth Management >> Quality of Service

General Setup | [Set to Factory Default](#) |

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 Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

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

Bandwidth Management >> Quality of Service

Class Index #1

Name Tag packets as:

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

3. For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Ethernet Type IPv4 IPv6

Local Address

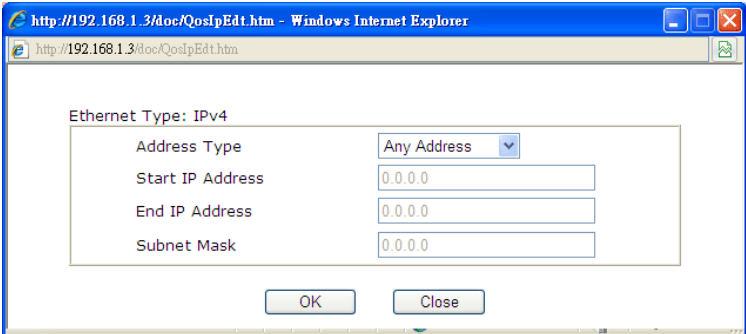
Remote Address

DiffServ CodePoint

Service Type

Note: Please choose/setup the **Service Type** first.

Available settings are explained as follows:

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 Edit button to set the local IP address (on LAN) for the rule.
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.
Edit	<p>It allows you to edit source address information.</p>  <p>Address Type – Determine the address type for the source address.</p> <p>For Single Address, you have to fill in Start IP address.</p> <p>For Range Address, you have to fill in Start IP address and End IP address.</p> <p>For Subnet Address, you have to fill in Start IP address and Subnet Mask.</p>
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.

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.

[Bandwidth Management >> Quality of Service](#)

Class Index #1

Name Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input checked="" type="radio"/>	Active	Any	Any	ANY	ANY
2 <input type="radio"/>	Active	192.168.1.25	Any	IP precedence 1	SMTP(TCP:25)

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](#)

General Setup | [Set to Factory Default](#) |

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	Setup
WAN3	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN4	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup
WAN5	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Status	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

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

[Bandwidth Management >> Quality of Service](#)

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

- For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	<input type="text"/>
Service Type	TCP <input type="button" value="v"/> <input type="text" value="6"/>
Port Configuration	
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range
Port Number	<input type="text" value="0"/> - <input type="text" value="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 Single or Range as the Type . If you select Range, you have to type in the starting port number and the end porting number on the boxes below. Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

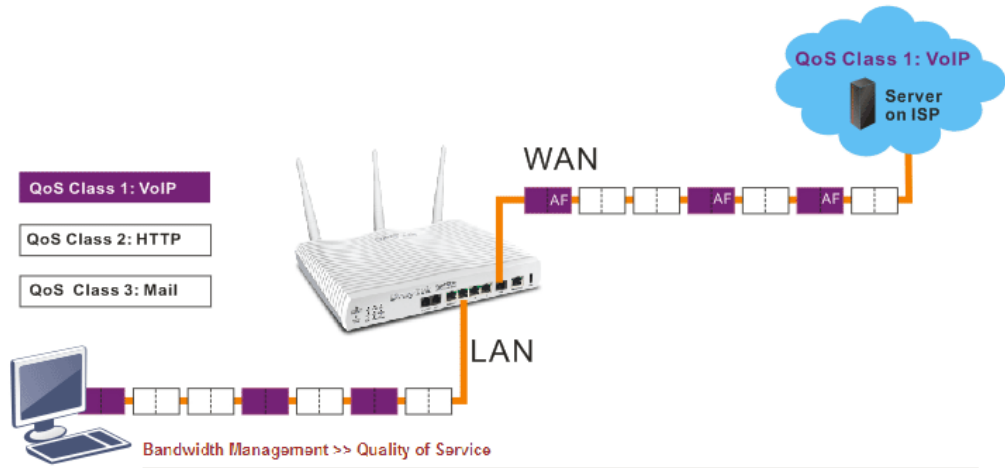
- After finishing all the settings here, please click **OK** to save the configuration.

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.



Class Index #1

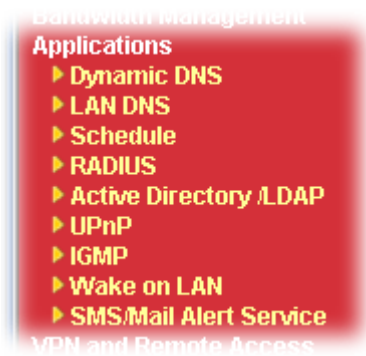
Name

Tag packets as:

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Active	Any	Any	ANY	ANY

4.10 Applications

Below shows the menu items for Applications.



4.10.1 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

Dynamic DNS Setup | [Set to Factory Default](#) |

Enable Dynamic DNS Setup [View Log](#) [Force Update](#)

Auto-Update interval Min(s) (1~14400)

Accounts:

Index	WAN Interface	Domain Name	Active
1.	WAN1 First		x
2.	WAN1 First		x
3.	WAN1 First		x
4.	WAN1 First		x
5.	WAN1 First		x
6.	WAN1 First		x

Available settings are explained as follows:

Item	Description
------	-------------

Item	Description
Set to Factory Default	Clear all profiles and recover to factory settings.
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.
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 Account

WAN Interface:

Service Provider:

Service Type:

Domain Name: .

Login Name: (max. 64 characters)

Password: (max. 23 characters)

Wildcards

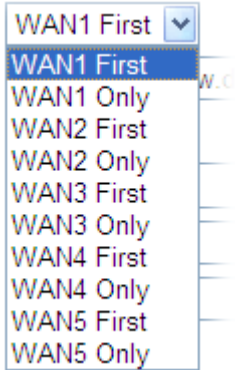
Backup MX

Mail Extender:

Determine Real WAN IP:

Available settings are explained as follows:

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

Item	Description
	<p>will use another WAN interface instead.</p> <p>WAN1/WAN2/WAN3/WAN4/WAN5 Only - While connecting, the router will use WAN1/WAN2/WAN3/WAN4/WAN5 as the only channel for such account.</p> 
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	<p>If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP.</p> <p>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.</p> <p>There are two methods offered for you to choose:</p> <p>WAN IP - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away.</p> <p>Internet IP – 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.</p>

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

Disable the Function and Clear all Dynamic DNS Accounts

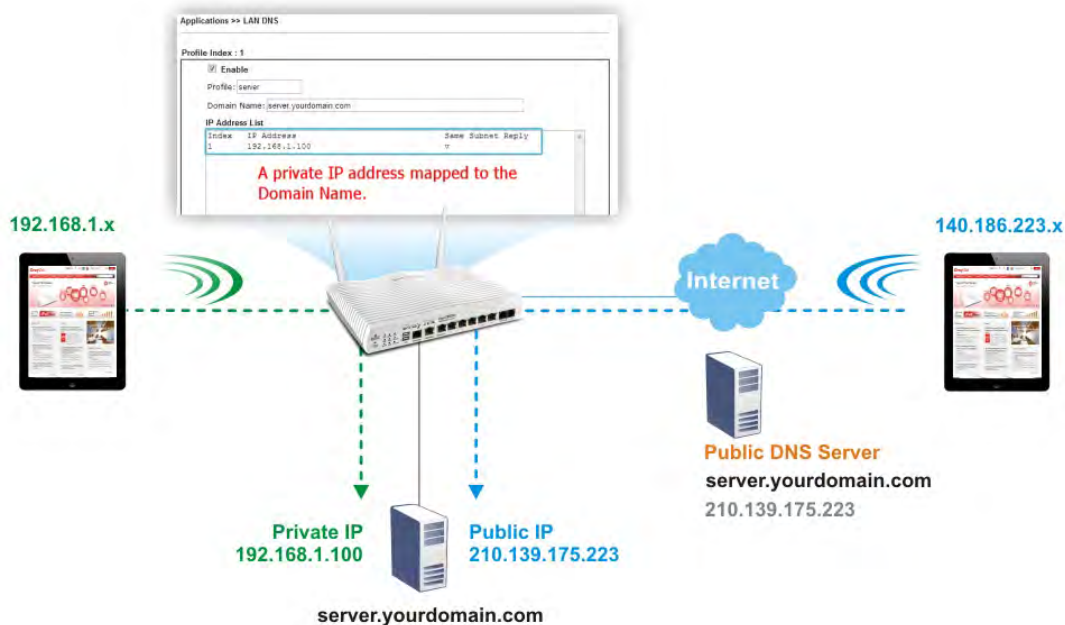
In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

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.

4.10.2 LAN DNS

The LAN DNS lets the network administrators host servers with privacy and security. When the network administrators of your office set up FTP, Mail or Web server inside LAN, you can specify specific private IP address(es) to correspondent servers. Thus, even the remote PC is adopting public DNS as the DNS server, the LAN DNS resolution on Vigor3200 Series will respond the specified private IP address.



Simply click **Application>>LAN DNS** to open the following page.

Applications >> LAN DNS

LAN DNS Resolution				Set to Factory Default
Enable	Index	Profile	Domain Name	
<input type="checkbox"/>	1.			
<input type="checkbox"/>	2.			
<input type="checkbox"/>	3.			
<input type="checkbox"/>	4.			
<input type="checkbox"/>	5.			
<input type="checkbox"/>	6.			
<input type="checkbox"/>	7.			
<input type="checkbox"/>	8.			
<input type="checkbox"/>	9.			
<input type="checkbox"/>	10.			

<< 1-10 | 11-20 >>

OK

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.
Profile	Display the name of the LAN DNS profile.

Item	Description
Domain Name	Display the domain name of the LAN DNS profile.

You can set up to 20 LAN DNS profiles.

To create a LAN DNS profile:

1. Click any index, say Index No. 1.
2. The detailed settings with index 1 are shown below.

Applications >> LAN DNS

Profile Index : 1

Enable


Profile:

Domain Name:

IP Address List

Index	IP Address	Same Subnet Reply

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Profile	Type a name for such profile. Note: If you type a name here for LAN DNS and click OK to save the configuration, the name also will be applied to conditional DNS forwarding automatically.
Domain Name	Type the domain name for such profile.
IP Address List	<p>The IP address listed here will be used for mapping with the domain name specified above. In general, one domain name maps with one IP address. If required, you can configure two IP addresses mapping with the same domain name.</p> <p>Add – Click it to open a dialog to type the host's IP address.</p>  <p>● Only responds to the DNS.... – Different LAN PCs can share the same domain name. However, you have to check this box to make the router identify & respond the IP address for the DNS query coming from different</p>

	LAN PC. Delete – Click it to remove an existed IP address on the list.
--	--

- Click **OK** button to save the settings.

4.10.3 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.

Applications >> Schedule

Schedule:		Set to Factory Default	
Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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 Factory Default](#) |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1

Enable Schedule Setup

Start Date (yyyy-mm-dd) 2000 1 1

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

Idle Timeout 0 minute(s).(max. 255, 0 for default)

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

Available settings are explained as follows:

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. Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field.

Item	Description
	Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. How often -Specify how often the schedule will be applied Once -The schedule will be applied just once Weekdays -Specify which days in one week should perform the schedule.

- 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).

Office

Hour:

(Force On)



Mon - Sun 9:00 am to 6:00 pm

- Make sure the PPPoE connection and **Time Setup** is working properly.
- Configure the PPPoE always on from 9:00 to 18:00 for whole week.
- Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- 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.

4.10.4 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

<input checked="" type="checkbox"/> Enable	
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>

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
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

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

4.10.5 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

This page allows you to enable the function and specify general settings for LDAP server.

[Applications >> Active Directory /LDAP](#)

Active Directory /LDAP
[Set to Factory Default](#)

General Setup

Active Directory / LDAP Profiles

Enable

Bind Type

Server Address

Destination Port

Use SSL

Regular DN

Regular Password

Simple Mode ▾

389

Note: After finishing the configuration of the LDAP profiles, they will be listed in the page of [VPN and Remote Access >> PPP General Setup](#). If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in [VPN and Remote Access >> PPP General Setup](#) first.

Available settings are explained as follows:

Item	Description
Enable	Check to enable such function.
Bind Type	<p>There are three types of bind type supported.</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> <div style="background-color: #e0e0e0; padding: 2px;">Simple Mode ▾</div> <div style="background-color: #e0e0e0; padding: 2px;">Simple Mode</div> <div style="background-color: #e0e0e0; padding: 2px;">Anonymous</div> <div style="background-color: #e0e0e0; padding: 2px;">Regular Mode</div> </div> <p>Simple Mode – Just simply do the bind authentication without any search action.</p> <p>Anonymous – Perform a search action first with Anonymous account then do the bind authentication.</p> <p>Regular Mode– Mostly it is the same with anonymous mode.</p>

	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 .
Server Address	Enter the IP address of LDAP server.
Destination Port	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 Regular Mode is selected as Bind Type .
Regular Password	Specify a password if Regular Mode is selected as Bind Type .

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](#)

Active Directory /LDAP
[Set to Factory Default](#)

General Setup



Active Directory / LDAP Profiles

Index	Name	Distinguished Name
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		


Note: After finishing the configuration of the LDAP profiles, they will be listed in the page of [VPN and Remote Access >> PPP General Setup](#). If you want to use the profiles for VPN authentication, check the boxes under PPTP LDAP Profiles in [VPN and Remote Access >> PPP General Setup](#) first.

Click any index number link to open the following page.

Index No. 1

Name	<input type="text" value="RD1"/>	
Common Name Identifier	<input type="text" value="UID"/>	
Base Distinguished Name	<input type="text"/>	
Additional Filter	<input type="text"/>	
<p>Note: Please type in your additional filter for BaseDN search request. For example, 1) For OpenLDAP: (gidNumber=500) 2) For AD: (msNPAllowDialin=TRUE)</p>		
Group Distinguished Name	<input type="text"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

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”.
Additional Filter	Type the condition for additional filter.
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  button 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.

4.10.6 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.

UPnP

Enable UPnP Service

Enable Connection control Service

Enable Connection Status Service

Default WAN Default WAN
WAN1
WAN2
WAN3
WAN4
WAN5

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

appropriate service above to

Available settings are explained as follows:

Item	Description
Enable UPNP Service	Accordingly, you can enable either the Connection Control Service or Connection Status Service .
Default WAN	It is used to specify the WAN interface for applying such function.

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.

4.10.7 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

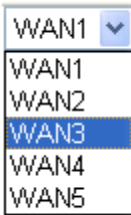
Enable IGMP Proxy WAN1 ▾
 IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function **take no affect when Bridge Mode is enabled**.

Enable IGMP Snooping
 Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

| [Refresh](#) |

Working Multicast Groups		
Index	Group ID	P1

Available settings are explained as follows:

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. <div style="margin-top: 10px;">  </div>
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.

4.10.8 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting.

[Application >> Wake on LAN](#)

Wake on 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:

Result

Available settings are explained as follows:

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.
	<p>Wake by: <input type="text" value="MAC Address"/></p> <div style="border: 1px solid #ccc; padding: 2px;"> <p>MAC Address</p> <p>IP Address</p> </div>
IP Address	The IP addresses that have been configured in Firewall>>Bind IP to MAC 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.
	<p>Application >> Wake on LAN</p> <p>Wake on LAN</p> <p>Note: Wake on LAN cooperate with Bind IP to MAC function, only binded PCs can wake up through IP.</p> <p>Wake by: <input type="text" value="MAC Address"/></p> <p>IP Address: <input type="text" value="---"/></p> <p>MAC Address: <input type="text" value=": : : : : :"/> <input type="button" value="Wake Up!"/></p> <p>Result</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Send command to client done.</p> </div>

4.10.9 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.

Application >> SMS / Mail Alert Service

SMS Provider		Mail Server		Set to Factory Default	
Index	SMS Provider	Recipient	Notify Profile	Schedule(1-15)	
1 <input checked="" type="checkbox"/>	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
2 <input type="checkbox"/>	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
3 <input type="checkbox"/>	2 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
4 <input type="checkbox"/>	3 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
5 <input type="checkbox"/>	4 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
6 <input type="checkbox"/>	5 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
7 <input type="checkbox"/>	6 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
8 <input type="checkbox"/>	7 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
9 <input type="checkbox"/>	8 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
10 <input type="checkbox"/>	9 - Custom 1	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
	10 - Custom 2	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>
	1 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>

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 SMS Provider 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 Notify Profile 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 Schedule(1-15) 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.

Application >> SMS / Mail Alert Service

SMS Provider		Mail Server			Set to Factory Default	
Index	Mail Service	Recipient	Notify Profile	Schedule(1-15)		
1 <input checked="" type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
2 <input checked="" type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
3 <input type="checkbox"/>	1 - Mail_Notify 2 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
4 <input type="checkbox"/>	3 - ??? 4 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
5 <input type="checkbox"/>	5 - ??? 6 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
6 <input type="checkbox"/>	7 - ??? 8 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
7 <input type="checkbox"/>	9 - ??? 10 - ???	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
8 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
9 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	
10 <input type="checkbox"/>	1 - Mail_Notify	<input type="text"/>	1 - ???	<input type="text"/>	<input type="text"/>	

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 Mail Service 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 Notify Profile link to define the content of the mail message.
Schedule(1-15)	Type the schedule number that the notification will be sent out. You can click the Schedule(1-15) link to define the schedule.

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

4.11 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.



4.11.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service (e.g., PPTP VPN, IPsec VPN, L2TP VPN, SSL VPN, etc.) of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPsec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

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

4.11.2 PPP General Setup

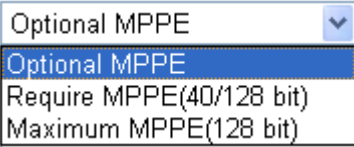
This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

VPN and Remote Access >> PPP General Setup

PPP General Setup													
<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication: <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>Dial-In PPP Encryption(MPPE): <input type="text" value="Optional MPPE"/></p> <p>Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <table border="1"> <tr> <td>Assigned IP start</td> <td>LAN 1</td> <td><input type="text" value="192.168.1.200"/></td> </tr> <tr> <td></td> <td>LAN 2</td> <td><input type="text" value="192.168.2.200"/></td> </tr> <tr> <td></td> <td>LAN 3</td> <td><input type="text" value="192.168.3.200"/></td> </tr> <tr> <td></td> <td>LAN 4</td> <td><input type="text" value="192.168.4.200"/></td> </tr> </table>	Assigned IP start	LAN 1	<input type="text" value="192.168.1.200"/>		LAN 2	<input type="text" value="192.168.2.200"/>		LAN 3	<input type="text" value="192.168.3.200"/>		LAN 4	<input type="text" value="192.168.4.200"/>	<p>PPP Authentication Methods</p> <p><input checked="" type="checkbox"/> Remote Dial-in User</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p><input checked="" type="checkbox"/> AD/LDAP</p> <p>PPTP LDAP Profile</p> <p>Note: Please select 'PAP Only' in 'Dial-In PPP Authentication', if you want to use AD/LDAP for PPP Authentication!!</p> <p>Note: Default priority is Remote Dial-in User -> RADIUS -> AD/LDAP.</p> <p>While using Radius or LDAP Authentication: Assign IP from subnet: <input type="text" value="LAN1"/></p>
Assigned IP start	LAN 1	<input type="text" value="192.168.1.200"/>											
	LAN 2	<input type="text" value="192.168.2.200"/>											
	LAN 3	<input type="text" value="192.168.3.200"/>											
	LAN 4	<input type="text" value="192.168.4.200"/>											

Available settings are explained as follows:

Item	Description
Dial-In PPP Authentication	<p>PAP Only - elect this option to force the router to authenticate dial-in users with the PAP protocol.</p> <p>PAP/CHAP/MS-CHAP/MS-CHAPv2 - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for</p>

Item	Description
	authentication.
Dial-In PPP Encryption (MPPE Optional MPPE)	<p>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.</p>  <p>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.</p> <p>Maximum MPPE (128 bit)- This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.</p>
Mutual Authentication (PAP)	<p>The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.</p>
Assigned IP Start	<p>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.</p> <p>You can configure up to four start IP addresses for LAN1 ~ LAN4.</p>
PPP Authentication Methods	<p>Select the method(s) to be used for authentication in PPP connection.</p> <p>PPP Authentication Methods</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Remote Dial-in User <input checked="" type="checkbox"/> RADIUS <input checked="" type="checkbox"/> AD/LDAP
PPTP LDAP Profile	<p>Configured LDAP profiles will be listed under such item. Simply check the one you want to enable the PPP authentication by LDAP server profiles.</p> <p>However, if there is no profile listed, simply click the link of PPTP LDAP Profile to create/add some new LDAP profiles you want.</p>

Item	Description
While using RADIUS or LDAP Authentication	If PPP connection will be authenticated via RADIUS server or LDAP profiles, it is necessary to specify the LAN profile for the dial-in user to get IP from.

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

4.11.3 IPSec General Setup

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

There are two phases of IPSec.

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

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

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

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and 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 will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

Available settings are explained as follows:

Item	Description
IKE Authentication Method	<p>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 dial-in user, Certificate (X.509) and Pre-Shared Key.</p> <p>Certificate for Dial-in – Choose one of the local certificates from the drop down list.</p> <p>Pre-Shared Key- Specify a key for IKE authentication.</p> <p>Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.</p> <p>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.</p>
IPSec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High (ESP) - 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.</p>

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

4.11.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **64** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

[Set to Factory Default](#) |

X509 Peer ID Accounts:					
Index	Name	Status	Index	Name	Status
1.	???	×	17.	???	×
2.	???	×	18.	???	×
3.	???	×	19.	???	×
4.	???	×	20.	???	×
5.	???	×	21.	???	×
6.	???	×	22.	???	×
7.	???	×	23.	???	×
8.	???	×	24.	???	×
9.	???	×	25.	???	×
10.	???	×	26.	???	×
11.	???	×	27.	???	×
12.	???	×	28.	???	×
13.	???	×	29.	???	×
14.	???	×	30.	???	×
15.	???	×	31.	???	×
16.	???	×	32.	???	×

<< [1-32](#) | [33-64](#) >> [Next](#) >>

Each item will be explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPSec Peer Identity.
Name	Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1

Profile Name

Enable this account

Accept Any Peer ID

Accept Subject Alternative Name

Type

IP

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

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 IP Address , Domain , or E-mail Address . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C) , State (ST) , Location (L) , Organization (O) , Organization Unit (OU) , Common Name (CN) , and Email (E) .

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

4.11.5 Remote Dial-in User

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

The router provides **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.

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | [Set to Factory Default](#) |

View: All Online Offline

Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >> [Next](#) >>

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 ??? 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.

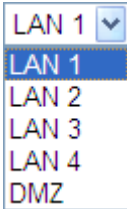
VPN and Remote Access >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input type="text" value="jos"/></p> <p>Password(Max 19 char) <input type="text" value="•••"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input type="text"/></p> <p>Secret <input type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input type="text"/></p>
---	--

Available settings are explained as follows:

Item	Description
User account and Authentication	<p>Enable this account - Check the box to enable this function.</p> <p>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.</p>
Allowed Dial-In Type	<p>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.</p> <p>IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.</p> <p>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:</p> <ul style="list-style-type: none"> ● 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
	<p>connection becomes one pure L2TP connection.</p> <ul style="list-style-type: none"> ● Must -Specify the IPSec policy to be definitely applied on the L2TP connection. <p>SSL Tunnel - 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)</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p>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.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● 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. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass – Click this button to let multicast packets pass through the router. ● Block – This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p>  <p>Assign Static IP Address – Please type a static IP address for the subnet you specified.</p>
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Enable Mobile One-Time Passwords (mOTP)	<p>Check this box to make the authentication with mOTP function.</p> <p>PIN Code – Type the code for authentication (e.g, 1234).</p> <p>Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>

Item	Description
IKE Authentication Method	<p>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.</p> <p>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.</p> <p>Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.</p>
IPSec Security Method	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

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

4.11.6 LAN to LAN

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

The router supports up to **64** VPN tunnels simultaneously. The following figure shows the summary table.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | [Set to Factory Default](#) |

View: All Online Offline Trunk

Index	Name	Active	Status	Index	Name	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >> [Next](#) >>

[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.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

View: All Online Offline Trunk

Name	Activate	Members	Status
RD1213	<input checked="" type="checkbox"/>	Sandy	Offline
		Marketing	Offline

Each item will be explained as follows:

Item	Description
Set to Factory Default	Click to clear all indexes.
View	All – Click it to show all of profiles.

Item	Description
	Online/Offline – Click it to show the active/inactive profiles Trunk - 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:

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.

[VPN and Remote Access >> LAN to LAN](#)

Profile Index : 1

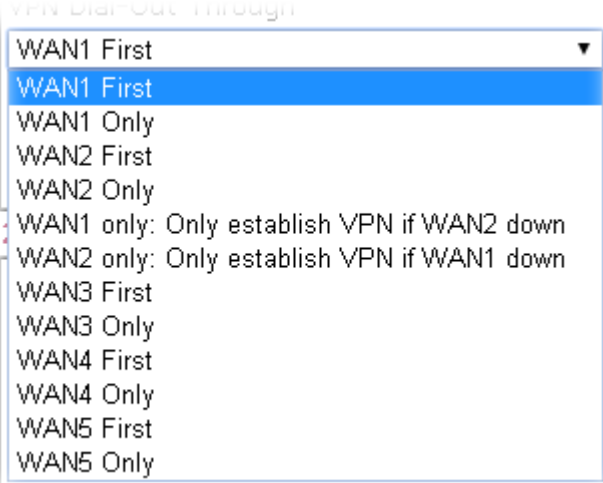
1. Common Settings

Profile Name <input data-bbox="646 936 866 967" type="text" value="???"/>	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through <input data-bbox="624 1037 756 1068" type="text" value="WAN1 First"/>	Idle Timeout <input data-bbox="1145 1010 1209 1041" type="text" value="300"/> second(s)
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	PING to the IP <input data-bbox="1145 1081 1366 1113" type="text"/>

2. Dial-Out Settings

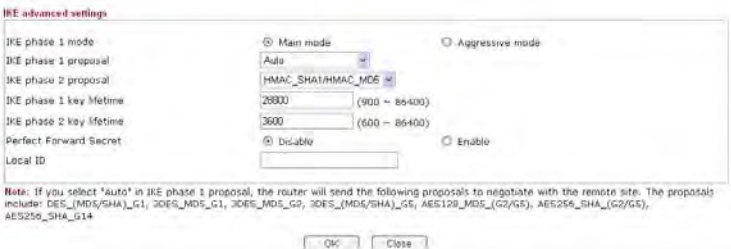
Type of Server I am calling <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input data-bbox="667 1317 807 1348" type="text" value="None"/>	Username <input data-bbox="1161 1216 1382 1247" type="text" value="???"/> Password <input data-bbox="1161 1256 1369 1288" type="text"/> PPP Authentication <input data-bbox="1166 1294 1289 1326" type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input data-bbox="400 1435 707 1467" type="text"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input data-bbox="1161 1451 1369 1482" type="text"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input data-bbox="1161 1525 1361 1556" type="text" value="None"/> Local ID <input type="radio"/> Alternative Subject Name First <input checked="" type="radio"/> Subject Name First Local Certificate <input data-bbox="1161 1659 1361 1691" type="text" value="None"/>
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input data-bbox="1034 1780 1313 1812" type="text" value="DES without Authentication"/> <input data-bbox="906 1821 1018 1852" type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input data-bbox="898 1906 962 1937" type="text"/> , <input data-bbox="986 1906 1050 1937" type="text"/> , <input data-bbox="1074 1906 1137 1937" type="text"/> , <input data-bbox="1161 1906 1225 1937" type="text"/>

Available settings are explained as follows:

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	<p>Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.</p>  <p>WAN1 /WAN2 /WAN3 /WAN4 /WAN5 First - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.</p> <p>WAN1 /WAN2 /WAN3 /WAN4 /WAN5 Only - While connecting, the router will use WAN1 /WAN2 /WAN3 /WAN4 /WAN5 as the only channel for VPN connection.</p> <p>WAN1 Only: Only establish VPN if WAN2 down - While connecting, the router will use WAN2 for VPN connection. If WAN2 fails, the router will use backup WAN1 interface instead.</p> <p>WAN2 Only: Only establish VPN if WAN1 down - While connecting, the router will use WAN1 for VPN connection. If WAN1 fails, the router will use backup WAN2 interface instead.</p>
Netbios Naming Packet	<p>Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <p>Pass – Click this button to let multicast packets pass through the router.</p> <p>Block – This is default setting. Click this button to let</p>

Item	Description
	multicast packets be blocked by the router.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. Both: -initiator/responder Dial-Out- initiator only Dial-In- responder only.
Always On or Idle Timeout	Always On- Check to enable router always keep VPN connection. Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel. Enable PING to keep alive 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	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. IPSec Tunnel - Build an IPSec VPN connection to the server through Internet. 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: <ul style="list-style-type: none"> ● 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-out VPN connection becomes one pure L2TP connection. ● Must: Specify the IPSec policy to be definitely applied on the L2TP connection.
Username	This field is applicable when you select, PPTP or L2TP with or without IPSec policy above.

Item	Description
Password	This field is applicable when you select PPTP or L2TP with or without IPsec policy above.
PPP Authentication	This field is applicable when you select, PPTP or L2TP with or without IPsec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPsec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.
IKE Authentication Method	<p>This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy.</p> <p>Pre-Shared Key - Input 1-63 characters as pre-shared key.</p> <p>Digital Signature (X.509) – Check the box of Digital Signature to invoke this function. Then, specify the following items for authentication with digital signature.</p> <ul style="list-style-type: none"> ● Peer ID - Select one of the predefined Profiles set in VPN and Remote Access >>IPsec Peer Identity. ● 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. <p>Local Certificate – Select one of the profiles set in Certificate Management>>Local Certificate.</p>
IPsec Security Method	<p>This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy.</p> <p>Medium AH (Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</p> <p>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</p> <p>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</p> <p>3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</p> <p>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</p> <p>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</p> <p>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</p>
Advanced	<p>Specify mode, proposal and key life of each IKE phase, Gateway, etc.</p> <p>The window of advance setup is shown as below:</p>

Item	Description
	 <p>IKE phase 1 mode -Select from Main mode and Aggressive mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. Main mode is more secure than Aggressive mode since more exchanges are done in a secure channel to set up the IPSec session. However, the Aggressive mode is faster. The default value in Vigor router is Main mode.</p> <p>IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for Main mode. We suggest you select the combination that covers the most schemes.</p> <p>IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.</p> <p>IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.</p> <p>IKE phase 2 key lifetime-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.</p> <p>Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.</p> <p>Local ID-In Aggressive mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.</p>

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy None	Username <input type="text"/> Password(Max 11 char) <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
	IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

4. GRE over IPsec Settings

<input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec <input type="checkbox"/> Logical Traffic	My GRE IP <input type="text"/> Peer GRE IP <input type="text"/>
--	---

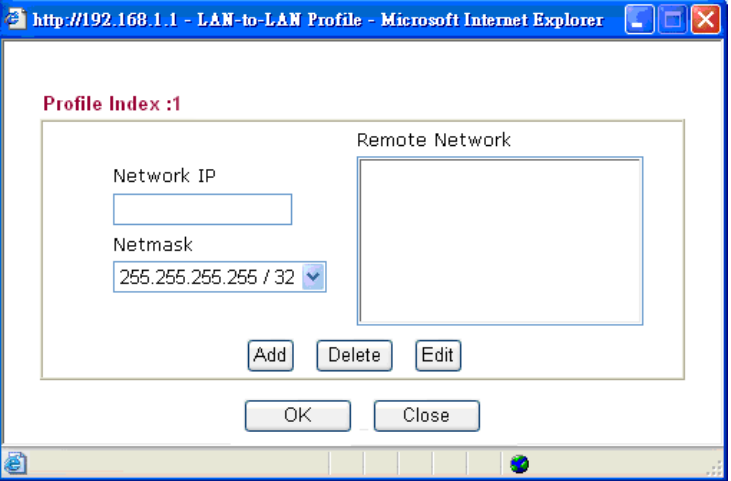
5. TCP/IP Network Settings

My WAN IP <input type="text"/> 0.0.0.0 Remote Gateway IP <input type="text"/> 0.0.0.0 Remote Network IP <input type="text"/> 0.0.0.0 Remote Network Mask <input type="text"/> 255.255.255.0 Local Network IP <input type="text"/> 192.168.1.5 Local Network Mask <input type="text"/> 255.255.255.0 <input type="button" value="More"/>	RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	--

Item	Description
Allowed Dial-In Type	<p>Determine the dial-in connection with different types.</p> <p>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.</p> <p>IPSec Tunnel- Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.</p> <p>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:</p> <ul style="list-style-type: none"> ● 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. <p>Specify Remote VPN Gateway - You can specify the IP</p>

Item	Description
	<p>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.</p> <p>User Name - This field is applicable when you select PPTP or L2TP with or without IPsec policy above.</p> <p>Password (Max 11 char) - This field is applicable when you select PPTP or L2TP with or without IPsec policy above.</p> <p>VJ Compression - VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above.</p>
<p>IKE Authentication Method</p>	<p>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.</p> <p>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.</p> <p>Digital Signature (X.509) –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.</p> <p>Local ID – Specify which one will be inspected first.</p> <ul style="list-style-type: none"> ● Alternative Subject Name First – The alternative subject name (configured in Certificate Management>>Local Certificate) will be inspected first. ● Subject Name First – The subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
<p>IPsec Security Method</p>	<p>This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.</p> <p>Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>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.</p>
<p>GRE over IPsec Settings</p>	<p>Enable IPsec Dial-Out function GRE over IPsec: 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.</p>

Item	Description
	<p>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 hacker 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.</p> <p>My GRE IP: Type the virtual IP for router itself for verified by peer.</p> <p>Peer GRE IP: Type the virtual IP of peer host for verified by router.</p>
<p>TCP/IP Network Settings</p>	<p>My WAN IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.</p> <p>Remote Gateway IP - This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.</p> <p>Remote Network IP/ Remote Network Mask - Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.</p> <p>Local Network IP / Local Network Mask - Add a static route to direct all traffic destined to Local Network IP Address/Local Network Mask through the VPN connection.</p> <p>More - Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.</p>

Item	Description
	 <p>RIP Direction - 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.</p> <p>From first subnet to remote network, you have to do - If the remote network only allows you to dial in with single IP, please choose NAT, otherwise choose Route.</p> <p>Change default route to this VPN tunnel - 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.</p>

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

4.11.7 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
- Fully 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

Backup Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1 (&Active) Type	Member2 (&Active) Type

Advanced

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disabled or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1 (&Active) Type	Member2 (&Active) Type

Advanced

General Setup

Status Enable Disable

Profile Name

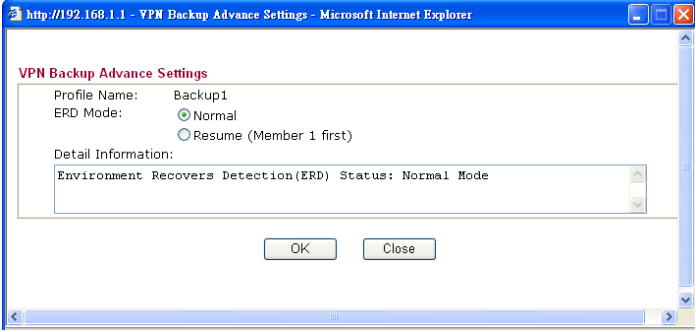
Member1

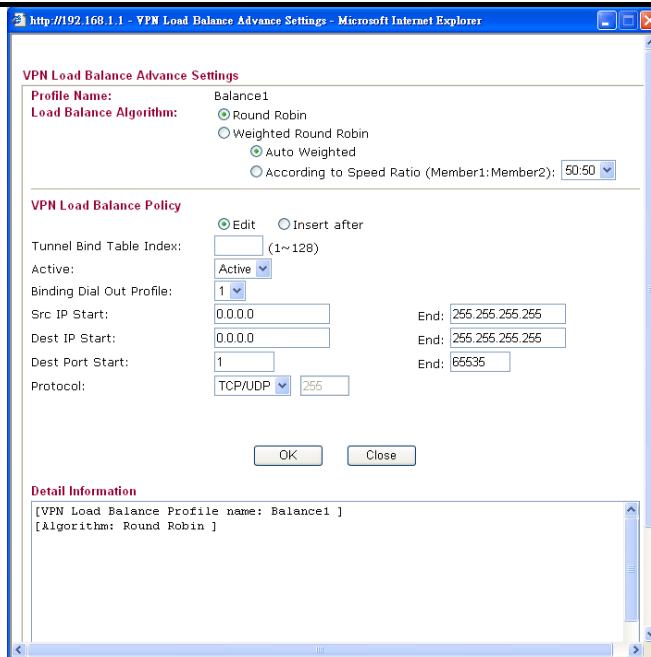
Member2

Active Mode Backup Load Balance

Available settings are explained as follows:

Item	Description
Backup Profile List	<p>Set to Factory Default - Click to clear all VPN TRUNK-VPN Backup mechanism profile.</p> <p>No – The order of VPN TRUNK-VPN Backup mechanism profile.</p> <p>Status (on Backup Profile field) - “v” means such profile is enabled; “x” means such profile is disabled.</p> <p>Name (on Backup Profile field) - Display the name of VPN TRUNK-VPN Backup mechanism profile.</p> <p>Member1 (on Backup Profile field) - Display the dial-out profile selected from the Member1 drop down list below.</p> <p>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.</p>

	<p>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.</p> <p>Member2 (on Backup Profile field) - Display the dial-out profile selected from the Member2 drop down list below.</p> <p>Advanced – This button is available only when LAN to LAN profile (or more) is created.</p>  <p>Detailed information for this dialog, see later section - Advanced Load Balance and Backup.</p>
<p>Load Balance Profile List</p>	<p>Set to Factory Default - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.</p> <p>No - The order of VPN TRUNK-VPN Load Balance mechanism profile.</p> <p>Status - “v” means such profile is enabled; ”x” means such profile is disabled.</p> <p>Name - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.</p> <p>Member1 - Display the dial-out profile selected from the Member1 drop down list below.</p> <p>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.</p> <p>Type - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.</p> <p>Member2 - Display the dial-out profile selected from the Member2 drop down list below.</p> <p>Advanced – This button is only available when there is one or more profiles created in this page.</p>



Detailed information for this dialog, see later section - **Advanced Load Balance and Backup.**

General Setup

Status- After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.

Profile Name- 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.

No - Index number of LAN-to-LAN dial-out profile.

Name - Profile name of LAN-to-LAN dial-out profile.

Connection Type - Connection type of LAN-to-LAN dial-out profile.

VPN ServerIP (Private Network) - VPN Server IP of LAN-to-LAN dial-out profiles.

Active Mode - Display available mode for you to choose. Choose **Backup** or **Load Balance** 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 Status (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?

1. 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.

General Setup

Status: Enable Disable

Profile Name: 071023

Member1: Please choose the combination that you want.

Member2: Please choose the combination that you want.

Attribute Mode:

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
1	To-A PlaceIPSec		192.168.2.25(20.20.20.0)
2	To-B Site IPSec		192.168.2.26(20.20.21.0)

Add Edit Delete

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	▼
<u>2.</u>	To-B Site	▼
<u>3.</u>	To-C place	▼
<u>4.</u>	To-D Site	▼
5	???	▼

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 minute(s)

4. GRE over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec
 Logical Traffic
 My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP
 Remote Gateway IP
 Remote Network IP
 Remote Network Mask
 RIP Direction
 From first subnet to remote network, you have to do

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 minute(s)

4. GRE over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec
 Logical Traffic
 My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP
 Remote Gateway IP
 Remote Network IP
 Remote Network Mask

 RIP Direction
 From first subnet to remote network, you have to do
 Change default route to this VPN tunnel (Only single WAN supports this)

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

The screenshot shows the 'VPN Load Balance Advance Settings' window. The 'Profile Name' is 'Balance1'. Under 'Load Balance Algorithm', 'Auto Weighted' is selected, and the 'According to Speed Ratio (Member1:Member2)' is set to '50:50'. In the 'VPN Load Balance Policy' section, 'Edit' is selected. The 'Tunnel Bind Table Index' is empty. 'Active' is set to 'Active'. 'Binding Dial Out Profile' is '1'. 'Src IP Start' and 'Dest IP Start' are both '0.0.0.0'. 'Src IP End' and 'Dest IP End' are both '255.255.255.255'. 'Dest Port Start' is '1' and 'Dest Port End' is '65535'. 'Protocol' is 'TCP/UDP' with a value of '255'. The 'Detail Information' section shows: '[VPN Load Balance Profile name: Balance1]' and '[Algorithm: Round Robin]'. 'OK' and 'Close' buttons are at the bottom.

Available settings are explained as follows:

Item	Description
Profile Name	List the load balance profile name.
Load Balance Algorithm	<p>Round Robin – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.</p> <p>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).</p>

VPN Load Balance Policy

Below shows the algorithm for Load Balance.

Edit – 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.

Tunnel Bind Table Index- 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.

Binding Dial Out Index – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.

Src IP Start /End– Specify source IP addresses as starting point and ending point.

Dest IP Start/End – Specify destination IP addresses as starting point and ending point.

Dest Port Start /End– Specify destination service port as starting point and ending point.

Protocol – **Any** 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.

TCP 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. **UDP** 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. **TCP/UDP** means when the source IP, 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. **ICMP** 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. **Other** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.

Detail Information

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 After insert
 Tunnel Bind Table Index: (1~400)
 Active:
 Binding Dial Out Index:
 Binding Src IP Start: End:
 Binding Dest IP Start: End:
 Binding Dest Port Start: End:
 Binding Fragmented: Binding Protocol:

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 Dest IP = 192.168.1.20 ~ 192.168.1.20
 Binding Dest 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

VPN Backup Advance Settings
 Profile Name: Backup1
 ERD Mode: Normal Resume (Member 1 first)
 Detail Information:
 Environment Recovers Detection(ERD) Status: Normal Mode

Available settings are explained as follows:

Item	Description
Profile Name	List the backup profile name.
ERD Mode	ERD means “Environment Recovers Detection”. Normal – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively. Resume – 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.

4.11.8 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

Dial-out Tool Refresh Seconds : 10

General Mode:

Backup Mode:

Load Balance Mode:

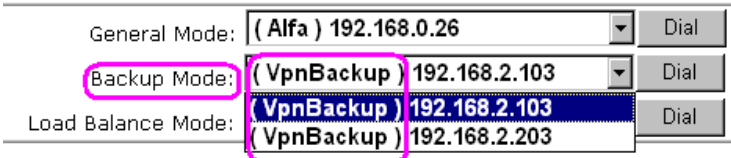
VPN Connection Status Current Page: 1 Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.

Available settings are explained as follows:

Item	Description																								
Dial-out Tool	<p>General Mode - This field 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.</p> <p>Refresh Seconds :</p> <p>General Mode: <input type="text"/> <input type="button" value="Dial"/></p> <p>Backup Mode: <input type="text"/> <input type="button" value="Dial"/></p> <p>Load Balance Mode: <input type="text"/> <input type="button" value="Dial"/></p> <p>n Status 1</p> <p>Type Remote</p> <table border="1"> <tbody> <tr> <td>(Alfa) 192.168.0.26</td> <td><input type="button" value="Dial"/></td> </tr> <tr> <td>Alfa) 192.168.0.26</td> <td><input type="button" value="Dial"/></td> </tr> <tr> <td>Bentley) 192.168.0.27</td> <td><input type="button" value="Dial"/></td> </tr> <tr> <td>Audi) 192.168.0.28</td> <td><input type="button" value="Dial"/></td> </tr> <tr> <td>BMW) 192.168.0.29</td> <td></td> </tr> <tr> <td>Buick) 192.168.0.30</td> <td></td> </tr> <tr> <td>Cadillac) 192.168.0.31</td> <td></td> </tr> <tr> <td>Chrysler) 192.168.0.32</td> <td></td> </tr> <tr> <td>Citroen) 192.168.0.33</td> <td></td> </tr> <tr> <td>Daihatsu) 192.168.0.34</td> <td></td> </tr> <tr> <td>Ferrari) 192.168.0.35</td> <td></td> </tr> <tr> <td>Fiat) 192.168.0.36</td> <td></td> </tr> </tbody> </table> <p>Page No. Rx Pkts Rx Rate : Data is er : Data isn't</p> <p>Backup Mode - This field displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.</p>	(Alfa) 192.168.0.26	<input type="button" value="Dial"/>	Alfa) 192.168.0.26	<input type="button" value="Dial"/>	Bentley) 192.168.0.27	<input type="button" value="Dial"/>	Audi) 192.168.0.28	<input type="button" value="Dial"/>	BMW) 192.168.0.29		Buick) 192.168.0.30		Cadillac) 192.168.0.31		Chrysler) 192.168.0.32		Citroen) 192.168.0.33		Daihatsu) 192.168.0.34		Ferrari) 192.168.0.35		Fiat) 192.168.0.36	
(Alfa) 192.168.0.26	<input type="button" value="Dial"/>																								
Alfa) 192.168.0.26	<input type="button" value="Dial"/>																								
Bentley) 192.168.0.27	<input type="button" value="Dial"/>																								
Audi) 192.168.0.28	<input type="button" value="Dial"/>																								
BMW) 192.168.0.29																									
Buick) 192.168.0.30																									
Cadillac) 192.168.0.31																									
Chrysler) 192.168.0.32																									
Citroen) 192.168.0.33																									
Daihatsu) 192.168.0.34																									
Ferrari) 192.168.0.35																									
Fiat) 192.168.0.36																									

	 <p>Dial - Click this button to execute dial out function.</p>
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	<p>Display current connected VPN status.</p> <p>VPN – Display the name of the VPN profile.</p> <p>Type – Display the VPN connection mode such as PPTP or IPSec.</p> <p>Remote IP – Display the IP address of remote peer.</p> <p>Virtual Network – Display the remote network IP address with subnet address.</p> <p>Tx Pkts – Display the transmission packets passing through such VPN channel.</p> <p>Tx Rate – Display the transmission rate for data through such VPN tunnel.</p> <p>Rx Pkts – Display the receiving packets passing through such VPN channel.</p> <p>Rx Rate – Display the receiving rate for data through such VPN tunnel.</p>

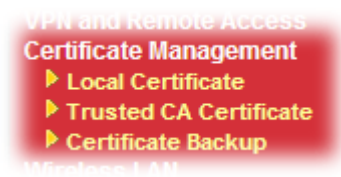
4.12 Certificate Management

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.



4.12.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

Available settings are explained as follows:

Item	Description
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.
Delete	Click this button to delete selected name with certification information.

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 Management >> Local Certificate

Generate Certificate Signing Request

Certificate Name	<input type="text"/>
Subject Alternative Name	
Type	IP Address <input type="button" value="v"/>
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA <input type="button" value="v"/>
Key Size	1024 Bit <input type="button" value="v"/>

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	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

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

Import X509 Local Certificate

Upload Local Certificate
 Select a local certificate file.
 Certificate file:
 Click [Import](#) to upload the local certificate.

Upload PKCS12 Certificate
 Select a PKCS12 file.
 PKCS12 file:
 Password:
 Click [Import](#) to upload the PKCS12 file.

Upload Certificate and Private Key
 Select a certificate file and a matchable Private Key.
 Certificate file:
 Key file:
 Password:
 Click [Import](#) to upload the local certificate and private key.

Available settings are explained as follows:

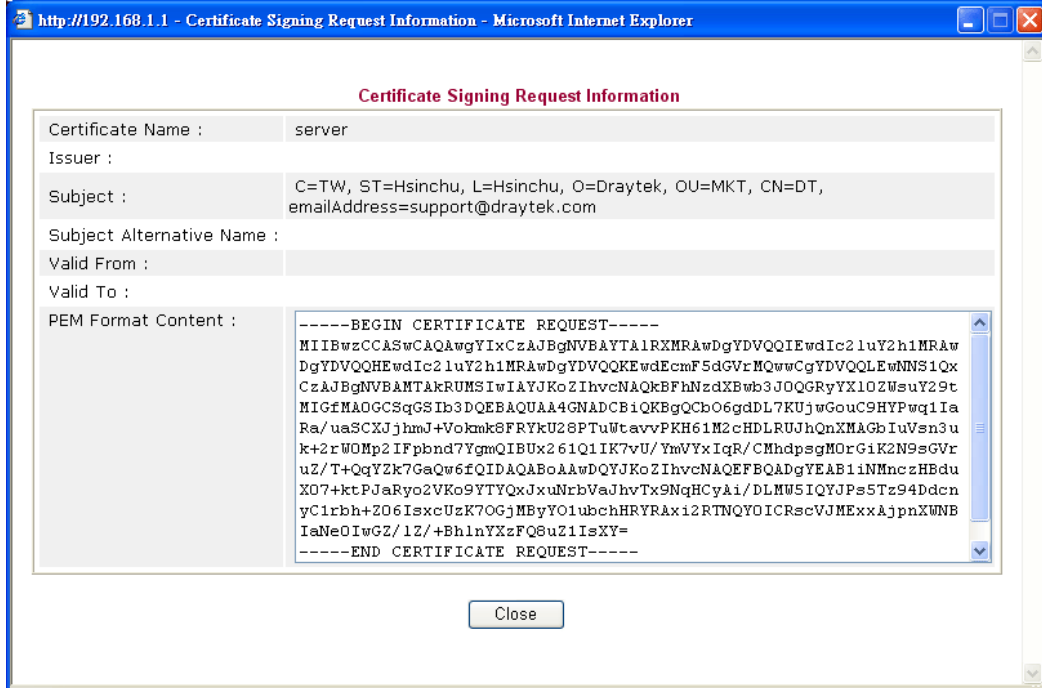
Item	Description																
Upload Local Certificate	<p>It allows users to import the certificate which is generated by vigor router and signed by CA server.</p> <p>If you have done well in certificate generation, the Status of the certificate will be shown as “OK”.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">Import X509 Local Certificate</p> <p style="text-align: center;">Congratulation! Local Certificate has been imported successfully.</p> <p style="text-align: center;">Please click <input type="button" value="Back"/> to view the certificate.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">X509 Local Certificate Configuration</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Subject</th> <th>Status</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>draytekdemo</td> <td>/O=Draytek/OU=Draytek Sales/...</td> <td>OK</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="View"/> <input type="button" value="Delete"/></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="GENERATE"/> <input type="button" value="IMPORT"/> <input type="button" value="REFRESH"/> </p> </div>	Name	Subject	Status	Modify	draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>	---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>
Name	Subject	Status	Modify														
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
---	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>														
Upload PKCS12 Certificate	<p>It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.</p> <p>Note: 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.</p>																
Upload Certificate and Private Key	<p>It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.</p>																

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.



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.

4.12.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

[Certificate Management >> Trusted CA Certificate](#)

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify	
Trusted CA-1	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/>	<input type="button" value="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.

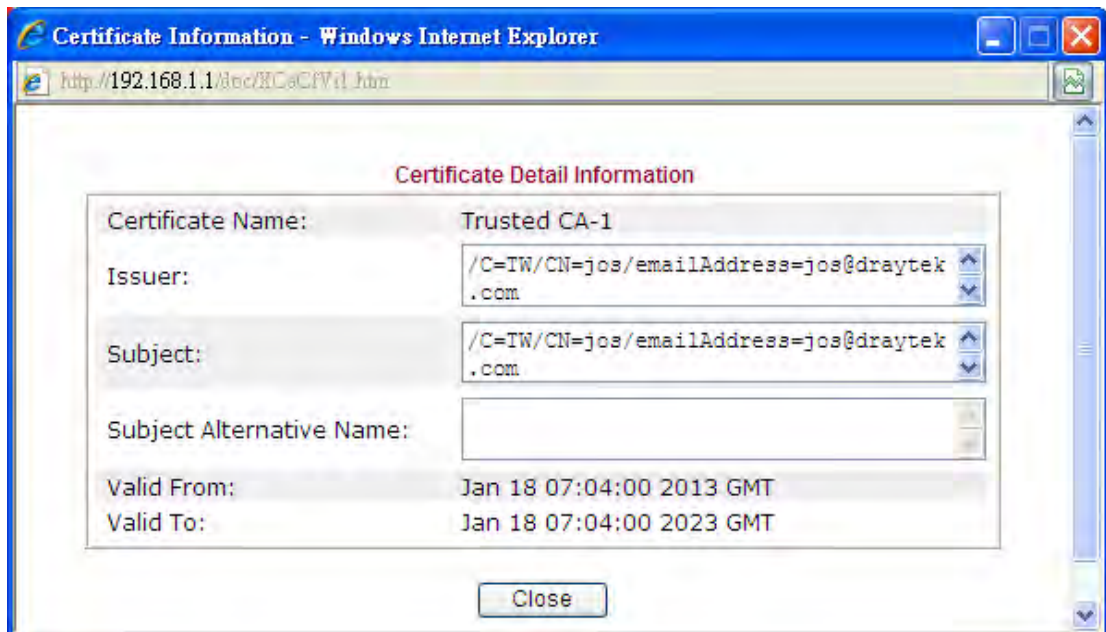
[Certificate Management >> Trusted CA Certificate](#)

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click [Import](#) to upload the certification.

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.



4.12.3 Certificate Backup

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

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

[Certificate Management >> Certificate Backup](#)

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

4.13 Wireless LAN

This function is used for “n” models only.

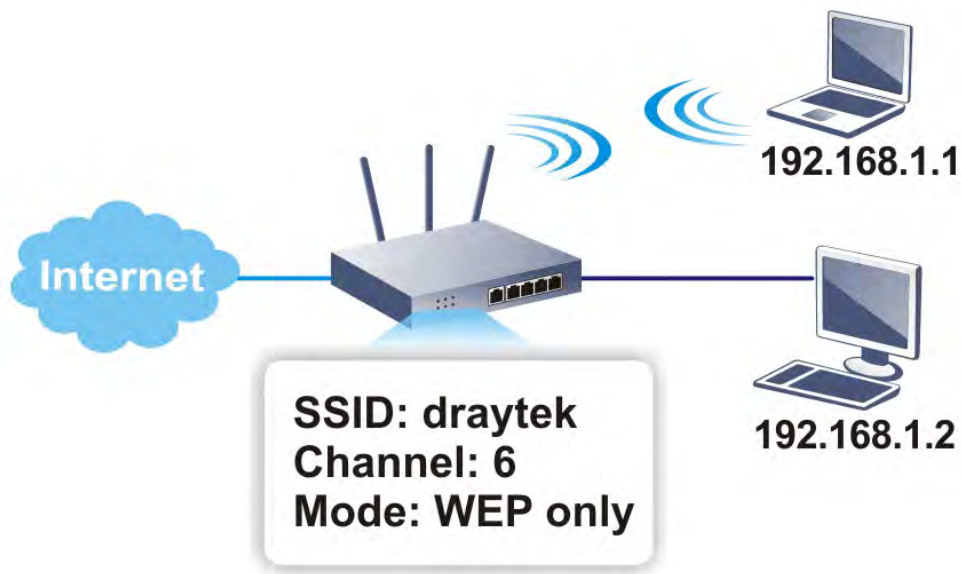
4.13.1 Basic Concepts

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

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

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

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



Multiple SSIDs

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

Security Overview

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

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

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

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

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

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

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

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

Below shows the menu items for Wireless LAN.



4.13.2 General Setup

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

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

Index(1-15) in [Schedule](#) Setup: , , ,

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.

Isolate VPN: isolate wireless with remote dial-in and LAN to LAN VPN.

Channel: Channel 6, 2437MHz Long Preamble:

Long Preamble: necessary for some old 802.11 b devices only(lower performance)

Packet-OVERDRIVE™

Tx Burst

Note:
The same technology must also be supported in clients to boost WLAN performance.

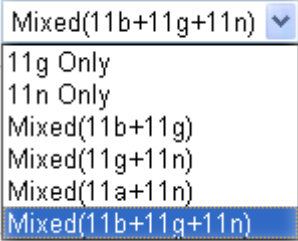
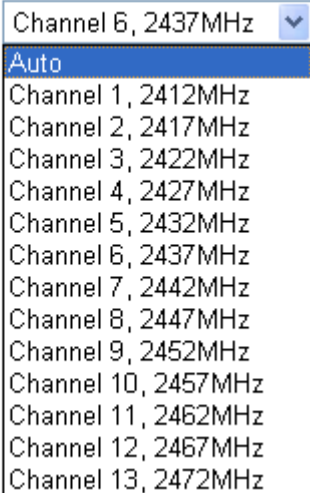
Rate Control

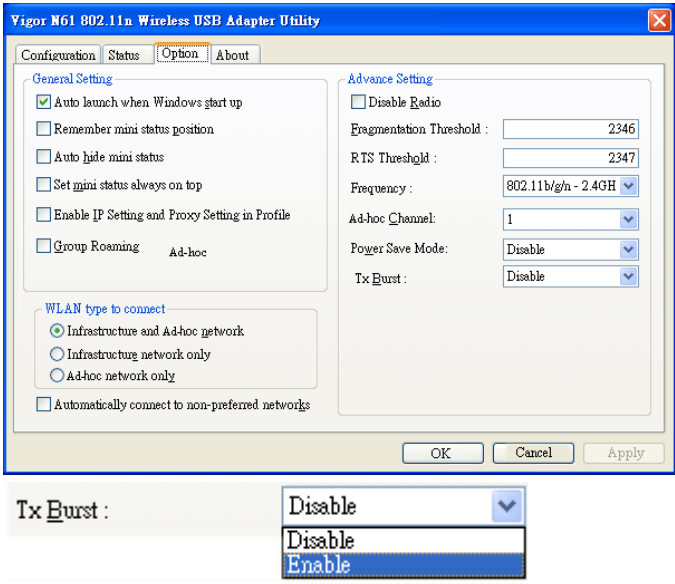
	Enable	Upload	Download
SSID 1	<input type="checkbox"/>	30000 kbps	30000 kbps
SSID 2	<input type="checkbox"/>	30000 kbps	30000 kbps
SSID 3	<input type="checkbox"/>	30000 kbps	30000 kbps
SSID 4	<input type="checkbox"/>	30000 kbps	30000 kbps

Note: range 100~50,000 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.

	 <p>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.</p>
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 Applications >> Schedule 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	<p>VPN – Check this box to make the wireless clients (stations) with different VPN not accessing for each other.</p> <p>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</p>
Channel	<p>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.</p> 

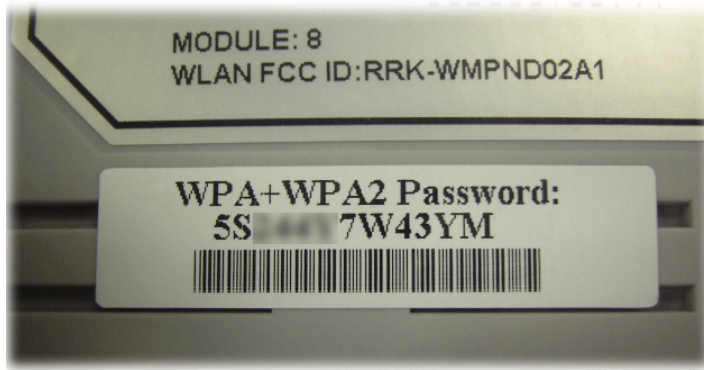
<p>Long Preamble</p>	<p>This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.</p>
<p>Packet-OVERDRIVE</p>	<p>This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burst). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.</p> <p>Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose Enable for TxBURST on the tab of Option).</p>  <p>Note: * means the real transmission rate depends on the environment of the network.</p>
<p>Rate Control</p>	<p>It controls the data transmission rate through wireless connection.</p> <p>Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.</p> <p>Download – Type the transmitting rate for data download. Default value is 30,000 kbps.</p>

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

4.13.3 Security

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

The default security mode is **Mixed (WPA+WPA2)/PSK**. Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.

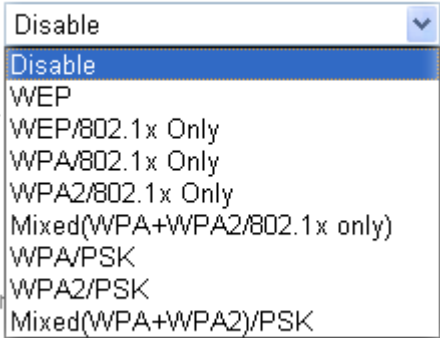


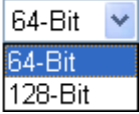
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

[Wireless LAN >> Security Settings](#)

SSID 1	SSID 2	SSID 3	SSID 4
Mode: <input type="text" value="Disable"/>			
Set up RADIUS Server if 802.1x is enabled.			
WPA:			
Encryption Mode: TKIP for WPA/AES for WPA2			
Pre-Shared Key(PSK): <input type="text" value="*****"/>			
Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".			
WEP:			
Encryption Mode: <input type="text" value="64-Bit"/>			
<input checked="" type="radio"/> Key 1 : <input type="text" value="*****"/>			
<input type="radio"/> Key 2 : <input type="text" value="*****"/>			
<input type="radio"/> Key 3 : <input type="text" value="*****"/>			
<input type="radio"/> Key 4 : <input type="text" value="*****"/>			
For 64 bit WEP key			
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".			
For 128 bit WEP key			
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".			

Available settings are explained as follows:

Item	Description
<p>Mode</p>	<p>There are several modes provided for you to choose.</p>  <p>Note: You should also set RADIUS Server simultaneously if 802.1x mode is selected.</p> <p>Disable - Turn off the encryption mechanism.</p> <p>WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.</p> <p>WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.</p> <p>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.</p> <p>WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.</p> <p>WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.</p> <p>Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.</p>
<p>WPA</p>	<p>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...").</p> <p>Type - Select from Mixed (WPA+WPA2) or WPA2 only.</p> <p>Pre-Shared Key (PSK) - Either 8~63 ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such</p>

Item	Description
	as "0x321253abcde...").
WEP	<p>64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)</p> <p>128-Bit - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).</p> <p>Encryption Mode: </p> <p>All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.</p>

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

4.13.4 Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

Wireless LAN >> Access Control

Access Control

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 MAC Address : : : : : :

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

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	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

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

4.13.5 WPS

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



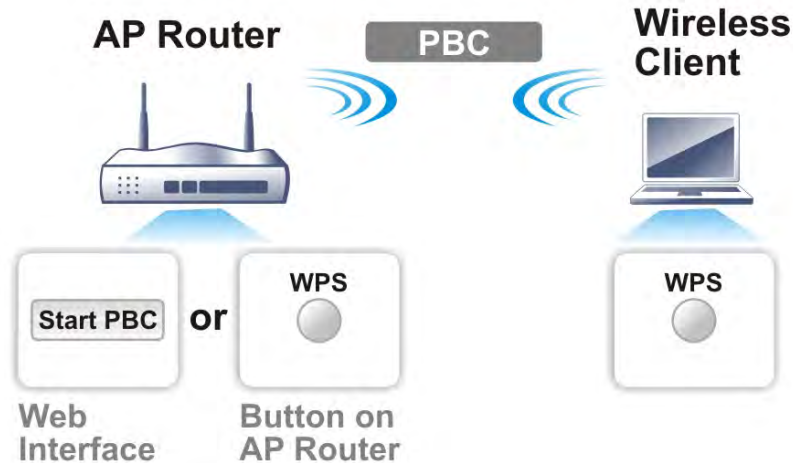
Note: Such function is available for the wireless station with WPS supported.

It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to

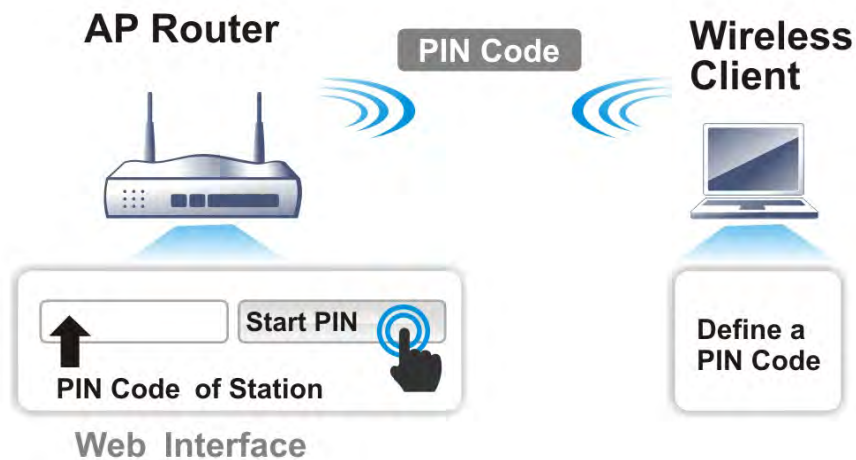
setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

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

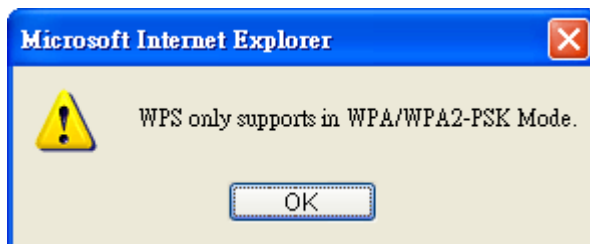
- On the side of Vigor 3200 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- 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.



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	<input type="button" value="Start PBC"/>
Configure via Client PinCode	<input type="text"/> <input type="button" value="Start PIN"/>

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

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

: WPS is Disabled.

: WPS is Enabled.

: Waiting for WPS requests from wireless clients.

Available settings are explained as follows:

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 Start PBC 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 Start PIN button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

4.13.6 WDS

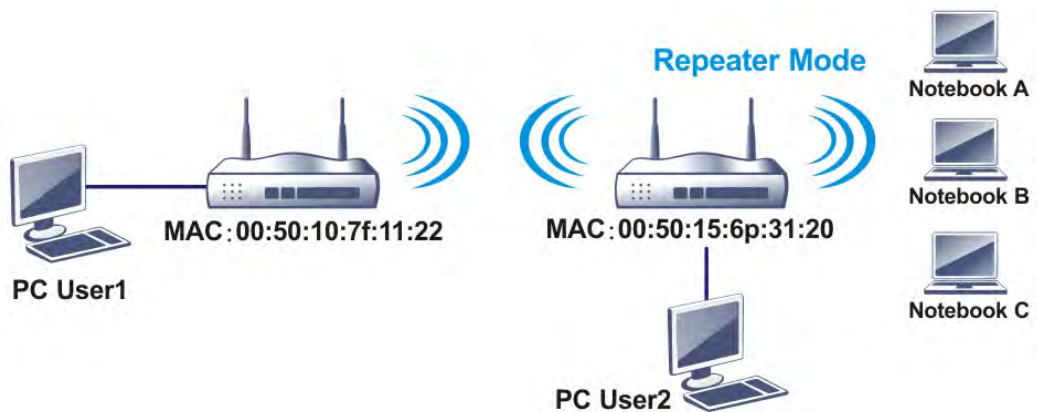
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

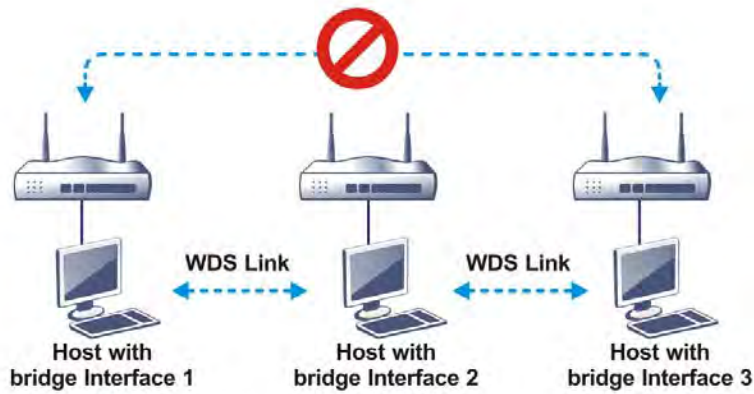


The application for the WDS-Repeater mode is depicted as below:



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

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



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

Wireless LAN >> WDS Settings

WDS Settings
[Set to Factory Default](#)

Mode: Bridge

Security:
 Disable WEP Pre-shared Key

WEP:
 Use the same WEP key set in [Security Settings](#).

Pre-shared Key:
 Type:
 DrayTek WPA WPA WPA2
 Key :
Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

Bridge

Enable Peer MAC Address

<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>

Note: Disable unused links to get better performance.

Repeater

Enable Peer MAC Address

<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>

Access Point Function:
 Enable Disable

Status:
 Send "Hello" message to peers.

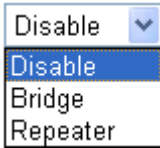
Link Status

Note: The status is valid only when the peer also supports this function.

OK
Cancel

Available settings are explained as follows:

Item	Description
Mode	Choose the mode for WDS setting. Disable mode will not invoke any WDS setting. Bridge mode is designed to fulfill the first type of application. Repeater mode is for the second one.

Item	Description
	
Security	There are three types for security, Disable , WEP and Pre-shared key . 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 Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
Pre-shared Key	<p>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.</p> <p>Key - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.</p>
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 Enable 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 Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable 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.

4.13.7 Advanced Setting

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

Wireless LAN >> Advanced Setting

HT Physical Mode

Operation Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Bandwidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> auto
Aggregation MSDU(A-MSDU)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

OK

Available settings are explained as follows:

Item	Description
Operation Mode	<p>Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.</p> <p>Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.</p>
Channel Bandwidth	<p>20- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</p> <p>20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</p>
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto 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 Enable .

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

4.13.8 WMM Configuration

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

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

WMM Configuration | [Set to Factory Default](#) |

WMM Capable Enable Disable
 APSD Capable Enable Disable

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Available settings are explained as follows:

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the Enable radio button.
APSD Capable	The default setting is Disable .
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	CWMin means contention Window-Min and CWMax 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.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is

Item	Description
	checked. Note: 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 **OK** to save the configuration.

4.13.9 AP Discovery

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

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

[Wireless LAN >> Access Point Discovery](#)

Access Point List

BSSID	Channel	SSID

See [Statistics](#).

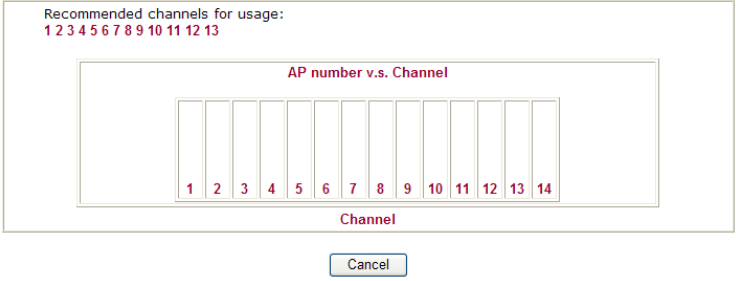
Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to [WDS Settings](#) :

AP's MAC address : : : : :

Bridge Repeater

Available settings are explained as follows:

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 
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click Add to . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

4.13.10 Station List

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

Wireless LAN >> Station List

Station List

Status	MAC Address	Associated with

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to [Access Control](#) :

Client's MAC address : : : : :

Available settings are explained as follows:

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 .

4.14 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.



4.14.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

SSL VPN General Setup

Bind to WAN	<input checked="" type="checkbox"/> WAN1	<input checked="" type="checkbox"/> WAN2	<input checked="" type="checkbox"/> WAN3	<input checked="" type="checkbox"/> WAN4	<input checked="" type="checkbox"/> WAN5	<input checked="" type="checkbox"/> WAN6
Port	443 (Default: 443)					
Server Certificate	self-signed ▼					

Note: The settings will act on all SSL applications.

Please go to [System Maintenance >> Management](#) to enable SSLv3.0 .

OK Cancel

Available settings are explained as follows:

Item	Description
Bind to WAN	Choose and check WAN interface(s) for SSL VPN tunnel establishment.
Port	Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in System Maintenance>>Management . 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 Self-signed to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

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

4.14.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.

[SSL VPN >> SSL Web Proxy](#)

SSL Web Proxy Servers Profiles: [Set to Factory Default](#)

Index	Name	URL	Active
1.			x
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

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](#)

Profile Index : 1

Name	<input type="text"/>
URL	<input type="text"/>
Host IP Address	<input type="text"/>
Access Method	<input type="text" value="Disable"/> <ul style="list-style-type: none"> Disable Secured Port Redirection SSL

Note:

1. URL format must be entered as `http://ip.port/directory` or `http://Domain_name/directory` where Domain_name is a FQDN.
2. SSL proxy cannot be compatible with all websites, many websites developed with new web coding technology may not work with proxy mode. We suggest using SSL Tunnel when SSL proxy is not working.

Available settings are explained as follows:

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	<p>There are three modes for you to choose</p> <p>Disable – the profile will be inactive. If you choose Disable, all the web proxy profile appeared under VPN remote dial-in web page will disappear.</p> <p>Secured Port Redirection – 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.</p> <p>SSL – if you choose such selection, web proxy over SSL will be applied for VPN.</p>

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

4.14.3 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 Application](#)

SSL Applications Profiles: [Set to Factory Default](#)

Index	Name	Host Address	Service	Active
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

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 Application](#)

Profile Index : 1

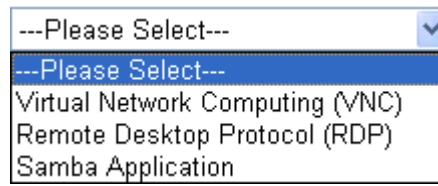
Enable Application Service
 Application Name
 Application
 Samba Path

Note: Samba Path format must be entered as \\ip\directory or \\Computer Name\directory.

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

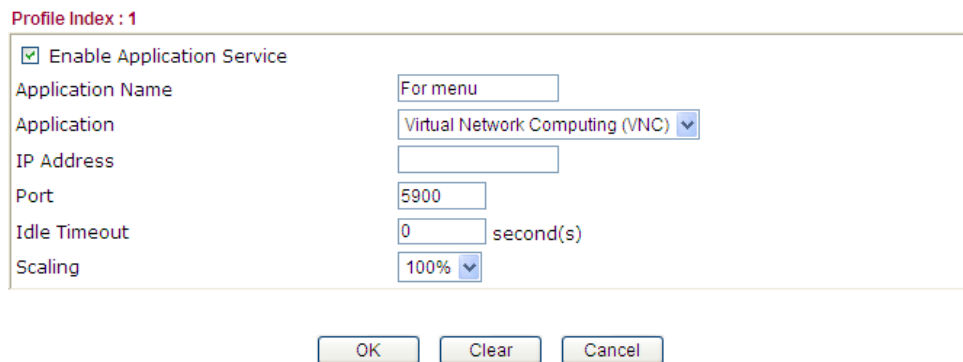
this profile.



Different application type will lead different web pages.
Refer to the following:

- **Virtual Network Computing** – Choose this item for accessing and controlling a remote PC through VNC protocol.

SSL VPN >> SSL Application



IP Address - Type the IP address for this protocol.

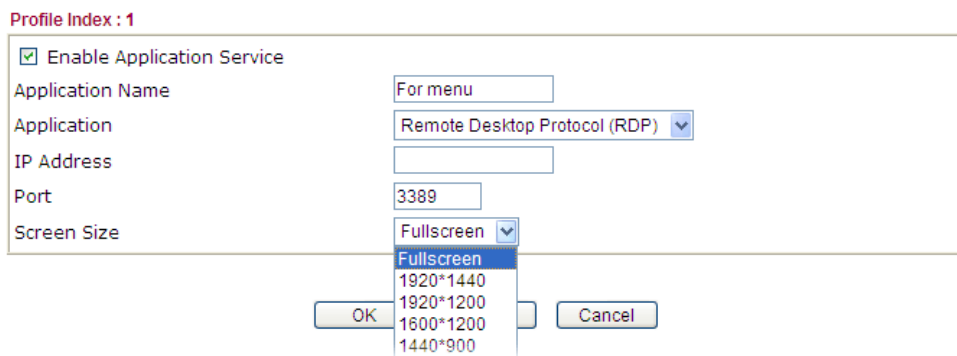
Port - Specify the port used for this protocol. The default setting is 5900.

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.

SSL VPN >> SSL Application



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

SSL VPN >> SSL Application

Profile Index : 1

<input type="checkbox"/> Enable Application Service	
Application Name	<input type="text"/>
Application	Samba Application <input type="button" value="v"/>
Samba Path	<input type="text"/>

Note: Samba Path format must be entered as \\ip\directory or \\Computer Name\directory.

Samba Path - Specify the path for this application.

4.14.4 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**.

SSL VPN >> Remote Dial-in User

Remote Access User Accounts: | [Set to Factory Default](#) |

View: All Online Offline Search

Index	User	Active	Status	Index	User	Active	Status
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >>

[Next](#) >>

Note: User Accounts need to be added into User Group to enable SSL Portal Login.

Click each index to edit one remote user profile.

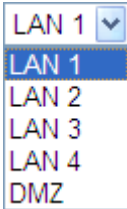
SSL VPN >> Remote Dial-in User

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <p>Subnet</p> <p><input type="text" value="LAN 1"/></p> <p><input type="checkbox"/> Assign Static IP Address</p> <p><input type="text" value="0.0.0.0"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password(Max 19 char) <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP)</p> <p>PIN Code <input style="width: 100px;" type="text"/></p> <p>Secret <input style="width: 100px;" type="text"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium(AH)</p> <p>High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID (optional) <input style="width: 100px;" type="text"/></p>
--	--

Available settings are explained as follows:

Item	Description
User account and Authentication	<p>Enable this account - Check the box to enable this function.</p> <p>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.</p>
Allowed Dial-In Type	<p>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.</p> <p>IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.</p> <p>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:</p> <ul style="list-style-type: none"> ● 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.

Item	Description
	<p>SSL Tunnel - 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)</p> <p>If you check this box, the function of SSL Tunnel for this account will be activated immediately.</p> <p>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.</p> <p>Netbios Naming Packet</p> <ul style="list-style-type: none"> ● 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. <p>Multicast via VPN - Some programs might send multicast packets via VPN connection.</p> <ul style="list-style-type: none"> ● Pass – Click this button to let multicast packets pass through the router. ● Block – This is default setting. Click this button to let multicast packets be blocked by the router.
Subnet	<p>Chose one of the subnet selections for such VPN profile.</p>  <p>Assign Static IP Address – Please type a static IP address for the subnet you specified.</p>
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Enable Mobile One-Time Passwords (mOTP)	<p>Check this box to make the authentication with mOTP function.</p> <p>PIN Code – Type the code for authentication (e.g., 1234).</p> <p>Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).</p>
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)

Item	Description
	<p>can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.</p> <p>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.</p> <p>Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.</p>
IPSec Security Method	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

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

4.14.5 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](#)

SSL User Group Profiles: [Set to Factory Default](#)

Index	Name	Status
1.		x
2.		x
3.		x
4.		x
5.		x
6.		x
7.		x
8.		x
9.		x
10.		x

Each item is explained as follows:

Item	Description
Index	Display the number of the client which connecting to FTP server.
Name	Display the name of the group profile.

Click any index number link to open the following page for detailed configuration.

[SSL VPN >> User Group](#)

Index No. 1

Enable

Group Name

Access Authority

SSL Web Proxy SSL Application
 Web_Test For menu


Authentication Methods

Local User DataBase

Available User Accounts	Selected User Accounts
<input type="button" value=">>"/> <input type="button" value="<<"/>	

RADIUS
 LDAP / Active Directory

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable such profile.
Group Name	Type a name for such profile.
Access Authority	<p>Specify the authority for such profile.</p> <p>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.</p>  <p>The screenshot shows a section titled "Access Authority" with a list of four items: "SSL Web Proxy" (checked), "SSL Application" (checked), "Web_Test" (unchecked), and "For menu" (unchecked). Below this list is a section titled "Authentication Methods".</p>
Authentication Methods	<p>It can determine the authentication method used for such profile.</p> <p>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.</p> <p>RADIUS – The RADIUS server will do the authentication by using the username and password</p> <p>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.</p> <p>If the above three options are enabled, the system will do the authentication based on them in sequence.</p>

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

4.14.6 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.

The screenshot shows the DrayTek SSL VPN portal interface. At the top left is the DrayTek logo. Below it, the text 'Provide SSL VPN' is visible. The main navigation bar includes 'Home', 'SSL Web Proxy', and 'SSL Tunnel', with 'SSL Web Proxy' selected. A '[logout]' link is in the top right corner. On the left, an 'INFO' box displays the user 'mike' with IP '172.17.1.42' and a 'Welcome to DrayTek SSL VPN!' message. Below this, it states 'Timeout after 5 minutes.' with a '[Reset]' link. The main content area, titled 'Main Page:', shows a success message: 'You have successfully logged in! You are given the following privileges:' followed by a list of two items: 'SSL Web Proxy' and 'SSL Tunnel'. At the bottom right, there is a copyright notice: 'Copyright © 2006, DrayTek Corp. All Rights Reserved.'

Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.

SSL VPN >> Online Status

Refresh Seconds :

Active User	Host IP	Time out(seconds)	Action
caesar	172.17.1.42	292	<input type="button" value="Drop"/>

Each item is explained as follows:

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.

4.15 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.



4.15.1 USB General Settings

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

USB Application >> USB General Settings

USB General Settings

General Settings

Simultaneous FTP Connections: (Maximum 6)

Default Charset:

Samba Service Settings(Network Neighborhood)

Enable Disable

Access Mode

LAN Only LAN And WAN

NetBios Name Service

Workgroup Name:

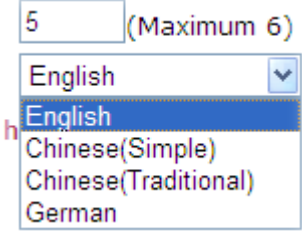
Host Name:

Note: 1. If Charset is set to "English", only English long file name is supported.
 2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
 3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: . : " < > * + = / \ | ?.

OK

Available settings are explained as follows:

Item	Description
General Settings	<p>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.</p> <p>Default Charset - At present, Vigor router supports several</p>

Item	Description
	<p>types of character sets.</p> 
Samba Service Settings	Click Enable to invoke samba service via the router.
Access Mode	<p>LAN Only – Users coming from internet cannot connect to the samba server of the router.</p> <p>LAN And WAN - Both LAN and WAN users can access samba server of the router.</p>
NetBios Name Service	<p>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--- ; : " < > * + = \ ?.</p> <p>Workgroup Name – Type a name for the workgroup.</p> <p>Host Name – Type the host name for the router.</p>

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

4.15.2 USB User Management

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

[USB Application >> USB User Management](#)

USB User Management			Set to Factory Default		
Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		

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


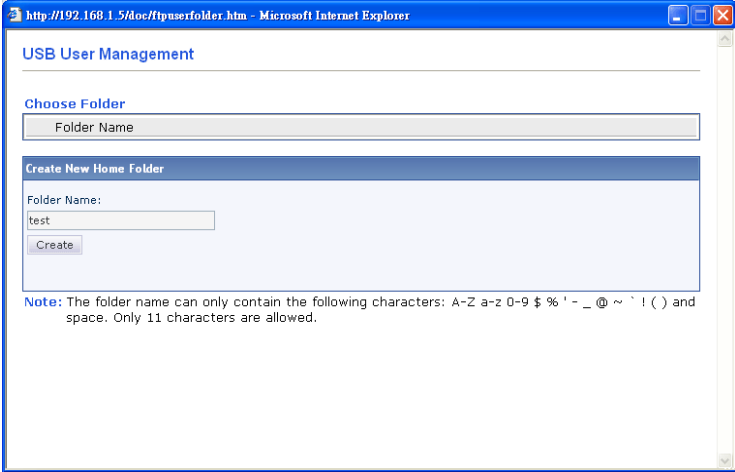
Profile Index: 1

FTP/Samba User	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/> (Maximum 11 Characters)
Confirm Password	<input type="text"/>
Home Folder	<input type="text"/> 
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () / and space.

Available settings are explained as follows:

Item	Description
FTP/Samba User	<p>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.</p> <p>Disable – Click this button to disable such profile.</p>
Username	<p>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.</p> <div style="border: 1px solid black; padding: 5px;"> <p>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.</p> <p>Note: FTP Passive mode is not supported by Vigor Router.</p> <p>Please disable that mode on the FTP client.</p> </div>
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 Folder	It determines the folder for the client to access into. The user can enter a directory name in this field. Then, after clicking OK , the router will create the specific/new folder in the USB storage disk. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB

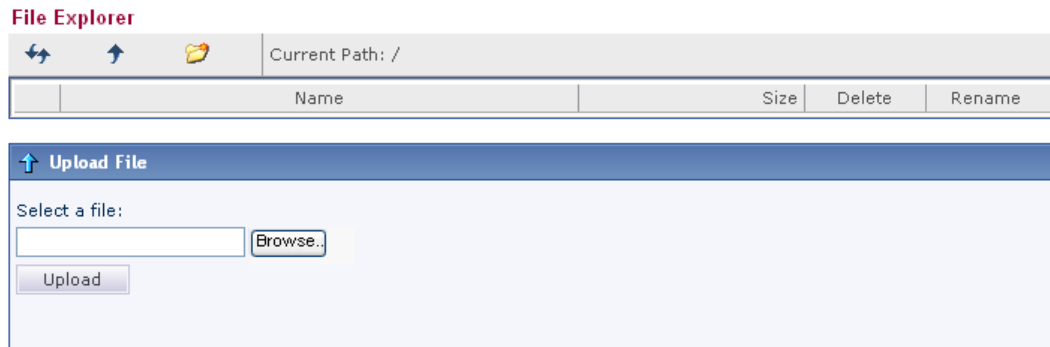
Item	Description
	<p>storage disk.</p> <p>Note: When write protect status for the USB storage disk is ON, you cannot type any new folder name in this field. Only “/” can be used in such case.</p> <p>You can click  to open the following dialog to add any new folder which can be specified as the Home Folder.</p> 
Access Rule	<p>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.</p> <p>File – Check the items (Read, Write and Delete) for such profile.</p> <p>Directory –Check the items (List, Create and Remove) for such profile.</p>

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.

4.15.3 File Explorer

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

[USB Application >> File Explorer](#)



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

Available settings are explained as follows:

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.

4.15.4 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 Device Status](#)



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.

4.15.5 Modem Support List

Such page provides the information about the brand name and model name of the USB modems which are supported by Vigor router.

USB Application >> Modem Support List

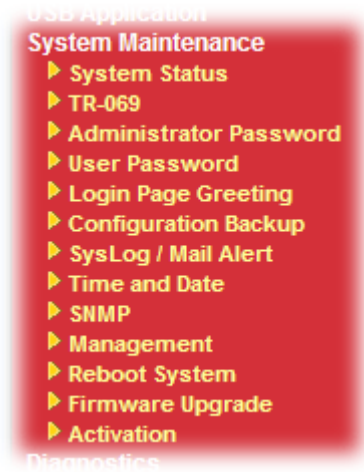
The following compatibility tests listed above Vigor router models with USB modems / mobiles. If it is confirmed as the latest and still does not work, please contact support@draytek.com

3.5G		
Brand	Model	Status
Alcatel	L100V	Y
Alcatel	W100	Y
AnyDATA	ADU-500A	Y
AnyDATA	ADU-510A	Y
BandRich	Bandlux C321	Y
Huawei	Huawei E150	Y
Huawei	Huawei E153	Y
Huawei	Huawei E160E	Y
Huawei	Huawei E171	Y
Huawei	Huawei E173	Y
Huawei	Huawei E1750C	Y
Huawei	Huawei E176c	Y
Huawei	Huawei E177	Y
Huawei	Huawei E188	Y
Huawei	Huawei EC306	Y
Mobidata	MBD-220HU	Y

4.16 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.16.1 System Status

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

System Status

Model Name : Vigor3200
Firmware Version : 3.6.8.5
Build Date/Time : Jun 1 2016 10:57:08

LAN					
	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-CE-46-FC	192.168.1.1	255.255.255.0	ON	8.8.8.8
LAN2	00-50-7F-CE-46-FC	192.168.2.1	255.255.255.0	ON	8.8.8.8
LAN3	00-50-7F-CE-46-FC	192.168.3.1	255.255.255.0	ON	8.8.8.8
LAN4	00-50-7F-CE-46-FC	192.168.4.1	255.255.255.0	ON	8.8.8.8
DMZ PORT	00-50-7F-CE-46-FC	192.168.5.1	255.255.255.0	ON	8.8.8.8
IP Routed Subnet	00-50-7F-CE-46-FC	192.168.0.1	255.255.255.0	ON	8.8.8.8

WAN					
	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Disconnected	00-50-7F-CE-46-FD	---	---	---
WAN2	Disconnected	00-50-7F-CE-46-FE	---	---	---
WAN3	Disconnected	00-50-7F-CE-46-FF	---	---	---
WAN4	Disconnected	00-50-7F-CE-46-00	---	---	---
WAN5	Disconnected	00-50-7F-CE-46-01	---	---	---

IPv6			
	Address	Scope	Internet Access Mode
LAN	FE80::250:7FFF:FECE:46FC/64	Link	---

User Mode is OFF now.

Each item is explained as follows:

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	<p>MAC Address - Display the MAC address of the LAN Interface.</p> <p>IP Address - Display the IP address of the LAN interface.</p> <p>Subnet Mask - Display the subnet mask address of the LAN interface.</p> <p>DHCP Server - Display the current status of DHCP server of the LAN interface</p> <p>DNS - Display the assigned IP address of the primary DNS.</p>
Wireless LAN	<p>MAC Address - Display the MAC address of the wireless LAN.</p> <p>Frequency Domain - It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.</p> <p>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.</p> <p>SSID - Display the SSID of the router.</p>
WAN	<p>Link Status - Display current connection status.</p> <p>MAC Address - Display the MAC address of the WAN Interface.</p> <p>Connection - Display the connection type.</p> <p>IP Address - Display the IP address of the WAN interface.</p> <p>Default Gateway - Display the assigned IP address of the default gateway.</p>
IPv6	<p>Address - Display the IPv6 address for LAN.</p> <p>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.</p> <p>Internet Access Mode – Display the connection mode chosen for accessing into Internet.</p>

4.16.2 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.

[System Maintenance >> TR-069 Setting](#)

ACS and CPE Settings

ACS Server On	Internet
ACS Server	
URL	<input type="text"/> <input type="button" value="Wizard"/>
Username	<input type="text"/>
Password	<input type="text"/>
	<input type="button" value="Test With Inform"/> Event Code
	PERIODIC
Last Inform Response Time :(NA)	●
CPE Client	
<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
<input type="radio"/> Http <input type="radio"/> Https	
URL	<input type="text"/>
Port	8069
Username	vigor
Password	*****

Periodic Inform Settings

<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	
Interval Time	900 second(s)

STUN Settings

<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
Server Address	<input type="text"/>
Server Port	3478
Minimum Keep Alive Period	60 second(s)
Maximum Keep Alive Period	-1 second(s)

Available parameters are explained as follows:

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<p>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.</p> <p>Test With Inform – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server.</p> <p>Event Code – Use the drop down menu to specify an event to perform the test.</p> <p>Last Inform Response Time – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.</p>

Item	Description
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. Username and Password – Type the username and password that VigorACS can use to access into such 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 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.

4.16.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="text"/>	
New Password	<input type="text"/>	(Max. 23 characters allowed)
Confirm Password	<input type="text"/>	(Max. 23 characters allowed)

Note: Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()

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.

4.16.4 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**.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password | [Set to Factory Default](#) |

Password	<input type="text"/>
Confirm Password	<input type="text"/>

Note: 1.Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()
 2.Password can't be only *.Example: '*' or '**' or '***' is illegal, but '123*' or '*45' is OK.

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**.

System Maintenance >> User Password

Enable User Mode for simple web configuration

User Password | [Set to Factory Default](#) |

Password	<input type="password"/>
Confirm Password	<input type="password"/>

Note: Password can contain only a-z A-Z 0-9 , ; : . " < > * + = \ | ? @ # ^ ! ()

3. The following screen will appear. Simply click **OK**.

Active Configuration

Password	: *****
----------	---------

4. Log out Vigor router Web user interface.

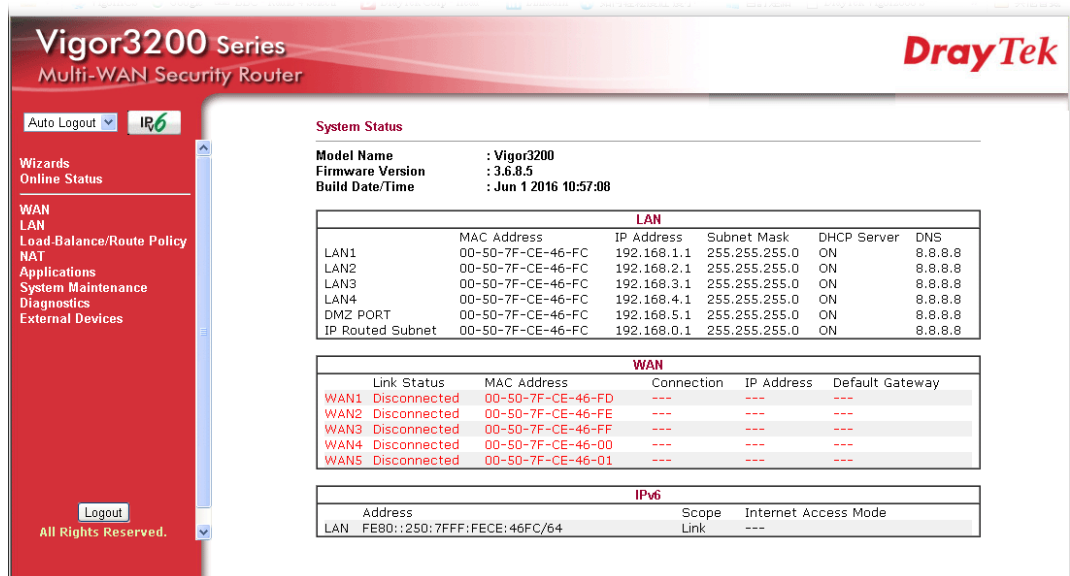


5. The following window will be open to ask for username and password. Type the new user password in the field of **Password** and click **Login**.

A screenshot of the login window. It has a light gray background with rounded corners. On the left, there are labels 'Username' and 'Password'. To the right of 'Username' is a white text input field. To the right of 'Password' is a white text input field with four black dots. Below the input fields is a 'Login' button. At the bottom right, there is a red and black banner with the 'DrayTek' logo.

Copyright © 2016 DrayTek Corp. All Rights Reserved.

6. The main screen with User Mode will be shown as follows.



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

4.16.5 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.

[System Maintenance >> Login Page Greeting](#)

Login Page Greeting

Enable

Login Page Title (31 char max.)

Welcome Message and Bulletin (Max 511 characters) [Preview](#) | [Set to Factory Default](#) |

```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p><ol><li>The welcome message can be written in HTML so lists such as this one can be created </li><li>Other markup tags such as p, font or img can be used</li></ol>
```

Examples of Welcome Message and Bulletin:

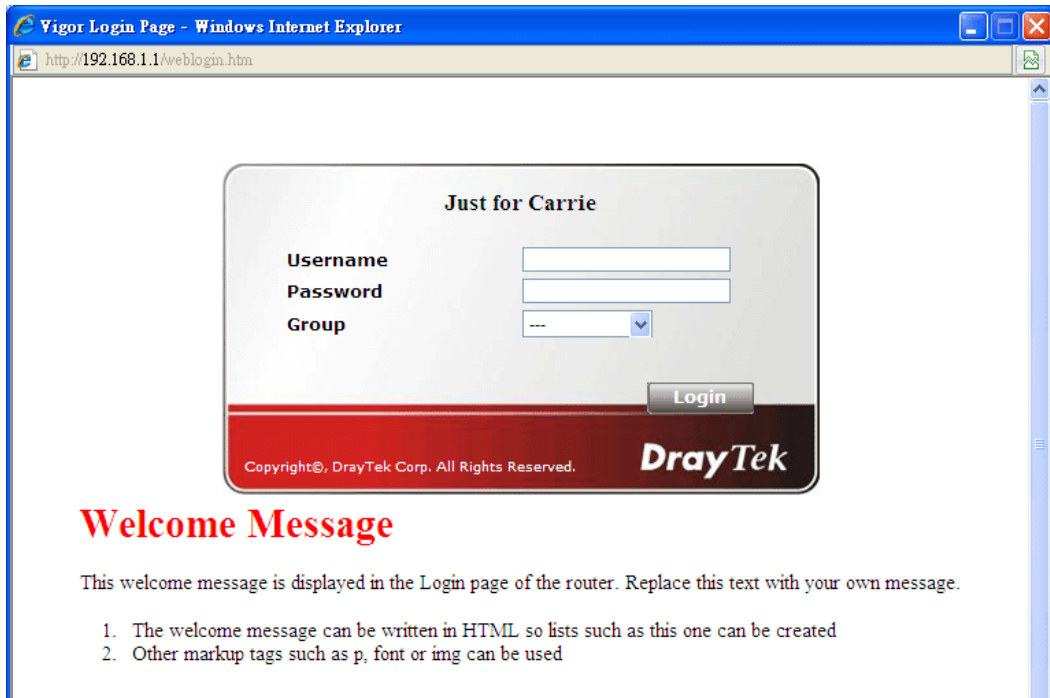
```
<h1><b><font color=red>Welcome Message</font></b></h1>
<p>Message</p>
```

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 based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Description and Bulletin.



4.16.6 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

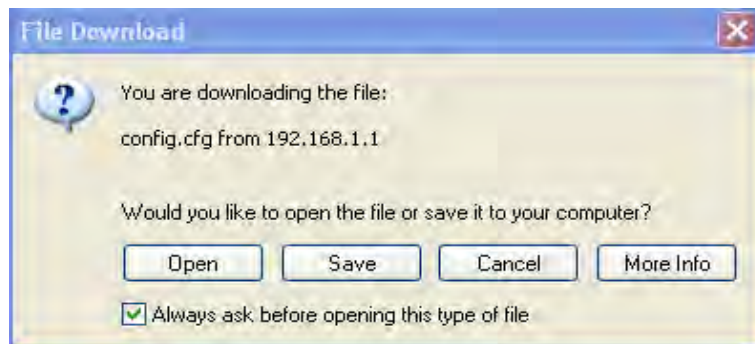
Select a configuration file.

Click Restore to upload the file.

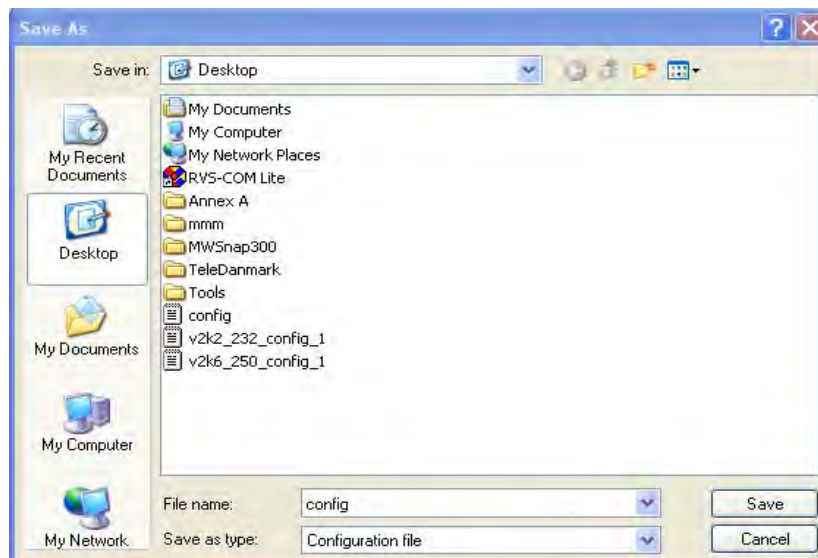
Backup

Click Backup to download current running configurations as a file.

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



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



4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Note: Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

<p>Restoration</p> <p>Select a configuration file.</p> <input type="text"/> <input type="button" value="Browse.."/> <p>Click Restore to upload the file.</p> <input type="button" value="Restore"/>
<p>Backup</p> <p>Click Backup to download current running configurations as a file.</p> <input type="button" value="Backup"/> <input type="button" value="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.

4.16.7 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.

[System Maintenance >> SysLog / Mail Alert Setup](#)

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Syslog Save to:</p> <p><input checked="" type="checkbox"/> Syslog Server</p> <p><input type="checkbox"/> USB Disk</p> <p>Router Name <input style="width: 100%;" type="text"/></p> <p>Server IP Address <input style="width: 100%;" type="text"/></p> <p>Destination Port <input style="width: 50%;" type="text" value="514"/></p> <p>Mail Syslog <input type="checkbox"/> Enable</p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p> <p>AlertLog Setup</p> <p><input type="checkbox"/> Enable</p> <p>AlertLog Port <input style="width: 50%;" type="text" value="514"/></p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input style="width: 100%;" type="text"/></p> <p>SMTP Port <input style="width: 50%;" type="text" value="25"/></p> <p>Mail To <input style="width: 100%;" type="text"/></p> <p>Return-Path <input style="width: 100%;" type="text"/></p> <p><input type="checkbox"/> Use SSL</p> <p><input type="checkbox"/> Authentication</p> <p>Username <input style="width: 100%;" type="text"/></p> <p>Password <input style="width: 100%;" type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> VPN LOG</p>
--	--

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.
 3. We only support secured SMTP connection on port 465.

Available parameters are explained as follows:

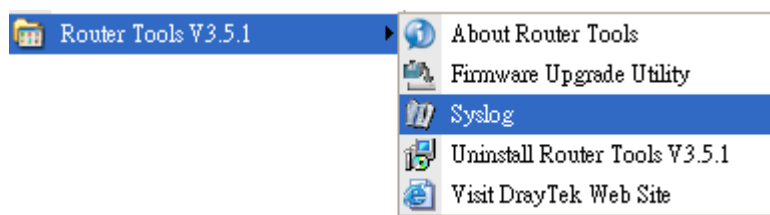
Item	Description
SysLog Access Setup	<p>Enable - Check Enable to activate function of syslog.</p> <p>Syslog Save to – Check Syslog Server to save the log to Syslog server.</p> <p>USB Disk - Check USB Disk to save the log to the attached USB storage disk.</p> <p>Router Name - Display the name for such router configured in System Maintenance>>Management.</p> <p>If there is no name here, simply lick the link to access into System Maintenance>>Management to set the router name.</p> <p>Server IP Address -The IP address of the Syslog server.</p> <p>Destination Port - Assign a port for the Syslog protocol.</p> <p>Mail Syslog – Check the box to recode the mail event on Syslog.</p> <p>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.</p>
AlertLog Setup	<p>Check Enable to activate function of alert log.</p>

Item	Description
	AlertLog Port - Type the port number for alert log. The default setting is 514.
Mail Alert Setup	<p>Check Enable to activate function of mail alert.</p> <p>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.</p> <p>SMTP Server/SMTP Port - The IP address/Port number of the SMTP server.</p> <p>Mail To - Assign a mail address for sending mails out.</p> <p>Return-Path - Assign a path for receiving the mail from outside.</p> <p>Use SSL - Check this box to use port 465 for SMTP server for some e-mail server uses https as the transmission method.</p> <p>Authentication - Check this box to activate this function while using e-mail application.</p> <ul style="list-style-type: none"> ● User Name - Type the user name for authentication. ● Password - Type the password for authentication. <p>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.</p>

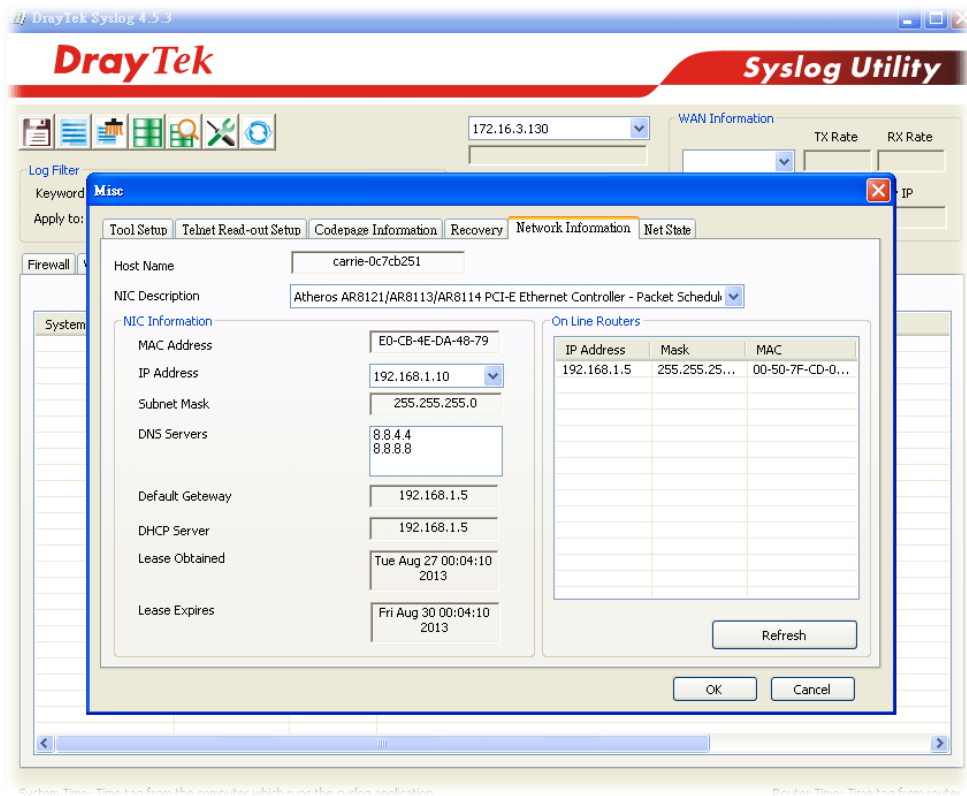
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



4.16.8 Time and Date

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

System Maintenance >> Time and Date

Time Information

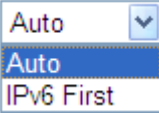
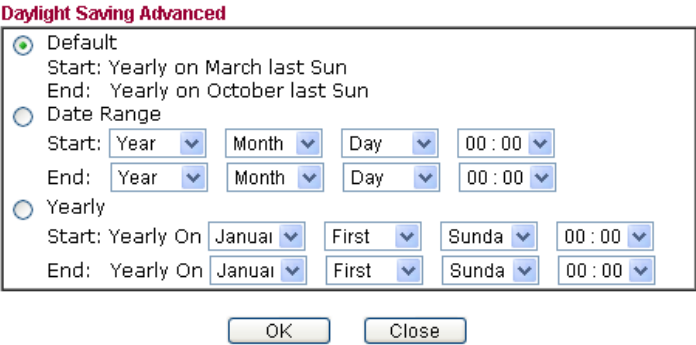
Current System Time	2000 Jan 1 Sat 0 : 16 : 53	<input type="button" value="Inquire Time"/>
---------------------	----------------------------	---

Time Setup

<input type="radio"/>	Use Browser Time	
<input checked="" type="radio"/>	Use Internet Time	
	Time Server	<input type="text" value="pool.ntp.org"/>
	Priority	<input type="text" value="Auto"/>
	Time Zone	<input type="text" value="(GMT) Greenwich Mean Time : Dublin"/>
	Enable Daylight Saving	<input type="checkbox"/> <input type="button" value="Advanced"/>
	Automatically Update Interval	<input type="text" value="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.

Item	Description
Time Server	Type the IP address or domain name of the time server.
Priority	<p>IPv6 First – If the time server configured with a domain name that supports IPv6; such option will be the first choice.</p> <p>Auto – It is the default setting. If you have no idea whether the time server supports IPv6 or IPv4, simply choose Auto as the priority.</p> 
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	<p>Check the box to enable the daylight saving. Such feature is available for certain area.</p> <p>Advanced – Click it to open a pop up dialog.</p>  <p>Use the default time setting or set user defined time for your requirement.</p>
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.16.9 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.

System Maintenance >> SNMP

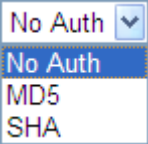
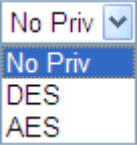
SNMP Setup

<input checked="" type="checkbox"/> Enable SNMP Agent	
Get Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
Manager Host IP(IPv4)	Index IP Subnet Mask
	1 <input type="text"/> <input type="text" value=""/>
	2 <input type="text"/> <input type="text" value=""/>
	3 <input type="text"/> <input type="text" value=""/>
Manager Host IP(IPv6)	Index IPv6 Address / Prefix Length
	1 <input type="text"/> / <input type="text" value="0"/>
	2 <input type="text"/> / <input type="text" value="0"/>
	3 <input type="text"/> / <input type="text" value="0"/>
Trap Community	<input type="text" value="public"/>
Notification Host IP(IPv4)	Index IP
	1 <input type="text"/>
	2 <input type="text"/>
Notification Host IP(IPv6)	Index IPv6 Address
	1 <input type="text"/>
	2 <input type="text"/>
Trap Timeout	<input type="text" value="10"/>
<input type="checkbox"/> Enable SNMPV3 Agent	
USM User	<input type="text"/>
Auth Algorithm	<input type="text" value="No Auth"/>
Auth Password	<input type="text"/>
Privacy Algorithm	<input type="text" value="No Priv"/>
Privacy Password	<input type="text"/>

OK Cancel

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. 
Auth Password	Type a password for authentication.
Privacy Algorithm	Choose one of the methods listed below as the privacy algorithm. 
Privacy Password	Type a password for privacy.

Click **OK** to save these settings.

4.16.10 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 Management Setup	IPv6 Management Setup												
Router Name <input type="text"/> <input type="checkbox"/> Default: Disable Auto-Logout Internet Access Control <input type="checkbox"/> Allow management from the Internet Domain name allowed <input type="text"/> <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input checked="" type="checkbox"/> TR069 Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet LAN Access Control <input checked="" type="checkbox"/> Allow management from LAN <input checked="" type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input checked="" type="checkbox"/> SSH Server Apply To Subnet <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input checked="" type="checkbox"/> LAN4 <input checked="" type="checkbox"/> DMZ <input checked="" type="checkbox"/> IP Routed Subnet Access List from the Internet <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) TR069 Port <input type="text" value="8069"/> (Default: 8069) SSH Port <input type="text" value="22"/> (Default: 22) TLS/SSL Encryption Setup <input checked="" type="checkbox"/> Enable TLS 1.2 <input checked="" type="checkbox"/> Enable TLS 1.1 <input checked="" type="checkbox"/> Enable TLS 1.0 <input type="checkbox"/> Enable SSL 3.0 External Device Control <input checked="" type="checkbox"/> No respond to External Device
List	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											

Note: Subnet LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.

OK

Available parameters are explained as follows:

Item	Description
Router Name	Type a name as an identification for such router.

<p>Default: Disable Auto-Logout</p>	<p>If it is enabled, the function of auto-logout for web user interface will be disabled.</p>  <p>The web user interface will be open until you click the Logout icon manually.</p> 
<p>Internet Access Control</p>	<p>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.</p> <p>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.</p>
<p>LAN Access Control</p>	<p>Allow management from LAN- Enable the checkbox to allow system administrators to login from LAN interface. There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify.</p> <p>Apply To Subnet – Check the interface for the administrator to use for accessing into web user interface of Vigor router.</p>
<p>Access List from the Internet</p>	<p>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.</p> <p>List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.</p>
<p>Management Port Setup</p>	<p>User Defined Ports - Check to specify user-defined port numbers for the Telnet, HTTP, FTP, SSH servers.</p> <p>Default Ports - Check to use standard port numbers for the Telnet and HTTP servers.</p>
<p>TLS/SSL Encryption Setup</p>	<p>Enable SSL 3.0 – Check the box to enable the function of SSL 3.0 if required.</p> <p>Due to security consideration, the built-in HTTPS and SSL VPN server of the router had upgraded to TLS1.x protocol. If you are using old browser(eg. IE6.0) or old SmartVPN Client, you may still need to enable SSL 3.0 to make sure you can connect, however, it's not recommended.</p>

Device Management	<p>Check the box to enable the device management function for Vigor3200.</p> <p>Respond to external device – If it is enabled, Vigor3200 will be regarded as slave device. When the external device (master device) sends request packet to Vigor3200, Vigor3200 would send back information to respond the request coming from the external device which is able to manage Vigor3200.</p>
--------------------------	---

For IPv6

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup
<p>Management Access Control</p> <p>Allow management from the Internet</p> <p><input type="checkbox"/> Telnet Server (Port : 23)</p> <p><input type="checkbox"/> HTTP Server (Port : 80)</p> <p><input type="checkbox"/> Enable PING from the Internet</p> <hr/> <p>Access List</p> <p>List IPv6 Address / Prefix Length</p> <p>1. <input type="text"/> / <input type="text" value="128"/></p> <p>2. <input type="text"/> / <input type="text" value="128"/></p> <p>3. <input type="text"/> / <input type="text" value="128"/></p> <p>Note : Telnt / Http server port is the same as IPv4.</p>	
<input type="button" value="OK"/>	

Available settings are explained as follows:

Item	Description
Management Access Control	<p>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.</p> <p>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.</p>
Access List	<p>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.</p> <p>IPv6 Address /Prefix Length- Indicate the IP address(es) allowed to login to the router.</p>

Click **OK** to save these settings.

4.16.11 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 ?

- Using current configuration
- Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in **Schedule** Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

Cancel

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for performing system reboot. All the schedules can be set previously in **Applications >> Schedule** web page and you can use the number that you have set in that web page.

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

4.16.12 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.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.6.8.5


Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is complete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

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

System Maintenance >> Firmware Upgrade

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

4.16.13 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>.

System Maintenance >> Activation Activate via interface : auto-selected ▾

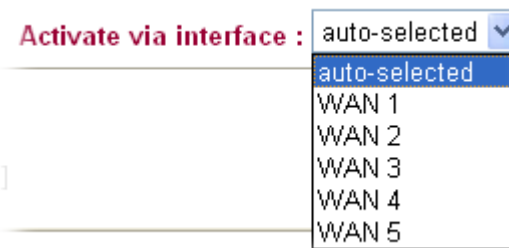
Web-Filter License [Activate](#)
 [Status: **Not Activated**]

Authentication Message

```
WebFilter, service not activate 2010-08-16 07:58:36
```

Note: If you want to use email alert or syslog, please configure the SysLog/Mail Alert Setup page.
 If you change the service provider, the configuration of the function will be reset.

Available parameters are explained as follows:

Item	Description
Activate via Interface	Choose WAN interface used by such device for activating Web Content Filter. 
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:

System Maintenance >> Activation Activate via interface : auto-selected ▾

Web-Filter License [Activate](#)
[Status:Commtouch] [Start Date:2010-07-27 Expire Date:2010-08-27]

Authentication Message

```
Activated Wiz, Activated Wizard query license status Successful, 2010-07-27  
08:47:13
```

Note: If you want to use email alert or syslog, please configure the SysLog/Mail Alert Setup page.
If you change the service provider, the configuration of the function will be reset.

4.17 Diagnostics

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

Below shows the menu items for Diagnostics.

- System Maintenance
- Diagnostics**
- ▶ Dial-out Triggering
- ▶ Routing Table
- ▶ ARP Cache Table
- ▶ IPv6 Neighbour Table
- ▶ DHCP Table
- ▶ NAT Sessions Table
- ▶ DNS Cache Table
- ▶ Data Flow Monitor
- ▶ Traffic Graph
- ▶ Ping Diagnosis
- ▶ Trace Route
- ▶ Syslog Explorer
- ▶ IPv6 TSPC Status
- External Devices

4.17.1 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 Triggered 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 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 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

Decoded Format:

0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)

Each item is explained as follows:

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.

4.17.2 Routing Table

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

[Diagnostics >> View Routing Table](#)

Current Running Routing Table		IPv6 Routing Table		Refresh	
Key: C - connected, S - static, R - RIP, * - default, ~ - private					
*	0.0.0.0/ 0.0.0.0	via 172.16.1.1		WAN1	
C~	192.168.1.0/ 255.255.255.0	directly connected		LAN1	
C	172.16.0.0/ 255.255.0.0	directly connected		WAN1	

[Diagnostics >> View Routing Table](#)

Current Running Routing Table		IPv6 Routing Table			Refresh	
Destination	Interface	Flags	Metric	Next Hop		
FE80::/64	LAN	U	256			
FF00::/8	LAN	U	256			

Each item is explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.17.3 ARP Cache Table

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

[Diagnostics >> View ARP Cache Table](#)

Ethernet ARP Cache Table | [Clear](#) | [Refresh](#) |

IP Address	MAC Address
192.168.1.10	00-0E-A6-2A-D5-A1
172.16.3.112	00-40-CA-6E-56-BA
172.16.3.132	00-05-5D-E4-ED-86
172.16.3.20	00-0D-60-6F-83-BC
172.16.3.121	00-0C-6E-E7-79-99
172.16.3.141	00-11-2F-C7-39-0B
172.16.3.133	00-50-7F-23-4D-B1
172.16.3.179	00-11-2F-4E-15-F2
172.16.3.21	00-05-5D-A1-2B-FF
172.16.3.2	00-11-D8-68-0D-AE
172.16.3.18	00-50-FC-2F-3D-17
172.16.3.151	00-50-7F-2F-33-FF
172.16.3.19	00-0D-60-6F-89-CA

Each item is explained as follows:

Item	Description
Clear	Click it to clear the whole table.
Refresh	Click it to reload the page.

4.17.4 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 Neighbour Table | [Refresh](#) |

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	00-00-00-00-00-00	USB2	CONNECTED
FF02::1:2	00-00-00-00-00-00	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	00-00-00-00-00-00	USB2	CONNECTED
FF02::16	33-33-00-00-00-16	LAN	CONNECTED

Each item is explained as follows:

Item	Description
Refresh	Click it to reload the page.

4.17.5 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.

[Diagnostics >> View DHCP Assigned IP Addresses](#)

DHCP IP Assignment Table		DHCPv6 IP Assignment Table			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-48-79 66:48:43		carrie-0c7cb251	
2	192.168.1.11	CC-F3-A5-02-9F-06 49:42:04		android_b4636b55c154acb4 a"lêß	
3	192.168.1.12	7C-61-93-18-EA-DF 68:02:44		android_807f1d0bfff92630 ðP "¼	
4	192.168.1.13	A0-F4-50-1C-94-BD 71:56:12		Android_358968044568596	
5	192.168.1.14	68-09-27-BE-CF-22 70:35:08		Vivian-iPhone	
6	192.168.1.15	F0-DC-E2-42-24-C7 67:58:32		Hua-iPhone	
7	192.168.1.24	70-DE-E2-E5-EF-80 50:07:04		iPad	
8	192.168.1.133	00-0E-2E-44-68-A8 51:01:02		ubuntukyeh	
9	192.168.1.1	00-50-7F-CE-46-FC			
DMZ Port : 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](#)

DHCP IP Assignment Table		DHCPv6 IP Assignment Table		Refresh
DHCPv6 server binding client:				
Index	IPv6 Address	MAC Address	Leased Time	

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.

4.17.6 NAT Sessions Table

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

[Diagnostics >> NAT Sessions Table](#)

NAT Active Sessions Table

| [Refresh](#) |

Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface
192.168.1.10	1032	34440	216.156.209.25	8888	WAN2
192.168.1.10	1032	34440	208.91.112.195	8888	WAN2
192.168.1.10	1032	34440	174.137.33.91	8888	WAN2
192.168.1.10	1033	34441	208.91.112.195	8888	WAN2
192.168.1.10	1033	34441	216.156.209.25	8888	WAN2
192.168.1.10	1034	34442	216.156.209.25	8888	WAN2
192.168.1.10	1034	34442	208.91.112.195	8888	WAN2
192.168.1.10	1034	34442	174.137.33.91	8888	WAN2
192.168.1.10	1057	34465	61.64.70.126	5653	WAN2
192.168.1.10	1871	35279	207.46.125.36	1863	WAN2
192.168.1.10	2458	35866	118.168.178.13	34542	WAN2
192.168.1.10	2460	35868	218.161.51.137	2625	WAN2
192.168.1.10	2461	35869	115.165.232.72	10465	WAN2

Each item is explained as follows:

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.

4.17.7 DNS Cache Table

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

The record of domain Name and the mapping IP address for answering the DNS query from LAN will be stored on Vigor router's Cache temporarily and displayed on **Diagnostics >> DNS Cache Table**.

Diagnostics >> DNS Cache Table

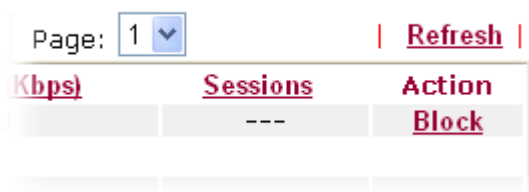

IPv4 DNS Cache Table		IPv6 DNS Cache Table		Clear	Refresh
Domain Name	IP Address	TTL (s)			

Note: The LAN DNS entry's TTL is static.

When an entry's TTL is larger than s, this entry will be deleted from the table.

Available settings are explained as follows:

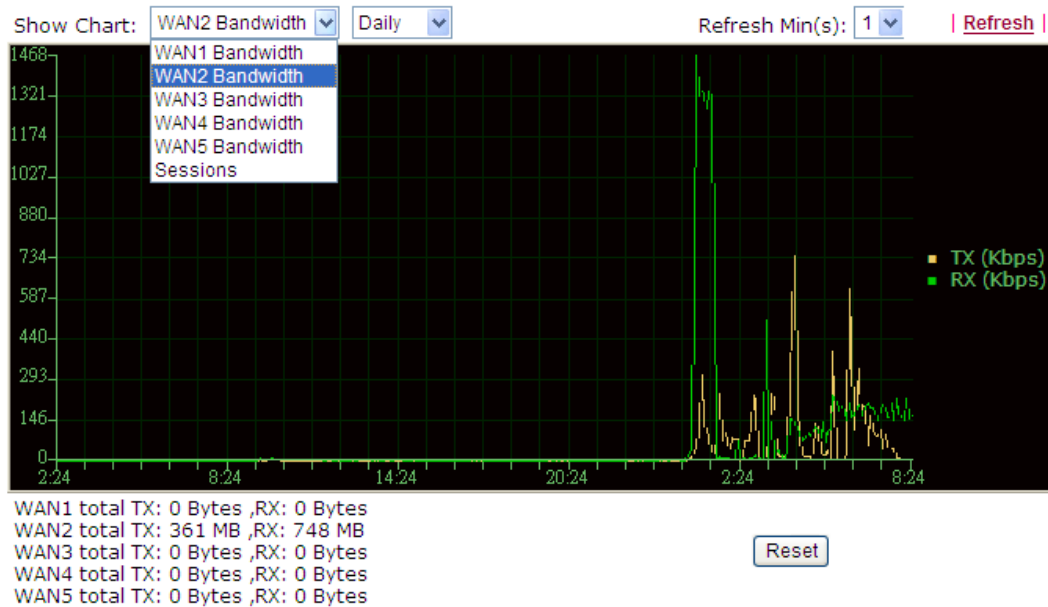
Item	Description
Clear	Click this link to remove the result on the window.
Refresh	Click it to reload the page.
When an entry's TTL is larger than....	Check the box the type the value of TTL (time to live) for each entry. Click OK to enable such function. It means when the TTL value of each DNS query reaches the threshold of the value specified here, the corresponding record will be deleted from router's Cache automatically.

Item	Description
	<p>automatically.</p> <p>Refresh Seconds: <input type="text" value="10"/> <input type="button" value="v"/> <input type="text" value="10"/> <input type="text" value="15"/> <input type="text" value="30"/></p>
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	<p>Block - can prevent specified PC accessing into Internet within 5 minutes.</p>  <p>Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.</p> 
APP QoS	Use the drop down list to change the priority in data transmission for the specified IP address (host)
Current /Peak/Speed	<p>Current means current transmission rate and receiving rate for WAN interface.</p> <p>Peak means the highest peak value detected by the router in data transmission.</p> <p>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.</p>

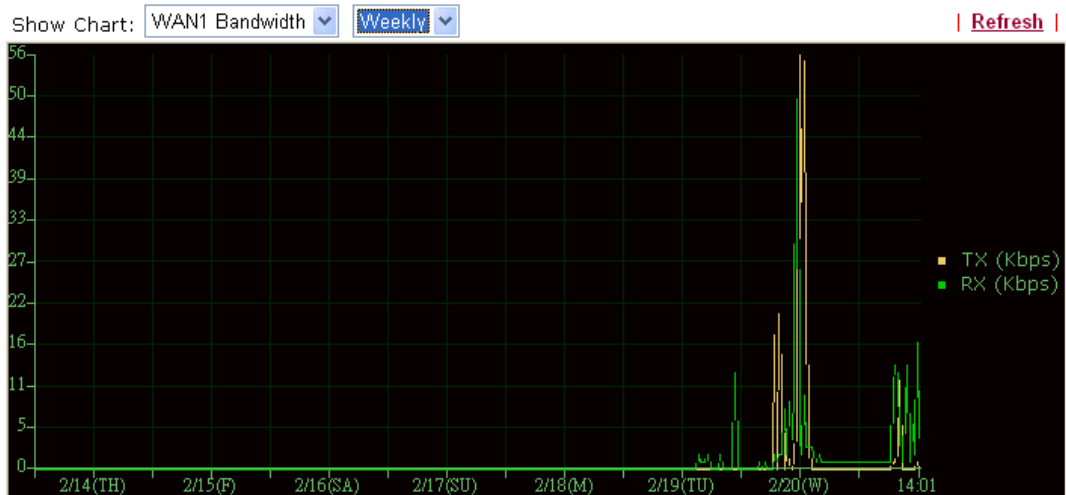
4.17.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to open the web page. Choose WAN1/WAN2/WAN3/WAN4/WAN5 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Reset** to zero the accumulated RX/TX (received and transmitted) data of WAN. Click **Refresh** to renew the graph at any time.

Diagnostics >> Traffic Graph



Diagnostics >> Traffic Graph



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

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

4.17.10 Ping Diagnosis

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

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

IPV4
 IPV6

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping through:

Ping to: IP Address:

Result | [Clear](#) |

Host / IP

DNS

Gateway 1

Gateway 2

Gateway 3

Gateway 4

Gateway 5

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

IPV4
 IPV6

Ping IPv6 Address:

Result | [Clear](#) |

Each item is explained as follows:

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.

4.17.11 Trace Route

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

[Diagnostics >> Trace Route](#)

Trace Route

IPv4 IPv6

Trace through:

Protocol:

Host / IP Address:

Result | [Clear](#)

[Diagnostics >> Trace Route](#)

Trace Route

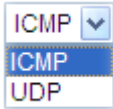
IPv4 IPv6

Trace Host / IP Address:

Result | [Clear](#)

Each item is explained as follows:

Item	Description
Trace through	Use the drop down list to choose the WAN interface that you want to ping through.
Protocol	Use the drop down list to choose the protocol that you want to

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

4.17.12 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

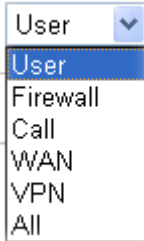
For Web Syslog

This page displays the time and message for User/Firewall/call/WAN/VPN settings. You can check **Enable Web Syslog**, specify the type of Syslog and choose the display mode you want. Later, the event of Syslog with specified type will be shown for your reference.

[Diagnostics >> Syslog Explorer](#)



Available settings 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. 
Export	Click this link to save the data as a file.
Refresh	Click this link to refresh this page manually.
Clear	Click this link to clear information on this page.
Display Mode	There are two modes for you to choose.

	<div style="border: 1px solid black; padding: 2px;"> Stop record when fulls ▼ Stop record when fulls Always record the new event </div> <p>Stop record when fulls – when the capacity of syslog is full, the system will stop recording.</p> <p>Always record the new event – only the newest events will be recorded by the system.</p>
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.

[Diagnostics >> Syslog Explorer](#)

Web Syslog	USB Syslog	
<p>Note:The syslog will show while the saved syslog file size is over 1MB. Folder: n/a File: n/a Page: n/a Log Type: n/a</p>		
Time	Log Type	Message

Available settings are 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.

4.17.13 IPv6 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 Enabled					
TSPC Connection Status					
Local Endpoint v4 Address :		1.169.155.138			
Local Endpoint v6 Address :		2001:05c0:1400:000b:0000:0000:0000:b527			
Router DNS name :		vigor2850.broker.freenet6.net			
Remote Endpoint v4 Address :		81.171.72.11			
Remote Endpoint v6 Address :		2001:05c0:1400:000b:0000:0000:0000:b526			
Tspc Prefix :		2001:05c0:1513:5900:0000:0000:0000:0000			
Tspc Prefixlen :		56			
Tunnel Broker :		amsterdam.freenet6.net			
Tunnel Status :		Connected			

Available settings are explained as follows:

Item	Description
Refresh	Click this link to refresh this page manually.

4.18 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 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.

5

Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

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

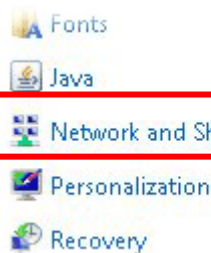
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is still failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

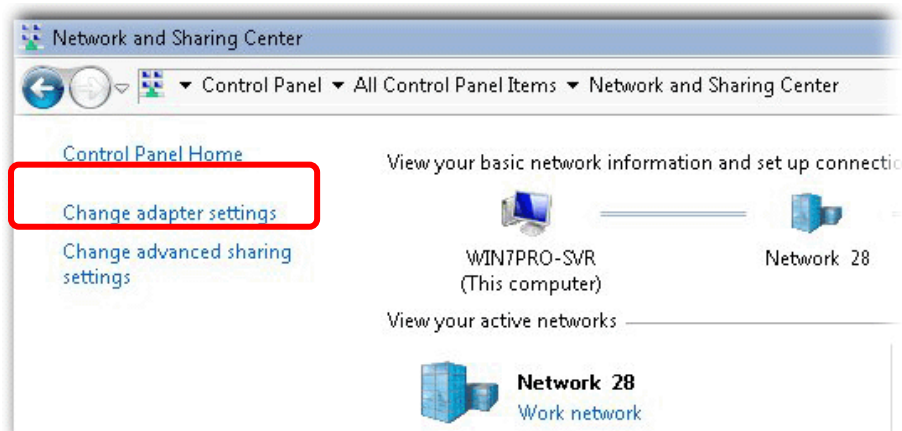


The example is based on Windows 7. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.DrayTek.com.

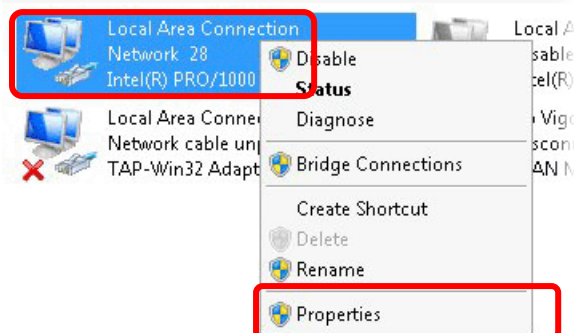
1. Open **All Programs>>Getting Started>>Control Panel**. Click **Network and Sharing Center**.



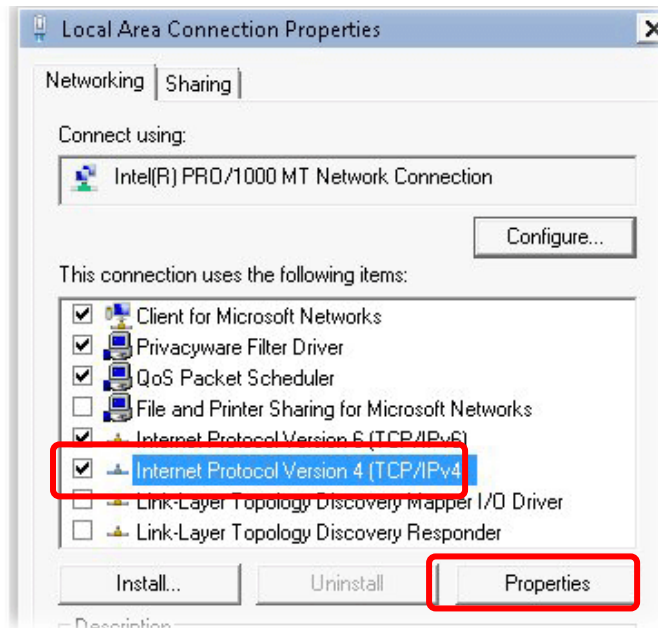
2. In the following window, click **Change adapter settings**.



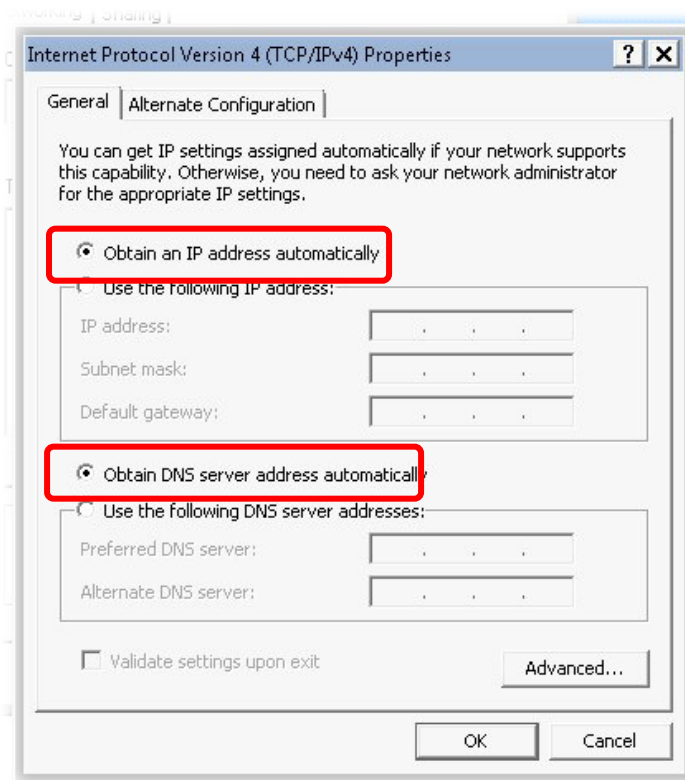
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

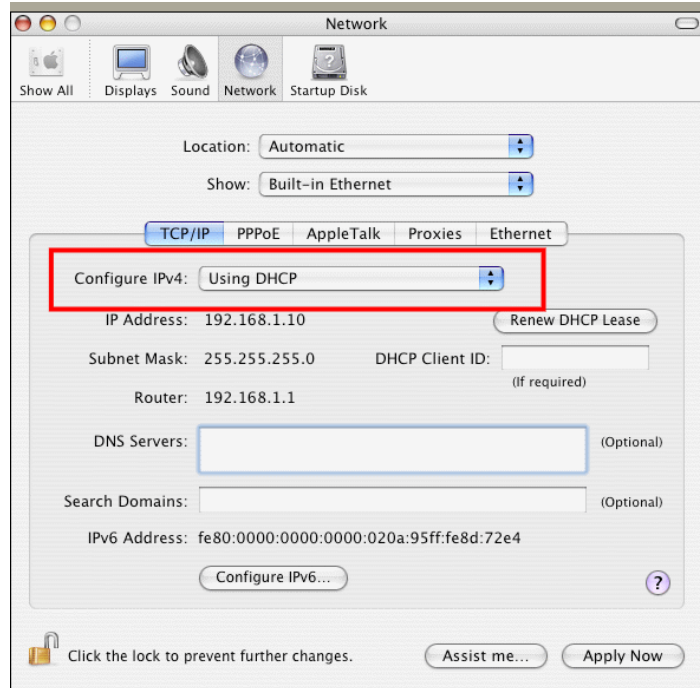


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



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.



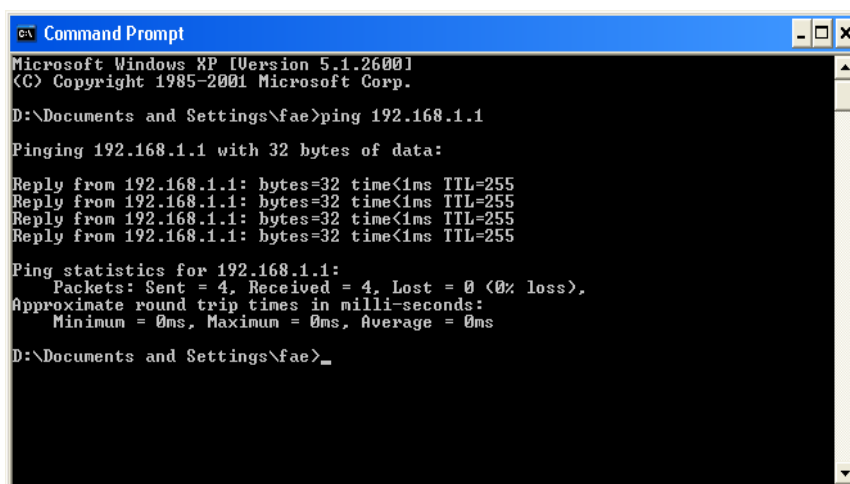
5.3 Pinging the Router from Your Computer

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/7). The DOS command dialog will appear.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

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.

```

Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

```

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

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.

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.

The screenshot displays the DrayTek Syslog Utility interface. At the top, the DrayTek logo is on the left and 'Syslog Utility' is on the right. Below the logo is a navigation bar with icons for various system functions. The main area is divided into several sections:

- Log Filter:** Includes a 'Keyword:' field, an 'Apply to:' dropdown set to 'All', and a 'Refresh' button.
- WAN Information:** Shows the WAN IP address as 172.16.3.130. It also has fields for TX Rate, RX Rate, WAN IP, and Gateway IP.
- LAN Information:** Includes fields for TX Packets and RX Packets.
- Navigation Tabs:** 'Firewall', 'VPN', 'User Access', 'Connection', 'WAN' (selected), 'IPPEX', and 'Others'.
- Display Options:** Radio buttons for 'Show Syslog List' (selected) and 'Show Traffic Graph', along with a 'Pause' checkbox.
- Syslog List Table:** A table with columns for System Time, Router Time, Host, and Message. The messages include session statistics and USB device connection details.

System Time	Router Time	Host	Message
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: Session Usage: 123 (5 min average)
2013-08-27 15:11:09	Aug 27 07:10:53	Vigor-router	statistic: WAN1: Tx 81 Kbps, Rx 12 Kbps (5 min average)
2013-08-27 15:10:07	Aug 27 07:09:51	Vigor-router	[USB]Host Controller Driver: OTG
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=82 (in), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]EndpointAddress=01 (out), Attributes=02 (Bulk)
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Mass Storage device class
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface Class:SubClass:Protocol = [08:06:50]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Interface: 0
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Per-interface classes
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Device Class:SubClass:Protocol = [00:00:00]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]SerialNumber:[3] ED96E018
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Product:[2] Mass Storage
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Manufacturer:[1] Generic
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Usb new device: Vendor ID [058F], Product ID: [6387]
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]num of interfaces=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]usb_set_configuration: configuration=1
2013-08-27 15:10:06	Aug 27 07:09:51	Vigor-router	[USB]Usb Device Connected at Port 0

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.



Warning: After pressing **factory default setting**, you will lose 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 ?

- Using current configuration
- Using factory default configuration

Reboot Now

Auto Reboot Time Schedule

Index(1-15) in **Schedule** Setup: , , ,

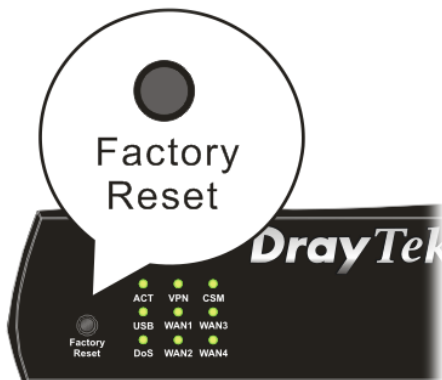
Note: Action and Idle Timeout settings will be ignored.

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 DrayTek

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.